SANS AUD507 – Auditing & Monitoring Networks, Perimeters, and Systems

Topics

Effective Audit, Risk Assessment & Report

1) Introduction	507.1–2-30
2) Basic Risk	507.1–31-40
3) Practical Risk Assessment	507.1–41-63
4) Time Based Security	507.1–64-93
5) The Audit Process	507.1–94-128
6) Auditing the Cloud	507.1–129-160

Effective Network & Perimeter Auditing

1) Introduction	507.2–2-7
2) Networks	507.2–8-37
3) Firewalls & Routers	507.2–38-82
4) Network Access	507.2–83-97
5) Public Services	507.2–98-114
6) Population Auditing	507.2–115-125
7) Remediation	507.2–126-139

Web Application Auditing

1) Stating the Problem	507.3–3-22
2) Web Basics	507.3–23-52
3) Server Security	507.3–53-66
4) Configuration Testing	507.3–67-80
5) Authentication	507.3–81-98
6) Session Management	507.3–99-122
7) Sensitive Information	507.3–123-175

Advanced Windows Auditing & Monitoring

1) Introduction	507.4–3-12
2) WMIC	507.4–13-24
3) Scripting Basics	507.4–25-44
4) Basic System Information	507.4–45-76
5) Users, Groups & Passwords	507.4–77-110
6) Protecting Data	507.4–111-134
7) OS & Application Security	507.4–135-156
8) Auditing & Logging	507.4–157-180
9) Continuous Monitoring	507.4–181-185

Advanced Unix Auditing & Monitoring

1) Introduction	507.5–3-4
2) Accreditation	507.5–5-10
3) Scripting	507.5–11-40
4) Auditing Unix	507.5–41-56
5) Objectives & Activities	507.5–57-140
6) Unix Logging	507.5–141-152
7) Extra Tools & Ongoing Auditing	507.5–153-161
Appendix - Unix Basics	507.5–161-193

Categories

Summary

Auditing	507.1–30
Authentication	507.3–97
Sensitive Information	507.3–174
Session Tracking	507.3–121
Time Based Security	507.1–93
Web Applications	507.3–22, 51, 78-79

Audit Objectives & Activities

🐧

1- System Information	507.5–58
2- Operating Profile (Services)	507.5–67
3- Unauthorized Access (Network-level)	507.5–84
4- User Management/Access	507.5–90
5- Unauthorized Access (User-level)	507.5–105
6- Unauthorized Access (Critical files)	507.5–105
7- Operating Profile (Info disclosure)	507.5–127
8- Secure Configuration	507.5–135

⊞

1- Basic OS Information	507.4–47-48
2- System Patches/Updates	507.4–55
3- Unnecessary Components/Services	507.4–64
4- Valid Users	507.4–80
5- Appropriate Groups	507.4–96
6- Strong Passwords	507.4–99
7- Restrict Access to Resources	507.4–111
8- File Integrity	507.4–131
9- OS-Specific Vulnerabilities	507.4–136
10- Audit Trail	507.4–157
11- Log Review & Mgt	507.4–166, 169, 176

Checklist Items

Authentication	507.3–97
Basic OS Information ⊞	507.4–51
Cisco	507.2–18
DNS	507.2–104
Group Management ⊞	507.4–108
Group Policy ⊞	507.4–146-147
Logging	507.2–22
Network Behavior 🐧	507.5–81
Network Device	507.2–40
Out of Band Management	507.2–95
Passwords ⊞	507.4–108
Patching	507.2–24
Permissions ⊞	507.4–133
Routing Protections	507.2–65
Security Policy ⊞	507.4–153
Session Tracking	507.3–121
SNMP	507.2–21
System Patches/Updates ⊞	507.4–63
Third Parties / Contracts	507.2–96
Unnecessary Components/Services ⊞	507.4–75
User Account Management ⊞	507.4–108
Virtualization	507.1–160
VLAN	507.2–15
Web Application	507.3–78-79
Web Application Input/Output	507.3–174

