

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
Adversary	
Emulation	1.24, 1.79
Emulation vs Simulation	1.24
Profiles	1.76-77
Simulation	1.24
APTs	
APT28	3.53
APT3	1.44
APT32	1.141
AS-REP	
Roasting	5.11
Tools	
Cobalt Strike	5.12
Empire	5.12
Attack Flows	1.81
Attack Infrastructure	
*nix Mail Servers	2.66
Advanced	2.55
Baseline	2.68
Cloud Providers	2.63
Digital Certificates	2.62
DNS	
Settings for Phishing	2.64
Setup for Mail Services	2.65
Domain Names	2.59
Categorization	2.61
Considerations	2.60
Purchasing	2.61
Functional Segregation	2.57
RedELK	2.56
Redirectors	2.58
Software	2.69
Standard	2.54
Third-Party Email Hosting	2.67

B

Blue Team	1.21
Evasion	2.110

C

C2 Client	2.17
Jitter	2.20
Proxy Awareness	2.18
Sleep	2.19
C2 Matrix	2.25
C2 Server	
Command & Control Tiers	2.14
Examples	2.16
Long Haul	2.15

Short Haul	2.15
Communications Channels	2.7
DNS	2.11
DNS Channels	2.13
HTTP	2.8
HTTP Channels	2.9-10
Non-Cached DNS Resolution	2.12
Listeners	2.6
Cobalt Strike	2.32, 2.40-48
Beacons	2.43
Data	2.47
Graph	2.46
Indicators	2.48
Launchers	2.42
Listeners	2.41
Logging	2.45
Tasks	2.44
Collection	5.106
Data Staging	5.108
Screen Capture	5.107
Covenant	2.28

D

Database Attacks	5.91-101
Credential Hunting	5.95
DCSync	5.16
Tools	
Cobalt Strike	5.18
Empire	5.18
Mimikatzs	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 Fronting	5.103
Headers	5.104
Domain Persistence	
Cheat Sheet	5.75
Hiding	5.77-78
Setting SPN	5.76

E

Empire	2.27
Engagement Closure	
Actions for Red Team	5.123

SEC565 – Red Team Operations

Analysis and Response	5.124
Closure Phase	5.122
Remediation and Action Plan	5.136
Example	5.137
Replay	5.128
Reporting	5.130
Tools	5.131
Reveal	5.125
Ethical Hacking	1.15
Maturity Model	1.25
evilginx2	1.151
Exchange	
Priv Esc	5.59
Flow	5.60
SharpProxyLogon	5.61
Execution Phase	1.113
Building a Team	
Documentation	1.118
Skill Development	1.114
Team Data	1.117
Team Dynamics	1.115
Team Workflow	1.116
Exchange Remote Access Protocols	1.133
Information Disclosure	1.127
OSINT	1.126
Password Attacks	1.128
Account Lockouts & Policies	1.137-139
ADFS Password Spraying	1.135
Azure AD Password Spraying	1.136
Credential Stuffing	1.132
Outlook Web Services Spraying	1.134
Password Guessing	1.130
Password Spraying	1.131
Stolen Credentials	1.129
PRE-ATT&CK	1.119
Reconnaissance	1.120
Active	1.123
Active Tools	1.124
Frameworks	1.125
Passive Sources	1.121
Passive Tools	1.122
Social Engineering	1.140
Adversary Emulation	1.145
APT32	1.141
ChatGPT	1.143-144
Link Trackers	1.148-149
MFA	1.150
MFA Attack - evilginx2	1.151
Phishing Awareness	1.146
Phishing for Credentials	1.147
Pretext	1.142
Vishing	1.152
Exfiltration	5.110
Safe	5.113
Unsafe	5.111-112

G

Gather Intelligence	1.72
---------------------------	------

Ghostwriter	5.131
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

I

Identify Adversary	1.71
Impact	5.115
Emulating Ransomware	5.116
Initial Access	2.45
Exploitation	2.46
Hardware Additions	2.54
Spear Phishing	
Attachment	2.49
Link	2.50
Service	2.51
Supply Chain Compromise	2.52
Trusted Relationships	2.53
Web Applications	2.47
Webshells	2.48

K

Kerberoasting	5.8-10
Kerberos	5.8

M

Merlin	2.30
Metasploit	2.26
MITRE ATT&CK	1.119
PRE-ATT&CK	1.119

N

NoPac	5.49-52
Tooling	5.50

O

Offensive Operations	1.16
----------------------------	------

P

Penetration Testing	1.19
Planning Phase	1.87
Engagement Frequency	1.94
Objectives & Scope	
Assume(d) Breach	1.93
End-to-End Testing Model	1.92

SEC565 – Red Team Operations

Metrics	1.91
Objectives	1.89
Scenario	1.91
Scope	1.90
TTPs	1.91
Risk Avoidance	1.100
Roles & Responsibilities	1.96
Engagement Coordinator	1.98
Governance	1.97
Project Management	1.98
Trusted Agents	1.95
Rules of Engagement (ROE)	1.101
Breach Notification or Injects	1.106
Communication Plan	1.102
De-Chain	1.105
Deconfliction	1.104
Pausing or Ending an Engagement	1.107
Player Rules	1.103
Time Estimations	1.99
Triggers	1.88
PlexTrac	5.131
PrintSpooler	5.27
PetitPotam	5.28
Privilege Escalation	5.59, 5.63
Exchange → Exchange Priv Esc	
SQL → SQL Priv Esc	
Purple Team	1.22, 5.129

R

Ransomware	5.116
Red Team	1.20
Red Team Tools	
C2 Comparison	2.34
C2 Matrix	2.25
Cobalt Strike	2.32
Commercial vs OS	2.24
Covenant	2.28
Empire	2.27
Merlin	2.30
Metasploit	2.26
SCYTHE	2.33
Sliver	2.29
RedELK	2.56
Redirectors	
Comparison socat to IPtables	2.98
DNS	
IPtables	2.95
socat	2.94
HTTP/S	
Caddy	2.101
IPtables	2.97
mod_rewrite	2.99
Nginx	2.100
Satellite	2.102
socat	2.96
Retesting	
Tools	

APT Simulator	5.142
Atomic Red Team	5.141
MITRE CALDERA	5.144
Network Flight Simulator	5.143
SCYTHE	5.145

S

S4U2PROXY	5.33-39
S4U2SELF	5.33-39, 5.49
sAMAccount → NoPac	
SCYTHE	2.33
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
Sliver	2.29
Spear Phishing	2.62, 1.64
Initial Access	1.75
Through Attachment	2.49
Through Link	2.50
Through Service	2.51
With Cobalt Strike	2.32
SQL	
Priv Esc	5.63
Supply Chain Compromise	2.52

T

Tabletop Exercises	1.23
Tactics, Techniques, and Procedures	
TTPs	1.73, 1.91

U

UAC	5.6
-----------	-----

V

VECTR	5.131
Heat Map	5.134
Summary	5.133
Test Cases	5.126, 5.132
Trends	5.135
Vulnerability Assessments	1.18
Vulnerability Scanning	1.17

W

Wargaming	1.23
Web Applications	2.47
Webshells	2.48
Why Red Team	2.29

SEC565 – Red Team Operations

Cognitive Biases	2.33	People	2.34
Focus on Stealth	2.37	Process	2.34
Holistic View of an Org	2.32	Technology	2.34
Motivation	2.31	Train & Improve Blue Team	2.36
Test		What is Red Team	2.30
Assumptions	2.35		