

မာတိကာ		
CHAPTER 1: Pen-Test Machine Install ပြုလုပ်ခြင်း		
Sr#	Description	Page
1.1.	Kali Linux ကို Install ပြုလုပ်ခြင်း	19-34
CHAPTER 2: လေ့ကျင့်ရေးကွင်း တည်ဆောက်ခြင်း		
Sr#	Description	Page
2.1.	လက်တွေ့ လေ့ကျင့်ရန်အတွက် တရားဝင် Lab တည်ဆောက်ခြင်း	35-50
CHAPTER 3: သိမှတ်ထားသင့်သော Terminal Command များနှင့် Bash Shell အကြောင်း		
Sr#	Description	Page
3.1.	အသုံးဝင်သော Linux command များကို လေ့လာခြင်း	52
3.1.1.	Locate	52
3.1.2.	Which	52
3.1.3.	Find	54
3.2.	Kali Linux မှာရှိတဲ့ Service များအကြောင်း	54
3.3.	Service Management အကြောင်း	57
3.4.	Service Boot Persistence	59
3.5.	Bash Shell	59
3.5.1.	Basic Knowledge for Bash Shell	59
3.5.2.	ပထမဆုံး Bash Program ဖန်တီးခြင်း	60
3.5.3.	ဒုတိယမြောက် Bash Program	63
3.5.4.	တတိယမြောက် Bash Program	64
3.6.	Grep အကြောင်း	65
3.7.	Domain နှင့် Sub=Domain IP များရှာဖွေခြင်း နှင့် Bash Script	67
3.8.	Network အတွင်းရှိ Live Host IP များကို ရှာဖွေခြင်း	76
CHAPTER 4: Penetration-Testing အတွက် လိုအပ်သော Tool များ		
Sr#	Description	Page
4.1.	Kali Linux ကို Install ပြုလုပ်ခြင်း	83
4.1.1.	NetCat	83
4.2.	TCP & UDP Port များနှင့် ချိတ်ဆက်ခြင်း	86
4.3.	NetCat နှင့် ဖိုင်များ ပေးပို့သယ်ယူခြင်း	93

6.11.	SMB Enumeration	182
6.12.	Net BIOS Service ကို Scan ဖတ်ခြင်း	183
6.13.	Null Session Enumeration	184
6.14.	Nmap SMB NSE Scripts	186
6.15.	SMTP Enumeration	189
6.16.	SNMP Enumeration	192
CHAPTER 7: အားနည်းချက်များ ရှာဖွေသတ်မှတ်ခြင်း		
Sr#	Description	Page
7.1.	Vulnerabilities Scanning	195
7.2.	Nmap ကို အသုံးပြုပြီး Vulnerabilities ရှာဖွေခြင်း	195
7.3.	Open VAS ကို သုံးကြည့်ခြင်း	198
CHAPTER 8: Buffer Overflow		
Sr#	Description	Page
8.1.	Buffer Overflow မိတ်ဆက်	207
8.2.	DEP & ASLR	209
8.3.	Buffer Overflow Exploit	210
8.4.	Buffer Overflow (နမူနာ ၂)	227
8.5.	Buffer Overflow (နမူနာ ၃)	236
8.6.	Shell ရယူခြင်း	262
CHAPTER 9: Exploit များနှင့် လုပ်ဆောင်ခြင်း		
Sr#	Description	Page
9.1.	Exploit များနှင့် မိတ်ဆက်ခြင်း	264
9.2.	Kali မှာရှိတဲ့ Exploit များကို ရှာဖွေခြင်း	265
9.3.	အင်တာနက်မှတစ်ဆင့် Exploit ရှာဖွေခြင်း	266
9.4.	Exploit များကို စိတ်ကြိုက်ပြင်ဆင်ခြင်း	267
9.5.	Exploit အတွက် Development Environment တည်ဆောက်ခြင်း	268
9.6.	Exploit Code Language များ	269
9.7.	Shell Code များကို ပြုပြင်ခြင်း	269
9.7.1.	Exploit-db 643.c	270
9.7.2.	Exploit-db 646.c	274

CHAPTER 10: ဖိုင်များပေးပို့ခြင်း		
Sr#	Description	Page
10.1.	မိတ်ဆက်	277
10.2.	Anti-Virus များနှင့်တွေ့ဆုံခြင်း	277
10.3.	အပြန်အလှန်သက်ရောက်မှုမရှိသော Shell များ	278
10.4.	TFTP နှင့် ဖိုင်များတင်ပို့ခြင်း	280
10.5.	FTP ကိုသုံးပြီး ဖိုင်များ Upload တင်ပို့ခြင်း	282
10.6.	Scripting Language များသုံးပြီး File Upload တင်ပို့ခြင်း	285
10.6.1.	VBS Script မြင့် File Upload ပြုလုပ်ခြင်း	285
10.6.2.	PowerShell မြင့် File Upload ပြုလုပ်ခြင်း	287
10.7.	Debug သုံးပြီး ဖိုင်များကူးပြောင်းခြင်း	289
CHAPTER 11: လုပ်ပိုင်ခွင့် တိုးမြှင့်ရယူခြင်း		
Sr#	Description	Page
11.1.	Privilege Escalation ဆိုတာ	292
11.2.	Linux မှာ Local Privilege Escalation Exploit အသုံးပြုခြင်း	292
CHAPTER 12: Client-Side Attack		
Sr#	Description	Page
12.1.	Client-Side Attack ဆိုတာ	301
12.2.	Passive Client Information Gathering	302
12.3.	Active Client Information Gathering	302
12.4.	Social Engineering & Client Side Attack	303
12.6.	Client-Side Exploit တည်ဆောက်ခြင်း	305
12.6.	Java Signed Applet Attack	308
CHAPTER 13: Web Application Attack များအကြောင်း		
Sr#	Description	Page
13.1.	Web Application Attack မိတ်ဆက်	312
13.2.	Cross Site Scripting (XSS)	312
13.3.	Reflected XSS attack	314
13.4.	Attacking Session Cookie	316
13.5.	Persistence XSS (or) Stored XSS	316
13.6.	လိပ်စာပြောင်းညွှန်ခြင်းနှင့် iFrame ထည့်သွင်းခြင်း	320
13.7.	Cookie များနှင့် Session Information များကို ခိုးယူခြင်း	322

