

# Foundation of Cyber Security

Author - Han Niux



Myanmar Pentest Society

<https://mmpentestsociety.blogspot.com>

# အမှာစာ

ဒီစာအုပ်ကတော့ Cyber Security ကိုလေ့လာချင်တဲ့ သူတွေအတွက် ကိုရည်ရွယ်ပြီး အစကတော့ Free အနေနဲ့ပေးဖို့ရေးတာဖြစ်ပါတယ်။ ဒါပေမယ့် တော်လှန်ရေးကာလမှာ အခက်ခဲဖြစ်နေတဲ့သူတွက် ကူညီချင် တာကြောင့် စာဖတ်သူတို့ဆိုက အဆင်ပြေတဲ့ဈေးနဲ့ပဲ ရောင်းချပြီး ရတဲ့ ပိုက်ဆံတွက် တစ်ကယ်ခက်ခဲ နေတဲ့သူတွက်လူဒါန်းပေးသွားမှာဖြစ်ပါတယ်။ ဒီစာအုပ်ထဲမှာ ပါဝင် တဲ့ အကြောင်းရာတွေက CompTIA Security + စာအုပ်တို့မှုထုတ်နှုတ်ထားတာဖြစ်ပါတယ်။ ယခုစာအုပ်အား လေ့လာပြီး ပါက CompTIA Security + Exam ဖြေမယ့်သူတွေ အတွက် အထောက်ကူပြုမှာဖြစ်ပါတယ်။ ဒီစာအုပ်ဟာ Theory ပိုင်းကိုဌီးစားပေးရေးတာဖြစ်တဲ့ အတွက် အနည်းငယ်တော့ပျင်းဖို့ကောင်းမှာ အသေချာပဲဖြစ်ပါတယ်။ ဒါပေမယ့် basic level မှာ Theory ကိုကောင်းစွာနားလည်မှသာ တခြား level တွက်ဘူးတဲ့အခါ အဆင်ပြေမှာဖြစ်ပါတယ်။ Theory ဆိုပေမယ့်လဲ စာဖတ်သူတွေပျင်းမှာဆိုးလို့ short note ပုံစံမျိုးနဲ့ပဲရေးသားထားပါတယ်။

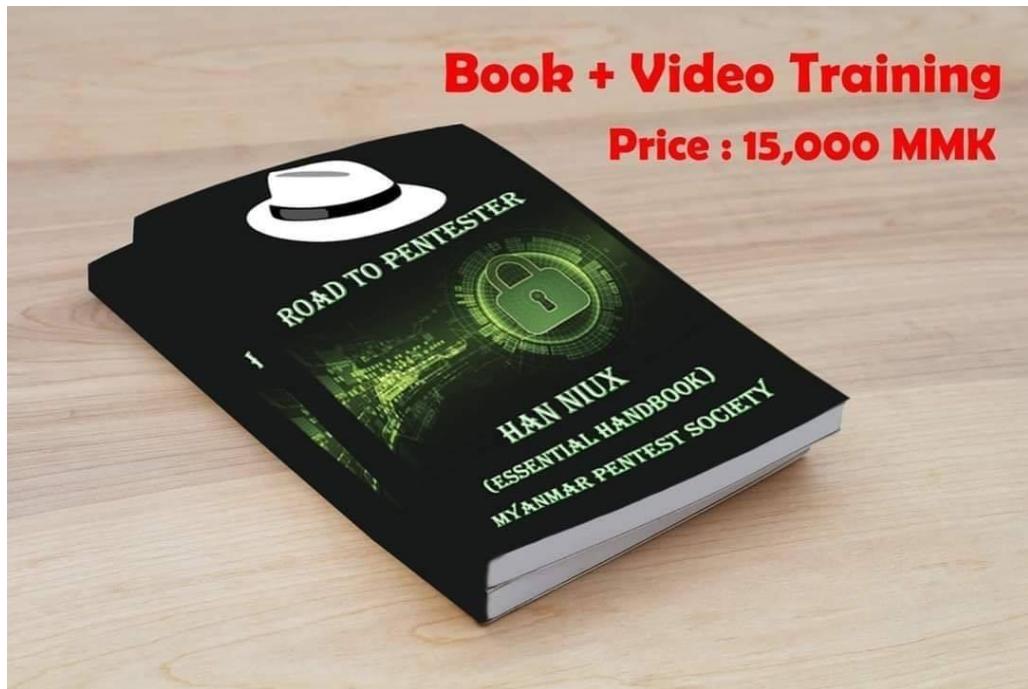
Han Niux

Myanmar Pентest Society

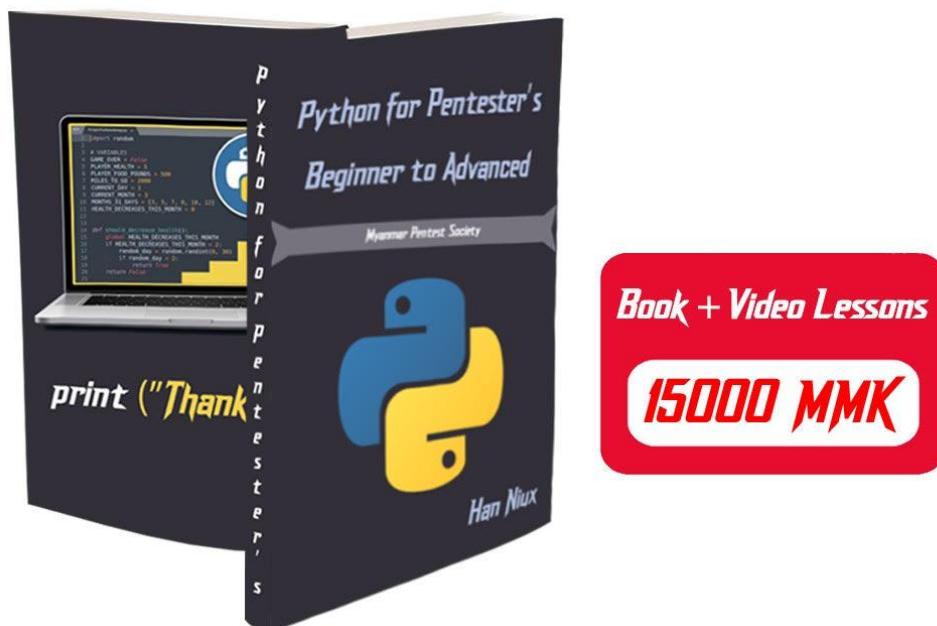
# စာရေးသူထုတ်ဝေခြင်းသော စာအုပ်များ

Penetration Testing ကိစ္စတင်လွှဲလာလိုသူများအတွက်

## 1) Road to Pentester



## 2) Python for Pentester's



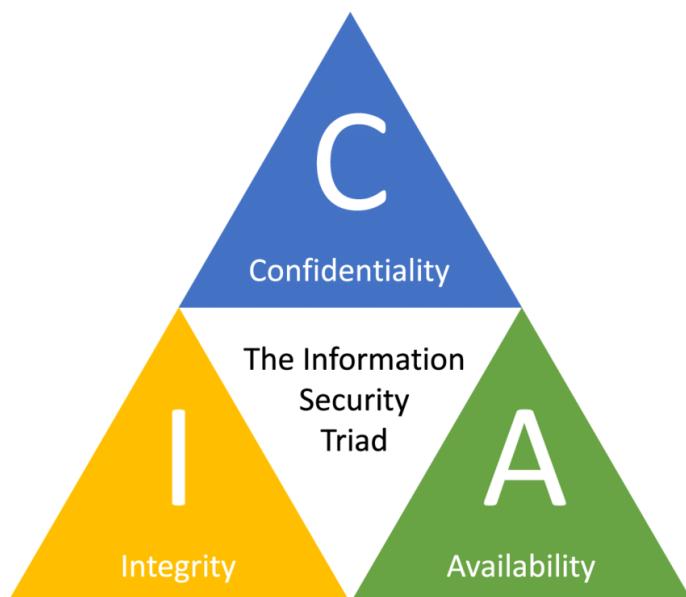
# Contents

Chapter 1 – Introduction to Cyber Security	Page – 1
Chapter 2 – Identity and access management (IAM)	Page – 25
Chapter 3 – Network Security	Page – 36
Chapter 4 – System Security	Page – 63
Chapter 5 – Application Security	Page – 93
Chapter 6 – Vulnerability and Risk Assessment	Page – 101
Chapter 7 – Monitoring and Auditing	Page – 126
Chapter 8 – Cryptography	Page – 148
Chapter 9 – Dealing with Incidents	Page – 162

## Chapter – 1

### Introduction to Cyber Security

Cyber Security ဆိုတာက Organizations တွေရဲ့ Sensitive Information, Resource, Access စတာတွေကို မသက်ဆိုင်တဲ့သူများ အလွယ်တကူဝင်ရောက် အသုံးပြုခြင့်မရအောင် လုပ်ဆောင်ရတာမျိုးကို ဆိုလိုတာဖြစ်ပါတယ်။ အမိကအနေနဲ့ CIA Triangle ကိုအခြေခံပြီးတော့ ကာကွယ်တာဖြစ်ပါတယ်။



#### What is CIA?

CIA ဆိုတာက Confidentiality, Integrity, Availability သုံးမျိုးကိုပေါင်းပြီး ခေါ်ဆိုတာဖြစ်ပါတယ်။ တစ်ခုချင်းစီအကြောင်းကိုဆက်ပြီးတော့လေ့လာကြည့်ရအောင်။

#### Confidentiality

Confidentiality ဆိုတာက Organization တွေရဲ့အရေးကြီးတဲ့ Secret Information တွေကို မသက်ဆိုင်တဲ့သူတွေမရရှိအောင် ကာကွယ်ရတာဖြစ်ပါတယ်။ ဥပမာပြောရရင် Username, Password တို့လိုမျိုးဖြစ်ပါတယ်။

## Integrity

**Integrity** ဆိုတာက Organization တွေရဲ့ Sensitive Data တွေကိုမသက်ဆိုင်တဲ့သူတွေက ဝင်ရောက်ပြုပြင်တာမျိုးတွေလုပ်ဆောင်လို့မရအောင် လုပ်ရတာကိုပြောတာဖြစ်ပါတယ်။ ဥပမာပြောရရင် Organization တွေရဲ့ Finical Information တွေကိုမသက်ဆိုင်တဲ့သူတွေက ပြုပြင်လို့မရအောင်လုပ်ဆောင်ရတာမျိုးဖြစ်ပါတယ်။ နောက်ပြီး files တွေကိုပြင်ထား/မထားဆိုတာကို hashing လုပ်ကြည့်ရပါတယ်။ တစ်ကယ်လို့ hash values တွေပြောင်းလဲနေတယ်ဆိုရင်တော့ files ကိုပြင်ထားတယ်လို့သတ်မှတ်လို့ရပါတယ်။

## Availability

**Availability** ဆိုတာက Organization တွေရဲ့ Sensitive Data တွေကိုတရားဝင် အသုံးပြုခွင့်ရှိတဲ့ User တွေကအချိန်မရွေးဝင်ရောက်အသုံးပြုလို့ရအောင်လုပ်ဆောင်ရတာမျိုးဖြစ်ပါတယ်။ ဥပမာပြောရရင် HR Department ကလူတွေက HRM software လို့မျိုး Software တွေကိုလိုအပ်တဲ့အချိန်မှာ အချိန်မရွေးဝင်ရောက်အသုံးပြုခွင့်ရအောင်လုပ်ဆောင်ပေးရတာဖြစ်ပါတယ်။

အပေါ်မှာကျွန်တော်ရှင်းပြသွားတာကတော့ CIA Triangle နဲ့ပတ်သက်ပြီးတော့ အကျဉ်းချုပ်ရှင်းပြထားတာဖြစ်ပါတယ်။ နောက်ပြီး Cyber Security နဲ့ပတ်သက်ပြီး အလုပ်လုပ်ဆောင်ချင်တဲ့သူတွေအနေနဲ့ CIA Traid ကိုကောင်းစွာသဘာပေါက်နားလည်ပြီး ပြန်လည်အသုံးချိန်ဖို့လို့အပ်ပါတယ်။

## The Basic of Information Security

**Information Security** ဆိုတာက Organization တွေရဲ့ System, Data တွေကို မသက်ဆိုင်တဲ့သူတွေကဝင်ရောက်အသုံးပြုမှာ ခွင့်ပြချက်မရှိပဲ အချက်လက်များအား ပြုပြင်ပြောင်းလဲမှာ စတဲ့လုပ်ဆောင်ချက်တွေကို တားဆီးကာကွယ်ရတာဖြစ်ပါတယ်။ Information Security မှာကျွန်တော်တို့သိထားသင့်တဲ့ Threads အမျိုးစားတွေရှိပါတယ်။ အဲဒါတွေကိုအောက်မှာတစ်ခုချင်းဖော်ပြပေးထားပါတယ်။

### 1) Malicious software

**Malicious Software** ကို Malware လိုလဲလူသိများပါတယ်။ Malicious software တွေထဲမှာဆိုရင် Computer Viruses, worm, Trojan horses, spyware, rootkits, adware, ransomware, crypto malware နဲ့တခြား unwanted software တွေပါဝင်ပါတယ်။ တစ်ခုချင်းဆီအကြောင်းကို Chapter - 4 System Security အခန်းမှာလေ့လာရမှာဖြစ်ပါတယ်။

### 2) Unauthorized access

Computer, Server ထဲမှာရှိနေတဲ့အချက်လက်တွေကို ပိုင်ရှင်မသိအောင်ခိုးဝင်ပြီး အချက်လက်များရယူခြင်းကို Unauthorized access လုပ်တယ်လို့ခေါ်ပါတယ်။

### 3) System failure

System failure ဆိုတာက system တစ်ခုလုံးအသုံးပြုလိုမရတော့တဲ့ အနေထားမျိုးကို ဆိုလိုတာဖြစ်ပြီး Computer, Server crashes ကြောင့်လဲဖြစ်နိုင်သလို Application failure ကြောင့်လဲ System failure ဖြစ်နိုင်ပါတယ်။ နောက်ထပ် system failure ဖြစ်နိုင်တဲ့အကြောင်းရင်းတွေလဲရှိပါတယ်။ အဲဒါတွေကတော့ User error, malicious activity, hardware failure တို့ပဲဖြစ်ပါတယ်။

### 4) Social engineering

Social engineering ဆိုတာက users တွေကိုအယုံသွင်းလှည့်စားပြီး organization / person တို့ရဲ့ sensitive information တွေကိုရယူတဲ့နည်းလမ်းဖြစ်ပါတယ်။

ကျွန်ုတ်တို့အနေနဲ့ Information တွေကို secure ဖြစ်စေချင်တဲ့အခါ Security နဲ့ သက်ဆိုင်တဲ့ technologies, concepts တွေကိုအသုံးပြုပြီးကာကွယ်လို့ရသလို threats တွေကြောင့်တို့က်ခိုက်ခံရလျှင်လဲ recover ပြန်လုပ်ဖို့အတွက် အကူညီဖြစ်မှာ ဖြစ်ပါတယ်။

## 5) Vulnerability

Vulnerability ဆိုတာက Network, System, Application တို့၏လုပ်ခြေရေးဆိုင်ရာ အားနည်းချက်ကို ပြောတာဖြစ်ပါတယ်။

## 6) Exploit

Vulnerability မှတစ်ဆင့် Network, System ထဲကိုဝင်ရောက်လိုရတဲ့ malicious code ကိုပြောတာဖြစ်ပါတယ်။

### Identifying Security Controls

Security Administrator တွေအနေနဲ့ Information တွေကိုကာကွယ်ဖို့အတွက် Security Plan ရေးဆွဲတဲ့အခါ မဖြစ်မနေ Security Controls တွေကိုအသုံးပြုဖို့ရေး ဆွဲသင့်ပါတယ်။ ကျွန်ုတ်တို့ Security Plan တစ်ခုကိုရေးဆွဲတဲ့အခါ အသုံးပြုသင့်တဲ့ Security controls တွေကို ၃ မျိုးဆွဲထားပါတယ်။ အဲဒါတွေကတော့-

- 1) Administrative Controls
- 2) Technical Controls
- 3) Physical Controls

တို့ပဲဖြစ်ပါတယ်။      တစ်ခုချင်းစီအကြောင်းကိုအောက်မှာဆက်ပြီးလေ့လာကြည့်ရ အောင်။

### 1) Administrative Controls

Administrative Controls ဆိုတာက risks တွေလျော့ချဖို့အတွက် Organization တွင်း မှာအသုံးပြုတဲ့ Policies တွေကိုရေးဆွဲတာဖြစ်ပါတယ်။ စာဖတ်သူတွေမြင်သာအောင် ပြောရရင် Organization တစ်ခုမှာ Internet-Policies တစ်ခုကိုရေးဆွဲတယ် ဆိုပါစို့။ အဲဒါ Policies မှာဆိုရင် ဝန်ထမ်းတွေအနေနဲ့ ရုံးတွင်းက Network ကိုအသုံးပြုပြီး Social Media မှာအသုံးမပြုရန်အတွက်တားမြစ်ခြင်းမျိုးဖြစ်ပါတယ်။ Administrative Controls မှာပါဝင်တာတွေကတော့-

- **Security Awareness Training:** ဝန်ထမ်းတွေကို Security ပိုင်းနဲ့ပတ်သက်ပြီး Knowledge များရဖော်အတွက် Training များလုပ်ပေးတာဖြစ်ပါတယ်။ ဥပမာ ဝန်ထမ်းများအား Social Engineering အကြောင်းကိုရှင်းပြပေးထားခြင်း အားဖြင့် ပြင်ပ Email များမှာပါဝင်လာတဲ့ attachment မှာပါဝင်တဲ့ files များကို အလွယ်တကူနှိပ်မိချင်းမှ ကာကွယ်နှင့်ခြင်း၊ Login Credentials များကို အလွယ်တကူ ပေးမိချင်းမှကာကွယ်နှင့်ခြင်း စတဲ့ကောင်းကျိုးတွေကိုရရှိစေမှာ ဖြစ်ပါတယ်။
- **Risk Assessment:** Risk assessment လုပ်တယ်ဆိုတာ attack ဖြစ်ခဲ့ရင် ဘယ်လောက်ထိဆုံးရှုံးမှုတွေ ဖြစ်နိုင်တယ်ဆိုတာကို တွက်ချက်တာဖြစ်ပါတယ်။

## 2) Technical controls

Technical controls ကတော့ business ကိုထိခိုက်နိုင်တဲ့ risk ကိုလျော့ချိုင်ဖို့ IT team ကလုပ်ဆောင်ရတာဖြစ်ပါတယ်။ အဲလိုလုပ်ဆောင်တဲ့အခါ အောက်ပါ control တွေကိုအသုံးပြုရပါတယ်။

- **Firewall rules:** Firewalls ဆိုတာက Network ထဲကိုခွင့်ပြုချက်မရှိတဲ့ IP address, application, protocol တွေဝင်ရောက်မလာနိုင်အောင် ကာကွယ် ရတာဖြစ်ပါတယ်။
- **Antivirus/antimalware:** Antivirus software ကိုတော့ Organization မှာ ရှိနေတဲ့ PC တွေအကုန်လုံးမှာ Install လုပ်ထားပြီး အမြဲ update ဖြစ်အောင်လဲ လုပ်ဆောင်သင့်ပါတယ်။
- **Screen savers:** ဒါကတော့ မိမိအလုပ်လုပ်တဲ့ Computer ရှေ့ကနေခန် တစ်ဖြုတ် ထသွားတဲ့အခါမျိုးမှာ တွေ့ခြားသူတစ်ဦးဦးက computer ကိုဝင်အသုံး ပြုခြင်းမျိုးမှကာကွယ်ပေးပါတယ်။
- **Screen filters:** ဒါကတော့ တွေ့ခြားသူတစ်ဦးဦးကလမ်းလျောက်ရင်းဖြစ်ဖြစ် ဖြတ်သွားရင်းဖြစ်ဖြစ် ကျွန်တော်တို့ Computer screen ပေါ်က data တွေကို ဖတ်လို့မရအောင်ကာကွယ်ပေးပါတယ်။

- **Intrusion Prevention Systems (IPS) / Intrusion Detection Systems (IDS):** IPS က network ပေါ်မှာတစ်ခုခုပြောင်းလဲသွားတာမျိုးတွေကို monitoring လုပ်တာဖြစ်ပြီး IDS ကတော့ System ကိုလာလုပ်တဲ့ attacks တွေကိုရုပ်တန်အောင်လုပ်ဆောင်ပေးပါတယ်။

### 3) Physical controls

Physical controls တွေကိုအောက်မှာဖော်ပြပေးထားပါတယ်။

- **Cable locks:** Computer ကိုခိုးပူးခြင်းမှကာကွယ်ပေးပါတယ်။ Cable locks တွေကို Computer အရောင်းဆိုင်တွေမှများသောအားဖြင့်တွေ့နှင်ပါတယ်။ Cable lock ကိုအောက်မှာနာပုံနဲ့ပြပေးထားပါတယ်။



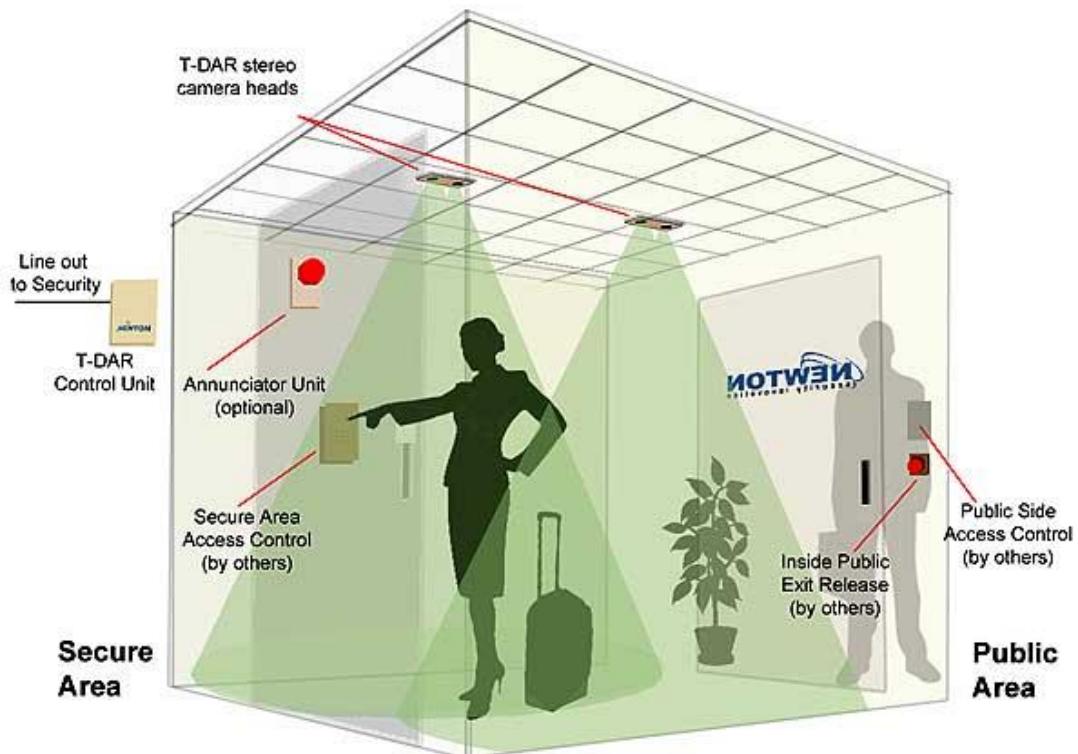
- **Biometric locks:** Biometric locks မှာဆိုရရှင် Fingerprint, voice, iris scanner နဲ့facial recognition တို့ပါဝင်ပါတယ်။
- **Gates:** Organization တွေရဲ့အခိုကလုပြံရေးထဲမှာ Security Gates ကလဲမရှိမဖြစ်လိုအပ်ပါတယ်။ ဒါမှသာအခွင့်မရှိတဲ့သူတွေ ဝင်ခြင်တိုင်းဝင် ထွက်ခြင်တိုင်းထွက် လုပ်လိုမရမှာဖြစ်ပါတယ်။

- **Burglar alarms:** Burglar alarms ဆိုတာက တစ်စုံတစ်ယောက်က ခြီးစဉ်းရှိုး တွေကိုဖြတ်ဖို့ကြိုးစားခြင်း၊ ထိမိခြင်း စတဲ့အခါမျိုးမှာ alarms ထမြည်တာမျိုး ဖြစ်ပါတယ်။ အောက်မှာ Burglar alarm ရဲနဲ့မူနာပုံလေးကိုပြပေးထားပါတယ်။



- **Fire alarms/Smoke detectors:** ဒါကတော့ မီးလောင်တာမျိုး၊ ဆေးလိပ်ငွေလို့ မီးချိငွေလွှာ ထွက်လာတဲ့အခါအားလုံးလွှတ်ရာကို ရှောင်လို့ရအောင် alarms ပေးတာဖြစ်ပါတယ်။
- **Security guards:** ကျွန်တော်တို့ဝန်းထဲကိုဝင်လာတဲ့ လူတိုင်းကိုစစ်ဆေးဖို့ အတွက်ကို Security guards တွေလို့အပ်ပါတယ်။ နောက်ပြီးတားမြစ်ထားတဲ့ နေရာတွေကို မသက်ဆိုင်တဲ့သူတွေသွားလာတာမျိုးတွေမဖြစ်အောင် security guards တွေက တားဆီးပေးပါတယ်။
- **Mantraps:** ဒါကတော့အဆောက်ဦးဝန်းထဲကိုဝင်တဲ့ တစ်ကြိမ်ကို တစ်ယောက် သာဝင်ခွင့်ပေးတာမျိုးဖြစ်ပါတယ်။ စာဖတ်သူတို့မြင်သာအောင်ပြောရရင် Company မှာ mgmg ဆိုတဲ့ဝန်ထမ်းရှိတယ်။ အဲ့ဝန်ထမ်းက ရုံးထဲကိုဝင်တဲ့အခါ တံခါးရဲ့ sensor မှာ ID card နဲ့ပြရတာ အဲ့လို့မှုသာတံခါးကပွင့်တာဖြစ်တယ်။

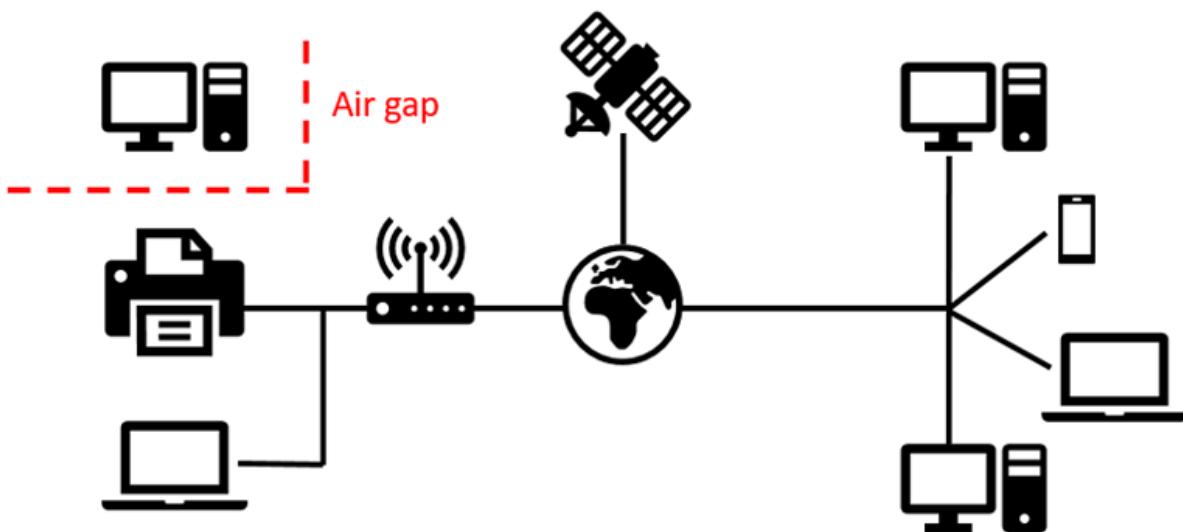
နောက် zawzaw သူကတော့ attacker ပေါ့သူမှာ အထဲကိုဝင်ဖို့ ID card မရှိဘူး၊ အဲတော့ mgmg ကသူရဲ့ ID card ကို တံခါးရဲ့ sensor မှာ ID card ပြပြီးဝင်တဲ့အခါ တံခါးပွင့်တဲ့အချိန်မှာ zawzaw ကပါအနောက်ကလိုက်ဝင်လို့ရပါတော့ တယ်။ အပေါ်မှာကျွန်တော်ပြောခဲ့တဲ့ ဥပမာ လိုမျိုးမဖြစ်ရအောင် Mantraps ကို အသုံးပြုသင့်ပါတယ်။ စာဖတ်သူတွေမြင်သာအောင်လဲ အောက်မှာပုံနဲ့ပြပေး ထားပါတယ်။



- **Perimeter protection:** Perimeter protection ဆိုတာကဝန်းထဲ ကားတွေကို ဝင်ထွက် သွားလာတဲ့အခါ အခွင့်မရှိပဲမသွားလာနိုင်အောင် တားတဲ့အခါအသုံးပြုတာဖြစ်ပါတယ်။ အောက်မှာပုံပြပေးထားပါတယ်။



- AirGap: ဒါကတော့ Devices တွေကိုသီးခြား Network တစ်ခုထဲမှာထားတာကို ပြောတာဖြစ်ပါတယ်။ အဲဒီ Network ကတ္ထား Network တွေနဲ့ချိတ်ဆက်ထားခြင်းမရှိသလို အလွယ်တကူလဲ connect လုပ်ဆောင်လို့မရပါဘူး ပြီးတော့ AirGap ကိုချိတ်ဆက်မယ်ဆိုရင် Physical အရပဲချိတ်ဆက်လို့ရပါတယ်။ LAN ပုံစမျိုးဖြစ်ပါတယ် ဒါပေမယ့်မတူတဲ့အချက်က LAN ထပ်ပို့ပြီး secure အောင်လုပ်ဆောင်တာဖြစ်တဲ့အတွက်သီးခြားအခန်းထဲမှာထားရတာဖြစ်ပါတယ် နောက်ပြီးအဲအခန်းထဲကိုမသက်ဆိုင်တဲ့သူတွေအလွယ်တကူ ဝင်ထွက်သွားလာ ခွင့်မရှိပါဘူး။ အောက်မှာ AirGap network ပုံကိုနှမူနာအနေနဲ့ပြပေးထားပါတယ်။



အပေါ်မှာကျန်တော်ဖော်ပြခဲ့တဲ့ Security controls တွေကိုအသုံးပြုပြီး CIA ကို ကာကွယ်နိုင်ပါတယ်။ အဲ Security controls တွေကိုမှာအောက်ပါအတိုင်းထပ်ပြီး ခဲ့ခြားလို့ရပါတယ်။

## Preventative controls

Preventative controls ဆိုတာက မည်သည့် attack မျိုးကိုမဆိုတားဆီးပေးတာဖြစ်ပါတယ်။ ဥပမာ အဆောက်အအုံးဝန်းတွင်းသို့သွေ့ဖက် ချိုးဝင်ရောက်ခြင်းကိုတားဆီးဖို့အတွက်ဆိုရင် လုံခြုံရေးက ခွဲးနဲ့အတူ ဝန်းအတွင်းမှာလှည့်ပတ်နေဖို့လို့အပ်ပါတယ်။ Preventative controls အတွက်ဆိုရင်လုပ်ဆောင်ဖို့လို့အပ်တဲ့ အချက် (j) ချက်ရှိပါတယ်။ အဲဒါတွေကတော့

- **Disable user accounts:** တစ်ကယ်လို့ Company မှုဝန်ထမ်းတစ်ဦးဦးက အလုပ်ကနေအပြီးထွက်သွားတဲ့အခါ အဲဝန်ထမ်းအသုံးပြုခဲ့တဲ့ computer မှာသူ အတွက်ဖွင့်ပေးထားတဲ့ user account ကို disable လုပ်ပေးဖို့လို့အပ်ပါတယ်။ အဲလိုလုပ်ဆောင်ခြင်းအားဖြင့် data တွေဆုံးရှုံးခြင်းမှကာကွယ်ပေးနိုင်ပါတယ်။ နောက်ပြီးအလုပ်ထွက်သွားတဲ့ ဝန်ထမ်းတွေ access လုပ်ဆောင်လို့မရအောင် password တွေကိုပြောင်းလဲဖို့လို့အပ်ပါတယ်။
- **Operating system hardening:** ကျန်တော်တို့ Company မှာအသုံးပြုနေတဲ့ Operating System တွေကို secure ဖြစ်အောင်လုပ်ဆောင်ဖို့လို့အပ်ပါတယ်။ အဲလိုလုပ်ဆောင်ဖို့အတွက်ဆိုရင် အချက်တွေအများကြီးရှိပါတယ် တချို့ကို ကျန်တော်ဖော်ပြပေးပါမယ်။
  - မသုံးတဲ့ / မလိုအပ်တဲ့ features နဲ့ services တွေကိုပိတ်ထားခြင်း
  - Software နဲ့ Antivirus တွေကိုအမြဲ updates ဖြစ်အောင်လုပ်ဆောင်ခြင်း စတာတွေဖြစ်ပါတယ်။

## Deterrent controls

**Deterrent controls** မှာဆိုရင် CCTV နဲ့ motions sensors တွေပါဝင်ပါတယ်။ တစ်ကယ်လို့ အဆောက်ဒီးဝန်းထဲမှာ တစ်ယောက်ယောက်က အချိန်မတော်လမ်းလျှောက်နောက် motion sensors တွေက detect သိမှာဖြစ်ပါတယ်။

## Detective controls

**Detective controls** ကတော့ incident တစ်ခုခုဖြစ်တဲ့အခါ စုစမ်းစစ်ဆေးဖို့အတွက်အသုံးပြုတာဖြစ်ပါတယ်။ အဲလိုစစ်ဆေးတဲ့အခါ အောက်ပါတို့ကိုအသုံးပြုပြီးစစ်ဆေးပါတယ်။

- **CCTV:** ဥပမာ အဆောက်ဒီးထဲက အခန်းတစ်ခုခုထဲမှာ မီးလောင်တာတို့မီးလန့်တာတို့ဖြစ်ခဲ့တဲ့အခါ အဲလိုမဖြစ်ခင် နောက်ဆုံးဘယ်သူအခန်းထဲဝင်သလဲဆိုတာသိဖို့ အတွက် CCTV records တွေကိုပြန်ကြည့်ပြီးစစ်ဆေးပါတယ်။
- **Log files:** တစ်ကယ်လို့ Company ရဲ့အရေးကြီး Data တွေပြင်ပကိုပေါက်ကြားခဲ့တဲ့ အခါမျိုးမှာဆိုရင် System ကိုဘယ်သူတွေ access လုပ်ခဲ့သလဲ ဘယ်သူတွေက data တွေကို download ဆွဲလဲဆိုတာသိဖို့အတွက်တော့ log files တွေကို ပြန်ကြည့်ပြီးစစ်ဆေးရပါတယ်။ အဲဒါ logs files တွေထဲမှာဆိုရင် time, date, event စတဲ့အချက်လက်တွေအများကြီးကိုတွေ့ရမှာဖြစ်ပါတယ်။

## Corrective controls

**Corrective controls** ကိုတော့ incident ဖြစ်တဲ့ recover ပြန်လုပ်ဖို့အသုံးပြုပါတယ်။ စာဖတ်သူတို့မြင်သာအောင်ပြောရရင် အရေးကြီးတဲ့ data တွေပါတဲ့ HDD တစ်လုံး ပျောက်သွားတယ်ဆိုပါစို့ ဒါဆိုရင်ကျွန်တော်တို့ကအဲ data တွေကို replace ပြန်လုပ်ဖို့ အတွက်ဆိုရင်အဲ data တွေ backup ရှိနေဖို့လို့အပ်ပါတယ်။ နောက် Fire-suppression systems ဟာဆိုရင် corrective control တစ်ခုဖြစ်ပါတယ်။

## Access controls

**Access controls** မှာဆိုရင် အဓိကအစိတ်ပိုင်း (၃) ပိုင်းပါဝင်ပါတယ်။ အဲဒါတွေ ကိုအောက်မှာ တစ်ခုချင်းဆီရှင်းပြပေးထားပါတယ်။

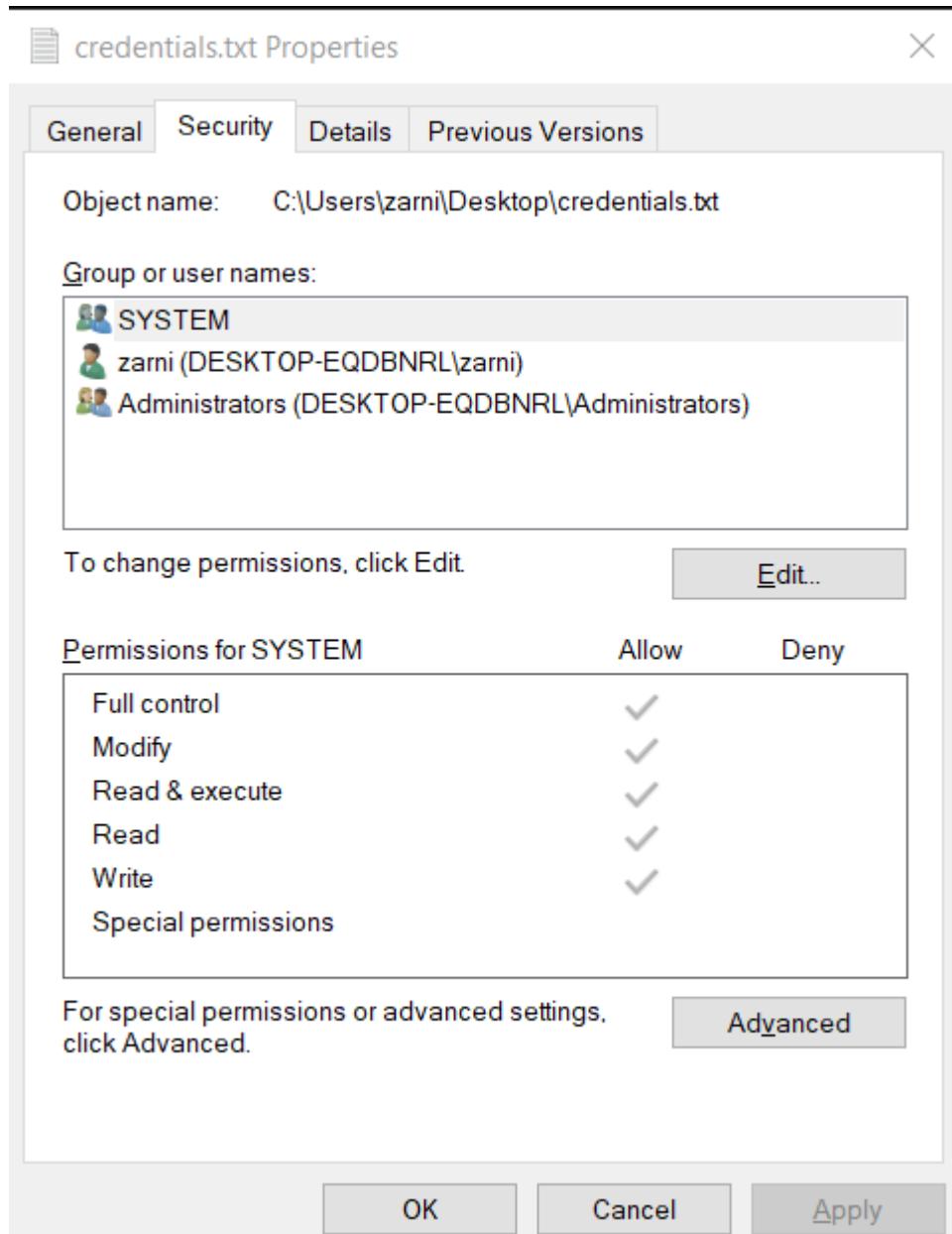
- **Identification:** ဒါကဘာကိုပြောတာလဲဆိုရင် လူတစ်ယောက်ကို သက်ဆိုင်ရာ information တွေနဲ့တွဲပြီးမှတ်လိုက်တာဖြစ်ပါတယ် စာဖတ်သူတွေမြင်သာ အောင်ပြောရရင် မှတ်ပုံတင် ဖြစ်ပါတယ်။ မှတ်ပုံတင်မှာဆိုရင် ကျွန်တော်တို့ ရဲ့သက်ဆိုင်တဲ့ information တွေအကုန်ပါပါတယ်။ နောက်ပြီး မှတ်ပုံတင် number ကလဲတူလို့မရသလို ထပ်လိုလဲမရပါဘူး။
- **Authentication:** Authentication ဆိုတာက System တစ်ခုထဲကို Login ဝင်တဲ့အခါ တရားဝင် အသုံးပြုခွင့်ရှိတဲ့ User ဟုတ်မဟုတ်ကိုစစ်ဆေးတာဖြစ်ပါတယ်။ စာဖတ်သူတွေ မြင်သာ ပြောရရင် ကျွန်တော်တို့ရဲ့ ကိုယ်ပိုင် Phone ကို ကျွန်တော်တို့သတ်မှတ် ပေးထားတဲ့ Password ဒါမှမဟုတ် Finger print တို့ကို အသုံးပြုပြီးဖွင့်မှသာ Phone ကိုအသုံးပြု လိုရတဲ့ပုံစံမျိုးကိုပြောတာဖြစ်ပါတယ်။နောက်ဥပမာပေးရ ရင် Facebook တို့လိုပေါ့။
- **Authorization:** Authorization ဆိုတာက Organization တွေရဲ့ Access တွေကိုတရားဝင် အသုံးပြုခွင့်ရှိတဲ့ User တွေကိုပဲပေးသုံးတာမျိုးကိုပြောတာ ဖြစ်ပါတယ်။ အဲလိုမျိုးတွေ ပေးသုံးတဲ့အခါမှာလဲ Permission တွေ Access control lists တွေကိုပါသတ်မှတ်ထား တာဖြစ်ပါတယ်။ Access ဆိုတာက Organization ကပိုင်တဲ့ Computer / Laptop, Phone, Printer စတာတွေပါဝင်ပါတယ်။ စာဖတ်သူတွေမြင်သာအောင်ပြောရရင် Company မှာဝန်ထမ်း အသစ်ဝင်တဲ့အခါ များသောအားဖြင့် အဲဝန်ထမ်းအသုံးပြုဖို့ Laptop ပေးရပါတယ်။ အဲလိုပေးတဲ့အခါ Computer User ကို Admin Level အနေနဲ့ ပေးသုံးတာမျိုးမဟုတ်ပဲ Normal User Account နဲ့သာအသုံးပြုခွင့်ပေးတာမျိုးဖြစ်ပါတယ်။

## Discretionary access control (DAC)

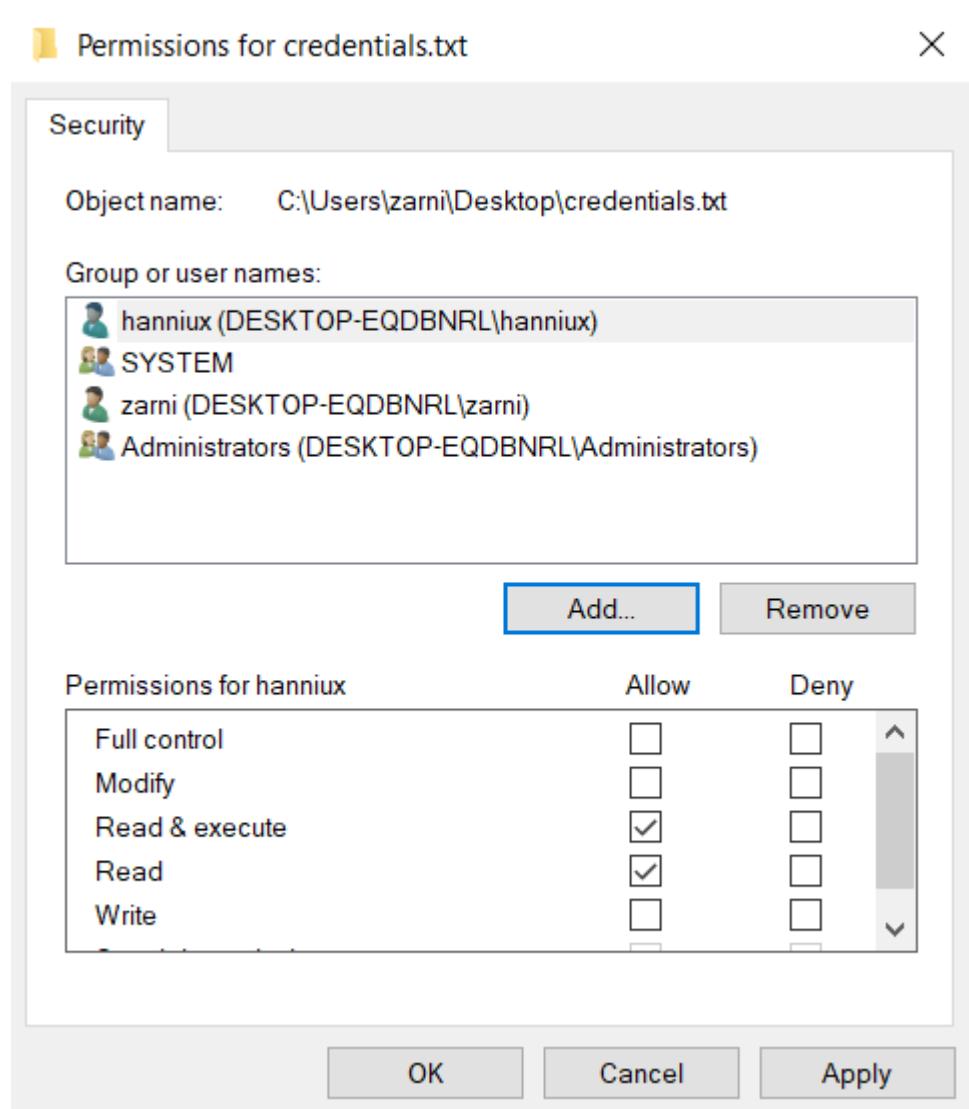
Discretionary access control ဆိုတာက files တွက် permission သတ်မှတ်တာဖြစ်ပါတယ်။ အဲလိုသတ်မှတ်ရာမှာဆိုရင် Microsoft Operating systems မှာဆိုရင် New Technology File System (NTFS) ကိုအသုံးပြုလိုရပါတယ်။ Discretionary access control ကိုအသုံးပြုထားခြင်းအားဖြင့် user က files တွက် access ပေးထားတဲ့ permissions အတိုင်းပဲလုပ်ဆောင်လို့ရမှာဖြစ်ပါတယ်။ Permissions အမျိုးစားတွေအများကြီးရှိပါတယ် အဲဒါတွေကတော့-

- Full control
- Modify
- Read and execute
- List folder contents
- Read
- Write
- Special permissions
- Data creator/owner

စတာတွေပဲဖြစ်ပါတယ်။ Windows မှာ permissions သတ်မှတ်ဖို့အတွက်ဆိုရင် သက်ဆိုင်ရာ file ကို right click နိုင်ပြီး properties ထဲကိုသွားပါမယ်။ ပြီးရင် security tab ကိုနိုပ်ပါမယ်။



Permissions သတ်မှတ်ဖို့အတွက် Edit ဆိုတဲ့ button ကိုနှစ်ပါမယ်။ အဲမှာ permissions သတ်မှတ်ချင်တဲ့ user ကို add လုပ်ပြီး permissions သတ်မှတ်လိုရပြီဖြစ်ပါတယ်။



## Least privilege

Least privilege ဆိုတာက user တွေရဲ့ access level ကို limited လုပ်တာဖြစ်ပါတယ်။ အဲလိုလုပ်ဆောင်တဲ့အခါ သူတို့နဲ့သက်ဆိုင်တဲ့အလုပ် တွေလုပ်ဆောင်လို့ရတဲ့ level ကိုပဲပေးသုံးတာဖြစ်ပါတယ်။

## Mandatory access control

Mandatory Access Control (MAC) ဆိုတာက data ရဲ့ classification level ပေါ်မှာအခြေခံထားတာဖြစ်ပါတယ်။ Government ပိုင်းတွေမှာတော့ MAC ကိုအသုံးပြုကြပါတယ် ဘာကြောင့်လဲဆိုရင် နိုင်ငံအကျိုးစီးပွားသယ်လောက်ပျက်စီးသွားနိုင်

သလဲဆိုတာတွက်ချက်လို့ရတဲ့အတွက်ကြောင့်ဖြစ်ပါတယ်။ နောက်ပြီး MAC ကို  
အမျိုးစားတွေခဲ့ခြားထားပါတယ် အဲဒါတွေကတော့

- Top secret
- Secret
- Confidential
- Restricted

**Mandatory Access Control (MAC)** နဲ့သက်ဆိုင်တဲ့ ဥပမာတစ်ခုကိုအောက်မှာ ပေါ်လော်  
နဲ့ဖော်ပြပေးထားပါတယ်။

Data types	Classification
Nuclear energy project	Top secret
Research and development	Secret
Ongoing legal issues	Confidential
Government payroll	Restricted

## Role-based access control

Department ပေါ်မှတည်ပြီးတော့ access ပေးလုပ်တာကို Role-based access control လိုအပ်ပါတယ်။ စာဖတ်သူတွေမြင်သာအောင် အောက်မှာ table နဲ့ပြပေးထားပါတယ်။

Sale Dept	Finance Dept	IT Dept
Customer Database	Customer Database	Customer Database
Payroll	Payroll	Payroll
Codebase	Codebase	Codebase

Table မှာဆိုရင် Sale, Finance, IT ဆိုပြီး Dept (၃) ခုရှိပါတယ်။ အဲ (၃) ခုမှာဆိုရင် customer database ကို access လုပ်ခွင့်ရှိတာက Sale Dept ဖြစ်ပါတယ် နောက် Payroll ကို access လုပ်ခွင့်ရှိတာက Finance Dept ဖြစ်ပြီး Codebase ကို access လုပ်ခွင့်ရှိတာကတော့ IT Dept ကဖြစ်ပါတယ်။ ဒါဆိုရင်စာဖတ်သူတွေအနေနဲ့ Role-based access control ကိုနားလည်မယ်လို့ထင်ပါတယ်။

## Rule-based access control

Rule-based access control ဆိုတာက ဝန်ထမ်းတွေအကုန်လုံးကို rule သတ်မှတ်တာဖြစ်ပါတယ်။ ဥပမာ Office Network ကိုအသုံးပြုပြီးတော့ online game ကစားခြင်းတွေပြုလုပ်လို့မရအောင် ကန့်သတ်တာမျိုးတွေဖြစ်ပါတယ်။

## Attribute-based access control

Attribute-based access control (ABAC) ဆိုတာက user တွေရဲ့ level ပေါ်မှာ မူတည်ပြီးသတ်မှတ်တာဖြစ်ပါတယ်။ ဥပမာ CEO တစ်ယောက်ရတဲ့ wifi access နဲ့ user တစ်ယောက်ရတဲ့ wifi access ကမတူနိုင်ပါဘူး။ ဘာကြောင့်လဲဆိုရင် CEO တစ်ယောက်ရတဲ့ wifi access မှာဆိုရင် Youtube, Facebook စတာတွေကိုအသုံး

ပြနိုင်ပေမယ့် user တစ်ယောက်ရတဲ့ wifi access တွေမှာတော့ ရချင်မှုရမှာဖြစ်ပါတယ်။

### Group-based access

Group-based access ဆိုတာ Data တွေကို access လုပ်တဲ့ နေရာမှာထိန်းချုပ်ဖို့ အတွက် user တွေအတွက် group တွေဖဲ့ပြီး access လုပ်စေတာဖြစ်ပါတယ်။

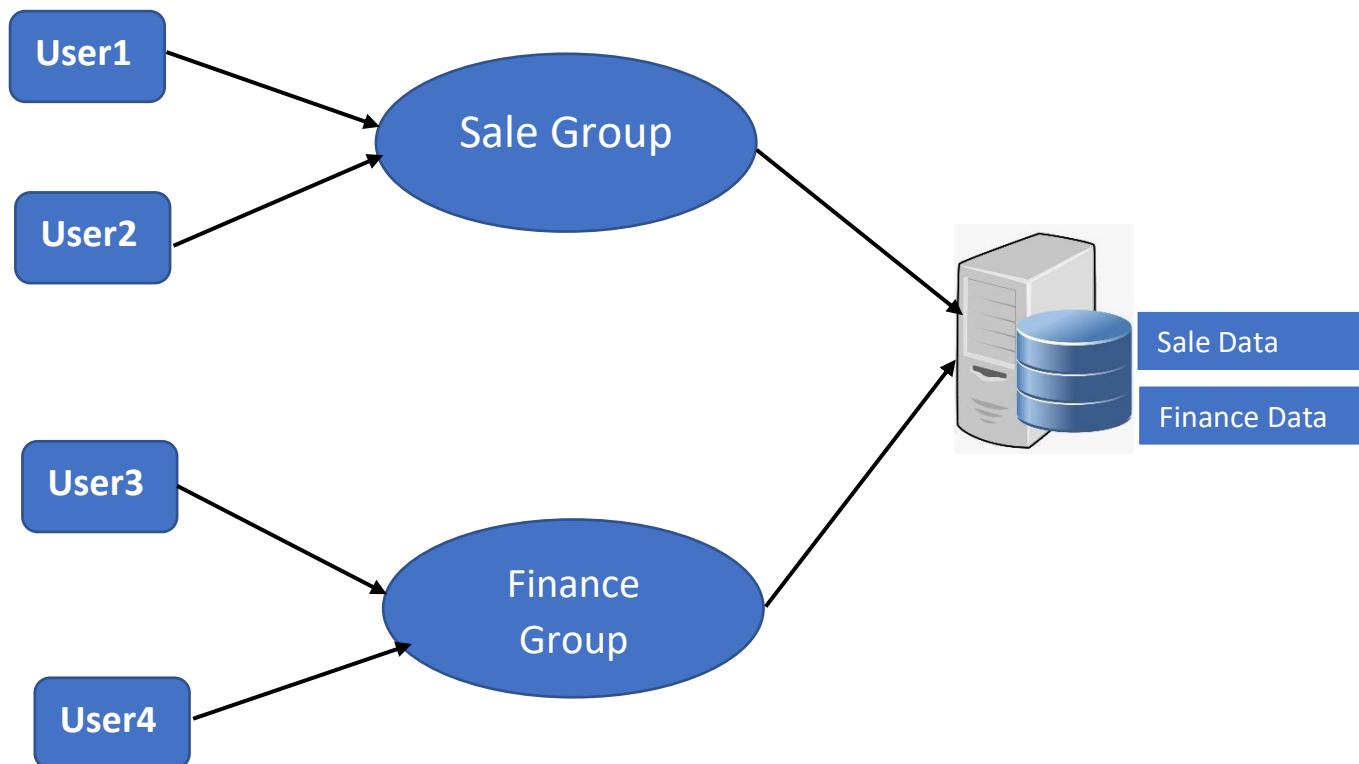


Diagram မှာ ဆိုရင် User1, User2 တို့က Sale Group ထဲကဖြစ်ပြီး Server ထဲက Sale data ကိုပဲ access ပေးလုပ်တာဖြစ်ပြီး User3, User4 တို့က Finance Group ထဲက ဖြစ်ပြီး server ထဲက Finance Data ကိုပဲ access လုပ်စေတာဖြစ်ပါတယ်။

### Hashing and data integrity

**Hashing:** Hashing ဆိုတာက document တစ်ခုထဲမှာရှိနေတဲ့ data တွေကို algorithm တစ်ခုခုဗ္ဗာ Secure Hash Algorithm version 1 (SHA1), Message

**Digest version 5 (MD5)** တိုကိုအသုံးပြုပြီး hashed လုပ်တာဖြစ်ပါတယ်။ Data တွေကိုပြင်ထားလား မပြင်ထားဘူးလားဆိုတာကို Hashing လုပ်ပြီး hash value တွေကိုစစ်လို့ရပါတယ်။

**Hashing the same data:** တစ်ကယ်လို့ ကျွန်တော်တိုက file တစ်ခုကို copy ကူးလိုက်တဲ့အခါ တူညီတဲ့ file (.) ခုဖြစ်သွားပါတယ်။ အဲလိုဖြစ်သွားတဲ့အခါ အထဲမှာပါတဲ့ data တွေကလဲအတူတူပဲဖြစ်ပါတယ်။ အဲ file တွေကိုတူညီတဲ့ hashing algorithm တစ်ခုခုကိုအသုံးပြုပြီး hash လုပ်ကြည့်ရင် တူညီတဲ့ hash value ပဲရမှာဖြစ်ပါတယ်။

**Verifying integrity:** Forensic analysis လုပ်တဲ့အခါမှာ investigation မလုပ်ခင်မှာ အရင်ဆုံး data တွေကို copy လုပ်ပါတယ်။ ပြီးတော့ investigation လုပ်နေတဲ့အချိန် တွင်းမှာလဲ အနောက်ယူက်တွေမရှိအောင်လဲလုပ်ဆောင်ရပါတယ်။ အရင်ဆုံး analysis မလုပ်ခင် data တွေရဲ့ hash value တွေကိုမှတ်ထားပြီး ပြီးသွားတဲ့ခါ hash value တွေတူမတူစစ်ရပါတယ်။ တစ်ကယ်လို့ hash value တွေကတူခဲ့တယ်ဆိုရင်တော့ data တွေကိုပြုပြင်ထားခြင်းမရှိဘူးလို့သတ်မှတ်လို့ရပါတယ်။ အဲလိုလုပ်ဆောင်တာကို verifying integrity လုပ်တယ်လို့ခေါ်ပါတယ်။

## Hash practical

အခုကျွန်တော်တို့ data တွေကို hash လုပ်တဲ့နည်းလေ့လာကြည့်ရအောင်။ အရင်ဆုံး txt file တစ်ခု create လုပ်ပါမယ်။ အဲထဲမှာ မိမိထည့်သွင်းချင်တဲ့ text တွေကိုထည့်ပါ။ Hash လုပ်တာကိုတော့ Windows မှာ default ပါဝင်တဲ့ CertUtil ဆိုတဲ့ tools ကိုအသုံးပြုပါမယ်။ Command ကတော့ certutil -hashfile location\file.txt ဖြစ်ပါတယ်။

```
C:\Users\zarni\Desktop>certutil -hashfile data.txt
SHA1 hash of data.txt:
637dd3894df6b16a956ab46ed377e5d85a7b2310
CertUtil: -hashfile command completed successfully.
```



