

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
- ASLR B4-138-46
- assembly language B4-36-8
- basic blocks B3-153
- bgp B1-137
- bit flipping B2-31, L131
- border gateway protocol B1-137
- browser
 - caching B1-105
- bss B4-19
- canaries B5-45, 100, B4-126-9
- captive portal B1-52-69
- cdecl B4-31
- 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
- control flow enforcement B5-58
- control flow guard B5-57
- data execution prevention B5-39, B5-79, L5397
 - disable B5-99
- deferred frees B5-55
- 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
- egg hunting B4-84
- ELF B4-40
- environment variable pointer B4-119
- exploit guard B5-54
- exploit suggesters B2-90
- export address table B4-81
- fastcall B4-31
- 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
- gadgets B4-113
- ghostwriting B1-27
- global offset table B4-42
- 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
- indirect branch tracking B5-58
- 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
- isolated heap B5-55
- IV collision B2-48
- jop B4-117
- juniper
 - lldcp-med B1-78
- kernel pool B4-17
- kernel32.dll B4-80
- kiosk mode B2-70, L1130
- kmcs B5-6
- krack attack B2-53
- lazy linking B5-14
- LdrpCheckNXCompatibility B5-83
- library loading B2-107-13
- link-state advertisements B1-132
- linkers B4-39
- loaders B4-39
- low fragmentation heap B5-51
- lsa B1-132
- memgc B5-56
- mmap B4-138, 153
- multicast B1-124
- NAC B1-49

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

clientless	B1–51	seh	B4–81
dissolvable agent	B1–51	sehop	B5–44
neighbor discovery	B1–151	setuid	B4–97
network admission control	B1–49	shadow stacks	B5–58
ntdll	B5–83	shellcode	
object files	B4–20	linux	B4–59–74
open shortest path first protocol	B1–132	multistage	B4–84
oracle padding	B2–35	return-oriented	B4–119
ospf	B1–132	windows	B4–78
dictionary attack	B1–136	signature detection	B1–27
enumeration	B1–134	smb	
route injection	L183	capture	B1–106
state tree	B1–134	relay	B1–107
OUI	B1–61	signing	B1–107
padding	B2–35	software restriction policies	B2–66
pae	B4–16, B1–71	sslstrip	B1–113
paging	B4–17	stack	
pairwise	B2–53	operations	B4–21
pe/coff	B5–10–4	overflows	
magic	B5–14	linux	B4–92–6, L4266, 310
peb	B4–81	pivoting	B5–111
physical memory	B4–5	pointer	B4–11
PIE	B4–150	protection	B4–126–46
PKCS	B2–36	shadow	B5–58
pop-pop-ret	B5–43, 70	tweaks	B3–167
port		stateless	B1–74
access	B1–78	stdcall	B4–31
trunk	B1–78	stripped programs	B4–106
port access entity	B1–71	structured exception handling	B4–81
position independent executable	B4–150	supplicant	B1–71
powershell		symbol resolution	B4–39
autoruns	B2–86	system calls	B4–60
command order	B2–84	test case splicing	B3–167
command precedence	B2–84	thread information block	B4–14
persistent modules	B2–87	tib	B4–14
procedure		tlb	B4–5, 18
calling conventions	B4–31	tracing	
epilogue	B4–27–9	linux	B2–102
prologue	B4–24–5	windows	B2–103–5
procedure linkage	B4–42	translation lookaside buffers	B4–5
process environment block	B4–81	UAC	B1–26
ProcessExecuteFlags	B5–83	use-after-free	B5–55
ProcessInformationClass	B5–83	user account control	B1–26
processors	B4–5	virtual memory	B4–16
RADIUS	B1–71	virtual router redundancy protocol	B1–128
registers		virtual routers	B1–138
general	B4–7–14	virtualization	B2–69
segments	B4–14	VirtualProtect()	B5–99–113
relative virtual addresses	B4–39	VLAN	
relocation	B4–39	hopping	B1–85
return2libc	B4–107, L4295	trunking	B1–78
risk analysis	B3–51	voice hopping	B1–85
rop	B4–112	vrrp	B1–128
disable DEP	B5–99–113	WDAC	B1–26
routing traffic	B1–131	wdac	B2–67
safe unlinking	B5–48	windows	
security cookie	B5–45	AMSI	B2–126
heap	B5–47	api	B5–24

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

aslr	B5–53
cet	B5–58
cfg	B5–51
defender application control	B2–67
defenses	B2–126
EAT	B5–10
EMET	B2–126
hardening	B5–60
hardware dep	B5–79
IAT	B5–10
kernel	B5–6
kernel resources	B4–79
lfh	B5–51
overflow	L5357
peb	B5–26, B5–46
randomization	B5–46
seh	B5–27-8, 40-4
overwrites	B5–66, L5378
tib	B5–25
wow64	B5–29
Windows Defender	
App Control	B1–26
wired shadow attack	B1–74
wpa2	B2–53
ws2_32.dll	B4–84

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
ldd B4-149
ltrace B2-102
modprobe B1-84
objdump B4-44
ping6 B1-149
readelf B4-44
sysctl B1-152, 154
vconfig B1-84
xxd B4-66
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
GDB B4-32-5
hash_extender B2-58
HookDump B2-113
hurricane electric B1-155
ida sploiter B4-122
ImageMagick B2-16
Immunity Debugger B5-15-24

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
Netwide Assmebler B4-65
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
PEDA B4-98, 151
POODLE B2-43
Probable Password List B1-23
ProcessMonitor B2-103
PSAttack B2-72
pwn plug B1-75
pwnie express B1-75
pwntools B4-122
Responder B1-107
Ropper B4-122
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
x64dbg B5-16
yersinia B1-80-3, 127