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

Topics

Incident Response Steps 508.1–20-21
- 1. Preparation 508.20–21
- 2. Identification 508.20–21
- 3. Containment 508.20–21
- 4. Eradication 508.20–21
- 5. Recovery 508.20–21
- 6. Lessons Learned 508.20–21

Service Name
- `DcomLaunch` 508.1–76
- `LocalServiceAndNoImpersonation` 508.1–76
- `LocalServiceNetworkRestricted` 508.1–76
- `LocalServiceNoNetwork` 508.1–76
- `netsvcs` 508.1–76
- `NetworkService` 508.1–76
- `RPCSS` 508.1–76

Windows Process
- `csrss.exe` 508.1–77
- `explorer.exe` 508.1–78
- `lsaiso.exe` 508.1–78
- `LSASS.exe` 508.1–79
- `ntoskrnl.exe` 508.1–80
- `RuntimeBroker.exe` 508.1–80
- `services.exe` 508.1–77
- `smss.exe` 508.1–77
- `svchost.exe` 508.1–76
- `System` 508.1–76
- `taskhostw.exe` 508.1–79
- `userinit.exe` 508.1–79
- `wininit.exe` 508.1–78, 508.1–80
- `winlogon.exe` 508.1–79, 80

wmic
- `group` 508.1–137
- `netuse` 508.1–137
- `process` 508.1–137
- `qfe` 508.1–137
- `startup` 508.1–137
- `useraccount` 508.1–137

Categories

$STANDARD_INFORMATION 508.4–38, 508.4–154, 508.4–156
$FILE_NAME 508.4–154, 508.4–157
$DATA 508.4–168
$logfile Operation Codes 508.4–186
$UsnJrnl 508.4–187
- Parsing 508.4–190
- Reason Code 508.4–189

A

Account
- Built-in accounts 508.2–83
- Enumeration 508.2–100
- Logon Event 508.2–95
- Tracking Administrator 508.2–85
- Tracking Creation 508.2–87
- Tracking Usage 508.2–73
- Tracking Usage (RDP) 508.2–89
- Usage (RDP) 508.2–91

AceHash 508.2–10, 508.2–24, 508.2–28
ACMRU 508.4–17
Admin Shares 508.2–134
- Destination Artifacts 508.2–134
- Source Artifacts 508.2–133

ADMIN$ 508.W-2.4–7
Advanced NTFS Journal Parser (ANJP) 508.4–192
Alternate Data Stream 508.1–67, 508.4–171
Amcache.hve 508.2–55
- Parsing 508.2–57

`AmcacheParser.exe` 508.2–58
AMSI → Anti-Malware Scanning Interface
Analysis Scenario 508.2–72
AnalyzeMFT 508.4–157, 508.4–163
ANJP → Advanced NTFS Journal Parser
ANONYMOUS LOGON 508.2–83
Anti-Forensics 508.1–67, 508.4–119
Anti-Malware Script Obfuscation 508.2–170
Anti-Virus
- Bypass 508.1–67
- Logs 508.2–156

AppCompatCache → Application Compatibility Cache
`AppCompatCacheParser.exe` 508.2–54
Application Compatibility Cache 508.4–12, 508.2–52
Application Deployment Software 508.2–148
APT19 508.3–85
Archives (embedded timestamp) 508.4–39
Armoring 508.1–67
Artifacts 508.4–9
- Account Usage 508.4–23
- Browser Usage 508.4–24
- Deleted file or File Knowledge 508.4–17
- File Opening/Creation 508.4–14
- Network 508.3–123
- Network Shares 508.2–133
- OS Unusual 508.1–74
- Physical Location 508.4–19
- PowerShell 508.2–145
- Program Execution 508.4–12
- `PsExec` 508.2–135-136
- Remote Desktop Protocol (RDP) 508.2–130-132
- Remote Service 508.2–141
- Scheduled Tasks 508.2–142
- USB or Drive Usage 508.4–20
- WMI 508.2–143

`at.exe` 508.1–75, 508.1–101, 508.2–139
ATT&CK 508.1–47, 508.1–52
- Collection 508.1–51
- Command and Control 508.1–51