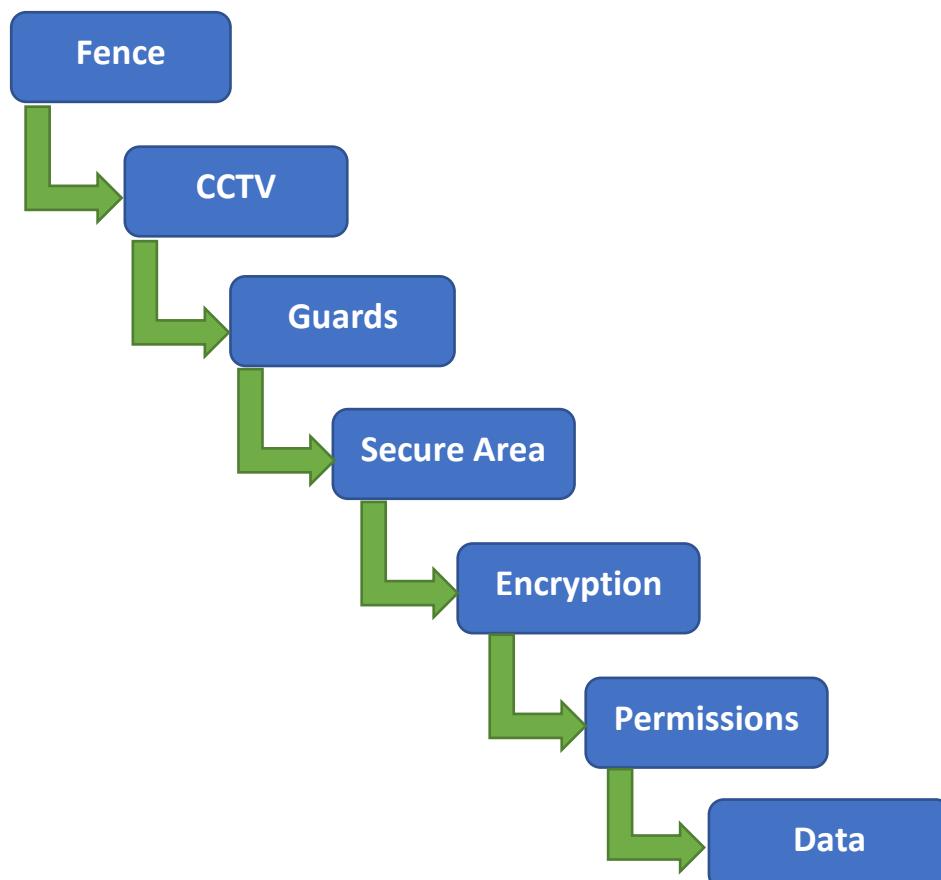
ပုံမှာဆိုရင် hash value ကိုများပြုပေးထားပါတယ်။ အခုက္ခန်းတော်တို့ txt file ထဲမှာ နောက်ထပ်စာသားတစ်လုံးလောက်ထပ်ထည့်ကြည့်ပါမယ်။ ပြီးရင် hash value ပြန်ထုတ်ကြည့်ပါမယ်။

```
C:\Users\zarni\Desktop>certutil -hashfile data.txt
SHA1 hash of data.txt:
2075851c74c0a4a8c90ae4c2a6f33e6ad947214b
CertUtil: -hashfile command completed successfully.
```

ပုံမှာဆိုရင်တော့ hash value မတူတာကိုစာဖတ်သူတွေတွေမြင်ရမှာဖြစ်ပါတယ်။ ဒါဆိုရင်တော့ file ကပြုပြင်ထားတယ်လိုက္ခန်းတော်တို့သတ်မှတ်လိုပါတယ်။

### Defense in depth model

Defense in depth model ဆိုတာက company က data ကိုကာကွယ်တဲ့ layers တွေဖြစ်ပြီး တစ်ကယ်လို့ layers တစ်ခု fails ဖြစ်သွားရင် နောက်ထပ်တဲ့ layers တွေက attack ကိုတားဆီးပေးမှာဖြစ်ပါတယ်။ ပါဝင်တဲ့ layers တွေကတော့



အဲ layers တွေကို စာဖတ်သူတိနားလည်အောင်ပြန်ရေးပြရမယ်ဆိုရင်

- အရင်ဆုံး Data တွေကို server မှာသိမ်းပါတယ်။
- အဲ Data တွေမှာ file permissions တွေသတ်မှတ်ထားပါတယ်။
- ပြီးတော့ Data တွေကို encrypted ပါလှပ်ထားပါတယ်။
- Data တွေကိုထားတဲ့နေရာက  
စိတ်ချေရတဲ့အဆောက်ဒီးထဲမှာထည့်ထားတာဖြစ်ပါတယ်။
- အဲဒီ building ထဲကိုဝင်မယ်ဆိုရင်လုံခြုံရေးတွေက  
စစ်ဆေးပြီးမှပေးဝင်တာဖြစ်ပါတယ်။
- Building ဝန်းထဲမှာလဲ CCTV တွေတပ်ထားပါတယ်
- အဲဝန်းကိုလဲခြုံစည်းရှိုးအမြင့်တွေနဲ့ကာထားတာဖြစ်ပါတယ်။

## Type of Attacks

### Application/service attacks

- Denial of Service Attack (DoS)
- Distributed Denial of Service Attacks (DDoS)
- Amplification Attack
- Man-in-the-Middle (MIM) Attack
- Man-in-the Browser (MITB)
- Replay Attack
- Zero-day Attack
- Pass the hash Attack
- Domain hijacking
- DNS poisoning
- DNSSEC
- ARP poisoning
- MAC spoofing attack

- IP spoofing
- Privilege escalation

## Programming attacks

- Christmas tree attack
- Dynamic Link Library (DLL) injection
- Cross-site request forgery (XSRF)
- Cross-site scripting (XSS)
- Buffer overflow
- SQL injection

## Hijacking related attacks

- Bluejacking
- Bluesnarfing
- Session hijacking
- URL hijacking
- Clickjacking

## Cryptographic attacks

- Birthday
- Digital signatures
- Rainbow tables
- Collision attack
- Salting passwords
- Key stretching

## Password attacks

- Dictionary attack
- Brute force attack
- Hybrid attack
- Account lockout

## Wireless attacks

- Evil twin
- Rouge access point
- Jamming
- WPS attack

စတာတွေပဲဖြစ်ပါတယ်။ Attack တွေအကြောင်းကိုတော့ သက်ဆိုင်ရာသင်ခန်းစာတွေ မှာရှင်းပြပေးထားပါတယ်။

## Penetration testing/Vulnerability Scanning

Penetration testing ဆိုတာက Real world မှာဖြစ်နိုင်မယ့် attack တွေပုံစံ အတိုင်းတိုက်ခိုက်ရတာ ဖြစ်ပါတယ်။ အဲလို့ attack တွေလုပ်ဆောင်ခြင်းအားဖြင့် organization မှာရှိနေ တဲ့အားနည်းချက်များကိုရှာဖွေဖော်ထုတ်နိုင်ပြီး လိုအပ်တာတွေ ကို attack မဖြစ်ခင်မှာပြုပြင်နိုင်မှာဖြစ်ပါတယ်။ Penetration testing မှာဆိုရင်

- Black box
- Gray box
- White box

ဆိုပြီး (၃) မျိုးရှိပါတယ်။

**Black box:** Black box ဆိုတာက Pentester ၏ target မှာအသုံးပြုတဲ့ Network, System, Service စတာတွေရဲ့ information တွေကိုလုံးဝမသိတဲ့အနေထားကနေ pentest လုပ်ဆောင်တာဖြစ်ပါတယ်။

**Gray box:** Gray box မှာတော့ pentester ကို target က information တရှိပို့ကို  
ပေးထားပါတယ်။

**White box:** White box မှာဆိုရင်တော့ pentester က target ရဲ့ information  
အကုန်လုံးကိုသိတဲ့အနေထားမျိုးဖြစ်ပါတယ်။

### Penetration testing techniques

Penetration testing မှာအသုံးပြုတဲ့ techniques တွေကတော့

- **Planning & Reconnaissance:** ဒီအဆင့်ကတော့ Pentest လုပ်ဖို့  
အတွက်စတင်ပြင်ဆင်တဲ့ အပိုင်းဖြစ်ပါတယ်။ Reconnaissance ဆိုတာ  
က target နဲ့သက်ဆိုင်တဲ့ information တွေကိုရယူတဲ့အပိုင်းဖြစ်ပါ  
တယ်။
- **Scanning:** ဒီအပိုင်းကတော့ Target ရဲ့ network/system တို့ရဲ့  
vulnerability ရှာဖွေတဲ့အပိုင်းဖြစ်ပါတယ်။
- **Gaining Access:** ဒီအဆင့်ကတော့ Target ရဲ့ network/system တို့ရဲ့  
vulnerability မှာတစ်ဆင့် ဝင်ရောက်တဲ့အပိုင်းဖြစ်ပါတယ်။
- **Privilege Escalation:** ဒါကတော့ gaining access ရပြီးသွားတဲ့အခါ  
root access ဖြစ်အောင်လုပ်ဆောင်တာဖြစ်ပါတယ်။ User level ကို  
မြင့်တယ်လို့လဲသတ်မှတ်လို့ရပါတယ်။
- **Maintaining Access:** Target ကို gaining access လုပ်ဆောင်ပြီးတဲ့  
အခါ နောက်တစ်ကြိမ်ဝင်ရောက်တဲ့အခါ အလွယ်တကူဝင်ရောက်ဖို့  
အတွက် backdoor ထည့်သွင်းတာဖြစ်ပါတယ်။

## Chapter – 2

# Understanding identity and access management concepts (IAM)

ပထမဦးဆုံးအနေနဲ့ IT security တွေတွေကြံရမှာက company ရဲ့ network resources တွေကို တခြားတစ်ယောက်ကို သူတို့အလုပ်အတွက်ပေးသုံးရတာဖြစ်ပါတယ်။ အဲလိုပေးသုံးတဲ့အခါဝန်ထမ်းတိုင်းကို သူတို့မည်သူမည်ဝါဖြစ်ကြောင်း သက်သေပြီးအတွက်ကိုလို အပ်ပါတယ်။ အဲအတွက် username ကနေ smart card ထိလိုအပ်ပါတယ်။ မည်သူမည်ဝါဖြစ်ကြောင်းကို သက်ပြေပြပြီးတဲ့အခါ အထောက်ထားတွေကို နောက်တစ်ဆင့် အတည်ပြုဖိုလိုပါသေးတယ်။ အဲလိုအတည်ပြုတဲ့အခါ နည်းလမ်းတွေအများကြီးရှုပါတယ် ဥပမာ password ဒါမာမဟုတ် pin တို့ပဲဖြစ်ပါတယ်။

### Passwords

User တွေကို authenticating လုပ်ဖို့အတွက် passwords တွေကိုကလဲ နည်းလမ်း တွေထဲကတစ်ခုဖြစ်ပါတယ်။ ဒါပေမယ့် password တွေက higher, lower-case, number နဲ့ special characters တွေကိုအသုံးပြုရတာဖြစ်တဲ့အတွက် အမြဲလိုလိုမှားထည့်နိုင်တဲ့ authentication factor တစ်ခုဖြစ်ပါတယ်။ တစ်ချို့လူတွေကတော့ caps lock ပွင့်နေတာကိုမသိပဲ password ရှိက်တာမျိုးတွေလဲရှုပါတယ်။ Password တွေကို insert လုပ်တဲ့အခါ users တွေက plain text အနေနဲ့မမြင်ရပဲ dots တွေနဲ့ပဲမြင်ရတာဖြစ်ပါတယ်။ ဒါပေမယ့် Windows 10 login မှာတော့ password ထည့်တဲ့ အခါ မြင်ရဖို့ မျက်လုံးပုံလေးကိုနှိပ်ပြီးကြည့်လို့ရပါတယ်။

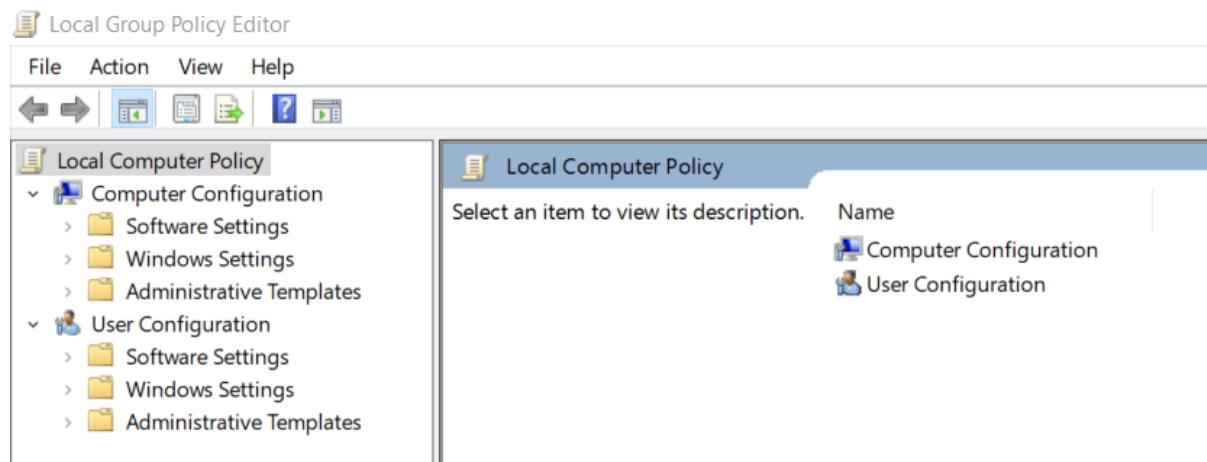
### Default/administrator password

Systems တစ်ခုမှာ administrator account ၂ ကောင့် ရှိသင့်ပါတယ်။ တစ်ခုကတော့ day-to-day အလုပ်တွေလုပ်ဆောင်ဖို့နဲ့ နောက်တစ်ခုကတော့ administrative tasks တွေကိုလုပ်ဆောင်ဖို့အတွက်ဖြစ်ပါတယ်။ Company မှာ အသုံး

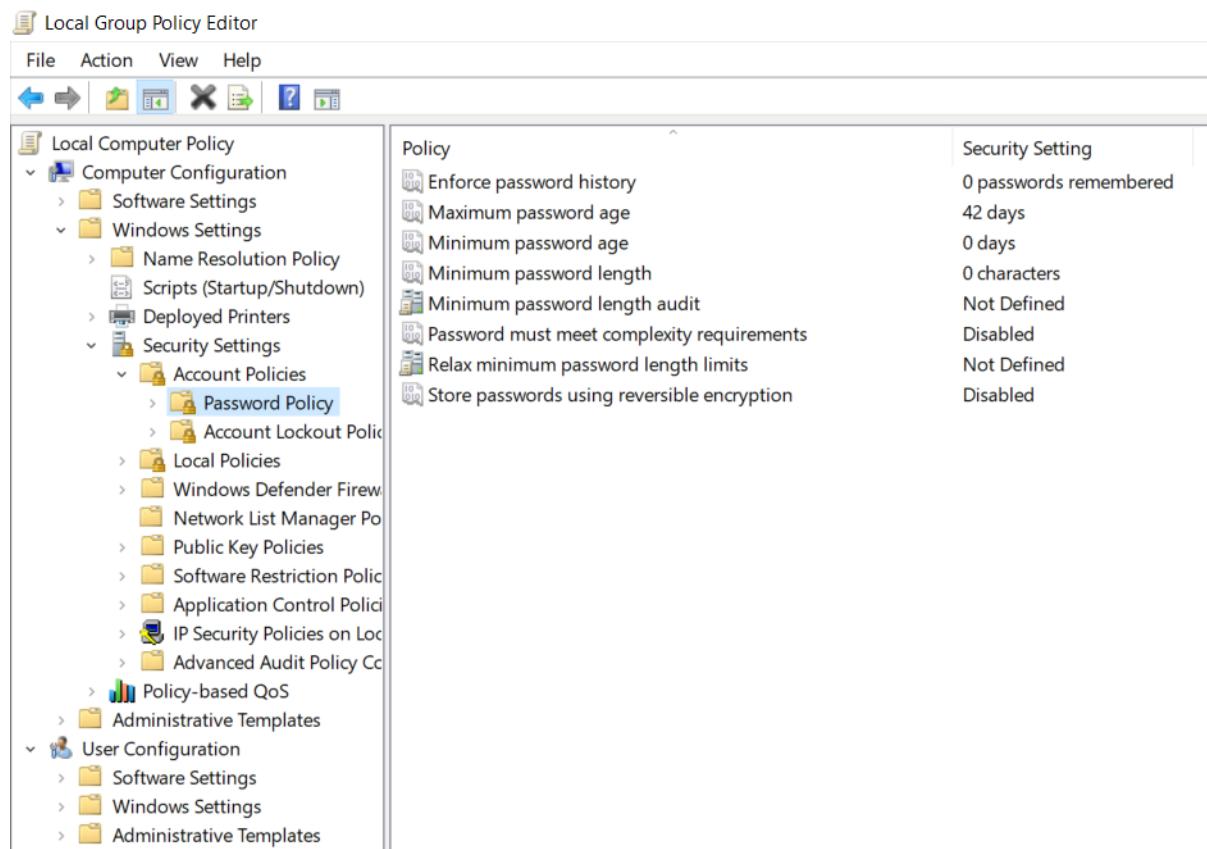
ပြုတဲ့ device တွေဖြစ်တဲ့ wireless router, firewall စတာတွေကိုတော့ default administrative username နဲ့ password တွေကိုတော့ပြောင်းသင့်ပါတယ်။

## Passwords-group policy

Security Administrator တွေအနေနဲ့ passwords policy တွေကို windows မှာဆိုရင် group policy မှာလိုအပ်သလိုပြင်ဆင်လိုပါတယ်။ အရင်ဆုံး run box ကနေ gpedit.msc ဆိုပြီးရိုက်ပါမယ်။



ပြီးရင် Computer Configuration မှတစ်ဆင့် Windows Settings > Security Settings > Account Policies > Password Policy ဆိုပြီးသွား လိုက်ရင်အောက်က ပုံအတိုင်း passwords policy သတ်မှတ်တဲ့နေရာကို ရောက်ပြီဖြစ်ပါတယ်။



ဆက်ပြီးတော့ password policy မှာပါဝင်တဲ့ Policy အကြောင်းတွေကိုဆက်လောက်ည့်ရအောင်။

**Enforce password history:** Enforce password history ဆိုတာက တူညီတဲ့ passwords တွေကိုခနေခနာသုံးပြုခြင်းကိုကာကွယ်ဖို့အတွက်ဖြစ်ပါတယ်။ အဲမှာဆိုရင် အများဆုံးမှတ်မိန့်တဲ့ password အရေတွက်က ၂၄ ခုဖြစ်ပါတယ်။ ဒါကဘာကိုဆိုလိုတာလဲဆိုရင် ကျွန်ုတ်တို့ ပထမဗျားဆုံး password တစ်ခုကိုသတ်မှတ်ပြီးတဲ့အခါ အဲဒါကိုထပ်ပြီးမသုံးခင် နောက်ထပ် password 24 ခုကိုလိုအပ်မှာဖြစ်ပါတယ်။

**Maximum password age:** ဒါကတော့ Password တစ်ခုရဲ့အများဆုံးအသုံးပြုခြင့်တဲ့ သက်တမ်းကိုသတ်မှတ်တာဖြစ်ပါတယ်။ Default ကတော့ 42 ရက်ဖြစ်ပါတယ်။

**Minimum password age:** Minimum password age ကိုသတ်မှတ်ထားခြင်းအားဖြင့် တစ်နေ့ထဲမှာ password ကိုခနေခနာပြောင်းလဲတာကိုကာကွယ်ပေးပါတယ်။ အဲမှာ

ကျွန်တော်တို့က အကြိမ်ရေတွက်ကိုသတ်မှတ်ထားလို့ရပါတယ်။ နောက်ပြီး password expiry date လိုလဲမှတ်လို့ရပါတယ်။

**Password must meet complexity requirements:** ဒါကို enable လုပ်ထားရင်တော့ password ပေးတဲ့အခါ complex ဖြစ်ရပါတယ်။ Complex password ပါဝင်တာတွေက

- Lowercase: abc
- Uppercase: ABC
- Numbers: 123
- Special characters not used in programming: \$@

**Store passwords using reversible encryption:** ဒါကတော့ user က password ကိုထည့်သွင်းလိုက်တဲ့အခါ အဲဒီ password ကို plain text အနေနဲ့သိမ်းတာမဟုတ်ပဲ encrypt လုပ်ပြီးမှသိမ်းတာဖြစ်ပါတယ်။

## Password recovery

ကျွန်တော်တို့တွေအနေနဲ့ တစ်ခါတစ်လေ ပေးထားတဲ့ password ကိုမေ့တာမျိုး တွေ ကံဖူးကြမှာဖြစ်ပါတယ်။ အဲအခါ password reset ပြန်လုပ်ဖို့လိုအပ်ပါတယ်။ Password reset ပြန်လုပ်တဲ့အခါ ကျွန်တော်တို့ရဲ့ personal details တွေကိုပြန်ထွေးပေးရပြီး code ကို phone SMS ဒါမှုမဟုတ် mail ကနေပြန်ပို့ပေးပါတယ်။ ဥပမာ Facebook password reset လုပ်သလိုပေါ့။ တချို့ Desktop Operating Systems တွေမှာဆိုရင် SD card, USB Drive တို့ကို အသုံးပြုပြီး password reset disk တွေလုပ်လို့ရပါတယ်။

## Authentication factors

Authentication factors မှာဆိုရင် password, iris scanner စတဲ့မတူညီတဲ့ နည်းတွေရှိပါတယ်။ အောက်မှာမတူညီတဲ့ authentication factors တွေကိုဖော်ပြုပေးထားပါတယ်။

- **Multifactor authentication:** မတူညီတဲ့ authentication တွေကို group အနေဖြင့်အသုံးပြုတာကို multifactor authentication လိုခေါ်ပါတယ်။ Multifactor authentication မှာဆိုရင် PIN, Biometric စတာတွေပါဝင်ပါတယ်။



- **Something you know:** ဒါကတော့ username, password စတာတွေကို ပြောတာဖြစ်ပါတယ်။
- **Something you have:** Secure token, key fob, card စတာတွေပါဝင်ပါတယ်။ Hardware token ကတော့ second 60 ပြည့်တိုင်း PIN အသဲထုတ်ပေးပါတယ်။ Key fob ဆိုတာက proximity card လိုမျိုးဖြစ်ပါတယ်။
- **Something you are:** Biometric authentication ကိုပြောတာဖြစ်ပါတယ်။ အဲမှာဆိုရင် iris ဒါမှမဟုတ် retina scanner, palm ဒါမှမဟုတ် fingerprint reader ဒါမှမဟုတ် အသံစတာတွေပါဝင်ပါတယ်။
- **Somewhere you are:** ဒါကတော့ location နဲ့သတ်မှတ်တာဖြစ်ပါတယ်။

### Number of factor examples

အခုက္ခန်တော်တို့ factor အမျိုးစားတွေကိုဆက်ပြီးလေ့လာကြည့်ရအောင်။ တစ်ခုချင်းဆီကိုအောက်မှာဖော်ပြပေးထားပါတယ်။

- **Single factor:** ဒါကတော့ username, password မဟုတ်ရင် PIN စတာတွေကိုအသုံးပြုတာဖြစ်ပါတယ်။

- **Two factors:** Two factor မှာဆိုရင် password / pin တင်မဟုတ်ပဲ smart card/otp စတာတွေပါအသုံးပြုပါတယ်။
- **Multifactor:** Multifactor ကတေသ့ factor တစ်ခုထပ်ပိုပြီးသုံးထားတာကို multifactor လိုက်ပေါ်ပါတယ်။ ဥပမာ Hardware token ကို PIN နဲ့ပေါင်းစပ်ထားတာမျိုးပါ။

## Shibboleth

Shibboleth ဆိုတာက open-source federation service တစ်ခုဖြစ်ပြီး SAML (Small Federation Service Environment) authentication အတွက်ကိုအသုံးပြုပါတယ်။

## Single sign-on

Single sign-on ကို domain environment တွေမှာအသုံးပြုပါတယ်။ File, email server တွေကို access လုပ်ဖို့လိုတဲ့အခါ credentials တွေကိုထပ်ပြီးထည့်သွင်းဖို့မလိုပါဘူး domain မှာတော့ logs တွေအနေနဲ့ သိမ်းထားတာကြောင့်ဖြစ်ပါတယ်။ Federation services, Kerberos (Microsoft Authentication Protocol) ဂုဏ်လုံးဟာ single sign-on တွေဖြစ်ကြပါတယ်။

## Authentication, authorization, and accounting (AAA) servers

AAA servers တွေမှာဆိုရင်အဓိကအားဖြင့် Microsoft's Remote Authentication Dial-In User Service (RADIUS) and CISCO's Terminal Access controller Access-Control System Plus (TACACS+) တို့ကိုအသုံးပြုကြပါတယ်။

- **RADIUS server:** RADIUS server က UDP based ကိုအသုံးပြုထားတဲ့ authenticates server ဖြစ်ပါတယ်။ Virtual private network (VPN) servers, remote access services (RAS) servers နဲ့ 802.1x authentication switch တို့က radius clients တွေဖြစ်ကြပါတယ်။ Radius clients တိုင်းက secret key နောက်မျိုး session key ကို

အသုံးပြုပြီး RADIUS ကို join ရပါတယ်။ RADIUS communicates က UDP port 1812 ကိုအသုံးပြုပါတယ်။

- **TACACS+:** ဒါကတော့ CISCO ရဲ့ AAA server ဖြစ်ပြီး TCP ကိုအသုံးပြုတဲ့ အတွက် RADIUS ထပ်ပိုပြီးတော့ secure ဖြစ်ပါတယ်။ သူကတော့ Port 49 ကိုအသုံးပြုပါတယ်။

## Learning about Identity and access management controls

ဒီအပိုင်းမှာတော့ ကျွန်တော်တို့ IAM controls တေအကြောင်းကိုလေ့လာကြ ပါမယ်။

### 1) Biometrics

- **Fingerprint scanner:** Fingerprint scanner ဆိုတာကလက်မွေ ကိုအသုံးပြုပြီး identity လုပ်တာဖြစ်ပါတယ်။ Fingerprint scanner တွေကိုအခုန်က်ပိုင်းကာလတွေမှာ ဖုန်းတွေအထိမှာပါ အသုံးပြုလာကြပါတယ်။
- **Retina scanner:** Retina ဆိုတာကမျက်ကြည်လွှာကိုအသုံးပြုပြီး identity လုပ်တာဖြစ်ပါတယ်။
- **Iris scanner:** Iris ဆိုတာကမျက်လုံးကိုအသုံးပြုပြီး identity လုပ်တာဖြစ်ပါတယ်။
- **Voice recognition:** ဒါကတော့အသုံးပြုပြီး identity လုပ်တာဖြစ်ပါတယ်။
- **Facial recognition:** ဒါကတော့မျက်နှာကိုအသုံးပြုပြီး identity လုပ်တာဖြစ်ပါတယ်။

### 2) Security tokens and devices

- **Time-Based One-Time Password (TOTP):** TOTP ကိုအသုံးပြု မယ်ဆိုရင် time synchronization လိုအပ်ပါတယ် ဘာကြောင့်လဲဆို

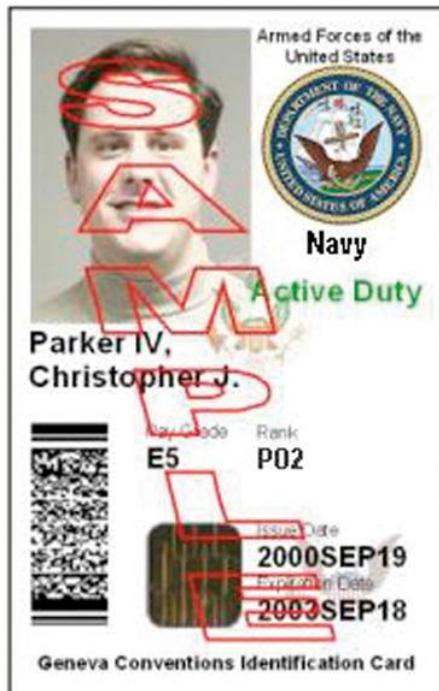
တော့ password ကိုအသုံးပြုလိုရတဲ့အချိန်ကအရမ်းတိုတဲ့အတွက်ဖြစ်ပါတယ်။ ပုံမှန်ကတော့ 30 second ကနေ 60 second ထိဖြစ်ပါတယ်။

- **HMAC-based One-Time Password (HOTP):** HOTP က TOTP လိုပဲ one-time password ပဲဖြစ်ပါတယ်။ အဓိကအရေးကြီးတာက အချိန်ကန့်သတ်မှတ်ချက်မရှိပါဘူး ဒါပေမယ့် password ကတော့တစ်ကြိမ်သာအသုံးပြုခွင့်ရှိပါတယ်။

### 3) Certification-based authentication

Certificate-based authentication ပိုပြီးနာမည်ကြီးရတဲ့အကြောင်းရင်းကတော့ two-factor authentication ကို provides လုပ်ပေးနိုင်လို့ဖြစ်ပါတယ်။ ဒါဟာ single-factor authentication ထပ်ပိုပြီးတော့ secure ဖြစ်ပါတယ်။

- **Smart card:** Smart card ဆိုတာက card ထဲမှာ chip ကိုထည့်သွင်းထားတာဖြစ်ပါတယ်။ အဲ chip ထဲမှာ certificate ပါဝင်ပါတယ်။
- **Common Access Card (CAC):** CAC ကိုတော့များသောအားဖြင့် government တွေကအသုံးများပြီး စစ်တပ်မှာဆိုရင်တော့ authentication နဲ့ identification တို့အတွက် ကဒ်ပိုင်ရှင်ရဲ့ပုံပါ ကဒ်မှာဖော်ပြထားပါတယ်။ စာဖတ်သူတို့မြင်သာအောင်ပြောရရင် ဝန်ထမ်းကဒ်လိုပါ။ Card ရဲ့အရှေ့ဘက်မှာဆိုရင် card ပိုင်ရှင်ရဲ့စာတ်ပုံ၊ တာဝန်ထမ်းဆောင်တဲ့ department ဥပမာ army, navy, air force စတာတွေပါဝင်ပါတယ်။ Common Access Card ရဲ့နူးနာပုံကိုအောက်မှာဖော်ပြပေးထားပါတယ်။



- Personal Identity Verification (PIV): CAC နဲ့ပုံစံတူပါတယ် မတူတာက federal agencies တွေမှာအသုံးပြုပါတယ်။

#### 4) Port-based authentication

Port-based authentication ကတေသာ 1EEE 802.1x protocol မှာအသုံးပြုတာဖြစ်ပြီး device တွေက switch ဒါမှုမဟုတ် user တွေက wireless access point တို့မှာလာရောက်ချိတ်ဆက်တဲ့အခါ authenticates လုပ်ဖို့အတွက်အသုံးပြုပါတယ်။

#### Common account management practices

Account management မှာဆိုရင် account creation ကနေ ဝန်ထမ်းတစ်ဦး company ကနေထွက်သွားတဲ့အချိန် disable လုပ်တဲ့အထိပါဝင်ပါတယ်။

- Account types

User တွေက Microsoft Active Directory environment ကို access လုပ်ဖို့အတွက်ဆိုရင် user account လိုအပ်ပါတယ်။ အဲ user account မှာဆိုရင် account ကို Security Identifier (SID) နဲ့ချိတ်ဆက်ထားပါတယ်။ ကျွန်တော်တို့က hanniux ဆိုတဲ့ user account တစ်ခုကို create လုပ်လိုက်ပြီဆိုရင် သူ့ရဲ့ SID မှာဆိုရင်

SID 1-5-1-2345678-345678 ဆိုပြီးပါလာမှာဖြစ်ပါတယ်။ Account ကို delete လုပ်လိုက်ပြီဆိုရင် SID ပါပျက်သွားမှာဖြစ်ပါတယ်။ ဥပမာ IT team က hanniux လိုခေါ်တဲ့ user account ကို delete လုပ်ပြီး နောက် hanniux ဆိုတဲ့ account အသစ်ကိုထပ်ပြီး create လုပ်လိုက်ပြီဆိုရင် SID က SID 1-5-1-2345678-3499999 ဆိုပြီးဖြစ်သွားမှာဖြစ်ပါတယ်။ ဆက်ပြီး ကျွန်တော်တို့သိတော်သင့်တဲ့ user account type တွေကိုဖော်ပြပေးပါမယ်။

- **User account:** ဒါကတော့ normal user account ဖြစ်ပါတယ်။ ဒီ account နဲ့ဆိုရင် software တွေကိုလဲကိုယ်တိုင် install လုပ်ဆောင်လိုမရသလို computer systems ထဲက resources တွေကိုအကန္နသတ်နဲ့ပဲရမှာဖြစ်ပါတယ်။ User account အမျိုးစား (၂) မျိုးရှိပါတယ် Local user account နဲ့ domain user account တို့ဖြစ်ပါတယ်။
- **Guest account:** Guest account ဆိုတာက computer မှာ default ပါတဲ့ account ဖြစ်ပါတယ်။ သူလဲ limited access ဖြစ်ပါတယ်။ ဒီအကောင့်က default အနေနဲ့ဆိုရင် disable ဖြစ်နေပါတယ်။
- **Privilege account:** User accounts ထပ်ပိုပြီး access တွေကိုရရှိတဲ့အကောင့် ဖြစ်ပါတယ်။ များသောအားဖြင့် IT team ကပဲအသုံးပြုတဲ့ အကောင့်ဆိုလဲမမှားပါဘူး။ စာဖတ်သူတို့မြင်သာအောင်ပြောရရင် Administrators တွေက privilege accounts တွေဖြစ်ပါတယ်။
- **Administrative account:** Administrative account တွေက software တွေကို install လုပ်နိုင်ပါတယ် နောက်ပြီး server ဒါမှမဟုတ် computer တွေမှာ လိုအပ်သလို configuration တွေပါလုပ်ဆောင်နိုင်ပါတယ်။ နောက်ပြီး user account တွေကို create, delete စတာတွေလုပ်ဆောင်နိုင်ပါတယ်။
- **Shared account:** ဝန်ထမ်းတွေကတူညီတဲ့ duties ဥပမာ customer services လိုမျိုးအလုပ်တွေမှာ shared account ကိုအသုံးပြုကြပါတယ်။ Facebook page တွေမှာဆိုရင် admin အနည်းဆုံး (၂) ယောက်လောက်ရှိပါတယ် အဲအခါ

customer ထံကနေ message ဝင်တဲ့အခါ တစ်ယောက်မအားရင် နောက် တစ်ယောက်ကဝင်ပြီးပြောလိုရပါတယ်။

## Security Information and Event Management (SIEM)

SIEM ဆိုတာက information security အတွက် event management နဲ့ organizations တွေအတွက် next-generation detection, analytics နဲ့ response တို့အတွက်အသုံးပြုတဲ့ software ဖြစ်ပါတယ်။ SIEM software က security information management (SIM) နဲ့ security event management (SEM) နှစ်ခုပေါင်းထားတာဖြစ်ပြီး network hardware နဲ့ applications တို့မှာဖြစ်ပေါ်နေတဲ့ security alerts တွေကို real-time analysis လုပ်နိုင်ပါတယ်။ ဒါအပြင် advanced threats ကိုပါ detect သိနိုင်ဖို့အတွက် globally gathered intelligence နဲ့ analytics engines ပါဝင်ပါတယ်။ အဲဒါက security teams တွေအတွက် IT environment ထဲက activities တွေရဲ့ record တွေကိုခြေရာခံနိုင်ပြီး data analysis, event correlation, aggregation, reporting နဲ့ log management တို့ကိုလုပ်ဆောင်နိုင်ပါတယ်။ SIEM software မှာပါဝင်တဲ့ features နဲ့ benefits တွေကတော့

- Consolidation of multiple data points
- Custom dashboards and alert workflow management
- Integration with other products

စတာတွေပဲဖြစ်ပါတယ်။

## Chapter 3

### Network Security

#### OSI – reference model

Open Systems Interconnection (OSI) ကို Internet Standards Organization (ISO) က create လုပ်ခဲ့တာဖြစ်ပြီး အဲဒီ model ကို communication အတွက်အသုံးပြုပါတယ်။ OSI မှာ Layers 7 ချို့ပြုး တစ်ခုချင်းဆီမှာ မတူညီတဲ့ protocols တွေကတာဝန်ယူပါတယ်။ အောက်မှာ Layers 7 ခုစလုံးကို Table နဲ့ဖော်ပြပေးထားပါတယ်။

Layer	Description	Example	Devices	Packet Structure
7	Application	HTTP, SMTP		
6	Presentation	Encryption, Formatting		
5	Session	Logging On / Off		
4	Transport	TCP, UDP		Datagrams
3	Network	IP, ICMP	Router	Packets
2	Data Link	IP Sec, VLAN, ARP	Switch	Frames
1	Physical	Cables	Hub	Bits-01010101

Layer တစ်ခုချင်းဆီအကြောင်းကိုအောက်မှာဆက်ပြီးဖော်ပြပေးထားပါတယ်။

**Application layer:** Application layer မှာဆိုရင် Web site တွေကြည့်ဖို့ HTTP, Email တွေလက်ခံဖို့ SMTP စတာတွေပါဝင်ပါတယ်။ Web Application Firewall (WAF) ရဲတာဝန်က web-based application တွေကို ဒီ layer မှာကာကွယ်ဖို့အတွက်အသုံးပြုပါတယ်။

**Presentation layer:** ဒီ layer မှာဆိုရင်တော့ data တွေကို character code ဖြစ်တဲ့ Unicode ဒါမှာမဟုတ် ASCII။ အဖြစ်သို့ပြောင်းလဲပေးပါတယ်။ Encryption က ဒီ layer မှာလုပ်ဆောင်တာဖြစ်ပါတယ်။

**Session layer:** ဒီ layer ကတော့ login နဲ့ logout စတဲ့ session နဲ့သက်ဆိုင်တာ တွေကိုလုပ်ဆောင်ပေးပါတယ်။

**Transport layer:** ဒီ Layer မှာဆိုရင် TCP နဲ့ UDP တို့ပါဝင်ပါတယ်။ TCP connection က three-way handshake ကိုအသုံးပြုပြီး packet တိုင်းရဲ့ acknowledges ကိုလက်ခံတာကြောင့် စိတ်ချရပါတယ်။ UDP ကတော့ connectionless ဖြစ်ပြီး application တွေရဲ့ data တွေရောက်မရောက်ကိုစစ်ဖို့အတွက်အသုံးပြုပါတယ်။ Ports တော်တော် များများဟာ TCP-based တွေဖြစ်ပြီး video streaming အတွက်ကတော့ UDP က ပိုကောင်းပါတယ် ဘာကြောင့်လဲဆိုရင် TCP တဲ့အတွက်ကြောင့်ပါ။

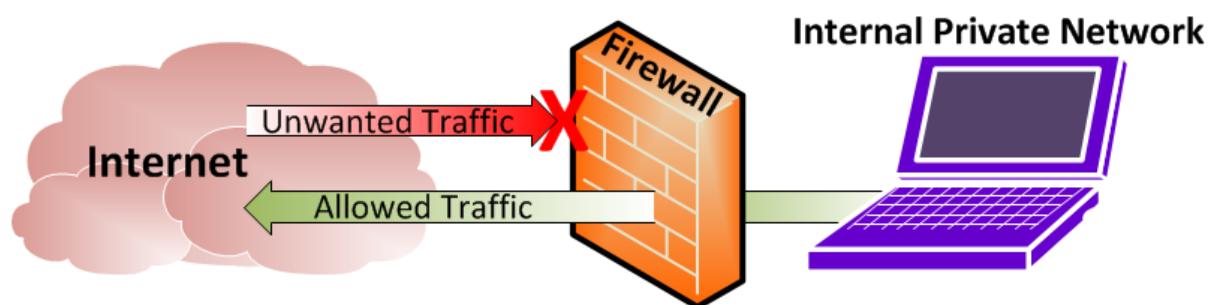
**Network layer:** Network layer ရဲ့တာဝန်ကတော့ IP addressing နဲ့ routing အတွက်ဖြစ်ပါတယ်။ Routing ဆိုတာကမတူညီတဲ့ network တွေအချင်းချင်း ချိတ်ဆက်လို့ရအောင်လုပ်ဆောင်တာကိုပြောတာဖြစ်ပါတယ်။ Internet Control Message Protocol (ICMP) က ဒီ layer မှာလုပ်ဆောင်တာဖြစ်ပါတယ်။ Network troubleshooting လုပ်တဲ့ tools တွေဖြစ်တဲ့ ping, tracert, pathping တို့က ICMP ကိုအသုံးပြုပြီး replies လုပ်တာဖြစ်ပါတယ်။

**Data-link layer:** ဒီ layer မှာဆိုရင် အဓိက functions (၃) ရှိပါတယ်။ Transmission errors တွေကို ဖြေရှင်းဖို့, data စီးဆင်းမှုတွေကို ထိန်းညီဖို့ နဲ့ network layer က interface တွေကောင်းစွာလုပ်ဆောင်နိုင်ဖို့တို့ဖြစ်ပါတယ်။ MAC addresses က ဒီ layer မှာပါဝင်တာဖြစ်ပြီး ဒီ layer မှာဆိုရင် switch ကလုပ်ဆောင်တာဖြစ်ပါတယ်။ ဒါအပြင် ဒီ layer မှာတခြားလုပ်ဆောင်တာတွေကတော့လုပ်ဆောင်တာတွေကတော့ Address Resolution Protocol (IP ကနေ MAC ပြောင်းတဲ့အခါအသုံးပြုပါတယ်), IPSec (encryption-tunneling protocol), Virtual local area network (VLAN) တို့ဖြစ်ပါတယ်။

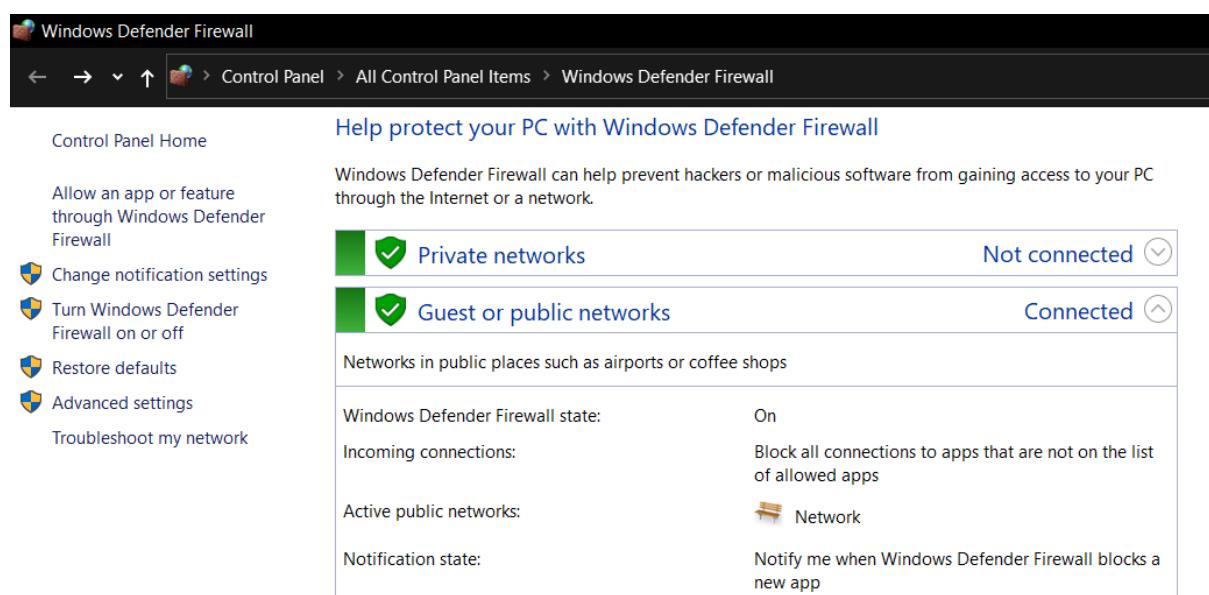
**Physical layer:** ဒီ layer မှာတော့ Ethernet, coaxial, wireless communication စိတာတွေပါဝင်ပါတယ်။

## Firewall

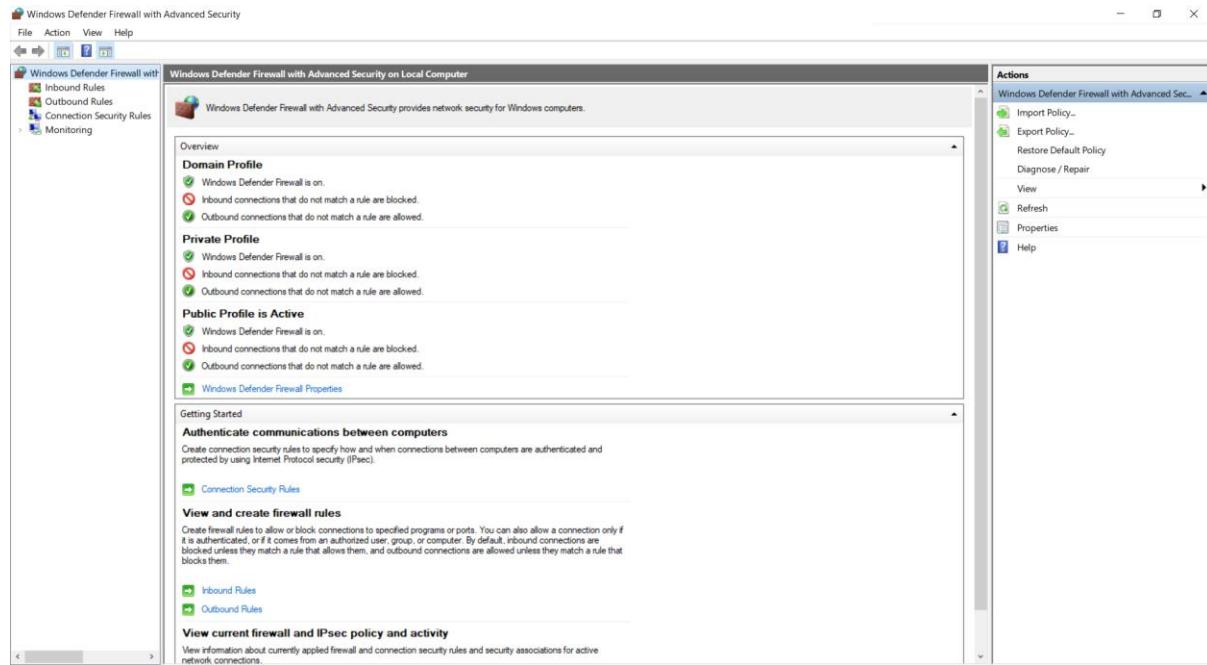
Firewall ဆိုတာက network ထဲကိုခွင့်ပြုချက်မရှိပဲ ဝင်ရောက်အသုံးပြုမှုကို ကာကွယ်ပေးတာဖြစ်ပါတယ်။ အလွယ်မှတ်ရရင် inbound နဲ့ outbound တို့ကို allow/deny စတဲ့ policies တွေကိုသတ်မှတ်ပေးတာဖြစ်ပါတယ်။ Firewall အမျိုးစား တွေကိုအောက်မှာဆက်ပြီးဖော်ပြုပေးထားပါတယ်။



- **Host-based firewall:** ဒါကတော့ application firewall လိုခေါ်ဆိုနိုင်ပြီး Operating System (ဥပမာ - Windows) ထဲမှာ default ပါဝင်တဲ့ firewall ဖြစ်ပါတယ်။ Windows မှာ firewall ကိုအသုံးပြုချင်တယ်ဆိုရင် run box ကနေ firewall.cpl ဆိုပြီးရိုက်လိုက်ပါ။



Rules တွေကိုသတ်မှတ်ချင်တယ်ဆိုရင်တော့ Advanced settings ထဲကိုဝင်လိုက်ပါ။



**Network-based firewall:** Network safe ဖြစ်ဖို့အတွက်အသုံးပြုတဲ့ hardware firewall ဖြစ်ပါတယ်။ သူ့ရဲ့အဓိကလုပ်ဆောင်ချက်ကတော့ လိုအပ်တဲ့ ports တွေကို ဖွင့်ပေးတာဖြစ်ပါတယ်။ အဓိကအသုံးပြုတဲ့နေရာကတော့ edge မှာ unauthorized access ကိုကာကွယ်ဖို့အတွက်အသုံးပြုပါတယ်။

**Stateful firewall:** Stateful firewall ကို OSI ရဲ့ Layers 3 နဲ့ Layers 4 မှာအသုံးပြု ပါတယ်။ အဓိကအသုံးပြုတာကတော့ network မှာလာရောက် ချိတ်ဆက်တဲ့ connection တွေရဲ့ incoming traffic တွေကို analyzing လုပ်ပြီး risk ဖြစ်နိုင်ခြေားတာကိုရှာပါတယ်။

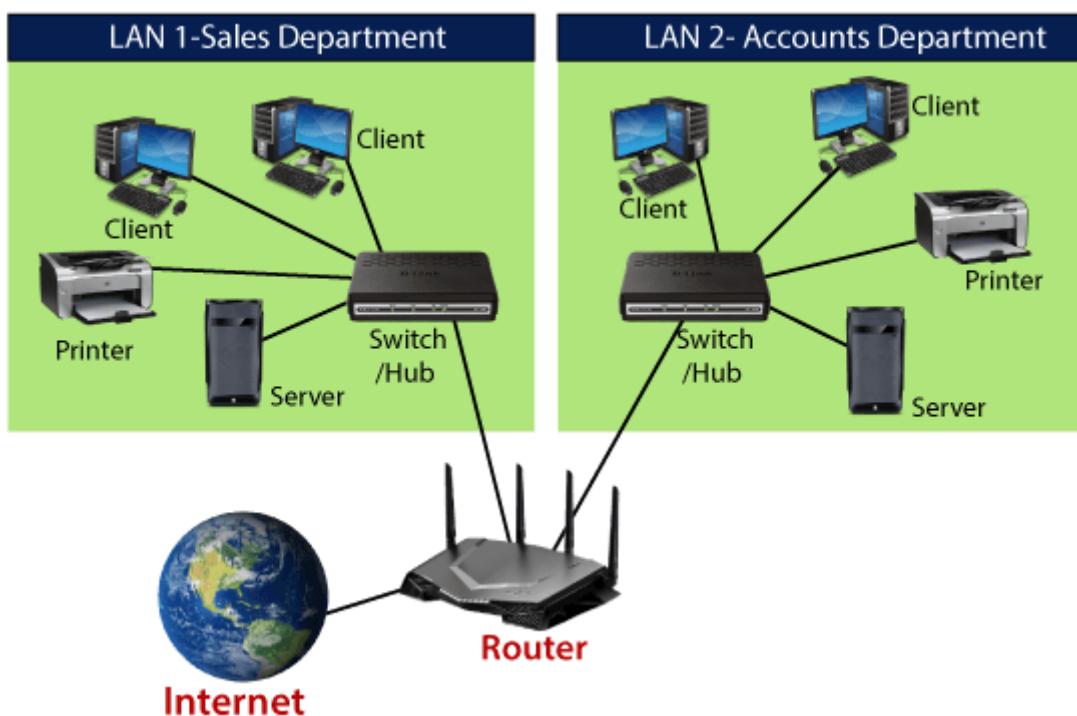
**Stateless firewall:** Stateless firewall တွေကိုတော့ packet-filtering firewall လို့လဲ ခေါ်ပါတယ်။ သူ့ရဲ့လုပ်ဆောင်ချက်ကတော့ Network ထဲကိုခွင့်ပြုချက် မရှိပဲဝင်လာတဲ့ packet တွေကိုစောင့်ကြည့်တာဖြစ်ပါတယ်။

**Web Application Firewall (WAF):** Web Application Firewall ကတေသာ ရှင်းပါတယ် Web application တွေကို secure ဖြစ်စေနိုင်အတွက် အသုံးပြုတာ ဖြစ်ပါတယ်။

**Unified Threat Management Firewall (UTM):** UTM ဆိုတာက multipurpose firewall ဖြစ်ပါတယ်။ သူကဘာတွေလုပ်ဆောင်နိုင်လဲဆိုရင် Malware detect, Content & URL filtering တွေကိုလုပ်ဆောင်နိုင်ပါတယ်။ All-in-one security appliance လိုလဲခေါ်ဆိုနိုင်ပါတယ်။

## Router

မတူညီတဲ့ network (2) ခုကို connect လုပ်ဖို့အတွက်အသုံးပြုတဲ့ device ဖြစ်ပါတယ်။ Router ကို company တွေကနေ တခြား networks တွေကို access လုပ်ချင်တဲ့ အခါအသုံးပြုကြပါတယ် ဥပမာပြာရရင် Internet ပါ။ Router ထဲမှာဆိုရင် routing table ရှိပါတယ်။ ဝင်လာတဲ့ packet တွေက routing table ကိုကြည့်ပြီးမှ receiver ထံကိုသွားတာဖြစ်ပါတယ်။



**Access Control List (ACL):** Router ရဲ့ external interface မှာဆိုရင် ACL ကို အသုံးပြုပါတယ်။ ACL ဆိုတာက incoming traffic တွေကို filter လုပ်တာဖြစ်ပါတယ်။ ဘာတွေသုံးပြီး filter လုပ်လဲဆိုရင်

- Port number
- Protocol
- IP address

တို့ဖြစ်ပါတယ်။

**Anti-spoofing:** Anti-spoofing ကိုတော့ router ရဲ့ inside interface မှာအသုံးပြုတာဖြစ်ပြီး packet တွေကို subnet ရဲ့ address range အတွင်းမှလာတာ ကိုပဲ allow လုပ်ပေးပါတယ်။ မမှန်တဲ့ source address မှလာတဲ့ packets တွေကို တော့ရှင်းပစ် လိုက်ပါတယ်။

### Intrusion-prevention system (IPS)

Intrusion-Prevention Systems (IPS) မှာဆိုရင် အမျိုးစား (၂) ခုရှိပါတယ်။ ပထမတစ်ခုက Network Intrusion Prevention System (NIPS) ဖြစ်ပြီး Network ပေါ်မှာပဲလုပ်ဆောင်တာဖြစ်ပါတယ် host မှာတော့မလုပ်ဆောင်ပါဘူး။ ဒုတိယတစ်ခု ကတော့ Host Intrusion Prevention System (HIPS) ဖြစ်ပြီး host machine မှာပဲလုပ်ဆောင်ပါတယ်။ Network ပေါ်မှာမလုပ်ဆောင်နိုင်ပါ။ NIPS က internal network device တစ်ခုဖြစ်ပြီး network ကို access လာလုပ်တာတွေကို ကာကွယ်ပေးပါတယ်။ NIPS ကိုတော့ firewall ရဲ့အနောက်မှာထားရပါတယ်။

### Intrusion-detection system (IDS)

Intrusion-Detection System (IDS) ကလဲ IPS လိုပါပဲ သူ့မှာတော့ HIDS ပဲရှိတာဖြစ်ပြီး host မှာပဲအလုပ်လုပ်ဆောင်တာဖြစ်ပါတယ်။ အဲ ၂ ခုကိုစာဖတ်သူတို့ မြင်သာအောင်ပြောရရင် IDS က နာမည်ကြီးစုံထောက် ရှားလေ့ဟုမ်း နဲ့တူပါတယ် ဘာကြောင့်လဲဆိုတော့ သူကစုံစမ်းစစ်ဆေးတာဖြစ်တာကြောင့်ပါ။ NIPS ကတော့

ဘာနဲ့တူလဲဆိုရင် Rambo နဲ့တူပါတယ် သူကတော့နှစ်နှင်းတဲ့နေရာမှာအသုံးပြုတဲ့ အတွက်ပါ။

### Modes of detection

NIPS/NIDS တို့မှာ detection အတွက်အသုံးပြုတဲ့ modes (3) ခုရှိပါတယ်။ အဲဒါတွေကတော့

- Signature-based
- Anomaly-based
- Heuristic/behavioral-based

တို့ပဲဖြစ်ပါတယ်။

### Modes of operation

NIPS/NIDS တို့မှာ operation အတွက်အသုံးပြုတဲ့ modes (2) ခုရှိပါတယ်။ အဲဒါတွေကတော့

- **Inline:** NIPS ကို firewall နဲ့အနီးဆုံးနေရာမှာထားတာဖြစ်ပြီး inline mode ကိုအသုံးပြုထားတဲ့အချိန်မှာဆိုရင် traffic တွေက NIPS ကနေဖြတ်ပြီးသွားမှာဖြစ်ပါတယ်။ အဲဒါကို in-band လို့ခေါ်ပါတယ်။
- **Passive:** ဒီ mode မှာတော့ traffic က NIPS ကနေဖြတ်မှာမဟုတ်ပါဘူး။ ပုံမှန်အနေထားမှာ ဒီ mode ကိုအသုံးပြုခြင်းအားဖြင့် local network ထဲမှာ traffic ပုံစံပြောင်းသွားမှသာ NIDS က detects သိမှာဖြစ်ပါတယ်။ ဒါကိုတော့ out of band လို့ခေါ်ပါတယ်။

### Monitoring data

Data တွေကို analyze လုပ်တဲ့အခါ IPS/IDS တို့မှာသတ်မှတ်ထားတဲ့ rules ပေါ်မှုတည်ပြီး လုပ်ဆောင်တာဖြစ်ပါတယ်။ အဲလိုလုပ်ဆောင်တဲ့အခါ မတူညီတဲ့ အမျိုးစား (J) ခုရှိပါတယ်။

