

SEC560— Enterprise Penetration Testing

Terms

/etc/shadow	B3: 68	ESC8	B5: 82-3
access control		certificate transparency	B1: 79
entities	B5: 70	chaining	B2: 80
ACE	B5: 70	challenge-response	
ADCS	B5: 46	Kerberos	B3: 99
ADDS	B5: 117	LANMAN	B3: 63
admin hunting	B1: 63	NTLMv1	B3: 63
aes	B5: 22	NTLMv2	B3: 65-6, 100-01
amsi	B4: 56-60	CIDR	B1: 78
bypasses	B4: 58-60	cloud shell	B5: 108
AmsiScanBuffer	B4: 57	cmd.exe autorun	B3: 40
annual reports	B1: 68	common subdomains	B1: 72
application control	B4: 71	competitive intel	B1: 68
ASNs	B1: 75	cpassword	B3: 15-6
asrep roast	B5: 104	credential guard	B4: 44
assumed breach	B2: 68	credential reuse	B4: 6
attack phases		credential stuffing	B2: 9-10
covering tracks	B1: 17	crypt3	B3: 58-66
exploitation	B1: 17	daisy-chaining	B2: 80
maintaining access	B1: 17	data breaches	B1: 85
post-exploitation	B1: 17	data dump forums	B1: 85
recon	B1: 17	DCShadow	B5: 40
scanning	B1: 17	DCSync	B5: 38
authenticated proxy	B2: 89	dedicated systems	B1: 36
autonomous systems numbers	B1: 75	dhcpcclient	B2: 131
azure		directory replication service remote	B5: 39
access control	B5: 109, 116	dirty cow	B3: 8
AD	B5: 111, 117	document-reading apps	B2: 33
authentication	B5: 111-8	documented permission	B1: 20, 23
external recon	B5: 121	domain	
federation	B5: 118	admin	B5: 30, 35, B2: 129
IAM	B5: 109	administration	B2: 126
legacy protocols	B5: 128	cleanup	B2: 130
management portals	B5: 108	controllers plural	B5: 36
password attacks	B5: 131-40	DCShadow	B5: 40
recon	B5: 120-29	DCSync	B5: 38
request throttle	B5: 125	groups	B2: 129
scope	B5: 116	ntds file	B5: 33
shell	B5: 108	persistence	B5: 32
synchronization	B5: 118	privesc	B5: 101-4
user enumeration	B5: 122-27	replication	B5: 38
backup servers	B5: 33	skeleton key	B5: 36
BGP	B1: 78	users	B2: 127
browser	B2: 46	DRSR	B5: 39
browsers	B2: 33	dynamic code generation	B2: 77
c2	B2: 72	dynamic data exchange	B2: 100
C:/Windows/Panther	B3: 15-6	env variable	B2: 124
certificate		ephemeral shell	B1: 47
authority	B5: 46	ESC	
internal	B5: 49	1	B5: 50-69
enrollment	B5: 82	4	B5: 71-81
service	B5: 46	8	B5: 82-3
signing request	B5: 46	etypes	B5: 22
template	B5: 50	evasion	B4: 52-69
access control	B5: 70	amsi	B4: 56-60
ESC1	B5: 50-70	application control	B4: 72-80
ESC4	B5: 71-81	signature detection	B4: 64
		static analysis	B4: 61

