SANS SEC560 – Network Pen Testing & Ethical Hacking

Topics

PenTest Planning, Scoping & Recon
560.1–5-192
- 1 – Planning ... 560.1–8-121
- 2 – Recon ... 560.1–122-191

In-Depth Scanning
560.2–4-182

Exploitation
560.3–4-193

Post-Exploitation & Merciless Pivoting
560.4–4-185
- 1 – Post-Exploitation ... 560.4–4-105
- 2 – Password Attacks ... 560.4–106-171
- 3 – Merciless Pivoting ... 560.4–172-184

Password Attacks & Web App PenTesting
560.5–4-192
- 1 – Password Attacks ... 560.5–5-76
- 2 – Web App Attacks ... 560.5–77-190

Penetration Test & CTF Workshop
560.6–2-26

Categories

Labs
- Empire ... 560.3–169-192
- Enumerating Users ... 560.2–161-165
- Hydra ... 560.4–132-141
- Metadata Treasure Hunt ... 560.1–132-144
- Metasploit DB & Tool Integration . 560.3–136-147
- Meterpreter ... 560.3–77-98
- Msf `psexec` & `kiwi` ... 560.4–173-184
- Msf `psexec` & run `hashdump` ... 560.4–160-166
- Msfconsole ... 560.3–37-61
- Nessus ... 560.2–134-149
- Netcat for the Pen Tester ... 560.2–176-181
- Nmap ... 560.2–60-67
- Nmap –O –sV ... 560.2–74-79
- NSE ... 560.2–118-125
- Port Pivot Relays ... 560.3–154-160
- PowerShell ... 560.4–96-105
- Recon-ng DNS Analysis ... 560.1–178-192
- Running Commands with `sc` & `wmic` . 560.4–62-72
- Scapy & Tcpdump ... 560.2–98-106
- Scope & RoE Role Play ... 560.1–97-101
- Setting Up The Image ... 560.1–56-66
- Using Veil-Evasion ... 560.3–108-125
- Windows Command-Line Challenges . 560.4–38-48

Training Environments
- Damn Vulnerable Linux ... 560.6–25
- Damn Vulnerable Web App ... 560.6–25
- Hacme Applications (Foundstone) ... 560.6–25
- Metasploitable ... 560.6–25
- Mutillidae (Irongeek) ... 560.6–25
- PenTest Lab (R00tSec) ... 560.6–25
- WebGoat (OWASP) ... 560.6–25

Tools
- 3D Traceroute ... 560.2–27
- Absinthe ... 560.5–178
- Aircrack-ng-CUDA ... 560.5–12
- `ALockout.dll` ⊞ ... 560.4–121
- Amap ... 560.3–129, 133
- App Scanner (Trustwave) ... 560.1–37
- BeEF ... 560.5–130, 132-133
- Burp Suite ... 560.5–96, 170
  - Intruder Module ... 560.5–170
- Cain ... 560.5–25, 560.5–25-27, 31
  - Cracking Tools ... 560.5–25
  - Hash Calculator ... 560.5–32
  - Sniffers ... 560.5–25
  - Wordlists ... 560.5–32
- CANVAS Pro (Immunity) ... 560.1–37
  ... 560.3–21
- CeWL ... 560.4–113
- Cobalt Strike ... 560.3–21
- Commix ... 560.5–160
- CoWPAtty ... 560.5–12
- CUDA Multiforcer ... 560.1–90
- CUDA-Multiforcer ... 560.5–12
- Dradis ... 560.1–120
- Empire ⊞ ... 560.3–162, 169
  - Agents ... 560.3–176-180, 188
  - Commands ... 560.3–170
  - Encrypted Communication ... 560.3–172
  - Features ... 560.3–163-164
  - Listeners ... 560.3–171-174, 180
  - Modules ... 560.3–165-167, 181-185, 189-190
  - Stager ... 560.3–174-175
- Enlightenment Exploit Pack ... 560.3–19
- Enum ⊞ ... 560.2–156, 158, 162-163
- Etherpad ... 560.1–121
- ExifTool ... 560.1–128-129
- FOCA ... 560.1–128
- FoundScan ... 560.2–151
- Free Rainbow Tables Project ... 560.5–55
- Hashcat ... 560.5–13
- HTTrack ... 560.4–6
- Hydra ... 560.2–140-141
  ... 560.4–129
  ... 560.5–76
- IMPACT (Core Security) ... 560.1–37
  ... 560.2–151
  ... 560.3–16, 21
- Jikto ... 560.5–129
- John the Ripper ... 560.4–117, 133, 156

