

# SANS SEC504 – Hackers Techniques and Incident Handling

## Topics

<b>6-step Incident Handling Process</b>	504.1–15
1) Preparation	504.1–18-46
2) Identification	504.1–47-96
3) Containment	504.1–97-114
4) Eradication	504.1–115-120
5) Recovery	504.1–121-124
6) Lessons Learned	504.1–125-128
<b>Incident Tips</b>	504.1–134-182
<b>Law, Crime, and Evidence</b>	504.1–183-203
<b>5-step Attack Process</b>	504.2–4
1) Reconnaissance	504.2–16-52
2) Scanning	504.2–53-203
3) Exploit Systems	504.3–3
– Gaining Access	504.3–4-221
– Web App Attacks	504.4–85-145
– Denial of Service	504.4–146-211
4) Keeping Access	504.5–5-118
5) Covering the Tracks	504.5–119-233
<b>Putting It All Together</b>	504.5–234-263
<b>Conclusions and References</b>	504.5–235-285
<b>Hacker Tools Workshop</b>	504.6–4-59

## Categories

### Commands 🐣

PATH	504.1–250
apropos	504.1–269
arp	504.1–278
	504.3–75, 86
bg	504.1–252
cat	504.1–245, 279
cd	504.1–236, 238
chkconfig	504.1–274
	504.2–117
chmod	504.1–287
	504.5–141
cp	504.1–287-288
crontab	504.1–279
df	504.1–283
echo	504.1–248
	504.5–77
eject	504.1–240
export	504.4–55
	504.5–127
fg	504.1–253
find	504.1–243, 275, 281, 287
free	504.1–283
gedit	504.1–244


grep	504.1–266-267, 280, 290, 292
	504.3–93-96
id	504.1–232
ifconfig	504.1–257
	504.3–6, 74
info	504.1–268
jobs	504.1–253
killall	504.1–286, 288, 292
	504.2–117
	504.5–127
less	504.1–246, 259, 280
locate	504.1–243
ls	504.1–57, 259, 273, 276, 278, 286-289
	504.2–117
ls	504.1–237, 279
	504.5–77
make	504.1–263
man	504.1–268
mkdir	504.1–241
mknod	504.3–26, 31
mount	504.1–239
	504.2–218
nc	504.1–286
	504.3–20, 22-29
netstat	504.1–259, 267, 278
	504.2–117
	504.5–25
nohup	504.3–26
	504.5–141
passwd	504.1–231
	504.4–44
ping	504.1–258
	504.4–96
ps	504.1–251, 273, 286
pwd	504.1–236, 238
reboot	504.1–270
rm	504.1–287
rpm	504.1–262, 277
schred	504.4–49
service	504.1–256
	504.2–159, 169, 173
shutdown	504.1–270
sort	504.1–280, 291
source	504.3–197
ssh	504.5–142
su	504.1–232
tar	504.1–261
tcpdump	504.1–292
	504.2–123, 504.2–170
telinit	504.1–233
top	504.1–251
unlink	504.1–288
unname	504.5–139
updatedb	504.1–243
uptime	504.1–283
useradd	504.1–230, 290
	504.4–44
userdel	504.1–291

# SANS SEC504 – Hackers Techniques and Incident Handling

.....	504.4–48	NetStumbler .....	504.2–81
wget .....	504.5–140	Nmap .....	504.2–121–124
whatis .....	504.1–269	Null Session .....	504.2–203–209
which .....	504.1–248	Samba Client .....	504.2–211–219
whoami .....	504.1–232	Shell History File Analysis .....	504.5–133–143
<b>Commands</b> 🌐		Volatility to Analyze Attack 🌐 .....	504.5–39–58
arp .....	504.3–75, 86	Windows Cheat Sheet .....	504.1–79–91
control .....	504.3–191	Windows Format String .....	504.3–186
cp .....	504.5–145		
hostname .....	504.2–208	<b>Legal Terms</b>	
ipconfig .....	504.3–75, 86	Arrest .....	504.1–186
more .....	504.5–145	Blocking access .....	504.1–193
nbstat .....	504.1–71	Communication equipment .....	504.1–191
nc .....	504.1–85	Data alteration .....	504.1–196
.....	504.3–20, 22–29	Facilitation .....	504.1–193
netsh .....	504.1–72	Impairment .....	504.1–193, 197
.....	504.2–169, 172, 207	Interception .....	504.1–191, 194, 199
.....	504.3–6	Modification .....	504.1–193, 199
netstat .....	504.1–72, 85	Monitoring .....	504.1–191
.....	504.2–115, 171	Sabotage .....	504.1–196
.....	504.3–213	Stored information .....	504.1–191
.....	504.5–25	Unauthorized access .....	504.1–192–193, 197–199
net .....	504.1–68, 71, 75, 88, 124	Unauthorized use .....	504.1–194
.....	504.2–191, 208–209		
notepad .....	504.5–145	<b>Microsoft Management Console</b>	
nslookup .....	504.2–27	eventvwr.msc .....	504.1–90
.....	504.4–96	.....	504.2–171, 504.3–214
ping .....	504.4–96	gpmc.msc .....	504.2–199
reg query .....	504.1–70, 84	lusrmgr.msc .....	504.1–88
regedit .....	504.1–70	.....	504.3–204
runas .....	504.1–90	secpol.msc .....	504.1–89
schtasks .....	504.1–73, 87	.....	504.2–212–213
sc .....	504.1–68, 82	.....	504.3–192, 194
.....	504.2–116	services.msc .....	504.1–82
.....	504.3–194	.....	504.2–116, 206
sort .....	504.3–165, 186		
tasklist .....	504.1–67, 81	<b>Readings</b>	
.....	504.3–213	CloudBurst – VMware Escape History ..	504.4–83
type .....	504.5–145	Detecting Hydan Steganography .....	504.5–228
wmic .....	504.1–67, 74, 81, 124	DNS Amplification Attacks .....	504.4–166
.....	504.2–116	Don't Get Burned by Flame .....	504.4–59
.....	504.4–150	Drive-By Pharming (XSS) .....	504.4–119
.....	504.5–20, 47–48	Ettercap Filtering Language .....	504.3–83
		Format String Attacks .....	504.3–158
		Google Hacking .....	504.2–46
		Hardening Guide for VMware ESX .....	504.4–84
		ICMP Attacks Illustrated .....	504.2–94
		Introduction to Virtualization Security ..	504.4–83
		OWASP Guide for Secure Web Apps ...	504.4–107
		OWASP Testing Guide .....	504.4–87
		Phrack 56 – Bypassing StackGuard ...	504.3–145
		Secure Programming Howto 🌐 .....	504.3–147
		Smashing the Stack for Fun and Profit .	504.3–115
		Static Kernel Patching .....	504.5–89
		Taking Back Netcat .....	504.4–66
		Top Speed of Flash Worms .....	504.4–64
		Warhol Worms: Fast Internet Plagues ...	504.4–64
		Writing Secure Code 🌐 .....	504.3–147
<b>Exercises</b>			
Alternate Data Streams 🌐 .....	504.5–159–163		
ARP and MAC Analysis .....	504.3–89–97		
Covert_TCP File Transfer .....	504.5–180–184		
DoS Attack Evaluation .....	504.4–195–211		
Enum .....	504.2–209–210		
InSSIDer .....	504.2–82		
John the Ripper 🌐 .....	504.4–44–49		
John the Ripper 🌐 .....	504.4–50–51		
Linux Cheat Sheet .....	504.1–273–293		
Metasploit Attack and Analysis ...	504.3–188–221		
Nessus .....	504.2–159–173		
Netcat 🌐 🌐 .....	504.3–34–49		

# SANS SEC504 – Hackers Techniques and Incident Handling

## Specialized Linux Distributions

Grsecurity .....	504.3–143
Immunix .....	504.3–143
Offline  Pwd&Reg Editor Bootdisk ...	504.5–151
P. Nordahl's Free Bootable Linux CD ...	504.4–30
PaX .....	504.3–143