SANS AUD507 – Auditing & Monitoring Networks, Perimeters, and Systems

Tools

- **Active Directory** 🪟
  - ADExplorer . . . 507.4–93
  - `ADSchema.xls` . . . 507.4–96
  - DSQuery . . . 507.4–82-87, 91, 96, 98
- **Cracking**
  - Brutus . . . 507.3–96
  - Burp . . . 507.3–96
  - Cain & Abel . . . 507.4–106
  - Hydra . . . 507.3–96
  - John The Ripper . . . 507.4–106
  - . . . 507.5–104
  - LophtCrack . . . 507.4–106
  - Rainbowcrack . . . 507.4–106
- **File Integrity** 🐧
  - AIDE . . . 507.5–117
  - Samhain . . . 507.5–117
  - Tripwire . . . 507.5–117-124
- **Log Management** 🪟
  - ArcSight . . . 507.4–177
  - DAD/Lassie . . . 507.4–179-180
  - MOM/ACS . . . 507.4–177
  - Splunk . . . 507.4–177
- **Network**
  - Firewalk . . . 507.2–56
  - FPort . . . 507.4–69
  - HPing . . . 507.2–55-56
  - InSSIDer 🪟 . . . 507.2–84, 97
  - LinSSID 🐧 . . . 507.2–97
  - `mapper.rb` . . . 507.2–107
  - Netdisco . . . 507.2–120
  - NetScanToolsPro 🪟 ● . . . 507.2–113
  - Netstat . . . 507.4–64, 67
  - . . . 507.5–67-69
  - Network Miner 🪟 . . . 507.2–37
  - `nfstrace` . . . 507.5–154
  - Nipper 🪟 . . . 507.2–81
  - Nmap . . . 507.2–120-121
  - . . . 507.4–64, 68
  - Nslookup . . . 507.2–114
  - Openports . . . 507.4–69
  - OpenView NMS . . . 507.2–120
  - Socat . . . 507.2–65
- **Patch** 🪟
  - BigFix . . . 507.4–56, 60
  - HFNetChk . . . 507.4–56
  - Patchlink . . . 507.4–56, 60
  - SCCM . . . 507.4–56, 60
  - Shavlik . . . 507.4–56
  - WSUS . . . 507.4–56, 60-61
- **Reporting**
  - Nessus ● . . . 507.3–72, 77
  - OpenVMS . . . 507.2–137
  - QualysGuard ● . . . 507.2–136
  - Tripwire . . . 507.5–117-124
  - Yandiff . . . 507.2–124
- **Security Assessment**
  - COPS . . . 507.5–137
  - Lynis 🐧 . . . 507.5–136
  - Metasploit . . . 507.2–107
  - Tiger 🐧 . . . 507.5–137-138
- **System** 🪟
  - AccessEnum (Sysinternals) . . . 507.4–111
  - ACS . . . 507.4–178
  - Addusers . . . 507.4–80
  - `cacls.exe` . . . 507.4–114
  - DumpSec . . . 507.4–80, 94, 96, 99, 111, 126, 130
  - Event Viewer . . . 507.4–158, 178
  - FGDump . . . 507.4–107
  - GPMC . . . 507.4–152
  - `gpresult.exe` . . . 507.4–148
  - `gpupdate.exe` . . . 507.4–143
  - Group Policy . . . 507.4–148
  - Group Policy Editor . . . 507.4–145
  - Hyena . . . 507.4–94
  - LogParser . . . 507.4–158
  - MBSA . . . 507.4–56, 106, 155
  - Mimikatz . . . 507.4–114
  - MMC . . . 507.4–60, 67, 70-71
  - `msinfo32.exe` . . . 507.4–48
  - Net . . . 507.4–80, 98
  - Powershell . . . 507.4–43-44
  - Psinfo (Sysinternals) . . . 507.4–52
  - Psservice (Sysinternals) . . . 507.4–64, 67, 71
  - PWDumpX . . . 507.4–107
  - RSoP . . . 507.4–152
  - `sc.exe` . . . 507.4–64, 67, 71
  - SCA (MMC) . . . 507.4–111, 140-144, 149-150
  - `secedit.exe` . . . 507.4–143, 149
  - ShareEnum (Sysinternals) . . . 507.4–130
  - Showmbrs/Showusrs . . . 507.4–98
  - `systeminfo.exe` . . . 507.4–48-50
  - Tasklist . . . 507.4–64, 67, 73
  - `ver` . . . 507.4–48
  - WinInterrogate . . . 507.4–132
  - `winver` . . . 507.4–48
  - WMIC . . . 507.4–13-24, 49, 53-54, 67, 70, 72, 74
- **System** 🐧
  - `apropos` . . . 507.5–179
  - `cat` . . . 507.5–177
  - `chkconfig` . . . 507.5–68
  - `chklastlog` . . . 507.5–155-156
  - `chkrootkit` . . . 507.5–156
  - `chkwtmp` . . . 507.5–155-156
  - `chmod` . . . 507.5–174
  - `exportfs` . . . 507.5–128-129
  - `fdisk` . . . 507.5–61
  - `find` . . . 507.5–108-110
  - `finger` . . . 507.5–144, 146
  - `free` . . . 507.5–64
  - `gcc` . . . 507.5–52
  - `head` . . . 507.5–178
  - `ifconfig` . . . 507.5–131
  - `ifstatus` . . . 507.5–131
  - `inetd` . . . 507.5–72-73, 85, 88

initctl 507.5–77
inittab 507.5–95
last 507.5–146-147, 149
lastb 507.5–148-149
launchctl 507.5–79
launchd 507.5–76
ldd 507.5–52
less 507.5–178
ls 507.5–176
lsof 507.5–67, 70-71, 113, 156
mail 507.5–87
man 507.5–179
more 507.5–178
mount 507.5–60, 128, 130
patchdiag 507.5–65
pkginfo 507.5–126
ps 507.5–67, 131
pslist 507.5–79
rpcinfo 507.5–128, 131, 185
rpm 507.5–125-126
script 507.5–55
su 507.5–102, 106
sudo 507.5–106
sysctl 507.5–82-83
tail 507.5–178
top 507.5–67
touch 507.5–110-111, 148
uname 507.5–59
up2date 507.5–65
useradd 507.5–102
users 507.5–144
who 507.5–144-146
xinetd 507.5–72, 74-75, 88

