

SEC560— Enterprise Penetration Testing

Terms

/etc/shadow	B3:68	legacy protocols	B5:128
AADSTS-50053	B5:136	lockout bypass	B5:138-40
access control		management portals	B5:108
conditional	B5:147	OAuth Token	B5:131
entities	B5:70	password attacks	B5:131-40
ACE	B5:70	perms	B5:166-72
ADCS	B5:46	contributor	B5:167
ADDS	B5:117	IAM document	B5:168
ADFS Extranet Lockout	B5:137	inheritance	B5:169
admin hunting	B1:63	owner	B5:167
aes	B5:22	reader	B5:167
amsi	B4:56-60	plane	
bypasses	B4:58-60	control	B5:159
AmsiScanBuffer	B4:57	data	B5:159
annual reports	B1:68	recon	B5:120-29
application control	B4:71	request throttle	B5:125
ASNs	B1:75	roles	B5:167
asrep roast	B5:104	scope	B5:116
assumed breach	B2:68	shell	B5:108
attack phases		smart lockout	B5:136
covering tracks	B1:17	synchronization	B5:118
exploitation	B1:17	user access admin	B5:166
maintaining access	B1:17	user enumeration	B5:122-27
post-exploitation	B1:17	backup servers	B5:33
recon	B1:17	BGP	B1:78
scanning	B1:17	browser	B2:46
authenticated proxy	B2:89	browsers	B2:33
authentication		c2	B2:72
central	B5:144	C:/Windows/Panther	B3:15-6
FIDO2	B5:144	central auth server	B5:144
LDAPS	B5:144	certificate	
MFA	B5:144	authority	B5:46
autonomous systems numbers	B1:75	internal	B5:49
AWS		enrollment	B5:82
api gateway	B5:138	service	B5:46
azure		signing request	B5:46
access control	B5:109, 116	template	B5:50
AD	B5:111, 117	access control	B5:70
api manage	B5:157	ESC1	B5:50-70
auth library	B5:162	ESC4	B5:71-81
authentication	B5:111-8	ESC8	B5:82-3
automation	B5:163	certificate transparency	B1:79
backup	B5:157	chaining	B2:80
blobs	B5:157	challenge-response	
compute	B5:157	Kerberos	B3:99
devops	B5:157	LANMAN	B3:63
extensions	B5:163	NTLMv1	B3:63
external recon	B5:121	NTLMv2	B3:65-6, 100-01
federation	B5:118	CIDR	B1:78
global admin	B5:166	cloud shell	B5:108
groups		cmd.exe autorun	B3:40
management	B5:158	common subdomains	B1:72
resource	B5:158	competitive intel	B1:68
IAM	B5:109	conditional access policies	B5:147
identities	B5:171	cpassword	B3:15-6
identity token	B5:171	credential guard	B4:44
infrastructure	B5:157-9	credential reuse	B4:6
		credential stuffing	B2:9-10

SEC560— Enterprise Penetration Testing

crypt3	B3:58-66	install files	B3:15-6
daisy-chaining	B2:80	iso	B2:101
data breaches	B1:85	lnk-shortcuts	B2:103
data dump forums	B1:85	permissions	B3:10
DCShadow	B5:40	pilfering	B2:115-6, 132
DCSync	B5:38	searching	B2:125, 132
dedicated systems	B1:36	world-writeable	B3:10
dhcpcclient	B2:131	zip	B2:102
directory replication service remote	B5:39	file-transfer	B2:109-12
dirty cow	B3:8	file/print sharing	B4:42
document-reading apps	B2:33	firewall	B2:31, B2:131
documented permission	B1:20, 23	first-class citizen	B5:144
domain		full-knowledge	B1:26
admin	B5:30, 35, B2:129	GetCredentialType	B5:123-5
administration	B2:126	global admin	B5:166
cleanup	B2:130	golden ticket	B5:94-7
controllers plural	B5:36	grant	B5:155
DCShadow	B5:40	group policy	
DCSync	B5:38	objects	B3:17
groups	B2:129	preferences	B3:17-8
ntds file	B5:33	guardrails	B2:35, 80
persistence	B5:32	hash	
privesc	B5:101-4	formats	B3:68
replication	B5:38	LANMAN	B3:60, 63
skeleton key	B5:36	MD5	B3:69
users	B2:127	NT	B3:61
DRSR	B5:39	rounds	B3:69
dynamic code generation	B2:77	HKCU	B3:40
dynamic data exchange	B2:100	html application	B1:68
env variable	B2:124	hybrid auth	B5:111
ephemeral shell	B1:47	identity token	B5:171
ESC		IdsLocked	B5:136
1	B5:50-69	imds	B5:170
4	B5:71-81	impacket	
8	B5:82-3	kerberos	B4:33
etypes	B5:22	remote exec	B4:35-7
evasion	B4:52-69	secretsdump	B4:34
amsi	B4:56-60	syntax	B4:35
application control	B4:72-80	implant chaining	B2:80
signature detection	B4:64	infrastructure recon	B1:71-81
static analysis	B4:61	ingestors	B3:30
tactics	B4:52-69	inheritance	B5:169
windows defender	B4:65	initial access	B2:6
execution plan	B5:134	install from media	B5:34
exploit	B1:11	instance metadata service	B5:170
unquoted paths	B3:20	intrusion prevention	B2:31
exploitation	B2:26-8	ipsec	B2:131
client-side	B2:32-7	jitter	B2:72
framework	B2:41	job reqs	B1:85
local privesc	B2:38	JSON web token	B5:115
payload delivery	B2:36	junior testers	B1:61
server-side	B2:31	JWT	B5:115
social engineering	B2:34	kerberoasting	B5:21
types	B2:30	computer accounts	B5:22
windows	B2:45, 49-51	etypes	B5:22
extended key usage	B5:48	service accounts	B5:22
Extranet Lockout	B5:137	targets	B5:22
file		kerberos	B3:99