- 560.5–5
  - Configuration File 560.5–6
  - `john.pot` 560.4–117
  - 560.5–7, 21
  - `john.rec` 560.5–8
  - Output 560.5–9
  - Performance 560.5–10
- JSFuck 560.5–134
- Kon-Boot 560.4–127
- L0phtCrack 560.4–150
- Lair 560.1–120
- LFT 560.2–27
- Lm2ntcrack (Metasploit Script) 560.4–111
- LockoutStatus 🪟 560.4–121
- Lynx 560.4–6
- MagicTree 560.1–120
- Mallory 🐧 560.5–96
- MBSA 🪟 560.3–15-16
- MD5 Password Cracker 560.5–12
- MediaWiki 560.1–120
- Metadata Extraction Tool 560.1–128
- Metasploit DB 560.1–120
- 560.3–127-134
- Metasploit Pro (Rapid7) 560.1–37
- 560.2–151
- 560.3–21
  - Browser Autopwn 560.3–14
- Mimikatz 🪟 560.4–143, 157, 168
- Moxie Marlinspike 560.1–90
- N-Stalker (Aker) 560.1–37
- Nessus (Tenable Security) 560.1–37
- 560.2–127-132
- 560.3–129, 133, 140-143
- 560.5–81
  - Plugins 560.2–129-131, 139
  - Report Format 560.2–132, 148
  - Scan Policy 560.2–130-131, 135-146
- Netcat 560.2–167-181
- 560.4–46
  - Options 560.2–168
  - Relay 560.3–151-158
  - 560.4–176
  - Usages 560.2–169
- NeXCSer 560.2–132
- NeXpose (Rapid7) 560.1–37
- 560.2–151
- 560.3–133
- Nikto 560.5–81, 129
  - Options 560.5–83
  - Run 560.5–87
  - Tests 560.5–84-85
- Nmap 560.2–41-58, 167
- 560.3–129, 132-133
  - Badsum Scan 560.2–56, 66-67
  - Network Services File 560.2–50, 63, 71
  - Network Sweeping 560.2–47-49
  - NSE 560.2–112-125
  - 560.5–76
  - Output Formats 560.2–46, 62
  - Port Scanning 560.2–50-55, 61-65
  - Reason 560.2–65
  - Runtime Interaction 560.2–43
  - Service Probes File 560.2–72, 76
  - Timing Options 560.2–44-45
  - Version Detection 560.2–72, 125
- Ntdsxtract 🪟 560.4–170
- NTPasswd 560.4–127
- oclHashcat 560.1–90
- Odysseus 🪟 560.5–96
- OpenVAS 560.2–128
- Ophcrack 560.5–55, 57
  - Configuration 560.5–59, 62
  - Run 560.5–63
- PatchLink Scanner (Lumension) 560.2–151
- Posh-SecMod 🪟 560.3–162, 165
- PowerShell 🪟 560.4–74
  - Aliases 560.4–76
  - Help 560.4–78
  - Pagination 560.4–92
  - Pipeline 560.4–82-87
  - TCP Client 560.4–93, 103
  - Useful Cmdlets 560.4–77
  - Verbs 560.4–75
  - Web Client 560.4–6, 93, 104
  - WhatIf 560.4–81
- PowerShell-AD-Recon 🪟 560.3–162
- PowerSploit 🪟 560.3–162, 165
- PsExec 560.4–51
- PTH Toolkit 560.5–68
- PuTTY 🪟 560.3–152-158
- `pw-inspector` 560.4–130, 134
- PWN Plug (Pwnie Express) 560.1–92
- Pyrit 560.5–12
- Qualys 560.2–151
  - Guard 560.3–133
- Recon-ng 560.1–174-176, 179-189
- 560.3–101
- Retina (BeyondTrust) 560.1–37
- 560.2–151
- RtGen 560.5–55
- SAINT 560.1–37
- 560.2–151
- SATAN 560.2–151
- ScanRand 560.2–13
- Scapy 560.2–81-96
  - Land Attack 560.2–103-104
  - Ping 560.2–101-102
  - Supported Protocols 560.2–82
- SearchDiggity Suite 🪟 560.1–171-172
- Security AppScan (IBM) 560.1–37
- ServifyThis 560.4–58
- SID2user 🪟 560.2–141, 154, 158-159, 164-165
- Software Inspector (Secunia) 560.3–15
- SPI Dynamics 560.5–134
- SqlMap 560.5–169, 178
- Strings 560.1–128, 130

- Tcpdump 🐧 560.2–15-19, 91
  - Options 560.2–17
- Telemachus ⊞ 560.5–96
- THC-Hydra → Hydra
- Traceroute 🐧 560.2–24
- Tracert ⊞ 560.2–26
- UnmanagedPowerShell ⊞ 560.3–162
- Unshadow 560.4–156
- user2SID ⊞ 560.2–141, 154, 158-159, 165
- Veil Framework 560.3–104
  - Veil-Catapult 560.3–104
  - Veil-Evasion 560.3–100, 103-105, 110
  - Veil-Pillage 560.3–104
  - Veil-PowerUp 560.3–104
- VirusTotal 560.3–102
- VSSOwn ⊞ 560.4–169-170
- W3af 560.5–96
- WCE 560.5–68, 76
- WebInspect (HP) 560.1–37
- WebScarab (OWASP) 560.5–96
- Wget 560.4–6
- Wikto ⊞ 560.5–82
- WinDump ⊞ 560.2–16
- Winfingerprint ⊞ 560.2–158
- WinPcap ⊞ 560.5–31, 43
- xHydra 560.4–129, 135-140
- ZAP Proxy (OWASP) 560.5–82, 91, 134, 170
  - Cookie Alteration 560.5–103
  - Features 560.5–92-95
  - Hash Calculator 560.5–94
  - Interface 560.5–99, 101-102
  - Scanning Categories 560.5–93
- Zmap 560.2–13

Linux/Unix Commands

- `apropos` 560.1–231
- `bg` 560.1–215
- `dig` 560.1–162-163
- `exiftool` 560.1–137-138, 141
- `faillog` 560.4–127
- `fg` 560.1–216
- `find` 560.1–206
- `finger` 560.2–154
- `gpg` 560.6–19-20
- `ip neigh` 560.2–58
- `iptables` 560.3–156-157, 160
- `jobs` 560.1–216
- `killall` 560.2–125
- `ldapsearch` 560.2–154
- `locate` 560.1–206
- `lsof` 560.1–222
  - 560.2–124
  - 560.4–137
- `make` 560.1–225
- `md5sum` 560.3–172
- `mknod` 560.3–152, 158
  - 560.4–176
- `nc` 560.2–170-174, 178-181
  - 560.3–158
  - 560.4–176
- `netstat` 560.1–222, 229
- `nmap` 560.2–42, 50, 54, 58, 60-67, 75, 77-78
- `nslookup` 560.1–159-161
  - 560.5–158
- `passwd` 560.1–198
- `ping6` 560.2–58
- `ping` 560.5–156, 188
- `pkill` 560.5–158
- `pwd` 560.1–205
- `shred` 560.1–48
  - 560.5–22
- `smbclient` 560.5–36
- `ssh` 560.3–152
- `strings` 560.1–139-140, 143
- `tar` 560.1–224
- `tcpdump` 560.2–19, 25, 61, 74, 146
  - 560.3–159
- `traceroute` 560.2–25
- `useradd` 560.1–197
- `wget` 560.1–133
- `whatis` 560.1–231
- `which` 560.1–211
- `whois` 560.1–148-149
- `who` 560.2–154
- `ypcat` 560.2–154

