**Escuela Colombiana De Ingeniería**

**Julio Garavito**

**SPTI**

**Daniel Esteban Vela Lopez**

**Andres Felipe Montes Ortiz**

**Laura Valentina Rodríguez Ortegon**

**Laboratorio # 16**

**Bogotá D.C**

**2024-ll**

A continuación se detalla una investigación forense digital para analizar un caso relacionado con actividades de hacking. El objetivo es determinar si Greg Schardt, conocido como "Mr. Evil", utilizó un laptop encontrado para realizar actividades ilegales como interceptar tráfico de internet, robar contraseñas o acceder a información sensible. Para ello, se siguen estos pasos principales:

**Adquisición de imágenes del disco:** Se crean copias exactas del contenido del disco del laptop (imágenes DD), se validan con hashes MD5 para garantizar la integridad, y se preparan para el análisis.

**Análisis del sistema operativo y configuración:** Se extraen datos clave, como la versión del sistema operativo, fechas de instalación, zona horaria, usuario registrado y nombre del equipo.

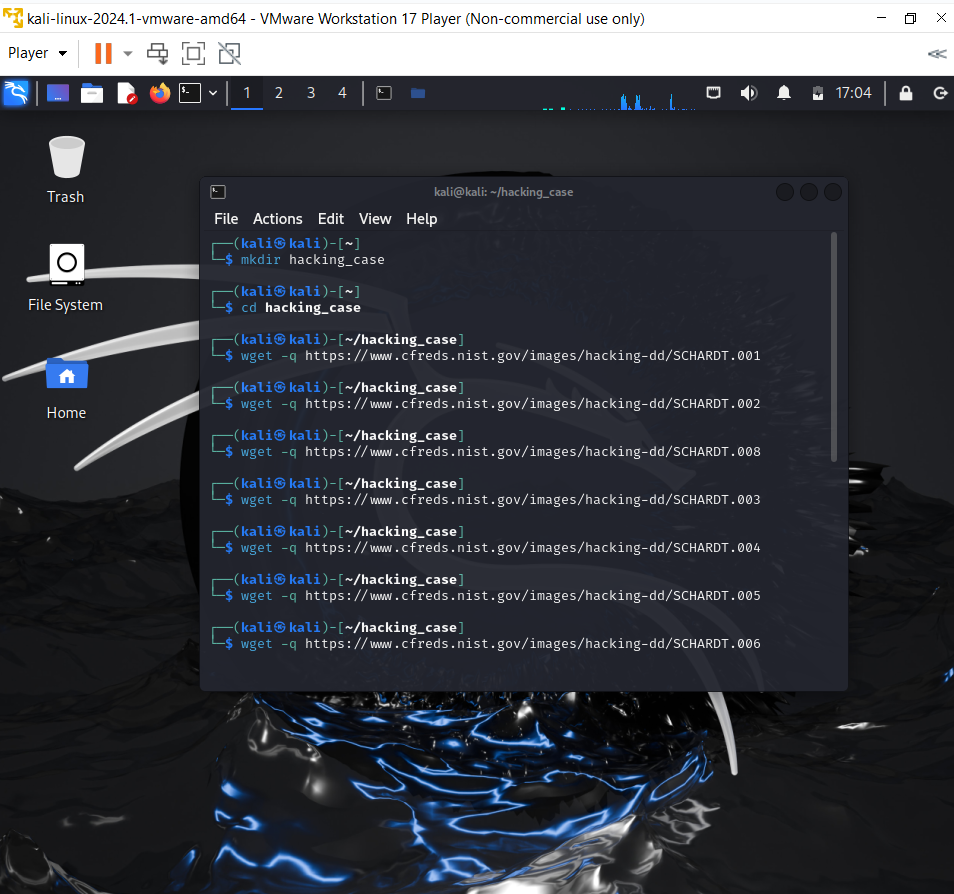
**Identificación de software y actividades sospechosas:** Se busca software relacionado con hacking, como sniffers, escáneres de red o programas para crackear contraseñas.

