

# SEC565 – Red Team Operations

---

## A

Abuse .....	2.67
Accounts	
Computer Account Enumeration	
Examples .....	4.61
Things to Look For .....	4.60
Domain Computer Account Enumeration	
C2s .....	4.62
Domain User Account Enumeration	
C2s .....	4.56
GUI .....	4.55
gMSA .....	4.85
Enumeration .....	4.86
LAPS .....	4.81
Local vs Domain .....	4.23
Service Account Enumeration .....	4.57
C2s .....	4.59
Honeypots .....	4.58
User Access .....	4.97
User Account Enumeration	
Considerations .....	4.39
Format Conversion .....	4.54
Honeypot Spotting .....	4.53
Honeypots .....	4.52
IoCs .....	4.51
Mental Model .....	4.38
Things to Look For .....	4.50
ACE	
Access Control Entry .....	4.32
DACL .....	4.33
Act .....	4.192
Active Directory Certificate Services .....	5.53-54
Abuse .....	5.55, 5.57
Automation .....	5.58
ADCS .....	
OpenSSL .....	5.56
Active Directory Module .....	4.41
Adcspwn .....	5.58
ADExplorer .....	4.48
ADFind .....	4.40, 4.44, 4.61
Administration .....	4.11, 4.41, 4.47, 4.66
Admins .....	5.16, 5.80
ADSI .....	4.49
Remote Recon .....	4.105
Adversary	
Emulation .....	1.24, 1.79
Emulation vs Simulation .....	1.24
Profiles .....	1.76-77
Simulation .....	1.24
Adversary Emulation Plans .....	1.79
Adversary Identification .....	1.71
AdvFirewall .....	2.88
AES .....	5.10, 5.14, 5.17, 5.20, 5.126
Agents .....	2.17, 2.25, 2.27
Alias .....	2.11, 12, 2.118, 119
AllProfiles (Powershell Selector) .....	2.88
AlphaSOC .....	5.143
AMSI .....	3.133

amsiContext	
Bypass .....	3.143
Bypass code .....	3.148
Locate .....	3.145
Override .....	3.144
Replace .....	3.146
AntiMalware Scan Interface .....	3.140
Bypass .....	3.142
Creation .....	3.147
Custom .....	3.143
In Action .....	3.149
Tools .....	3.150
Definitions .....	3.141
Under the Hood .....	3.146
APR .....	2.105
APTs	
APT Simulator .....	5.142
APT28 .....	3.53
APT3 .....	1.44
APT32 .....	1.141
Engagement Frequency .....	1.94
ARP .....	3.69, 3.104, 105, 3.107
AS-REP	
Roasting .....	5.11
Tools	
Cobalt Strike .....	5.12
Empire .....	5.12
ASCII .....	3.112, 3.145
AskTGT .....	4.139
Atomic .....	5.140, 141
ATT&CK Campaigns .....	1.80
ATT&CK Navigator .....	1.79
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
Auditing .....	5.101
Authority .....	4.21, 4.120, 4.150
Azure .....	2.105, 1.135, 136

## B

# SEC565 – Red Team Operations

---

Background .....	5.31, 32
Beacons .....	2.19, 2.27, 2.32, 2.39, 2.41-46
Behaviors .....	1.33, 1.47, 1.51, 1.66, 1.81
Bias .....	1.31, 1.33
Biases .....	1.33
Bidirectional .....	4.70
Binaries .....	2.42
Bloodhound .....	4.45
Cheatsheet .....	4.46
gMSA Enumeration .....	4.86, 87
Group Policy Enumeration .....	4.66
Example .....	4.67
Group Policy Objects .....	4.110
LAPS .....	4.84
Blue Team .....	1.21
Evasion .....	2.110
Brute Force .....	1.128, 1.130-132, 1.137

## C

C2 .....	
Comparison .....	2.34
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
Caddy .....	2.93, 2.101
Cafire .....	2.87
Caldera .....	5.140, 5.144
Capable .....	5.9, 5.20, 5.48, 5.50-52
CBEST .....	1.50, 51
CDN .....	2.103-105
Cert .....	2.11, 5.56, 2.82, 5.84, 2.87, 5.113
Certificate .....	5.4, 5.19, 5.53-56, 5.83, 84
Certify .....	5.55
Chain .....	1.22, 1.24, 1.31, 32
Changes .....	5.16, 5.75
Channel .....	2.4, 2.7, 2.9, 10, 2.13, 2.17, 2.25, 2.30
HTTP .....	
Example .....	2.10
ChatGPT .....	1.143, 144
Chisel .....	2.76, 2.80
Choice .....	4.6, 4.40, 4.141, 4.189
CimSession .....	4.176
Cloud .....	2.53, 2.63, 2.68, 2.113

