

# FOR508 – Advanced Incident Response, Threat Hunting, & Digital Forensics

## Topics

<b>Incident Response Steps</b>	1–20-21
1. Preparation	1–20
2. Identification	1–20
3. Containment	1–21
4. Eradication	1–21
5. Recovery	1–21
6. Lessons Learned	1–21

### Service Name

DcomLaunch	1–76
LocalServiceAndNoImpersonation	1–76
LocalServiceNetworkRestricted	1–76
LocalServiceNoNetwork	1–76
netsvcs	1–76
NetworkService	1–76
RPCSS	1–76

### Windows Process

csrss.exe	1–77
explorer.exe	1–78
lsaiso.exe	1–78
LSASS.exe	1–79
ntoskrnl.exe	1–80
RuntimeBroker.exe	1–80
services.exe	1–77
smss.exe	1–77
svchost.exe	1–76
System	1–76
taskhostw.exe	1–79
userinit.exe	1–79
wininit.exe	1–78, 1–80
winlogon.exe	1–79, 80

### wmic

group	1–137
netuse	1–137
process	1–137
qfe	1–137
startup	1–137
useraccount	1–137

## #

\$STANDARD_INFORMATION	... 4–38, 4–154, 4–156
\$FILE_NAME	4–154, 4–157
\$DATA	4–168
\$logfile Operation Codes	4–186
\$UsnJrnl	4–187
Parsing	4–190
Reason Code	4–189

## A

### Account

Built-in accounts	2–83
-------------------	------

Enumeration	2–100
Logon Event	2–95
Tracking Administrator	2–85
Tracking Creation	2–87
Tracking Usage	2–73
Tracking Usage (RDP)	2–89
Usage (RDP)	2–91
AceHash	2–10, 2–24, 2–28
ACMRU	4–17
Active Defense	1–24
Admin Shares	2–134
Destination Artifacts	2–134
Source Artifacts	2–133
ADMIN\$	W-2.4–7
Advanced NTFS Journal Parser (ANJP)	4–192
Alternate Data Stream	1–67, 4–171
Amcache.hve	2–55
Parsing	2–57
AmcacheParser.exe	2–58
AMSI → Anti-Malware Scanning Interface	
Analysis Scenario	2–72
AnalyzeMFT	4–157, 4–163
ANJP → Advanced NTFS Journal Parser	
ANONYMOUS LOGON	2–83
Anti-Forensics	1–67, 4–119
Anti-Malware Script Obfuscation	2–170
Anti-Virus	
Bypass	1–67
Logs	2–156
AppCompatCache → Application Compatibility	
Cache	
AppCompatCacheParser.exe	2–54
Application Compatibility Cache	4–12, 2–52
Application Deployment Software	2–148
APT19	3–85
Archives (embedded timestamp)	4–39
Armoring	1–67
Artifacts	4–9
Account Usage	4–23
Browser Usage	4–24
Deleted file or File Knowledge	4–17
File Opening/Creation	4–14
Network	3–123
Network Shares	2–133
OS Unusual	1–74
Physical Location	4–19
PowerShell	2–145
Program Execution	4–12
PsExec	2–135-136
Remote Desktop Protocol (RDP)	2–130-132
Remote Service	2–141
Scheduled Tasks	2–142
USB or Drive Usage	4–20
WMI	2–143
at.exe	1–75, 1–101, 2–139
ATT&CK	1–43
Collection	1–45
Command and Control	1–45



# FOR508 – Advanced Incident Response, Threat Hunting, & Digital Forensics

---

Credential Access	1–45
Defense Evasion	1–45
Discovery	1–45
Execution	1–45
Exfiltration	1–45
Impact	1–45
Initial Access	1–45
Lateral Movement	1–45
Persistence	1–45
Privilege Escalation	1–45
Attack Lifecycle	1–36
Asset access and data exfiltration	1–39
High privileges lateral movement cycle	1–36
Initial Compromise	1–36
Low privileges lateral movement cycle	1–36
AutoRun	1–67, 1–97
AutoRunsc.exe	1–100, 101, 1–104, 105
AutoStart (ASEPs)	1–69

