HACKERS
Standard Guide Book

ခေတ်မင်းသိုး

လူမိုက်လုလု

အခြေခံ Hacking နည်းပညာ

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

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 ပိုင်းရပ်များ 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 အမျိုးအစားခွဲခြားကြပါတယ်။ 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၊

ကွန်ပျူတာပိုင်းရပ်တွေကို 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 စိတ်မဝင်စားလျင်တောင်မှ 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

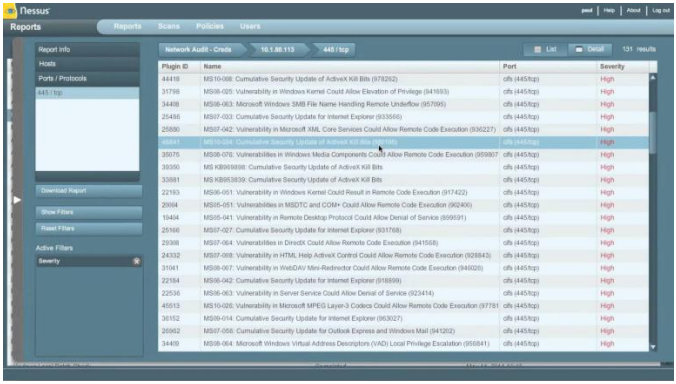
Ethical Hacking , Penetration Testing နဲ့ White Hat Hacking တို့ဟာ ခေါ်ဝေါ်သုံးစွဲမှုခြင်း ကွဲပြားပေမယ့် ဆိုလိုရင်းက တူညီကြပါတယ်။ Hacking ကို လုပ်ဆောင်တဲ့နေရာမှာ Ethic ဆိုတဲ့ ကိုယ်ကျင့်တရား စံနှုန်းတစ်ခု ပေါင်းစပ်လိုက်တဲ့အခါ Ethical Hacking ဆိုတာ ဖြစ်ပေါ်လာပါတယ်။

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။ ဒါ့ပြင် 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 တုပ လုပ်ဆောင်ခြင်းဖြစ်ပြီး 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 ဘာတစ်ခုကိုမျှ 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 ရှာဖွေ ဖော်ပြပေးနိုင်ပါတယ်။ 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 ယုံကြည်ရ လောက်သော သူက exploit ပြုလုပ်ခြင်းမျိုးပဲ ဖြစ်ပါတယ်။ အဲလို လုပ်ဆောင်နိုင်ဖို့အတွက် attacker တွေက target system ထဲမှာ ရှိနေတဲ့ ဝန်ထမ်းတွေကို အသုံးချနိုင်ဖို့ ကြိုးစားတတ်ကြပါတယ်။

အဲလို လုပ်ဆောင်နိုင်ဖို့အတွက်လည်း Social Engineering ကို အသုံးပြုလေ့ရှိပါတယ်။ တိုက်ခိုင်မှုတစ်ခု 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 တိုက်ခိုက်လာလျင် 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 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။

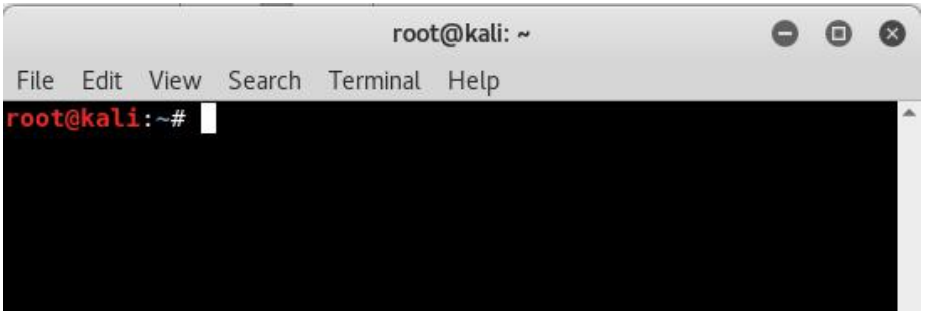
Hierarchical tree ရဲ့ starting point ကိုတော့ root လို့ ခေါ်ပြီး သင်္ကေတအနေနဲ့ 'မျဉ်းစောင်း' " / " ကို အသုံးပြုပါတယ်။ "root" directory ထဲမှာ sub-directories (directory ခွဲ) များစွာ ပါဝင်ပါတယ်။ ဥပမာ root ဆိုတဲ့ directory ထဲက home ဆိုတဲ့ directory ကို သင်္ကေတနဲ့ ဖော်ပြရင် /root/home ကဖြစ်ပါတယ်။ directory 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။ ဒါပြင် 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။