Web

Acunetix 507.3–74
AppScan 507.3–74
BURP Suite 507.3–50, 52, 119
IISBanner 507.3–69
J-Baah 507.3–117, 119
N-Stalker 507.3–74
URLScan 507.3–69
WebInspect 507.3–74
WebScarab 507.3–49, 52, 77, 117, 119
Wikto 507.3–74

Labs

1.1 Calculating Samples & Errors 507.1–118
1.2 Examining an ESXi Server 507.1–161
2.1 Layer 2 Traffic 507.2–37
2.2 Network Response 507.2–56
2.3 Firewall Config, ACLs and Validation 507.2–81
2.4 Wireless Clients 507.2–97
2.5 DNS & SMTP Configuration 507.2–114
2.6 Network Population Management 507.2–125
3.1 Using Burp/WebScarab 507.3–52
3.2 WebScarab Fuzzing 507.3–80
3.3 Brute Forcing 507.3–98
3.4 Session Analysis 507.3–122
3.5 Complete Audit 507.3–175
4.1 WMIC 507.4–16, 19, 23, 53-54
4.2 Basic Windows Scripting 507.4–41
4.3 Open Ports & Running Services 507.4–76
4.4 LDAP/DSQuery 507.4–92
4.5 Users, Groups & Passwords 507.4–109
4.6 Protecting Data 507.4–134
4.7 Security Config & Analysis 507.4–154
5.1 Basic Unix Scripting 507.5–14-16, 20-22, 36, 39
5.2 Auditing Unix 507.5–56
5.3 User Mgt & Unauthorized Access 507.5–114
5.4 Operating Profile & Secure Config 507.5–139
5.5 Logging & Additional Tools 507.5–159

SANS AUD507 – Auditing & Monitoring Networks, Perimeters, and Systems

A

- AAA 507.2–18-19
- Access Control 507.4–112, 114
- Account Lockouts 507.3–95
- Accounts 507.4–79-85
  507.5–102
  - Domain 507.4–79
  - Local 507.4–79
  - Orphaned/Unused 507.4–81-82
  - Service 507.4–95
  - Special 507.4–85
- ACK 507.2–54-55, 58, 121
  - Crafting 507.2–55
- ACL 507.2–40, 52-53, 59-66
  507.5–86
  - Discretionary 507.4–111
  - Example 507.2–60
  - Types 507.2–59
- Active Defense 507.5–88
- Active Directory 507.4–80, 88, 90, 103, 151
  507.5–103
  - Objects 507.4–89
- ADMIN$ 507.4–129
- Administration Interface 507.3–64-66
- Administrator 507.2–25, 76
  507.4–85
- AES 507.2–21, 87
- AFP 507.5–130
- AGULP 507.4–115
- AIX 507.5–49, 66
- AJAX 507.3–45-46
- Amazon 507.3–125
- Anti-Caching 507.3–136, 143-144
- Apache 507.3–69-70
- Application 507.3–20
- ARP 507.2–32
- ASR 507.5–119
- Audit 507.1–9
  - Architecture 507.5–158
  - Exception 507.1–9, 51
  - Fail 507.1–42-44
  - Levels 507.1–9
  - Plan 507.4–184
  - Planning 507.1–100-106
- Auditing Terms 507.1–9
- Auditor 507.1–16, 61
  507.2–76
  - Primary Objective 507.1–96-97
  - Reporting 507.1–98
- Authenticated Users 507.4–128
- Authentication 507.3–82-98
  507.4–100, 111
  - Client Side Certificate 507.3–85
  - Form-Based 507.3–84
  - HTTP Basic 507.3–83
  - HTTP Digest 507.3–82
  - NTLM 507.3–86
  - Two-Factor 507.4–101
- Authorization 507.4–111
  507.5–106
- Automated Report 507.5–157
- Automated Scanning Caveat 507.3–75
- Availability 507.4–113