## Summaries

Account Harvesting .....	504.4–93
App-Level Trojan Horse Backdoors .....	504.5–26
Covert Channel with ICMP Tunnel .....	504.5–169
Covert Channel with Rev www Shell ...	504.5–169
CpuHog .....	504.4–152
Distributed DoS .....	504.4–193
DNS Cache Poisoning .....	504.3–113
DNS Recon .....	504.2–30
DoS Suite .....	504.4–182
Editing Unix Accounting Entries .....	504.5–132
Editing Unix Log Files .....	504.5–128
Firewalk .....	504.2–136
Format String Attacks .....	504.3–184
Fragmentation for IDS Evasion .....	504.2–149
FU and FUToRootkits .....	504.5–109
Hiding Files by using dot names .....	504.5–123
IP Address Spoofing .....	504.3–15
KBeast .....	504.5–95
Kernel Intrusion System .....	504.5–102
Linux Rootkit Family .....	504.5–68
Netcat .....	504.3–33
Network Mapping .....	504.2–94
NTFS Alternate Data Streams .....	504.5–148
Null Session .....	504.2–202
OS Fingerprinting .....	504.2–120
Parser Vulnerabilities .....	504.3–156
Port Scanning .....	504.2–120
Session Hijacking .....	504.3–88
Slowloris .....	504.4–156
Smurf .....	504.4–164
Sniffing .....	504.3–77
Solaris LKM Rootkit .....	504.5–105
SQL Injection .....	504.4–109
SYN Flood .....	504.4–178
Vulnerability Scanners .....	504.2–158
War Dialing .....	504.2–62
War Driving .....	504.2–79
Web App State Maintenance .....	504.4–145
Web Application Command Injection ...	504.4–98
Web Site Searches .....	504.2–35
Web/CGI Scanning .....	504.2–187
Whois Reconnaissance .....	504.2–24
Windows Log Editing .....	504.5–156

## Tools

### Attack

Abel .....	504.4–24
BeEF .....	504.4–121
Cdoor (Backdoor) .....	504.5–196

firesheep .....	504.3–72
FragRoute .....	504.2–147
fragrouter .....	504.2–146
ISR-Evilgrade .....	504.2–13
Karmetasploit (Wifi) ★★ .....	504.2–73
Loki2 .....	504.2–94
Modified SAMBA code   .....	504.4–55
Pass-the-Hash Toolkit  .....	504.4–55
Reverse WWW Shell ★★★ .....	504.5–167
SADoor (Backdoor) .....	504.5–198
Smurf .....	504.2–94
sslstrip .....	504.3–72
Windows Credentials Editor  .....	504.4–55
XSS Shell .....	504.4–120

### Code Analysis

Coverity Static Analysis .....	504.3–148
Flawfinder .....	504.3–148
Fortify Source Code Analyzer .....	504.3–148
GrammarTech's CodeSonar .....	504.3–148
Klocwork Insight Pro .....	504.3–148
RATS .....	504.3–148
Veracode Suite .....	504.3–148




### Data Extraction

Enum ★★ .....	504.2–192
Winfingerprint .....	504.2–192





### DDoS Detection

Arbor Network's Peakflow .....	504.4–192
Cisco Guard DDoS Mitigation .....	504.4–192
Riverbed Cascade .....	504.4–192

### Detection

Blacklight .....	504.5–108
Chkrootkit .....	504.1–284
.....	504.5–113
Icesword .....	504.5–108
McAfee Rootkit Detective  .....	504.5–115
OSSEC Rootcheck   .....	504.5–113
Rootkit Hunter .....	504.5–113
Rootkit Revealer  .....	504.5–114
Sophos Anti-Rootkit  .....	504.5–115

### Forensics

AIDE .....	504.1–284
.....	504.5–78
Autopsy .....	504.1–40
Bastille .....	504.1–284
dd .....	504.1–40, 107
EnCase .....	504.1–40
.....	504.3–154
fastdump .....	504.5–34
Forensics Toolkit .....	504.1–40
GFI LANguard Syst Integrity Mon ..	504.5–116
Ionx Data Sentinel .....	504.5–116
LADS  ★ .....	504.5–147, 162
Log2timeline .....	504.1–41
Mandiant Memorize .....	504.1–107
.....	504.5–34
mdd .....	504.5–34
nCircle File Integrity Monitor  .....	504.5–78
OSSEC   .....	504.5–78, 116

# SANS SEC504 – Hackers Techniques and Incident Handling

Responder ●	504.5–34
Solidcore FIM ●	504.5–78
Streams 🌈	504.5–147
Streams Shell Extension 🌈	504.5–147
The Sleuth Kit	504.1–40
.....	504.3–154
Tripwire	504.1–284
.....	504.5–78, 81
Volatility Framework ★★★	504.1–41, 107
.....	504.5–34
win32dd	504.5–34
<b>IDS / IPS</b>	
Cisco IPS	504.5–117
Cisco Secure IDS	504.2–145
ForeScout	504.5–117
SecureLogix	504.2–61
Snort	504.2–145
.....	504.3–155
Sourcefire	504.5–117
Tipping Point	504.5–117
TopLayer	504.5–117
<b>Imaging</b>	
ncat	504.1–40
Netcat	504.1–40
SafeBack	504.1–40
<b>Keylogger</b>	
Actual key-logger 🌈	504.3–79
MyHook 🌈	504.3–79
Real Free Keylogger 🌈	504.3–79
REFOG 🌈	504.3–79
Revealer 🌈	504.3–79
TTYSnoop 🕸	504.3–79
TTYSpy 🕸	504.3–79
<b>Log Wiper</b>	
cloak.c 🕸 🗑	504.5–131
logwedit.c 🕸 🗑	504.5–131
marry.c 🕸 🗑	504.5–131
remove.c 🕸 🗑	504.5–131
WinZapper 🌈	504.5–153
wtmped.c 🕸 🗑	504.5–131
wzap.c 🕸 🗑	504.5–131
<b>Manipulation Proxy</b>	
Burp Proxy	504.4–137
Fiddler 🌈	504.4–137
Odysseus / Telemachus 🌈	504.4–137
w3af (MitM proxy)	504.4–137
WebScarab	504.4–87, 137
Zed Attack Proxy	504.4–101, 137–138
<b>Multi-Purpose</b>	
Cain	504.1–53
.....	504.4–25–29, 32
Cryptcat	504.3–17
Dnscat	504.3–17
Ettercap 🕸 ★★★	504.3–83–84
Linkcat	504.3–17
Ncat	504.3–17
Netcat ★★★	504.3–17
Socat	504.3–17
VMcat	504.4–83
<b>Network &amp; Port Mapping</b>	
Cheops	504.2–94
Firewalk	504.2–94
Firewalk ★★	504.2–130–135
Layer Four Traceroute	504.2–130
Nmap	504.1–57
.....	504.2–85, 89–90
Port Reporter	504.2–111
QueSO	504.2–111
tcptraceroute	504.2–130
XProbe (OS fingerprinting)	504.2–94, 111
Zenmap (Nmap GUI) ★★★	504.2–121
<b>Packer</b>	
ASPack	504.5–31
Exe32pack	504.5–31
EXES stealth	504.5–31
ExPressor	504.5–31
EZIP	504.5–31
PackMan	504.5–31
PEBundle ●	504.5–31
PECompact ●	504.5–31
PeTite	504.5–31
SPEC	504.5–31
Themida	504.5–31
Thinstall ●	504.5–31
UPX ★★	504.5–31
Yoda	504.5–31
<b>Packet Crafting</b>	
Bit-Twist	504.3–6
Hping	504.3–6
Nemesis	504.3–6
NetDude	504.3–6
Scapy	504.3–6, 74
<b>Penetration Testing</b>	
Metasploit 🌈 ★★★	504.2–73
.....	504.3–123, 132–141
OWASP ★★★	504.4–87
<b>Protection</b>	
Blackhole	504.2–119
IP Personality	504.2–119
IPlog	504.2–119
OSfuscate	504.2–119
Stealth Patch	504.2–119
<b>Password Recovery</b>	
Cain & Abel ★★	504.4–23–29
fgdump	504.4–30, 32
hashdump (Meterpreter) 🗑	504.4–30, 32
John the Ripper 🌈 🕸 ★★★	504.2–194
.....	504.4–13, 36–37, 40–41
pwdump	504.4–30, 32
SnadBoy 🕸	504.4–50
THC Hydra	504.4–8
<b>Remote Administration</b>	
BO2K	504.5–10
Dameware	504.5–10
NetBus	504.5–10
Sub7	504.5–10