Credential Access 508.1–50
Defense Evasion 508.1–50
Discovery 508.1–50
Execution 508.1–50
Exfiltration 508.1–51
Lateral Movement 508.1–50
Persistence 508.1–50
Privilege Escalation 508.1–50
AutoRun 508.1–67, 508.1–97
`AutoRunsc.exe` 508.1–100, 101, 508.1–104, 105
AutoStart 508.1–97

B

BadRabbit 508.1–139
`base64` 508.W-1.4–9
Beacons 508.1–67
Behavior Detection Anomaly 508.1–81
BelgaSoft 508.3–39
Binary Padding 508.1–67
blkls 508.2–42
Bloodhound 508.2–100
Browser
Cache 508.4–24
Cookies 508.4–24
Flash & Supercookies 508.4–25
History 508.4–24
Search Terms 508.4–20
Session Restore 508.4–25
Brute-Force Password Attack 508.2–81
`bstring.exe` 508.3–193
BulkExtractor 508.3–43
`bytehist` 508.1–82

C

Cached Credentials 508.2–24
Defense 508.2–27
`cachedump` 508.2–24
Cain 508.2–28
Capability 508.1–54
Certification Authority 508.1–69
Chat threads 508.3–37
CIM → Common Information Model
`cmd.exe` 508.1–75
Code Injection 508.1–74, 508.3–134
Reflective 508.3–149
Review 508.3–159
Code Signing 508.1–67, 508.1–69
Malware 508.1–71
Command Line Tracking 508.2–158
Common Information Model (CIM) 508.1–135
Compromise 508.1–39, 508.1–62, 508.1–65
Conficker 508.2–121
Containment and Intelligence Development 508.1–24
CozyDuke 508.3–101
`CreateInstance` 508.1–104
CreateRemoteThread 508.3–134, 135
creddump 508.2–10, 508.2–24, 508.2–28
Credential
Attacks (evolution) 508.2–8
Availability 508.2–12
Harvesting 508.2–6
Credential Guard 508.2–9
CredSSP 508.2–9, 508.1–119
CRITS 508.1–57
Cyber Threat Intelligence 508.1–33, 508.1–53
CyberChef 508.2–171

D

DarkComet 508.3–92
Data Collection 508.1–40
Data Encryption 508.4–120
Data Exfiltration 508.1–40
`dc3dd` 508.3–18
Deep Panda 508.3–85
Defense Manipulation 508.1–67
`densityscout` 508.1–82, 508.1–84
Device Guard 508.2–9
Digital Forensics & IR 508.1–32
Direct Kernel Object Manipulation (DKOM) 508.3–168
Directory Table Base (DTB) 508.3–50
DKOM → Direct Kernel Object Manipulation
DLL Hijacking
DLL Search Order Hijacking 508.1–102
DLL Side-Loading 508.1–102
Phantom DLL Hijacking 508.1–102
DLL Injection 508.1–67, 508.3–136
DLL Lists 508.3–140
Domain Protected User 508.2–9
Download.sqlite 508.4–11
Driver Acquisition 508.3–207
Driver Letter 508.4–21
DTB → Directory Table Base
DumpIt 508.3–39
Dun and Bradstreet Rating 508.1–69
DWM 508.2–83

E

E-mail Attachments 508.4–11
ECTXtract 508.2–183
EDR → Endpoint Detection and Response
Endpoint Detection and Response (EDR) 508.3–29
Challenge 508.3–31
Importance 508.3–30
Memory 508.3–32
`Enter-PSSession` 508.1–117, 508.1–119
EPROCESS 508.3–50, 508.3–68, 508.3–168
Eradication Without Proper Incident Scoping/Containment 508.1–22
Establish Foothold 508.1–39

- Evasion 508.1–67
- Event Log Explorer 508.W-2.3–1, 508.2–103, 508.2–183
- Event Viewer 508.2–74
- EventLog 508.2–64
  - Application 508.2–67
  - Clearing 508.2–123
  - Clearing (Selective) 508.2–126
  - Deletion 508.4–121
  - EventID 508.2–191
  - Extraction 508.2–183
  - Forwarding 508.W-3.4–11
  - PowerShell 508.2–185
  - Security 508.2–68
  - Security Event 508.2–69
  - Service 508.2–67
  - Summary 508.2–182
  - Tampering 508.4–121
  - Types 508.2–66
- eventlogedit 508.2–126
- `eventvwr.exe` 508.2–74
- EVT 508.2–64
- evtwalk 508.2–183
- EVTX 508.2–64
- evtx_view 508.2–183
- Executive Process Block 508.3–50

