HTB sherlocks - Logjammer

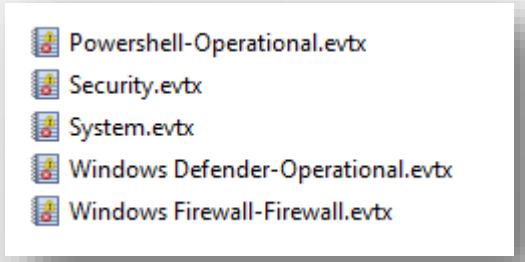
Write up by Chanan Shenker

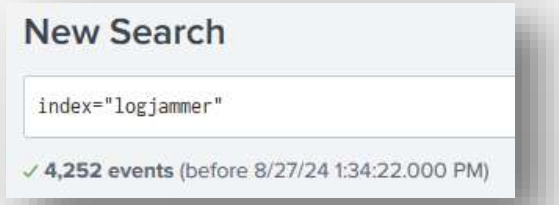
Scenario:

- 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:

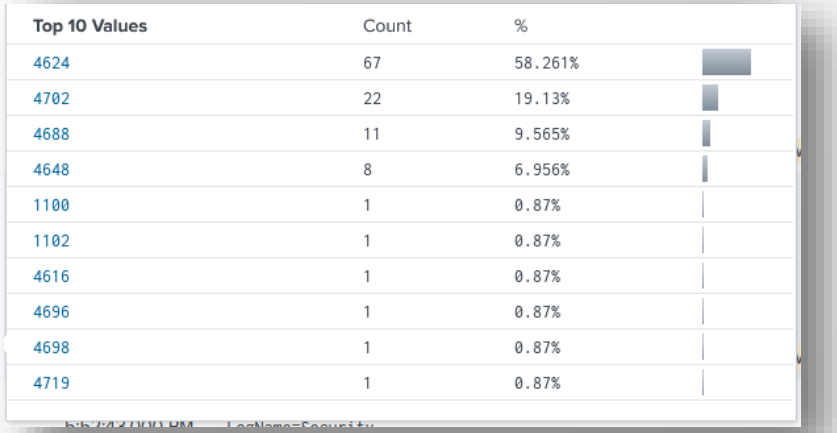
- To start, we are given 5 event log files.
- And to be as efficient as possible, I decided to load them up to Splunk and analyze them there.
- After loading the logs, we can see a total of 4252 logged events to analyze.





Security logs:

- Splunk makes analyzing event logs super easy, and one of the ways is by showing us statistics at the side of all the fields.
- Using that, I look to see what event IDs are present and can be useful for our investigation.
- Starting with event ID 4624. This event is triggered when a successful logon attempt is made; using this, we can try to see when the suspected user 'cyberjunkie' activity started and potentially minimize the amount of events we have to examine.
- Using Splunk's fields and search options, we can get all successful logon attempts that 'cyberjunkie' made and continue from there.



Top 10 Values	Count	%
4624	67	58.261%
4702	22	19.13%
4688	11	9.565%
4648	8	6.956%
1100	1	0.87%
1102	1	0.87%
4616	1	0.87%
4696	1	0.87%
4698	1	0.87%
4719	1	0.87%

- Looking at the first one presented from the search, we can see that the user logged in at '5:37:9 27/3/2023' (task 1), and now we can ignore everything that came before.
- Also, the logon type of '2' indicates to us that the user logged in physically and not remotely.

- That minimized a lot of the events.
- Next, we look at event ID 4698. This event is triggered when a scheduled task is created. Creating scheduled tasks can indicate attempts at gaining persistence.
- When we find the single event, we can see the name of the scheduled task (task 5) 'HTB-AUTOMATION', the path (task 6) 'C:\Users\CyberJunkie\Desktop\Automation-HTB.ps1', and the arguments given (task 7) '-A cyberjunkie@hackthebox.eu'.

Values	Count	%
4624	63	67.742%
4702	22	23.656%
4648	6	6.452%
4698	1	1.075%
4719	1	1.075%

Time	Event
3/27/23 5:51:21.000 PM	03/27/2023 05:51:21 PM LogName=Security EventCode=4698 EventType=0 ComputerName=DESKTOP-887GK2L Show all 70 lines host = DESKTOP-887GK2L source = Security.evtx sourcetype = WinEventLog:Security

```
CyberJunkie
DESKTOP-887GK2L
\HTB-AUTOMATION
<?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>
```

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

- The user created a scheduled task to run a Powershell script with a certain command. I couldn't find anything interesting about this Powershell script, but none the less, still suspicious.

