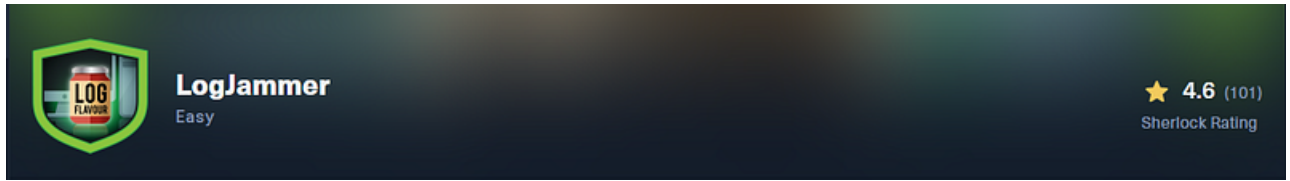


HTB Labs Sherlocks: LogJammer| DFIR Write-up



Scenario Overview

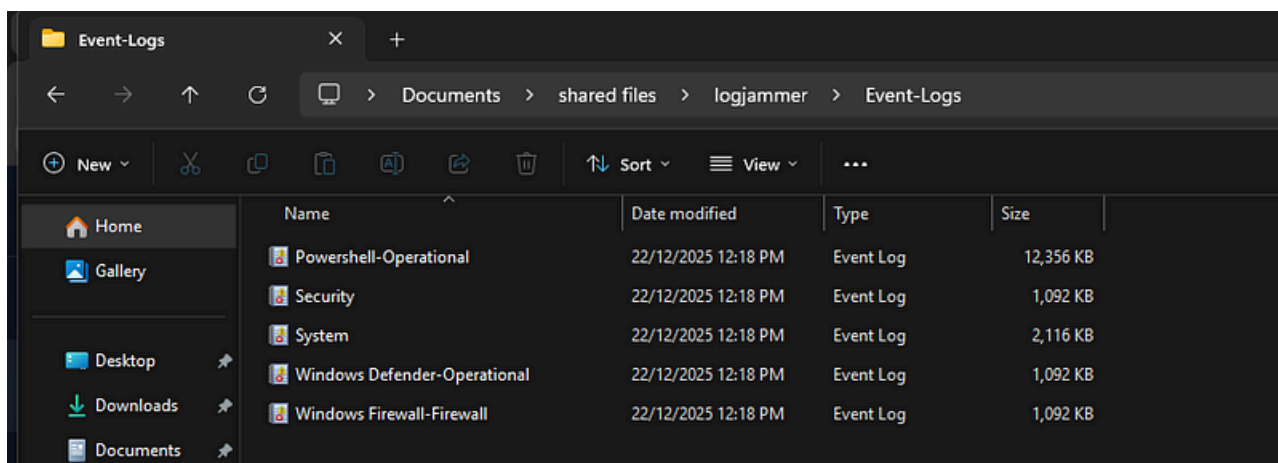
I was tasked with completing a technical assessment as a **junior DFIR consultant** for **Forela-Security**. The goal of the investigation was to analyze **Windows Event Logs** to determine whether the user **CyberJunkie** logged into the system and performed malicious actions.

The assessment focuses on identifying suspicious behavior using Windows logging artifacts.

Tool Used

Event Viewer

Event Viewer is a built-in Windows utility used to view and analyze system, security, application, and service logs. It is commonly used in DFIR investigations to reconstruct user activity, detect policy changes, and identify malicious behavior.



