

# SEC504 – Hacker Tools, Techniques, and Incident Handling

---

## Index

AADInternals .....	B2 – 27
AADSTS .....	B3 – 16
access logs .....	B1 – 72, B3 – 79
ACLs .....	B3 – 69
AppArmor .....	B4 – 11
application allow lists .....	B5 – 8
AppLocker	
blocking mode .....	B5 – 8
learning mode .....	B5 – 8
logs .....	B5 – 8
Argon2 .....	B3 – 45
ASEPs .....	WB – 20, B5 – 39
authentication	
Microsoft 365 .....	B3 – 15-6
Microsoft conditional access .....	B3 – 23
multifactor	
bypass .....	B3 – 23
deployment .....	B3 – 64
AWS .....	B4 – 92
CLI .....	B4 – 92
enumeration .....	B5 – 68
IAM policies .....	B5 – 69-70
pacu exploitation framework .....	B5 – 70
security token service .....	B5 – 68
AWS API gateway .....	B3 – 20
Azure	
smart logout .....	B3 – 19
backdoors .....	B3 – 90-1
behavioral analysis .....	B1 – 88, 92, 93
Berkeley Packet Filters .....	B1 – 70
broadcast protocols .....	B5 – 35
browsers .....	B4 – 20
hooks .....	B4 – 29
bypass	
DefenderCheck .....	B5 – 6
endpoint security .....	B5 – 5
C2 behavior .....	B5 – 56
certificate authorities .....	B2 – 15
certificates	
authority .....	B2 – 15
CN field .....	B2 – 20
transparency .....	B2 – 15-6
untrusted .....	B2 – 15
CIM .....	B1 – 42
client-side attacks .....	B4 – 18
cloud storage	
AWS S3 .....	B3 – 71
Azure blobs .....	B3 – 73
endpoint URLs .....	B3 – 70
GCP buckets .....	B3 – 72
ACLs .....	B3 – 69
permissions .....	B3 – 74
CN field .....	B2 – 20
command injection .....	B4 – 39
blind .....	B4 – 39
separators .....	B4 – 46
stacking .....	B4 – 43
common name .....	B2 – 20
compliance search .....	B5 – 73
COMSPEC .....	B1 – 55
conditional access .....	B3 – 23
containment .....	B1 – 29
continuous recording .....	B1 – 93
crawl .....	B2 – 25
credential stuffing .....	B3 – 8-9
crypt .....	B3 – 42
CSP .....	B4 – 60
detection .....	B1 – 26
behavioral anomaly analysis .....	B5 – 7
signature based .....	B5 – 7
differential analysis .....	B3 – 25, WB – 25-31, B1 – 57
discovery .....	B2 – 10
DLL injection .....	B4 – 8
DNS	
automated interrogation .....	B2 – 14
logs .....	B2 – 18, B3 – 79
multicast .....	B5 – 31
split .....	B2 – 18
zone transfer .....	B2 – 13
domain controller	
backup .....	B3 – 36
hashes .....	B3 – 36
drive-by .....	B4 – 19
empty hashes	
format .....	B3 – 40
encoding .....	B1 – 45
endpoint security	
bypass .....	B5 – 5
enumeration .....	B2 – 11
certificates .....	B2 – 15
cloud provider IP .....	B2 – 54
DNS .....	B2 – 12
SMB shares .....	B2 – 69-72
subdomains .....	B2 – 17
eradication .....	B1 – 30
EternalBlue .....	B2 – 76
evasion .....	B5 – 5
behavioral anomaly analysis .....	B5 – 7
signature-detection .....	B5 – 6-7
event logs .....	B5 – 49, B1 – 55
event of interest .....	B1 – 83
event subscription .....	B5 – 43
exfiltration .....	B5 – 72-3
exploit protection .....	B4 – 11
FIDO2 .....	B3 – 64
FIFO files .....	B3 – 93-4
flags	
HTTPOnly .....	B4 – 60
Secure .....	B4 – 60
gold image .....	B1 – 57
golden ticket attack .....	B5 – 45
GPO .....	B3 – 62
GPU .....	B3 – 44
group policy .....	B3 – 62

