# SANS SEC501 – Advanced Security Essentials

## Topics

### Defensive Network Infrastructure

1) Introduction 501.1–3-11
2) Network Infra Devices as Targets 501.1–12-80
3) Implementing CIS Benchmarks & the NSA Cisco IOS Switch Sec Config Guide 501.1–81-195
4) Advanced Controls 501.1–196-224
5) Conclusion 501.1–225-234

### Packet Analysis

1) Advanced Packet Inspection 501.2–2-27
2) Packet Analysis Fundamentals 501.2–28-106
3) Intrusion Prevention Systems 501.2–107-111
4) Open Source IPS and Network Forensics 501.2–112-192
5) Appendix - Advanced Device Testing 501.2–193-209

### Pentest

1) Introduction 501.3–2-16
2) Penetration Testing Process 501.3–17-220
1. Determine the Scope 501.3–19-26
2. Information Gathering 501.3–27-61
3. Scanning 501.3–62-139
4. Enumeration 501.3–140-147
5. Exploiting 501.3–148-207
6. Pivoting 501.3–208-210
7. Reporting 501.3–211-220
3) Appendix – Post-Exploitation 501.3–221-240

### First Responder

1) Fundamentals 501.4–4-56
2) First Response Skills 501.4–57-140
3) Additional Consideration Points 501.4–141-198
Case Study: Real Compromise 501.4–177-186

### Malware

1) Introduction 501.5–2-15
2) Windows Built-in Tools 501.5–2, 16-58
1. Basic CLI Tools 501.5–16-35
2. Advanced CLI Tools 501.5–36-58
3) Additional Tools 501.5–3, 59-358
1. HijackThis Tool to Fight BHO 501.5–59-76
2. MS Sysinternals Tools 501.5–77-110
3. MS Sysinternals ListDLLs 501.5–111-136
4. Fighting ADStreams 501.5–137-167
5. Fighting Persistent Malware 501.5–168-197
6. Fighting Rootkits 501.5–198-283
7. Cloud-Based Tools 501.5–284-294
8. Web-Based Tools 501.5–295-326
9. Malware Removal Starter Kit 501.5–327-358
4) Summary 501.5–359-364
5) Hands-on Answers 501.5–365-375

### Dala Loss Prevention

1) Introduction 501.6–2-3
2) Risk Management 501.6–4-37
3) Risk Mitigation 501.6–38-49
4) Threat Modeling 501.6–50-61
5) BCP/DRP 501.6–62-118
6) Data Classification 501.6–119-139
7) Insider Threat 501.6–140-169
8) Dala Loss Prevention 501.6–170-184

## Categories

### Summaries

Advanced Device Testing 501.2–209
Advanced Packet Inspection 501.2–27
Attack Tools & Techniques 501.1–59
CIS Benchmarks 501.1–161
Data Classification 501.6–139
Data Loss Prevention 501.6–184
First Responder Wrap-Up 501.4–151
Identifying & Removing Malware 501.5–360-364
Insider Threat 501.6–169
Intrusion Prevention Systems 501.2–111
MS Approach for Malware Removal 501.5–358
Open Source IPS and Network Forensics 501.2–192
Penetration Testing Methodology 501.3–220
Risk Management 501.6–61

### Labs

Additional Tools/Cmds for SIFT 501.4–119-140
Analyzing PCAPs with TCPdump 501.2–52-65
Attack Analysis with Wireshark 501.2–92-106
Attacking IOS Passwords 501.1–61-80
HijackThis Tool 501.5–68-76
Linux and Windows IR Scripts 501.4–187-198
Metasploit Basics 501.3–162-170
Miscellaneous Network Forensics Tools 501.2–186
More Scanning Options 501.3–108-117
MS Sysinternals PrExpl & TCPView 501.5–109-110
MS Sysinternals Streams 501.5–146-167
Observing Management Protocols 501.1–206-224
Packet Analysis with Wireshark 501.2–66-91
Persistent Malware 501.5–180-197
Rootkits & Anti-Rootkits 501.5–262-283
Scanning Fundamentals 501.3–80-93
Scanning with Nessus 501.3–132-139
Snort Basics 501.2–158-172
Tools/Commands for SIFT 501.4–73-101
Using Nipper 501.1–187-195
⊞ Advanced CLI Anti-Malware Tools 501.5–57-58
⊞ Basic CLI Anti-Malware Tools 501.5–35
Windows-Focused Analysis 501.4–152-186

# SANS SEC501 – Advanced Security Essentials

**Tools**

- Aircrack-NG 501.3–128
- AirSnort 501.3–128
- Amap 501.3–94-95, 110
- Anubis SandBox 501.5–298-305
- Ap0calypse 501.5–171-179
- ArpSpoof 501.1–215
- ASPack 501.5–91
- Asterisk PBX 501.3–201
- Autoruns 501.4–113
  - 501.5–292
- Avast
  - Virus Cleaner 501.5–341, 353
- BlackLight (F-Secure) 501.5–239-244
- Bloover 501.6–177
- Bluesnarf 501.6–177
- Brutus 501.3–184
- Burp 501.3–51, 103-104
- Cain & Abel 501.1–23, 215
- Cain ⊞ 501.3–177, 180
- Canvas (Immunity) ● 501.3–103
- CapMe 501.2–184-185
- Carwhisperer 501.6–177
- CGE 501.1–46, 217-219
- Crack 501.3–184
- CrowdInspect (CrowdStrike) 501.5–290-291
- Cuckoo 501.5–309
- Dcfldd 501.4–64
- Dd 501.4–10
- Demon Dialer 501.3–119
- Dig 501.3–37-38
- Drive Manager 501.5–341, 351
- Dsniff 501.1–23
  - 501.3–177
- DumpSec 501.3–146
- ELSA 501.2–184-185
- Enum 501.3–147
- Ethercap 501.3–172
- Etherpeek 501.3–172
- Ettercap 501.1–54, 215
  - 501.3–177
- Eureka 501.5–296
- Exiftool 501.3–59-61
- Fgdump 501.3–181
- Filemon ⊞ 501.4–113
- FixEVT 173
- FOCA 501.3–59, 61
- Fragroute 501.2–203
- FTK Imager ⊞ 501.4–117
- Fwsnort 501.2–117-118
- Ghost 501.4–10
- Goofile 501.3–50
- Goohost 501.3–50
- Gooscan 501.3–49
- Grave-Robber 501.4–106
- Hailstorm ● 501.3–103
- Handle ⊞ 501.4–113
- Helix 501.4–32
- HijackThis 501.5–60-76, 99-101, 118-119, 126-131, 148-149, 167, 190-197
- Hping 501.1–19
  - 501.2–202
  - 501.3–67, 101-102, 112
- Hunt 501.3–177
- Hybrid-Analysis VxSandbox 501.5–312-316
- Hydra 501.1–50-51
  - 501.3–179
- IceSword 501.5–246, 255-259
- InSSIDer 501.3–131
- Ios7decrypt 501.1–46, 74-75
- IP Browser ● 501.3–142
- IP Watcher 501.3–177
- IP360 ● 501.3–127
- ISIC 501.2–203
- ISS Internet Scanner 501.4–26
- John The Ripper 501.1–41, 47-49
  - 501.3–180, 184-185
- JSUnpack 501.5–296
- Juggernaut 501.3–177
- Kismet 501.3–128
- L0phtcrack 501.3–180
- LADS 501.5–142
- LANguard ● 501.3–127
- LDAP Browser 501.3–143
- Ldp.exe 501.3–143
- ListDLLs ⊞ 501.5–112-126
- Log Parser 501.4–153, 163-176
- Log2Timeline 501.4–138
- Lynx 501.3–48
- MAC-Robber 501.4–106, 124
- Macof 501.1–216
- MACtime 501.4–106, 124, 126
- Malicious Software Removal Tool 501.5–341
- Maltego 501.3–56
- Malware Removal Starter Kit 501.5–348
- MalwareViz 501.5–310-311
- Malwr Sandbox 501.5–306-311
- MBR (GMER) 501.5–277
- Md5deep 501.4–65, 107, 128
- Memoryze 501.4–64
- Metagoofil 501.3–50
- Metasploit 501.2–206
  - 501.3–157-170
- Mimikatz 501.3–181
- ModSecurity (Apache module) 501.2–173-178
- Morning Coffee 501.3–56
- Nessus ● 501.2–202
  - 501.3–118, 122-125, 127, 132-139
- Netcat 501.2–201
  - 501.3–97-100, 114-116, 187
- NetDude 501.2–205
- Netstumbler 501.3–128, 130
- Network Traffic Generator 501.2–200
- NetworkMiner 501.2–182-183
- Nexpose ● 501.3–127
- Nfsshell 501.3–144

