SEC504 – Hacker Tools, Techniques, Exploits, and Incident Handling

A

- AAD3 4–16
- Access Point Renegade 2–75
- Account 1–71
  - Harvesting 4–91
  - Harvesting (Defense) 4–96
- ACK Scan 2–93
- ACK Scanning 2–94
- Active Defense Harbinger Distribution 1–107
- ActiveX 3–149
- Add'n'edit Cookie 4–144
- Address Space Layout Randomization 3–109
- ADHD → Active Defense Harbinger Distribution
- Advanced Threat Analytics (Microsoft) 5–117
- AFRINIC 2–20
- AIDE 1–258
- Air Magnet 2–75
- Aircrack-ng 2–64
- Aldrick Ames 1–187
- Ankle Biters 2–9
- Anonymous Remailer 2–10
- Anti-disclosure 2–9
- Anti-Rootkit 5–66
- AntiPhishing.org 1–169
- API Hooking 5–45
- APNIC 2–2020
- Application Data
  - Snarfing 3–54
- Application Whitelisting 3–121, 3–145
- applocker 3–121
- apropos 1–243
- Arbor Networks 4–167, 4–171
- ARIN 2–20
- Armitage 3–113
- ARP 3–48, 1–252
  - ArpScan 2–142
  - ArpSpoof 3–51
  - ARPWatch 3–85
  - Cache poisoning 3–52
  - Display 🐧 3–85
  - Display ⊞ 3–85
  - Preload 4–185
  - Scan 2–93
  - Spoofing 3–49
- Aruba Networks 2–75
- ASLEAP 2–64
- ASLR → Address Space Layout Randomization
- ASN → Autonomous System Number
- Assembly 3–144
- at 1–73
- Audit Log Configuration 1–89
- Aurora 1–160
- Auto Start Entry Point 1–69, 1–142
- Autonomous System Number 3–8
- Autopsy 1–41
- autoruns.exe 1–69
- autorunssc.exe 1–141
- awk 5–143

B

- Backdoor 5–6
  - Application-Level 5–7, 5–9
  - BackdoorFactory 3–53, 3–146
  - Capabilities 5–15
- Backup 1–118
- Bad Characters 3–106
- Badsum 2–114
- Base64 1–76
- Bash 1–76
- BCP → Business Continuity Plan
- Beacon 1–136
- BEAST 3–66
- Beef → Browser Exploitation Framework
- Bell-LaPadula 4–123
- BetterCap 3–51, 3–53, 3–58
- BeyondTrust 2–119
- bg 1–227
- BGP Hijacking 3–8
  - Defense 3–9
- Binders 5–18
- BIOS 3–6
- BlackShade 5–9
- Blame game 1–115
- BloodHound 2–143
- Blowfish 5–150
- BlueCoat 1–172
- BluePill 5–58
- bonk 4–161
- Bot 4–66
  - Communication 4–68
  - Defense 4–74
  - Distribution 4–67
  - Functionality 4–72
  - Herder 4–66
- Botnet 4–66
- Bounce operation 5–130
- BreachAlarm 2–43
- Bro 1–147
- Browser Cache 4–132
- Browser Exploitation Framework 4–76, 4–120
- Brute-force Attack 4–10, 4–12
- btmp 5–89
- Buffer Overflow 3–95
  - Defense 3–121, 3–125, 3–128-129
  - Exploit 3–100
  - Exploitation Steps 3–102
- Bugtraq 1–15
- Burp 4–91, 4–104, 4–146
- Business Continuity Plan 1–10
- Bypass 3–136