F

- F-Response 508.3–7
  - Acquire Memory 508.3–18
  - Agent Service 508.3–15
  - Attach Remote Drive 508.3–17
  - Enterprise 508.3–8
  - GPO 508.3–14
  - MSI 508.3–12
  - SIFT 508.3–39
- Fast forensics 508.4–80
- fgdump 508.2–10
- File
  - Delete 508.4–119
  - Download 508.4–11
  - Handle 508.3–111
  - Wiping 508.4–119
- File System
  - Journaling 508.4–182-185
- Filename
  - Hijacking 508.1–67
- Filename 508.4–176
- filter_windows 508.4–81
- Firmware 508.1–67
- fls 508.4–30, 508.4–48
- foremost 508.2–42
- Forensics (Remote) 508.3–4
- `Format-Wide` 508.1–115
- fr_ace
  - add 508.3–16
  - mount 508.3–17
  - query 508.3–16
- Frequent Compilation 508.1–67
- FU Rootkit 508.3–170
- `fxsst.dll` 508.1–103

G

- `Get-Alias` 508.1–115
- `Get-ChildItem` 508.1–115
- `Get-LsaSecret.ps1` 508.2–29
- `Get-Process` 508.1–115
- `Get-Service` 508.1–115
- `Get-SvcFail.ps1` 508.1–100
- `Get-WinEvent` 508.2–185
- `Get-WmiObject` 508.1–104, 508.1–140
- GlassRAT 508.1–100
- Golden Ticket 508.2–31, 508.2–34
- `gpedit.msc` 508.2–68
- `grep` 508.3–194
- Group Enumeration 508.2–100
- Group Managed Service Account 508.2–9
- GRR 508.3–7, 508.3–210
- `gsecdump` 508.2–10, 508.2–13, 508.2–28

H

- Handle 508.3–111
- Hashes 508.2–10
  - Defense 508.2–17
- Hibernation Files 508.3–39, 508.3–43
  - Windows 10 508.3–47
- Hibernation Recon 508.3–43
- `hibr2bin` 508.3–43
- Hiding in Plain Sight 508.1–66
- Historical Data 508.4–124
- Hunting 508.1–31-34
  - Automated to Manual 508.1–64
  - Steps (color) 508.1–62

I

- I/O Request Packet (IRP) 508.3–161
- IAT → Import Address Table
- Identification 508.1–31-34
- IDT → Interrupt Descriptor Table
- Impact 508.1–53
- Import Address Table (IAT) 508.3–161
- Incident Response
  - Intelligence-Driven 508.1–39
  - Process 508.1–38
  - Remote 508.3–4
  - Team 508.1–32
- Incident Response Detection and Intelligence Loop 508.1–27
- Incognito 508.2–19, 508.1–119
- Incognito mode 508.3–37
- Index.dat 508.4–12, 508.4–17
- Indicator of Compromise 508.1–56
  - Atomic 508.1–41
  - Behavioral 508.1–42

  - Computed 508.1–42
  - IOC Editor 508.1–57
  - Language 508.1–56
- `InInitializationOrderModule` List 508.3–140
- Initial Compromise 508.1–39
- Inline API 508.3–161
- `InLoadOrderModule` List 508.3–140
- `InMemoryOrderModule` List 508.3–140
- Intelligence-Driven Incident Response 508.1–39
- Intent 508.1–54
- Internet Evidence Finder 508.3–43
- Interrupt Descriptor Table (IDT) 508.3–161
- `Invoke-Command` 508.1–117
- IOC Analysis 508.3–212
- IPRIP → RIP Listener Service
- IRP → I/O Request Packet
- `istat` 508.4–162, 508.4–173-175