SEC560— Enterprise Penetration Testing

tactics	B4: 52-69	JWT	B5: 115
windows defender	B4: 65	kerberoasting	B5: 21
exploit	B1: 11	computer accounts	B5: 22
unquoted paths	B3: 20	etypes	B5: 22
exploitation	B2: 26-8	service accounts	B5: 22
client-side	B2: 32-7	targets	B5: 22
framework	B2: 41	kerberos	B3: 99
local privesc	B2: 38	asrep roast	B5: 104
payload delivery	B2: 36	asreq/asrep	B5: 8
server-side	B2: 31	auth	B5: 6
social engineering	B2: 34	golden ticket	94-7
types	B2: 30	impacket	B4: 33
windows	B2: 45, 49-51	kdc	B5: 5-7
extended key usage	B5: 48	kerberoasting	B5: 11
file		krbtgt account	B5: 30, 87-8, 94
install files	B3: 15-6	long-term keys	B5: 8, 88
iso	B2: 101	overpass-the-hash	B5: 29
lnk-shortcuts	B2: 103	pass-the-ticket	B5: 27-8
permissions	B3: 10	priv attribute cert	B5: 10
pilfering	B2: 115-6, 132	service ticket	B5: 11, 13-6
searching	B2: 125, 132	silver ticket	B5: 89
world-writeable	B3: 10	spn	B5: 12, 18
zip	B2: 102	stateless	B5: 95
file-transfer	B2: 109-12	tsreq/tsrep	B5: 11
file/print sharing	B4: 42	ticket reuse	B4: 12
firewall	B2: 31, B2: 131	ticket-granting ticket	B5: 10
full-knowledge	B1: 26	kernel	B3: 8
GetCredentialType	B5: 123-5	kernel attacks	B2: 39
golden ticket	B5: 94-7	keyrings	B2: 122
group policy		LDAP	B5: 116
objects	B3: 17	legacy authn	B5: 128
preferences	B3: 17-8	linux	
guardrails	B2: 35, 80	connections	B1: 51
hash		filesystem	B1: 46
formats	B3: 68	permissions	B1: 50
LANMAN	B3: 60, 63	suid	B1: 51
MD5	B3: 69	LLMNR	B3: 106
NT	B3: 61	local groups	B2: 128
rounds	B3: 69	lockout	B2: 15
HKCU	B3: 40	duration	B2: 16
html application	B1: 68	observation window	B2: 16
hybrid auth	B5: 111	threshold	B2: 16
impacket		login script	B2: 127
kerberos	B4: 33	LSASS	B4: 41, 77, B5: 103
remote exec	B4: 35-7	mangling	B3: 51
secretsdump	B4: 34	mDNS	B3: 106
syntax	B4: 35	memory dumps	B5: 103
implant chaining	B2: 80	mergers & acquisitions	B1: 67
infrastructure recon	B1: 71-81	metasploit	
ingestors	B3: 30	exploits	B2: 44-7
initial access	B2: 6	meterpreter	B2: 53-60
install from media	B5: 34	modules	B2: 44
intrusion prevention	B2: 31	payloads	B2: 44-51
ipsec	B2: 131	psexec	B4: 46
jitter	B2: 72	reliability	B2: 47
job reqs	B1: 85	meterpreter	B2: 53-60
JSON web token	B5: 115	microsoft	
junior testers	B1: 61	ADDS	B5: 117

SEC560— Enterprise Penetration Testing

authentication	B5: 116	startup folder	B3: 41
msbuild	B4: 74-80	WMI events	B3: 43
NBT-NS	B3: 106	pgp	B2: 122
network sweep	B1: 94	pivoting	
ntds file	B5: 33	linux	B4: 6, 84-91
ntds.dit	B3: 59, 75	ssh	B4: 87-8
ntlm		windows	B4: 9-28
relay	B5: 82	PKI	B5: 46
NTLMv1	B3: 64	plugins	B1: 149
NTLMv2	B3: 65-6, 100	polling interval	B2: 72
attacks	B3: 110	port forwarding	B4: 5
defense	B3: 113	port scan	B1: 94
NtProtectVirtualMemory	B4: 63	post-exploitation	B2: 108
OAuthToken	B5: 126-7	powershell	
obfuscation	B2: 134	obfuscation	B2: 134
office		pre-engagement	
dde	B2: 100	goals	B1: 22
macros	B2: 98	rules	B1: 24
OIDC	B5: 107	scope	B1: 23
opsec	B2: 89	press releases	B1: 68
organizational recon	B1: 67-9	priv attribute cert	B5: 10
os fingerprinting	B1: 94	privacy regulations	B1: 27
nmap	B1: 129	privesc	
PAC	B5: 10, 13, 88	domain	B5: 101-4
parallel scans	B1: 121	linux	
parent process spoofing	B2: 80	files	B3: 10
pass-the-hash	B4: 41-9, B3: 54	kernel	B3: 8
mitigations	B4: 44	service	B3: 9
pass-through auth	B5: 118	suid	B3: 11
password		local	B2: 38
guessing	B2: 11-22	windows	
spraying	B2: 18	alwaysinstallelevated	B3: 14
password attacks	B4: 47	dll hijacking	B3: 14
password hash synchronization	B5: 118	group policy preferences	B3: 17-8
passwords		unattended install files	B3: 15-6
cloud hardware	B3: 53	unquoted paths	B3: 20
dictionaries	B3: 50	writable service executables	B3: 14
in linux	B3: 58-66	privileged process	B2: 39
in windows	B3: 58-66	process dumps	B5: 103
keystroke	B3: 54	proxies	B3: 113
mangling	B3: 51	psexec	B2: 45
reporting	B3: 56	purple team	B1: 13
salt	B3: 61	race conditions	B2: 39
sniffing	B3: 54, 100-01	rc4	B5: 22, 36
synced	B3: 49	recon	
payload delivery	B2: 36	ethics	B1: 64
payloads	B2: 97	infrastructure	B1: 71-81
PCI	B1: 61	internal PCI	B1: 61
penetration test		light-touch	B1: 62
definition	B1: 15	organizational	B1: 67-9
types	B1: 16	user	B1: 82-9
permissions	B1: 50	zero-touch	B1: 62
persistence		red team	B1: 13
cmd.exe autorun	B3: 40	regional internet registries	B1: 78
domain/AD	B5: 32	registry	B2: 133
HKCU	B3: 40	registry keys	B3: 40
scheduled task	B3: 42	reporting	B4: 94-119
services	B3: 43	format	B4: 96

