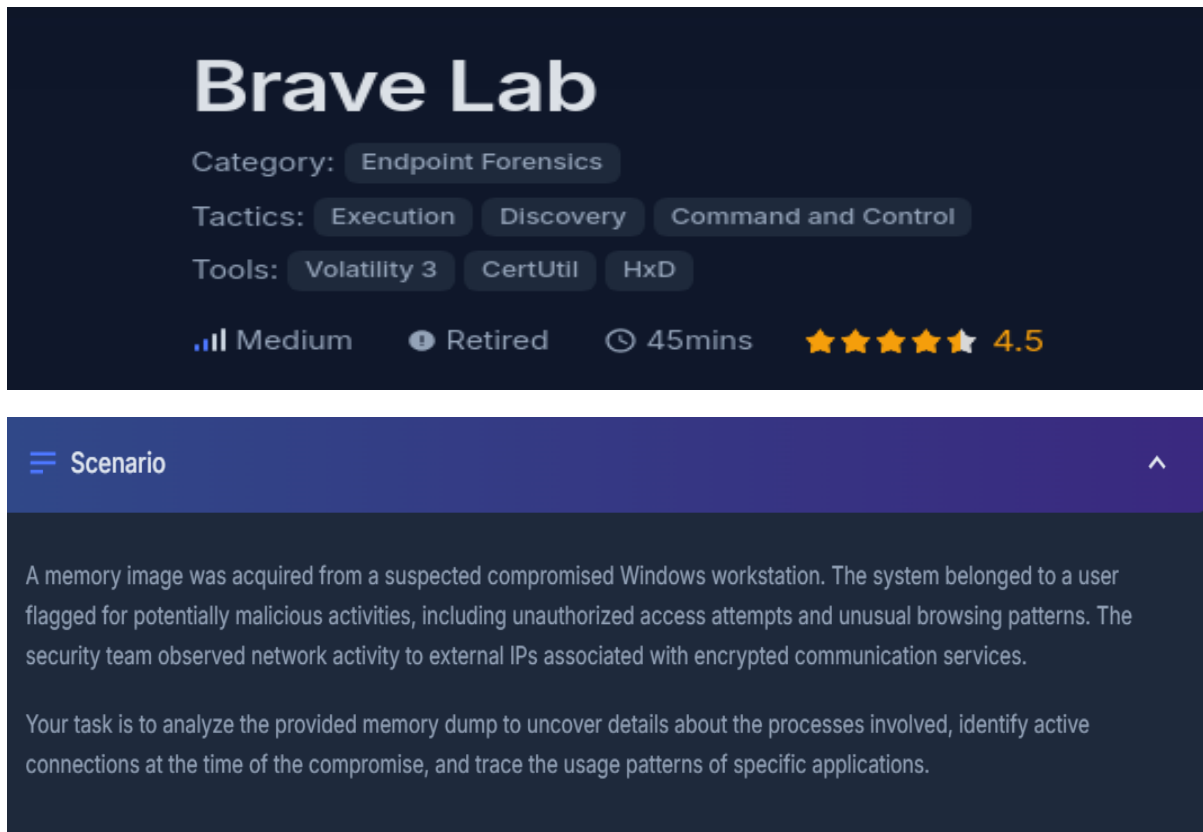


Reporte de Análisis Forense – CTF Brave con Volatility3



The screenshot displays the 'Brave Lab' CTF challenge interface. At the top, the title 'Brave Lab' is prominently shown. Below it, the 'Category' is 'Endpoint Forensics'. The 'Tactics' section includes 'Execution', 'Discovery', and 'Command and Control'. The 'Tools' section lists 'Volatility 3', 'CertUtil', and 'HxD'. A progress bar indicates 'Medium' difficulty, 'Retired' status, a '45mins' time limit, and a '4.5' star rating. The 'Scenario' section, which is expanded, provides a detailed description of the challenge: a memory image was acquired from a suspected compromised Windows workstation. The system belonged to a user flagged for potentially malicious activities, including unauthorized access attempts and unusual browsing patterns. The security team observed network activity to external IPs associated with encrypted communication services. The task is to analyze the provided memory dump to uncover details about the processes involved, identify active connections at the time of the compromise, and trace the usage patterns of specific applications.