CLSID .....	3.126
CNTLM .....	2.76
Cobalt Strike .....	2.32
AS-REP .....	5.12
Beacons .....	2.43
Data .....	2.47
DCSync .....	5.18
Framework .....	2.40
Golden Ticket .....	5.21
Graph .....	2.46
Indicators .....	2.48
Kerberoasting .....	5.9
Launchers .....	2.42
Listeners .....	2.41
Logging .....	2.45
NoPac Attack .....	5.51
sAMAccount Spoof .....	5.51
Screen Capture - Screenshot .....	5.107
Silver Ticket .....	5.15
Task .....	2.44
Unconstrained Delegation .....	5.31
Collection .....	5.106
Data Staging .....	5.108
Screen Capture .....	5.107
Commands .....	4.99-101, 4.162, 4.171, 4.178
Communication Channels .....	2.7
Compile .....	3.19
Compromised .....	1.93, 1.129
Computer .....	4.98, 4.108, 109, 4.113
ComputerName (Powershell Selector) .....	
GPO Correlation .....	4.113
GPO Correlation Reversed .....	4.114
Leveraging RPC .....	4.109
Process Ownership .....	
Powershell Magic .....	4.119
WMI .....	4.118
Remote Recon .....	4.105
Session Enumeration .....	4.116
ComputerSID .....	5.46
Conclusion .....	4.193
Controllers .....	5.16, 5.25, 5.29, 5.69
ConvertTo (Powershell comamnd) .....	4.88
Covenant .....	2.28
Credential Discovery .....	
Powershell .....	3.75
Credentials .....	
Access .....	3.93
Capture NTLM .....	
Challenge Response .....	3.103
Cleartext Files .....	3.95
Dumping .....	3.98
Dumping from Memory .....	3.101
Hijacked RDP .....	3.87
Input Capture .....	3.97
Network Sniffing .....	3.102
Pass-the-Hash .....	3.115
Password Managers .....	3.99
Passwords .....	3.94

# SEC565 – Red Team Operations

---

Saved Credentials .....	3.100
Unattended Install Files .....	3.96
CredentialsCapture NTLM	
MITM SNiffing .....	3.105
cURL .....	2.83
User-Agent .....	2.116
Wrapping	
Example .....	2.119
Logging .....	2.118
Currentversion .....	3.125
CVEs	
CVE-2016-5195 .....	3.90
Dirty Cow .....	3.90
CVE-2021-26855 .....	5.59
ProxyLogon .....	5.59
CVE-2021-42287 .....	5.49

## D

DACL .....	4.32
Example .....	4.33
gMSA .....	4.85
LAPS .....	4.81
Access .....	4.84
Windows Remoting .....	4.162
Data	
Emulating Ransomware .....	5.116
Data Collection .....	5.106
Data Consolidation .....	5.123
Data Destruction .....	5.115
Data Encryption .....	5.115
Data Exfiltration .....	5.110
Data Manipulation .....	5.115
Data Staging .....	5.108
Database Attacks .....	5.91-101
Credential Hunting .....	5.95
Datacenter .....	4.61
Datetime .....	4.54
dbms (SQLMap parameter) .....	5.98
DCOM .....	4.167
C2s .....	4.173
UAC Bypass .....	4.171
Well-Known Objects .....	4.172
Why DCOM .....	4.168
DCSync .....	5.16
Golden Ticket .....	5.20
Persistence .....	5.85
Tools	
Cobalt Strike .....	5.18
Empire .....	5.18
Mimikatzs .....	5.17
Debugger	
AMSI .....	3.146
Bypass .....	3.148, 149
Presence .....	3.41
Deception Technology .....	3.63
Deconfliction .....	1.104
Documenting Process .....	1.34

Pausing or Ending Engagement .....	1.107
Delegation .....	5.22
Constrained .....	5.33
Attacking .....	5.38
C2 .....	5.40
Identifying .....	5.37
Kerberos Only .....	5.34
S4u Kill Chain .....	5.39
S4U2PROXY → S4U2PROXY .....	
S4U2PROXY Flow .....	5.36
S4U2SELF → S4U2SELF .....	
Use Any Authentication .....	5.35
Resource based constrained .....	5.41
Abuse .....	5.42
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
Demiguise .....	3.12, 3.28
Deploying .....	5.144
Description .....	4.50-52, 4.60, 4.63
Dev .....	5.67, 5.112
Digits .....	3.112
Dirty Cow .....	3.90
Discovery .....	3.61
Account Discovery .....	3.65
Accounts .....	3.65
CLI .....	3.64
Deception .....	3.63
Local Network Enumeration .....	3.69
Local Networks .....	3.69
OpSec .....	3.62
Powershell .....	3.75
Process Discovery .....	3.66
Processes .....	3.66
Security Software and Controls .....	3.68
Service Discovery .....	3.67
Services .....	3.67
Sniffers .....	3.70
Software & Controls .....	3.68
WMIC .....	3.71, 3.71-74, 3.72, 73
WMI Ops .....	3.74
Displayname .....	4.67
Displays .....	3.69
DLL	
Active Directory Module .....	4.41
AMSI .....	3.140
Bypass .....	3.142
Creation & Modification .....	3.82
Hijack	
COM .....	3.126
UAC Bypass .....	3.84