- Ngrep 501.2–181
- Nidsbench 501.2–204
- Nikto 501.3–103, 106-107, 113
- Nipper 501.1–39, 183-185
- Nmap 501.1–107
  - 501.2–201
  - 501.3–67, 72-79, 145
- Notepad ⊞ 501.5–157
- Nslookup 501.3–36
- OpenVAS 501.3–126
  - 501.4–26
- P0f 501.2–110
  - 501.3–75
- Panda Anti-Rootkit 501.5–217-225
- Pastebin 501.3–52
- PastebinLeaks 501.3–56
- PastebinParser 501.3–55
- PasteLert 501.3–53-54
- Pastenum 501.3–56
- PECompact 501.5–91
- Petite 501.5–91
- PhishGuru ● 501.3–207
- PhishMe ● 501.3–207
- Phonesweep ● 501.3–120
- Pinger 501.3–67
- Process Explorer ⊞ 501.4–113
  - 501.5–79-97, 114-117, 293
- PsFile ⊞ 501.4–71, 113
- Pwdump 501.3–180
- QualysGuard ● 501.3–127
- RAT 501.1–39
- Regmon ⊞ 501.4–113
- RegRipper 501.4–153, 155-162
- Retina ● 501.3–139
- Rootkit Detective (McAfee) 501.5–226-238, 249
- Rootkit Revealer ⊞ 501.4–113
- Rootkit UnHooker 501.5–247, 251-254
- RootkitRemover (McAfee) 501.5–226
- Router Audit Tool (RAT) 501.1–179-182
- Rpcinfo 501.3–145
- SanityCheck 501.5–267-269
- Scapy 501.2–202
- SearchDiggity 501.3–49
- SecureSphere ● 501.2–9
- SecurityOnion 501.2–184-185
- SET 501.3–206
- Shodan 501.1–58
  - 501.3–52, 58
- Showmount 501.3–144
- SIFT 501.4–32, 49-56
- Sitedigger 501.3–49
- SleuthKit 501.4–129-137
- Smartbits 501.2–200
- Snmpwalk 501.3–142
- Snorby 501.2–184-185
- Snort 501.2–114-172
- Snot 501.2–204
- Spirent Avalanche 501.2–200
- SpoofApp 501.3–201
- SpoofCard 501.3–201
- Spybot: Search & Destroy 501.5–341
- SQLmap 501.3–104
- Stick 501.2–204
- Stinger (McAfee AVERT) 501.5–341, 353
- Streams ⊞ 501.5–144-147, 165-166
- Strings 501.3–59
- Swatch 501.4–38
- Sysinternals ⊞ 501.5–78-124, 144-147, 165-166
- System Spec 501.5–341
- T-Sight 501.3–177
- TcpDump 501.1–19
  - 501.2–36-51
- TCPReplay 501.2–200
- TCPtrace/TCPflow 501.2–179-180
- TCPView ⊞ 501.4–113
  - 501.5–82-93
- TDImon ⊞ 501.4–113
- TDSSKiller (Kaspersky) 501.5–270-272, 278-283
- THC-scan 501.3–120
- Threat Expert 501.5–324-326
- Traceroute 501.3–65-66
- Tripwire 501.1–205
  - 501.4–27
- TTY Watcher 501.3–177
- UPX 501.5–91
- Volatility 501.4–64, 129
- WarVOX 501.3–120-121
- Webapet 501.5–317-323
- WebDefend ● 501.2–9
- WebInspect ● 501.3–103
- WebScarab 501.3–51
- WEPcrack 501.3–128
- Wikto 501.3–49, 103, 106-107
- Win32dd 501.4–64
- WinDump 501.2–36
- WinMHR (Team Cymru) 501.5–286-289
- Wireshark 501.1–209-212
  - 501.2–63-106, 201
- WS_Ping ProPack 501.3–67
- XORSearch 501.5–160-163
- Xprobe2 501.3–96, 111
- Yersinia 501.1–53, 220-224
- Yoda 501.5–91
- ZAP 501.3–51, 103, 105

### Linux/Unix Commands

- `cat` 501.4–66
- `date` 501.4–66, 80
- `dc3dd` 501.4–117
- `dcfldd` 501.4–64, 117
- `dd` 501.4–117
- `env` 501.4–79
- `file` 501.4–115
- `find` 501.4–112
- `finger` 501.4–103
- `ifconfig` 501.4–86

- iostat 501.4–67
- lastb 501.4–103, 110
- last 501.4–88-89, 102, 110
- ldd 501.4–72
- lsof 501.4–69-71, 87
- ls 501.4–65, 69, 88
- memdump 501.4–64
- mpstat 501.4–67
- netstat 501.4–84-85
- ps 501.4–69, 92
- script 501.4–62
- strings 501.4–115
- tar 501.4–71
- top 501.4–69
- uname 501.4–66, 82
- uptime 501.4–66, 81
- vmstat 501.4–67, 83
- who 501.4–90, 102-103
- w 501.4–91, 102, 110

**Windows Commands**

- attrib 501.4–104
  501.5–9-10, 106-107
- at 501.4–104
- cscript 501.4–61
- date 501.4–66
- del 501.5–106, 108
- dir 501.4–65
  501.5–17-20, 143, 151
- doskey 501.4–112
- dumpuser 501.4–102
- echo 501.4–96
- findstr 501.5–25-29
- ipconfig 501.4–97
  501.5–186
- listdlls 501.4–72
- more 501.5–155
- netstat 501.4–98
  501.5–25-29
- net 501.4–99-100
- ntlast 501.4–102
- pmdump 501.4–68
- psfile 501.4–71
- psinfo 501.4–66
- pslist 501.4–68
- psloggedon 501.4–102
- psservice 501.4–68
- set 501.4–95
- systeminfo 501.4–66
- taskkill 501.5–30-34
- tasklist 501.4–101
  501.5–21-24
- tlist 501.4–68
- type 501.5–155
- userdump 501.4–68
- win32dd 501.4–64

**IOS Commands**

- aaa 501.1–91, 131, 135
  - accounting 501.1–135
  - authentication 501.1–91, 131
- access-class 501.1–100
- access-list 501.1–100, 109
- banner 501.1–102
- boot 501.1–119
- cdp 501.1–118
- clock 501.1–113
- crypto 501.1–98
- enable 501.1–104
- exec-timeout 501.1–99
- exec 501.1–101
- icmp 501.1–137
- interface 501.1–125, 137, 147-148, 153, 155, 167-168, 172, 174
- ip 501.1–98-99, 117-118, 125-126, 137-138, 147-148, 153, 174-175
  - address 501.1–137
  - authentication 501.1–148
  - bootp 501.1–118
  - dhcp 501.1–174
  - finger 501.1–117
  - http 501.1–118
  - identd 501.1–117
  - proxy-arp 501.1–153
  - source-route 501.1–126
  - ssh 501.1–99
  - tacacs 501.1–138
  - telnet 501.1–138
  - tftp 501.1–138
- key 501.1–148
- line 501.1–93, 99-101, 105, 133
- logging 501.1–121-122, 138
- login 501.1–93, 133
- ntp 501.1–114, 138
- passive-interface 501.1–145
- password 501.1–105, 133
- router 501.1–145, 147-148
- service 501.1–74, 105, 116-119, 123
- snmp-server 501.1–108-110
- spanning-tree 501.1–171-173
- switchport 501.1–168-169
- tacacs-server 501.1–130
- tftp-server 501.1–119
- transport 501.1–99, 101
- username 501.1–92
- user 501.1–95
- vlan 501.1–176
- vtp 501.1–167