J

- `jobparser.py` 508.2–115
- `jp` 508.4–191
- Jump List 508.4–13

K

- Kansa 508.1–120-129
  - 3rd party tools 508.1–126
  - Configuration 508.1–124
  - `Get-AutoRunsc.ps1` 508.1–126
  - `Get-CertStore.ps1` 508.1–126
  - `Get-FlsBodyfile.ps1` 508.1–126
  - `Get-Handle.ps1` 508.1–126
  - `Get-LogparserStack.ps1` 508.1–127
  - `Get-ProcDump.ps1` 508.1–126
  - `Get-RekalPslist.ps1` 508.1–126
  - Remote 508.W-1.5–6
- Kansa PowerShell Framework 508.1–104
- KAPE 508.3–22
  - Collection 508.3–25
  - Options 508.3–23
- KB2871997 508.2–8
- KDBG → Kernel Debugger Datablock
- `KdCopyDataBlock` 508.3–59
- Kerberoasting 508.2–31, 508.2–34
- Kerberos 508.2–96, 508.1–119
  - Attacks 508.2–34
  - Attacks (Defense) 508.2–38
- Kernel Debugger Datablock (KDBG) 508.3–50
  - Identification 508.3–59
- Kernel Patch Protection 508.3–164
- Kernel Processor Control Region (KPCR) 508.3–50
- Kill Chain 508.1–41, 508.1–43
  - Actions on Objectives 508.1–44
  - Delivery 508.1–43
  - Exploitation 508.1–43
  - Persistence 508.1–44
  - Reconnaissance 508.1–43
- kpartx 508.3–17
- `kpartx` 508.W-3.1–16
- KPCR → Kernel Processor Control Region

L

- LAPS → Local Administrator Password Solution
- Last visited MRU 508.4–12, 508.4–15, 508.4–17
- Lateral Movement 508.1–40
  - Overview 508.2–5
  - Scheduled Tasks 508.2–112
  - Shares 508.2–106
  - Tracking 508.2–105
- Least frequency of occurence analysis 508.1–127
- Link (soft and hard) 508.4–142
- LiveSSP 508.2–10
- `LoadLibrary` 508.3–134, 508.3–149
- Local Account 508.2–95
  - Abuse 508.2–98
- Local Admin (Limitations) 508.2–6-7
- Local Administrator Password Solution (LAPS) 508.2–17
- LOCAL SERVICE 508.2–83
- Location: Internet Explorer 508.4–17
- log2timeline 508.4–30, 508.4–60, 508.4–69
  - Arguments 508.4–70
  - Device examples 508.4–73
  - Parser lists 508.4–85
  - VSS 508.4–131
- Logon
  - Error Code 508.2–96
  - Event 508.2–95
  - Last 508.4–23
  - Session Identification 508.2–79
  - Success/Failure 508.4–23
  - Type 508.2–12, 508.4–23
  - Type Codes 508.2–77
- LSA Secret 508.2–28
  - Defense 508.2–30
- LSASS 508.2–10
  - Security EventLog 508.2–68

M

- MACB 508.4–35-36
- `mactime` 508.4–68
- MagnetForensics 508.3–39
- Maintain presence 508.1–39
- Malware
  - Code Signing 508.1–71
  - Dormant 508.1–62, 508.1–67
  - Evasion techniques 508.1–67
  - Execution 508.2–155
  - Fileless 508.4–120
  - Identification 508.1–81
  - Locations 508.1–66

- Names 508.1–66
- Paradox 508.1–61

Malware Persistence 508.1–96
- AutoStart Locations 508.1–97
- BIOS Flashing 508.1–96
- DLL Hijacking 508.1–102
- Local Group Policy 508.1–96
- MS Office Add-in 508.1–96
- Scheduled Tasks 508.1–101
- Service Creation/Replacement 508.1–99
- Service Failure Recovery 508.1–100
- WMI Event Consumers 508.1–104

Managed Service Account 508.2–8

Master File Table (MFT) 508.4–147
- File Record Header 508.4–152
- Outlier 508.4–166
- Sequential Entries 508.4–151
- Structure 508.4–148