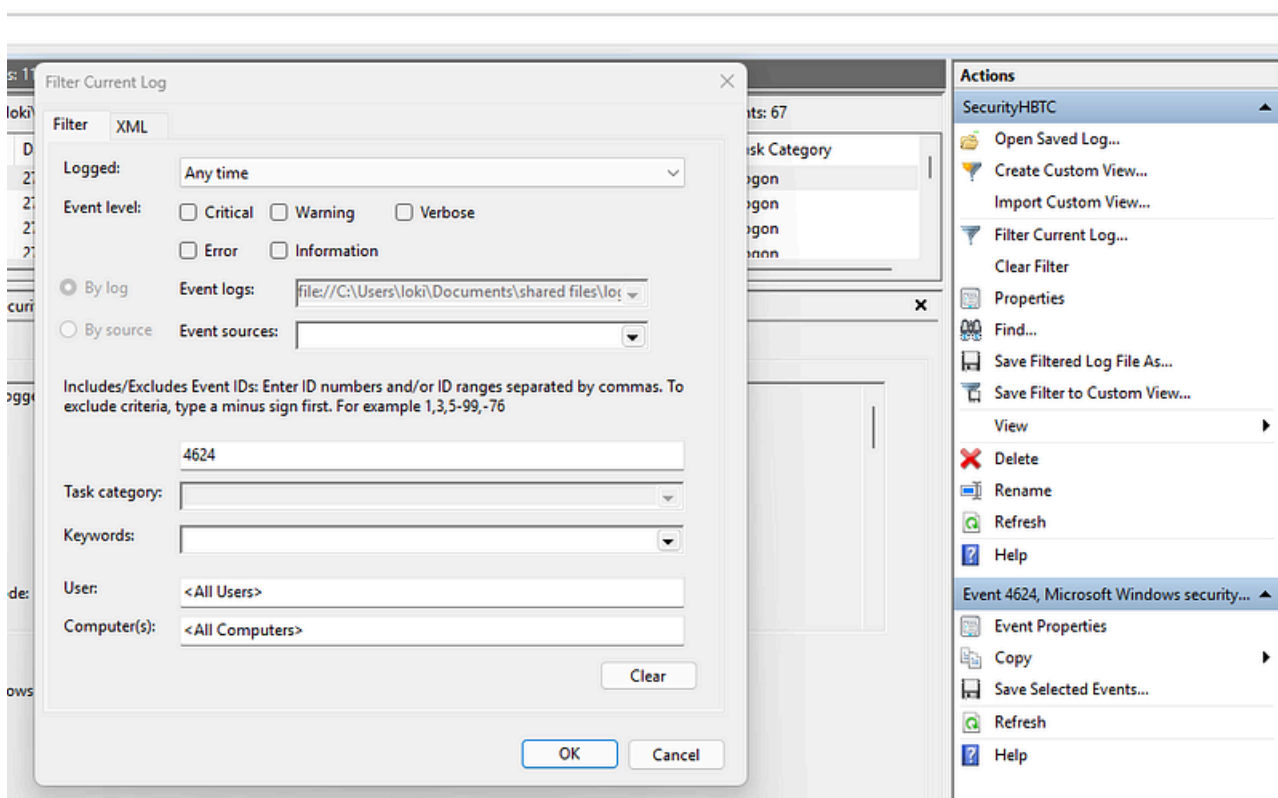
Task 1: First Successful Login (UTC)

Question: When did the CyberJunkie user first successfully log into the computer?

- **Event Log:** Security
- **Event ID:** 4624 (An account was successfully logged on)

To locate this:

