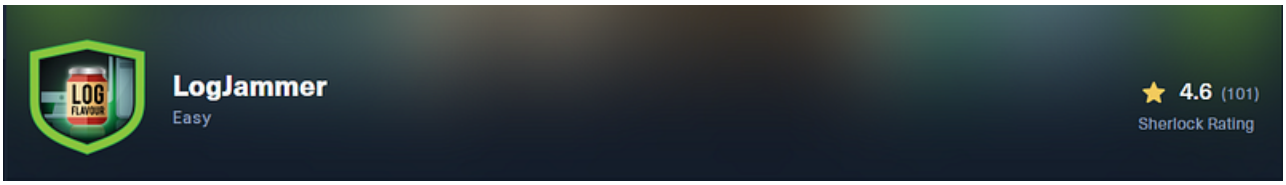
HTB Labs Sherlocks: LogJammer| DFIR Write-up



Scenario Overview

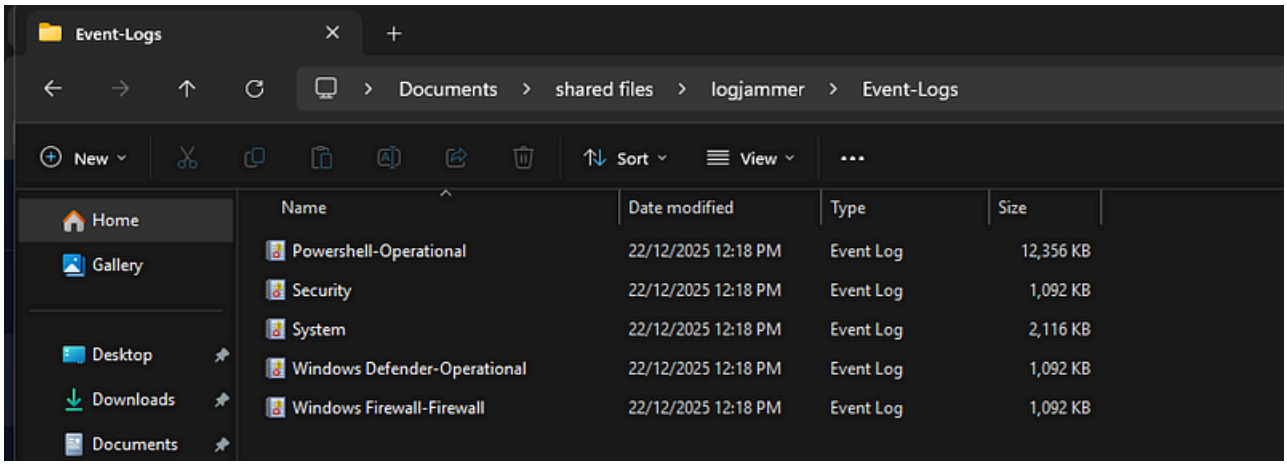
I was tasked with completing a technical assessment as a **junior DFIR consultant** for **Forela-Security**. The goal of the investigation was to analyze **Windows Event Logs** to determine whether the user **CyberJunkie** logged into the system and performed malicious actions.

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.



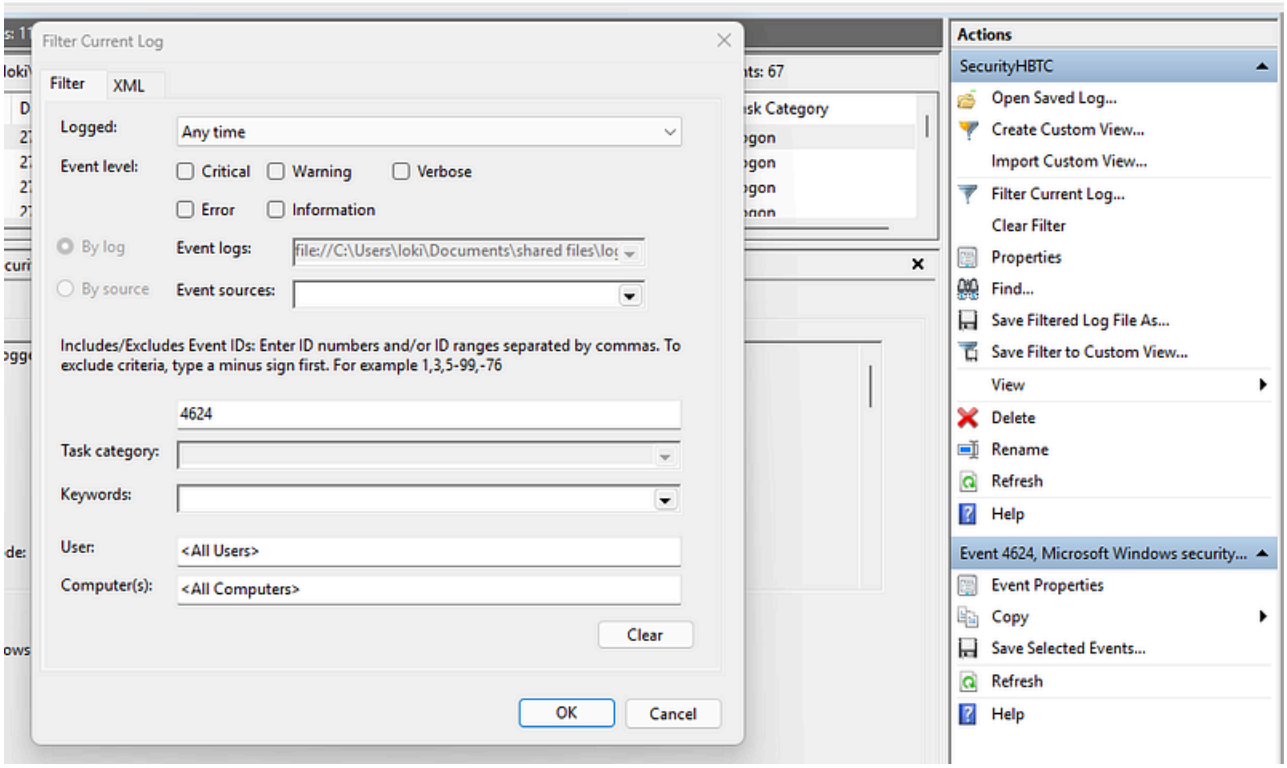
Task 1: First Successful Login (UTC)

