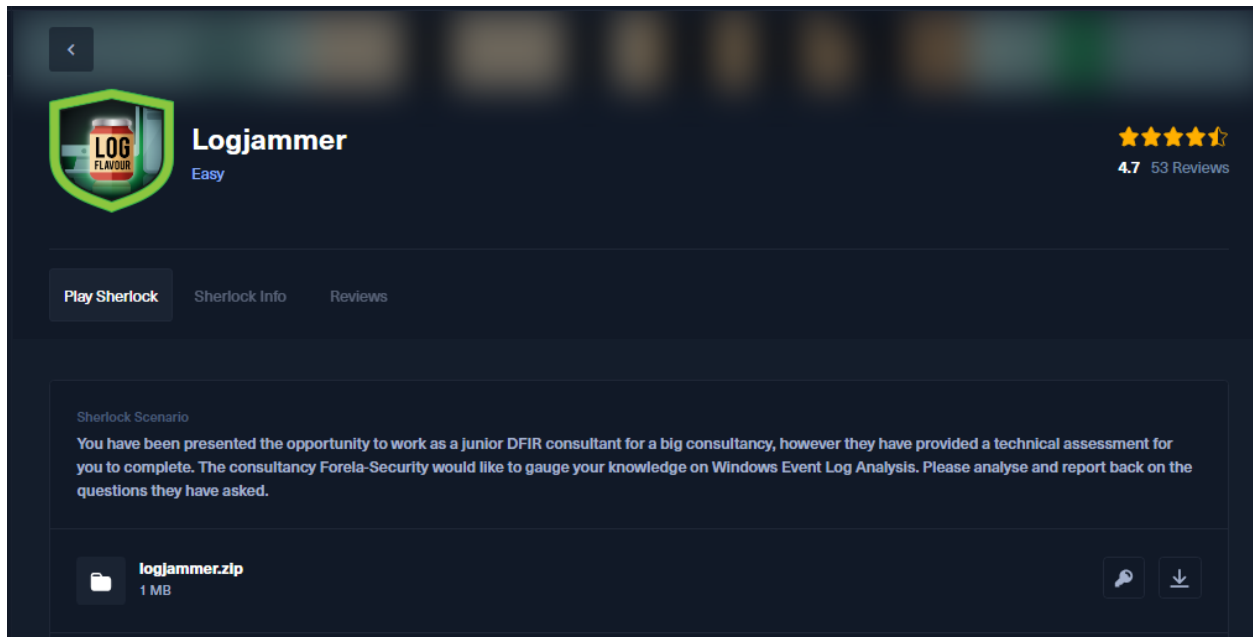


Resolviendo el sherlocks Logjammer

Link: <https://app.hackthebox.com/sherlocks/Logjammer>



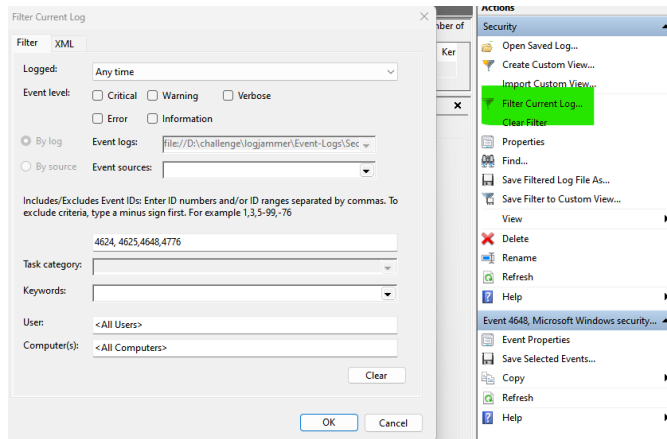
The screenshot shows the interface for the 'Logjammer' challenge on the HackTheBox platform. At the top, there is a navigation bar with a back arrow, the challenge icon (a green shield with a red 'LOG FLAVOUR' label), the title 'Logjammer', the difficulty 'Easy', and a rating of 4.7 stars from 53 reviews. Below the navigation bar, there are three tabs: 'Play Sherlock', 'Sherlock Info', and 'Reviews'. The 'Play Sherlock' tab is active, displaying the 'Sherlock Scenario' text: 'You have been presented 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 knowledge on Windows Event Log Analysis. Please analyse and report back on the questions they have asked.' At the bottom, there is a file download section showing 'logjammer.zip' (1 MB) with a download icon.