Windows Commands

- `arp` 560.4–12
- `at` 560.4–50, 55-56
- `cipher` 560.1–48
- `cmd.exe` 560.3–32, 92-93
  - 560.4–14-15, 58
- `cscript` 560.4–170
- `dir` 560.4–18
- `echo` 560.4–32
- `findstr` 560.4–16
- `find` 560.4–16, 32
- `for` 560.4–32-35, 45-48
- `ipconfig` 560.4–12
- `more` 560.4–16
- `nc.exe` 560.4–46-48, 66-67, 70-71
- `ncpa.cpl` 560.1–59
  - 560.3–78
- `netsh` 560.4–21-22
  - `advfirewall` 560.1–59, 64
  - `wlan` 560.4–11
- `netstat` 560.4–12, 65
- `net` 560.4–19-20
  - `[user|localgroup]` 560.2–161
  - 560.4–41-43
  - `accounts` 560.4–122, 125
  - `use` 560.2–155, 165
  - 560.4–24-25, 35, 52, 55, 57
- `nslookup` 560.1–159-161
  - 560.4–44-45
  - 560.5–158

passprop.exe 560.4–123
ping 560.4–33
  560.5–156
psexec 560.4–50-52
reg 560.4–23
runas 560.2–161
  560.4–39
schtasks 560.4–50, 55-56
sc 560.4–26, 50, 100-101
  [start|stop] 560.4–27, 55, 57, 65-66
  config 560.4–27
  create 560.4–57-58, 64, 66
  query 560.4–26, 28, 55, 64
service.msc 560.4–28
set 560.4–17
taskkill 560.4–65
tracert 560.2–26
type 560.4–16
wmic 560.4–28, 50, 59-60, 69-71, 123

Scapy Interactive Shell
Ether 560.2–84
ICMP 560.2–102
IP 560.2–85, 89, 100
lsc 560.2–83
ls 560.2–82, 86
packet 560.2–84-85
  show() 560.2–86
  summary() 560.2–86
rdpcap() 560.2–96
send(), sendp() 560.2–90
sniff() 560.2–96
sr(), srp() 560.2–90, 92
sr1(), srp1() 560.2–90
srloop() 560.2–95, 101-102
TCP 560.2–85, 87, 89, 100
  flags 560.2–87
wireshark() 560.2–96
wrpcap() 560.2–96

Metasploit Components
armitage 560.3–25-26
msfcli 560.3–25-26
msfconsole 560.3–25-26, 47, 105
msfd 560.3–25-26
msfencode (retired) 560.3–25-26, 103
msfopcode 560.3–25
msfpescan 560.3–25
msfrpcd 560.3–25-26
msfvenom 560.3–25-26, 44-45, 103
  Options 560.3–44
psexec 560.4–160-164, 173-176, 179-180
  560.5–69, 73-75
  Source 560.3–30

MsfConsole Commands
db_[connect|disconnect] 560.3–127
db_[import|export] 560.3–127, 133-134, 138, 143
db_autopwn 560.3–134
db_driver 560.3–127
db_nmap 560.3–129, 132, 137, 139
db_status 560.3–127, 136
exploit 560.3–52, 87, 119
  560.4–164
  560.5–75
hosts 560.3–139, 144, 146
info exploit/multi/handler 560.3–49
jobs 560.3–52
route 560.4–178-179
search [multi/handler|...] 560.3–48, 83
services 560.3–139
sessions 560.3–59-60, 89, 123
  560.4–184
set LHOST ... 560.3–52, 85, 119
  560.4–161
set PAYLOAD ... 560.3–51, 84, 119
  560.4–160
  560.5–73
set SERVICE_... ... 560.4–163
set SMB... ... 560.4–161, 175
set SMBPass [admin_hash] 560.5–69, 74
show advanced 560.4–162
show exploits 560.3–47
show options 560.3–51, 84-85
  560.4–161, 175
show payloads 560.3–50
use exploit/multi/handler 560.3–50, 119
use exploit/windows/smb/psexec 560.4–160
vulns 560.3–143, 145

Meterpreter Commands
background 560.4–179
cat 560.3–65
  560.4–8
cd 560.3–65
creds_all 560.4–183
download 560.3–65
  560.4–8
edit 560.3–65
  560.4–8
execute 560.3–66, 92
exit 560.3–64
getpid 560.3–66, 95
getprivs 560.4–164
getsystem 560.3–19, 74
getuid 560.3–19, 66, 90
  560.4–164
  560.5–75
getwd 560.3–65
hashdump 560.3–73
  560.4–158
help 560.3–64
idletime 560.3–68
interact 560.3–92
ipconfig 560.3–67
  560.4–181

keyscan_[start|dump|stop] 560.3–70, 96
kill 560.3–66
lcd 560.3–65
load [module] 560.3–75
  kiwi 560.4–183
ls 560.3–65, 91
migrate 560.3–66, 95
mkdir 560.3–65
msfmap 560.3–75
portfwd 560.3–67
ps 560.3–66, 90, 95
pwd 560.3–65, 91
reboot 560.3–64
record_[mic] 560.3–69
reg 560.3–64
rmdir 560.3–65
route 560.3–67, 71
run hashdump 560.4–158, 165, 177
run schtasksabuse 560.4–56
screenshot 560.3–68, 94
shell 560.3–93
shutdown 560.3–64
sysinfo 560.3–64, 90
  ....560.4–181
timestomp 560.3–73
uictl 560.3–68
upload 560.3–65
  ....560.4–8
use [module] 560.3–72
use priv 560.3–19, 72, 74
webcam_[list|snap] 560.3–69

PowerShell Cmdlets & Aliases

? 560.4–85
$_ 560.4–84, 94
% 560.4–84, 91, 94, 98-99
alias 560.4–76
echo 560.4–88
format-list 560.4–83
gcm 560.4–94
gc 560.4–87
gm 560.4–82, 94
help 560.4–78, 94
ls 560.4–87, 98-99
ping 560.4–91, 103
ps 560.4–83
select 560.4–86
sls 560.4–89, 91, 94, 99
wget 560.3–176
  ....560.4–93
ForEach-Object 560.4–84
Get-ChildItem 560.4–80
Get-Content 560.4–87
Get-Member 560.4–82
New-Object 560.4–103-104
New-Service 560.4–100-101
Select-Object 560.4–86
Select-String 560.4–89
Start-Service 560.4–101
Where-Object 560.4–85