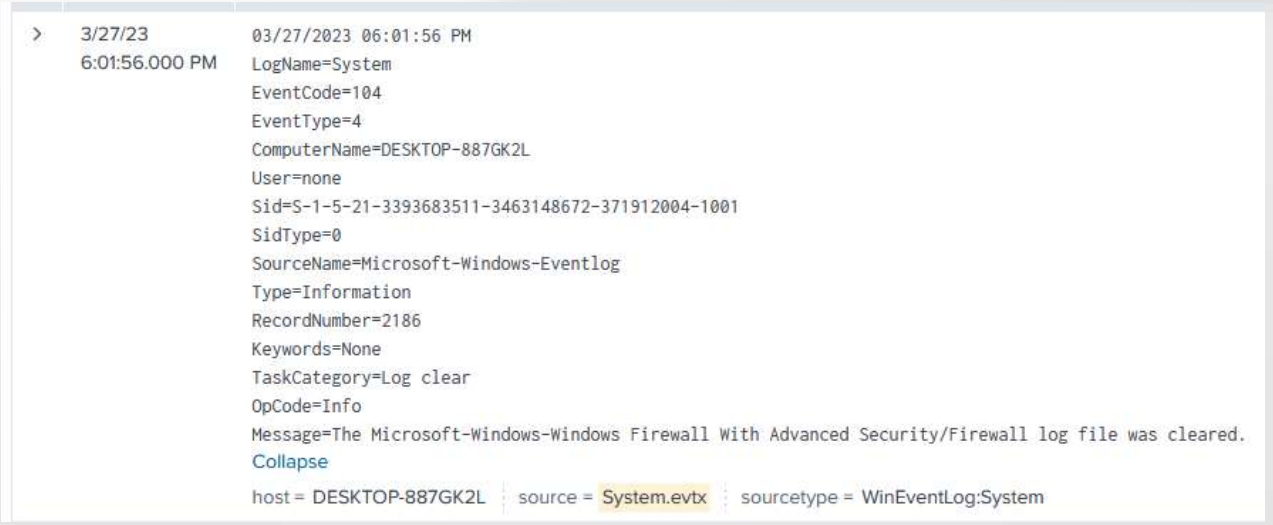
- And the last event for the security logs is event ID 4719. This event is triggered by someone altering the auditing policy. This can raise a lot of red flags since attackers can use it to cover their tracks.
- When we take a look at the event, we can see that 'cyberjunkie' added auditing success in other object access (task 4).

```
03/27/2023 05:50:03 PM
LogName=Security
EventCode=4719
EventType=0
ComputerName=DESKTOP-887GK2L
SourceName=Microsoft Windows security auditing.
Type=Information
RecordNumber=13102
Keywords=Audit Success
TaskCategory=Audit Policy Change
OpCode=Info
Message=System audit policy was changed.

Subject:
        Security ID:            NT AUTHORITY\SYSTEM
        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}
        Changes:                Success Added
```

System logs:

- In the system event logs there wasn't much to go off of. There was only one event that is suspicious. Event ID 104.
- This event is triggered when logs are cleared. Attackers clear event logs so that they can cover their tracks after they are done.

- As we can see, the user cleared the 'Microsoft-Windows-Windows Firewall With Advanced Security/Firewall' event logs (task 12).



```
>   3/27/23
    6:01:56.000 PM
    03/27/2023 06:01:56 PM
    LogName=System
    EventCode=104
    EventType=4
    ComputerName=DESKTOP-887GK2L
    User=none
    Sid=S-1-5-21-3393683511-3463148672-371912004-1001
    SidType=0
    SourceName=Microsoft-Windows-Eventlog
    Type=Information
    RecordNumber=2186
    Keywords=None
    TaskCategory=Log clear
    OpCode=Info
    Message=The Microsoft-Windows-Windows Firewall With Advanced Security/Firewall log file was cleared.
    Collapse
    host = DESKTOP-887GK2L | source = System.evtx | sourcetype = WinEventLog:System
```

Powershell logs:

- Was actually hoping I could find here more information on the script that was in the scheduled task, since when Powershell scripts run, you can see their content in the Powershell logs, but the script wasn't run at the time of these events.
- So I took a look through the Powershell logs but didn't find much interesting besides one command the user ran in Powershell.
- He ran 'Get-FileHash -Algorithm md5 .\Desktop\Automation-HTB.ps1' (task 11) to get the MD5 hash of the Powershell scripts he scheduled.
- Im not sure what this indicates to us, but I think he was trying to check the integrity of his Powershell script.

```
03/27/2023 05:58:33 PM
LogName=Microsoft-Windows-PowerShell/Operational
EventCode=4104
EventType=5
ComputerName=DESKTOP-887GK2L
User=none
Sid=S-1-5-21-3393683511-3463148672-371912004-1001
SidType=0
SourceName=Microsoft-Windows-PowerShell
Type=Verbose
RecordNumber=571
Keywords=None
TaskCategory=Execute a Remote Command
OpCode=On create calls
Message=Creating Scriptblock text (1 of 1):
Get-FileHash -Algorithm md5 .\Desktop\Automation-HTB.ps1

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

Windows defender logs:

- When looking at the Windows Defender logs, there are very useful things. We have event ID 1116 and 1117.
- 1116 is triggered when the defender has discovered a file that it deems malicious, and 1117 is triggered when the defender has taken action and stopped the malicious file.

Values	Count	%
5007	7	63.636%
1116	2	18.182%
1117	2	18.182%

- When looking at the event with the ID 1116, we can see that the defender has found a file named ‘sharphound.ps1’ (task8), ill explain in a bit what it does, and it found it once the user downloaded it.
- The defender stopped it when it was still compressed. And we can see the malware’s location in the file system (task 9).