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:

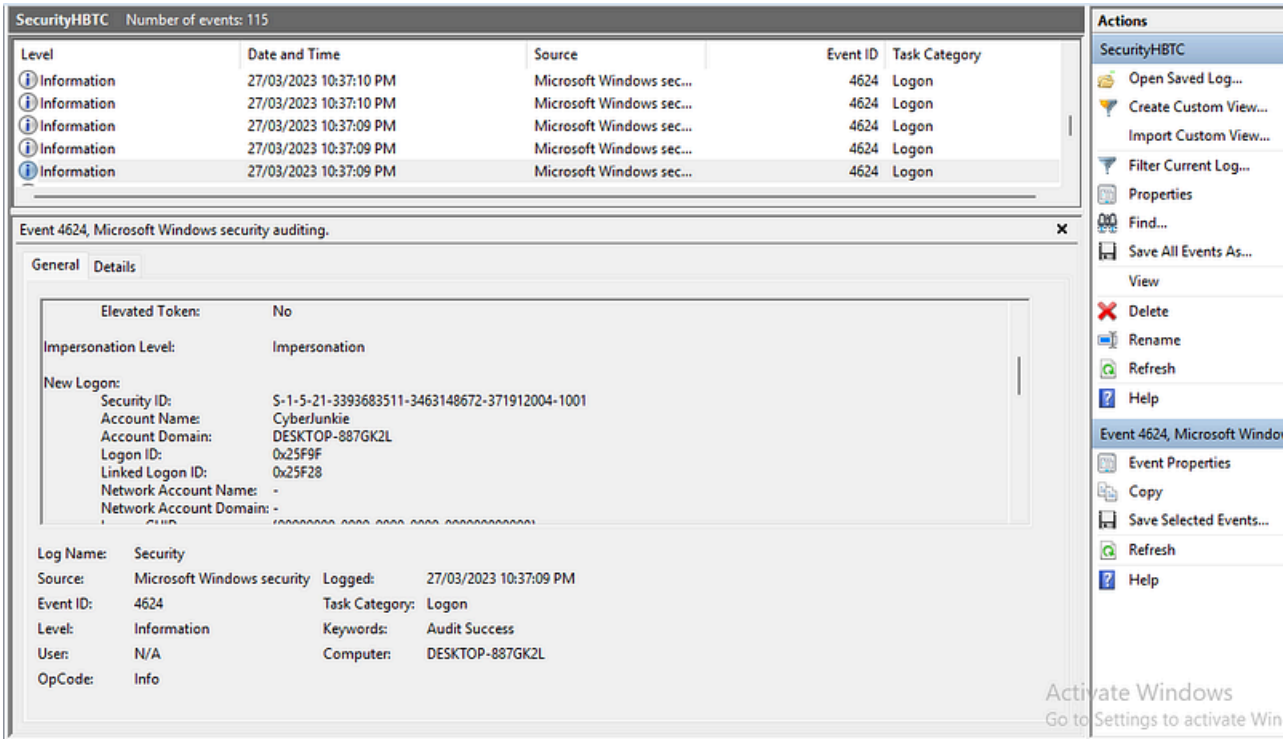
- Navigated to **Security** logs
- Filtered for **Event ID 4624**



- 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:



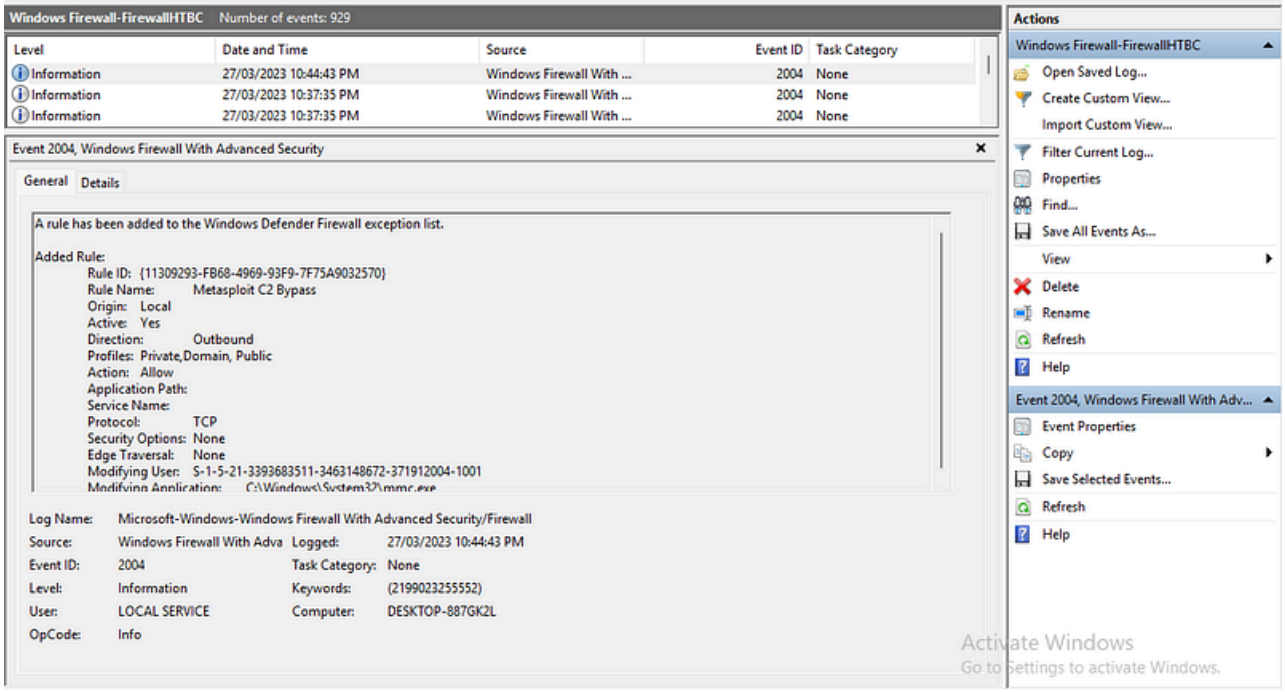
27/03/2023 14:37:09 UTC

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.



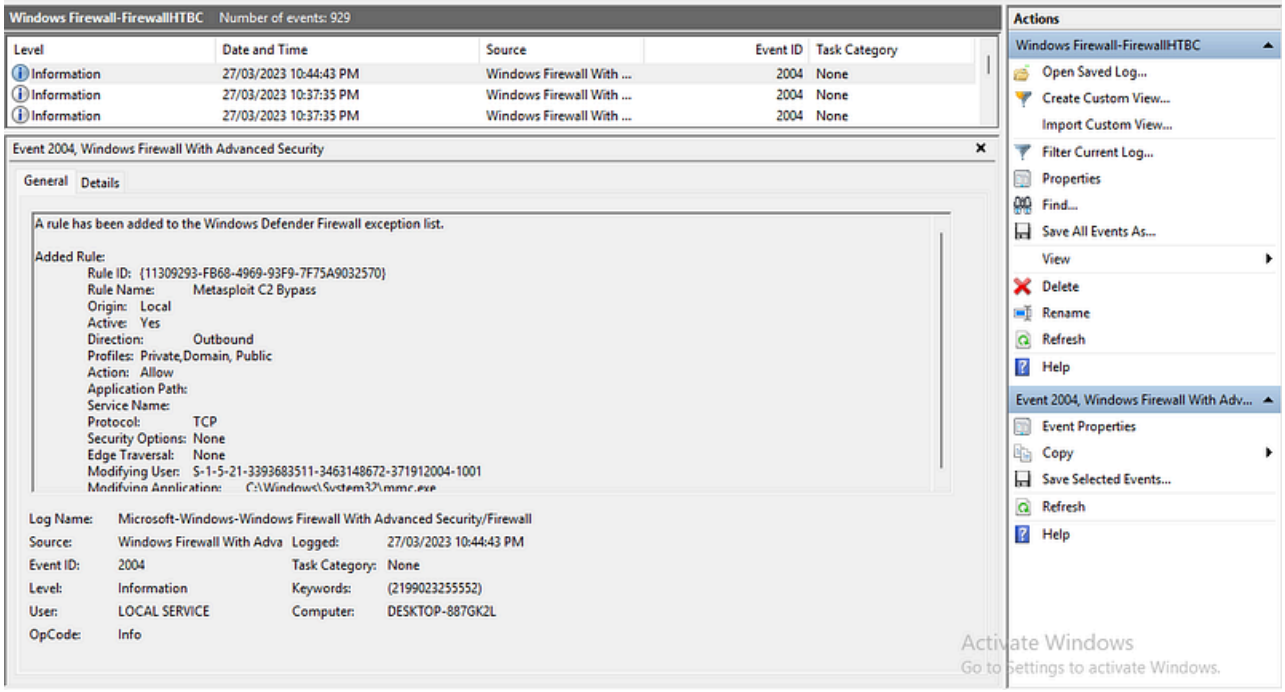
Answer:

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:

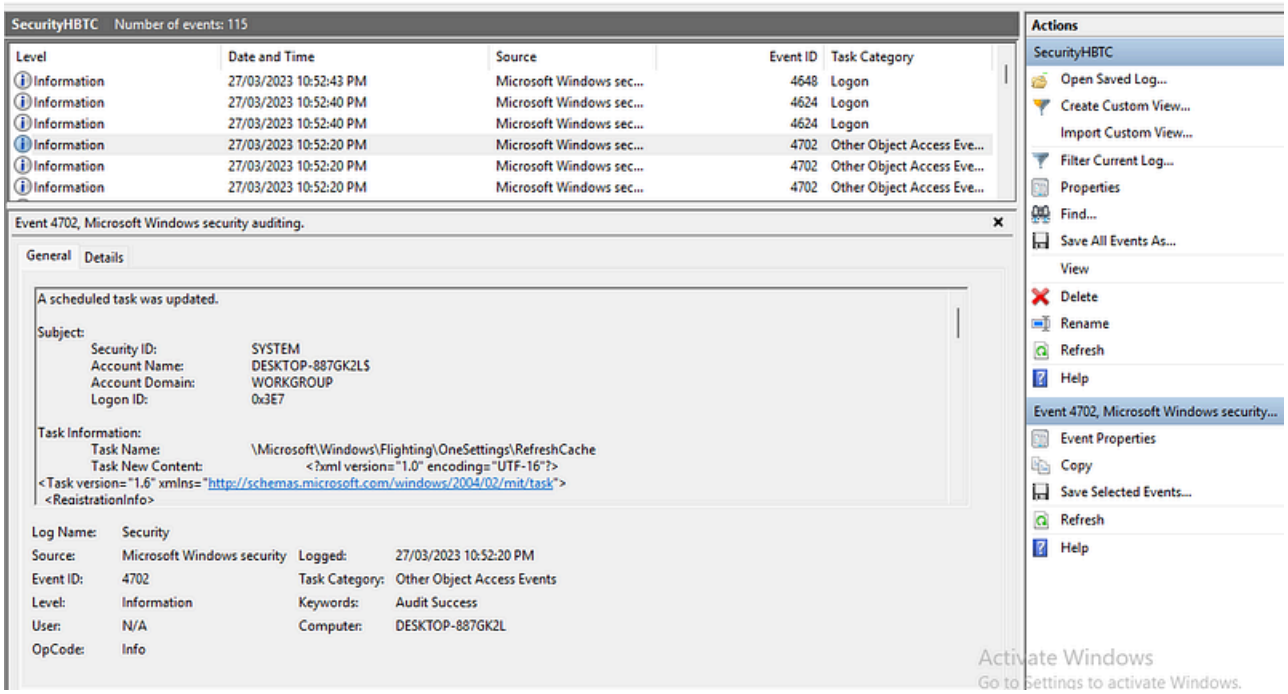
Outbound

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.



Answer:

Other Object Access Events

Task 5: Scheduled Task Created

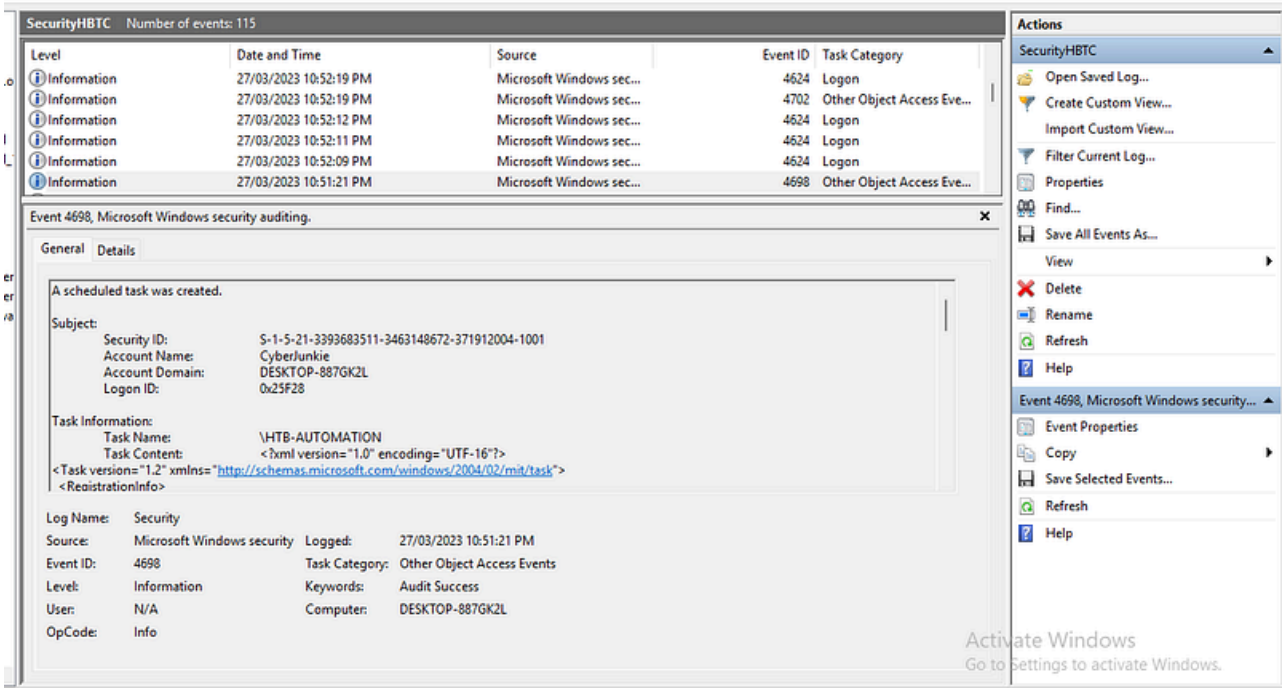
Question: What is the name of the scheduled task created by CyberJunkie?