- **False positive:** NIDS/NIPS တိုက attack ဖြစ်တဲ့အခါရရှိထားတဲ့ information ပေါ်မှုတည်ပြီးဆုံးဖြတ်တာဖြစ်ပါတယ်။ ဒါပေမယ့် network administrator က attack ဖြစ်တာဟုတ်မဟုတ် ကိုပြန်စစ်ဆေးဖို့လိုအပ်ပါတယ်။
- **False negative:** NIDS/NIPS က attack နဲ့ပတ်သက်ပြီးမည်သည့် detection မှမရှိတဲ့အခါ update မလုပ်ဆောင်ပါဘူး။

## Switch

Switch ဆိုတာက local-area network ထဲမှာရှိ device တွေကို users တွေက connect လုပ်ဖို့အတွက်အသုံးပြုတဲ့ device ဖြစ်ပါတယ်။ Switch မှာ connect လုပ်ထားတဲ့ host တွေရဲ့ MAC addresses table ပါဝင်ပါတယ်။ Switch မှာ security အတွက်လုပ်ဆောင်လိုရတာတွေကတော့-

- **Port security:** Port security ဆိုတာက ခွင့်ပြုချက်မရှိတဲ့ users တွေက wall-jack ports တွေမှာ laptop တွေကို network cable မှတစ်ဆင့်လာရောက် ချိတ်ဆက်ခြင်းကိုကာကွယ်တာဖြစ်ပါတယ်။
- **802.1x:** Port security အတွက် network administrator က 802.1x ကို အသုံးပြုပါတယ်။ အဲလိုအသုံးပြုတဲ့အခါ port မှာချိတ်ဆက်ခြင်တဲ့ device တွေကအရင်ဆုံး authenticated လုပ်ဆောင်ရပါတယ်။ အဲဒါမှသာ connect လုပ်နိုင်မှာဖြစ်ပါတယ်။
- **Flood guard:** MAC flooding နဲ့ Denial of Service attacks တို့လို attack တွေဖြစ်ခဲ့ရင် switch ကအရင်ဆုံး attack တွေကိုအမျိုးစားခဲ့ခြားပါတယ် ပြီးတော့ အဲဒီ attack တွေကိုကာကွယ်ပါတယ်။
- **Loop protection:** တစ်ကယ်လို့ switches တွေအများကြီးကို တွဲပြီးအသုံးပြုတဲ့ အခါ loop ဖြစ်စေတဲ့ broadcasts တွေဖန်တီးနိုင်ပါတယ်။ အဲအခါ ကျွန်တော်တို့ က Spanning Tree protocol ကိုအသုံးပြုပြီးကာကွယ်နိုင်ပါတယ်။ အဲ

protocol ကိုအသုံးပြုခြင်းအားဖြင့် forwarding, listening နဲ့တချို့မသုံးတဲ့ ports တွေကို block လုပ်နိုင်ပါတယ်။

### Layer 3 switch

OSI reference model မှာဆိုရင် ပုံမှန် switch က layer 2 မှာလုပ်ဆောင်တာဖြစ်ပါတယ်။ သို့သော် layer 3 switch တွေကတော့ network layer မှာလုပ်ဆောင်တာဖြစ်ပြီး IP address ကိုအသုံးပြုတာဖြစ်ပါတယ်။ ပြီးတော့ သူက router လိုမျိုး packets တွေကို route တဲ့အတွက် switch ထပ်ပိုပြီး performance ပိုကောင်းပါတယ်။ နောက်ပြီး IP နဲ့ MAC address ကိုတွဲပြီးသုံးတာမဟုတ်တဲ့အတွက် Layer 2 မှာဖြစ်တဲ့ ARP attacks ဖြစ်ပေါ်ခြင်းမှလဲကာကွယ်နိုင်ပါတယ်။

### Remote access

Remote access ဆိုတာက server ထဲကို network မှတစ်ဆင့် access လုပ်ခြင် တဲ့အခါအသုံးပြုပါတယ်။ အဲလိုအသုံးပြုတဲ့အခါ အဓိကအမျိုးစား (j) ခုကိုအသုံးပြုပါတယ်။

- **Remote Access Server (RAS):** ဒါကတော့ server က company network တွင်းမှာရှိနေပြီး ကျွန်တော်တို့က ပြင်ပတဗြား network ကနေ access လုပ်ခြင်တယ်ဆိုရင် ကျွန်တော်တို့ရဲ့ computer မှာ client software ကို install လုပ်ပြီး communication လုပ်ဖို့အတွက် allow လုပ်ပေးဖို့လိုအပ်ပါတယ်။ နှစ်ဖက်စလုံးကတော့ internet access ရှိဖို့လိုအပ်ပါတယ်။
- **Virtual Private Network (VPN):** သူကလဲ RAS လိုပဲ company's network မှာရှိနေတဲ့ resource တွေကိုပြင်ပကတစ်ဆင့် access လုပ်ဖို့အတွက်အသုံးပြုတာဖြစ်ပါတယ်။ ဒါပေမယ့် VPN ကပိုပြီးတော့ဈေးသက်သပါတယ်။ ဥပမာ wi-fi free ရတဲ့နေရာတွေကပါ access လုပ်လိုရနိုင်တာကြောင့်ဖြစ်ပါတယ်။ နောက် secure ဖြစ်ဖို့အတွက် tunnel

protocol တွက်အသုံးပြုထားပါတယ်။ အမိက tunneling protocols တွကတော့

- **L2TP/IPsec:** Secureဖြစ်ဖို့အသုံးပြုတဲ့ tunneling protocol တွက  
က certification, Kerberos authentication ဒါမှမဟုတ်  
preshared key တိုကိုအသုံးပြုပြီး authenticate လုပ်ပါတယ်။
- **Secure Socket Layer (SSL) VPN:** Systems တွမှာ SSL  
Certification ကို authentication အသုံးပြုတာဖြစ်ပါတယ်။

ဆက်ပြီးတော့ tunneling protocol တွေအကြောင်းကိုဆက်လေ့လာ ကြည့်ရအောင်။

### **Virtual private network using L2TP/IPSec**

Protocols တွေအကြောင်းကိုမလေ့လာခဲ့ encryption အကြောင်းနည်းနည်း  
လောက်လေ့လာကြည့်ရအောင်။ Encryption မှာဆိုရင် asymmetric နဲ့ symmetric  
ဆိုပြီး (၂) မျိုးရှိပါတယ်။ Encryption ဆိုတာက plain text data တွကိုပို့ဆောင်တဲ့  
အခါ ciphertext အနေနဲ့ပြောင်းလဲလိုက်တာဖြစ်ပါတယ်။ အဲလိုပြောင်းလိုက်တဲ့အခါ  
data တွကအလွယ်တကူဖတ်လို့မရတော့ပါဘူး။ VPN ရဲ့အရေးကြီးတဲ့အချက်တွကို  
အောက်မှာဆက်ပြီးတော့ဖော်ပြပေးထားပါတယ်။

- **Asymmetric encryption:** Encryption အတွက်ဆိုရင် certificates တွကို  
အသုံးပြုပါတယ် အဲလိုအသုံးပြုတဲ့အခါ private key နဲ့ public key ဆိုပြီး keys  
(2) ခုကိုအသုံးပြုပါတယ်။ Public key ကတော့ encrypting အတွက်အသုံးပြု  
တာဖြစ်ပြီး private key ကိုတော့ data တွကို decrypting ပြန်လုပ်ဖို့အတွက်  
အသုံးပြုပါတယ်။
- **Symmetric encryption:** Asymmetric မှာလို key 2 ခုကိုမသုံးတော့ပဲ key  
တစ်ခုထဲနဲ့ပဲ data တွကို encrypting, decrypting လုပ်ဆောင်ပါတယ်။  
အဲလိုလုပ်ဆောင်ခြင်းဟာ ပိုမြန်တယ်ဆိုပေမယ့် asymmetric encryption  
ထပ်စာရင်တော့ secure ပိုင်းမှာ စိတ်မချရပါဘူး။

- **Key length:** Certificate keys ထဲမှာပါတဲ့ units တွေကို bits လိုခေါ်ပါတယ်။ Bits နည်းလေ encrypt နဲ့ decrypt လုပ်တဲ့အချင်ပိုပြီးတော့မြန်လေဖြစ်ပါတယ်။ တစ်ကယ်လို့ bits တွေများခဲ့မယ်ဆိုရင် encrypt နဲ့ decrypt လုပ်တဲ့ အချင်ကပိုကြာပေမယ့်ပိုပြီးတော့ secure ဖြစ်ပါတယ်။ ဒါကြောင့် asymmetric keys တွေကို 4096 bits အောက်ကိုမသုံးသင့်ပါဘူး။

ရုံးက server တွေကို အိမ်ကနေ access ရခြင်တဲ့အခါ ကျွန်တော်တို့က internet ကဖြတ်ပြီးတော့ VPN tunnel တွေကို create လုပ်ဖို့လိုအပ်ပါတယ်။ အဲလိုလုပ်တဲ့အခါ L2TP/IPSec tunnel ကိုအသုံးပြုရပြီးသူက OSI ရဲ့ Layer 2 မှာလုပ်ဆောင်တာဖြစ်တာ ကြောင့် data ကို encrypt လုပ်ပါတယ်။ IPSec မှာ packet တွေကို မတူညီတဲ့အပိုင်း (၂) ပိုင်းအဖြစ်ပုံစံပြောင်းပါတယ်။

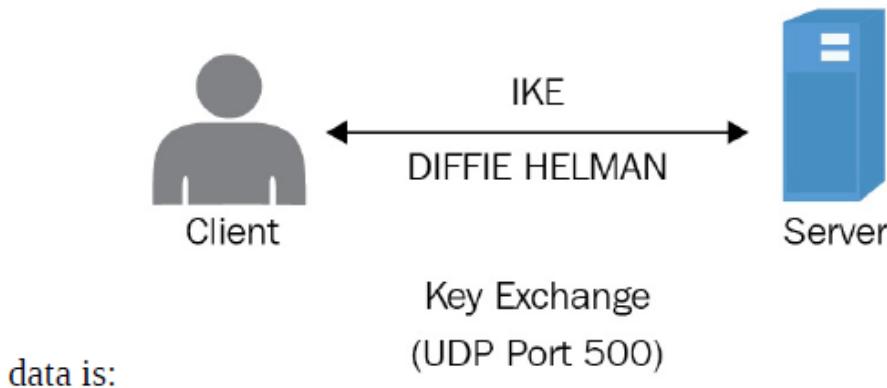
- **AH:** SHA-1 (160 bits) ဒါမှာမဟုတ် MD5 (128 bits) hashing တို့ပါဝင်ပါတယ်။ သူကတော့ packet header ကို transit လုပ်တဲ့အခါပြောင်းလဲလိုမရအောင်လုပ် ဆောင်ပါတယ်။
- **ESP:** DES (64 bits), 3 DES (168 bits), AES (256 bits) တို့ပါဝင်ပြီး data တွေကို transfer လုပ်တဲ့အခါ ပိုပြီးတော့မြန်ပါတယ်။

## IPSec

IPSec ကို client computer နဲ့ server ကြား secure session ဖြစ်ဖို့အတွက်ကို အသုံးပြုတာဖြစ်ပါတယ်။ IPSec ကိုအသုံးပြုခြင်းအားဖြင့် တစ်စုံတစ်ယောက်က packet sniffer လုပ်ပြီး data တွေကိုခိုးယူခြင်းမှ ကာကွယ်နိုင်ပါတယ်။

## IPSec – handshake

ပထမဦးဆုံးအဆင့်က IPSec က secure tunnel ဖြစ်ဖို့အတွက် session ကို create လုပ်တာဖြစ်ပါတယ်။ အဲလိုလုပ်တာကို security association လိုခေါ်ပါတယ်။ နောက်တစ်မျိုး IKE (Internet Key Exchange) လိုလေခေါ်နိုင်ပါတယ်။



IKE phase ၂ Diffie Hellman ကို UDP port 500 ကနေ IPsec session ကို create လုပ်တာဖြစ်ပါတယ် အဲဒါကို quick mode လိုခေါ်ပါတယ်။ အဲလို session ကို create လုပ်ပြီးသွားရင် data ကိုပို့လို့ရပြီဖြစ်ပါတယ်။

ဒုတိယအဆင့်ကတော့ data ကို DES, 3DES, AES စတာတွေကိုအသုံးပြုပြီး encrypt လုပ်တာဖြစ်ပါတယ်။ ဒီမှာဆိုရင်မတူညီတဲ့ IPsec modes (၂) မျိုးရှိပါတယ်။

- **Tunnel mode:** Tunnel mode ကတော့ IPsec session ၂ Internet ကိုအသုံးပြုတာဖြစ်ပါတယ်။
- **Transport mode:** Transport mode ကတော့ client နဲ့ server ကြားထဲက internal network အတွင်းမှာ IPsec tunnel ကို create လုပ်တာဖြစ်ပါတယ်။

### VPN concentrator

IKE phase မှာ secure tunnel ဖြစ်အောင် VPN concentrator ကိုအသုံးပြုတာဖြစ်ပါတယ်။

### SSL VPN

SSL VPN ဆိုတာက web browser ၂ encryption အတွက် SSL certificate ကိုအသုံးပြုတဲ့ VPN ဖြစ်ပါတယ်။ နောက်ပိုင်းမှာတော့ Transport Layer Security (TLS) ကိုအသုံးပြုလာကြပါတယ်။

## Data-loss prevention

Data loss prevention (DLP) ဆိုတာ users တွေက company ရဲ့ sensitive data တွေကိုအပြင်သိမပို့ဆောင်နိုင်အောင်ကာကွယ်ပေးတာဖြစ်ပါတယ်။ စာဖတ်သူ တွေမြင်သာအောင်ပြောပြရရင် data တွေပြင်ပကိုမပေါက်ကြားနိုင်အောင် ကာကွယ် တာဖြစ်ပါတယ်။ Data တွေပြင်ပကိုပေါက်ကြားစေတဲ့ sources တွေရှိပါတယ် အဲဒါ တွေကတော့

- Chat
- Server
- Cloud
- ISP
- Mobile
- USB
- Website
- Printer
- Bluetooth / wifi
- Email

စတာတွေဖြစ်ပါတယ်။

## Causes of Data Leaks

Data Leask ဖြစ်ရတဲ့အကြောင်းရင်းတွေ အများကြီးရှိပါတယ်။ အဲတဲက တချို့ကိုဖော်ပြပေးလိုက်ပါတယ်။

- **Insider threats:** Insider threats ဆိုတာက Company အတွင်းက သစ္ဓာဖောက်ဝန်ထမ်းတွေကိုဆိုလိုတာဖြစ်ပါတယ်။ Insider threats တွေက data တွေကို တခြားပြိုင်ဘက် company တွေကိုပေးခြင်း ဒါမှမဟုတ် ရောင်းချခြင်းကိုလုပ်ဆောင်ကြပါတယ်။

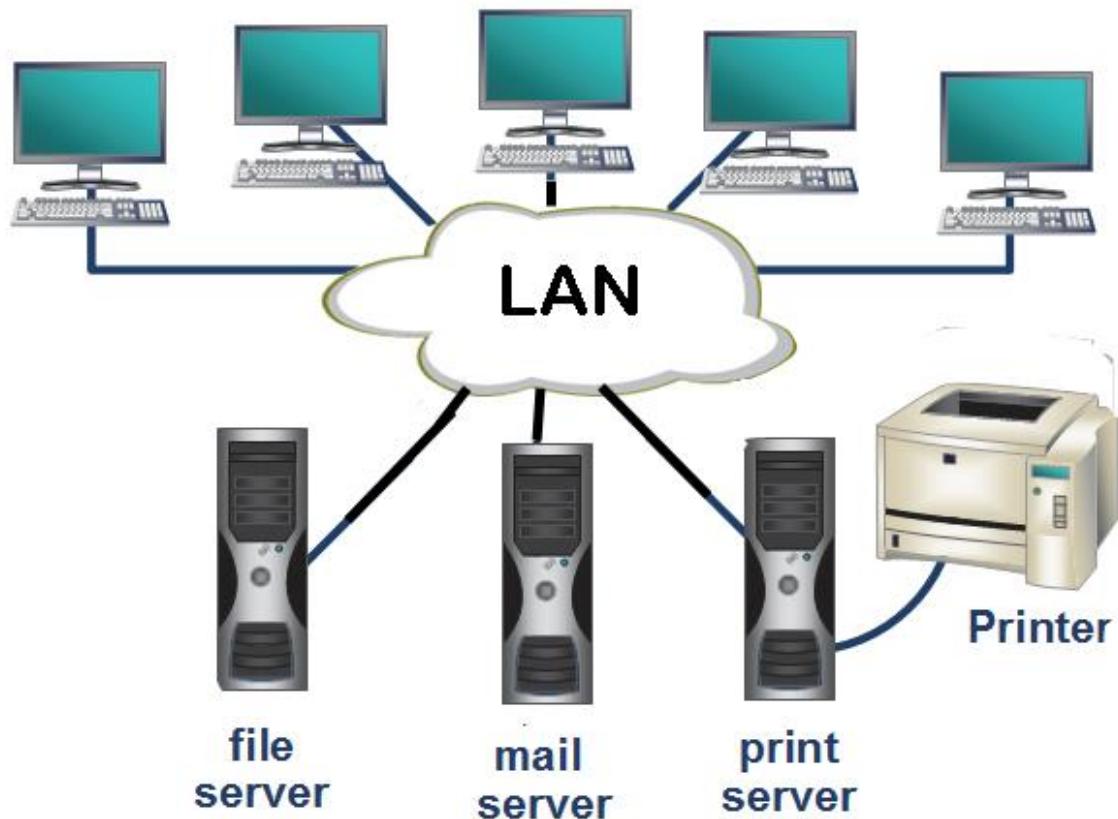
- **Extrusion by attackers:** Cyber attacks တွေဖြစ်ပွားရတဲ့အကြောင်း တွေထဲက တစ်ခုက data တွေကိုရယူခြင်လိုဖြစ်ပါတယ်။ Attacker က phishing, malware, code injection စတဲ့နည်းလမ်းတွေကိုအသုံးပြုပြီး data တွေကိုရရှိအောင်ကြီးစားကြပါတယ်။
- **Unintentional or negligent data exposure:** Data leaks တွေဖြစ်ရတဲ့နောက်တစ်ချက်ကတော့ ပေါ့စတဲ့ ဝန်ထမ်းတွေကြောင့်လဲဖြစ်နိုင်ပါတယ်။ ဒါပေမယ့် သူတို့ကတော့ insider တွေလိုရည်ရွယ်ချက်ရှိရှိ လုပ်ဆောင်တာမျိုးတော့မဟုတ်ပါဘူး။

အခုက္ခန်တော်ဖော်ပြပေးသွားတာတွေကတော့ Data leaks ဖြစ်နိုင်တဲ့ နည်းလမ်းတရာ့ပဲဖြစ်ပါတယ်။

### Secure network architecture concepts

Company တစ်ခုရဲ့ network လုပ်ခြုံရေးဆိုတာ အဓိကအရေးကြီးတဲ့အပိုင်းမှာပါဝင်ပါတယ်။ Unauthorized access တွေကိုကာကွယ်ဖို့အတွက်ဆိုရင် မတူတဲ့ zones တွေနဲ့ topologies တွေကိုအသုံးပြုခြင်း၊ network တွေကိုခွဲထားခြင်း၊ Firewall တွေကိုအသုံးပြုခြင်း စတဲ့နည်းလမ်းတွေကိုအသုံးပြုနိုင်ပါတယ်။ အခုက္ခန်တော်တို့ မတူညီတဲ့ zones နဲ့ topologies တွေအကြောင်းကိုလေ့လာကြည့်ရအောင်။ Zones တွေမှာဆိုရင် LAN, WAN, DMZ ဆိုပြီး (၃) မျိုးရှိပါတယ်။

- **Local Area Network (LAN):** ဒါကတော့ Internal / Local မှာအသုံးပြုတဲ့ network ဖြစ်ပါတယ်။ အဲ့ network ကိုအသုံးပြုပြီးတော့ files sharing, remote access, print sharing စတာတွေကိုလုပ်ဆောင်နိုင်ပါတယ်။ LAN ကိုတော့ cable, wireless စတာတွေနဲ့ချိတ်ဆက်အသုံးပြုနိုင်ပါတယ်။ အောက်မှာ LAN ရဲ့ simple ပုံလေးကိုဖော်ပြပေးထားပါတယ်။

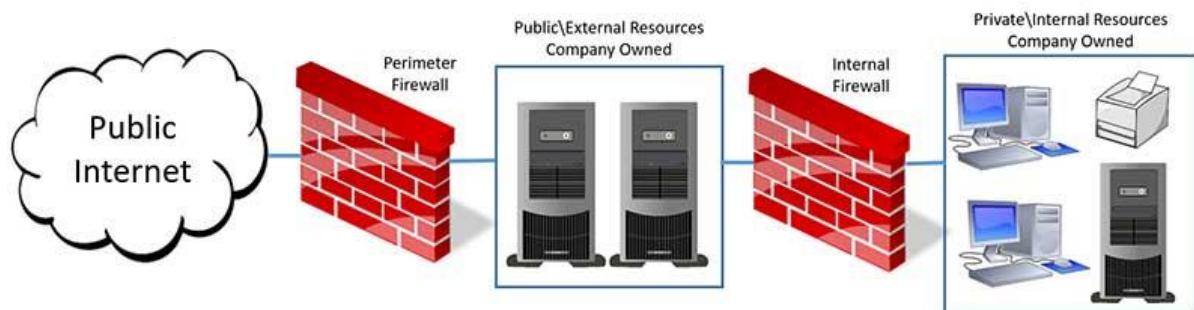


- **Wide Area Network (WAN):** WAN ကတေသာ အခုက္ခန်တော်တို့အသုံးပြုနေတဲ့ internet ကိုပြောတာဖြစ်ပါတယ်။ စာဖတ်သူတို့မြင်သာအောင်ပြောရရင် ကျွန်ုင်တော်တို့အိမ်ကတေသာ [www.google.com](http://www.google.com) ဆိုတဲ့ website ကို access လုပ် နိုင်ခြင်းနောက် google drive ကိုအသုံးပြုပြီး files တွေ sharing လုပ်နိုင်ခြင်း စတာတွေဟာ WAN ကိုအသုံးပြုထားတာကြောင့်ဖြစ်ပါတယ်။ အောက်မှာ WAN နဲ့သာက်ဆိုင်တဲ့ simple ပုံကိုဖော်ပြပေးထားပါတယ်။



- **Demilitarized Zone (DMZ)** : DMZ ဆိုတာက LAN နဲ့ WAN တို့ရဲ့ကြားထဲမှာ ရှိတဲ့ zone ကိုပြောတာဖြစ်ပါတယ်။ Public ကနေ access လုပ်စေခဲ့တဲ့ services တွေဖြစ်တဲ့ E-mail server, FTP server, Web server တို့ကို DMZ မှာ ထားခြင်းအားဖြင့် public ကနေ access လုပ်ဆောင်လိုပါတယ်။ Companies တွေက public ကိုပေးချင် တဲ့ information တွေကို DMZ မှာထားတဲ့ web server ပေါ်မှာတင်ထား လေ့ရှိပါတယ်။ DMZ ကိုအသုံးပြုခြင်းအားဖြင့် မလိုအပ် တဲ့ traffic တွေ internal network ထဲကိုဝင်ရောက်လာခြင်းမှာလဲ ကာကွယ်နိုင်ပါတယ်။ အောက်မှာ DMZ ရဲ့ simple ပုံလေးကိုဖော်ပြထားပါတယ်။

## DMZ (Demilitarized Zone)

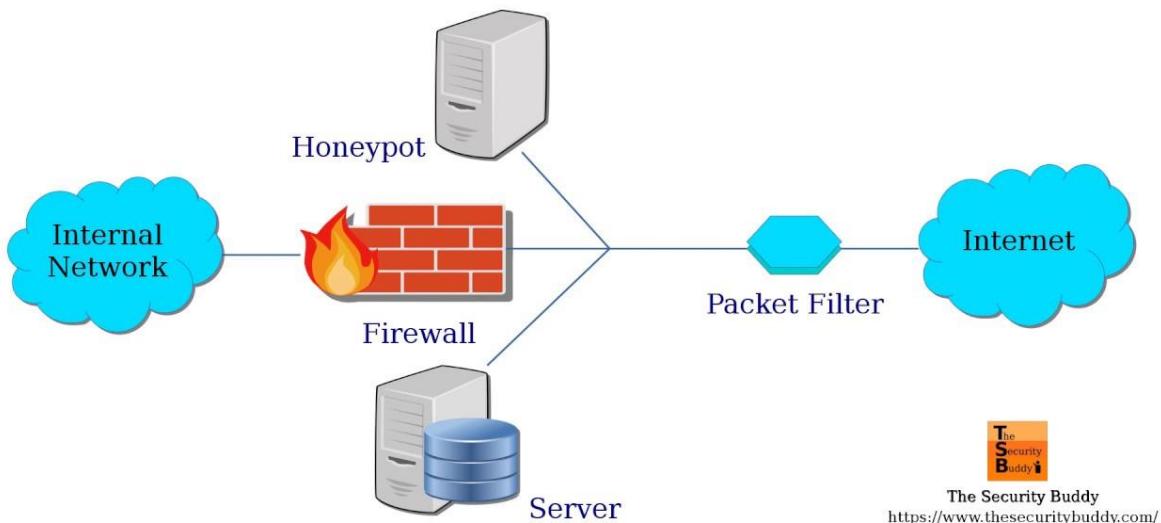


## Honeypot

Honeypot ဆိုတာက ထောင်ချောက်ဖြစ်ပါတယ်။ ဘယ်လိုမျိုးလဲဆိုရင် ဥပမာ [www.google.com](http://www.google.com) ဆိုတာကတရားဝင်လက်ရှိအသုံးပြုနေတဲ့ website တစ်ခုဖြစ်ပါတယ်။ အဲဒီ website ကို attacker တွေကတိုက်ခိုင်လာနိုင်ခြေရှိတဲ့အတွက် google security team က ပုံစံတူ website တစ်ခုကို create လုပ်ပါတယ် ဒါပေမယ့် website ရဲ့ security ကတော့ သိပ်မကောင်းဘူးပေါ့။ အဲဒီပုံစံတူ website ကို attacker တွေက တိုက်ခိုက်အောင်မြင်သွားတယ်စိုပါစို့ attacker တွေကတစ်ကယ့် website ကိုရသွားတယ်ထင်မိတက်ပါတယ်။ သူတို့အမှန်ရသွားတဲ့ site က ပုံစံတူ website တစ်ခုသာဖြစ်ပါတယ်။ အဲလို honeypot ကိုအသုံးပြုခြင်းအားဖြင့် attacker တွေတိုက်ခိုက်လာနိုင်တဲ့ နည်းလမ်းတွေကိုသိရှိပြီး ကြိုတင်ကာကွယ်မှုတွေကို လုပ်ဆောင်လာနိုင်မှာဖြစ်ပါ

တယ်။ နောက် honeypots တွေကို group အနေဖြင့် အသုံးပြုတာကိုတော့ honeynet လို့ ခေါ်ပါတယ်။ အောက်မှာ honeypot ရဲ့ diagram ကိုပြပေးထားပါတယ်။

## Honeypot



## Secure Socket Layer accelerators

Secure Socket Layer (SSL) ကို data တွေပို့ဆောင်တဲ့ အခါ ကြားဖြတ်ခိုးယူ ခြင်း တွေက နောက် ကွယ်ဖို့ အတွက် encrypt လုပ်ဖို့ အသုံးပြုတာဖြစ်ပါတယ်။ ဒါပေမယ့် တချို့ server တွေ ဥပမာ database servers တွေမှာ ဆိုရင် SSL encryption လုပ် ဆောင်ခြင်းက CPU တွေကိုပို့ပြီး အသုံးပြုပေါ်တယ်။ အဲလို့ အခါမျိုး တွေမှာ ဆိုရင် SSL acceleration ကို အသုံးပြုပြီး SSL encryption, decryption လုပ်ဆောင်တဲ့ အခါ CPU ပို့အသုံးပြုခြင်း မှာ သာက်သာ ပေါ်တယ်။

## SSL/TLS decryptor

ကျွန်ုတ်တို့ network ထဲကို internet က နောက်လာတဲ့ traffic တွေက encrypted လုပ်ထားတာ တွေဖြစ်ပါတယ်။ အဲအခါ Firewall, NIPS, NIDS, DLP နဲ့ တခြားသော network devices တွေက data တွေကို ခြားလို့ မရပါဘူး။ အဲဒါကြောင့် traffic တွေက firewall ကိုဖြတ်လာပြီး တဲ့ အခါ SSL/TLS decryptor တွေက data တွေကို inline NIPS ကိုမဖြတ်ခင် decrypt လုပ်ပါတယ်။ ဒါဟာဘာကို ဆိုလိုတာလဲ

ဆိုရင် NIPS တွေက malicious traffic တွေ local area network ကို access မလုပ်နိုင်အောင်ကာကွယ်ပေးတာဖြစ်ပါတယ်။

## DDoS mitigator

Distributed Denial of Service (DDoS) attack ဆိုတာက traffic တွေအများကြီးက server တစ်ခုထဲဆီကိုစုပ်ပြုဝင်ရောက်လာခြင်းဖြစ်ပါတယ်။ အဲလိုဝင်ရောက်လာတဲ့အခါ server က overwhelmed ဖြစ်ပြီး အလုပ်မလုပ်ဆောင်နိုင်တော့ပါဘူး။ DDoS mitigator ဆိုတာက device ဖြစ်ပါတယ် အရင်အပိုင်းမှာလေ့လာခဲ့ရတဲ့ stateful firewall လို့မျိုးပေါ့။

## Implementing secure protocols

Protocol အကြောင်းလေးအရင်ရှင်းပြပေးပါမယ်။ Protocol ဆိုတာက network တွေချိတ်ဆက်ပြီးအသုံးပြုလို့ရအောင် ကြားကနေလုပ်ဆောင်ပေးတာကို protocol လို့ခေါ်ပါတယ်။ ဥပမာ Remote access တွေကို RDP (Remote Desktop Protocol) ကိုအသုံးပြုပါတယ် website တွေကြည့်ဖို့အတွက်ဆိုရင် http(Hyper Text Transfer Protocol) ကိုအသုံးပြုပါတယ်။ အဲဒီ protocols တိုင်းမှာသူတို့နဲ့သက်ဆိုင်တဲ့ port number တွေရှုပါတယ်။ Protocol မှာအမျိုးစား (j) မျိုးရှုပါတယ်။ အဲဒါတွေက တော့ TCP (Transmission Control Protocol) နဲ့ UDP (User Datagram Protocol) တို့ပဲဖြစ်ပါတယ်။ သူတို့အကြောင်းတွေကို သင်ခန်းစာ အစမှာရှင်းပြခဲ့ပြီးသားဖြစ်တဲ့ အတွက်ကြောင့် ဆက်မရှင်းတော့ပါဘူး။ အခုကျွန်တော်တို့ အသုံးများတဲ့ ports တွေအကြောင်းကိုဆက်လေ့လာကြည့်ရအောင် အောက်မှာ table နဲ့ဖော်ပြပေးထားပါတယ်။

Protocol	UDP/TCP	Port	Use
File Transfer Protocol (FTP)	TCP	21	File transfer
Secure Shell (SSH)	TCP	22	Run remote command (securely)
Secure Copy Protocol (SCP)	TCP	22	Secure copy to Unix/Linux
Secure FTP (SFTP)	TCP	22	Secure FTP download
Telnet	TCP	23	Run remote command (unsecure)
Simple Mail Transfer Protocol (SMTP)	TCP	25	Transport mail between Mail servers
Domain Name System (DNS)	UDP	53 53 53	Host name resolution Zone transfer Name queries
Dynamic Host Configuration Protocol (DHCP)	UDP	67/68	Automatic IP address allocation
Trivial File Transfer Protocol	UDP	69	File Transfer using UDP
Hypertext Transfer Protocol	TCP	80	Web browser
Kerberos	TCP	88	Microsoft authentication using tickets
Post Office Protocol 3	TCP	110	Server, no copy left on mail server
NETBIOS	UDP	137-139	NETBIOS to IP address resolution

Internet Message Access Protocol (IMAP 4)	TCP	143	Pull mail from mail server
Simple Network Management Protocol (SNMP)	UDP	161	Notifies the status and creates reports on network devices
Simple Network Management Protocol Version 3 (SNMP v3)	UDP	162	Secure version of SNMP
Lightweight Directory Access Protocol (LDAP)	TCP	389	Stores X500 objects, searches for active directory information
Lightweight Directory Access Protocol Secure (LDAPS)	TCP	636	Secure LDAP where the session is encrypted
Secure Internet Message Access Protocol (IMAP 4)	TCP	993	Secure IMAP4
Secure Post Office Protocol 3	TCP	995	Secure POP3
File Transfer Protocol Secure (FTPS)	TCP	989/990	Download of large files securely
Remote Desktop Protocol	TCP	3389	Microsoft remote access
Session Initiated Protocol (SIP)	TCP	5060/5061	Connects internet-based calls
Secure Real Time Protocol (SRTP)	TCP	5061	Secure voice traffic

## Wireless Security

Wireless security ကို encryption မလုပ်ပဲ ပုံမှန်အတိုင်း secure ဖြစ်အောင်လုပ်လိုရတဲ့ မည်းလမ်း (၃) ခုရှိပါတယ်။

- **Default username and password:** ကျွန်တော်တို့ network device တွေထဲတဲ့ အခါ default username & password တွေပါဝင်ပါတယ်။ တစ်ကယ်လို့ ကျွန်တော်တို့တွေ devices တွေကိုစပြီးအသုံးပြုတော့မယ်ဆိုရင် default username & password တွေကိုပြောင်းလဲဖို့လိုအပ်ပါတယ်။ အဲလိုပြောင်းလဲတဲ့ အခါမှာလဲ credentials တွေကို အလွယ်တကူမရနိုင်ဖို့ special character တွေပါထည့်သွင်းအသုံးပြုသင့်ပါတယ်။
- **Disable the SSID:** SSID ဆိုတာက wireless network ရဲ့ network name ကို ပြောတာဖြစ်ပါတယ်။ ပုံမှာဆိုရင် ကျွန်တော်တို့ရဲ့ Laptop တို့ smart phone တို့ကို wireless network ရှိတဲ့နေရာမှာ wifi ဖွင့်လိုက်ရင် SSID name ကို တွေ့မြင်ရမှာဖြစ်ပါတယ်။ အဲလိုမှာမြင်ရဖို့အတွက်ဆိုရင် SSID ကို hide လုပ်လိုရပါတယ်။
- **MAC filtering:** Network ချိတ်ဆက်အသုံးပြုလိုရတဲ့ မည်သည့် device တွေမှာ မဆို MAC address တွေရှိပါတယ်။ စာဖတ်သူတွေမြင်သာအောင်ပြောရရင် ကျွန်တော်တို့ပိုင်တဲ့ NRC card number တွေလိုပေါ့။ တူလိုလဲမရသလို ထပ်လို့ လဲမရပါဘူး။ MAC filtering ဆိုတာက wireless access point မှာ ချိတ်ဆက်စေချင်တဲ့ Device တွေရဲ့ MAC တွေကိုပဲ allow လုပ်ပေးထားတာဖြစ်ပါတယ်။ အဲလို allow လုပ်ပေးထားတဲ့ အခါ list ထဲမှာမရှိတဲ့ device ကလာရောက် ချိတ်ဆက်တဲ့ အခါ ချိတ်ဆက်လို့ရမှာမဟုတ်ပါဘူး။

## Wireless bandwidth/band selection

Wireless တွေမှာဆိုရင်မတူညီတဲ့ standards တွေရှိပါတယ်။ အောက်မှာ table နဲ့ပြပေးထားပါတယ်။

Standard	Frequency	Speed	Remarks
802.11 a	5 GHz	54 Mbps	5 GHz channel bandwidth is 40 MHz
802.11 b	2.4 GHz	11 Mbps	2.4 GHz channel bandwidth is 20 MHz
802.11 g	2.4 GHz	54 Mbps	
802.11 n	2.4 GHz/5Hz	150 Mbps	MIMO – Multiple Input Multiple Output and travels the furthest distance

## Wireless encryption

Wireless network တွေကို secure ဖြစ်ဖို့အတွက်အသုံးပြုတဲ့ encryption ပုံစံတွေရှိပါတယ်။ ပထမဦးဆုံးအသုံးတာကတော့ WEP ဖြစ်ပါတယ်။ အဲဒါကတော့ အားနည်းချက်တွေရှိတဲ့အတွက် သူ့ထပ်ပိုပြီး secure ဖြစ်တဲ့ WPA2-CCMP ကို နောက်ပိုင်းမှာ အသုံးပြုလာကြပါတယ်။ အခုအဲ encryption တစ်ခုချင်းဆီကို အောက်မှာဆက်ပြီးဖော်ပြုပေးထားပါတယ်။

- **Wired Encryption Privacy / Wired Encryption Protocol (WEP):** WEP ကို wireless security အတွက်ကိုအသုံးပြုတာဖြစ်ပါတယ်။ သူရဲ့ key က 40-bit ဖြစ်တဲ့အတွက် crack လုပ်ရတာအရမ်းလွယ်ကူပါတယ်။ ဒါကြောင့် WEP က security မကောင်းပါဘူး။

## Encryption Type

- 64-bit
- 128-bit

## Advantages

- Easy to configure
- Widely supported security system
- Secures your wireless network better than no encryption at all

## Disadvantages

- Not fully secure
- Other encryption protocols are more secure

➤ **Wi-Fi Protected Access (WPA and WPA2):** WPA / WPA2 က အပေါ်မှာ ကျန်တော်တို့လေ့လာခဲ့တဲ့ WEP ထပ်ပိုပြီး secure ဖြစ်ပါတယ်။

## Encryption Type

- **TKIP:** Temporal Key Integrity Protocol
- **PSK:** Pre-shared key or Personal mode. 256-bit encryption that requires a 64 hexadecimal digit password or 8 – 63 ASCII character passphrase.
- **EAP:** Extensible Authentication Protocol

## Advantages

- Easy to configure
- Strong encryption
- Easy to manage

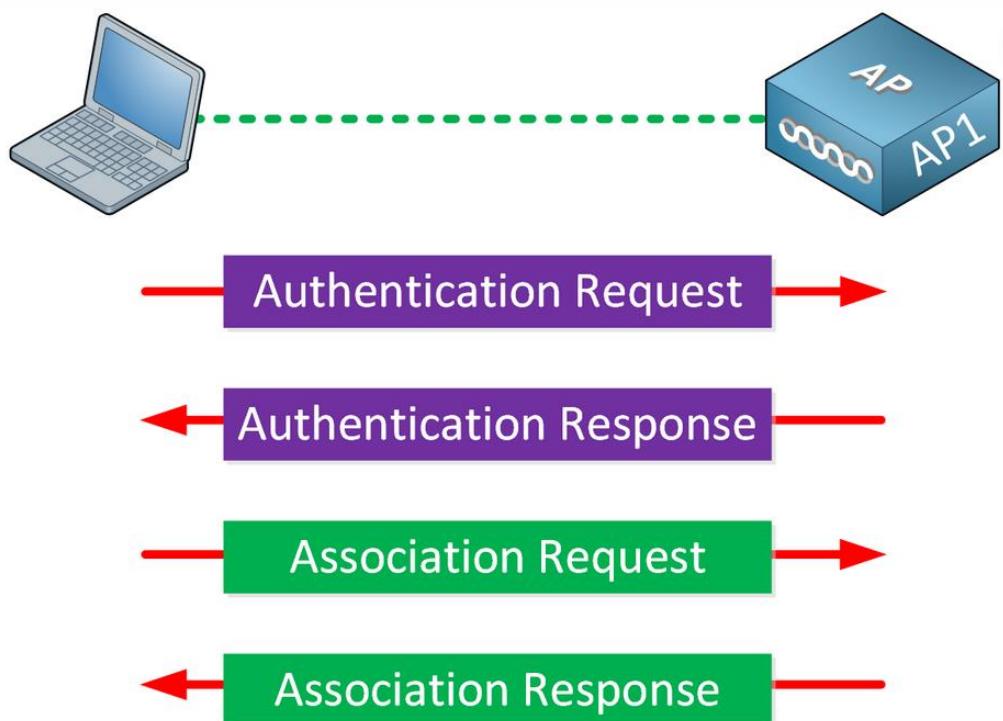
## Disadvantages

- Not supported by all devices

## Wireless – Open System Authentication

Open authentication ဆိုတာက wifi network မှာ authentication လုပ်ဖို့အတွက်အသုံးပြုတာဖြစ်ပါတယ်။ ဒီမှာဆိုရင် wireless client က authentication request ကို Access Point ကိုပိုပါတယ်။ အဲ Access Point က request ကို accepts လုပ်တဲ့အခါ authentication response ကိုပြန်ပိုပေးပါတယ်။ ဒီမှာဆိုရင် pre-shared တို့ credentials တို့မလိုအပ်ပါဘူး။ အောက်မှာ

Open system authentication ရဲအလုပ်လုပ်ဆောင်ပုံကိုပုံနှင့်တက္ကဖော်ပြုပေးထားပါတယ်။



### Wireless – WPS

WPS (Wi-Fi Protect Setup) ဆုတာက wireless device တွေက router ကိုအလွယ်တကူချိတ်ဆက်လို့ရအောင် အသုံးပြုပါတာဖြစ်ပါတယ်။ အဲမှာဆိုရင် password အတွက်ဆိုရင် router, access point တို့မှာပါတဲ့ WPS button ကိုနှိပ်ပြီး အသုံးပြုနိုင်ပါတယ်။

### Wireless – captive portal

Wireless network ကို airport, hotel စတဲ့ free ပေးတဲ့နေရာတွေမှာ ဆိုရင် wifi ကိုတန်းပြီး join လို့မရပါဘူး။ Connect လုပ်ပြီးတာနဲ့ email address, phone number စတဲ့ information တရာ့ကိုတောင်းတဲ့ webpage ကိုရောက်သွားပါတယ်။ အဲမှာ information တွေကိုဖြည့်သွင်းပြီးမှသာ internet ကိုအသုံးပြုနိုင်မှာဖြစ်ပါတယ်။

## Wireless attacks

Wireless networks မှာ attack (၂) မျိုးရှိပါတယ်။

- **Evil twin:** Evil twin ဆိုတာက attacker က fake SSID ကိုအသုံးပြုပြီး data တွေကိုရရှိအောင်လုပ်ဆောင်တာဖြစ်ပါတယ်။ စာဖတ်သူတို့မြင်သာအောင်ပြာ ရရင် Company A မှာ AAA ဆိုတဲ့ SSID name နဲ့ wifi ကို ဝန်ထမ်းတွေကအသုံး ပြုကြပါတယ်။ အဲအခါ attacker က data တွေလိုချင်တဲ့အတွက် AAA ဆိုတဲ့ SSID name နဲ့ wifi ကို ဝန်ထမ်းတွေ connect လုပ်လို့ရမယ့်နေရာလောက်က နေလွှင့်ပါတယ်။ ဝန်ထမ်းတွေကတော့ သူတို့ပုံမှန်သုံးနေကြ AAA ထင်ပြီးချိတ်ကြပါတယ်။ အမှန်သူတို့ချိတ်တာက attacker ကလွှင့်ထားတဲ့ wifi ဖြစ်နေပါတယ်။ အဲအခါ attacker ကသူ့ network ထဲကိုဝင်လာတဲ့ traffic တွေကို capture လုပ်လို့ရပြုဖြစ်ပါတယ်။ Evil twin attack ဆိုတာက Man-in-the-middle attack အမျိုးစားတဲ့က တစ်ခုဖြစ်ပါတယ်။



- **Rouge access point:** Route access point ဆိုတာက access point ကို network owner ခွင့်ပြုချက်မရှိပဲ တပ်ဆင်ထားတာကိုပြောတာဖြစ်ပါတယ်။ တစ်ကယ်လို့ attacker access point ကိုတပ်ဆင်ထားပြီဆိုရင် data တွေကိုရ ယူလို့ရပြီဖြစ်ပါတယ်။ ဒါကြောင့်မလို့ coffee ဆိုင်တွေမှာ သူတို့ network ပေါ်မှာခွင့်ပြုချက်မရှိပဲ access point တွေကိုတပ်ဆင်ပြီး data တွေကိုဖမ်းယူတာမျိုးမလုပ်ကြဖို့တားမြစ်ကြတာဖြစ်ပါတယ်။

### Wireless authentication protocols

Wireless မှာအသုံးပြုတဲ့ authentication protocol တွေကိုအောက်မှာဖော်ပြထားပါတယ်။

- **IEEE 802.1x:** IEEE 802.1x ဆိုတာက certificates ကိုအသုံးပြုတာဖြစ်ပါတယ်။ နောက်ပြီးအဲဒါကို enterprise မှာ RADIUS server နဲ့တွဲပြီးအသုံးပြုကြပါတယ်။
- **RADIUS federation:** RADIUS Federation က federation service ဖြစ်ပြီး network ကို access လုပ်ဖို့အတွက်အသုံးပြုတာဖြစ်ပါတယ်။
- **EAP:** EAP ဆိုတာက authentication framework ဖြစ်ပြီး point-to-point connections အတွက်အသုံးပြုတာဖြစ်ပါတယ်။
- **Protected Extensible Authentication Protocol (PEAP):** Protected Extensible Authentication Protocol ဆိုတာက EAP ရဲ့ version တစ်ခုဖြစ်ပြီး အလွယ်ပြောရရင် WLANS ပေါ်မှာ data တွေကို secure ဖြစ်အောင်လုပ်ဆောင်တာဖြစ်ပါတယ်။
- **EAP-FAST:** EAP-FAST ဆိုတာ wireless networks နဲ့ point-to-point connection တွေမှာ session authentication လုပ်ဆောင်တာဖြစ်ပါတယ်။
- **EAP-TLS:** EAP-TLS ဆိုတာ TLS public key certification authentication ကိုလုပ်ဆောင်တဲ့နည်းလမ်းဖြစ်ပါတယ်။ Client ကနေ Server, Server ကနေ Client အပြန်လုန် authentication လုပ်ဆောင်ဖို့အတွက်ဖြစ်ပါတယ်။

- **EAP-TTLS:** EAP-TTLS က phases ၂ ခုကိုအသုံးပြုပါတယ်။ ပထမဦးဆုံးအဆင့် ကတော့ server ကနေ client ကိုသွားတဲ့ session ကို secure ဖြစ်အောင်လုပ် ဆောင်တာဖြစ်ပါတယ်။ အဲနောက်မှာတော့ protocol တွေဖြစ်တဲ့ MS-CHAP က session အောင်မြင်အောင်လုပ်ဆောင်ပါတယ်။

## Chapter 4

# Computer System Security

### Malicious Software Types

Malicious software ဒါမှုမဟုတ် Malware ဆိုတာက computer system ကို ထိခိုက်အောင်လုပ်တာဖြစ်ပါတယ်။ Malware မှာဆိုရင် viruses, worms, Trojan horses, spyware, rootkits, adware စတာတွေပါဝင်ပါတယ်။

#### Viruses

Virus ဆိုတာက user တွေနားမလည်းနိုင်တဲ့ code တွေကိုအသုံးပြုပြီး computer မှာ run အောင်လုပ်ဆောင်ထားတာဖြစ်ပါတယ်။ တစ်ကယ်လို့ computer ထဲကို virus ဝင်ရောက်ခဲ့ပြုဆိုရင် တခြား program တွေကို execute လုပ်ဆောင်နိုင်ခြင်း သူကိုယ်တိုင် copy တွေလုပ်ဆောင်နိုင်ခြင်း အပြင် တခြား လုပ်ဆောင်နိုင်တာတွေအများကြီးရှုပါတယ်။ နောက်ပြီးတခြား computer တွေ ကိုလဲ virus ရှိတဲ့ computer ထဲက files တွေကိုတွေကူးယူခြင်းမှတဆင့်ကူးစပ် နိုင်ပါတယ်။ 2000 ခုနှစ်တုန်းက “I love you” ဆိုတဲ့ virus ဟာ တစ်ကမ္ဘာလုံး ကိုကူးစပ်ခဲ့ပါတယ်။ အဲဒီ virus က email မှာ love-letter-for-you.txt.vbs ဆိုတဲ့ attachment ကတစ်ဆင့်ကူးတာဖြစ်ပါတယ်။ တချို့ user တွေကတော့ သာမန် text file တစ်ခုထင်ပြီးဖွင့်ကြည့်ကြပါတယ် ဒါပေမယ့် သူ့ extension အမှန်က .vbs ပါ။ အဲ virus က files တွေကို delete လုပ်နိုင်ခြင်း, usernames နဲ့ password တွေကို virus creator ထံကိုပို့ဆောင်ခြင်း တို့ကိုလုပ်ဆောင်နိုင်ပါတယ်။ Computer တွေ 15 million လောက်ကူးခံရပြီး \$5 billion လောက် ဆုံးရှုံးခဲ့ပါတယ်။ Virus အမျိုးစားတွေအများကြီးရှုပါတယ်။ အဲဒါတွေကတော့

- **Boot sector:** ဒီ virus က hard drive ကနေမှတစ်ဆင့် computer boots တက်တဲ့အခါ virus က memory ထဲကိုဝင်ရောက်တာဖြစ်ပါတယ်။

- **Macro:** ဒီ virus ကတေသာ documents တွေကတစ်ဆင့်ကူးတာဖြစ်ပါတယ်။ Users တွေက documents တွေကိုဖွင့်လိုက်တဲ့အခါvirus က computer ထဲကိုဝင်ရောက်တာဖြစ်ပါတယ်။
- **Program:** ဒါကတေသာ executable files တွေကတစ်ဆင့်ကူးတာဖြစ်ပါတယ်။
- **Encrypted:** ဒီ virus က ရုံးရှင်းတဲ့ cipher တွေကိုအသုံးပြုပြီးသူ့ဟာသူ့ encrypt လုပ်တာဖြစ်ပါတယ်။ အဲ virus ထဲမှာဆိုရင် encrypted လုပ်ထားတဲ့ virus code copy နဲ့ decryption module ပါပါဝင်ပါတယ်။ Virus ကူးစပ်ခံရပါက file တိုင်းကိုမတူညီတဲ့ keys တွေကိုအသုံးပြုပြီး encrypting လုပ်ပါတယ်။ ဒါပေမယ့် decrypt ပြန်လုပ်တဲ့ code ကတေသာ့တစ်ခုပဲဖြစ်ပါတယ်။
- **Polymorphic:** သူရဲ့ပုံစံက encrypted virus နဲ့တူပါတယ်။ ဒါပေမယ့် decrypting module ကတေသာ virus ရဲ့သက်ရောက်မှုပေါ်မှုတည်ပြီးလိုအပ်သလိုပြုပြင်ရပါတယ်။ ဒါကြောင့် antivirus တွေရဲ့ detect ကိုရှောင်ဖို့အတွက် အမြဲလိုပြောင်းလဲပြီး executed လုပ်ကြပါတယ်။
- **Metamorphic:** သူကလဲ polymorphic နဲ့တူပါတယ် ဒါပေမယ့် detection တွေကိုရှောင်ဖို့အတွက် နောက်ထပ် file အသစ်အနေနဲ့အမြဲတမ်း rewrites လုပ်ပါတယ်။

အခုက္ခန်းတော်ဖော်ပြပေးသွားတဲ့ virus တွေကတေသာ နာမည်ကြီး လူသိများတဲ့ virus အမျိုးစားတွေဖြစ်ပါတယ်။

## Worms

Worm ဆိုတာက malicious program တစ်ခုဖြစ်ပြီး computer တစ်ခုကနေနောက်တစ်ခုဆီကို Network ဒါမှုမဟုတ် Internet ကနေကူးနိုင်ပါတယ်။ 2001 ခုနစ်တုန်းက Nimda ဆိုတဲ့ worm ဟာ Internet ပေါ်ကနေ 22 minutes ကြာအောင်ရှိနေခဲ့ပြီးတော်တော်များများထိခိုက်ခဲ့ပါတယ်။ အဲ worm ဟာ network share, mass e-mail နဲ့ operating system ရဲ့ vulnerabilities တို့ကနေကူးတာဖြစ်ပါတယ်။



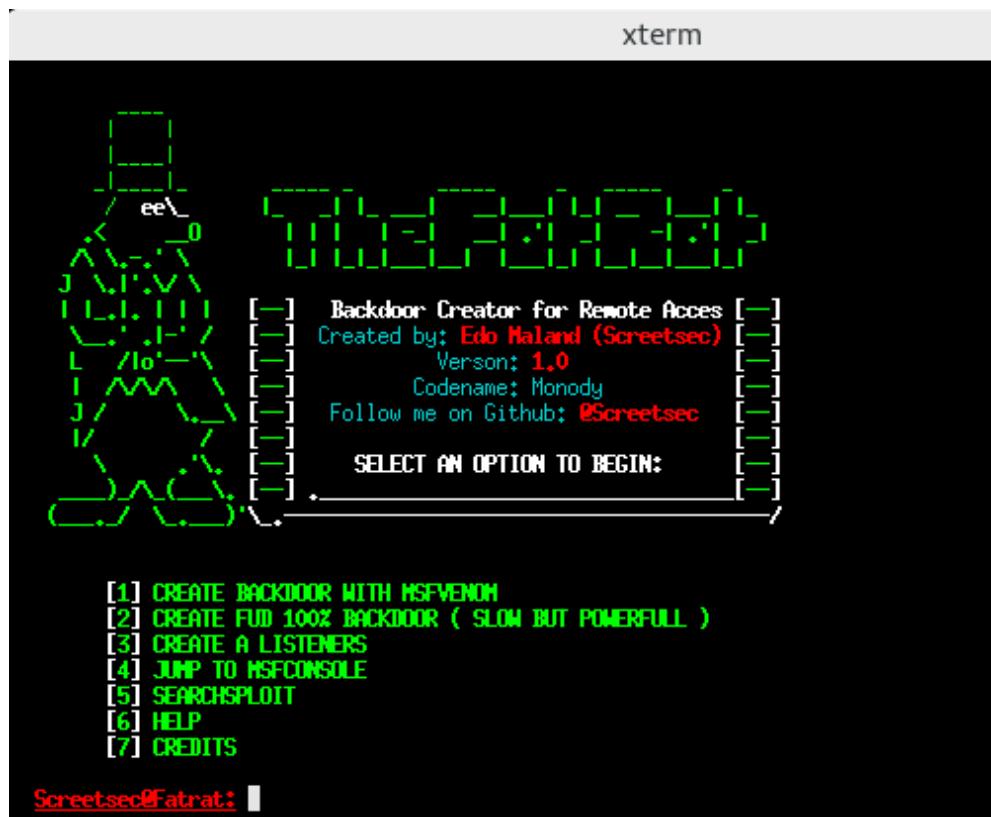
## Trojan Horses

Trojan horse ဒါမှုမဟုတ် Trojan ဆိုတာ malware အမျိုးစားတစ်ခုဖြစ်ပြီး legitimate software တွေရဲ့နောက်ကွယ်မှာပုံးခိုပြီးမှဝင်ရောက်တာဖြစ်ပါတယ်။ Hacker တွေက user တွေရဲ့ system ကို access ရဖို့အတွက် social engineering ကိုအသုံးပြုပြီး trojan ထည့်သွင်းထားတဲ့ software ကို user ကသူ့ system ထဲကို download လုပ်အောင် လုပ်ဆောင်ပါတယ်။ Trojans ကိုအသုံးပြုပြီး sensitive data များရယူခြင်း, system ကို ဝင်ရောက်နိုင်ဖို့ backdoor များထားနိုင်ခြင်း စတာတွေလုပ်ဆောင်နိုင်ပါတယ်။



## Remote access Trojans (RATs)

RATs ဆိုတာက Trojan အမျိုးစားတစ်ခုဖြစ်ပြီး system ထဲကို remote access လုပ်ဖို့အတွက် အသုံးပြုတာဖြစ်ပါတယ်။ RATs ကိုနောက်တစ်မျိုး Creepware လို့လဲခေါ်ဆိုကြပါတယ်။ User က RAT ကို execute လုပ်ပြီဆိုတာနဲ့ Hacker ဘက်ကနေ access ရရှိသွားပြီဖြစ်ပါတယ်။



## Ransomware

Ransomware ဆိုတာက malware အမျိုးစားတစ်မျိုးဖြစ်ပြီး သူဝင်ရောက်ခဲ့ရင် တော့ victim's စက်ထဲမှာရှုတဲ့ files တွေကို encrypts လုပ်လိုက်တာဖြစ်ပါတယ်။ Files တွေကို decrypt ပြန်လုပ်ချင်တယ်ဆိုရင်တော့ ransomware owner ကိုပိုက်ဆံပေးရ ပါတယ်။ အဲလိုပေးမှ ဟိုဘက်က decrypt ပြန်လုပ်ဖို့ decrypting key ကိုပေးမှာဖြစ်ပါတယ်။

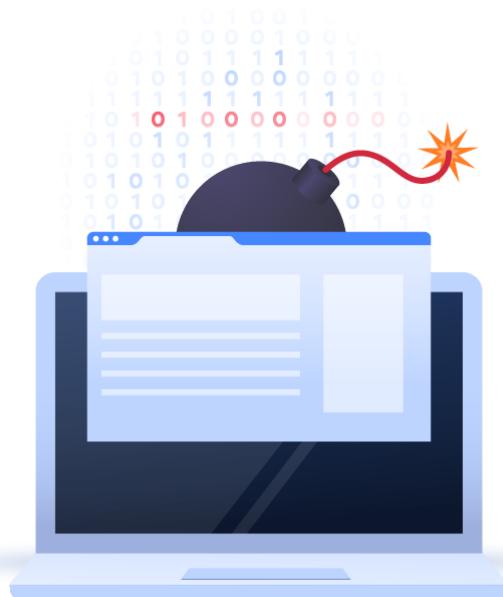


## Spyware

Spyware ဆိတာက system ထဲက information တွေကိုခြုံးယူပြီး creator ထံကို  
ပြန်ပို့တဲ့ malicious software တစ်မျိုးဖြစ်ပါတယ်။ နောက်ပြီး user တွေရဲ့ online  
activity ကိုစောင့်ကြည့်ပြီး information တွေကို black market တွေမှာ hacker တွေ  
က ပြန်ပြီးရောင်းစားကြပါတယ်။ Spyware ကိုအသုံးပြုပြီး personal information ဖြစ်  
တဲ့ account passwords, credit card numbers စတာတွေကိုခြုံးယူနိုင်ပါတယ်။



