

SEC560— Enterprise Penetration Testing

Terms

/etc/shadow	B3: 68	payload delivery	B2: 36
admin hunting	B1: 63	server-side	B2: 31
annual reports	B1: 68	social engineering	B2: 34
ASNs	B1: 75	types	B2: 30
assumed breach	B2: 68	windows	B2: 45, 49-51
attack phases		file	
covering tracks	B1: 17	install files	B3: 15-6
exploitation	B1: 17	iso	B2: 101
maintaining access	B1: 17	lnk-shortcuts	B2: 103
post-exploitation	B1: 17	permissions	B3: 10
recon	B1: 17	pilfering	B2: 115-6, 132
scanning	B1: 17	searching	B2: 125, 132
authenticated proxy	B2: 89	world-writeable	B3: 10
autonomous systems numbers	B1: 75	zip	B2: 102
BGP	B1: 78	file-transfer	B2: 109-12
browser	B2: 46	firewall	B2: 31, B2: 131
browsers	B2: 33	full-knowledge	B1: 26
c2	B2: 72	group policy	
C:/Windows/Panther	B3: 15-6	objects	B3: 17
certificate transparency	B1: 79	preferences	B3: 17-8
chaining	B2: 80	guardrails	B2: 35, 80
challenge-response		hash	
Kerberos	B3: 99	formats	B3: 68
LANMAN	B3: 63	LANMAN	B3: 60, 63
NTLMv1	B3: 63	MD5	B3: 69
NTLMv2	B3: 65-6, 100-01	NT	B3: 61
CIDR	B1: 78	rounds	B3: 69
cmd.exe autorun	B3: 40	HKCU	B3: 40
common subdomains	B1: 72	html application	B1: 68
competitive intel	B1: 68	implant chaining	B2: 80
cpassword	B3: 15-6	infrastructure recon	B1: 71-81
credential stuffing	B2: 9-10	ingestors	B3: 30
crypt3	B3: 58-66	initial access	B2: 6
daisy-chaining	B2: 80	intrusion prevention	B2: 31
data breaches	B1: 85	ipsec	B2: 131
data dump forums	B1: 85	jitter	B2: 72
dedicated systems	B1: 36	job reqs	B1: 85
dhcpcd	B2: 131	junior testers	B1: 61
dirty cow	B3: 8	kerberos	B3: 99
document-reading apps	B2: 33	kernel	B3: 8
documented permission	B1: 20, 23	kernel attacks	B2: 39
domain		keyrings	B2: 122
admin	B2: 129	linux	
administration	B2: 126	connections	B1: 51
cleanup	B2: 130	filesystem	B1: 46
groups	B2: 129	permissions	B1: 50
users	B2: 127	suid	B1: 51
dynamic code generation	B2: 77	LLMNR	B3: 106
dynamic data exchange	B2: 100	local groups	B2: 128
env variable	B2: 124	lockout	B2: 15
ephemeral shell	B1: 47	duration	B2: 16
exploit	B1: 11	observation window	B2: 16
unquoted paths	B3: 20	threshold	B2: 16
exploitation	B2: 26-8	logon script	B2: 127
client-side	B2: 32-7	LSASS	77
framework	B2: 41	mangling	B3: 51
local privesc	B2: 38	mDNS	B3: 106
		mergers & acquisitions	B1: 67