# SEC565 – Red Team Operations

---

Hijack COM: Example .....	3.127	Eaba .....	5.17, 5.20
Hijacking		Ecrela .....	3.32
Callbacks .....	4.186	Eenum .....	4.94
Example .....	4.184	Elastic .....	2.56
Weaponization .....	4.185	Elatelr .....	4.192
Lateral Movement .....	4.188	Email .... 3.11, 3.17, 2.32, 3.34-36, 3.40, 3.45, 3.49, 50,	
Loading .....	4.183	2.53, 2.57, 2.62, 2.64, 65, 2.67	
Rundll32 .....	3.24	Empire .....	2.27
Search Order .....	3.81	Analysis & Response .....	5.124
DMZ .....	4.16	AS-REP .....	5.12
DNS .....	2.11	DCOM .....	4.173
AntiMalware Bypass .....	3.41	Delegation	
Channel		Constrained .....	5.40
Example .....	2.13	Resource-Based Constrained .....	5.48
Cobalt Strike		Unconstrained .....	5.32
Listener .....	2.41	Enumeration	
Domain Fronting		Domain Computer Accounts .....	4.62
Headers .....	2.104	Domain Groups .....	4.65
Enumeration		Domain Trusts .....	4.71
ipconfig .....	3.69	Domain User Accounts .....	4.56
Extraction .....	4.90	Fine-Grained Password Policy .....	4.80
nslookup Alternative .....	4.91	gMSA Passwords .....	4.89
Infrastructure .....	2.55	GPOs .....	4.68
iptables .....	2.95	LAPS .....	4.83
Mail Services		Password Policy .....	4.76
Setup .....	2.65	Service Accounts .....	4.59
Non-Cached .....	2.12	Exchange Privilege Escalation .....	5.62
Phishing		Golden Ticket .....	5.21
Settings .....	2.64	Hopping the Trust .....	5.68
socat .....	2.94	Kerberoasting .....	5.9
Spoof		Lateral Movement .....	4.181
NBNS .....	3.107	NoPac .....	5.52
NBNS Capture .....	3.107	OverPass-the-Hash .....	4.140
NTLM Sniffing .....	3.104	Pass-the-Hash .....	4.135
NTLM Sniffing Capture .....	3.105	Pass-the-Ticket .....	4.140
SSHuttle		Payload Testing .....	3.26
Proxy .....	2.81	sAMAccount Spoof .....	5.52
Domain .... 2.11, 12, 2.30, 2.41, 2.54, 2.59-65, 2.93,		Scheduled Task .....	4.177
2.103-105, 2.111, 2.115		Screen Capture .....	5.107
Domain Fronting .....	5.103	SCT .....	3.23
Headers .....	5.104	Silver Ticket .....	5.15
Domain Persistence		Token Creation .....	4.130
Cheat Sheet .....	5.75	Token Impersonation .....	4.128
Hiding .....	5.77-78	Who Is Running What Process? .....	4.121
Setting SPN .....	5.76	Windows Remoting .....	4.164
Domain Purchasing .....	2.61	WMI .....	4.166
Domains .....	4.4, 4.14-16, 4.69	Emulating .....	5.105, 5.115, 116
Don .....	5.78	Enabled .... 4.29, 4.82, 4.101, 4.121, 4.128, 4.158, 159,	
Draconem .....	4.14, 15	4.162, 163	
Driver .....	4.120	End-to-End Testing Model .....	1.92
Dumping .....	3.59, 3.93, 3.98, 3.101	Endpoint .....	5.57, 5.60, 5.115, 5.142
Dynamic .... 3.22, 3.24, 3.81, 3.131, 3.133, 3.137-140		Engagement Closure	
Dynamic Analysis .....	3.137	Actions for Red Team .....	5.123
AMSI .....	3.140	Analysis and Response .....	5.124
Bypass .....	3.139	Closure Phase .....	5.122
Downsides .....	3.138	Remediation and Action Plan .....	5.136
		Example .....	5.137
		Replay .....	5.128

## E

# SEC565 – Red Team Operations

---

Reporting .....	5.130
Tools .....	5.131
Reveal .....	5.125
Engineering .....	4.39, 4.147, 4.150, 4.152, 153
Enrollment .....	5.57
Enter .....	4.25, 4.161, 4.163
Environ .....	2.118
Epivolt .....	2.91
Esettlin .....	2.124
Ethical Hacking .....	1.15
Maturity Model .....	1.25
Event .....	3.18, 3.71, 3.102, 3.120, 3.123, 3.128
Evilginx .....	1.151
evilginx2 .....	1.151
Exchange .....	5.34, 5.56, 5.59, 60, 5.62, 1.73, 1.76, 77, 1.133, 134
Priv Esc .....	5.59
Flow .....	5.60
SharpProxyLogon .....	5.61
Exec .....	5.99, 100
Executables .....	3.4, 3.6, 7, 3.9, 3.80, 3.84, 3.151
Execute .....	5.9, 5.12, 5.15, 5.22, 5.31, 5.40, 5.48, 5.51, 5.62, 63, 5.67, 68, 5.83, 5.148
execute_assembly (C# pragma) .....	5.51
Executeshellcommand .....	4.169, 170
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
Exercises .....	5.129, 5.135, 5.148
Exfiltration .....	5.110
Safe .....	5.113
Unsafe .....	5.111-112
Exim .....	2.66

## F

Fake .....	3.106
Filter .....	3.127, 128
Fine .....	4.30, 4.33, 4.39, 4.77-80, 4.86, 4.99
Flightsim .....	5.143
Font .....	4.120
Forceful .....	5.26
Forest .....	4.7, 4.14-17, 4.24, 4.39, 4.70, 4.72, 73
Forests .....	4.4, 4.14
Format .....	4.23, 4.42, 4.45, 4.53, 54
Fortra .....	2.32, 2.56
Forwarding .....	2.75, 2.77-79, 2.83, 84, 2.88, 2.95, 2.97
FTP .....	5.108, 5.110, 111
Functional .....	4.72, 73
Functions .....	4.54, 4.169, 4.172, 4.179

