SEC560– Enterprise Penetration Testing

Terms

admin hunting ..... B1 – 63
annual reports ..... B1 – 68
ASNs ..... B1 – 75
attack phases
  covering tracks ..... B1 – 17
  exploitation ..... B1 – 17
  maintaining access ..... B1 – 17
  post-exploitation ..... B1 – 17
  recon ..... B1 – 17
  scanning ..... B1 – 17
autonomous systems numbers ..... B1 – 75
BGP ..... B1 – 78
certificate transparency ..... B1 – 79
CIDR ..... B1 – 78
common subdomains ..... B1 – 72
competitive intel ..... B1 – 68
data breaches ..... B1 – 85
data dump forums ..... B1 – 85
dedicated systems ..... B1 – 36
documented permission ..... B1 – 20, 23
ephemeral shell ..... B1 – 47
exploit ..... B1 – 11
full-knowledge ..... B1 – 26
html application ..... B1 – 68
infrastructure recon ..... B1 – 71-81
job reqs ..... B1 – 85
junior testers ..... B1 – 61
linux
  connections ..... B1 – 51
  filesystem ..... B1 – 46
  permissions ..... B1 – 50
  setuid ..... B1 – 51
mergers & acquisitions ..... B1 – 67
network sweep ..... B1 – 94
organizational recon ..... B1 – 67-9
os fingerprinting ..... B1 – 94
PCI ..... B1 – 61
penetration test
  definition ..... B1 – 15
  types ..... B1 – 16
permissions ..... B1 – 50
port scan ..... B1 – 94
pre-engagement
  goals ..... B1 – 22
  rules ..... B1 – 24
  scope ..... B1 – 23
press releases ..... B1 – 68
privacy regulations ..... B1 – 27
purple team ..... B1 – 13
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
RIRs ..... B1 – 78
risk ..... B1 – 12
rules of engagement ..... B1 – 24
scans
  asynchronous ..... B1 – 96
  efficiency ..... B1 – 96
  tcp ..... B1 – 103-4, 115-6
  types ..... B1 – 94
  udp ..... B1 – 106-7, 117
scope ..... B1 – 23
security audit ..... B1 – 14
sensitive data ..... B1 – 27
setuid ..... B1 – 51
shells
  ephemeral ..... B1 – 47
  prompts ..... B1 – 55
sudo ..... B1 – 52
tcp ..... B1 – 99-102
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
version scan ..... B1 – 94
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

`lsof` connections ..... B1 – 53
`netstat` connections ..... B1 – 53

Tools/Sites

crt.sh ..... B1 – 79
DeHashed ..... B1 – 85
DNSDumpster ..... B1 – 75-7
DNSRecon ..... B1 – 73-4
Dradis Reporting ..... B1 – 40
ExploitDB ..... B1 – 37
GatherContacts ..... B1 – 86
HaveIBeenPwned ..... B1 – 85
Hunter.io ..... B1 – 83
Masscan ..... B1 – 96
MITRE ATTACK ..... B1 – 38
MITRE CVE ..... B1 – 37
Monster.com ..... B1 – 86
nmap ..... B1 – 109-21
phonebook.cz ..... B1 – 84
RIRs ..... B1 – 78
ScanRand ..... B1 – 96
Shodan ..... B1 – 80-1