

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
- basic blocks B3-153
- bgp B1-137
- bit flipping B2-31, L131
- border gateway protocol B1-137
- browser
 - caching B1-105
- captive portal B1-52-69
- ciphers
 - block B2-12
 - stream B2-9
 - IV reuse B2-48
- cisco
 - discovery protocol B1-88
 - dtp B1-78
 - port status codes B1-79
- client-side exploit B2-90-100, L1150
- designated router B1-134
- dll hijacking B2-111
- 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
- exploit suggesters B2-90
- filter
 - ettercap B1-105
 - manipulation B1-105
- fuzzing B3-93
 - block coverage B3-153
 - grammar B3-125
 - instrumented B3-97
 - intelligent mutation B3-98
 - source-assisted B3-164, L3237
- Sulley
 - agents B3-136
 - analysis B3-142
 - grammar B3-125
- ghostwriting B1-27
- GPOs B2-66
- group policy objects B2-66
- hash
 - extension B2-55
 - padding algorithms B2-56
- 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
- IV collision B2-48
- juniper
 - l1dep-med B1-78
- kiosk mode B2-70, L1130
- krack attack B2-53
- library loading B2-107-13
- 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
- oracle padding B2-35
- ospf B1-132
 - dictionary attack B1-136
 - enumeration B1-134
 - route injection L183
 - state tree B1-134
- OUI B1-61
- padding B2-35
- pae B1-71
- pairwise B2-53
- PKCS B2-36
- port
 - access B1-78
 - trunk B1-78
- port access entity B1-71
- powershell
 - autoruns B2-86
 - command order B2-84
 - command precedence B2-84
 - persistent modules B2-87
- RADIUS B1-71
- risk analysis B3-51
- routing traffic B1-131
- signature detection B1-27
- smb
 - capture B1-106

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

relay	B1–107
signing	B1–107
software restriction policies	B2–66
sslstrip	B1–113
stacked tweaks	B3–167
stateless	B1–74
supplicant	B1–71
test case splicing	B3–167
tracing	
linux	B2–102
windows	B2–103-5
UAC	B1–26
user account control	B1–26
virtual router redundancy protocol	B1–128
virtual routers	B1–138
virtualization	B2–69
VLAN	
hopping	B1–85
trunking	B1–78
voice hopping	B1–85
vrrp	B1–128
WDAC	B1–26
wdac	B2–67
windows	
AMSI	B2–126
defender application control	B2–67
defenses	B2–126
EMET	B2–126
Windows Defender	
App Control	B1–26
wired shadow attack	B1–74
wpa2	B2–53

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

Tools/Commands

Invoke-AMSIBypass	B1-30
Invoke-Obfuscation	B1-30
arp	B1-97
certutil.exe	B2-73
debug.exe	B2-73
drltrace	B2-105
http_hijack.py	B1-119
iptables	B1-66
ltrace	B2-102
modprobe	B1-84
ping6	B1-149
sysctl	B1-152, 154
vconfig	B1-84
AFL	B3-165, L3259
amsi.fail	B1-31
APIMonitor	B2-104
arpspoof	B1-117
Bettercap	B1-111
autopwn	B1-115
caplets	B1-112
sslstrip	B1-168
Boofuzz	B3-145-7
Cain	B1-55
chimera	B1-30
chiron	B1-155
Coalfire NPK	B1-23
COMB	B1-23
cpscam	B1-60
detect-new-ip6	B1-149
DLHell	B2-112
Dr. Memory	B2-105
DynamoRIO	B3-154, L3237
Drcov	B3-155
Dynapstalker	B3-157, L3237
eapmd5fuzzies	B1-73
Empire	B2-88, L1171
ent	B2-27
ettercap	B1-98
filters	B1-102
Event Tracing For Windows	B2-103
evilginx	B1-177
fake_router6	B1-154
fingerbank	B1-68
Firewalker	B2-113
hash_extender	B2-58
HookDump	B2-113
hurricane electric	B1-155
ImageMagick	B2-16
jackelope	B3-178

KRACK	B2-53
Loki	B1-129, 135
macshift	B1-58
Magic Unicorn	B1-20
metasploit	
smb capture	B1-106
Mimikittenz	L1158
miredo	B1-155
mitmdump	B1-117
mitmproxy	B1-117, 120, 171
msfvenom	B2-74
nmap	B1-150
NotPowershell	B2-72
NPK	B1-23
OSfuscate	B1-65
PacketFence	B1-53
panopticlick	B1-68
parasite6	B1-152
pcaphistogram	B2-24
PDFSharp	B2-81
POODLE	B2-43
Probable Password List	B1-23
ProcessMonitor	B2-103
PSAttack	B2-72
pwn plug	B1-75
pwnie express	B1-75
Responder	B1-107
scapy	B2-29, B1-67
fuzzing	B3-70-89, L3245
Seatbelt.exe	L1150
SharpHook	B2-114
Shelter	B1-27
Sherlock	B2-90
sixxs	B1-155
socat	B1-157
SprayWMI	B1-20
sslstrip	B1-163-6
Sulley	B1-73, B3-112, L3251
tcpick	B2-27
Teredo	B1-155
theC2Matrix	B1-19
TinyInst	B3-178
unicorn	B2-74
UnmanagedPowershell	B2-72
User Agent Switcher	B1-63
voiphopper	B1-90
Watson	B2-90
Winpeas	L1163
yersinia	B1-80-3, 127