Brave Lab

Category: Endpoint Forensics

Tactics: Execution Discovery Command and Control

Tools: Volatility 3 CertUtil HxD

Medium Retired 45mins 4.5

Scenario

A memory image was acquired from a suspected compromised Windows workstation. The system belonged to a user flagged for potentially malicious activities, including unauthorized access attempts and unusual browsing patterns. The security team observed network activity to external IPs associated with encrypted communication services.

Your task is to analyze the provided memory dump to uncover details about the processes involved, identify active connections at the time of the compromise, and trace the usage patterns of specific applications.

Introducción

Este informe detalla el procedimiento realizado durante un análisis forense de memoria RAM enfocado en el navegador **Brave**, utilizando la herramienta **Volatility3**. El objetivo fue identificar diversas **flags** que representan evidencia digital útil dentro de un entorno comprometido. A través de comandos específicos y técnicas forenses, se buscó comprender el comportamiento del sistema y posibles indicios de actividad maliciosa.

Desarrollo del análisis

Flag 1 – Información general de la imagen de memoria

Q1  Solved : 1095

What time was the RAM image acquired according to the suspect system?

Cómo:

Se utilizó el plugin windows.info para extraer metadatos de la imagen de memoria, como el perfil del sistema operativo, fecha y hora de la captura.

python3 vol.py -f <direccion_de_memoria> windows.info

```
> python3 vol.py -f /home/csi/Desktop/20210430-Win10Home-20H2-64bit-memdump.mem windows.info
Volatility 3 Framework 2.0.2
Progress: 100.00 PDB scanning finished
Variable Value
Kernel Base 0xf8043cc00000
DTB 0x1aa000
Symbols file:///opt/volatility3/volatility3/symbols/windows/ntkrnlmp.pdb/769C521E4833ECF72E21F02BF33691A5-1.json.xz
Is64Bit True
IsPAE False
Layer_name 0 WindowsIntel32e
memory_layer 1 FileLayer
KdVersionBlock 0xf8043d80f368
Major/Minor 15.19041
MachineType 34404
NumberProcessors 4
SystemTime 2021-04-30 17:52:19
NtSystemRoot C:\Windows
NtProductType NtProductWinNt
NtMajorVersion 10
NtMinorVersion 0
PE MajorOperatingSystemVersion 10
PE MinorOperatingSystemVersion 0
PE Machine 34404
PE TimeDateStamp Tue Oct 11 07:04:26 1977
```

Por qué:

Este paso permite validar la imagen, determinar su origen y asegurarse de que se puedan aplicar los plugins de Volatility correctamente.

Q1  Solved : 1096

What time was the RAM image acquired according to the suspect system?

2021-04-30 17:52



 Hints

 Submit

La flag es 2021-04-30 17:52

Flag 2 – Verificación del hash de la imagen

Q2 ☐ Solved : 1109

What is the SHA256 hash value of the RAM image?

SHA256 Hash

Cómo:

Se empleó el comando estándar sha256sum para calcular el hash SHA-256 de la imagen RAM.

sha256sum <nombre_de_la_imagen>

```
08:15:44 csi@csi ~
> ls
Cases Documents Images Pictures Templates powerup.log wxtoimg
Desktop Downloads Music Public Videos snap

08:22:02 csi@csi ~
> cd Desktop/

08:22:05 csi@csi ~/Desktop
> ls
159-Ramnit.zip analisis_volatil
20210430-Win10Home-20H2-64bit-memdump.mem analisis_volatil1
67-AfricanFalls2.zip temp_extract_dir
Cases volatility3
Start a Case.desktop'

08:22:05 csi@csi ~/Desktop
> sha256sum 20210430-Win10Home-20H2-64bit-memdump.mem
9db01b1e7b19a3b2113bfb65e860fffd7a1630bdf2b18613d206ebf2aa0ea172 20210430-Win10Home-20H2-64bit-memdump.mem

08:22:50 csi@csi ~/Desktop
> ^C

08:23:11 csi@csi ~/Desktop
>
```

Por qué:

Verificar el hash garantiza la integridad de la imagen analizada y permite detectar manipulaciones o corrupción del archivo.

Q2 ☒ Solved : 1110

What is the SHA256 hash value of the RAM image?