A

- Account Lockout 560.4–35, 108, 111, 121-127
  560.5–67
  - Settings 560.4–122
- Account Names Harvesting → User Enumeration
- ACK 560.2–30
  - Scan 560.2–53
- Acrobat Reader 560.1–126
- Action Center 560.3–41
- Active Directory 560.4–117, 144, 147
  560.5–28
- Active OS Fingerprinting → OS Fingerprinting
- Address Probing 560.2–47
- AFS 560.5–5
- Agent 560.3–162, 176-180
  - High Integrity 560.3–186
- Amazon Marketplace 560.1–90
- Anonymous Pipe → Forward Pipe
- Antispyware 560.3–81
- Antivirus 560.3–81, 101
  - Evasion 560.3–25, 100-103
- APNIC 560.1–150
- APOP-MD5 560.5–27
- APR 560.5–28
- ARIN 560.1–150-152
- ARP 560.2–49
  560.3–75
  - Cache Poisoning 560.2–83
    560.5–25, 27
  - Poisoned Rounting → ARP Cache Poisoning
  - Request 560.2–47
  - Scan 560.2–60
    560.3–167
- AS(N) 560.1–150
- ASCII 560.1–130
  - Mode 560.4–6
- ASP 560.5–81
- Attack Phases 560.1–22
- Audit 560.1–15
- Authenticated Scan 560.2–137-138
- Auxiliary 560.3–22, 129-130
- AWS 560.1–89
  - Vulnerability/PenTesting Request Form
- AXFR 560.1–162-163

B

- Backdoors 560.1–22
- Backpipe 560.3–152
- Bad Cheksum Scan 560.2–56, 66-67
- Banner Harvesting 560.2–170-172
- Basic Authentication 560.5–95
- BAT File 560.3–174-176
  560.4–36
- Beep 560.2–173-174
  560.4–32
- Behavior-Discoverable Vulnerabilities 560.2–108
- BGP 560.1–150
- BHDB 560.1–170-171
- BID 560.1–35
- Big Endian 560.1–130
- Bind TCP → TCP Bind
- Bing 560.1–170
- BingDiggity 560.1–171
- BitLocker 560.1–47
- Black Box Testing 560.1–81
- Black Hat Hacking 560.1–11
- Blowfish 560.4–152
- BPF 560.2–91
- Bridged Mode 560.1–52, 60-62
  560.3–109
- Browser Exploits 560.3–29
- Browser Wrapper 560.3–81
- Brute Force 560.2–114
  560.4–115
  560.5–6
- BSDi 560.4–152
- Bugtraq ID 560.3–30
- Business Impact 560.1–107
- BypassUAC Attack 560.3–184-187

C

- Cache Snooping → DNS Cache Snooping
- CAPTCHA 560.5–113
- CFS 560.1–47
- CGI 560.5–81
- Chain 560.5–50-54
- Checksum 560.2–56
- CIDR 560.1–150
  560.2–88
  560.3–130
- Cisco 560.5–26
- CISecurity 560.1–46
- Client Browser 560.5–93
- Client-Side Penetration 560.1–93
- Client-Side Test 560.1–20
- Closed Ports 560.2–35
- Cloud 560.1–89-90
- Code Execution 560.3–165-166
- Coldwar Wrapper 560.3–111
- Collaboration Tools 560.1–120-121
- Command & Control 560.3–164
- Command Channel 560.3–5
- Command Injection 560.5–107, 155-156, 169, 176, 187-188
  - Blind 560.5–162-163, 165
  - Useful Commands 560.5–156-158
- `command.com` 560.4–74
- Common TCP Ports 560.2–50
- Common UDP Ports 560.2–55
- Commonly Vulnerable Software 560.3–12
- Compromise 560.1–119
- Contact Information 560.1–76
- Course USB 560.1–50-54

Courtesy Shell 560.3–34
Covert Channels 560.1–22
CRAM-MD5 .... 560.5–27
Credentialed Scan → Authenticated Scan ....
Crypt 560.4–152
Cryptanalysis Attack 560.1–21
Crystal Box Testing 560.1–81
.... 560.2–8
Cscript 560.4–74, 170
CSRF 560.5–107, 109-113
  Token 560.5–113
CSRSS 560.3–19
CUDA 560.5–12
CVE 560.3–30
CWR 560.2–30

D

Dangerous Exploit 560.1–95
Data Disclosure 560.1–82, 85
Data Exfiltration 560.3–166
Data Leakage Prevention 560.1–171
DCE Endpoint 560.2–49
DCERPC 560.3–29
Debriefing 560.1–77
Defacement 560.1–85
Denial of Service 560.1–22, 94
.... 560.2–13, 114, 131, 139
.... 560.4–108, 121
DES 560.4–145, 148-149, 152-153
/dev/tcp Technique → Shell Access Bash ....
Dictionary → Wordlist ....
DigiNinja 560.4–113
Directory Indexing 560.5–89
DLL Injection 560.3–63, 66, 166
DllInject 560.3–34
DLP 560.3–166
DLPDiggity 560.1–171
DMZ 560.2–57
DNS 560.1–158
  Cache Snooping 560.1–161, 175, 187-188
  .... 560.3–101
  Interrogation 560.3–22
  Recursion Desired 560.1–162
  Recursive Lookup 560.1–161-162
  .... 560.2–116
  Reverse Lookup 560.1–119
    cmd.exe → Windows Cmd-Line Reverse DNS .
  .... 560.3–167
  Zone Transfer 560.1–119, 160, 162-163
  .... 560.2–116
Document Metadata → Metadata ....
Domain Service 560.2–55
Drive-by-Download 560.1–171
Dumpster Diving 560.1–22
Dynamic Memory Management 560.3–27

E

Ease of Exploitation 560.1–110
EC2 .... 560.1–90
.... 560.4–115
ECE 560.2–30
Echo 560.4–8
Echo Service 560.2–55
EFS 560.1–47
.... 560.4–127
Elite Speak 560.2–46
Email 560.3–101
  Relay 560.2–116
Encrypted ZIP 560.1–76
Ethical Hacking 560.1–11-12
  Test Types 560.1–20-21
European Data Privacy Directives 560.1–82
Evasion → Antivirus Evasion ....
Executive Summary 560.1–106-107
Exploit 560.3–5, 22, 25, 27
  Client-Side 560.3–11
  Local 560.3–19
  Service-Side 560.3–10
Exploit DB 560.1–35, 168
Exploitation 560.1–22
.... 560.3–5-7
  Campaign 560.3–13
ExploitHub 560.1–36

