

Logjammer Challenge

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.

Task 1:

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

I opened all logs in Log Explorer tool.

Filtered in Security logs for event Id 4624 and cyberjunkie

To see the UTC time we need to view the XML tab

Event ID(s):
4624
Enter ID numbers &
Text in description:
cyberjunkie

Type	Date	Time	Event	Source	Category	User	Computer
Audit: Success	3/27/2023	7:38:32 AM	4624	Microsoft-Windows	Logon	N/A	DESKTOP-887GK2L
Audit: Success	3/27/2023	7:38:32 AM	4624	Microsoft-Windows	Logon	N/A	DESKTOP-887GK2L
Audit: Success	3/27/2023	7:37:09 AM	4624	Microsoft-Windows	Logon	N/A	DESKTOP-887GK2L
Audit: Success	3/27/2023	7:37:09 AM	4624	Microsoft-Windows	Logon	N/A	DESKTOP-887GK2L

Event Properties - File: C:\Users\Bubble\Desktop\Event-Logs\Sec...
Standard XML
[SystemTime] 2023-03-27T14:37:09.8798913Z

Answer:

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?

In Firewall logs, Event ID 2004: This event indicates changes to Windows Firewall rules, such as the creation, modification, or deletion of a rule.

The first log rule description was the metasploit

Type	Date	Time	Event	Source	Category	User	Computer
Information	3/27/2023	7:44:43 AM	2004	Microsoft-Windows	None	NT AUTHORITY\LOCAL	DESKTOP-887GK2L
Information	3/27/2023	7:37:35 AM	2004	Microsoft-Windows	None	NT AUTHORITY\LOCAL	DESKTOP-887GK2L
Information	3/27/2023	7:37:35 AM	2004	Microsoft-Windows	None	NT AUTHORITY\LOCAL	DESKTOP-887GK2L
Information	3/27/2023	7:33:32 AM	2004	Microsoft-Windows	None	NT AUTHORITY\LOCAL	DESKTOP-887GK2L
Information	3/27/2023	7:33:27 AM	2004	Microsoft-Windows	None	NT AUTHORITY\LOCAL	DESKTOP-887GK2L
Information	3/27/2023	7:33:27 AM	2004	Microsoft-Windows	None	NT AUTHORITY\LOCAL	DESKTOP-887GK2L
Information	3/24/2023	4:46:13 AM	2004	Microsoft-Windows	None	NT AUTHORITY\LOCAL	DESKTOP-887GK2L
Information	3/23/2023	1:55:53 PM	2004	Microsoft-Windows	None	NT AUTHORITY\LOCAL	DESKTOP-887GK2L
Information	3/23/2023	1:55:53 PM	2004	Microsoft-Windows	None	NT AUTHORITY\LOCAL	DESKTOP-887GK2L
Information	3/23/2023	12:21:27 PM	2004	Microsoft-Windows	None	NT AUTHORITY\LOCAL	DESKTOP-887GK2L
Information	3/23/2023	12:21:27 PM	2004	Microsoft-Windows	None	NT AUTHORITY\LOCAL	DESKTOP-887GK2L
Information	3/23/2023	11:51:13 AM	2004	Microsoft-Windows	None	NT AUTHORITY\LOCAL	DESKTOP-887GK2L
Information	3/23/2023	11:51:13 AM	2004	Microsoft-Windows	None	NT AUTHORITY\LOCAL	DESKTOP-887GK2L

Description
A rule has been added to the Windows Defender Firewall exception list.
Added Rule:
Rule ID: {11309293-FB68-4969-93F9-7F75A9032570}
Rule Name: Metasploit C2 Bypass
Origin: 1
Active: 1
Direction: 2
Profiles: 2147483647
Action: 3
Application Path:
Service Name:
Protocol: 6
Security Options: 0
Edge Traversal: 0
Modifying User: S-1-5-21-3393683511-3463148672-371912004-1001
Modifying Application: C:\Windows\System32\mmc.exe

Answer:

Metasploit C2 Bypass

Task 3:

Whats the direction of the firewall rule?

