

SEC565 – Red Team Operations

Topics

Course Philosophy	1.1-10
Definitions	1.11-50
Chapters	
Book 1	
1) First chapter	1.1-60
2) Second chapter	1.61-100
Book 2	
1) First chapter	2.1-80
2) Second chapter	2.81-120

Categories

Basic Principles	
#1 First principle	1.51-60
#2 Second principle	1.61-70
#3 Third principle	1.71-80
#4 Fourth principle	1.81-90
Labs	
Environment Orientation	1.L1
Consuming Threat Intelligence	1.L2
Red Team Planning	1.L3
Reconnaissance and Password Attacks	1.L4
Username Enumeration and Password Spraying	
1.L5	
Lab 1.1	2.L1
First lab	2.L2
Second lab	2.L3
Third lab	2.L4
Lab Setup	2.L5
Tools	
Cobalt Strike	4.0
Empire	4.22
Impacket	3.22
Rubeus	4.57

SEC565 – Red Team Operations

A

Active Directory Certificate Services	5.53-54
Abuse	5.55, 5.57
Abuse Automation	5.58
ADCS	
OpenSSL	5.56
AS-REP	
Roasting	5.11
Tools	
Cobalt Strike	5.12
Empire	5.12

D

Database Attacks	5.91-101
Credential Hunting	5.95
DCSync	5.16
Tools	
Cobalt Strike	5.18
Empire	5.18
Mimikatz	5.17
Delegation	5.22
Constrained	5.33
C2	5.40
S4U2PROXY → S4U2PROXY	
S4U2SELF → S4U2SELF	
Resource based constrained	5.41
C2	5.48
Identifying	5.43-44
Kill Chain	5.45-47
Unconstrained	5.23
Cobalt Strike	5.31
Empire	5.32
Flow	5.24
Forced Auth	5.29
Recognizing	5.25
Rubeus Abuse	5.30
Domain Persistence	
Cheat Sheet	5.75
Hiding	5.77-78
Setting SPN	5.76

E

Exchange Priv Esc	5.59
Flow	5.60
SharpProxyLogon	5.61

G

Golden Ticket	5.19
C2s	5.21
Creation	5.20

H

Hopping the Trust	5.64-65, 5.68-69
Adding History	5.66-67

K

Kerberoasting	5.8-10
---------------------	--------

N

NoPac	5.49-52
Tooling	5.50

P

PrintSpooler	5.27
PetitPotam	5.28
Privilege Escalation	
Exchange → Exchange Priv Esc	
SQL → SQL Priv Esc	

S

S4U2PROXY	5.33-39
S4U2SELF	5.33-39, 5.49
sAMAccount → NoPac	
Shadow Credentials Attack	
Execution	5.84
Pre-Requisites	5.83
Silver Ticket	5.13
Tools	
Cobalt Strike	5.15
Empire	5.15
Mimikatz	5.14
Rubeus	5.14
SQL Priv Esc	5.63