

Topics

Ransomware

(Not)Petya	1–31
Cerber	1–31
Crysis	1–31
Goldeneye	1–31
HDDCryptor	1–31
Jigsaw	1–31
LeChiffre	1–31
Locky	1–31
Petya	1–31
Popcorn Time	1–31
Sage	2–109
Wcry	1–31

Malware

Agent.BTZ	1–50
Angler	2–6, 2–58
BlackEnergy	1–44–45, 2–120
Carbanak	1–19
Carberp	1–19
Citadel	1–17
Dridex	1–17, 1–21
EternalBlue	1–47
EternalRomance	1–47
KillDisk	1–45
liboradb.dll	1–26
NotPetya	1–46–47
Rig	2–6, 2–58
s7otbxdx.dll	1–42
Shamoon	3–137
SpyEye	1–17
Stuxnet	1–34–43
Sundown	2–58
Terror	2–58
Turla	1–50
Zbot → Zeus	
Zeus	1–18
ZitMo	1–18

MetaSploit

exploit/	
multi/handler	W–8
post/windows/gather/	
enum_ad_computers	W–19
enum_applications	W–19
enum_files	W–19
post/windows/local/	
persistnce/	3–141
registry_persistence	3–141

Assembly

JNZ	1–26
NOP	1–26
POP	2–109
PUSH	2–109
RET	2–109
TEST	1–26

XCHG	2–109
XOR	1–26
ESP	2–109
RSP	2–109
ZF (Zero Flag)	1–26

Microsoft Security Bulletin

MS10-046	1–37
MS10-061	1–37, 3–151
MS10-073	1–38
MS10-092	1–38
MS14-025	4–49
MS17-010	1–46

Windows API

CreateThreat	2–119
RtlMoveMemory	2–119
ShellExecute	2–117
URLDownloadFile	2–117
VirtualAlloc	2–119

PowerShell

Get-ChildItem	5–36
Get-ExecutionPolicy	2–135
Invoke-Command	5–36
Invoke-Expression	2–135
Start-Transcript	2–155
Test-Connection	2–133
Write-Host	2–134

EventId

106	3–139
140	3–139
141	3–139
4104	2–159
4624	4–107, W–314
4634	4–107
4648	4–114
4657	3–142
4672	4–107
4688	4–117, 2–152
4689	4–117
4697	3–145
4728	5–22
4768	5–24
4769	4–105
5137	5–27
5140	5–40
5141	5–27

#

1-Day Exploit	3-50
802.1AE-2010	2-32
802.1X	2-24, 2-27, 2-33
802.1X-2010	2-32
%TEMP%	2-123
%SYSVOL%	4-50

A

Active Defense Harbinger Distribution (ADHD)	4-125
Active Directory	4-6
Admin Levels	4-14
Architecture	4-9
Authentication	4-7
Authorization	4-7
Backup	5-4
Database	4-13
Identification	4-7
Persistence	5-3
Backup files	5-3
Golden Ticket	5-9-11, 5-24
Impersonation	5-18, 5-27
New user	5-7, 5-22
Replication	5-16, 5-26
Skeleton Key	5-14, 5-23
Tiered Admin	4-30
Trust	4-20
Users and groups	4-14, 4-27
Local users and groups	4-32
ActiveX	2-104, 2-106, 2-109, 2-111, 2-125
Address Space Layout Random. (ASLR) ...	3-70, 3-78
Bottom-Up ASLR (BASLR)	3-101
Mandatory ASLR (MASLR)	3-101
AddressOfFunction	3-100
ADHD → Active Defense Harbinger Distribution	
Admin Approval Mode	4-36-37
ADMX Template	1-109
ADS → Alternate Data Stream	
Adversary Emulation	1-65
AFL → American Fuzzy Loop	
AIL	1-151
Alert Fatigue	5-103
AlienVault OTX	5-79
Alternate Data Stream (ADS)	2-131
American Fuzzy Loop (AFL)	3-40
AMSI → Antimalware Scanning Interface	
Anonymous	4-57
Ansible	1-111
Antimalware Scanning Interface (AMSI)	2-144
Anunak	1-19
Apache	3-135
AppArmor	2-90
Application Blacklisting	2-89, 2-99
Application Whitelisting	2-89, 3-138
AppLocker	2-90, W-101
Bypass	W-111