**CIS Benchmarks Rules**

**By Plane**

- L1 - Management 501.1–91-110
- L1 - Control 501.1–111-123
- L1 - Data 501.1–124-126
- L2 - Management 501.1–127-135
- L2 - Control 501.1–136-139

- L2 - Data 501.1–140-156
- **Level 1** 501.1–91-126
  - Banners 501.1–102
  - Clock Time Zone 501.1–113
  - Configure External Time Sources 501.1–114
  - Configure Remote Access 501.1–99
  - Configure SSH Support 501.1–98
  - Create Local Users 501.1–92
  - Define SNMP Access List 501.1–109
  - Disable AUX Port 501.1–101
  - Disable Directed Broadcasts 501.1–125
  - Disable finger, identd 501.1–117
  - Disable IP Source Routing 501.1–126
  - Disable SNMP/Default Community Strings 501.1–108
  - Disable Unneeded Services 501.1–118-119
  - Enable AAA for Local Auth 501.1–91
  - Limit SNMP Traps 501.1–110
  - Local/Console Logging 501.1–121
  - Privilege Level 1 for Local Users 501.1–95
  - Remote Logging 501.1–122
  - Require AAA for All Lines 501.1–93
  - Require Enable Secret 501.1–104
  - Require Password Encryption 501.1–105
  - Restrict Remote Access 501.1–100
  - Timestamp Configuration/Loopback 501.1–123
- **Level 2** 501.1–127-156
  - Apply AAA to Management Lines 501.1–133
  - Authenticated Routing 501.1–147-148
  - Centralized AAA 501.1–128-129
  - Configure Accounting 501.1–134-135
  - Configure TACACS+ 501.1–130
  - Control Route Advertisements 501.1–145-146
  - Disable Proxy ARP on All Interfaces 501.1–153
  - IOS AutoSecure 501.1–156
  - Loopback Interface 501.1–137
  - NTP Authentication 501.1–139
  - Protocol Configuration 501.1–138
  - Remove Tunnel Interfaces 501.1–155
  - Traffic Filtering 501.1–141-142
  - Unicast Reverse Path Forwarding 501.1–149
  - Use TACACS+ for Login and Enable 501.1–131

**Switch Config SANS Gold Standard**

- DHCP Snooping 501.1–174
- IP Source Guard 501.1–175
- Port Security 501.1–169
- STP 501.1–170-173
- Trunks 501.1–168
- Unused Interfaces 501.1–176
- VLAN 501.1–166-167

## A

- AAA 501.1–89, 164
  - List 501.1–91
  - Local 501.1–91-92
- AACS 501.6–137
- Abnormalities 501.4–38
- Accessing Files 501.4–105-106
- Account lockout 501.1–16
- ACL 501.1–177
  - 501.2–6
- ACS 501.1–28
- Active Directory 501.1–128
  - 501.3–180
- Active Response 501.2–16
- Adm 501.4–110
- Adobe Acrobat Reader Exploit Snort Rule 501.2–144
- ADS 501.5–138-167
  - Access 501.5–154-157
  - Basics 501.5–138-143
  - Removal 501.5–164-167
  - View with Windows 501.5–150-152
- AIK 501.5–334
- AIX 501.3–227
- ALE 501.6–18
- Alternative Sites 501.6–95-96
- Anomaly Detection 501.2–10
  - 501.6–165
- Anti-Rootkits 501.5–216, 245
- Anti-Spyware 501.5–333
- Antivirus 501.5–333
- AP Spoofing 501.3–129
- Apache 501.3–190
  - 501.4–115
- API 501.5–201-202
- Application Control 501.2–19
- Application Proxies 501.2–8
- APT 501.1–23
  - 501.5–170
- Arachnids 501.2–128
- ARIN 501.3–39
- ARO 501.6–18
- ARP 501.1–24
  - Cache Poisoning 501.1–23, 215-216
  - Proxy 501.1–151-153
  - Spoofing 501.1–169
- Art of Deception 501.3–197
- Aruba 501.1–202
- ASIC 501.2–25-26
- Asset Identification & Evaluation 501.6–24-25
- Asterisk PBX 501.3–201
- At-Rest Data 501.6–175
  - Threats 501.6–176
- Attack 501.3–6
  - Process 501.3–15
  - Types 501.6–60
- Attack Surface 501.6–55
- Attack Tools & Techniques 501.1–45-59
- Audit 501.6–44, 46

Authenticated Peers 501.1–147-148
Auto-Loading Programs 🪟 501.5–47-50
Automated Deception 501.2–16
Autoruns 501.4–113
AV 501.6–18
Awareness Training 501.6–45

## B

Backdoor 501.3–149, 187-188
  501.4–25
  Example 501.2–57
Backup 501.4–23-24
  (Recovery) 501.6–99-100
Banner Grabbing 501.3–100
Baseline 501.4–47, 102
BCP 501.6–63-65, 72
  Appendices 501.6–109
  Development 501.6–103-111
  Goal 501.6–67
  Key Components 501.6–73
  Mistakes 501.6–117-118
  Phases 501.6–71
    1. Project Initiation 501.6–71-80
    2. Current State Assessment 501.6–81-90
    3. Design & Development 501.6–91-100
    4. Implementation 501.6–101-114
    5. Management 501.6–116
  Resource Requirements 501.6–88
  Structure 501.6–102
  Testing & Training 501.6–101, 110-114
    Types 501.6–112
  Update 501.6–111
  Versus DRP 501.6–67-68
  Why 501.6–69-70
BeyondTrust 501.3–139
BGP 501.1–143-144
BHO 501.5–3, 6, 61, 113
BIA 501.6–73, 86-87
  Questions 501.6–86
BitLocker 501.4–61
BlackHole Exploit Kit 501.5–61
Blacklist 501.2–118
BlackShades 501.5–3
Bleeding Edge 501.2–144
BlueCoat 501.2–17
Botnet 501.2–85, 89
  501.4–11
  Example 501.5–203
  IRC Commands 501.5–92, 305
Boyer-Moore Algorithm 501.2–130
BPDU 501.1–171, 220-222
  Guard 501.1–173, 224
Bradford 501.1–202
Brute Force Attack 501.2–64
  Snort Rule 501.2–151, 168
BSOD 501.5–253, 259
Btmp 🐧 501.4–88-89, 103, 110

Buffer Overflow 501.1–217, 219
  501.2–149
  501.3–149-150
  Detection & Mitigation 501.3–153-154
  Exploitation 501.3–151-152
BugBear 501.2–146
Bugtraq 501.2–128

