

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

Topics

Incident Response Steps	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	1-72, 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, 1-137
netuse	1-109, 1-137
process	1-109, 1-137
qfe	1-137
qfe(KBpatch listing)	1-109
startup	1-109, 1-137
useraccount	1-109, 1-137

#

\$STANDARD_INFORMATION	4-38, 4-53, 4-154, 4-156, 4-159
\$FILE_NAME	4-154, 4-157, 4-163
\$DATA	4-168, 4-171
\$logfile	4-188
mala	4-199
Operation Codes	4-196
\$logfile Operation Codes	4-186
\$UsnJrnl	4-187, 4-190
MFTEcmd	4-201
Parsing	4-190

Reason Code	4-189
\$UsnJrnl & \$Logfile Common pattern	4-192

A

Account

Built-in accounts	2-83, 2-93
Enumeration	2-100, 2-109
Logon Event	2-95, 2-104
Tracking Administrator	2-85, 2-94
Tracking Creation	2-87, 2-96
Tracking Usage	2-73, 2-82
Tracking Usage (RDP)	2-89, 2-98
Usage (RDP)	2-91, 2-98
AceHash	2-10, 2-24, 2-28
ACMRU	4-17
Active Defense	1-24
Admin Shares	2-134, 2-149-150
Destination Artifacts	2-134, 2-150
Source Artifacts	2-133, 2-149
ADMIN\$	W-2.4-7
Advanced NTFS Journal Parser (ANJP)	4-192
Alternate Data Stream	1-67, 4-171, 4-173
Amcache.hve	2-53, 2-55
Executable presence	2-55
Installed drivers	2-57
InventoryApplication	2-53
InventoryApplicationFile	2-53
Parsing	2-57
AmcacheParser.exe	2-58, 59
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, 4-127-128
Anti-Forensics countermeasures	4-231
System History	4-231
Anti-Malware Script Obfuscation	2-170, 2-187
Anti-Virus	
Bypass	1-67
Logs	2-156, 2-172
AppCompatCache → Application Compatibility Cache	
AppCompatCacheParser.exe	2-52, 2-54
AppCompatProcessor.py	2-66
Application Compatibility Cache	4-12, 2-50, 2-52
Application Deployment Software	2-148, 2-164-165
APT19	3-81, 3-85
Archives (embedded timestamp)	4-39
Armoring	1-67
Artifacts	4-9, 4-26-42
Account Usage	4-23, 24, 4-40
Browser Usage	4-24
Deleted File or File Knowledge	4-34
Last visited MRU	4-34
Recycle Bin	4-35
Thumbnails	4-35

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

Win7-10 Search WordWheelQuery	4-36
XP Search (ACMRU)	4-34
Deleted file or File Knowledge	4-17
File Download	4-28
Downloads.sqlite	4-28
Email Attachements	4-28
Index.dat/Places.sqlite	4-29
Open/Save MRU	4-28
Skype History	4-28
File Opening/Creation	4-14, 4-31
Index.dat	4-34
JumpList4	30
Last visited MRU	4-32
Office Recent Files	4-33
Open/Save MRU	4-31
Prefetch	4-33
Recent Files	4-32
Shell bags	4-32
Shortcut (LNK) files	4-33
Network	3-112, 3-123
Network Shares	2-133, 2-149
OS Unusual	1-74
Physical Location	4-19, 4-36
Cookies	4-37
Network History	4-37
Timezone	4-36
PowerShell	2-145, 2-161
Program Execution	4-12, 4-29
JumpList	4-30
Last Visited MRU	4-29
Prefetch	4-30
RunMRU	4-31
Services Events	4-30
UserAssist	4-31
PsExec	2-135-136, 2-152-154
Remote Desktop Protocol (RDP)	2-130-132, 2-146-148
Remote Service	2-141, 2-157
Scheduled Tasks	2-142, 2-158
USB or Drive Usage	4-20, 4-38
Driver Letter	4-38
Plug-and-Play Event Log	4-38
Shortcut (LNK) files	4-38
USB First/Last Times	4-38
USB Key Identification	4-38
Volume Name	4-38
Volume Serial Number	4-38
WMI	2-143, 2-159-160
at.exe	1-75, 1-101, 2-139, 2-156
ATT&CK	1-43, 1-47, 1-52
Collection	1-45, 1-51
Command and Control	1-45, 1-51
Credential Access	1-45, 1-50
Defense Evasion	1-45, 1-50
Discovery	1-45, 1-50
Execution	1-45, 1-50
Exfiltration	1-45, 1-51
Impact	1-45