SHA256 Hash


Flag 2: 9db01b1e7b19a3b2113bfb65e860fffd7a1630bdf2b18613d206ebf2aa0ea172


Flag 3 – PID del navegador Brave

Q3 ☐ Solved : 1101

What is the process ID of **brave.exe**?

123 Enter your answer...

 Hints

 Submit

Cómo:

Se usó el plugin **pslist** combinado con **grep** para buscar el proceso **brave.exe** y obtener su PID.

python3 vol.py -f <direccion_de_memoria> windows.pslist | grep brave.exe

```
08:10:02 csi@csi /opt/volatility3
> python3 vol.py -f /home/csi/Desktop/20210430-Win10Home-20H2-64bit-memdump.mem windows.pslist | grep brave.exe
4856ress187200.0brave.exe 0xbff0f6ca782c0 0 . 1 False 2021-04-30 17:48:45.000000 2021-04-30 17:50:56.000000 Disabled
```


Por qué:


Identificar el PID de Brave es esencial para analizar su comportamiento, conexiones de red y archivos asociados.

Q3 ☒ Solved : 1102

What is the process ID of **brave.exe**?

123 4856

 Hints

 Submit

Flag 3: **4856**

Flag 4 – Conexiones establecidas

Q4 ○ Solved : 1041

How many established network connections were there at the time of acquisition?

123 **

Please enter a numeric answer.

💡 Hints Submit

Cómo:

Se utilizó el plugin **netscan** para listar las conexiones activas, filtrando por el estado "ESTABLISHED".

```
python3 vol.py -f <direccion_de_memoria> windows.netscan | grep -i "established" | nl
```

```
python3 vol.py -f /home/csi/Desktop/20210430-Win10Home-20H2-64bit-memdump.mem windows.netscan | grep -i "established" | nl
1 1s0xbff0f6a53ca20 TCPv4 10.0.2.15ing fin49833 52.230.222.68 443 ESTABLISHED 2812 svchost.exe 2021-04-30 17:50:07.000000
2 0xbff0f6ad16050 TCPv4 10.0.2.15 49829 142.250.191.208 443 ESTABLISHED 5624 svchost.exe 2021-04-30 17:49:58.000000
3 0xbff0f6ad1fad0 TCPv4 10.0.2.15 49847 52.230.222.68 443 ESTABLISHED 2812 svchost.exe 2021-04-30 17:52:17.000000
4 0xbff0f6c6352b0 TCPv4 10.0.2.15 49842 52.113.196.254 443 ESTABLISHED 5104 SearchApp.exe 2021-04-30 17:51:25.000000
5 0xbff0f6c7104d0 TCPv4 10.0.2.15 49778 185.70.41.130 443 ESTABLISHED 1840 chrome.exe 2021-04-30 17:45:00.000000
6 0xbff0f6cd4fa20 TCPv4 10.0.2.15 49837 204.79.197.200 443 ESTABLISHED 5104 SearchApp.exe 2021-04-30 17:51:18.000000
7 0xbff0f6d0c64a0 TCPv4 10.0.2.15 49843 204.79.197.222 443 ESTABLISHED 5104 SearchApp.exe 2021-04-30 17:51:26.000000
8 0xbff0f6d51c4a0 TCPv4 10.0.2.15 49838 13.107.3.254 443 ESTABLISHED 5104 SearchApp.exe 2021-04-30 17:51:23.000000
9 0xbff0f6d525a20 TCPv4 10.0.2.15 49845 23.101.202.202 443 ESTABLISHED 1156 MsMpEng.exe 2021-04-30 17:51:36.000000
10 0xe80000193a20 TCPv4 10.0.2.15 49845 23.101.202.202 443 ESTABLISHED 1156 MsMpEng.exe 2021-04-30 17:51:36.000000
```

Por que:

Observar conexiones establecidas permite identificar comunicación activa entre el sistema y posibles destinos maliciosos o sospechosos.

Q4 ✔ Solved : 1041

How many established network connections were there at the time of acquisition?