F

Facebook 560.1–156
False Positives 560.2–108
  Reduction 560.2–132
  .... 560.3–6
FIFO 560.3–152
File Pilfering 560.4–10-12
File Share Mounting 560.4–24
File Transfer 560.3–5
.... 560.4–5-8
FileVault 560.1–47
Filtered 560.2–34
Filtered Port 560.2–52, 106
FIN 560.2–30
  Scan 560.2–53
Findings 560.1–104, 107-108
Finger 560.2–154
Firewall 560.1–44-45
.... 560.2–33-34, 38-39, 56-57
.... 560.3–10-11
  Rule 560.3–156-157
  Ruleset 560.2–11
  Spotting 560.2–56
  Workaround 560.3–151
Forensics Analysis 560.4–144
Forward Pipe 560.3–152
FSDB 560.1–170-171
FTP 560.4–6
  ASCII Mode 560.4–6
  Data 560.2–82

- Fuzzer ... 560.2–114-115

G

- GECOS ... 560.5–6
- Gedit ... 560.4–118
- Get Out of Jail Free Card ... 560.1–69, 71, 75
- GHDB ... 560.1–168-169, 171
  - ... 560.5–82
- Ghost Writing ... 560.3–100
- GLBA ... 560.1–82
- Google Dork ... 560.1–168
- Google Search ... 560.1–119
  - ... 560.4–117
  - Directives ... 560.1–155, 165-167
- Google+ ... 560.1–156
- GoogleDiggity ... 560.1–171
- GPG ... 560.1–76, 169
  - ... 560.4–10
  - ... 560.6–14-15
  - Keyrings ... 560.6–18
- GPU ... 560.5–12-13, 560.4–115
- Gratuitous ARP ... 560.5–28-29

H

- Hackerstorm ... 560.1–36
- Hacking ... 560.1–11
- Half-open Scanning ... 560.2–34
- Hardcoded Password → Password Hardcoded ...
- Hardening ... 560.1–46
- Hash Dump ... 560.3–185, 187
  - ... 560.4–10, 157-158, 173, 177
- Heartbeat ... 560.2–173
- HIPAA ... 560.1–82
- HMAC-MD5 ... 560.4–150-151
- Hop Limit ... 560.2–22
- Host-Only Networking ... 560.3–78
- Hostname ... 560.1–111
  - ... 560.2–8
- HUP ... 560.2–125
- Hybrid Guessing ... 560.4–114
- Hybrid Testing ... 560.1–81

I

- IaaS ... 560.1–89
- IANA ... 560.2–71-72
- IceCast ... 560.3–77, 79
- ICF ... 560.3–32
- ICMP ... 560.2–49
  - ... 560.3–75
  - Address Mask Request ... 560.2–49
  - Echo Request ... 560.2–24, 26, 47, 49, 101
  - ... 560.4–33
  - ... 560.5–156-157
  - Port Unreachable ... 560.2–12, 34, 38, 55
  - Timestamp Request ... 560.2–47, 49
  - TTL Exceeded in Transit ... 560.2–21, 24, 26
- IIS ... 560.3–29
- IKE ... 560.5–26
- Information Gathering ... 560.5–93
- Injected DLL → DLL Injection ...
- Injection Attacks ... 560.5–107
- Input Devices ... 560.3–68
- Insurance ... 560.1–70
- Intelligence ... 560.1–154
- Internal Access ... 560.1–92
- Internal Network Scanning ... 560.2–137
- InterNIC ... 560.1–146
- Intranet ... 560.2–57
- Inventory of Software ... 560.3–15
- Inventory of Target ... 560.1–109, 118, 191
  - ... 560.3–129
  - ... 560.6–22
- IP Probing → Address Probing ...
- IPS ... 560.1–45
  - ... 560.2–56-57
  - ... 560.3–81
- IPv4 Header ... 560.2–21
- IPv6 ... 560.2–57-58
  - ... 560.3–33
  - Header ... 560.2–22
- Isakmp ... 560.2–55
- ISECOM ... 560.1–25
- ISP ... 560.1–43, 88, 150
- IXFR ... 560.1–162

J

- Java Stored Procedures ... 560.5–176
- Javascript ... 560.3–14
- JBoss ... 560.3–166
- Jenkins ... 560.3–166
- JRE ... 560.5–91

K

- Kali Linux ... 560.1–33, 35
  - AMI ... 560.1–90
- Kerberos ... 560.4–147, 157, 171
  - ... 560.5–5, 68
  - Ticket ... 560.2–137
- Kernel Attack ... 560.3–19
- Keystroke Logger ... 560.3–70, 165-166
  - ... 560.4–116
- Kill Date ... 560.3–171
- Kiwi → Meterpreter Modules Kiwi ...

L

- Laboratory ... 560.1–40-48
- LACNIC ... 560.1–150
- Land Attack ... 560.2–103-104
- LANMAN ... 560.1–46
  - ... 560.4–111, 116, 143-144, 147-149, 171

- 560.5–26
    - Challenge/Response 560.4–148, 157
        - Cracking 560.5–34
    - Hash Algorithm 560.4–145
- Large Scan 560.2–9-13
    - Speed Up 560.2–12-13
- LastSeen Time 560.3–179
- Lawyer 560.1–70-71
- LDAP 560.2–154
    - Injection 560.5–107
- Limitation of Liability 560.1–70, 75
- LinkedIn 560.1–156
- Linux 560.1–194
    - Accounts 560.1–197-199
    - Building Tools 560.1–224-226
    - Network 560.1–218-222
    - Processes 560.1–211-216
    - Shortcut Keys 560.1–195
- Linux Networking 560.1–63
- Linux Rescue 560.4–127
- Little Endian 560.1–130
- `LMCompatibilityLevel` 560.1–46
- Load Balancing 560.2–8
- Local Privilege Escalation → Privilege Escalation
- `LookupAccountName` 560.2–158
- LSASS 560.3–19, 167
    - 560.4–157, 168, 182
- Lua 560.2–113