Initial Access	1-45
Lateral Movement	1-45, 1-50
Persistence	1-45, 1-50
Privilege Escalation	1-45, 1-50
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	1-79-80, 1-100, 101, 1-104, 105
AutoStart	1-97
AutoStart (ASEPs)	1-69

B

BadRabbit	1-111, 1-139
base64	W-1.4-9
Beacons	1-67
Behavior Detection Anomaly	4-4, 1-81
BelgaSoft	3-34, 3-39
Binary Padding	1-67
blkls	2-42
Bloodhound	2-100, 2-109
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, 2-90
bstring.exe	3-193
Built-in accounts	
ANONYMOUS LOGON	2-92
DWM	2-92
LOCAL SERVICE	2-92
NETWORK SERVICE	2-92
SYSTEM	2-92
UMFD	2-92
BulkExtractor	3-38, 3-43
bytechist	1-82

C

Cached Credentials	2-24
cachedlogonscount	2-27
Defense	2-27
MsCach2	2-24
Security\Cache key	2-24
cachedump	2-24
Cain	2-28
Capability	1-54
Certification Authority	1-62, 1-69
Chat threads	3-37
CIM → Common Information Model	
cmd.exe	1-75

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

Code Injection	1-74, 3-123, 3-134
Reflective	3-138, 3-149
Review	3-148, 3-159
Code Signing	1-62, 1-67, 1-69
Malware	1-63, 1-71
Command Line Tracking	2-158, 2-178
Common Information Model (CIM)	1-107, 1-135
Compromise	1-62, 1-65
Compromise Type	1-55
Conficker	2-121, 2-136
Containment	1-24
CozyDuke	3-97, 3-101
CreateInstance	1-76, 1-104
CreateRemoteThread	3-123, 124, 3-134, 135
creddump	2-10, 2-24, 2-28
Local NT Hashes & Cached Hashes	2-24
Credential	
Attacks (evolution)	2-8
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
Credential Guard	2-9
CredSSP	2-9, 1-119
CRITS	1-49, 1-57
csrss	3-158
Cyber Threat Intelligence	1-35, 1-53
CyberChef	2-171, 2-188

D

DarkComet	3-88, 3-92
Data Encryption	4-120, 4-128
dc3dd	3-18
DCSync	2-35
Deep Panda	3-81, 3-85
Defense Manipulation	1-67
DensityScout	4-9-11
densityscout	4-5, 1-82, 1-84
deskthrd	3-158
Device Guard	2-9
Direct Kernel Object Manipulation (DKOM) ...	3-157, 3-168
Directory Table Base (DTB)	3-45, 3-50
DKOM → Direct Kernel Object Manipulation	
DLL Hijacking	
DLL Search Order Hijacking	1-74, 1-102
DLL Side-Loading	1-75, 1-102
Phantom DLL Hijacking	1-75, 1-102

DLL Injection	1-67, 3-125, 3-136
DLL Lists	3-140
Domain Protected User	2-9
Download.sqlite	4-11
Driver Acquisition	3-207
Driver Acquisition Review	3-198
Driver Letter	4-21
DTB → Directory Table Base	
DumpIt	3-34, 3-39
Dun and Bradstreet Rating	1-62, 1-69
DWM	2-83