123 10

💡 Hints Submit

Flag 4: 10 (corresponde al número de conexiones establecidas detectadas)

Flag 5 – Dominio remoto asociado

Cómo:

Tras identificar una conexión establecida por el proceso **chrome.exe**, se investigó la IP remota 185.70.41.130 mediante servicios de geolocalización como **ipinfo.io**.

```
08:46:15 csi@csi /opt/volatility3
python3 vol.py -f /home/csi/Desktop/20210430-Win10Home-20H2-64bit-memdump.mem windows.netscan | grep -i "established" | grep chrome
xbf0f6c7104d0.0TCPv4 10.0.2.15DB scan49778f n185.70.41.130 443 ESTABLISHED 1840 chrome.exe 2021-04-30 17:45:00.000000
```

Explore our IP Address Database Downloads for instant access to our IP address insights [Learn more](#)

IPInfo Products Solutions Why IPInfo? Pricing Resources Docs Login [Sign up](#)

[All IP Ranges](#) > [185.0.0.0/8](#) > [185.70.0.0/16](#) > [185.70.41.0/24](#) > 185.70.41.130

185.70.41.130

🇨🇭 Zürich, Zurich, Switzerland

🌐 hosting

Search an IP or AS number

Need more data or want to access it via API or data downloads? Sign up to get free access [Sign up for free](#)

Summary

Geolocation

Summary

ASN [AS62371 - Proton AG](#)

Por qué:

Analizar las direcciones IP a las que se conecta el sistema permite detectar relaciones con dominios sospechosos, en este caso relacionado con **ProtonMail**.

Explore our IP Address Database Downloads for instant access to our IP address insights [Learn more](#)

IPInfo Products Solutions Why IPInfo? Pricing Resources Docs Login [Sign up](#)

Need more data or want to access it via API or data downloads? Sign up to get free access [Sign up for free](#)

Summary

Geolocation

Privacy

ASN

Company

Abuse

Hosted domains

Summary

ASN [AS62371 - Proton AG](#)

Hostname [185-70-41-130.protonmail.ch](#)

Range [185.70.41.0/24](#)

Company Proton AG

Hosted domains 1

Privacy ☒ True

Anycast ☐ False

ASN type Business

Abuse contact [abuse@protonmail.ch](#)

Flag 5: protonmail.ch

Flag 6 – Hash MD5 del ejecutable de OneDrive

Cómo:

1. Se identificó el proceso con PID 6988 usando pslist.

```
python3 vol.py -f <direccion_de_memoria> windows.pslist | grep 6988
```

```
09:26:22 csi@csi /opt/volatility3
> python3 vol.py -f /home/csi/Desktop/20210430-Win10Home-20H2-64bit-memdump.mem windows.pslist | grep 6988
6988 4352 OneDrive.exe 0xbf0f6d4262c0 26 - 1 True 2021-04-30 17:40:01.000000 N/A Disabled
```

- Se localizaron archivos relacionados con el proceso usando filescan.

python3 vol.py -f <direccion_de_memoria> windows.filescan | grep 6988

```
09:30:27 csi@csi /opt/volatility3
> python3 vol.py -f /home/csi/Desktop/20210430-Win10Home-20H2-64bit-memdump.mem windows.filescan | grep 6988
0xbf0f6abb7c00\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Cache\8ff0e5bb7fd9ab0df2709d2d761abc29b6988eec\content.bin 216
0xbf0f6abb7c00\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Cache\8ff0e5bb7fd9ab0df2709d2d761abc29b6988eec\content.phf 216
0xbf0f6d2539f0 \Users\John Doe\AppData\Local\Microsoft\OneDrive\logs\Personal\SyncEngine-2021-04-30_1740_6988_1_andl_216
0xbf0f6d25d950 \Users\John Doe\AppData\Local\Microsoft\OneDrive\setup\logs\Update_2021-04-30_174002_6988-6992.log 216
```

- Se extrajo el ejecutable usando el plugin pslist --dump.

python3 vol.py -f <direccion_de_memoria> windows.pslist --pid 6988 --dump

```
09:46:23 csi@csi /opt/volatility3
> python3 vol.py -f /home/csi/Desktop/20210430-Win10Home-20H2-64bit-memdump.mem windows.pslist --pid 6988 --dump
Volatility 3 Framework 2.0.2
Progress: 100.00 PDB scanning finished
PID PPID ImageFileName Offset(V) Threads Handles SessionId Wow64 CreateTime ExitTime File output
6988 4352 OneDrive.exe 0xbf0f6d4262c0 26 - 1 True 2021-04-30 17:40:01.000000 N/A pid.6988.0x1c0000.dmp
```

- Se calculó el hash MD5 del archivo.

```
09:47:44 csi@csi /opt/volatility3
> md5sum pid.6988.0x1c0000.dmp
0b493d8e26f03ccd2060e0be85f430af pid.6988.0x1c0000.dmp
09:47:47 csi@csi /opt/volatility3
>
```

Por qué:

Obtener el hash del binario permite compararlo con bases de datos de malware para confirmar su legitimidad o identificar variantes maliciosas.