# SEC504 – Hacker Tools, Techniques, and Incident Handling

---

hashcat	
attack modes	
combinator	B3 – 54
hybrid	B3 – 57-8
mask	B3 – 55-6
straight	B3 – 53
potfile	B3 – 59
rules	B3 – 60
hashes	B3 – 46
domain controller	B3 – 33
empty	B3 – 40
indicators	B3 – 42
LANMAN	B3 – 32
Linux format	B3 – 42
MD4,5	B3 – 42-44
NT	B3 – 33
PBKDF2	B3 – 44
SHA256,512	B3 – 42-44
Windows format	B3 – 40
hashing rounds	B3 – 43-4
algorithms	B3 – 42, 45
Hayabusa	B2 – 86
high-low strategy	B5 – 6
hijacking attacks	B5 – 31
HKCU	WB – 20
HKLM	WB – 20
hooks	B4 – 29
host attribution	B2 – 54
http192-254-169-254	B4 – 91
IANA	B2 – 40
IMDS	B4 – 91
credential disclosure	B4 – 94
headers	B4 – 94
v2	B4 – 97
input filtering	B4 – 59, 78
json	
cloud	B2 – 50
kerberos	B3 – 62
golden ticket attack	B5 – 45
krbtgt	B5 – 45
root of trust	B5 – 45
LANMAN hashes	B3 – 32
living off the land	
linux	B5 – 14
windows	B5 – 11-3
LLMNR	B5 – 31
login	
bypass	B3 – 23, 90
logs	
access	B1 – 72, B3 – 79
AppLocker	B5 – 8
cloud	B5 – 79
DNS	B2 – 18, B3 – 79
event	B5 – 49, B1 – 55
overflow	B5 – 79
zeek	B5 – 56
LSASS	B1 – 42-3
macros	B4 – 22
malware	
obfuscation	B5 – 7
malware analysis	
behavioral	B1 – 88, 92-3
online	B1 – 89
static	B1 – 88, 98
man-in-the-middle	B5 – 31
managed object format	B5 – 43
Masscan	B2 – 54
mDNS	B5 – 31
metasploit	
auxiliary	B4 – 5
exploits	B4 – 6
meterpreter	B4 – 8-10
payloads	B4 – 8
post-exploitation	B4 – 5
Microsoft 365	
authentication	B3 – 15-6
compliance search	B5 – 73
lockout bypass	B3 – 20-24
smart lockout	B3 – 19
unified audit logging	B3 – 25
Microsoft conditional access	B3 – 23
mitm	B5 – 31
MITRE ATT&CK	B2 – 6-8
mof	B5 – 43
multifactor	B3 – 64
bypass	B3 – 23
named pipes	B3 – 93-4
netcat	
backdoors	B3 – 90-1
client	B3 – 86
data transfer	B3 – 88
listen	B3 – 87
port scanner	B3 – 89
relays	B3 – 93-4
NMAP	B2 – 14, 35-47
default behavior	B2 – 37
port scan	B2 – 39
scripts	B2 – 44-5
NoLMHash	B3 – 61
NSE scripts	B2 – 44-5
NT hashes	B3 – 33
NTDS.dit	B3 – 36
obfuscation	B5 – 7
Object Relational Mapping	B4 – 75
ORM	B4 – 75
OSINT	B2 – 23
framework	B2 – 31
output encoding	B4 – 59
pacu exploitation framework	B5 – 70
PAM	B3 – 62
password	
cracking	B3 – 49
guessing	B3 – 4
hashes	B3 – 46
length	B3 – 62
mutation	B3 – 49