Category	2-93
Configuration	2-93, W-101
Event logs	2-96
GPO	W-104
Rule	2-94-95
Service	2-92
AppVerifier	3-31
APT Groups	1-56
APT Simulator	1-82
APT28	3-140, 3-146, 3-154
APT29	3-149, 3-169
APT30	3-140
Artillery	4-131
ASLR → Address Space Layout Randomization	
ASR → Attack Surface Reduction	
Assembly, example (liboradb.dll)	1-26
AssemblyLine	5-138, 5-150
Atomic Red Team	1-84
Attack Surface Reduction (ASR)	3-110
AutoPlay	2-16
Autopsy	5-138, 5-146
AutoRun	2-16
Autoruns	3-158-160, W-196
Awareness	3-7-9

B

Bangladesh Heist	1-17, 1-21
Fraud	1-29
Intrusion	1-25
Malware	1-26-28
Takeaways	1-30
Banking Trojan	1-18
Base64	2-118
Basic	2-103
BASLR → Bottom-Up ASLR	
Beaconing	3-177
beRoot	W-243
BeRoot.exe	4-51
Binary Scrambling	3-126
BinDiff	3-65
BlackEnergy	1-44-45
BloodHound	4-85-87, W-271
Deception	4-137
Prevention and detection	4-88
Blue Team	1-70
Bootkit	3-153, 3-155
Box	5-50
Bro	5-61, 1-96
Bromium vSentry	3-125
Bug Bounty	3-29
BYOD → Bring-your-own-device	2-27

C

C99	3-135
Cabinet File Content	3-56

SEC599 – Defeating Advanced Adversaries

Caldera	1-85
Canary	4-127, 4-134
BloodHound	4-137
Domain Administrator	4-137
Fake Administrative Accounts	4-135
Fake documents	4-139
Honeyhash	4-136
Tools	4-140
Canarytoken	4-140-144
Capability	5-67
Carbanak	1-17, 1-19, 3-143
CCleaner	1-46
Censys	1-157
CERT	5-122
Certificate	5-45
CertStream	1-157
CFG → Control Flow Guard	
CFI → Control Flow Integrity	
China Chopper	3-134
CIRCLearn	2-22
CIRT	5-122-123
CIS Controls	1-88
Cisco Umbrella	1-91
Client Isolation	1-101
Cloudflare	1-93
Cobalt	3-141
Code analysis	3-31
Dynamic	3-11
Static	3-10, 3-32
Code Coverage	3-40
CodeSearchDiggity	3-32
COM Object Hijacking	1-52
ATT&CK	1-79
COM Search Order	1-52
Phantom COM	1-52
Command & Control	3-165
Detection	3-172
Prevention	3-171
Command-Line Logging	2-152
Common Information Model (CIM)	3-149
Compound File Binary Format → OLE	
Control Flow Guard (CFG)	3-70, 3-84
Control Flow Integrity (CFI)	3-87
Control Panel Item	1-19
CopyKittens	3-137
CoreImpact	3-50
Cortex	5-138, 5-152
Cowrie	4-132
CPM → Control Panel Item	
CRC32	1-38
Credential Guard	4-59, 4-66, 4-74
Architecture	4-74
Remote	4-80
vs. Keylogger	4-79
vs. Pass-the-hash	4-78
Credential Theft	4-55
Access Token	4-56
BloodHound	4-85

Cached credentials	4-58
Finding where	4-85
LSASS Memory	4-59
Prevention	4-68
Credentials leaks	1-145
Crypto-mining	1-32
CScript → Windows Script Host (WSH)	
Cuckoo	2-67
Architecture	2-68
Installation	2-72
Reporting	2-69
Signature	2-71
CVSS	3-19
Cybercrime	1-15, 1-17