E

E-mail Attachments	4-11
ECTXtract	2-183
EDR → Endpoint Detection and Response	
Endpoint Detection and Response (EDR) ..	3-23, 3-29
Challenge	3-25, 3-31
Importance	3-24, 3-30
Memory	3-26, 3-32
Enter-PSSession	1-117, 1-119
EPROCESS	3-45, 3-50, 3-63, 3-68, 3-168
Eradication Without Identification	1-22
Evasion	1-67
Event Log Explorer W-2.3-1, 2-103, 2-112, 2-183,	2-200
Event Log Forwarding	2-200
Event Viewer	2-74
EventLog	2-64, 2-74
Application	2-67
Clearing	2-123, 2-138
Clearing (Selective)	2-126, 2-141
Deletion	4-121, 4-128
EventID	2-191
Extraction	2-183, 2-200
Forwarding	W-3.4-11
PowerShell	2-185
Security	2-68
Security Event	2-69, 2-78
Service	2-67, 2-77
Summary	2-182, 2-199
Tampering	4-121, 4-128
Types	2-66, 2-76
eventlogedit	2-126, 2-141
eventvwr.exe	2-74
Evidence Recovery	4-206
EventLogs Recovery	4-225
File Recovery	4-216
Fileless Malware in registry	4-215
Registry Key	4-214
SDELETE	4-207
VSS Recovery	4-221
Wipers	4-209
EVT	2-64, 2-74
evtwalk	2-183
EVTX	2-64, 2-74
evtx_view	2-183
Executive Process Block	3-45, 3-50

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

F

F-Response	3-7
Acquire Memory	3-18
Agent Service	3-15
Attach Remote Drive	3-17
Enterprise	3-8, 9
GPO	3-14
MSI	3-12
SIFT	3-34, 3-39
Fast forensics	4-80, 4-95
fgdump	2-10
File	
Delete	4-119, 4-127
Download	4-11
Handle	3-105, 3-111
Wiping	4-119, 4-127
File System	
Journaling	4-182-185, 4-187
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, 1-115
fr_ace	
add	3-16
mount	3-17
query	3-16
Frequent Compilation	1-67
FU Rootkit	3-159, 3-170
fxsst.dll	1-75, 1-103

G

Get-Alias	1-88, 1-115
Get-ChildItem	1-88, 1-115
Get-LsaSecret.ps1	2-29
Get-Process	1-88, 1-115
Get-Service	1-88, 1-115
Get-SvcFail.ps1	1-72, 1-100
Get-WinEvent	2-185, 2-202
Get-WmiObject	1-104, 1-112, 1-140
GlassRAT	1-71, 1-100
Golden Ticket	2-31, 2-34
gpedit.msc	2-68
grep	3-182, 3-194
Group Enumeration	2-100, 2-109
Group Managed Service Account	2-9
GRR	3-7, 3-201, 3-210
gsecdump	2-10, 2-13, 2-28

H

Handle	3-105, 3-111
--------	--------------

Hashes	2-10
Defense	2-17
Hibernation Files	3-34, 3-38, 39, 3-43
Windows 10	3-42, 3-47
Hibernation Recon	3-39, 3-43
hibr2bin	3-39, 3-43
Hiding in Plain Sight	1-59, 1-66
Historical Data	4-124, 4-131
Hunting	1-29, 1-31-34
Automated to Manual	1-56, 1-64
Steps (color)	1-62
Steps (Roadmap)	1-54

I

I/O Request Packet (IRP)	3-151, 3-161
IAT → Import Address Table	
IDT → Interrupt Descriptor Table	
Impact	1-53
Import Address Table (IAT)	3-151, 3-161
Incident Response	1-20-21
Remote	3-3, 4
Team	1-32
Incognito	2-19, 1-119
Incognito mode	3-32, 3-37
Index.dat	4-12, 4-17
Indicator of Compromise	1-38, 1-48, 1-56
Atomic	1-38, 1-41
Behavioral	1-39, 1-42
Computed	1-39, 1-42
IOC Editor	1-57
Language	1-49, 1-56
InInitializationOrderModule List	3-140
Inline API	3-151, 3-161
InLoadOrderModule List	3-140
InMemoryOrderModule List	3-140
Intelligence Development	1-24
Intent	1-54
Internet Evidence Finder	3-38, 3-43
Interrupt Descriptor Table (IDT)	3-150, 3-161
Invoke-Command	1-117
IOC Analysis	3-203, 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, 1-120-129
3 rd party tools	1-99, 1-126
Configuration	1-95, 1-124
Get-AutoRunsc.ps1	1-99, 1-126