SEC560— Enterprise Penetration Testing

representative sample	B2: 37	pivots	B2: 80
rid 512	B5: 30	RST	B1: 122
RIRs	B1: 78	test types	
risk	B1: 12	full-knowledge	B1: 26
rules of engagement	B1: 24	unannounced	B1: 25
runtime env	B2: 33	zero-knowledge	B1: 26
SAM database	B4: 41, B3: 58, 75	threat	B1: 12
sam database	B2: 122	TLS	B1: 79
scada	B2: 46	torrents	B1: 85
ScanContent	B4: 57	UAC	B4: 44
scans		udp	B1: 105
asynchronous	B1: 96	unannounced test	B1: 25
efficiency	B1: 96	unattend.xml	B3: 15-6
parallel	B1: 121	unquoted paths	B3: 20
stateless	B1: 122	UPN	B5: 114
tcp	B1: 103-4, 115-6, 122	user account control	B3: 21-2
types	B1: 94	bypass	B3: 23
udp	B1: 106-7, 117	user principal name	B5: 114
ultrafast	B1: 122	user recon	B1: 82-9
vulnerability	B1: 145-51	usernames	B2: 14
scf file	B3: 109	vba	B2: 98
scheduled tasks	B3: 42	version scan	B1: 94
scope	B1: 23	VLANs	B3: 113
security audit	B1: 14	Volume Shadow Copy Service ...	B5: 33, B3: 74
security identifiers	B4: 44	VSS	B5: 33, B3: 74
sensitive data	B1: 27	vuln scanning	B1: 145-51
services	B3: 43	agent-based	B1: 148
controller	B4: 14	authenticated	B1: 148
name	B4: 16	plugins	B1: 149
shared object	B3: 9	unauthenticated	B1: 148
shells		vulnerability	B1: 11
ephemeral	B1: 47	vulnerability assessment	B1: 14
prompts	B1: 55	vulnerability scan	B1: 94
silver ticket	B5: 89-90	web proxy auto discovery	B3: 108
singles	B2: 48	whois	B1: 78
situational awareness	B2: 114	windows	
linux	B2: 118-22	exploit obfuscation	B2: 134
skeleton key	B5: 36	file/print sharing	B4: 42
smart cards	B3: 67	files	B2: 132
smb	B4: 13, B2: 46	firewall	B2: 131
named pipes	B2: 80	passwords	B3: 58-66, 72-7
smb relaying	B3: 111	registry	B2: 133
smb signing	B3: 113	WinInet InternetQueryOption	B3: 108
source anchor	B5: 118	WinRM	B4: 10-11
SPN	B5: 12, 18	wlan	B2: 131
SPNs	B3: 99	WMI	
ssh		event subscription	B3: 44
key theft	B4: 6	world-writeable	B1: 51
port forwarding	B4: 87-8	WPAD	B3: 108
stagers	B2: 48	X509	B5: 117
stages	B2: 48	zero-knowledge	B1: 26
startup folder	B3: 41		
sudo	B1: 52		
suid	B3: 11, B2: 39, B1: 51, 120		
SYSTEM registry	B5: 33		
sysvol	B2: 127		
tactics	B2: 108		
tcp	B1: 99-102		