The "Direction" field specifies the direction of the network traffic that the rule applies to. The values for the "Direction" field are:

- 1: Inbound (traffic coming into the system)
- 2: Outbound (traffic going out of the system)

Description
A rule has been added to the Windows Defender Firewall exception list.
Added Rule:
Rule ID: {11309293-FB68-4969-93F9-7F75A9032570}
Rule Name: Metasploit C2 Bypass
Origin: 1

Description

A rule has been added to the Windows Defender Firewall exception list.

Added Rule:

Rule ID: {11309293-FB68-4969-93F9-7F75A9032570}
Rule Name: Metasploit C2 Bypass
Origin: 1
Active: 1
Direction: 2
Profiles: 2147483647
Action: 3
Application Path:
Service Name:
Protocol: 6
Security Options: 0
Edge Traversal: 0
Modifying User: S-1-5-21-3393683511-3463148672-371912004-1001
Modifying Application: C:\Windows\System32\mmc.exe

Answer: Outbound

Task 4:

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

Checking event ID 4719 in Security logs to identify changes where success or failure auditing is removed

Description

System audit policy was changed.

Subject:

Security ID: S-1-5-18
Account Name: DESKTOP-887GK2L\$
Account Domain: WORKGROUP
Logon ID: 0x3e7

Audit Policy Change:

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

Answer: Other Object Access Events

Task 5:

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

Filtered in Security logs for event ID 4698 to identify a scheduled task that was created

Description	
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> <Date>2023-03-27T07:51:21.4599985</Date> <Author>DESKTOP-887GK2L\CyberJunkie</Author> <Description>practice</Description> <URI>\HTB-AUTOMATION</URI> </RegistrationInfo> <Triggers> <CalendarTrigger> <StartBoundary>2023-03-27T09:00:00</StartBoundary> <Enabled>true</Enabled> <ScheduleByDay> <DaysInterval>1</DaysInterval> </ScheduleByDay> </CalendarTrigger> </Triggers> <Principals> <Principal id="Author"> <RunLevel>LeastPrivilege</RunLevel> <UserId>DESKTOP-887GK2L\CyberJunkie</UserId> <LogonType>InteractiveToken</LogonType> </Principal> </Principals> <Settings> <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy> <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries> <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries> <AllowHardTerminate>true</AllowHardTerminate> <StartWhenAvailable>false</StartWhenAvailable> <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable> <IdleSettings> <Duration>PT10M</Duration> <WaitTimeout>PT1H</WaitTimeout> <StopOnIdleEnd>true</StopOnIdleEnd> <RestartOnIdle>false</RestartOnIdle> </IdleSettings> <AllowStartOnDemand>true</AllowStartOnDemand> <Enabled>true</Enabled> <Hidden>false</Hidden> <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>
Other Information:	ProcessCreationTime: 4222124650660162 ClientProcessId: 9320 ParentProcessId: 6112 FQDN: 0

Answer: HTB-AUTOMATION

Task 6:

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

Same as in task 5

```
<Actions Context="Author">
  <Exec>
    <Command>C:\Users\CyberJunkie\Desktop\Automation-HTB.ps1</Command>
    <Arguments>-A cyberjunkie@hackthebox.eu</Arguments>
  </Exec>
</Actions>
</Task>
```

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

Task 7:

What are the arguments of the command?

Same as the picture in task 5

```
<Actions Context="Author">
  <Exec>
    <Command>C:\Users\CyberJunkie\Desktop\Automation-HTB.ps1</Command>
    <Arguments>-A cyberjunkie@hackthebox.eu</Arguments>
  </Exec>
</Actions>
</Task>
```

Answer: -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?

Filtered for event ID 1116 in Windows Defender - Operational to identify a detected malware or other PUA software