## G

Gather Intelligence .....	1.72
Gets .....	5.5, 5.35, 5.38, 5.41, 5.75, 5.77
Ghostpack .....	3.20, 3.86, 3.90, 3.99
Ghostwriter .....	5.131
Given .....	5.41, 5.79, 5.108
gMSA .....	4.85-89
GNU .....	2.84
Golden Ticket .....	5.19, 5.67, 68
C2s .....	5.21
Creation .....	5.20
Got .....	5.28, 5.53, 5.58, 59, 5.61
Governance .....	1.88, 1.90, 1.96, 97, 1.99, 100, 1.102
GPOs .....	4.9, 4.106, 4.110-114
Bloodhound .....	4.45
Conclusions .....	4.13
Enumeration .....	4.66
C2s .....	4.68
Example .....	4.67
Local Policy .....	4.11
Non-Local Policy .....	4.12
PowerView .....	4.42
Starter .....	4.10
GPU .....	3.110, 3.113
Grant .....	5.85
Group .....	5.5, 5.61, 5.65, 5.77, 5.80, 81, 4.162
Grunts .....	2.10, 2.17, 2.28
Gui .....	4.8, 4.24, 4.32, 4.47, 4.55, 4.155, 4.160
Guidelines .....	1.52, 53, 1.101

# SEC565 – Red Team Operations

---

## H

Hamsik .....	2.79
Hardware .....	3.44, 45, 3.54, 3.97, 3.110
Hash .....	4.126, 4.131-137, 4.140, 4.156-158
Hashcat .....	3.110, 3.113
Haul .....	2.14-16
Header .....	2.9, 2.100, 101, 2.104
Headers .....	2.104, 2.116
Heat .....	5.134
Helpdesk .....	4.63, 4.79, 4.113, 114
Hijack .....	3.84, 3.86, 3.103, 3.126, 127
Hijacking .....	3.21, 3.80-82, 3.85, 3.87, 3.120
Historical .....	5.135
History .....	5.65-67, 5.106
Hkcu .....	3.127
Hkey .....	3.81, 3.125, 126
Hklm .....	3.82, 3.127
Hmac .....	5.17
Hooks .....	2.79
Hop .....	5.64, 65
Hopping the Trust .....	5.64-65, 5.68-69
Adding History .....	5.66-67
Hosting .....	2.53, 2.57, 2.67, 2.102
Hosts .....	2.48, 2.113, 2.115
HTA .....	3.11, 12
HTTP .....	2.8
Advanced Infrastructure .....	2.55
Caddy .....	2.101
Channels .....	2.9
Example .....	2.10
Chisel .....	2.80
cURL .....	2.83
Domain Fronting Headers .....	2.104
iptables .....	2.97
Jitter .....	2.20
mod_rewrite .....	2.99
Nginx .....	2.100
ProxyChains .....	2.79
Purchase Domains & Categorization .....	2.61
Satellite .....	2.102
socat .....	2.96
wget .....	2.84

## I

Identify Adversary .....	1.71
Ilm .....	4.192
Impact .....	5.115
Emulating Ransomware .....	5.116
Impersonate .....	4.1, 4.128, 4.135, 4.163
Impersonation .....	4.19, 4.34-36, 4.93-95, 4.123-142, 4.163, 4.191
Import .....	2.32, 2.118
Improper .....	5.63
Indicators .....	2.28, 2.32, 2.39, 2.48, 2.108, 2.110, 111
Info .....	5.98, 5.151
Initial Access .....	2.45

Exploitation .....	2.46
Hardware Additions .....	2.54
Spear Phishing .....	
Link .....	2.50
Service .....	2.51
Supply Chain Compromise .....	2.52
Trusted Relationships .....	2.53
Web Applications .....	2.47
Webshells .....	2.48
Injection .....	4.126, 4.142
Instant .....	2.67
Int .....	4.16
Integrity .....	4.164, 4.186
Interact .....	5.22, 5.93
Interfaces .....	4.4, 4.49
Internal .....	2.12, 2.68, 2.77, 4.115, 4.147, 4.149-153
Internals .....	4.132
Internet .....	3.5, 3.10, 3.13, 3.22, 3.35, 3.47, 3.94
Invoke .....	3.74, 75, 3.85, 3.123, 3.135
invoke_assembly (C# pragma) .....	5.52
Ipconfig .....	3.69
Iptables .....	2.76, 2.85, 2.93, 2.95, 2.97, 98
Ipv .....	4.91

## J

Javascript .....	3.9-11, 3.24
Jitter .....	2.4, 2.20
Jobs .....	5.31
John .....	3.104, 105, 3.109-113

## K

Kdc .....	4.21, 4.23, 24, 4.27-31, 4.136
Kerberoasting .....	5.4, 5.8, 5.8-10, 5.9, 10, 5.76
Kerberos .....	5.8, 4.23, 24, 4.26-31, 4.126, 4.131, 4.137, 4.158
Key .....	4.21, 4.23, 24, 4.28-31, 4.39, 40, 4.84, 4.96
Keylogging .....	3.93, 3.97, 3.99
Kill Chain .....	1.22-24, 1.31-33, 1.43-46, 1.56-58, 1.63, 1.79, 1.92, 1.105, 1.137, 1.156
Krbtgt .....	5.17, 5.19, 20, 5.66, 67
krbtgt .....	
History Addition .....	5.66

## L

Labor .....	4.134
Language .....	5.91, 5.93, 94, 5.145
Lap .....	5.81
Laps .....	4.39, 4.67, 4.81-85, 4.88
Launchers .....	2.39, 2.42
Ldap .....	3.73, 3.108
Legacydn .....	5.60, 61
Length .....	4.25, 4.39, 4.74, 3.148
Letter .....	2.103

