

Hunt Evil: Lateral Movement

During incident response and threat hunting, it is critical to understand how attackers move around your network. Lateral movement is an inescapable requirement for attackers to stealthily move from system to system and accomplish their objectives. Every adversary, including the most skilled, will use some form of lateral movement technique described here during a breach. Understanding lateral movement tools and techniques allows responders to hunt more efficiently, quickly perform incident response scoping, and better anticipate future attacker activity.

Tools and techniques to hunt the artifacts described below are detailed in the SANS DFIR course FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting

Additional Event Logs

Process-tracking events, Sysmon, and similar logging capabilities are not listed here for the sake of brevity. However, this type of enhanced logging can provide significant visibility of an intruder's lateral movement, given that the logs are not overwritten or otherwise deleted.

Additional File System Artifacts

Deep-dive analysis techniques such as file carving, volume shadow analysis, and NTFS log file analysis can be instrumental in recovering many of these artifacts (including the recovery of registry and event log files and records).

Additional References

SANS DFIR FOR508 course: <http://sans.org/FOR508>
ATT&CK Lateral Movement: <http://for508.com/attck-lm>
JPCERT Lateral Movement: <http://for508.com/jpcert-lm>

Artifacts in Memory Analysis

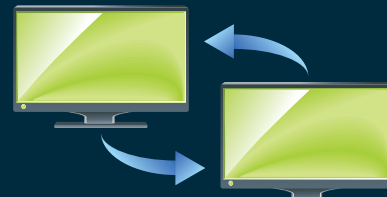
Artifacts in memory analysis will allow for additional tracking of potential evidence of execution and command line history. We recommend auditing and dumping the "conhost" processes on the various systems. Example:
`vol.py -f memory.img --profile=<profile> memdump -n conhost --dmp-dir=.strings -t d -e l *.dmp >> conhost.uni`
Perform searches for executable keywords using grep. Also check running processes (mstsc, rdpclip, etc.).

REMOTE ACCESS

SOURCE

EVENT LOGS	REGISTRY	FILE SYSTEM
<ul style="list-style-type: none">security.evtx4648 - Logon specifying alternate credentials - if NLA enabled on destination<ul style="list-style-type: none">Current logged-on User NameAlternate User NameDestination Host Name/IPProcess NameMicrosoft-Windows-TerminalServices-RDPClient4Operational.evtx1024<ul style="list-style-type: none">Destination Host Name1102<ul style="list-style-type: none">Destination IP Address	<ul style="list-style-type: none">Remote desktop destinations are tracked per-user<ul style="list-style-type: none">NTUSER\Software\Microsoft\Terminal Server Client\ServersShimCache - SYSTEM<ul style="list-style-type: none">mstsc.exe Remote Desktop ClientBAM/DAM - SYSTEM - Last Time Executed<ul style="list-style-type: none">mstsc.exe Remote Desktop ClientAmCache.hve - First Time Executed<ul style="list-style-type: none">mstsc.exe	<ul style="list-style-type: none">Jumplist - C:\Users\<Username>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations*psexec.exe-(hash).pfAutomaticDestinations-ms<ul style="list-style-type: none">Tracks remote desktop connection destination and timesPrefetch - C:\Windows\Prefetch*mstsc.exe-(hash).pfBitmap Cache - C:\Users\<USERNAME>\AppData\Local\Microsoft\Terminal Server Client\Cache<ul style="list-style-type: none">bcache###.bmccache####.bin

Remote Desktop



DESTINATION

EVENT LOGS	REGISTRY	FILE SYSTEM
<ul style="list-style-type: none">Security Event Log - security.evtx4624 Logon Type 10<ul style="list-style-type: none">Source IP/Logon User Name4778/4779<ul style="list-style-type: none">IP Address of Source/Source System NameLogon User NameMicrosoft-Windows-RemoteDesktopServices-RdpCoreTS4Operational.evtx131 - Connection Attempts<ul style="list-style-type: none">Source IP/Logon User Name98 - Successful Connections	<ul style="list-style-type: none">Microsoft-Windows-TerminalServices-RemoteConnectionManager4Operational.evtx1149<ul style="list-style-type: none">Source IP/Logon User NameBlank user name may indicate use of Sticky KeysMicrosoft-Windows-TerminalServices-LocalSessionManager4Operational.evtx21, 22, 25<ul style="list-style-type: none">Source IP/Logon User Name41<ul style="list-style-type: none">Logon User Name	<ul style="list-style-type: none">Prefetch - C:\Windows\Prefetch*psxescv.exe-(hash).pf*tstheme.exe-(hash).pfAmCache.hve - First Time Executed<ul style="list-style-type: none">rdpclip.exetstheme.exe