SEC560— Enterprise Penetration Testing

asrep roast	B5:104	msbuild	B4:74-80
asreq/asrep	B5:8	MSOL	B5:146
auth	B5:6	NBT-NS	B3:106
golden ticket	94-7	network sweep	B1:94
impacket	B4:33	ntds file	B5:33
kdc	B5:5-7	ntds.dit	B3:59, 75
kerberoasting	B5:11	ntlm	
krbtgt account	B5:30, 87-8, 94	relay	B5:82
long-term keys	B5:8, 88	NTLMv1	B3:64
overpass-the-hash	B5:29	NTLMv2	B3:65-6, 100
pass-the-ticket	B5:27-8	attacks	B3:110
priv attribute cert	B5:10	defense	B3:113
service ticket	B5:11, 13-6	NtProtectVirtualMemory	B4:63
silver ticket	B5:89	OAuth Token	B5:131
spn	B5:12, 18	Oauth2	
stateless	B5:95	access token	B5:149, 152
tsreq/tgsrep	B5:11	claims	B5:150
ticket reuse	B4:12	code flow	B5:144-54
ticket-granting ticket	B5:10	flow types	B5:155
kernel	B3:8	JWT	B5:149
kernel attacks	B2:39	refresh token	B5:152-4
keyrings	B2:122	OAuthToken	B5:126-7
LDAP	B5:116	obfuscation	B2:134
legacy authen	B5:128	office	
linux		dde	B2:100
connections	B1:51	macros	B2:98
filesystem	B1:46	OIDC	B5:107
permissions	B1:50	OpenID	
suid	B1:51	access token	B5:149, 152
LLMNR	B3:106	claims	B5:150
load balancing	B5:138	Connect	B5:144, 166
local groups	B2:128	JWT	B5:149
lockout	B2:15	refresh token	B5:152-4
duration	B2:16	opsec	B2:89
observation window	B2:16	organizational recon	B1:67-9
threshold	B2:16	os fingerprinting	B1:94
login.microsoftonline	B5:146	nmap	B1:129
logon script	B2:127	PAC	B5:10, 13, 88
LSASS	B4:41, 77, B5:103	parallel scans	B1:121
managed identity		parent process spoofing	B2:80
system assigned	B5:171	pass-the-hash	B4:41-9, B3:54
user assigned	B5:171	mitigations	B4:44
mangling	B3:51	pass-through auth	B5:118
mDNS	B3:106	password	
memory dumps	B5:103	guessing	B2:11-22
mergers & acquisitions	B1:67	spraying	B2:18
metasploit		password attacks	B4:47
exploits	B2:44-7	password hash synchronization	B5:118
meterpreter	B2:53-60	passwords	
modules	B2:44	cloud hardware	B3:53
payloads	B2:44-51	dictionaries	B3:50
psexec	B4:46	in linux	B3:58-66
reliability	B2:47	in windows	B3:58-66
meterpreter	B2:53-60	keystroke	B3:54
microsoft		mangling	B3:51
ADDS	B5:117	reporting	B3:56
authentication	B5:116	salt	B3:61
MSAL	B5:162	sniffing	B3:54, 100-01