## C

Cain 🪟 501.3–177, 180
  Capabilities 501.3–183
CAM 501.1–216
Camera 501.3–205
CAPEX 501.6–35
Cardinal Rules 501.4–12-13
Catalyst 501.1–177
CatOS 501.1–83
CCB 501.1–233
CDP 501.1–24, 39, 223-224
  Flood 501.1–224
  Information Disclosure 501.1–40
CEF 501.1–149
Centralized Access Control 501.1–62
Centralized Log 501.4–47
Cenzic/TrustWave 501.3–103
CEO 501.6–76
Cewl 501.3–104
CGE 501.1–46, 217-219
CGI 501.3–192
Chain of Custody 501.4–12
Check Point 501.2–15
CIDR 501.2–125
CIS Benchmarks 501.1–4, 8, 81-161
  Additional 501.1–159
  Consensus 501.1–84
  Groups 501.1–87
  Level 1 501.1–85
    Control Plane Rules 501.1–111-123
    Data Plane Rules 501.1–124-126
    Management Plane Rules 501.1–89-110
  Level 2 501.1–86
    Control Plane Rules 501.1–136-139
    Data Plane Rules 501.1–140-159
    Management Plane Rules 501.1–127-135
Cisco 501.2–24
  Easy VPN 501.1–157
  ISE 501.1–202
  Password Encryption 501.1–41-42, 47-48, 74, 105
    Cracking 501.1–72-79
    Declaration 501.1–92
  PSIRT 501.1–35, 83
  Secure ACS 501.1–128
  Vulnerabilities 501.1–26, 28, 43
Classification of Assets 501.6–163
Clearing tracks 501.3–16
CLI 501.5–5
Cloud Computing 501.6–178

- Cloud-Based Rootkit Tools 501.5–285
- CNSS 501.3–6
- CO2 501.3–104
- CodePad 501.3–57
- Command & Control Channel 501.5–7
- Command & Control Method 501.5–93
- Command & Control Server 501.2–89
- Common Areas of Compromise 501.3–11
- Compromise Impact 501.1–27
- Computer Forensics 501.4–5
- Computer Security Lab 501.5–317
- Confidential Data Loss 501.6–181
- Confirmation 501.4–5
- Connect Scan 501.3–73
- Connection Decryption 501.2–21
- Consultant 501.4–43
- Containment 501.4–23-24, 142-143
- Contingency Planning 501.6–64
  - Mistakes 501.6–117-118
- Continuity 501.6–83, 97
- Control 501.6–35
  - Assessment 501.6–36
  - Categories 501.6–41
  - Detective 501.6–37
  - Selecion 501.6–37
- Control Plane 501.1–87
- COOP 501.6–47
- Cost Analysis 501.4–29
- Cost/Benefit Analysis 501.6–18
- Countermeasures 501.3–24
  - 501.6–16, 22
  - → Control
- Crisis Management Plan 501.6–71, 91, 101
- Critical Business Function 501.6–90
- Critical Controls 501.1–160
- Cron 501.4–104
- Cryptographic Key Management 501.6–42
- CSIRP 501.4–32
- CSIRT 501.4–31-32, 43
- CSS 501.6–137
- CUPS 501.4–85
- Cutwail 501.5–203
- CVE 501.2–128
- CVSS 501.6–56, 58-59

## D

- DAC 501.6–42
- DACL 501.3–146
- DarkCommet 501.5–3
- Data Breach Insurance 501.6–32
- Data Classification 501.6–121, 123, 181
  - Auditability 501.6–127
  - Criteria 501.6–124
  - Distribution 501.6–126
  - Process 501.6–122, 125
  - Roles & Responsibilities 501.6–128-135
- Data Collection 501.4–40-42
  - Real Example 501.4–179-180, 183
  - Scripts 501.4–188-198
- Data Destruction 501.6–182
- Data Plane 501.1–87
- Data Spill 501.6–175
- Dd 501.4–10
- Default Services 501.1–115
- Defense-In-Depth 501.1–86, 161
  - 501.2–113, 117-118, 173, 192
  - 501.3–194
- Defensive Kali 501.2–184
- Dell Sonicwall 501.2–15
- DHCP 501.1–172
  - Snooping 501.1–174
- Dial-Up 501.4–35
- Diameter 501.1–198
- Dictionary Lookup 501.6–180
- Didier Stevens 501.5–160
- Digital Equipment Corporation 501.1–170
- Digital Forensics 501.4–6
  - Best Practices 501.4–7
  - Methodology 501.4–4, 9
  - Report 501.4–11
- Directory Listing 501.3–191
- Directory Traversal 501.2–13, 132
- DISA 501.1–158
- Disaster Recovery Plan 501.4–19
- Disclosure 501.4–43
- Disinfection 501.5–94-108, 127-136
- DLL 501.4–72
  - Injection → Injected DLL
  - Usual Information 501.5–125
- DLP 501.6–172
  - Concerns 501.6–174
  - Identify/Discover 501.6–173
  - Identify/Monitor 501.6–179-180
  - Manage/Mitigate 501.6–183
  - Prevention 501.6–181-182
- DMZ 501.3–191
- DNI 501.1–8
- DNS 501.2–12
  - Records 501.3–34
  - Remote Shell 501.2–56-57
  - Zone Transfers 501.3–35
- DNS Rebinding Attack Snort Rule 501.2–154
- DOE 501.4–16
- DoS Attack 501.1–220, 222
  - 501.2–35
  - 501.3–129, 142
- DoS Mitigation 501.2–110
- Doskey 501.4–112
- Downtime 501.6–87-88, 501.1–157
  - Questions 501.6–88
- DREAD 501.6–51
- Driver (Rootkit) 501.5–332
- DRM 501.6–136-138, 501.5–205
- DRP 501.6–65-66, 98
  - Backup Solutions 501.6–100

  - Mistakes 501.6–117-118
  - Structure 501.6–98
  - Versus BCP 501.6–67-68
  - Why 501.6–69-70
- DTP 501.1–166
- Dumpster Diving 501.3–31
- DUT 501.2–196

## E

- E-Commerce 501.3–190
- E-mail Attachments 501.2–18
- EAP 501.1–198
- EC-Council 501.3–13
- EF 501.6–18
- EIGRP 501.1–145, 148
- Electronic Communications Privacy Act 501.4–23
- ELF 501.4–115
- Emerging Threats 501.2–139
- Endace 501.2–17
- Enterasys 501.1–202
- Enum 501.3–147
- Enumeration 501.3–18
  - Objectives 501.3–141
- Environment Variables 501.4–79, 95
- EOC 501.6–93, 101
- Eradication 501.4–25-26, 144-145
  - Real Example 501.4–185-186
- ERT 501.6–113
- Ethercap 501.3–172
- Ethereal 501.2–67
- Ethernet 501.1–166
  - Header 501.2–31
- Etherpeek 501.3–172
- Event 501.4–5
- Event Logs 501.4–108
  - Fixing 501.4–173
- Executive Management 501.6–63
- Executive Summary 501.3–24, 214
- Exploit 501.3–6, 153-154
  - Links 501.3–189
- Exploitation 501.3–18, 149
  501.6–12

## F

- F-Secure 501.5–205
- False Positive 501.2–10, 110
- FAT 501.5–139
- FERPA 501.6–124
- File Fingerprinting 501.6–180
- File Integrity 501.4–105
- Files of Interest 501.4–113-115
- Filtering Device Location 501.3–78
- Findings Report 501.3–24
- Finger 501.1–117
  501.3–145
- Firewall 501.1–137, 141, 177
  - Evasion 501.3–120, 195
  - Recommendation 501.3–195
  - Ruleset 501.2–118
- First Responder 501.4–14-15
  - Framework 501.4–31
    - Activate CSIRT 501.4–43
    - Initial Triage 501.4–34-35, 43
    - Live Triage 501.4–36-37
    - Monitoring Enhancements 501.4–46-47
    - Observation 501.4–44-45
    - Preparation 501.4–32-33
  - Jump Bag 501.4–33
- Flash 501.5–317
- FOIA 501.6–126
- Foofus 501.3–181
- Footprinting 501.3–29
- Fortinet 501.2–15
- Foundstone 501.3–49
- Fraggle 501.1–31, 125
- Fragmentation 501.2–118
- FrubarPaste 501.3–57
- FTP 501.2–167
  - Attack 501.2–62-64, 165
  - Log 501.4–111
- Full Packet Capture 501.2–17
- Fwsnort 501.2–117-118
  - Configuration 501.2–118