## B

BadRabbit	1–139
base64	W-1.4–9
Beacons	1–67
Behavior Detection Anomaly	1–81
BelgaSoft	3–39
Binary Padding	1–67
blks	2–42
Bloodhound	2–100
Browser	
Cache	4–24
Cookies	4–24
Flash & Supercookies	4–25
History	4–24
Search Terms	4–20
Session Restore	4–25
Brute-Force Password Attack	2–81
bstring.exe	3–193
BulkExtractor	3–43
bytehist	1–82

## C

Cached Credentials	2–24
Defense	2–27
cachedump	2–24
Cain	2–28
Certification Authority	1–62
Chat threads	3–37
CIM → Common Information Model	
cmd.exe	1–75
Code Injection	1–74, 3–134
Reflective	3–149
Review	3–159
Code Signing	1–62
Malware	1–64
Command Line Tracking	2–158

Common Information Model (CIM)	1–135
Compromise Type	1–55
Conficker	2–121
Containment	1–24
CozyDuke	3–101
CreateInstance	1–104
CreateRemoteThread	3–134, 135
creddump	2–10, 2–24, 2–28
Credential	
Attacks (evolution)	2–8
Availability	2–12
Harvesting	2–6
Credential Guard	2–9
CredSSP	2–9, 1–119
CRITS	1–49
Cyber Threat Intelligence	1–35, 1–53
CyberChef	2–171

## D

DarkComet	3–92
Data Encryption	4–120
dc3dd	3–18
Deep Panda	3–85
Defense Manipulation	1–67
densityscout	1–82, 1–84
Device Guard	2–9
Direct Kernel Object Manipulation (DKOM)	3–168
Directory Table Base (DTB)	3–50
DKOM → Direct Kernel Object Manipulation	
DLL Hijacking	
DLL Search Order Hijacking	1–102
DLL Side-Loading	1–102
Phantom DLL Hijacking	1–102
DLL Injection	1–67, 3–136
DLL Lists	3–140
Domain Protected User	2–9
Download.sqlite	4–11
Driver Acquisition	3–207
Driver Letter	4–21
DTB → Directory Table Base	
DumpIt	3–39
Dun and Bradstreet Rating	1–62
DWM	2–83

## E

E-mail Attachments	4–11
ECTXtract	2–183
EDR → Endpoint Detection and Response	
Endpoint Detection and Response (EDR)	3–29
Challenge	3–31
Importance	3–30
Memory	3–32
Enter-PSSession	1–117, 1–119
EPROCESS	3–50, 3–68, 3–168
Eradication Without Identification	1–22

# FOR508 – Advanced Incident Response, Threat Hunting, & Digital Forensics

---

Evasion .....	1-67
Event Log Explorer .....	W-2.3-1, 2-103, 2-183
Event Viewer .....	2-74
EventLog .....	2-64
Application .....	2-67
Clearing .....	2-123
Clearing (Selective) .....	2-126
Deletion .....	4-121
EventID .....	2-191
Extraction .....	2-183
Forwarding .....	W-3.4-11
PowerShell .....	2-185
Security .....	2-68
Security Event .....	2-69
Service .....	2-67
Summary .....	2-182
Tampering .....	4-121
Types .....	2-66
eventlogedit .....	2-126
eventvwr.exe .....	2-74
EVT .....	2-64
evtwalk .....	2-183
EVTX .....	2-64
evt_x_view .....	2-183
Executive Process Block .....	3-50

## F

F-Response .....	3-7
Acquire Memory .....	3-18
Agent Service .....	3-15
Attach Remote Drive .....	3-17
Enterprise .....	3-8
GPO .....	3-14
MSI .....	3-12
SIFT .....	3-39
Fast forensics .....	4-80
fgdump .....	2-10
File	
Delete .....	4-119
Download .....	4-11
Handle .....	3-111
Wiping .....	4-119
File System	
Journaling .....	4-182-185
Filename	
Hijacking .....	1-67
Filename .....	4-176
filter_windows .....	4-81
Firmware .....	1-67
fls .....	4-30, 4-48
foremost .....	2-42
Forensics (Remote) .....	3-4
Format-Wide .....	1-115
fr_ace	
add .....	3-16
mount .....	3-17
query .....	3-16