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 # သင်္ကေတကတော့ 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။

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။ အဲသည်အတွက် 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#
```

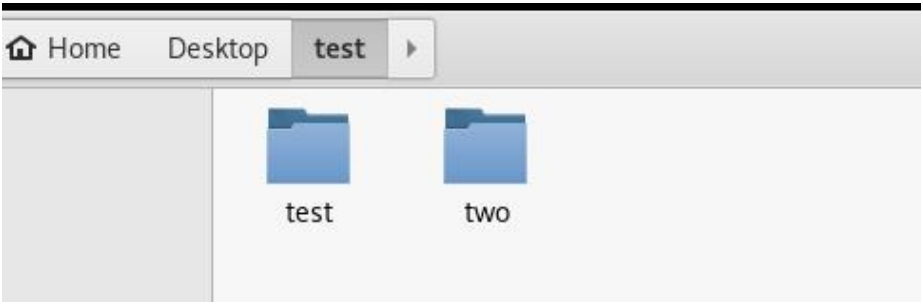
အထက်ပါ ပုံမှာ test ဆိုတဲ့ dir တစ်ခု ထပ်တိုးလာတာကို တွေ့ရမှာပါ။ cd ကို သုံးပြီး ထပ်ဝင်လိုက်ရအောင်။ cd test နဲ့ ဝင်ရောက်လိုက်တဲ့အခါ test folder ထဲကို ဝင်ရောက်ပြီး ဖြစ်တာ တွေ့ရပါမယ်။

```
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#
```

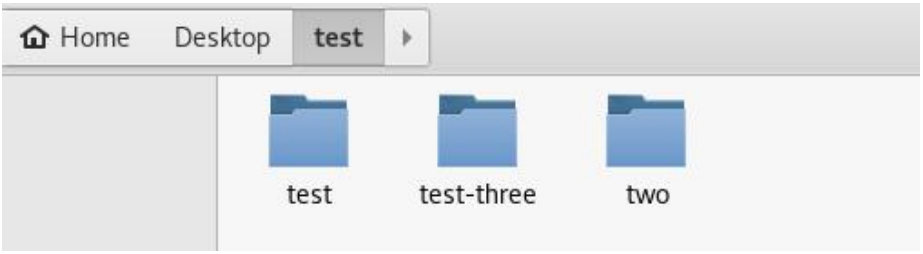
အထက်ပါ ပုံအရ Desktop ပေါ်က test directory ထဲမှာ test two ဆိုတဲ့ နာမည်နဲ့ folder တစ်ခု တည်ဆောက်တာဖြစ်ပါတယ်။ ဒါပေမယ့် ခုချိန်မှာ Desktop ပေါ်မှာရှိတဲ့ test folder ကို ဖွင့်ကြည့်မယ်ဆိုရင်တော့



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#
```

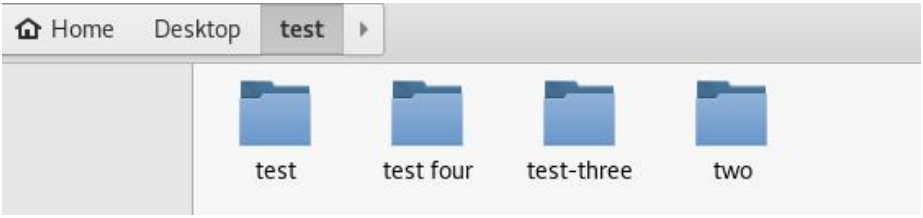
ကျွန်တော်က mkdir test-three ဆိုပြီး အထက်ပါ ပုံအတိုင်း နောက်တစ်ခု ဖန်တီးကြည့်ပါတယ်။



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@                                  root@kali:
File  Edit  View  Search  Terminal  Help   File  Edit  View  Search  Terminal  Help
root@kali:~# cd Desktop                root@kali:~# cd Desktop/test/two
root@kali:~/Desktop# ls                root@kali:~/Desktop/test/two#
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 ပုံတွင်ကြည့်လျင် cd command ကိုသုံးပြီး တစ်ဆင့်စီ