SOURCE

EVENT LOGS	REGISTRY	FILE SYSTEM
<ul style="list-style-type: none">security.evtx4648 - Logon specifying alternate credentials<ul style="list-style-type: none">Current logged-on User NameAlternate User NameDestination Host Name/IPProcess NameMicrosoft-Windows-SmbClient4Security.evtx31001 - Failed logon to destination<ul style="list-style-type: none">Destination Host NameUser Name for failed logonReason code for failed destination logon (e.g. bad password)	<ul style="list-style-type: none">MountPoints2 - Remotely mapped shares<ul style="list-style-type: none">NTUSER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2Shellbags - USRCLASS.DAT<ul style="list-style-type: none">Remote folders accessed inside an interactive session via Explorer by attackersShimCache - SYSTEM<ul style="list-style-type: none">net.exenet1.exeBAM/DAM - NTUSER.DAT - Last Time Executed<ul style="list-style-type: none">net.exenet1.exeAmCache.hve - First Time Executed<ul style="list-style-type: none">net.exenet1.exe	<ul style="list-style-type: none">Prefetch - C:\Windows\Prefetch*net.exe-(hash).pf*net1.exe-(hash).pfUser Profile Artifacts<ul style="list-style-type: none">Review shortcut files and jumplists for remote files accessed by attackers, if they had interactive access (RDP)

Map Network Shares (net.exe)



```
net use z: \\host\c$ /user:domain\username <password>
```

DESTINATION

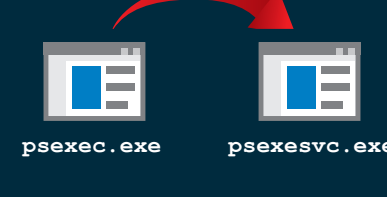
EVENT LOGS	REGISTRY	FILE SYSTEM
<ul style="list-style-type: none">Security Event Log - security.evtx4624 Logon Type 3<ul style="list-style-type: none">Source IP/Logon User Name4672<ul style="list-style-type: none">Logon User NameLogon by user with administrative rightsRequirement for accessing default shares such as C\$ and ADMIN\$4776 - NTLM if authenticating to Local System<ul style="list-style-type: none">Source Host Name/Logon User Name	<ul style="list-style-type: none">4768 - TGT Granted<ul style="list-style-type: none">Source Host Name/Logon User Name4769 - Service Ticket Granted if authenticating to Domain Controller<ul style="list-style-type: none">Destination Host Name/Logon User NameSource IPAvailable only on domain controller5140 - Share Access5145 - Auditing of shared files - NOISY!	<ul style="list-style-type: none">File Creation<ul style="list-style-type: none">Attacker's files (malware) copied to destination systemLook for Modified Time before Creation TimeCreation Time is time of file copy

REMOTE EXECUTION

SOURCE

EVENT LOGS	REGISTRY	FILE SYSTEM
<ul style="list-style-type: none">security.evtx4648 - Logon specifying alternate credentials<ul style="list-style-type: none">Current logged-on User NameAlternate User NameDestination Host Name/IPProcess Name	<ul style="list-style-type: none">NTUSER.DAT<ul style="list-style-type: none">Software\SysInternals\Psexec\EulaAcceptedShimCache - SYSTEM<ul style="list-style-type: none">psexec.exeBAM/DAM - SYSTEM - Last Time Executed<ul style="list-style-type: none">psexec.exeAmCache.hve - First Time Executed<ul style="list-style-type: none">psexec.exe	<ul style="list-style-type: none">Prefetch - C:\Windows\Prefetch*psexec.exe-(hash).pfPossible references to other files accessed by psexec.exe, such as executables copied to target system with the "-c" optionFile Creation<ul style="list-style-type: none">psexec.exe file downloaded and created on local host as the file is not native to Windows