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

Get-CertStore.ps1	1-99, 1-126
Get-FlsBodyfile.ps1	1-99, 1-126
Get-Handle.ps1	1-99, 1-126
Get-LogparserStack.ps1	1-100, 1-127
Get-ProcDump.ps1	1-99, 1-126
Get-RekalPslist.ps1	1-99, 1-126
Remote	W-1.5-6
Run	1-97
Kansa PowerShell Framework	1-104
KAPE	3-13, 3-22
Collection	3-25
Options	3-23
Target Collection	3-15
KB2871997	2-8
KDBG → Kernel Debugger Datablock	,
KdCopyDataBlock	3-57, 3-59
Kerberoasting	2-31, 2-34
Kerberos	2-96, 1-119
Attacks	2-34
Attacks (Defense)	2-38
Kerberos logon errors	2-105
Kernel Debugger Datablock (KDBG)	3-45, 3-50
Identification	3-57, 3-59
Kernel Patch Protection	3-153, 3-164
Kernel Processor Control Region (KPCR) ..	3-45, 3-50
Kill Chain	1-38, 1-43
Actions on Objectives	1-41, 1-44
Delivery	1-40, 1-43
Exploitation	1-40, 1-43
Persistence	1-40-41, 1-44
Reconnaissance	1-40, 1-43
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	
Network Shares	2-121
Overview	2-5
RunAs	2-124
Scheduled Tasks	2-112, 2-127
Shares	2-106
Tracking	2-105, 2-121
ldrmodules	3-128
InInitializationOrderModule List	3-130
InLoadOrderModule List	3-130
InMemoryOrderModule List	3-130
StuxNet	3-136
TDL3/TDSS	3-133
Least frequency of occurrence analysis	1-100, 1-127
Link (soft and hard)	4-142, 143
LiveSSP	2-10
Living off the Land Binaries (LOLbin)	1-60
LoadLibrary	3-123, 3-134, 3-149
Local Account	2-95, 2-104

Abuse	2-98
Local Admin (Limitations)	2-6-7
Local Administrator Password Solution (LAPS) ..	2-17, 18
LOCAL SERVICE	2-83
Location: Internet Explorer	4-17
log2timeline	4-30, 4-60, 4-69, 4-72, 4-80
Arguments	4-70
Device examples	4-73
Filter Files	4-90
Linux/Android/Mac Parsers	4-78
mactime	4-79
Parser lists	4-85, 4-89
Registry Parsers	4-75
VSS	4-131, 4-139
Web History Parsers	4-77
Windows Parsers	4-73
Logon	
Error Code	2-96, 2-105
Event	2-95, 2-104
Last	4-23
Session Identification	2-79, 2-88
Success/Failure	4-23
Type	2-12, 4-23
Type Codes	2-77, 2-87
LSA Secret	2-28
Defense	2-30
LSASS	2-10
Security EventLog	2-68, 2-77

M

MACB	4-35-36
mactime	4-68
MagnetForensics	3-34, 3-39
Malware	
Code Signing	1-63, 1-71
Dormant	1-55, 1-62, 1-67
Evasion techniques	1-61, 1-67
Execution	2-155, 2-171-172
Fileless	4-120, 4-128
Identification	4-4, 1-81
Locations	1-59, 1-66
Names	1-59, 1-66
Paradox	1-53, 1-61
Search tips	2-63
Malware Discovery	4-4
Malware Persistence	1-68, 1-96
AutoStart Locations	1-69, 1-97
BIOS Flashing	1-78, 1-96
DLL Hijacking	1-74, 1-102
Local Group Policy	1-78, 1-96
MS Office Add-in	1-78, 1-96
Scheduled Tasks	1-73, 1-101
Service Creation/Replacement	1-71, 1-99
Service Failure Recovery	1-72, 1-100
WMI Event Consumers	1-76, 1-104
Managed Service Account	2-8