ဝင်ရောက်ခြင်း နှင့် cd command ဖြင့် တိုက်ရိုက်ဝင်ရောက်ခြင်း တို့ရဲ့ ကွာခြားမှုကို တွေ့မြင်နိုင်ပါတယ်။

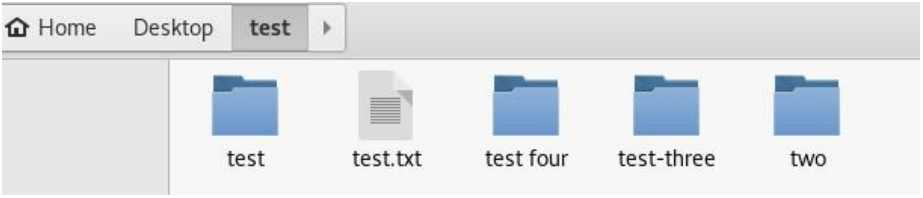
ဒီခါတော့ စာရိုက်တဲ့အပိုင်းကို ဆက်ရအောင်ပါ။ terminal တွေ ရှုပ်မနေရအောင် ခုန ဖွင့်ထားတာတွေကို ပိတ်လိုက်ပြီး အသစ်ပြန်ဖွင့်လိုက်ရအောင်။ ပြီးရင် Desktop ပေါ်က test ဆိုတဲ့ folder ထဲ ဝင်ထားလိုက်ပါ။ ဒီနေရာမှာ နည်းနည်းလေး ပြောလိုတာက ကျွန်တော်တို့ သုံးမယ့် Kali Linux မှာ Pop-up (GUI) အနေနဲ့ အသုံးပြုနိုင်တဲ့ စာရိုက်နိုင်တဲ့ 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။

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

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 ရှာတာတွေ့မှာမဟုတ်ပါဘူး။ 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 ယူဆ ပါတယ်။ 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။

ပို၍ရှင်းအောင် 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 စတင် အသုံးပြုတဲ့အချိန်နဲ့ 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 နိုင်ပါတယ်။ 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။

```
root@kali:~# apt upgrade -y
```

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 များပြားလာတဲ့အခါမှာတော့ 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) ကြားခံသုံးပါတယ်။ 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။

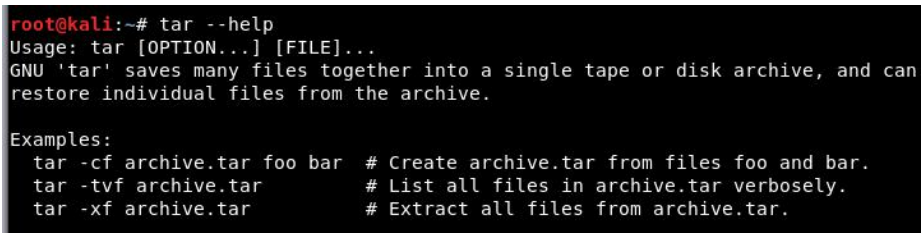
```
root@kali:~/Desktop/a# rm 1.txt
root@kali:~/Desktop/a# rm 2.txt
root@kali:~/Desktop/a# ls
test2.tar.gz  test.tar.gz
```

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 ပြထားပါတယ်။ ls ဖော်ကြည့်တဲ့အခါ tar ထဲ ထည့်ထားတဲ့ ဖိုင်နှစ်ခု ပြန်တွေ့ရပါပြီ။ file list ပါ ကြည့်ရင်း ပြန်ဖော်ချင်ရင်တော့ tar -xvf ကို အသုံးပြုနိုင်ပါတယ်။

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



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 ဖော်ပြဆွေးနွေးပေးခဲ့တာ 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 ကျွန်တော်ရဲ့ 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 မသက်ဘဖွယ် အုပ်စု (group) တစ်ခုကို တွေ့တယ်ဆိုကြပါစို့။ ကျွန်တော်တို့က ဥပဒေဘက်တော်သားတွေ အနေနဲ့ တွေးကြည့်ရအောင်။ ပထမဆုံး ဘာလုပ်မလဲ။ ထို အုပ်စုကို တိုက်ရိုက် သွားဖမ်းမလား။ ဒီနေရာမှာ ကျွန်တော်တို့စဉ်းစားရမှာက ဘာအချက်အလက်မှ ရှိမထားဘဲနဲ့ သွားဖမ်းရင် ကိုယ့်ရှုးကိုယ်ပတ်ပြီး ကိုယ့်ဘက် မြားဦးပြန်လည်လာမှာဖြစ်သလို အရေးကြီးသော ကွင်းဆက်တွေပါ ပြတ်သွားမှာဖြစ်ပါတယ်။