Psexec



```
psexec.exe \\host -accepteula -d -c c:\temp\evil.exe
```

DESTINATION

EVENT LOGS	REGISTRY	FILE SYSTEM
<ul style="list-style-type: none">security.evtx4624 Logon Type 3 (and Type 2 if "-u" Alternate Credentials are used)<ul style="list-style-type: none">Source IP/Logon User Name4672<ul style="list-style-type: none">Logon User NameLogon by user with administrative rightsRequirement for access default shares such as C\$ and ADMIN\$5140 - Share Access<ul style="list-style-type: none">ADMIN\$ share used by PsExecsystem.evtx7045 - Service Install	<ul style="list-style-type: none">New service creation configured in SYSTEM\CurrentControlSet\Services\PSEXESVC<ul style="list-style-type: none">"-e" option can allow attacker to rename serviceShimCache - SYSTEM<ul style="list-style-type: none">psxescv.exeAmCache.hve - First Time Executed<ul style="list-style-type: none">psxescv.exe	<ul style="list-style-type: none">Prefetch - C:\Windows\Prefetch*evil.exe-(hash).pf*evill.exe-(hash).pfFile Creation<ul style="list-style-type: none">User profile directory structure created unless "-e" option usedpsxescv.exe will be placed in ADMIN\$ (Windows) by default, as well as other executables (evil.exe) pushed by PsExec

SOURCE

EVENT LOGS	REGISTRY	FILE SYSTEM
<ul style="list-style-type: none">security.evtx4648 - Logon specifying alternate credentials<ul style="list-style-type: none">Current logged-on User NameAlternate User NameDestination Host Name/IPProcess Name	<ul style="list-style-type: none">ShimCache - SYSTEM<ul style="list-style-type: none">at.exeschtasks.exeBAM/DAM - SYSTEM - Last Time Executed<ul style="list-style-type: none">at.exeschtasks.exeAmCache.hve - First Time Executed<ul style="list-style-type: none">at.exeschtasks.exe	<ul style="list-style-type: none">Prefetch - C:\Windows\Prefetch*at.exe-(hash).pf*schtasks.exe-(hash).pf

Scheduled Tasks



```
at \\host 13:00 "c:\temp\evil.exe" schtasks /CREATE /TN taskname /TR c:\temp\evil.exe /SC once /RU "SYSTEM" /ST 13:00 /S host /U username
```

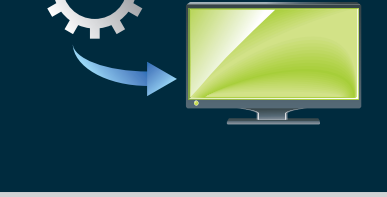
DESTINATION

EVENT LOGS	REGISTRY	FILE SYSTEM
<ul style="list-style-type: none">security.evtx4624 Logon Type 3<ul style="list-style-type: none">Source IP/Logon User Name4672<ul style="list-style-type: none">Logon User NameLogon by a user with administrative rightsRequirement for accessing default shares such as C\$ and ADMIN\$system.evtx7045 - Service Install	<ul style="list-style-type: none">SOFTWARE<ul style="list-style-type: none">Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\TasksMicrosoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\ShimCache - SYSTEM<ul style="list-style-type: none">evil.exeAmCache.hve - First Time Executed<ul style="list-style-type: none">evil.exe	<ul style="list-style-type: none">File Creation<ul style="list-style-type: none">evil.exeJob files created in C:\Windows\TasksXML task files created in C:\Windows\System32\TasksAuthor tag under "RegistrationInfo" can identify:<ul style="list-style-type: none">Source system nameCreator usernamePrefetch - C:\Windows\Prefetch*evil.exe-(hash).pf

SOURCE

EVENT LOGS	REGISTRY	FILE SYSTEM
<ul style="list-style-type: none">security.evtx4648 - Logon specifying alternate credentials<ul style="list-style-type: none">Current logged-on User NameAlternate User NameDestination Host Name/IPProcess Name	<ul style="list-style-type: none">ShimCache - SYSTEM<ul style="list-style-type: none">sc.exeBAM/DAM - SYSTEM - Last Time Executed<ul style="list-style-type: none">sc.exeAmCache.hve - First Time Executed<ul style="list-style-type: none">sc.exe	<ul style="list-style-type: none">Prefetch - C:\Windows\Prefetch*sc.exe-(hash).pf

Services



```
sc \\host create servicename binpath= "c:\temp\evil.exe" sc \\host start servicename
```

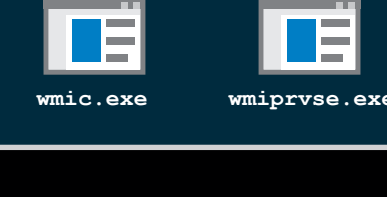
DESTINATION

EVENT LOGS	REGISTRY	FILE SYSTEM
<ul style="list-style-type: none">security.evtx4624 Logon Type 3<ul style="list-style-type: none">Source IP/Logon User Name4697 - Security records service install, if enabled<ul style="list-style-type: none">Enabling non-default Security events such as ID 4697 are particularly useful if only the Security logs are forwarded to a centralized log server	<ul style="list-style-type: none">system.evtx7034 - Service crashed unexpectedly7035 - Service sent a Start/Stop control7036 - Service started or stopped7040 - Start type changed (Boot On Request Disabled)7045 - A Service was installed on the system	<ul style="list-style-type: none">File Creation<ul style="list-style-type: none">evil.exe or evil.dll malicious service executable or service DLLPrefetch - C:\Windows\Prefetch*evil.exe-(hash).pf

