

# 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	1–109
netuse	1–109
process	1–109
qfe(KBpatch listing)	1–109
startup	1–109
useraccount	1–109

## #

\$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, 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
AutoRunsc.exe .....	1–79-80
AutoStart (ASEPs) .....	1–69

## B

BadRabbit .....	1–111
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
bytehyst .....	1–82

## C

Cached Credentials .....	2–24
Defense .....	2–27
MsCach2 .....	2–24
Security\Cache key .....	2–24
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, 1–67

Malware .....	1–63
Command Line Tracking .....	2–158
Common Information Model (CIM) .....	1–107
Compromise Type .....	1–55
Conficker .....	2–121
Containment .....	1–24
CozyDuke .....	3–101
CreateInstance .....	1–76
CreateRemoteThread .....	3–134, 135
creddump .....	2–10, 2–28
Local NT Hashes & Cached Hashes .....	2–24
Credential .....	
Availability .....	2–12
Harvesting .....	2–6
Credential Attacks mitigation .....	2–8
Credential Guard .....	2–9
Device Guard .....	2–9
Domain Protected User .....	2–9
Group Managed Service Account .....	2–9
KB2871997 .....	2–8
Managed Service Account .....	2–8
Protected Processes .....	2–9
Remote Credential Guard .....	2–9
Restricted Admin .....	2–9
User Access Control (UAC) .....	2–8
CredSSP .....	2–9
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
Direct Kernel Object Manipulation (DKOM) ..	3–168
Directory Table Base (DTB) .....	3–50
DKOM → Direct Kernel Object Manipulation .....	
DLL Hijacking .....	
DLL Search Order Hijacking .....	1–74
DLL Side-Loading .....	1–75
Phantom DLL Hijacking .....	1–75
DLL Injection .....	1–67, 3–136
DLL Lists .....	3–140
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
--------------------------	------



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

---

ECTXtract .....	2-183
EDR → Endpoint Detection and Response .....	
Endpoint Detection and Response (EDR) .....	3-29
Challenge .....	3-31
Importance .....	3-30
Memory .....	3-32
EPROCESS .....	3-50, 3-68, 3-168
Eradication Without Identification .....	1-22
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_xview .....	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 .....	1-88
fr_ace .....	
add .....	3-16
mount .....	3-17
query .....	3-16
Frequent Compilation .....	1-67
FU Rootkit .....	3-170
fxsst.dll .....	1-75

## G

Get-Alias .....	1-88
Get-ChildItem .....	1-88
Get-LsaSecret.ps1 .....	2-29
Get-Process .....	1-88
Get-Service .....	1-88
Get-SvcFail.ps1 .....	1-72
Get-WinEvent .....	2-185
Get-WmiObject .....	1-112
GlassRAT .....	1-71
Golden Ticket .....	2-31, 2-34
gpedit.msc .....	2-68
grep .....	3-194
Group Enumeration .....	2-100
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
Incognito mode .....	3-37
Index.dat .....	4-12, 4-17
Indicator of Compromise .....	1-38, 1-48
Atomic .....	1-38
Behavioral .....	1-39

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

Computed .....	1–39
Language .....	1–49
InInitializationOrderModule List .....	3–140
Inline API .....	3–161
InLoadOrderModule List .....	3–140
InMemoryOrderModule List .....	3–140
Intelligence Development .....	1–24
Internet Evidence Finder .....	3–43
Interrupt Descriptor Table (IDT) .....	3–161
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 .....	1–93–103
3 <sup>rd</sup> party tools .....	1–99
Configuration .....	1–95
Get-AutoRunsc.ps1 .....	1–99
Get-CertStore.ps1 .....	1–99
Get-FlsBodyfile.ps1 .....	1–99
Get-Handle.ps1 .....	1–99
Get-LogparserStack.ps1 .....	1–100
Get-ProcDump.ps1 .....	1–99
Get-RekalPslist.ps1 .....	1–99
Remote .....	W-1.5–6
Run .....	1–97
KAPE .....	3–22
Collection .....	3–25
Options .....	3–23
KDBG → Kernel Debugger Datablock .....	
KdCopyDataBlock .....	3–59
Kerberoasting .....	2–31, 2–34
Kerberos .....	2–96
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 .....	1–100
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) .....	2–18
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 .....	1–63
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 .....	1–78
DLL Hijacking .....	1–74
Local Group Policy .....	1–78



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

---

MS Office Add-in .....	1-78
Scheduled Tasks .....	1-73
Service Creation/Replacement .....	1-71
Service Failure Recovery .....	1-72
WMI Event Consumers .....	1-76
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, 2-28, 2-32
EventLog Clearing .....	2-126
Token Stealing .....	2-20
MOF .....	1-112
MOF → WMI/MOF Files .....	
mofcomp.exe .....	1-123, 2-144
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 .....	1-88
NetTraveler .....	1-75
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 .....	1-88
Nishang .....	2-29

NotPetya .....	1-111
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 .....	1-95
Out-GridView .....	1-88
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, 2-15
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
Persistence .....	1-68
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 .....	1-75
Poison Ivy .....	1-103
Ports .....	W-3.4-4