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

Master File Table (MFT)	4-147
File Record Header	4-152, 4-155
Outlier	4-166
Sequential Entries	4-151, 4-153
Structure	4-148, 4-148-151
Memory	
Acquisition	3-34, 3-39
Analysis	3-44, 3-49
Analysis 	3-45, 3-50
Compression	3-40, 3-45
Dump	3-35, 3-39
Finding the first hit	3-61, 3-66
Forensics	3-30, 3-35
Advantages	3-32, 3-37
Motivations	3-31, 3-36
Windows 10	3-40, 3-45
Offset	3-75, 3-79
Page Execute ReadWrite	3-139, 3-150
Virtual Machine	3-36, 3-41
Memory representation	3-47
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, 2-88
Mimikatz	2-9, 10, 2-15, 2-20, 2-28, 2-32, 1-119
EventLog Clearing	2-126, 2-141
Token Stealing	2-20
MOF	1-112, 1-141
MOF → WMI/MOF Files	
mofcomp.exe	1-104, 1-123, 2-144, 1-150
mount	3-17
MountPoints2	4-43, 4-55, 1-75, 2-133, 2-149
MsCash2	2-24
mstsc.exe	2-130, 2-146
Mutant	3-108, 3-113
Mutex	3-108, 3-113
MZ	3-141-143, 3-152-154

N

net.exe	1-75, 2-133, 2-149
net1.exe	2-133, 2-149
netstat.exe	1-88, 1-115
NetTraveler	1-75, 1-103
Network Artifacts	3-112, 3-123
Review	3-129
Network History	4-20
NETWORK SERVICE	2-83
Network Shares	
Admin	2-133, 2-149
Tracking	2-106, 2-121
New-PSDrive	1-88, 1-115
Nishang	2-29
NotPetya	1-111, 1-139
NTDS.DIT	2-39
ntdsdump	2-39
NTDSXtract	2-39

NTFS	4-140, 4-143
\$I30	4-178
Alternate Data Stream	4-171, 4-173
Features	4-142, 143
File Deletion	4-195, 4-203
File Write	4-194
Index slack space	4-180
System Files	4-144
Timestamp	4-36
NTLM	2-10
NTLM logon errors	2-106
ntoskrnl.exe	3-150, 3-161


O

Office Recent Files	4-15
Open/Save MRU	4-11, 4-14
OpenIOC	1-49, 1-57
Opportunity	1-54
Order of Volatility	1-95, 1-124
Out-GridView	1-88, 1-115
Overpass the Hash	2-34

P

Packing	1-67
Page Directory Offset (PDB)	3-74, 3-78
Page File	3-35, 3-39
Pass-the-hash attacks	2-10, 2-15, 2-107
Mitigations	2-9
Pass-the-ticket	2-31, 2-34
Passware	3-38, 3-43
Password	
Last change	4-23
PatchGuard	3-153, 3-164
PDB → Page Directory Offset	
PEB → Process Environment Block	
PECmd.exe	2-46, 47
Perimeter	3-24, 3-30
Persistence	1-68
pescan	4-5, 4-12-14, 1-82, 1-87
Phishing Attack	4-98-100
Photorec	4-219
pinfo	4-89, 4-99
pinfo	4-60, 4-72
Pivot	4-26-27, 4-43-44
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, 1-103
Poison Ivy	4-11, 1-103
Ports	W-3.4-4

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

powercfg.exe	3-38, 3-43
PowerShell	1-87, 1-114
Authentication	1-92, 1-119
Basics	1-88, 1-115
Command History	2-176
Download file	2-185
wsmprovhost.exe	2-163
Enabling logs	2-166, 2-182
Log hunting	2-168
Logs	2-164, 2-180-181
Malicious (logs)	2-167
Obfuscation	2-170, 2-187
Processes	3-83, 3-87
Remote Artifacts	2-147, 2-163
Remoting	1-117
Source Artifacts	2-145, 2-161
powershell.exe	2-163
Stealth	2-185
Tracking	
Log hunting (quick wins)	2-186
Malicious (logs)	2-183
PSReadline:ConsoleHost_history.txt	2-193
Transcript Logs	2-190-191
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, 2-109
Prefetch	4-13, 4-15, 2-42, 43
First/Last Execution	2-45
From memory	4-137
prefetchparser	4-137
Privileged Local Account Abuse	2-98, 2-107
Proactive Response	1-29
ProcDump	1-75
Process	
Acquisition	3-207
Acquisition Review	3-198
Analysis	3-65-66, 3-70
Anomaly 	1-76
Environment Block (PEB)	3-45, 3-50
Hollowing	3-124, 3-135, 136
Injection	1-67
Objects	3-93, 94, 3-121
Process tree	3-33
Rogue	1-73
Terminated	3-80
Tracking	2-158, 2-160, 2-174, 2-176
Command Line	2-162, 2-178
Profiling Account Usage	2-72
Protected Processes	2-9
PsActiveProcessHead	3-45, 3-50
PsExec	2-10, 11, 1-75, 2-121, 2-135, 136