¿Cuándo el usuario Cyberjunkie inició sesión exitosamente en su computadora? (UTC)	3
El usuario manipuló la configuración del firewall en el sistema. Analice los registros de eventos del firewall para averiguar el nombre de la regla de firewall agregada.	4
¿Cuál es la dirección de la regla del firewall?	4
El usuario "cyberjunkie" creó una tarea programada. ¿Cómo se llama esta tarea?	6
¿Cuál es la ruta completa del archivo programado para la tarea?	6
¿Qué acción tomó el antivirus?	8
El usuario usó Powershell para ejecutar comandos. ¿Qué comando fue ejecutado por el usuario?	9
Sospechamos que el usuario eliminó algunos registros de eventos. ¿Qué archivo de registro de eventos se borró?	10
Datos curiosos	10

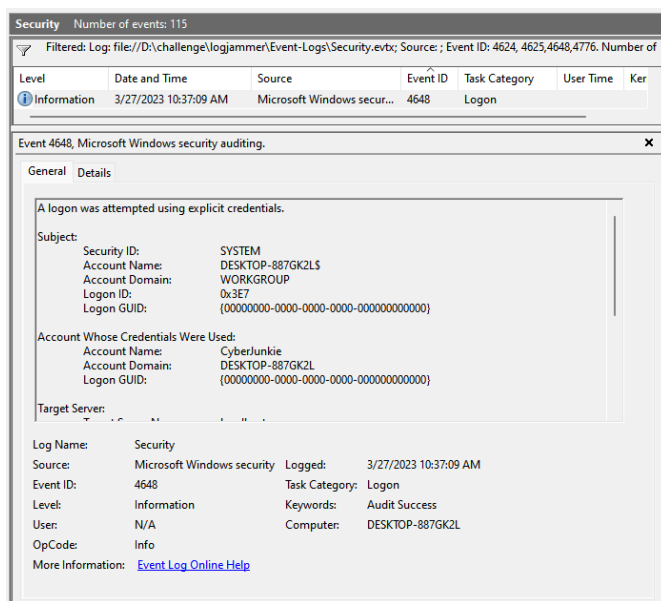
¿Cuándo el usuario Cyberjunkie inició sesión exitosamente en su computadora? (UTC)

Buscamos algunos event id comunes de inicio de sección: 4624, 4625, 4648, 4776. En los eventos de seguridad.

Vamos al apartado de filtros e ingresamos los id de los eventos que comenzaremos investigando:



Organizamos los eventos según la fecha y recorremos los eventos buscando el usuario “Cyberjunkie” y lo encontramos



Tenemos el evento y la fecha, ahora necesitamos convertirlo a utc.

Busco en google alguna página para esto, la tercera opción es la ganadora:

3/27/2023 10:37:09 AM es la hora del evento pasándola a utc tenemos 14:37 y le ponemos los segundos.

27/03/2023 14:37:09

El usuario manipuló la configuración del firewall en el sistema. Analice los registros de eventos del firewall para averiguar el nombre de la regla de firewall agregada.

Jaja, con este paso algo curioso que al organizar por tiempo la primera que esta es la que estábamos buscando, un punto a la organización por fecha. Aunque debemos correlacionar los eventos por ejemplo sabemos que la fecha de ingreso es 3/27/2023 10:37:09 AM la idea sería buscar eventos a partir de esta fecha.

Aun así, guardamos el ID 2004 “A rule has been added to the Windows Defender Firewall exception list”.

The screenshot displays the Windows Firewall event log. The top section shows a list of events with columns for Level, Date and Time, Source, Event ID, and Task Category. The bottom section shows the details for Event 2004, titled "Event 2004, Windows Firewall With Advanced Security".

