






HTB Sherlock's Writeup: Logjammer

Sherlock Scenario:

You have been presented with the opportunity to work as a junior DFIR consultant for a big consultancy. However, they have provided a technical assessment for you to complete. The consultancy Forela-Security would like to gauge your Windows Event Log Analysis knowledge. We believe the Cyberjunkie user logged in to his computer and may have taken malicious actions. Please analyze the given event logs and report back.

start:

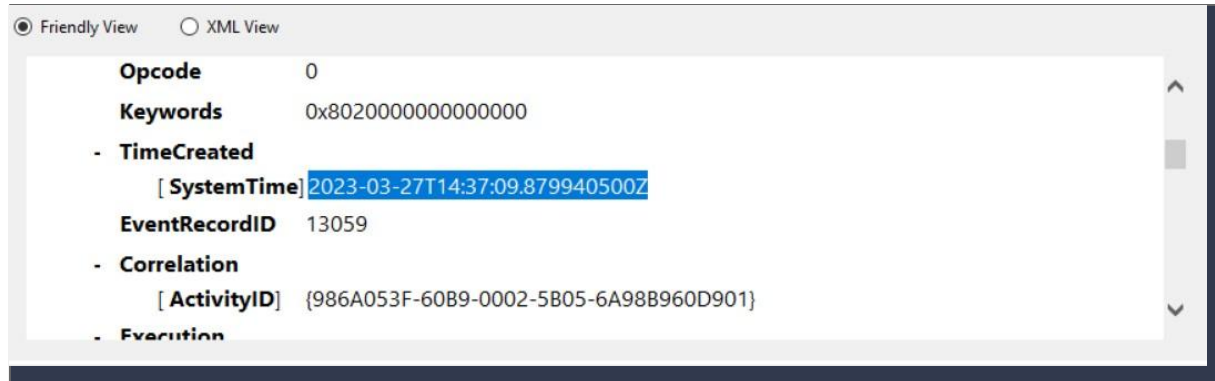
Started the challenge with 5 event viewer files

Date modified	Name
 3/27/2023 1...	Powershell-Operational.evtx
 3/27/2023 9:...	Security.evtx
 3/27/2023 1...	System.evtx
 3/27/2023 9:...	Windows Defender-Operational.evtx
 3/27/2023 9:...	Windows Firewall-Firewall.evtx

task 1: When did the cyberjunkie user first successfully log into his computer? (UTC)

I examined the security log file to find the first successful login attempt by the Cyberjunkie user. I looked for a 4624 event code to identify the successful login and found it.

Answer 1: 27/03/2023 14:37:09



Task 2: The user tampered with firewall settings on the system. Analyze the firewall event logs to find out the Name of the firewall rule added?

I analyzed the firewall event log file and searched for the new rule added by the user. The rule identified is named "Metasploit C2 Bypass."

Answer 2: Metasploit C2 Bypass

The screenshot displays the Windows Firewall event log interface. The top section shows a list of events with columns for Level, Date and Time, Source, Event ID, and Task Category. The bottom section provides a detailed view of a specific event (Event 2004).

Level	Date and Time	Source	Event ID	Task Category
Information	3/27/2023 5:44:43 PM	Windo...	2004	None
Information	3/27/2023 5:37:35 PM	Windo...	2004	None
Information	3/27/2023 5:37:35 PM	Windo...	2004	None
Information	3/27/2023 5:37:35 PM	Windo...	2006	None
Information	3/27/2023 5:37:35 PM	Windo...	2006	None
Information	3/27/2023 5:37:11 PM	Windo...	2010	None
Information	3/27/2023 5:37:11 PM	Windo...	2051	None
Information	3/27/2023 5:37:11 PM	Windo...	2033	None