Destination Artifacts	2-136
Source Artifacts	2-135, 2-152
psexecsvc.exe	2-137
Destination Artifacts	2-153-154
PsLoggedOn	1-75
PsLogList	2-183, 2-200
psort	4-93, 4-104
psort	4-60, 4-72
PspCid	3-158, 3-170
PSReadline	2-176
PWDump	2-172
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, 1-100
rdpclip.exe	2-132, 2-148
Reactive Response	1-29, 1-31
Recent Files	4-14
RecentFileCache.bcf	2-53, 2-55
Reconnaissance Tracking	2-100, 2-109
Recycle Bin	4-18
RedLine	1-57
reg.exe	1-75, 2-139, 2-156
Registry	
Deletion	4-120, 4-128
Hiding Data	4-120, 4-128
RegRipper	1-98, 2-130, 2-146
Rekall	1-103, 1-130, 3-201, 3-210
Remediation	1-27
Requirements	1-28
Steps	1-29
Remote Credential Guard	2-9
Remote Desktop Protocol (RDP)	
Destination Artifacts	2-146
Logging	2-93, 2-102
Source Artifacts	2-130, 2-146
Usage	4-24
Remote Service Artifacts	2-141, 2-157
Restricted Admin	2-9
RID 500	2-7
RIP Listener Service (IPRIP)	1-71, 1-99
rip.pl	W-3.1-18
Rogue Process Analysis	3-94
Rootkit	1-67, 1-74, 1-103, 1-130
Detection	3-180
Detection Review	3-169
Hooking	3-150, 3-161

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

Run MRU	4-14
RunAs	
Tracking	2-124

S

SACL → System Access Control List	
Sakula	1-103
SAM Registry Hive	2-10
sc.exe	1-72, 1-74, 75, 1-100, 2-139, 2-155
Scheduled Tasks	1-73
Artifacts	2-142, 2-158
Artifacts (v1.2)	2-115, 2-131
at.exe	1-73
Logs	2-114, 2-129
schtasks.exe	1-73
Tracking	2-112, 2-127
schtasks.exe	1-75, 1-101, 2-139, 2-156
SCM → Service Control Manager	
scrcons.exe	3-83, 3-87, 2-144, 2-180, 2-197
Scripting	1-85, 1-112
Bash	1-85, 1-112
PowerShell	1-85, 1-112
WMI	1-85, 1-112
Search (Win7-10)	4-19
Search (XP)	4-17
Security Identifier (SID)	3-103, 3-107
Security Tokens → Tokens	
SeDebug	2-85, 2-94
SeImpersonate	2-19, 2-94
Select-String	1-88, 1-115
Service Control Manager	2-119, 2-134
Service Events	4-13
Service Hijacking	1-67
Service Replacement	1-67
Services	
Suspicious	2-119, 2-134
Unknown	1-74
Set-WmiInstance	1-104
SeTakeOwnership	2-85, 2-94
SetWindowsHookEx	3-124, 3-135
Shell bags	4-15
ShimCache	2-50, 51, 4-138
shimcachemem	4-138
Shortcut (LNK) files	4-15, 4-22
SID → Security Identifier	
sigcheck	4-5, 4-15-17, 1-82, 1-89
Silver Ticket	2-34
Skeleton Key	2-34, 35
Skype	4-11
SleuthKit	
fls	4-60
icat	4-175
istat	4-157-158
mactime	4-60
SMB	2-11
File copy	4-43, 4-55
SMBShell	2-10