Memory
- Acquisition 508.3–39
- Analysis 508.3–49
- Analysis 508.3–50
- Compression 508.3–45
- Dump 508.3–39
- Finding the first hit 508.3–66
- Forensics 508.3–35
  - Advantages 508.3–37
  - Motivations 508.3–36
  - Windows 10 508.3–45
- Offset 508.3–79
- Page Execute ReadWrite 508.3–150
- Virtual Machine 508.3–41

Metadata Layer 508.4–150

MetaSploit 508.2–10, 508.2–19, 508.2–24, 508.2–28, 508.2–39

MFT → Master File Table

`MFTECmd` 508.4–30, 508.4–46, 508.4–157

Microsoft Online Accounts 508.2–79

Mimikatz 508.2–9, 10, 508.2–15, 508.2–20, 508.2–28, 508.2–32, 508.1–119
- EventLog Clearing 508.2–126

MOF 508.1–141

MOF → WMI/MOF Files

`mofcomp.exe` 508.1–104, 508.2–144, 508.1–150

`mount` 508.3–17

`MountPoints2` 508.4–43, 508.1–75, 508.2–133

MsCash2 508.2–24

`mstsc.exe` 508.2–130

Mutant 508.3–113

Mutex 508.3–113

MZ 508.3–152-154

N

`net.exe` 508.1–75, 508.2–133

`net1.exe` 508.2–133

`netstat.exe` 508.1–115

NetTraveler 508.1–103

Network Artifacts 508.3–123
- Review 508.3–129

Network History 508.4–20

NETWORK SERVICE 508.2–83

Network Shares
- Admin 508.2–133
- Tracking 508.2–106

`New-PSDrive` 508.1–115

Nishang 508.2–29

NotPetya 508.1–139

NTDS.DIT 508.2–39

`ntdsdump` 508.2–39

`NTDSXtract` 508.2–39

NTFS 508.4–140
- Alternate Data Stream 508.4–171
- Features 508.4–142
- File Deletion 508.4–195
- File Write 508.4–194
- Index slack space 508.4–180
- System Files 508.4–144
- Timestamp 508.4–36