M

- MACE 560.3–73
- Magic Root 560.4–124
- Mail Relay → Email Relay
- Maimon Scan 560.2–53
- Malware Encoding 560.3–100
- MalwareDiggity 560.1–171
- Man-in-the-Middle 560.5–27-28, 96
- Manipulation 560.1–93
- MD4 560.4–146
- MD5 560.4–152
- Metadata 560.1–125
    - Analysis 560.1–127
    - 560.3–14
- Metasploit 560.2–46
    - 560.5–130
- Metasploit Exploitation Framework 560.3–19, 23
    - Arsenal 560.3–22, 28
    - Auxiliary Modules 560.3–129-130
    - Components 560.3–25
    - Database 560.3–127-134
        - Commands 560.3–127
        - Manual Entry 560.3–131
        - Tables 560.3–128
    - RC Configuration File 560.3–108, 116, 119-120
- Meterpreter 560.3–19, 34, 63
    - Commands 560.3–64-75
    - Communication 560.3–63
    - DLL 560.3–66
    - Modules 560.3–72-73
        - Core 560.3–72
        - Kiwi 560.4–168, 178, 182
        - MSFMap 560.3–75
        - Post 560.3–19
        - Priv 560.3–19, 73-74
        - 560.4–158
        - Stdapi 560.3–67, 72
    - Scheduled Task Abuse 560.4–56
- MFT 560.3–73
- Microsoft Office 560.1–126
- Microsoft Sysinternals → Sysinternals
- Mimikatz 560.4–143, 157, 178, 182
- Misconfiguration 560.2–109
    - 560.5–81
- MITRE 560.1–36
- MMX 560.5–5, 10
- Monad 560.4–74
- Monster 560.1–155
- Mount Share → File Share Mounting
- MPI 560.5–11
- MS SQL 560.5–170-171, 560.5–175-176
- MS09-012 560.3–74
- MS10-015 560.3–74
- MS10-021 560.3–74
- Multicast 560.2–58
- MX 560.1–158
- MySQL 560.3–127
    - 560.5–26-27, 170-171, 175-176

N

- Named Pipe 560.3–152
- NAT 560.1–44
    - 560.3–13
- NDA 560.1–68, 127
- Neighbor Discovery 560.2–58
- NetBIOS 560.2–49, 55, 120
    - 560.4–7, 157
- Netcat 560.4–7
    - Annoying Console 560.4–71
    - Backdoor 560.4–63
    - Relay 560.3–152-158
    - 560.4–176
- Netcat-Style Shell Access 560.5–164
- Network Authentication 560.5–67
- Network Penetration 560.1–93
- Network Service Test 560.1–20
- Network Sweep 560.1–119
    - 560.2–6, 48-49
    - 560.3–167
- Network Tracing 560.2–6
- NFS 560.2–55
    - 560.4–7
- NIS 560.2–154
- NIST 560.1–27
    - SP 800-115 560.1–27

  - SP 800-42 560.1–27
  - SP 800-53A 560.1–27
- NLNZ 560.1–128
- No Magic Root → Magic Root
- NOP 560.3–100
  - Sled 560.3–27
- Notes Taking 560.1–45
- NS 560.1–158
- NSE 560.2–41, 110, 112-116
  - Categories 560.2–114
  - PsExec 560.2–121
  - Scripts 560.2–116, 118
    - With Version Scanning 560.2–125
- NT 560.4–111, 116, 143-144, 147-149
  - Hash Algorithm 560.4–146
- `ntds.dit` 560.4–117, 144, 157, 169-170
- NTLM 560.1–46
  560.2–137
  560.4–147, 151, 157, 171
  560.5–26, 95
  - Challenge/Response 560.4–149-150
    - Cracking 560.5–34
- NTP 560.2–55
- Null RPC 560.2–72
- Null Scan 560.2–53
- Null Session → SMB Null Session

O

- Obfuscation 560.3–66
- Open Job Requisitions 560.1–155
- OpenCL 560.5–13
- OpenMP 560.5–11
- Oracle 560.5–26, 170-171, 175-176
- OS Fingerprinting 560.2–6, 69-70, 72, 75
  560.3–139
  560.5–157
  - Methods 560.2–70
- OSSTMM 560.1–25
- OSVDB 560.3–30
  560.5–87
- Out-of-Scope Attack 560.3–13
- Outbound Access 560.3–11
- OWASP 560.1–28
  560.5–91
- OWF 560.4–145, 150-151

P

- PaaS 560.1–89
- Packet Crafting 560.2–54, 81, 84-85
- Packet Tracing 560.2–42, 58
- Packetstorm Security 560.1–35
- PAM 560.4–124
  - Tally 560.4–124
- Paros Proxy 560.5–91
- Pass-the-Hash 560.2–137
  560.4–53, 59, 116
  560.5–76
  - Metasploit 560.5–69
  - Technique 560.5–67
- Pass-the-Token 560.5–68
- Password 560.4–107
  - Attacks 560.5–76
  - Cracking 560.4–108, 110, 112, 121
    560.5–45, 67, 76
    - Tools 560.5–12
  - Files 560.4–117-119, 156
    - Gedit 560.4–118
  - Guessing 560.4–35, 108, 112, 121, 125
    560.5–67, 76
    - Tool 560.4–129
  - Hardcoded 560.4–11
  - Policy 560.4–130
- Paste 560.4–8
- PAT 560.1–44
- Payload 560.2–55
  560.3–22, 25, 31
  - Encoding 560.3–103
- Penetration Testing 560.1–12-14
  - Duration 560.1–86
  - Process 560.1–68
    - 1) Preparation (NDA, RoE, Scope)
    - 2) Testing (Recon, Scanning, Exploitation, ...)
    - 3) Conclusion (Reporting)
  - Test Types 560.1–20-21
- PenTester's Job 560.1–9
- PenTester's Mindset 560.1–7
- Permission Memo 560.1–69-70, 88
- Persistence 560.3–165
- Persistent XSS → Stored XSS
- Personal Firewall 560.3–81
- PGP 560.1–47, 76, 169
  560.4–10
- Phishing Campaign → Social Engineering Campaign
- PHP 560.5–81
- Physical Assessment 560.1–119
- Physical Penetration 560.1–93
- Physical Security Test 560.1–21
- PII 560.1–139
  560.3–166
  560.6–22
- Pilfering → File Pilfering
- Ping 560.5–156-158
  - Sweep 560.1–93
    560.3–75
    - `cmd.exe` → Windows Cmd-Line Ping Sweep
    - PowerShell → PowerShell Ping Sweep
- Pinterest 560.1–156
- Pivot 560.1–85
  560.3–181
  560.4–178-180
- Pivoting 560.3–67, 71
- POC 560.1–152
- Port Forwarding 560.3–67