```
03/27/2023 05:42:34 PM
LogName=Microsoft-Windows-Windows Defender/Operational
EventCode=1116
EventType=3
ComputerName=DESKTOP-887GK2L
User=SYSTEM
Sid=S-1-5-18
SidType=1
SourceName=Microsoft-Windows-Windows Defender
Type=Warning
RecordNumber=440
Keywords=None
TaskCategory=None
OpCode=Info
Message=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:PowerShell/SharpHound.B&threatid=2147823920&enterprise=0
        Name: HackTool:PowerShell/SharpHound.B
        ID: 2147823920
        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.ps1; webfile:_C:\Users
\CyberJunkie\Downloads\SharpHound-v1.1.0.zip|https://objects.githubusercontent.com/github-production-release-asset-2e65be/385323486/70d776cc-8f83-44d5-b226-2dccc4f7c1e3?X-Amz-A
lgorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A4.18.2302.7F202303274.18.2302.7Fus-east-14.18.2302.7Fs34.18.2302.7Faws4_request&X-Amz-Date=20230327T144228Z&X-Am
z-Expires=300&X-Amz-Signature=f969ef5ca3eec150dc1e23623434adc1e4a444ba026423c32edf5e85d881a771&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=385323486&response-content-d
isposition=attachment{0EBC4BEA-5532-4EFB-8A34-64F91CC8702E}BDESKTOP-887GK2L\CyberJunkiefilename{0EBC4BEA-5532-4EFB-8A34-64F91CC8702E}DSharpHound-v1.1.0.zip&response-content-typ
e=application4.18.2302.7Foctet-stream|pid:3532,ProcessStart:133244017530289775
        Detection Origin: Internet
        Detection Type: Concrete
        Detection Source: Downloads and attachments
        User: DESKTOP-887GK2L\CyberJunkie
```

- When looking at event ID 1117, we can see that the defender took action to stop this malware and quarantine it (task 10).

```
User: NT AUTHORITY\SYSTEM
Process Name: Unknown
Action: Quarantine
Action Status:  No additional a
```

