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
- Argon2 B3 – 45
- ASEPs WB – 20
- authentication
  - Microsoft 365 B3 – 15-6
  - Microsoft conditional access B3 – 23
  - multifactor
    - bypass B3 – 23
    - deployment B3 – 64
- AWS B4 – 92
  - CLI B4 – 92
- AWS API gateway B3 – 20
- Azure
  - smart lockout B3 – 19
- backdoors B3 – 90-1
- behavioral analysis B1 – 88, 92, 93
- Berkeley Packet Filters B1 – 70
- browsers B4 – 20
  - hooks B4 – 29
- 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
- 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
- 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
  - 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
- 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
- event of interest B1 – 83
- exploit protection B4 – 11
- FIDO2 B3 – 64
- FIFO files B3 – 93-4
- flags
  - HTTPOnly B4 – 60
  - Secure B4 – 60
- gold image B1 – 57
- GPO B3 – 62
- GPU B3 – 44
- group policy B3 – 62
- 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
- HKCU WB – 20
- HKLM WB – 20
- hooks B4 – 29
- host attribution B2 – 54
- http192-254-169-254 B4 – 91

SEC504 – Hacker Tools, Techniques, and Incident Handling

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
LANMAN hashes B3 – 32
login
  bypass B3 – 23, 90
logs
  access B1 – 72, B3 – 79
  DNS B2 – 18, B3 – 79
LSASS B1 – 42-3
macros B4 – 22
malware analysis
  behavioral B1 – 88, 92-3
  online B1 – 89
  static B1 – 88, 98
Masscan B2 – 54
metasploit
  auxiliary B4 – 5
  exploits B4 – 6
  meterpreter B4 – 8-10
  payloads B4 – 8
  post-exploitation B4 – 5
Microsoft 365
  authentication B3 – 15-6
  lockout bypass B3 – 20-24
  smart lockout B3 – 19
  unified audit logging B3 – 25
Microsoft conditional access B3 – 23
MITRE ATT&CK B2 – 6-8
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
Object Relational Mapping B4 – 75
ORM B4 – 75
OSINT B2 – 23
  framework B2 – 31
output encoding B4 – 59
PAM B3 – 62
password
  cracking B3 – 49
  guessing B3 – 4
  hashes B3 – 46
  length B3 – 62
  mutation B3 – 49
  reset B2 – 79
  salts B3 – 33-5
  spraying B3 – 5
  wordlist generation B3 – 7
PBKDF2 B3 – 45
ports
  common B2 – 40
  SMB B2 – 81
post-incident B1 – 33
prefetch B1 – 95
preparation B1 – 25
proc virtual file system B4 – 96
proxies
  API gateways B3 – 20
  relay B3 – 93
  web B1 – 71
RADIUS B3 – 62
recovery B1 – 31
registry keys WB – 20
  SYSTEM hive B3 – 36
relays B3 – 93-4
remediation B1 – 32
salts B3 – 33-5
SAM B3 – 33
scoping B1 – 28
SELinux B4 – 11
shells
  bind B4 – 8
  reverse B4 – 8
Sigma rules B2 – 86
SMB
  password attacks B2 – 77
  shares B2 – 69-73
  versions B2 – 68
SMBGhost B2 – 76
SMBleed B2 – 76
snapshot B1 – 93
SNI B3 – 79
Snort B2 – 86
split DNS B2 – 18
SQL B4 – 66
  error-based B4 – 69-70
  ORM B4 – 75
  SQLMap B4 – 71-5
  statements formatting B4 – 66
  unions B4 – 69-70
SSRF
  cloud B4 – 90
  exploits B4 – 84-9
  IMDS B4 – 90
static analysis B1 – 88

SEC504 – Hacker Tools, Techniques, and Incident Handling

SYSTEM hive .... B3 – 36
tautology .... B4 – 67
threat hunting .... B4 – 13
    RITA .... B4 – 13
typo-squatting .... B4 – 18
unified audit logging .... B3 – 25
VLAN .... B2 – 81, B3 – 95
WAF .... B4 – 45
watering-hole .... B4 – 21
web
    application firewall .... B4 – 45, B2 – 61
    browsers .... B4 – 20
    crawl .... B2 – 25
    proxies .... B1 – 71
Windows
    Defender .... B4 – 11
    Event Log .... B1 – 55
    Exploit Protection .... B4 – 11
WMI .... B1 – 42
wordlist generation
    bucket names .... B3 – 78
    passwords .... B3 – 7
XSS
    CSP .... B4 – 60
    HTTPOnly .... B4 – 60
    input filtering .... B4 – 59
    output encoding .... B4 – 59
    polyglot .... B4 – 58
    reflected .... B4 – 53-5
    Secure .... B4 – 60
    stored .... B4 – 52
YARA .... B2 – 86
Yescrypt .... B3 – 45
zone transfer .... B2 – 13

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
- `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
- `net.exe` B2 – 69, B2 – 80
- `nslookup` B2 – 12
- `ntdsutil.exe` B3 – 36-9

Tools

- AADInternals B2 – 27
- AppArmor B4 – 11
- AWS Cloudwatch B4 – 97
- AWS-CLI B4 – 92
- 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
- Dehashed B2 – 29
- DomainPasswordSpray B2 – 78
- Elastic Filebeat B3 – 80
- exiftool B2 – 26
- EyeWitness B2 – 59, 60
- FireProx B3 – 22
- Forefront TMG B1 – 71
- GCPBucketBrute B3 – 72
- Ghidra B1 – 98
- gsutil B3 – 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
- Java Encoder Project B4 – 59
- Joi B4 – 59
- jslinksummary B2 – 24
- JSON Query B3 – 16, B2 – 50
- LocalPasswordSpray.ps1 B2 – 77
- Masscan B2 – 54
- Metasploit and Armitage B4 – 6
- Meterpreter
  - Hashdump B3 – 38
- MFASweep B3 – 23
- Mimikatz B3 – 38
- ModSecurity B4 – 79
- msfvenom B4 – 27-31
- MSOLSpray B3 – 18
- Netcat B3 – 85-98
- NetSShareEnum B2 – 70
- NMAP B2 – 14, 35-47
- openssl B2 – 56
- OSINT Framework B2 – 31
- Powershell B1 – 39
  - cheatsheet B1 – 59, 60
- Regshot B1 – 94-5
- RITA B4 – 13
- Samba `smb/rpcclient` B2 – 74-5
- SELinux B4 – 11
- Shodan B2 – 30
- SMBeagle B2 – 71
- Snort B2 – 86
- SQLMap B4 – 71-4

Squid .... B1 – 71
Subfinder .... B2 – 17
Sysinternals .... B1 – 61
  Autoruns .... B1 – 61
  Procdump .... 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

Offense

- Cloud
  - challenges and opportunities B2 – 49
  - cloud IP enumeration B2 – 52-55
  - defenses B2 – 52-55
  - host attribution B2 – 52-55
  - IMDS B4 – 90
  - IMDSv2 B4 – 97
  - 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 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