Event 2004, Windows Firewall With Advanced Security

General Details

☒ Friendly View ☐ XML View

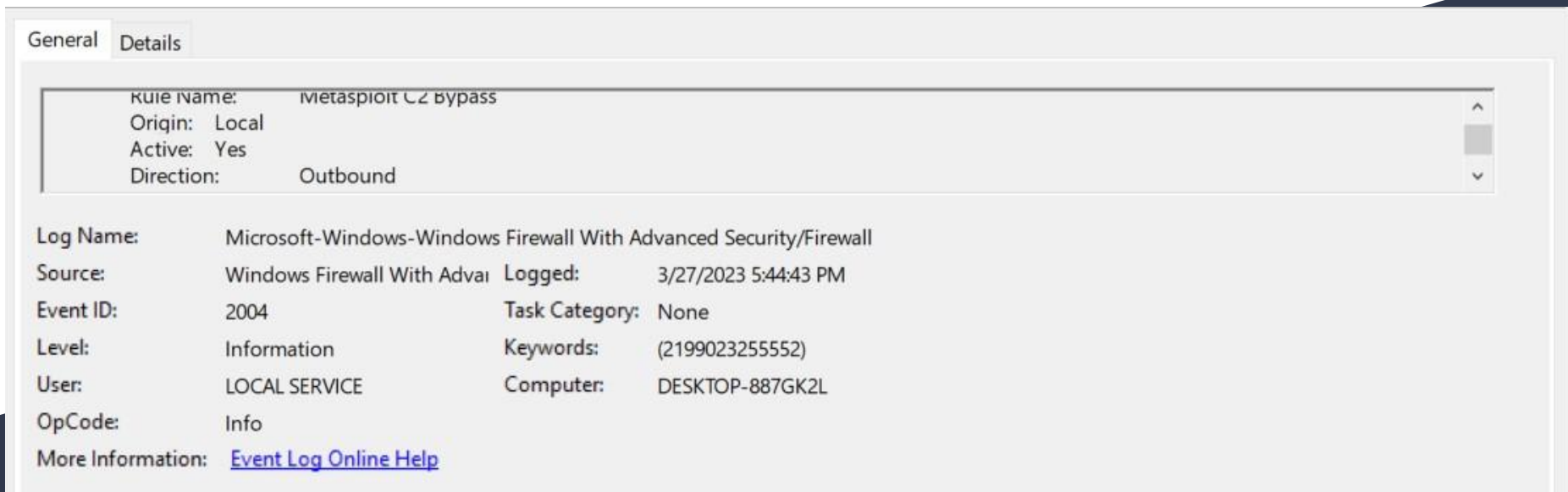
EventData

- RuleId** {11309293-FB68-4969-93F9-7F75A9032570}
- RuleName** Metasploit C2 Bypass
- Origin** 1
- ApplicationPath**
- ServiceName**
- Direction** 2
- Protocol** 6

Task 3: Whats the direction of the firewall rule?

we can see that the direction of the new rule is an outbound rule.

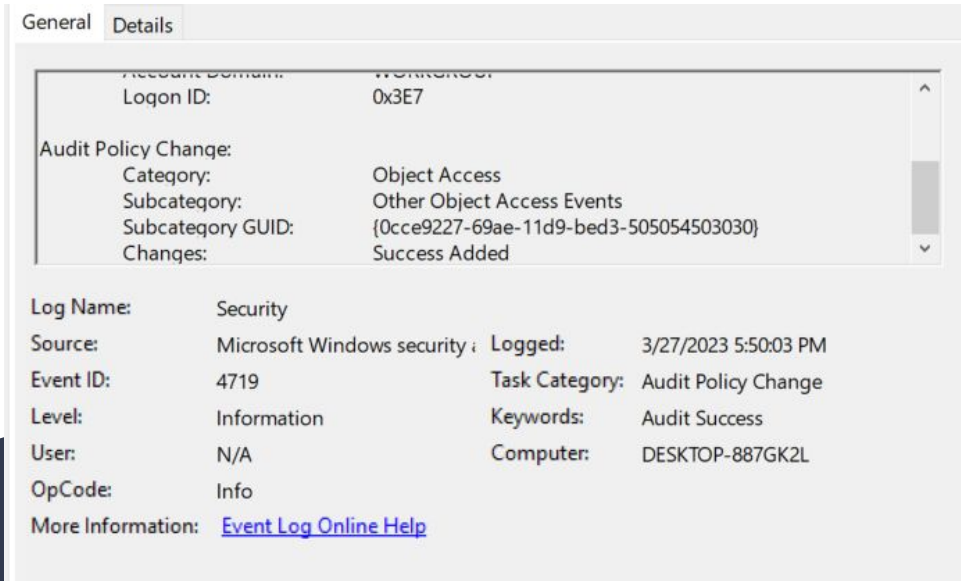
Answer 3: Outbound



Task 4: The user changed audit policy of the computer. Whats the Subcategory of this changed policy?

I examined the audit policy changes and identified the subcategory as "Other Object Access Events."