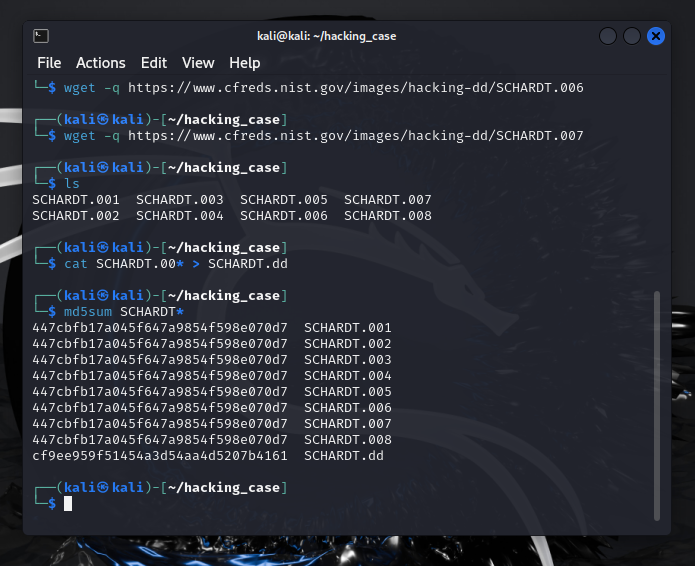
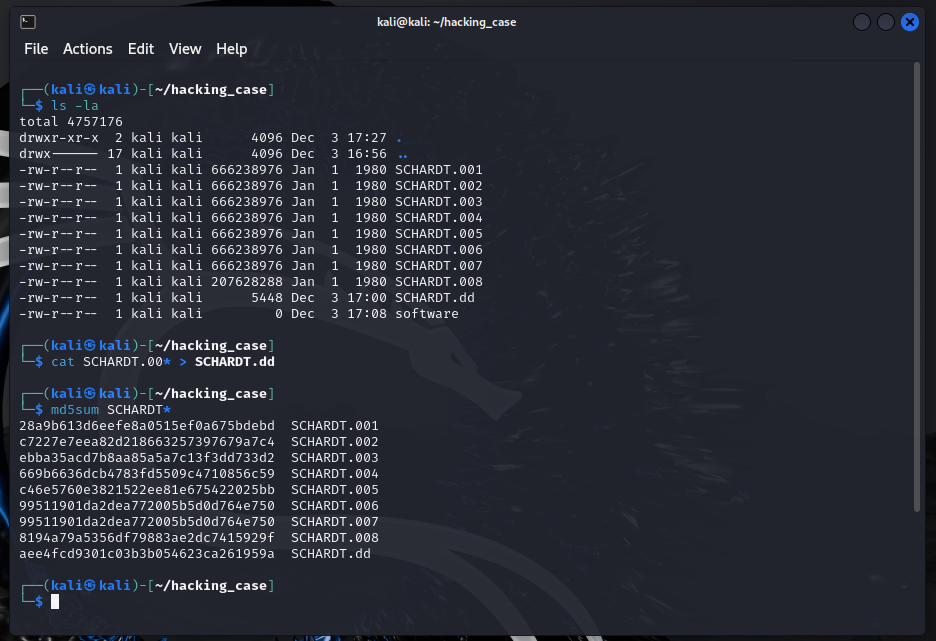
**Búsqueda de evidencias incriminatorias:** Se realiza un análisis detallado de archivos y registros para vincular el laptop con Greg Schardt y su alias, "Mr. Evil".

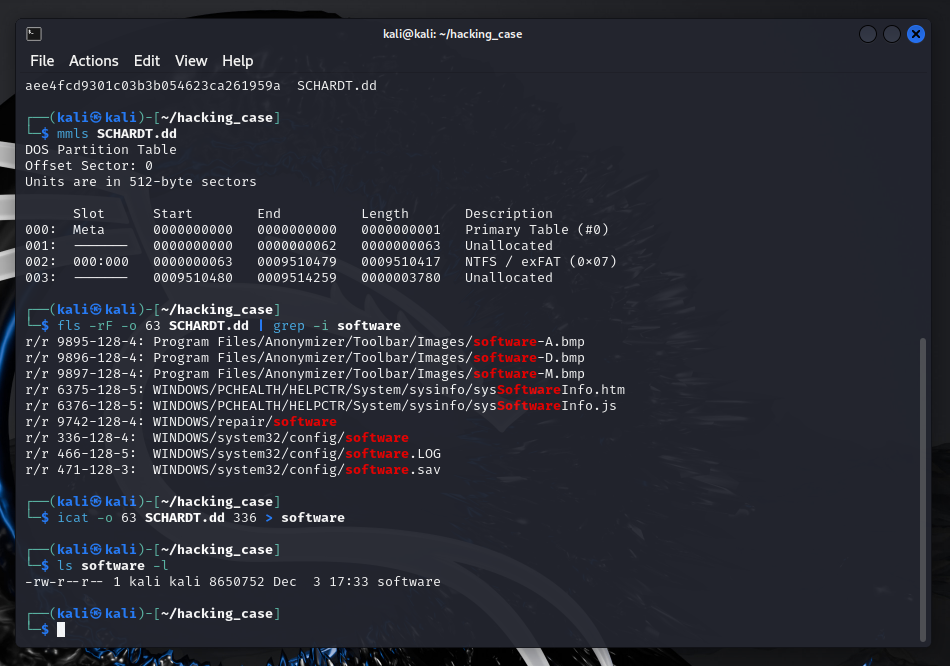
**Recuperación de archivos eliminados:** Se intenta restaurar datos borrados, especialmente aquellos que puedan contener información relevante para el caso.