# SANS SEC504 – Hackers Techniques and Incident Handling

VNC .....	504.5–10	Nushu ★ .....	504.5–186
<b>Recon</b>		PingChat .....	504.5–171
Dig .....	504.2–26	Ptunnel 🇺🇸 🇦🇩 ★ .....	504.5–171-172
GHDB scanning tool (SecApp) .....	504.2–45	<b>Utilities</b>	
Maltego ★★ .....	504.2–48-50	Active Ports 🇺🇸 .....	504.5–24, 194
SearchDiggity .....	504.2–45	ADMutate .....	504.4–67
SiteDigger .....	504.2–44-45	Burndump .....	504.5–30
Wikto .....	504.2–44-45	Burneye .....	504.5–29
<b>Rootkit</b>		EtherApe ★ .....	504.5–117
AFX Windows Rootkit 🇺🇸 .....	504.5–72-76	Evt2sys .....	504.5–157
FU 🇺🇸 .....	504.5–88, 107	!exploitable 🇺🇸 .....	504.3–125
FUTo 🇺🇸 .....	504.5–108	gedit 🇦🇩 .....	504.3–91
KBeast 🇦🇩 .....	504.5–91	Kiwi's Syslog ● .....	504.5–157
KIS 🇦🇩 .....	504.5–91	md5deep .....	504.1–41, 107
LRK6 🇦🇩 .....	504.5–64-66	md5sum .....	504.1–107
SInAr 🇺🇸 .....	504.5–104	Msyslog .....	504.5–158
SubVirt .....	504.5–90	Nmap Scripting Engine 🇺🇸 .....	504.4–101
SUCKit 🇦🇩 .....	504.5–88	Password Guard .....	504.4–34
Vitriol .....	504.5–90	SL4NT ● .....	504.5–157
<b>Sniffer</b>		Snare Agent and Log Server ● .....	504.5–157
Drifnet .....	504.3–62	SysTrace 🇦🇩 .....	504.5–111
Dsniff ★★★ .....	504.3–53	TCPView (Sysinternals) 🇺🇸 .....	504.5–24, 194
FloP .....	504.2–127	wget 🇺🇸 🇦🇩 .....	504.4–67
Kismet (Wifi) .....	504.2–70	XOR Payloads & Encoder .....	504.4–67
NetMon .....	504.3–155	<b>VM Environment</b>	
netstat .....	504.1–56	BOCHS .....	504.4–81
Niksun .....	504.3–62	Qemu .....	504.4–81
Omnipeek (Wifi) .....	504.2–70	User-Mode Linux .....	504.4–81
P0F .....	504.2–127	VirtualPC .....	504.4–81, 83
Sniffit .....	504.3–84	VMware .....	504.1–205-225
tcpdump .....	504.1–55	.....	504.4–81, 83
.....	504.2–27, 70, 123, 140, 166	Xen .....	504.4–81, 83
.....	504.3–52, 155	<b>Vulnerability Scanner</b>	
VOMIT .....	504.1–53	BeyondTrust Retina .....	504.2–152
Wireshark ★★ .....	504.1–41, 53	Burp Suite .....	504.4–101
.....	504.2–70, 504.3–152, 155	Nessus ★★★ .....	504.2–153-156
.....	504.3–52	.....	504.3–23
<b>Sniffer Detector</b>		OpenVAS .....	504.2–152
ARPWatch .....	504.3–75, 86	Rapid7 NeXpose .....	504.2–152
Promqry 🇺🇸 .....	504.3–74	SAINT .....	504.2–152
Sentinel .....	504.3–74	SATAN .....	504.2–151
.....	504.4–25	.....	504.3–23
<b>Steganography</b>		Sqlmap .....	504.4–101
Hydan ★★★ .....	504.5–223-228	<b>War Dialing</b>	
Invisible Secrets .....	504.5–223	Phonesweep .....	504.2–60
Jsteg .....	504.5–223	THC Scan .....	504.2–55-56
MP3Stego .....	504.5–223	WarVOX .....	504.2–57-58
S-Mail .....	504.5–223	<b>War Driving</b>	
S-Tools ★★ .....	504.5–219	InSSIDer .....	504.2–65, 67, 82-83
Stash .....	504.5–223	NetStumbler .....	504.2–65-66, 80-81
Stegdetect .....	504.5–233	Wellenreiter .....	504.2–68-69
<b>Tracking</b>		<b>Web Application Firewall</b>	
Orion Live CD .....	504.1–102	Cisco's ACE WAF .....	504.4–143
RTIR .....	504.1–102	Citrix Netscaler App FW .....	504.4–143
<b>Tunneler</b>		F5 App Security Manager .....	504.4–143
Covert_TCP ★★ .....	504.5–175	Free OWASP Stinger .....	504.4–143
ICMPCmd 🇺🇸 .....	504.5–171	<b>Web Scanner</b>	
ICMPShell 🇦🇩 .....	504.5–171	aglimpse .....	504.2–177

# SANS SEC504 – Hackers Techniques and Incident Handling

---

AWstats .....	504.2–177
campas .....	504.2–177
cgiscan .....	504.2–177
Jikto .....	504.4–119
LibWhisker .....	504.2–178
Nikto ** .....	504.2–177
phf .....	504.2–177
phpBB .....	504.2–177
showcode.asp .....	504.2–177
Whisker .....	504.2–181

## Wifi Cracking

Aircrack-ng (WEP) .....	504.2–70
ASLEAP (LEAP) .....	504.2–70
CoWPAtty (WPA) .....	504.2–70
IKE Crack .....	504.2–77
WEPCrack (WEP) .....	504.2–70

## Wrapper

AFX File Lace .....	504.5–28
EliteWrap .....	504.5–28
SaranWrap .....	504.5–28
Trojan Man .....	504.5–28

## Websites



Anti-Phishing .....	504.1–149
Arbor Networks' Peakflow .....	504.4–192
bugtraq .....	504.1–12
Center for Internet Security ** .....	504.5–110
CIS Hardening Guidelines .....	504.1–284
Cisco Guard DDoS Mitigation .....	504.4–192
Cybercrime Law .....	504.1–197
DNS Stuffs .....	504.2–52
ECTF .....	504.1–22
Exploit Database .....	504.2–37
.....	504.3–121
Forensics Wiki .....	504.5–35
Free Rainbow Tables .....	504.4–22
HTCIA .....	504.1–22
IANA .....	504.2–97
InfraGard .....	504.1–22
Internet Storm Center .....	504.1–12
.....	504.5–78
IPSECS .....	504.5–93
JigSaw .....	504.2–33
Koders (Code Search Engine) .....	504.3–124
McAfee's Foundscan .....	504.2–152
MD5 Crack Project .....	504.4–22
Moss tingrett (Legal framework) .....	504.1–189
Mykonos Web Security .....	504.4–93
Network-Tools .....	504.2–52
Nmap OS detection defeat tools .....	504.2–119
Packet Storm Security *** .....	504.2–130, 177
.....	504.3–121
.....	504.4–180
Phrack Magazine * .....	504.3–145
.....	504.5–89
Pipl .....	504.2–33
PLXpatrol .....	504.4–163
Project Rainbow Crack .....	504.4–22

Qualys (Vulnerability Scan) .....	504.2–152
Riverbed Cascade .....	504.4–192
Security Focus .....	504.1–12
Security Space .....	504.2–52
Shodan .....	504.2–52
Skull Security .....	504.4–13
Sysinternals .....	504.4–151
Tenable Network Security .....	504.2–153
Traceroute .....	504.2–52
XSS Encoding Technique .....	504.4–112