Level	Date and Time	Source	Event ID	Task Category
Information	3/27/2023 10:44:43 AM	Windows Firewall With ...	2004	None
Information	3/27/2023 10:37:35 AM	Windows Firewall With ...	2004	None
Information	3/27/2023 10:37:35 AM	Windows Firewall With ...	2004	None
Information	3/27/2023 10:37:35 AM	Windows Firewall With ...	2006	None
Information	3/27/2023 10:37:35 AM	Windows Firewall With ...	2006	None
Information	3/27/2023 10:37:11 AM	Windows Firewall With ...	2010	None

Event 2004, Windows Firewall With Advanced Security

General | Details

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: Local
- Active: Yes
- Direction: Outbound
- Profiles: Private, Domain, Public
- Action: Allow
- Application Path:
- Service Name:

Log Name: Microsoft-Windows-Windows Firewall With Advanced Security/Firewall

Source: Windows Firewall With Adva **Logged:** 3/27/2023 10:44:43 AM

Event ID: 2004 **Task Category:** None

Level: Information **Keywords:** (2199023255552)

User: LOCAL SERVICE **Computer:** DESKTOP-887GK2L

OpCode: Info

More Information: [Event Log Online Help](#)

¿Cuál es la dirección de la regla del firewall?

Lo podemos ver en el evento anterior.

El usuario cambió la política de auditoría de la computadora. ¿Cuál es la subcategoría de esta política modificada?

Buscamos el ID 4719 “se cambió la directiva de auditoría del sistema”, para más información <https://learn.microsoft.com/es-es/windows/security/threat-protection/auditing/event-4719>

En este caso solo vemos un evento:

Filtered: Log: file://D:\challenge\logjammer\Event-Logs\Security.evtx; Source: ; Event ID: 4719. Number of events: 1

Level	Date and Time	Source	Event ID	Task Category
Information	3/27/2023 10:50:03 AM	Microsoft Windows sec...	4719	Audit Policy Change

Event 4719, Microsoft Windows security auditing.

General Details

System audit policy was changed.

Subject:

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

Audit Policy Change:

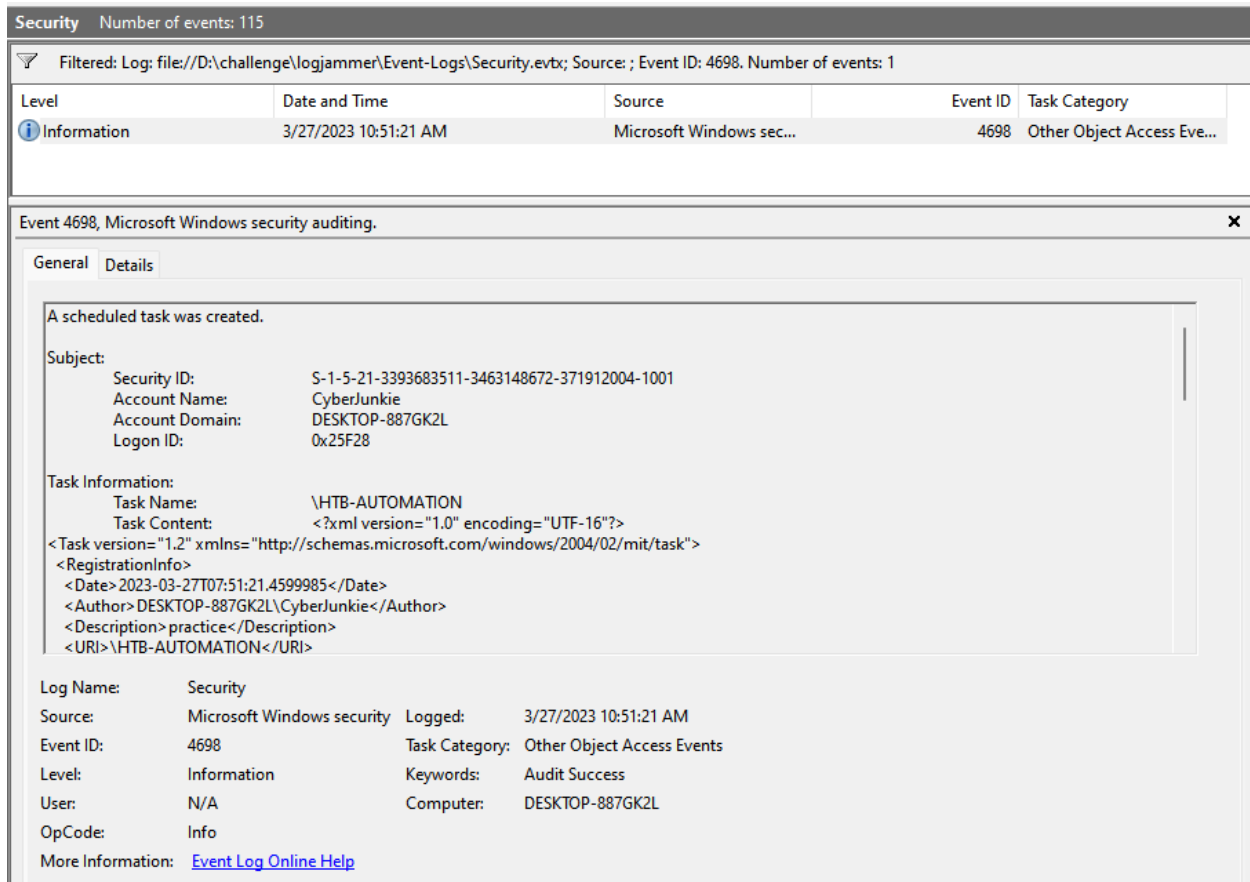
Category: Object Access
Subcategory: Other Object Access Events
Subcategory GUID: {0cce9227-69ae-11d9-bed3-505054503030}
Changes: Success Added

