

# 508.2 – Intrusion Analysis

## Advanced Evidence of Execution..... 6-33

Prefetch .....	6-13
Review .....	6-8
Evidence of execution .....	8
‘PECmd.exe’ – Prefetch file analysis.....	9-13
Overview .....	9
Usage .....	10
Output and analysis .....	11
ShimCache (AppCompatCache) .....	14-16
Timescomp detection.....	15
‘AppCompatParser.exe’ – Execution history.....	16
Amcache.hve .....	17-26
Overview.....	17-18
Parsing Amcache .....	19-22
Auditing executable presence .....	19
Auditing installed drivers.....	21
‘amcacheparser.exe’ – Amcache extraction .....	23-26
Overview .....	23
Example output.....	24-25
Associated vs. Unassociated.....	24
What to look for .....	25
Application Execution Analysis .....	2
Scaling automatic execution analysis.....	27-31
Overview .....	27
‘appcompatprocessor.py’ – Scaling analysis.....	28-30
Stacking with appcompatprocessor.py.....	32
Least frequency of occurrence.....	32

## Even Log Analysis for Responders and Hunters..... 37-43

Event Log Fundamentals .....	38-43
Where to find event logs.....	38-39
History.....	38
Max size options.....	39
Types of event logs.....	40

Security log.....	41-43
Categories.....	42
Analysis Scenarios .....	44-
Security log: Tracking account usage .....	46-72
Detailed log properties .....	48
Logon type codes.....	50
Identifying logon sessions.....	52
Logon ID .....	52
Session duration/length .....	52
Identifying brute force attacks .....	54
Built-in Accounts.....	56-57
Tracking admin account activity .....	58
Auditing account creation.....	60
Tracking RDP sessions .....	62-67
Remote desktop logging.....	67
TerminalServices/RDPClient log.....	67
Account logon events.....	69-72
NTLM .....	69
Kerberos.....	69
Logon error codes.....	70-71
Pass the hash .....	72
Security log: Tracking recon .....	74-75
Account and group enumeration.....	74-75
Security log: Tracking lateral movement .....	85-104
Network shares .....	85-86
Overview .....	85
Cobalt strike example.....	86
Runas / Explicit Credentials.....	88-92
Runas detection.....	90
Cobalt strike example (make_token & pth).....	92
Auditing scheduled tasks .....	94-99
Hunting .....	95
Remote task scheduler artifacts .....	98-99
Suspicious services.....	101-104
Overview .....	101
PsExec .....	103-104
Event log clearing.....	106-107
Event log attacks.....	109-110

mimikatz - 'event::drop' .....	109
DanderSpiritz - 'eventloggedit' .....	109
Invoke-Phantom .....	109
Event log analysis tools .....	77-82
Event log explorer .....	77
'EvtxCmd.exe' - cmd event log parser .....	79-82
EvtxCmd maps .....	80
Grouping and filtering EvtxCmd results .....	82
<b>Lateral Movement Adverary Tactics. 113-134</b>	
Lateral movement: Copy malware .....	113-118
RDP services .....	114-116
Source system artifacts .....	114-115
Destination system artifacts .....	116
Windows admin shares .....	117-118
Source system artifacts .....	117
Destination system artifacts .....	118
Lateral movement: Execution .....	119-134
PsExec .....	120-122
Source system artifacts .....	120
Destination system artifacts .....	121-122
Remote management tools .....	123-134
Remote services .....	125
Overview .....	123-124
Artifacts .....	125
Remote scheduled tasks .....	126
Overview .....	123-124
Artifacts .....	126
Remote registry interaction .....	124
Overview .....	124
Windows remote shell (WinRS) .....	123-124
Overview .....	123-124
WMI .....	127-128
Artifacts .....	127-128
PowerShell Remoting .....	129-131
Source system artifacts .....	129-130
Destination system artifacts .....	131
Application deployment software .....	132-133
Vulnerability Exploitation .....	134
Warning, error and crash logs .....	139-140
'report.wer' - Windows error reporting .....	142
Process tracking and capturing CLI .....	143-145
CLI Auditing example .....	145
WMI - Windows Management Instrumentation. 147-156	
Overview .....	147
WBEM/CIM/WMIC .....	147
WMI Attacks .....	148-151
Recon .....	149
Privilege Escalation .....	150
wmic service / Get-WmiObject -Class win32_process .....	150
Lateral movement .....	151
process call create .....	151
Capturing WMI commands .....	152
Auditing WMI Persistence .....	153-154
'WMI-Activity/Operational' log .....	153
Quick wins .....	154
PowerShell logging .....	156-171
WinRM (PowerShell Remoting) .....	158
PS downgrade attacks .....	158
Enable PowerShell logging .....	159
Script block logging .....	160
PowerShell 'stealth' syntax .....	162
Quick wins .....	163
PowerShell script obfuscation .....	163-164
Cyberchef .....	164
PowerShell transcript logs .....	167-169
PSReadline/'ConsoleHost_history.txt' (PowerShell command history) .....	171
Event log summary/cheatsheet .....	173
Event log collection .....	174-177
Live system collection .....	174
Log forwarding .....	175
PowerShell - 'Get-WinEvent' .....	176
Scaling log analysis .....	177
Event log resources .....	179-182
Sysmon .....	179-180
Log analysis resources .....	182
<b>CLI, PowerShell and WMI Analysis... 139-182</b>	
Evidence of malware execution .....	139-145