B

- Backdoor 507.5–89
- Banner 507.3–87, 507.5–132-133
- Base-64 507.3–110
- Baseline 507.1–17-19
  507.4–9, 182
  507.5–120, 153, 157
- Bash 507.5–12
  - Awk 507.5–36
  - Echo 507.5–11-39
  - Function 507.5–22
  - Grep 507.5–26-34
  - If 507.5–16-21
  - Sed 507.5–35
  - Shabang 507.5–13
  - Variables 507.5–14
- Basic OS Information 507.4–47-50
- Bastille 507.5–153
- Batch 507.4–26-42
  - For 507.4–38-40
  - If 507.4–31-32
  - Labels 507.4–34-36
  - Return Code 507.4–33
  - Variables 507.4–28
- BitLocker 507.4–102
- Bitwise UserAccountControl 507.4–90
- Blacklist 507.5–88
- Boot Process 507.5–80
- Boot Time Security 507.5–91
- Bootloader 507.5–93
- BOOTP 507.2–26-27
- BPDU 507.2–28-29
- BREACH 507.3–137
- Brute Force 507.3–95-96, 116
  - Attack 507.4–105
- BSD 507.5–61, 103, 118, 136
- `btmp` 507.5–141, 148-149
- Bugbear 507.4–129
- BURP 507.3–50, 76

C

- CA 507.3–85
- CCA 507.1–60, 62
  - Use Case (Event Tree) 507.1–52-54
  - Use Case (Fault Tree) 507.1–59
- CDE 507.5–191-192
- CDP 507.2–26-27
- Certificate 507.3–85
  507.5–98-99

CGI 507.3–5, 61-63
Change Control 507.4–63
507.5–122-123
Checklists 507.1–20-22
CIM 507.4–17
Cipher Inventory 507.3–138
CIS 507.1–103
Cisco 507.2–17-20, 54, 59, 61-62
  Configuration Example 507.2–19, 23, 27, 29, 31, 60
  Password Type 5 & 7 507.2–20
Clean Shell 507.5–54
Client-Side Authentication 507.3–58
Cloud 507.1–130, 132-133
  Auditing 507.1–131, 134-135
  Hybrid 507.1–133
CMS 507.3–9
COBIT 507.1–102
Compliance 507.4–63
Components/Services 507.4–65
Confidentiality 507.4–113
CONNECT 507.1–102
Consequence Cause Analysis 507.1–60
Contracts 507.2–96
Control-Alt-Delete 507.5–95
Controls 507.1–13, 42-43, 50-51, 62
Cookies 507.3–38-43, 105-107
  Types 507.3–43
Cooperative Audit 507.1–28
Correct Process 507.1–45
Creator/Owner 507.4–128
Credentials 507.2–20
507.3–11, 111
507.5–102
Critical Failure 507.1–50
Critical Processes 507.1–45
Critical Update 507.4–57
CRL 507.2–112
Cron 507.5–157-158
  Job 507.5–102, 153
Cross Domain Request 507.3–42
CRUD 507.3–126
CSMA/C[A,D] 507.2–84
CSRF 507.3–169-172
CSS 507.3–47
CVE 507.2–131
Cyber-Defense 507.4–179

D

DACL 507.4–111
DAD 507.4–179
DC 507.1–149
Debian 507.5–66
Deep Packet Inspection 507.2–82
Defense-in-Depth 507.1–67-69, 73
507.2–40-41
DES 507.2–21
507.3–137
507.4–101, 103
`dev` 507.5–130
Device 🐧 507.5–130
Dictionary Attack 507.4–105
Directory Indexing 507.3–55
Disk Encryption 507.4–102
DNS 507.2–102-108, 113
  Cache Poisoning 507.2–104
  Recursion 507.2–104
  Reverse Query 507.2–106
  Zone Transfer 507.2–104
DNSSec 507.2–108
Domain Administrators 507.1–151-152
DoS 507.3–95
507.5–81
Downtime 507.1–55
DSQuery Formulas 507.4–84
DSSS 507.2–85
Dynamically Linked Executables 507.5–52-53

E

EAP 507.2–88
Easter Egg 507.3–57
Eavesdropping 507.3–116
EFS 507.4–102, 113
EIGRP 507.2–65
Elevator Statements 507.1–29
Encrypted Drive 507.5–92
Encryption 507.4–113
Enterprise Mode 507.2–84, 87-88
Entrance Conference 507.1–22, 107-110
ESXi 507.1–136, 138-146
  507.5–92
  Password 507.1–145
  Remote 507.1–141
  Setup Guide 507.1–146
`etc` 507.5–76, 107, 128, 132
Ethernet 507.2–9
EUID 507.5–170
Event Driven Startup 507.5–77
Event Tree 507.1–50-54, 60
Event Viewer 507.4–158-159, 167-169, 178
  ID 507.4–165, 171, 173, 175
Everyone 507.4–128-130
Exception 507.4–63
Exit Conference 507.1–121-124
EXPN 507.2–110
`exports` 507.5–128-129, 188

F

Facility 507.5–150
Failed Login 507.5–148
Failure Scenario 507.1–51
False Positives/Negatives 507.2–137-138
FAT32 507.4–51-52, 54, 111