# SEC565 – Red Team Operations

---

Letters .....	3.112
Level .....	4.23, 4.72, 73, 4.179, 180, 4.186
Leveraging .....	4.109, 4.116
Libc .....	2.79
Link 3.11, 3.22, 3.35, 3.40, 3.45, 3.50, 3.81, 5.100, 3.128	
Links .....	5.0, 5.91, 5.100
Listeners .....	2.41
Little .....	4.45, 4.53, 4.84, 4.156
Living Off the Land Binaries and Scripts	
LOLBAS .....	3.21
Regsrv32 .....	3.22
Rundll32 .....	3.24
Shortcuts .....	3.25
Lockout .....	4.39, 4.74, 4.77, 1.130, 131, 1.135-139
Logged .....	4.22, 4.34, 4.54, 4.96, 4.98, 4.115
Logging ... 2.11, 12, 2.32, 2.34, 2.45, 2.101, 2.110, 111, 2.118	
Logoncount .....	4.58, 4.61
Logs .....	3.18, 3.68, 3.71, 3.74, 75, 3.109, 3.125
Lolbas .....	4.165
Lots .....	2.83
Lsa .....	4.21
Lsadump .....	5.17

## M

Machine .....	5.0, 5.7, 5.23, 5.29, 5.45, 46
Macro .....	4.153
Mail .....	2.11, 2.62, 2.64-66
Making .....	4.45, 4.82, 4.134
Malicious .....	4.52, 4.152, 153, 4.188
Mandatory .....	4.101
Map .....	5.75, 5.134
Mapping .....	1.58, 1.61, 1.74, 1.122
Mask .....	3.111, 112, 3.139
Maturity .....	1.14, 1.26, 1.94
Member .....	4.29, 4.44
Members .....	5.80, 5.128, 5.131
Merlin .....	2.30
Metasploit .....	2.26, 2.41
Methodology .....	3.78
Milgab .....	3.32
Mimikatz .....	5.14, 15, 5.17, 18, 5.20, 21, 5.67, 68
Getting In & Staying In .....	3.6, 3.20, 3.87, 3.98, 3.101, 3.134
Lateral Movement .....	4.131, 4.135, 4.137, 4.141, 4.156, 157
Minimum .....	4.39, 4.74, 4.148
Mitre .....	5.115, 5.140, 141, 5.144, 5.148
MITRE ATT&CK .....	1.119
PRE-ATT&CK .....	1.119
Mmc .....	4.167, 4.169, 4.171
Mod .....	2.93, 2.99
Monitor .....	5.30, 31, 5.137
Msbuild .....	3.14, 3.28
Msds .. 5.33-37, 5.43-46, 4.73, 4.78, 79, 5.82, 5.84, 4.88	
Mshta .....	3.11
Mstsc .....	4.156, 157

Mtoevemreont .....	4.192
Multi .....	2.28, 2.34
Must .....	5.147
Myriad .....	2.83

## N

Names .....	2.32, 2.59-61, 2.111, 2.115
Nameserver .....	2.12
Namespace .....	3.72, 73
Native .....	5.107
Navigator .....	1.61, 1.78
Nbns .....	3.103, 3.106, 107
Net .....	4.38, 4.99, 100, 4.111, 112, 4.131, 4.167
Netcat .....	2.76
Netsh .....	2.88
Netstat .....	3.69, 3.75
Network .....	5.106, 5.110, 5.115, 5.140, 5.143
Network Flight Simulator .....	5.143
Newpassword .....	5.79
Nicks .....	5.94
Non .....	3.0, 3.17, 18, 3.79, 3.90, 3.112, 3.115, 3.145
NoPac .....	5.49-52
Tooling .....	5.50
Nopac .....	5.49-52
Note .....	2.73
Notorious .....	4.57, 4.149
Npk .....	3.110, 3.114
Nslookup .....	4.90, 91
NTLM ... 5.17, 5.57, 5.99, 3.103-107, 3.109, 3.113, 114	
AD Attacks .....	4.16, 17, 4.20, 4.23, 4.26, 4.88
Lateral Movement .....	4.127, 4.131, 4.136, 137, 4.157
Null .....	4.50, 4.105, 4.171

## O

Offensive Operations .....	1.16
OpenSSL .....	5.56, 2.76, 2.82, 2.87, 5.113
Operatingssystem .....	4.61
Opportune .....	3.93
Orchilles .....	3.1, 5.1, 5.151, 3.156, 4.194
OSINT .....	1.114, 1.122, 1.125, 126
Osint .....	3.51
Outer .....	2.103
Outflank .....	2.56
Overpass .....	4.126, 4.136, 4.140
Override .....	2.117, 3.144
Owa .....	1.134

## P

Package .....	2.103
Parent .....	5.64-66, 5.68, 69
Pass .....	4.105, 4.131-137, 4.141, 4.156, 4.158
Password	
AD Attacks ... 4.22, 4.25-29, 4.31, 4.34, 4.37, 4.39, 4.51-53, 4.57, 58, 4.74-88	
Lateral Movement .....	4.100, 4.126, 4.129, 4.131, 4.136-138, 4.155, 4.157, 4.160, 4.165, 4.176