# SEC504 – Hacker Tools, Techniques, and Incident Handling

---

reset .....	B2 – 79	SQL .....	B4 – 66
salts .....	B3 – 33-5	error-based .....	B4 – 69-70
spraying .....	B3 – 5	ORM .....	B4 – 75
wordlist generation .....	B3 – 7	SQLMap .....	B4 – 71-5
PBKDF2 .....	B3 – 45	statements formatting .....	B4 – 66
persistence .....	B5 – 39	unions .....	B4 – 69-70
pivoting		ssh	
meterpreter .....	B5 – 21-3	tunneling .....	B5 – 24
port forwarding		SSRF	
meterpreter .....	B5 – 21-3	cloud .....	B4 – 90
netsh .....	B5 – 25	exploits .....	B4 – 84-9
ssh .....	B5 – 24	IMDS .....	B4 – 90
ports		static analysis .....	B1 – 88
common .....	B2 – 40	SYSTEM hive .....	B3 – 36
SMB .....	B2 – 81	tautology .....	B4 – 67
post-incident .....	B1 – 33	threat hunting .....	B4 – 13
prefetch .....	B1 – 95	RITA .....	B4 – 13
preparation .....	B1 – 25	ticket granting ticket .....	B5 – 45
proc virtual file system .....	B4 – 96	typo-squatting .....	B4 – 18
proxies		unified audit logging .....	B3 – 25
API gateways .....	B3 – 20	VLAN .....	B2 – 81, B3 – 95
meterpreter .....	B5 – 21	WAF .....	B4 – 45
netsh .....	B5 – 25	watering-hole .....	B4 – 21
relay .....	B3 – 93	web	
web .....	B1 – 71	application firewall .....	B4 – 45, B2 – 61
RADIUS .....	B3 – 62	browsers .....	B4 – 20
recovery .....	B1 – 31	crawl .....	B2 – 25
reflection .....	B5 – 12-3	proxies .....	B1 – 71
registry keys .....	WB – 20	shells .....	B5 – 47
SYSTEM hive .....	B3 – 36	Windows	
relays .....	B3 – 93-4	Defender .....	B4 – 11
remediation .....	B1 – 32	Event Log .....	B1 – 55
RITA .....	B5 – 56	Exploit Protection .....	B4 – 11
root of trust .....	B5 – 45	Windows services .....	B5 – 42
salts .....	B3 – 33-5	WMI .....	B1 – 42
SAM .....	B3 – 33	event subscription .....	B5 – 43
scheduled tasks .....	B5 – 43	wordlist generation	
scoping .....	B1 – 28	bucket names .....	B3 – 78
security token service .....	B5 – 68	passwords .....	B3 – 7
SELinux .....	B4 – 11	wrapping .....	B5 – 7
services .....	B5 – 42	XSS	
setuid .....	B5 – 14	CSP .....	B4 – 60
shells		definition .....	B4 – 50
bind .....	B4 – 8	HTTPOnly .....	B4 – 60
reverse .....	B4 – 8	input filtering .....	B4 – 59
Sigma rules .....	B2 – 86	output encoding .....	B4 – 59
signature detection .....	B5 – 6	polyglot .....	B4 – 58
situation report .....	B5 – 68	reflected .....	B4 – 53-5
SMB		Secure .....	B4 – 60
password attacks .....	B2 – 77	stored .....	B4 – 52
shares .....	B2 – 69-73	YARA .....	B2 – 86
versions .....	B2 – 68	Yescrypt .....	B3 – 45
SMBGhost .....	B2 – 76	zeek .....	B5 – 56
SMBleed .....	B2 – 76	zone transfer .....	B2 – 13
snapshot .....	B1 – 93		
SNI .....	B3 – 79		
Snort .....	B2 – 86		
split DNS .....	B2 – 18		

# SEC504 – Hacker Tools, Techniques, and Incident Handling

---

## Commands

### Linux

dig .....	B2 – 12-4
exiftool .....	B2 – 26
gsutil .....	B3 – 75
hashdump .....	B3 – 38
mkfifo .....	B3 – 94
msfconsole .....	B4 – 28
msfvenom .....	B4 – 27
nc .....	B3 – 88
nmap .....	B2 – 38-46
nohup .....	B3 – 91
openssl .....	B2 – 56
rpcclient .....	B2 – 75
secretsdump.py .....	B3 – 37
sha256sum .....	B1 – 91
shred .....	B3 – 59
smbclient .....	B2 – 74
strings .....	B1 – 91
tcpdump .....	B1 – 68-9