- Fault Tree ... 507.1–57-60
- FIA ... 507.5–116-126
- Fieldwork ... 507.1–111-118
- File 🐧 ... 507.5–113
- File Integrity ... 507.4–131
- File Integrity Assessment ... 507.5–117-126
- Finger ... 507.5–88
- Firewall ... 507.1–11
  - ... 507.2–50-54, 131
  - Information Flow ... 507.2–50
  - Next Generation ... 507.2–82
  - Rules ... 507.2–63-64, 70, 72
  - Types ... 507.2–52
  - Validation ... 507.2–71-80
- FISCAM ... 507.1–102
- FISMA ... 507.4–63, 153
- Fix ... 507.1–61
- Flash ... 507.3–42
- Formula ... 507.1–32, 55, 70
- `fstab` ... 507.5–128-129, 188
- FTP ... 507.5–88
- Fuzzer ... 507.3–77

G

- GDM ... 507.5–190
- GHDB ... 507.3–7-9
- Gmail ... 507.3–89
- Gold Disk ... 507.4–9
- Google ... 507.3–7, 33
- GPO ... 507.4–147, 151
- Group ... 507.4–78, 128
  - Built-In ... 507.4–97
  - Nested ... 507.4–115
  - Permissions ... 507.4–97
  - Policy ... 507.4–104, 126, 146-153, 167
    - Application Frequency ... 507.4–148, 507.4–151
    - Audit ... 507.4–148
    - Principle ... 507.4–150
    - Structure ... 507.4–147
    - Testing ... 507.4–148
  - Rights ... 507.4–97
  - Special ... 507.4–128
- Grub ... 507.5–93-94
- Guest ... 507.4–85
- GVRP ... 507.2–13, 34

H

- Hardening ... 507.5–153
- Hash ... 507.4–107, 132
  - ... 507.5–100
- Heartbleed ... 507.3–137
- Helix ... 507.5–49
- HelpAssistant ... 507.4–85
- Hidden Disk Space ... 507.5–112
- High-Level OS Checklist ... 507.4–12
- HIPAA ... 507.4–63, 153
- Hoelzer's Law ... 507.1–24
- Host Based Assessment ... 507.5–136
- `hosts.`[`allow`,`deny`] ... 507.5–86, 188
- Hot Key ... 507.5–95
- Hotfix ... 507.4–57-58
- HP-UX ... 507.5–49, 136, 153
- HTML ... 507.3–24-30
  - Forms ... 507.3–30
  - Hidden Fields ... 507.3–113
  - Rules ... 507.3–27
- HTTP ... 507.3–28-37, 100
  - Basic Authentication ... 507.3–108-112
  - Expires ... 507.3–144
  - GET Exposure ... 507.3–127-133
  - GET/POST ... 507.3–31, 37, 124
  - HEAD ... 507.3–31
  - Referer ... 507.3–104, 132
  - Verbs ... 507.3–31-32, 126
- Hybrid Attack ... 507.4–105
- Hypervisor ... 507.1–136

I

- IaaS ... 507.1–133
- IAVA ... 507.4–63
- ICMP ... 507.2–65-66, 121
- IDS/IPS ... 507.2–131
  - ... 507.5–154
- IIS ... 507.3–69, 71, 86, 111
- Incident Handling ... 507.1–23
- Infix ... 507.4–88
- Information Flow ... 507.2–42-49
- Input Testing ... 507.3–145
- Insider Attack ... 507.4–112
- Integrity ... 507.4–113
- Investigation ... 507.5–147
- IPSec ... 507.2–16, 50
- IPv6 ... 507.2–65-66
- `issue` ... 507.5–132-133
- IUSR ... 507.4–85, 128
- IV ... 507.2–85
- IWAM ... 507.4–85, 128

K

- Kali ... 507.5–49
- KB ... 507.4–59
- Kerberos ... 507.5–103
- Kerckhoffs' Principle ... 507.1–83
- Kevin Mitnick ... 507.5–116
- Key ... 507.5–98-99
- Klez ... 507.4–129
- Knowledge Base (Microsoft) ... 507.4–59, 172

L

- L2 Management Protocols 507.2–13, 28, 34, 36
- Lazy Configuration 507.3–61-63
- LDAP 507.4–86-91
  - 507.5–103
  - Objects 507.4–89
  - Queries 507.4–87
- LILO 507.5–93
- Link Count 507.5–113
- LLDP 507.2–27
- LM 507.4–101, 103-104
- Local Service 507.4–95
- LocalSystem 507.4–95
- Log 507.4–158-160
  - Audit 507.4–162, 165
  - Configuration 507.5–150
  - Location 🐧 507.5–150
  - Login Attempts 507.5–99
  - Management 507.4–174, 176-179
    - Best Practice 507.4–177
  - Rotation 🐧 507.5–150
  - Subscription 507.4–167
  - Unix 507.5–141-151
  - Zeroed Entry 🐧 507.5–155
- Logging 507.2–22
  - 507.5–151
  - Levels 🐧 507.5–150
- Logon 507.4–164, 170-171
- `logrotate.conf` 507.5–150
- LRK5 .... 507.5–42-47
- LSASS 507.4–125

