508.2 - Intrusion Analysis

[Advanced Evidence of Execution](#_Toc122116799) 6-33

[Prefetch](#_Toc122116800) 6-13

[Review](#_Toc122116801) 6-8

[Evidence of execution](#_Toc122116802) 8

[‘PECmd.exe’ – Prefetch file analysis](#_Toc122116803) 9-13

[Overview](#_Toc122116804) 9

[Usage](#_Toc122116805) 10

[Output and analysis](#_Toc122116806) 11

[ShimCache (AppCompatCache)](#_Toc122116807) 14-16

[Timestomp detection](#_Toc122116808) 15

[‘AppCompatParser.exe’ – Execution history](#_Toc122116809) 16

[Amcache.hve](#_Toc122116810) 17-26

[Overview](#_Toc122116811) 17-18

[Parsing Amcache](#_Toc122116812) 19-22

[Auditing executable presence](#_Toc122116813) 19

[Auditing installed drivers](#_Toc122116814) 21

[‘amcacheparser.exe’ – Amcache extraction](#_Toc122116815) 23-26

[Overview](#_Toc122116816) 23

[Example output](#_Toc122116817) 24-25

[Associated vs. Unassociated](#_Toc122116818) 24

[What to look for](#_Toc122116819) 25

[Application Execution Analysis](#_Toc122116820) 2

[Scaling automatic execution analysis](#_Toc122116821) 27-31

[Overview](#_Toc122116822) 27

[‘appcompatprocessor.py’ – Scaling analysis](#_Toc122431926) 28-30

[Stacking with appcompatprocessor.py](#_Toc122431927) 32

[Least frequency of occourance](#_Toc122431928) 32

[Even Log Analysis for Responders and Hunters](#_Toc122431929) 37-43

[Event Log Fundamentals](#_Toc122431930) 38-43

[Where to find event logs](#_Toc122431931) 38-39

[History](#_Toc122431932) 38

[Max size options](#_Toc122431933) 39

[Types of event logs](#_Toc122431934) 40

[Security log](#_Toc122431935) 41-43

[Categories](#_Toc122431936) 42

[Analysis Scenarios](#_Toc122431937) 44-

[Security log: Tracking account usage](#_Toc122431938) 46-72

[Detailed log properties](#_Toc122431939) 48

[Logon type codes](#_Toc122431940) 50

[Identifying logon sessions](#_Toc122431941) 52

[Logon ID](#_Toc122431942) 52

[Session duration/length](#_Toc122431943) 52

[Identifying brute force attacks](#_Toc122431944) 54

[Built-in Accounts](#_Toc122431945) 56-57

[Tracking admin account activity](#_Toc122431946) 58

[Auditing account creation](#_Toc122431947) 60

[Tracking RDP sessions](#_Toc122431948) 62-67

[Remote desktop logging](#_Toc122431949) 67

[TerminalServices/RDPclient log](#_Toc122431950) 67

[Account logon events](#_Toc122431951) 69-72

[NTLM](#_Toc122431952) 69

[Kerberos](#_Toc122431953) 69

[Logon error codes](#_Toc122431954) 70-71

[Pass the hash](#_Toc122431955) 72

[Security log: Tracking recon](#_Toc122431956) 74-75

[Account and group enumeration](#_Toc122431957) 74-75

[Security log: Tracking lateral movement](#_Toc122431958) 85-104

[Network shares](#_Toc122431959) 85-86

[Overview](#_Toc122431960) 85

[Cobalt strike example](#_Toc122431961) 86

[Runas / Explicit Credentials](#_Toc122431962) 88-92

[Runas detection](#_Toc122431963) 90

[Cobalt strike example (make\_token & pth)](#_Toc122431964) 92

[Auditing scheduled tasks](#_Toc122431965) 94-99

[Hunting](#_Toc122431966) 95

[Remote task scheduler artifacts](#_Toc122431967) 98-99

[Suspicious services](#_Toc122431968) 101-104

[Overview](#_Toc122431969) 101

[PsExec](#_Toc122431970) 103-104

[Event log clearing](#_Toc122431971) 106-107

[Event log attacks](#_Toc122431972) 109-110