D

DarunGrim	3-65
Data Execution Prevention (DEP)	3-70, 3-79
Data Exfiltration	5-31
Behavior-Based Detection	5-58-61
Bro Exfil Detection	5-61
Collect	5-33, 5-48
Exfiltrate	5-33, 5-49, 5-63
Exfiltrate prevention	5-56
Network protocols	5-53
Online Storage	5-50-51
Print	5-62
Search	5-32, 5-34
Search detection and prevention	5-40
Signature-Based Detection	5-57
Tools for searching	5-36-38
Yara	5-39
Data Exfiltration Framework	1-100
Data Loss Prevention (DLP)	5-56
Data Offline	5-43-45
DCOM	3-149
DCShadow	5-18-20, 5-27
DCSync	5-16, 5-26
Deception	4-126, 4-146
Decoy	4-126, 4-146
File	5-47
Deep Panda	3-134
Demiguise	2-112
Denial of service	1-15
DEP → Data Execution Prevention	
Detecting Attacks	
Complexity	5-104
Real-Time	5-101
Statistics	5-105
vs. Hunting	5-107
Detection	1-115
Device driver 🌈	1-40
Device Guard	2-60
DIAMETER	2-24
Diaphora	3-65
DigiNotar	5-46
Directory Replication Service Remote (DRSR) ...	5-17



SEC599 – Defeating Advanced Adversaries

DKIM	2–6
DKIM → Domain Keys Identified Mail	
DLL	
liboradb.dll	1–26
LNK loading	1–37
Patching	1–26
payloadrestrictions.dll	W–184
scobj.dll	2–99
Search Order Hijacking	3–146-148
DLP → Data Loss Prevention	
DMARC → Domain-Based Message Authentication, Reporting and Conformance	
DNS	
Exfiltration	5–53, 5–60
Securing Traffic	1–93
Traffic pattern	1–98
Domain	5–74
Domain anomaly detection	3–174
Domain Fronting	3–167
Prevention and detection	3–168
Domain Keys Identified Mail (DKIM)	2–52
Domain-Based Message Authentication, Reporting and Conformance (DMARC)	2–6, 2–54
DownDelph	3–146, 3–154
DREAD	3–19, 3–27
DropBox	5–50, 3–170
DropSmack	3–170
DRSR → Directory Replication Service Remote	
DuckHunt	2–18
Duqu	3–111
Dynamic Base	3–70, 3–78

E

EAF → ExploitGuard, Export Address Table Filtering 3–100	
EAP	2–24
EAP Over LAN (EAPoL)	2–24
EAP-IKEv2	2–24
EAP-PSK	2–24
EAP-PWD	2–24
EAT → Export Address Table	3–100
ECMAScript	2–103
EDR → Endpoint Detection & Response	
EE-Outliers	1–116
ElasticSearch	1–116
Security	1–117
ElasticStack	1–116
EMET	3–92, 2–119
Attack Surface Reduction (ASR)	3–110
Bypasses	3–119-121
Caller Check	3–107
MemProt	3–106
Empire	1–81, 2–139, W–207
ENDBR32/ENDBR64	3–87
Endpoint Detection & Response	1–139
ESE → Extensible Storage Engine	4–13
Espionage	1–15, 1–49

EVE JSON	1–99
Event log	
AutoRun	3–160
EventID	4–113, 1–120
Mapping to ATT&CK	1–122
EventLog	4–113, 1–119-121
Forwarding	1–123
What to collect?	1–132
eventvwr.msc	1–119
EVT(X)	1–119
eXecute Disable (XD)	3–79
Exploit Kit	2–58
Behavior	2–60
Defense	2–60
Exploit Mitigation Controls	3–70
Summary	3–88
ExploitGuard	3–92
Arbitrary Code Guard	3–106
Block Low Integrity Images	3–117
Block Remote Image	3–104
Block Untrusted Fonts	3–111
Bypasses	3–119
Code Integrity Guard	3–110
Configuration	3–96-97
Core Isolation and Memory Integrity	3–118
Disable Extension Points	3–113
Disable Win2k System Calls	3–114
Do not Allow Child Processes	3–115
Export Address Table Filtering	3–100
GUI	3–95
Import Address Filtering (IAF)	3–101
Inner working	3–94
Load Library Protection	3–104
SimExec	3–108
Validate API Invocation	3–107
Validate Handle Usage	3–112
Validate Heap Integrity	3–105
Validate Image Dependency	3–116
Validate Stack Integrity	3–108, 109