C

- Cain 4–16, 4–24
- Cain and Abel 4–10, 4–23
- Canary 3–124

- Canonicalization 4–110
- CasFax 2–38
- cat 1–220
- cat 🪟 3–32
- cd 1–214
- Center for Internet Security 5–64, 1–77
- Chain of Custody 1–97
- CheatSheets 1–60
- Checklist 1–31
- Child Pornography 1–171
- Chkrootkit 5–65, 1–257
- Chris Truncer 2–98
- CIS Hardening Guidelines 1–258
- CISCO 2–75
- Cisco Guard DDoS Mitigation 4–171
- Citrix NetScaler 4–150
- CloudFlare 4–171
- Code Cave 3–146
- Code Checking Tools 3–127
- COM+ 3–149
- Command Injection 4–98
  - Defense 4–101
- Command Post 1–32
- CommandLineKungFu 1–126
- Communication Channels 1–52
- Computer Staff (College, University) 1–109
- Cone of Silence 5–61
- configure 1–237
- Connect Scan 2–93
- Connection Broker 3–11
- Connection Data 1–136
- Containment
  - Deployment 1–101
  - Long-term 1–113-114
  - Managment 1–103
  - Objective 1–99
  - Short-term 1–107-108
  - Sub-phases 1–100
- Contains and Clear 1–22
- Continuing Operation 1–112
- Copyright 1–182
- Counter Hack Challenge 1–37
- Counting
  - command 4–174
  - connections (established,linux) 4–188
  - connections (established,win) 4–182
  - connections (half-open,linux) 4–187
  - connections (half-open,win) 4–179
  - process 🐧 4–183
  - process 🪟 4–178
- Court Order 1–24
- Coverity Static Analysis 3–127
- Covert Channel 5–120
  - Defense 5–134, 5–145
  - Plain-Sight 5–136
  - TCP 5–127
- Covert_TCP 5–127
  - Extensions 5–131
- CoWPAtty 2–65
- CPU Hog 4–154
- Crack Station 4–22
- Cracker 2–5
- Crawler 2–33
- Credential
  - Bypass 3–4
  - Harvesting 3–64
- Credentialed scan 2–124
- Credentials Hacking 2–67
- CRIME 3–66
- crontab 1–253
- Cross-Site Scripting 4–113
  - Admin 4–122
  - Anti-XSS 4–124
  - Defense 4–124-126
  - Evidence 4–132
  - Example 4–115
  - Internal System 4–119
  - Reflected 4–117
  - Stored 4–118
  - Walkthrough 4–117
- Crown Jewels 1–161, 1–182
- cryptcat 3–11
- Crypto Key 1–34
- CVE Mitre 1–95
- Cyber Crime Law 1–185
- CyberCPR 1–105
- CyberSponse 1–104

D

- Damage 1–95
- Dameware 5–9
- Dan Kaminisky 3–11, 2–97
- Data Execution Prevention 3–123
- Data Link Layer Vulnerability 3–51
- Data Loss Prevention 4–111
- DataSentinel 5–67
- Dave Hull 1–140
- dd 1–41, 1–178
- DeathStar 2–143
- debsums 1–251
- Debug Priviledge 5–45
- Deception 1–164
- Defense Improvement 1–120
- Denial-of-Service 4–153
  - Bot 4–161
  - Category 4–154
  - Defense 4–170
  - Distributed 4–163
  - Distributed (architecture) 4–164
  - Distributed (pulsing zombie) 4–166
  - Distributed (reflected attack) 4–165
  - Flooding 2–75
  - Suite 4–161
- Detection 1–53
  - Application-level 1–58

  - Host Perimeter 1–55-56
  - Network Perimeter 1–54
  - System-level (Host) 1–57
- Device Driver 5–55
- df 1–257
- Dictionary Attack 4–10-11
- dig 2–24
- Digital Millenium Copyright Act 2–9
- Disaster Recovery Plan 1–10
- Disclaimer 2–7
- Distributed Attacks 5–189
- Distributed Denial-of-Service 4–163
- DLP → Data Loss Prevention
- DMCA → Digital Millenium Copyright Act
- DNS 3–47, 3–50, 1–134
  - Amplification Attack 4–156
  - Amplification Attack (architecture) 4–158
  - Display ⊞ 3–85
  - EDNS 4–157
  - Foiling 3–56
  - Record 2–25
  - Round-robin 4–70
  - Spoofing 3–58
  - Spoofing Effect 3–57
  - Zone transfert 2–25
  - Zone transfert (defense) 2–27
- DNS Servers 2–84
- dnscat 3–11
- DNSCat2 5–132
- DNSniff 3–63
- DNSStuff.com 2–51
- DoDNIC 2–20
- Domain Name Registration 2–18
- Domain Password Spraying 2–161
- Drive Duplicator 1–111
- DroidSheep 3–67
- DRP → Disaster Recovery Plan
- DShield 1–15

E

- EasyCreds 2–67
- Ebowla 3–146
- ECP → Emergency Communication Plan
- ECTF → Electronic Crime Task Force
- Edge Router 2–84
- EDI → Electronic Data Interchange
- EDNS 4–157
- Egress
  - Anti-spoof 4–170
- Egress,Data 1–133
- Electronic Crime Task Force 1–25
- Electronic Data Interchange 4–123
- EliteWrap 5–18
- Email Evidence 1–167
- Emergency Communication Plan 1–33
- EMET → Microsoft Enhanced Mitigation Experience Technique
- Employee 1–174
  - Monitoring 1–178
- EnCase 1–41
- Enhanced Mitigation Experience Technique (Microsoft) 3–122
- Enterprise Incident Reponse 1–132
- enum 2–139
- Equipment Seizure 1–24
- Eradication 1–117
- Eric Conrad 1–136
- Espionage 1–160-161
  - Identification 1–162
- Ettercap 2–68
- Event (definition) 1–12
- EventLogEdit 5–115
- eventquery.vbs 1–74, 1–191
- eventvwr.msc 1–74
- Evil Grade 2–12, 2–68
- Exabeam 5–117
- Exe32pack 5–19
- Exec2VBA 5–18
- Exec2VBS 5–18
- ExpertWitness 1–179
- Exploit-DB 3–101
- Exploit-db 2–35
- exploitable 3–104
- External Access 3–136
- EyeWitness 2–98