## G

- Gaining Access 501.3–16
- Gateway Interaction Devices 501.2–109
- Get Out of Jail Free 501.3–20
- Getent 501.3–227
- GFI 501.3–127
- Gh0st 501.5–3
- GLB 501.6–173
- Google Hacking 501.3–40, 42-50
  - Database 501.3–41
  - Examples 501.3–45-47
  - File Types 501.3–44
  - Tools 501.3–49, 107
- Google Talk IM 501.5–140
- GPS Tracking 501.3–205
- GRE 501.1–21
- GUI 501.5–5

## H

- Hacker Defender Rootkit 501.5–202
- Hackers Choice 501.3–94
- Hashing 501.4–107
- HE4Rootkit 501.5–203
- Helix 501.4–32, 36
  - Real Example 501.4–184
- Help Desk 501.4–21
- Heysoft 501.5–142
- HFS 501.5–139
- Hidden Mode 501.5–9

- Hide Signed Microsoft Entries 501.4–113
- HijackThis 501.5–60, 99-101
  - ADS Spy 501.5–148-149, 167
  - Backup 501.5–131
  - Basics 501.5–62-66
  - BHO Example 501.5–67
  - File Missing 501.5–136
  - Malicious DLLs Example 501.5–118-119, 127-131
    - Summary 501.5–126
  - Malware Example 501.5–70-71
  - Misc Tools 501.5–72-75
  - Persistent Malware Disinfection 501.5–190-197
  - Rescan 501.5–76, 129
- HIPAA 501.6–124, 135, 173
- History 501.4–112
- Honeynet Project 501.2–121
- Honeypot 501.2–16
- Honeywall 501.2–121
- HP SPI Dynamics 501.3–103
- Hping 501.1–19
  - 501.2–202
  - 501.3–67, 101-102, 112
  - Options 501.3–101-102
- HTTP 501.1–218
  - 501.2–12, 18
  - Snort Rule 501.2–143
    - Within SMB Session 501.2–156
  - Tunneling 501.2–13
- Hub 501.1–216
  - 501.4–41
- HVAC 501.6–48
- HyTrust 501.2–24

# I

- I'll Be Back Mode 501.5–10, 47, 94
- ICMP 501.1–137
  - 501.2–12
  - Floods 501.1–31
  - Snort Rule 501.2–141
  - Unreachable 501.2–115
    - 501.3–74
- Identd 501.1–117
- Identification 501.4–21-22
  - Real Example 501.4–182
- IDS 501.1–177
  - 501.6–44
  - Evasion 501.2–98, 102-104
    - 501.3–120, 194
- IEEE
  - 802.1d 501.1–170
  - 802.1q 501.1–166
  - 802.1w 501.1–170
  - 802.1x 501.1–197
  - 802.11x 501.3–186
- IGP 501.1–143, 145-146
- IHL 501.2–32
- IIS 501.3–190
- Imaging 501.4–116-117
- IMAP 501.1–19
- IMAP Buffer Overflow Snort Rule 501.2–149
- Impact 501.6–15, 59
- Imperva 501.2–9
- Important Files 501.3–230-231
- In-Transit Data 501.6–177
- Incident 501.4–5
  - Response 501.4–5
- Incident Handler Prime Responsibility 501.4–23
- Incident Handler VS First Responder 501.4–14
- Incident Handling 501.4–14-30
  - Communication 501.4–18, 21
  - Key Mistakes 501.4–30
  - Methodology 501.4–4, 14
  - Real Example 501.4–178
  - Six-Step Process 501.4–14-16
    1. Preparation 501.4–17-20
    2. Identification 501.4–21-22
    3. Containment 501.4–23-24
    4. Eradication 501.4–25-26
    5. Recovery 501.4–27-28
    6. Lessons Learned 501.4–29
- Indicators of Compromise 501.4–38-39
- Inetd 501.3–188
- InfoExpress 501.1–202
- Information Disclosure 501.4–43
- Information Gathering 501.3–17, 28-29
  - Sources 501.3–30
- Injected DLLs 501.5–113, 332
  - Disinfection 501.5–127-136
  - Example 501.5–123-124
- Inline Network Devices 501.2–109
- Inline SSL Decryption 501.2–22
- Insider Threat 501.6–142
  - Abilities 501.6–166-167
  - Controls 501.6–161-164
  - Impact 501.6–154-155
  - Prevention/Detection 501.6–156-158, 165
  - Risks 501.6–150-153
  - Traits 501.6–148
  - Types 501.6–145-147
  - Why 501.6–143-144, 149
- Intellectual Property Loss 501.6–181
- Interview Questions 501.4–181
- Invalidation 501.4–5
- IOC 501.5–326
- IOS 501.1–83
  - Accounting 501.1–134
  - Advances 501.1–157
  - AutoSecure 501.1–156
  - Default Services 501.1–39
  - Fallback Password 501.1–133
  - Lines 501.1–93
  - Logging 501.1–36-37, 120-123
    - Configuration 501.1–38
    - Types 501.1–134-135
  - Password Encryption 501.1–41-42, 47-48, 74, 105

Cracking 501.1–72-79
Declaration 501.1–92
Software Advisory 501.1–83
Trains 501.1–83
Wait Time 501.1–50
IOX 501.1–157
IP Source Guard 501.1–175, 216
IP Spoofing 501.1–175
IPC 501.2–96
IPS 501.2–108
Evasion 501.2–110, 118
IPSec 501.2–21
IPTables 501.2–117-119
IPv4 Header 501.2–32
IPv6 Header 501.2–33
IR Scripts 501.4–188-198
IR Stick 501.4–65
IRC 501.2–84, 89
501.5–29, 88, 305
Bot Commands 501.5–92
ISE 501.1–202
ISL 501.1–166
ISO 17779 501.6–82
ISP 501.1–144
ISS Internet Scanner 501.4–26
IStream 501.5–140

## J

Javascript 501.5–317
Jump Bag 501.4–19-20
Juniper 501.2–15-16, 24
UAC 501.1–202
Vulnerabilities 501.1–29

## K

Kali Linux 501.1–56, 183, 208
Kaspersky 501.5–140
Kerberos Tickets 501.3–228
Kernel Patch Protection 501.5–206
Kevin Mitnick 501.1–117
501.3–196-197
Kmart 501.1–177

## L

LAND Packet 501.2–135
LANMAN 501.3–182
Law Enforcement 501.4–17, 21
LDAP 501.1–128
LDAP Browser 501.3–143
Least Privilege 501.6–163
Lessons Learned 501.4–29, 148-149
Libnet 501.2–115
Libraries 501.4–72
LibWhisker 501.3–106
Likelihood 501.6–9, 14, 59
LimeWire 501.2–155
Line Passwords 501.1–105
Linux 501.3–223-224
Commands, Checks, Files → Unix *
Files to Check 501.3–223
Init 501.4–115
IR Commands 501.4–75-78, 77, 122-130
IR Script 501.4–190-192
System Checks 501.3–224
ListDLLs 501.5–112
Usage Example 501.5–120-126
Summary 501.5–126
Live Data Collection 501.4–40-42
Live Response 501.4–7
Examples 501.4–8
LKM 501.3–188
Local System Assessment 501.3–210
Lockpicking 501.3–205
Logs 501.4–108-109
Analysis 501.4–110-111
Parsing 501.4–170-171
Loopback 501.1–137
LSA 501.3–181
LSP 501.5–353
Lua 501.3–90

## M

MAC 501.6–42
MAC Hijinks 501.1–216
MAC Spoofing 501.3–129
MAC Times 501.4–104-106, 123
Preservation 501.4–106
Magic Number 501.4–115
Mail Aliases 501.3–227
Maintaining Access 501.3–16
Malicious Data 501.2–18
Malicious DLLs 501.5–113
Disinfection 501.5–127-136
Example 501.5–123-124
Malware 501.5–7-13
Basic Behavior 501.5–9
Disinfection 501.5–94-108
Injected 501.5–113
Most Frequently Used Stuffs 501.5–10-13
Network Communications 501.2–69
Packed 501.5–91
Persistent 501.5–169-170
Builder 501.5–171-179
Disinfection 501.5–187-196
Example 501.5–181-186
Types 501.6–60
Visualization 501.5–310-311
Malware Infestation 501.6–182
Management Plane 501.1–87
Management Security Controls 501.6–45-47
MBR 501.5–204