NTLM 508.2–10

`ntoskrnl.exe` 508.3–161

O

Office Recent Files 508.4–15

Open/Save MRU 508.4–11, 508.4–14

OpenIOC 508.1–57

Opportunity 508.1–54

Order of Volatility 508.1–124

`Out-GridView` 508.1–115

Overpass the Hash 508.2–34

P

Packing 508.1–67

Page Directory Offset (PDB) 508.3–78

Page File 508.3–39

Pass-the-hash attacks 508.2–10
- Mitigations 508.2–9

Pass-the-ticket 508.2–31, 508.2–34

Passware 508.3–43

Password
- Last change 508.4–23

PatchGuard 508.3–164

PDB → Page Directory Offset

PEB → Process Environment Block

`PECmd.exe` 508.2–47

Perimeter 508.3–30

`pescan` 508.1–82, 508.1–87

Phishing Attack 508.4–98-100

pinfo 508.4–89

`pinfo` 508.4–60

Pivot 508.4–26-27

Places.sqlite 508.4–12

Plaso 508.4–60

  - Linux/Android/Mac Parsers 508.4–66
  - mactime 508.4–68
  - Registry Parsers 508.4–63
  - Web History Parsers 508.4–65
  - Windows Parsers 508.4–61
- Plug-and-Play Event Log 508.4–22
- PlugX 508.1–103
- Poison Ivy 508.1–103
- Ports 508.W-3.4–4
- `powercfg.exe` 508.3–43
- PowerShell 508.1–114
  - Authentication 508.1–119
  - Basics 508.1–115
  - Command History 508.2–176
  - Enabling logs 508.2–166
  - Log hunting 508.2–168
  - Logs 508.2–164
  - Malicious (logs) 508.2–167
  - Obfuscation 508.2–170
  - Processes 508.3–87
  - Remote Artifacts 508.2–147
  - Remoting 508.1–117
  - Source Artifacts 508.2–145
  - Transcript Logs 508.2–173-174
- `powershell.exe` 508.1–75, 508.2–146
- PowerView 508.2–100
- Prefetch 508.4–13, 508.4–15, 508.2–42
  - First/Last Execution 508.2–45
  - From memory 508.4–137
- `prefetchparser` 508.4–137
- Privileged Local Account Abuse 508.2–98
- Proactive Response 508.1–29
- `ProcDump` 508.1–75
- Process
  - Acquisition 508.3–207
  - Analysis 508.3–70
  - Anomaly 508.1–76
  - Environment Block (PEB) 508.3–50
  - Hollowing 508.3–135
  - Injection 508.1–67
  - Objects 508.3–94, 508.3–121
  - Process tree 508.3–33
  - Rogue 508.1–73
  - Terminated 508.3–80
  - Tracking 508.2–158, 508.2–160
    - Command Line 508.2–162
- Profiling Account Usage 508.2–72
- Protected Processes 508.2–9
- PsActiveProcessHead 508.3–50
- `PsExec` 508.2–10, 508.1–75, 508.2–121, 508.2–136
  - Destination Artifacts 508.2–136
  - Source Artifacts 508.2–135
- `psexesvc.exe` 508.2–137
- `PsLoggedOn` 508.1–75
- `PsLogList` 508.2–183
- psort 508.4–93
- `psort` 508.4–60
- `PspCid` 508.3–170
- `PSReadline` 508.2–176
- PWDumpX 508.2–24
- `PWDumpX` 508.2–10

Q

- `qc` 508.1–74
- `qprivs` 508.1–74
- `qtriggerinfo` 508.1–74
- `queryex` 508.1–74

R

- `rar.exe` 508.1–75
- RasAuto 508.1–100
- `rdpclip.exe` 508.2–132
- Reactive Response 508.1–29, 508.1–31-34
- Real-Time Remediation 508.1–30
- Recent Files 508.4–14
- RecentFileCache.bcf 508.2–55
- Reconnaissance Tracking 508.2–100
- Recycle Bin 508.4–18
- RedLine 508.1–57
- `reg.exe` 508.1–75, 508.2–139
- Registry
  - Deletion 508.4–120
  - Hiding Data 508.4–120
- RegRipper 508.1–98, 508.2–130
- Rekall 508.1–130, 508.3–210
- Remediation 508.1–27-29, 508.1–35
  - Requirements 508.1–36
  - Steps 508.1–37
- Remediation controls 508.1–27-29
- Remote Credential Guard 508.2–9
- Remote Desktop Protocol (RDP)
  - Logging 508.2–93
  - Source Artifacts 508.2–130
  - Usage 508.4–24
- Remote Service Artifacts 508.2–141
- Restricted Admin 508.2–9
- RID 500 .... 508.2–7
- RIP Listener Service (IPRIP) 508.1–99
- rip.pl 508.W-3.1–18
- Rogue Process Analysis 508.3–94
- Rootkit 508.1–67, 508.1–74, 508.1–130
  - Detection 508.3–180
  - Hooking 508.3–161
- Run MRU 508.4–14

S

- SACL → System Access Control List ....
- Sakula 508.1–103
- SAM Registry Hive 508.2–10
- `sc.exe` 508.1–74, 75, 508.1–100, 508.2–139
- Scheduled Tasks
  - Artifacts 508.2–142
  - Artifacts (v1.2) 508.2–115
  - Logs 508.2–114