F

- F5 Application Security Manager 4–150
- False Positive 1–94
- Fast-flux 4–69-71
- fboweb 2–38
- fc 1–72
- fg 1–228
- fgdump 4–29, 4–35
- fgets 3–96, 3–103
- Fiddler 4–146
- File,Integrity Checking 5–67
- File,Parser 3–133
- Files
  - large 1–72
  - unusual 1–72
- FIN Scan 2–93
- find 4–174, 1–218, 1–249
- findstr 1–83
- Firebug 4–144
- FireSheep 3–67
- Firewire 3–4
- Fixes 1–130
- Flash (worm) 4–61
- FlawFinder 3–127
- FOCA 2–41-42
- FOR 1–72
- Forensics Image 1–110
- Forensics Toolkit 1–41

- Fortify Source Code Analyzed 3–127
- Fragmented Routing 3–12
- FragRouter 3–52
- free 1–257
- FTKImager 5–22
- FTP Proxy Bounce Attack 2–93
- FU 5–56
- Full Disclosure 2–9
- Future 5–189

G

- GCat 5–133
- GECOS 4–36
- gedit 1–219
- Generic Route Encapsulation 4–73
- gets 3–96, 3–103
- getws 3–103
- ghost 1–178
- GhostRAT 5–9
- Ghostwriting 3–143
- Gmail 5–133
- Golden age 2–14
- Google cache 2–39
- Google Dork 2–35
- Google Maps 2–36
- Google Search Engine 2–40
- GrammarTech 3–127
- GRE → Generic Route Encapsulation
- grep 4–174, 1–240
- GRR 1–39
- grsecurity 3–122

H

- Hacker 2–5
- Hacktivism 2–10
- Handle.exe 1–141
- Hard-drive Encryption 3–4
- Hardening Template 5–64, 1–77
- Harrasment 1–168
- Hash 2–13
- Hashcat 4–10
- hashdump 4–29
- head 1–220
- HearthBleed 3–65
- Help Desk 1–39
- Hg.org 1–185
- Hiding files 🐧 5–82
- Hiding files 🪟 5–104
- Hiding tools (Categories) 5–44
- High Orbit Ion Canon 4–169
- High Tech Crime Investigation Association 1–25
- Hijacking 3–79
  - Defense 3–84
- HKCU 1–69
- HKLM 1–69
- HOIC → High Orbit Ion Canon
- honeynet 1–22
- Hop Limit 2–81
- host 2–24
- HP SPI Dynamics 4–146
- hping 4–179
- HR 1–177
- HSTS → HTTP Strict Transport Security
- HTCIA → High Tech Crime Investigation Association
- HTTP Flood 4–167
- HTTP Request Manipulation 4–144
- HTTP Strict Transport Security 3–68
- hub 3–45
- Human Ressource 1–170
- Hunting 1–136
- Hydan 5–148
  - detection 5–153
  - efficency rate 5–153

I

- IANA 1–56, 2–89
- IAX Protocol → Inter-Asterix Protocol
- IBM 2–75
- ICMP 2–82
- ICMP Tunnel 5–122
- ICMPCmd 5–124
- ICMPShell 5–124
- id 5–98
- Idle Scan 2–93
- IDS
  - Evasion 2–114
  - Evasion (defense) 2–116
  - Wireless 2–75
- ifconfig 1–232
- IKE → Internet Key Exchange
- IKE Crack 4–26
- Immunity Debugger 5–20
- Inappropriate Web Access 1–170, 1–172
- Inception 3–4
- Incident
  - Characteristics 1–102
  - Definition 1–11
  - Identification 1–53
- Incident Handler Assignment 1–50
- Incident Handling
  - Definition 1–10
  - PICERL 1–14
  - Preparation 1–19
  - Steps 1–17
- Incident Reporting 1–36
- Incident Update Report 1–29
- inetd 2–104
- Information Corroborating 1–12
  - Example 1–13
- Information Sharing 2–10
- InfraGuard 1–25
- Ingress Data 1–133