Answer 4: Other Object Access Events



The screenshot displays the Windows Event Viewer interface. The 'Details' tab is selected, showing a list of event details for Event ID 4719. The 'Audit Policy Change' section is expanded, revealing the following information:

- Logon ID: 0x3E7
- Category: Object Access
- Subcategory: Other Object Access Events
- Subcategory GUID: {0cce9227-69ae-11d9-bed3-505054503030}
- Changes: Success Added

Below this, the 'Log Name' is Security. The 'Source' is Microsoft Windows security. The 'Event ID' is 4719. The 'Level' is Information. The 'User' is N/A. The 'OpCode' is Info. The 'Task Category' is Audit Policy Change. The 'Keywords' are Audit Success. The 'Computer' is DESKTOP-887GK2L. The 'Logged' time is 3/27/2023 5:50:03 PM. A link for 'More Information' is provided as [Event Log Online Help](#).

Task 5: The user "cyberjunkie" created a scheduled task.
Whats the name of this task?

I examined the security file for scheduled task events, searching for those containing the name "cyberjunkie," and identified the created task as "HTB-AUTOMATION."

Answer 5: HTB-AUTOMATION

Filtered Log: file://C:\Users\Malware\Desktop\Event-Logs\Security.evtx; Source: ; Event ID: 4698. Number of events: 1

Level	Date and Time	Source	Event ID	Task Category
Information	3/27/2023 5:51:21 PM	Microsoft Windows secu...	4698	Other Object Access Even...

Event Properties - Event 4698, Microsoft Windows security auditing.

General Details

☒ Friendly View ☐ XML View

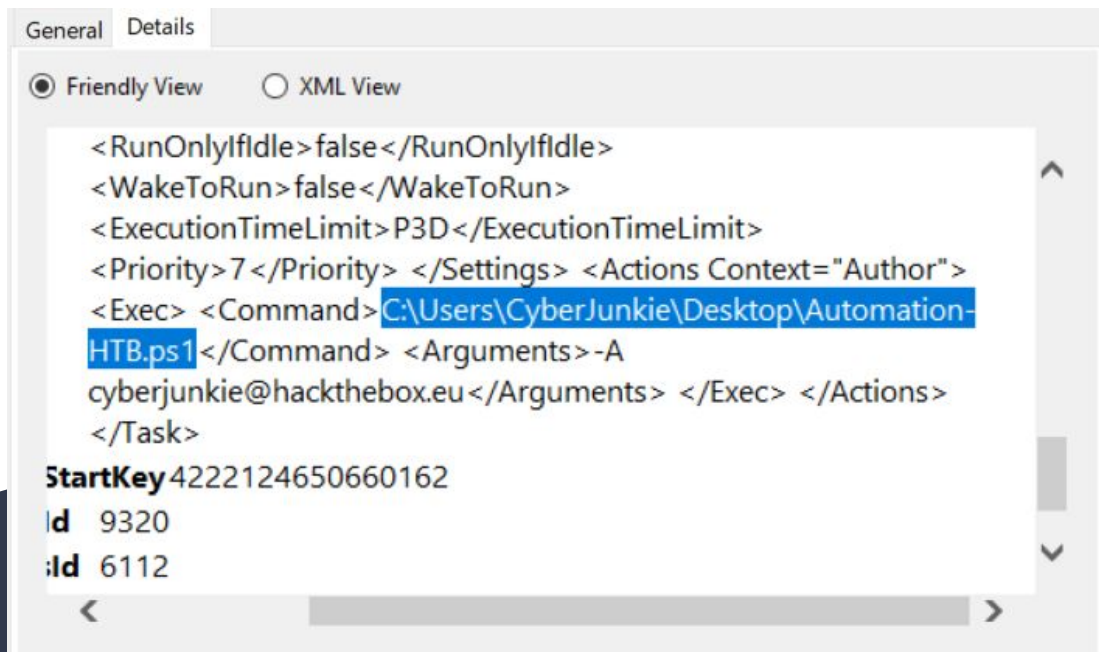
+ System

- EventData
 - SubjectUserSid** S-1-5-21-3393683511-3463148672-371912004-1001
 - SubjectUserName** CyberJunkie
 - SubjectDomainName** DESKTOP-887GK2L
 - SubjectLogonId** 0x25f28
 - TaskName** HTB-AUTOMATION
 - TaskContent** <?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
-RegistrationInfo- <Data> 2023-03-27T07:51:21-15000000 </Data>

Task 6: Whats the full path of the file which was scheduled for the task?

I found his path by looking in the detailed view.