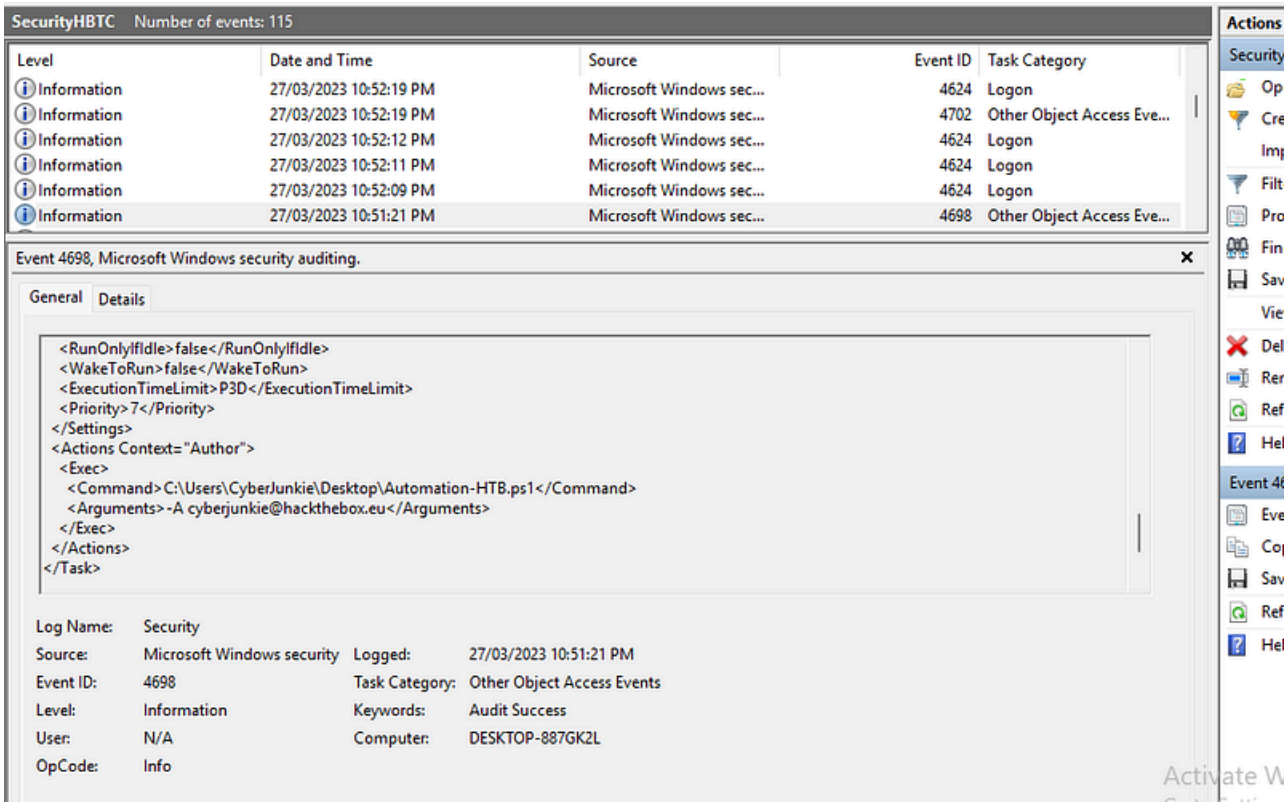
- **Event Log:** Security
- **Event ID:** 4698
- **Timestamp:** 27/03/2023 22:51:21

This event indicates the creation of a scheduled task.