### Windows

Close-SmbSession .....	B2 – 79
Disable-WindowsOptionalFeature .....	B2 – 68
Export-ScheduledTask .....	B1 – 54
Format-List .....	B1 – 50
Get-ChildItem .....	B1 – 51
Get-CimInstance .....	B1 – 40, B2 – 69
Get-FileHash .....	B1 – 91
Get-ItemProperty .....	B1 – 51
Get-LocalGroupMember .....	B1 – 53
Get-LocalGroup .....	B1 – 53
Get-LocalUser .....	B1 – 53
Get-MsolUser .....	B2 – 80
Get-NetTCPConnection .....	B1 – 46
Get-Process .....	WB – 14-6, B1 – 40
Get-ScheduledTaskInfo .....	B1 – 54
Get-ScheduledTask .....	B1 – 54
Get-Service .....	B1 – 50
Get-SmbSession .....	B2 – 79
Get-WinEvent .....	B1 – 55
Import-Module .....	B2 – 27
InstallUtil .....	B5 – 12-3
Invoke-AADIntReconAsOutsider ...	B2 – 27
Invoke-AADIntUserEnumerationAsOutsider .....	B2 – 27
Invoke-LocalPasswordSpray .....	B2 – 77
New-SmbMapping .....	B2 – 77
Remove-ItemProperty .....	WB – 23, 24
Select-Object .....	WB – 15-7, B1 – 40
Stop-Process .....	B1 – 40
Where-Object .....	WB – 15-7, B1 – 53
mofcomp .....	B5 – 43
net.exe .....	B5 – 41, B2 – 69, 80
netsh .....	B5 – 25
nslookup .....	B2 – 12
ntdsutil.exe .....	B3 – 36-9

## Tools

AADInternals .....	B2 – 27
--------------------	---------

AppArmor .....	B4 – 11
AppLocker .....	B5 – 8
AWS CloudMapper .....	B5 – 76
AWS Cloudwatch .....	B4 – 97
AWS-CLI .....	B5 – 48, 68, B4 – 92
AzViz .....	B5 – 76
Basic Blob Finder .....	B3 – 73
BeEF .....	B4 – 29
Blue Coat .....	B1 – 71
Bucket Finder .....	B3 – 71
BuiltWith .....	B2 – 51
Burp Suite .....	B2 – 24
cert.sh .....	B2 – 16
CeWL .....	B2 – 25
Copernic Desktop Search .....	B2 – 71
CyberChef .....	B1 – 45
DefenderCheck .....	B5 – 6
Dehashed .....	B2 – 29
DomainPasswordSpray .....	B2 – 78
Elastic Filebeat .....	B3 – 80
exiftool .....	B2 – 26
EyeWitness .....	B2 – 59, 60
FireProx .....	B3 – 22
Forefront TMG .....	B1 – 71
gcloud cli .....	B5 – 72
GCPBucketBrute .....	B3 – 72
Ghidra .....	B1 – 98
Google Network Topology Tool ....	B5 – 76
gsutil .....	B3 – 72, B5 – 72, 75
Hashcat .....	B3 – 49-60
haveibeenpwned .....	B2 – 28
Hayabusa .....	B2 – 86
HTML Purifier .....	B4 – 59
Hybrid Analysis .....	B1 – 89
Hydra .....	B3 – 6
IDA Pro .....	B1 – 98
Impacket .....	
secretsdump.py .....	B3 – 37
IronPython .....	B5 – 6
Java Encoder Project .....	B4 – 59
Joi .....	B4 – 59
jslinksummary .....	B2 – 24
JSON Query .....	B3 – 16, B2 – 50
LocalPasswordSpray.ps1 .....	B2 – 77
LOLBAS .....	B5 – 11
Masscan .....	B2 – 54
Metasploit and Armitage .....	B4 – 6
Meterpreter .....	
Hashdump .....	B3 – 38
persistence .....	B5 – 41-4
pivoting .....	B5 – 21-3
MFASweep .....	B3 – 23
Mimikatz .....	B5 – 9-10, B3 – 38
ModSecurity .....	B4 – 79
msfvenom .....	B4 – 27-31
MSOLSpray .....	B3 – 18
Netcat .....	B3 – 85-98
NetSShareEnum .....	B2 – 70