Description

Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
For more information please see the following:
<https://go.microsoft.com/fwlink/?linkid=37020&name=HackTool:MSIL/SharpHound!MSR&threatid=2147814944&enterprise=0>
Name: HackTool:MSIL/SharpHound!MSR
ID: 2147814944
Severity: High
Category: Tool
Path: containerfile: C:\Users\CyberJunkie\Downloads\SharpHound-v1.1.0.zip; file: C:\Users\CyberJunkie\Downloads\SharpHound-v1.1.0.zip->SharpHound.exe; webfile: C:\Users\CyberJunkie\Downloads\SharpHound-v1.1.0.zip [https://objects.githubusercontent.com/github-production-release-asset-2e65be/385323486/70d776cc-8f83-44d5-b226-2dccc47c1e37X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWUNYAX4CSVEH53A4.18.2302.7F202303274.18.2302.7Fus-east-14.18.2302.7Fs34.18.2302.7Faws4_request&X-Amz-Date=20230327T144228Z&X-Amz-Expires=300&X-Amz-Signature=f969ef5ca3eec150dc1e23623434adc1e4a444ba026423c32edf5e85d881a771&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=385323486&response-content-disposition=attachment{0EB48EA-5532-4EFB-8A34-64F91CC8702E}BDESKTOP-887GK2L\CyberJunkie\filename{0EB48EA-5532-4EFB-8A34-64F91CC8702E}DSharpHound-v1.1.0.zip&response-content-type=application4.18.2302.7Foctet-stream|pid:3532,ProcessStart:133244017530289775
Detection Origin: Internet
Detection Type: Concrete
Detection Source: Downloads and attachments
User: DESKTOP-887GK2L\CyberJunkie
Process Name: Unknown
Security Intelligence Version: AV: 1.385.1261.0, AS: 1.385.1261.0, NIS: 1.385.1261.0
Engine Version: AM: 1.1.20100.6, NIS: 1.1.20100.6

Answer: SharpHound

Task 9:

Whats the full path of the malware which raised the alert?

Same from task 8 picture

Path: containerfile: C:\Users\CyberJunkie\Downloads\SharpHound-v1.1.0.zip; file: C:\Users\CyberJunkie\Downloads\SharpHound-v1.1.0.zip->SharpHound.exe;

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

Task 10:

What action was taken by the antivirus?

Filtered for event ID 1117 to identify the action of the defender on the detection.

Description

Microsoft Defender Antivirus has taken action to protect this machine from malware or other potentially unwanted software.
For more information please see the following:
<https://go.microsoft.com/fwlink/?linkid=37020&name=HackTool:MSIL/SharpHound!MSR&threatid=2147814944&enterprise=0>
Name: HackTool:MSIL/SharpHound!MSR
ID: 2147814944
Severity: High
Category: Tool
Path: containerfile: C:\Users\CyberJunkie\Downloads\SharpHound-v1.1.0.zip; file: C:\Users\CyberJunkie\Downloads\SharpHound-v1.1.0.zip->SharpHound.exe; webfile: C:\Users\CyberJunkie\Downloads\SharpHound-v1.1.0.zip [https://objects.githubusercontent.com/github-production-release-asset-2e65be/385323486/70d776cc-8f83-44d5-b226-2dccc47c1e37X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWUNYAX4CSVEH53A4.18.2302.7F202303274.18.2302.7Fus-east-14.18.2302.7Fs34.18.2302.7Faws4_request&X-Amz-Date=20230327T144228Z&X-Amz-Expires=300&X-Amz-Signature=f969ef5ca3eec150dc1e23623434adc1e4a444ba026423c32edf5e85d881a771&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=385323486&response-content-disposition=attachment{0EB48EA-5532-4EFB-8A34-64F91CC8702E}BDESKTOP-887GK2L\CyberJunkie\filename{0EB48EA-5532-4EFB-8A34-64F91CC8702E}DSharpHound-v1.1.0.zip&response-content-type=application4.18.2302.7Foctet-stream|pid:3532,ProcessStart:133244017530289775
Detection Origin: Internet
Detection Type: Concrete
Detection Source: Downloads and attachments
User: NT AUTHORITY\SYSTEM
Process Name: Unknown
Action: Quarantine
Action Status: No additional actions required
Error Code: 0x80508023
Error description: The program could not find the malware and other potentially unwanted software on this device.
Security Intelligence Version: AV: 1.385.1261.0, AS: 1.385.1261.0, NIS: 1.385.1261.0
Engine Version: AM: 1.1.20100.6, NIS: 1.1.20100.6

Answer: Quarantine

Task 11:

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

Filtered for event ID 4104 in Powershell - Operational logs to see the Powershell script block.

Description

Creating Scriptblock text (1 of 1):
Get-FileHash -Algorithm md5 .\Desktop\Automation-HTB.ps1
ScriptBlock ID: b4fcf72f-abdc-4a84-923f-8e06a758000b
Path:

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

Task 12:

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

Filtered for event ID 104 in System logs to identify a log clear event

Description

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

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