Frequent Compilation .....	1-67
FU Rootkit .....	3-170
fxsst.dll .....	1-103

## G

Get-Alias .....	1-115
Get-ChildItem .....	1-115
Get-LsaSecret.ps1 .....	2-29
Get-Process .....	1-115
Get-Service .....	1-115
Get-SvcFail.ps1 .....	1-100
Get-WinEvent .....	2-185
Get-WmiObject .....	1-104, 1-140
GlassRAT .....	1-100
Golden Ticket .....	2-31, 2-34
gpedit.msc .....	2-68
grep .....	3-194
Group Enumeration .....	2-100
Group Managed Service Account .....	2-9
GRR .....	3-7, 3-210
gsecdump .....	2-10, 2-13, 2-28

## H

Handle .....	3-111
Hashes .....	2-10
Defense .....	2-17
Hibernation Files .....	3-39, 3-43
Windows 10 .....	3-47
Hibernation Recon .....	3-43
hibr2bin .....	3-43
Hiding in Plain Sight .....	1-59
Historical Data .....	4-124
Hunting .....	1-29, 1-31-34
Automated to Manual .....	1-56
Steps (Roadmap) .....	1-54

## I

I/O Request Packet (IRP) .....	3-161
IAT → Import Address Table .....	
IDT → Interrupt Descriptor Table .....	
Import Address Table (IAT) .....	3-161
Incident Response .....	1-20-21
Remote .....	3-4
Team .....	1-32
Incognito .....	2-19, 1-119
Incognito mode .....	3-37
Index.dat .....	4-12, 4-17
Indicator of Compromise .....	1-38, 1-48
Atomic .....	1-38
Behavioral .....	1-39
Computed .....	1-39
Language .....	1-49
InInitializationOrderModule List .....	3-140
Inline API .....	3-161
InLoadOrderModule List .....	3-140
InMemoryOrderModule List .....	3-140

# FOR508 – Advanced Incident Response, Threat Hunting, & Digital Forensics

---

Intelligence Development .....	1-24
Internet Evidence Finder .....	3-43
Interrupt Descriptor Table (IDT) .....	3-161
Invoke-Command .....	1-117
IOC Analysis .....	3-212
IPRIP → RIP Listener Service .....	
IRP → I/O Request Packet .....	
istat .....	4-162, 4-173-175

## J

jobparser.py .....	2-115
jp .....	4-191
Jump List .....	4-13

## K

Kansa .....	1-120-129
3 <sup>rd</sup> party tools .....	1-126
Configuration .....	1-124
Get-AutoRunsc.ps1 .....	1-126
Get-CertStore.ps1 .....	1-126
Get-FlsBodyfile.ps1 .....	1-126
Get-Handle.ps1 .....	1-126
Get-LogparserStack.ps1 .....	1-127
Get-ProcDump.ps1 .....	1-126
Get-RekalPslist.ps1 .....	1-126
Remote .....	W-1.5-6
Kansa PowerShell Framework .....	1-104
KAPE .....	3-22
Collection .....	3-25
Options .....	3-23
KB2871997 .....	2-8
KDBG → Kernel Debugger Datablock .....	
KdCopyDataBlock .....	3-59
Kerberoasting .....	2-31, 2-34
Kerberos .....	2-96, 1-119
Attacks .....	2-34
Attacks (Defense) .....	2-38
Kernel Debugger Datablock (KDBG) .....	3-50
Identification .....	3-59
Kernel Patch Protection .....	3-164
Kernel Processor Control Region (KPCR) .....	3-50
Kill Chain .....	1-38
Actions on Objectives .....	1-41
Delivery .....	1-40
Exploitation .....	1-40
Persistence .....	1-40-41
Reconnaissance .....	1-40
kpartx .....	3-17
kpartx .....	W-3.1-16
KPCR → Kernel Processor Control Region .....	

