
Table of Contents

Note	1.1
Introduction	1.2
Introduction	1.2.1
Contributors	1.2.2
Structure of the Book	1.2.3
Topics Not Covered	1.2.4
Acknowledgments	1.2.5
Useful Links	1.2.6
Exploitation Tools	1.3
Armitage	1.3.1
Backdoor Factory	1.3.2
BeEF	1.3.3
cisco-auditing-tool	1.3.4
cisco-global-exploiter	1.3.5
cisco-ocs	1.3.6
cisco-torch	1.3.7
Commix	1.3.8
crackle	1.3.9
jboss-autopwn	1.3.10
Linux Exploit Suggester	1.3.11
Maltego Teeth	1.3.12
SET	1.3.13
ShellNoob	1.3.14
sqlmap	1.3.15
THC-IPV6	1.3.16
Yersinia	1.3.17
Forensics Tools	1.4
Binwalk	1.4.1
bulk-extractor	1.4.2
Capstone	1.4.3

chntpw	1.4.4
Cuckoo	1.4.5
dc3dd	1.4.6
ddrescue	1.4.7
DFF	1.4.8
diStorm3	1.4.9
Dumpzilla	1.4.10
extundelete	1.4.11
Foremost	1.4.12
Galleta	1.4.13
Guymager	1.4.14
iPhone Backup Analyzer	1.4.15
p0f	1.4.16
pdf-parser	1.4.17
pdfid	1.4.18
peepdf	1.4.19
RegRipper	1.4.20
Volatility	1.4.21
Xplico	1.4.22
Hardware Hacking	1.5
android-sdk	1.5.1
apktool	1.5.2
Arduino	1.5.3
dex2jar	1.5.4
Sakis3G	1.5.5
smali	1.5.6
Information Gathering	1.6
acccheck	1.6.1
ace-voip	1.6.2
Amap	1.6.3
Automater	1.6.4
bing-ip2hosts	1.6.5
braa	1.6.6
CaseFile	1.6.7

CDPSnarf	1.6.8
cisco-torch	1.6.9
Cookie Cadger	1.6.10
copy-router-config	1.6.11
DMitry	1.6.12
dnmap	1.6.13
dnsenum	1.6.14
dnsmap	1.6.15
DNSRecon	1.6.16
dnstracer	1.6.17
dnswalk	1.6.18
DotDotPwn	1.6.19
enum4linux	1.6.20
enumIAX	1.6.21
exploitdb	1.6.22
Fierce	1.6.23
Firewalk	1.6.24
fragroute	1.6.25
fragrouter	1.6.26
Ghost Phisher	1.6.27
GoLismero	1.6.28
goofile	1.6.29
hping3	1.6.30
InTrace	1.6.31
iSMTP	1.6.32
lbd	1.6.33
Maltego Teeth	1.6.34
masscan	1.6.35
Metagoofil	1.6.36
Miranda	1.6.37
Nmap	1.6.38
ntop	1.6.39
p0f	1.6.40

Parsero	1.6.41
Recon-ng	1.6.42
SET	1.6.43
smtp-user-enum	1.6.44
snmpcheck	1.6.45
sslcaudit	1.6.46
SSLsplit	1.6.47
sslstrip	1.6.48
SSLyze	1.6.49
THC-IPV6	1.6.50
theHarvester	1.6.51
TLSSLed	1.6.52
twofi	1.6.53
URLCrazy	1.6.54
Wireshark	1.6.55
WOL-E	1.6.56
Xplico	1.6.57
Maintaining Access	1.7
CryptCat	1.7.1
Cymothoa	1.7.2
dbd	1.7.3
dns2tcp	1.7.4
http-tunnel	1.7.5
HTTPTunnel	1.7.6
Intersect	1.7.7
Nishang	1.7.8
polenum	1.7.9
PowerSploit	1.7.10
pwnat	1.7.11
RidEnum	1.7.12
sbd	1.7.13
U3-Pwn	1.7.14
Webshells	1.7.15
Weevely	1.7.16

Winexe	1.7.17
Password Attacks	1.8
acccheck	1.8.1
Burp Suite	1.8.2
CeWL	1.8.3
chntpw	1.8.4
cisco-auditing-tool	1.8.5
CmosPwd	1.8.6
creddump	1.8.7
crunch	1.8.8
DBPwAudit	1.8.9
findmyhash	1.8.10
gpp-decrypt	1.8.11
hash-identifier	1.8.12
HexorBase	1.8.13
THC-Hydra	1.8.14
John the Ripper	1.8.15
Johnny	1.8.16
keimpx	1.8.17
Maltego Teeth	1.8.18
Maskprocessor	1.8.19
multiforcer	1.8.20
Ncrack	1.8.21
oclgausscrack	1.8.22
PACK	1.8.23
patator	1.8.24
phrasendrescher	1.8.25
polenum	1.8.26
RainbowCrack	1.8.27
rcracki-mt	1.8.28
RSMangler	1.8.29
SQLdict	1.8.30
Statsprocessor	1.8.31

[Click here to download full PDF material](#)