# SANS SEC504 – Hackers Techniques and Incident Handling

## A

Abel .....	504.4–24
Account Harvesting .....	504.4–89-91
Defense .....	504.4–92
ACK Scanning .....	504.2–102
ACK Storms .....	504.3–81
Active Directory .....	504.2–197
.....	504.4–5, 34
Active Ports  .....	504.5–24, 194
ActiveX .....	504.4–114, 138, 150
Actual key-logger  .....	504.3–79
ADMutate .....	504.4–67
AFX File Lace .....	504.5–28
AFX Windows Rootkit .....	504.5–72-76
aglimpse .....	504.2–177
AIDE .....	504.1–284
.....	504.5–78
Aircrack-ng (WEP) .....	504.2–70
Alternate Data Streams .....	504.5–145-147
Amplification Factor .....	504.4–166-167
Anti-Reverse Engineering .....	504.5–29, 31
Anti-spoof Filters .....	504.3–13
Apache .....	504.4–107, 125
API Hooking .....	504.5–70
Arbor Network's Peakflow .....	504.4–192
ARP .....	504.3–55-59
Cache .....	504.3–56, 91, 94
Cache Poisoning .....	504.3–57, 59, 82, 94
.....	504.4–25
Security .....	504.3–73
Spoofing .....	504.3–82
Table Hardcoding .....	504.3–73, 85
Arpspoof .....	504.3–58
ARPWatch .....	504.3–75, 86
Artifacts .....	504.1–124
ASLEAP (LEAP) .....	504.2–70
ASP .....	504.2–175
ASPack .....	504.5–31
Assessment Questions .....	504.1–93-94
Autopsy .....	504.1–40
AWstats .....	504.2–177

## B

Backdoor .....	504.3–25, 31
.....	504.4–71
.....	504.5–6, 194
Alternate Names .....	504.5–20
XSS .....	504.4–120
Bash History  .....	504.5–126
Bastille .....	504.1–284
BEAST-style Attack .....	504.3–73
BeEF .....	504.4–121
BeyondTrust Retina .....	504.2–152
BIND .....	504.3–99
BIOS .....	504.5–7-8
Bit-Twist .....	504.3–6

Blackhole .....	504.2–119
Blacklight .....	504.5–108
Blaster .....	504.4–59
Blowfish .....	504.4–41
.....	504.5–225
BO2K .....	504.5–10, 504.5–16
BOCHS .....	504.4–81
Boot Sector .....	504.5–8
Bot .....	504.4–71-78
Communication Channels .....	504.4–73
Defense .....	504.4–79
Distribution .....	504.4–72
Fast Flux .....	504.4–74-76
Functionality .....	504.4–77-78
Botnets .....	504.4–71, 73-75
Broadcast Address .....	504.4–159-160
Browser Exploit Attack .....	504.4–72
Browser Exploitation Framework .....	504.4–121
Brute Force Approach .....	504.3–125
.....	504.4–12
Buffer Overflow .....	504.3–115-120
Cram Input .....	504.3–126
Defense .....	504.3–142-150
Exploit Creation .....	504.3–121-130
Burndump .....	504.5–30
Burneye .....	504.5–29
Defense .....	504.5–30
Burp Proxy .....	504.4–137
Burp Suite .....	504.4–101

## C

Cain .....	504.4–25, 28-29, 504.1–53
.....	504.4–25-29, 32
Cain & Abel ★★ .....	504.4–23, 504.4–23-29
Caller ID Spoofing .....	504.2–57
CAM Table .....	504.3–51, 91, 95
campas .....	504.2–177
Canary .....	504.3–145
Cdoor (Backdoor) .....	504.5–196
Certificate Authority .....	504.3–67, 70
CGI .....	504.2–175
.....	504.5–23
cgiscan .....	504.2–177
Chain of Custody .....	504.1–95
Character Insertion .....	504.3–83
Cheat Sheets .....	504.1–64
Checklist .....	504.1–31, 164-166
Cheops .....	504.2–94
Chief Security Officer .....	504.1–137
Chkrootkit .....	504.1–284
.....	504.5–113
Chroot'ed Environment .....	504.2–186
CIO .....	504.1–137
Cisco Guard DDoS Mitigation .....	504.4–192
Cisco IPS .....	504.5–117
Cisco Secure IDS .....	504.2–145
Cisco's ACE WAF .....	504.4–143

# SANS SEC504 – Hackers Techniques and Incident Handling

Citrix Netscaler App FW .....	504.4–143
Clearev .....	504.5–155
cloak.c 🗑️ .....	504.5–131
CloudBurst .....	504.4–83
Code Search Engine .....	504.3–124
Cold Fusion .....	504.2–175
Command Injection .....	504.4–95-96
Defense .....	504.4–97
Cone of Silence .....	504.5–100
Conficker 🌈 .....	504.4–61-62
Connexion Queue .....	504.4–173
Containment subphases .....	504.1–98
Cookie .....	504.4–130, 133
SYN .....	504.4–176
Copyright .....	504.1–171
Covering Tracks .....	504.5–121-156
Defense .....	504.5–157-158
Coverity Static Analysis .....	504.3–148
Covert Channel .....	504.5–165, 175, 186
Defense .....	504.5–191-192
Covert_TCP ★★ .....	504.5–175
CoWPAtty (WPA) .....	504.2–70
CPU .....	504.5–8
CpuHog .....	504.4–150
Defense .....	504.4–151
Cross-Site Scripting .....	504.4–111-124
Defense .....	504.4–125-127
Overview .....	504.4–113
Possibilities .....	504.4–118
Walkthrough .....	504.4–114-116
Cryptcat .....	504.3–17
Cryptography .....	504.5–204-207
CURL .....	504.4–89
Cyber Crime Laws .....	504.1–189-199

## D

Dameware .....	504.5–10
Data Encryption .....	504.4–79
Data Execution Prevention 🌈 .....	504.3–144
Database Manipulation .....	504.4–102
dd .....	504.1–40, 107
Deadly Sins .....	504.1–129
Denial of Service .....	504.3–9, 81
.....	504.4–71, 147
Distributed .....	504.4–184-190
Defense .....	504.4–191
Types .....	504.4–148
DES .....	504.4–41
Detection Zones .....	504.1–54
Device Drivers .....	504.5–87
DHCP Snooping .....	504.3–73, 85
Dictionary Attack .....	504.2–194
Dig .....	504.2–26
Directed Broadcast Attack .....	504.4–158
DLL Injection .....	504.5–70, 152
DMCA .....	504.2–10
DMZ .....	504.2–130

DNS .....	504.1–104, 202
.....	504.2–22
.....	504.3–55, 79
Amplification Attack .....	504.4–166-169
Defense .....	504.4–170
Attack .....	504.3–64
Cache Check .....	504.3–75, 86, 112
Cache Poisoning .....	504.3–101-107
Defense .....	504.3–108-112
Kaminsky's variation ★★ .....	504.3–105-107
Overview .....	504.3–99-100
Query ID .....	504.3–100, 102, 108
Recon .....	504.2–26
Defense .....	504.2–29
Record .....	504.2–27
Recursive Lookup .....	504.3–109
Round-Robin .....	504.4–75-76
TTL .....	504.4–76
Zone Transfer .....	504.2–27-28
Dnscat .....	504.3–17
DNSSpoof .....	504.3–63-66
Domain Controller .....	504.4–30, 33
DoS Attack .....	504.4–147-148
DoS Suite .....	504.4–180
Defense .....	504.4–181
Double-Flux Technique .....	504.4–76
Drifnet .....	504.3–62
Drive Duplicator .....	504.1–109
Drive-By Download .....	504.4–72
Drive-By Pharming .....	504.4–119
Dsniff .....	504.3–53-54, 58-59
Dsniff ★★★ .....	504.3–53
Dynamic ARP Inspection .....	504.3–73, 85