## L

LAPS → Local Administrator Password Solution .....	
--	--

Last visited MRU .....	4-12, 4-15, 4-17
Lateral Movement .....	
Overview .....	2-5
Scheduled Tasks .....	2-112
Shares .....	2-106
Tracking .....	2-105
Least frequency of occurrence analysis .....	1-127
Link (soft and hard) .....	4-142
LiveSSP .....	2-10
Living off the Land Binaries (LOLbin) .....	1-60
LoadLibrary .....	3-134, 3-149
Local Account .....	2-95
Abuse .....	2-98
Local Admin (Limitations) .....	2-6-7
Local Administrator Password Solution (LAPS) .....	2-17
LOCAL SERVICE .....	2-83
Location: Internet Explorer .....	4-17
log2timeline .....	4-30, 4-60, 4-69
Arguments .....	4-70
Device examples .....	4-73
Parser lists .....	4-85
VSS .....	4-131

Logon .....	
Error Code .....	2-96
Event .....	2-95
Last .....	4-23
Session Identification .....	2-79
Success/Failure .....	4-23
Type .....	2-12, 4-23
Type Codes .....	2-77
LSA Secret .....	2-28
Defense .....	2-30
LSASS .....	2-10
Security EventLog .....	2-68

## M

MACB .....	4-35-36
mactime .....	4-68
MagnetForensics .....	3-39
Malware .....	
Code Signing .....	1-64
Dormant .....	1-55, 1-67
Evasion techniques .....	1-61
Execution .....	2-155
Fileless .....	4-120
Identification .....	1-81
Locations .....	1-59
Names .....	1-59
Paradox .....	1-53
Malware Persistence .....	1-68
AutoStart Locations .....	1-69
BIOS Flashing .....	1-96
DLL Hijacking .....	1-102
Local Group Policy .....	1-96
MS Office Add-in .....	1-96
Scheduled Tasks .....	1-101
Service Creation/Replacement .....	1-71-72

# FOR508 – Advanced Incident Response, Threat Hunting, & Digital Forensics

Service Failure Recovery .....	1-100
WMI Event Consumers .....	1-104
Managed Service Account .....	2-8
Master File Table (MFT) .....	4-147
File Record Header .....	4-152
Outlier .....	4-166
Sequential Entries .....	4-151
Structure .....	4-148
Memory .....	
Acquisition .....	3-39
Analysis .....	3-49
Analysis 🌈 .....	3-50
Compression .....	3-45
Dump .....	3-39
Finding the first hit .....	3-66
Forensics .....	3-35
Advantages .....	3-37
Motivations .....	3-36
Windows 10 .....	3-45
Offset .....	3-79
Page Execute ReadWrite .....	3-150
Virtual Machine .....	3-41
Metadata Layer .....	4-150
MetaSploit .....	2-10, 2-19, 2-24, 2-28, 2-39
MFT → Master File Table .....	
MFTECmd .....	4-30, 4-46, 4-157
Microsoft Online Accounts .....	2-79
Mimikatz .....	2-9, 10, 2-15, 2-20, 2-28, 2-32, 1-119
EventLog Clearing .....	2-126
MOF .....	1-141
MOF → WMI/MOF Files .....	
mofcomp.exe .....	1-104, 2-144, 1-150
mount .....	3-17
MountPoints2 .....	4-43, 1-75, 2-133
MsCash2 .....	2-24
mstsc.exe .....	2-130
Mutant .....	3-113
Mutex .....	3-113
MZ .....	3-152-154

## N

net.exe .....	1-75, 2-133
net1.exe .....	2-133
netstat.exe .....	1-115
NetTraveler .....	1-103
Network Artifacts .....	3-123
Review .....	3-129
Network History .....	4-20
NETWORK SERVICE .....	2-83
Network Shares .....	
Admin .....	2-133
Tracking .....	2-106
New-PSDrive .....	1-115
Nishang .....	2-29
NotPetya .....	1-139
NTDS.DIT .....	2-39
ntdsdump .....	2-39

NTDSXtract .....	2-39
NTFS .....	4-140
Alternate Data Stream .....	4-171
Features .....	4-142
File Deletion .....	4-195
File Write .....	4-194
Index slack space .....	4-180
System Files .....	4-144
Timestamp .....	4-36
NTLM .....	2-10
ntoskrnl.exe .....	3-161

## O

Office Recent Files .....	4-15
Open/Save MRU .....	4-11, 4-14
OpenIOC .....	1-49
Order of Volatility .....	1-124
Out-GridView .....	1-115
Overpass the Hash .....	2-34