Q6 Solved : 960

What is the MD5 hash value of the process executable for PID 6988?

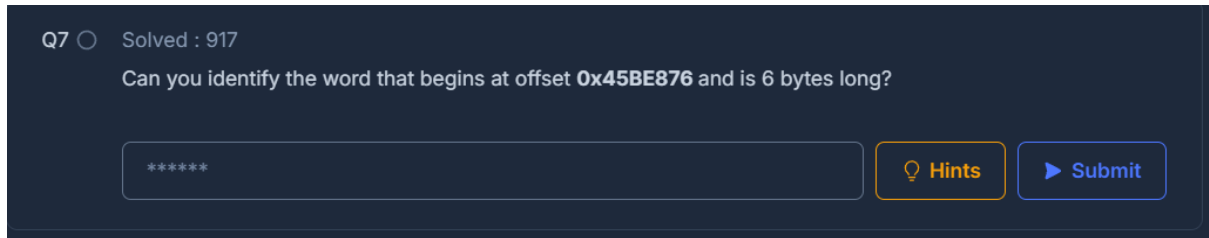
MD5 Hash

Hints

Submit

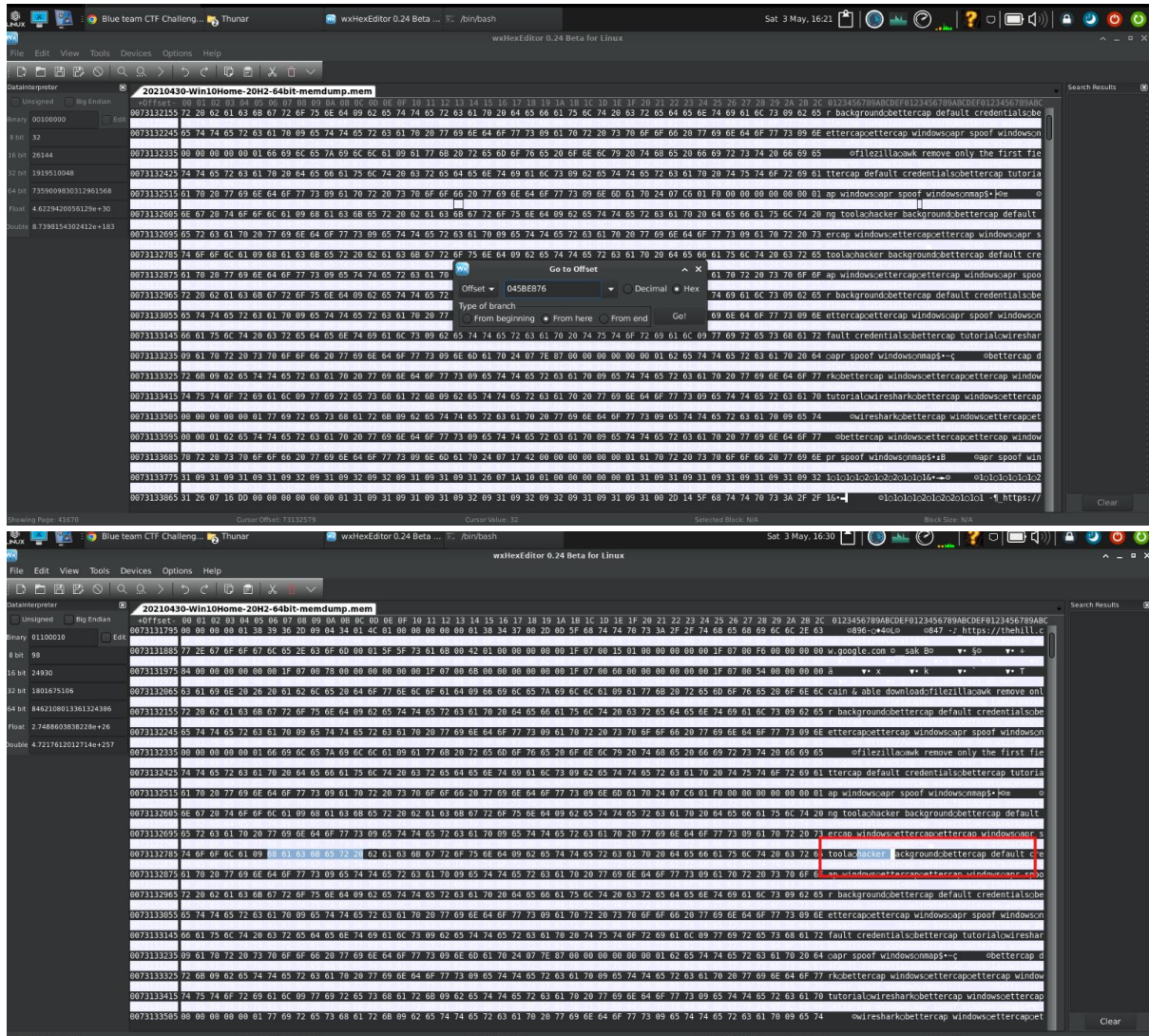
Flag 6: 0b493d8e26f03ccd2060e0be85f430af