[mimikatz - ‘event::drop’](#_Toc122431973) 109

[DanderSpiritz – ‘eventlogedit’](#_Toc122431974) 109

[Invoke-Phant0m](#_Toc122431975) 109

[Event log analysis tools](#_Toc122431976) 77-82

[Event log explorer](#_Toc122431977) 77

[‘EvtxCmd.exe’ – cmd event log parser](#_Toc122431978) 79-82

[EvtxCmd maps](#_Toc122431979) 80

[Grouping and filtering EvtxCmd results](#_Toc122431980) 82

[Lateral Movement Adverary Tactics](#_Toc122431981) 113-134

[Lateral movement: Copy malware](#_Toc122431982) 113-118

[RDP services](#_Toc122431983) 114-116

[Source system artifacts](#_Toc122431984) 114-115

[Destination system artifacts](#_Toc122431985) 116

[Windows admin shares](#_Toc122431986) 117-118

[Source system artifacts](#_Toc122431987) 117

[Destination system artifacts](#_Toc122431988) 118

[Lateral movement: Execution](#_Toc122431989) 119-134

[PsExec](#_Toc122431990) 120-122

[Source system artifacts](#_Toc122431991) 120

[Destination system artifacts](#_Toc122431992) 121-122

[Remote management tools](#_Toc122431993) 123-134

[Remote services](#_Toc122431994) 125

[Overview](#_Toc122431995) 123-124

[Artifacts](#_Toc122431996) 125

[Remote scheduled tasks](#_Toc122431997) 126

[Overview](#_Toc122431998) 123-124

[Artifacts](#_Toc122431999) 126

[Remote registry interaction](#_Toc122432000) 124

[Overview](#_Toc122432001) 124

[Windows remote shell (WinRS)](#_Toc122432003) 123-124

[Overview](#_Toc122432004) 123-124

[WMI](#_Toc122432006) 127-128

[Artifacts](#_Toc122432007) 127-128

[PowerShell Remoting](#_Toc122432008) 129-131

[Source system artifacts](#_Toc122432009) 129-130

[Destination system artifacts](#_Toc122432010) 131

[Application deployment software](#_Toc122432011) 132-133

[Vulnerability Exploitation](#_Toc122432012) 134

[CLI, PowerShell and WMI Analysis](#_Toc122432013) 139-182

[Evidence of malware execution](#_Toc122432014) 139-145

[Warning, error and crash logs](#_Toc122432015) 139-140

[‘report.wer’ – Windows error reporting](#_Toc122432016) 142

[Process tracking and capturing CLI](#_Toc122432017) 143-145

[CLI Auditing example](#_Toc122432018) 145

[WMI – Windows Management Instrumentation](#_Toc122432019) 147-156

[Overview](#_Toc122432020) 147

[WBEM/CIM/WMIC](#_Toc122432021) 147

[WMI Attacks](#_Toc122432022) 148-151

[Recon](#_Toc122432023) 149

[Privilege Escalation](#_Toc122432024) 150

[wmic service / Get-WmiObject –Class win32\_process](#_Toc122432025) 150

[Lateral movement](#_Toc122432026) 151

[process call create](#_Toc122432027) 151

[Capturing WMI commands](#_Toc122432028) 152

[Auditing WMI Persistence](#_Toc122432029) 153-154

[‘WMI-Activity/Operational’ log](#_Toc122432030) 153

[Quick wins](#_Toc122432031) 154

[PowerShell logging](#_Toc122432032) 156-171

[WinRM (PowerShell Remoting)](#_Toc122432033) 158

[PS downgrade attacks](#_Toc122432034) 158

[Enable PowerShell logging](#_Toc122432035) 159

[Script block logging](#_Toc122432036) 160

[PowerShell ‘stealth’ syntax](#_Toc122432037) 162

[Quick wins](#_Toc122432038) 163

[PowerShell script obfuscation](#_Toc122432039) 163-164

[Cyberchef](#_Toc122432040) 164

[PowerShell transcript logs](#_Toc122432041) 167-169

[PSReadline/’ConsoleHost\_history.txt’ (PowerShell command history)](#_Toc122432042) 171