F

Fenrir	2–30
File Extension	
Association	2–114
Blocking	2–98
Double extensions	2–17
File upload	
Bypass protection	3–135
FileBeat	W–362
FireGlass	2–63
Firewall	1–103
Flare	3–177-179
FlashFlood	3–140
Flightsim	1–83
Flow data	3–177
Footprint	1–143
Assessment	1–148



SEC599 – Defeating Advanced Adversaries

Technical	1-146
Form grabbing	1-18
Fortify	3-10, 3-32
freq.py	3-174
Full Packet Capture	1-95
Fuzzing	3-11, 3-33
Intelligent Mutation	3-39
Mutation	3-38
Randomized	3-37
Static	3-36
FxCop	3-31

G

GateKeeper	2-90
GDR → General Distribution Release	3-53-54
Global Offset Table (GOT)	3-101
Golden Ticket → Kerberos	
Google Chrome	1-110
Google Drive	5-50
Google Search Operators	1-149
GoPhish	2-10
GOT → Global Offset Table	
GPO	
AppLocker	W-104
Group Policy Management	W-28
SMB Signing	W-76
SysMon	W-132
User Account Control (UAC)	4-36-39
Grok	1-118
GroundBait	3-146
Group Managed Service Accounts	4-107
Group Policy Directory	4-6
Group Policy Preference	4-49-50
GRR	5-138, 5-147-150

H

Hammertoss	3-169
Hardening	1-104
Browser	1-109
Checklists	1-105
Hardware Security Module (HSM)	5-45
Hash	5-72
HashCat	5-6, 2-41
Heap Spray Protection	3-99
HoneyBadger	4-130
Honeyhash	4-136
Honeypot	4-127, 128, 4-133
Artillery	4-131
Cowrie	4-132
HoneyBadger	4-130
Kippo Fake SSH	4-132
HSM → Hardware Security Module	
HSTS → HTTP Strict Transport Security	3-168
HTA → HTML Application	
HTML Application	2-103, 2-112

Defense	2-113
HTTP Service Name Indication (SNI)	3-168
Hunting	5-118

I

IAF → Import Address Filtering	
IAT → Import Address Table	
ICMP Exfiltration	5-53
Identity Theft	2-56
IDS	1-96
Host-based	1-103
Impact	5-67
Impersonation	4-17
Import Address Table (IAT)	3-101
Incident Response	5-121, 5-137
Containment	5-133
Eradication	5-134
Identification	5-132
Lessons Learned	5-136
Motivation	5-124
OODA	5-126
Playbooks	5-130
Preparation	5-127-129
Process	5-125
Recovery	5-135
Tools	5-138, 5-154
Incognito	4-56-57
Indirect Branch Tracking	3-87
Instagram	1-54
Installutil.exe	2-99
Intent	5-67
IOC scanner	5-89
IP	5-73
IPS	1-96
IRMA	5-152
Ivanti	3-45

J

JA3	3-176, W-220
JavaScript	2-103
Javelin AD	4-140, 4-145
JEA → Just Enough Admin	
JHUHUGIT	3-140
John	W-4
John the Ripper	5-6
JScript	2-103
Downloader	2-109
Dropper	2-110
Just Enough Admin (JEA)	4-28-29