Log Name: Security
Source: Microsoft Windows security
Event ID: 4719
Level: Information
User: N/A
OpCode: Info
More Information: [Event Log Online Help](#)

Logged: 3/27/2023 10:50:03 AM
Task Category: Audit Policy Change
Keywords: Audit Success
Computer: DESKTOP-887GK2L

El usuario "cyberjunkie" creó una tarea programada. ¿Cómo se llama esta tarea?

Buscamos el ID 4698 "Se creó una tarea programada", para más información <https://learn.microsoft.com/es-es/windows/security/threat-protection/auditing/event-4698>



Security Number of events: 115

Filtered: Log: file://D:\challenge\logjammer\Event-Logs\Security.evtx; Source: ; Event ID: 4698. Number of events: 1

Level	Date and Time	Source	Event ID	Task Category
Information	3/27/2023 10:51:21 AM	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><Date>2023-03-27T07:51:21.459985</Date><Author>DESKTOP-887GK2L\CyberJunkie</Author><Description>practice</Description><URI>\HTB-AUTOMATION</URI></Task></xml>

Log Name: Security

Source: Microsoft Windows security Logged: 3/27/2023 10:51:21 AM

Event ID: 4698 Task Category: Other Object Access Events

Level: Information Keywords: Audit Success

User: N/A Computer: DESKTOP-887GK2L

OpCode: Info

More Information: [Event Log Online Help](#)

¿Cuál es la ruta completa del archivo programado para la tarea?

Para responder esta pregunta usamos el evento anterior en el campo "Command", podemos ver la información buscando la ruta xml o también podemos darle al apartado de detalles y buscarla.

¿Cuáles son los argumentos del comando?

Esta respuesta también está en el log anterior en el campo "Arguments".

El antivirus que se ejecuta en el sistema identificó una amenaza y realizó acciones al respecto. ¿Qué herramienta fue identificada como malware por el antivirus?