**Logic bomb:** Logic bomb ဆိုတာက virus တစ်မျိုးဖြစ်ပြီး သူရဲ့လုပ်ဆောင်ပုံက ချိန်ကိုက်ပုံးနဲ့ တူပါတယ်။ သတ်မှတ်ထားတဲ့ အချိန် ဒါမှမဟုတ် command တစ်ခုခုမှာ bind ထားတဲ့အခါ အဲအချိန်ရောက်တဲ့အခါ ဒါမှမဟုတ် command ကို execute လုပ်တဲ့ အခါ logic bomb ကအလုပ်လုပ်ဆောင်တာဖြစ်ပါတယ်။ Logic bomb မှာ malicious function တွေအကုန်ပါဝင်ပါတယ်။



## Summary of Malware Threats

Malware Threat	Definition	Example
Virus	Code that runs on a computer without the user's knowledge; it infects the computer when the code is accessed and executed.	Love Bug virus Eg: love-letter-for-you.txt.vbs
Worm	Similar to viruses except that it self-replicates, whereas a virus does not.	Nimda Propagated through network shares and mass e-mail
Trojan horse	Appears to perform desired functions but actually is performing malicious functions behind the scenes.	Remote access Trojan Eg: PlugX
Ransomware	Malware that restricts access to computer files and demands a ransom be paid by the user	Often propagated via a Trojan Eg: Crypto Locker
Spyware	Malicious software either downloaded unwittingly from a website or installed along with some other third-party software.	Internet Optimizer (a.k.a.aDyFuCA)

## Malware Prevention Techniques

ဒီသင်ခန်းစာမျာတော့ malware တွေကိုယ်ကာကွယ်ဖို့ နည်းလမ်းများကို လေ့လာရမှာဖြစ်ပါတယ်။

### Virus

Virus ကိုကွယ်ဖို့အတွက် နည်းလမ်းတချို့ကတော့-

- Antivirus software တစ်မျိုးမျိုးကိုအသုံးပြုခြင်း၊ ပုံမှန် update လုပ်ပေးခြင်း
- System ကို antivirus software နဲ့ပုံမှန် scan ပြုလုပ်ပေးခြင်း
- Operating system ကိုပုံမှန် update လုပ်ပေးခြင်း
- Firewall ကိုအသုံးပြုပေးခြင်း

### Worm

Worm တွေကိုကာကွယ်ဖို့အတွက်ဆိုရင်

- Antivirus software တစ်မျိုးမျိုးကိုအသုံးပြုခြင်း ပုံမှန် update လုပ်ဆောင်ပေးခြင်း
- System ကို antivirus software နဲ့ပုံမှန် scan ပြုလုပ်ပေးခြင်း

### Trojan horse

Trojan horse ကိုကာကွယ်ဖို့အတွက်ဆိုရင်

- Antivirus software တစ်မျိုးမျိုးကိုအသုံးပြုခြင်း၊ ပုံမှန် update လုပ်ဆောင်ပေးခြင်း
- System ကို antivirus software နဲ့ပုံမှန် scan လုပ်ပေးခြင်း
- Trojan scan ကိုအသုံးပြုပြီး စစ်ဆေးခြင်း

## Spyware

Spyware ကိုကာကွယ်ဖို့အတွက်ဆိုရင်

- Anti-spyware software တစ်မျိုးမျိုးကိုအသုံးပြုခြင်း၊ ပုံမှန် update လုပ်ဆောင်ပေးခြင်း
- System ကိုပုံမှန် scan လုပ်ပေးခြင်း
- Web browser settings တွေကို security ကောင်းဖို့အတွက်ပြုပြင်ခြင်း
- Spyware ကိုတားဆီးနိုင်တဲ့နည်းလမ်းကိုလိုက်နာခြင်း

## Rootkit

Rootkit ကိုကာကွယ်ဖို့အတွက်ဆိုရင်

- Antivirus software တစ်မျိုးမျိုးကိုအသုံးပြုခြင်း၊ ပုံမှန် update လုပ်ဆောင်ပေးခြင်း
- Rootkit detector programs ကိုအသုံးပြုခြင်း

## Spam

Spam ကိုကာကွယ်ဖို့အတွက်ဆိုရင်

- Spam filter ကိုအသုံးပြုခြင်း
- Network မှာ whitelists နဲ့ blacklists တို့ကို configure လုပ်ဆောင်ခြင်း
- Mail relays အားမလိုအပ်ပါကပါတ်ထားခြင်း
- User တို့ကို spam နဲ့ပတ်သက်တဲ့ knowledge များအား share ပေးခြင်း

အခုက္ခန်းတော်ဖော်ပြပေးခဲ့တာကတော့ Malware ကိုကာကွယ်နိုင်တဲ့ နည်းလမ်းတရာ့။  
ပဲဖြစ်ပါတယ်။

## Implementing Security Applications

အပေါ်မှာကျွန်တော်တို့ Malware တွေကို endpoint protection တွေကိုအသုံး  
ပြုပြီးကာကွယ်နိုင်တဲ့နည်းလမ်းတွေကို လေ့လာခဲ့ပြီးဖြစ်ပါတယ်။ အခုဆက်ပြီးတော့ endpoint protection အမျိုးစားတွေကိုဆက်ပြီးတော့ လေ့လာကြည့်ရအောင်။

### Personal Software Firewalls

Personal firewall တွေက Computer တွေကို unwanted Internet traffic မဖြတ်စေဖို့အတွက်အသုံးပြုတဲ့ application ဖြစ်ပါတယ်။ အဲမှာဆိုရင် ကျွန်တော်တို့က rules နဲ့ policies တွေကိုသတ်မှတ်နိုင်ပါတယ်။ အခု software-based personal firewalls တချို့ကိုအောက်မှာဖော်ပြလိုက်ပါတယ်။

- **Windows Firewall:** Windows firewall အကြောင်းကို Chapter 3 မှာဖော်ပြခဲ့ပြီးသားဖြစ်ပါတယ်။
- **ZoneAlarm:** ZoneAlarm ဆိုတာကလဲ security applications တွေထဲက တစ်ခုဖြစ်ပါတယ်။ သူ့ကို Check Point ကနေဝါယ်လိုက်တာဖြစ်ပါတယ်။ Free version အနေနဲ့အသုံးပြုနိုင်ပါတယ်။
- **PF (packet filter) and IPFW (IP Firewall):** PF ဆိုတာက command-line-based firewall ဖြစ်ပြီး OS X version 10.10 နဲ့အထပ်မှာဆိုရင် built-in ပါဝင် ပါတယ်။
- **iptables:** Iptables ကို Linux systems မှာအသုံးပြုတာဖြစ်ပါတယ်။ Linux kernel firewall အနေနဲ့အသုံးပြုတာဖြစ်ပါတယ်။

Anti-malware အတွက်ဆိုရင်နာမည်ကြီးတဲ့ suites တွေကတော့ Symantec, McAfee, Kaspersky စတာတွေပဲဖြစ်ပါတယ်။

### Securing Computer Hardware and Peripherals

ဒီသင်ခန်းစာမှာတော့ Operating system ပိုပြီး secure ဖြစ်ဖို့အတွက် hardware, BIOS နဲ့ external devices တွေကိုပါ secure ဖြစ်အောင်လုပ်ဆောင်ရမယ့်

နည်းလမ်းတွေကိုလွှဲလာရမှာဖြစ်ပါတယ်။ External devices တွေဆိုတာက Computer system မှာတပ်ဆင်လို့ရတဲ့ devices တွေဖြစ်တဲ့ USB flash drives, external SATA hard drives, optical discs စတာတွေပါဝင်ပါတယ်။

## Securing the BIOS

BIOS တွေကယ်လဲ malicious attacks တွေမှုတစ်ဆင့် victim ဖြစ်သွားနိုင်ပါတယ်။ BIOS က system ကို rest လုပ်ဖို့ gateway အနေနဲ့ဖြစ်နိုင်ပါတယ်။ ဒါကြောင့် BIOS ကလဲ secure ဖြစ်ဖို့လိုအပ်ပါတယ်။ တစ်ကယ်လို့ ကျွန်တော်တို့ရဲ့ computer boot မတက်ခဲ့ဘူးဆိုရင်တော့ အောက်ပါအချက်တွေကိုလုပ်ဆောင်ကြည့်နိုင်ပါတယ်။

- **Flash the BIOS:** ဒါကတော့ BIOS ကို update လုပ်တာကိုပြောတာဖြစ်ပါတယ်။ BIOS ကိုနောက်ဆုံး version ရောက်တဲ့အထိ update လုပ်ခဲ့မယ်ဆိုရင် exploits လုပ်ဆောင်ခံရခြင်း နဲ့ BIOS errors တွေကိုမဖြစ်အောင် ကာကွယ်နိုင်မှာဖြစ်ပါတယ်။ နောက် BIOS ကို update လုပ်ဆောင်ခြင်းဖြင့် Electromagnetic Interface (EMI) နဲ့ Electromagnetic Pluses (EMP) တို့ကို ကောင်းစွာကာကွယ်ပေးနိုင်မှာဖြစ်ပါတယ်။
- **Use a BIOS password:** BIOS password ကတော့ attacker က BIOS ကို gaining access လုပ်ဆောင်လို့မရအောင်ကာကွယ်ပေးတာဖြစ်ပါတယ်။ BIOS password ကို တချို့က user login လုပ်တဲ့အခါလိုအပ်တဲ့ password နဲ့မှားတက်ပါတယ်။ တစ်ကယ်ကမတူပါဘူး။
- **Configure the BIOS boot order:** BIOS မှာဖြစ်နိုင်ခြေရှိတဲ့ risk တွေကို လျှော့ချဖို့အတွက် အသုံးပြုသင့်ပါတယ်။ စာဖတ်သူတွေမြင်သာအောင်ပြောရရင် BIOS boot က ပထမဗြီးဆုံးအနေနဲ့ Hard Drive ကိုပထမဗြီးစားပေးအနေနဲ့ ထားသင့်ပါတယ်။

- **Disable external ports and devices:** ဖြစ်နိုင်မယ်ဆိုရင် Company တွေရဲ့ policy တွေမှာ removable media တွေဖြစ်တဲ့ optical drives, eSATA ports နဲ့ USB ports တွေကို disable လုပ်ဖို့ထည့်သွင်းဖော်ပြသင့်ပါတယ်။
- **Enable the secure boot option:** UEFI 2.3.1 နဲ့အမြင့်တွေမှာဆိုရင် secure boot ဆိုတဲ့ option ပါဝင်ပါတယ်။ အဲဒါက boot process တွေမှာ လုပ်ဆောင် တဲ့ firmware drivers နဲ့ operating system တို့ရဲ့ signature ကိုစစ်ဆေးတာ ဖြစ်ပါတယ်။ တစ်ကယ်လို့ signatures တွေကအဆင်ပြေတယ်ဆိုရင်တော့ PC က boots တက်ပြီး firmware က operating system ကို control ပေးလုပ်မှာ ဖြစ်ပါတယ်။ ကျွန်ုတ်တို့က Secure Boot ကို enabled လုပ်ထားခဲ့မယ်ဆိုရင် တော့ Operating system နဲ့ တခြား boot media တွေက secure Boot နဲ့ အံဝင်ခွင်ကျဖြစ်ဖို့လို့အပ်ပါတယ်။

## Securing Storage Devices

Storage Devices တွေကို အဓိက failure point တွေအဖြစ် အသိများ ကြပါတယ် ဘာကြောင့်လဲဆိုရင် storage devices တွေရဲ့အစိတ်ပိုင်းတွေဟာ အလွယ်တကူပြောင်းရွှေ့လို့ ရခြင်းဥပမာ removable media လိုမျိုးပေါ့။ Storage devices တွေကလဲအန္တရာယ်ဖြစ်စေနိုင်ပါတယ် ဘာကြောင့်လဲဆိုရင် များသောအားဖြင့် ပြင်ပကနေ computer system ကိုချိတ်ဆက်နိုင်တာကြောင့် ဖြစ်ပါတယ်။ အဲလိုပဲ removable media တွေကိုခြေရာခံဖို့ဆိုရင်သိပ်မလွယ်ကူ ပါဘူး။ Physical security, encryption, policies တွေကိုအသုံးပြုပြီး removable media တွေအသုံးမပြုနိုင်အောင်ကာကွယ်ခြင်းကသာ အဆင်ပြေ တဲ့နည်းလမ်းတွေဖြစ်ပါတယ်။

## Removable Storage

Removable storage ဒါမှမဟုတ် removable media ဆိုတာက Optical discs, USB devices, eSATA devices နဲ့ floppy disks တို့ပါဝင်ပါတယ်။ Network Administrator တွေက removable media တွေကိုအသုံးမပြု

နိုင်အောင် BIOS မှတစ်ဆင့်ကာကွယ်နိုင်ပါတယ်။ များသောအားဖြင့် Company တော်တော်များများမှာ removable media တွေကို blocked လုပ်ထားပြီး တချို့လိုအပ်တဲ့ devices တွေကိုပေးသုံးတာဖြစ်ပါတယ်။

USB devices တွေကိုအထူးကရှိစိုက်သင့်ပါတယ် ဘာကြောင့်လဲဆိုရင် သူတို့ဟာ သေးငယ်ပေမယ့် data တွေအများကြီးကိုသယ်ဆောင်နိုင်တာကြောင့် ဖြစ်ပါတယ်။ USB devices တွေကြောင့် victim ဖြစ်သွားတဲ့ computer တွေ အများကြီးရှိပါတယ်။ ဥပမာပြောရရင် Attacker က malware တစ်မျိုးမျိုးကို USB ထဲမှာထည့်သွင်းထားတယ်ဆိုပါစို့ အဲ USB ကို user ကသူ့ computer မှာ တပ်ဆင်လိုက်တဲ့အခါ attacker ထည့်သွင်းထားတဲ့ malware က user ရဲ့ computer ထဲကိုဝင်ရောက်သွားမှာဖြစ်ပါတယ်။

## Network Attached Storage

Network Attached Storage (NAS) ဆိုတာက storage device တစ်ခု ဖြစ်ပြီး Ethernet network မှတစ်ဆင့် connect လုပ်ရတာဖြစ်ပါတယ်။ NAS devices တွေကိုတော့ home နဲ့ office တွေမှာအသုံးပြုပါတယ်။ NAS ကို secure ဖြစ်စိုးအတွက်ဆိုရင်

- 1) Implement strong password security
- 2) Ensure that NAS firmware is routinely updated
- 3) Never use default admin accounts
- 4) Secure your connection and ports
- 5) Make use of your NAS firewall
- 6) Enable DoS protection
- 7) Use a VPN whenever you use your NAS

စတဲ့နည်းလမ်းတွေပဲဖြစ်ပါတယ်။ အောက်မှာတော့ NAS ရဲ့ပုံကို နမူနာအနေနဲ့ ပြပေးထားပါတယ်။



## Whole Disk Encryption

Encryption ဆိုတာက computer security အတွက်အရေးပါတဲ့အခန်း ကနေပါဝင်ပါတယ်။ Hard drive တွေကို encrypt လုပ်မယ်ဆိုရင် Self-Encrypting Drive (SED) ဒါမှမဟုတ် Full Disk Encryption (FDE) software တို့ကိုအသုံးပြုနိုင်ပါတယ်။ FDE software တွေကို market တွေမှာအလွယ် တကူးဝယ်ယူလိုက်နိုင်သလို Microsoft မှာ default ပါဝင်တဲ့ BitLocker ကိုလဲ အသုံးပြုနိုင်ပါတယ်။ Full disk encryption software တွေက disk တစ်ခုလုံး ကို encrypt လုပ်နိုင်ပါတယ်။ Drive တစ်ခုလုံးကို encrypt လုပ်ဖို့ဆိုရင် အောက်ပါ အချက်တွေကိုလိုအပ်ပါတယ်။

- Trusted Platform module (TPM) Chip တစ်ခုဖြစ်ပြီး motherboard ပေါ်မှာရှိတာပါ အဲမှာတော့ encrypted keys တွေကို stores လုပ်တာဖြစ်ပါတယ်။
- Encrypted keys တွေကို store လုပ်ဖို့အတွက် external USB လိုအပ်ပါတယ်။

➤ ပုံမှန် Computer တွေရဲ့ Hard drive တွေမှာဆိုရင် C နဲ့ D ဆိုပြီး volumes (2) ခုရှိပါတယ်။ ပထမ C ဆိုတဲ့ volume ကတေသာ operating system အတွက်အသုံးပြုတာဖြစ်ပြီး သူကတေသာ encrypted လုပ်ပြီးသား ဖြစ်ပါတယ်။ နောက် volume ကတေသာ data တွေကိုသိမ်းဖို့အသုံးပြုတာ ဖြစ်ပြီး encrypt မလုပ်ရသေးတဲ့ volume ဖြစ်ပါတယ်။ အဲ volume ကို encrypt လုပ်ချင်တယ်ဆိုရင်တော့ BitLocker ကိုအသုံးပြုနိုင်ပါတယ်။

BitLocker ဆိုတာက software တစ်ခုဖြစ်ပြီး Advanced Encryption Standard (AES) မှာအခြေခံထားတာဖြစ်ပါတယ်။ သူ့ကိုတော့ 128-bit နဲ့ 256-bit keys တို့ကိုအသုံးပြုပါတယ်။

## Hardening Operating Systems

OS hardening ဆိုတာက ပိုပြီး secure ဖြစ်ဖို့အတွက် rules နဲ့ policies တွေ သတ်မှတ်တာ နောက်ပြီး မသုံးတဲ့ applications နဲ့ services တွေကို remove လုပ်တာ စတာတွေပါဝင်ပါတယ်။ အဲလိုလုပ်ဆောင်ခြင်းအားဖြင့် OS လိုထိခိုက်နှင့်တဲ့ threats နဲ့ risk တွေကိုလျှော့ချုန်မှာဖြစ်ပါတယ်။ ဒါပေမယ့် ကျွန်တော်တို့သိထားရမှာက မည်သည့် system ကမှ 100% secure ဖြစ်နေဘူးဆိုတာဖြစ်ပါတယ်။ အဲဒါကြာင့်မလို risk level ကို zero ဖြစ်တဲ့အထိလျှော့ချို့ဆိုတာမဖြစ်နိုင်ပါတယ်။

ဒီအပိုင်းမှာဆိုရင် Patch management, hotfixes, group policies, security templates နဲ့ configuration baseline တွေကိုလေ့လာရမှာဖြစ်ပါတယ်။ အရင်ဆုံး ကျွန်တော်တို့ system မှာ မလိုအပ်တဲ့ application နဲ့ services တွေ running ဖြစ်နေလဲဆိုတာ ရှာပါမယ် ပြီးရင်တော့ အဲဒါတွေကို remove ပါမယ်။

## Removing Unnecessary Applications and Services

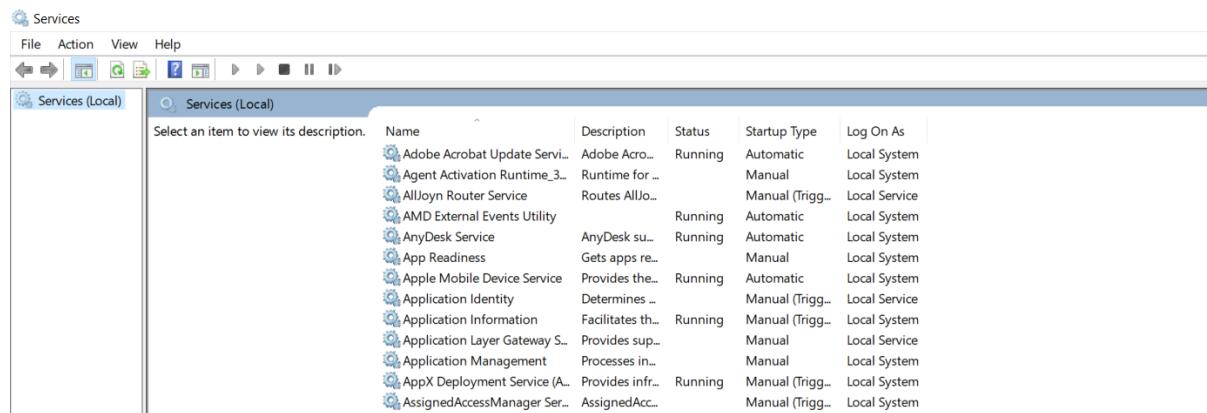
အသုံးမလိုတဲ့ applications နဲ့ services တွေက HDD space တွေကိုလဲ နေရာယူသလို power ကိုလဲပို့ကုန်ဖောပါတယ်။ အဲဒါတွေထပ်ပိုပြီးတော့ အရေးကြီးတာ operating system ကို vulnerabilities ဖြစ်စေနိုင်ပါတယ်။ ဒါကြာင့် organizations တွေက computers နဲ့ တွေား information systems

တွေမှာ essential functions တွေကိုပဲအသုံးပြုနိုင်အောင်လုပ်ဆောင်ထားတာဖြစ်ပါတယ်။ ဒီနည်းလမ်းကိုအသုံးပြုပြီး Security Administrator တွေက applications, services, ports နဲ့ protocols တွေအသုံးပြုခွင့်ကိုကန္နာသတ်ထားတာဖြစ်ပါတယ်။ အဲလိုတိန်းချုပ်တာကို NIST ကဖော်ပြထားတဲ့ CM-7 လိုခေါ်ပါတယ်။ NIST ရဲ့ website ကိုတွေ့အောက်မှာဖော်ပြထားပါတယ်။

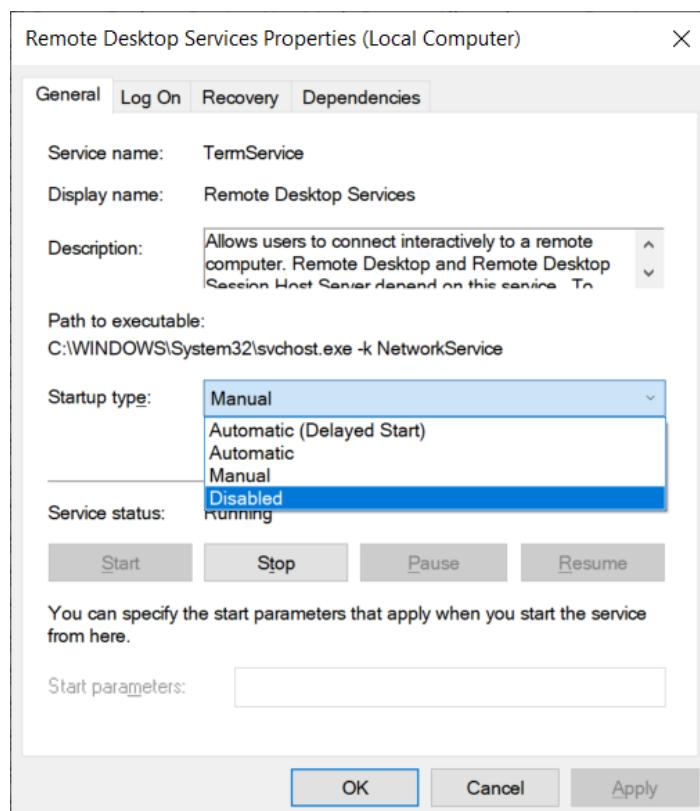
<https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/control?version=4.0&number=CM-7>

အဲအချက်တွေက System ကိုစိတ်မချေရတဲ့ အန္တရာယ်ရှိတဲ့ applications နဲ့ services တွေရဲ့ရန်ကနေကာကွယ်ပေးနိုင်ပါတယ်။ ဥပမာ instance messaging programs က အန္တရာယ်ရှိနေတယ်ဆိုရင် အဲ programs ကိုလုပ်ငန်းခွင်မှာအသုံးပြု ခြင်းကနေကန္နာသတ်ရမှဖြစ်ပါတယ်။ နောက် security viewpoint ကနေကြည့်မယ် ဆိုရင် အဲ programs တွေမှာ backdoors တွေပါဝင်လာနိုင်ပြီး attackers ကအလွယ် တကူဗုံး access ရနိုင်သွားစေပါတယ်။

နောက် remote control programs တွေကိုလဲစောင့်ကြည့်ဖို့လိုအပ်ပါတယ်။ ဘာကြောင့်လဲဆိုရင် application တချို့မှာ computer ကို remote control လုပ်နိုင် တာကြောင့်ဖြစ်ပါတယ်။ ဥပမာ Remote Desktop Connection ဆိုတာက Windows-based remote control program ဖြစ်ပါတယ်။ သူအသုံးပြုတဲ့ default port ကတော့ 3389 ဖြစ်ပြီး အဲဒါကို attackers တိုင်းကသိပါတယ်။ ဒါကြောင့်ကျွန်တော်တို့က default port ကိုပြောင်းပြီးသုံးဖို့လိုအပ်ပါတယ်။ တကယ်လို့ အသုံးမလိုဘူးဆိုရင် disabled လုပ်ထားနိုင်ပါတယ်။ Services တွေကို start / stop လုပ်ချင်တယ်ဆိုရင် Run box ကနေ services.msc ဆိုပြီးရှိက်လိုက်ပါ အောက်ကပုံအတိုင်း တွေ့မြင်ရမှာဖြစ်ပါတယ်။ ဒါအပြင် disabled လဲလုပ်ဆောင်နိုင်ပါတယ်။



အဲကမှတစ်ဆင့် မလိုအပ်တဲ့ အသုံးမလိုတဲ့ services တစ်ခုချင်းကို Disabled လုပ်နိုင်ပါ တယ်။ အခုက္ခန်းတော်တို့ နမူနာ အနေနဲ့ Remote Desktop Services ကို Disabled လုပ်ကြည့်ရအောင်။ အရင်ဆုံး disabled လုပ်ချင်တဲ့ services ကိုရှာပါမယ် ကျွန်တော်က Remote Desktop Services ကို disable လုပ်မှာဖြစ်တဲ့အတွက် အဲအပေါ်မှာ double click နိပ်ပါမယ်။



ပြီးရင်တော့ Disabled ကိုရွေးပြီး Ok နိပ်ပြီးထွက်ပါမယ်။ ဒါဆိုရင်တော့ Remote Desktop Services က Disabled ဖြစ်သွားပြီဖြစ်ပါတယ်။ ဒါဆိုရင် စာဖတ်သူတွေ services တွေကို Enabled , Disabled

လုပ်တာကိုသိမယ်လို့ထင်ပါတယ်။ အခါ ကျွန်တော် စမ်းပြေပေးသွားတာ Windows မှာဖြစ်ပါတယ်။ ဆက်ပြီးတော့ Linux မှာ Services တွေကို start, stop လုပ်တာကိုလေ့လာရမှာဖြစ်ပါတယ်။ Terminal မှာ service --status-all ဆိုတဲ့ command ကိုရှိက်လိုက်ပါ ဒါဆိုရင် services တွေကိုတွေ့ရမှာဖြစ်ပါတယ်။

```
root@kali:~# service --status-all
[ - ] apache-htcacheclean
[ + ] apache2
[ - ] apparmor
[ - ] atftpd
[ - ] avahi-daemon
[ + ] binfmt-support
[ - ] bluetooth
[ - ] console-setup.sh
[ + ] cron
[ - ] cryptdisks
[ - ] cryptdisks-early
[ + ] dbus
[ - ] dns2tcp
[ - ] gdomap
[ + ] haveged
```

ပုံမှာဆိုရင် running ဖြစ်တဲ့ services တွေကို [+] နဲ့ပြတာဖြစ်ပြီး stop ဖြစ်နေတဲ့ services တွေကိုတော့ [-] နဲ့ပြတာဖြစ်ပါတယ်။ အခါကျွန်တော်နူးနာအနေနဲ့ running ဖြစ်နေတဲ့ services ထဲက apache2 ဆိုတဲ့ services ကို stop လုပ်ပါမယ်။ Command ကတော့ systemctl stop apache2 ဖြစ်ပါတယ်။

```
root@kali:~# systemctl stop apache2
root@kali:~#
```

ပြီးရင် ပထမ္မားဆုံးကြည့်ခဲ့တဲ့ command ကိုအသုံးပြုပြီး service status ကိုကြည့် ပါမယ်။

```
root@kali:~# service --status-all
[ - ] apache-htcacheclean
[ - ] apache2
[ - ] apparmor
[ - ] atftpd
[ - ] avahi-daemon
[ + ] binfmt-support
[ - ] bluetooth
[ - ] console-setup.sh
[ + ] cron
[ - ] cryptdisks
[ - ] cryptdisks-early
[ + ] dbus
[ - ] dns2tcp
[ - ] gdomap
[ + ] haveged
```

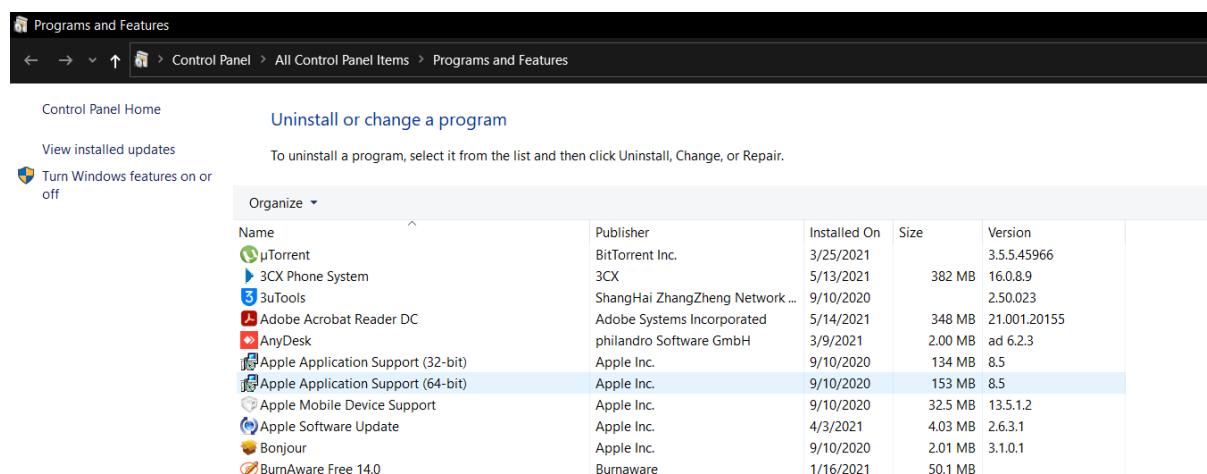
ဒါလိုရင်တော့ services က stop ဖြစ်နေတာကိုတွေ့ရမှာဖြစ်ပါတယ်။ အခု ကျွန်တော် ကြည့်တာက services တွေအကုန်လုံးကိုကြည့်တာဖြစ်ပါတယ်။ Services တစ်ခုချင်း ရဲ့ status ကိုကြည့်မယ်ဆိုရင်တော့ systemctl status service\_name ဖြစ်ပါတယ်။

```
root@kali:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
    Loaded: loaded (/lib/systemd/system/apache2.service)
    Active: inactive (dead)
      Docs: https://httpd.apache.org/docs/2.4/
           ↑
           ↓
May 17 09:45:06 kali systemd[1]: Starting The Apache >
May 17 09:45:06 kali apachectl[2116]: AH00558: apache>
May 17 09:45:06 kali systemd[1]: Started The Apache H>
May 17 09:49:51 kali systemd[1]: Stopping The Apache >
May 17 09:49:51 kali apachectl[3122]: AH00558: apache>
May 17 09:49:52 kali systemd[1]: apache2.service: Suc>
May 17 09:49:52 kali systemd[1]: Stopped The Apache H>
lines 1-12/12 (END)
```

ပုံမှာဆိုရင် dead ဆိုပြီးတွေ့ရမှာဖြစ်ပါတယ် ဒါဆိုရင် stop ဖြစ်နေတယ်လို့  
သတ်မှတ်ပါတယ်။ Service ကို start လုပ်ချင်တယ်ဆိုရင်တော့ systemctl  
start apache2 ဖြစ်ပါတယ်။

```
root@kali:~# systemctl start apache2
root@kali:~#
```

ဆက်ပြီးတော့ အသုံးမလိုတဲ့ programs တွေကို uninstall လုပ်တဲ့အပိုင်း  
ကိုလေ့လာကြည့်ရအောင်။ Program တွေကို uninstall လုပ်မယ်ဆိုရင် Run  
box ကနေ appwiz.cpl လို့ရှိက်လိုက်ပါ။



အဲကမှတစ်ဆင့် မလိုအပ်တဲ့ program တွေကို uninstall လုပ်လိုရပါတယ်။ ဒါပေမယ့် ဒီနည်းလမ်းဟာ Computer ၁ လုံးထဲအတွက်ဆိုရင် အဆင်ပြေပေ မယ့် Computer အလုံး ၁၀၀၀ လောက်ဆိုရင်အဆင်မပြေတော့ပါဘူး။ အဲအခါ ကျွန်တော်တိုက Centralized Management ကိုအသုံးပြုဖို့လိုလာ ပါတယ်။ ဥပမာ Microsoft's System Center Configuration Manager (SCCM) နဲ့ Mobile Device Management (MDM) တို့လိုပေါ့။ အဲ program တွေက security administrator တွေ computer အများ ကြီးကို software management, configurations, policies စတာတွေကို local workstation ကနေလုပ်ဆောင်နိုင်ပါတယ်။ Local workstation ဆိုတာက Computer ကိုပဲ ပြောတာဖြစ်ပါတယ်။

## Windows Update, Patches, and Hotfixes

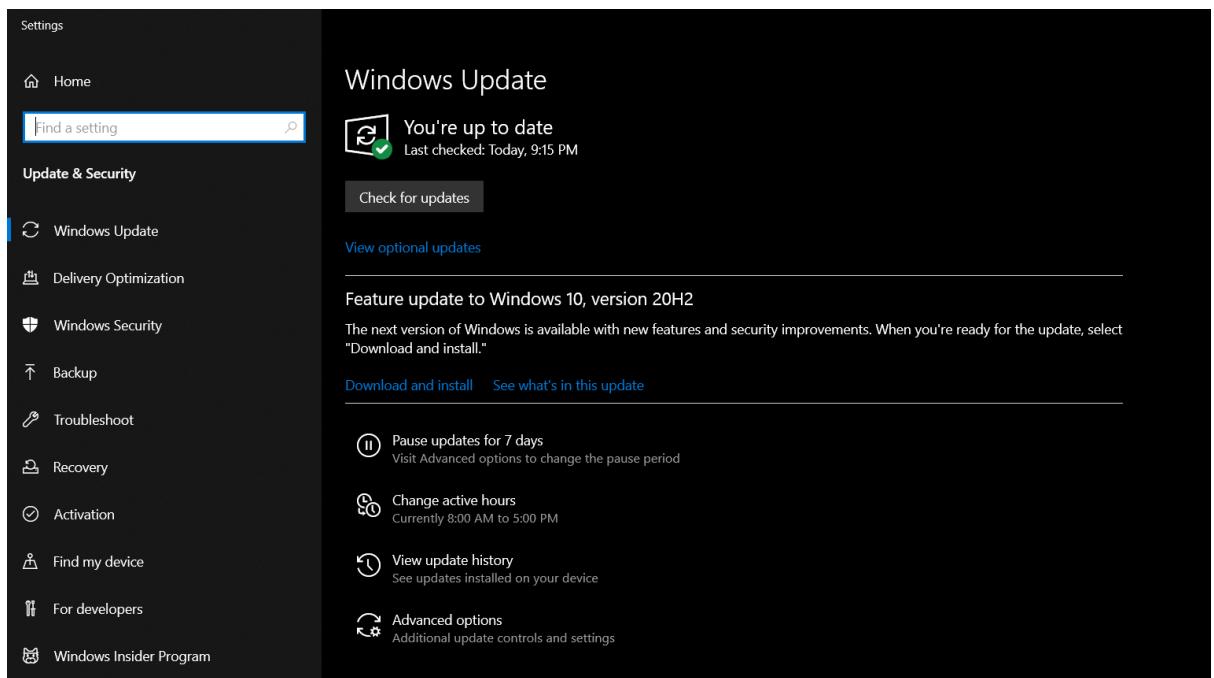
Operating System တစ်ခုက secure ဖြစ်ဖို့ဆိုရင် Trusted Operating System (TOS) လိုခေါ်တဲ့စံကိုလိုက်နာရပါတယ်။ TOS certified ဖြစ်ထားတဲ့ Operating system တွေကိုနူးမူနာအနေနဲ့ပြောရမယ်ဆိုရင် Windows, OS X , FreeBSD နဲ့ Red Hat Enterprise Server စတာတွေပါဝင်ပါတယ်။ TOS ကို လိုက်နာဖို့ဆိုရင် System တွေကိုထုတ်တဲ့ Company တွေရဲ့ Policies တွေက ကောင်းမွန်ဖို့လိုပြီး updates နဲ့ patching တွေကိုပုံမှန်ထုတ်ပေးနိုင်ဖို့လိုအပ်ပါတယ်။ TOS ကိုမလိုက်နာပဲနဲ့လဲ Operating system တွေကိုပုံမှန် updated လုပ်လိုရပါတယ်။ ဥပမာပြောရရင် Microsoft ရဲ့ OS မှာ vulnerability တွေပြီး exploit လုပ်ဆောင်လိုရခဲ့မယ်ဆိုရင် patches အသစ်ကို create လုပ်ပြီး OS performance ကိုပိုကောင်းအောင်လုပ်ပြီးတော့လဲ system ကိုကာကွယ်နိုင်ပါတယ်။

ကျွန်တော်တိုက OS တစ်ခုကို update လုပ်တော့မယ်ဆိုရင် အရင်ဆုံး version number, build number နဲ့ patch level တို့ကိုသိအောင်အရင်လုပ်ရပါတယ်။ Windows မှာအဲ information တွေကိုကြည့်မယ်ဆိုရင် cmd ကတော့

`msinfo32` ဆိုတဲ့ command ကိုအသုံးပြုပြီးတော့ကြည့်နိုင်ပါတယ်။ အောက်မှာ နှုန်းများအနေဖြင့်ပြပေးထားပါတယ်။

Item	Value
OS Name	Microsoft Windows 10 Pro
Version	10.0.19041 Build 19041
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation

နောက် `winver` , `systeminfo` command ကိုအသုံးပြုပြီးတော့လဲကြည့်လို့ရပါတယ်။ Windows မှာဆိုရင် Windows Update program ကိုအသုံးပြုပြီး updates တွေကို manage လုပ်လို့ရပါတယ်။ Windows 10 အရှေ့က version တွေတူနဲ့က အဲ feature က Control Panel ထဲမှာပါ။ Windows 10 မှာဆိုရင်တော့ Settings ထဲကိုသွားပြီး manage လုပ်လို့ရသလို Run box ကနေ `ms-settings:windowsupdate` ဆိုတဲ့ command နဲ့သွားလို့ရပါတယ်။



Updates မှာဆိုရင် မတူညီတဲ့ အမျိုးစားတွေရှိပါတယ်။ အဲဒါတွေကတော့

- **Security update:** ဒါကတော့ systems မှာ vulnerability ဖြစ်တဲ့အခါ ပေးတဲ့ update ဖြစ်ပါတယ်။ Security vulnerability ကလဲ ပြင်းထန်မှု ပေါ်မှုတည်ပြီးကွဲပြားပါတယ်။ အဲဒါတွေက Microsoft Security Bulletin တွေဖြစ်တဲ့ critical, important, moderate နဲ့ low တို့ဖြစ်ပါတယ်။
- **Critical update:** Non-security-related bug တွေအတွက်ကိုထုတ်ပေး တဲ့ update ဖြစ်ပါတယ်။
- **Windows update:** အသုံးပြုတဲ့သူတွေတွေကြံ့ရတဲ့ noncritical problem တွေကို fix လုပ်ထားတဲ့ update ဖြစ်ပါတယ်။ ဒါ update မှာဆို ရင် features အသစ်တွေပါပါဝင်တက်ပါတယ်။
- **Driver update:** Hardware အသစ်တစ်ခုကိုတပ်ဆင်လိုက်တဲ့အခါ အလုပ်လုပ်ဆောင်ဖို့အတွက် driver လိုအပ်ပါတယ်။ အဲလိုအပ်တဲ့ driver ကို Driver update လုပ်ပြီး install လုပ်ဆောင်လို့ရပါတယ်။

## Patches and Hotfixes

Patches နဲ့ hotfixes တို့အတွက်ဆိုရင် အကောင်းဆုံးနေရာကတော့ manufacture website ပဲဖြစ်ပါတယ်။ Patches နဲ့ hotfixes တို့က တစ်ခါတစ်ခု အပြန်လှန်အသုံးပြုနိုင်ပါတယ်။ Windows updates ဆိုတာ hotfixes တွေကို စုပြီးဖွဲ့စည်းထားတာဖြစ်ပါတယ်။ Hotfix ဆိုတာက OS ဒါမှုမဟုတ် application တစ်ခုစိုး single problem တွေကို fix လုပ်တာဖြစ်ပါတယ်။ Hotfix လုပ်ပြီး သွားတဲ့အခါ reboot ချို့မလိုပါဘူး။ System ရဲ့ hotfix တွေကို ကြည့်မယ်ဆိုရင် cmd ကနေ systeminfo ဆိုတဲ့ command နဲ့ကြည့်လို့ရပါ တယ်။

```
Hotfix(s): 15 Hotfix(s) Installed.
[01]: KB4601554
[02]: KB4559309
[03]: KB4560366
[04]: KB4561600
[05]: KB4566785
[06]: KB4570334
[07]: KB4577266
[08]: KB4577586
[09]: KB4580325
[10]: KB4586864
[11]: KB4589212
[12]: KB4593175
[13]: KB4598481
[14]: KB5003173
[15]: KB5003242
```

Hotfixes ၏ application ဒါမှမဟုတ် system တစ်ခုချင်းစီအတွက်ထုတ်ပေးတဲ့ single patches ဖြစ်ပါတယ်။

Patches ဆိုတာက problem သေးသေးလေးတွေကိုဖြေရှင်းဖို့အတွက်ထုတ်ပေးတာဖြစ်ပါတယ်။ ဒါပေမယ့် problem အကြီးတွေကိုဖြေရှင်းဖို့အတွက်ကြတော့ update ဒါမှမဟုတ် service packs လို့ခေါ်ဆိုပါတယ်။ စာဖတ်သူတွေမှတ်ထားရမှာက OS မှာ single security issue ရှိနေခဲ့ပြီဆိုရင် တော့ အဲဒါကိုဖြေရှင်းဖို့ကတော့ patch ပဲဖြစ်ပါတယ်။ ဥပမာပေး ရရင် Windows ရဲ့ old version တွေကို Trojans တွေက attack လုပ်နေခဲ့တယ်ဆိုရင် အဲဒါကို fix လုပ်ဖို့အတွက် Microsoft ၏ patch တစ်ခုကိုထုတ်ပေးပါတယ်။ အဲ patch ကိုinstall လုပ်ပြီးသွားတဲ့အခါ Trojans တွေက remote access လုပ်ဆောင်လို့မရတော့ဘူးဖြစ်ပါတယ်။

## Securing Mobile Devices

Smartphones နဲ့ Tablets ဒါမှမဟုတ် တခြားသော mobile devices တွေက attacker တွေရဲ့ victims ဖြစ်လာနိုင်ပါတယ်။ Attackers တွေက ကျွန်တော်တို့ရဲ့ device တွေ တိုက်ခိုက်မှုတွေမှာကြားခံအနေနဲ့အသုံးပြုဖို့ တိုက်ခိုက်သလို ကျွန်တော်တို့ရဲ့ account information တွေကိုရယူဖို့အတွက်လဲ mobile devices တွေကို

တိုက်ခိုက်လာနိုင်ပါတယ်။ အသုံးပြုသူတွေအနေနဲ့သူတို့ရဲ့ phone number တွေကို  
တွေးမရင်းနီးတဲ့ လူတိုင်းကိုမပေးသင့်ပါဘူး။ ဘာကြောင့်လဲဆိုရင် phone number  
ကိုအသုံးပြုပြီးဖွင့်ထားတဲ့ mail, social media စတဲ့ information တွေကို attacker က  
သိသွားနိုင်တာကြောင့်ဖြစ်ပါတယ်။ ဒါအပြင် Phone number ကို SMS မှ တစ်ဆင့်  
အန္တရာယ်ရှုတဲ့ link တွေကိုပို့ဆောင်တာမျိုးတွေလုပ်ဆောင်နိုင်ပါတယ်။

Mobile operating system software တွေကိုလဲ ကျွန်တော်တို့အနေနဲ့ပုံမှန်  
update လုပ်တာမျိုးတွေလုပ်ဆောင်သင့်ပါတယ်။ ကျွန်တော်တို့ရဲ့ devices တွေကို  
update တွေပုံမှန်လုပ်ထားတဲ့အခါ viruses နဲ့ တွေးသော malware တွေကူးစပ်ခံရမှု  
မှသက်သာစေမှာဖြစ်ပါတယ်။ ကျွန်တော်တို့ရဲ့ phone ထဲက data တွေကို စိတ်ချရတဲ့  
နည်းလမ်းတွေကို encrypted လုပ်သင့်ပါတယ်။ တချို့ organizations တွေမှာတော့  
data တွေကို ဘယ်လို encrypted လုပ်မလဲဆိုတဲ့ policies တွေရှိပါတယ်။ ပိုကောင်းတဲ့  
အကြံပေးချက်တွေကိုတော့ National Cyber Awareness System (NCAS) နဲ့  
U.S.Computer Emergency Readiness Team (US-CERT) တို့ကနေရရှုယူနိုင်ပါ  
တယ်။ အဲ websites (၂) ခုကိုအောက်မှာဖော်ပြထားပါတယ်။

- <https://www.us-cert.gov/ncas>
- <https://www.us-cert.gov/ncas/tips/ST05-017.html>

ဒါအပြင် Myanmar Computer Emergency Readiness Team ကနေလဲအကြံညွှန်  
တွေရရှုယူနိုင်ပါတယ်။ အောက်မှာ websites address ထည့်ပေးထားပါတယ်။

- <https://www.mmcert.org.mm>

အခုဆက်ပြီးတော့ mobile devices တွေမှာဖြစ်လာနိုင်တဲ့ attack တချို့ကိုလွှဲလာ  
ကြည့်ရအောင်။

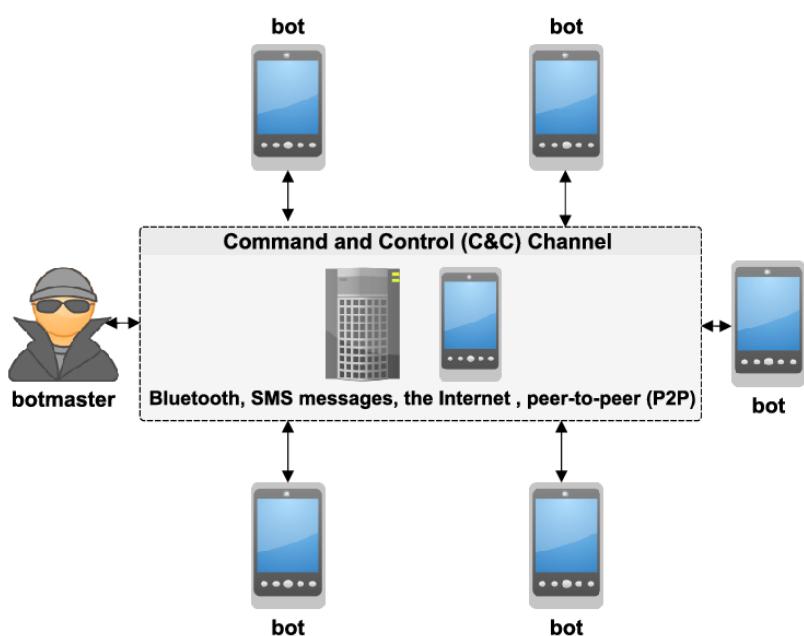
## Malware

Windows တွေတင်မဟုတ်ဘူး Mobile devices တွေမှာလဲ malware  
တွေဝင်ရောက်လာနိုင်ပါတယ်။ Operating system မှာအားနည်းချက်တွေရှိပါ

တယ်နည်းတာနဲ့ များတာပဲကွာပါတယ်။ သမိုင်းကြောင်းအရ mobile device တွေ marketplace ထဲမှ Android ဟာ malware တွေအများဆုံးဝင်ရောက်နိုင် ကြောင်းကိုလဲ GinMaster Trojan က သက်သေဖြစ်ပါတယ်။ အဲ trojan က Android device က confidential information တွေကိုချိုးယူပြီး remote website ကိုပြန်ပို့တာမျိုးတွေလုပ်ဆောင်ပါတယ်။ Virus, worms, rootkits နဲ့ malware တို့ကိုအများဆုံးဝင်ရောက်တာကတော့ Android OS ကအများဆုံးဖြစ်ပြီး iOS နဲ့ တခြား Mobile device operating system တွေမှာလဲ ဝင်ရောက်တာမျိုးတွေရှိပါတယ်။

## Botnet Activity

Mobile devices တွေကလဲ computer တွေလို့မျိုး botnets တွေအတွက် zombie တွေဖြစ်လာနိုင်ပါတယ်။ ဘာကြောင်လဲဆိုတော့ mobile devices တွေက access လုပ်ဖို့အတွက်ပိုပြီးတော့လွယ်ကူတာကြောင့်ပါ။ Mobile devices တွေကမှ တစ်ဆင့် Distributed denial-of-service (DDoS) attacks တွေဖြစ်လာနိုင်ဖို့ အစိတ်ပိုင်းတစ်ခု အနေနဲ့ဖြစ်နိုင်သလို Scam message တွေကို user တွေရဲ့ mobile device တွေကို sms မှတစ်ဆင့်ပို့ဆောင်တာမျိုးတွေလဲ ဖြစ်လာနိုင်ပါတယ်။



## SIM Cloning and Carrier Unlocking

Smartphones တွေမှာဖြစ်နိုင်တဲ့ နောက်ထား SIM cloning attack ဖြစ်ပါတယ်။ ဒီ attack က SIM card ကို duplicate လုပ်ဆောင် တာဖြစ်ပါတယ်။ အဲလို SIM cloning လုပ်ခြင်းအားဖြင့် attacker က victims တွေရဲ့ data တွေကိုရယူနိုင်ပါတယ်။ SIM cloning လုပ်ဆောင်ဖို့အတွက်ဆိုရင် Card Reader လိုအပ်ပါတယ်။ အဲ card reader ထဲမှာ Clone လုပ်ခြင်း SIM card ကိုထည့်ပါတယ်။ ပြီးရင် အဲ sim card ထဲက International Mobile Subscriber Identity (IMSI) နဲ့ Encryption key တို့ကို copy လုပ်ထားပြီး နောက် SIM card အလွတ်တစ်ခုကိုထည့်ပြီး ကူးထည့်တာဖြစ်ပါတယ်။ အောက်မှာ SIM card reader ပုံကိုဖော်ပြပေးထားပါတယ်။



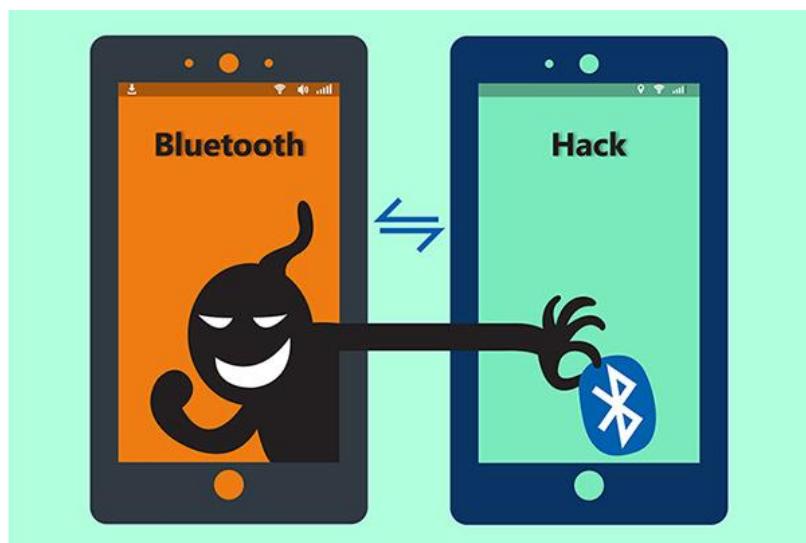
## Wireless Attacks

Smartphone တွေမှာဆိုရင်တော့ wireless service တွေကိုအသုံးပြုလိုရပါတယ်။ Wireless မှာဆိုရင် 4G, 3G, GSM, Wi-Fi, infrared, RFID, Bluetooth စတာတွေပါဝင်ပါတယ်။ အဲထဲမှာဆိုရင် အန္တရာယ်အရှိနှုန်းက Wi-Fi နဲ့ Bluetooth တို့ပဲ ဖြစ်ပါတယ်။ Wireless ကတော့ vulnerabilities အပေါဆုံးပဲ ဖြစ်ပါတယ်။ Mobile devices တွေကို connect လုပ်တဲ့အခါ စိတ်ချရတဲ့ encrypted fashion တွေအသုံးပြု ယုံတင်မဟုတ်ပဲ Security administrator တွေကအသစ်ထွက်တဲ့ CVEs တွေကိုပါ သိထားဖို့လိုအပ်ပါတယ်။ အဲလို CVEs တွေသိထားမှသာ vulnerabilities တွေအတွက် patches အသစ်တွေထွက်တဲ့အခါ update လုပ်နိုင်မှာဖြစ်ပါတယ်။ ဒီ process ကို စာဖတ်သူတွေနားလည် အောင်ရှင်းပြရရင် Wi-Fi လွှင့်တဲ့ Access Point မှာ Buffer overflows vulnerability ရှိတယ်ဆိုရင် attacker က Wi-Fi ကနေမှတစ်ဆင့် remote connect လုပ်လိုရမှာဖြစ်ပါတယ်။ ဒါကြောင့် Access Point တွေမှာ vulnerability ရှိမရှိကို Security Administrator တွေအနေနဲ့ အမြဲလေ့လာနေဖို့လိုအပ်ပါတယ်။ နောက်ပြီး Access Point တွေကို Firmware update ပေးခဲ့ရင်လဲ update လုပ်ဆောင် ပေးဖို့လိုအပ်ပါတယ်။ အခုကျွန်တော်တို့ဆက်ပြီးတော့ Bluetooth မှာဖြစ်နိုင်တဲ့ vulnerability တွေအကြောင်းလေ့လာကြည့်ရအောင်။ Bluetooth မှာဖြစ်နိုင်တဲ့ vulnerability တွေကတော့ Bluejacking နဲ့ Bluesnarfing တို့ပဲဖြစ်ပါတယ်။

**Bluejacking** ဆိုတာက ချိတ်ဆက်ထားတဲ့ devices တွေကို unsolicited messages တွေကိုပို့တဲ့ attack ဖြစ်ပါတယ်။ Bluejacking ကို stop လုပ်ဖို့ အတွက်ဆိုရင် Bluetooth ကိုပိတ်မှုရမှာဖြစ်ပါတယ်။



**Bluesnarfing** ဆိုတာက Bluetooth ချိတ်ဆက်ထားတဲ့ device တွေထံက information တွေကိုရယူတာဖြစ်ပါတယ်။



### Accessing the device

Mobile device တွေဟာသေးငယ်တဲ့အတွက် အခိုးခံရဖို့ အလွန်လွယ်ကူပါတယ်။ တစ်ကယ်လို့ အဲလို့တွေဖြစ်လာခဲ့ရင် data တွေကို တြေားသူတွေမရအောင်ကာကွယ်ဖို့လိုအပ်ပါတယ်။ အဲအတွက် ပထမဦးဆုံးအနေနဲ့ screen locks နဲ့ passwords ကိုအသုံးပြုရပါမယ် နောက် biometric နဲ့ context-aware

authentication တိုကိုအသုံးပြုသင့်ပါတယ်။ တစ်ခုချင်းစီအကြောင်းကို ဆက်ပြီး လေ့လာကြည့်ရအောင်။

- **Screen lock:** Screen lock ဆိုတာက mobile device ကိုမသုံးတဲ့အခါ screen ကို deactivate လုပ်ထားတာဖြစ်ပါတယ်။ အဲလိုလုပ်လိုက်တဲ့အခါ device က locks ဖြစ်သွားပြီး အသုံးပြုချင်တယ်ဆိုရင်တော့ PIN number ကိုထည့်သွင်းပေးမှသာအသုံးပြုနိုင်မှာဖြစ်ပါတယ်။
- **Passwords and PINs:** Mobile တွေမှာဆိုရင် Passwords နဲ့ PINs ဆိုပြီး authentication တွေရှုပါတယ်။ Passwords မှာဆိုရင် numbers, characters, special character စတာတွေနဲ့တဲ့သတ်မှတ်နိုင်ပြီး PIN မှာဆိုရင်တော့ characters 6 လုံးကနေ အထပ်အသုံးပြုနိုင်ပါတယ်။
- **Biometrics:** နောက်ပိုင်း mobile devices တွေမှာဆိုရင် fingerprint, facial စတဲ့ biometrics authentication တွေကိုအသုံးပြုလာကြပါတယ်။
- **Context-aware authentication:** Context-aware security မှာဆိုရင် user ကဘယ်သူလဲ, user ကဘာတွေကို request လုပ်နေသလဲ, user ကဘယ်လို connect လုပ်တာလဲ, user က information တွေကို ဘယ်အချိန်မှာ request လုပ်တာလဲ နောက် user ကဘယ်မှာရှိနေလဲ စတာတွေကိုသိဖို့လိုအပ်ပါတယ်။ သူ့ရဲ့အဓိကပန်းတိုင်က end users ရဲ့ data တွေကိုအလွယ်တကူ access လုပ် ဆောင်လို့မရနိုင်အောင်ကာကွယ်ပေးတာဖြစ်ပါတယ်။ စာဖတ်သူတွေ မြင်သာ အောင်ဉာဏ်ပြောရရင် John က Marketing Department ရဲ့ director တစ်ဦးဖြစ်ပြီး Yangon မှာနေတယ်ပေါ့။ Context-aware authentication အသုံးပြုထားတဲ့အခါ authentication successful ဖြစ်ဖို့ဆိုရင် user က ကြိမ်းသော John ဖြစ်ဖို့လိုအပ်ပါတယ်။ နောက်အချိန်ကလဲ မနက် ၉ နာရီကနေ ၅ နာရီအတွင်း ရက်စွဲက Monday to Friday ဖြစ်ရပါမယ်။ နေတာက Yangon ဖြစ်ရပါမယ်။ တစ်ကယ်လို့ အဲဒါတွေသာမမှန်ခဲ့ဘူးဆိုရင်တော့ authentication fails မှာဖြစ်ပါတယ်။