# SEC565 – Red Team Operations

Passwords .....	3.60, 3.68, 3.94, 95, 3.98, 99
Persistence .....	3.102, 3.110, 111, 3.115
Pausing .....	1.86, 1.107
Payload .....	5.86, 5.100, 5.111
Peer .....	2.7, 2.32, 2.46
Penetration Testing .....	1.19
Penguin .....	2.81
Performing .....	5.9, 10, 5.48, 5.51, 52
Permissions .....	3.65, 3.78, 79, 3.82, 83, 3.88, 89, 3.98
PetitPotam .....	4.28, 5.28
Petitpotam .....	5.28, 5.30
Phish .....	1.146
Phishing .....	3.35, 3.40, 3.44, 45, 3.49, 50, 4.50, 3.51, 4.97, 4.150-152
Physical .....	3.27, 3.34, 3.38, 3.54, 3.97
Ping .....	3.70
Pipe .....	4.178
Pivoting .....	2.2, 3, 2.22, 2.32, 2.36, 2.38, 2.50, 2.52, 2.71-76, 2.90-92, 2.107, 2.123, 2.125
Tools .....	2.76
Planning Phase .....	1.87
Engagement Frequency .....	1.94
Objectives & Scope .....	
Assume(d) Breach .....	1.93
End-to-End Testing Model .....	1.92
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
Policies .....	4.4, 5, 4.7, 4.9, 10, 4.13, 4.37, 4.66, 4.77, 78, 4.86, 4.110
Policy .....	4.5, 4.9-12, 3.16, 17, 4.39, 4.47, 4.66, 67, 3.68, 4.74-80, 3.98
Port .....	2.11, 2.41, 3.70, 2.75, 3.75, 2.77-80, 2.82-86, 3.86, 2.88, 2.95-97, 2.100, 101, 2.117
Postfix .....	2.66
Powershell .....	5.9, 5.12, 5.15, 5.18, 5.21, 5.40, 5.45, 46, 5.48, 5.50-52, 5.62, 5.68, 5.80, 5.101, 5.108
Powerup .....	3.85, 86
Powerupsql .....	5.91, 5.101
PowerView .....	4.42
Powerview .....	4.24, 4.40, 4.42, 43, 4.56, 4.59, 4.62, 4.65-68, 4.70, 71, 4.73, 4.76, 4.112, 4.116
Press .....	3.19, 5.98, 5.151, 3.156, 4.194
Pretext .....	1.142, 1.144, 1.152
Pretexts .....	1.142, 143
Preventing .....	4.13
Previous .....	4.80, 4.126
PrintSpooler .....	5.27
PetitPotam .....	5.28
Privilege Escalation .....	5.59, 5.63
Exchange → Exchange Priv Esc .....	
SQL → SQL Priv Esc .....	
Proc .....	4.119
Process .....	4.21, 22, 4.25, 4.34, 4.40, 4.50, 4.55, 4.96, 4.108, 4.117-121, 4.126-128, 4.132-135, 4.140, 4.142, 4.148, 4.163, 4.165, 4.180, 4.186
Processname .....	4.118
Procs .....	4.119
Program .....	3.22, 3.28, 3.46, 2.79, 3.80, 81, 3.89, 3.123, 3.125, 126, 3.128, 3.139, 140, 3.142
Propagation .....	3.46, 3.59, 60, 3.155
Protocol .....	5.16, 5.27, 28, 5.33, 5.35, 5.37, 38, 5.60, 5.108, 5.110
Proxy .....	2.4, 2.18, 2.27, 2.41, 2.76, 2.78, 2.80, 81, 2.83, 84, 2.100-102, 2.120
Proxychains .....	2.76, 2.79
Psexec .....	4.147, 4.154, 4.178, 179
Ptr .....	3.35, 3.148
Publicized .....	4.168
Purple .....	1.14, 15, 1.22, 1.43, 1.49, 1.94, 5.121, 122, 5.124, 5.129, 5.148
Purple Team .....	1.22, 5.129
Pwneip .....	3.1, 3.24, 3.87, 3.112
Pwnmachine .....	5.45, 5.47
Pyramid .....	1.64, 65

## Q

Queries .....	2.12, 13, 2.81
---------------	----------------

## R

Ransomware .....	5.104, 105, 5.116
Rdp .....	4.9, 4.63, 3.66, 4.66, 3.67, 3.87, 3.101, 4.117, 4.154-158, 4.160
Read .....	4.0, 4.30, 4.32, 33, 4.53, 4.82, 4.84, 85, 4.87, 88
Record .....	2.11, 12, 2.65
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



# SEC565 – Red Team Operations

---

SCYTHE .....	2.33
Sliver .....	2.29
RedELK .....	2.56
Redelk .....	2.53, 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
Redteam .....	1.2
Redteamer .....	2.80
Registry .....	4.106, 4.108, 4.118, 4.159
Regsvr .....	3.22, 23, 3.25, 3.126
Relational .....	5.93, 5.99
Remoting .....	4.147, 4.161, 162, 4.164, 4.176
Replay .....	5.121, 122, 5.124, 5.128
Rerdiroectlo .....	2.124
Reset .....	5.79
Resource ...	5.22, 5.41-43, 5.45, 5.48, 5.65, 5.111, 5.115
Responder .....	3.103, 3.108, 109
Response .....	4.26, 4.29, 4.31, 4.90
Restricted .....	4.112, 4.158, 159
Retesting .....	5.2, 3, 5.71, 5.73, 5.88, 5.90, 5.103, 5.109, 5.114, 5.118, 5.120, 5.136, 137, 5.139-145, 5.147, 5.149
Tools	
APT Simulator .....	5.142
Atomic Red Team .....	5.141
MITRE CALDERA .....	5.144
Network Flight Simulator .....	5.143
SCYTHE .....	5.145
Roasting .....	5.4, 5.10-12
Roles & Responsibilities .....	1.96
Root ....	3.46, 3.60, 3.70, 3.72, 73, 3.79, 3.88, 89, 3.95, 3.98, 3.122
Rpc ....	4.46, 4.99, 4.103, 4.106, 4.108, 109, 1.133, 134, 4.174, 4.176, 4.180
RSAT .....	4.47
AD .....	4.41
Enumeration .....	4.40
Rubeus ..	5.9, 5.12, 5.14, 15, 5.20, 21, 5.30-32, 5.38-40, 5.47, 5.56, 5.68, 5.84, 4.137
AS-REP .....	5.12
Delegation	
Constrained .....	5.38-40
Final .....	5.47
Unconstrained .....	5.29-32
Golden Ticket .....	5.20-21
Kerberoasting .....	5.9
OpenSSL .....	5.56
OverPass the Hash .....	4.136, 137, 4.139, 4.141