Flag 7 – Análisis manual en hexadecimal



Cómo:

Se cargó la imagen RAM en un editor hexadecimal. Luego se navegó manualmente hasta un offset específico utilizando Ctrl + G.



Por qué:

Algunos valores solo se encuentran con inspección directa de la memoria. Este tipo de análisis puede revelar datos ocultos que no son detectables con plugins automatizados.

Q7 Solved : 917

Can you identify the word that begins at offset **0x45BE876** and is 6 bytes long?

hacker

Hints Submit

Flag 7: hacker

Flag 8 – Creación del proceso padre de PowerShell

Q8 Solved : 958

What is the creation date and time of the parent process of **powershell.exe**?

YYYY-MM-DD HH:MM

Hints Submit

Cómo:

Se localizó powershell.exe con **pslist**, identificando su PID. Luego se buscó el proceso padre con ese PID.

python3 vol.py -f <direccion_de_memoria> windows.pslist | grep Powershell.exe

```
10:37:19 csi@csi /opt/volatility3
> python3 vol.py -f /home/csi/Desktop/20210430-Win10Home-20H2-64bit-memdump.mem windows.pslist | grep powershell.exe
5096ress435200.0powershell.exe 0xbf0f6d97f2c0 12 - 1 False 2021-04-30 17:51:19.000000 N/A Disabled
```

python3 vol.py -f <direccion_de_memoria> windows.pslist | grep 4352


```
10:38:51 csi@csi /opt/volatility3
> python3 vol.py -f /home/csi/Desktop/20210430-Win10Home-20H2-64bit-memdump.mem windows.pslist | grep 4352
4352 4296 explorer.exe 0xbf0f6ca662c0 82 - 1 False 2021-04-30 17:39:48.000000 N/A Disabled
6772 4352 SecurityHealth 0xbf0f6d493080 1 - 1 False 2021-04-30 17:40:00.000000 N/A Disabled
6884 4352 VBoxTray.exe 0xbf0f6d186080 11 - 1 False 2021-04-30 17:40:01.000000 N/A Disabled
6988 4352 OneDrive.exe 0xbf0f6d4262c0 26 - 1 True 2021-04-30 17:40:01.000000 N/A Disabled
1328 4352 chrome.exe 0xbf0f6d53e080 26 - 1 False 2021-04-30 17:44:52.000000 N/A Disabled
5096 4352 powershell.exe 0xbf0f6d97f2c0 12 - 1 False 2021-04-30 17:51:19.000000 N/A Disabled
```

Por qué:


Analizar el árbol de procesos permite comprender cómo se inició PowerShell, una herramienta que puede ser abusada por atacantes.



Por qué:

Analizar el árbol de procesos permite comprender cómo se inició PowerShell, una herramienta que puede ser abusada por atacantes.