  - Tracking 508.2–112
- `schtasks.exe` 508.1–75, 508.1–101, 508.2–139
- SCM → Service Control Manager
- `scrcons.exe` 508.3–87, 508.2–144, 508.2–180
- Scripting 508.1–112
  - Bash 508.1–112
  - PowerShell 508.1–112
  - WMI 508.1–112
- Search (Win7-10) 508.4–19
- Search (XP) 508.4–17
- Security Identifier (SID) 508.3–103, 508.3–107
- Security Tokens → Tokens
- `SeDebug` 508.2–85
- `SeImpersonate` 508.2–19
- `Select-String` 508.1–115
- Service Control Manager 508.2–119
- Service Events 508.4–13
- Service Hijacking 508.1–67
- Service Replacement 508.1–67
- Services
  - Suspicious 508.2–119
  - Unknown 508.1–74
- `Set-WmiInstance` 508.1–104
- `SeTakeOwnership` 508.2–85
- `SetWindowsHookEx` 508.3–135
- Shell bags 508.4–15
- ShimCache 508.2–51, 508.4–138
- `shimcachemem` 508.4–138
- Shortcut (LNK) files 508.4–15, 508.4–22
- SID → Security Identifier
- `sigcheck` 508.1–82, 508.1–89
- Silver Ticket 508.2–34
- Skeleton Key 508.2–34
- Skype 508.4–11
- SMB
  - File copy 508.4–43
  - SMBShell 508.2–10
- SSDT → System Service Descriptor Table
- Stacking 508.1–127
- STIX 508.1–56
- Strings 508.3–193
- StuxNet 508.1–141, 508.3–147
- Super Timeline 508.4–53
  - Creation steps 508.4–96
  - Filter 508.4–78
  - Output 508.4–105
  - Targeted 508.4–75
- Suspicious Services 508.2–119
- Swap File 508.3–39
- SxS → DLL Hijacking/DLL Side-Loading
- SysMon 508.2–188
- SYSTEM 508.2–83
- System Access Control List 508.2–69
- System Service Descriptor Table (SSDT) 508.3–161
- SYSTEM32 508.W-2.1–9
- SYSWOW64 508.W-2.1–9

T

- Target Collection 508.3–25
- Task (Start time) 508.W-2.4–22
- TDL3/TDSS 508.3–144
- TeamViewer 508.2–131
- Temporal proximity 508.4–26
- Threat 508.1–53
- Thumbnails 508.4–18
- Thumbs.db 508.4–19
- Tickets 508.2–31
  - Defense 508.2–36
- Timeline
  - Benefits 508.4–5
  - Comparison 508.4–30
  - Context 508.4–29
  - Filesystem 508.4–44
  - Process Analysis 508.4–32
  - Super Timeline 508.4–53
  - Utopia and Reality 508.4–5-6
- Timestamp 508.4–35-36
  - Lateral Movement Analysis 508.4–43
- Timestomp 508.1–67, 508.4–119
  - Detection 508.4–162
  - Evidence 508.2–51
- Timezone 508.4–19
- Tokens 508.2–19
  - Defense 508.2–22
- Tracking
  - Account Creation 508.2–87
  - Account Usage 508.2–73
  - Account Usage (RDP) 508.2–89
  - Command Line 508.2–158-162
  - Lateral Movement 508.2–105
  - Network Shares 508.2–106
  - Process 508.2–158-160
  - Reconnaissance 508.2–100
  - Scheduled Tasks 508.2–112
- Triage 508.4–80
  - Filesystem Timeline 508.4–35
- Trusted Code 508.1–69
- TsPkg 508.2–9, 10
- `tstheme.exe` 508.2–132

U

- UAC → User Acess Control
- UMFD 508.2–83
- USB First/Last Times 508.4–21
- USB Key Identification 508.4–20
- User Acess Control (UAC) 508.2–8
- UserAssist 508.4–14

V

- VAD → Virtual Address Descriptor
- Virtual Address Descriptor (VAD) 508.3–50
- Virtual Secure Mode 508.3–45
- `VirtualAllocEx` 508.3–135
- Visibility 508.3–30
- VNC 508.2–131