- Initial Analysis 1–106
- Initial Assessment 1–96
- Insider Activity Identification 1–176
- Insider Threat 1–174
- InSSIDer 2–61, 2–77
  - Defense 2–61
- InstallUtile-Shellcode.cs 3–147
- Instruction Pointer 3–97
- Intellectual Property 1–10, 1–181
- Inter-Asterix Protocol 2–54
- Internet Key Exchange 4–26
- Internet Storm Center 1–15, 1–59
- InterNIC 2–19
- Intrusion Detection 1–63
- InvisibleSecret 5–148
- IP Block 2–20
- IP Header 2–81
- IPSec 4–26
- iptables 1–203
- IPv6 Scanning 2–93
- ISP 1–109

J

- jobs 1–228
- John the Ripper 4–10, 4–35, 4–46
  - Cracking modes 4–38
  - Input/Output 4–39
- jolt 4–161
- Jordan Ritter 2–139
- Josh Wright 2–65
- JSteg 5–148
- Judy Novak 2–114
- Jump Bag 1–40-47

K

- Kansa 1–140-144
- Karma 2–69
- Karmetasploit 2–69-71
- Kerberos 4–25
- Kernel module 5–55
  - defense 5–56
- Keylogger (JS) 3–54
- kill 2–104
- killall 2–104
- Kismet 2–63
- Kiwi Syslog 5–117
- Klocword Insight Pro 3–127
- Kon-boot 3–4, 4–29

L

- LaBrea 1–22
- LACNIC 2–20
- LADS 5–106
- LANMAN
  - Disabling 4–32
  - hash 4–16-18
  - hash (benchmark) 4–18
  - Pass-the-Hash 4–49
- LanTurtle 3–4
- Law enforcement 1–23-25
- Layer 3 Encryption 2–73
- Leak 1–162
- LEAP 2–60, 2–64
- Lenny Zeltser 1–96
- less 1–221
- Lesson Learned 1–128
  - Meeting 1–129
- linkcat 3–11
- LinRES 1–104
- Linux
  - Account 1–255
  - File structure 1–213
  - Files 1–252
  - Find unowned files 1–230
  - Free Space 1–256
  - Log 1–247
  - Memory 1–257
  - Network Usage 1–253
  - Processes 1–248
  - Scheduled Tasks 1–254
  - Services 1–250
  - Uptime 1–257
- LLMNR → Local Link Multicast Name Resolution
- LM Challenge 4–25
- Local Link Multicast Name Resolution 3–6, 3–50, 3–79
- Local Security Authority Subsystem Service 4–49
- locate 1–218
- Log 1–133
- Log Files 1–74
  - accounting 🐧 5–89
  - Edit (windows) 5–114
  - edit 🐧 5–85
  - Editing (Defense) 5–117
  - Espionage 1–163
- Log Server 5–117
- Log Wiper 5–89
- LogParser 1–141
- LOIC → Low Orbit Ion Canon
- LOKI 5–124
- Long-tail Analysis 1–140
- Low Orbit Ion Canon 4–168
- ls 1–215
- LSASS → Local Security Authority Subsystem Service
- lsof 1–56, 2–103, 1–234, 1–247, 1–250, 1–252
- lusrmgr.msc 1–88

M

- Mac Address Filtering 2–72
- macro_safe.py 3–143
- Mag Stripe 4–123

- make 1–237
- Malformed Packet Attack 4–154
- Maltego 2–46, 47
  - Defenses 2–48
  - Transforms 2–47
- Malware Domain List 1–134
- Malware Layer 5–7
- man 1–243
- Man-in-the-middle Framework 3–51, 3–53, 54
- Masscan 2–97
- McAfee Foundation Scan 2–119
- MD5 2–13
- mdd 5–22
- memcpy 3–103
- memmove 3–103
- Memory Analysis 5–22
- Memory Dump 5–22
- Memory hog 5–56
- Memoryze MemoryDD 5–22
- Metasploit 3–111
  - Additional features 3–118
  - Architecture 3–112
  - Benefits 3–120
- Meterpreter 3–116
  - clearev 5–116
- Mimikatz 4–51
- mkdir 1–217
- ModSecurity 4–110, 4–124, 4–150
- Money Making 2–11
- Monitoring (After eradication) 1–125-126
- Morto (worm) 4–58
- Motorola Air Defense 2–75
- MP3Stego 5–148
- msconfig 1–70
- msfelfscan 5–56, 3–119
- msfpayload 4–77
- msfpescan 5–56, 3–119
- msfvenom 4–77, 3–137
- msyslog 5–119