M

- MAC 507.2–32
  - Filtering 507.2–90
- Maintenance 507.4–63
- Man in the Middle 507.3–49
- MD4 .... 507.4–103
- MD5 .... 507.4–132
- 507.5–101, 125
- Membership 507.4–78
- Memory 507.5–64
- `messages` 507.5–141-143
- Metacharacters 507.5–27-28
- Mission Statement 507.1–13-15
- Mixed Content/Frames 507.3–141-142
- MOM 507.4–179
- Monitoring 507.4–182
- MOP 507.2–27
- Moscow Rule 507.3–14
- MSTP 507.2–13, 34
- `mtab` 507.5–128
- MTTR 507.2–135
- Multi-Domain 507.4–115
- Multi-Tiered Solution 507.3–20-21
- MVRP 507.2–13, 34

N

- Netscreen 507.2–79
- Network Interfaces 507.5–134
- Network Mapping/Scanning 507.2–116-124
- Network Segregation 507.1–153-159
- Network Service 507.4–95
- NFS 507.5–128-131, 154, 183, 187
  - Configuration 507.5–188
- NIST 507.1–130
- 507.4–11
- Nmap 507.2–121
  - Example 507.4–68
  - Scans 507.2–121
- NoLMHash 507.4–103
- NSX 507.1–137
- NTFS 507.4–51-52, 54, 111, 113
  - Permissions 507.4–127-129
- NTLM 507.4–101, 103-104
- NTP 507.2–23
- Null Session 507.4–136, 138

O

- Object 507.4–114
  - Shared 507.4–129
- Objectives 507.1–13
- Opaserv 507.4–129
- OpenSSH 507.5–98
- Oracle 507.5–66
- OS X 507.5–69, 76, 79, 83, 153
- OSPF 507.2–65
- Out of Band Management 507.2–95
- OWA 507.2–111
- OWASP 507.3–13, 15, 48

P

- PaaS 507.1–133
- Package Manager 🐧 507.5–126
- PAM 507.5–103, 143
- Partition 507.5–62-63
- Password 507.3–91
  - 507.4–78, 100-101
  - 507.5–94
  - Assessment 507.4–106
  - Boot Time 507.5–91
  - File 🐧 507.5–100
  - Policy 507.4–99
  - 507.5–101
  - Testing 507.4–105
- Patching 507.2–24-25, 40, 100
  - 507.4–55
  - Install 507.4–58
  - Process 507.4–62
  - Validation 507.4–59
- PCI 507.2–42, 57
- Permissions 507.4–111-112, 114, 127-129
  - Best Practice 507.4–115
- Persistent 507.3–20

PFS 507.2–85
PGP 507.2–112
PHP Fusion 507.3–9
Physical Access 507.5–91
PKI 507.2–112
Policy 507.1–9, 23
PoLP 507.1–152
507.2–26
507.4–11, 85
POODLE 507.3–137
Port List 507.4–68
Portmapper 507.5–183-184, 192
Postfix 507.4–88
Powershell 507.4–43-44
Prefix 507.4–88
Presentation 507.3–20
Principles 507.2–99
    Complete Mediation 507.3–19
    Economy of Mechanism 507.2–26, 93
    Hoelzer's Law 507.1–24
    Kerckhoffs 507.1–83
    Least Privileges 507.1–152
    507.2–26
    Robust Error Handling 507.3–14
    Separation of Duties 507.1–150, 152
    507.2–93
    Trust Nothing 507.3–14
    Unneeded Services 507.2–26
    507.4–66
    Validation 507.2–75, 130
Private VLAN Bypass 507.2–33
`proc` 507.5–113, 130
Process 🐧 507.5–113
    Table 507.5–131
Process Tracking 507.4–165
Promiscuous Mode 507.5–134
Proxy 507.2–52
PSK 507.2–87
PSTools 507.4–71