## E

EDNS .....	504.4–167
ELF .....	504.5–29
EliteWrap .....	504.5–28
Emergency Comm Plan ((Identification)) .....	504.1–32
EnCase .....	504.1–40
.....	504.3–154
Encryption .....	504.2–77
Enum .....	504.2–193-196
Exercise .....	504.2–210
Enum ★★ .....	504.2–192
Espionage .....	504.1–136
EtherApe ★ .....	504.5–117
EtherARP .....	504.3–74
Etherping .....	504.3–74
Ethical Worm .....	504.4–70
Ettercap 🗑️ ★★★ .....	504.3–83-84
Event .....	504.1–9
Evidence .....	504.1–200-202
EVT File Format 🌈 .....	504.5–150
Evt2sys .....	504.5–157
Exe32pack .....	504.5–31
Executable Protection Layers .....	504.5–30



# SANS SEC504 – Hackers Techniques and Incident Handling

EXEStealth .....	504.5–31
Exploit .....	504.3–127-128, 132-133
!exploitable 🚩 .....	504.3–125
ExPressor .....	504.5–31
EZIP .....	504.5–31

## F

F5 App Security Manager .....	504.4–143
Facebook .....	504.3–72
Fast Flux Technique .....	504.4–74
fastdump .....	504.5–34
fgdump .....	504.4–30, 32
Fiddler 🚩 .....	504.4–137
File Integrity Check .....	504.5–116
File Parser .....	504.3–154
Defense .....	504.3–155
File Sharing .....	504.2–213-214, 218
.....	504.4–77
File System .....	504.5–89
FileMaker .....	504.2–43
filesnarf .....	504.3–61
Filtering Language .....	504.3–83
Firefox Extensions	
Add N Edit Cookies .....	504.4–134
Firebug .....	504.4–134
NoScript .....	504.4–126
Tamper Data ★ .....	504.4–134
firesheep .....	504.3–72
Firewall .....	504.2–94, 504.2–130-135
Defense .....	504.2–135
Firewall ★★ .....	504.2–130-135
Firewall .....	504.2–61, 131
Directed Broadcast .....	504.4–162
Disable .....	504.3–189
Host .....	504.4–56
Port Scanning .....	504.2–130
Rules .....	504.2–135
Web Application .....	504.4–97, 143
FloP .....	504.2–127
Flame .....	504.4–59
Flash .....	504.4–64
Flawfinder .....	504.3–148
Forensics Imaging .....	504.1–107
Forensics Toolkit .....	504.1–40
ForeScout .....	504.5–117
Format String Attack .....	504.3–158-186
Defense .....	504.3–183
Stack View .....	504.3–168-179
Vulnerable Code .....	504.3–163
Windows Sort .....	504.3–165
Exercise .....	504.3–186
Fortify Source Code Analyzer .....	504.3–148
Fraggle .....	504.4–158
Fragment Overlap Attack .....	504.2–144
FragRoute .....	504.2–147
fragrouter .....	504.2–146
Fraud Investigation .....	504.4–108, 127

Freak88 .....	504.4–184
Free OWASP Stinger .....	504.4–143
FTP .....	504.2–110
.....	504.3–79
.....	504.4–77, 124
Bounce Capability .....	504.2–103
Control Connection .....	504.2–110
Data Connection .....	504.2–110
FTP Bounce Scanning .....	504.2–103
FU 🚩 .....	504.5–88, 107
FUTo .....	504.5–108
FUTo 🚩 .....	504.5–108

## G

GECOS .....	504.4–38, 40
gedit 🚩 .....	504.3–91
GFI LANguard Syst Integrity Mon .....	504.5–116
GHDB scanning tool (SecApp) .....	504.2–45
Google	
Cache .....	504.2–41
Hacking Database .....	504.2–37
Maps .....	504.2–38
Recon .....	504.2–44
Defense .....	504.2–46
Search Directives .....	504.2–39
Wayback .....	504.2–41
Google API .....	504.2–44
GPO .....	504.4–34
GPS .....	504.2–65
GrammaTech’s CodeSonar .....	504.3–148
GRE .....	504.4–78
Grsecurity .....	504.3–143

## H

Hacker Manifesto .....	504.2–15
Hacktivism .....	504.2–11
Hash Dumper .....	504.4–25
hashdump (Meterpreter) 🚩 .....	504.4–30, 32
Hidden Form Element .....	504.4–130
Hiding Files in NTFS .....	504.5–145
Hijack .....	504.3–83
API .....	504.3–83
HOIC .....	504.4–190
Honeypot .....	504.4–81
Host Perimeter .....	504.1–56
Hping .....	504.3–6
HTML .....	504.1–149
.....	504.4–113, 130
HTTP .....	504.1–164
.....	504.4–124, 130
Proxy .....	504.4–71, 78
HTTPS .....	504.3–72
.....	504.4–124
.....	504.5–22
HUP Signal .....	504.3–182
Hydan ★★★ .....	504.5–223-228
Hydan Technique .....	504.5–225-227

# SANS SEC504 – Hackers Techniques and Incident Handling

## I

IANA .....	504.1–57
Icesword .....	504.5–108
ICMP .....	504.2–87, 92, 94, 113, 134
.....	504.3–60
.....	504.4–158, 160, 162
Tunnel .....	504.5–171
ICMPCmd 🌈 .....	504.5–171
ICMPShell 🐞 .....	504.5–171
IDS .....	504.1–164, 178
.....	504.2–78, 135, 138
.....	504.4–127, 181
Evasion Techniques .....	504.2–143–144, 182–185
Signature Matching .....	504.2–141
IIS/Sadmind .....	504.4–59, 62
IKE Crack .....	504.2–77
Immunix .....	504.3–143
Incident .....	504.1–8
Characteristics .....	504.1–100
Handling Team .....	504.1–29, 33
Response Capability .....	504.4–79
Tracking .....	504.1–102
Insider Threat .....	504.1–155
Casual .....	504.1–157
Intentional .....	504.1–159
InSSIDer .....	504.2–65, 67, 82–83
Instruction Pointer .....	504.3–117
Integrity Check .....	504.5–158, 231
Invisible Secrets .....	504.5–223
Ionx Data Sentinel .....	504.5–116
IP .....	504.2–96
.....	504.3–55
.....	504.5–165
Address Spoofing .....	504.2–105
.....	504.3–5–12
Defense .....	504.3–13–14
Forwarding .....	504.3–59
Fragmentation Attack .....	504.2–138, 142, 146
Defense .....	504.2–148
Header .....	504.2–86, 139
.....	504.5–176
Identification Field .....	504.2–106
Identification Scanning .....	504.2–108
IP Identification (Idle) Scan .....	504.2–104–108
IP Personality .....	504.2–119
IPlog .....	504.2–119
IPS .....	504.2–61, 138
IPSec .....	504.3–73
IRC .....	504.4–36, 71, 73–74, 185
ISN .....	504.2–98
.....	504.3–7
.....	504.5–187–188
ISP .....	504.1–106, 149
.....	504.4–74, 163, 170, 177, 187
ISR-Evilgrade .....	504.2–13

## J

Jikto .....	504.4–119
John the Ripper .....	504.2–194
.....	504.4–36–37, 40–41
unshadow .....	504.4–37
Cracking Modes .....	504.4–40
John the Ripper 🌈 🐞 *** .....	504.2–194
.....	504.4–13, 36–37, 40–41
JSP .....	504.2–175
Jsteg .....	504.5–223
Jump Bag .....	504.1–39

## K

Karmetasexploit (Wifi) ** .....	504.2–73
KBeast .....	504.5–93–94
KBeast 🐞 .....	504.5–91
Kerberos .....	504.4–26, 31, 36, 42–43
Kernel .....	504.5–82, 85
File .....	504.5–89
Intrusion System .....	504.5–97–101
Memory Map .....	504.5–88
Kernel-Mode Rootkit .....	504.5–81–93, 116
Defense .....	504.5–110–118
Types .....	504.5–86–91
KIS 🐞 .....	504.5–91
Kismet (Wifi) .....	504.2–70
Kiwi's Syslog 🟡 .....	504.5–157
Klez .....	504.4–67
Klocwork Insight Pro .....	504.3–148

