# Logjammer Challenge

### Sherlock Scenario

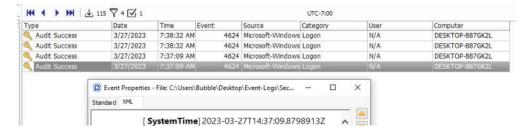
You have been presented with the opportunity to work as a junior DFIR consultant for a big consultancy. However, they have provided a technical assessment for you to complete. The consultancy Forela - Security would like to gauge your Windows Event Log Analysis knowledge. We believe the Cyberjunkie user 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





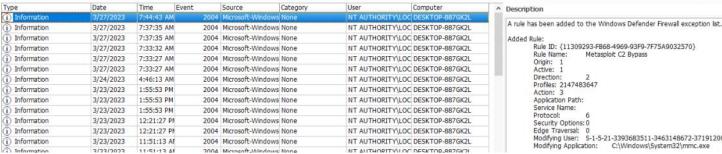
27/03/2023 14:37:09

## 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

The first log rule description was the metasploit



Added Rule: Rule ID: {11309293-FB68-4969-93F9-7F75A9032570} Metasploit C2 Bypass Rule Name: Origin: 1
Active: 1
Direction: 2
Profiles: 2147483647
Action: 3
Acolication Paths Application Path: Service Name: Protocol: Froucil: 6
Security Options: 0
Edge Traversal: 0
Modifying User: 5-1-5-21-3393683511-3463148672-371912004-1001
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)

# 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 Rule Name: Origin: 1

# Description

```
A rule has been added to the Windows Defender Firewall exception list.
                     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
Added Rule:
```

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

### Description

System audit policy was changed.

Subject:

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

Audit Policy Change: Category: Subcategory: Subcategory GUID: Changels: Object Access Other Object Access Events {0cce9227-69ae-11d9-bed3-505054503030} 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:
Account Domain:
Logon ID:
                                                                                                                                                                                     CyberJunkie
DESKTOP-887GK2L
          Task Information:
          Task Information:
Task Name: \hTB-AUTOMATION
Task Content: <?xml version="1.0" encoding="UTF-16"?>
<Task Content: <?xml version="1.1" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
<Registration.info>
<Date>2023-03-27T07:51:21.4599985</Date>
<Author>DESKTOP-887GK2L\cyberJunkie</Author>
<Description>practice<//Description>
<URI>\hTB-AUTOMATION</URI>
</Resistration.info>
                <uRI>\HTB-AUTOMATION</URI>
</RegistrationInfo>
</riggers>
</a>
<a href="California"></a>
<a href="California"><a h
               <Enabled>rrue<ScheduleByDay>
<DaysInterval>1</DaysInterval>
</ScheduleByDay>
</CalendarTrigger>
</Triggers>
<Principals>
<Principals</pre>
                <Principals>
<Principal id ="Author">
<Principal id ="Author">
<RunLevel> (astPrivilege</RunLevel>
<UserId> >DESKTOP-8876KZ1(CyberJunkie</UserId>
<LogonType>InteractiveToken</LogonType>
</Principal>
</Principal></principal></principal>
                <Settings>
                       Settings>
- (MultipleInstancesPolicy> IgnoreNew</ MultipleInstancesPolicy>
- (SisallowStartIfOnBatteries> true </ DisallowStartIfOnBatteries>
- StopIfGoingOnBatteries> true </ StopIfGoingOnBatteries>
- StopIfGoingOnBatteries>
- AllowHardTerminate> rrue </ AllowHardTerminate>
- StartWhenAvaliable> false </ StartWhenAvaliable>
- (RunOnlyIfletworkAvaliable> false </ RunOnlyIfletworkAvaliable>
                     KUNDINJINETWOKKAVAIIADIE> JAISE
KUNTATIONS
VUNTATIONS
VINTATIONS
VINTAT
                         </IdleSettings>
<AllowStartOnDemand>true</AllowStartOnDemand>
                       <aliowstartUnDemand>true</aliowstartUnDemand>
clabiled>true</aliowstartUnDemand>
clabiled>true</a> {Inididen>
clabiled>true
clabiled>tr
               </settings>
<Actions Context="Author">
<Exec>
<Command>C:\Users\CyberJunkie\Desktop\Automation-HTB.ps1</Command>
<Arguments>-A cyberjunkie@hackthebox.eu</Arguments>
<Exec>
           </Actions>
        Other Information:
ProcessCreationTime:
ClientProcessId:
ParentProcessId:
                                                                                                                                                                                                                           4222124650660162
9320
                                                                                                                                                                                                                                                                          6112
                                                   FODN:
 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">
                  Actions context— radios /
<Exec> <Command>C:\Users\CyberJunkie\Desktop\Automation-HTB.ps1</Command>
<Arguments>-A cyberjunkie@hackthebox.eu</Arguments>
                    </Exec>
 </Actions>
 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">
 Answer: -A cyberjunkie@hackthebox.eu
```

ruismen. 7. eyserjanniee nachenessanes

Task 8:

The antivirus running on the system identified a threat and performed actions on it. Which tool was

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

```
Description

Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
For more information please see the following:
<a href="https://go.microsoft.com/fwlink/?linkid=37020&name=HackTool:MSIL/SharpHoundIMSR&threatid=2147814944&enterprise=0">https://go.microsoft.com/fwlinkid=37020&name=HackTool:MSIL/SharpHoundIMSR</a>
Name: HackTool:MSIL/SharpHoundIMSR
```

ID: 2147814944 Severity: High Category: Tool

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.

Microsoft Defender Antivirus has taken action to protect this machine from malware or other potentially unwanted software.

For more information please see the following:

Intus://qo.microsoft.com/fwilmk/Pinkid=37020&name=HackTool:MSIL/SharpHoundIMSR&threatid=2147814944&enterprise=0

Name: HackTool:MSIL/SharpHoundIMSR
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-SharpHound.exe; webfile:\_C:\Users\CyberJunkie\Downloads\SharpHound-v1.1.0.zip-SharpHound.exe; webfile:\_C:\Users\CyberJunkie\Downloads\SharpHound-v1.1.0.zip\Intus://objects.githubusercontent.com/github-production-release-asset-2e55be/385323486/70d776cc-8f83-44d5-b226-2dccc4f7c1e37X-Amz-Algorithm=AWS4-HMAC-SHAZ56&X-Amz-Credentai=AKIAIN/NIYAX4CSVEH53A4.18.2302.7F2042303247 18.2302.7Fsa4:18.

8A34-64F91(C8702E)OSharpHound-v1.1.0.zip&response-content-type=application4.18.2302.7Foctet-stream|pid:3532,Proc
Detection Origin: Internet
Detection Type: Concrete
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: 1.1.2010.0.6, NIS: 1.1.20100.6

Answer: Quarantine

Task 11:

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

 $\hbox{Filtered for event ID 4104 in Powershell - Operational logs to see the Powershell script block. } \\$ 

Description

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

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

ScriptBlock ID: D4fct/2f-abdc-4a84-923f-8e06a/58000t 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