SEC560— Enterprise Penetration Testing

syncd	B3:49	proxies	B3:113
payload delivery	B2:36	http	B5:140
payloads	B2:97	ssh	B5:139
PCI	B1:61	psexec	B2:45
penetration test		purple team	B1:13
definition	B1:15	race conditions	B2:39
types	B1:16	rc4	B5:22, 36
permissions	B1:50	recon	
persistence		ethics	B1:64
cmd.exe autorun	B3:40	infrastructure	B1:71-81
domain/AD	B5:32	internal PCI	B1:61
HKCU	B3:40	light-touch	B1:62
scheduled task	B3:42	organizational	B1:67-9
services	B3:43	user	B1:82-9
startup folder	B3:41	zero-touch	B1:62
WMI events	B3:43	red team	B1:13
pgp	B2:122	regional internet registries	B1:78
phishing		registry	B2:133
device code flow	B5:162	registry keys	B3:40
pivoting		reporting	B4:94-119
linux	B4:6, 84-91	format	B4:96
ssh	B4:87-8	representative sample	B2:37
windows	B4:9-28	rid 512	B5:30
PKCE	B5:155	RIRs	B1:78
PKI	B5:46	risk	B1:12
plugins	B1:149	rules of engagement	B1:24
polling interval	B2:72	runtime env	B2:33
port forwarding	B4:5	SAM database	B4:41, B3:58, 75
port scan	B1:94	sam database	B2:122
post-exploitation	B2:108	scada	B2:46
powershell		ScanContent	B4:57
obfuscation	B2:134	scans	
pre-engagement		asynchronous	B1:96
goals	B1:22	efficiency	B1:96
rules	B1:24	parallel	B1:121
scope	B1:23	stateless	B1:122
press releases	B1:68	tcp	B1:103-4, 115-6, 122
primary refresh token	B5:152-4	types	B1:94
priv attribute cert	B5:10	udp	B1:106-7, 117
privacy regulations	B1:27	ultrafast	B1:122
privesc		vulnerability	B1:145-51
domain	B5:101-4	SCCM	B5:163
linux		scf file	B3:109
files	B3:10	scheduled tasks	B3:42
kernel	B3:8	scope	B1:23
service	B3:9	security audit	B1:14
suid	B3:11	security identifiers	B4:44
local	B2:38	sensitive data	B1:27
windows		services	B3:43
alwaysinstallelevated	B3:14	controller	B4:14
dll hijacking	B3:14	name	B4:16
group policy preferences	B3:17-8	shared object	B3:9
unattended install files	B3:15-6	shells	
unquoted paths	B3:20	ephemeral	B1:47
writable service executables	B3:14	prompts	B1:55
privileged process	B2:39	silver ticket	B5:89-90
process dumps	B5:103	singles	B2:48
proof key code exchange	B5:155	situational awareness	B2:114

SEC560— Enterprise Penetration Testing

linux	B2:118-22	web proxy auto discovery	B3:108
skeleton key	B5:36	whois	B1:78
smart cards	B3:67	windows	
smb	B4:13, B2:46	exploit obfuscation	B2:134
named pipes	B2:80	file/print sharing	B4:42
smb relaying	B3:111	files	B2:132
smb signing	B3:113	firewall	B2:131
source anchor	B5:118	passwords	B3:58-66, 72-7
SPN	B5:12, 18	registry	B2:133
SPNs	B3:99	WinInet InternetQueryOption	B3:108
ssh		WinRM	B4:10-11
key theft	B4:6	wlan	B2:131
port forwarding	B4:87-8	WMI	
stagers	B2:48	event subscription	B3:44
stages	B2:48	world-writeable	B1:51
startup folder	B3:41	WPAD	B3:108
sudo	B1:52	X509	B5:117
suid	B3:11, B2:39, B1:51, 120	zero-knowledge	B1:26
SYSTEM registry	B5:33		
sysvol	B2:127		
tactics	B2:108		
tcp	B1:99-102		
pivots	B2:80		
RST	B1:122		
terraform automation	B5:155		
test types			
full-knowledge	B1:26		
unannounced	B1:25		
zero-knowledge	B1:26		
threat	B1:12		
TLS	B1:79		
torrents	B1:85		
tunnels	B5:176		
UAC	B4:44		
udp	B1:105		
unannounced test	B1:25		
unattend.xml	B3:15-6		
unquoted paths	B3:20		
UPN	B5:114		
user access admin	B5:166		
user account control	B3:21-2		
bypass	B3:23		
user principal name	B5:114		
user recon	B1:82-9		
usernames	B2:14		
vba	B2:98		
version scan	B1:94		
VLANs	B3:113		
Volume Shadow Copy Service	B5:33, B3:74		
VSS	B5:33, 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		