## P

Packing .....	1-67
Page Directory Offset (PDB) .....	3-78
Page File .....	3-39
Pass-the-hash attacks .....	2-10
Mitigations .....	2-9
Pass-the-ticket .....	2-31, 2-34
Password .....	3-43
Password .....	
Last change .....	4-23
PatchGuard .....	3-164
PDB → Page Directory Offset .....	
PEB → Process Environment Block .....	
PECmd.exe .....	2-47
Perimeter .....	3-30
pescan .....	1-82, 1-87
Phishing Attack .....	4-98-100
pinfo .....	4-89
pinfo .....	4-60
Pivot .....	4-26-27
Places.sqlite .....	4-12
Plaso .....	4-60
Linux/Android/Mac Parsers .....	4-66
mactime .....	4-68
Registry Parsers .....	4-63
Web History Parsers .....	4-65
Windows Parsers .....	4-61
Plug-and-Play Event Log .....	4-22
PlugX .....	1-103
Poison Ivy .....	1-103
Ports .....	W-3.4-4
powercfg.exe .....	3-43
PowerShell .....	1-114
Authentication .....	1-119
Basics .....	1-115

# FOR508 – Advanced Incident Response, Threat Hunting, & Digital Forensics

Command History .....	2-176
Enabling logs .....	2-166
Log hunting .....	2-168
Logs .....	2-164
Malicious (logs) .....	2-167
Obfuscation .....	2-170
Processes .....	3-87
Remote Artifacts .....	2-147
Remoting .....	1-117
Source Artifacts .....	2-145
Transcript Logs .....	2-173-174
<b>powershell.exe</b> .....	1-75, 2-146
PowerView .....	2-100
Prefetch .....	4-13, 4-15, 2-42
First/Last Execution .....	2-45
From memory .....	4-137
<b>prefetchparser</b> .....	4-137
Privileged Local Account Abuse .....	2-98
Proactive Response .....	1-29
<b>ProcDump</b> .....	1-75
Process	
Acquisition .....	3-207
Analysis .....	3-70
Anomaly 🌈 .....	1-76
Environment Block (PEB) .....	3-50
Hollowing .....	3-135
Injection .....	1-67
Objects .....	3-94, 3-121
Process tree .....	3-33
Rogue .....	1-73
Terminated .....	3-80
Tracking .....	2-158, 2-160
Command Line .....	2-162
Profiling Account Usage .....	2-72
Protected Processes .....	2-9
PsActiveProcessHead .....	3-50
<b>PsExec</b> .....	2-10, 1-75, 2-121, 2-136
Destination Artifacts .....	2-136
Source Artifacts .....	2-135
<b>psxessvc.exe</b> .....	2-137
<b>PsLoggedOn</b> .....	1-75
<b>PsLogList</b> .....	2-183
<b>psort</b> .....	4-93
<b>psort</b> .....	4-60
<b>PspCid</b> .....	3-170
<b>PSReadline</b> .....	2-176
<b>PWDumpX</b> .....	2-24
<b>PWDumpX</b> .....	2-10

## Q

<b>qc</b> .....	1-74
<b>qprivs</b> .....	1-74
<b>qtriggerinfo</b> .....	1-74
<b>queryex</b> .....	1-74

## R

<b>rar.exe</b> .....	1-75
RasAuto .....	1-100
<b>rdpclip.exe</b> .....	2-132
Reactive Response .....	1-29, 1-31
Recent Files .....	4-14
RecentFileCache.bcf .....	2-55
Reconnaissance Tracking .....	2-100
Recycle Bin .....	4-18
<b>reg.exe</b> .....	1-75, 2-139
Registry	
Deletion .....	4-120
Hiding Data .....	4-120
RegRipper .....	1-98, 2-130
Rekall .....	1-130, 3-210
Remediation .....	1-27
Requirements .....	1-28
Steps .....	1-29
Remote Credential Guard .....	2-9
Remote Desktop Protocol (RDP)	
Logging .....	2-93
Source Artifacts .....	2-130
Usage .....	4-24
Remote Service Artifacts .....	2-141
Restricted Admin .....	2-9
RID 500 .....	2-7
rip.pl .....	W-3.1-18
Rogue Process Analysis .....	3-94
Rootkit .....	1-67, 1-74, 1-130
Detection .....	3-180
Hooking .....	3-161
Run MRU .....	4-14