K

Kali	4-124
Kansa	5-138, 5-153
Kerberoast	W-285
Kerberos	4-10-11
AS-REQ	4-96



Attack	4-101, 4-106, 4-108
Details	4-92
Encryption types	4-94-95
Fallback	2-36
Golden Ticket	5-9-11
Mimikatz	5-12
Kerberoasting	4-101-102
Kerberoasting (Defense)	4-105
Kerberoasting (Tools)	4-104
Keys	4-100
Over-pass-the-hash	4-108
PAC	4-97
PAC Validation	4-99
Pre-authentication	4-96
Silver Ticket	4-106
Silver Ticket (Defense)	4-107
Skeleton Key	5-14
ST (Service Ticket)	4-98
TGT (Ticket Granting Ticket)	4-97
Keyboard Layout 🇺🇸	1-38
Keylogging	1-18
Kibana	W-42, 1-116
Dashboard	W-376
Security	1-117
Visualization	W-372
Kill Chain	1-66
Limitations	1-67
Unified	1-68
KillDisk	1-45
Kippo Fake SSH	4-132
klist	5-25
KolideFleet	1-137, W-363

L

LAPS → Local Administrator Password Solution
Lateral Movement	4-3
Detection	4-115, 4-118, 4-121, 122
M\$ Advanced Threat Analytics (MATA)	4-122
Scenario	4-3
Sigma	4-118
Zeek	4-121
Lazarus	3-140, 3-143
lcamtuf	3-40
Least Privilege	4-24-26
Link-local Multicast Name Resolution (LLMNR)	2-36, W-79
Linkos Group	1-46
LLMNR → Link-local Multicast Name Resolution
LNK files	1-37
.local file	3-148
Local Administrator Password Solution (LAPS)	4-33
LogStash	1-116
Configuration	W-38
Configuration and Parsing	1-118
Loki	5-89, W-357
CLI	5-91-92
Log	5-96

Output	5-93
Scoring	5-90
Lookaside Lists	3-105
Lookyloo	2-65
Low Fragmentation Heap (LFH)	3-105
LSASS	4-17, 4-56
Process tree	5-143-144
Protected Process	W-262
Lumension	3-49

M

Macro Content	2-128
Macros, blocking	2-98
MACsec	2-32
Mail Spoofing	2-57
Malware Traffic Analysis	2-60
Malwarebyte	3-122
Conflict with EMET	3-124
Man-in-the-browser	1-18
Mandatory Integrity Control (MIC)	3-117
.manifest file	3-148
Mark-of-web	2-131
Market Share	
Browsers	3-43
Operating Systems	3-42
MASLR → Mandatory ASLR
MassScan	1-153
Master Boot Record	1-46
Master Boot Record (MBR)	1-31, 3-153
MATA → Microsoft Advanced Threat Analytics	4-122
MBAE → Malwarebyte
MBR → Master Boot Record
MDM	2-33
MDM → Mobile Device Management
MEDoc	1-46
MemGC	3-70
Memory Forensics	5-141-145
MetaSploit	W-7, 1-81
UAC Bypass	4-40
MIC → Mandatory Integrity Control	3-117
Micro-Virtualization	3-125
Microsoft Advanced Threat Analytics (MATA)	4-122
Microsoft Intune	2-90
Mimikatz	4-60-63, W-228
Deception	4-136
Detection	4-116
Dump credentials	W-254
Golden Ticket	5-12
Pass-the-hash	4-66
Remove Protected Process	W-265
Skeleton Key	5-14
MISP	5-81-87
MITRE ATT&CK	1-78
Navigator	1-80
Mobile Device Management (MDM)	2-28, 2-90
Mobile Transaction Authentication Number	1-18
msfvenom	W-5

SEC599 – Defeating Advanced Adversaries

mshsta.exe	2-112
mTAN→ Mobile Transaction Authentication Number	
MZ	2-80

N

NAC → Network Access Control	
NBT-NS → NetBios NameServer	
NetBios NameServer (NBT-NS)	2-36
Netflow	1-95
Network Access Control (NAC)	2-23
Bypass	2-29-31
Network Artifacts	5-75
Network Flight Simulator→ Flightsim	
Network Monitoring	1-94
Network Segmentation	1-101
NIST Checklists	1-105
NOSTRO/VOSTRO	1-22
Not Executable (XD)	3-79
NotPetya	
Attack chain	1-47
NSM (Network Security Monitoring)	1-96
ntds.dit	5-4
Extraction tools	5-5
ntdsxtract	5-5
NTLMv2	4-12, 2-34
Challenge	2-35
NTOWF → NTLM One-Way Function	4-13
NX Bit	3-79
NXDOMAIN	1-93
NXLog	1-123
nxLog	
Configuration	W-129