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

---

powercfg.exe .....	3-43
PowerShell .....	1-87
Authentication .....	1-92
Basics .....	1-88
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
Source Artifacts .....	2-145
Transcript Logs .....	2-173-174
PowerShell Authentication .....	1-92
CredSSP .....	1-92
Enter-PSSession .....	1-92
PowerShell Remoting .....	1-90
Enter-PSSession .....	1-90
Invoke-Command .....	1-90
WS-Management (WSMAN) .....	1-90
powershell.exe .....	1-75, 2-146
PowerView .....	2-100
Prefetch .....	4-13, 4-15, 2-42
First/Last Execution .....	2-45
From memory .....	4-137
prefetchparser .....	4-137
Privileged Local Account Abuse .....	2-98
Proactive Response .....	1-29
ProcDump .....	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
PsActiveProcessHead .....	3-50
PsExec .....	2-11, 1-75, 2-121, 2-136
Destination Artifacts .....	2-136
Source Artifacts .....	2-135
psxessvc.exe .....	2-137
PsLoggedOn .....	1-75
PsLogList .....	2-183
psort .....	4-93
psort .....	4-60
PspCid .....	3-170
PSReadline .....	2-176
PWDumpX .....	2-24
PWDumpX .....	2-10

## Q

qc .....	1-74
qprivs .....	1-74
qtriggerinfo .....	1-74
queryex .....	1-74

## R

rar.exe .....	1-75
RasAuto .....	1-72
rdpclip.exe .....	2-132
Reactive Response .....	1-29, 1-31
Recent Files .....	4-14
RecentFileCache.bcf .....	2-55
Reconnaissance Tracking .....	2-100
Recycle Bin .....	4-18
reg.exe .....	1-75, 2-139
Registry .....	
Deletion .....	4-120
Hiding Data .....	4-120
RegRipper .....	1-98, 2-130
Rekall .....	1-103, 3-210
Remediation .....	1-27
Requirements .....	1-28
Steps .....	1-29
Remote Desktop Protocol (RDP) .....	
Logging .....	2-93
Source Artifacts .....	2-130
Usage .....	4-24
Remote Service Artifacts .....	2-141
RID 500 .....	2-7
RIP Listener Service (IPRIP) .....	1-71
rip.pl .....	W-3.1-18
Rogue Process Analysis .....	3-94
Rootkit .....	1-67, 1-74, 1-103
Detection .....	3-180
Hooking .....	3-161
Run MRU .....	4-14

## S

SACL → System Access Control List .....	
Sakula .....	1-103
SAM Registry Hive .....	2-10
sc.exe .....	1-72, 1-74, 75, 2-139
Scheduled Tasks .....	1-73
Artifacts .....	2-142
Artifacts (v1.2) .....	2-115
at.exe .....	1-73
Logs .....	2-114
schtasks.exe .....	1-73
Tracking .....	2-112
schtasks.exe .....	1-75, 2-139
SCM → Service Control Manager .....	
scrcons.exe .....	3-87, 2-144, 2-180
Scripting .....	1-85
Bash .....	1-85
PowerShell .....	1-85



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

---

WMI	1–85
Search (Win7-10)	4–19
Search (XP)	4–17
Security Identifier (SID)	3–103, 3–107
Security Tokens → Tokens	
SeDebug	2–85
Select-String	1–88
Service Control Manager	2–119
Service Events	4–13
Service Hijacking	1–67
Service Replacement	1–67
Services	
Suspicious	2–119
Unknown	1–74
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	2–11
File copy	4–43
SSDT → System Service Descriptor Table	
Stacking	1–100
Statistics (incident)	1–13
STIX	1–49
Strings	3–193
StuxNet	1–112, 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
SeImpersonate	2–19
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
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

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

---

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
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

WannaCry .....	1-111
WBEM → Web-Based Enterprise Management .....	
WCE .....	2-10
WDigest .....	2-9, 10
WDigest Registry key .....	2-17
Web Server Intrusion .....	4-97
Web-Based Enterprise Management (WBEM) ...	1-107
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
Windows Time Rules .....	4-38, 4-160-161
winpmem Driver .....	3-39, 1-103
winrm.vbs .....	1-75
winrs.exe .....	2-139
wisp .....	4-180
WMI .....	1-76, 1-85, 86, 1-107
Attacks .....	1-108
Binding .....	1-76
Database .....	1-118
Destination Artifacts .....	2-144
Event Consumer Backdoor .....	1-112
Event Consumer types .....	1-120
Event Consumers .....	1-76
Event Filter (trigger) .....	1-76
Get-WmiObject .....	1-77
Hunting tips .....	1-121
Investigation .....	1-114
Lateral Movement .....	1-111
Log Hunting .....	2-180
Logs .....	2-177
MOF Files .....	1-123
mofcomp.exe .....	1-76
Persistence .....	2-177
PowerShell commands .....	1-116
Privilege Escalation .....	1-110
Processes .....	3-87
Processes (scrons.exe for ActiveScriptEventCon-	
sumers) .....	1-128
Processes (svchost.exe/WmiPrvSE.exe for com-	
mandLineEventConsumers) .....	1-127
PyWMIPersistenceFinder.py .....	1-119
Reconnaissance .....	1-109
Source Artifacts .....	2-143
Threat hunting .....	1-129
WBEM AutoRecover Folder .....	1-125
WBEM AutoRecover Key .....	1-126
WMI explorer .....	1-118
wmic.exe .....	1-75, 1-86, 3-87, 2-143
wmiprvse.exe .....	3-87, 2-144
WordWheelQuery .....	4-19
WriteProcessMemory .....	3-135
wsmprovhost.exe .....	3-87, 2-147

W

Y



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

---

Yara .....	1–50	Zbot .....	3–178
		Zero Configuration .....	1–67
		Zeus .....	3–178
		Zone Identifier .....	4–172

**Z**