## S

SACL → System Access Control List .....	
Sakula .....	1-103
SAM Registry Hive .....	2-10
<b>sc.exe</b> .....	1-74, 75, 1-100, 2-139
Scheduled Tasks	
Artifacts .....	2-142
Artifacts (v1.2) .....	2-115
Logs .....	2-114
Tracking .....	2-112
<b>schtasks.exe</b> .....	1-75, 1-101, 2-139
SCM → Service Control Manager .....	
<b>scrcons.exe</b> .....	3-87, 2-144, 2-180
Scripting .....	1-112
Bash .....	1-112
PowerShell .....	1-112
WMI .....	1-112
Search (Win7-10) .....	4-19
Search (XP) .....	4-17
Security Identifier (SID) .....	3-103, 3-107
Security Tokens → Tokens .....	
<b>SeDebug</b> .....	2-85
<b>SeImpersonate</b> .....	2-19
<b>Select-String</b> .....	1-115
Service Control Manager .....	2-119
Service Events .....	4-13



# FOR508 – Advanced Incident Response, Threat Hunting, & Digital Forensics

---

Service Hijacking .....	1-67
Service Replacement .....	1-67
Services .....	
Suspicious .....	2-119
Unknown .....	1-74
Set-WmiInstance .....	1-104
SeTakeOwnership .....	2-85
SetWindowsHookEx .....	3-135
Shell bags .....	4-15
ShimCache .....	2-51, 4-138
shimcachemem .....	4-138
Shortcut (LNK) files .....	4-15, 4-22
SID → Security Identifier .....	
sigcheck .....	1-82, 1-89
Silver Ticket .....	2-34
Skeleton Key .....	2-34
Skype .....	4-11
SMB .....	
File copy .....	4-43
SMBShell .....	2-10
SSDT → System Service Descriptor Table .....	
Stacking .....	1-127
Statistics (incident) .....	1-13
STIX .....	1-49
Strings .....	3-193
StuxNet .....	1-141, 3-147
Super Timeline .....	4-53
Creation steps .....	4-96
Filter .....	4-78
Output .....	4-105
Targeted .....	4-75
Suspicious Services .....	2-119
Swap File .....	3-39
SxS → DLL Hijacking/DLL Side-Loading .....	
SysMon .....	2-188
SYSTEM .....	2-83
System Access Control List .....	2-69
System Service Descriptor Table (SSDT) .....	3-161
SYSTEM32 .....	W-2.1-9
SYSWOW64 .....	W-2.1-9

## T

Target Collection .....	3-25
Task (Start time) .....	W-2.4-22
TDL3/TDSS .....	3-144
TeamViewer .....	2-131
Temporal proximity .....	4-26
Thumbnails .....	4-18
Thumbs.db .....	4-19
Tickets .....	2-31
Defense .....	2-36
Timeline .....	
Benefits .....	4-5
Comparison .....	4-30
Context .....	4-29
Filesystem .....	4-44
Process Analysis .....	4-32

Super Timeline .....	4-53
Utopia and Reality .....	4-5-6
Timestamp .....	4-35-36
Lateral Movement Analysis .....	4-43
Timestamp .....	1-67, 4-119
Detection .....	4-162
Evidence .....	2-51
Timezone .....	4-19
Tokens .....	2-19
Defense .....	2-22
Tracking .....	
Account Creation .....	2-87
Account Usage .....	2-73
Account Usage (RDP) .....	2-89
Command Line .....	2-158-162
Lateral Movement .....	2-105
Network Shares .....	2-106
Process .....	2-158-160
Reconnaissance .....	2-100
Scheduled Tasks .....	2-112
Triage .....	4-80
Filesystem Timeline .....	4-35
Trusted Code .....	1-62
TsPkg .....	2-9, 10
tstheme.exe .....	2-132

## U

UAC → User Access Control .....	
UMFD .....	2-83
USB First/Last Times .....	4-21
USB Key Identification .....	4-20
User Access Control (UAC) .....	2-8
UserAssist .....	4-14