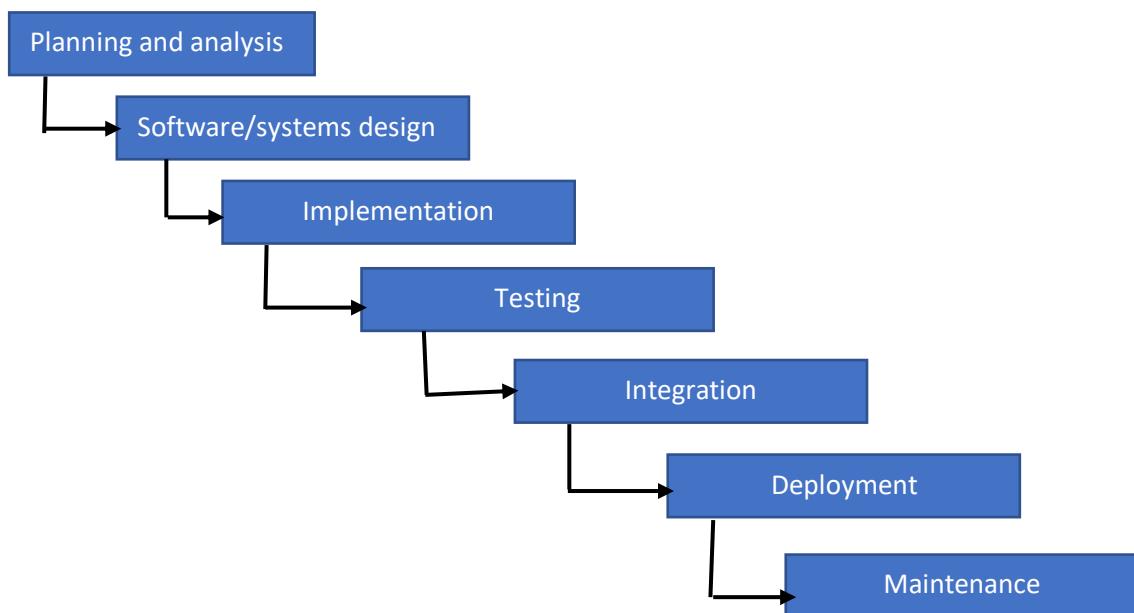
## Chapter 5 – Application Security

### Secure Programming

Secure coding သဘောတရားကတော့ application တွေရေးသားတဲ့အခါ secure ဖြစ်ဖို့အတွက် လုပ်ဆောင်ရတာဖြစ်ပါတယ်။ အခုသင်ခန်းစာများကတော့ programmers တွေအတွက် secure coding သဘောတရားတွေနဲ့ သိထားသင့်တဲ့ vulnerabilities တရှို့ကိုဖော်ပြပေးသွားမှာဖြစ်ပါတယ်။

### Software Development Life Cycle

Software Development Life Cycle ဆိုတာက software development လုပ်တဲ့အခါ လုပ်ငန်းစဉ်တွေဖြစ်တဲ့ planning, developing, testing, deploying, maintaining systems နဲ့ applications တို့ကိုစုစည်းထားတာဖြစ်ပါတယ်။ SDLC ကို company က waterfall model အနေနဲ့အသုံးပြုကြပါတယ်။ ဆက်ပြီး SDLC ကအခြားထားတဲ့ waterfall model မှာပါဝင်တဲ့ အဆင့်တွေကိုလေ့လာကြည့်ရအောင်။



- 1) **Planning and analysis:** Software တစ်ခုရေးသားဖို့အတွက် လိုအပ်တာတွေ ကိုစိစ္စတဲ့အပိုင်းဖြစ်ပါတယ်။
- 2) **Software/systems design:** System ဒါမှုမဟုတ် Application design မှာ သတ်မှတ်မယ့် diagram ဖြစ်ပါတယ်။
- 3) **Implementation:** Project မှာရေးမယ့် code အပိုင်းဖြစ်ပါတယ်။
- 4) **Testing:** System ဒါမှုမဟုတ် Application ရေးပြီးသွားတဲ့အခါ ပြန်လည် စမ်းသပ်တာ ဖြစ်ပါတယ်။
- 5) **Integration:** Application မှာ multiple systems တွေပါဝင်ခဲ့ရင် အဲ application ကို systems တွေနဲ့ပြီးတော့ test လုပ်တာဖြစ်ပါတယ်။ ဥပမာ Application နဲ့ database server တွဲသုံးသလိုမျိုးဖြစ်ပါတယ်။
- 6) **Deployment:** ဒါကတော့ Application ဒါမှုမဟုတ် System ကို user တွေ အသုံးပြုနိုင် အောင်လုပ်ဆောင်တာဖြစ်ပါတယ်။
- 7) **Maintenance:** Maintenance မှာတော့ update, version control စတာတွေ ပါဝင်ပါတယ်။

အခုက္ခန်းတော်ဖော်ပြပေးသွားတာကတော့ SDLC methodology ရဲ့အခြေခံ အဆင့် တွေဖြစ်ပါတယ်။

## Programming Testing Methods

Programmers တွေက system testing, input validation, fuzzing စတဲ့ နည်းလမ်းတွေနဲ့ code တွေကိုစမ်းသပ်ကြပါတယ်။ အဲလို testing လုပ်တာတွေက SDLC ရဲ့ testing အဆင့်မှာပါဝင်ပါတယ်။

## White-box and Black-box Testing

System testing မှာဆိုရင် black-box နဲ့ white-box ဆိုပြီး (၂) မျိုးရှိပါတယ်။ **Black-box** testing မှာဆိုရင် tester က system နဲ့ပတ်သက်တဲ့ မည်သည့် information ကိုမှုမသိပါဘူး။ အဲ testing ကို test လုပ်တဲ့အခါ tester တွေက system မှာအသုံး ပြုထားတဲ့ code တွေနဲ့ပတ်သက်ပြီး ကိုသိထားဖို့လို

အပ်ပါတယ် နောက် programing knowledge လဲအနည်းငယ်ရှိဖို့လဲလိုအပ်ပါတယ်။ Black-box testing ရဲ့အဓိကပန်းတိုင်တွေထဲက တစ်ခုကတော့ system crash ဖြစ်သွားဖို့ပဲဖြစ်ပါတယ်။ တစ်ကယ်လို့ user က မမှန်ကန်တဲ့ input တွေကိုထည့်သွင်းမိလို့ system က crash ဖြစ်ခဲ့မယ်ဆိုရင် programmer က error-handling code နဲ့ input validation တို့ကိုစစ်ဆေးရမှာဖြစ်ပါတယ်။

**White-box testing** မှာတော့ application / system က အမှန်တစ်ကယ် အလုပ်လုပ်မလုပ် ကိုစစ်ဆေးတာဖြစ်ပါတယ်။ Testers က programming knowledge တွေရှိဖို့လိုအပ်ပြီး system နဲ့သက်ဆိုင်တဲ့ information တွေဖြစ်တဲ့ login details, production documentation နဲ့ source code စတာတွေကို ပေးဖို့လိုအပ်ပါတယ်။ Tester က stress testing, penetration testing, sandboxes စတဲ့နည်းလမ်းတွေကို ပေါင်းစပ်ပြီးတော့ test လုပ်မှာဖြစ်ပါတယ်။ Stress testing ဆိုတာက ပုံမှန်အားဖြင့်တော့ system ဒါမှမဟုတ် application ကို critical ဖြစ်အောင် real-time စမ်းသပ်တာဖြစ်ပါတယ်။ Penetration testing ဆိုတာက system security အတွက် simulation attack လုပ်ဆောင် တာဖြစ်ပါတယ်။ Sandboxes ဆိုတာကတော့ code ကို virtual environment မှာ run တာဖြစ်ပြီး တခြား running ဖြစ်နေတဲ့ process တွေကိုထိခိုက်မှာစိုးလို့ အသုံးပြုတာဖြစ်ပါတယ်။ Sandboxing technology ကို malware, malignant code နဲ့ error ဖြစ်စေတဲ့ buffer overflows စတဲ့ unverified applications တွေအတွက်ကိုလဲအသုံးပြုရပါတယ်။

## Input Validation

Input validation က Website design နဲ့ Application development အတွက်အလွန်အရေးပါ ပါတယ်။ Input validation ဒါမှမဟုတ် data validation ဆိုတာက users တွေက web forms မှာ input လုပ်လိုက်တဲ့ data တွေမှန်မမှန်စစ်ဆေးတာဖြစ်ပါတယ်။ တစ်ကယ်လို့ data တွေကမှန်ကန်မှုမရှိပါ က အဲကမှတစ်ဆင့် application မှာ vulnerability ဖြစ်ပေါ်စေနိုင်ပြီး sensitive

data တွက်ရရှိနိုင်သွားစေပါတယ်။ Input validation ကို client side မှာသာ မက server side မှာပါလျှပ်ဆောင်သင့်ပါတယ်။ XSS, SQL injection စတဲ့ vulnerability တွေက Input validation မှတစ်ဆင့်ဖြစ်ပေါ်တာဖြစ်ပါတယ်။

## Static and Dynamic Code Analysis

Static code analysis ဆိုတာက debugging အမျိုးစားဖြစ်ပြီး code တွက် program executing လုပ်ဖို့မလိုပဲ စစ်ဆေးတာဖြစ်ပါတယ်။ အဲလို code တွက်စစ်တဲ့အခါ language ပေါ်မှုတည်ပြီး manual လဲစစ်နိုင်သလို automated tools တွက်အသုံးပြုပြီးတော့လဲစစ်နိုင်ပါတယ်။ Static code analysis က program မှာ ဖြစ်စေနိုင်တဲ့ issues တွက်ဖော်ထုတ်ဖို့ ကူညီပေးပါတယ်။ SDLC ရဲ့ testing အဆင့်မှာဆိုရင် ဒါဟာအရေးပါပါတယ်။ တစ်ခါတစ်လေ dynamic analysis ဥပမာ fuzz testing လဲလျှပ်ဆောင်ပါတယ်။

## Fuzz Testing

Fuzz testing ကိုတော့ dynamic analysis လိုခေါ်ပါတယ်။ Fuzzing လုပ်ဆောင်တဲ့အခါ random data တွက် input လုပ်ပြီး vulnerabilities ရှာတာဖြစ်ပါတယ်။ ဒီနည်းလမ်းကိုတော့ program ရဲ့ source code နဲ့ပတ်သက်ပြီး knowledge မရှိတဲ့အခါမျိုးမှာအသုံးပြုပါတယ်။ Program ကို test လုပ်ဖို့အတွက် run လိုက်တယ်ပြီးရင် data တွေ input လုပ်ပါတယ်။ အဲနောက် program ဟာ crashes ဖြစ်မဖြစ်ကို monitoring လုပ်ပါတယ်။ Fuzz testing က full system failures, memory leaks, error-handling issues တွေကိုလဲဖော်ထုတ်ပေးနိုင်ပါတယ်။

## Programming Vulnerabilities and Attacks

အခုခြားအပိုင်းမှာတော့ application level မှာဖြစ်ပေါ်တဲ့ vulnerabilities တွေနဲ့ attacks တွေအကြောင်းကိုလေ့လာရမှာဖြစ်ပါတယ်။

## Backdoors

တချို့ application တွေမှာ backdoor တွေပါဝင်တက်ပါတယ်။ Programmer က program ကို launch လုပ်ပြီးတဲ့အခါ နောက်တစ်ကြိမ် လိုအပ်တာ တွေကို ပြန်လည်ပြပြင်ဖို့လိုအပ်လာတဲ့အခါ အသုံးပြုဖို့ backdoor code ကိုထည့်သွင်းထားတက်ပါတယ်။ ကျွန်တော်တို့အနေနဲ့ program ကို အသုံးပြုတဲ့အခါ programmer တွေက backdoor တွေကိုဖြုတ်ထားလား မဖြုတ်ထားဘူးလား ဆိုတာသိဖို့အတွက် analyze လုပ်သင့်ပါတယ်။ ဘာကြောင့်လဲဆိုရင် attacker က ဒီအားနည်းချက်ကိုတွေ့သွားတဲ့အခါ unauthorized access ဖြစ်လာနိုင်ပါတယ်။

## Memory/Buffer Vulnerabilities

ဒါကိုတော့ Buffer overflow လိုပေါ်ပါတယ်။ Buffer overflow vulnerabilities ဖြစ်စေတဲ့အကြောင်းက program ထဲကို data တွေအများကြီး ထည့်သွင်းတဲ့အခါမျိုးမှာဖြစ်တက်ပါတယ်။ အဲလို data တွေအများကြီး ထည့်သွင်းတဲ့ အခါ data တွေက memory ထဲက space တွေကိုပျက်စီးစေ ပြီးနောက် memory ထဲက တခြား data တွေကိုပါပြောင်းလဲသွားစေနိုင်ပါတယ်။ အဲအခါ program ကနေ error report ကိုပြပေးမှာဖြစ်ပါတယ်။ ဒါက တော့ Buffer overflow ကိုအတိုချုံရေးသား ဖော်ပြလိုက်တာဖြစ်ပါတယ်။ စာဖတ်သူတွေအနေနဲ့ ဒီထပ်ပိုပြီးတော့ detail သိချင် တယ်ဆိုရင် <https://www.acunetix.com/blog/web-security-zone/what-is-buffer-overflow/> အဲမှာသွားရောက်ဖတ်လိုရမှာဖြစ်ပါတယ်။

## Remote Code Execution

Remote Code Execution ဆိုတာ attacker က target computer ကို vulnerability မှတစ်ဆင့် ဝင်ရောက်ထိန်းချုပ်နိုင်တာကိုပြောတာဖြစ်ပါတယ်။ အဲလို ထိန်းချုပ်ပြီးတဲ့အခါ remote computer ကို commands တွေ execute

လုပ်ဆောင်နိုင်မှာဖြစ်ပါတယ်။ Program မှာ exploit လုပ်ဆောင်လိုအပ်နိုင်တဲ့ bugs ဒါမှမဟုတ် vulnerability ရှိနေခဲ့မယ်ဆိုရင် အဲဒါကို Remote Code Execution Exploit လိုခေါ်ပါတယ်။ RCE commands တွေကို target computer ထံကိုပို့ဆောင်တဲ့အခါ browser ရဲ URL မှသော်လည်းကောင်း Netcat service စတာတွေနဲ့လို့ဆောင်နိုင်ပါတယ်။ RCE ကိုကာကွယ်ဖို့ အတွက်ဆိုရင် အသုံးပြုတဲ့ application တွေက update ဖြစ်နေဖို့လိုအပ်ပါတယ်။ တစ်ကယ်လိုဝယ်သုံးတဲ့ application မဟုတ်ပဲ company မှာပဲ develop လုပ်တဲ့ application ဆိုရင်တော့ fuzz testing ကိုအသုံးပြုပြီးစစ်ဆေးသင့်ပါတယ်။

## XSS and XSRF

Cross-Site-Scripting (XSS) နဲ့ Cross-Site-Request Forgery (XSRF) ဆိုတာက web application တွေမှာတွေ့ရတဲ့ vulnerabilities တွေဖြစ်ပါတယ်။ XSS ဆိုတာက code injection အမျိုးစားဖြစ်ပါတယ်။ User input မှာ attacker က JavaScript လိုမျိုး scripting ကိုအသုံးပြုပြီး malicious code တွေ ကို inject လုပ်ဆောင်တာဖြစ်ပါတယ်။ XSS vulnerability မှတစ်ဆင့် web site ကိုအသုံးပြုနေတဲ့ users တွေရဲ cookies တွေကိုရယူသွားနိုင်ပါတယ်။ Cookies ဆိုတာက login session information တွေကိုပြောတာဖြစ်ပါတယ်။ Cookie ကိုအောက်မှာနူးနာအနေနဲ့ဖော်ပြထားပါတယ်။

PHPSESSIONID: abcdefghijkl00099912829

XSS vulnerability မှာဆိုရင် အမျိုးစား (၃) မျိုးရှိပါတယ်။ အဲဒါတွေကတော့-

- 1) Reflected XSS
- 2) Stored XSS
- 3) DOM

တို့ပဲဖြစ်ပါတယ်။

XSRF/CSRF ကိုတော့နောက်တစ်မျိုး session riding လိုလဲခေါ်ပါတယ်။ End user တွေကို authenticated ဖြစ်ပြီးသား web application မှာ unwanted action တွေကိုလုပ်ဆောင်စေတာမျိုးဖြစ်ပါတယ်။ ဥပမာ jenny ဆိုတဲ့ user မှာ login username : jenny ဖြစ်ပြီး password : 1234 ဆိုပါစူး။ ဒါကို attacker က web application ရဲ့ vulnerability ကိုအခွင့်ကောင်းယူပြီး username : jenny , password : 5678 ဆိုပြီး form တစ်ခုကို create လုပ်ပါတယ်။ အဲနောက် jenny ဆိုတဲ့ user ထံကို email, chat တို့မှတစ်ဆင့် အဲ link ကိုပိုပြီး social engineering ကိုအသုံးပြီး click လုပ်စေပါတယ်။ User က click လုပ်လိုက်တဲ့အခါ login information တွေက attacker create လုပ်ခဲ့တဲ့ အတိုင်းဖြစ်သွားပါတယ်။ XSRF ကို one-click attack လိုလဲခေါ်ပါသေးတယ်။

## Code Injection Attack

Code Injection attack မှာဆိုရင် SQL Injection, XML Injection, LDAP Injection တွေပါဝင်ပါတယ်။

SQL Injection ဆိုတာက database နဲ့ချိတ်ဆက်ထားတဲ့ application တွေမှာတွေရတဲ့ vulnerability ဖြစ်ပါတယ်။ အဲ vulnerability မှာတစ်ဆင့် SQL Query ကို input လုပ်ပြီး database ထဲက data တွေကိုဆွဲထုတ်ကြည့်နိုင်ပါတယ်။ ဥပမာ username, password, phone number, email address စတာတွေဖြစ်ပါတယ်။

XML Injection ဆိုတာက XML (Extensible Markup Language) ကိုအသုံးပြုထားတဲ့ applications တွေမှာတွေရတဲ့ vulnerability အမျိုးစားဖြစ်ပါတယ်။ ဥပမာ XML structures မှာဆိုရင် users အတွက် codes တွေပါဝင်ပါတယ်။ အဲကမှတစ်ဆင့် users အသစ်ကို create လုပ်ပြီး administrative access ရတဲ့အထိလုပ်ဆောင်နိုင်ပါတယ်။

LDAP Injection ကတော့ SQL injection နဲ့ပုံစံတူပါတယ်။ LDAP (Lightweight Directory Access Protocol) ဆိုတာက protocol တစ်ခုဖြစ်ပြီး

user account လို့ information တွေကိုထိန်းသိမ်းတာဖြစ်ပါတယ်။ LDAP Injection ကိုတော့ input box ကနေမှတစ်ဆင့် gain access ရအောင်လုပ် နိုင်သလို လုံခြုံရေးအားနည်းတဲ့ LDAP configuration မှတစ်ဆင့်လဲ exploit လုပ်ဆောင်နိုင်ပါတယ်။

### Directory Traversal

Directory Traversal ဒါမှမဟုတ် ../(dot dot slash) vulnerability ဆိုတာက web application မှတစ်ဆင့် system ထဲက files တွေကို read လုပ်ဆောင်လို့ရတာ ဖြစ်ပါတယ်။

### Zero Day Attack

Zero Day Attack ဆိုတာက software ဖြစ်ပေါ်တဲ့ vulnerability ဖြစ်ပြီး အဲ vulnerability ကို fix လုပ်ဖို့အတွက် patch ကို create မလုပ်ရသေးတဲ့ အခြေနေကိုခေါ်တာဖြစ်ပါတယ်။

## Chapter 6 – Vulnerability and Risk Assessment

Vulnerability ဆိုတာ risk management ရဲ့အစိတ်ပိုင်းတစ်ခုဖြစ်ပါတယ်။ Risk မှာ ဆိုရင် vulnerabilities, potential dangers, possible hardware and software failure စသာတွေပါဝင်ပါတယ်။

### Risk management

Risk ဆိုတာက Company မှာရှိနေတဲ့ access (access တွေကိုအောက်မှာ ဖော်ပြပေးထားပါတယ်)တွေကို ထိခိုက်စေနိုင်တာကို risk လို့ခေါ်ပါတယ်။ Risk management ဆိုတာက Company မှာရှိနေတဲ့ risk တွေကို သတ်မှတ် တယ်ပြီးရင်အဲ risks level တွေကိုဘယ်လိုလျှော့ချရ မလဲဆိုတာကို လုပ်ဆောင်ရတာ ဖြစ်ပါတယ်။ ကျွန်တော်တို့က risk တွေကိုလုံးဝ ပျောက်သွားအောင်တော့ လုပ်ဆောင် လို့မရပေမယ့် တက်နိုင်သလောက်တော့ လျှော့ချရမှာဖြစ်ပါတယ်။ ပထမဗြို့ဆုံး risk management လုပ်ဖို့အတွက်လုပ်ရမှာက asset တွေကိုသတ်မှတ်တာဖြစ်ပါတယ်။ အဲလို့လုပ်ခြင်းအားဖြင့် asset တွေကို ဘယ်လိုကိုင်တွယ်မလဲ၊ ဘယ်လိုသိမ်းမလဲ၊ ဘယ်လိုကာကွယ်ရမလဲ နဲ့ ဘယ်သူတွေက asset တွေကို access လုပ်နေတာလဲဆိုတာတွေ ကိုသိနိုင်မှာဖြစ်ပါတယ်။ Risk management လုပ်တော့မယ်ဆိုရင် ကျွန်တော်တို့က အောက်မှာဖော်ပြထားတဲ့ module 5 ခုကိုသိထားဖို့လိုအပ်ပါတယ်။

- Defining Risk
- Risk Management Concepts
- Risk Assessment
- Risk Response
- Business Impact Analysis

တို့ပဲဖြစ်ပါတယ်။

## Module 1: Defining Risk

ဒီ module မှာတော့ risk တွေကိုဘယ်လိုသတ်မှတ်ရမလဲဆိုတာကိုလေ့လာရမှာ  
ဖြစ်ပါတယ်။ အဲလို့ risk တွေကိုသတ်မှတ်တဲ့အခါ risk ဖြစ်နိုင်တဲ့အောက်ပါအချက်တို့  
ကို သိထားဖို့လိုအပ်ပါတယ်။

- Vulnerability
- Threat
- Asset

### Vulnerability and Threat

Vulnerability ဆိုတာက လုပ်ချေးဆိုင်ရာအားနည်းချက်ကိုပြောတာဖြစ်  
ပါတယ်။

Threat ဆိုတာက Vulnerability မှတစ်ဆင့်ထိခိုက်စေနိုင်တာကို ပြော  
တာဖြစ်ပါတယ်။

Vulnerability နဲ့ Threat ကိုစာဖတ်သူတွေမြင်သာအောင်ပြောရရင် Web  
Server မှာအသုံးပြုထားတဲ့ service ဖြစ်တဲ့ apache2 ရဲ့ version က  
vulnerability ဖြစ်နေတယ်ဆိုပါစို့ အဲဒါကို attacker ကတွေ့သွားပြီး access ရ<sup>လို</sup>  
ရှိအောင်ကြိုးစားတာဖြစ်ပါတယ်။

### Asset

Asset ဆိုတာက IT infrastructure ထဲမှာပါတဲ့အစိတ်ပိုင်းတွေ အားလုံး  
ပါဝင်ပါတယ်။ စာဖတ်သူတွေမြင်သာအောင်ဆိုရင်

- Servers
- Workstations
- Applications
- Data
- Personnel

- Wireless access
- Internet services

အပေါ်မှာဖော်ပြထားတာတွေအကုန်လုံးက Asset တွေပဲဖြစ်ပါတယ်။ အခုက္ခန်တော်တို့ Risk Defining ကိုဆက်သွားရအောင်။အဓိက risk ဖြစ်စေတာ ကတော့

**Risk = Threat + Vulnerability + Asset**

တို့ကြောင့်ပဲဖြစ်ပါတယ်။



## Module 2: Risk Management Concepts

IT security professionals တွေအနေနဲ့ သူတို့ရဲ့ organizations လုံခြုံဖို့အတွက် risk management နည်းလမ်းတွေကိုပြင်ဆင်ရသလို threats တွေကိုလဲ လျှော့ချို့ အတွက်လိုအပ်ပါတယ်။ ဒီမှာတော့ ရှုံးထောင် င့် ခုကနေ risk management လုပ်ပါ မယ်။ အဲဒါတွေကတော့ Infrastructure, Security Controls, Risk Management Frameworks, Industry-standard frameworks တို့ပဲဖြစ်ပါတယ်။

## Infrastructure

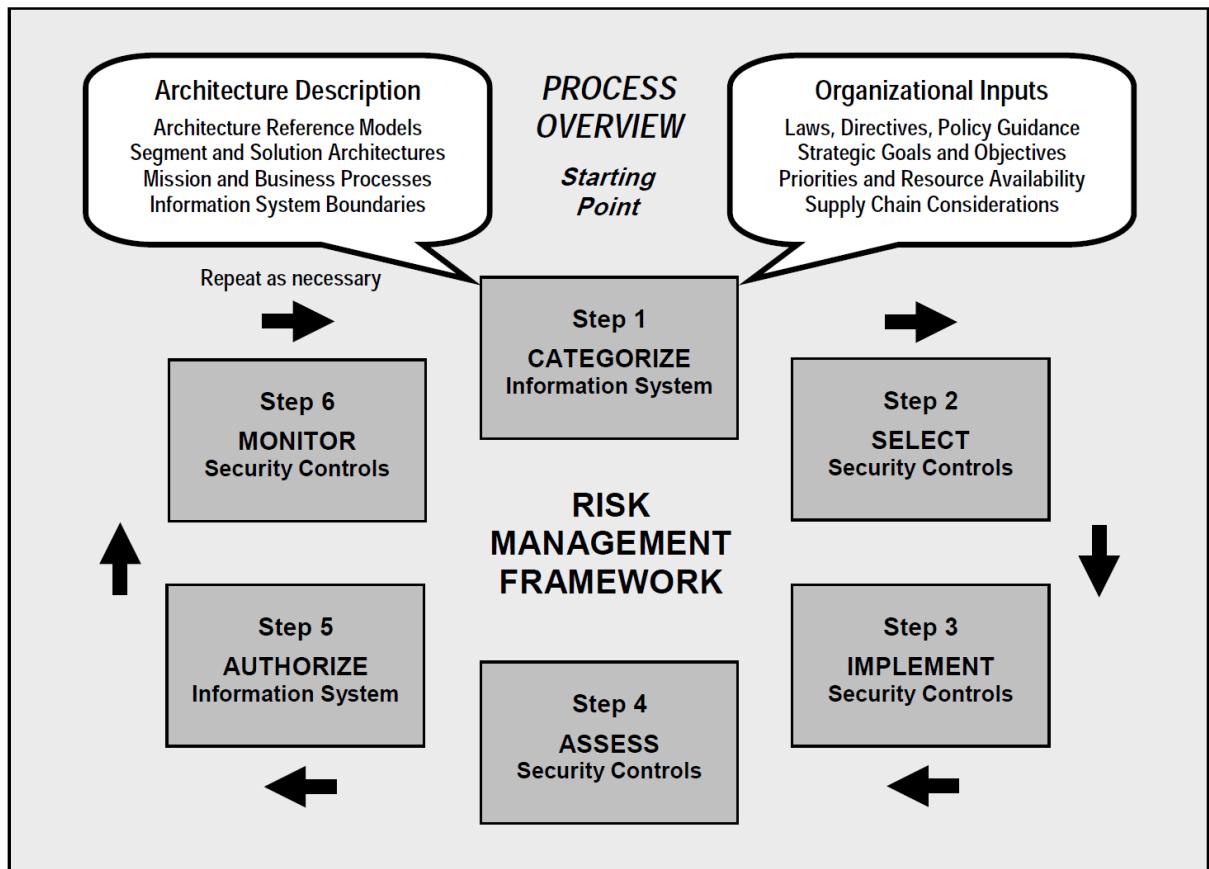
IT risk management မှာဆိုရင် infrastructure ဟာအဓိကအရေးပါပါတယ်။ ဒဲ infrastructure မှာဆိုရင် computers, networks, employees, physical security တို့ပါဝင်ပါတယ်။

## Security Controls

Security controls တွေဆိုတာ Organizations တစ်ခုလုံး၏ဖြို့အတွက် မသုံးမဖြစ်သုံးရတာတွေကိုပြောတာဖြစ်ပါတယ်။ အသေးစိတ်ကို Chapter 1 မှာ ဖော်ပြခဲ့ပြီးသားဖြစ်ပါတယ်။

## Risk Management Framework (RMF)

Risk Management Framework မှာဆိုရင် risk management လုပ်ဆောင်ရမယ့် လုပ်ငန်းစဉ်တွေ, အဓိကအရေးကြီးတဲ့အဆင့်တွေနဲ့ အဲအဆင့် တွေတစ်ခုခြင်းကို အာရုံစိုက်ခြင်းတို့ကိုဖော်ပြထားတာဖြစ်ပါတယ်။ Framework ထဲမှာဆိုရင် National Institute of Standards and Technology (NIST) ကအလွယ်ကူဆုံးနဲ့ အထင်ရှားဆုံးဖြစ်ပါတယ်။ အဲဒါကိုအောက်မှာပုံနဲ့ ဖော်ပြပေးထားပါတယ်။



NIST RMF ၏ Architecture Description နဲ့ Organizational Inputs ဆိုပြီး အဓိက major 2 ခုကိုဖော်ပြထားပါတယ်။ Architecture Description ၏ organization မှာအသုံးပြုနေတဲ့ information systems ရဲ့ ပုံစံ နဲ့ဖွဲ့စည်းထားပုံ ကိုဖော်ပြထားတာဖြစ်ပြီး architecture ၏တော့ security controls တွေကို ပြောတာဖြစ်ပါတယ်။ Organizational Inputs ၏တော့ ပိုပြီးတော့စိတ်ဝင်စားဖို့ ကောင်းပါတယ်။ အဲမှာဆိုရင်တော့ resource တွေကာဘယ် security controls တွေကနေလာလဲဆိုတာကိုဖော်ပြထားတာဖြစ်ပါတယ်။ Resources မှာဆိုရင် Laws, Standards, best practices, security policies တို့ပါဝင်ပါတယ်။

### Module 3: Risk Assessment

Risk assessment ဆိုတာက risk ဖြစ်နိုင်တာတွေကိုရှာမယ် ပြီးရင် အသင့်တော် ဆုံးနည်းလမ်းတွေကိုအသုံးပြုပြီး risk တွေကလျှော့ချတာဖြစ်ပါတယ်။ Risk assessment လုပ်ဖို့အတွက် ဆိုရင် အောက်ပါအချက်တွေလိုအပ်ပါတယ်။

- Identifying all threats
- Identifying all scenario of risk to the organization
- Mapping the risks on likelihood and criticality
- Recommendations on how to fix them

Risk assessment လုပ်တဲ့နေရာမှာနည်းလမ်း (၂) မျိုးရှိပါတယ် အဲဒါတွေက တော့ -

- Qualitative Risk Assessment
- Quantitative Risk Assessment

တို့ပဲဖြစ်ပါတယ်။

### **Qualitative Risk Assessment**

Qualitative risk assessment ဆိုတာက risk ဖြစ်နိုင်ခြေရှိတာတွေနဲ့ အဲ risk ကနေမှတစ်ဆင့် system ဒါမှမဟုတ် network ပေါ်သက်ရောက်နိုင်မှုကို numeric values တွေသတ်မှတ်ပြီး assessment လုပ်တာဖြစ်ပါတယ်။ သူက Quantitative risk assessment နဲ့မတူတာက assets တွေနဲ့ဆုံးရှုံးမှုတန်ဖိုးတွေ ကိုမသတ်မှတ်နိုင်ပါဘူး။ Qualitative risk assessment ကိုအသုံးပြုခြင်းက လွယ်ကူခြင်း၊ မြန်ဆန်ခြင်း နဲ့ ကုန်ကျစရိတ်သက်သာခြင်းတို့ပဲဖြစ်ပါတယ်။ ဒီနည်းလမ်းကိုအသုံးပြုပြီး risks တွေကို 1 to 10 ဒါမှမဟုတ် 1 to 100 စတဲ့ ranges တွေကို သတ်မှတ်နိုင်ပါတယ်။ အမြင့်ဆုံး number က risk အမြင်ဆုံး ဖြစ်နိုင်ပြီး system ကိုထိခိုက်မှုအပြင်းထန်ဆုံးဖြစ်ပါတယ်။

### **Quantitative risk Assessment**

Quantitative risk assessment ဆိုတာက risk ရဲ့သက်ရောက်မှုကြောင့် ကုန်ကျနိုင်မယ့် ငွေကြေးပေါ်မှုတည်ပြီးတိုင်းတာဖြစ်ပါတယ်။ အဲမှာဆိုရင် asset တွေဖြစ်တဲ့ servers, router တိုးသော network equipment တွေရဲ့ values တွေပါဝင်ပါတယ်။ Quantitative risk ကိုတွက်တဲ့အခါ values ၃ ခုကိုအသုံးပြုပါတယ်။ အဲဒါတွေကတော့

- Single loss expectancy (SLE): Incident တစ်ခုဖြစ်တိုင်းကုန်ကျတဲ့ ငွေကြေးတန်ဖိုးဖြစ်ပါတယ်။
- Annualized rate of occurrence (ARO): နှစ်တိုင်းမှာဖြစ်တဲ့ incident တွေဖြစ်တဲ့အကြိမ်အရေအတွက်ကိုပြောတာဖြစ်ပါတယ်။
- Annualized loss expectancy (ALE): ဒါကတော့ incident ကြောင့် ကုန်ကျခဲ့ရတဲ့ တစ်နှစ်အတွင်းကုန်ကြောင့် ငွေကြေးတန်ဖိုးစုစုပေါင်းကိုပြောတာဖြစ်ပါတယ်။

အပေါ်က ၃ ခုကိုအသုံးပြုပြီး Quantitative Risk တွက်တဲ့အခါ

$$\text{SLE} \times \text{ARO} = \text{ALE}$$

ဖြစ်ပါတယ်။

#### Module 4: Risk Response

အပေါ်အပိုင်းတွေမှာတူန်းက risk တွေကိုဘယ်လို analyzed လုပ်ရမလဲ ဘယ်လိုသတ်မှတ်ရမလဲဆိုတာတွေကို လေ့လာခဲ့ပြီးသားဖြစ်ပါတယ်။ အခုသင်ခန်းစာ မှာတော့ risk တွေက organization တွေပေါ်သက်ရောက်နိုင်မှုတွေကို ဘယ်လိုလျော့ချရမလဲဆိုတာကိုလေ့လာရမှာဖြစ်ပါတယ်။ Risk response မှာဆိုရင် နည်းလမ်း င ခုရှိပါတယ်။ အဲဒါတွေကတော့

- Mitigate
- Transfer
- Accept
- Avoid

တို့ပဲဖြစ်ပါတယ်။ Organization တွေက cost, effectiveness စတာတွေပေါ်မှုတည်ပြီး risk တွေကို mitigation, transfer, accept, avoid စတာတွေကိုရွေးချယ်နိုင်ပါတယ်။

**Risk mitigation** ဆိုတာက risk ကိုလျှော့ချခြင်း ဒါမှမဟုတ် asset တွေအပေါ် သက်ရောက်မှုနည်းနိုင်သမျှ နည်းအောင်လုပ်ဆောင်တာဖြစ်ပါတယ်။ ဥပမာ Computer တစ်လုံးမှာ antivirus မတင်ထားဘူးဆိုရင် ဒါဟာ risk တစ်ခုပါ။ အဲ risk ကိုလျှော့ချဖို့အတွက်ဆိုရင် antivirus တစ်ခုခုကိုဝယ်သုံးခြင်းဖြစ်ပါတယ်။

**Risk transfer** ဆိုတာက organization ထဲမှာရှိနေတဲ့ risk ကို တခြား third party ကိုအခကြားငွေပေးပြီး တာဝန်ယူစေခြင်းမျိုးဖြစ်ပါတယ်။ ဥပမာ Organization မှာ Cyber Security နဲ့ပတ်သက်တဲ့ ဝန်ထမ်းမရှိဘူးဆိုပါစို့ ဒါဆိုရင် Cyber Security Solutions လုပ်တဲ့ Company တစ်ခုခုကိုငှားရမ်းအသုံးပြုခြင်းဖြင့် Risk ကို transfer လုပ်နိုင်ပါတယ်။

**Risk accept** ဆိုတာ organization မှာရှိနေတဲ့ risk ကိုလုံးဝမလျှော့ချတာဖြစ်ပါတယ်။ ဒီနည်းလမ်းကိုဘယ်အချိန်မှာရွေးလဲဆိုရင် risk ကိုလျှော့ချဖို့အသုံးပြုရမယ် တန်ဖိုးက အဲ risk ကြောင့်ဆုံးရှုံးနိုင်တဲ့တန်ဖိုးထပ်များနေတဲ့အခါမျိုးမှာဆိုရင် organization တွေက risk accept လုပ်ကြပါတယ်။ စာဖတ်သူတို့မြင်သာအောင်ပြောရရင် risk ကြောင့်ဆုံးရှုံးနိုင်တဲ့တန်ဖိုးက \$100 ဆိုပါစို့ အဲ risk ကိုလျှော့ချဖို့အတွက် အသုံးပြုရမယ့်ပမာဏက \$1000 ဆိုရင် risk ကို accept ပဲလုပ်လိုက်တာဖြစ်ပါတယ်။

**Risk Avoid** ကတော့ risk accept နဲ့ပြောင်းပြန်ဖြစ်ပါတယ်။ Risk ကြောင့်ဆုံးရှုံးနိုင်တဲ့ပမာဏ ကဘယ်လောက်ပဲဖြစ်ဖြစ် အဲ risk ကိုလျှော့ချဖို့အတွက် ငွေကြားဘယ်လောက်ကုန်ကုန်အသုံးပြုမှာဖြစ်ပါတယ်။

## Module 5: Business Impact Analysis

IT infrastructure တွေ incidents တွေကိုကာကွယ်ဖို့အတွက်ဆိုရင် risk assessment ကိုလိုအပ်ပါတယ်။ ကျွန်တော်တို့အနေနဲ့ incident ကနေဖြစ်လာမယ့် အကျိုးဆက်တွေက Organization အပေါ်ဘယ်လိုသက်ရောက်မှုမျိုးတွေ ရှိလာနိုင်တယ်ဆိုတာကိုသိထားဖို့လိုအပ်ပါတယ်။ အဲလိုတွေသိဖို့ဆိုရင် Security Professional တွေအနေနဲ့ Business Impact Analysis (BIA) ကိုလုပ်ဆောင်ဖို့လိုအပ်ပြီး BIA က incidents ဖြစ်တဲ့အကျိုးဆက်တွေကို incidents ဖြစ်တဲ့အခါ ထိခိုက်သွားတဲ့

resources တွေကို recover လုပ်ဖို့နဲ့ ကြောချိန်ကိုပါ ခန့်မှန်းနိုင်မှာဖြစ်ပါတယ်။ NIST ရဲ့ SP 800-34, Revision 1, "Contingency Planning Guide for Federal Information Systems," မှာဆိုရင် BIA ကို အဆင့် (၃) ဆင့် နဲ့ဖော်ပြထားပါတယ်။

### **1) Determine Mission/business processes and recovery criticality**

Mission/Business က systems တွေကိုသတ်မှတ်ပေးတယ် နောက်ပြီး system တွေကိုခဲ့ဝေအသုံးပြုတဲ့အခါဖြစ်လာနိုင်တဲ့ impact တွေနဲ့ downtime တွေကိုပါခန့်မှန်းထားတာတွေကို support ပေးပါတယ်။

### **2) Identify resource requirements**

Realistic recovery ဆိုတာက mission/business ပြန်လည်စတင်ဖို့အတွက် အဓိကလိုအပ်တဲ့ resource တွေရဲ့တန်ဖိုးတွေကိုသတ်မှတ်တာဖြစ်ပါတယ်။

### **3) Identify recovery priorities for system resources**

အရှေ့မှာကျန်တော်တို့ လုပ်ဆောင်ခဲ့တာတွေရဲ့ ရလဒ်တွေပေါ် မူတည်ပြီးတော့ systems resources တွေ က mission/business တို့ရဲ့လုပ်ငန်းတွေကိုပိုပြီး ချိတ်ဆက်နိုင်မှာဖြစ်ပါတယ်။ အဲလိုလုပ်ဆောင်ခြင်းအားဖြင့် resources တွေကို recovery လုပ်ဆောင်တဲ့အခါ priority levels တွေသတ်မှတ်ပြီးလုပ်ဆောင်နိုင်မှာဖြစ်ပါတယ်။

## **Vulnerability Management**

Vulnerability Management ဆိုတာက Systems နဲ့ Networks တို့မှာ ရှိနေတဲ့ vulnerability ကိုရှာပြီးတော့လျှော့ချတာဖြစ်ပါတယ်။ ဒီအပိုင်းမှာတော့ security tools တွေကိုအသုံးပြုပြီး vulnerability ရှာခြင်း၊ လျှော့ချခြင်း၊ monitoring လုပ်ခြင်း စတာတွေပါဝင်ပါတယ်။ Vulnerability ကို management လုပ်ဖို့အတွက် အဆင့် ၅ ဆင့်ရှိပါတယ်။

**Step 1. Define the desired state of security:** Organization တွမှာ secure ဖြစ်ဖိုအတွက် secure policies တွကိုသတ်မှတ်သင့်ပါတယ်။ အဲ policies တွမှာဆိုရင် access control rules, device configurations, network configurations, network documentation စတာတွေပါဝင်ရပါမယ်။

**Step 2. Create baselines:** Security policies တွေသတ်မှတ်ပြီးတဲ့အခါ accessလုပ်နေတဲ့ Computers, Servers, Network devices, Network တို့ရဲ့လက်ရှိ security အခြေနေတွေကိုလဲသိထားဖို့လိုအပ်ပါတယ်။ အဲလိုလုပ်ဆောင်တာကို Vulnerability Assessments လိုပေါ်ပါတယ်။ Vulnerability Assessments မှာဆိုရင် Vulnerability တွေဖြစ်နိုင်တာတွေကို vulnerability scanning tools တွကိုအသုံးပြုပြီး auditing လုပ်ပါတယ်။

**Step 3. Prioritize vulnerabilities:** ကျွန်တော်တို့ရှာတွေထားတဲ့ vulnerability တွေထဲကဘယ်ဟာတွေကို ဦးစားပေးလုပ်ဆောင်သင့်တယ်ဆိုတာကို ဒီအဆင့်မှာ ဆုံးဖြတ်တာ ဖြစ်ပါတယ်။

**Step 4. Mitigate vulnerabilities:** Vulnerabilities တွေရဲ့ ဦးစားပေး list ထဲမှာပါတာတွေ အကုန်လုံးကိုတက်နိုင်သမျှလျှော့ချို့လိုအပ်ပါတယ်။ ဒါပေမယ့် အဲဒါက organizations ကခွင့်ပြုထားတဲ့ risk ကို accept လုပ်ဖိုသတ်မှတ်ထားတဲ့ levels ပေါ်မူတည်ပါတယ်။ Mitigation techniques မှာဆိုရင် secure code review, review of system, application architecture, system design တို့ပါဝင်ပါတယ်။

**Step 5. Monitor the environment:** Mitigation လုပ်ဆောင်ပြီးသွားတဲ့အခါ results တွေကို monitor လုပ်ဆောင်ဖို့လိုအပ်ပါသေးတယ်။

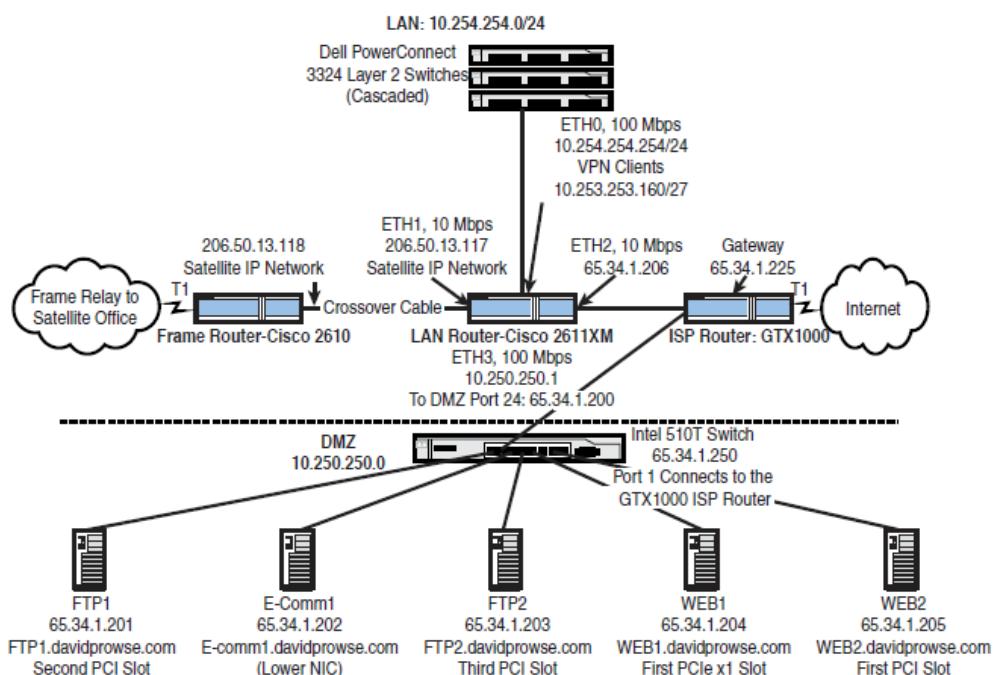
အပေါ်မှာဖော်ပြခဲ့တဲ့ step တွေက vulnerabilities တွေကို manage လုပ်ဖိုအတွက် များစွာအထောက်ကူပြုပါတယ်။ Vulnerabilities management ရဲ့အဓိကအစိတ်ပိုင်းက vulnerabilities တွေကိုရှာမယ် ပြီးရင်တော့လျှော့ချို့ရမှာဖြစ်ပါတယ်။

## Assessing Vulnerability with Security Tools

Vulnerabilities assessment လုပ်ဖို့အတွက်အသုံးပြုတဲ့ tools တွေက တော့ Network mappers, port scanners, vulnerabilities scanners, ping scanners, protocol analyzers/network sniffers, password crackers တို့ပဲ ဖြစ်ပါတယ်။ Vulnerabilities assessment မှာဆိုရင် confidential data / sensitive data တွေကို ရှာဖွေခြင်း, ပွင့်နေတဲ့ ports တွေကိုရှာခြင်း, passwords တွေက weak ဖြစ်နေလား စစ်ဆေးခြင်း, default configurations တွေကိုအသုံး ပြုထားလားစစ်ဆေးခြင်း စတာ တွေကို လုပ်ဆောင်ရပါတယ်။

## Network Mapping

Network documentation ဆိုတာက security အတွက်အရေးပါတဲ့ အစိတ်ပိုင်းတစ်ခုဖြစ်ပါတယ်။ အဲ documentation မှာဆိုရင် Networks တွေချိတ်ဆက်ထားတဲ့ physical & logical connectivity တွေပါဝင်ပါတယ်။ စာဖတ်သူတွေ အလွယ်မှတ်လို့ရအောင်ပြောရရင်တော့ Network Diagrams လိုပေါ်ပါတယ်။ အဲမှာ connectivity တွေအပြင် အသုံးပြုထားတဲ့ devices names, IP address, route information စတဲ့အချက်လက်တွေပါဝင်ပါတယ်။ အောက်မှာ နမူနာပုံကိုဖော်ပြထားပါတယ်။



## Vulnerability Scanning

Vulnerability scanning ဆိုတာက network ထဲမှာရှိနေတဲ့ threats ကိုရှာဖွံ့ဖြိုးအတွက်အသုံးပြုတဲ့နည်းလမ်းဖြစ်ပါတယ်။ ကျွန်တော်တို့ network ထဲမှာရှိနေတဲ့ vulnerability တွေရဲ့ level ကိုသိဖိုးအတွက်ဆိုရင် vulnerability scanner ဒါမှမဟုတ် port scanner ကိုအသုံးပြုရပါမယ်။ Network ထဲမှာရှိနေတဲ့ systems တွေအကုန်လုံးကို scan လုပ်ခြင်းအားဖြင့် အဲ system တွေကို တိုက်ခိုက်လာနိုင်တာတွေကို သိရှိနိုင်ပြီး risk တွေကိုလျှော့ချိန်မှာဖြစ်ပါတယ်။ Vulnerability scanner တွေထဲမှာဆိုရင် အကောင်းဆုံးလိုပြောလိုရတဲ့ scanner တစ်ခုရှိပါတယ်။ အဲဒါက Nessus ဖြစ်ပါတယ်။ Nessus ကိုအသုံးပြုပြီး system တစ်ခုချင်းဆီသော်လည်းကောင်း Networks ထဲမှာရှိနေတဲ့ systems တွေ အကုန်လုံးကိုလည်းကောင်း scan လုပ်ဆောင်နိုင်မှာဖြစ်ပါတယ်။ Port Scanning အတွက်ဆိုရင်တော့ Nmap ကအသင့်တော်ဆုံးဖြစ်ပါတယ်။ Nmap မှာဆိုရင် cli နဲ့ gui version ဂမျိုးပါဝင်ပါတယ်။ အရင်ဆုံး Nmap ကိုအသုံးပြုပြီး port scan လုပ်ဆောင်ကြည့်ရအောင်။ Nmap ကို download ဆွဲမယ်ဆိုရင် <https://nmap.org/download.html> အဲမှာ download လုပ်လို့ရပါတယ်။ Platform ပေါ်မူတည်ပြီးရွေးချယ်ဖို့တော့လိုအပ်ပါတယ်။ ကျွန်တော်ကတော့ Windows အတွက်အသုံးပြုမှာဖြစ်တာကြောင့် .exe နဲ့ဟာကို download ဆွဲမှာ ဖြစ်ပါတယ်။ Nmap ကို download ဆွဲပြီးရင်တော့ Install လုပ်ဆောင်ပါမယ်။ Install လုပ်ဆောင်ပြီးသွားပြီဆိုရင်တော့ Nmap ကိုအသုံးပြုနိုင်ပြီဖြစ်ပါတယ်။ CLI မှာဆိုရင် Nmap လိုခေါ်ပြီး GUI အတွက်ဆိုရင်တော့ Nmap - Zenmap ဖြစ်ပါတယ်။ Version 2 မျိုးစလုံးအတွက် Installer တစ်ခုထဲကိုပဲ Install လုပ်ပေးဖို့လိုအပ်ပါတယ်။ အခု CLI version အတွက်စမ်းကြည့်ပါမယ် cmd ကနေ nmap လို့ရှိက်လိုက်ပါ။

```

Nmap 7.91 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)

```

အပေါ်မှာပြထားတဲ့ပုံကတော့ nmap မှာအသုံးပြည့်ရတဲ့ options တွေပဲဖြစ်ပါတယ်။ ဒါတွေအကြောင်းကိုတော့ ကျွန်တော်မရှင်းပြတော့ပါဘူး။ အခုံ nmap ကိုအသုံးပြပြီးတော့ port scan လုပ်ကြည့်ပါမယ်။ Command ကတော့ nmap -p 80 www.google.com ဖြစ်ပါတယ်။ ဒါ command မှာပါဝင်တဲ့ -p ဆိုတာက specific port ကိုသတ်မှတ်လိုက်တာပါ ကျွန်တော်က 80 ဆိုပြီးသုံးထားတဲ့ အတွက် [www.google.com](http://www.google.com) ဆိုတဲ့ website မှာ port 80 ရဲ့ status ကို စစ်ဆေးတာဖြစ်ပါတယ်။

```
C:\Users\ >nmap -p 80 www.google.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-24 20:04 Myanmar Standard Time
Nmap scan report for www.google.com (172.217.194.99)
Host is up (0.065s latency).
Other addresses for www.google.com (not scanned): 172.217.194.105 172.217.194.104 172.217.194.106
03:c04::6a

PORT      STATE SERVICE
80/tcp    open  http
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 1.10 seconds
```

ပုံမှာဆိုရင် port 80 ရဲ့ status က open ဖြစ်နေတာကိုစာဖတ်သူတွေ တွေ့မြင် ရမှာဖြစ်ပါတယ်။ အခုဆက်ပြီးတော့ အဲဒီ website မှာ port 22 ရဲ့ status ကို ထပ်ပြီးတော့စစ်ကြည့်ရအောင်။

```
C:\Users\ >nmap -p 22 www.google.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-24 20:09 Myanmar Standard Time
Nmap scan report for www.google.com (74.125.24.105)
Host is up (0.021s latency).
Other addresses for www.google.com (not scanned): 74.125.24.99 74.125.24.147 74.125.24.148

PORT      STATE SERVICE
22/tcp    filtered ssh
22/tcp    filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 0.86 seconds
```

ဒါပုံမှာဆိုရင်တော့ port 22 ရဲ့ status က filtered ဆိုပြီးဖြစ်နေတာကိုတွေ့ရ မှာ ဖြစ်ပါတယ်။ အဲဒါဟာဘာကိုဆိုလိုတာလဲဆိုရင် Security controls တစ်ခုခု firewall ကိုအသုံးပြုထားတယ်လို့သတ်မှတ်လို့ရပါတယ်။ ဒီအပိုင်းမှာဆိုရင် ကျွန်ုတ် scan လုပ်ပြုသွားတာက target ကို domain ကိုအသုံးပြုပြီးတော့ စစ်ပြုသွားတာဖြစ်ပါတယ်။ အခု ip address ကိုအသုံးပြုပြီး scan လုပ်တာကို ဆက်ကြည့်ရအောင်။

```
C:\Users\ >nmap -p 3389 192.168.99.52
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-24 20:18 Myanmar Standard Time
Nmap scan report for DESKTOP-EQDBNRL.lan (192.168.99.52)
Host is up (0.0010s latency).

PORT      STATE SERVICE
3389/tcp  closed ms-wbt-server
3389/tcp  closed ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
```

ပုံမှာဆိုရင် target နေရာမှာ ကျွန်တော် laptop ရဲ့ ip address ကိုထည့်သွင်းပြီး port 3389 ရဲ့ status ကိုစစ်ကြည့်တဲ့အခါ closed ဆိုပြီးဖြနေတာကိုတွေ့ရမှာ ဖြစ်ပါတယ်။ ဒါဆိုရင် port 3389 က closed ဖြစ်နေတယ် လို့ သတ်မှတ်လို့ရပါတယ်။ အခုကျွန်တော်စမ်းပြုပေးသွားတာကတော့ single port scan ပဲဖြစ်ပါတယ်။ Multiple port scan မှာဆိုရင် range, common port, all port ဆိုပြီးတော့ရှိပါသေးတယ်။ နမူနာအနေနဲ့ port range scan လုပ်ပြုပါမယ်။

```
C:\Users\      >nmap -p 80-150 192.168.0.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-08 11:19 Myanmar Standard Time
Nmap scan report for 192.168.0.1
Host is up (0.0019s latency).
Not shown: 70 closed ports
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 

Nmap done: 1 IP address (1 host up) scanned in 8.49 seconds
```

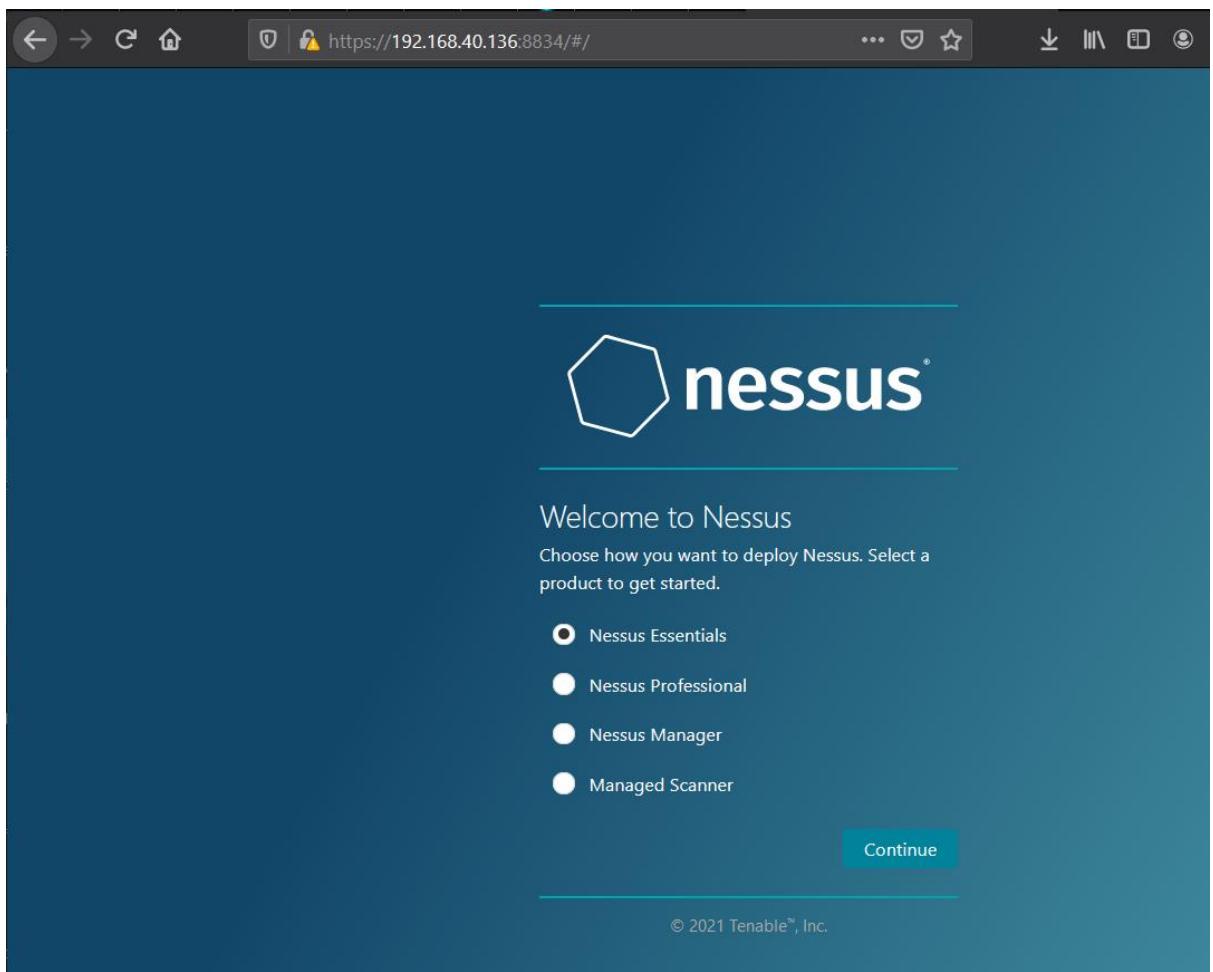
အခုကျွန်တော်စမ်းပြုသွားတာကတော့ Nmap ကို cli အနေနဲ့ စမ်းပြု သွားတာ ဖြစ်ပါတယ်။ GUI နဲ့စမ်းမယ်ဆိုရင် Windows ရဲ့ search zenmap လို့ရှိက်လိုက်ပါ။ ဒါဆိုရင် GUI version ကိုတွေ့ရမှာဖြစ်ပါတယ်။ ဒါကိုတော့ စာဖတ်သူတွေ ကိုယ်တိုင်ပဲစမ်းကြည့်ပါ။ အခုကျွန်တော်တို့ Vulnerability scanning ကိုဆက်လေ့လာကြည့်ရအောင်။ Vulnerability scanning tools ကို download ဆွဲဖို့အတွက်