## L

LADS 🌈 ★ .....	504.5–147, 162
LAN Manager .....	504.2–212
LANMAN (LM) ....	504.4–16–18, 25, 32–33, 36, 41, 51
Authentication .....	504.4–33
Challenge/Response .....	504.4–31, 33, 53
Lastlog 🐞 .....	504.5–130
Law Enforcement .....	504.1–20, 504.1–185
Layer Four Traceroute .....	504.2–130
LDAP .....	504.4–36
Level, Application- or System- .....	504.1–54
LibWhisker .....	504.2–178
Linkcat .....	504.3–17
Linux .....	504.1–273–293
Accounting Entries .....	504.5–130
File System Structure .....	504.1–235
Hiding Files .....	504.5–121–122
Hosts File .....	504.3–8
Kernel Mode .....	504.5–91
Log Files .....	504.5–125
Monolithic .....	504.5–111
Network Configuration .....	504.1–255–258
Password File .....	504.4–37–38
Passwords File .....	504.4–5
Shadow File .....	504.4–39
Shell History .....	504.5–126–127
Specialized Versions .....	504.3–143

# SANS SEC504 – Hackers Techniques and Incident Handling

Standard Shell Redirects .....	504.3–20
Supporting Tools .....	504.1–284
Listening Ports .....	504.2–115–118
Local check on Linux .....	504.2–117
Local check on Windows .....	504.2–115
Load Balancing .....	504.4–75
Loadable Kernel Modules .....	504.5–87
Log .....	504.1–163
Editing 🗑️ .....	504.5–130
Editing 🌈 .....	504.5–150
LOG File Format 🌈 .....	504.5–150
Log Wiper .....	504.5–131
Log2timeline .....	504.1–41
logwedit.c 🗑️ 📁 .....	504.5–131
LOIC .....	504.4–189
Loki2 .....	504.2–94
Long-term actions .....	504.1–112
LRK .....	504.5–62–66
Backdoor Components .....	504.5–65–66
LRK6 🗑️ .....	504.5–64–66

## M

MAC .....	504.2–67, 76
.....	504.3–55–56, 85
Cisco Router ARP Cache .....	504.3–94
Virtual Machine .....	504.1–211
Macof .....	504.3–58
Mail Relay .....	504.4–71
mailsnarf .....	504.3–61
Maltego ★★ .....	504.2–48–50
Malware .....	504.5–7–8
Examples ★★ .....	504.5–7
Man In The Middle Attack .....	504.3–63, 65
Mandiant Memorize .....	504.1–107
.....	504.5–34
marry.c 🗑️ 📁 .....	504.5–131
McAfee Rootkit Detective 🌈 .....	504.5–115
md5deep .....	504.1–41, 107
md5sum .....	504.4–141
md5sum .....	504.1–107
mdd .....	504.5–34
MDx .....	504.4–25, 27
Mebromi .....	504.5–7
Meeting .....	504.1–127
Memory Analysis .....	504.5–34
Metasploit 🌈 ★★★ .....	504.2–73
.....	504.3–123, 132–141
Metasploit Framework .....	504.3–132–141
.....	504.4–121
msfconsole .....	504.3–197–207
msfelfscan .....	504.3–123
msfpescan .....	504.3–123
Arsenal .....	504.3–133
Exploits .....	504.3–135
Payloads .....	504.3–136
psexec .....	504.3–199–200
psexec .....	203

User Interfaces .....	504.3–134
Meterpreter .....	504.3–137–139, 207–211
hashdump .....	504.3–210
migrate .....	504.3–217
shell .....	504.3–211
Modified SAMBA code 🗑️ 📁 .....	504.4–55
Monitoring .....	504.1–123, 163
Morphing Engine .....	504.4–67
Morto 🌈 .....	504.4–62
MP3Stego .....	504.5–223
Msfelfscan .....	140
Msfpescan .....	140
Msgsnarf .....	504.3–61
Mstream .....	504.4–184
Msyslog .....	504.5–158
MyHook 🌈 .....	504.3–79

## N

NASL .....	504.2–156
NAT .....	504.1–202
Ncat .....	504.3–17
ncat .....	504.1–40
nCircle File Integrity Monitor 🟡 .....	504.5–78
Nemesis .....	504.3–6
Nessus .....	504.2–153–156
.....	504.3–23
Exercise .....	504.2–159–173
NetBIOS .....	504.2–190, 201, 207
NetBus .....	504.5–10
Netcat .....	504.3–17–49, 504.1–40
.....	504.5–20
BackPipe Relay .....	504.3–29–30, 41, 46
Client-to-Client Relay .....	504.5–53
Command Switches .....	504.3–20
Defense .....	504.3–32
Exercise .....	504.3–34
Modes .....	504.3–18–19
Persistent .....	504.3–26
Uses .....	504.3–21
Netcat ★★★ .....	504.3–17
NetDude .....	504.3–6
NetMon .....	504.3–155
netstat .....	504.1–56
NetStumbler .....	504.2–65–66, 80–81
Network Forensics .....	504.5–117
Network Mapping .....	504.2–87
Defense .....	504.2–92–93
Network Neighborhood .....	504.2–189
Network Perimeter .....	504.1–57
Niksun .....	504.3–62
Nikto .....	504.2–178–185
Nimda 🌈 .....	504.4–61–62
NIST .....	504.5–78
Nmap .....	504.2–85
.....	504.2–85, 89–90
.....	504.5–24
Exercise .....	504.2–121–124

# SANS SEC504 – Hackers Techniques and Incident Handling

OS Fingerprinting Techniques (Gn 1) ..	504.2-111
OS Fingerprinting Techniques (Gn 2) ..	504.2-113
Scan Types .....	504.2-101
Nmap Scripting Engine 🗄 .....	504.4-101
NOP .....	504.3-130, 182
Nslookup .....	504.2-26
NSRL .....	504.5-78
NT .....	504.4-19, 25, 36, 41
NTLM .....	504.4-26, 31-33, 36, 41, 53
Null Session .....	504.2-189-192, 208
Defense .....	504.2-199-201
Exercise .....	504.2-203-209
Nushu .....	186, 504.5-187-190

## O

Odysseus / Telemachus 🌈 .....	504.4-137
OLE .....	504.5-22
Ollydbg .....	504.5-32
Omnipeek (Wifi) .....	504.2-70
Open Source .....	504.2-33
OpenIOC (Mandiant) .....	504.1-51
OpenSSH .....	504.3-69
OpenVAS .....	504.2-152
Orion Live CD .....	504.1-102
OS .....	504.1-164
.....	504.5-8
Fingerprinting (Active) .....	504.2-111-112
Defense .....	504.2-119
Fingerprinting (Passive) .....	504.2-126-127
.....	504.3-83
Defense .....	504.2-128
OSfuscate .....	504.2-119
OSSEC 🌈 ● .....	504.5-78, 116
OSSEC Rootcheck 🌈 ● .....	504.5-113
OWASP .....	504.4-87

## P

P0F .....	504.2-127
Packer .....	504.5-31
Defense .....	504.5-32
Packet Fragmentation .....	504.2-106
PackMan .....	504.5-31
PAM .....	504.4-43
PapaSmurf .....	504.4-158
Pass-the-Hash Attack .....	504.4-53-55
Defense .....	504.4-56
Pass-the-Hash Toolkit 🌈 .....	504.4-55
Password .....	504.4-5
Complexity .....	504.4-34
Cracking .....	504.4-9, 25
Brute Force Attack .....	504.4-12, 18, 40
Defense .....	504.4-32-33, 504.4-42-43
Dictionary Attack .....	504.4-11, 28
Hybrid Attack .....	504.4-13, 28
Dumping .....	504.4-30, 32