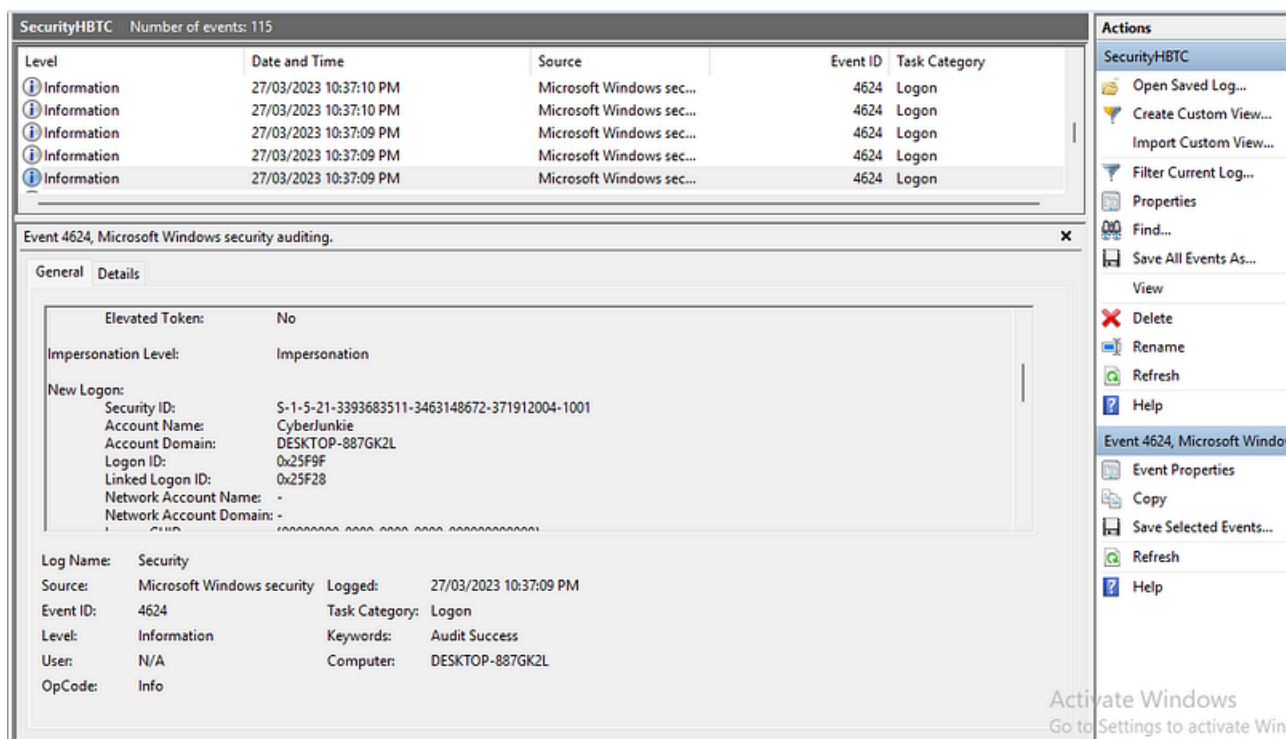
- Navigated to **Security** logs
- Filtered for **Event ID 4624**



- Identified the first successful logon entry for the user *CyberJunkie*

The event timestamp was initially observed as **27/03/2023 21:37:09** (local time). Since the system operates in **UTC+7**, the time was converted back to UTC.

Answer:



27/03/2023 14:37:09 UTC

Task 2: Firewall Rule Added

Question: What is the name of the firewall rule added?

- Event Log:** Windows Firewall-Firewall

At **27/03/2023 22:44:43**, a firewall rule was added to the Windows Defender Firewall exception list.

The screenshot displays the Windows Firewall event log with the following data:

Level	Date and Time	Source	Event ID	Task Category
Information	27/03/2023 10:44:43 PM	Windows Firewall With ...	2004	None
Information	27/03/2023 10:37:35 PM	Windows Firewall With ...	2004	None
Information	27/03/2023 10:37:35 PM	Windows Firewall With ...	2004	None

The selected event (ID 2004) details are as follows:

- Log Name:** Microsoft-Windows-Windows Firewall With Advanced Security/Firewall
- Source:** Windows Firewall With Adva
- Event ID:** 2004
- Level:** Information
- User:** LOCAL SERVICE
- OpCode:** Info
- Task Category:** None
- Keywords:** (2199023255552)
- Computer:** DESKTOP-887GK2L

The event description states: "A rule has been added to the Windows Defender Firewall exception list." The added rule details are:

- Rule ID:** {11309293-FB68-4969-93F9-7F75A9032570}
- Rule Name:** Metasploit C2 Bypass
- Origin:** Local
- Active:** Yes
- Direction:** Outbound
- Profiles:** Private, Domain, Public
- Action:** Allow
- Application Path:**
- Service Name:**
- Protocol:** TCP
- Security Options:** None
- Edge Traversal:** None
- Modifying User:** S-1-5-21-3393683511-3463148672-371912004-1001
- Modifying Application:** C:\Windows\System32\mmc.exe