McAfee 501.2–128
  501.3–49
  AvertLabs 501.5–236
  Rootkit Detective Task Manager 501.5–233-234
MebRoot 501.5–204
Media Analysis 501.4–10
Media Drops 501.3–203-204
Metadata Search 501.3–52, 59
Metageek 501.3–131
Metasploit 501.1–57
  501.2–206
  501.3–157-170, 203
  Configuration 501.3–165
  Exploit Categories 501.3–158
  Exploit Settings 501.3–166
  Quick Start 501.3–159
  Sessions 501.3–167
Meterpreter 501.3–160-161, 168-169
  Commands 501.3–160, 169
MFT 501.5–137
MHR 501.5–286, 290-291
MIB 501.3–142
Microphone 501.3–205
Mirror 501.6–95
MITM 501.1–19-21, 54, 143, 169
  501.3–149, 174-175
  501.6–178
Mobile IP 501.1–152
ModSecurity 501.2–173-178
  Configuration 501.2–177
  Rules 501.2–175-177
Monitoring 501.4–118
Monolithic Kernel 501.1–35
Motivation 501.6–9
Mounting 501.4–62-63
MS Approach on Malware Removal 501.5–328-329
MS Outlook Exploit Snort Rule 501.2–147
MS08-067 501.2–94-96
MS11-100 501.6–9-10
Mykonos 501.2–16

## N

NAC 501.1–197, 200-202
NAP 501.1–202
NCircle 501.3–127
NCSC 501.6–64
NDA 501.6–126
Nessus 501.2–128, 202
  501.3–118, 122-125, 127, 132-139
NetBIOS Nmap Script 501.3–92
NetBIOS Session 501.4–102
Netcat 501.2–201
  501.3–97-100, 114-116
  Backdoor 501.3–187
  Banner Grabbing 501.3–100, 116
NetOptics 501.2–22
Netstat (Advanced) → TCPView
Network Connections 501.4–84-85, 98
Network Data 501.4–8
  Collection 501.4–40-42
Network Forensics 501.2–17
Network Infra Security Challenges 501.1–33-43
Network Interfaces 501.4–86, 97
Network Mapping 501.3–64, 67
Network Monitoring Enhancements 501.4–46-47
Network Processors 501.2–26-27
Network Traffic Generator 501.2–200
NFS 501.3–144
NGFW 501.2–14-15, 22
NIDS 501.2–204
NIS Accounts 501.3–227
NIST 501.3–6
  SP 800-18 501.6–45
  SP 800-30 501.6–5
  SP 800-34 501.6–103
  SP 800-94 501.6–47
Nmap 501.1–107
  501.2–201
  501.3–67-69, 72-74, 76-79, 145
  Default Scan 501.3–73
  Examples 501.3–79
  Fingerprinting 501.3–76-77
  Other Capabilities 501.3–78
  Results Analysis 501.3–88
  Scanning Options 501.3–68-69, 72
  Scripts 501.3–90-92
Non-Repudiation 501.6–43
Non-Secure Protocols 501.3–171
NOP 501.3–152
Notes 501.4–24
NSE 501.3–90
NTFS 501.5–139
NTLM 501.3–182
NTP 501.1–112-114, 136, 139, 164
  Spoofing Attacks 501.1–139
NtRootkit 501.5–203
Numerical Password 501.4–61
NX-OS 501.1–157

## O

Observation 501.4–44-45
OCTAVE 501.6–56
Office 501.5–312
Offline Analysis 501.5–330-333
Offset 501.2–32
Open Files 501.4–71
Open Source Network Security 501.2–114, 192
OpenVAS 501.3–126
  501.4–26
OPEX 501.6–35
Order of Volatility 501.4–7, 60
OS and Services Scan 501.3–87
OS Fingerprinting 501.3–64, 75
OSPF 501.1–145, 147

- OSSTMM 501.3–25
- Overlap Attack 501.2–100
- OWASP 501.2–207-208
  - 501.3–105
  - 501.6–51
  - Ten Questions about AppSec Systems 501.2–208

## P

- P2P 501.2–13
- P2P Software Snort Rule 501.2–155
- Packer 501.5–91, 501.5–178
- Packet Filtering 501.2–6
- Packet Inspection 501.2–5, 11
  - Weaknesses 501.2–4
- Packet Size 501.2–27
- PAD 501.1–119
- Palo Alto 501.2–15
- PAM 501.1–128
- Paros 501.3–51, 105
- Passive Interface 501.1–146
- Password Attacks 501.3–149, 178
- Pastie 501.3–57
- Patch Guard 501.5–206
- Pattern Matching 501.6–180
- Payload 501.6–12-13
- Payload Security 501.5–312
- PBX 501.3–21
- PcAnywhere 501.3–120
- PCI DSS 501.6–173
- PCTools 501.5–324
- PD 317
- PDA 501.6–177
- PDF 501.5–312
- PE 501.5–312
- Penetration Testing 501.3–4-27
  - Approach 501.3–17
  - Definitions and Terms 501.3–6
  - Deliverables 501.3–24
  - Final Meeting 501.3–220
  - Methodologies 501.3–25
  - Process 501.3–19
  - Rationale 501.3–10
  - Scope Definition 501.3–21
- People 501.3–198
- Persistence Method 501.5–176, 189, 291
- Persistent Data 501.4–8, 36
- Personnel Security 501.6–45-46
- PGP 501.2–21
  - 501.3–20
  - Keys 501.3–228
  - WDE 501.4–61
- Phishing 501.3–199-200
- Physical Hacking 501.3–205
- Ping Sweep 501.3–67
- Pivoting 501.3–209-210
  - Goals 501.3–209
- Planning 501.4–17
- Pod Slurping 501.6–176
- Poison Ivy 501.5–3, 141
- Policy 501.4–17
- Polymorphism 501.2–13
- POP 501.1–19
  - 501.2–12
  - Attack Snort Rule 501.2–151
- Port Mapping 501.3–64, 71-72
- Port Scanning 501.3–70
- Port Security 501.1–23, 169, 216
- Portfast 501.1–170, 172-173, 224
- Post Mortem Analysis 501.4–148
- Post-Exploitation 501.3–222-240
- Preparation 501.4–17-20
  - Real Example 501.4–181
- Pretexting 501.3–201
- Privileged Passwords 501.4–19
- Privileged User Management & Moniroting 501.2–24
- Process Explorer 501.5–79
  - Malicious DLLs 501.5–114-117
  - Properties 501.5–87
  - Strings 501.5–91-92
  - Toolbar 501.5–80-81
  - Usage Example 501.5–85-97
    - Summary 501.5–90, 93
- Process Manager 501.5–73
- Processes 501.4–68-70
- Proof of Wholeness 501.6–44
- Protector 501.5–91
- Protocol Anomaly Detection 501.2–13
- Protocol Standards Compliance 501.2–12
- PsTools 501.4–66
- PTES 501.3–25-26
- Python 501.5–38

## Q

- QoS 501.1–177

## R

- Race Condition 501.2–110
- Radia Perlman 501.1–170
- RADIUS 501.1–90, 129, 198
- Rainbow Tables 501.3–182
- RainbowCrack 501.3–182
- RAM 501.4–64
- RANCID 501.1–205
- Rapid7 501.3–127, 157
- RAT 501.1–39, 85, 179-182
  - 501.5–3, 170
- Read-Only Mode 501.5–10
- Real Compromised System 501.4–178-186
- Reconnaissance 501.3–15
  - Traces Example 501.4–170
- Recovery 501.4–27-28, 147
  - Activities 501.6–107