N

- Name resolution 3–50
- Namechk 2–30
- NAT 3–11
- nbtstat 1–65
- nc 2–14, 1–81, 2–111
- ncat 3–11, 1–41
- Need to Know 1–51
- Nessus 2–119-120, 2–120, 1–121, 2–121
  - Architecture 2–121
  - Attack Scripting Language 2–123
  - Platform Support 2–122
  - Plugins 2–123
- nestea 4–161
- net
  - localgroup 1–71
  - session 2–146
  - start 1–68
  - use 2–137, 138, 2–146
  - use (pass-the-hash) 4–50
  - user 1–71
  - view 2–139
  - view/session/use 1–65
- NetBIOS
  - Name Resolution 3–50
  - nbstat 1–65
  - SMB 2–137
- netcat 3–11, 1–41
  - Backdoor 3–19-20
  - Backpipe relay 3–23-24
  - Client mode 3–12
  - Data transfert 3–16
  - Defense 3–26
  - Establishing Connection 2–111
  - Establishing connection 3–18
  - Gaping security hole 3–25
  - Listen mode 3–13
  - Options 3–14
  - Port scanning 3–17
  - Relay 3–22
  - Relay without -e 3–25
  - Reverse shell 3–21
  - Use 3–15
  - Vulnerability scanning 3–17
- Netflow 1–136
- Netsh 2–73-74
- netsh 3–30, 1–66, 1–203
- netstat 1–55, 56, 1–81, 1–234, 1–252
  - Linux 2–103
  - Options 1–66
  - Win 2–101
- NetStumbler 2–61
  - Defense 2–61
- Network layers 3–47
- Network Mapping 2–80
  - Defense 2–85-86
- Network Miner 3–55
- Network Usage 1–65
- Network-Tools.com 2–51
- NeuStar SiteProtect 4–171
- newtear 4–161
- Night Dragon 1–161
- Nimda 1–96
- Nmap 2–80, 2–107, 1–121
  - Active OS fingerprinting 2–95
  - Default packets 2–82
  - Root vs non-root 2–107
  - Scan types 2–93
- No Free Bug 2–9
- nohup 3–20, 5–100
- Non-repudiation 4–14
- NOP 3–109
- Note 1–27
- nslookup 2–24-25
- NT hash 4–16, 4–19

- NTFS ... 5–104
  - Alternate Data Stream ... 5–105
  - Finding Hidden Stream ... 5–106
- NTLDR ... 5–57
- NTLM ... 4–25
  - NTLMv1 (Pass-the-Hash) ... 4–49
  - NTLMv2 ... 3–88
- Ntoskrnl.exe ... 5–57

O

- omnipeek ... 2–64
- Onion Live ... 1–104
- Open Web Application Security Project ... 4–89
- OpenPuff ... 5–149
- OpenStego ... 5–149
- OpenVAS ... 2–119, 1–121
- OS Fingerprinting ... 2–95
- OSINT ... 2–30
  - defense ... 2–33
- OSSEC ... 5–67
- Out-of-Band Communication ... 1–52, 2–53
- OWASP → Open Web Application Security Project ..
- OWASP Stinger ... 4–150

P

- PacDoor ... 3–83
- Packer ... 5–19
- Packet Flooding ... 4–154
- Packet Storm Security ... 3–101
- PAM → Policy Authentication Modules ...
- Pass-the-Hash
  - Architecture ... 4–50
  - Attacks ... 4–49
  - Defense ... 4–52
  - Tools ... 4–51
- passwd ... 1–210, 1–254
- Password ... 1–34
  - Blank ... 4–16
  - Cracking ... 4–9
  - Defense ... 4–31
  - Dumping ... 4–29
  - Dumping ⊞ ... 3–4
  - Expiration Policy ... 4–10
  - file 🐧 ... 4–36
  - file:// ... 4–30
  - Guessing ... 4–6
  - Lenght ... 4–17, 4–33
  - Policy enforcement 🐧 ... 4–40
  - Policy enforcement ⊞ ... 4–33
  - Salt ... 4–19-20
  - smb:// ... 4–30
  - Spraying ... 4–7
  - Windows Storage ... 4–16
- Password Storage ... 4–5
- Patent ... 1–182
- PATH ... 1–223
- PaX ... 3–122
- Payload (keyed) ... 3–146
- PE Bundle ... 5–19
- PE Compact ... 5–19
- PeepNTom ... 2–98
- Peer Notification ... 1–26
- PenTestGeek ... 3–143
- Permission to Attack ... 2–8
- Personal Healthcare Information ... 1–23
- Personally Identifiable Information ... 1–23, 4–111
- PGP Signature ... 2–13
- PHI → Personal Healthcare Information ...
- Phishing ... 1–20, 1–169
- PHP PDO ... 4–110
- Physical Access
  - Attacks ... 3–4
  - Defense ... 3–6
- PII → Personally Identifiable Information ...
- ping ... 1–233
- Ping of Death ... 4–154
- Ping sweeps ... 2–93
- PingChat ... 5–124
- PoisonIvy ... 5–9, 5–14
  - Configuration ... 5–14
- Policy
  - Banners ... 1–21
  - Response Strategies ... 1–22
- Policy Authentication Modules ... 4–41
- Port
  - Listing 🐧 ... 2–103
  - Listing ⊞ ... 2–101
  - Scanner ... 2–88
  - Scanner (Defense) ... 2–100
  - wrapping ... 2–113
- Port 111 ... 2–93
- Port 135-139 ... 2–137, 2–148
- Port 137-139 ... 2–109
- Port 161 ... 2–93
- Port 445 ... 2–89, 2–109, 2–137, 2–148
- Port 53 ... 2–89
- Port 80 ... 2–89
- Port 8834 ... 2–121
- Positive Skew Analysis ... 1–140
- Post-Exploitation ... 3–112
- Postal Mail ... 4–123
- POT file ... 4–39
- Powerbleed ... 3–65
- Powerpoint ... 3–139
- PowerShell ... 1–140, 2–159
  - Import-Module ... 2–155
  - Set-ExecutionPolicy ... 2–155
- PowerShellEmpire ... 2–142
- Procedure ... 1–31
- Process Explorer ... 1–77
- Process Monitor ... 1–77
- Processes ... 1–67
- Program

