SEC660– Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Index

- 802.1
  - Q/ISL B1–78
  - shadow B1–75
  - supplicant B1–71
- AMSI B1–26-31
- arp spoofing B1–95
- bgp B1–137
- border gateway protocol B1–137
- browser
  - caching B1–105
- captive portal B1–52-69
- cisco
  - discovery protocol B1–88
  - dtp B1–78
  - port status codes B1–79
- designated router B1–134
- DTP B1–78
  - VLAN hopping attack B1–79-86
- dynamic trunking protocol B1–78
- EAP
  - MD5 B1–71
  - TLS B1–71
  - wired shadow attack B1–74
- filter
  - ettercap B1–105
  - manipulation B1–105
- ghostwriting B1–27
- hot standby router protocol B1–124
- hsrp B1–124
- http
  - redirection B1–163
  - strict transport security B1–167
  - tampering L169
- impersonation
  - browser B1–68-9
  - MAC B1–58, 74
  - operating system B1–65-8
  - user-agent B1–63
- inter-switch
  - LAN B1–78
- IPv6 L160, B1–142-158
  - anycast B1–144
  - enumeration B1–149
  - multicast B1–144
  - neighbor discovery B1–151
  - prefixes B1–144
  - remote discovery B1–156
  - router advertisement B1–153
  - router solicitation B1–153
  - unicast B1–144
- juniper
  - lldep-med B1–78
- link-state advertisements B1–132
- lsa B1–132
- multicast B1–124
- NAC B1–49
  - clientless B1–51
  - dissolvable agent B1–51
- neighbor discovery B1–151
- network admission control B1–49
- open shortest path first protocol B1–132
- ospf B1–132
  - dictionary attack B1–136
  - enumeration B1–134
  - route injection L183
  - state tree B1–134
- OUI B1–61
- pae B1–71
- port
  - access B1–78
  - trunk B1–78
- port access entity B1–71
- RADIUS B1–71
- routing traffic B1–131
- signature detection B1–27
- smb
  - capture B1–106
  - relay B1–107
  - signing B1–107
- sslstrip B1–113
- stateless B1–74
- supplicant B1–71
- UAC B1–26
- user account control B1–26
- virtual router redundancy protocol B1–128
- virtual routers B1–138
- VLAN
  - hopping B1–85
  - trunking B1–78
  - voice hopping B1–85
- vrrp B1–128
- WDAC B1–26
- Windows Defender
  - App Control B1–26
- wired shadow attack B1–74

SEC660– Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Tools/Commands

- `Invoke-AMSIBypass` B1–30
- `Invoke-Obfuscation` B1–30
- `arp` B1–97
- `http_hijack.py` B1–119
- `iptables` B1–66
- `modprobe` B1–84
- `ping6` B1–149
- `sysctl` B1–152, 154
- `vconfig` B1–84
- amsi.fail B1–31
- arpspoof B1–117
- Bettercap B1–111
  - autopwn B1–115
  - caplets B1–112
  - sslstrip B1–168
- Cain B1–55
- chimera B1–30
- chiron B1–155
- Coalfire NPK B1–23
- COMB B1–23
- cpscam B1–60
- detect-new-ip6 ..... B1–149
- eapmd5fuzzies B1–73
- ettercap B1–98
  - filters B1–102
- evilginx B1–177
- fake_router6 ..... B1–154
- fingerbank B1–68
- hurricane electric B1–155
- Loki B1–129, 135
- macshift B1–58
- Magic Unicorn B1–20
- metasploit
  - smb capture B1–106
- miredo B1–155
- mitmdump B1–117
- mitmproxy B1–117, 120, 171
- nmap B1–150
- NPK B1–23
- OSfuscate B1–65
- PacketFence B1–53
- panopticlick B1–68
- parasite6 ..... B1–152
- Probable Password List B1–23
- pwn plug B1–75
- pwnie express B1–75
- Responder B1–107
- scapy B1–67
- Shelter B1–27
- sixxs B1–155
- socat B1–157
- SprayWMI B1–20
- sslstrip B1–163-6
- Sulley B1–73
- Teredo B1–155
- theC2Matrix B1–19
- User Agent Switcher B1–63
- voiphopper B1–90
- yersinia B1–80-3, 127