SSDT → System Service Descriptor Table	
Stacking	1-100, 1-127
Statistics (incident)	1-13
STIX	1-49, 1-56
Strings	3-181, 3-193
StuxNet	1-112, 1-141, 3-147
Super Timeline	4-53, 4-66-71
Creation steps	4-96
Filter	4-78
Output	4-105, 4-113-116
Remote Creation	4-108
Targeted	4-75, 4-84
Web Server Intrusion	4-107
Suspicious Services	2-119, 2-134
PsExec	2-136
Swap File	3-35, 3-39
SxS → DLL Hijacking/DLL Side-Loading	
SysMon	2-188, 2-205-206
SYSTEM	2-83
System Access Control List	2-69, 2-78
System Service Descriptor Table (SSDT)	3-150, 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, 2-147
Temporal proximity	4-26
thrdproc	3-158
Threat	1-53
Thumbnails	4-18
Thumbs.db	4-19
Tickets	2-31
Defense	2-36
Timeline	
Benefits	4-5, 4-22
Comparison	4-30, 4-46
Context	4-29
Filesystem	4-44, 4-56
fls	4-46, 4-60
log2timeline	4-46
MACB	4-51
mactime	4-60
MFTECmd	4-46, 4-58-59
NTFS Timestamp	4-51
Process Analysis	4-32, 4-47
Super Timeline	4-53, 4-66-71
Triage	
Filesystem Timeline	4-50
Utopia and Reality	4-5-6, 4-23-24
Windows Time Rules	4-53
Timestamp	4-35-36
Lateral Movement Analysis	4-43, 4-55
Timestamp	1-67, 4-119, 4-127
Detection	4-162, 4-168-170

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

Evidence	2-51
Timezone	4-19
Tokens	2-19
Defense	2-22
SeImpersonate	2-19
Tracking	
Account Creation	2-87, 2-96
Account Usage	2-73, 2-82
Account Usage (RDP)	2-89, 2-98
Command Line	2-158-162, 2-174-162
Lateral Movement	2-105
Network Shares	2-106, 2-121
Process	2-158-160, 2-174-160
Reconnaissance	2-100, 2-109
RunAs	2-124
Scheduled Tasks	2-112, 2-127
Triage	4-80, 4-96
Filesystem Timeline	4-35
Trusted Code	1-62, 1-69
TsPkg	2-9, 10
tstheme.exe	2-132, 2-148

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	
Velociraptor	3-7, 3-16
Virtual Address Descriptor (VAD)	3-45, 3-50
Virtual Secure Mode	3-40, 3-45
VirtualAllocEx	3-124, 3-135
Visibility	3-24, 3-30
VNC	2-131, 2-147
Volatility	3-38, 3-43, 3-48, 3-53
apihooks	3-152, 3-163, 3-166, 3-177
baseline	3-87, 3-91
build	3-55
cmdline	3-99
cmdscan	3-173, 3-184, 3-185-187, 3-197-198
connections	3-114, 3-125
connscan	3-114, 3-125
consoles	3-173, 3-184, 3-185-187, 3-197-198
devicetree	3-161, 3-172
dlldump	3-173, 174, 3-184, 185
dlllist	3-96-97, 3-99, 100
driverbl	3-87, 3-91, 3-164, 3-175
driverirp	3-152, 3-163
dumpfiles	3-173, 3-184, 3-191, 3-201
filescan	3-61, 3-105, 3-173, 3-184, 3-194-195, 3-204

getsids	3-99, 3-103
handles	3-99, 3-105, 3-110
hivelist	3-61
hollowfind	3-128, 3-139
idt	3-152, 3-163
imagecopy	3-43, 3-59-60, 3-64
imageinfo	3-54, 3-58
kdbgscan	3-56-57, 3-59, 3-62
ldrmodules	3-128, 3-139, 140
malfind	3-128, 3-139, 3-140-147, 3-151
malprocfind	3-73, 3-85-86, 3-89
memdump	3-173, 3-180, 3-184, 3-192
moddump	3-173, 3-176, 3-184, 3-187
modscan	3-152, 3-161, 3-163, 3-172
modules	3-161, 3-172
mutantscan	3-99, 3-105
netscan	3-114-115, 3-125, 126
openioc_scan	3-203, 3-212
page_brute.py	3-203
procdump	3-173, 3-179, 3-184, 3-191
processbl	3-73, 3-87, 88, 3-91
pslist	3-59, 3-61, 3-69, 3-73, 74
psscan	3-61, 3-73, 3-74-76, 3-78, 3-80
pstree	3-73, 3-78-82, 3-82
psxview	3-152, 3-158, 3-163, 3-169
servicebl	3-87, 3-91, 3-99, 3-119
shimcachemem	3-173
shimcacheme	3-197
sockets	3-114, 3-125
sockscan	3-114, 3-125
ssdt	3-152, 3-153-155, 3-163, 164
svcsan	3-99, 3-115
threadmap	3-128, 3-139
vaddump	3-180, 3-192
vainfo	3-201
yarascan	3-203
Help	3-56
Image identification	3-55, 3-61
Profile	3-54, 3-60
Usage	3-49, 3-54