  - run (how) 3–97
  - stack 3–99
- Protocol Parser 3–132
- ProxyCanon 2–99
- ps 1–226, 1–247
- psexec 4–51, 2–137
- PTunnel 5–124
- PunkSpider 2–51
- PushPin 2–31
- pwd 1–214
- pwdump3 4–35
- PwnedList 2–43

Q

- Qualys 2–119, 1–121
- QueSO 2–95
- QUICK 5–132

R

- Rainbow table 4–22
  - Project Rainbow Crack 4–22
- Ransomware 2–10
- Rapid7 NeXpose 2–119, 1–121
- Rapid7 User Behavioral Analytics 5–177
- RATS 3–127
- RDP 2–98
- reboot 1–245
- Recon-ng 2–43
- Reconnaissance 2–16
- Recovery 1–123
- Reddit 1–29
- RedLine 1–131
- reg 1–69, 2–137
- regedit 1–70
- Registry Keys 1–69
- Rekall 1–110
  - dlllist 5–27
  - modules 5–23
  - netscan 5–25
  - netstat 5–25
  - pslist 5–26
- Relative Identifier 2–153, 2–155
- Relay 3–11
- Remote Desktop 1–119
- Remux 2–99
- Renaud Deraison 2–120
- Report 1–128
- Reporting (horizontal/vertical) 1–104
- Responder 3–4, 3–80, 3–88
- Response Team 1–30, 1–32
  - Training 1–37
- Restore Operation 1–124
- Return pointer 3–108
- Reverse HTTP Shell 5–122
- RFC 1149 5–120
- RFC 2549 5–120
- RID → Relative Identifier
- Ring 5–51
- RIPE 2–20
- RIPEMD-160 2–13
- RITA 3–128, 1–147
- Riverbed Cascade 4–167, 4–171
- Robert D. Gratam 2–97
- Robert Manssen 1–187
- Rootcheck 5–65
- Rootkit 5–41
  - Altering files 5–57
  - Altering memory 5–56
  - Avatar 5–62
  - Defense 5–64
  - Detection 🐧 5–65
  - Detection 🪟 5–66
  - Eradication 1–119
  - Fontanini 5–63
  - Hiding 🪟 5–47
  - Kernel-mode 5–7, 5–50-52
  - Kernel-mode Technique 5–54
  - Linux Components 5–43
  - Platform 5–42
  - User-mode 5–7
  - Virtualization 5–58
  - Windows User-mode 5–45
- Rootkit Detective 5–66
- Rootkit Hunter 5–65
- Rootkit Revealer 5–66
- Rooty 5–60
- Royce Davis 3–143
- RPC Scan 2–93
- RPCClient 2–145
- rpcclient 2–137
  - queryuser 2–155
- RSA SecurID 4–24
- RTIR 1–104
- Rubber Duckies 3–5, 2–74

S

- S-Mail 5–148
- SafeBack 1–178
- SAINT 2–119
- SAM Database 4–5
- Santy Worm 2–42
- SaranWrap 5–18
- Sasser 4–59
- sc 1–68, 2–137
  - config 2–102
  - query 2–102
  - stop 2–102
- scanf 3–103
- ScanRand 2–97
- ScareWare 5–16
- SCCM → System Center Configuration Manager
- Scheduled tasks 1–73