Empire .....	4.140
Pass the Ticket .....	4.136
Empire .....	4.140
Shadow Credentials .....	5.84
Silver Ticket .....	5.14-15
Trust .....	5.68
Rundll .....	3.24, 25, 3.126
Running .....	4.22, 4.38, 4.47, 4.60, 4.66, 4.72, 4.96, 4.98, 4.106, 4.108, 4.117-121, 4.130, 4.140, 141, 4.157, 4.180
Rusty .....	2.85

## S

S4U2PROXY .....	5.33-39
S4U2SELF .....	5.33-39, 5.49
Sacrificial .....	4.136-138, 4.140
Sales .....	1.33, 1.69
sAMAccount → NoPac .....	
Satellite .....	2.93, 2.102
Scanning ...	1.14, 15, 1.17, 18, 1.94, 1.119, 1.123, 1.150
Schedule .....	3.124
Scheduled .....	4.98, 4.106, 4.108, 4.147, 4.174-177
Schtasks .....	3.82, 3.124, 4.175, 4.177
Screen .....	5.106, 107
Screen Capture .....	5.107
Scripting .....	3.9-11, 3.13, 3.15, 2.88, 3.128
Sct .....	3.11, 3.23
SCYTHE .....	2.33
Scythe .....	2.31, 2.33, 1.49, 1.65, 1.79, 5.140, 5.145
Sdbytes .....	5.46
Seconds .....	2.20
Secret .....	4.28
Section .....	4.1, 4.193
Segmentation .....	2.72, 2.74
Sendmail .....	2.66
Sensitive .....	1.11, 1.117, 118, 1.127
Service .....	5.8, 5.10, 5.13, 14, 5.16, 5.19, 5.24, 5.33-36, 5.38, 39, 5.41, 42, 5.49, 50, 5.57, 5.76, 5.81, 5.104, 5.108, 5.115
Serviceprincipalname .....	4.58
Session ....	4.23, 4.28-31, 3.69, 3.81, 3.87, 3.102, 3.115, 4.116, 117, 4.136-138, 4.141
Sessions .....	3.87
Set (Powershell COmmand) ...	3.5, 3.10, 3.16, 17, 3.23, 3.35, 36, 3.38, 5.42-47, 3.65, 5.65, 5.68, 3.71, 3.75, 5.76, 5.79, 3.82, 3.89, 5.94, 5.100, 3.102, 3.104, 3.106, 3.108, 3.122, 3.125, 5.142, 5.144, 5.148
Shadow Credentials Attack	
Execution .....	5.84
Pre-Requisites .....	5.83
Sharpmove .....	4.177, 4.189
Sharprdp .....	4.160
Sharpup .....	3.20, 3.86
SharpView .....	4.43
Sharpview ..	4.40, 4.43, 4.59, 4.62, 4.65, 4.68, 4.71, 4.76

# SEC565 – Red Team Operations

Shell .... 3.16, 17, 2.44, 3.48, 3.60, 3.64, 2.77, 78, 3.84, 3.89, 3.125

Shortcut ..... 3.25

Shortcuts ..... 3.25

SID ..... 5.14, 5.20, 5.45, 5.60, 5.65-67

Signing ..... 4.13, 4.31

Silver ..... 5.4, 5.13-15, 5.19, 20

Silver Ticket ..... 5.13

Tools

- Cobalt Strike ..... 5.15
- Empire ..... 5.15
- Mimikatz ..... 5.14
- Rubeus ..... 5.14

Simulator ..... 5.140, 5.142, 143

Singapore ..... 1.50, 1.53

Ski ..... 2.119

Sleep ..... 2.4, 2.14, 2.16, 2.19, 20, 2.40

Sliver ..... 2.29

Smb ..... 3.103, 3.106-108

SMB Connections ..... 4.99

Socat ..... 2.76, 2.86, 87, 2.93, 94, 2.96, 2.98, 5.113

Social ... 3.36, 3.38, 4.39, 3.40, 3.51, 3.84, 4.147, 4.150, 4.152, 153

Socks ..... 2.7, 2.78-80, 2.83, 84

Software ..... 4.0, 4.66, 4.98, 4.167, 4.182, 4.184

Spam ..... 2.60

Spear Phishing ..... 2.62, 1.64

- Initial Access ..... 1.75
- Through Link ..... 2.50
- Through Service ..... 2.51
- With Cobalt Strike ..... 2.32