SEC560— Enterprise Penetration Testing

metasploit	
exploits	B2: 44-7
meterpreter	B2: 53-60
modules	B2: 44
payloads	B2: 44-51
reliability	B2: 47
meterpreter	B2: 53-60
NBT-NS	B3: 106
network sweep	B1: 94
ntds.dit	B3: 59, 75
NTLMv1	B3: 64
NTLMv2	B3: 65-6, 100
attacks	B3: 110
defense	B3: 113
obfuscation	B2: 134
office	
dde	B2: 100
macros	B2: 98
opsec	B2: 89
organizational recon	B1: 67-9
os fingerprinting	B1: 94
nmap	B1: 129
parallel scans	B1: 121
parent process spoofing	B2: 80
pass-the-hash	B3: 54
password	
guessing	B2: 11-22
spraying	B2: 18
passwords	
cloud hardware	B3: 53
dictionaries	B3: 50
in linux	B3: 58-66
in windows	B3: 58-66
keystroke	B3: 54
mangling	B3: 51
reporting	B3: 56
salt	B3: 61
sniffing	B3: 54, 100-01
syncd	B3: 49
payload delivery	B2: 36
payloads	B2: 97
PCI	B1: 61
penetration test	
definition	B1: 15
types	B1: 16
permissions	B1: 50
persistence	
cmd.exe autorun	B3: 40
HKCU	B3: 40
scheduled task	B3: 42
services	B3: 43
startup folder	B3: 41
WMI events	B3: 43
pgp	B2: 122
plugins	B1: 149
polling interval	B2: 72
port scan	B1: 94
post-exploitation	B2: 108
powershell	
obfuscation	B2: 134
pre-engagement	
goals	B1: 22
rules	B1: 24
scope	B1: 23
press releases	B1: 68
privacy regulations	B1: 27
privesc	
linux	
files	B3: 10
kernel	B3: 8
service	B3: 9
suid	B3: 11
local	B2: 38
windows	
alwaysinstallelevated	B3: 14
dll hijacking	B3: 14
group policy preferences	B3: 17-8
unattended install files	B3: 15-6
unquoted paths	B3: 20
writable service executables	B3: 14
privileged process	B2: 39
psexec	B2: 45
purple team	B1: 13
race conditions	B2: 39
recon	
ethics	B1: 64
infrastructure	B1: 71-81
internal PCI	B1: 61
light-touch	B1: 62
organizational	B1: 67-9
user	B1: 82-9
zero-touch	B1: 62
red team	B1: 13
regional internet registries	B1: 78
registry	B2: 133
registry keys	B3: 40
representative sample	B2: 37
RIRs	B1: 78
risk	B1: 12
rules of engagement	B1: 24
runtime env	B2: 33
SAM database	B3: 58, 75
sam database	B2: 122
scada	B2: 46
scans	
asynchronous	B1: 96
efficiency	B1: 96
parallel	B1: 121
stateless	B1: 122
tcp	B1: 103-4, 115-6, 122
types	B1: 94
udp	B1: 106-7, 117
ultrafast	B1: 122
vulnerability	B1: 145-51
scf file	B3: 109
scheduled tasks	B3: 42

SEC560— Enterprise Penetration Testing

scope	B1: 23	exploit obfuscation	B2: 134
security audit	B1: 14	files	B2: 132
sensitive data	B1: 27	firewall	B2: 131
services	B3: 43	passwords	B3: 58-66, 72-7
shared object	B3: 9	registry	B2: 133
shells		WinInet InternetQueryOption	B3: 108
ephemeral	B1: 47	wlan	B2: 131
prompts	B1: 55	WMI	
singles	B2: 48	event subscription	B3: 44
situational awareness	B2: 114	world-writeable	B1: 51
linux	B2: 118-22	WPAD	B3: 108
smart cards	B3: 67	zero-knowledge	B1: 26
smb	B2: 46		
named pipes	B2: 80		
smb relaying	B3: 111		
smb signing	B3: 113		
SPNs	B3: 99		
stagers	B2: 48		
stages	B2: 48		
startup folder	B3: 41		
sudo	B1: 52		
suid	B3: 11, B2: 39, B1: 51, 120		
sysvol	B2: 127		
tactics	B2: 108		
tcp	B1: 99-102		
pivots	B2: 80		
RST	B1: 122		
test types			
full-knowledge	B1: 26		
unannounced	B1: 25		
zero-knowledge	B1: 26		
threat	B1: 12		
TLS	B1: 79		
torrents	B1: 85		
udp	B1: 105		
unannounced test	B1: 25		
unattend.xml	B3: 15-6		
unquoted paths	B3: 20		
user account control	B3: 21-2		
bypass	B3: 23		
user recon	B1: 82-9		
usernames	B2: 14		
vba	B2: 98		
version scan	B1: 94		
VLANs	B3: 113		
Volume Shadow Copy Service	B3: 74		
VSS	B3: 74		
vuln scanning	B1: 145-51		
agent-based	B1: 148		
authenticated	B1: 148		
plugins	B1: 149		
unauthenticated	B1: 148		
vulnerability	B1: 11		
vulnerability assessment	B1: 14		
vulnerability scan	B1: 94		
web proxy auto discovery	B3: 108		
whois	B1: 78		
windows			