Q

QFE 507.4–57
Qualys 507.2–136
507.3–139-140

R

RADIUS 507.2–17-19
RBAC 507.4–115
RC-4 507.2–85-87
507.4–178
RedHat 507.5–65-66, 94, 125
Regex 507.5–29-34
Registry 507.4–126
Regular Expression 507.5–27-28
Remediation 507.2–135
Remote Access 507.5–96-99
Replay Attack 507.4–104
Report to Management 507.1–125-128
Reporting 507.1–119-120
507.2–128-130, 134
507.5–118
Resource 507.4–111
REST 507.3–126
Retention 507.4–160
`.rhosts` 507.5–116
Rights 507.4–114
    Recommendations 507.4–114-125
RIP 507.2–65
Risk 507.1–32
    Analysis Process Using TBS 507.1–82-89
    Assessment 507.1–41, 62
        Characteristics 507.1–46
        Formula 507.1–32, 92
        Use Case (Wireless) 507.1–81-83, 85
    Based Approach 507.2–118-119
    Driven Process 507.2–5
    High-Level Assessment 507.2–130
Roaming Profiles 507.4–102
`robots.txt` 507.3–59-60
Root Cause 507.1–47-48, 60-61
Rootkit 507.5–134, 156
Router 507.2–52, 64
Routing Protection 507.2–65
507.5–81-83
RPC 507.5–128, 131, 182-185, 192
    Working 507.5–183
RSA 507.3–12
`rsync` 507.5–75
Rules 507.2–72
Runlevel 507.5–78

S

S/MIME 507.2–112
SaaS 507.1–133
SAM 507.4–103, 113
SAMBA 507.5–128
Sampling 507.1–114-118
SAN 507.1–155-159
    Permissions 507.1–157
SAT 507.4–104
Schema Admins 507.4–97
Schwab 507.3–35, 92
SECUR 507.5–153
`secure` 507.5–141, 143
`securetty` 507.5–96-97
Security Audit 507.1–9
Security Bulletin 507.4–59
Security Template 507.4–70, 126, 142, 151
507.5–153
    Hisec 507.4–142
    Secure 507.4–142
Sensitive Data 507.4–113
Service 🐧 507.5–72

- Listening 507.5–71
- Service Pack 507.4–51, 57
- Services 507.2–26-27
- Session Tracking 507.3–100-121
  - Attacks 507.3–116-118
  - Auditing 507.3–114, 119-120
  - ID 507.3–101-102, 114-115
    - Best Practice 507.3–115, 119
    - Properties 507.3–115
  - Methods 507.3–103
    - Basic Authentication 507.3–108-112
    - Cookies 507.3–105-107
    - Hidden Fields 507.3–113
    - URL Rewriting 507.3–104
- SGID 507.5–107, 171-173
- SHA1 507.4–132
- Shadow File 🐧 507.5–101-102
- Share Permissions 507.5–128
- Shell Scripting 507.5–11-39
- Shimomura 507.5–116
- Signatures 507.2–137
- Single-Domain 507.4–115
- Six-Step Auditing Process 507.1–98
  - 1- Audit Planning 507.1–100-106
  - 2- Entrance Conference 507.1–107-110
  - 3- Fieldwork 507.1–111-118
  - 4- Preparing the Report 507.1–119-120
  - 5- Exit Conference 507.1–121-124
  - 6- Report to Management 507.1–125-128
- Smarthost 507.2–109
- SMB 507.5–130
- SMTP 507.2–109-113
- Sniffer 507.2–73-74, 89, 138
  507.5–134, 154
- SNMP 507.2–16, 21, 120
- SOA 507.3–32
- Social Engineering 507.2–103
- SOCKS 507.5–88
- SoD 507.1–150, 152
  507.2–93
  507.4–11
- Solaris 507.5–49, 65-66, 118, 134, 136
- Source Routing 507.2–65-69
  507.5–81
  - Example 507.2–67-69
- SPB 507.2–13
- Speed Bump 507.3–95
- Speed Limit Test 507.1–25
- Split-DNS 507.2–105
- SQL 507.3–145
  - Injection 507.3–16, 146-160
    - Protection 507.3–160
- SSH 507.1–140
  507.2–16, 19
  507.3–12
  507.5–87, 97-99
- `sshd_config` 507.5–97
- SSL 507.2–16
  507.3–44, 136-137, 142
- Standards 507.1–42, 45, 63
  507.2–40
  507.4–9
- Startup 507.5–76-80, 133
- Startup Mode 507.4–72
- Stateful Filtering 507.2–52, 58
- Static Packet Filtering 507.2–52-54
- Statically Linked Executables 507.5–52-53
- Sticky Bit 507.5–171-173
- STP 507.2–13-14, 28-29, 34
- Strategy 507.1–15, 47, 106
- Subjective Risk Analysis 507.1–83
- SUID 507.5–107, 109, 170-173
- Sun 507.5–66
- SunSolve 507.5–66
- Super Daemon 507.5–72
- SUPPORT 507.4–85
- Swap 507.5–64
- Switch 507.2–10
  - ARP Attack 507.2–32
  - Configuration Example 507.2–19, 23, 27, 29, 31, 60
  - Private VLAN Bypass 507.2–33
- SYN 507.2–54-55, 58
  507.5–88
- Sysadmins 507.1–16
- `sysctl.conf` 507.5–82
- SYSKEY 507.4–103
- `syslog` 507.5–142-143, 150
- SYSTEM 507.4–95
- System Events 507.4–165