Justo tengo una lista de ID de eventos interesantes de Windows Defender

```
Windows Defender
Applications and Services Logs > Microsoft > Windows > Windows Defender.
Event ID 1006 MALWAREPROTECTION_MALWARE_DETECTED
Event ID 1007 MALWAREPROTECTION_MALWARE_ACTION_TAKEN
Event ID 1008 MALWAREPROTECTION_MALWARE_ACTION_FAILED
Event ID 1009 MALWAREPROTECTION_QUARANTINE_RESTORE
Event ID 1011 MALWAREPROTECTION_QUARANTINE_DELETE
Event ID 1013 MALWAREPROTECTION_MALWARE_HISTORY_DELETE
Event ID 1014 MALWAREPROTECTION_MALWARE_HISTORY_DELETE_FAILED
Event ID 1015 MALWAREPROTECTION_BEHAVIOR_DETECTED
Event ID 1116 MALWAREPROTECTION_STATE_MALWARE_DETECTED
Event ID 1117 MALWAREPROTECTION_STATE_MALWARE_ACTION_TAKEN
Event ID 1118 MALWAREPROTECTION_STATE_MALWARE_ACTION_FAILED
Event ID 1127 MALWAREPROTECTION_FOLDER_GUARD_SECTOR_BLOCK
Event ID 5008 MALWAREPROTECTION_ENGINE_FAILURE
Event ID 5010 MALWAREPROTECTION_ANTISPYWARE_DISABLED

Event ID 5011 MALWAREPROTECTION_ANTIVIRUS_ENABLED
Event ID 5012 MALWAREPROTECTION_ANTIVIRUS_DISABLED
Event ID 3002 MALWAREPROTECTION_RTP_FEATURE_FAILURE Real-time protection
Event ID 5001 MALWAREPROTECTION_RTP_DISABLED Real-time protection
```

En este caso usaremos la información previa recopilada tenemos que la fecha de ingreso del usuario es 3/27/2023 10:37:09 AM buscaremos a partir de esta.

Encontramos el evento de detención con el ID 1116:

Windows Defender-Operational Number of events: 444

Level	Date and Time	Source	Event ID	Task Category
Information	3/27/2023 10:37:16 AM	Windows Defender	5007	None
Information	3/27/2023 10:37:18 AM	Windows Defender	5007	None
Information	3/27/2023 10:37:18 AM	Windows Defender	5007	None
Information	3/27/2023 10:41:45 AM	Windows Defender	5007	None
Warning	3/27/2023 10:42:34 AM	Windows Defender	1116	None
Warning	3/27/2023 10:42:34 AM	Windows Defender	1116	None
Information	3/27/2023 10:42:34 AM	Windows Defender	5007	None
Information	3/27/2023 10:42:48 AM	Windows Defender	1117	None
Information	3/27/2023 10:42:48 AM	Windows Defender	1117	None

Event 1116, Windows Defender

General Details

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-Algorithm=AWS4-HMAC-SHA256&X-Amz-

¿Cuál es la ruta completa del malware que generó la alerta?

En el evento anterior tenemos esta información.

¿Qué acción tomó el antivirus?

Que ocurre en este caso que en los IDs adjuntos de forma anterior tenemos que el 1116 es el evento de detención y el 1117 es el de acción tomada, buscamos este id ahora.

Windows Defender-Operational Number of events: 444

Level	Date and Time	Source	Event ID	Task Category
Warning	3/27/2023 10:42:34 AM	Windows Defender	1116	None
Warning	3/27/2023 10:42:34 AM	Windows Defender	1116	None
Information	3/27/2023 10:42:34 AM	Windows Defender	5007	None
Information	3/27/2023 10:42:48 AM	Windows Defender	1117	None
Information	3/27/2023 10:42:48 AM	Windows Defender	1117	None

Event 1117, Windows Defender

General Details

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-b226-2dccc4f7c1e3?X-Amz-Algorithm=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-Amz-Expires=300&X-Amz-Signature=f969ef5ca3eec150dc1e23623434adc1e4a444ba026423c32edf5e85d881a771&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=385323486&response-content-disposition=attachment(0EBC4BEA-5532-4EFB-8A34-64F91CC8702E)JDESKTOP-887GK2L\CyberJunkie\file(0EBC4BEA-5532-4EFB-8A34-64F91CC8702E)JDESKTOP-887GK2L\SharpHound-v1.1.0.zip&response-content-type=application/zip; ProcessStart: 133244017530289775

Log Name: Microsoft-Windows-Windows Defender/Operational
Source: Windows Defender Logged: 3/27/2023 10:42:48 AM
Event ID: 1117 Task Category: None
Level: Information Keywords:
User: SYSTEM Computer: DESKTOP-887GK2L
OpCode: Info
More Information: [Event Log Online Help](#)

El usuario usó Powershell para ejecutar comandos. ¿Qué comando fue ejecutado por el usuario?