SEC560— Enterprise Penetration Testing

Commands

arp	B2: 116
base64	B2: 112
bitsadmin	B3: 26
cscript	B3: 74
dir	B2: 124
findstr	B2: 132
find	B3: 12, B2: 132
ip	B2: 116
lsof connections	B1: 53
more	B2: 132
net.exe	B2: 16
net/net1	B2: 126-30
netsh	B2: 131
netstat connections	B1: 53, B2: 116
ntdsutil.exe	B3: 76
ps	B3: 9
reg	B2: 133
schtasks	B3: 42
set	B2: 124
ss	B2: 116
type	B2: 132
uname	B3: 8
uniq	B3: 50

Tools/Sites

AD Explorer	B2: 135
ALockout.dll	B2: 15
BeRoot	B3: 24
BloodHound	B3: 30-5
C2 Matrix	B2: 73
Cain	B3: 102
CeWL	B3: 51
Chameleon	B2: 134
Cobalt Strike	B2: 39
Core IMPACT	B2: 36
crt.sh	B1: 79
DeHashed	B1: 85
DNSDumpster	B1: 75-7
DNSRecon	B1: 73-4
Dradis Reporting	B1: 40
Empire	B3: 23, B2: 88-92
modules	B2: 90-2
ExploitDB	B1: 37
EyeWitness	B1: 140-3
GatherContacts	B1: 86
GetFFGP	
FineGrainedPassPolicy	B2: 18
GhostPack	B2: 137-9
GTFOBins	B3: 12
Hashcat	B3: 89-94
HaveIBeenPwned	B1: 85
Hunter.io	B1: 83
Hydra	B2: 20-2

Immunity CANVAS	B2: 39
JohnTheRipper	B3: 83-6
potfile	B3: 83
unshadow	B3: 71
L0phtCrack	B3: 59
LinPEAS	B2: 39
LinuxExploitSuggester	B2: 39
LockoutStatus.exe	B2: 15
LOLBAS	B3: 26
Masscan	B1: 96, 123-5
Metasploit	B2: 19, B3: 23, B2: 42-60
Meterpreter	B2: 53-60
creds _{all}	B3: 77
hashdump	B3: 73
load kiwi	B3: 77
Mimikatz	B3: 77
MITRE ATTACK	B1: 38
MITRE CVE	B1: 37
Monster.com	B1: 86
NCrack	B2: 19
Netcat	B1: 133-8
nmap	B1: 109-21, 129-33
limitations	B1: 121, 151
os fingerprinting	B1: 129
script.db	B1: 156
scripting engine	B1: 153-6
NPK	B3: 53
NTDSUtil	B3: 76
Patator	B2: 19
Pcredz	B3: 102-4
phonebook.cz	B1: 84
Pipal	B3: 95
Posh-SecMod	B2: 90
PowerBreach	B2: 90
PowerSploit	B2: 90, 134
PowerUp	B3: 25, B2: 90
PowerView	B2: 90, 134
pw-inspector	B2: 13
Responder	B3: 106-13
RIRs	B1: 78
ScanRand	B1: 96
schtasksabuse	B3: 42
Seatbelt	B2: 137-9
secretsdump.py	B3: 59
Shodan	B1: 80-1
SkullSecurity Passwords	B3: 50
Sliver	B2: 76-83
commands	B2: 81
payloads	B2: 79-80, 83
server-client	B2: 82
UACME	B3: 23
Verizon DBIR	B2: 69
VSSOwn	B3: 74
Watson	B3: 24