[Event log summary/cheatsheet](#_Toc122432043) 173

[Event log collection](#_Toc122432044) 174-177

[Live system collection](#_Toc122432045) 174

[Log forwarding](#_Toc122432046) 175

[PowerShell - ‘Get-WinEvent’](#_Toc122432047) 176

[Scaling log analysis](#_Toc122432048) 177

[Event log resources](#_Toc122432049) 179-182

[Sysmon](#_Toc122432050) 179-180

[Log analysis resources](#_Toc122432051) 182

# Advanced Evidence of Execution

## Prefetch

### Review

#### Evidence of execution

### ‘PECmd.exe’ – Prefetch file analysis

#### Overview

#### Usage

#### Output and analysis

## ShimCache (AppCompatCache)

### Timestomp detection

### ‘AppCompatParser.exe’ – Execution history

## Amcache.hve

### Overview

### Parsing Amcache

#### Auditing executable presence

#### Auditing installed drivers

### ‘amcacheparser.exe’ – Amcache extraction

#### Overview

#### Example output

##### Associated vs. Unassociated

##### What to look for

## Application Execution Analysis

### Scaling automatic execution analysis

#### Overview

### ‘appcompatprocessor.py’ – Scaling analysis

#### Stacking with appcompatprocessor.py

##### Least frequency of occourance

# Even Log Analysis for Responders and Hunters

## Event Log Fundamentals

### Where to find event logs

#### History

#### Max size options

### Types of event logs

### Security log

#### Categories

## Analysis Scenarios

### Security log: Tracking account usage

#### Detailed log properties

#### Logon type codes

#### Identifying logon sessions

##### Logon ID

##### Session duration/length

#### Identifying brute force attacks

#### Built-in Accounts

#### Tracking admin account activity

#### Auditing account creation

#### Tracking RDP sessions

##### Remote desktop logging

##### TerminalServices/RDPclient log

#### Account logon events

##### NTLM

##### Kerberos

##### Logon error codes

##### Pass the hash

### Security log: Tracking recon

#### Account and group enumeration

### Security log: Tracking lateral movement

#### Network shares

##### Overview

##### Cobalt strike example

#### Runas / Explicit Credentials

##### Runas detection

##### Cobalt strike example (make\_token & pth)

#### Auditing scheduled tasks

##### Hunting

##### Remote task scheduler artifacts

#### Suspicious services

##### Overview

##### PsExec

#### Event log clearing

#### Event log attacks

##### mimikatz - ‘event::drop’

##### DanderSpiritz – ‘eventlogedit’

##### Invoke-Phant0m

### Event log analysis tools

#### Event log explorer

#### ‘EvtxCmd.exe’ – cmd event log parser

##### EvtxCmd maps

##### Grouping and filtering EvtxCmd results

# Lateral Movement Adverary Tactics

## Lateral movement: Copy malware

### RDP services

#### Source system artifacts

#### Destination system artifacts

### Windows admin shares

#### Source system artifacts

#### Destination system artifacts

## Lateral movement: Execution

### PsExec

#### Source system artifacts

#### Destination system artifacts

### Remote management tools

#### Remote services

##### Overview

##### Artifacts

#### Remote scheduled tasks

##### Overview

##### Artifacts

#### Remote registry interaction

##### Overview

##### Artifacts

#### Windows remote shell (WinRS)

##### Overview

##### Artifacts

#### WMI

##### Artifacts

#### PowerShell Remoting

##### Source system artifacts

##### Destination system artifacts

#### Application deployment software

#### Vulnerability Exploitation

# CLI, PowerShell and WMI Analysis

## Evidence of malware execution

### Warning, error and crash logs

### ‘report.wer’ – Windows error reporting

### Process tracking and capturing CLI

#### CLI Auditing example

### WMI – Windows Management Instrumentation

#### Overview

##### WBEM/CIM/WMIC

#### WMI Attacks

##### Recon

##### Privilege Escalation

###### wmic service / Get-WmiObject –Class win32\_process

##### Lateral movement

###### process call create

#### Capturing WMI commands

#### Auditing WMI Persistence

##### ‘WMI-Activity/Operational’ log

##### Quick wins

### PowerShell logging

#### WinRM (PowerShell Remoting)

#### PS downgrade attacks

#### Enable PowerShell logging

#### Script block logging

#### PowerShell ‘stealth’ syntax

#### Quick wins

#### PowerShell script obfuscation

##### Cyberchef

#### PowerShell transcript logs

#### PSReadline/’ConsoleHost\_history.txt’ (PowerShell command history)

### Event log summary/cheatsheet

### Event log collection

#### Live system collection

#### Log forwarding

#### PowerShell - ‘Get-WinEvent’

#### Scaling log analysis

### Event log resources

#### Sysmon

#### Log analysis resources