SPN

- Setting Up ..... 5.76

Spoof ..... 3.103, 104, 3.106-108

SQL ..... 5.63, 5.91, 5.93, 94, 5.96, 97, 5.99-101

- Priv Esc ..... 5.63

SQLmap ..... 5.91, 5.97, 98

SSH ..... 5.5, 2.16, 2.76-79, 2.83, 84, 5.108, 5.113

SSHUTTLE ..... 2.76, 2.81

Stack ..... 2.56

Standards ..... 1.56

Standin ..... 5.45, 5.47, 48

Stands ..... 4.175

Starter ..... 4.9, 10

Static Analysis ..... 3.134

- Bypass ..... 3.135

Steal ..... 4.120, 4.127, 128, 4.132

Stealing ..... 3.93

Steals ..... 4.134

Storage ..... 3.37

Strategic ..... 5.130, 5.136, 137

Strike . 5.9, 5.12, 5.15, 5.18, 5.21, 5.31, 5.40, 5.48, 5.51, 5.62, 5.68, 5.107

String ..... 4.169, 170

Subject ..... 5.0, 5.54, 55

Subnet ..... 2.81

Sudo ..... 3.88

Supply ..... 3.41, 3.44, 45, 3.52

Supply Chain Compromise ..... 2.52

Svchost ..... 4.117, 4.119, 120

Sys ..... 2.118

## T

Tabletop Exercise .. 3.2, 4.2, 5.2, 1.14, 1.23, 1.30, 3.69, 5.93, 94, 5.99

Tabletop Exercises ..... 1.23

Tactical ..... 5.130, 5.136, 137

Tactics, Techniques, and Procedures → TTPs .....

Targetname ..... 4.70

Task ..... 2.39, 2.44, 45

Tasklist ..... 4.117, 4.121

Tasks ..... 2.6, 2.19

TCP .. 2.7, 2.11, 2.41, 1.77, 2.79, 80, 2.85, 86, 2.96-98, 1.132

Template ..... 5.54, 55

TGS ..... 5.8, 5.13, 5.23, 24, 5.34, 5.36

Threatsims ..... 2.119

Tiber ..... 1.50, 1.52, 1.67, 1.95

Ticket .. 5.8, 5.11, 5.13-15, 5.19-21, 5.24, 4.27, 4.29-31, 5.33-36, 5.39, 5.49, 5.67, 68, 4.136, 137, 4.141

Tier ..... 2.14-16

Timeline ..... 5.125, 5.132

Timestamp ..... 4.28, 29

Tmp ..... 2.82

Token . 4.20, 4.34, 4.117, 4.120, 4.126-130, 4.132, 4.134, 135, 4.138, 4.140, 4.163

Tokenvator ..... 4.120, 121

Toolkit ..... 5.101

Toolset ..... 2.31

Tracker ..... 1.148, 149

Trackers ..... 1.148

Tracking ..... 1.81

Traffic ..... 2.11, 2.18-20, 2.30, 2.58, 2.61, 62, 2.73-75, 2.77-79, 2.81, 2.85, 2.93, 2.95, 2.97, 2.99, 100, 2.102-104, 2.110-112, 2.121

Training ..... 5.131

Transitive ..... 4.14-17

Tree ..... 4.14, 15, 4.17

Trending ..... 5.135

Tresotingl ..... 3.32

Trust . 4.14-17, 4.37, 5.41, 5.64-68, 4.69, 5.69, 4.70, 71, 5.82, 5.91, 5.100

Trustdirection ..... 4.70

Trusted ..... 3.14, 3.22, 3.44, 45, 3.53

Trustedtoauth ..... 5.37

Trusts ..... 4.4, 4.14-17, 4.37, 4.39, 4.69

TTPs 1.22, 1.34, 1.37, 1.64-66, 1.73, 74, 1.88, 1.90, 91, 1.94, 4.189

Tuition ..... 5.151, 3.156

Tunneling ..... 5.143

## U

UAC ..... 5.6, 3.21, 3.83, 84

# SEC565 – Red Team Operations

---

UDP .....	2.11, 2.79, 2.94, 95, 2.98
Unattended .....	3.95, 96
Unconstrained .....	5.22-27, 5.29-33, 5.35-37, 5.45, 5.69
Unicorn .....	3.26
URL .....	3.22, 3.34, 3.36, 3.40
USB .....	3.34, 3.37, 3.44
User-Agent	
Configurations .....	2.116
Username .....	5.17, 5.20, 5.44, 5.96

## V

Variant .....	5.10, 5.41
VBA .....	3.10, 3.13, 3.15, 3.17, 3.133
VBscript .....	3.10, 11, 3.13, 3.22
VECTR .....	5.126, 127, 5.131-135, 5.149
Heat Map .....	5.134
Summary .....	5.133
Test Cases .....	5.126, 5.132
Trends .....	5.135
Vishing .....	4.152
Voice .....	1.30, 1.152
VPN .....	2.105, 2.108, 2.121
Vulnerability .....	1.14-19, 1.31, 1.35, 1.71, 1.88, 1.94, 1.99, 1.114, 1.123
Vulnerability Assessments .....	1.18
Vulnerability Scanning .....	1.17

## W

Wargaming .....	1.23
Web Applications .....	2.47
Webshells .....	2.48

wget .....	2.76, 2.84, 2.116
whoami .....	4.24, 25, 4.99, 4.101, 4.163
Why Red Team .....	2.29
Cognitive Biases .....	2.33
Focus on Stealth .....	2.37
Holistic View of an Org .....	2.32
Motivation .....	2.31
Test	
People .....	2.34
Process .....	2.34
Technology .....	2.34
Train & Improve Blue Team .....	2.36
What is Red Team .....	2.30
WinNT .....	4.105
WinRM .....	4.154, 4.161-163
WMI ...	3.20, 4.117, 118, 4.154, 4.166, 4.168, 4.184-187
Event Subscription .....	3.128
Persistence .....	3.120
Powershell .....	3.75
WMI Ops .....	3.74
WMIC .....	4.165
Account Discovery .....	3.65
Discovery .....	3.71-73
Path Hijacking .....	3.80
Process Discovery .....	3.66
Service Discovery .....	3.67
Weak File Perms .....	3.82
Wrapping	
Bypass .....	2.119

## X

XML .....	3.14, 3.96
-----------	------------