SEC560– Enterprise Penetration Testing

Terms

- /etc/shadow B3: 68
- admin hunting B1: 63
- amsi B4: 56-60
  - bypasses B4: 58-60
- AmsiScanBuffer B4: 57
- annual reports B1: 68
- application control B4: 71
- ASNs B1: 75
- assumed breach B2: 68
- attack phases
  - covering tracks B1: 17
  - exploitation B1: 17
  - maintaining access B1: 17
  - post-exploitation B1: 17
  - recon B1: 17
  - scanning B1: 17
- authenticated proxy B2: 89
- autonomous systems numbers B1: 75
- BGP B1: 78
- browser B2: 46
- browsers B2: 33
- c2 B2: 72
- C:/Windows/Panther B3: 15-6
- certificate transparency B1: 79
- chaining B2: 80
- challenge-response
  - Kerberos B3: 99
  - LANMAN B3: 63
  - NTLMv1 B3: 63
  - NTLMv2 B3: 65-6, 100-01
- CIDR B1: 78
- cmd.exe autorun B3: 40
- common subdomains B1: 72
- competitive intel B1: 68
- cpassword B3: 15-6
- credential guard B4: 44
- credential reuse B4: 6
- credential stuffing B2: 9-10
- crypt3 B3: 58-66
- daisy-chaining B2: 80
- data breaches B1: 85
- data dump forums B1: 85
- dedicated systems B1: 36
- dhcpclient B2: 131
- dirty cow B3: 8
- document-reading apps B2: 33
- documented permission B1: 20, 23
- domain
  - admin B2: 129
  - administration B2: 126
  - cleanup B2: 130
  - groups B2: 129
  - users B2: 127
- dynamic code generation B2: 77
- dynamic data exchange B2: 100
- env variable B2: 124
- ephemeral shell B1: 47
- evasion B4: 52-69
  - amsi B4: 56-60
  - application control B4: 72-80
  - signature detection B4: 64
  - static analysis B4: 61
  - tactics B4: 52-69
  - windows defender B4: 65
- exploit B1: 11
  - unquoted paths B3: 20
- exploitation B2: 26-8
  - client-side B2: 32-7
  - framework B2: 41
  - local privesc B2: 38
  - payload delivery B2: 36
  - server-side B2: 31
  - social engineering B2: 34
  - types B2: 30
  - windows B2: 45, 49-51
- file
  - install files B3: 15-6
  - iso B2: 101
  - lnk-shortcuts B2: 103
  - permissions B3: 10
  - pilfering B2: 115-6, 132
  - searching B2: 125, 132
  - world-writeable B3: 10
  - zip B2: 102
- file-transfer B2: 109-12
- file/print sharing B4: 42
- firewall B2: 31, B2: 131
- full-knowledge B1: 26
- group policy
  - objects B3: 17
  - preferences B3: 17-8
- guardrails B2: 35, 80
- hash
  - formats B3: 68
  - LANMAN B3: 60, 63
  - MD5 B3: 69
  - NT B3: 61
  - rounds B3: 69
- HKCU B3: 40
- html application B1: 68
- impacket
  - kerberos B4: 33
  - remote exec B4: 35-7
  - secretsdump B4: 34
  - syntax B4: 35
- implant chaining B2: 80
- infrastructure recon B1: 71-81
- ingestors B3: 30
- initial access B2: 6
- intrusion prevention B2: 31
- ipsec B2: 131
- jitter B2: 72
- job reqs B1: 85
- junior testers B1: 61
- kerberos B3: 99

- impacket B4: 33
- ticket reuse B4: 12

kernel B3: 8
kernel attacks B2: 39
keyrings B2: 122
linux
- connections B1: 51
- filesystem B1: 46
- permissions B1: 50
- suid B1: 51

LLMNR B3: 106
local groups B2: 128
lockout B2: 15
- duration B2: 16
- observation window B2: 16
- threshold B2: 16

logon script B2: 127
LSASS B4: 41, 77
mangling B3: 51
mDNS B3: 106
mergers & acquisitions B1: 67
metasploit
- exploits B2: 44-7
- meterpreter B2: 53-60
- modules B2: 44
- payloads B2: 44-51
- psexec B4: 46
- reliability B2: 47

meterpreter B2: 53-60
msbuild B4: 74-80
NBT-NS B3: 106
network sweep B1: 94
ntds.dit B3: 59, 75
NTLMv1 B3: 64
NTLMv2 B3: 65-6, 100
- attacks B3: 110
- defense B3: 113

NtProtectVirtualMemory B4: 63
obfuscation B2: 134
office
- dde B2: 100
- macros B2: 98

opsec B2: 89
organizational recon B1: 67-9
os fingerprinting B1: 94
- nmap B1: 129

parallel scans B1: 121
parent process spoofing B2: 80
pass-the-hash B4: 41-9, B3: 54
- mitigations B4: 44

password
- guessing B2: 11-22
- spraying B2: 18

password attacks B4: 47
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
- HKCU B3: 40
- scheduled task B3: 42
- services B3: 43
- startup folder B3: 41
- WMI events B3: 43

pgp B2: 122
pivoting
- linux B4: 6, 84-91
- ssh B4: 87-8
- windows B4: 9-28

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
privacy regulations B1: 27
privesc
- linux
  - files B3: 10
  - kernel B3: 8
  - service B3: 9
  - suid B3: 11
- local B2: 38
- 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
proxies B3: 113
psexec B2: 45
purple team B1: 13
race conditions B2: 39