- schtasks 1–73, 1–87
- Screenshoter (JS) 3–54
- Script Kiddies 2–9, 2–16
- SCT Script 3–149, 150
- SCTP 5–132
- Search Engine 2–35
  - Directives 2–37, 38
  - Recon (Defense) 2–44
- SearchDiggity 2–43
- Searching Vulnerable Systems 2–42
- secpol.msc 5–45, 1–89
- Secret Squirel 5–18
- Secure Safe 1–52
- Secure Sphere 4–150
- SecureLogix Voice 2–58
- Security Identifier 2–145
- Security Manager 4–150
- SecuritySpace.cm 2–51
- SELinux 3–122
- Sentinel 4–24
- Service
  - Disabling 🐧 2–104
  - Disabling ⊞ 2–102
  - Listing ⊞ 1–68
- service 1–231, 1–248
- Servicemark 1–182
- Services 1–68
- services.msc 1–68
- Session
  - Cookie Tracking 4–143
  - URL Tracking 4–143
- SET → Social Engineering Toolkit
- Sexually Explicit Content 1–171
- SHA1 2–13
- SHA256 2–13
- Shadow file 4–5, 4–20, 4–37
- ShareFinder 2–142
- Shell
  - reverse 3–21
  - shoveling 3–21
- ShellShock 4–98
- Shodan 2–51
- shutdown 1–244
- SID → Security Identifier
- SIFT 1–42-43
- Signal Science 4–150
- SilentEye 5–149
- sleuthkit 1–41
- SMB 1–65, 2–137
  - Administrative Share 2–139
  - Establish connection 2–138, 2–144
  - NULL Session 2–138, 2–147
  - Pass-the-hash 4–51
  - Session Defense 2–141, 2–147
  - Session Dropping 2–146
  - Session Listing 2–146
- smbclient 2–137, 2–144
- smbmount 2–137
- Smurf Attack 4–156
- SnapBack 1–178
- Snare Agent 5–117
- Snarfing 3–54
- Sneakin 5–59
- sneakin 3–18
- Sniffer 3–45
- Sniffing
  - Passive 2–63
  - Wireless 2–61, 2–64
- socat 3–11
- Social Engineering 1–20, 2–29
  - Social Engineering Toolkit 4–87
- Social Engineering Toolkit 5–18
- Social Problems 1–168
- SOCMINT 2–30-32
  - defense 2–33
- Software Distro Site
  - Attacks 2–12
  - Defense 2–13
- Software Update 2–12
- Solar Designer 4–41
- sort 1–265
- Source Routing 3–12
- SpeedGuide 1–56
- sprintf 3–103
- SQL 4–103
- SQL Injection 4–104
  - Defenses 4–110-111
  - Dropping Data 4–107
  - Finding errors 4–106
  - Grabbing Data 4–108
  - Grabbing Database Structure 4–109
  - Looking for 4–105
- SQLmap 4–104
- SQLSlammer 1–96
- SS7 4–123
- SSH 1–119
  - Sniffing 3–60, 3–63
  - SSHmitm 3–63
- SSID 2–60, 2–72
- SSL
  - Sniffing 3–60
  - SSLStrip 3–64, 3–67, 68
  - Warning Message 3–61-62, 3–65
- SSLSplit 2–68
- SSLStrip 2–68
- Stack (Not executable) 3–122
- Startup Items 1–69, 70
- Stash 5–148
- Static Code Analysis 3–127
- Statically Linked Binary 1–42
- Steganography 5–147
  - Defense 5–154
- StegExpose 5–154
- Stego → Steganography
- strcat 3–103
- strcopy 3–96, 3–103

- su 1–211
- Sub7 5–9
- Subroutinge 3–98
- Subterfuge 3–64
- SubVert 5–58
- Sumfuq 5–50
- Super User Control Kit (SUCKit) 5–56
- Suspicious Activity Report 1–23
- Suterusu 5–71
- switch 3–45
- SYN Flood 4–167
- SYN Scan 2–93
- syndrop 4–161
- SYSKey 4–31
- System Administrator Identification 1–63
- System call 5–50
  - table 5–53
- System Center Configuration Manager 1–139
- systemctl 2–104

T

- tail 1–220
- Tamper Data 4–144
- Tap (Ethernet) 1–44
- tar 1–236
- Target Analysis 1–183
- tasklist 1–67, 1–69
- TCP
  - Checksum bypass 2–114
  - Handshake 2–25, 2–90
  - Header 2–91
  - Port 2–89
  - Redirector 4–73
  - Sequence Prediction 2–93
- TCP Layer 3–53
- TCP/IP 2–88
- tcpdump 2–25, 2–64, 5–101, 2–106
- TCPVcon 2–101
- TCPView 1–77, 2–101
- teardrop 4–161
- Teardrop Attack 4–154
- telnet 3–18
- THC Hydra 4–8
- THC-Scan 2–54
- Themida 5–19
- Thinstall 5–19
- Thunderbolt 3–4
- Tiger 2–13
- Time-to-live 2–81
- Titan rain 1–160
- TLC 3–66
- TOR 2–82
- traceroute 2–81
- Tracerouting 2–83
- tracert 2–81
- Tracert.org 2–51
- Trade Secret 1–182
- Trademark 1–182
- Travelocity 2–38
- Tresorit 1–52
- Tribe Flood Networks 4–163
- TripWire 5–67, 1–258
- Trojan Horse 5–6
- Trust Relationship 1–112
- TS Duration 1–151
- TS Score 1–151
- Tunneling 5–120
- type 3–32, 5–110

