

SEC560– Enterprise Penetration Testing

Index

attack phases	
covering tracks	B1 – 17
exploitation	B1 – 17
maintaining access	B1 – 17
post-exploitation	B1 – 17
recon	B1 – 17
scanning	B1 – 17
dedicated systems	B1 – 36
documented permission	B1 – 20, 23
ephemeral shell	B1 – 47
exploit	B1 – 11
full-knowledge	B1 – 26
linux	
connections	B1 – 51
filesystem	B1 – 46
permissions	B1 – 50
setuid	B1 – 51
penetration test	
definition	B1 – 15
types	B1 – 16
permissions	B1 – 50
pre-engagement	
goals	B1 – 22
rules	B1 – 24
scope	B1 – 23
privacy regulations	B1 – 27
purple team	B1 – 13
red team	B1 – 13

risk	B1 – 12
rules of engagement	B1 – 24
scope	B1 – 23
security audit	B1 – 14
sensitive data	B1 – 27
setuid	B1 – 51
shells	
ephemeral	B1 – 47
sudo	B1 – 52
test types	
full-knowledge	B1 – 26
unannounced	B1 – 25
zero-knowledge	B1 – 26
threat	B1 – 12
unannounced test	B1 – 25
vulnerability	B1 – 11
vulnerability assessment	B1 – 14
world-writeable	B1 – 51
zero-knowledge	B1 – 26

Commands

lsof conenctions	B1 – 53
netstat connections	B1 – 53

Tools/Sites

Dradis Reporting	B1 – 40
ExploitDB	B1 – 37
MITRE ATTACK	B1 – 38
MITRE CVE	B1 – 37