- Recovery Key 501.4–61
- Recovery Strategies 501.6–92-94
- Recovery Timeframes Questions 501.6–87
- Regedit 501.5–70
- Regular Expressions 501.2–20
- Reinfection 501.4–25
- Remote Access Tool 501.4–11
- Removal Kit 501.5–328-329
  - Build 501.5–334-347
    - Procedure 501.5–344-347
  - Recommended Tools 501.5–341-343
  - Usage 501.5–348-356
- Reporting 501.3–212-219
  501.4–29
  - Executive Summary 501.3–214
    501.4–29
  - Goals 501.3–212
  - Introduction/Conclusion 501.3–218
  - Outline 501.3–213
  - Technical Section 501.3–219
- Residual Data 501.6–175
- Residual Risk 501.6–33, 41
- Response Disk 501.4–65
- Response Plan 501.5–329
- Restore Secure State 501.6–44
- Restore/Rebuild 501.4–146
- Reverse Shells 501.3–232-233
- RFC 501.2–12
- RFP 501.3–106
- RIP 501.1–145, 148
- RISC 501.2–26
- Risk 501.6–6-7, 82
  - Acceptance 501.6–33, 85
  - Analysis 501.6–16, 85
    - Qualitative 501.6–19-21
    - Quantitative 501.6–17-18, 21, 25
    - Questions 501.6–82
    - System-Specific 501.6–26
  - Avoidance 501.6–30, 85
  - Determination 501.6–27
  - Excessive 501.6–28
  - Key for Success 501.6–49
  - Management 501.3–215-217
    501.6–8, 22
  - Matrix 501.6–20
  - Mitigation 501.6–29, 34, 39
    - Methodology 501.6–40
  - Rating 501.3–215
    - Example 501.3–216
  - Reduction 501.6–23, 54-55, 59, 85
  - Sharing 501.6–31
  - Transfer 501.6–31, 85
- ROI 501.6–18, 36-37
- Root Bridge 501.1–170-171, 224
- Root Cause Analysis 501.4–25
  - Real Example 501.4–185-186
- Root Guard 501.1–173, 224
- Rootkit 501.3–188
  501.5–3, 199-205
  - Effect 501.4–12
  - Examples 501.5–207-214
  - Hooked Services 501.5–231
  - Identification 501.5–209-216, 260-274, 285-294
  - Kernel Mode 501.5–203
  - MBR 501.5–204
    - Fighting 501.5–276-283
  - User Mode 501.5–201-202
- Rooty 501.3–188
- Rotation of Duties 501.6–163
- Router 501.1–164
  - What Attackers Can Do 501.1–31
- Routing Protocols 501.1–143
- RPC 501.3–145
- Rules of Engagement 501.3–20, 22

## S

- SACL 501.3–146
- Safe Mode 501.5–177, 193
- Salt 501.3–182
- SAM 501.3–180
- Sam Spade 501.3–32
- Samba 501.3–227
- Sandbox 501.5–296
  - Online 501.5–296-326
  - Report 501.5–301-305, 308, 315-316, 321-323, 326
- SAR 501.1–125
- SBU 501.6–123
- Scanning 501.3–15-17
  - Activities 501.3–64
  - Objectives 501.3–63
- Scheduled Tasks 501.4–104
- SCM 501.6–55
- Scope Definition 501.3–17, 21, 23
- Script Command 501.4–62
  - Real Example 501.4–183
- SDLC 501.6–51
- Search Engine Queries 501.3–40
- SEC 501.6–135
- Secure Systems Lab 501.5–298
- SecureSphere 501.2–9
- Security Awareness 501.6–162, 183
- Security Controls 501.6–41-48
- Security Failure 501.3–10
- Security Hardware 501.2–25-26
- Security Policy 501.6–64
- Security Weakness 501.3–10
- Senior Management 501.4–21
  501.6–39, 49, 129
- Sensepost 501.3–49
- Separation of Duties 501.6–163
- Services 501.5–52-56
- Session Hijacking 501.3–149, 175-177
  - Active VS Passive 501.3–176
  - Tools 501.3–177
- Session Sniping 501.2–109, 115

- Session Splicing 501.2–118
- Shared Accounts 501.1–89
- Shared Drives 501.4–100
  - 501.5–51
- Shell History 501.4–112
- Shimomura 501.1–117
- Shmoo Group 501.3–182
- SID 501.2–117
- SIFT 501.4–32
  - Installation 501.4–49-56
- Signature Matching 501.2–20
- Sinowal 501.5–204
- SIP 501.2–12
- SLA 501.6–31
- Slammer 501.2–55
- SLE 501.6–18
- Slexy 501.3–57
- SMB 501.2–95-98
  - Enumeration 501.3–147
  - HTTP Within Session Snort Rule 501.2–156
- SMTP 501.1–19
- Smurf 501.1–31, 125
- Sniffing 501.3–129, 171-173
  - Active VS Passive 501.3–173
  - Tools 501.3–172
- SNMP 501.1–106-107, 164
  - 501.3–141
  - Community Strings 501.1–108
  - Enumeration 501.3–142
  - Trap Logging 501.1–37
  - Traps 501.1–110
    - 501.3–142
- Snmpwalk 501.3–142
- Snort 501.2–114-172
  - Configuration 501.2–116
  - Flexible Response 501.2–115-116, 136
  - Inline 501.2–119-121
  - PCAP Analysis 501.2–160
  - Response Mechanisms 501.2–116
  - Rules 501.2–123-157
    - Actions 501.2–120
    - Anatomy 501.2–123, 138
    - Examples 501.2–140-157
    - Header 501.2–124-126
    - Options 501.2–120, 127-137
    - Regex 501.2–153
    - Sources 501.2–139
    - Tracking 501.2–141
  - Stealth Mode 501.2–115, 119
  - Whitelist 501.2–121
- SOAP 501.2–11
- Social Engineering 501.3–21, 149, 196-198
  - 501.6–167
- Softerra 501.3–143
- Solaris Logs 501.4–109-110
- Solarwinds 501.1–205
  - 501.3–67, 142
- Somarsoft 501.3–146
- Sony 501.5–205
  - 501.6–32
- Sourcefire 501.2–15, 24
  - VRT 501.2–139
- SOX 501.6–173
- Spidering 501.3–105, 107
- Spoofing Attacks 501.1–139, 142
- SQL 501.5–40
  - Injection 501.3–193
  - Server 501.2–55
- SSDT 501.5–203
- SSH 501.1–34, 50, 96-99
  - 501.4–115
  - Keys 501.3–228
  - Line Passwords 501.1–98
  - Nmap Script 501.3–91
- SSID 501.3–186
- SSL 501.2–21
- Startup Programs 501.5–47-50
- Stat 501.4–67
- Stateful Filtering 501.2–7
- Steganography 501.2–18
- Sticky Learning 501.1–169
- STIGS 501.1–158
- StillSecure 501.1–202
- Stoned Bootkit 501.5–204
- STP 501.1–24, 170-173
  - Loops 501.1–172
  - Rapid 501.1–170
- StrataCloud 501.2–24
- STRIDE 501.6–51
- Suspicious IP Snort Rule 501.2–148
- Swatch 501.4–38
- Switch 501.1–164
  - Config SANS Gold Standard 501.1–163-177
  - High-End 501.1–177
  - Protocols 501.1–13, 24
- Symantec 501.5–324
- SYN Scan 501.3–85
- Sysinternals Suite 501.5–78
  - Process Explorer 501.5–79
  - PsLoggedOn 501.4–102
  - Streams 501.5–144-147
  - Strings 501.5–343
  - TCPView 501.5–82-93
- Syslog 501.1–37-38, 164
  - 501.4–109-111
  - Facilities & Priorities 501.4–111
- System Files 501.4–113-115
- System Info 501.4–66
- System Mode 501.5–10
- System Protection 501.2–109
- System Restore Options 501.4–27
- System Security Plan 501.6–45