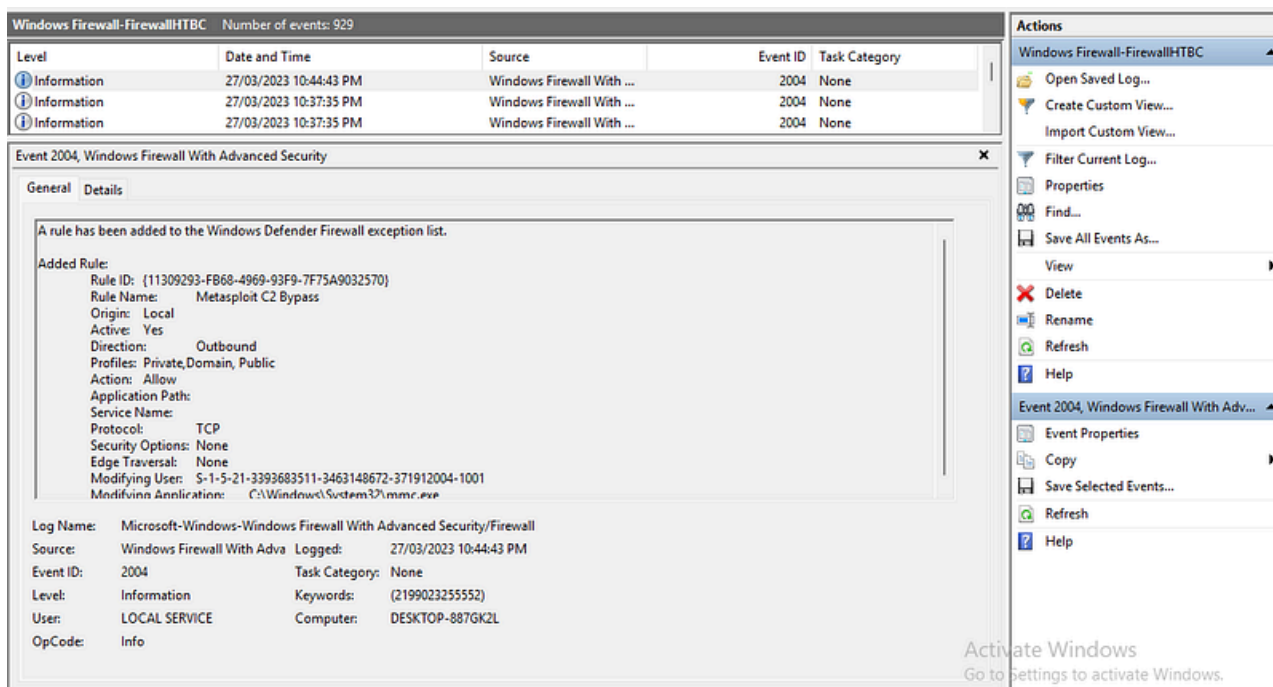
Answer:

Metasploit C2 Bypass

Task 3: Firewall Rule Direction

Question: What is the direction of the firewall rule?

- **Event Log:** Microsoft-Windows-Windows Firewall With Advanced Security/Firewall
- **Event ID:** 2004



Reviewing the same firewall event revealed the rule direction.

Answer:

Outbound

Task 4: Audit Policy Change

Question: What is the subcategory of the audit policy that was changed?

- **Event Log:** Security
- **Event ID:** 4702

Audit policy change events are recorded in the Security log. Upon inspection, the **Task Category** (subcategory) of the modified audit policy was identified.

The screenshot shows the Windows Event Viewer interface. The top pane displays a list of security events from the 'SecurityHBTC' log. The bottom pane shows the details for event 4702, 'Other Object Access Events'.

Level	Date and Time	Source	Event ID	Task Category
Information	27/03/2023 10:52:43 PM	Microsoft Windows sec...	4648	Logon
Information	27/03/2023 10:52:40 PM	Microsoft Windows sec...	4624	Logon
Information	27/03/2023 10:52:40 PM	Microsoft Windows sec...	4624	Logon
Information	27/03/2023 10:52:20 PM	Microsoft Windows sec...	4702	Other Object Access Eve...
Information	27/03/2023 10:52:20 PM	Microsoft Windows sec...	4702	Other Object Access Eve...
Information	27/03/2023 10:52:20 PM	Microsoft Windows sec...	4702	Other Object Access Eve...

Event 4702, Microsoft Windows security auditing.