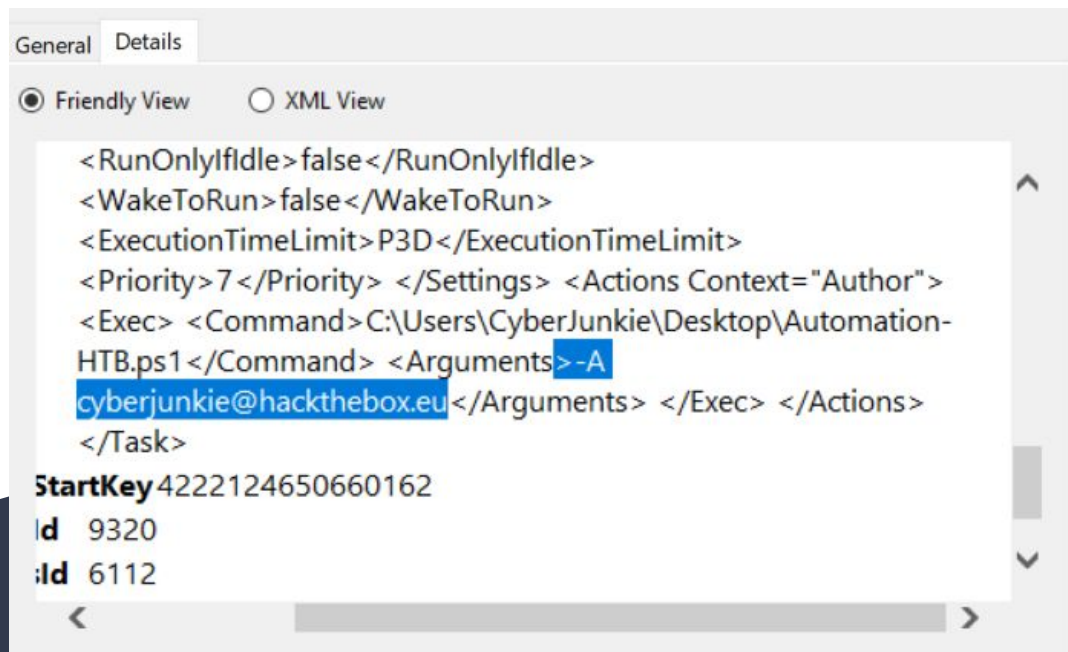
Answer 6: C:\Users\CyberJunkie\Desktop\Automation-HTB.ps1



Task 7: What are the arguments of the command?

We can see the commands argument under the files path.

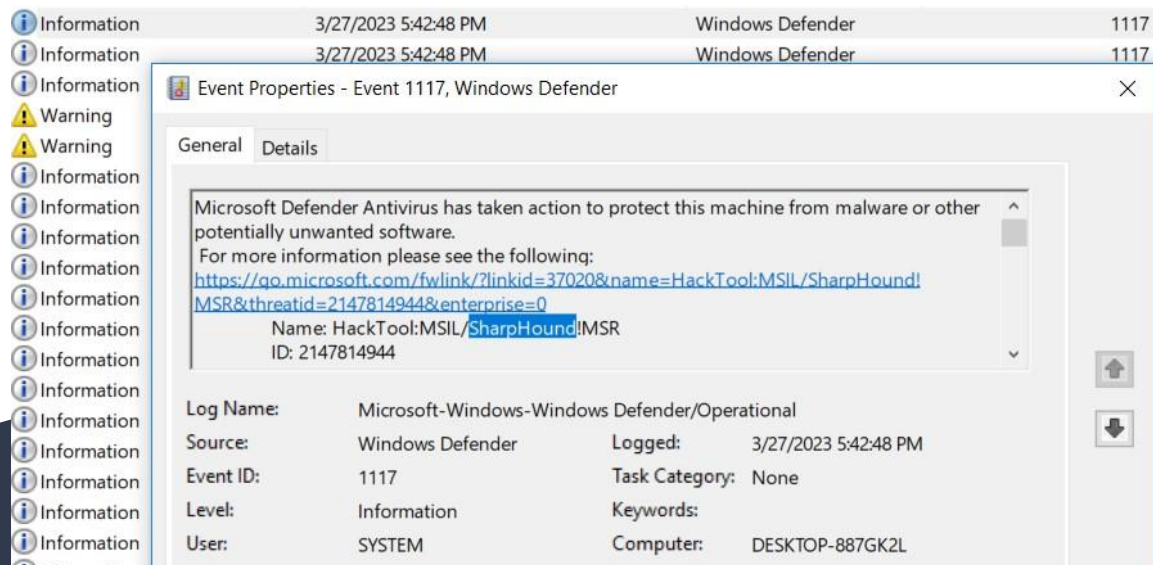
Answer 7: -A cyberjunkie@hackthebox.eu



Task 8: The antivirus running on the system identified a threat and performed actions on it. Which tool was identified as malware by antivirus?