ဒီတော့ ကျွန်တော်တို့ ဘာလုပ်ကြမလဲ။ ထို မသက်ဘဖွယ်အုပ်စုကို 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 လုပ်ဆောင်မယ် ဆိုပါက 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

ရန်သူနယ်မြေနဲ့ ကပ်လျက်ရှိတဲ့ တောင်ပူစာလေးပေါ်မှာ ရောက်ရှိနေတဲ့ စစ်သားတစ်ယောက်ကို မြင်ယောင်ကြည့်ပါ။ Only one နော်။ သူ့လက်ထဲမှာ လမ်းညွှန် မြေပုံညွှန်းတစ်ခု 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 ဆက်လက် ဖော်ပြပေးသွားပါမယ်။

Phase 3. Exploitation

တကယ့် စစ်သားတွေအတွက်တော့ ဒီအဆင့်မှာ တိုက်ခိုက်နေတာလည်း ဖြစ်ကောင်း ဖြစ်နေနိုင်ပါတယ်။ ဒါပေမယ့် Ethical Hacking မှာတော့ အနည်းငယ် ပုံစံ ပြောင်းလိုက်ရအောင်။ ဒီအဆင့်မှာတော့ စောစောက ပြောခဲ့တဲ့ စစ်သားလေးဟာ မှိန်ပျပျလရောင် နဲ့ အုံနေတဲ့ တိမ်တိုက်တွေကို အကာအကွယ်ယူပြီး ရန်သူ့စခန်း စည်းရိုးအနားကို 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 ရန်သူစခန်းထဲ ဖောက်ဝင်နိုင်ခဲ့တဲ့ စစ်သားလေးရဲ့ အတွေ့အကြုံနဲ့ ရေးဆွဲထားတဲ့ ပုံတွေအရ ကျွမ်းကျင်တဲ့ အင်ဂျီနီယာတွေဟာ ပင်မ အဆောက်အဦ ရဲ့ အချက်အချာအကျဆုံးအခန်း အောက်တည့်တည့်ထိ မြေအောက်ကနေ ဥမင်လှိုက်ခေါင်း 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 သတင်းအချက်အလက်မှန်သမျှကို 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 ဒီသုံးခုက 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 ပြင်ပ လူတွေဆီကနေ 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။ ထို အလုပ်ခေါ်စာတွေမှာ 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 ဖော်ပြချက်မျိုးဟာ 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။


```
root@kali:~# ls
apt-remove-duplicate-source-entries.py  index.html  VirtualBox VMs
backblue.gif                            Music       vmware
cs                                      n           w3af
Desktop                                 Pictures    webmitm.crt
Documents                               pipewire    websites
Downloads                               Public      wget-log
fade.gif                                Templates   www.bible-history.com
```

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။

```
root@kali:~# man wget
```