# SEC504 – Hacker Tools, Techniques, and Incident Handling

---

NMAP .....	B2 – 14, 35-47
openssl .....	B2 – 56
OSINT Framework .....	B2 – 31
Pacu .....	B5 – 69
Powershell .....	B1 – 39
cheatsheet .....	B1 – 59, 60
Regshot .....	B1 – 94-5
Responder .....	B5 – 33-4
RITA .....	B4 – 13, B5 – 56-63
Samba <code>smb/rpcclient</code> .....	B2 – 74-5
ScoutSuite .....	B5 – 77
SELinux .....	B4 – 11
Shodan .....	B2 – 30
SMBegle .....	B2 – 71
Snort .....	B2 – 86
SQLMap .....	B4 – 71-4
Squid .....	B1 – 71
Subfinder .....	B2 – 17
Sysinternals .....	B1 – 61
Autoruns .....	B5 – 49, B1 – 61
Procdump .....	B5 – 9, B1 – 61
Process Explorer .....	B1 – 61
Process Monitor .....	B1 – 61, 96-7
Sysmon .....	B1 – 61
TCPView .....	B1 – 61
Timeline Explorer .....	B2 – 98
TLS-Scan .....	B2 – 57-8
VirusTotal .....	B1 – 89
Volatility .....	B1 – 77-82
Windows Defender .....	B4 – 11
WinPmem .....	B1 – 77-82
YARA .....	B2 – 86

# SEC504 – Hacker Tools, Techniques, and Incident Handling

---

## DFIR

AI for IR	
summary of .....	B1 – 103, 120
Incident Response	
DAIR Dynamic Approach ....	B1 – 25-34
PICERL Six-Step Process ....	B1 – 21-2
summary of .....	B1 – 35-6
Live Examination	
of accounts .....	B1 – 53
of encoded data .....	B1 – 45
of logs .....	B1 – 55
of network activity .....	B1 – 46-9
of processes .....	B1 – 40-5
of registry keys .....	B1 – 51-2
of scheduled tasks .....	B1 – 54
of services .....	B1 – 50
summary of .....	B1 – 62
Malware Investigations	
monitoring the environment ....	B1 – 92
summary of .....	B1 – 99
Memory Investigations	
summary of .....	B1 – 99
Network Investigations	
summary of .....	B1 – 73
Sigma Rules .....	B2 – 88-98
Threat Hunting	
C2 characteristics .....	B5 – 57-61
summary .....	B5 – 62-4

## Defense Evasion

allow lists .....	B5 – 8-14
defenses .....	B5 – 15
evading signature-detection .....	B5 – 6
living off the land .....	B5 – 8-14
obfuscation and wrapping .....	B5 – 7
password attacks .....	B3 – 20-24
summary .....	B5 – 15

## Initial Access

Cloud	
challenges and opportunities ....	B2 – 49
cloud IP enumeration .....	B2 – 52-55
defenses .....	B2 – 52-55
host attribution .....	B2 – 52-55
IAM .....	B5 – 48
IMDS .....	B4 – 90
IMDSv2 .....	B4 – 97
persistence .....	B5 – 48
SSRF .....	B4 – 90-9
storage bucket exploit .....	B3 – 75-7
storage buckets .....	B3 – 68-82
summary of .....	B2 – 63-4
Command Injection	
defense .....	B4 – 45
summary .....	B4 – 46-7
Discovery and Enumeration	
certificates .....	B2 – 15-6
defense against .....	B2 – 18
DNS .....	B2 – 12-4
subdomains .....	B2 – 17