- Volatility ... 508.3–43, 508.3–53
  - apihooks ... 508.3–163, 508.3–177
  - baseline ... 508.3–91
  - cmdline ... 508.3–99
  - cmdscan ... 508.3–184, 508.3–197-198
  - connections ... 508.3–125
  - connscan ... 508.3–125
  - consoles ... 508.3–184, 508.3–197-198
  - devicetree ... 508.3–172
  - dlldump ... 508.3–184, 185
  - dlllist ... 508.3–99, 100
  - driverbl ... 508.3–91, 508.3–175
  - driverirp ... 508.3–163
  - dumpfiles ... 508.3–184, 508.3–201
  - filescan ... 508.3–61, 508.3–184, 508.3–204
  - getsids ... 508.3–99, 508.3–103
  - handles ... 508.3–99, 508.3–110
  - hivelist ... 508.3–61
  - hollowfind ... 508.3–139
  - idt ... 508.3–163
  - imagecopy ... 508.3–43, 508.3–64
  - imageinfo ... 508.3–58
  - kdbgscan ... 508.3–59, 508.3–62
  - ldrmodules ... 508.3–139, 140
  - malfind ... 508.3–139, 508.3–151
  - malprocfind ... 508.3–73, 508.3–89
  - memdump ... 508.3–184, 508.3–192
  - moddump ... 508.3–184, 508.3–187
  - modscan ... 508.3–163, 508.3–172
  - modules ... 508.3–172
  - mutantscan ... 508.3–99
  - netscan ... 508.3–125, 126
  - openioc_scan ... 508.3–212
  - procdump ... 508.3–184, 508.3–191
  - processbl ... 508.3–73, 508.3–91
  - pslist ... 508.3–59, 508.3–61, 508.3–73, 74
  - psscan ... 508.3–61, 508.3–73, 508.3–78, 508.3–80
  - pstree ... 508.3–73, 508.3–82
  - psxview ... 508.3–163, 508.3–169
  - servicebl ... 508.3–91, 508.3–99, 508.3–119
  - sockets ... 508.3–125
  - sockscan ... 508.3–125
  - ssdt ... 508.3–163, 164
  - svcscan ... 508.3–99, 508.3–115
  - threadmap ... 508.3–139
  - vaddump ... 508.3–192
  - vainfo ... 508.3–201
  - Help ... 508.3–56
  - Image identification ... 508.3–61
  - Profile ... 508.3–60
  - Usage ... 508.3–54
- Volume GUID ... 508.2–55
- Volume Name ... 508.4–21
- Volume Serial Number ... 508.4–22
- Volume Shadow Copy ... 508.4–124
  - Examination ... 508.4–126
  - log2timeline ... 508.4–131
- vshadowinfo ... 508.4–127
- vshadowmount ... 508.4–128
- VSM → Virtual Secure Mode ...
- VSSAdmin ... 508.2–39
- Vulnerability ... 508.1–53
  - Exploitation ... 508.2–150

W

- WannaCry ... 508.1–139
- WBEM → Web-Based Entreprise Managment ...
- WCE ... 508.2–10
- WDigest ... 508.2–9, 10
- Web Server Intrusion ... 508.4–97
- Web-Based Entreprise Managment (WBEM) ... 508.1–135
- WebShell ... 508.1–67, 508.3–85
- What is Evil? ... 508.1–73
- What is Normal? ... 508.1–73
- win32k.sys ... 508.3–161
- Windows Remote Management ... 508.2–115, 508.2–139
- Windows Service ... 508.1–99
- Windows Time Rules ... 508.4–38, 508.4–160-161
- winpmem Driver ... 508.3–39, 508.1–130
- winrm.vbs ... 508.1–75, 508.1–117
- winrs.exe ... 508.2–139
- wisp ... 508.4–180
- WMI ... 508.1–112, 508.1–135
  - Attacks ... 508.1–136
  - Consumers ... 508.1–148
  - Database ... 508.1–146
  - Destination Artifacts ... 508.2–144
  - Event Consumer Backdoor ... 508.1–140
  - Event Consumers ... 508.1–104
  - Hunting ... 508.1–149
  - Investigation ... 508.1–142
  - Lateral Movement ... 508.1–139
  - Log Hunting ... 508.2–180
  - Logs ... 508.2–177
  - MOF Files ... 508.1–150
  - Persistence ... 508.2–177
  - PowerShell ... 508.1–144
  - Privilege Escalation ... 508.1–138
  - Processes ... 508.3–87
  - PyWMIPersistenceFinder.py ... 508.1–147
  - Source Artifacts ... 508.2–143
  - WBEM AutoRecover Folder ... 508.1–152
  - WBEM AutoRecover Key ... 508.1–154
- wmic.exe ... 508.1–75, 508.3–87, 508.1–113, 508.2–143
- wmiprvse.exe ... 508.3–87, 508.2–144
- WordWheelQuery ... 508.4–19
- WriteProcessMemory ... 508.3–135
- WSMAN ... 508.1–117
- wsmprovhost.exe ... 508.3–87, 508.2–147

Y

- Yara ... 508.1–57

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

Z

Zbot 508.3–178

Zero Configuration 508.1–67

Zeus 508.3–178

Zone Identifier 508.4–172