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 ပြောင်းဆွေးနွေးရအောင်။

Google Search

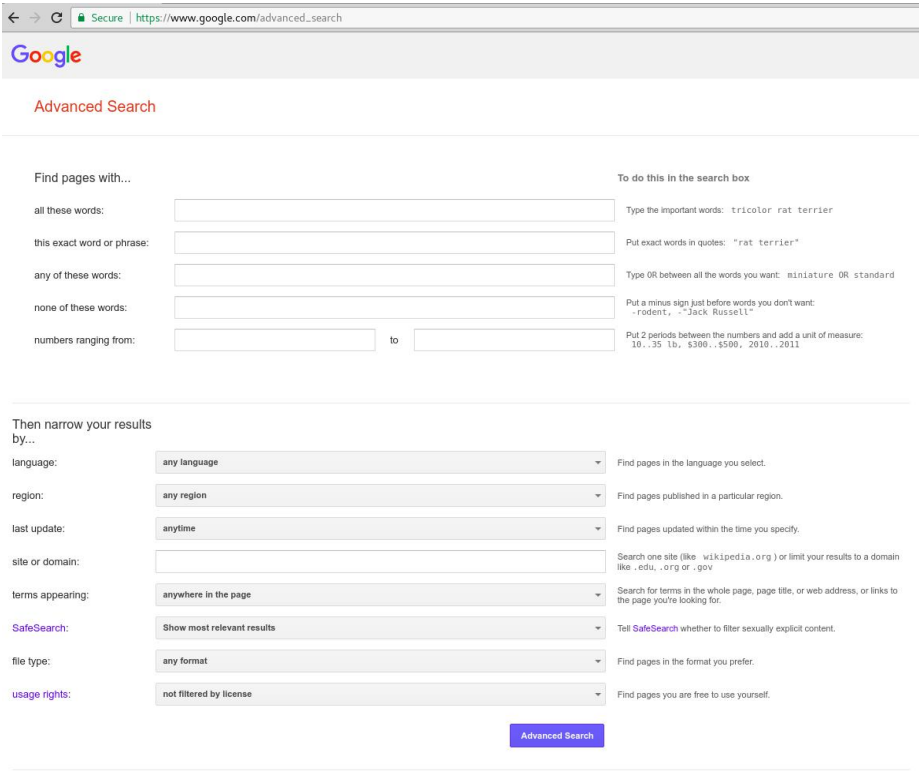
ဒီခါတော့ ကျွန်တော်တို့ အများစု အသုံးမပြုဖြစ်ကြတဲ့ google search အကြောင်းလေး ဆွေးနွေးပါမယ်။ Google Search များ ငါတို့ သုံးနေကျပါကွာလို့ ပြောချင်တဲ့သူလည်း ရှိကောင်း ရှိပါလိမ့်မယ်။ ကဲ ကြည့်ရအောင်နော်။

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 လက်ကိုင်မှန်ဘီလူးပိုင်း ကလေးကို 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 သာလျင် 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။

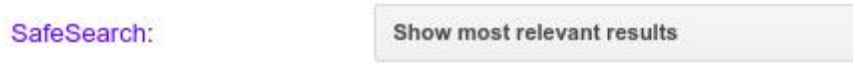
ရှာဖွေတဲ့အခါ result တွေ သိပ်များနေမှာစိုးရင် site or domain ကနေ ကန့်သတ်နိုင်ပါသေးတယ်။ ဥပမာ wikipedia.org စသည်ဖြင့်ပေါ့။ ပုံမှန် search

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

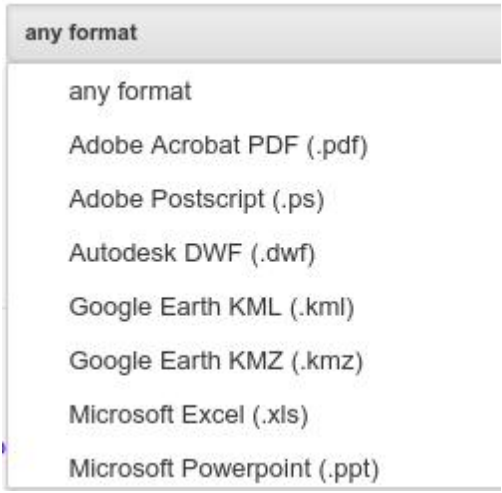
နောက်တစ်ခုက terms appearing ပါ။ အဲသည်မှာ ရွေးချယ်စရာတွေ ထဲက ပထမတစ်ခုက "anywhere in the page" ပါ။ ပုံမှန်ရှာဖွေသလိုပဲ ရှာဖွေတဲ့အကြောင်းအရာ ဘယ်နေရာမှာပါပါ result လာပေါ်ပြမှာ ဖြစ်ပါတယ်။ နောက်တစ်ခု "in the title of the page" ကတော့ ကျွန်တော်တို့ ရှာဖွေမယ့် အကြောင်းအရာသည် title နေရာမှာ ရှိနေတာတွေကိုပဲ ထုတ်ပြပါ 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