Formats .....	504.4-26-27, 29
Guessing .....	504.4-6-8
Policy .....	504.4-32, 34, 42
Shadowed .....	504.4-37-39, 42
Spraying .....	504.4-7
Password Collector .....	504.3-83
Password Guard .....	504.4-34
Patent .....	504.1-170
PaX .....	504.3-143
Payload .....	504.3-132-133, 200
.....	504.4-68-69, 72
PEBundle ● .....	504.5-31
PECompact ● .....	504.5-31
Permission Memo .....	504.2-8
PeTite .....	504.5-31
PGP .....	504.1-32
.....	504.2-14
.....	504.5-205
phf .....	504.2-177
Phishing .....	504.1-133, 144
.....	504.4-74-75
Phonesweep .....	504.2-60
PHP .....	504.2-175
phpBB .....	504.2-177
PID .....	504.5-35, 46-52
Ping of Death .....	504.4-148
Ping Sweep .....	504.2-101
PingChat .....	504.5-171
Pivoting .....	504.3-139
PKI .....	504.4-42
Points of Contact .....	504.1-34
Poison Ivy .....	504.5-7
Configuration .....	504.5-15-16
Port Reporter .....	504.2-111
Port Scanning .....	504.2-102-104
Defense .....	504.2-114
Useful Ports .....	504.2-109
Port-level Security .....	504.3-73, 85
Privilege Escalation Attack .....	504.3-139
Promiscuous Mode .....	504.1-282
.....	504.3-51, 74
.....	504.4-25
.....	504.5-100
Promqry 🌈 .....	504.3-74
Protection Techniques .....	504.1-118
Protocol Layers .....	504.3-55
Protocol Parser .....	504.3-52, 152-153
Defense .....	504.3-155
Proxy .....	504.4-135-137, 504.1-153
Web App Attack .....	504.4-137
Web App Manipulation .....	504.4-136, 139
Psexec Exploit .....	504.3-199
.....	504.4-55
Ptunnel 🌈 🗄 ★ .....	504.5-171-172
pwdump .....	504.4-30, 32

## Q

# SANS SEC504 – Hackers Techniques and Incident Handling

Qemu ..... 504.4–81  
QueSO ..... 504.2–111

## R

RADIUS ..... 504.4–43  
Rainbow Tables ..... 504.4–22  
Ramen 🍜 ..... 504.4–61-62  
Rapid7 NeXpose ..... 504.2–152  
RATS ..... 504.3–148  
RDP ..... 504.2–43  
Real Free Keylogger 🗝️ ..... 504.3–79  
Referral ..... 504.3–106-107  
Reflective DLL Injection ..... 504.5–56  
REFOG 🌈 ..... 504.3–79  
Registrar ..... 504.2–20  
Registration Attack ..... 504.3–100  
Registration Authority ..... 504.3–70  
Remote Control Backdoor Capabilities ★ 504.5–16-19  
remove.c 🗑️ ..... 504.5–131  
Reporting ..... 504.1–28, 35, 126, 160  
Responder 🟡 ..... 504.5–34  
Response Strategies ..... 504.1–19  
Response Time ..... 504.1–30  
Restore ..... 504.1–122  
Return Pointer ..... 504.3–119-120, 179-180  
Revealer 🌈 ..... 504.3–79  
Reverse Engineering ..... 504.4–69, 78, 81, 86  
..... 504.5–29  
Reverse WWW Shell ★★★ ..... 504.5–167  
RIPEMD-160 ..... 504.4–25  
Riverbed Cascade ..... 504.4–192  
RLogin ..... 504.3–79  
robots.txt ..... 504.2–46, 179  
Rootkit ..... 504.1–117  
..... 504.5–7, 504.5–59-62  
    Kernel-Mode ..... 504.5–83  
    Linux ..... 504.5–62-66  
    User-Mode ..... 504.5–70  
Rootkit Hunter ..... 504.5–113  
Rootkit Revealer 🌈 ..... 504.5–114  
RTIR ..... 504.1–102

## S

S-Mail ..... 504.5–223  
S-Tools ★★ ..... 504.5–219  
SADoor (Backdoor) ..... 504.5–198  
SafeBack ..... 504.1–40  
SAINT ..... 504.2–152  
Salt ..... 504.4–20-21  
SAM Database ..... 504.3–139  
..... 504.4–5, 32  
..... 504.5–17  
Santy ..... 504.2–43  
SaranWrap ..... 504.5–28  
Sasser 🌈 ..... 504.4–62-63

SATAN ..... 504.2–151  
..... 504.3–23  
Scan Types  
    FTP as Source Port ..... 504.2–110  
Scapy ..... 504.3–6, 74  
Script Kiddie Approach ..... 504.3–121  
SearchDiggity ..... 504.2–45  
SEC's Edgar database ..... 504.2–33  
Secure Shell ..... 504.3–13, 85  
..... 504.5–172  
SecureLogix ..... 504.2–61  
Sentinel ..... 504.3–74  
..... 504.4–25  
Session Hijacking ..... 504.3–79  
    Defense ..... 504.3–85-87  
Session Tracking ..... 504.4–129-130  
    Defense ..... 504.4–141-144  
    Information ..... 504.4–131-132, 140  
Setiri ..... 504.5–22-23  
SHA-x ..... 504.4–25  
Shaft ..... 504.4–184  
Shell ..... 504.4–95  
    Listening ..... 504.4–77  
    Login ..... 504.3–25  
    Remote Command ..... 504.4–24  
    Reverse ..... 504.3–27, 40  
    ..... 504.5–53  
    Reverse WWW ..... 504.5–167-168  
    Shoveling ..... 504.3–27  
    XSS ..... 504.4–120-121  
Short-term actions ..... 504.1–104  
showcode.asp ..... 504.2–177  
SIFT kit ..... 504.1–41  
SInAr 🌈 ..... 504.5–104  
SiteDigger ..... 504.2–44-45  
SL4NT 🟡 ..... 504.5–157  
SlashDot ..... 504.4–112  
Slowloris Attack ..... 504.4–154  
    Defense ..... 504.4–155  
SMB ..... 504.2–190, 201  
..... 504.4–54  
    smbclient ..... 504.2–211, 216-217  
    ..... 504.3–204  
    ..... 504.5–146  
Smurf ..... 504.2–94, 504.4–158  
    Amplifier ..... 504.4–160-161  
    Attack ..... 504.4–160  
    Defense ..... 504.4–162-163  
SnadBoy 🗑️ ..... 504.4–50  
Snare Agent and Log Server 🟡 ..... 504.5–157  
Snarfing ★★ ..... 504.3–61  
Sniffers ..... 504.3–51  
Sniffing Backdoor ..... 504.5–195-200  
    Defense ..... 504.5–201  
Sniffit ..... 504.3–84  
SNMP ..... 504.2–197  
Snort ..... 504.2–145  
..... 504.3–155

# SANS SEC504 – Hackers Techniques and Incident Handling

Socat .....	504.3–17
Social Engineering .....	504.2–19
.....	504.3–71
.....	504.5–260-261
Social Networking .....	504.4–73
Solidcore FIM ● .....	504.5–78
Sophos Anti-Rootkit 🌈 .....	504.5–115
Source Routing .....	504.3–11, 18
Sourcefire .....	504.5–117
SPEC .....	504.5–31
Speed Guide .....	504.1–57
Spike .....	504.4–180
Split DNS .....	504.3–109-110
SQL Injection .....	504.4–100-106
Defense .....	504.4–107-108
Example .....	504.4–103-106
Standard DB Logic Elements .....	504.4–102
Useful Entities .....	504.4–102
Sqlmap .....	504.4–101
SSH .....	504.3–73, 79
.....	504.5–165
SSHmitm .....	504.3–63, 69
SSID .....	504.2–64-69
Cloaking .....	504.2–64-65
SSL .....	504.2–180
.....	504.4–130, 504.4–138-139
Certificate .....	504.4–138-139
Connection .....	504.4–139
Dodging Browser Warnings .....	504.3–70-71
Sniffing .....	504.3–66
sslstrip .....	504.3–72
Stacheldraht .....	504.4–184
Stack .....	504.3–119-120
Stash .....	504.5–223
Stealth Patch .....	504.2–119
Steganography .....	504.5–203-230
Defense .....	504.5–231-233
File Generation .....	504.5–213
Injection .....	504.5–210-211
Substitution .....	504.5–212
Stegdetect .....	504.5–233
Storm .....	504.4–59
Streams 🌈 .....	504.5–147
Streams Shell Extension 🌈 .....	504.5–147
Stuxnet .....	504.4–59, 61-63
.....	504.5–87
Sub7 .....	504.5–10, 504.5–16
SubVirt .....	504.5–90
SUCKit 🌈 .....	504.5–88
Symbolic Link (attack) .....	504.1–131
SYN Floods .....	504.4–172-174
Defense .....	504.4–175-176
SYN-ACK .....	504.4–173, 176
Syscall Table .....	504.5–111
SYSKEY .....	504.4–32
Syslog .....	504.5–157
System .....	504.5–82
Call .....	504.5–82, 85