Nuevamente mencionamos que ya sabemos la fecha del ingreso, detención del antivirus y script ejecutado con todos estos datos no duraremos mucho para encontrar lo solicitado.

Powershell-Operational Number of events: 578

Level	Date and Time	Source	Event ID	Task Category
Information	3/27/2023 10:58:33 AM	PowerS...	4103	Executing Pipeline
Verbose	3/27/2023 10:58:33 AM	PowerS...	4104	Execute a Remote Command
Information	3/27/2023 10:58:33 AM	PowerS...	4103	Executing Pipeline
Information	3/27/2023 10:58:31 AM	PowerS...	4103	Executing Pipeline
Information	3/27/2023 10:58:28 AM	PowerS...	4103	Executing Pipeline
Information	3/27/2023 10:58:07 AM	PowerS...	4103	Executing Pipeline
Information	3/27/2023 10:58:07 AM	PowerS...	4103	Executing Pipeline
Verbose	3/27/2023 10:58:07 AM	PowerS...	4104	Execute a Remote Command

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: 3/27/2023 10:58:33 AM
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
More Information: [Event Log Online Help](#)

Para futuros casos pueden usar el ID 4104

Sospechamos que el usuario eliminó algunos registros de eventos. ¿Qué archivo de registro de eventos se borró?

Para buscar estos tenemos los ID 1102.

The screenshot shows the Windows Event Viewer interface. At the top, a filter bar indicates 'Filtered: Log: file://D:\challenge\logjammer\Event-Logs\Security.evtx; Source: ; Event ID: 1102. Number of events: 1'. Below this, a table lists the filtered events:

Level	Date and Time	Source	Event ID	Task Category	User Time	Kernel
Information	3/27/2023 10:36:45 AM	Eventlog	1102	Log clear		

Below the table, the 'Event 1102, Eventlog' details window is open. It has two tabs: 'General' and 'Details'. The 'General' tab is selected, showing the following information:

The audit log was cleared.
Subject:
Security ID: S-1-5-21-3393683511-3463148672-371912004-1001
Account Name: CyberJunkie
Domain Name: DESKTOP-887GK2L
Logon ID: 0x25235

Below the subject information, the following details are listed:

Log Name: Security
Source: Eventlog
Event ID: 1102
Level: Information
User: N/A
OpCode: Info
More Information: [Event Log Online Help](#)




Additional details on the right side of the 'General' tab include:

Logged: 3/27/2023 10:36:45 AM
Task Category: Log clear
Keywords: Audit Success
Computer: DESKTOP-887GK2L

Esta pregunta si tiene una dificultad más elevada y deberemos revisar más registros para obtenerla, la dejare sin responder en este caso así pueden tomarse el tiempo de buscarla, si la necesitan pueden escribirme al correo eliasramirezs2108@gmail.com


Datos curiosos

Al buscar los ID de inicio de sección podemos ver que en este caso tenemos el 4648 y 4624 generados al mismo tiempo. Aun así, se recomienda buscar ambos para una visibilidad general.

Level	Date and Time	Source	Event ID	Task Category	User Time	Ker
 Information	3/27/2023 10:37:09 AM	Microsoft Windows secur...	4648	Logon		
 Information	3/27/2023 10:37:09 AM	Microsoft Windows secur...	4624	Logon		
 Information	3/27/2023 10:37:09 AM	Microsoft Windows secur...	4624	Logon		

Security Number of events: 115

Filtered: Log: file://D:\challenge\logjammer\Event-Logs\Security.evtx; Source: ; Event ID: 4719. Number of events: 1

Level	Date and Time	Source	Event ID	Task Category
 Information	3/27/2023 10:50:03 AM	Microsoft Windows secur...	4719	Audit Policy Ch...

Event 4719, Microsoft Windows security auditing.

General Details

System audit policy was changed.

Subject:

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

Audit Policy Change:

Category: Object Access
Subcategory: Other Object Access Events

Log Name: Security
Source: Microsoft Windows security
Event ID: 4719
Level: Information
User: N/A
OpCode: Info
More Information: [Event Log Online Help](#)

Logged: 3/27/2023 10:50:03 AM
Task Category: Audit Policy Change
Keywords: Audit Success
Computer: DESKTOP-887GK2L