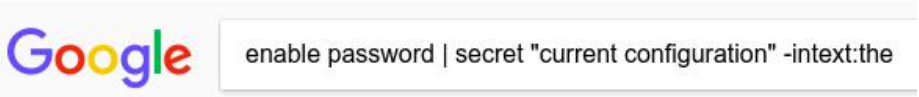
ဒီခေါင်းစဉ်လေးကိုတော့ အားလုံး သိကြ ရင်းနှီးကြလိမ့်မယ်လို့ ယူဆပါတယ်။ Johnny Long က စတင်တီထွင်ခဲ့ပြီး Google operators & terms တွေကို Google Search engine နဲ့ ပေါင်းစပ်ပြီး အလွန်တန်ဖိုးရှိတဲ့ အချက်အလက်တွေကို အင်တာနက်မှ တစ်ဆင့် ရရှိနိုင်စေဖို့ ဖန်တီးထားတဲ့ နည်းပညာတစ်ခု ဖြစ်ပါတယ်။ People & organizations 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 အတော် နည်းပါသေးတယ်။ 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 ရည်ညွှန်းတယ်ဆိုတာ တော့ အားလုံးနီးပါး သိကြပြီးဖြစ်ပါတယ်။ Google ကို google.com လို့ မှတ်ရတာက 173.194.46.19 လို့ မှတ်ရတာထက် ပိုမိုလွယ်ကူပြီး မှတ်မိနိုင်တာကြောင့် ကျွန်တော်တို့တွေက DNS ကို အသုံးပြုကြတယ်ဆိုတာကိုလည်း အားလုံး သိရှိပြီး ဖြစ်ပါတယ်။ 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။

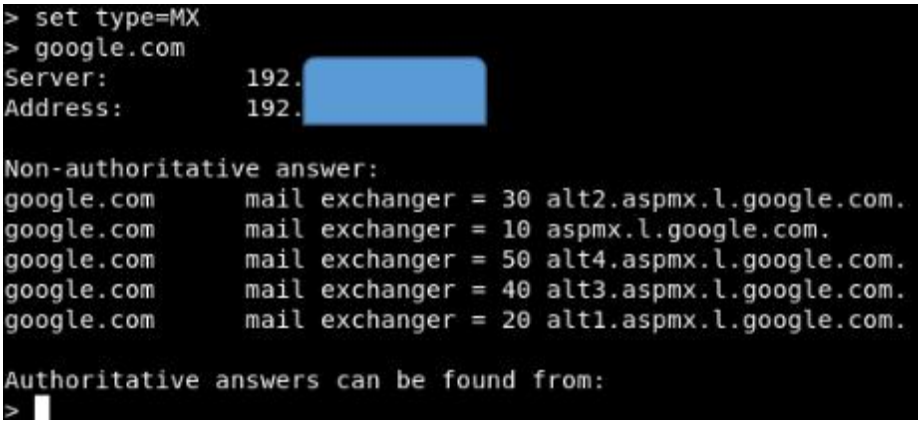
nslookup ထဲ ပြန်ဝင်ကြည့်ရအောင်။ Terminal မှာ nslookup လို့ ရိုက်ပြီး enter လိုက်ပါ။

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

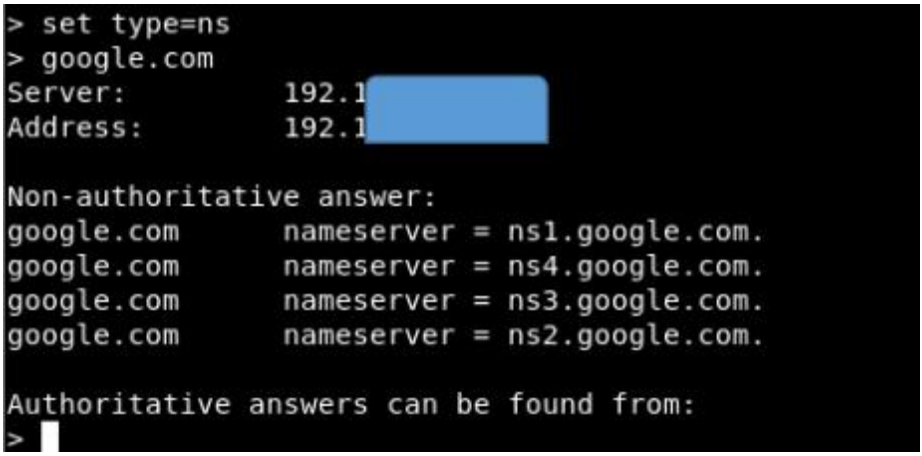
authoritative နဲ့ non-authoritative ဆိုပြီး နှစ်မျိုး ဖော်ပြတာကို တွေ့ရပါမယ်။ Non-authoritative answer သည် server's cache တွေရဲ့ information တွေကို ညွှန်ပြနိုင်တာဖြစ်လို့ သိပ်ကောင်းတဲ့ information source လို့ ဆိုနိုင်ပါတယ်။ ပြန်မထွက်သေးဘဲ နောက်ထပ် ထပ်ဆက်ရှာကြည့်ရအောင်ဗျ။