General Details

A scheduled task was updated.

Subject:

- Security ID: SYSTEM
- Account Name: DESKTOP-887GK2LS
- Account Domain: WORKGROUP
- Logon ID: 0x3E7

Task Information:

- Task Name: \Microsoft\Windows\Flighting\OneSettings\RefreshCache
- Task New Content: <?xml version="1.0" encoding="UTF-16"?>
- <Task version="1.6" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
- <RegistrationInfo>

Log Name: Security

Source: Microsoft Windows security

Event ID: 4702

Level: Information

User: N/A

OpCode: Info

Logged: 27/03/2023 10:52:20 PM

Task Category: Other Object Access Events

Keywords: Audit Success

Computer: DESKTOP-887GK2L

Answer:

Other Object Access Events

Task 5: Scheduled Task Created

Question: What is the name of the scheduled task created by CyberJunkie?

- **Event Log:** Security
- **Event ID:** 4698
- **Timestamp:** 27/03/2023 22:51:21

This event indicates the creation of a scheduled task.

Answer:

HTB-AUTOMATION

SecurityHBTC Number of events: 115

Level	Date and Time	Source	Event ID	Task Category
Information	27/03/2023 10:52:19 PM	Microsoft Windows sec...	4624	Login
Information	27/03/2023 10:52:19 PM	Microsoft Windows sec...	4702	Other Object Access Eve...
Information	27/03/2023 10:52:12 PM	Microsoft Windows sec...	4624	Login
Information	27/03/2023 10:52:11 PM	Microsoft Windows sec...	4624	Login
Information	27/03/2023 10:52:09 PM	Microsoft Windows sec...	4624	Login
Information	27/03/2023 10:51:21 PM	Microsoft Windows sec...	4698	Other Object Access Eve...

Event 4698, Microsoft Windows security auditing.

General Details

A scheduled task was created.

Subject:

Security ID: S-1-5-21-3393683511-3463148672-371912004-1001
 Account Name: CyberJunkie
 Account Domain: DESKTOP-887GK2L
 Logon ID: 0x25F28

Task Information:

Task Name: \HTB-AUTOMATION
 Task Content: <?xml version='1.0' encoding='UTF-16'?><Task version='1.2' xmlns='http://schemas.microsoft.com/windows/2004/02/mit/task'><RegistrationInfo>

Log Name: Security
 Source: Microsoft Windows security Logged: 27/03/2023 10:51:21 PM
 Event ID: 4698 Task Category: Other Object Access Events
 Level: Information Keywords: Audit Success
 User: N/A Computer: DESKTOP-887GK2L
 OpCode: Info

Activate Windows
Go to Settings to activate Windows.

SecurityHBTC Number of events: 115

Level	Date and Time	Source	Event ID	Task Category
Information	27/03/2023 10:52:19 PM	Microsoft Windows sec...	4624	Login
Information	27/03/2023 10:52:19 PM	Microsoft Windows sec...	4702	Other Object Access Eve...
Information	27/03/2023 10:52:12 PM	Microsoft Windows sec...	4624	Login
Information	27/03/2023 10:52:11 PM	Microsoft Windows sec...	4624	Login
Information	27/03/2023 10:52:09 PM	Microsoft Windows sec...	4624	Login
Information	27/03/2023 10:51:21 PM	Microsoft Windows sec...	4698	Other Object Access Eve...

Event 4698, Microsoft Windows security auditing.

General Details

<RunOnlyIfIdle>false</RunOnlyIfIdle>
 <WakeToRun>false</WakeToRun>
 <ExecutionTimeLimit>P3D</ExecutionTimeLimit>
 <Priority>7</Priority>
 </Settings>
 <Actions Context="Author">
 <Exec>
 <Command>C:\Users\CyberJunkie\Desktop\Automation-HTB.ps1</Command>
 <Arguments>-A cyberjunkie@hackthebox.eu</Arguments>
 </Exec>
 </Actions>
 </Task>

Log Name: Security
 Source: Microsoft Windows security Logged: 27/03/2023 10:51:21 PM
 Event ID: 4698 Task Category: Other Object Access Events
 Level: Information Keywords: Audit Success
 User: N/A Computer: DESKTOP-887GK2L
 OpCode: Info

Activate W

Task 6: Scheduled Task File Path

Question: What is the full path of the file scheduled for execution?