O

Obfuscation	2-107, 2-138
OCTAVE	3-19
OLE	2-120
oledump.py	2-120
OneDrive	5-50
OpenDNS	1-93
Operation BlockBuster	3-143
Opportunity	5-67
OSQuery	1-135, 3-161
Example	1-136
Kolide Fleet	1-138
Outlook	
Backdoor	1-51, 1-55
OVAL format	1-106

P

Paranoid Phish	2-74
Pass-the-hash	4-64-65
Mimikatz	4-66
Pass-the-ticket	4-67

PassiveDNS	1-93
Password	4-19
Paste sites	5-51, 1-150
Patch	
Binary Diffing	3-64
Binary Diffing (Example)	3-66-67
Uninstall	3-68
Patch Reverse Engineering	3-50
PatchClear	3-61
PatchDiff2	3-65
PatchExtract	3-60
Patching	3-44-45
Extraction Tool	3-53, 3-55
Microsoft Patch Distribution	3-49
Microsoft Patch Extension	3-51
Microsoft Patch Tuesday	3-46
PatchLink	3-49
Payload delivery	2-3
Prevention	2-6
Payload Execution	2-88, 2-151
PE	2-80
PE infection	W-6
Persistence	3-130
Bootkits	3-153
Detection	3-157
Prevention	3-156
Registry Manipulations	3-140
Strategies	3-133
Task Scheduler	3-137
Web Shells	3-134
Windows Management Instrument. (WMI)	3-149
Windows Service	3-143
Petya/NotPetya	3-137
Phishing	2-4-5
PingCastle	4-21
PKI	5-45, 46
PLC (Programmable Logic Controller)	1-33
Polymorphic Malware	2-127
Polyverse	3-126
PowerShell	2-103, 2-133
Constrained Language Mode	3-138, 2-143
.....	W-114, W-127
Encoded Command	2-137
Execution Policy	2-134-135
Hardening	2-141
Logs	2-157-158
Monitoring	2-154
Obfuscation	2-138
PE Injection	2-99
Script Block Logging	2-158
Suspicious Commands	2-160
Transcript	2-155
v2	2-146
Without PowerShell	2-147
PowerUp	4-51, 3-147, W-244
PowserSploit	2-133
Prevention vs. Detection	1-87
Prikormka	3-146




SEC599 – Defeating Advanced Adversaries

Print Spooler Service	1–37
Printer dots	5–62
Private VLAN	1–102
Privilege Escalation	4–45
Group Policy Preference	4–49–50
Service to System	4–56
Unattended files	4–48
Unquoted Path	4–46–47
Process Creation Logging	2–152
ProcFilter	W–147, 2–164
Configuration	2–166
Installing	2–165
Logs	2–168
ProjectSauron	3–137
Protected Domain Users	4–69
Protected Process	4–70, W–262
Bypass	4–72, W–265
Configuration	4–71
Mimikatz	4–72
Protected View	2–124, 2–129
Proxy	1–90
Proxy Cloud	1–91
PSHunt	5–116
PsLogList	1–119
Purple Team	1–71–73
vs. Red team	1–74
PwnPlug	2–29
Pyramid of Pain	5–71
Domain	5–74
Hash	5–72
IP	5–73
Network Artifacts	5–75
Tools	5–76
TTPs	5–77

Q

QFE → Quick Fix Release	3–53–54
Quad9	1–93

R

RADIUS	2–24
Ransomware	1–15
RDP 	1–31
Real Intel. Threat Analytics (RITA)	1–100, 3–175
Realtek	1–40
Red Team	1–70
ReflectivePick	2–147
Registry Manipulations	3–140
Prevention and detection	3–142
regsvr32.exe	W–111
Rekall	5–138, 5–147
Remsec	3–137
Responder	2–37, W–68, 4–138
ResponderGuard	4–138
Return Oriented Programming (ROP)	3–84