>set type=MX

>google.com



Google.com အတွက် Mail server တွေကို တွေ့မြင်ရပြီနော်။



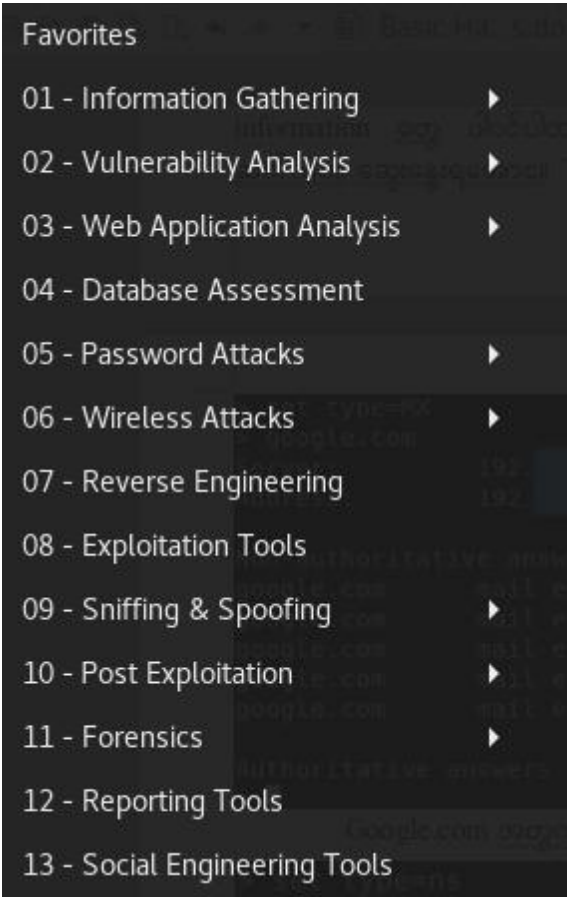
set type=ns သတ်မှတ်ပေးပြီး Google.com ကို ပြန်ရိုက်လိုက်တဲ့အခါ google ရဲ့ name server (ns) တွေကို တွေ့မြင်လာရပြီ ဖြစ်ပါတယ်။

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။

[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

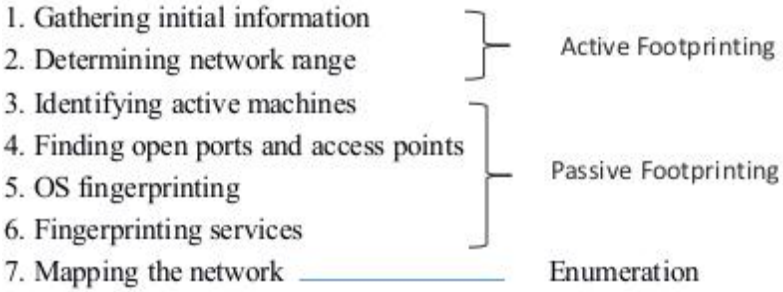


Information Gathering နဲ့ ပတ်သက်ပြီး Kali Linux မှာ build-in tools တွေ များစွာ ရှိကြပါတယ်။ DNS Analysis, IDS/IPS Identification, Live Host Identification, Network & Port Scanner, OSINT Analysis, Route Analysis, SMB Analysis, SMTP Analysis, SNMP Analysis နဲ့ SSL Analysis ဆိုပြီး ခွဲခြားထားတဲ့ tool group 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 စုဆောင်းတဲ့ နေရာမှာ 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။