U

- UAT → User Acceptance Test
- UDP
  - Header 2–92
  - Port 2–89
  - Scan 2–93
- uname 5–98
- Unauthorized Use 1–166
- unshadow 4–35
- Unusual 1–75
- UPC 2–38
- updatedb 1–218
- uptime 1–257
- UPX 5–19
- URL Length 1–135
- USB 3–6
- USB Device History 1–192
- USB Token RAM Device 1–44
- User Acceptance Test 1–123
- User Behavior Analytics 5–117
- User Input 1–58
- User-Agent String 1–135
- useradd 1–209
- utmp 5–89
- UUNET 1–96
- uWhois 2–20

V

- Veil 5–18
- Veracode 3–127
- Version Scanning 2–93
- vi 1–219
- VIN 2–38
- Virtual Machine (detection) 4–73
- Vitriol 5–58
- vmcat 3–11
- vmlinuz 5–57
- VMWare 1–196
  - Files 1–198
  - Network Options 1–202
  - Screen Views 1–200
- VNC 5–9
  - Active client 5–12

  - Overview 5–10
  - Plafform 5–11
  - WinVNC 5–13
- VOIP 1–52, 2–54
- Volatility Framework 5–22, 1–110
- VPN 2–73
  - Blocking 3–64
- VPN Configuration Attack 2–73
- VPN Key Exchange 4–26
- VSAgent 5–137
- Vulnerability 1–96
  - Analysis 1–121
- Vulnerability Scanner 2–118
  - Defense 2–124

W

- W3af 4–146
- War Dialing 2–53
  - Defense 2–57-58
- War Driving 2–61
  - Defense 2–72-75
- War Games 1–37
- War Room 1–36
- Warhol (worm) 4–61
- Warning Banners 1–21, 1–26, 1–175
- Warvox 2–54
- Watch and Learn 1–22
- Wayback Machine 2–39
- wc 4–174
- Web Application
  - Defense 4–150
  - Firewall 4–101, 4–150
  - Manipulation Proxy 4–146
    - Tools 4–150
- Web Proxy 1–135, 1–172
- Web Proxy Auto-Detect 3–79
- Web Spider 2–33
- Web-Based
  - Attack Tool 2–50
  - Reconnaissance 2–50
- WebScarab 4–146
- WebSense 1–172
- Website Searches 2–29
  - Defense 2–33
- Website Tampering 2–10
- Wellenreiter 5–164
- WEP 2–60, 2–64
- wevtutil 1–74, 1–190
- whatis 1–243
- Whirlpool 2–13
- who 5–89
- whoami 5–98, 1–211
- Whois 2–19
  - Defense 2–22
- Win32dd 5–22
- win32k.sys 5–57
- Windows Anti-Reverse Engineering 5–19
- Windows Credential Editor 4–51
- Windows Firewall 1–66
- WinNuke 4–161
- winpmem 5–22
- WinRM 1–141
- winrtgen.exe 4–27
- Wireless Network
  - Configuration 2–74
  - Misconfiguration 2–60
  - Password 2–72
- wireshark 3–46, 2–64
- wmic
  - computersystem 1–189
  - process 5–26-27, 1–67, 2–102
  - product 1–138
  - startup 1–70
- Word Mangling 4–10
- WordWebBugs 1–107
- Worm 4–54
  - Defense 4–74
  - Future payload 4–64
  - History 4–55
  - Infection speed 4–60
  - Metamorphic 4–65
  - Multi-exploit 4–57
  - Multi-platform 4–58
  - Polymorphic 4–62-63
  - vs Virus 4–55
  - Zero-Day Exploit 4–59
- WPA 2–64-65, 2–72, 2–74
- WPAD → Web Proxy Auto-Detect ....
- Wrapper 5–18
- Write Blocker 1–111
- Writing Secure code 3–126
- wtmp 5–89

X

- X-Ways Forensics 1–41
- X.25 4–123
- xinetd 2–104
- Xplico 3–55

Y

- Yersinia 3–59
- Yoda 5–19

Z

- ZAP → Zed Attack Proxy ....
- Zed Attack Proxy 4–89, 4–104, 4–146-147
- Zenmap GUI 2–84
- Zero-day Exploit 3–101
- Zero-day exploit 4–59, 1–95
- ZigBee 2–63
- Zombie (pulsing) 4–166
- Zotob 4–59