Answer:

HTB-AUTOMATION





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

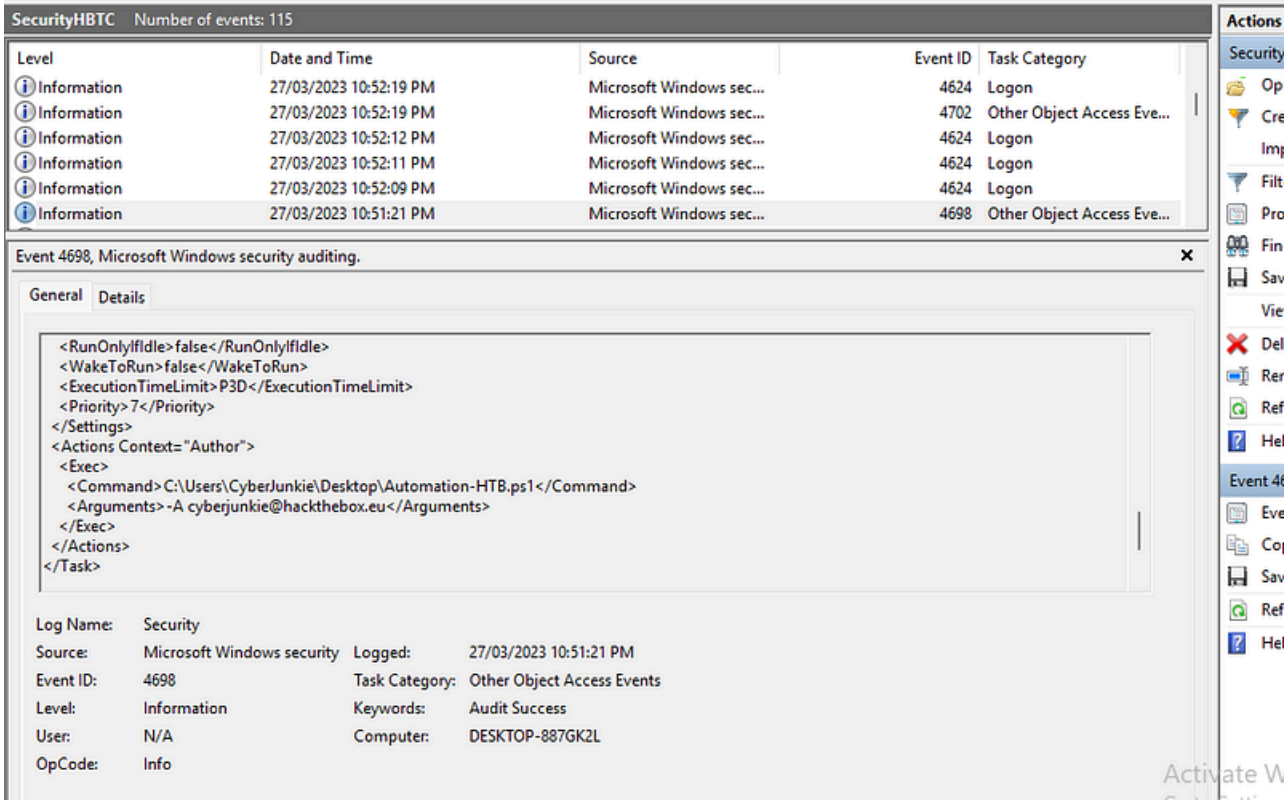
Question: What arguments were passed to the scheduled task command?

- **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



Task 8: Malware Identified by Antivirus

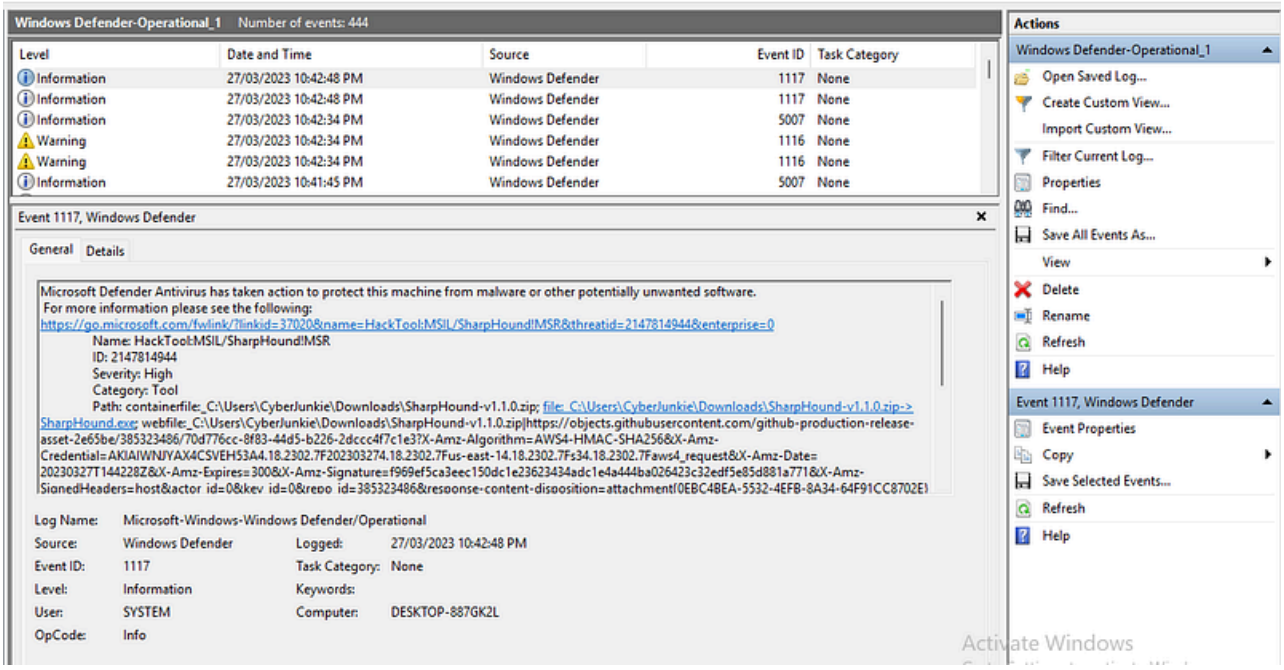
Question: Which tool was identified as malware?