SEC560— Enterprise Penetration Testing

Tools/Commands

Get-Credential	B4: 11
Test-WSMan	B4: 11
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
msbuild.exe	B4: 72-9
net.exe	B4: 13, B2: 16
net/net1	B2: 126-30
netsh	B2: 131
netstat connections	B1: 53, B2: 116
ntdsutil.exe	B5: 34, B3: 76
ps	B3: 9
reg	B2: 133
schtasks	B4: 21, B3: 42
sc	B4: 14, 23
services.msc	B4: 16
setspn.exe	B5: 12, 19
set	B2: 124
ss	B2: 116
type	B2: 132
uname	B3: 8
uniq	B3: 50
winrs	B4: 10
wmic	B4: 25-6
AAD-Internals	B5: 120-1
AD Explorer	B2: 135
ADCSPwn	B5: 83
ALockout.dll	B2: 15
BeRoot	B3: 24
BloodHound	B3: 30-5
C2 Matrix	B2: 73
Cain	B3: 102
Certify	
ESC1	B5: 57-61
ESC4	B5: 73-4
Certipy	
ESC1	B5: 65-9
ESC4	B5: 75-81
CeWL	B3: 51
Chameleon	B2: 134
Cobalt Strike	B2: 39
Core IMPACT	B2: 36
crt.sh	B1: 79
DefenderCheck	B4: 65
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
Ews-Crack	B5: 128
ExploitDB	B1: 37
EyeWitness	B1: 140-3
GatherContacts	B1: 86
GetFFGP	
FineGrainedPassPolicy	B2: 18
GetUserSPN	B5: 20
GhostPack	B2: 137-9
GTFOBins	B3: 12
Hashcat	B5: 22, B3: 89-94
HaveIBeenPwned	B1: 85
Hunter.io	B1: 83
Hydra	B2: 20-2
Immunity CANVAS	B2: 39
Impacket	B4: 32-7
golden ticket	B5: 97
silver ticket	B5: 89-90
smbexec/wmiexec	B4: 37
Invoke-Kerberoast	B5: 20
Iptables	B4: 5
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
MailSniper	B5: 128
Masscan	B1: 96, 123-5
Metasploit	B2: 19, B3: 23, 42-60
owa_login	B5: 128
pivoting	B4: 84
psexec	B4: 46
Meterpreter	B2: 53-60
creds_all	B3: 77
hashdump	B3: 73
load kiwi	B3: 77
pivoting	B4: 85-6
Mimikatz	B5: 27-8, B3: 77
DCShadow	B5: 41
DCSync	B5: 39
golden ticket	B5: 97
skeleton key	B5: 37
MITRE ATTACK	B1: 38
MITRE CVE	B1: 37
Monster.com	B1: 86
MSBuild	B4: 72-9
NCrack	B2: 19
Netcat	B4: 5, B1: 133-8
nmap	B4: 10, 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
ntlmrelayx.py	B5: 83

SEC560— Enterprise Penetration Testing

Patator	B2: 19	schtasksabuse	B3: 42
Pcredz	B3: 102-4	Seatbelt	B2: 137-9
phonebook.cz	B1: 84	secretsdump.py	B5: 33, B3: 59
Pipal	B3: 95	SharpBlock	B4: 63
Posh-SecMod	B2: 90	Shodan	B1: 80-1
PowerBreach	B2: 90	SkullSecurity Passwords	B3: 50
PowerSploit	B2: 90, 134	Sliver	B2: 76-83
Out-MiniDump	B5: 103	commands	B2: 81
Remove-Comment	B4: 62	payloads	B2: 79-80, 83
PowerStripper	B4: 62	server-client	B2: 82
PowerUp	B3: 25, B2: 90	UACME	B3: 23
PowerView	B2: 90, 134	VeilEvasion	B4: 53, 69
domain privesc	B5: 101-2	Verizon DBIR	B2: 69
PsExec	B4: 18-20	VirtualProtect	B4: 63
pw-inspector	B2: 13	VirusTotal	B4: 54
Responder	B3: 106-13	VSSAdmin	B4: 34
RIRs	B1: 78	VSSOwn	B3: 74
Rubeus	B4: 12, B5: 27	Watson	B3: 24
ESC1	B5: 62-4	WMIC	B4: 16
ScanRand	B1: 96		