Q8  Solved : 959


What is the creation date and time of the parent process of powershell.exe?

2021-04-30 17:39 

 Hints  Submit



Flag 8: 2021-04-30 17:39

Flag 9 – Ruta completa de ejecución de notepad.exe

Q9  Solved : 945

What is the full path and name of the last file opened in notepad?

File Path(e.g.,C:\path\)

 Hints  Submit

Cómo:

Se utilizó el plugin **cmdline** para recuperar los comandos utilizados en cada proceso, filtrando por notepad.

python3 vol.py -f <direccion_de_memoria> windows.cmdline | grep notepad

```
10:51:37 csi@csi /opt/volatility3
> python3 vol.py -f /home/csi/Desktop/20210430-Win10Home-20H2-64bit-memdump.mem windows.cmdline | grep notepad
2520ressnotepad.exe "C:\Windows\system32\notepad.exe" C:\Users\JOHNDO-1\AppData\Local\Temp\7z04FB31F24\accountNum
```

Por qué:

La línea de comandos puede mostrar cómo se ejecutó un programa, desde qué ruta y con qué argumentos, lo cual es útil para rastrear scripts o archivos maliciosos.

Q9  Solved : 946

What is the full path and name of the last file opened in notepad?

File Path (e.g., C:\path\)

C:\Users\JOHNDO~1\AppData\Local\Temp\7zO4FB31F24\accountNum

 Hints

 Submit

Flag 9: C:\Users\JOHNDO~1\AppData\Local\Temp\7zO4FB31F24\accountNum

Flag 10 – Tiempo de uso de Brave\


Q10  Solved : 899

How long did the suspect use **Brave** browser? (In Hours)

Note: Round to the nearest whole number in hours.

123 *

 Hints

 Submit

Wrong Answer, Answer Format: *

Cómo:

Se usó el plugin **registry.userassist**, que recopila métricas de uso de programas por parte del usuario.

python3 vol.py -f <direccion_de_memoria> windows.registry.userassist | grep Brave

```
08:59:55 csi@csi /opt/volatility3
> python3 vol.py -f /home/csi/Desktop/20210430-Win10Home-20H2-64bit-memdump.mem windows.registry.userassist | grep -i brave
* 0xa80333cda000 \??\C:\Users\John Doe\ntuser.dat ntuser.dat\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count 2021-04-30 17:52:18.000000
/alue %ProgramFiles%\BraveSoftware\Temp\GUM20E0.tmp\BraveUpdate.exe N/A 0 0 0:00:03.531000 N/A
* 0xa80333cda000 \??\C:\Users\John Doe\ntuser.dat ntuser.dat\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count 2021-04-30 17:52:18.000000
/alue %ProgramFiles%\BraveSoftware\Update\BraveUpdate.exe N/A 0 1 0:00:24.797000 N/A
* 0xa80333cda000 \??\C:\Users\John Doe\ntuser.dat ntuser.dat\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count 2021-04-30 17:52:18.000000
/alue Brave N/A 9 22 4:01:54.328000 2021-04-30 17:48:45.000000
* 0xa80333cda000 \??\C:\Users\John Doe\ntuser.dat ntuser.dat\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE3309F}\Count 2021-04-30 17:51:18.000000
/alue C:\Users\Public\Desktop\Brave.Lnk N/A 8 0 0:00:00.588000 2021-04-30 17:48:45.000000
```

Por qué:


Saber cuánto tiempo se usó un programa puede indicar si fue parte de una actividad legítima o relacionada con un incidente.

Q10  Solved : 900
How long did the suspect use **Brave** browser? (In Hours)

Note: Round to the nearest whole number in hours.

123 4

 Hints

 Submit

Flag 10: 4 (horas de uso del navegador Brave)



Congratulations

You have successfully completed this lab!

Share your achievement



I successfully completed Brave Blue Team Lab at @CyberDefenders!
<https://cyberdefenders.org/blueteam-ctf-challenges/achievements/malowerr/brave/>

#CyberDefenders #CyberSecurity #BlueYard #BlueTeam #InfoSec #SOC
#SOCAnalyst #DFIR #CCD #CyberDefender

Feel free to personalize the text before sharing.



Rating:



Difficulty:



Easy



Medium



Hard



Insane

BY Manuel Pérez

NK Maloweer