- **Event Log:** Security
- **Event ID:** 4698

Scrolling through the event details reveals the file path associated with the task.

Answer:

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

Task 7: Command Arguments

Question: What arguments were passed to the scheduled task command?

- **Event Log:** Security
- **Event ID:** 4698

The command arguments are listed directly below the executable path in the event details.

Answer:

-A cyberjunkie@hackthebox.eu

SecurityHBTC Number of events: 115

Level	Date and Time	Source	Event ID	Task Category
Information	27/03/2023 10:52:19 PM	Microsoft Windows sec...	4624	Logon
Information	27/03/2023 10:52:19 PM	Microsoft Windows sec...	4702	Other Object Access Eve...
Information	27/03/2023 10:52:12 PM	Microsoft Windows sec...	4624	Logon
Information	27/03/2023 10:52:11 PM	Microsoft Windows sec...	4624	Logon
Information	27/03/2023 10:52:09 PM	Microsoft Windows sec...	4624	Logon
Information	27/03/2023 10:51:21 PM	Microsoft Windows sec...	4698	Other Object Access Eve...

Event 4698, Microsoft Windows security auditing.

General Details

```
<RunOnlyIfIdle>false</RunOnlyIfIdle>
<WakeToRun>false</WakeToRun>
<ExecutionTimeLimit>P3D</ExecutionTimeLimit>
<Priority>7</Priority>
</Settings>
<Actions Context="Author">
  <Exec>
    <Command>C:\Users\CyberJunkie\Desktop\Automation-HTB.ps1</Command>
    <Arguments>-A cyberjunkie@hackthebox.eu</Arguments>
  </Exec>
</Actions>
</Task>
```

Log Name: Security
Source: Microsoft Windows security Logged: 27/03/2023 10:51:21 PM
Event ID: 4698 Task Category: Other Object Access Events
Level: Information Keywords: Audit Success
User: N/A Computer: DESKTOP-887GK2L
OpCode: Info

Task 8: Malware Identified by Antivirus

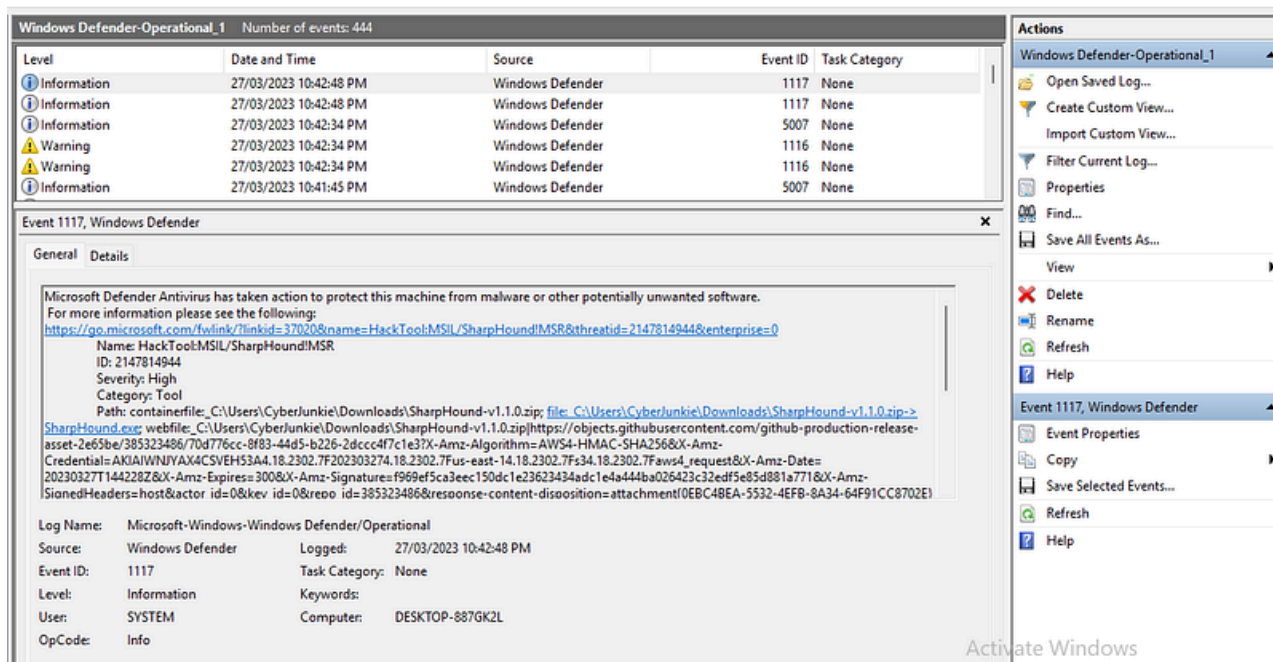
Question: Which tool was identified as malware?