13.8.	Fule Inclusion Vulnerabilities	325
13.9.	Local File Inclusion (LFI)	326
13.10.	Contamination Log File	328
13.11.	LFI မှ Code Execution သို့	329
13.12.	Remote File Inclusion (RFI)	330
13.13.	MySQL နှင့် SQL Injection	331
13.13.1.	SQL Injection in DVWA (Low Level Security)	333
13.13.2.	SQL Injection in DVWA (Medium Level Security) & Burp Suite Beginning	336
13.13.3.	SQL Injection in DVWA (High Level Security)	343
13.13.4.	Blind SQL Injection & SQL Map	345
CHAPTER 14: Password Attack များကို လေ့လာခြင်း		
Sr#	Description	Page
14.1.	Brute-force Attack အတွက် ပြင်ဆင်ခြင်း	350
14.1.1.	Password Dictionary File ဆိုတာ	350
14.1.2.	Key-space Brute-force	351
14.2.	Pwdump နှင့် Fgdump အကြောင်း	353
14.3.	Windows Credential Editor(WCE)	354
14.4.	John, The Ripper	355
14.5.	Password Profiling	356
CHAPTER 15: Online Password Attack များနှင့် Password Cracking Tool များအကြောင်း		
Sr#	Description	Page
15.1.	Online Password Attack ဟူသည်	358
15.2.	Hydra ကို လေ့လာခြင်း	358
15.3.	Medusa ကို လေ့လာခြင်း	361
15.4.	သတိထားရမယ့် Account Lookup နဲ့ Log Alert များအကြောင်း	362
15.5.	မှန်ကန်သော Protocol ရွေးချယ်ခြင်း	363
15.6.	Password Hashes Attack များအကြောင်း	363
15.6.1.	Password Cracking	364
15.7.	Rainbow Table များကိုလေ့လာခြင်း	365

CHAPTER 16: Port Redirecting & Tunneling		
Sr#	Description	Page
16.1.	Port Redirect နဲ့ Tunnel အကြောင်း	367
16.2.	Port Forwarding / Redirecting	367
16.3.	SSH Tunneling အကြောင်း	369
16.3.1.	Local Port Forwarding	370
16.3.2.	Remote Port Forwarding	371
16.4.	Dynamic Port Forwarding	371
16.5.	HTTP Tunneling	372
CHAPTER 17: Metasploit Framework ကို လေ့လာခြင်း		
Sr#	Description	Page
17.1.	Metasploit Framework	375
17.2.	User Interfaces	375
17.3.	MSF Syntax များကို လေ့လာခြင်း	378
17.3.1.	Auxiliary Modules	378
17.4.	FTP Brute-force	384
17.5.	Metasploit Database Access	385
17.6.	Exploit Modules	387
17.7.	Metasploit Payloads	390
17.7.1.	Staged & Non-Staged Payloads	390
17.7.2.	Meterpreter Payloads	391
17.7.3.	Meterpreter Command များကို လေ့လာခြင်း	392
CHAPTER 18: Anti-Virus များကို ကျော်ဖြတ်ခြင်း နှင့် VIM		
Sr#	Description	Page
18.1.	Anti-Virus ဟူသည်	400
18.2.	Payload ကို Encode ပြုလုပ်ခြင်း	402
18.3.	VIM ကို လေ့လာခြင်း	403

CHAPTER 19: Android Hacking		
Sr#	Description	Page
19.1.	နိဒါန်း	406
19.2.	ဥပမာ -၁ (Local Area Network)	406
19.3.	ဥပမာ -၂ (Wide Area Network)	409
19.4.	ဥပမာ -၃	409
CHAPTER 20: နိဒါးချုပ်စည်းရေးခြင်း		
Sr#	Description	Page
20.1.	အချက်အလက် စုဆောင်းရယူခြင်း	414
20.2.	Scan ပြုလုပ်ခြင်း	415
20.3.	Exploit ပြုလုပ်ခြင်း	419
20.4.	Privilege Escalation နှင့် Backdoor ထည့်သွင်းခြင်း	420
20.5.	VPN အသုံးပြုခြင်း	427
20.6.	လက်တွေ့ လေ့ကျင့်ရေးများ	431
Grade 3 Hacking "Hacking ဒုတိယတန်း" စာအုပ်အတွက် ကျမ်းကိုးစာရင်း		434