Volume GUID	2-55
Volume Name	4-21
Volume Serial Number	4-22
Volume Shadow Copy	4-124, 4-131
Examination	4-126, 4-133
log2timeline	4-131, 4-139
vshadowinfo	4-127, 4-135
vshadowmount	4-128, 4-136
VSM → Virtual Secure Mode	
vss_carver.py	4-221
VSSAdmin	2-39
Vulnerability	1-53
Exploitation	2-150, 2-166

W

WannaCry	1-111, 1-139
WBEM → Web-Based Enterprise Management	

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

WCE	2-10	mofcomp.exe	1-76
WDigest	2-9, 10	Persistence	2-177
WDigest Registry key	2-17	PowerShell	1-144
Web Server Intrusion	4-97	PowerShell commands	1-116
Web-Based Enterprise Managment (WBEM) ...	1-107, 1-135	Privilege Escalation	1-110, 1-138
WebShell	1-67, 3-81, 3-85	Processes	3-83, 3-87
What is Evil?	1-73	Processes (scrons.exe for ActiveScriptEventConsumers)	1-128
What is Normal?	1-73	Processes (svchost.exe/WmiPrvSE.exe for commandLineEventConsumers)	1-127
Win10 Mem Compression	3-189	PyWMIPersistenceFinder.py	1-119, 1-147
win10memcompression.py	3-189	Reconnaissance	1-109
winmem_decompress.py	3-189	Source Artifacts	2-143, 2-159
win32k.sys	3-150, 3-161	wmic.exe	2-159
Windows Remote Management ..	2-115, 2-131, 2-139, 2-155, 156	Threat hunting	1-129
Windows Service	1-71, 1-99	Tracking	
Windows Time Rules	4-38, 4-160-161, 4-166-167	Common legit consumer	2-197
winpmem Driver	3-34, 3-39, 1-103, 1-130	Logs	2-194-197
winrm → Windows Remote Management		Persistence	2-194-195
winrm.vbs	1-75, 1-117	WBEM AutoRecover Folder	1-125, 1-152
winrs.exe	2-139, 2-156	WBEM AutoRecover Key	1-126, 1-154
wisp	4-180, 4-185	WMI explorer	1-118
WMI	1-76, 1-85, 86, 1-107, 1-112, 1-135	wmic.exe	1-75, 3-83, 1-86, 3-87, 1-113, 2-143
Attacks	1-108, 1-136	wmiprvse.exe	3-83, 3-87, 2-144
Binding	1-76	WordWheelQuery	4-19
Consumers	1-148	WriteProcessMemory	3-123, 3-135
Database	1-118, 1-146	WSMAN	1-117
Destination Artifacts	2-144, 2-160	wsmprovhost.exe	3-83, 3-87, 2-147
mofcomp.exe	2-160		
scrcons.exe	2-160		
wmiprvse.exe	2-160		
Event Consumer Backdoor	1-112, 1-140		
Event Consumer types	1-120		
Event Consumers	1-76, 1-104		
Event Filter (trigger)	1-76		
Get-WmiObject	1-77		
Hunting	1-149		
Hunting tips	1-121		
Investigation	1-114, 1-142		
Lateral Movement	1-111, 1-139		
Log Hunting	2-180		
Logs	2-177		
MOF Files	1-123, 1-150		

Y

Yara	1-50, 1-57
yara	4-5, 4-6-8

Z

Zbot	3-178
Zero Configuration	1-67
Zeus	3-178
Zeus/Zbot	3-168
Zone Identifier	4-172, 4-176