<https://www.tenable.com/downloads/nessus?loginAttempted=true>

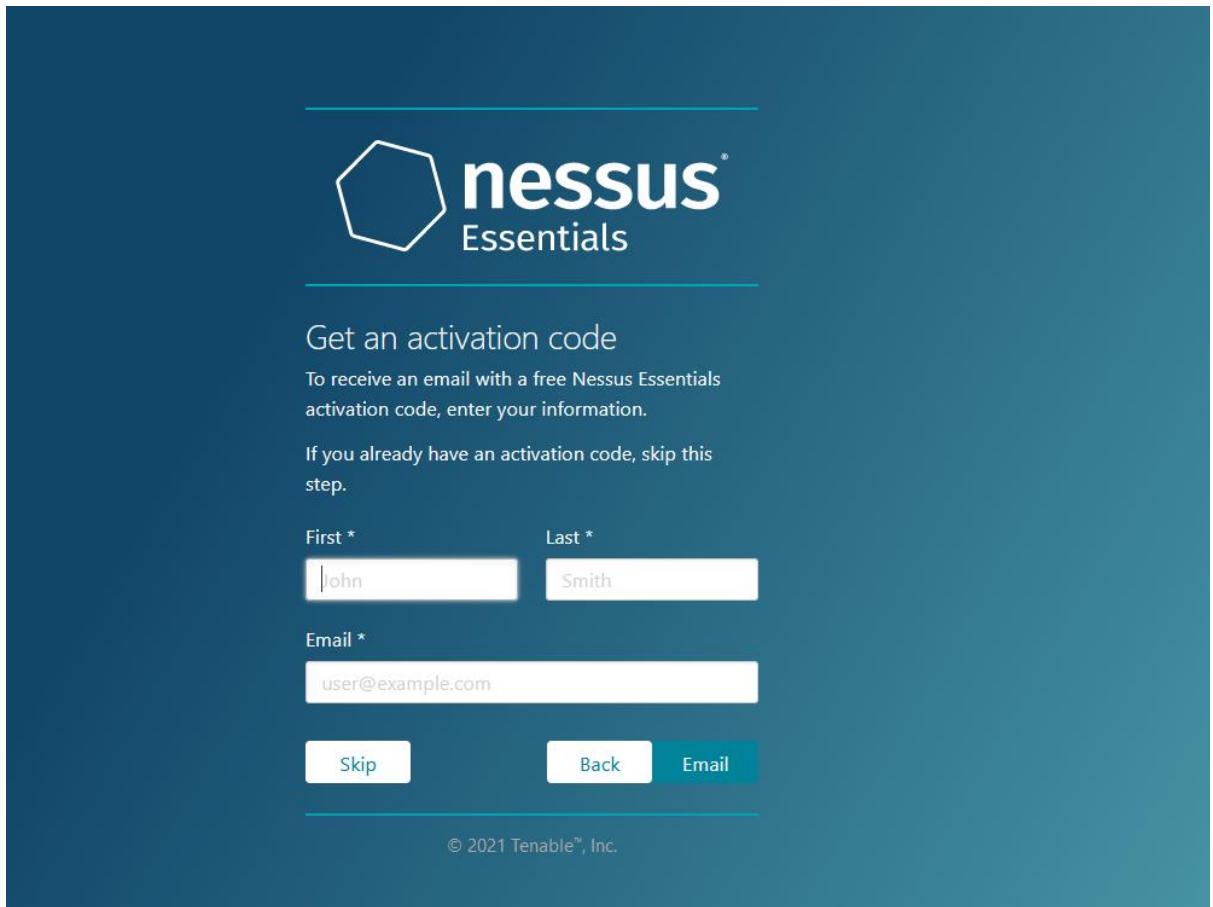
ကိုသွားလိုက်ပါ။ ပြီးရင်အသုံးပြုမယ့် platform အတွက်ကို download လုပ်ပေးရပါမယ် ကျွန်တော်ကတော့ Windows သုံးတာဖြစ်တဲ့အတွက် .msi ဆို download ဆွဲပါမယ်။ ဒီနေရာမှာသတိထားရမှာက စာဖတ်သူတို့ရဲ့ Windows က 32 bit ဆိုရင် Win32.msi နဲ့ဆုံးတာကို download လုပ်ရမှာဖြစ်ပြီး 64 bit ဆိုရင် တော့ x64.msi နဲ့ဆုံးတာကို download လုပ်ရမှာဖြစ်ပါတယ်။ တစ်ကယ်လို့ စာဖတ်သူတို့က ဘယ် architect ကိုအသုံးပြုလဲဆိုတာမသိရင် run box ကနေ msinfo32 ဆိုပြီးရှိက်လိုက်ပါ။ System Type မှာဖော်ပြပေးထားမှာဖြစ်ပါတယ်။

System Manufacturer	Dell Inc.
System Model	Vostro 3578
<u>System Type</u>	x64-based PC
System SKU	0844

အခု Nessus ကို download ဆွဲပြီး install လုပ်ပါမယ်။ Nessus ကို install လုပ်ပြီးသွားတဲ့အခါ browser ကနေ <https://ip:8834> ဆိုပြီးရှိက်တဲ့အခါအောက်ကပ္ပါဒ်တိုင်းတွေ့ရမှာဖြစ်ပါတယ်။



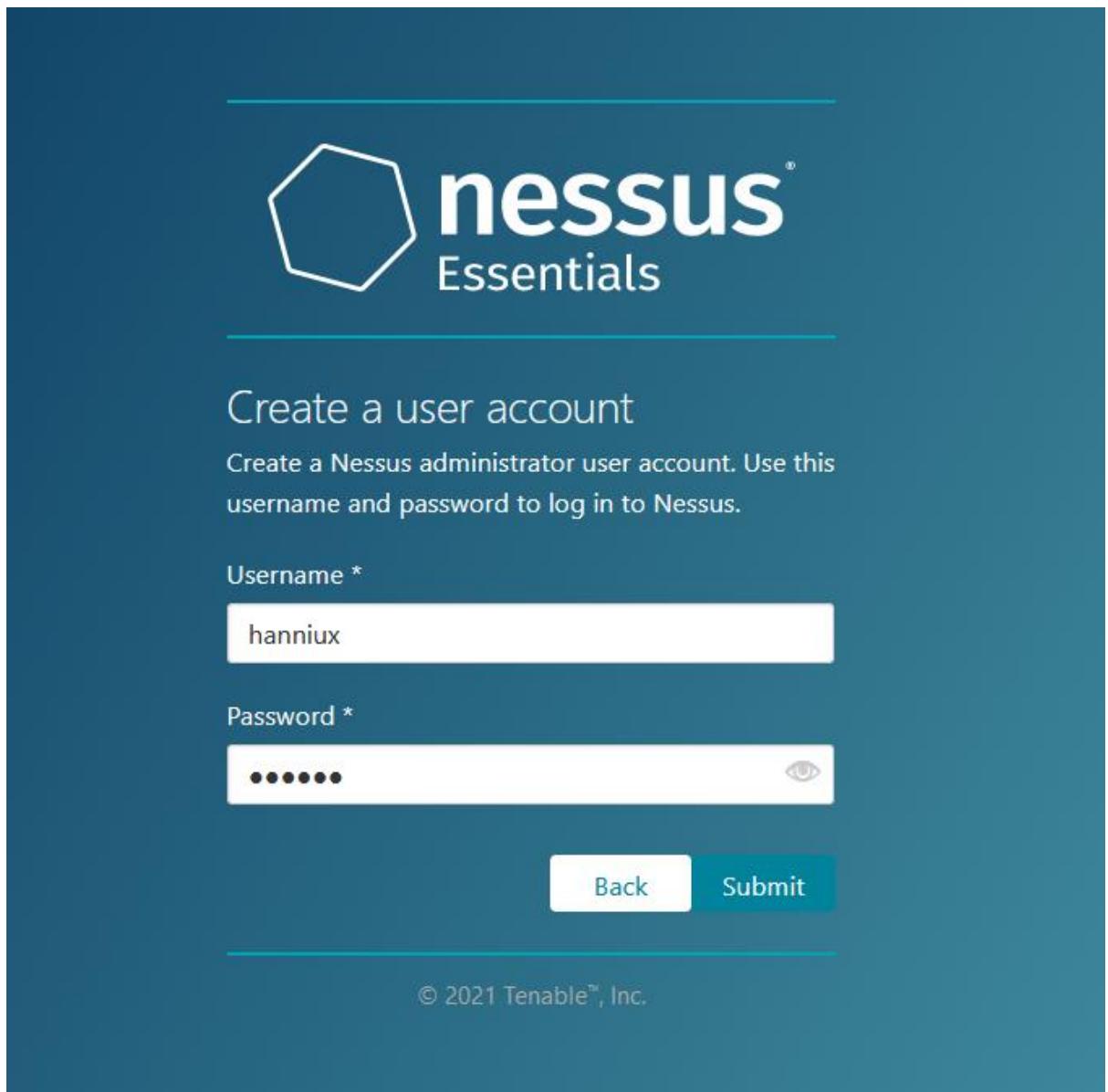
Nessus Essentials ကိုပဲရွေးပြီး Continue ကိုပဲနိုင်ပါမယ်။



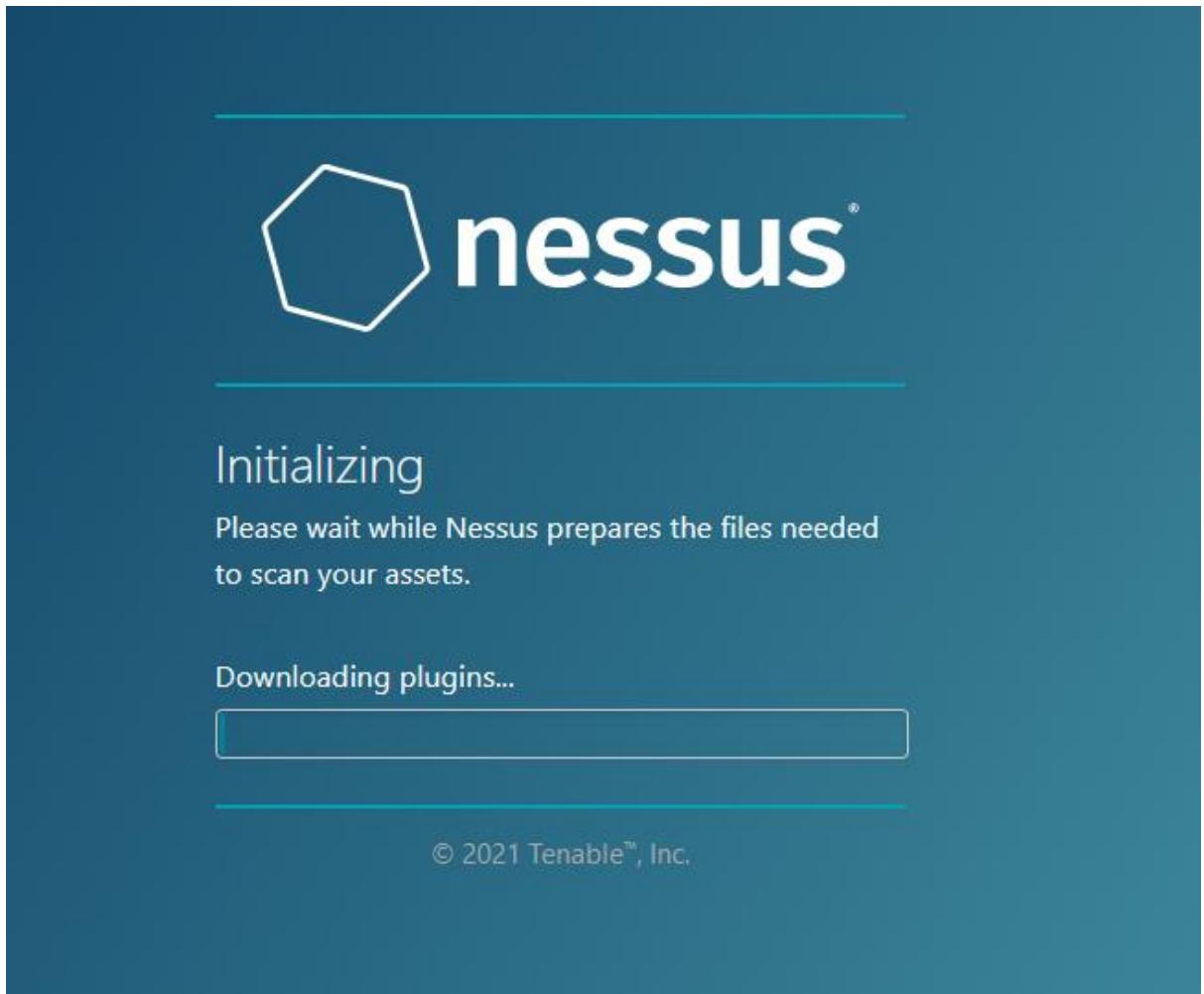
Nessus ကိုကျွန်ုင်တော်တို့က Activation လုပ်ပေးဖို့လိုအပ်ပါတယ်။ အဲဒါကြောင့် ပုံမှာပြထားတဲ့ information တွေထည့်ပြီး Email ဆိုတဲ့ button ကိုသွားပါမယ်။ အဲအခါ Activation code ထည့်တဲ့နေရာကိုရောက်မှာဖြစ်ပါတယ်။ Activation code ကိုကျွန်ုင်တော်တို့ ထည့်ထားတဲ့ mail ကနေရမှာဖြစ်ပါတယ်။



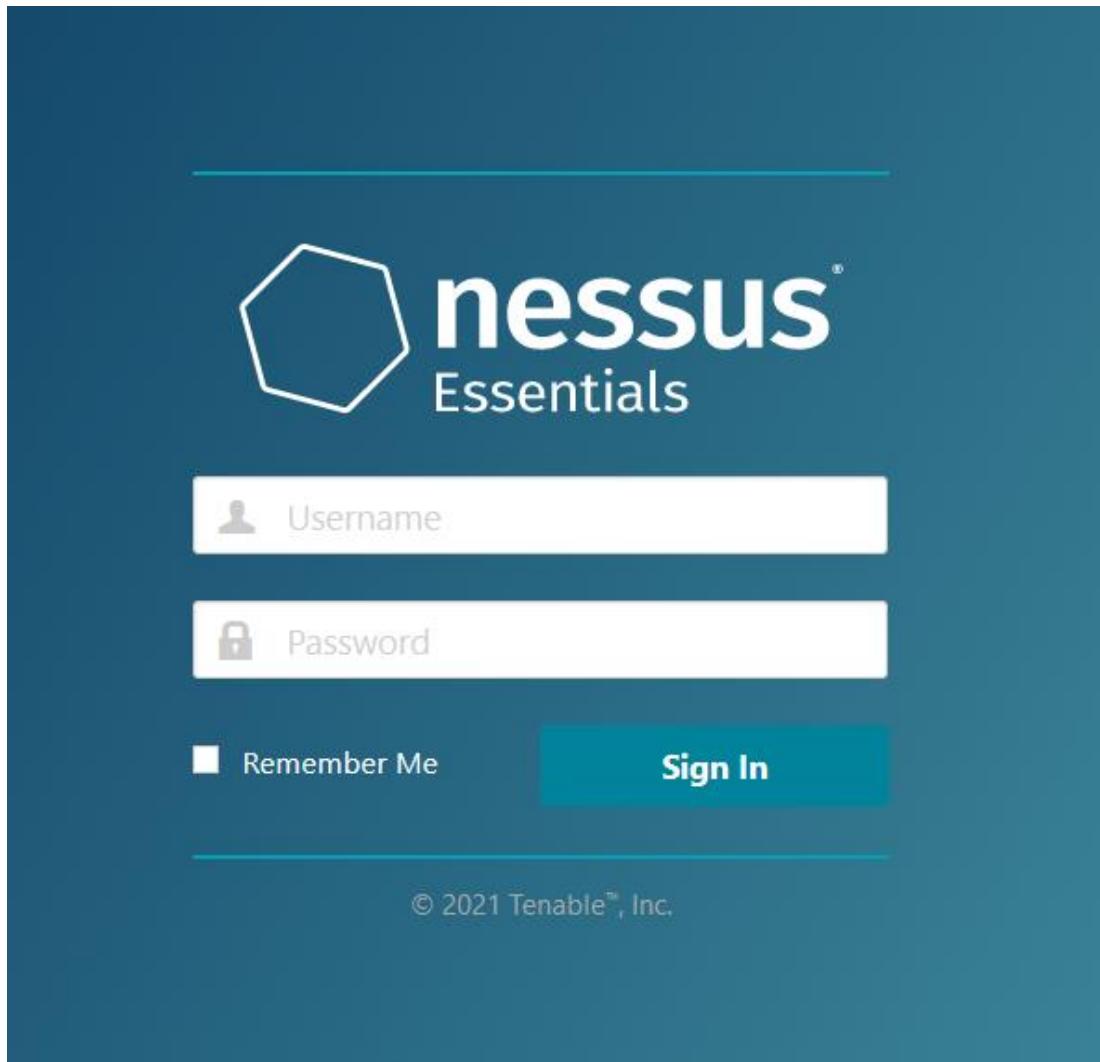
Activation code ထည့်ပြုးရင်တော့ Continue ကိုနိပါမယ်။ ဒါဆိုရင်တော့ Username နဲ့ Password ကို create လုပ်ပေးရမယ့်အပိုင်းကိုရောက်မှာဖြစ်ပါတယ်။



ပြီးရင်တော့ Submit ကိုနှင့်လိုက်ပါ။ Plugin တွေကို download ဆဲတဲ့အဆင့်ကို  
ရောက်ပြီဖြစ်ပါတယ်။

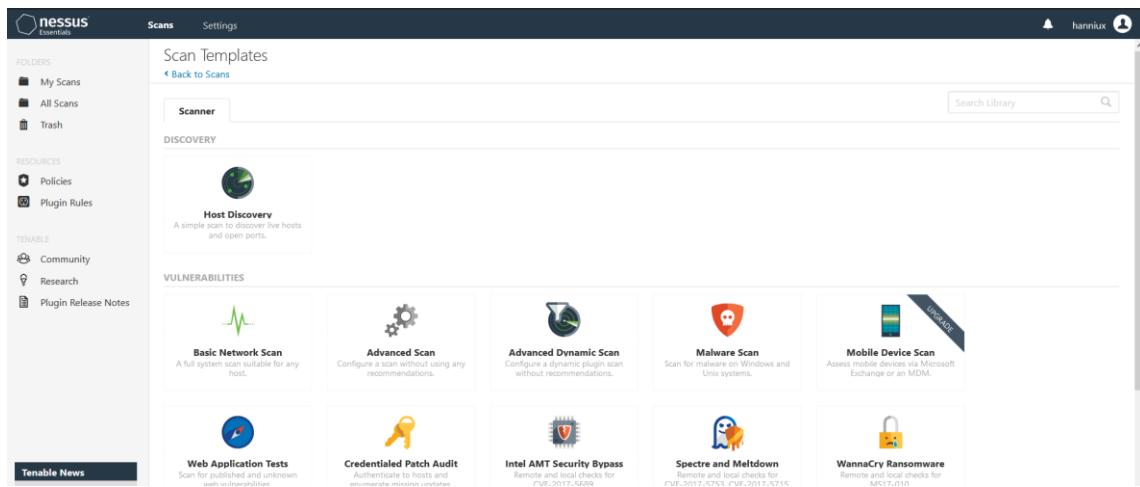


ဒီအဆင့်ပြီးသွားရင်တော့ အောက်ကပုံအတိုင်း nessus login ဝင်တဲ့ နေရာကို  
ရောက်ပြီဖြစ်ပါတယ်။



အပေါကပုံအတိုင်းဖြစ်သွားပြီဆိုရင်တော့ ကျွန်တော်တို့ခုနကသတ်မှတ်ထားတဲ့ username နဲ့ password ကိုအသုံးပြုပြီး Sign In လုပ်လိုက်ရင် Nessus ထဲကို ရောက်ပြုဖြစ်ပါတယ်။

ဒါဆိုရင် ကျွန်တော်တို့ Vulnerability Scan လုပ်ဆောင်လို့ရပြုဖြစ်ပါတယ်။ New Scan ဆိုတဲ့ button ကိုနှိပ်ပါမယ်။ အဲမှာ Scan Templates တွေကို တွေ့ရမှာဖြစ်ပါတယ်။



ကျွန်တော်က Basic Network Scan ဆိုတဲ့ templates ကိုရွေးပါမယ်။  
ပြီးရင်တော့ အောက်ကပုအတိုင်း information တွေကိုဖြည့်သွင်းရပါမယ်။  
Target နေရာမှာ ကျွန်တော်က ကျွန်တော်စက်ကိုပဲ scan လုပ်မှာဖြစ်တဲ့အတွက်  
localhost လို့ထည့်ပါတယ်။ ပြီးရင်တော့ Save button ကိုနှိပ်ပါမယ်။

New Scan / Basic Network Scan  
Back to Scan Templates

**Settings**   **Credentials**   **Plugins**

**BASIC**

- General
- Schedule
- Notifications

**DISCOVERY**

**ASSESSMENT**

**REPORT**

**ADVANCED**

Name: Testing  
Description:  
Folder: My Scans  
Targets: localhost  
Upload Targets   Add File

Save   Cancel

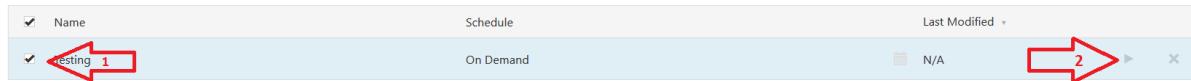
Save လုပ်ပြီးရင်တော့ အောက်ကပုအတိုင်းတွေရမှာဖြစ်ပါတယ်။

My Scans

Import   New Folder   + New Scan

Name	Schedule	Last Modified
Testing	On Demand	N/A

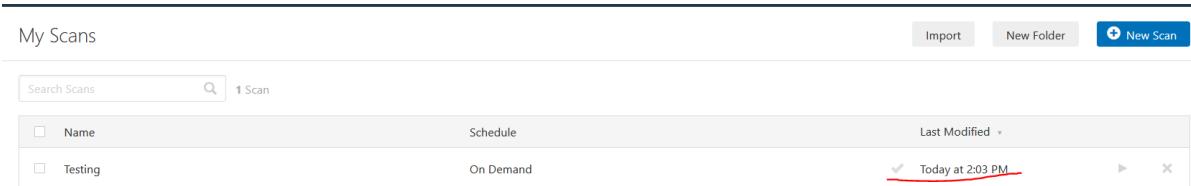
အခု scan လုပ်မှာဖြစ်တဲ့အတွက် Testing ဆိုတဲ့ scan name ဘေးက box လေးကို အမှန်ခြစ်ပြီး Launch ဆိုတဲ့ button ကိုနှိပ်ပါမယ်။



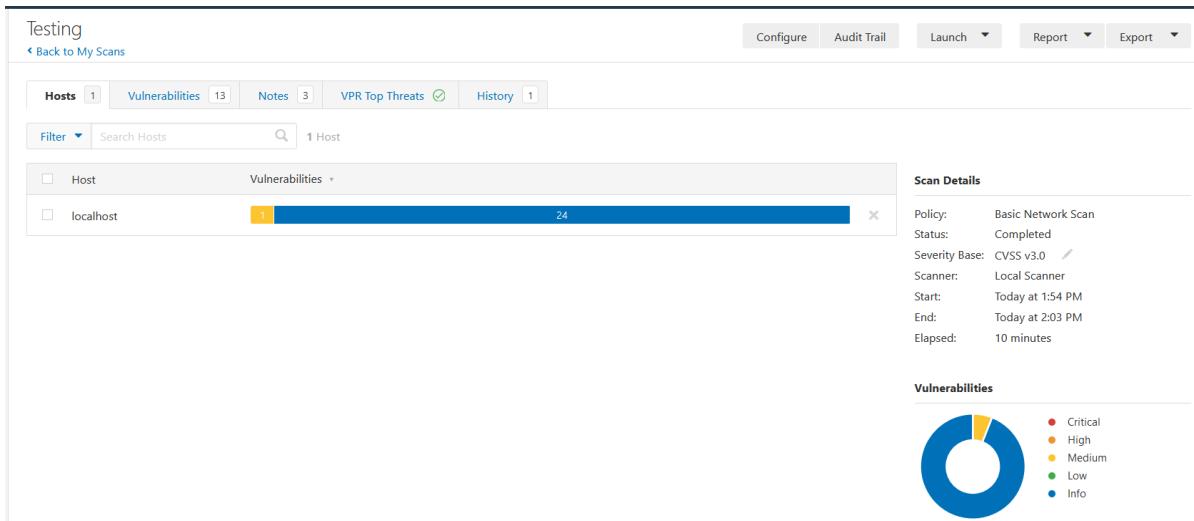
ဒါဆိုရင်တော့အောက်ကပုံအတိုင်း scan လုပ်ဆောင်နေတာကို တွေ့ရမှာဖြစ်ပါတယ်။



Scan လုပ်တာပြီးသွားရင်တော့ အောက်ကပုံအတိုင်းတွေ့ရမှာဖြစ်ပါတယ်။



Scan result ကိုအဲထဲကိုဝင်ကြည့်ပါမယ်။



ပုံထဲမှာဆိုရင် Summary view ကို Hosts tab ထဲမှာဖော်ပြထားပါတယ်။ Vulnerabilities tab ထဲမှာတော့ vulnerability information အပြည့်စုံကိုဖော်ပြထားပါတယ်။

Testing

[Back to My Scans](#)

Hosts 1 | Vulnerabilities 13 | Notes 3 | VPR Top Threats | History 1

Filter | Search Vulnerabilities | 13 Vulnerabilities

Sev	Name	Family	Count	Actions
MEDIUM	SMB Signing not required	Misc.	1	<a href="#">Edit</a> <a href="#">Delete</a>
INFO	DCE Services Enumeration	Windows	9	<a href="#">Edit</a> <a href="#">Delete</a>
INFO	4 SMB (Multiple Issues)	Windows	4	<a href="#">Edit</a> <a href="#">Delete</a>
INFO	Microsoft Windows (Multiple Issues)	Windows	2	<a href="#">Edit</a> <a href="#">Delete</a>
INFO	Authenticated Check : OS Name and Installed Package Enumeration	Settings	1	<a href="#">Edit</a> <a href="#">Delete</a>
INFO	Common Platform Enumeration (CPE)	General	1	<a href="#">Edit</a> <a href="#">Delete</a>
INFO	Device Type	General	1	<a href="#">Edit</a> <a href="#">Delete</a>
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1	<a href="#">Edit</a> <a href="#">Delete</a>
INFO	Local Checks Not Enabled (info)	Settings	1	<a href="#">Edit</a> <a href="#">Delete</a>
INFO	Nessus Scan Information	Settings	1	<a href="#">Edit</a> <a href="#">Delete</a>

**Scan Details**

Policy: Basic Network Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 1:54 PM  
End: Today at 2:03 PM  
Elapsed: 10 minutes

**Vulnerabilities**

Critical: 0, High: 0, Medium: 1, Low: 4, Info: 8

နောက် vulnerabilities တွေရဲ့ status ကို color တွေနဲ့ဖော်ပြထားပါတယ်။  
အနီဆိုရင် Critical , လိမ့်ဆိုရင် High, အဝါဆိုရင် Medium, အစိမ်းဆိုရင် Low, အပြာဆိုရင် တော့ Info ပေါ့။ ကျွန်တော့စက်ကို scan လုပ်တာတော့ အမြင့်ဆုံးက အဝါဖြစ်ပါတယ်။ အဲဒါကို click နိုင်ပြီးဝင်ကြည့်လိုက်ရင် အောက် ကပ္ပါတိုင်း Information အပြည့်စုံကို တွေ့ရမှာဖြစ်ပါတယ်။

Testing / Plugin #57608

[Back to Vulnerabilities](#)

Hosts 1 | Vulnerabilities 13 | Notes 3 | VPR Top Threats | History 1

**MEDIUM** SMB Signing not required

**Description**  
Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

**Solution**  
Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

**See Also**  
<http://www.nessus.org/u?df39b8b3>  
<http://technet.microsoft.com/en-us/library/cc731957.aspx>  
<http://www.nessus.org/u?74b80723>  
<https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>  
<http://www.nessus.org/u?a3cac4ea>

**Output**  
No output recorded.

Port	Hosts
445 / tcp / dfs	localhost

**Plugin Details**

Severity: Medium  
ID: 57608  
Version: 1.19  
Type: remote  
Family: Misc.  
Published: January 19, 2012  
Modified: March 15, 2021

**Risk Information**

Risk Factor: Medium  
**CVSS v3.0 Base Score 5.3**  
CVSS v3.0 Vector: CVSS3.0/AV:N/AC:L/PR:N/I:H/N/S/U/C/N/L/A/N  
CVSS v3.0 Temporal Vector: CVSS3.0/E:U/RL:O/RC:C  
CVSS v3.0 Temporal Score: 4.6  
CVSS v2.0 Base Score: 5.0  
CVSS v2.0 Temporal Score: 3.7  
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N  
CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:O/RC:C

**Vulnerability Information**

CPE: cpe:/o:microsoft:windows cpe:/a:samba:samba

ပုံမှာဆိုရင် Vulnerability နဲ့ပတ်သက်တဲ့ Description ကိုလဲဖော်ပြထားသလို  
Solution ကိုလဲဖော်ပြထားတာတွေ့ရမှာဖြစ်ပါတယ်။ နောက် Risk

Information ကိုလဲ တွေ့ရမှာဖြစ်ပါတယ်။ အဲမှာဆိုရင် CVSS (Common Vulnerability Scoring System) ဆိုတာက vulnerability နဲ့သက်ဆိုင်တဲ့ Score ဖြစ်ပြီး number နဲ့ပြပါတယ်။ အဲဒါကို ကျွန်တော်အောက်မှာ Table နဲ့ဖော်ပြုထားပါတယ်။

Rating	CVSS Score
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

ဒါဆိုရင်စာဖတ်သူတွေအနေနဲ့ Vulnerability scanning နဲ့ပတ်သက်ပြီးနားလည်မယ် လို့ထင်ပါတယ်။ အခုခက်ပြီးတော့ သိထားသင့်တဲ့ CVE အကြောင်းကိုလေ့လာကြည့်ရအောင်။

### What is CVE (Common Vulnerabilities Exposures)

CVE ဆိုတာက Vulnerabilities တွေကို ID တွေသတ်မှတ်တာဖြစ်ပါတယ်။ CVE ကိုသတ်မှတ်တဲ့အခါ vulnerabilities ဖြစ်တဲ့ ခုနှစ် နဲ့ ID number ပါဝင်ပါတယ်။ ဥပမာ CVE-2021-30245 ပေါ့။ Vulnerabilities ဖြစ်နေတဲ့ services တွေ ရဲ့ CVE ID ကို ကြည့်ချင်တယ်ဆိုရင် <https://cve.mitre.org/> မှာသွားရောက်လေ့လာနိုင်ပါတယ်။

## Chapter 7 – Monitoring and Auditing

### Monitoring Methodologies

Network တစ်ခု secure တစ်ခုဖြစ်ဖို့အတွက်ဆိုရင် Applications, Servers, Network Devices, Power Devices စတာတွေကို သေချာစောင့်ကြည့်ဖို့အတွက်လို အပ်ပါတယ်။ Network တွေကိုစောင့်ကြည့်ခြင်းအားဖြင့်ကျန်တော်တို့ရဲ့ infrastructure ကိုပို့ပြီးတော့ security ကောင်းမွန်လာစေပါတယ်။ Network ထဲ မှာသွားလာနေတဲ့ traffic အားလုံးကိုစောင့်ကြည့်ခြင်းအားဖြင့် နေ့စဉ်ပုံမှန် ဖြစ်ပျက် နေတာတွေကိုသိလာနိုင်သလို ဘယ်လို traffic တွေသွားလာနေလဲ ဆိုတာပါ analyze လုပ်နိုင်မှာဖြစ်ပါတယ်။

Monitoring လုပ်တဲ့အခါ manual monitoring နဲ့ automate monitoring ဆိုပြီးနည်းလမ်း (၂) မျိုးရှိပါတယ်။ Manually monitoring လုပ်တဲ့အခါ log files, policies, permissions စတာတွေကိုစနစ်တကျ တွေ့နိုင်မှာဖြစ်ပါတယ်။ ဒါပေမယ့် အဲဒါကို automate မှာလဲလုပ်ဆောင်နိုင်ပါတယ်။ Automate မှာဆိုရင် Antivirus, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) စတာ တွေပါဝင်ပြီး error, malicious attacks, anomalies တို့ကို automatically ဖြေရှင်း ပေးနိုင်ပါတယ်။ Automate monitoring မှာဆိုရင် signature-based, anomaly-based, behavior-based ဆိုပြီး အမျိုးစား (၃) မျိုးရှိပါတယ်။

### Signature-Based Monitoring

Signature-based monitoring မှာဆိုရင် Network traffic ထဲမှာသွား နေတဲ့ frames နဲ့ packets တွေကို attack pattern နဲ့ပုံမှန် စစ်ဆေးပါ တယ်။ အဲ attack pattern ဆိုတာကို signatures လို့ခေါ်ပါတယ်။ Signatures တွေကို security controls တွေရဲ့ database ထဲမှာသိမ်းထားတာဖြစ်ပြီး network security ပိုကောင်း လာဖို့အတွက် ပုံမှန် update လုပ်ပေးသင့်ပါတယ်။ ဒါနေ့ ခေတ်မှာတော့ attack တွေက သူတို့ရဲ့ကိုယ်ပိုင် signature တွေနဲ့ ဖြစ်သွားပါပြီ။

ဒါပေမယ့် အထူးသတ်မှတ်ထားတဲ့ signature တွေနဲ့ကိုက်ညီမှ ရှိတဲ့ attack တွေဆိုရင်တော့ detect သိမှာဖြစ်ပါတယ်။ Malicious activity က မတူညီတဲ့ signature တွေကိုသုံးထားတာကြောင့် အနည်းငယ် တော့လဲတာတွေ ဖြစ်ကောင်းဖြစ်နိုင်ပါတယ်။ Signature-based monitoring မှာ vulnerable ဆိုရင် false negatives နဲ့ပြတာကြောင့်တစ်ခါတစ်လေ attack ဒါမှမဟုတ် error ဆိုရင် detect မသိတာမျိုးတွေဖြစ်နိုင်ပါတယ်။ အဲလိုပြုသနာတွေကို ဖြေရှင်းဖို့အတွက်ဆိုရင် signature-based system ကိုနောက်ဆုံး version ထိရောက်အောင် update လုပ်ဆောင်သင့်ပါတယ်။

## Anomaly-Based Monitoring

Anomaly-based monitoring ဆိုတာကပုံမှန်သွားလာနေတဲ့ network traffic ကိုစစ်ဆေးပြီးသတ်မှတ်ထားတာဖြစ်ပြီး performance ကိုအခြေခံထားတာဖြစ်ပါတယ်။ အဲလိုစစ်ဆေးတဲ့အခါ Network နဲ့ Servers တွေကပုံမှန် working hours တွေမှာ work load တွေကပျမ်းမျှဖြစ်နေဖို့လိုအပ်ပါတယ်။ ဒီ monitoring method က လက်ရှိ network ထဲက activity တွေကိုနှိုင်းယှဉ်ပြီး baseline တစ်ခုကို create လုပ်ပြီးစောင့်ကြည့်နေတာဖြစ်ပါတယ်။ တစ်ကယ်လိုပုံမှန်မဟုတ် traffic တစ်ခုက network ထဲကိုဝင်လာခဲ့မယ်ဆိုရင် systems က detect သိမှာဖြစ်ပြီး administrator ကို alert ပို့မှာဖြစ်ပါတယ်။ ဒါကြောင့် ဒီ monitoring method က baseline ပေါ်အခြေခံထားတာဖြစ်ပါတယ်။ တစ်ကယ်လို့ ကျွန်တော်တို့က baseline ကိုမြှင့်လိုက်မယ်ဆိုရင် false indicators တွေဖြစ်တဲ့ false positives တွေပါဝင်လာနိုင်ပါတယ်။ ပုံမှာ false positives ကို system ကသိပြီဆိုရင် ဒါဟာ attack ဒါမှမဟုတ် error တစ်ခုခု ကြောင့်ဆိုတာ system ကတန်းသိပါတယ်။ တစ်ကယ်လို့ security administrator က false indicator နဲ့သက်ဆိုင်တဲ့ alert message တွေအများကြီးရနေခဲ့ပြီဆိုရင်တော့ IDS/IPS ပြန်ပြီး reconfigured လုပ်တာမျိုးတွေ နောက် baselines တွေကိုပြန်စစ်ဆေးတာမျိုးတွေလုပ်ဆောင်သင့်ပါတယ်။

## Behavior-Based Monitoring

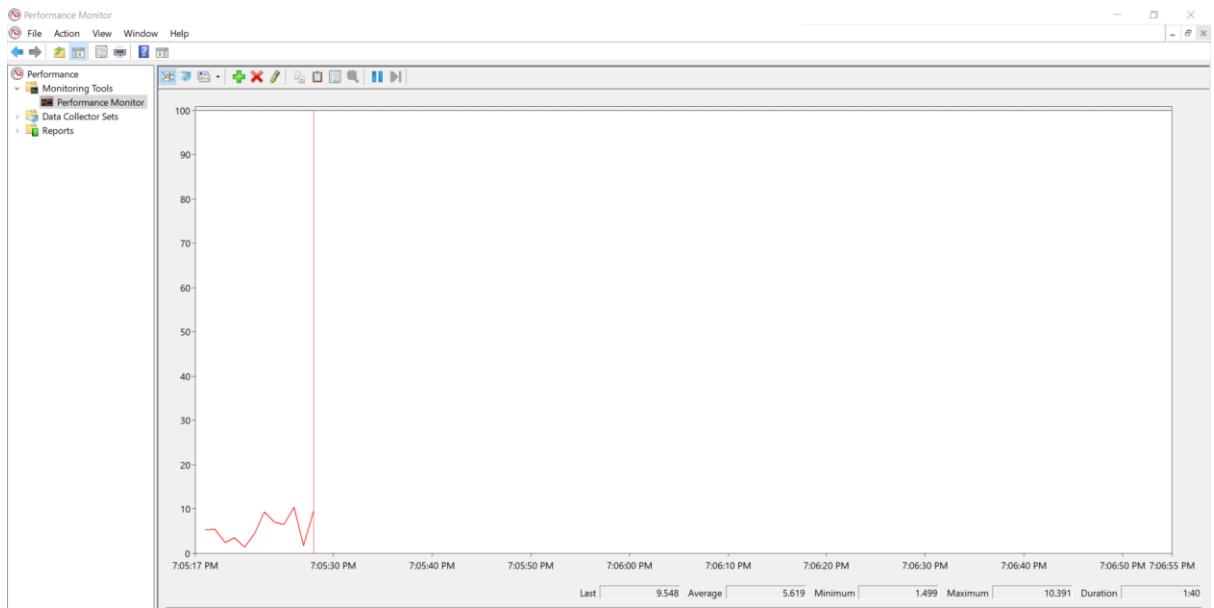
Behavior-based monitoring ဆိုတာက application, executables တွေရဲ့ Operating System ပေါ်မှာလက်ရှိလုပ်ဆောင်နေတဲ့ လုပ်ဆောင်မှုတွေ ကိုစောင့်ကြည့်တာဖြစ်ပါတယ်။ တစ်ကယ်လို့ application တွေရဲ့လုပ်ဆောင်မှု တွေကနောက်ပိုင်းမှာပုံမှန်မဟုတ်တော့ဘူးဆိုရင်တော့ monitoring system က အဲလုပ်ဆောင်မှုတွေကိုရပ်တန်လိုက်တာဖြစ်ပါတယ်။ ဒါဟာ behavior-based ရဲ့အားသာချက်ဖြစ်ပါတယ် အဲလိုလုပ်ဆောင်ဖို့အတွက်ဆိုရင်လဲ update လုပ်ပေးဖို့မလိုပါဘူး။ ဒါပေမယ့် applications အမျိုးစားတွေကလဲအများကြီး နောက် အဲ applications နဲ့ပတ်သက်နေတာတွေကလဲအများကြီးဆိုရင် အထူး ဂရုစိုက်ပြီး configure လုပ်ပေးဖို့လိုအပ်ပါတယ်။ အဲလိုမှုမဟုတ်ရင် false positives အနေနဲ့ alarms message ပို့လာနိုင်ပါတယ်။

## Using Tools to Monitor Systems and Networks

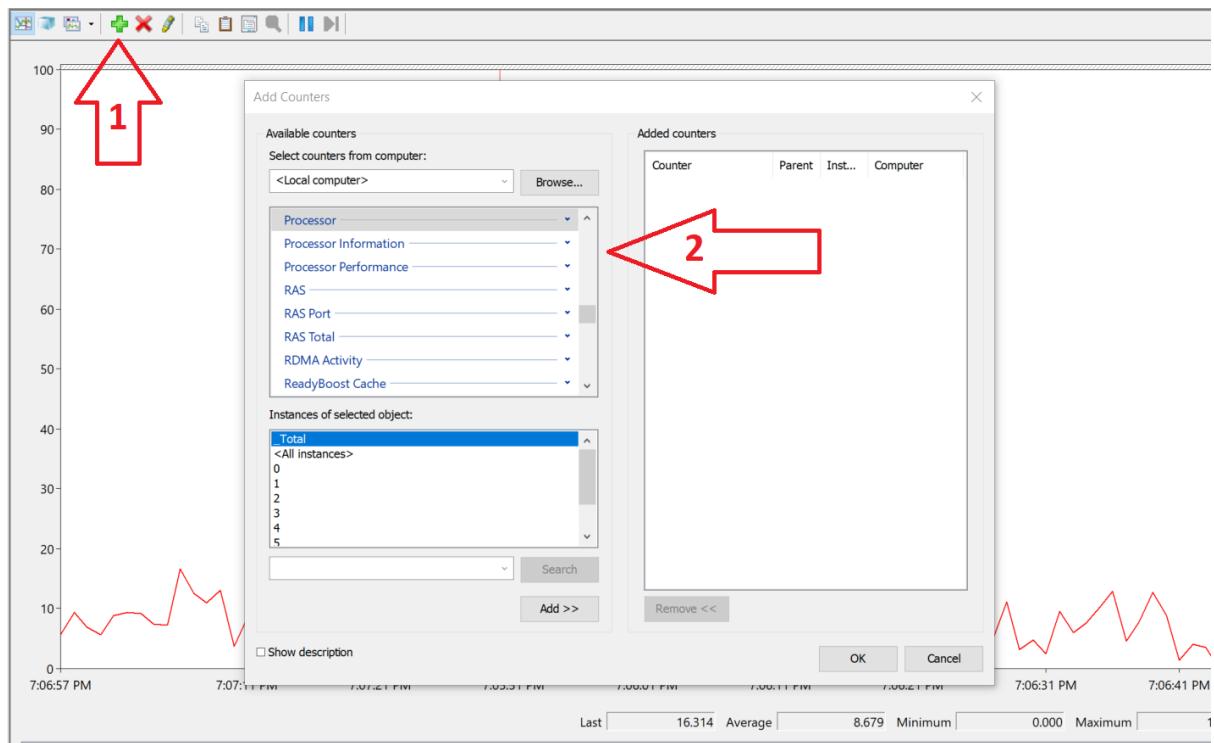
ဒီအပိုင်းမှာတော့ tools တွေကိုအသုံးပြုပြီး Systems နဲ့ Networks တွေကို ဘယ်လို monitoring လုပ်မလဲဆိုတာကိုလေ့လာရမှာဖြစ်ပါတယ်။ အဲလို monitoring လုပ်တဲ့အခါ Performance, Network Traffic စတာတွေ အတွက်ကို GUI , CLI software တွေကိုအသုံးပြုပြီး monitoring လုပ်ဆောင် ကြည့်ကြပါမယ်။

## Performance Monitoring

Performance monitoring ဆိုတာက systems ထဲမှာရှိနေတဲ့ Memory, CPU, HDD စတာတွေရဲ့ status တွေကိုစောင့်ကြည့်တာဖြစ်ပါတယ်။ အဲလို စောင့်ကြည့်မှသာလျှင် systems failure ကိုကာကွယ်နိုင်မှာဖြစ်ပါတယ်။ Performance monitoring အတွက်ဆိုရင် Windows မှာ default ပါဝင်တဲ့ Performance Monitor ကိုအသုံးပြုနိုင်ပါတယ်။



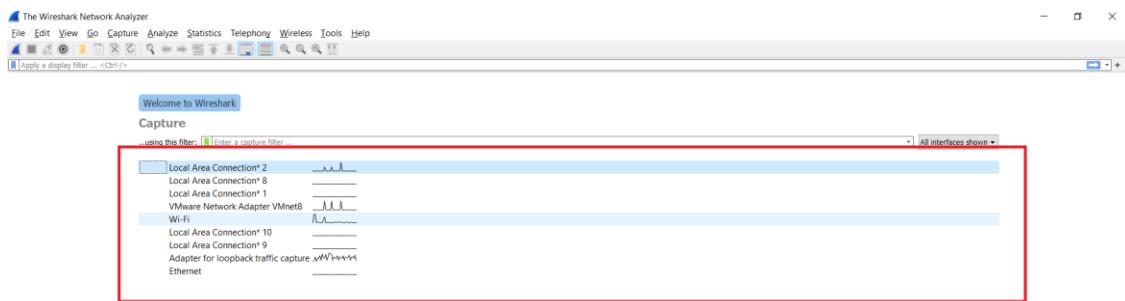
ပုံမှာဆိုရင်တော့ default အတိုင်း CPU ကို monitoring လုပ်တာ  
ဖြစ်ပါတယ်။ Customize လုပ်ချင်တယ်ဆိုရင်တော့ + လေးကို နှိပ်ပြီး  
monitoring လုပ်ချင် တာကိုရွေးချယ်လိုပါတယ်။



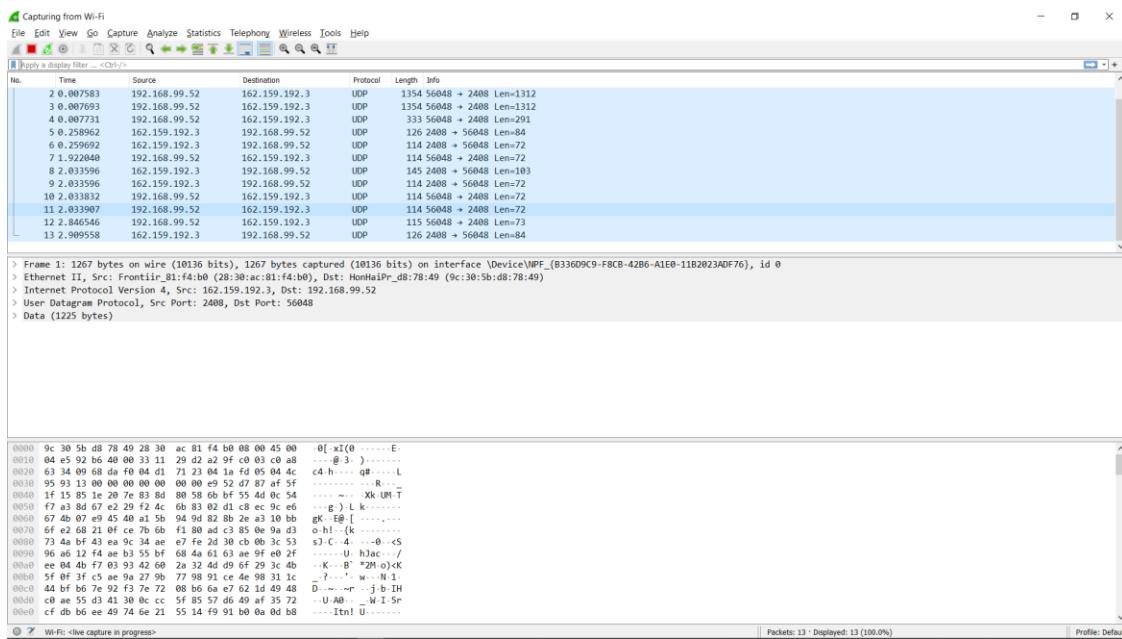
ပုံမှာပြထားတဲ့အတိုင်းရွေးပြီးရင် Ok button ကိုနှိပ်လိုက်ပါ။ စာဖတ်သူ  
monitor လုပ်ချင်တာကိုရွေးပြီး monitoring လုပ်ဆောင်နိုင်ပြီဖြစ်ပါ  
တယ်။

## Protocol Analyzers

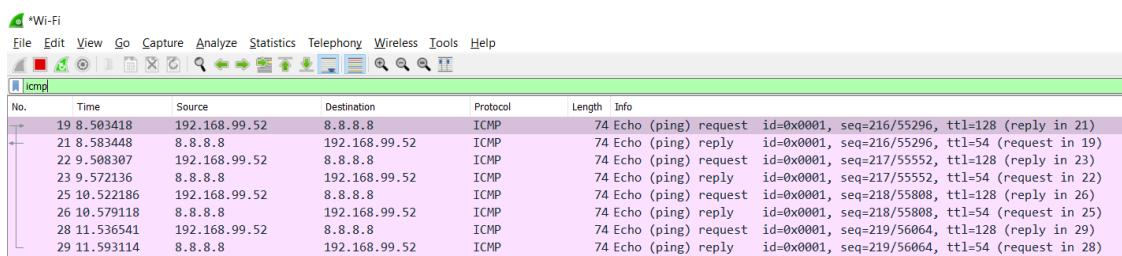
Protocol analyzers ဆိုတာ tools တစ်မျိုးဖြစ်ပြီး IT administrators နဲ့ Security Teams တွေက network traffic တွေကို capture လုပ်တဲ့အခါအသုံး ပြုပါတယ်။ Capture လုပ်ပြီးရလာတဲ့ data တွေကို analysis လုပ်တဲ့အခါ network traffic ထဲက problems တွေနဲ့ potential malicious activity တွေကို သိနိုင်မှာဖြစ်ပါ တယ်။ အဲ traffic data တွေက real time မှာဆိုရင် technician တွေ troubleshooting လုပ်ဖို့အတွက်နဲ့ monitored ဆိုရင် network ထဲမှာ ရှိနေတဲ့ threats တွေကိုရှာဖွေဖို့ ဒါမှုမဟုတ် network breach ဖြစ်တဲ့အခါ forensic analysis လုပ်ဆောင်ဖို့ အတွက် အသုံးပြုတာဖြစ်ပါတယ်။ Protocol analyzers ထဲမှာဆိုရင် Wireshark က free လဲဖြစ်သလို အသုံးလဲပိုများပါတယ်။ အခုက္ခန်းတော်တို့ Wireshark ကို download လုပ်ပြီးစက်မှာ install လုပ်ပါ မယ်။ Wireshark ကို download လုပ်ဖို့အတွက် <https://www.wireshark.org/> ကိုသွားလိုက်ပါ။ ပြီးရင် Download ဆိုတဲ့ icon ကိုနှိပ်လိုက်ပါ။ Wireshark ကို download လုပ်ပြီးသွားရင် install လုပ်ပါ။ Wireshark ကို install လုပ်ပြီးရင် တော့ run လိုက်ပါအောက်ကပုံအတိုင်းတွေ့ရမှာဖြစ်ပါတယ်။



ပုံမှာဆိုရင် အနီရောင်နဲ့ဘောင်ခတ်ပြထားတာက sniffing လုပ်မယ့် interface ကိုရွေးပေးရမယ့်နေရာဖြစ်ပါတယ်။ ဒီမှာတော့ ကျွန်းတော်က Wi-Fi ကိုပဲရွေးလိုက်ပါမယ်။



Wi-Fi ကိုရွေးပြီးတဲ့အခါ အပေါ်ကပုံအတိုင်း packets တွေကိုတွေ့မြင်ရမှာဖြစ်ပါတယ်။ အပေါ်ဆုံး Apply a display filter ဆိုတဲ့နေရာက filter လုပ်ဖို့အတွက်ဖြစ်ပါတယ်။ နမူနာအနေနဲ့ အဲနေရာမှာ icmp ဆိုပြီးထည့်ကြည့်ပါမယ်။ ပြီးရင် ကျွန်ုတ်တို့ laptop ကနေ 8.8.8.8 ကို ping လုပ်ပါမယ်။ ဒါဆိုရင် Wireshark မှာအောက်ကပုံအတိုင်း icmp traffic ကိုတွေ့ရမှာဖြစ်ပါတယ်။



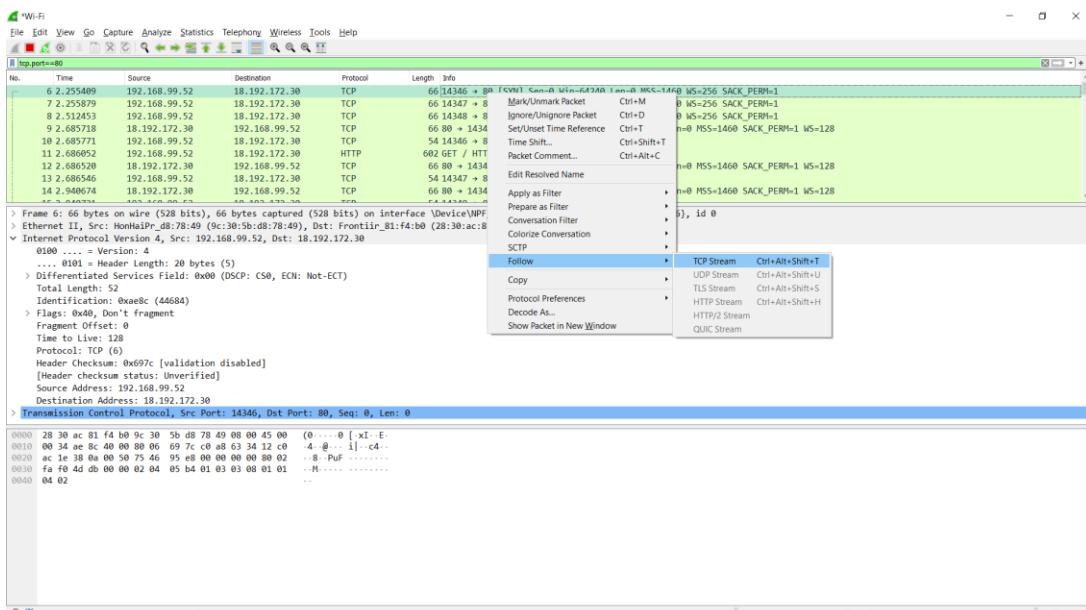
ဒါကတော့ နမူနာအနေနဲ့ ICMP protocol ကိုအသုံးပြုပြီးစမ်းပြထားတာဖြစ်ပါတယ်။ အခုကျွန်ုတ်တို့ Port ကိုအသုံးပြုပြီးတော့ analyze လုပ်ကြည့်ပါမယ်။ Filter နေရာမှာ tcp.port==80ဆိုပြီးထည့်ကြည့်ပါမယ်။ ဒါကဘာကို ရည်ညွှန်းလဲဆိုရင် TCP Port က 80 ဖြစ်တဲ့ packet တွေကို filter လုပ်တာဖြစ်ပါတယ်။ အဲလို filter လုပ်ပြီးသွားရင် browser ကနေ [www.vulnweb.com](http://www.vulnweb.com) ဆိုပြီး ရိုက်လိုက်ပါ။ ဒါဆိုရင်အောက်မှာဖော်ပြထားတဲ့ ပုံအတိုင်း traffic တွေကိုတွေ့ရမှာဖြစ်ပါတယ်။

tcp.port==80						
No.	Time	Source	Destination	Protocol	Length	Info
6	2.255409	192.168.99.52	18.192.172.30	TCP	66	14346 → 88 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
7	2.255879	192.168.99.52	18.192.172.30	TCP	66	14347 → 88 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
8	2.512453	192.168.99.52	18.192.172.30	TCP	66	14348 → 88 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
9	2.685718	18.192.172.30	192.168.99.52	TCP	66	80 → 14346 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=1460 SACK_PERM=1 WS=128
10	2.685771	192.168.99.52	18.192.172.30	TCP	54	14346 → 88 [ACK] Seq=1 Ack=1 Win=131328 Len=0
11	2.686052	192.168.99.52	18.192.172.30	HTTP	602	GET / HTTP/1.1
12	2.686520	18.192.172.30	192.168.99.52	TCP	66	80 → 14347 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=1460 SACK_PERM=1 WS=128
13	2.686546	192.168.99.52	18.192.172.30	TCP	54	14347 → 88 [ACK] Seq=1 Ack=1 Win=131328 Len=0
14	2.940674	18.192.172.30	192.168.99.52	TCP	66	80 → 14348 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=1460 SACK_PERM=1 WS=128
15	2.940724	192.168.99.52	18.192.172.30	TCP	54	14348 → 88 [ACK] Seq=1 Ack=1 Win=131328 Len=0

> Frame 6: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{B336D9C9-F8CB-4286-A1E0-11B2023ADF76}, id 0  
> Ethernet II, Src: HonkaiP\_08:78:49 (0c:30:5b:08:78:49), Dst: Frontiir\_81:f4:b0 (28:30:ac:81:f4:b0)  
> Internet Protocol Version 4, Src: 192.168.99.52, Dst: 18.192.172.30  
0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
> Differentiated Services Field: 0x00 (DSSCP: CS0, ECN: Not-ECT)  
Total Length: 52  
Identification: 0xae8c (44684)  
> Flags: 0x40, Don't fragment  
Fragment Offset: 0  
Time to Live: 128  
Protocol: TCP (6)  
Header Checksum: 0x697c [validation disabled]  
[Header checksum status: Unverified]  
Source Address: 192.168.99.52  
Destination Address: 18.192.172.30  
> Transmission Control Protocol, Src Port: 14346, Dst Port: 80, Seq: 0, Len: 0

0000 28 30 ac 81 f4 b0 9c 30 5b d8 78 49 08 00 45 00 (0.....0 [x1]-E-
0010 00 34 ae 8c 40 00 80 06 69 7c c0 a8 63 34 12 c0 4-@... 1]-c4-
0020 ac 1e 38 0a 00 50 75 46 95 e8 00 00 00 00 00 02 .8-PuF .....
0030 fa f0 4d db 00 00 02 04 05 b4 01 03 03 08 01 01 .M.....
0040 04 02 .....