T

- TACACS 507.2–17-18
- TCPWrappers 507.5–73-74, 85-86, 88, 143
- Telnet 507.5–88
- Tenable 507.2–137
- Third Parties 507.2–96
- Threat 507.1–32
  - Internal 507.1–33-40
- Three-way Handshake 507.2–54, 121
- Time Based Security 507.1–65-93
  - Analysis Process 507.1–76-79
  - Auditing 507.1–91
  - Example 507.2–101
  - Exposure Time 507.1–84, 88, 90
  - Formula 507.1–70-72
  - Lessons Learned 507.1–72
  - Use Case 507.1–75
- Timestamp 🐧 507.5–110
  - Format 507.5–111
- TKIP 507.2–86
- TLS 507.3–44, 136-137
- Toolkit 507.5–48-51, 54
- Topology (adding Firewall) 507.2–50-51
- TRILL 507.2–13-14
- Tripwire 507.5–118

- Trojan ... 507.4–69

U

- Ubuntu ... 507.5–49, 66
- UDP ... 507.2–121, 123
- UID ... 507.5–107
- Unix ... 507.5–164-193
  - Files & Permissions ... 507.5–170-175
  - GUI ... 507.5–190-192
  - Links ... 507.5–172
  - Philosophy ... 507.5–167-169
  - Services ... 507.5–181-189
- UNKNOWN ... 507.5–149
- Upstart ... 507.5–77, 95
- URL ... 507.3–34
  - Rewriting ... 507.3–104
- User ... 507.4–78
  - Active/Idle 🐧 ... 507.5–145
  - Control 🐧 ... 507.5–103
  - Inputs ... 507.3–124, 133-134
  - Name Harvesting ... 507.3–88-90, 93-94
  - Permissions ... 507.4–97
  - Rights ... 507.4–97, 126
- UserAccountControl ... 507.4–90
- USGCB ... 507.4–138
- USMASK ... 507.5–171
- utmp ... 507.5–141, 144-145

V

- Validation How To ... 507.2–75-76
- var ... 507.5–141
- VAX ... 507.2–27
- VBS ... 507.4–27
- Viewstate ... 507.3–113
- Virtualization ... 507.1–134-161
  - Audit Checklist ... 507.1–160
  - Cluster ... 507.1–149
  - Lessons Learned ... 507.1–135
- VLAN ... 507.2–11-15, 28-30
- VMKernel ... 507.1–155-157
- VMS ... 507.2–27
- VNC ... 507.4–68
- VOIP ... 507.2–28
- VPN ... 507.2–50, 93-95
  ... 507.5–92
- VRFY ... 507.2–110
- VSAN ... 507.1–137
- VSC ... 507.4–107
- vSphere ... 507.1–136-138, 146
  - Admin Role ... 507.1–146
- VTP ... 507.2–13-14, 28-29, 34
- Vulnerability ... 507.1–32, 37
  - Assessment ... 507.2–127-130
    ... 507.5–136-138
  - Scanner ... 507.2–89, 131-138
    ... 507.3–68, 72-73, 76
    ... 507.4–155

W

- Web Applications ... 507.3–4-6, 22
  - Firewall ... 507.3–48
  - Flow ... 507.3–101
  - Good Practice ... 507.3–13, 17
  - Hidden Content ... 507.3–58
  - Programming Errors ... 507.3–10
  - Protection ... 507.3–173
  - Rule of Thumb ... 507.3–37
- WebDAV ... 507.3–32
- WebScarab ... 507.3–49-50, 62, 107
- WEP ... 507.2–85
- Whitelisting ... 507.3–134-135
- Whois ... 507.2–102
- Wildcards ... 507.2–61-62
- Windows ... 507.4–6-8
  - Backup ... 507.4–107
  - Default Shares ... 507.4–129
  - Domain Auditing ... 507.4–10, 46
  - Important Dates ... 507.4–7
  - NTFS Permissions ... 507.4–127-129
  - Rights ... 507.4–116-125
  - Vulnerabilities ... 507.4–138
- WinFS ... 507.4–51
- Wireless ... 507.2–84-92
  - Encryption ... 507.2–85-87
  - IPS ... 507.2–91
  - Typical Deployment ... 507.2–92
- WMI ... 507.4–149
- WMIC ... 507.4–13-24, 53-54
  - Compatibility ... 507.4–16
  - Functionalities ... 507.4–17
  - History ... 507.4–15
  - Reporting ... 507.4–19-21
- WPA ... 507.2–86
- WPA2 ... 507.2–84, 87
- wtmp ... 507.5–141, 146-147, 155
- WWW-authenticate ... 507.3–109

X

- X-Window ... 507.5–190-191
- X.509 Certificate ... 507.3–85
- XDM ... 507.5–190
- XML ... 507.3–45
- XSS ... 507.3–116, 161-168
  - Types ... 507.3–168

Z

- Zone Transfer ... 507.2–104