By examining the Windows Defender events, I was able to identify the tool recognized as malware.

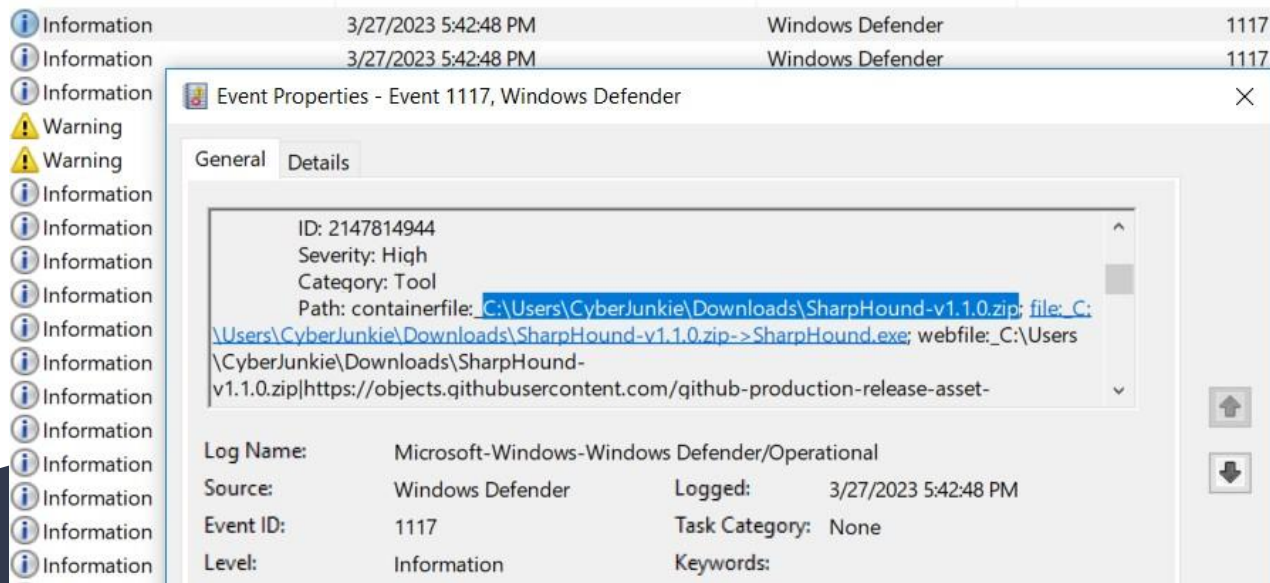
Answer 8: Sharphound



Task 9: Whats the full path of the malware which raised the alert?

In the same event as the previous task, we can see the full path to the malware.

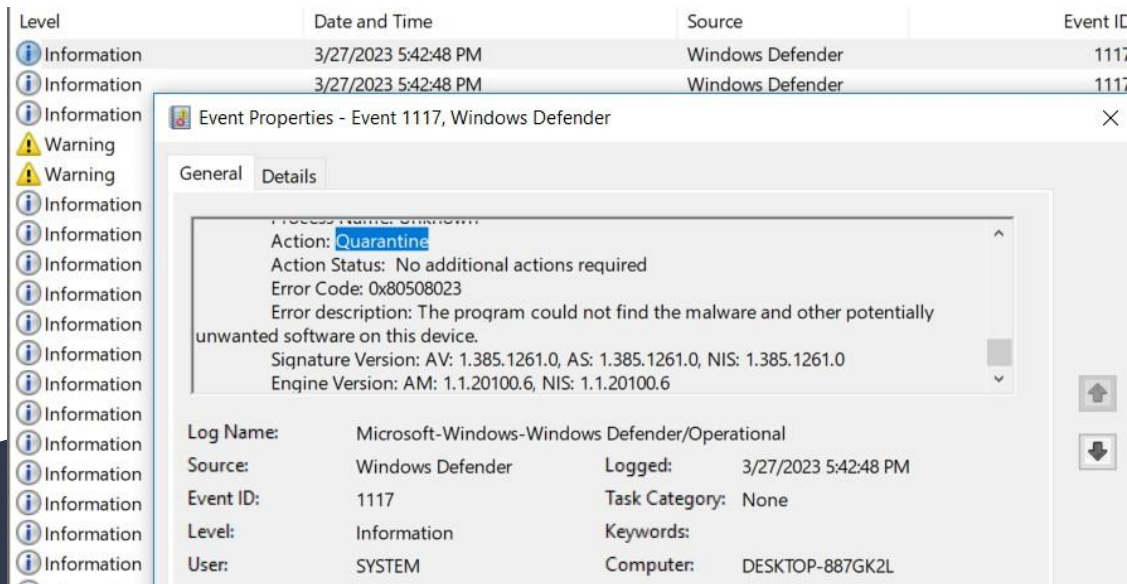
Answer 9: C:\Users\CyberJunkie\Downloads\SharpHound-v1.1.0.zip