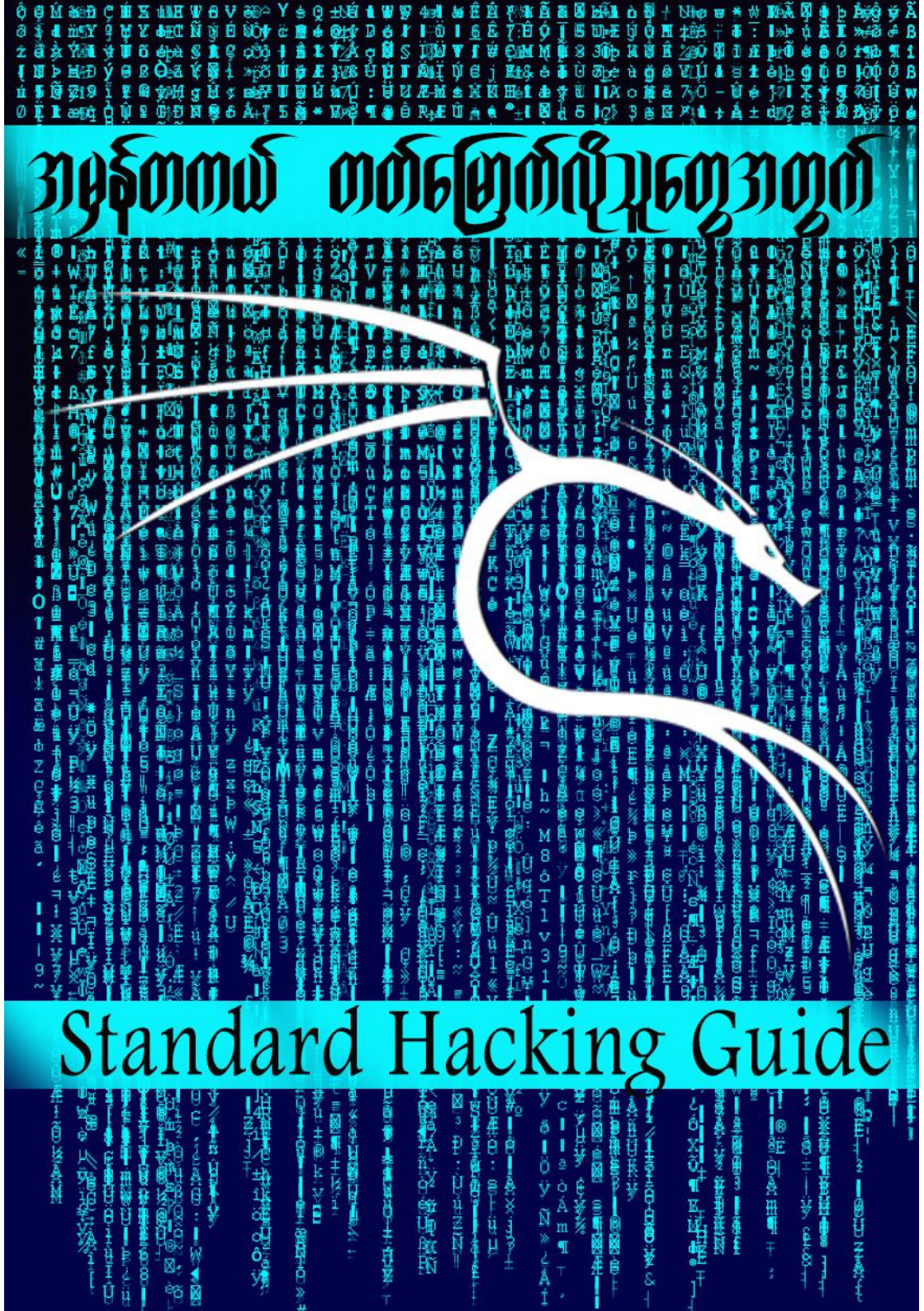
```
root@kali:~# host -t ns bible-history.com
bible-history.com name server ns57.domaincontrol.com.
bible-history.com name server ns58.domaincontrol.com.
root@kali:~# host -l bible-history.com ns57.domaincontrol.com
;; communications error to 216.69.185.29#53: end of file
;; communications error to 216.69.185.29#53: 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။ :)

အမှန်တကယ် တတ်မြောက်လိုသူတွေအတွက်



Standard Hacking Guide