Port Scan 560.1–93
  560.2–178
  560.3–189-190
Port Scanner 560.2–41
  560.3–129
  `cmd.exe` → Windows Cmd-Line Port Scanner
  PowerShell → PowerShell Port Scanner
Port Scanning 560.2–6, 32, 37, 50-55
  560.3–22, 75
Post-Exploitation 560.3–6, 22, 104
  Activities 560.3–149
    560.4–5
  Framework 560.3–162
PostgreSQL 560.3–127
  560.5–170
PowerShell 560.3–104, 108, 118
  560.4–74-94
  Echo 560.4–93
  File Search 560.4–98-99
  Options 560.3–118
  Ping Sweep 560.4–91
  Port Scanner 560.4–93, 103
  Service Deletion 560.4–100
PowerUp 560.3–104, 165
Pre-Shared Key 560.4–11
  560.5–12
Privilege Escalation 560.3–18-19, 104, 165, 181, 184
Process Migration 560.3–95
Product Security Test 560.1–21
Production Environment 560.1–91
Prompts 560.1–53
Pseudo-Internal Access 560.1–92
Pseudo-Random String 560.3–183
PsExec 560.2–121
  560.3–29, 166
  560.4–51-53, 160-164, 173-176, 179-180
  560.5–69, 73-75
  If Failure → Veil-Catapult
  Pent Tester's Pledge 560.4–54
PSK 560.4–11
PTES 560.1–26
PTF 560.1–29
PTR 560.1–158
Pwnie Express 560.1–92
PyInstaller Wrapper 560.3–111

R

Race Condition 560.3–19
RADIUS 560.2–55
Rainbow Table 560.4–114, 146
  560.5–45, 47, 76
  Available 560.5–55
  Build 560.5–50-51
  LANMAN 560.5–47, 55
  Lookup 560.5–53
  NT 560.5–55
  Requirements 560.5–48
  Storage 560.5–49, 52
  Unsalted MD5 560.5–55
RD → DNS Recursion Desired
RDP 560.5–27, 560.3–104
Recommendations 560.1–113-114
Reconnaissance 560.1–22, 123, 191
  560.3–101, 181
  Duration 560.1–123
Recovery Mode 560.4–144
Red Teaming 560.1–13
  560.3–163
Reduction Function 560.5–50-52
Reflected XSS 560.5–131-132, 134
Regular Expression 560.4–16
Remote Commands ⊞ 560.4–50
Remote Dial-Up War Dial 560.1–20
Remote Shell 560.3–31
Reporting 560.1–68, 103
  Appendices 560.1–116
  Conclusions 560.1–115
  Duration 560.1–86
  Executive Summary 560.1–106-107
  Format 560.1–105
  Recommendations 560.1–113-114
Representative Sample 560.3–17
Resequencing 560.2–28
`RestrictAnonymousSAM` 560.2–156, 158
Retransmission 560.2–28
Reverse HTTPS 560.3–108
Reverse TCP → TCP Reverse
RFC 1918 560.5–93
RFC 3168 560.2–30
RFC 4960 560.2–63
RFC 793 560.2–32, 53
RFP 560.1–96, 98
RHEL 560.2–108
`RHOSTS` 560.3–130, 144-145
RID 560.2–141
RID 500 560.5–67
RIPE NCC 560.1–150
RIR 560.1–150, 176
Risk 560.1–9
Risk Level 560.1–110
  560.2–132
Risk Posture 560.1–106
Rlogin 560.2–147
`robots.txt` 560.1–169
  560.2–119
Root Cause 560.1–107, 113
Rootkits 560.1–22
Round Robin DNS 560.2–8
Routing Table 560.3–67
  560.4–12
RPC 560.2–55, 72
  560.3–25, 29
RSH 560.4–124
RST 560.2–12, 30, 33, 51-52, 56, 67, 106
  560.3–130

- RTP 560.5–27
- Rules of Engagement 560.1–22, 68, 93
  - 560.2–131
  - 560.3–5, 7, 17, 101, 149
  - 560.4–5, 10, 110, 116-117
  - 560.6–11-12
  - Document 560.1–73-83
  - Template 560.1–27
- Runtime Interaction 560.2–43, 60

S

- SaaS 560.1–89
- Salt 560.4–146, 152-154
  - 560.5–48
- SAM 560.4–10, 117, 143
  - 560.5–28
  - Extraction 560.4–158
- SCADA 560.3–29
- Scan Policy 560.2–130-131, 135-136
  - 560.5–93
- Scanning 560.1–22
  - 560.2–5, 7
  - Good Practice 560.2–15
  - Types 560.2–6-7
- Scope 560.1–68, 73, 108
  - 560.3–101, 149
  - 560.4–110
  - Creep 560.1–86
  - Document 560.1–85-95
  - How 560.1–93
  - Limitation 560.2–10
  - What 560.1–87
- SCP 560.4–6
- Screenshot 560.1–111-112
  - 560.3–165-166
- Script Kiddie 560.2–46
- Script Scanning 560.2–72
- Script Tracing 560.2–113, 122
- SCTP 560.2–63
- Search Databases 560.1–168-170
- Search Engines 560.1–154
- SEBUG 560.1–35
- Secure File Deletion Tool 560.1–48
- SecureState 560.3–75
- Security Advisory 2871997 560.5–67
- Security Assessment 560.1–14
- Security Focus 560.1–35
- Sensitive Info Disclosure → Data Disclosure
- Server Security 560.5–93
- Service Info Grabbing → Banner Harvesting
- SetUID 560.3–19
- SHA-256 560.4–152, 154
- SHA-512 560.4–152, 154
- Shell Access 560.1–111
  - Bash & `/dev/tcp` 560.5–164-165
- Shell History 560.1–169
- Shell Session 560.3–57
- Shellcode Injection 560.3–105
- Shells 560.1–53
- Shunning of Traffic 560.1–80
- SID 560.2–141, 157
- SIMD 560.5–10
- SimpleHTTPServer 560.3–46, 122
- Single 560.3–31-32
- SIP 560.5–27
- Skip Tracing Framework 560.1–123
- SkullSecurity 560.4–112
- SLDB 560.1–170-171
- Slingshot 560.1–33, 56
- SMB 560.2–49, 121, 155
  - 560.3–29
  - 560.4–7, 35, 157
  - Client 560.5–34
  - Enumeration 560.2–121, 141
  - Null Session 560.2–156, 158
  - Scan 560.3–167
  - Session 560.2–154-156
    - 560.4–23-26
    - Establishment 560.2–155, 159
  - Vulnerabilities 560.2–116
- Sniffer 560.2–15
- Sniffing 560.4–116, 171
  - 560.5–76
- SNMP 560.2–55, 137
- Social Engineering 560.1–22, 93
  - 560.3–11, 101
  - Campaign 560.3–13, 16
  - Test 560.1–20
- Social Networking Sites 560.1–156
- Software Inventory → Inventory of Software
- Source Code 560.4–11
- Spear Phishing 560.3–13
- Spoofed Address 560.2–13
- SQL 560.5–107, 167, 171
  - Elements 560.5–173-174
  - Injection 560.5–93, 107, 167-169
    - Blind 560.5–172, 177-178
  - Statements 560.5–172
- SQLite 560.3–127
- SSD 560.5–54
- SSE2 560.5–5, 10, 16-17
- SSH 560.2–122-123
  - 560.3–151-158
  - 560.4–6, 10
  - Tunnel 560.1–92
- SSL 560.2–167
  - 560.5–95
- Stage 560.3–31, 34
- Stager 560.3–31, 33, 174-175
- Staging Key 560.3–171
- Standard Error 560.4–44-45
- Standard Input 560.3–152
- Standard Output 560.3–152
- Stealth Scan 560.2–52
- Stolen Equipment Test 560.1–21

