

# 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	refresh token .....	B5:152-4
ASNs .....	B1:75	request throttle .....	B5:125
asrep roast .....	B5:104	roles .....	B5:167
assumed breach .....	B2:68	scope .....	B5:116
attack phases		shell .....	B5:108
covering tracks .....	B1:17	smart lockout .....	B5:136
exploitation .....	B1:17	synchronization .....	B5:118
maintaining access .....	B1:17	user access admin .....	B5:166
post-exploitation .....	B1:17	user enumeration .....	B5:122-27
recon .....	B1:17	backup servers .....	B5:33
scanning .....	B1:17	BGP .....	B1:78
authenticated proxy .....	B2:89	browser .....	B2:46
authentication		browsers .....	B2:33
central .....	B5:144	c2 .....	B2:72
FIDO2 .....	B5:144	C:/Windows/Panther .....	B3:15-6
LDAPS .....	B5:144	central auth server .....	B5:144
MFA .....	B5:144	certificate	
autonomous systems numbers .....	B1:75	authority .....	B5:46
AWS		internal .....	B5:49
api gateway .....	B5:138	enrollment .....	B5:82
azure		pfx .....	B5:61
access control .....	B5:109, 116	service .....	B5:46
AD .....	B5:111, 117	signing request .....	B5:46
api manage .....	B5:157	template .....	B5:50
auth library .....	B5:162	access control .....	B5:70
authentication .....	B5:111-8	ESC1 .....	B5:50-70
automation .....	B5:163	ESC4 .....	B5:71-81
backup .....	B5:157	ESC8 .....	B5:82-3
blobs .....	B5:157	certificate transparency .....	B1:79
compute .....	B5:157	chaining .....	B2:80
devops .....	B5:157	challenge-response	
extensions .....	B5:163	Kerberos .....	B3:99
external recon .....	B5:121	LANMAN .....	B3:63
federation .....	B5:118	NTLMv1 .....	B3:63
global admin .....	B5:166	NTLMv2 .....	B3:65-6, 100-01
groups		CIDR .....	B1:78
management .....	B5:158	cloud shell .....	B5:108
resource .....	B5:158	cmd.exe autorun .....	B3:40
IAM .....	B5:109	common subdomains .....	B1:72
identities .....	B5:171	competitive intel .....	B1:68
identity token .....	B5:171	conditional access policies .....	B5:147
infrastructure .....	B5:157-9	cpassword .....	B3:15-6
		credential guard .....	B4:44

# SEC560— Enterprise Penetration Testing

---

credential reuse .....	B4:6	types .....	B2:30
credential stuffing .....	B2:9-10	windows .....	B2:45, 49-51
crypt3 .....	B3:58-66	extended key usage .....	B5:48
daisy-chaining .....	B2:80	Extranet Lockout .....	B5:137
data breaches .....	B1:85	file	
data dump forums .....	B1:85	install files .....	B3:15-6
DCShadow .....	B5:40	iso .....	B2:101
DCSync .....	B5:38	lnk-shortcuts .....	B2:103
dedicated systems .....	B1:36	permissions .....	B3:10
dhcpcd .....	B2:131	pilfering .....	B2:115-6, 132
directory replication service remote .....	B5:39	searching .....	B2:125, 132
dirty cow .....	B3:8	world-writeable .....	B3:10
document-reading apps .....	B2:33	zip .....	B2:102
documented permission .....	B1:20, 23	file-transfer .....	B2:109-12
domain		file/print sharing .....	B4:42
admin .....	B5:30, 35, B2:129	firewall .....	B2:31, B2:131
administration .....	B2:126	first-class citizen .....	B5:144
cleanup .....	B2:130	full-knowledge .....	B1:26
controllers plural .....	B5:36	GetCredentialType .....	B5:123-5
DCShadow .....	B5:40	global admin .....	B5:166
DCSync .....	B5:38	golden ticket .....	B5:94-7
groups .....	B2:129	Google search .....	B1:86
ntds file .....	B5:33	grant .....	B5:155
persistence .....	B5:32	group policy	
privesc .....	B5:101-4	objects .....	B3:17
replication .....	B5:38	preferences .....	B3:17-8
skeleton key .....	B5:36	guardrails .....	B2:35, 80
users .....	B2:127	hash	
DRSR .....	B5:39	formats .....	B3:68
dynamic code generation .....	B2:77	LANMAN .....	B3:60, 63
dynamic data exchange .....	B2:100	MD5 .....	B3:69
env variable .....	B2:124	NT .....	B3:61
ephemeral shell .....	B1:47	rounds .....	B3:69
ESC		HKCU .....	B3:40
1 .....	B5:50-69	html application .....	B1:68
4 .....	B5:71-81	hybrid auth .....	B5:111
8 .....	B5:82-3	identity token .....	B5:171
etypes .....	B5:22	IdsLocked .....	B5:136
evasion .....	B4:52-69	imds .....	B5:170
amsi .....	B4:56-60	impacket	
application control .....	B4:72-80	kerberos .....	B4:33
signature detection .....	B4:64	remote exec .....	B4:35-7
static analysis .....	B4:61	secretsdump .....	B4:34
tactics .....	B4:52-69	syntax .....	B4:35
windows defender .....	B4:65	implant chaining .....	B2:80
event logs		infrastructure recon .....	B1:71-81
DCShadow .....	B5:40	ingestors .....	B3:30
ID-5137-5141 .....	B5:40	inheritance .....	B5:169
execution plan .....	B5:134	initial access .....	B2:6
exploit .....	B1:11	install from media .....	B5:34
unquoted paths .....	B3:20	instance metadata service .....	B5:170
exploitation .....	B2:26-8	intrusion prevention .....	B2:31
client-side .....	B2:32-7	ipsec .....	B2:131
framework .....	B2:41	jitter .....	B2:72
local privesc .....	B2:38	job reqs .....	B1:85
payload delivery .....	B2:36	JSON web token .....	B5:115
server-side .....	B2:31	junior testers .....	B1:61
social engineering .....	B2:34	JWT .....	B5:115