Library .....	504.5–82, 85
Memory Map .....	504.5–88
System Rebuild .....	504.3–86, 150
.....	504.4–97
.....	504.5–79
System-Level Processes .....	504.2–189
Systrace 🌈 .....	504.5–111

## T

Targa .....	504.4–180
TCP .....	504.2–96-99
3-Way Handshake .....	504.2–98, 101, 179
.....	504.3–6, 10
.....	504.4–172, 186
.....	504.5–177
Header .....	504.2–99
.....	504.5–176
Redirector .....	504.4–78
Scans .....	504.2–101
Sequence Number .....	504.3–8-10, 81
TCP/IP Stack .....	504.3–13
.....	504.4–173
tcpdump .....	504.1–55
.....	504.2–27, 70, 123, 140, 166
.....	504.3–52, 155
tcpkill .....	504.3–60
tcpnice .....	504.3–60
tcptraceroute .....	504.2–130
TCPView (Sysinternals) 🌈 .....	504.5–24, 194
TearDrop .....	504.4–148
Telnet .....	504.3–79-80, 85
THC Hydra .....	504.4–8
THC Scan .....	504.2–55-56
The Sleuth Kit .....	504.1–40
.....	504.3–154
Themida .....	504.5–31
Thinstall ● .....	504.5–31
Tini (backdoor) .....	504.1–56
Tiny Fragment Attack .....	504.2–143
Tipping Point .....	504.5–117
TLS .....	504.3–138
Tmp File Format 🌈 .....	504.5–130
Toast .....	504.4–180
TopLayer .....	504.5–117
Traceroute .....	504.2–88-90
.....	504.4–25
Trade Secret .....	504.1–176
Trademark .....	504.1–173
Transaction ID Number .....	504.3–100
Tribe Flood Network .....	504.4–184
Trin00 .....	504.4–184
Tripwire .....	504.5–78, 81, 116, 504.1–284
.....	504.5–78, 81
Trojan Horse .....	504.1–55, 249
.....	504.2–13
.....	504.4–68
.....	504.5–6, 28



# SANS SEC504 – Hackers Techniques and Incident Handling

Backdoor .....	504.5–10, 22
Defense .....	504.5–24-25
Trojan Man .....	504.5–28
TTL .....	504.2–86, 113, 126-127, 134
Shenanigan .....	504.2–135
TTYSn00p 🐼 .....	504.3–79
TTYSpy 🐼 .....	504.3–79
Tunneling .....	504.5–165
Twitter .....	504.3–72
.....	504.4–73

## U

UDP .....	504.2–96-97
Header .....	504.2–100
Unauthorized Use .....	504.1–143
Unusual Items .....	
Accounts .....	504.1–75, 88, 280-281
Files .....	504.1–69, 83, 275-277, 287-288
Log entries .....	504.1–76, 89, 282, 292
Network Usage .....	504.1–85, 278, 289
Processes .....	504.1–67, 81, 273, 286
Registry keys .....	504.1–70, 84
Scheduled Tasks .....	504.1–86-87, 279
Services .....	504.1–68, 82, 274
UPX ★★ .....	504.5–31
URL .....	504.4–90-91, 95, 111-113
URLsnarf .....	504.3–61
User Input Validation .....	504.4–87
User-Mode Linux .....	504.4–81
User-Mode Rootkit .....	504.5–70-76
Defense .....	504.5–77

## V

Vbootkit .....	504.5–7
Veracode Suite .....	504.3–148
ViewFrame Google Recon Technique .....	504.2–43
Virtual Machine .....	504.4–81-84
Detection .....	504.4–81-82
Environment .....	504.4–81-84
Escape .....	504.4–83
VirtualPC .....	504.4–81, 83
Vitriol .....	504.5–90
VMcat .....	504.4–83
VMware .....	504.1–205-225
.....	504.4–81, 83
VNC .....	504.5–10, 504.5–11-14
Client .....	504.5–13
VoIP .....	504.2–57
Volatility Framework .....	504.5–35-38
Volatility Framework ★★★ .....	504.1–41, 107
.....	504.5–34
VOMIT .....	504.1–53
VPN .....	504.1–23
.....	504.2–77
.....	504.3–13, 73, 79, 85
Vulnerability .....	

Analysis .....	504.1–119
Scanners .....	504.2–151
Defense .....	504.2–157
Vulnerable Systems .....	504.2–43
.....	504.4–65, 77

## W

w3af (MitM proxy) .....	504.4–137
WAF .....	504.4–143
War Dialing .....	504.2–19, 54
War Driving .....	504.2–19
.....	504.4–25
Defense .....	504.2–76-78
Warhol .....	504.4–64
Warhol/Flash Technique .....	504.4–65
Warning Banner .....	504.1–18, 137, 161
WarVOX .....	504.2–57-58
Waste (Peer-2-Peer) .....	504.4–73
Weak Functions .....	504.3–123
gets .....	504.3–116
printf .....	504.3–159, 166
snprintf .....	504.3–162, 167, 171-179
strcpy .....	504.3–116
Web Application .....	504.4–141
Defense .....	504.4–141-144
Pen Test .....	504.4–87
Web Scanners .....	504.2–177
Defense .....	504.2–186
Web Site Searches .....	504.2–32
WebGoat .....	504.4–87
Webmitm .....	504.3–63, 66
WebScarab .....	504.4–87, 137
Webspy .....	504.3–62
Wellenreiter .....	504.2–68-69
WEP .....	504.2–64, 66-67, 70
WEPCrack (WEP) .....	504.2–70
wget 🌐 🐼 .....	504.4–67
Whisker .....	504.2–179, 504.2–181, 181-185
White List Approach .....	504.4–125
Whois .....	504.4–163
Databases .....	504.2–20-21, 54
Defense .....	504.2–23
Reconnaissance .....	504.2–24
Wikto .....	504.2–44-45
win32dd .....	504.5–34
Windows Credentials Editor 🌐 .....	504.4–55
Windows Event Log Files .....	504.5–150
Editing .....	504.5–152-153
Winfingerprint .....	504.2–192, 504.2–197-198
WinNuke .....	504.4–148
WinTrin00 .....	504.4–184
WinVNC .....	504.5–14
WinZapper 🌐 .....	504.5–153
Wireshark .....	504.3–52, 152, 155
WMI .....	504.2–197
Word Mangling .....	504.4–13
Worm .....	504.4–58-70

# SANS SEC504 – Hackers Techniques and Incident Handling

---

Defense .....	504.4-70, 79
Fast-Spreading .....	504.4-64, 70
History & Evolution .....	504.4-59-60
Metamorphic .....	504.4-69
Multi-Exploit .....	504.4-61
Multi-Platform .....	504.4-62
Polymorphic .....	504.4-66-67
Purpose .....	504.4-68
Segment .....	504.4-58, 65-66
Zero-Day Exploit .....	504.4-63
WPA .....	66-67, 71
Wrapper .....	504.5-28
wtmped.c 🚩 📁 .....	504.5-131
wzap.c 🚩 📁 .....	504.5-131

## X

Xcrush .....	504.4-180
--------------	-----------

Xen .....	504.4-81, 83
XOR Payloads & Encoder .....	504.4-67
XProbe (OS fingerprinting) .....	504.2-94, 111
XSS Attack .....	504.4-115-117, 123, 127
XSS Shell .....	504.4-120

## Y

Yoda .....	504.5-31
------------	----------

## Z

Zed Attack Proxy .....	504.4-101, 137-138
Zenmap (Nmap GUI) ★★★ .....	504.2-121
Zero-Day Exploit .....	504.3-121
.....	504.4-63
Zombie .....	504.4-186-187
Zotob .....	504.4-59, 63