ပုံမှာဆိုရင် အဓိကစာဖတ်သူတွေမှတ်ထားရမှာက Source, Destination, Protocol, Length, Info တို့ပဲဖြစ်ပါတယ်။ Source မှာဆိုရင် No 6 အကြောင်းက request လုပ်တဲ့ကျွန်တော်တို့ စက်ရဲ့ IP address ဖြစ်ပြီး Destination မှာ တော့ response ပြန်တဲ့ Website ရဲ့ IP address ဖြစ်ပါတယ်။ အဲ No 6 အကြောင်းကို ကျွန်တော်တို့ right click နိုင်ပါမယ်။ ပြီးရင် Follow ထဲက TCP Stream ကိုနှိပ်လိုက်ပါ။



အပေါ်ကပုံအတိုင်းနှိပ်ပြီးတဲ့အခါ အောက်ကအတိုင်း http header information တွေကိုတွေ့ရမှာဖြစ်ပါတယ်။

```

GET / HTTP/1.1
Host: www.vulnweb.com
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 Edg/90.0.818.66
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
If-None-Match: W/"5f1fedf1-fb2"
If-Modified-Since: Tue, 28 Jul 2020 09:20:49 GMT

HTTP/1.1 304 Not Modified
Server: nginx/1.19.0
Date: Wed, 26 May 2021 15:02:04 GMT
Last-Modified: Tue, 28 Jul 2020 09:20:49 GMT
Connection: keep-alive
ETag: "5f1fedf1-fb2"

```

အပေါ်ကပုံမှာဆိုရင် response ပြန်တဲ့ server မှာအသုံးပြထားတဲ့ http method, Host, Server, Modified Date စတဲ့ information တွေကိုတွေ့မြင်ရမှာဖြစ်ပါတယ်။ နောက် protocol name တွေနဲ့လဲ filter လုပ်လိုပါတယ်။ ဥပမာအနေနဲ့ ကျွန်ုတ်၏ http ကို filter လုပ်ပြပါမယ်။

http						
No.	Time	Source	Destination	Protocol	Length	Info
18	3.614466	192.168.188.215	18.192.172.30	HTTP	602	GET / HTTP/1.1
> Frame 18: 602 bytes on wire (4816 bits), 602 bytes captured (4816 bits) on interface \Device\NPF_{ACCE0960-821B-4E5A-8627-6FBEE65D4655}, id 0 > Ethernet II, Src: Dell_38:ab:d2 (58:8a:5a:38:ab:d2), Dst: Sonicwall_0f:81:27 (18:b1:69:0f:81:27) > Internet Protocol Version 4, Src: 192.168.188.215, Dst: 18.192.172.30 > Transmission Control Protocol, Src Port: 2238, Dst Port: 80, Seq: 1, Ack: 1, Len: 548     Source Port: 2238     Destination Port: 80     [Stream index: 10]     [TCP Segment Len: 548]     Sequence Number: 1 (relative sequence number)     Sequence Number (raw): 2028883223     [Next Sequence Number: 549 (relative sequence number)]     Acknowledgment Number: 1 (relative ack number)     Acknowledgment number (raw): 164847634						
0000 18 b1 69 0f 81 27 58 8a 5a 38 ab d2 08 00 45 00 ..i..X Z8...E 0010 02 4c cc 5b 40 00 80 06 ef f1 c0 a8 bc d7 12 c0 ..L[@... ..... 0020 ac 1e 08 be 00 50 78 ee 4d 17 09 d3 60 12 50 18 ...Px M...`P. 0030 04 02 5a a6 00 00 47 45 54 20 2f 20 48 54 50 ..Z..GE T / HTTP 0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 2e /1.1-Ho st: www. 0050 76 75 6c 6e 77 65 62 2e 63 6f 6d 0d 0a 43 6f 6e vulnweb. com-Con 0060 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6e nection: keep-al						

ပုံထဲကမှ Transmission Control Protocol ကိုနှိပ်လိုက်ပါ။

18.3.614466	192.168.188.215	18.192.172.30	HTTP	602 GET / HTTP/1.1
> Frame 18: 602 bytes on wire (4816 bits), 602 bytes captured (4816 bits) on interface \Device\NPF_{ACEE0960-821B-4E5A-8627-6FBEE65D4655}, id 0				
> Ethernet II, Src: Dell_38:ab:d2 (58:8:a5:38:ab:d2), Dst: Sonicwall_0f:81:27 (18:b1:69:0f:81:27)				
> Internet Protocol Version 4, Src: 192.168.188.215, Dst: 18.192.172.30				
> Transmission Control Protocol, Src Port: 2238, Dst Port: 80, Seq: 1, Ack: 1, Len: 548				
Source Port: 2238 Destination Port: 80 [Stream index: 10] [TCP Segment Len: 548] Sequence Number: 1 (relative sequence number) Sequence Number (raw): 2028883223 [Next Sequence Number: 549 (relative sequence number)] Acknowledgment Number: 1 (relative ack number) Acknowledgment number (raw): 164847634 0101 .... = Header Length: 20 bytes (5) > Flags: 0x018 (PSH, ACK) Window: 1026 [Calculated window size: 262656] [Window size scaling factor: 256] Checksum: 0x5aa6 [unverified] [Checksum Status: Unverified] Urgent Pointer: 0 > [SEQ/ACK analysis] > [Timestamps] TCP payload (548 bytes)				
> Hypertext Transfer Protocol				
<pre>0000 18 b1 69 0f 81 27 58 8a 5a 38 ab d2 08 00 45 00 ..i.'X Z8...E. 0010 02 4c cc 5b 40 00 80 06 ef f1 c0 a8 bc d7 12 c0 .L.[@... ..... 0020 ac 1e 08 be 00 50 78 ee 4d 17 09 d3 60 12 50 18 ....Px. M...`..P. 0030 04 02 5a a6 00 00 47 45 54 20 2f 20 48 54 54 58 ..Z--GE T / HTTP 0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e /1.1-Ho st: www. 0050 76 75 6c 77 65 62 2e 63 6f 6d 0d 0a 43 6f 6e vulnweb. com..Con 0060 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c nnection: keep-al 0070 69 76 65 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 ive..Cac he-Contr 0080 6f 6c 3a 20 6d 61 78 2d 61 67 65 3d 30 0d 0a 55 ol: max- age=0..U 0090 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d pgrade-I nsecure- 00a0 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 Requests : 1..Use 00b0 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 r-Agent: Mozilla 00c0 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 /5.0 (Wi ndows NT</pre>				

ပုံမှာဆိုရင် Source Port, Destination Port, Flags စိတဲ့ information တွေကို  
တွေ့ရမှာဖြစ်ပါတယ်။

## SNMP

Simple Network Management Protocol (SNMP) ဆိုတာက TCP/IP protocol ဖြစ်ပြီး Network devices တွေနဲ့ systems တွေကို monitoring လုပ် ပိုအတွက်အသုံးပြုတာဖြစ်ပါတယ်။ SNMP ကိုအသုံးပြုဖို့ဆိုရင် components ၃ ခုလိုအပ်ပါတယ်။

- Manage devices
- Agent
- Network Management System (NMS)

SNMP ၏ ports 161 နဲ့ 162 ကိုအသုံးပြုပါတယ်။ SNMP agents ၏ requests တွေကို port 161 ကနေလက်ခံပါတယ်။ Notifications တွေကိုတော့ port 162 ကနေလက်ခံတာဖြစ်ပါတယ်။ SNMP versions တွေဖြစ်တဲ့ 1 နဲ့ 2 တွေက security ပိုင်းမှာအားနည်းချက်တွေရှိပါတယ်။ ဒါကြောင့်နောက်ပိုင်းမှာ SNMP

version 3 ကို develop လုပ်ခဲ့ပါတယ်။ Version 3 မှာဆိုရင် confidentiality တွေကို encrypted လုပ်ပါတယ်။

## Analytical Tools

Security အတွက်အသုံးပြုရတဲ့ analytical tools တွေအများကြီးရှိပါတယ်။ Windows မှာဆိုရင် openfiles ဆိုတဲ့ command က default ပါဝင်ပါတယ် အဲ command ကိုအသုံးပြုပြီးတော့ local က open files တွေကိုတွေ့ရမှာဖြစ်ပါတယ်။ အရင်ဆုံး cmd ကို Administrator အနေနဲ့ run ပါ။ ပြီးရင် cmd မှာ openfiles /? ဆိုပြီးရှိက်လိုက်ပါ သူ့မှာပါတဲ့ parameter တွေကိုတွေ့ရမှာဖြစ်ပါတယ်။ Openfiles command မှာ Maintain Objects List global flag ကိုအရင်ဆုံး enabled လုပ်ပေးဖို့လိုအပ်ပါတယ်။ Command ကတော့ openfiles /local on ဖြစ်ပါတယ်။

```
C:\Windows\system32>openfiles /local on
SUCCESS: The system global flag 'maintain objects list' is enabled.
          This will take effect after the system is restarted.

C:\Windows\system32>
```

ပြီးရင်တော့ restart လုပ်ပေးဖို့လိုအပ်ပါတယ်။ Restart ချုပြုးတာနဲ့ cmd ကနေ openfiles / Query command ရှိက်လိုက်ပါက အောက်ကပုံအတိုင်း local က open files တွေကိုတွေ့ရမှာဖြစ်ပါတယ်။

```
C:\Windows\system32>openfiles /Query

Files Opened Locally:
-----

ID      Process Name          Open File (Path\executable)
=====  ======  =====
64      sihost.exe           C:\Windows\System32
432     sihost.exe           C:\Windows\Registration\R000000000006.clb
1648    sihost.exe           C:\Windows\System32\en-US\KernelBase.dll.mui
72      svchost.exe          C:\Windows\System32
304     svchost.exe          C:\Windows\System32\en-US\svchost.exe.mui
408     svchost.exe          C:\Windows\Registration\R000000000006.clb
836     svchost.exe          C:\..\Windows\Notifications\wpndatabase.db-wal
840     svchost.exe          C:\..\Windows\Notifications\wpndatabase.db-shm
932     svchost.exe          C:\..\Windows\Notifications\wpndatabase.db
936     svchost.exe          C:\Windows\System32\en-US\KernelBase.dll.mui
1200    svchost.exe          C:\Windows\System32\en-US\crypt32.dll.mui
2104    svchost.exe          C:\Windows\System32\en-US\winnlsres.dll.mui
2148    svchost.exe          C:\..\L.hanniu\ActivitiesCache.db-shm
2208    svchost.exe          C:\Windows\System32\en-US\mswsock.dll.mui
2496    svchost.exe          C:\..\L.hanniu\ActivitiesCache.db
2508    svchost.exe          C:\..\L.hanniu\ActivitiesCache.db-wal
```

အဲထဲကမှ disconnect လုပ်ချင်တယ်ဆိုရင် openfiles /disconnect / id \*\*  
ဖြစ်ပါတယ်။

```
C:\Windows\system32>
C:\Windows\system32>openfiles /disconnect /id 68

C:\Windows\system32>
```

System မှာချိတ်ဆက်နေတဲ့ connection တွေကိုစစ်ဆေးခြင်တယ်ဆိုရင်တော့  
netstat -an ဆိုတဲ့ command ကိုအသုံးပြုနိုင်ပါတယ်။

C:\WINDOWS\system32>netstat -an			
Active Connections			
Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:808	0.0.0.0:0	LISTENING
TCP	0.0.0.0:902	0.0.0.0:0	LISTENING
TCP	0.0.0.0:912	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5000	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5001	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5060	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5061	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5090	0.0.0.0:0	LISTENING
TCP	0.0.0.0:7070	0.0.0.0:0	LISTENING
TCP	0.0.0.0:7680	0.0.0.0:0	LISTENING
TCP	0.0.0.0:28451	0.0.0.0:0	LISTENING
TCP	0.0.0.0:28459	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49679	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49713	0.0.0.0:0	LISTENING
TCP	127.0.0.1:5004	0.0.0.0:0	LISTENING
TCP	127.0.0.1:5004	127.0.0.1:49751	ESTABLISHED
TCP	127.0.0.1:5354	0.0.0.0:0	LISTENING
TCP	127.0.0.1:5354	127.0.0.1:49683	ESTABLISHED
TCP	127.0.0.1:5354	127.0.0.1:49684	ESTABLISHED
TCP	127.0.0.1:5480	0.0.0.0:0	LISTENING
TCP	127.0.0.1:5480	127.0.0.1:49707	ESTABLISHED
TCP	127.0.0.1:5480	127.0.0.1:49708	ESTABLISHED
TCP	127.0.0.1:5480	127.0.0.1:49709	ESTABLISHED
TCP	127.0.0.1:5480	127.0.0.1:49734	ESTABLISHED
TCP	127.0.0.1:5480	127.0.0.1:49743	ESTABLISHED

ဒါဆိုရင် active connection တွေကို port တွေနဲ့အတူတွေ့ရမှာဖြစ်ပါတယ်။  
 တစ်ကယ်လို့ send နဲ့ received တို့အတွက် bytes နဲ့ packets တို့ကိုသိချင်တယ်  
 ဆိုရင်တော့ netstat -e ဆိုတဲ့ command ကိုအသုံးပြုနိုင်ပါတယ်။

C:\WINDOWS\system32>netstat -e		
Interface Statistics		
	Received	Sent
Bytes	2100948942	94670417
Unicast packets	1578458	822547
Non-unicast packets	18934	12740
Discards	0	0
Errors	0	0
Unknown protocols	0	0

အခုက္ခန်တော်စမ်းပြသားတာ Windows မှာဖြစ်ပြီး Linux မှာ open files ကိုကြည့်မယ်ဆိုရင် **lsof** command ကိုအသုံးပြုနိုင်ပါတယ်။

```
~$ lsof
COMMAND PID TASKCMD USER FD   TYPE   DEVICE SIZE/OFF NODE NAME
tini    1          user cwd   DIR    0,400    4096  6712497 /
tini    1          user rtd   DIR    0,400    4096  6712497 /
tini    1          user txt   REG    0,202  24064  166825 /cocalc/bin/tini (10.105.159.225:
tini    1          user mem   REG    0,202 2029224 34213541 /lib/x86_64-linux-gnu/libc-2.31.s
tini    1          user mem   REG    0,202 191480 34213535 /lib/x86_64-linux-gnu/ld-2.31.so
tini    1          user Ou    CHR    1,3     0t0      7 /dev/null
tini    1          user 1w    FIFO   0,13    0t0 11490744 pipe
tini    1          user 2w    FIFO   0,13    0t0 11490745 pipe
sh    7          user cwd   DIR    0,400    4096  6712497 /
sh    7          user rtd   DIR    0,400    4096  6712497 /
sh    7          user txt   REG    0,202 129816 26480183 /usr/bin/dash (10.105.159.225:/ub
sh    7          user mem   REG    0,202 2029224 34213541 /lib/x86_64-linux-gnu/libc-2.31.s
sh    7          user mem   REG    0,202 191480 34213535 /lib/x86_64-linux-gnu/ld-2.31.so
sh    7          user Ou    CHR    1,3     0t0      7 /dev/null
sh    7          user 1w    FIFO   0,13    0t0 11490744 pipe
sh    7          user 2w    FIFO   0,13    0t0 11490745 pipe
node   8          user cwd   DIR    0,387    13      34 /home/user
node   8          user rtd   DIR    0,400    4096  6712497 /
node   8          user txt   REG    0,202 73873984 167209 /cocalc/nvm/versions/node/v14.16.
node   8          user mem   REG    0,202 25144   65155 /cocalc/src/smc-project/node_modu
-proj-metrics-async)
node   8          user mem   REG    0,202 1533768  52643 /cocalc/src/smc-project/jupyter/n
proj-metrics-async)
node   8          user mem   REG    0,202 35392   69668 /cocalc/src/smc-project/node_modu
etrics-async)
node   8          user mem   REG    0,202 1615104  61689 /cocalc/src/smc-project/node_modu
```

Active connection ကတော့ **netstat -an** command ကိုပဲအသုံးပြုနိုင်ပါတယ်။

```
~$ netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:6000             0.0.0.0:*
                                         LISTEN
tcp        0      0 192.168.21.49:6001       0.0.0.0:*
                                         LISTEN
tcp        0      0 0.0.0.0:2222             0.0.0.0:*
                                         LISTEN
tcp        0      0 192.168.21.49:6001       192.168.101.16:60736 TIME_WAIT
tcp        0      0 192.168.21.49:6000       192.168.164.7:38506 ESTABLISHED
tcp        0      0 192.168.21.49:6001       192.168.101.16:36624 ESTABLISHED
tcp        0      0 192.168.21.49:6001       192.168.153.32:52040 ESTABLISHED
tcp        0      0 192.168.21.49:6001       192.168.128.236:50940 TIME_WAIT
tcp6       0      0 ::::45311              ::::*
                                         LISTEN
tcp6       0      0 ::::2222               ::::*
                                         LISTEN
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type      State      I-Node Path
~$
```

စာဖတ်သူတို့စက်ထဲမှာ Linux ကိုမတင်ထားရသေးဘူးဆိုရင်တော့ အောက်က link မှာဝင်ပြီး command တွေကိုအသုံးပြုလိုရနိုင်ပါတယ်။

<https://cocalc.com/doc/terminal.html>

## Conducting Audits

Computer security audits ဆိုတာ applications, systems, networks တိုကို technical ပိုင်း assessments လုပ်တာဖြစ်ပါတယ်။ Audits လုပ်တဲ့အခါ manually ဒါမှမဟုတ် programs တွေကိုအသုံးပြုပြီးလုပ်လိုပါတယ်။ Manually assessments လုပ်မယ်ဆိုရင် အောက်ပါအချက်တို့ပါဝင်ပါတယ်။

- Review of security logs
- Review of access control lists
- Review of user rights and permissions
- Review of group policies
- Performance of vulnerability scans
- Review of written organization policies
- Interviewing organization personnel

တို့ပဲဖြစ်ပါတယ်။ Programs ကိုအသုံးပြုပြီး networks, systems တိုကို audit လုပ်မယ်ဆိုရင် Belarc Advisor ဒါမှမဟုတ် Windows နဲ့ Linux တို့မှာ default ပါဝင်တဲ့ auditing features တွေကိုအသုံးပြုပြီးတော့လုပ်ဆောင်နိုင်ပါတယ်။ Opensource အတွက်ဆိုရင်တော့ OpenXDAS project ကိုအသုံးပြုနိုင်ပါတယ်။ IT security မှာ audit လုပ်တဲ့အခါ အောက်ပါအခြေခံအချက်တွေကိုလိုအပ်ပါတယ်။

- Step 1. Define exactly what is to be audited
- Step 2. Create backups
- Step 3. Scan for, analyze, and create a list of vulnerabilities, threats, and issues that have already occurred.
- Step 4. Calculate risk

- Step 5. Develop a plan to mitigate risk and present it to the appropriate personnel.

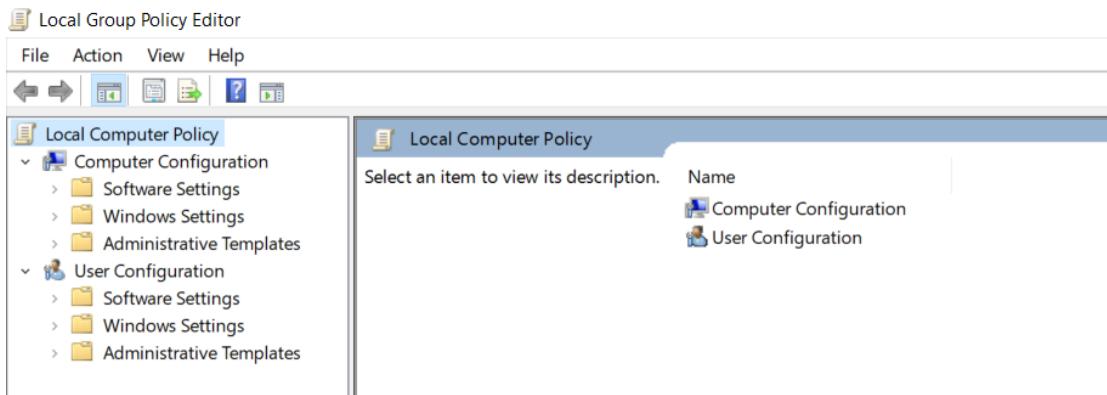
Security auditors တွေအနေနဲ့အပေါ်မှာဖော်ပြထားတဲ့ အချက်တွေကိုလုပ်ဆောင်ဖို့လိုအပ်သလို security administrator တွေအနေနဲ့ logs, systems security settings တွေကိုလဲ audit လုပ်ဖို့လိုအပ်ပါတယ်။

### Auditing Files

Auditing လုပ်တယ်ဆိုတာ ဘယ်သူက, ဘာကို, ဘယ်အချိန်မှာ resources တွေကိုအသုံးပြုနေလဲဆိုတာသိဖို့အတွက်ဖြစ်ပါတယ်။ Files တွေကို audit လုပ်မယ်ဆိုရင် အောက်ပါအချက် (၃) ချက်တို့ကိုလုပ်ဆောင်ဖို့ လိုအပ်ပါတယ်။

- Step 1. Turn on an auditing policy.
- Step 2. Enable auditing for particular objects such as files, folders, and printers.
- Step 3. Review the security logs to determine who did what to a resource and when.

Auditing လုပ်မယ်ဆိုရင် Windows မှာဆိုရင် default အနေနဲ့ပါဝင်တဲ့ Group Policy ကိုအသုံးပြုပြီး policy တွေကိုသတ်မှတ်လိုပါတယ်။ Group policy ကို access လုပ်မယ်ဆိုရင် run box ကနေ gpedit.msc ဆိုတဲ့ command ကိုအသုံးပြုနိုင်ပါတယ်။



Policy သတ်မှတ်ဖို့အတွက် Windows Settings > Security Settings > Audit Policy ကိုနှစ်လိုက်ရင် Default သတ်မှတ်ထားတဲ့ policy တွေကိုတွေ့ရမှာဖြစ်ပါတယ်။

Policy	Security Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

ဒါပေမယ့် Security Setting မှာဆိုရင်တော့ No auditing ဆိုပြီးဖြစ်နေတာ တွေ့ရမှာဖြစ်ပါတယ်။ အခုကျွန်ုတ်တို့ Audit object access ဆိုတာရဲ့ Security Setting ကို Success, Failure အဖြစ်ပြောင်းပါမယ်။ Double click နှင့် လိုက်ပါ။

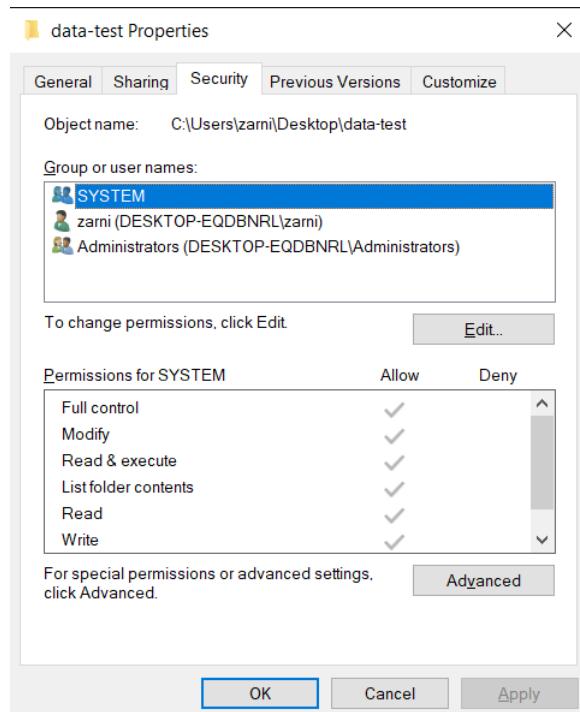
Policy	Security Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
<b>Audit object access</b>	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

ပုံမှာပြထားတဲ့အတိုင်း Success နဲ့ Failure တို့ရဲ့ဘေးက box ထဲမှာ အမှန်ခြစ်ခြစ်ဖြီးရင် Ok နဲ့ပြန်ထွက်လိုက်ပါ။ ဒါဆိုရင်တော့ Security Setting မှာအောက်ကပုံအတိုင်းတွေ့ရမှာဖြစ်ပါတယ်။

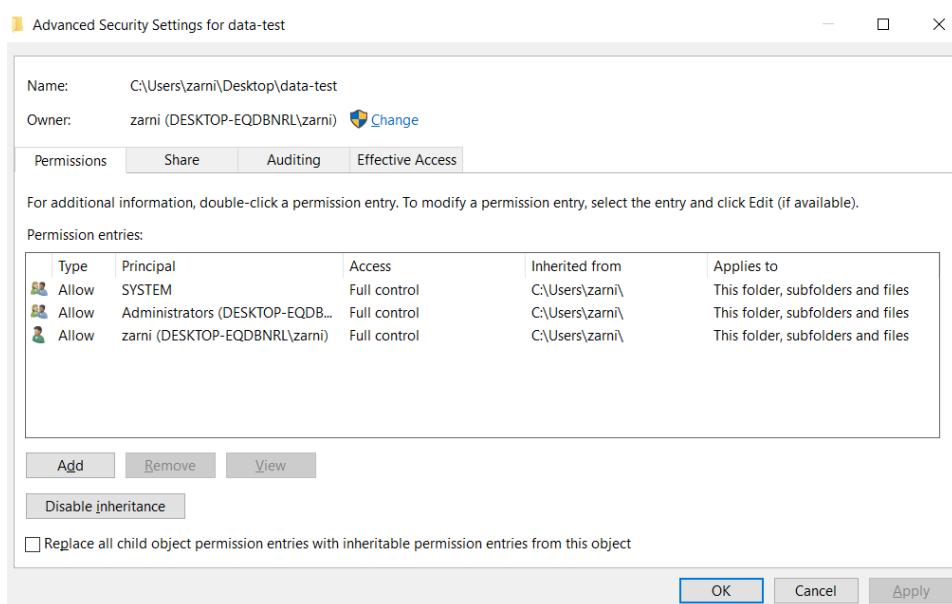
Policy	Security Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
<b>Audit object access</b>	Success, Failure
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

ဒါ policy က files, folders တွေကို audit လုပ်ဖို့အတွက် အသုံးပြုတာဖြစ်ပါတယ်။

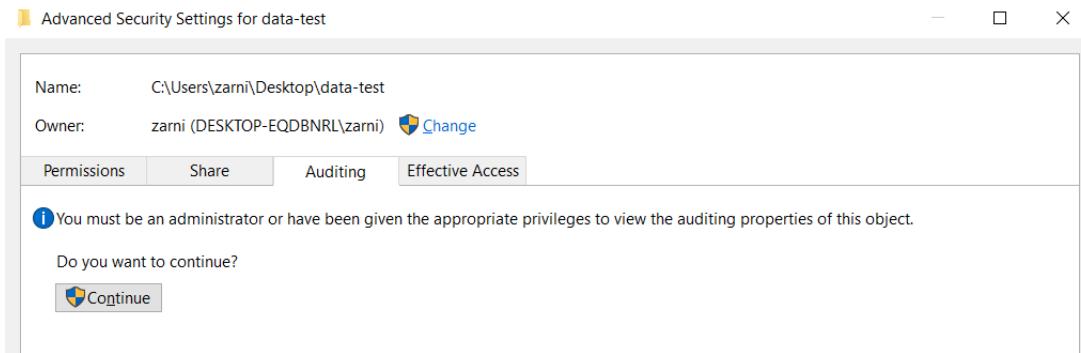
အခုက္ခန်တော်တို့ folder တစ်ခုကို create လုပ်ပါမယ် ပြီးရင် အဲ folder ကို auditing အတွက်သတ်မှတ်ပါမယ်။ Create လုပ်ထားတဲ့ folder ပေါ်မှာ right click နိုင်ပါမယ် ပြီးရင် Properties ထဲကိုသွားပါမယ်။ Properties ထဲကမှတ်ဆင့် Security tag ထဲကိုသွားမှာဖြစ်ပါတယ်။



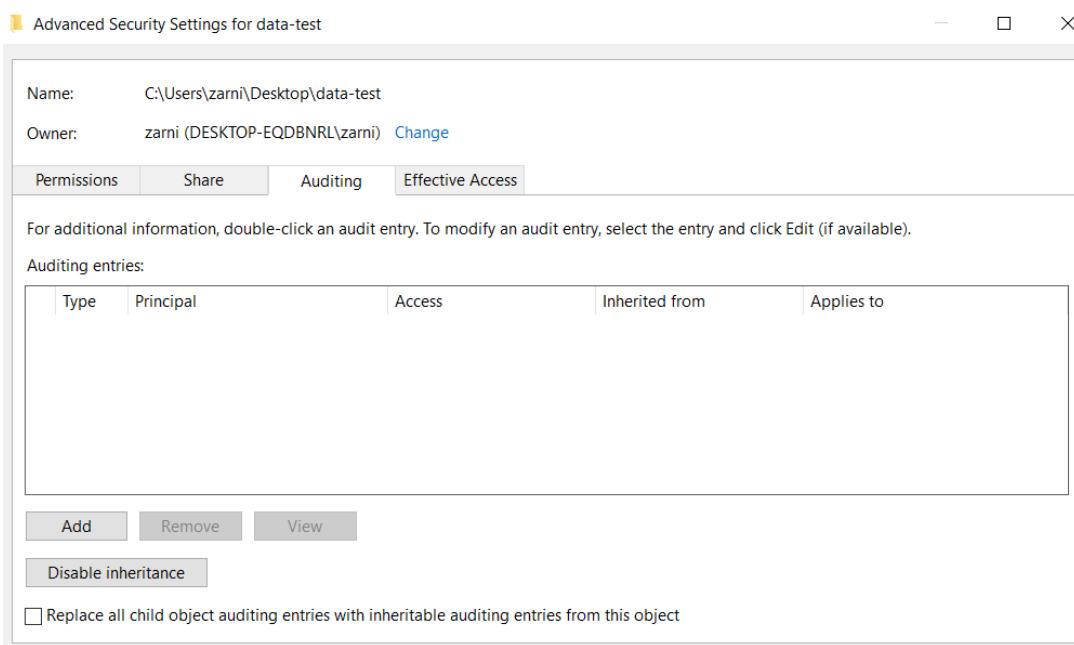
အဲထဲကမှ Advanced ဆိုတဲ့ button ကိုနိုင်ပါမယ်။



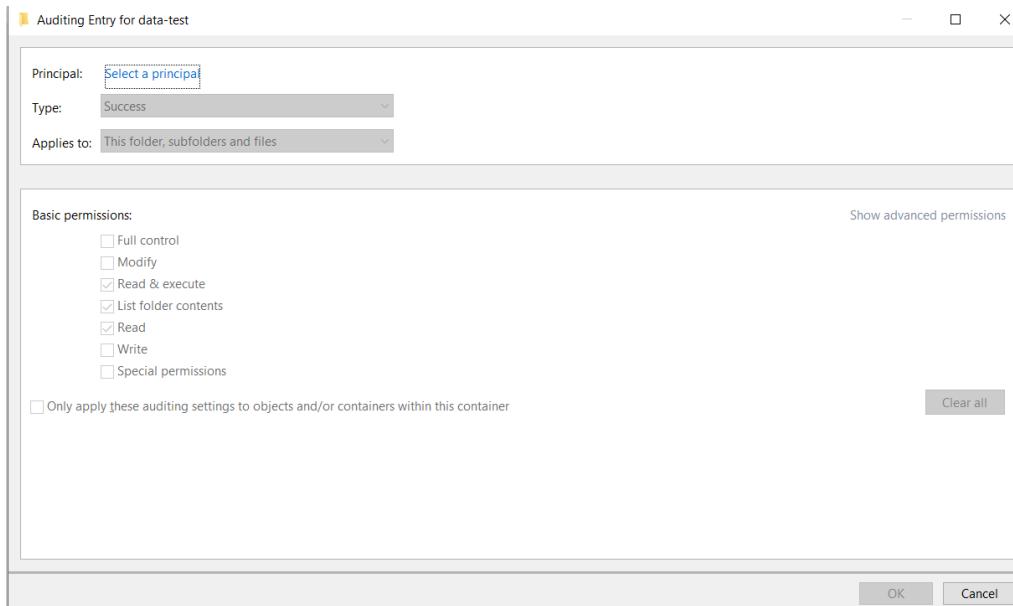
နောက်ကုန်တော်တို့ဆက်ပြီး Auditing tag ထဲကိုသွားပါမယ်။



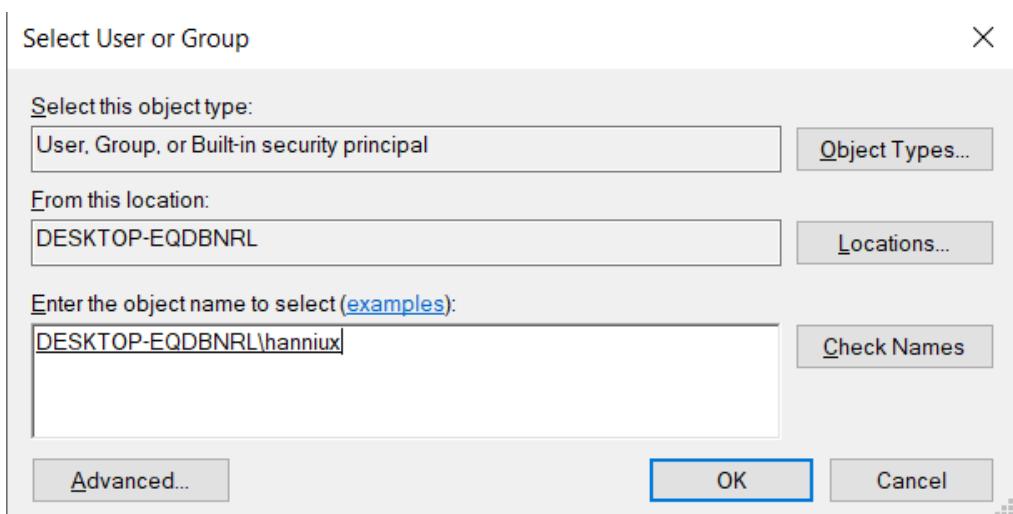
Continue ဆိုတဲ့ button ကိုနှစ်လိုက်ပါ။ အောက်ကပုံအတိုင်းတွေရမှာဖြစ်ပါတယ်။



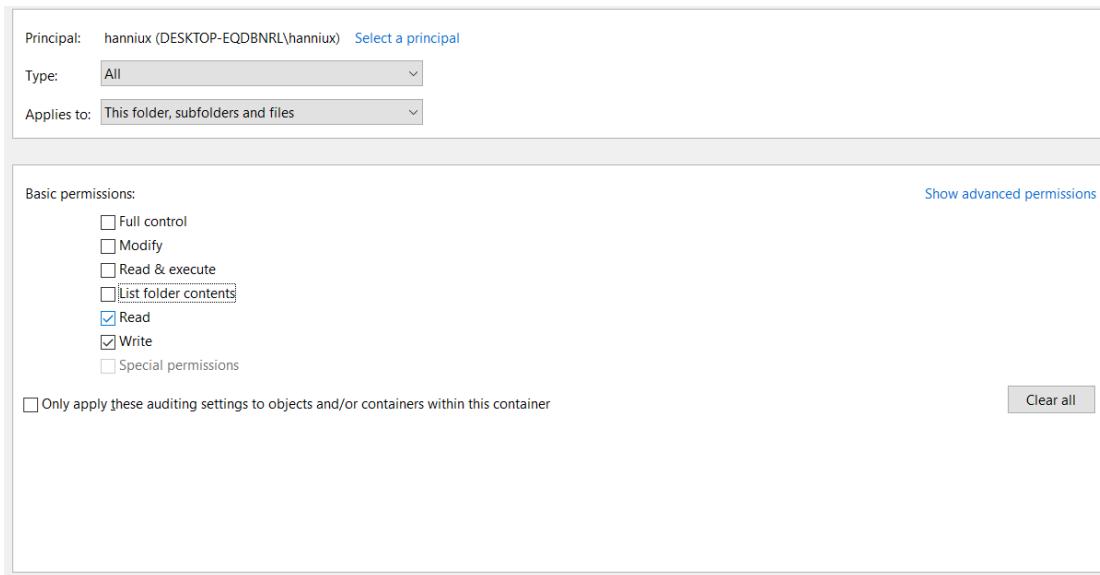
Add button ကိုနှစ်ပြီး Auditing Entry လုပ်ပါမယ်။ အောက်ကပုံမှာဆိုရင် Select a principal ဆိုတဲ့စာတန်းအပြာနဲ့ စာသားရှိပါတယ်။ အဲစာသားကိုနှစ်လိုက်ပါ။



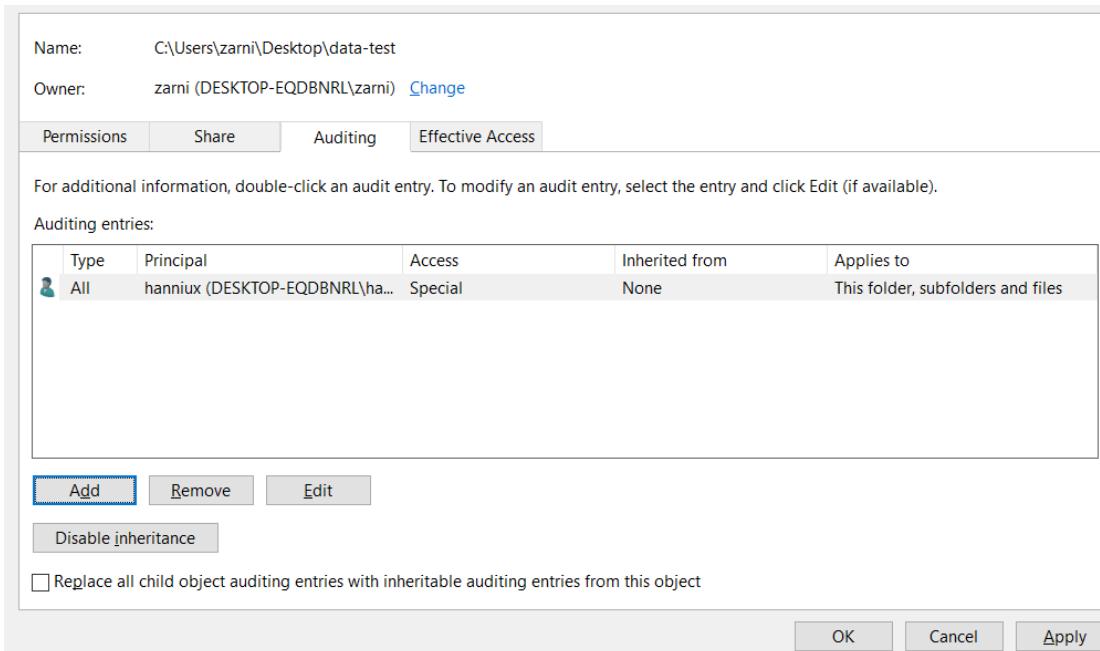
Select a principal ကိုနှင့်လိုက်ရင်တော့အောက်ကပုံအတိုင်း User သတ်မှတ်ပေးရမယ့်နေရာကိုရောက်မှာဖြစ်ပါတယ် ဒဲမှာ audit လုပ်ချင်တဲ့ user ကို ထည့်ပေးရမှာဖြစ်ပါတယ်။။ စာဖတ်သူတို့သတ်မှတ်ချင်တဲ့ user account ကို ထည့်ပေးရမှာဖြစ်ပါတယ်။ ကျွန်ုတ်ကတော့ လက်ရှိအသုံးပြုနေတဲ့ user account ကိုပဲ add ပါမယ်။



ကျွန်ုတ် username ကိုထည့်ပြီးတော့ Check Names ဆိုတဲ့ button ကိုနှင့် လိုက်ပါတယ်။ Name မှန်ရင်တော့ Text box ထဲကအတိုင်းတွေ့ရမှာဖြစ်ပါတယ်။ ပြီးရင်တော့ OK နှင့်ပြီးပြန်ထွက်ပါမယ်။

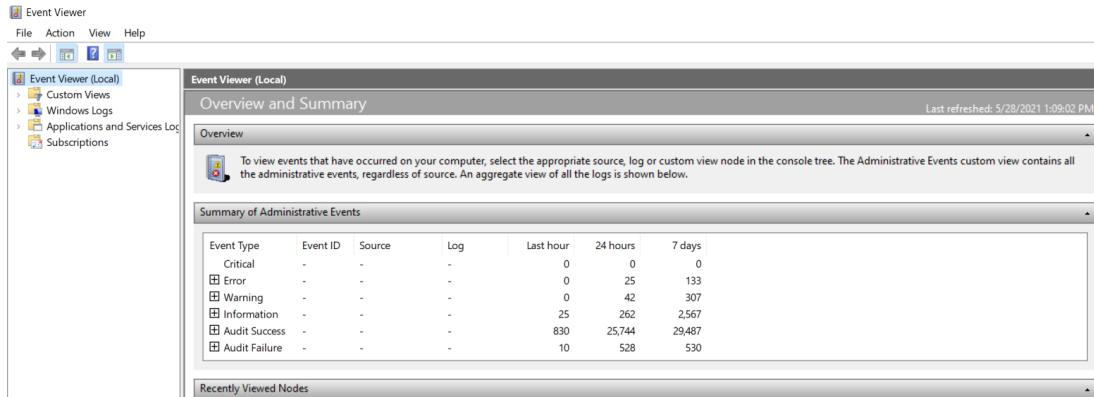


အပေါက်ပုံအတိုင်း Type မှာဆိုရင် All ကိုရွေးပါမယ်။ Basic permissions မှာတော့ Read, Write (၂) မျိုးကိုပဲသတ်မှတ်ထားပြီး Ok button ကိုနှိပ်မယ်။ အားလုံးပြီးသွားရင်တော့ အောက်ကပုံအတိုင်းတွေ့ရမှာဖြစ်ပါတယ်။

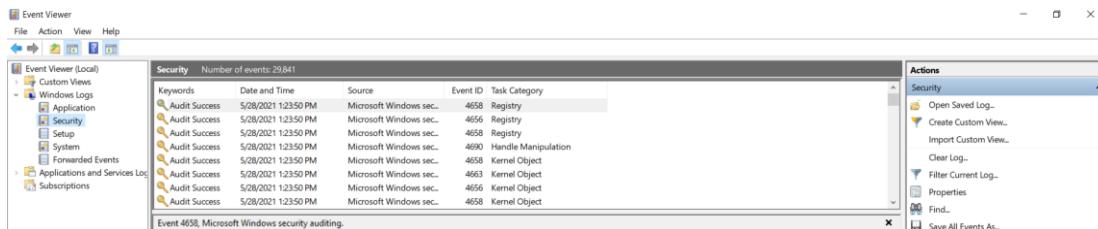


ဒါဆိုရင်တော့ Audit ပိုင်းအတွက်လုပ်ဆောင်တာပြီးသွားပြီဖြစ်ပါတယ်။ Apply နဲ့ OK button ကိုနှိပ်ပြီးထွက်ပါမယ်။ အခုက္ခန်းတော်တို့ security logs အပိုင်းကို ဆက်ပြီးတော့သွားကြရအောင်။ Security logs မှာဆိုရင်ဘယ်သူက ဘယ်အချိန်မှာ ကျွန်ုင်တော်တို့ system ထဲကာဘာကို access လုပ်ခဲ့လဲဆိုတာကို တွေ့ကိုပြန်ကြည့်လို့ရပါတယ်။ ဒါအပြင် security logs မှာ users က access

လုပ်ခဲ့တာက success ဖြစ်လား ဒါမှမဟုတ် failed ဖြစ်လား, နောက် modify, delete လုပ်ခဲ့လား စတာတွေကိုပါတွေ့မြင်နိုင်မှာဖြစ်ပါတယ်။ Security Logs တွေကိုပြန်ကြည့်မယ်ဆိုရင် Event Viewer ထဲကနေဝင်ကြည့်လို့ရပါတယ်။ Event Viewer ကို access လုပ်မယ်ဆိုရင် run box ကနေ eventvwr လို့ရှိက်ပါ။



Security log ကိုကြည့်မယ်ဆိုရင်တော့ Windows Logs > Security ကိုကြည့်ရ မှာဖြစ်ပါတယ်။



အဲထဲက Security Logs မှာဆိုရင် local computer ဒါမှမဟုတ် domain ကို access လုပ်တာ, modify, file delete လုပ်တာ, policies တွေပြင်တာ စတာ တွေကို logs အနေနဲ့သိမ်းတာဖြစ်ပါတယ်။ အခုဆက်ပြီး event viewer ထဲမှာ နောက်အရေးပါတဲ့ logs တွေရှိပါတယ်။ အဲဒါတွေကတော့

- System: System shutdown လုပ်တာတို့နောက် driver fail တာတွေ စတဲ့ဖြစ်စဉ်တွေကို log အနေနဲ့သိမ်းတာဖြစ်ပါတယ်။
- Application: Operating system applications တွေနဲ့ third-party programs တွေရဲ့ events တွေကို log အနေနဲ့သိမ်းတာဖြစ်ပါတယ်။

## Chapter 8 – Cryptography

Organizations တွေမှာ authorized users တွေပဲ access လုပ်ခွင့်ရှိတဲ့ private data တွေရှိပါတယ်။ အဲ private data တွေဆိုတာ customer databases, business strategies နဲ့သက်ဆိုင်တဲ့ email တွေ စတဲ့ data တွေပါဝင်ပါတယ်။ Organizations တွေက အဲ data တွေကို secure ဖြစ်အောင်သိမ်းဖို့လိုအပ်ပါတယ်။ Data တွေ secure ဖြစ်ဖို့အတွက်ဆိုရင် encryption ကိုအသုံးပြုရမှာဖြစ်ပါတယ်။

### Cryptography

Cryptography ဆိုတာက information တွေကိုပြီးတော့စိတ်ချရဖို့အတွက် hiding လုပ်တယ်လို့သတ်မှတ်လို့ရပါတယ်။

### Encryption

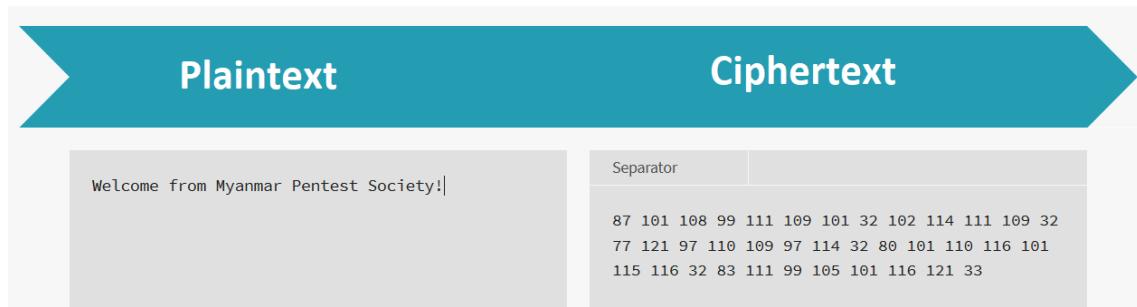
Encryption ဆိုတာက information တွေကို algorithm တစ်ခုခု ဥပမာ - AES, RSA ကိုအသုံးပြုပြီး အလွယ်တကူဖတ်လို့မရအောင် လုပ်ဆောင်တာဖြစ်ပါတယ်။ Encryption ကို secure communications နဲ့ data တွေ transfer လုပ်တဲ့အခါ အသုံးပြုပါတယ်။

### Decryption

Decryption ဆိုတာက encrypt လုပ်ထားတဲ့ information တွေကိုမှုရင်းအတိုင်း ဖြစ်အောင်ပြန်လည်လုပ်ဆောင်တာကိုပြောတာဖြစ်ပါတယ်။

### Cipher

Cipher ဆိုတာက encryption နဲ့ decryption လုပ်တဲ့အခါအသုံးပြုတဲ့ algorithm ဖြစ်ပါတယ်။ စာဖတ်သူတွေမြင်သာအောင်ပြောရရင် “Welcome from Myanmar Pentes Society!” ဆိုတဲ့ plaintext ကို ciphertext ပြောင်းလိုက်တဲ့အခါ အောက်ပါအတိုင်းတွေရမှာဖြစ်ပါတယ်။



## Key

Key ဆိုတာက cipher မှာအရေးပါတဲ့နေရာကပါဝင်ပါတယ်။ Information တွေကို encrypt လုပ်တဲ့အခါမှာ key ကိုအသုံးပြုရပါတယ်။ Encrypt လုပ်ထားတဲ့ information တွေကို plaintext တွေကို decrypt ပြန်လုပ်တဲ့အခါလဲ encrypt လုပ်တုန်းကအသုံးပြုခဲ့တဲ့ key ကိုပဲအသုံးပြုပေးရတာဖြစ်ပါတယ်။ Key ကိုအသုံးပြုရမှာ Public key နဲ့ Private key ဆိုပြီး (၂) မျိုးရှိပါတယ်။ Private key ကတော့ users တွေကပဲသိခွင့်ရှိတာဖြစ်ပါတယ်။ Private key နဲ့သက်ဆိုင်တဲ့ ဥပမာပေးရရင်တော့ authentication အတွက်အသုံးပြုတဲ့ smart card, ExpressCard/PC Card technology စတာတွေဖြစ်ပါတယ်။ Public key ကတော့ organization, group ထဲမှာပါဝင်တဲ့ users တွေအကုန်သိလို့ရပါတယ်။ Public key နဲ့သက်ဆိုင်တဲ့ ဥပမာကတော့ user (၂) ယောက်က Internet ကနေ secure communication လုပ်ဆောင်လိုတဲ့အခါ public key ကို သူတို့ (၂) ယောက်စလုံးမှာရှိနေဖို့လိုအပ်ပါတယ်။ အဲအခါ network ပေါ်ကနေ key ကို transfer လုပ်ဖို့လိုအပ်လာပါတယ်။ အဲဒါကို in-band key exchange လိုခေါ်ပါတယ်။

## Key Algorithms

Key algorithms မှာဆိုရင် Symmetric နဲ့ Asymmetric ဆိုပြီး (၂) မျိုးရှိပါတယ်။

### Symmetric Key Algorithms

Symmetric key algorithm ဆိုတာက encrypt အတွက်ကော့ decrypt အတွက်ပါ key တစ်ခုထဲကိုအသုံးပြုပြီးလုပ်ဆောင်တာဖြစ်ပါတယ်။ စာဖတ်သူ တွေရှင်းသွားအောင် အောက်မှာပုံနဲ့တက္ကဖော်ပြပေးထားပါတယ်။

## Symmetric Encryption



Symmetric key algorithms မှာဆိုရင် အမျိုးစား (၂) မျိုးရှိပါတယ်။

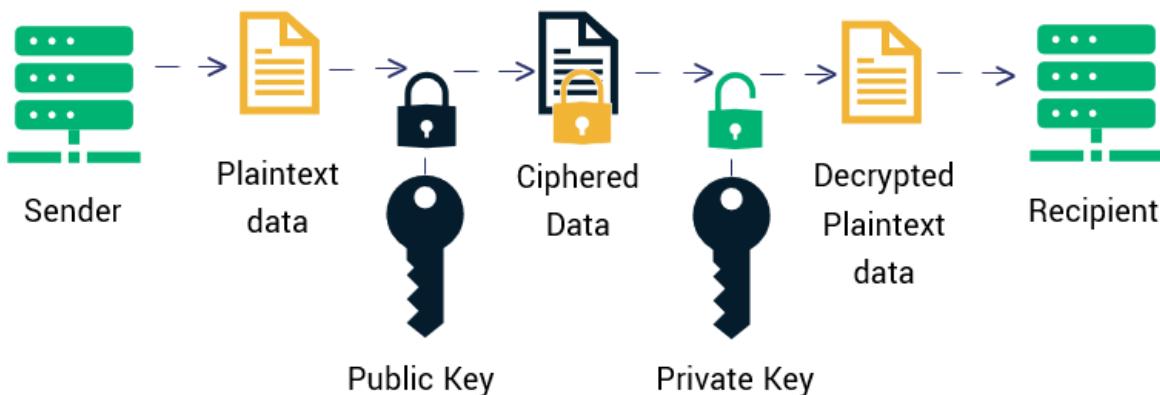
**Stream cipher** ဆိုတာက algorithm အမျိုးစားတစ်ခုဖြစ်ပြီး data stream ထဲက binary digit တွေကို encrypt လုပ်တဲ့အခါ တစ်ကြိမ်လျှင် 1-bit ကို encrypt လုပ်တာဖြစ်ပါတယ်။

**Block cipher** ဆိုတာက algorithm အမျိုးစားတစ်ခုဖြစ်ပြီး တစ်ကြိမ်တွင် စာပုဒ်တစ်ပုဒ်လုံးကို encrypt လုပ်တာဖြစ်ပါတယ်။ Block cipher မှာဆိုရင် Advanced Encryption Standard (AES) algorithm က 128-bit ဒါမှမဟုတ် 256-bit ကိုအသုံးပြုပါတယ်။

## Asymmetric Key Algorithms

Asymmetric ကတေသူ key ၂ ခုကိုအသုံးပြုပြီး encrypt, decrypt လုပ်တာဖြစ်ပါတယ်။ Encrypt အတွက်ကို public key အသုံးပြုတာဖြစ်ပြီး decrypt အတွက်ကိုတေသူ private key ကိုအသုံးပြုတာဖြစ်ပါတယ်။

## Asymmetric Encryption



### Encryption Algorithms

အရင်အပိုင်းမှာတုန်းက cipher ကိုအသုံးပြုပြီးတော့ data တွေကို encrypt, decrypt လုပ်လိုရတယ်ဆိုတာကိုလေ့လာခဲ့ပြီးဖြစ်ပါတယ်။ အခုခြီးသင်ခန်းစာမှာတော့ encryption algorithms တွေအကြောင်းကိုလေ့လာရမှာဖြစ်ပါတယ်။

### DES and 3DES

Data Encryption Standard (DES) ဆိုတာက အရင်တုန်းကအသုံးပြုခဲ့တဲ့ block cipher အမျိုးစားဖြစ်ပြီး U.S. federal government က 1970 မှာ encryption standard တစ်ခုအနေနဲ့အသုံးပြုခဲ့ပါတယ်။ ဒါပေမယ့် key ပိုင်းမှာ အားနည်း ချက်တွေရှိတဲ့အတွက် တခြား standard တစ်ခုအစားထိုးခဲ့ပါတယ်။ Block cipher တွေစပေါ်တုန်းက 64 bits ကိုအသုံးပြုတာဖြစ်ပါတယ်။ ဒါပေမယ့် အဲဒါက powerful မဖြစ်တဲ့အပြင် အရေးကြီးတဲ့ key size က 56-bit ဖြစ်တဲ့အတွက် brute-force attack ဒါမှမဟုတ် cryptanalysis attack နဲ့အလွယ်တကူ attack လုပ်ဆောင် လိုရနိုင်ပါတယ်။ ဒါကြောင့် DES နေရာမှို့ 3DES ကို 1999 မှာ အစားထိုးအသုံးပြုခဲ့ပါတယ်။ 3DES မှာတော့ cipher block size ကတော့ 64 bits ပဲဆိုပေမယ့် key size ကတော့ 168-bit ဖြစ်တဲ့အတွက် အလွယ်တကူ attack လုပ်ဆောင်လို့မရတော့ဘူး ဖြစ်ပါတယ်။ သို့သော်

နောက်ပိုင်းမှာတော့ DES နဲ့ 3DES အစား AES ကို 2001 နောက်ပိုင်းမှာ အစားထိုးအသုံး ပြုလာကြပါတယ်။

## AES

National Institute of Standards and Technology (NIST) က AES(Advanced Encryption Standards) ကို Develop လုပ်ခဲ့ပါတယ်။ 2002 ခုနှစ်မှာတော့ U.S. federal government က standard တစ်ခု အနေနဲ့အသုံးပြုလာကြပါတယ်။ AES မှာဆိုရင် block cipher အနေနဲ့က 128-bit ဖြစ်ပြီး key size အနေနဲ့တော့ 128-bit, 192-bit, 256 bit ဆိုပြီး ရှုပါတယ်။ AES ကိုအသုံးပြုပြီး encryption, decryption လုပ်တဲ့အခါ ပိုပြီးမြန်သလို resources လဲသိပ်မယူပါဘူး။ AES ကိုတော့ remote protocol တွေမှာလဲအသုံးပြုသလို Windows Encrypting File System (EFS) နဲ့ disk တစ်ခုလုံးကို encryption လုပ်တဲ့နည်းပညာတွေဖြစ်တဲ့ BitLocker လိုမျိုးမှာလဲအသုံးပြုပါတယ်။