# SEC560— Enterprise Penetration Testing

---

kerberoasting .....	B5:21	reliability .....	B2:47
computer accounts .....	B5:22	stagers .....	B2:48-50
etypes .....	B5:22	stages .....	B2:51
service accounts .....	B5:22	user interfaces .....	B2:43
targets .....	B5:22	meterpreter .....	B2:53-60
kerberos .....	B3:99	modules .....	B2:60
asrep roast .....	B5:104	microsoft	
asreq/asrep .....	B5:8	ADDS .....	B5:117
auth .....	B5:6	authentication .....	B5:116
golden ticket .....	94-7	MSAL .....	B5:162
impacket .....	B4:33	msbuild .....	B4:74-80
kdc .....	B5:5-7	MSOL .....	B5:146
kerberoasting .....	B5:11	NBT-NS .....	B3:106
krbtgt account .....	B5:30, 87-8, 94	network sweep .....	B1:94
long-term keys .....	B5:8, 88	ntds file .....	B5:33
overpass-the-hash .....	B5:29	ntds.dit .....	B3:59, 75
pass-the-ticket .....	B5:27-8	ntlm	
priv attribute cert .....	B5:10	relay .....	B5:82
service ticket .....	B5:11, 13-6	NTLMv1 .....	B3:64
silver ticket .....	B5:89	NTLMv2 .....	B3:65-6, 100
spn .....	B5:12, 18	attacks .....	B3:110
stateless .....	B5:95	defense .....	B3:113
tsreq/tgsrep .....	B5:11	NtProtectVirtualMemory .....	B4:63
ticket reuse .....	B4:12	OAuth Token .....	B5:131
ticket-granting ticket .....	B5:10	Oauth2	
kernel .....	B3:8	access token .....	B5:149, 152
kernel attacks .....	B2:39	claims .....	B5:150
keyrings .....	B2:122	code flow .....	B5:144-54
LDAP .....	B5:116	flow types .....	B5:155
legacy authen .....	B5:128	JWT .....	B5:149
linux		refresh token .....	B5:152-4
connections .....	B1:51	OAuthToken .....	B5:126-7
filesystem .....	B1:46	obfuscation .....	B2:134
permissions .....	B1:50	office	
suid .....	B1:51	dde .....	B2:100
LLMNR .....	B3:106	macros .....	B2:98
load balancing .....	B5:138	OIDC .....	B5:107
local groups .....	B2:128	OpenID	
lockout .....	B2:15	access token .....	B5:149, 152
duration .....	B2:16	claims .....	B5:150
observation window .....	B2:16	Connect .....	B5:144, 166
threshold .....	B2:16	JWT .....	B5:149
login.microsoftonline .....	B5:146	refresh token .....	B5:152-4
logon script .....	B2:127	opsec .....	B2:89
LSASS .....	B4:41, 77, B5:103	organizational recon .....	B1:67-9
managed identity		os fingerprinting .....	B1:94
system assigned .....	B5:171	nmap .....	B1:129
user assigned .....	B5:171	PAC .....	B5:10, 13, 88
mangling .....	B3:51	parallel scans .....	B1:121
mDNS .....	B3:106	parent process spoofing .....	B2:80
memory dumps .....	B5:103	pass-the-hash .....	B4:41-9, B3:54
mergers & acquisitions .....	B1:67	mitigations .....	B4:44
metasploit		pass-through auth .....	B5:118
exploits .....	B2:44-7	password	
meterpreter .....	B2:53-60	guessing .....	B2:11-22
modules .....	B2:44	spraying .....	B2:18
payloads .....	B2:44-51	password attacks .....	B4:47
psexec .....	B4:46	password hash synchronization .....	B5:118