SEC560— Enterprise Penetration Testing

Tools/Commands

Get-Credential	B4:11	DNSDumpster	B1:75-7
Test-WSMan	B4:11	DNSRecon	B1:73-4
arp	B2:116	Dradis Reporting	B1:40
base64	B2:112	Empire	B3:23, B2:88-92
bitsadmin	B3:26	modules	B2:90-2
cscript	B3:74	Ews-Crack	B5:128
dir	B2:124	ExploitDB	B1:37
findstr	B2:132	EyeWitness	B1:140-3
find	B3:12, B2:132	GatherContacts	B1:86
ip	B2:116	GetFFGP	
lsof connections	B1:53	FineGrainedPassPolicy	B2:18
more	B2:132	GetUserSPN	B5:20
msbuild.exe	B4:72-9	GhostPack	B2:137-9
net.exe	B4:13, B2:16	GTFOBins	B3:12
net/net1	B2:126-30	Hashcat	B5:22, B3:89-94
netsh	B2:131	HaveIBeenPwned	B1:85
netstat connections	B1:53, B2:116	Hunter.io	B1:83
ntdsutil.exe	B5:34, B3:76	Hydra	B2:20-2
ps	B3:9	Immunity CANVAS	B2:39
reg	B2:133	Impacket	B4:32-7
schtasks	B4:21, B3:42	golden ticket	B5:97
sc	B4:14, 23	silver ticket	B5:89-90
services.msc	B4:16	smbexec/wmiexec	B4:37
setspn.exe	B5:12, 19	Invoke-Kerberoast	B5:20
set	B2:124	Iptables	B4:5
ss	B2:116	JohnTheRipper	B3:83-6
type	B2:132	potfile	B3:83
uname	B3:8	unshadow	B3:71
uniq	B3:50	jwt.ms	B5:138-40
winrs	B4:10	L0phtCrack	B3:59
wmic	B4:25-6	LinPEAS	B2:39
AAD-Internals	B5:120-1	LinuxExploitSuggester	B2:39
AD Explorer	B2:135	LockoutStatus.exe	B2:15
ADCSPwn	B5:83	LOLBAS	B3:26
ALockout.dll	B2:15	MailSniper	B5:128
AWS API Gateway	B5:138-40	Masscan	B1:96, 123-5
Azure CLI	B5:162-4	Metasploit	B2:19, B3:23, 42-60
Run-Command	B5:164	owa_login	B5:128
BeRoot	B3:24	pivoting	B4:84
BloodHound	B3:30-5	psexec	B4:46
Burp		Meterpreter	B2:53-60
IP Rotate	B5:140	creds_all	B3:77
C2 Matrix	B2:73	hashdump	B3:73
Cain	B3:102	load kiwi	B3:77
Certify		pivoting	B4:85-6
ESC1	B5:57-61	Mimikatz	B5:27-8, B3:77
ESC4	B5:73-4	DCShadow	B5:41
Certipy		DCSync	B5:39
ESC1	B5:65-9	golden ticket	B5:97
ESC4	B5:75-81	skeleton key	B5:37
CeWL	B3:51	MITRE ATTACK	B1:38
Chameleon	B2:134	MITRE CVE	B1:37
Cobalt Strike	B2:39	Monster.com	B1:86
Core IMPACT	B2:36	MSBuild	B4:72-9
crt.sh	B1:79	MSOLSpray	B5:131
DefenderCheck	B4:65	NCrack	B2:19
DeHashed	B1:85	Netcat	B4:5, B1:133-8
		ngrok	B5:175-8

SEC560— Enterprise Penetration Testing

nmap	B4:10, B1:109-21, 129-33	ESC1	B5:62-4
limitations	B1:121, 151	ScanRand	B1:96
os fingerprinting	B1:129	schtasksabuse	B3:42
script.db	B1:156	Seatbelt	B2:137-9
scripting engine	B1:153-6	secretsdump.py	B5:33, B3:59
NPK	B3:53	SharpBlock	B4:63
NTDSUtil	B3:76	Shodan	B1:80-1
ntlmrelayx.py	B5:83	SkullSecurity Passwords	B3:50
Patator	B2:19	Sliver	B2:76-83
Pcredz	B3:102-4	commands	B2:81
phonebook.cz	B1:84	payloads	B2:79-80, 83
Pipal	B3:95	server-client	B2:82
Posh-SecMod	B2:90	Spray365	B5:132
PowerBreach	B2:90	load balance	140
PowerSploit	B2:90, 134	TrevorSpray	B5:132
Out-MiniDump	B5:103	load balance	139
Remove-Comment	B4:62	UACME	B3:23
PowerStripper	B4:62	VeilEvasion	B4:53, 69
PowerUp	B3:25, B2:90	Verizon DBIR	B2:69
PowerView	B2:90, 134	VirtualProtect	B4:63
domain privesc	B5:101-2	VirusTotal	B4:54
PsExec	B4:18-20	VSSAdmin	B4:34
pw-inspector	B2:13	VSSOwn	B3:74
Responder	B3:106-13	Watson	B3:24
RIRs	B1:78	WMIC	B4:16
Rubeus	B4:12, B5:27		