## RC

RC ကို Ron Rivest က create လုပ်ခဲ့တာဖြစ်ပြီး symmetric-key encryption အတွက်ကိုအသုံးပြုတာဖြစ်ပါတယ်။ RC algorithms အမျိုးစား (၆) ခုရှိပါတယ်။

- RC 1
- RC 2
- RC 3
- RC 4
- RC 5
- RC 6

တို့ပဲဖြစ်ပါတယ်။ RC 1 ကတော့အသုံးပြုခဲ့ခြင်းမရှိပါဘူး။ RC 2 ကတော့ 64-bit block cipher ဖြစ်ပြီး 1987 မှာ develop လုပ်ခဲ့တာဖြစ်ပါတယ်။

RC 3 ကိုလဲအသုံးပြုခဲ့ခြင်းမရှိပါဘူး။ RC 4 ကတော့ stream cipher ဖြစ်ပြီး SSL,WEP နဲ့ RDP တို့မှာအသုံးပြုပါတယ်။ နောက် RC 4 က 128-bit ကိုအသုံးပြုပါတယ်။ RC 5 ကတော့ block cipher ဖြစ်ပြီး 32-bit, 64-bit, 128-bit ဆိုပြီး (၃) မျိုးရှိပါတယ်။ RC 6 ကတော့ block cipher ဖြစ်ပြီး AES နဲ့ပြုက်ဘက်တွေဖြစ်ပါတယ်။ Block size နဲ့ key size တွေက AES နဲ့တူပြီး မတူညီတဲ့ mathematical methods ကိုအသုံးပြုထားပါတယ်။

### **Blowfish and Twofish**

Blowfish နဲ့ Twofish ဆိုတဲ့ ciphers (၂) မျိုးကို create လုပ်ခဲ့တာ ကတော့ Bruce Schneier ဖြစ်ပါတယ်။ Original Blowfish ကတော့ block cipher ပုံစံမျိုးဖြစ်ပါတယ်။ Blowfish မှာဆိုရင် block size ကတော့ 64-bit ဖြစ်ပြီး key size တွေကတော့ 32-bit နဲ့ 448-bit ဆိုပြီး (၂) မျိုးရှိပါတယ်။ Bruce Schneier ကတော့ Twofish cipher ကိုပဲအသုံးပြုဖို့ပဲတိုက်တွန်းထားပါတယ်။ Twofish cipher မှာဆိုရင် block size က 128-bit ဖြစ်ပြီး kye size ကို 256-bit အထိအသုံးပြုနိုင်ပါတယ်။

ပေါ်မှာလေ့လာခဲ့ရတဲ့ algorithm တွေက Symmetric Encryption အမျိုးစားတွေဖြစ်ပါတယ်။ အခုဆက်ပြီး Asymmetric Encryption မှာပါဝင်တဲ့ algorithm တွေကိုလေ့လာကြည့်ရအောင်။

### **RSA**

RSA ကိုတော့ Rivest, Shamir, Adleman တို့ကို creator လုပ်ထားတာဖြစ်တာကြောင့် RSA ဆိုပြီးတော့အတိုကောက်ခေါ်တာဖြစ်ပါတယ်။ RSA က public key cryptography algorithm အမျိုးစားဖြစ်ပါတယ်။ Key size ကလဲ security အတွက်စိတ်ချေသလို protocol တွေကို secure ဖြစ်စေတဲ့အတွက် e-commerce တွေမှာအသုံးများပါတယ်။ Symmetric key algorithms တွေထပ်တော့နေးပေမယ့် ကောင်းတဲ့အချက်က encryption အတွက်တော့ပိုပြီးတော့အဆင်ပြေပါတယ်။

RSA က Credit Card security နဲ့ TLS/SSL တို့မှာကောင်းစွာအသုံးပြုနိုင်ပါတယ်။ RSA မှာအသုံးပြုတဲ့ keys size တွေကတော့ 512-bit, 1024-bit, 2048-bit ဆိုပြီးရှိပါတယ်။

### Diffie-Hellman

Diffie-Hellman key exchange ကို 1970 လောက်မှာ တိုတွင်ခဲ့တာဖြစ်ပြီး unprotected communications channel ကနေ secret key တွေကို shared လုပ်ဖို့အတွက်စတင်အသုံးပြုခဲ့တာဖြစ်ပါတယ်။ Diffie-Hellman က data တွေကို transfer လုပ်ဖို့အတွက် secure key exchange ကိုလိုက်နာပါတယ်။ အဲ key exchange က public network ပေါ်မှာ secret communication အတွက် secret key ကို shared လုပ်ပြီး established လုပ်ပါတယ်။ Diffie-Hellman ကြားဖြတ်ခိုးနားထောင်နှင့်တာတွေကိုပါထည့်သွင်းစဉ်းစားတာကြောင့် အဲပြုသနာကိုဖြေရှင်းဖို့အတွက် ခက်ခဲ့တဲ့ mathematically တွေကိုအသုံးပြုပြီးဖြေရှင်းခဲ့ပါတယ်။ သို့သော် အဲ vulnerable က man-in-the-middle attack ဖြစ်ပါတယ်။ ဒါကိုကာကွယ်ဖို့အတွက်ဆိုရင် password authentication တို့လို့ authentication method တွေကိုအသုံးပြုသင့်ပါတယ်။ ဒါ algorithm ကိုတော့ Transport Layer Security (TLS) protocol အနေ နဲ့ web sessions တွေကို encrypted လုပ်နေစဉ်မှာအသုံးပြုပါတယ်။

အခုကျွန်ုံးတော်ဆွေးနွေးခဲ့တာကတော့ asymmetric encryption algorithm တွေဖြစ်ပါတယ်။

### Hashing Algorithms

Encryption ဆိုတာက plaintext ကိုဖတ်လို့မရအောင်လုပ်တာဖြစ်ပြီး hashing ကတော့ text ကို encrypt လုပ်တာမဟုတ်ပါဘူး။ Hashing ကတော့အဲ text တွေကို ကိုယ်စားပြုတဲ့ hash value ဒါမှုမဟုတ် message digest ကိုပဲ generate လုပ်ပေးတာဖြစ်ပါတယ်။ Hashing က algorithms တစ်ခုထဲလိုအပ်ပြီး keys တွေမလိုပါဘူး။ Hash

လုပ်တာကို Chapter - 1 မှာတူန်းကန်မူနာအနေနဲ့စမ်းပြေပေးခဲ့ပြီးဖြစ်ပါတယ်။ Hashing လုပ်ရာမှာအသုံးပြုတဲ့ algorithms တွေကတော့

- MD5
- SHA
- RIPEMD
- HMAC

## MD5

Message Digest version 5 (MD5) hashing algorithm က 128-bit hash နဲ့ 32 hexadecimal characters တွေကို generate လုပ်ပေးပါတယ်။ MD4 version မှာ လုပ်ခြင်းတိုင်းဆိုင်ရာအားနည်းချက်တွေရှိတဲ့အတွက် MD5 ကို အစားထိုးအသုံးပြု တာဖြစ်ပါတယ်။

## SHA

Secure Hash Algorithm (SHA) ဆိုတာက NIST က sponsored လုပ်ထားတဲ့ hashing functions တစ်ခုဖြစ်ပါတယ်။ SHA မှာဆိုရင် version တွေ အနေနဲ့ SHA-0, SHA-1, SHA-2 နဲ့ SHA-3 ဆိုပြီးရှိပါတယ်။ SHA-1 က 160-bit algorithm ဖြစ်ပြီး United States အတွက် Digital Signature Algorithm အနေနဲ့ ပြုလုပ်ထားတာဖြစ်ပါ တယ်။ SHA-1 နဲ့ MD5 တို့က cryptographic flaws ဆင်တူ ဖြစ်ပါတယ်။ SHA-2 မှာဆိုရင် algorithms (၂) မျိုးထပ်ပြီးခဲ့ထားတာရှိပါတယ် အဲဒါ တွေကတော့ SHA-256 နဲ့ SHA-512 တို့ဖြစ်ပါတယ်။

## RIPEMD

RACE Integrity Primitives Evaluation Message Digest (RIPEMD) ဆိုတာက hashing algorithm တစ်ခုဖြစ်ပါတယ်။ RIPEMD ကို open-standard ပုံစံမျိုး အနေနဲ့ develop လုပ်ခဲ့တာဖြစ်ပြီး SHA နဲ့ဆန္ဒကျင်ဘက်

ဖြစ်ပါတယ်။ RIPEMD မှာ 128-bit, 160-bit, 256-bit, 320-bit ဆိုပြီး versions တွေရှိပါတယ်။ ဒါပေမယ့် RIPEMD ကိုတော့အသုံးတော့နည်းပါတယ်။

## HMAC

Hash Message Authentication Code (HMAC) ကို message တွေကို authenticate နဲ့ verify လုပ်ဖို့အတွက် symmetric key နဲ့တဲ့ပြီးတော့ အသုံးပြုတာ ဖြစ်ပါတယ်။ HMAC ကို MD5, SHA စတဲ့ hashing algorithms နဲ့တဲ့သုံးလို့ရပါတယ် အဲဒါကိုတော့ HMAC-MD5 ဒါမှမဟုတ် HMAC-SHA1/2/3 ဆိုပြီးခေါ်ဆိုနိုင်မှာဖြစ်ပါ တယ်။ HMAC ရဲ့အလုပ်လုပ်ဆောင်ပုံက message authentication code (MAC) ရဲ့ hash value ကိုထုတ်ပေးတာဖြစ်ပါတယ်။ ကျွန်တော်တိုက် plaintext ဒါမှမဟုတ် data တွေကို တူညီတဲ့ hashing algorithm ကိုအသုံးပြုပြီး hash ထုတ်တဲ့ အခါမည်သည့်အချိန်မှာမဆိုတူညီတဲ့ hash value ကို ပဲရရှိမှာဖြစ်ပါတယ်။ Integrity ကို verify လုပ်ချင်တဲ့အခါမျိုး တွေမှာ ဒီနည်းလမ်းကိုအသုံးပြုနိုင်ပါတယ်။

HMAC က secret (symmetric) key ကိုအသုံးပြုပြီး hashing process ကိုလုပ်ဆောင်ပါတယ်။ တစ်ယောက်ယောက်က data ကိုပို့လိုက်တဲ့အခါ integrity လုပ်ဖို့အတွက်ဆိုရင် key ကိုလိုအပ်ပါတယ်။ တစ်ကယ်လို့ key မရှိခဲ့ဘူးဆိုရင်တော့ data ရဲ့ hash ကိုထုတ်လို့ရမှာမဟုတ်ပါဘူး။ Key ရှိခဲ့ရင် တော့ same hash ကို ရမှာဖြစ်ပါတယ်။

## Digital Signatures and Certificates

ကျွန်တော်တို့ Web site ပေါ်ကနေငွေချေတာမျိုးမှာဆိုရင် Web server နဲ့ ကျွန်တော်တို့ client မှာ credit card number တွေမထည့်ခင် စိတ်ချရဖို့လိုအပ်ပါတယ်။ အဲလို စိတ်ချရဖို့အတွက်ဆိုရင် digital signatures နဲ့ digital certificates တွေလိုအပ်ပါတယ်။

## Digital Signatures

Web sites တစ်ခု secure ဖြစ်ဖို့ဆိုရင် asymmetric encryption အတွက် RSA key ကိုအသုံးပြုရပါတယ်။ Web site ကို လာတဲ့ connection တိုင်း secure ဖြစ်ဖို့အတွက်လိုရင် key exchange ကိုလုပ်အပ်ပါတယ်။ Web server က clients တွေအတွက်ကို public keys တွေကိုထုတ်ပေးပါတယ် client က data တွေကို secure လုပ်ဖို့အတွက် အဲ key နဲ့ encrypt လုပ်နိုင်ပါတယ်။ တစ်ချို့ ဖြစ်စဉ်တွေမှာကြတော့ client တွေက public key တွေကို share ပေးရပါတယ်။ စာဖတ်သူတွေမြင်သာအောင်ပြောရရင် sender က data ကို public key ကိုအသုံးပြုပြီးတော့ encrypt လုပ်ပါတယ် receiver ကသူ့ရဲ့ private key ကိုအသုံးပြုပြီး decrypt ပြန်လုပ်ဆောင်ပါတယ်။ အဲလိုပဲ sender ကသူ့ရဲ့ private key ကိုအသုံးပြုပြီး encrypt လုပ်တဲ့အခါ receiver က သူ့ဆီ မှာရှိနေတဲ့ public key နဲ့ decrypt ပြန်လုပ်နိုင်ပါတယ်။ ဒါဟာ digital signatures ရဲ့သဘောတရားဖြစ်ပါတယ်။

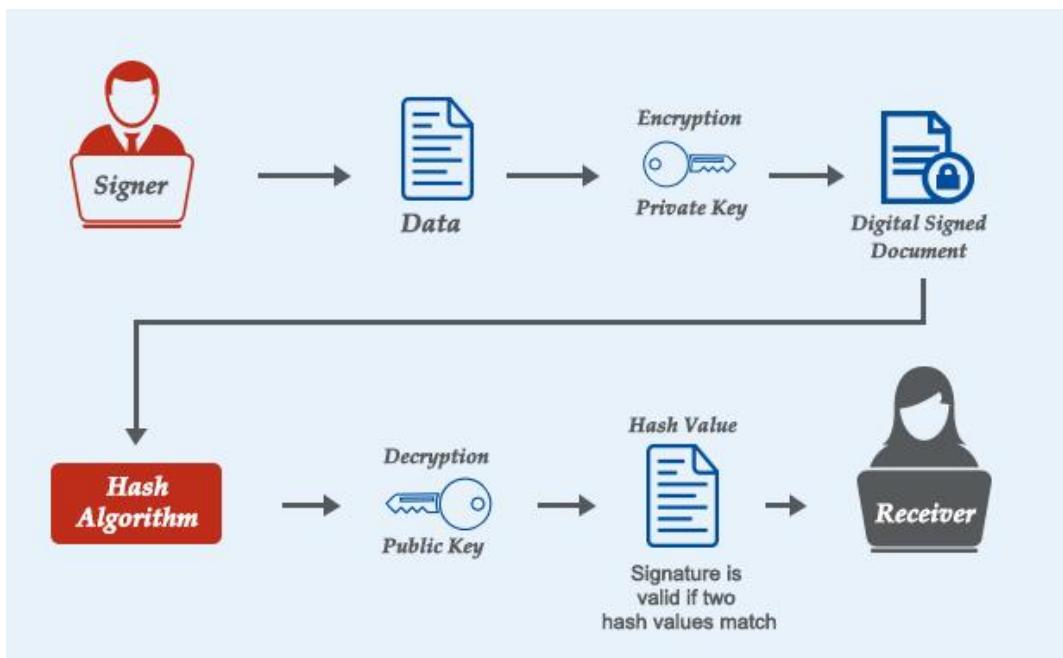
Server ကနေရလာတဲ့ public key ကို client ကလက်ခံရရှိပြီးတဲ့အခါ web server က digital signature ကို add လုပ်လိုက်ပါတယ်။ Web server က web pages တွေကို secure ဖြစ်စေဖို့အတွက်အောက်ပါအချက်တွေအတိုင်း လုပ်ဆောင်ပါတယ်။

- အရှင်ဆုံး Page ကို client's public key နဲ့ encrypt လုပ်ပါတယ်။
- အဲနောက်မှာတော့ page ကို hashing လုပ်ဆောင်ပါတယ်။
- Server ရဲ့ private key ကို hash နဲ့ encrypt လုပ်ပါတယ်။
- နောက်ဆုံးမှာတော့ Client က web page ကို ခေါ်တဲ့အခါ public key, hash နဲ့ page ကို client ထံသို့ပို့ဆောင်ပါတယ်။

အဲနောက် client အလှည့်ရောက်တဲ့အခါ

- Client က server ထံမှလာသမျှကို server public key ကိုအသုံးပြုပြီး hash တွေကို decrypt လုပ်ကာ verify လုပ်ဆောင်ပါတယ်။

- Client က data ကို decrypt လုပ်တဲ့အခါ သူရဲ့ private key ကို အသုံးပြုပြီးတော့ လုပ်ဆောင်တာဖြစ်ပါတယ်။ ဒီလိုလုပ်ဆောင်ပုံတွေ ကိုစာဖတ်သူနားလည်အောင် အောက်မှာပုံနဲ့တက္ကဖော်ပြပေးထားပါတယ်။



ဒါဆိုရင် စာဖတ်သူတွေအနေနဲ့ Digital Signatures ရဲ့အလုပ်လုပ်ဆောင်ပုံကို နားလည်မယ်လို့ထင်ပါတယ်။

## Digital Certificates

Digital Certificates ဆိုတာက public key certificate ကိုခေါ်တာဖြစ်ပါတယ်။ အဓိကအသုံးပြုတာကတော့ SSL (Secure Socket Layer) မှာ Web browser နဲ့ Web server ကြားထဲက connection ကို secure ဖြစ်ဖို့အတွက်အသုံးပြုတာဖြစ်ပါတယ်။ ဒုဥက္ခာပြင် digital certificate ကို public keys ကို sharing လုပ်ပြီး encryption နဲ့ authentication လုပ်ဖို့အတွက် အသုံးပြုတာဖြစ်ပါတယ်။ Digital certificates တဲ့မှာ public key ပါဝင်တဲ့အပြင် public key နဲ့သက်ဆိုင်တဲ့ အဖွဲ့စည်းရဲ့ information တွေ, digital certificate နဲ့ digital signature တို့နဲ့သက်ဆိုင်တဲ့ metadata တွေပါဝင် ပါတယ်။ Digital

certificates တွကိုဖြန့်ဝေခြင်း, မှန်ကန်ကြောင်းအတည်ပြုခြင်း, ဖျက်သီမ်းခြင်း တို့ဟာ PKI (Public key infrastructure) ရဲ့ အဓိကရည်ရွယ်ချက်ဖြစ်ပါတယ်။

## Public Key Infrastructure (PKI)

PKI ဆိုတာက users နဲ့ servers တွက secure ဖြစ်ဖို့အတွက် digital certificate ကိုအသုံးပြုပြီး data တွကို exchange လုပ်တဲ့ အခါအသုံးပြုရတဲ့ framework တစ်ခုဖြစ်ပါတယ်။ PKI ကိုအသုံးပြုရခြင်းက digital certificates တွကို distribute, manage, store နဲ့ revoke လုပ်ဆောင်ဖို့အတွက်အသုံးပြုတာဖြစ်ပါတယ်။ ကျွန်တော်တိုက secure ဖြစ်တဲ့ connection တစ်ခုကိုတည်ဆောက်လိုလျှင် PKI ကိုအသုံးပြုနိုင်ပါတယ်။ ဒုဥက္ခအပြင် PKI ကို secure e-mail transmissions, secure remote connection, secure remote network တို့အတွက်ပါအသုံးပြုနိုင်ပါတယ်။ PKI က users, client computers, servers, services စတာတွေကို encryption လုပ်ပြီးလွမ်းခြားထားတာဖြစ်ပါတယ်။ ဒါမူပေမယ့် PKI နဲ့ Public key encryption နဲ့မရောဖို့တော့လိုအပ်ပါတယ်။ ဒါပေမယ့် PKI က asymmetric key pairs, public key နဲ့ private key တို့ကို creates လုပ်ပေးပါတယ်။ Private key ကိုတော့သိမ်းထားဖို့လိုအပ်ပြီး public key ကိုတော့ distribute လုပ်လိုပါတယ်။ တစ်ကယ်လို့ keys ကို servers မှာ generate လုပ်တဲ့ အခါ centralized ဖြစ်ဖို့အတွက် ကိုစဉ်းစားဖို့လိုအပ်သလို public key ကို distributed လုပ်ဖို့လိုအပ်ပါတယ်။ Local system မှာအသုံးပြုဖို့ အတွက် Key pair ကို local computer မှာ generate လုပ်ခဲ့မယ်ဆိုရင်တော့ centralize ဖြစ်ဖို့လဲမလိုသလို key ကိုလဲ distribute လုပ်ဖို့လဲမ လိုအပ်ပါဘူး။ PKI ကို အတိုချုပြောရရင် public key နဲ့ user identities ကိုပေါင်းပြီး သတ်မှတ်ထားတာ ဖြစ်ပါတယ်။

## Certificate Authority

Certificate Authority (CA) ဆိုတာက digital certificates တွကို ရောင်းချ ပေးတဲ့ GoDaddy တို့လိုမျိုးအဖွဲ့စည်းတွေကိုပြောတာဖြစ်ပါတယ်။ တချို့ organization တွေကျတော့သူတို့ကိုယ်ပိုင် internal certificate တွေရှိပါတယ်။ CA

တွေက certificate တွေရောင်းချခြင်းအပြင် certificate server တွေကိုပါ manage လုပ်ဆောင်ရပါတယ်။ CA က user registration, identification နဲ့ validation processes တို့ကိုပါကိုင်တွယ်ရတာမျိုးတွေ လုပ်ရပါတယ်။

## Cryptographic Attacks

Cryptanalysis ဆိုတာက encryption ကိုတွေကိုဖောက်တဲ့နည်းပညာဖြစ်ပါတယ်။ ဒီသင်ခန်းစာမျာတော့ cryptographic attacks တွေနဲ့ပတ်သက်တာတွေကို လေ့လာရမှာဖြစ်ပါတယ်။ Cryptographic attacks ပါဝင်တာတွေကတော့

- Known-Plaintext Analysis (KPA)
- Chosen-Plaintext Analysis (CPA)
- Ciphertext-Only Analysis (COA)
- Man-In-The-Middle (MITM) attack
- Dictionary Attack
- Brute Force Attack (BFA)

တို့ပဲဖြစ်ပါတယ်။

### Known-Plaintext Analysis (KPA)

ဒီနည်းလမ်းမှာဆိုရင် attacker က ciphertext ထဲက တချို့အပိုင်းတွေရဲ့ plaintext ကိုသိနေပြီးသားဖြစ်ပါတယ်။ ဒါကြောင့် attacker က encryption key ကိုရှာဖွေဖို့လုပ်ဆောင်ရပါတယ်။ ဒီ attack ဟာဆိုရင်အရမ်းလွယ်ကူပြီး တော့ ရရှိထားတဲ့ information တွေကိုအသုံးပြုယုံပဲဖြစ်ပါတယ်။

### Chosen-Plaintext Analysis (CPA)

ဒီ attack မှာဆိုရင် attacker က random plaintext တွေကိုအသုံးပြုပြီးတော့ သက်ဆိုင်ရာ ciphertexts တွေနဲ့ encryption key ကိုရရှိအောင် လုပ်ဆောင်ရတဲ့နည်းလမ်းဖြစ်ပါတယ်။ သူကလဲ KPA လိုပဲရှိရှင်းပါတယ် ဒါပေမယ့် အောင်မြင်ဖို့နည်းလမ်းကတော့ အရမ်းနည်းပါတယ်။

## Ciphertext-Only Analysis (COA)

ဒီ attack အမျိုးစားက attacker က cipher-text တချို့ကိုသိထားဖို့လို အပ်ပြီး encryption key နဲ့ plaintext ကိုရှာဖွေရတာဖြစ်ပါတယ်။ ဒီနည်းလမ်း က ခက်ခဲ့တယ်ဆိုပေမယ့် ciphertext ပဲလိုအပ်တာကြောင့် အောင်မြင်နိုင်ခြား က တော့များပါတယ်။

## Man-In-The-Middle (MITM) attack

ဒီ attack မှာတော့ attacker က data/key ကို secure channel communication channel မှတစ်ဆင့် ကြေားဖြတ်ဖမ်းယူတာဖြစ်ပါတယ်။

## Dictionary Attack

ဒီ attack မှာဆိုရင် attacker က wordlist ကိုအရင် တည်ဆောက်ရပါတယ် အဲနောက် သူရရှိလာတဲ့ ciphertext ကို wordlist နဲ့တိုက်စစ်ပါတယ်။

## Brute Force Attack (BFA)

ဒီ attack မှာတော့ attacker က key ကိုရရှိအောင်လုပ်ဆောင်တဲ့ နည်းလမ်းဖြစ်ပါတယ်။ တစ်ကယ်လို့ key က 8 bits ဆိုရင်  $2^8$  ဆိုတော့ key က 256 ခုရရှိမှာဖြစ်ပါတယ်။ Attacker က ciphertext နဲ့ algorithm ကိုသိတယ် ဆိုရင်တော့ ရရှိထားတဲ့ keys တွေကိုအသုံးပြုပြီး တစ်ခုချင်းဆီနဲ့ decrypt လုပ်ကြည့်ယုံပဲဖြစ်ပါတယ်။ Key မြင့်လေ့ တိုက်ခိုက်ရတဲ့အချိန်ပိုကြာလေ့ဖြစ်ပါတယ်။

ဒါဆိုရင် စာဖတ်သူတွေအနေနဲ့ ဒီသင်ခန်းစာနဲ့ပတ်သက်ပြီးတော့ နားလည်မယ်လို့ မျှော်လင့်ပါတယ်။

## Chapter 9 – Dealing with Incidents

### Incident Response Concepts

Incident မှာဆိုရင် attack လုပ်ခံရတာတွေအပြင် system failure တွေပါပါဝင်ပါတယ်။ တချို့ concepts တွေကြတော့ policy တွေရေးဆွဲခြင်း၊ resources တွေကိုနေရာချထားရေး၊ Incident response team တွေကို ကျမ်းကျင်မှုရှိလာအောင်လေ့ကျင့်ပေးခြင်း၊ ဝန်ထမ်းတိုင်း responsibilities တွေကိုလိုက်နာလာအောင် train ပေးခြင်း စတဲ့ planning နဲ့ management functions တွေပါဝင်ပါတယ်။

Incident ဆိုတာ organization ကိုဆိုးကျိုးတွေဖြစ်စေနိုင်တဲ့ အပျက် သဘောဆောင်တဲ့ ဖြစ်စဉ်တွေကို ပြောတာဖြစ်ပါတယ်။ စာဖတ်သူတွေမြင်သာအောင် ဥပမာပေးရရင် Server Room မီးလောင်တယ်ဆိုရင် ဒါဟာ incident ပဲ၊ နောက် SQLi မှတစ်ဆင့် customers data တွေကိုပြုံးသွေ့က် company တွေရရှိသွားတယ်ဆိုရင် ဒါဟာ incident ဖြစ်ပါတယ်။

### Incident response procedures

Incident ဆိုတာက cyber attack ဒါမှုမဟုတ် systems failure ကြောင့်လက်တလော IT resource တွေကိုအသုံးပြုလိုမရတာကိုခေါ်တာဖြစ်ပါတယ်။ Incident အမျိုးစားတွေကအများကြီးရှိတဲ့အတွက် မတူညီတဲ့ incident response plan တွေကိုလို အပ်ပါတယ်။ စာဖတ်သူတွေမြင်သာအောင်ပြောရရင် DDoS တိုက်ခိုက်ခံရတယ်ဆိုရင် DDoS အတွက် response plan ကိုအသုံးပြုရမှာဖြစ်ပါတယ်။ Incident response အောင်မြင်ဖို့အတွက်ဆိုရင် အောက်ပါအချက်တွေကို လုပ်ဆောင် ဖို့လိုအပ်ပါတယ်။

- **Documented incident types:** Incident တွေနဲ့ပတ်သက်ပြီး response လုပ်ခဲ့တာတွေအဆင့်တိုင်းကို document တွေအနေနဲ့သိမ်းထားဖို့လို အပ်ပါတယ်။ အဲလို သိမ်းတဲ့အခါ categories တွေနဲ့သိမ်းဖို့လိုအပ်ပါတယ်။ ဥပမာ-
- Unauthorized access

- **Loss of computers or data**
- **Loss of availability**
- **Malware attack**
- **DDoS attack**
- **Power failure**
- **Natural disasters such as floods, tornados, hurricanes, and fires**
- **Cyber security incidents**

➤ **Roles and Responsibilities:** Incident Response Team တွေဖြစ်တဲ့အခါ Incident တွေကိုဖြေရှင်းဖို့လိုအပ်ပါတယ်။ အဲလို လုပ်ဆောင်တဲ့အခါ မတူညီတဲ့ roles တွေပါဝင်ပါတယ်။ အဲဒါတွေကတော့-

- **Incident Response manager:** A top level manager takes charge
- **Security analyst:** Technical support to the incident
- **IT auditor:** Check that the company is compliant
- **Risk analyst:** Evaluates all aspects of risk
- **HR:** Sometime employees are involved in the incident
- **Legal:** Gives advice and makes decision on legal issues
- **Public relations:** Deals with the press to reduce the impact

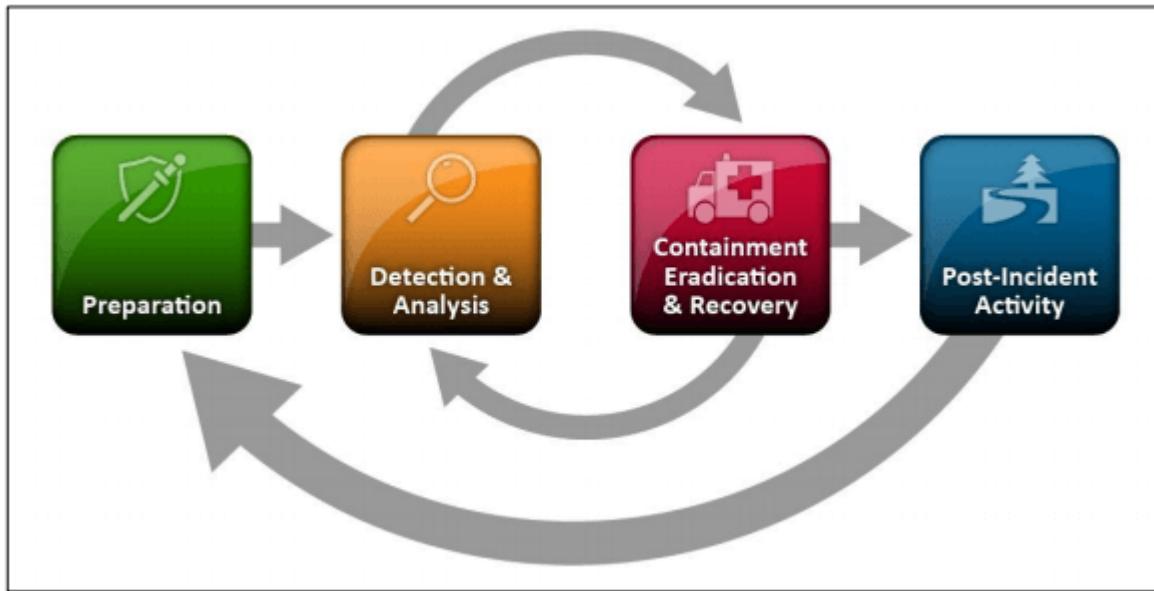
တို့ပဲဖြစ်ပါတယ်။

➤ **Reporting requirements/escalation:** Incident ဖြစ်တဲ့ ဖြစ်စဉ်ပေါ်မှုတည်ပြီး အထက်လူကြီးတွေကို report လုပ်ပေးရပါတယ်။ တစ်ကယ်လို့ customer ရဲ့ credit card information တွေခိုးခံရရင်တော့ ကျွန်တော်တို့တွေအနေနဲ့ customer တွေကိုအကြောင်းကြားတာမျိုးတွေ လုပ်ဆောင်သင့်ပါတယ်။ Incident response team တွေအနေနဲ့ incident နဲ့ပတ်သက်ပြီး response လုပ်မယ့်အစီစဉ်တွေကို ဖော်ဆောင်ဖို့လိုအပ်ပါတယ်။

- **Cyber incident response teams:** ယနေ့ခေတ်ကမ္မာကြီးမှာ cybercrime တွေက ပိုများပြားလာပါတယ်။ အဲလိုဖြစ်တဲ့ cybercrime တွေမှာ တချိုက ပိုက်ဆံတွေ ခိုးယူဖိုးအတွက်, တချိုက APT (Advanced Persistent threats) တွေကိုနဲ့ organization တွေကိုထိခိုက်အောင်လုပ်ဆောင်ကြတယ် စတဲ့ဖြစ်စဉ် များစွာရှုပါ တယ်။ အဲလိုဖြစ်စဉ်တွေ ဖြစ်လာခဲ့ရင် အဓိကလုပ်ဆောင်ရတာက Incident response team ကလုပ်ရတာဖြစ်ပါတယ်။ Incident Response team တွေကို incident တွေနဲ့ကြံလာတဲ့အခါ ဖြေရှင်းနိုင်ဖို့ training တွေပေး သင့်ပါတယ်။ ဒါအပြင် third-party specialist တွေငါးရမ်းပြီးတော့လဲ cybercrime တွေမဖြစ်ရ အောင် ကာကွယ်တာတွေလဲ လုပ်ဆောင်သင့်ပါတယ်။
- **Incident response exercises:** Organization တွေအနေနဲ့ incident response plan တွေခဲ့ပြီးတဲ့အခါ လက်တွေ့လေ့ကျင့်တာမျိုးတွေလုပ်ဆောင်သင့်ပါ တယ်။ အဲလိုလုပ်ဆောင်ထားမှသာ တစ်ကယ်ဖြစ်လာတဲ့အခါ အလွယ်တကူ ထိန်းချုပ်နိုင်မှာဖြစ်ပါတယ်။

## Incident Management

Incident Management ဆိုတာက threat ကို identifying, managing, recording နဲ့ analyzing လုပ်ဆောင်ရတာဖြစ်ပါတယ် တစ်ခါတစ်လေ Incident ဖြစ်နေစဉ်မှာလဲ လုပ်ဆောင်ရတာမျိုးတွေရှိတက်ပါတယ်။ အဲလိုတွေ လုပ်ဆောင်ခြင်း က IT infrastructure ထဲမှာ လုခြံရေးဆိုင်ရာအားနည်းချက်တွေကို တွေ့ရှိလာအောင် လုပ်ဆောင်ပေးပါတယ်။ Security Incident မှာဆိုရင် system တွေထဲကို ဝင်ရောက် တိုက်ခိုက်နိုင်ခြင်းမှ data တွေကိုပေါက်ကြားစေခြင်းထိကိုဖြစ်စေနိုင်ပါတယ်။ Security Incident မှတစ်ဆင့် health, financial, social security numbers နဲ့ personal data တွေကိုရရှိသွားနိုင်စေပါတယ်။ Incident ဖြစ်လာတဲ့အခါ ပြန်လည် တုန်ပြန်ဖို့အတွက် National Institute of Standards and Technology (NIST) ကနေထုတ်ပြန်ထားတဲ့ Incident Response lifecycle ရှိပါတယ်။ အဲဒါကိုအောက်မှာ ဖော်ပြပေးထားပါတယ်။



## Incident Response

Incident တွက အစရိတ်လုပ်ပါတယ် ပြီးတော့ အစနဲ့ အဆုံးကြားထဲမှာမတူညီတဲ့ အဆင့်တွေရှိတဲ့အတွက် အဲအဆင့်တိုင်းမှာလဲမတူညီတဲ့ response process တွေရှိပါတယ်။ Incident Response မှာဆိုရင်လုပ်ဆောင်ရမယ့် အဆင့် (၄) ဆင့်ရှိပါတယ်။ အဲဒါတွကတော့-

- 1) Preparation
- 2) Detection and Analysis
- 3) Containment, Eradication, and Recovery
- 4) Post-Incident Activity

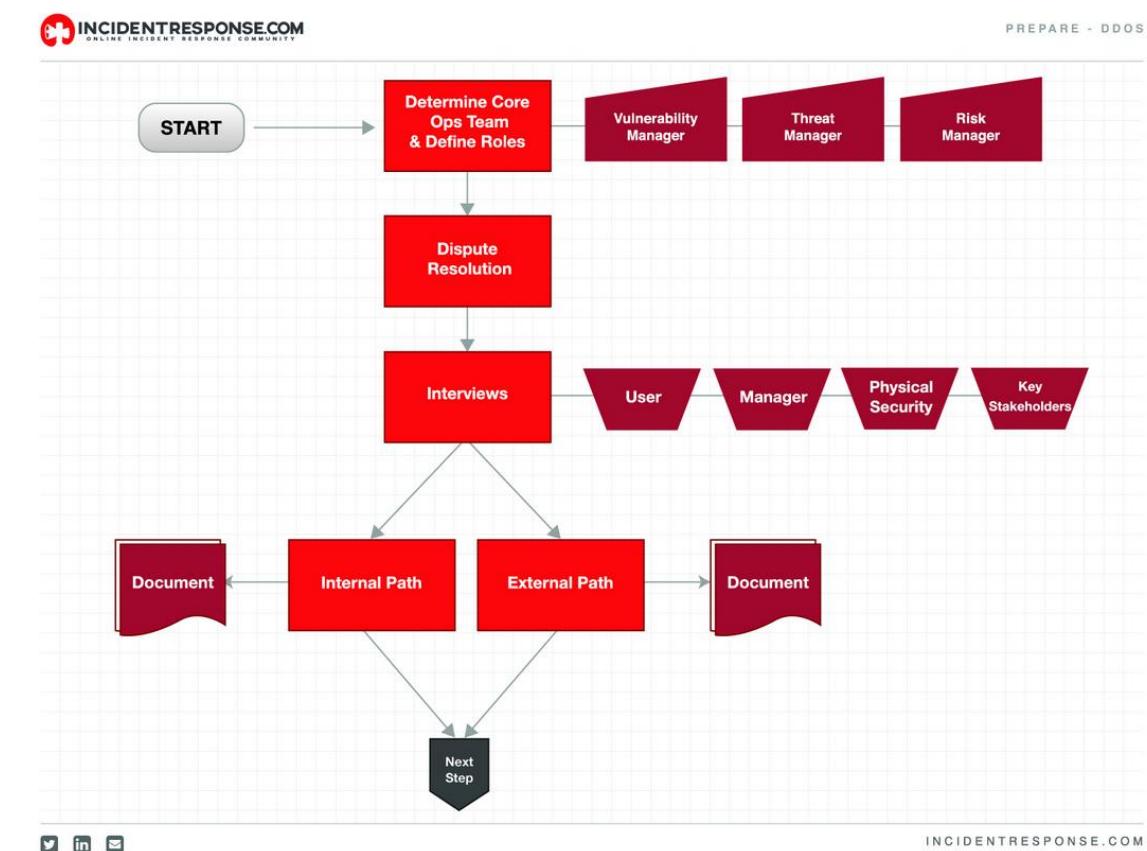
အသေးစိတ်ကိုအောက်မှာဆက်ပြီးလေ့လာကြည့်ရအောင်။

### 1) Preparation

Incidents မဖြစ်ခင်မှာကျန်တော်တို့တွေအနေနဲ့ networks, server and endpoints စတဲ့ assess တွေကို list တွေနဲ့လုပ်ဆောင်ထားဖို့လိုအပ်ပါတယ်။ ပုံမှန်အခြေနေတွေမှာလဲ monitoring လုပ်ဆောင်သင့်ပါတယ်။ Security တွေနဲ့သက်ဆိုင်တဲ့ ဖြစ်စဉ်တွေကိုသေချာစုစုမေးစစ်ဆေးဖို့လိုအပ်ပြီး incidents တစ်ခုခြင်းစီအတွက် response လုပ်ရမယ့်အဆင့်တွေကို

သေချာလုပ်ဆောင်ထားဖို့လိုအပ်ပါတယ်။ အဲလိုလုပ်ဆောင်တာကိုတော့ incident response playbook လုပ်တယ်လို့ခေါ်ပါတယ်။ Playbook ဆိုတာ က attack တစ်ခုက DDoS attack ပဲထားပါတော့ ကျွန်တော်တို့ အတိုက် ခံရပြီဆိုရင် လုပ်ဆောင်ရမယ့်အဆင့်မျိုးတွေပါဝင်တာကို Playbook လို့ခေါ်ပါတယ်။ နူးနာအနေနဲ့ simple Playbook တစ်ခုကိုအောက်မှာဖော်ပြထားပါတယ်။ တစ်ကယ်လိုစာဖတ်သူတွေအနေနဲ့ Playbook တွေကို လေ့လာချင်တယ်ဆိုရင်တော့အောက်မှာဖော်ပြထားတဲ့ link မှာ လေ့လာနိုင်ပါတယ်။

<https://www.incidentresponse.com/playbooks/>



အပေါ်မှာကျွန်တော်ဖော်ပြခဲ့တာတွေအပြင် preparation phases မှာ Endpoint protection, Malware protection, Network security စိတ် security controls တွေကိုပါပြင်ဆင်ထားဖို့လိုအပ်ပါတယ်။ အခုကျွန်တော်ဖော်ပြခဲ့တာတွေကတော့ Phase 1 မှာလုပ်ဆောင်ထားရမှာတွေဖြစ်ပါတယ်။

## 2) Detection and Analysis

Detection မှာဆိုရင် IT systems, security tools တွေနဲ့ အဖွဲ့စည်းတွင်း နှင့် ပြည်ပလူများထံမှာရရှိသော အချက်လက်များအရ တရို့နဲ့ချို့နဲ့မှာ attack ဖြစ်ပွားနိုင်ခြင်း နှင့် လက်ရှုံးချို့နဲ့တွင် attack တွေဖြစ်ပွားနေခြင်း စတဲ့ အချက်လက် တွေပါဝင်ပါတယ်။

Analysis မှာဆိုရင်တော့ system ကိုသက်ရောက်နိုင်တဲ့ လုပ်ဆောင်မှုတွေ ကိုစစ်ဆေးတာဖြစ်ပါတယ်။ အဲလိုစစ်ဆေးတဲ့အခါ ပုံမှန်ဖြစ်စဉ်တွေကိုပါ စစ်ဆေးဖို့လိုအပ်ပါတယ်။

## 3) Containment, Eradication, and Recovery

Containment ဆိုတာက resource တွေထိခိုက်မှုတွေပို့ပြင်းမထန်လာခင်မှာ attack တွေကိုရပ်တန်အောင်လုပ်ဆောင်ရတာဖြစ်ပါတယ်။ ကျွန်တော်တို့ ရေးဆွဲမယ့် containment strategy က incident ဖြစ်တဲ့ ထိခိုက်မှုပေါ်မှာ မူတည်တာဖြစ်ပါတယ်။ ဒါအပြင် ဝန်ထမ်းတွေ နဲ့ ဖောက်သည်တွေအတွက် အရေးကြီးတဲ့ services တွေကိုထိခိုက်သွားတဲ့အခါ ပြန်အသုံးပြုရနိုင်ရေး အတွက် temporary solution ဒါမှမဟုတ် permanent solution တွေကိုလဲ ပြင်ဆင်ထားသင့်ပါတယ်။ နောက် containment ရဲ့အရေးပါတဲ့အပိုင်းက တော့ attack ဖြစ်သွားတဲ့အခါ attack လုပ်တဲ့ host နဲ့ IP address ကို သေချာစီစစ်အတည်ပြုဖို့ကလဲအရေးကြီးပါတယ်။ အဲလိုသိထားတဲ့အခါ attacker ကလာရောက်ချိတ်ဆက်တဲ့ connection ကိုကျွန်တော်တို့ဘက်က နေ block လုပ်ဆောင်နိုင်မှာဖြစ်ပြီး threat actor ကိုလဲသိရှိနိုင်မှာဖြစ်ပါတယ်။

Eradication and Recovery အဆင့်မှာဆိုရင် incident ဖြစ်ပွားတာကို တားမြစ်နိုင်ပြီးတဲ့နောက်မှာတော့ ကျွန်တော်တို့တွေအနေနဲ့ တိုက်ခိုက်ခံရတဲ့ host တွေကိုခဲ့ခြားခြင်း, malware တွေကို remove လုပ်ခြင်း နဲ့ ပေါက်ကြား သွားတဲ့ user accounts တွေရဲ့ passwords တွေကိုပြန်လည်သတ် မှတ်ခြင်း စတာတွေ လုပ်ဆောင်သင့်ပါတယ်။

နောက်ဆုံးမှာတော့ threat threat တွေကိုဖယ်ရှားပြီးသည်နှင့် systems တွေကို ပုံမှန် အတိုင်းပြန်လည်ပတ်မှုများကို မြန်မြန်လုပ်ဆောင်ပြီး နောက် attack တွေမထပ်ဖြစ်အောင်ဆောင်ရွက်ခြင်းတွေ လုပ်ဆောင်ရပါတယ်။

#### 4) Post-Incident Activity

NIST ရဲ့ incident response methodology မှာအဓိကအပိုင်းကတော့ incident ဖြစ်ခဲ့ဘူးတာတွေကိုသင်ခန်းစာယူပြီး ပိုမိုတိုးတက်လာစေခြင်းပဲ ဖြစ်ပါတယ်။ စာဖတ်သူတွေမြင်သာအောင်ပြောရရင် DDoS attack တိုက်ခံရ တဲ့အခါ priority level မြင့်နေရင် အဲဒါကို containment strategy ကိုအသုံး ပြုပြီးရပ်တန်အောင်လုပ်ဆောင်လို့ရပါတယ်။ ဒါပေမယ့် အဲ strategy က same level မှာပဲအသုံးဝင်မှာဖြစ်ပြီး သူ့ထပ်မြင့်တဲ့ level တွေကြောင်တော့ အသုံးမဝင်တော့ပါဘူး။ အဲအခါ ကျွန်ုတ်တို့တွေအနေနဲ့ တခြား level တွေ အတွက်ကိုပါကြိုပြီးတော့ပြင်ဆင်ထားသင့်ပါတယ်။

#### Understanding the basic concepts of forensics

Forensics ဆိုတာက ရဲ့ တွေက အမှုတစ်ခုကိုစစ်ဆေးတဲ့အခါမှာအသုံးပြုတာ ဖြစ်ပြီး အဲအတွက်သက်သေအထောက်ထားတွေများစွာလို့အပ်ပါတယ်။ ကျွန်ုတ်တို့ တွေအနေနဲ့ computer နဲ့ web-based အတိုက်ခိုက်ရတယ်ဆိုပါစို့။ အဲအခါ မတူညီတဲ့ components တွေပါဝင်ပြီး တစ်ခုစီကိုအောက်မှာဖော်ပြပေးထားပါတယ်။

➤ **Order of volatility:** Order of volatility ဆိုတာက incident ဖြစ်တဲ့အခါ ပျက်စီးဆုံးသူးတဲ့ အထောက်ထားတွေကိုရှာဖို့ဖြစ်ပါတယ်။ ကျွန်ုတ်တို့က လုံလောက်တဲ့သက်သေအထောက်ထားတွေကိုမရရှိသေးပဲ attack တွေကို ရပ်တန်အောင်မကြိုးစားပါဘူး အဲလိုလုပ်ဆောင်မှသာလျှင် တိကျတဲ့ source တွေကိုရှာဖွေနိုင်မှာဖြစ်ပါတယ်။ အဲလိုလုပ်ဆောင်တာတွေကို order of volatility လိုခေါ်ပါတယ်။

- **Example 1 – Web-based attack:** Attacker က company website တွေကိုတို့က်ခိုက်နေပြုဆိုပါက Security Team တွေက network traffic

တွကို capture လုပ်ပြီး attack source ကိုအရင်ဆုံးရှာပါတယ်။ အဲဒါကိုသက်သေရှာတယ်လိုဆိုပါတယ်။

- **Example 2-attack inside a computer:** တစ်စုံတစ်ယောက်က ကျွန်တော်တို့ computer ကို attack လုပ်ပြုဆိုပါက ကျွန်တော်တို့အနေနဲ့သက်သေရဖို့အတွက် capture လုပ်ဖို့လိုအပ်ပါတယ်။ အဲလို လုပ်ဆောင်တဲ့အခါ အောက်မှာ ဖော်ပြထားတဲ့အချက်တွကို စစ်ဆေးဖို့လိုအပ်ပါတယ်။
  - **CPU cache:** Memory ကိုထိခိုက်စေမယ့် CPU ရဲ့အသုံးပြုမှုတွကိုတားစီးဖို့အတွက် CPU cache တွကိုစစ်ဆေးဖို့လိုအပ်ပါတယ်။
  - **Random Access Memory (RAM):** Memory ကိုအသုံးပြုနေတဲ့ application တွကိုလဲဖော်ထုတ်ဖို့လဲလိုအပ်ပါတယ်။
  - **Swap/page file:** Swap ဆိုတာက virtual memory ဖြစ်ပြီး application တွက memory ပေါ်မှာနေရာလွတ်မရှိတော့တဲ့အခါ swap ကိုအသုံးပြုတက်ကြပါတယ်။ ဒုက္ခာင့် swap ကိုပါစစ်ဆေးဖို့လိုအပ်ပါတယ်။
  - **Hard drive:** Hard drive ထဲမှာ store လုပ်ထားတဲ့ data တွကိုလဲပြန်လည်စစ်ဆေးဖို့လိုအပ်ပါတယ်။

အခုကျွန်တော်ဖော်ပြသွားတာတွကတော့ Order of volatility နဲ့သက်ဆိုင်တဲ့ ဥပမာတွေဖြစ်ပါတယ်။

- **Chain of custody:** Chain of custody ဆိုတာက ကျွန်တော်တို့သက်သေတွေရရှိပြီးတဲ့အခါ အဲသက်သေတွကို ဘယ်သူကအကြာကြီး ထိန်းသိမ်းခဲ့လဲဆိုတာကိုစစ်ဆေးတာဖြစ်ပါတယ်။ ဒီသဘောတရားကို စာဖတ်သူတွေမြင်သာအောင်ပြောရရင် A ဆိုတဲ့လူက 1 Gb ရှိတဲ့ data ကိုအကြာကြီးထိန်းသိမ်းခဲ့တယ်ဆိုပါစို့။ နောက် အဲ data တွကို B ဆိုတဲ့လူကိုလွှဲပြောင်းလိုက်တဲ့အခါ 1.5 Gb ဖြစ်

သွားတယ် ဆိုရင် ကျွန်တော်တို့အနေနဲ့ data တွေကို investigate လုပ်ဖို့လိုအပ်ပါတယ်။ ဒါကို chain of custody လိုခေါ်ပါတယ်။

- **Legal hold:** Legal hold ဆိုတာက သက်သေအထောက်ထားနဲ့ သက်ဆိုင်တဲ့ documents တွေမဆုံးရှုံးအောင် ထိန်းသိမ်းရတာဖြစ်ပါတယ်။
- **Data acquisition:** သက်သေတွေကို USB flash drives, cameras နဲ့ computers တွေမှတစ်ဆင့် ရယူတာဖြစ်ပါတယ်။
- **Record time offset:** ကျွန်တော်တို့သက်သေတွေကို computer မှရယူတဲ့အခါ အချိန်ကိုမှတ်တမ်းတင်ထားဖို့လိုအပ်ပါတယ်။
- **Forensic copy:** ကျွန်တော်တို့က analyze လုပ်တဲ့အခါ data တွေကို remove လုပ်ဖို့လိုအပ်လာတဲ့အခါ ဒီအတိုင်း remove မလုပ်ပဲ copy လုပ်ပြီး original data တွေကိုသိမ်းထားသင့်ပါတယ်။ အဲနောက်မှ copy ကို analyze လုပ်သင့်ပါတယ် ဒါမှာ original data တွေကမပြောင်းလဲပဲရှုံးမှာဖြစ်ပါတယ်။ အဲလိုလုပ်ဆောင်တာကို Forensic copy လိုခေါ်ပါတယ်။
- **Capture system image:** Forensic လုပ်တဲ့အခါ Laptop ဒါမှမဟုတ် Desktops ကိုလုပ်ဆောင်ဖို့လိုအပ်ပြီဆိုရင်တော့ system image တစ်ခုအရင်ရယူဖို့လိုအပ်ပါတယ်။ အဲနောက် original image ကိုသိမ်းထားပြီးတော့ criminal နဲ့သက်ဆိုင်တဲ့ activity တွေကို analyzed လုပ်ပြီးသက်သေရှာသင့်ပါတယ်။
- **Screenshots:** Desktops ပေါ်မှာရှိနေတဲ့ applications ဒါမှမဟုတ် viruses တွေကိုသက်သေအဖြစ်သိမ်းထားဖို့ screenshots တွေရှိက်ထားဖို့လိုအပ်ပါတယ်။
- **Taking hashes:** Forensic copy ဒါမှမဟုတ် system image တွေကို စစ်ဆေးတဲ့အခါ hashed တွေကိုအရင်ဆုံးထုတ်ထားဖို့လိုအပ်ပါတယ်။ Investigation လုပ်ပြီး တဲ့အခါ hash value တွေကိုပြန်ပြီးစစ်ကြည့်ဖို့ လိုအပ်ပါတယ်။ တစ်ကယ်လို့ investigation လုပ်နေစဉ်မှာ အမှုစစ်က တစ်ခုခုမှားလုပ်မိပြီလိုထင်တဲ့အခါ data ကို re-hashes ပြန်လုပ်ဖို့လိုအပ်ပါတယ်။

- **Network traffic and logs:** Web-based ဒါမှုမဟုတ် remote attack တွကို investigation လုပ်တဲ့အခါ attack ကိုမရပ်တန်ခင်မှာ network traffic တွကို capture လုပ်ဖို့လိုအပ်ပါတယ်။ အဲလိုလုပ်ဆောင်ခြင်းဟာ attack ရဲ့ source ကိုသိနိုင်မှာဖြစ်ပါတယ်။ ဒုအပြင် Firewall, NIPS, NIDS တွေထဲက log files တွကိုစစ်ဆေးသင့်ပါတယ်။ တစ်ကယ်လို့ SIEM ကိုအသုံးပြုထားတယ်ဆိုရင် တော့ attack တွေရဲ့ပုံးစွမ်းတွေကိုပါတွေ့မြင်ရမှာဖြစ်ပါတယ်။
- **Capture video:** တချို့သော attack တွေမှာဆိုရင် attack က office ကို ကျူးကျော်ဝင်ရောက်တဲ့ဖြစ်စဉ်မျိုးတွေရှုပါတယ်။ အဲလိုဖြစ်စဉ်တွေမှာဆိုရင် CCTV ကနေမှုတစ်ဆင့် attack ကိုဖော်ထုတ်နှင့်ပြီး ဘယ်အချိန်မှာ attack ကို စတင်လုပ်ဆောင်တယ်ဆိုတာကိုပါဖော်ထုတ်နှင့်မှာဖြစ်ပါတယ်။

အခုကျွန်ုံးတော်ဖော်ပြပေးသွားတဲ့ အချက်တွေကတော့ Forensic လုပ်ဆောင်တဲ့အခါ အသုံးပြုရမယ့် နည်းလမ်းတချို့ပဲဖြစ်ပါတယ်။

## Backup utilities

ကျွန်ုံးတော်တို့တွေအနေနဲ့ data တွေကို backup လုပ်ခြင်းဟာ အရမ်းအရေးပါပါတယ်။ Incident တစ်ခုခုကြောင့် systems fail ဖြစ်သွားတဲ့အခါ data တွေကို backup လုပ်ထားတဲ့အတွက် အဆင်ပြုမှာဖြစ်ပါတယ်။ Backup လုပ်ဖို့အတွက်ဆိုရင် နည်းလမ်းတွေကတော့ အများကြီးရှိပါတယ်။

- **Creating a snapshot**
- **Network location**
- **Backing up to tape**

တစ်ခုခြင်းအကြောင်းကို အောက်မှာဆက်ပြီးတော့ ဖော်ပြပေးထားပါတယ်။

## Creating a snapshot

ကျွန်တော်တို့ virtualization ကိုအသုံးပြုထားတယ်ဆိုရင် snapshot ကိုအသုံးပြုနိုင်ပါတယ်။ Snapshot လုပ်ဆောင်ထားခြင်းဖြင့် အကြောင်း တစ်ခု ခုကြောင့် Virtual Machine fail ဖြစ်သွားခဲ့သော် မူလအတိုင်းပြန်ဖြစ် အောင် လုပ်ဆောင်နိုင်ပါတယ်။

## Network location

ဒါတော့ backup လုပ်ထားတဲ့ data တွေကို fire share ကနေမှတစ်ဆင့် network ထဲက server ပေါ်မှာ backup လုပ်ဆောင်နိုင်ပါတယ်။ အဲလို့ backup အတွက်အသုံးပြုမယ့် server တွေကို redundancy အတွက် RIAD ကို setup လုပ်ထားသင့်သလို အဲလို့မှုမဟုတ် SAN storage ကိုအသုံးပြုနိုင်ပါတယ်။

## Backing up to tape

Magnetic tape ကိုအသုံးပြုပြီးတော့ data တွေကို backup လုပ်ဆောင် နိုင်ပါတယ် ဒါပေမယ့် အားနည်းချက်တော့ restore လုပ်တဲ့အခါ အချိန်တော့ပို့ကြာပါတယ်။

## Backup types

Backup အမျိုးစားတွေကိုအောက်မှာဖော်ပြပေးထားပါတယ်။

### Full backup

Full backup ဆိုတာက data တွေအကုန်လုံးကို backup လုပ်တာဖြစ်ပါတယ်။

### Incremental

Incremental ကိုအသုံးပြုပြီး backup လုပ်မယ်ဆိုရင် last full backup အမှုမဟုတ် last incremental ကိုအသုံးပြုနိုင်ပါတယ်။ Incremental backup လုပ်ဖို့အတွက်ဆိုရင် full backup အရင်လုပ်ထားဖို့လို့အပ်ပါတယ်။

## Differential

Differential backup ဆိုတာက last full backup လုပ်ပြီးသွားတဲ့အခါ အရန်အနေနဲ့ ထပ်ပြီးတော့ လုပ်တဲ့ backup type ဖြစ်ပါတယ်။ ဒါပေမယ့် ပြဿနာတစ်ခုက ကျေန်တော်တို့က full backup ကိုတစ်ပတ်တစ်ခါ လုပ်တယ် ဆိုရင် differential backup ကိုနေ့စွဲလုပ်ပေးရတာဖြစ်တာကြောင့် တဖြည်း ဖြည်း ပိုများလာပါတယ်။

စာဖတ်သူတွေအနေနဲ့ယခုစာအုပ်အား ဖတ်ပြီးပါက Cyber Security နဲ့ပတ်သက်ပြီး လိုအပ်တဲ့ အခြေခံသဘောတရားတွေကိုနားလည်လိမ့်မယ်လို့မျှော်လင့်ပါတယ်။ အောက်မှာတော့ Cyber Security အတွက်သိထားသင့်တဲ့ Certification Road Map ပုံကိုထည့်ပေးထားပါတယ်။ ပုံကတော့ Online ကနေကူးယူဖော်ပြထားခြင်းဖြစ်ပါတယ်။