Reverse Engineering	3–50
RFC 3748 (EAP)	2–24
Right-To-Left-Override	2–17
Risk	5–67
Rita	W–221
RITA → Real Intelligence Threat Analytics	3–175
RomeoAlfa	3–140
Rootkit	1–40
ROP → Return Oriented Programming	3–84
Rotten Potato	4–56
RPC	1–41
Rubber Duck	2–18
RunAsPPL	4–71

S

Sabotage	1–15, 1–33
Safe Structured Except. Handl. (SafeSEH)	3–70, 3–80
Chain	3–81
SafeSEH → Safe Structured Exception Handling	
SAINTExploit	3–50
Sandboxing	2–66
Limitations	2–73
Stealth	2–74
SANS SIFT	5–138, 5–140
Satellite Connectivity	1–53
Scans.io	1–153
SCAP (Security Content Automation Protocol)	1–105
Scripting Languages	2–103
SCT (Security Compliance Toolkit)	1–108
PolicyAnalyzer	W–21
SDL → Software Development Lifecycle	
SEADADDY	3–149, 3–151
Seasponge	3–20
secretsdump	5–5
Security Architecture	1–89
Security Compliance Manager (SCM)	1–108
Security Cookie	3–86
Security Identified (SID)	4–15
SEHOP → Structured Exception Handling	
Overwrite Protection	
SELinux	2–90
Sender Policy Framework (SPF)	2–6, 2–49
Check	2–50
Limitations	2–50
Session Initiation Protocol (SIP)	3–33, 1–100
Shadow IT	1–147
Shadow Stack	3–87
Shamoon	3–137, 3–144
Shavlik	3–45
ShellCode	2–119
Shellter	W–5
Shodan	1–154
SID → Security Identified	
Siemens Step 7	1–33
Sigma	1–133
Kerberos RC4	4–120
Over-pass-the-hash	4–119



SEC599 – Defeating Advanced Adversaries

Silver Ticket → Kerberos	
Single Sign-On	2–40
Skeleton Key	W–319
Sleuth Kit	5–138, 5–146
Sliding Scale of CyberSecurity	5–109
SMB	
Exploit (ShadowBroker)	1–31
GPO for SMB Signing	W–76
Outbound	2–40
Relaying	2–34, 2–42
Defense	2–44
Responder	2–43
Signing	W–71
Defense	2–44
Traffic	4–121
Snake → Turla	
Snort	1–96
Software Development Lifecycle (SDL)	3–3–4
Agile	3–16
Design	3–9
Implementation	3–10
Motivation	3–5
Phases	3–6
Release	3–12
Requirements	3–8
Response	3–13
Selling the process	3–14
Training	3–7
Verification	3–10
Software Restriction Policies (SRP)	2–90, 2–97
Rules	2–97
Source code review	3–31
Spear-phishing	1–45
SPF → Sender Policy Framework	
SpiderFoot	W–57, 1–152
Splunk	1–115, 1–123
SRP → Software Restriction Policies	
SSL/TLS	
Fingerprinting	3–176
Interception	1–92
SSO → Single Sign-On	
Stack	
Allocation	3–73
Canary	3–86
Mitigation	3–77
Overflow	3–75–76
Shield	3–87
Stager	W–210
StarFighter Empire Launcher	2–110
Steganography	1–51, 1–55, 1–94
STIG (Security Technical Implem. Guide)	1–107
STL (Statement List)	1–42
STRIDE	3–4, 3–19, 3–26
Strider	3–137
Structured Exception Handling	
Overwrite Protection (SEHOP)	3–70, 3–83
Stuxnet	3–149
Infection	1–37