- **Event Log:** Windows Defender-Operational
- **Event ID:** 1117

Windows Defender detected a malicious tool during system monitoring.

Answer:

SharpHound



Task 9: Malware File Path

Question: What is the full path of the detected malware?

- **Event Log:** Windows Defender-Operational
- **Event ID:** 1117

Answer:

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

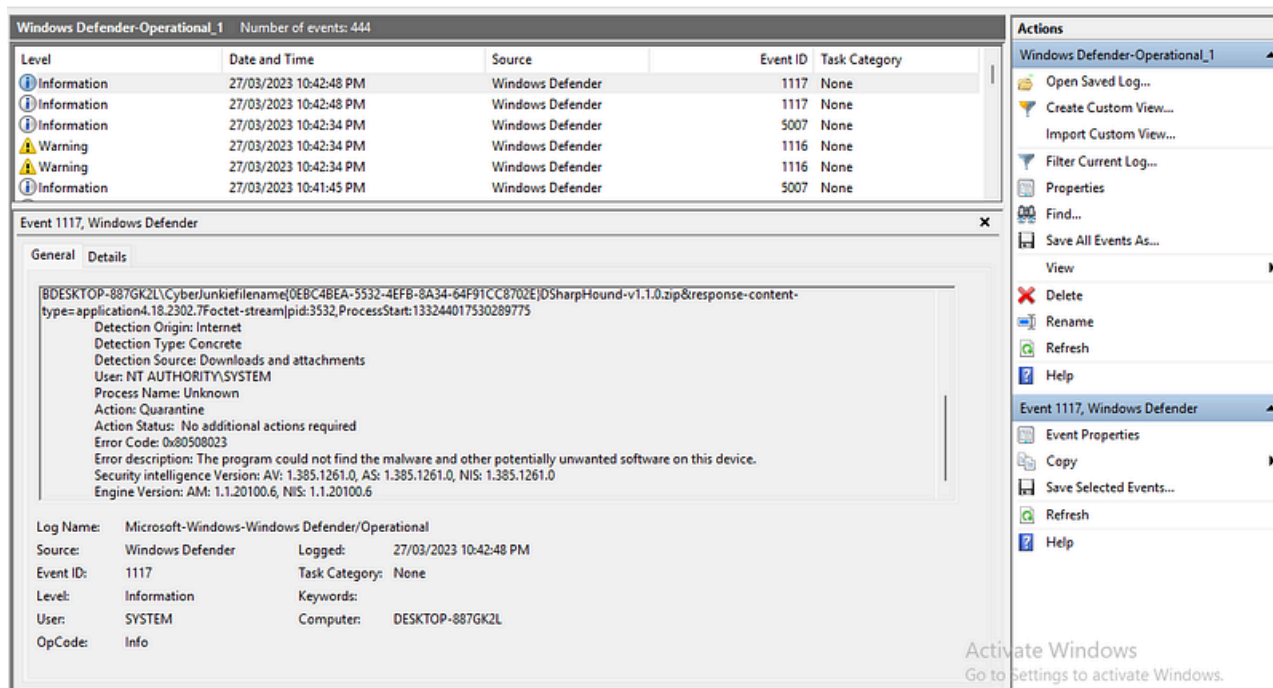
Task 10: Antivirus Action Taken

Question: What action was taken by the antivirus?