SOURCE

EVENT LOGS	REGISTRY	FILE SYSTEM
<ul style="list-style-type: none">security.evtx4648 - Logon specifying alternate credentials<ul style="list-style-type: none">Current logged-on User NameAlternate User NameDestination Host Name/IPProcess Name	<ul style="list-style-type: none">ShimCache - SYSTEM<ul style="list-style-type: none">wmic.exeBAM/DAM - SYSTEM - Last Time Executed<ul style="list-style-type: none">wmic.exeAmCache.hve - First Time Executed<ul style="list-style-type: none">wmic.exe	<ul style="list-style-type: none">Prefetch - C:\Windows\Prefetch*wmic.exe-(hash).pf

WMI/WMIC



```
wmic /node:host process call create "evil.exe" Invoke-WmiMethod -Computer host -Class Win32_Process -Name create -Argument "c:\temp\evil.exe"
```

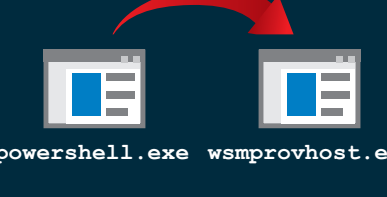
DESTINATION

EVENT LOGS	REGISTRY	FILE SYSTEM
<ul style="list-style-type: none">security.evtx4624 Logon Type 3<ul style="list-style-type: none">Source IP/Logon User Name4672<ul style="list-style-type: none">Logon User NameLogon by an user with administrative rightsMicrosoft-Windows-WMI-Activity4Operational.evtx5857<ul style="list-style-type: none">Indicates time of wmicprvse execution and path to provider DLL - attackers sometimes install malicious WMI provider DLLs5860, 5861<ul style="list-style-type: none">Registration of Temporary (5860) and Permanent (5861) Event Consumers. Typically used for persistence, but can be used for remote execution.	<ul style="list-style-type: none">ShimCache - SYSTEM<ul style="list-style-type: none">wmicprvse.exeevil.exemfcomp.exeAmCache.hve - First Time Executed<ul style="list-style-type: none">wmicprvse.exeevil.exemfcomp.exe	<ul style="list-style-type: none">File Creation<ul style="list-style-type: none">evil.exeevil.mof - .mof files can be used to manage the WMI RepositoryPrefetch - C:\Windows\Prefetch*evil.exe-(hash).pf*wmiexecv.exe-(hash).pf*mfcomp.exe-(hash).pfUnauthorized changes to the WMI Repository in C:\Windows\System32\wbem\Repository

SOURCE

EVENT LOGS	REGISTRY	FILE SYSTEM
<ul style="list-style-type: none">security.evtx4648 - Logon specifying alternate credentials<ul style="list-style-type: none">Current logged-on User NameAlternate User NameDestination Host Name/IPProcess NameMicrosoft-Windows-WinRM4Operational.evtx6 - WSMAN Session initialize<ul style="list-style-type: none">Session createdDestination Host Name or IPCurrent logged-on User Name	<ul style="list-style-type: none">8, 15, 16, 33 - WSMAN Session deinitialization<ul style="list-style-type: none">Closing of WSMAN sessionCurrent logged-on User NameMicrosoft-Windows-PowerShell4Operational.evtx40961, 40962<ul style="list-style-type: none">Records the local initiation of powershell.exe and associated user account8193 & 8194<ul style="list-style-type: none">Session created8197 - Connect<ul style="list-style-type: none">Session closed	<ul style="list-style-type: none">Prefetch - C:\Windows\Prefetch*powershell.exe-(hash).pf*powershell.exe-(hash).pfPowerShell scripts (.ps1 files) that run within 10 seconds of powershell.exe launching will be tracked in powershell.exe prefetch fileCommand history C:\Users\<USERNAME>\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt<ul style="list-style-type: none">With PS v5+, a history file with previous 4096 commands is maintained per user