```
03/27/2023 05:42:48 PM
LogName=Microsoft-Windows-Windows Defender/Operational
EventCode=1117
EventType=4
ComputerName=DESKTOP-887GK2L
User=SYSTEM
Sid=S-1-5-18
SidType=1
SourceName=Microsoft-Windows-Windows Defender
Type=Information
RecordNumber=443
Keywords=None
TaskCategory=None
OpCode=Info
Message=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
```

- 'SharpHound' is a tool used in Active Directory environments to collect data on user privileges, group memberships, and trust relationships. It's part of the 'BloodHound' toolkit and helps identify potential attack paths in a network.

BloodHound

From https://github.com/BloodHoundAD/BloodHound

> BloodHound is a single page Javascript web application, built on top of Linkurious, compiled with Electron, with a Neo4j database fed by a C# data collector.

BloodHound uses graph theory to reveal the hidden and often unintended relationships within an Active Directory or Azure environment. Attackers can use BloodHound to easily identify highly complex attack paths that would otherwise be impossible to quickly identify. Defenders can use BloodHound to identify and eliminate those same attack paths. Both blue and red teams can use BloodHound to easily gain a deeper understanding of privilege relationships in an Active Directory or Azure environment.

- To read more about 'bloodhound' click here: link

Firewall logs:

- When looking at the firewall logs, we see a few events that interest us.
- Firstly, the event ID 2033 ; when looking in it, we can see that all the firewall rules where cleared. I have a feeling this was done for the purpose of creating the challenge, but I'm not sure.
- Next, we see a few events with the ID 2004, that tells us that firewall rules where created or modified, which quite directly can indicate malicious activity.
- When looking at the first one I saw a run being created for Microsoft edge, but when looking deeper that's completely normal. Also, the SID isn't 'cyberjunkies' SID.
- So it's probably an automatic thing.

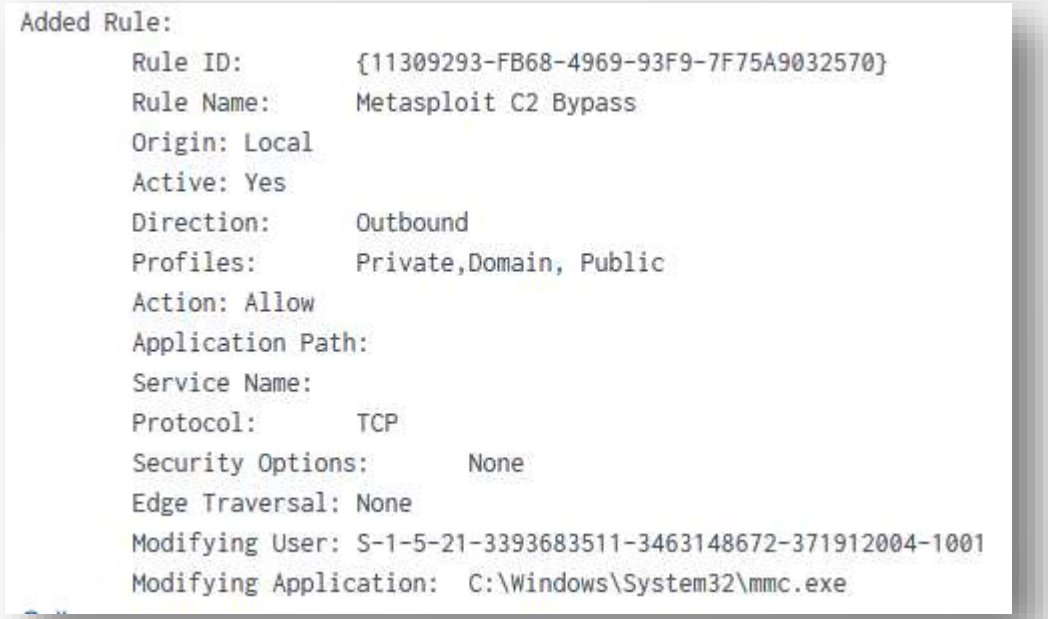
Values	Count	%
2004	3	37.5%
2006	2	25%
2010	1	12.5%
2033	1	12.5%
2051	1	12.5%

```
03/27/2023 05:37:11 PM
LogName=Microsoft-Windows-Windows Firewall With Advanced Security/Firewall
EventCode=2033
EventType=4
ComputerName=DESKTOP-887GK2L
User=LOCAL SERVICE
Sid=S-1-5-19
SidType=5
SourceName=Microsoft-Windows-Windows Firewall With Advanced Security
Type=Information
RecordNumber=1113
Keywords=None
TaskCategory=None
OpCode=Info
Message=All rules have been deleted from the Windows Defender Firewall configuration on this computer.

        Store Type:     12
        ModifyingUser:  NT SERVICE\MpsSvc
        ModifyingApplication:   C:\Windows\System32\svchost.exe
Collapse
```

```
03/27/2023 05:37:35 PM
LogName=Microsoft-Windows-Windows Firewall With Advanced Security/Firewall
EventCode=2004
EventType=4
ComputerName=DESKTOP-887GK2L
User=LOCAL SERVICE
Sid=S-1-5-19
SidType=5
SourceName=Microsoft-Windows-Windows Firewall With Advanced Security
Type=Information
RecordNumber=1118
Keywords=None
TaskCategory=None
OpCode=Info
Message=A rule has been added to the Windows Defender Firewall exception list.
```

```
Added Rule:
        Rule ID:        {B392BC66-2258-46F5-8A11-83F837B50783}
        Rule Name:      Microsoft Edge
        Origin: Local
        Active: Yes
        Direction:      Inbound
        Profiles:       Private,Domain, Public
        Action: Block
        Application Path:
        Service Name:
        Protocol:       Any
        Security Options:       None
        Edge Traversal: None
        Modifying User: NT SERVICE\MpsSvc
        Modifying Application:  C:\Windows\System32\svchost.exe
```

- Looking at the next event, I find that another urle has been created by ‘cyberjunkie’ this time, I know by the SID.
- He created a rule named ‘Metasploit C2 Bypass’ (task 2) that works on TCP protocol on all profile (public, private), and the rule allows outbound (task 3) connections.



Answers:

Task 1: 27/03/2023 14:37:09 (converted to UTC)

Task 2: Metasploit C2 Bypass

Task 3: Outbound

Task 4: Other Object Access Events

Task 5: HTB-AUTOMATION

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

Task 7: -A cyberjunkie@hackthebox.eu

Task 8: Sharphound

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

Task 10: Quarantine

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

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


LOG
FLAVOUR
Logjammer has been Solved!
Congratulations chananshenker, best of luck in capturing flags ahead!