- **Event Log:** Windows Defender-Operational
- **Event ID:** 1117

Answer:

Quarantine



Task 11: PowerShell Command Execution

Question: What PowerShell command was executed by the user?

- **Event Log:** Powershell-Operational
- **Event ID:** 4104
- **Timestamp:** 27/03/2023 22:58:33

This event records executed PowerShell script blocks.

Answer:

Get-FileHash -Algorithm md5 .\Desktop\Automation-HTB.ps1

Level	Date and Time	Source	Event ID	Task Category
Information	27/03/2023 10:58:33 PM	PowerShell (Microsoft-...	4103	Executing Pipeline
Verbose	27/03/2023 10:58:33 PM	PowerShell (Microsoft-...	4104	Execute a Remote Com...
Information	27/03/2023 10:58:33 PM	PowerShell (Microsoft-...	4103	Executing Pipeline
Information	27/03/2023 10:58:31 PM	PowerShell (Microsoft-...	4103	Executing Pipeline
Information	27/03/2023 10:58:28 PM	PowerShell (Microsoft-...	4103	Executing Pipeline
Information	27/03/2023 10:58:07 PM	PowerShell (Microsoft-...	4103	Executing Pipeline

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

General Details

Creating Scriptblock text (1 of 1):
Get-FileHash -Algorithm md5 .\Desktop\Automation-HTB.ps1

ScriptBlock ID: b4fcf72f-abdc-4a84-923f-8e06a758000b
Path:

Log Name: Microsoft-Windows-PowerShell/Operational
Source: PowerShell (Microsoft-Wind Logged: 27/03/2023 10:58:33 PM
Event ID: 4104 Task Category: Execute a Remote Command
Level: Verbose Keywords: None
User: S-1-5-21-3393683511-346314 Computer: DESKTOP-887GK2L
OpCode: On create calls

Actions

- PowerShell-Operational_1
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- View
- Delete
- Rename
- Refresh
- Help
- Event 4104, PowerShell (Microsoft-Win...
- Event Properties
- Copy
- Save Selected Events...
- Refresh
- Help

Task 12: Cleared Event Log

Question: Which event log file was cleared?

- **Event Log:** System
- **Event ID:** 104

The log clear event specifies which log was deleted.

Answer:

Microsoft-Windows-Windows Firewall With Advanced Security/Firewall

The screenshot displays the Windows Event Viewer interface. At the top, a summary bar for 'System_1' indicates 'Number of events: 2,186'. Below this is a table listing several events. The selected event, Event 104, is expanded to show its details. The main pane displays the message: 'The Microsoft-Windows-Windows Firewall With Advanced Security/Firewall log file was cleared.' The details pane at the bottom provides metadata for the event, including the log name, source, event ID, level, user, and computer name. A right-hand pane titled 'Actions' offers various options for managing the event log, such as opening saved logs, creating custom views, and deleting events.

Level	Date and Time	Source	Event ID	Task Category
Information	27/03/2023 11:01:56 PM	Eventlog	104	Log clear
Warning	27/03/2023 10:58:56 PM	DNS Client Events	1014 (1014)	
Information	27/03/2023 10:57:42 PM	GroupPolicy (Microsoft...)	1502	None
Information	27/03/2023 10:57:34 PM	GroupPolicy (Microsoft...)	1502	None
Information	27/03/2023 10:56:44 PM	GroupPolicy (Microsoft...)	1502	None
Information	27/03/2023 10:50:03 PM	GroupPolicy (Microsoft...)	1500	None

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
Level: Information
User: S-1-5-21-3393683511-346314
OpCode: Info

Logged: 27/03/2023 11:01:56 PM
Task Category: Log clear
Keywords:
Computer: DESKTOP-887GK2L

Actions

- System_1
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- View
- Delete
- Rename
- Refresh
- Help
- Event 104, Eventlog
- Event Properties
- Copy
- Save Selected Events...
- Refresh
- Help

By [Alexander Sapo](#) on [December 22, 2025](#).

[Canonical link](#)

Exported from [Medium](#) on February 7, 2026.