- Stored Procedures 560.5–176
- Stored XSS 560.5–131, 133-134
- SUID 560.3–19
- SYN 560.2–30
  - Spoofing 560.2–103-104
- Sysinternals 560.1–130
  - 560.2–121
  - 560.3–29, 104
  - 560.4–51
- Syskey 560.5–28
  - Decoder 560.5–28

T

- Target IP vs Hostname 560.2–8
- TCP 560.2–28
  - 3-Way Handshake 560.2–31
  - Bind 560.3–32-33
  - Control Bits 560.2–29-30, 54, 69, 89
  - Header 560.2–29
  - Port Scanning 560.2–33-34
    - Connect Scan 560.2–51
    - 560.3–130
    - Other Scan Types 560.2–53
    - SYN Scan 560.2–51-52
    - 560.3–130
  - Reverse 560.3–31-33
- Telnet 560.4–124
- Test Environment 560.1–91
- Test Infrastructure 560.1–40-48
- Test Machine Cleanup 560.1–48
- Test Results Scrubbing 560.1–48
- Testing Methods 560.1–93
  - From Inside 560.1–92
- TFTP 560.4–6
- Third Parties 560.1–88
- Third-Party Pen Testing 560.1–70
- Threat 560.1–9
- Time-Memory Trade-Off 560.5–46, 54
- TLS 560.3–63
- TRACE (HTTP Method) 560.5–88
- Traceroute 560.2–23-27, 72
  - 560.5–25
- TrollSploit 560.3–167, 181
- TrueCrypt 560.1–47
- TTL 560.2–21
- Twitter 560.1–156

U

- UAC 560.3–104
- UDP 560.2–28, 37
  - Common Services Detection 560.2–55
  - Header 560.2–36
  - Payload 560.2–39
  - Port Scanning 560.2–37-39, 55, 64
  - Sweep 560.3–130
- UID 0 560.2–47
  - 560.3–19
  - 560.4–156
- Unannouced Test 560.1–79
- Unneeded Services 560.1–46
- Unpatched Software 560.5–81
- US-CERT 560.1–36
- User Enumeration 560.2–153-165
- User-Agent 560.3–14

V

- VDay 560.3–106
- Version Scanning 560.2–6, 71-72, 77-78
  - 560.3–129
  - With NSE 560.2–125
- VI 560.3–65
- Viewing Data 560.1–82
- Virtual Host 560.5–83
- Virtual Machines 560.1–42
- VirusTotal 560.3–102
- VMWare 560.1–60-62
- VNC 560.3–29, 34
- VNC-3DES 560.5–26
- VoIP 560.5–27
- VPN Configuration 560.1–66
- VSS 560.4–157, 169-170
- Vulnerability 560.1–9
  - Assessment 560.1–14
  - Discovery Methods 560.2–108-109
  - Research Sources 560.1–36
  - Scan 560.1–93
  - Scanner 560.2–41, 110, 127
    - 560.3–129, 133
    - 560.5–81
  - Scanning 560.2–6, 151
    - Tools ● 560.1–37
- Vulnerability Check 560.3–22
- Vulnerable Service 560.3–10
- Vulnerable Training Environments 560.6–25

W

- WAR 560.3–111
- Web App 560.5–79
  - Attack Proxies 560.5–96
  - Pen Testing 560.5–78
- Web Application Test 560.1–20
- Web Spider 560.1–127
  - 560.5–92
- Webcam 560.3–69
- Website Defacement 560.1–85
- WEP 560.4–11
- White Hat Hacking 560.1–11
- Whois 560.1–146-152, 158
  - 560.5–25
  - Databases 560.1–150
  - Sample Lookup 560.1–152

Windows Command-Line 560.4–14-15
    FOR Loops 560.4–29-36
    Ping Sweep 560.4–33
    Port Scanner 560.4–46
    Reverse DNS Lookup 560.4–44-45
Windows Defender 560.3–40
Windows Exploits 560.3–29
Windows File Sharing 560.4–7, 157
Windows Firewall 560.1–59
    .... 560.3–78
    .... 560.5–35
    Disabling 560.3–32
Windows Info Enumeration 560.3–182-183
Windows Networking 560.1–59, 64
Windows Registry 560.4–158
WinLogon 560.3–19
Wireless Assessment 560.1–119
Wireless Client Profile 560.4–11
Wireless Security Test 560.1–20
WMIC 560.4–28, 50, 59-60, 69-70
Word Mangling 560.5–13
Wordlist 560.4–112-114
    Disposal 560.4–114
    Generator 560.4–113
Working Hours 560.3–171
WPA 560.4–11
    .... 560.5–12

X

XLS 560.1–138
Xmas Tree Scan 560.2–53
XML Injection 560.5–107
XPath Injection 560.5–107
XSRF → CSRF ....
XSS 560.5–81, 88, 93, 107, 109, 126-135
    Filtering 560.5–135
    Shell 560.5–130
    Types 560.5–131
    Usage 560.5–127
XST 560.5–88

Z

Zone Transfer → DNS Zone Transfer ....