# SEC560— Enterprise Penetration Testing

---

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	
synced	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	
domain/AD	B5:32	
HKCU	B3:40	
scheduled task	B3:42	
services	B3:43	
startup folder	B3:41	
WMI events	B3:43	
pxf	B5:61	
pgp	B2:122	
phishing		
device code flow	B5:162	
pivoting		
linux	B4:6, 84-91	
ssh	B4:87-8	
windows	B4:9-28	
PKCE	B5:155	
PKI	B5:46	
plugins	B1:149	
polling interval	B2:72	
port forwarding	B4:5	
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	
primary refresh token	B5:152-4	
priv attribute cert	B5:10	
privacy regulations	B1:27	
privesc		
domain	B5:101-4	
linux		
files	B3:10	
kernel	B3:8	
service	B3:9	
suid	B3:11	
local	B2:38	
motivations	B3:5	
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	
process dumps	B5:103	
proof key code exchange	B5:155	
proxies	B3:113	
http	B5:140	
ssh	B5:139	
psexec	B2:45	
purple team	B1:13	
race conditions	B2:39	
rc4	B5:22, 36	
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	
refresh token	B5:152-4	
regional internet registries	B1:78	
registry	B2:133	
registry keys	B3:40	
reporting	B4:94-119	
format	B4:96	
representative sample	B2:37	
rid 512	B5:30	
RIRs	B1:78	
risk	B1:12	
rules of engagement	B1:24	
runtime env	B2:33	
SAM database	B4:41, B3:58, 75	
sam database	B2:122	
scada	B2:46	
ScanContent	B4:57	
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	
SCCM	B5:163	
scf file	B3:109	
scheduled tasks	B3:42	
scope	B1:23	

# SEC560— Enterprise Penetration Testing

---

security audit .....	B1:14	vba .....	B2:98
security identifiers .....	B4:44	version scan .....	B1:94
sensitive data .....	B1:27	VLANs .....	B3:113
services .....	B3:43	Volume Shadow Copy Service ....	B5:33, B3:74
controller .....	B4:14	VSS .....	B5:33, B3:74
name .....	B4:16	vuln scanning .....	B1:145-51
shared object .....	B3:9	agent-based .....	B1:148
shells .....		authenticated .....	B1:148
ephemeral .....	B1:47	plugins .....	B1:149
prompts .....	B1:55	unauthenticated .....	B1:148
silver ticket .....	B5:89-90	vulnerability .....	B1:11
singles .....	B2:48	vulnerability assessment .....	B1:14
situational awareness .....	B2:114	vulnerability scan .....	B1:94
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		

# 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  
unshadow ..... B3:71  
winrs ..... B4:10  
wmic ..... B4:25-6  
AAD-Internals ..... B5:120-1  
AD Explorer ..... B2:135  
ADCSPwn ..... B5:83  
ALockout.dll ..... B2:15  
AWS API Gateway ..... B5:138-40  
Azure CLI ..... B5:162-4  
    Run-Command ..... B5:164  
BeRoot ..... B3:24  
BloodHound ..... B3:30-5  
Burp  
    IP Rotate ..... B5:140  
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  
    conf file ..... B3:82  
    potfile ..... B3:83  
    unshadow ..... B3:71  
jwt.ms ..... B5:138-40  
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  
    owalgin ..... B5:128  
    pivoting ..... B4:84  
    psexec ..... B4:46  
Meterpreter ..... B2:53-60  
    credsall ..... 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  
MSOLSpray ..... B5:131  
NCCrack ..... B2:19

# SEC560— Enterprise Penetration Testing

---

Netcat .....	B4:5, B1:133-8	Rubeus .....	B4:12, B5:27, 61
ngrok .....	B5:175-8	ESC1 .....	B5:62-4
nmap .....	B4:10, B1:109-21, 129-33	ScanRand .....	B1:96
limitations .....	B1:121, 151	schtasksabuse .....	B3:42
os fingerprinting .....	B1:129	Seatbelt .....	B2:137-9
script.db .....	B1:156	secretsdump.py .....	B5:33, B3:59
scripting engine .....	B1:153-6	SharpBlock .....	B4:63
NPK .....	B3:53	Shodan .....	B1:80-1
NTDSUtil .....	B3:76	SkullSecurity Passwords .....	B3:50
ntlmrelayx.py .....	B5:83	Sliver .....	B2:76-83
Patator .....	B2:19	commands .....	B2:81
Pcredz .....	B3:102-4	payloads .....	B2:79-80, 83
phonebook.cz .....	B1:84	server-client .....	B2:82
Pipal .....	B3:95	Spray365 .....	B5:132
Posh-SecMod .....	B2:90	load balance .....	140
PowerBreach .....	B2:90	TrevorSpray .....	B5:132
PowerSploit .....	B2:90, 134	load balance .....	139
Out-MiniDump .....	B5:103	UACME .....	B3:23
Remove-Comment .....	B4:62	VeilEvasion .....	B4:53, 69
PowerStripper .....	B4:62	Verizon DBIR .....	B2:69
PowerUp .....	B3:25, B2:90	VirtualProtect .....	B4:63
PowerView .....	B2:90, 134	VirusTotal .....	B4:54
domain privesc .....	B5:101-2	VSSAdmin .....	B4:34
PsExec .....	B4:18-20	VSSOwn .....	B3:74
pw-inspector .....	B2:13	Watson .....	B3:24
Responder .....	B3:106-13	WMIC .....	B4:16
RIRs .....	B1:78		