Task 10: What action was taken by the antivirus?

By examining the Windows Defender events, I was able to find the event specifying the action taken by the antivirus.

Answer 10: Quarantine



Task 11: The user used Powershell to execute commands. What command was executed by the user?

I found the execute command in the powershell event log.

Answer 11: `Get-FileHash -Algorithm md5 .\Desktop\Automation-HTB.ps1`

The screenshot displays the Windows Event Viewer interface. The 'Event Properties' window for Event 4104 (PowerShell) is open, showing the 'Details' tab. The 'ScriptBlockText' field contains the command: `Get-FileHash -Algorithm md5 .\Desktop\Automation-HTB.ps1`. The 'ScriptBlockId' is `b4fcf72f-abdc-4a84-923f-8e06a758000b`. The 'Path' field is empty. The 'Copy' and 'Close' buttons are visible at the bottom of the window.

In the background, the 'Event Viewer' window is visible, showing a list of events. The 'Task Category' column lists 'Execute a Remote Command' and 'Executing Pipeline'. The 'Number of events: 392' is displayed at the top of the list.

Event ID	Task Category
4104	Execute a Remote Command
4104	Execute a Remote Command
4104	Execute a Remote Command
4104	Execute a Remote Command
4104	Execute a Remote Command
4104	Execute a Remote Command
4104	Execute a Remote Command
4104	Execute a Remote Command
4104	Execute a Remote Command
4104	Execute a Remote Command
4104	Execute a Remote Command
4104	Execute a Remote Command
4103	Executing Pipeline
4103	Executing Pipeline
4103	Executing Pipeline
4103	Executing Pipeline
4103	Executing Pipeline
4104	Execute a Remote Command
4103	Executing Pipeline

Task 12: We suspect the user deleted some event logs. Which Event log file was cleared?

I identified the cleared log in the system event log under the log clear event.

Answer 12: Microsoft-Windows-Windows Firewall With Advanced Security/Firewall

The screenshot displays the Windows Event Viewer interface. At the top, the 'System' log is selected, showing 2,186 events. A filter is applied: 'Log: file://C:\Users\Malware\Desktop\Event-Logs\System.evtx; Source: ; Event ID: 104', resulting in 15 events. The event list shows multiple 'Log clear' events from the 'Eventlog' source. The 'Event Properties - Event 104, Eventlog' dialog box is open, showing the 'General' tab. The message text reads: 'The Microsoft-Windows-Windows Firewall With Advanced Security/Firewall log file was cleared.' Below the message, the event details are listed: Log Name: System, Source: Eventlog, Logged: 3/27/2023 6:01:56 PM, Event ID: 104, and Task Category: Log clear.

Level	Date and Time	Source	Event ID	Task Category
Information	3/27/2023 6:01:56 PM	Eventlog	104	Log clear
Information	3/25/2023 12:31:57 AM	Eventlog	104	Log clear
Information	3/25/2023 12:22:42 AM	Eventlog	104	Log clear
Information				Log clear
Information				Log clear
Information				Log clear
Information				Log clear
Information				Log clear
Information				Log clear
Information				Log clear
Information				Log clear
Information				Log clear
Information				Log clear
Information				Log clear
Information				Log clear
Information				Log clear

Event Properties - Event 104, Eventlog

General Details

The Microsoft-Windows-Windows Firewall With Advanced Security/Firewall log file was cleared.

Log Name: System
Source: Eventlog
Event ID: 104

Logged: 3/27/2023 6:01:56 PM
Task Category: Log clear



Logjammer has been Solved!

Congratulations  **shokoyanko**, best of luck in capturing flags ahead!

#1364

SHERLOCK RANK

07 Aug 2024

SOLVE DATE

RETIRED

SHERLOCK STATE