SEC560– Enterprise Penetration Testing

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
regional internet registries B1: 78
registry B2: 133
registry keys B3: 40
reporting B4: 94-119
- format B4: 96

representative sample B2: 37
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

scf file B3: 109
scheduled tasks B3: 42
scope B1: 23
security audit B1: 14
security identifiers B4: 44
sensitive data B1: 27
services B3: 43
- controller B4: 14
- name B4: 16

shared object B3: 9
shells
- ephemeral B1: 47
- prompts B1: 55

singles B2: 48
situational awareness B2: 114
- linux B2: 118-22

smart cards B3: 67
smb B4: 13, B2: 46
- named pipes B2: 80

smb relaying B3: 111
smb signing B3: 113
SPNs B3: 99
ssh
- key theft B4: 6
- port forwarding B4: 87-8

stagers B2: 48
stages B2: 48
startup folder B3: 41
sudo B1: 52
suid B3: 11, B2: 39, B1: 51, 120
sysvol B2: 127
tactics B2: 108
tcp B1: 99-102
- pivots B2: 80
- RST B1: 122

test types
- full-knowledge B1: 26
- unannounced B1: 25
- zero-knowledge B1: 26

threat B1: 12
TLS B1: 79
torrents B1: 85
UAC B4: 44
udp B1: 105
unannounced test B1: 25
unattend.xml B3: 15-6
unquoted paths B3: 20
user account control B3: 21-2
- bypass B3: 23

user recon B1: 82-9
usernames B2: 14
vba B2: 98
version scan B1: 94
VLANs B3: 113
Volume Shadow Copy Service B3: 74
VSS 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
web proxy auto discovery B3: 108
whois B1: 78
windows
- exploit obfuscation B2: 134
- file/print sharing B4: 42
- files B2: 132
- firewall B2: 131
- passwords B3: 58-66, 72-7
- registry B2: 133

WinInet InternetQueryOption B3: 108
WinRM B4: 10-11
wlan B2: 131
WMI
- event subscription B3: 44

world-writeable B1: 51
WPAD B3: 108
zero-knowledge B1: 26

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` ... B3: 76
- `ps` ... B3: 9
- `reg` ... B2: 133
- `schtasks` ... B4: 21, B3: 42
- `sc` ... B4: 14, 23
- `services.msc` ... B4: 16
- `set` ... B2: 124
- `ss` ... B2: 116
- `type` ... B2: 132
- `uname` ... B3: 8
- `uniq` ... B3: 50
- `winrs` ... B4: 10
- `wmic` ... B4: 25-6
- AD Explorer ... B2: 135
- ALockout.dll ... B2: 15
- BeRoot ... B3: 24
- BloodHound ... B3: 30-5
- C2 Matrix ... B2: 73
- Cain ... B3: 102
- 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
- ExploitDB ... B1: 37
- EyeWitness ... B1: 140-3
- GatherContacts ... B1: 86
- GetFFGP FineGrainedPassPolicy ... B2: 18
- GhostPack ... B2: 137-9
- GTFOBins ... B3: 12
- Hashcat ... B3: 89-94
- HaveIBeenPwned ... B1: 85
- Hunter.io ... B1: 83
- Hydra ... B2: 20-2
- Immunity CANVAS ... B2: 39
- Impacket ... B4: 32-7
  - smbexec/wmiexec ... B4: 37
- 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
- Masscan ... B1: 96, 123-5
- Metasploit ... B2: 19, B3: 23, 42-60
  - pivoting ... B4: 84
  - psexec ... B4: 46
- Meterpreter ... B2: 53-60
  - creds$_{a}ll$ ... $B3 : 77$
  - hashdump ... B3: 73
  - load kiwi ... B3: 77
  - pivoting ... B4: 85-6
- Mimikatz ... B3: 77
- 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
- Patator ... B2: 19
- Pcredz ... B3: 102-4
- phonebook.cz ... B1: 84
- Pipal ... B3: 95
- Posh-SecMod ... B2: 90
- PowerBreach ... B2: 90
- PowerSploit ... B2: 90, 134
  - Remove-Comment ... B4: 62
- PowerStripper ... B4: 62
- PowerUp ... B3: 25, B2: 90
- PowerView ... B2: 90, 134
- PsExec ... B4: 18-20
- pw-inspector ... B2: 13
- Responder ... B3: 106-13
- RIRs ... B1: 78
- Rubeus ... B4: 12
- ScanRand ... B1: 96
- schtasksabuse ... B3: 42
- Seatbelt ... B2: 137-9
- secretsdump.py ... B3: 59

SharpBlock B4: 63
Shodan B1: 80-1
SkullSecurity Passwords B3: 50
Sliver B2: 76-83
  commands B2: 81
  payloads B2: 79-80, 83
  server-client B2: 82
UACME B3: 23
VeilEvasion B4: 53, 69
Verizon DBIR B2: 69
VirtualProtect B4: 63
VirusTotal B4: 54
VSSAdmin B4: 34
VSSOwn B3: 74
Watson B3: 24
WMIC B4: 16