## LATERAL MOVEMENT ANALYSIS CHEAT SHEET v1.0 by Huntsman

Lateral Movement Analysis Cheat Sheet for DFIR Team to analysis, investigation and response.



WinRS

winrshost.exe

github.com/WirapongP Nuntsman-dfir.medium.com

SERVICES	
Detection	Investigation
	Source Host & Compromised Account Nam

· New Logon\Account Name services.exe had.exe Service Name & Service File Name

had.exe

Windows Event Logs (Security.evtx) - Event ID 4624 · Network Information\Source Network Address Windows Event Logs (System.evtx) - Event ID 7045 Service Name Service File Name Process Name & Process Command Line Windows Event Logs (Security.evtx) - Event ID 4688

Source Host & Compromised Account Name

**Process Name & Process Command Line** 

Creator Process Name == "winrshost.exe"

· Process Information\New Process Name

· Process Information\Process Commane Line

· Process Information\Process Commane Line

Logon Type == 3

· New Logon\Account Name

Windows Event Logs (Security.evtx) - Event ID 4624

Network Information\Source Network Address

Windows Event Logs (Security.evtx) - Event ID 4688

Creator Process Name == "Services exe" Process Information\New Process Name · Process Information\Process Commane Line

1. Change Password of Compromised Account 2. Kill Malware Process

1. Change Password of Compromised Account

· SYSTEM\CurrentControlSet\Services\[Service Name]

2. Delete Service >sc delete [Service Name]

3. Kill Malware Process

4. Delete Malware File

6. Investigate at Source Host

5. Malware Analysis

3. Delete Malware File 4. Malware Analysis 5. Investigate at Source Host

Powershell

wsmprovhost.exe

WMI/WMIC

wmiprvse.exe

Source Host & Compromised Account Name

Process Name & Process Command Line

Process Information\New Process Name

Windows Event Logs (Microsoft-Windows-

Source Host & Compromised Account Name

Windows Event Logs (Security.evtx) - Event ID 4624

· Network Information\Source Network Address

Process Name & Process Command Line Windows Event Logs (Security.evtx) - Event ID 4688

Creator Process Name == "wmiprvse.exe

Process Information\New Process Name

Process Information\New Process Name

Process Information\Process Commane Line

· Process Information\Process Commane Line

Process Information\Process Commane Line

PowerShell%4Operational.evtx) - Event ID 4103,4104

Logon Type == 3

Scriptblock

Logon Type == 3

· New Logon\Account Name

had.exe

bad.exe

· New Logon\Account Name

Windows Event Logs (Security.evtx) - Event ID 4624

· Network Information\Source Network Address

Windows Event Logs (Security.evtx) - Event ID 4688 Creator Process Name == "wsmprovhost exe"

> 1. Change Password of Compromised Account 2. Delete task >schtasks /delete /tn [Task Name] C:\Windows\Svstem32\Tasks 3. Kill Malware Process 4 Delete Malware File 5. Malware Analysis 6. Investigate at Source Host

5. Patch

6. Investigate at Source Host

1. Change Password of Compromised Account

1. Change Password of Compromised Account

2 Kill Malware Process

3. Delete Malware File

5. Investigate at Source Host

4 Malware Analysis

2. Kill Malware Process

3 Delete Malware File 4. Malware Analysis

5. Investigate at Source Host

Scheduled Tasks Investigation nvestigation Source Host & Compromised Account Name Source Host & Compromised Account Name 1. Change Password of Compromised Account Windows Event Logs (Security.evtx) - Event ID 4624 2. Kill Malware Process Windows Event Logs (Security.evtx) - Event ID 4624 Logon Type == 3 3. Delete Malware File 4. Malware Analysis · Network Information\Source Network Address PSEXESVC.exe · Network Information\Source Network Address sychost exe (netsycs) had eye · New Logon\Account Name · New Logon\Account Name 5. Investigate at Source Host **Process Name & Process Command Line** Process Name & Process Command Line Windows Event Logs (Security.evtx) - Event ID 4688 Windows Event Logs (Security.evtx) - Event ID 4688 Creator Process Name == "PSEXESVC.exe" Creator Process ID == [Process ID of svchost.exe -k Process Information\New Process Name netsycs1 Process Information\Process Commane Line · Process Information\New Process Name · Process Information\Process Commane Line Task Name & Author Windows Event Logs (Security.evtx) - Event ID 4698 Task Information\Task name · RegistrationInfo\Author **Exploitation of Remote Services** nvestigation Source Host & Compromised Account Name 1. Change Password of Compromised Account **Process Name & Process Command Line** 1. Change Password of Compromised Account 2. Kill Malware Process Windows Event Logs (Security.evtx) - Event ID 4688 2. Kill Malware Process Windows Event Logs (Security.evtx) - Event ID 4624 rdpclip.exe bad.exe 3. Delete Malware File Creator Process Name == "Isass.exe" OR (process of 3. Delete Malware File Logon Type == 10 vuln. service] 4. Malware Analysis

 Network Information\Source Network Address 4. Malware Analysis New Logon\Account Name 5. Investigate at Source Host explorer.exe had eye Abnormal child/parent relationships Process Name & Process Command Line (Hunts evil poster - SANS) Windows Event Logs (Security.evtx) - Event ID 4688 Creator Process Name == "explorer.exe" · Process Information\New Process Name