PowerShell Remoting



```
Enter-PSsession -ComputerName host Invoke-Command -ComputerName host -ScriptBlock {Start-Process c:\temp\evil.exe}
```

DESTINATION

EVENT LOGS	REGISTRY	FILE SYSTEM
<ul style="list-style-type: none">security.evtx4624 Logon Type 3<ul style="list-style-type: none">Source IP/Logon User Name4672<ul style="list-style-type: none">Logon User NameLogon by an user with administrative rightsMicrosoft-Windows-PowerShell4Operational.evtx4103, 4104 - Script Block logging<ul style="list-style-type: none">Logs suspicious scripts by default in PS v5Logs all scripts if configured53504 - Records the authenticating user	<ul style="list-style-type: none">Microsoft-Windows-WMI-Activity4Operational.evtx5857<ul style="list-style-type: none">Indicates time of wmicprvse execution and path to provider DLL - attackers sometimes install malicious WMI provider DLLs5860, 5861<ul style="list-style-type: none">Registration of Temporary (5860) and Permanent (5861) Event Consumers. Typically used for persistence, but can be used for remote execution.	<ul style="list-style-type: none">File Creation<ul style="list-style-type: none">evil.exeWith Enter-PSsession, a user profile directory may be createdPrefetch - C:\Windows\Prefetch*evil.exe-(hash).pf*wsmprovhost.exe-(hash).pf

Evidence of Program Execution

UserAssist

Description: GUI-based programs launched from the desktop are tracked in the launcher on a Windows System.

Location: NTUSER.DAT HIVE
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count

Interpretation: All values are NOT-13 Encoded
- GUID for Win7/8/10
- CEBFF5CD Executable File Execution
- FAE57C4B Shortcut File Execution

BAM/DAM

Description: Windows Background Activity Moderator (BAM)

Location: Win10
SYSTEM\CurrentControlSet\Services\Bam\UserSettings\{SID}
SYSTEM\CurrentControlSet\Services\DAM\UserSettings\{SID}

Investigative Notes: Provides full path of the executable file that was run on the system and last execution date/time

RecentApps

Description: Program execution launched on the Win10 system is tracked in the RecentApps key

Location: Win10
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Search\RecentApps

Interpretation: Each GUID key points to a recent application.
AppID = Name of Application
LastAccessTime = Last execution time in UTC
LaunchCount = Number of times executed

ShimCache

Description: Windows Application Compatibility Database is used by Windows to identify possible application compatibility challenges with executables.

Location: Windows 7/8/10
SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache

Interpretation: Any executable run on the Windows system could be found in this key. You can use this key to identify systems that specific malware was executed on. In addition, based on the interpretation of the time-based data you might be able to determine the last time of execution or activity on the system.

- Windows 7/8/10 contains at most 1024 entries
- LastupdateTime does not exist on Win7/8/10 systems

Jump Lists

Description: The Windows 7-10 task bar (Jump List) is engineered to allow users to "jump" or access items they have frequently or recently used quickly and easily. This functionality cannot only include recent media files, it must also include recent tasks.

Location: Win7/8/10
C:\Users\<PROFILE>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

Interpretation: - First time of execution of application.
- Creation Time = First time item added to the AppID file.
- Last time of execution of application with file open.
- Modification Time = Last time item added to the AppID file.
- List of Jump List IDs -> www.forensicswiki.org/wiki/List_of_Jump_List_IDs

Prefetch

Description: Increases performance of a system by pre-loading code pages of commonly used applications. Cache Manager monitors all files and directories referenced for each application or process and maps them into a .pf file. Utilized to know an application was executed on a system.

Location: Win7/8/10
C:\Windows\Prefetch

Interpretation: - Each .pf will include last time of execution, number of times run, and device and file handles used by the program
- Date/Time file by that name and path was first executed
- Creation Date of .pf file (-10 seconds)
- Date/Time file by that name and path was last executed
- Embedded last execution time of .pf file
- Last modification date of .pf file (-10 seconds)
- Win8-10 will contain last 8 times of execution

Amcache.hve

Description: ProgramDataUpdater (a task associated with the Application Experience Service) uses the registry file AmCache.hve to store data during process creation

Location: Win7/8/10
C:\Windows\AppCompat\Programs\AmCache.hve (Windows 7/8/10)

Interpretation: - AmCache.hve - Keys = AmCache.hve\Root\Files\{Volume GUID}\#####
- Entry for every executable run, full path information, File's \$StandardInfo Last Modification Time, and Disk volume the executable was run from
- First Run Time = Last Modification Time of Key
- SHA1 hash of executable also contained in the key