summary .....	B2 – 19
Drive-By Attacks	
defense .....	B4 – 32-3
summary .....	B4 – 34
Metasploit	
defenses .....	B4 – 11
payloads .....	B4 – 8
summary .....	B4 – 14-5
Netcat	
defenses .....	B3 – 95
purposes .....	B3 – 85-98
summary .....	B3 – 97
NMAP Scanning	
defaults .....	B2 – 37
summary of .....	B2 – 46
types .....	B2 – 41
Password Attacks	
APIs .....	B3 – 16
bypasses .....	B3 – 20-24
cloud .....	B3 – 15
cracking .....	B3 – 49-65
defenses .....	B3 – 61-4
domain controller .....	B3 – 36-8
hashes .....	B3 – 31-47
hashing algorithms .....	B3 – 44-5
hashing rounds .....	B3 – 42-3
local windows .....	B3 – 36-8
Microsoft 365 summary .....	B3 – 27
salting .....	B3 – 33-5
spraying,stuffing .....	B3 – 4-11
SMB	
challenges .....	B2 – 67
defenses .....	B5 – 35-6, B2 – 79-81
enumeration .....	B2 – 69-73
password attacks .....	B2 – 77
security features .....	B2 – 67
summary of .....	B2 – 83
SQL Injection	
cloud .....	B4 – 75
defense .....	B4 – 78
summary .....	B4 – 80-1
SSRF	
cloud .....	B4 – 90-9
defense .....	B4 – 97
summary .....	B4 – 98-9
Web Recon	
defenses .....	B2 – 32
summary of .....	B2 – 33
XSS	
defense .....	B4 – 59-60
impact .....	B4 – 56
summary .....	B4 – 61-2

## Post-Exploitation

Cloud	
exfiltration .....	B5 – 72-3
exfiltration defenses .....	B5 – 75-80
logging .....	B5 – 79
Pacu .....	B5 – 70

# SEC504 – Hacker Tools, Techniques, and Incident Handling

---

persistence defenses .....	B5 – 49
summary .....	B5 – 81
Persistence	
defenses .....	B5 – 49
summary .....	B5 – 51-3
with accounts .....	B5 – 41
with cloud resources .....	B5 – 48
with kerberos .....	B5 – 45-6
with scheduled tasks .....	B5 – 43
with services .....	B5 – 42
with web shells .....	B5 – 47
Pivoting	
lol .....	B5 – 24-6
metasploit .....	B5 – 20-3
summary .....	B5 – 27
Responder	
defenses .....	B5 – 35
hijacking attacks .....	B5 – 31-34
summary .....	B5 – 36

# SEC504 – Hacker Tools, Techniques, and Incident Handling

---

## Labs

### Live Investigation

- 1.1 Windows Host .....L1 – 13
- 1.2 Networks .....L1 – 45
- 1.3 Memory .....L1 – 45
- 1.4 Malware .....L1 – 45

### Recon, Scanning, Enumeration

- 2.1 DNS .....L1 – 116
- 2.2 NMAP .....L1 – 139
- 2.3 Cloud .....L1 – 162
- 2.4 SMB .....L1 – 180
- 3.4 Cloud Bucket Discovery ....L1 – 317

### Threat Analysis

- 2.5 Hayabusa .....L1 – 204

### Password Attacks

- 3.1 Metasploit .....L1 – 241
- 3.2 Microsoft 365 .....L1 – 261

- 3.3 Hashcat .....L1 – 290

### Remote Attacks

- 4.1 Metasploit .....L2 – 1
- 4.2 BeEF .....L2 – 31
- 4.3 Command Injection .....L2 – 44
- 4.4 XSS .....L2 – 57
- 4.5 SQL Injection .....L2 – 77
- 4.6 Cloud SSRF and IMDS .....L2 – 98

### Post-Exploitation

- 3.4 Netcat .....L1 – 350
- 5.1 Allow List Bypass .....L2 – 124
- 5.2 Pivoting .....L2 – 148
- 5.3 Responder .....L2 – 170
- 5.4 Metasploit .....L2 – 180
- 5.6 Cloud Configurations .....L2 – 227

### Threat Analysis

- 5.5 RITA .....L2 – 209