

# 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
- canaries ..... 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
- 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
- ELF ..... B4-40
- environment variable pointer ..... B4-119
- 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
- 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
- jop ..... B4-117
- juniper
  - lldep-med ..... B1-78
- kernel pool ..... B4-17
- kernel32.dll ..... B4-80
- kiosk mode ..... B2-70, L1130
- krack attack ..... B2-53
- library loading ..... B2-107-13
- link-state advertisements ..... B1-132
- linkers ..... B4-39
- loaders ..... B4-39
- lsa ..... B1-132
- mmap ..... B4-138, 153
- multicast ..... B1-124
- NAC ..... B1-49
  - clientless ..... B1-51
  - dissolvable agent ..... B1-51
- neighbor discovery ..... B1-151
- network admission control ..... B1-49
- object files ..... B4-20
- 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

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

---

paging .....	B4-17	symbol resolution .....	B4-39
pairwise .....	B2-53	system calls .....	B4-60
peb .....	B4-81	test case splicing .....	B3-167
physical memory .....	B4-5	tlb .....	B4-5, 18
PIE .....	B4-150	tracing	
PKCS .....	B2-36	linux .....	B2-102
port		windows .....	B2-103-5
access .....	B1-78	translation lookaside buffers .....	B4-5
trunk .....	B1-78	UAC .....	B1-26
port access entity .....	B1-71	user account control .....	B1-26
position independent executable .....	B4-150	virtual memory .....	B4-16
powershell		virtual router redundancy protocol .....	B1-128
autoruns .....	B2-86	virtual routers .....	B1-138
command order .....	B2-84	virtualization .....	B2-69
command precedence .....	B2-84	VLAN	
persistent modules .....	B2-87	hopping .....	B1-85
procedure		trunking .....	B1-78
calling conventions .....	B4-31	voice hopping .....	B1-85
epilogue .....	B4-27-9	vrrp .....	B1-128
prologue .....	B4-24-5	WDAC .....	B1-26
procedure linkage .....	B4-42	wdac .....	B2-67
process environment block .....	B4-81	windows	
processors .....	B4-5	AMSI .....	B2-126
RADIUS .....	B1-71	defender application control .....	B2-67
registers		defenses .....	B2-126
general .....	B4-7-14	EMET .....	B2-126
segments .....	B4-14	kernel resources .....	B4-79
relative virtual addresses .....	B4-39	Windows Defender	
relocation .....	B4-39	App Control .....	B1-26
return2libc .....	B4-107, L4295	wired shadow attack .....	B1-74
risk analysis .....	B3-51	wpa2 .....	B2-53
rop .....	B4-112	ws2_32.dll .....	B4-84
routing traffic .....	B1-131		
seh .....	B4-81		
setuid .....	B4-97		
shellcode			
linux .....	B4-59-74		
multistage .....	B4-84		
return-oriented .....	B4-119		
windows .....	B4-78		
signature detection .....	B1-27		
smb			
capture .....	B1-106		
relay .....	B1-107		
signing .....	B1-107		
software restriction policies .....	B2-66		
sslstrip .....	B1-113		
stack			
operations .....	B4-21		
overflows .....	B4-92-6, L4266, 310		
pointer .....	B4-11		
protection .....	B4-126-46		
tweaks .....	B3-167		
stateless .....	B1-74		
stdcall .....	B4-31		
stripped programs .....	B4-106		
structured exception handling .....	B4-81		
supplicant .....	B1-71		

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

---

## Tools/Commands

Invoke-AMSIBypass .....	B1-30	jackelope .....	B3-178
Invoke-Obfuscation .....	B1-30	KRACK .....	B2-53
arp .....	B1-97	Loki .....	B1-129, 135
certutil.exe .....	B2-73	macshift .....	B1-58
debug.exe .....	B2-73	Magic Unicorn .....	B1-20
drltrace .....	B2-105	metasploit	
http_hijack.py .....	B1-119	smb capture .....	B1-106
iptables .....	B1-66	Mimikittenz .....	L1158
ldd .....	B4-149	miredo .....	B1-155
ltrace .....	B2-102	mitmdump .....	B1-117
modprobe .....	B1-84	mitmproxy .....	B1-117, 120, 171
objdump .....	B4-44	msfvenom .....	B2-74
ping6 .....	B1-149	Netwide Assmebler .....	B4-65
readelf .....	B4-44	nmap .....	B1-150
sysctl .....	B1-152, 154	NotPowershell .....	B2-72
vconfig .....	B1-84	NPK .....	B1-23
xxd .....	B4-66	OSfuscate .....	B1-65
AFL .....	B3-165, L3259	PacketFence .....	B1-53
amsi.fail .....	B1-31	panopticlick .....	B1-68
APIMonitor .....	B2-104	parasite6 .....	B1-152
arpspoof .....	B1-117	pcaphistogram .....	B2-24
Bettercap .....	B1-111	PDFSharp .....	B2-81
autopwn .....	B1-115	PEDA .....	B4-98, 151
caplets .....	B1-112	POODLE .....	B2-43
sslstrip .....	B1-168	Probable Password List .....	B1-23
Boofuzz .....	B3-145-7	ProcessMonitor .....	B2-103
Cain .....	B1-55	PSAttack .....	B2-72
chimera .....	B1-30	pwn plug .....	B1-75
chiron .....	B1-155	pwnie express .....	B1-75
Coalfire NPK .....	B1-23	pwntools .....	B4-122
COMB .....	B1-23	Responder .....	B1-107
cpscam .....	B1-60	Ropper .....	B4-122
detect-new-ip6 .....	B1-149	scapy .....	B2-29, B1-67
DLHell .....	B2-112	fuzzing .....	B3-70-89, L3245
Dr. Memory .....	B2-105	Seatbelt.exe .....	L1150
DynamoRIO .....	B3-154, L3237	SharpHook .....	B2-114
Drcov .....	B3-155	Shelter .....	B1-27
Dynapstalker .....	B3-157, L3237	Sherlock .....	B2-90
eapmd5fuzzies .....	B1-73	sixxs .....	B1-155
Empire .....	B2-88, L1171	socat .....	B1-157
ent .....	B2-27	SprayWMI .....	B1-20
ettercap .....	B1-98	sslstrip .....	B1-163-6
filters .....	B1-102	Sulley .....	B1-73, B3-112, L3251
Event Tracing For Windows .....	B2-103	tcpick .....	B2-27
evilginx .....	B1-177	Teredo .....	B1-155
fake_router6 .....	B1-154	theC2Matrix .....	B1-19
fingerbank .....	B1-68	TinyInst .....	B3-178
Firewalker .....	B2-113	unicorn .....	B2-74
GDB .....	B4-32-5	UnmanagedPowershell .....	B2-72
hash_extender .....	B2-58	User Agent Switcher .....	B1-63
HookDump .....	B2-113	voiphopper .....	B1-90
hurricane electric .....	B1-155	Watson .....	B2-90
ida sploiter .....	B4-122	Winpeas .....	L1163
ImageMagick .....	B2-16	yersinia .....	B1-80-3, 127