SEC560– Enterprise Penetration Testing

Terms

admin hunting B1: 63
annual reports B1: 68
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
certificate transparency B1: 79
chaining B2: 80
CIDR B1: 78
common subdomains B1: 72
competitive intel B1: 68
credential stuffing B2: 9-10
daisy-chaining B2: 80
data breaches B1: 85
data dump forums B1: 85
dedicated systems B1: 36
document-reading apps B2: 33
documented permission B1: 20, 23
dynamic code generation B2: 77
dynamic data exchange B2: 100
ephemeral shell B1: 47
exploit B1: 11
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
  iso B2: 101
  lnk-shortcuts B2: 103
  zip B2: 102
file-transfer B2: 109-12
firewall B2: 31
full-knowledge B1: 26
guardrails B2: 35, 80
html application B1: 68
implant chaining B2: 80
infrastructure recon B1: 71-81
initial access B2: 6
intrusion prevention B2: 31
jitter B2: 72
job reqs B1: 85
junior testers B1: 61
kernel attacks B2: 39
keyrings B2: 122
linux
  connections B1: 51
  filesystem B1: 46
  permissions B1: 50
  suid B1: 51
lockout B2: 15
  duration B2: 16
  observation window B2: 16
  threshold B2: 16
mergers & acquisitions B1: 67
metasploit
  exploits B2: 44-7
  meterpreter B2: 53-60
  modules B2: 44
  payloads B2: 44-51
  reliability B2: 47
meterpreter B2: 53-60
network sweep B1: 94
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
password
  guessing B2: 11-22
  spraying B2: 18
payload delivery B2: 36
payloads B2: 97
PCI B1: 61
penetration test
  definition B1: 15
  types B1: 16
permissions B1: 50
pilfering B2: 115-6
plugins B1: 149
polling interval B2: 72
port scan B1: 94
post-exploitation B2: 108
pre-engagement
  goals B1: 22
  rules B1: 24
  scope B1: 23
press releases B1: 68
privacy regulations B1: 27
privileged process B2: 39
psexec B2: 45
purple team B1: 13
race conditions B2: 39
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
representative sample B2: 37
RIRs B1: 78
risk B1: 12
rules of engagement B1: 24
runtime env B2: 33
sam database B2: 122
scada B2: 46
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
scope B1: 23
security audit B1: 14
sensitive data B1: 27
shells
ephemeral B1: 47
prompts B1: 55
singles B2: 48
situational awareness B2: 114
linux B2: 118-22
smb B2: 46
named pipes B2: 80
stagers B2: 48
stages B2: 48
sudo B1: 52
suid B2: 39, B1: 51, 120
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
udp B1: 105
unannounced test B1: 25
user recon B1: 82-9
usernames B2: 14
vba B2: 98
version scan B1: 94
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
whois B1: 78
world-writeable B1: 51
zero-knowledge B1: 26

SEC560– Enterprise Penetration Testing

Commands

- `arp` ... B2: 116
- `base64` ... B2: 112
- `ip` ... B2: 116
- `lsof` connections ... B1: 53
- `net.exe` ... B2: 16
- `netstat` connections ... B1: 53, B2: 116
- `ss` ... B2: 116

Tools/Sites

- ALockout.dll ... B2: 15
- C2 Matrix ... B2: 73
- Cobalt Strike ... B2: 39
- Core IMPACT ... B2: 36
- crt.sh ... B1: 79
- DeHashed ... B1: 85
- DNSDumpster ... B1: 75-7
- DNSRecon ... B1: 73-4
- Dradis Reporting ... B1: 40
- Empire ... B2: 88-92
  - modules ... B2: 90-2
- ExploitDB ... B1: 37
- EyeWitness ... B1: 140-3
- GatherContacts ... B1: 86
- GetFFGP
  - FineGrainedPassPolicy ... B2: 18
- HaveIBeenPwned ... B1: 85
- Hunter.io ... B1: 83
- Hydra ... B2: 20-2
- Immunity CANVAS ... B2: 39
- LinPEAS ... B2: 39
- LinuxExploitSuggester ... B2: 39
- LockoutStatus.exe ... B2: 15
- Masscan ... B1: 96, 123-5
- Metasploit ... B2: 19, B2: 42-60
  - Meterpreter ... B2: 53-60
- MITRE ATTACK ... B1: 38
- MITRE CVE ... B1: 37
- Monster.com ... B1: 86
- NCrack ... B2: 19
- Netcat ... B1: 133-8
- nmap ... B1: 109-21, 129-33
  - limitations ... B1: 121, 151
  - os fingerprinting ... B1: 129
  - script.db ... B1: 156
  - scripting engine ... B1: 153-6
- Patator ... B2: 19
- phonebook.cz ... B1: 84
- Posh-SecMod ... B2: 90
- PowerBreach ... B2: 90
- PowerSploit ... B2: 90
- PowerUp ... B2: 90
- PowerView ... B2: 90
- pw-inspector ... B2: 13
- RIRs ... B1: 78
- ScanRand ... B1: 96
- Shodan ... B1: 80-1
- Sliver ... B2: 76-83
  - commands ... B2: 81
  - payloads ... B2: 79-80, 83
  - server-client ... B2: 82
- Verizon DBIR ... B2: 69