- **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

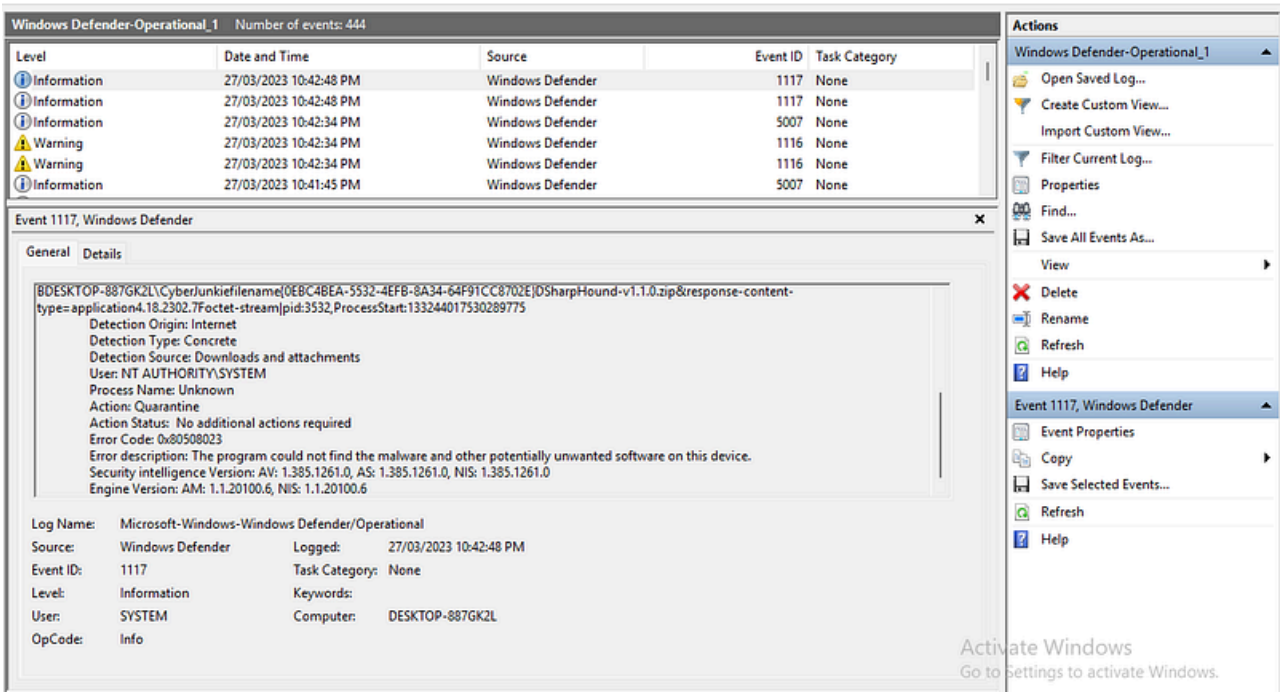
Task 10: Antivirus Action Taken

Question: What action was taken by the antivirus?

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

Answer:

Quarantine



Task 11: PowerShell Command Execution

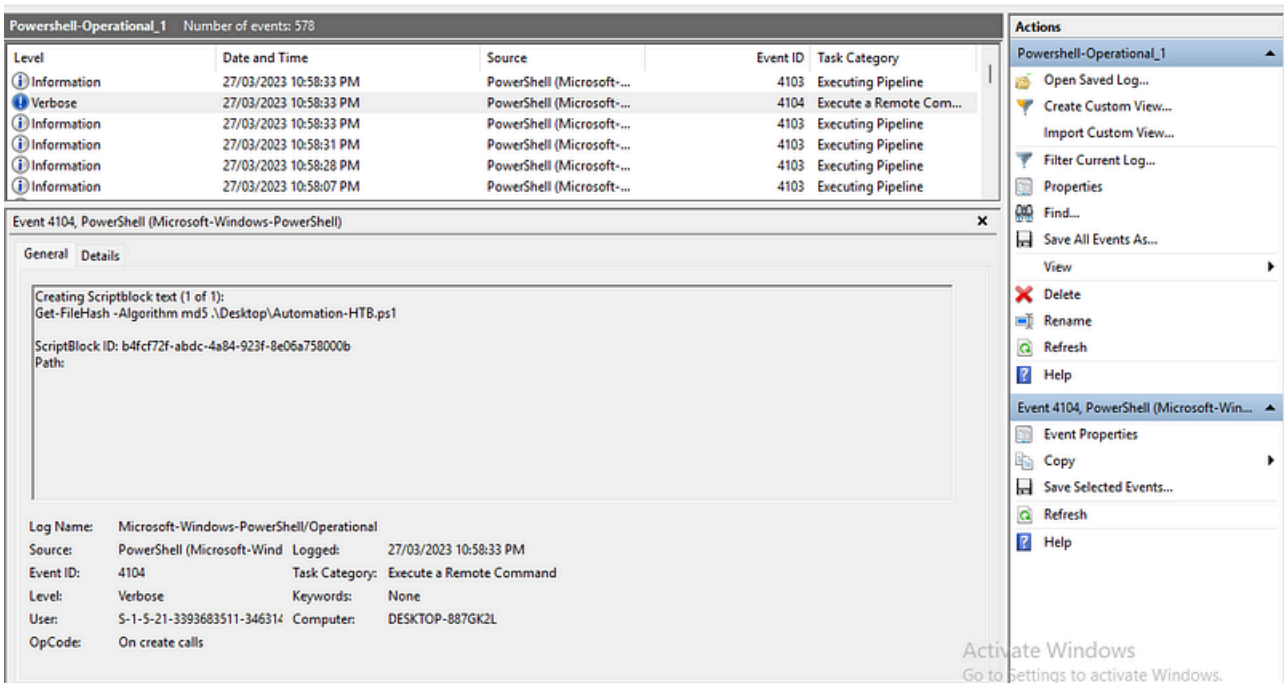
Question: What PowerShell command was executed by the user?

- **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



Task 12: Cleared Event Log

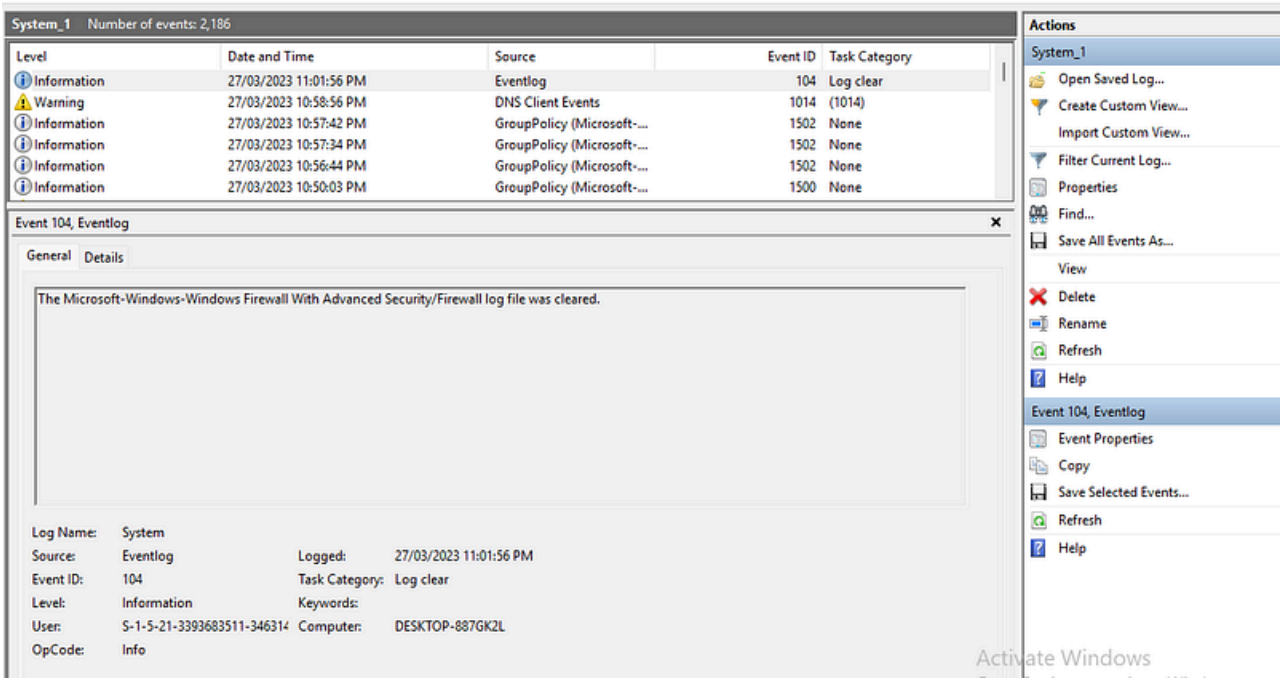
Question: Which event log file was cleared?

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

The log clear event specifies which log was deleted.

Answer:

Microsoft-Windows-Windows Firewall With Advanced Security/Firewall



By Alexander Sapo on December 22, 2025.

Canonical link

Exported from Medium on February 7, 2026.