## T

- T+ ........ 501.1–128
- TACACS ........ 501.1–89-90, 127-129, 134, 137
- Tailgating ........ 501.3–202
- Talos ........ 501.2–139
- Taps ........ 501.2–22
- Target of Evaluation ........ 501.3–6
- Task Manager (Advanced) → Process Explorer ....
- Task Manager Default Columns ........ 501.5–213
- TCL ........ 501.5–38
- TCN ........ 501.1–222
- TCO ........ 501.6–18, 36-37
- TCP Flags ........ 501.2–44
- TCP Header ........ 501.2–34
- TCP KeepAlives ........ 501.1–116
- TCP Scan ........ 501.3–86, 89
- TCP Wait Time Attack ........ 501.2–100-102
- TcpDump ........ 501.1–19
  ........ 501.2–36
  - Filtering ........ 501.2–40-41
  - Usage Examples ........ 501.2–39, 42-51
- TCPView ........ 501.5–82
  - Capabilities ........ 501.5–83
  - Usage Example ........ 501.5–88-90
    - Summary ........ 501.5–90, 93
- TDSS/TDL ........ 501.5–204, 226, 280
- TDSSKiller Quarantine ........ 501.5–282
- Teardrop Attack ........ 501.2–58-60, 163
- Technical Controls ........ 501.6–42-44
- Telnet ........ 501.1–34, 50, 96, 137
  - Snort Rule ........ 501.2–142
- Tenable ........ 501.3–127
- Testing ........ 501.2–194-209
  - Methodology ........ 501.2–197-199
  - Tools ........ 501.2–200-206
- TFTP ........ 501.1–52
- Thin Client ........ 501.6–165
- Threat ........ 501.3–6
  ........ 501.6–9
  - Identification ........ 501.6–52
  - Modeling ........ 501.6–51
  - Vectors ........ 501.6–54
- Thumb Sucking ........ 501.6–176
- Timeline ........ 501.4–10, 106
- Timestamps ........ 501.4–123, 125
- Traffic Filtering ........ 501.1–141-142
- Traffic Monitoring Solution ........ 501.2–24
- Transaction Privacy ........ 501.6–43
- Transport Layer Inline IPS ........ 501.2–117
- TrendMicro ........ 501.5–60
- Triage ........ 501.4–34-43
- Trojan ........ 501.3–188
  ........ 501.4–12, 501.4–72
- Trunk ........ 501.1–166-168
- Trustwave ........ 501.1–202
  ........ 501.2–9
- TShark ........ 501.2–67
- Tunnel ........ 501.1–20
  ........ 501.2–33
- Tunnel Interfaces ........ 501.1–154-155

## U

- UAC ........ 501.1–202
- UDP Header ........ 501.2–35
- UDP Scan ........ 501.3–74
- Unhooking ........ 501.5–253
- Unix ........ 501.3–225-233
  - Credentials ........ 501.3–228
  - Important Files ........ 501.3–230-231
  - Networking ........ 501.3–226
  - System Checks ........ 501.3–225
  - User Accounts ........ 501.3–227
  - User Info ........ 501.3–229
- Unix Epoch ........ 501.4–125
- Unix Password Cracking ........ 501.3–184
- Unneeded Services ........ 501.1–118-119
- Unshadow ........ 501.3–185
- Unused Interfaces ........ 501.1–176
- UPS ........ 501.6–48
- UPX ........ 501.5–178, 309, 322
- URL ........ 501.2–13
  - Encoding ........ 501.2–118
- URPF ........ 501.1–140, 149
- Users ........ 501.4–102-103
- Utmp ........ 501.4–110

## V

- VCR ........ 501.2–17
- Verification ........ 501.4–5
- Vigenere Cipher ........ 501.1–41, 47, 105
- Virtual Appliances ........ 501.2–24
- Virtual Network Infra ........ 501.1–30
- VirusTotal ........ 501.5–290-291, 309, 316, 322
- VLAN ........ 501.1–24, 166-167
  ........ 501.2–31
- VM Escape ........ 501.1–30
- VNC ........ 501.3–187
- VoIP ........ 501.2–12
  ........ 501.4–18
  - Connection Snort Rule ........ 501.2–157
- Volatile Data ........ 501.4–8, 36
- VPN ........ 501.1–152, 155, 157, 177
  ........ 501.4–35
- VSS Monitoring ........ 501.2–22
- VTP ........ 501.1–167
- Vulnerability ........ 501.3–6
  ........ 501.6–10-11
  - Assessment ........ 501.6–87, 90
  - Assessment Traces Example ........ 501.4–170
  - Identification ........ 501.6–53
  - Scanning ........ 501.3–64, 118
    ........ 501.4–26
  - Scoring ........ 501.6–56-59
  - Web-Based Applications ........ 501.3–192

## W

- W32/Autorun Worm .... 501.5–93
- WAF .... 501.2–9
- Walmart .... 501.1–177
- War Dialing .... 501.3–21, 64, 119-121
  - Goals .... 501.3–120
- War Driving .... 501.3–21, 130-131
- Watchdog .... 501.5–176, 189, 192
- Web Application Firewalls .... 501.2–9
- Web Application Scanning .... 501.3–103
- Web Application Testing .... 501.3–149, 190-192
- Web Application Vulnerabilities .... 501.3–192
- Web-Based Rootkit Tools .... 501.5–296
- WebDefend .... 501.2–9
- WEP .... 501.3–186
- WEP/WPA Cracking .... 501.3–129
- Whitelist .... 501.2–110, 118
- Whois .... 501.3–32
  - Lookup .... 501.3–33
- Windows .... 501.3–234-240
  - Configurations .... 501.3–238
  - Files to Check .... 501.3–234
  - Files to Grab .... 501.3–240
  - Important Files .... 501.3–239
  - IR Commands .... 501.4–93-94, 131-137
  - IR Script .... 501.4–193-195
  - Networking .... 501.3–236-237
  - Password Cracking .... 501.3–180
  - PE .... 501.5–328
  - Process Kill .... 501.5–195
  - Registry Analysis .... 501.4–160-162
  - Registry Keys .... 501.5–11-12
  - System Checks .... 501.3–235
  - System Restore/Rebuild .... 501.5–355-357
  - Tasks Folder .... 501.4–104
- Wireless Attacks .... 501.3–129
- Wireless Network Testing .... 501.3–186
- Wireless Scanning .... 501.3–64, 128
- Wireshark .... 501.2–67-69, 201
  - Expert Info .... 501.2–102, 104
  - Filters .... 501.2–75-77
  - Interface .... 501.2–74
  - TCP Stream .... 501.2–81
- WMIC .... 501.5–5, 37-56, 189
  - Output Formats .... 501.5–49
  - Services .... 501.5–52-56
  - Taskkill .... 501.5–45-46
  - Tasklist .... 501.5–43-44
- Wombat Security .... 501.3–207
- Word Detection Snort Rule .... 501.2–153
- Worm .... 501.5–7
  - Download Snort Rule .... 501.2–156
  - Snort Rule .... 501.2–146
- WoT .... 501.5–290
- Wpa_supplicant .... 501.1–199
- WQL .... 501.5–5, 38, 40-41
- WS_Ping ProPack .... 501.3–67
- Wtmp 🐧 .... 501.4–88-89, 103, 110

## X

- X-Window Sessions Snort Rule .... 501.2–150
- XCP .... 501.5–205
- Xferlog .... 501.4–111
- XMAS Scan .... 501.3–71
- XML .... 501.2–11
- XOR .... 501.5–160-163
- Xsupplicant .... 501.1–199

## Z

- Zero-day Attacks .... 501.2–13
- ZeroAccess .... 501.5–226
- Zipped DOC Snort Rule .... 501.2–152
- Zone Identifier .... 501.5–140