## V

VAD → Virtual Address Descriptor .....	
Virtual Address Descriptor (VAD) .....	3-50
Virtual Secure Mode .....	3-45
VirtualAllocEx .....	3-135
Visibility .....	3-30
VNC .....	2-131
Volatility .....	3-43, 3-53
apihooks .....	3-163, 3-177
baseline .....	3-91
cmdline .....	3-99
cmdscan .....	3-184, 3-197-198
connections .....	3-125
connscan .....	3-125
consoles .....	3-184, 3-197-198
devicetree .....	3-172
dlldump .....	3-184, 185
dlllist .....	3-99, 100
driverbl .....	3-91, 3-175
driverirp .....	3-163
dumpfiles .....	3-184, 3-201
filescan .....	3-61, 3-184, 3-204

# FOR508 – Advanced Incident Response, Threat Hunting, & Digital Forensics

---

getsids .....	3-99, 3-103
handles .....	3-99, 3-110
hivelist .....	3-61
hollowfind .....	3-139
idt .....	3-163
imagecopy .....	3-43, 3-64
imageinfo .....	3-58
kdbgscan .....	3-59, 3-62
ldrmodules .....	3-139, 140
malfind .....	3-139, 3-151
malprocfind .....	3-73, 3-89
memdump .....	3-184, 3-192
moddump .....	3-184, 3-187
modscan .....	3-163, 3-172
modules .....	3-172
mutantscan .....	3-99
netscan .....	3-125, 126
openioc_scan .....	3-212
procdump .....	3-184, 3-191
processbl .....	3-73, 3-91
pslist .....	3-59, 3-61, 3-73, 74
psscan .....	3-61, 3-73, 3-78, 3-80
pstree .....	3-73, 3-82
psxview .....	3-163, 3-169
servicebl .....	3-91, 3-99, 3-119
sockets .....	3-125
sockscan .....	3-125
ssdt .....	3-163, 164
svcsan .....	3-99, 3-115
threadmap .....	3-139
vaddump .....	3-192
vainfo .....	3-201
Help .....	3-56
Image identification .....	3-61
Profile .....	3-60
Usage .....	3-54
Volume GUID .....	2-55
Volume Name .....	4-21
Volume Serial Number .....	4-22
Volume Shadow Copy .....	4-124
Examination .....	4-126
log2timeline .....	4-131
vshadowinfo .....	4-127
vshadowmount .....	4-128
VSM → Virtual Secure Mode .....	
VSSAdmin .....	2-39
Vulnerability .....	
Exploitation .....	2-150

## W

WannaCry .....	1-139
WBEM → Web-Based Enterprise Management .....	
WCE .....	2-10
WDigest .....	2-9, 10

Web Server Intrusion .....	4-97
Web-Based Enterprise Management (WBEM) ...	1-135
WebShell .....	1-67, 3-85
What is Evil? .....	1-73
What is Normal? .....	1-73
win32k.sys .....	3-161
Windows Remote Management .....	2-115, 2-139
Windows Service .....	1-71
RasAuto .....	1-72
RIP Listener Service (IPRIP) .....	1-71
Service Creation/Replacement .....	1-71-72
Windows Time Rules .....	4-38, 4-160-161
winpmem Driver .....	3-39, 1-130
winrm.vbs .....	1-75, 1-117
winrs.exe .....	2-139
wisp .....	4-180
WMI .....	1-112, 1-135
Attacks .....	1-136
Consumers .....	1-148
Database .....	1-146
Destination Artifacts .....	2-144
Event Consumer Backdoor .....	1-140
Event Consumers .....	1-104
Hunting .....	1-149
Investigation .....	1-142
Lateral Movement .....	1-139
Log Hunting .....	2-180
Logs .....	2-177
MOF Files .....	1-150
Persistence .....	2-177
PowerShell .....	1-144
Privilege Escalation .....	1-138
Processes .....	3-87
PyWMIPersistenceFinder.py .....	1-147
Source Artifacts .....	2-143
WBEM AutoRecover Folder .....	1-152
WBEM AutoRecover Key .....	1-154
wmic.exe .....	1-75, 3-87, 1-113, 2-143
wmiprvse.exe .....	3-87, 2-144
WordWheelQuery .....	4-19
WriteProcessMemory .....	3-135
WSMAN .....	1-117
wsmprovhost.exe .....	3-87, 2-147

## Y

Yara .....	1-50
------------	------

## Z

Zbot .....	3-178
Zero Configuration .....	1-67
Zeus .....	3-178
Zone Identifier .....	4-172