Malware	1–42
Persistence	1–40
Privilege Escalation	1–28
Subscription (Eventlog)	1–123
Suricata	1–97
Ruleset	1–98
SWIFT	1–21–24
Alliance software	1–26
Customer Security Program	1–30
SwiftOnSecurity	1–129
SysMon	1–124, 2–153
Configuration	1–128, W–131
Events	1–125
GPO	W–132
Installation	1–126
Malicious use	1–21, 1–25
Mapping to ATT&CK	1–130
SysMonSearch (Visualization)	1–131

T

TAHITI Methodology	5–112
Task Scheduler	1–38, 3–137
Prevention and detection	3–138
TFTP	3–35
The Hive	5–138, 5–151
Threat	5–67
Threat Hunting	
Automation	5–114
Hypothesis Definition	5–113
Logs	5–115
Maturity	5–108
Methodology	5–112
Success Factors	5–111
Visualization	5–117
vs. Detection	5–107
Threat Identification	3–24
Threat Intelligence	5–68, 5–97
Feeds	5–78
Levels	5–69
Operationalization	5–88
Where to find?	5–78
Threat Modeling	3–18
Tool (Microsoft)	3–20
ThreatCrowd	5–80
TLP	5–84
TLS → SSL/TLS	
Tools	5–76
TRIKE	3–19
Trust Center	2–125
Macro Settings	2–127
Protected View	2–130
Trusted items	2–126
TTPs	1–65, 5–77
TurboDiff	3–65
Turla	1–50
Two factor authentication	4–18



U

UAC → User Account Control
UAF → Use After Free
Unicode
URL Analysis 2-64
urlquery.net 2-64
urlscan.io 2-64
Urobuos→ Turla
USB Weaponized 2-5, 2-15
BadUSB 2-19
Prevention 🚩 🍏 2-21
Prevention 🍏 2-20
USBGuard 2-21
USBHarpoon 2-18
USBKill 2-21
Use After Free (UAF) 3-11, 3-99-100
User Account Control (UAC) 4-34
Bypass 4-40
GPO 4-36-39
Levels 4-34

V

VBA 2-115
Declare statement 2-116
Defense 2-124
Downloader and Dropper 2-117
ShellCode 2-119
VBE → VBScript Encoding
VBR → Volume Boot Record
VBS → Virtualization Based Security
VBScript 2-103
Downloader 2-106
Encoding 2-108
Obfuscation 2-107
VeraCode 3-32
Vericode 3-10
Virtualization Based Security (VBS) 4-74
VirusTotal 5-157
Visual Basic → VBScript
VisualCodeGrepper 3-32
Volatility 5-138, 5-141-145
Volume Boot Record (VBR) 3-153
Vulnerability 5-67
Vulnerability Assessment 3-28

W

WaaS → Windows as a Service
Watering hole 2-5
Web Proxy Auto-Discovery (WPAD) 2-39
Web Shells 3-134-135
Prevention and detection 3-136

wevtutil.exe 1-119
Windows Access Token 4-16-17, 4-56
Windows Architecture 4-73
Windows as a Service (WaaS) 3-47
Branches 3-48
Windows Defender Application Control (WDAC) 2-90
Windows Defender Device Guard 2-91
Windows Event Collector Service 1-123
Windows Management Instrumentation (WMI) 3-149
Event Consumers 3-150
Event Filter 3-150
FilterToConsumer Binding 3-150
Prevention and detection 3-152
Windows Remote Management (WinRM) 1-123, 3-149
Windows Script Host (WSH) 2-104
Disable W-120
Hardening 2-111
Windows Service 3-143
Accounts 4-103
Prevention and detection 3-145
Privilege Escalation to System 4-56
Windows SKU 2-91
Winlogbeat 1-123
WMI → Windows Management Instrumentation
Worm 1-37
WPAD → Web Proxy Auto-Discovery
WSH → Windows Script Host
WSO 3-135
WSUS 3-46

X

XD Bit 3-79
--------	------------

Y

Yara 2-76
Modules 2-82
Repository 2-84
Rule generator 5-154
Rules 2-78-81
Use 2-83
YaraGenerator 5-155
yarGen 5-155

Z

Zeek 1-100
Supported protocols 1-100
Zero Width Joiner 1-54
Zero-Day 1-36
ZScaler 1-91