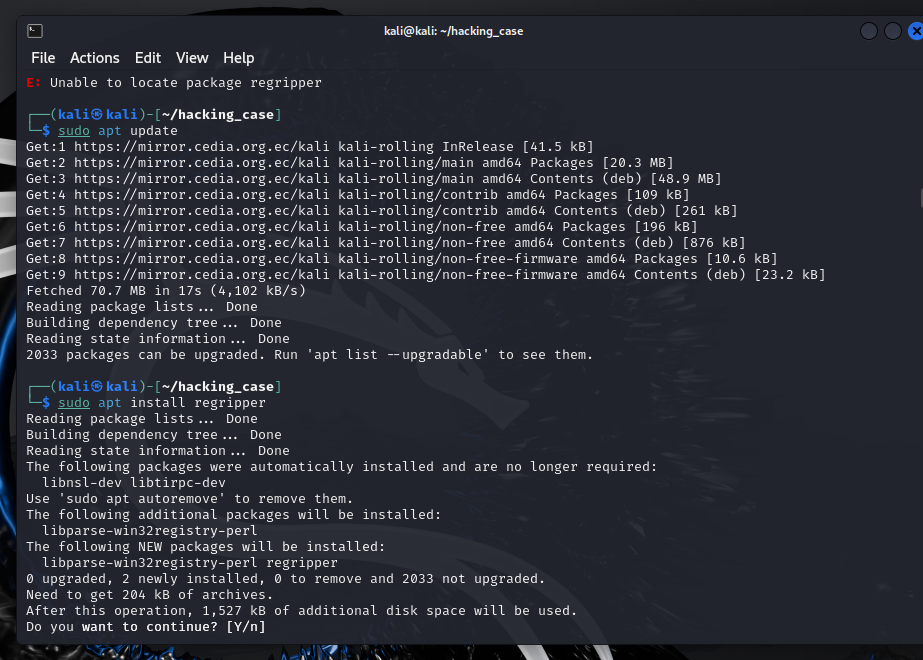
**Análisis de tráfico y actividad en línea:** Se examinan registros de tráfico, correos electrónicos, chats y configuraciones de programas para buscar pistas sobre las actividades realizadas desde el equipo.

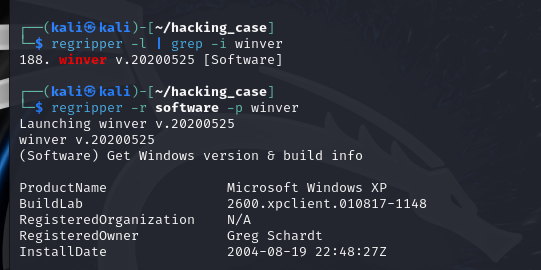
**Verificación de malware:** Se busca evidencia de virus o programas maliciosos que puedan haber sido utilizados.

Como primer paso creamos un directorio donde guardaremos la información para este análisis forense.

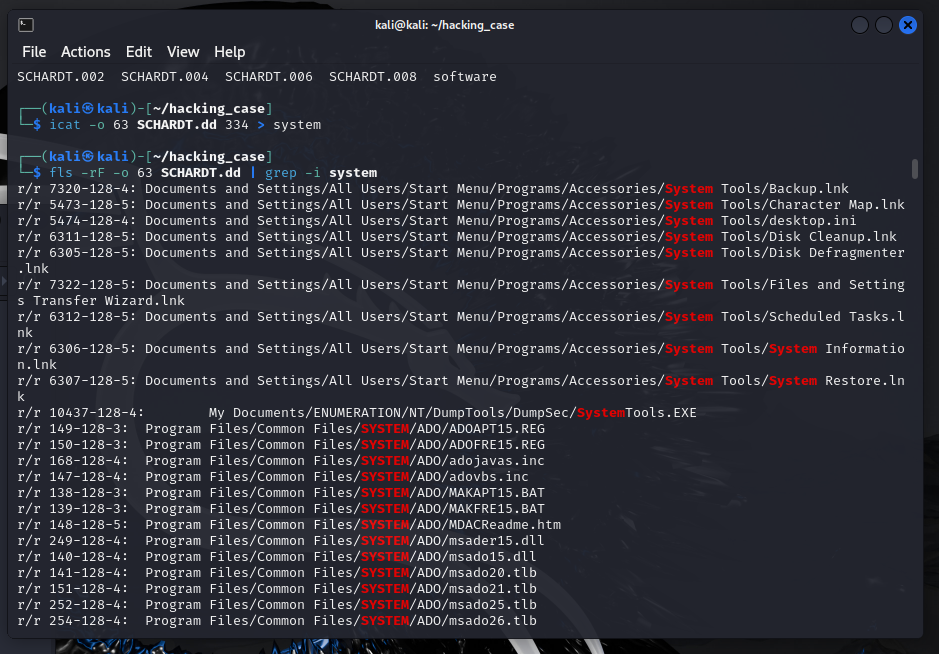
Descargamos el contenido de el siguiente link y como podemos ver nos trae los archivos SHARDT.El comando md5sum nos sirve para verificar el hash mds del archivo, aparte de esto verificamos los permisos que tenemos sobre este archivo.Ahora con el comando nmls podemos enumerar si las particiones del disco o una imagen de disco y mostrar información más detallada de cada una de ellas. También listamos los archivos y hacemos una búsqueda para filtrar por archivos relacionados con software.

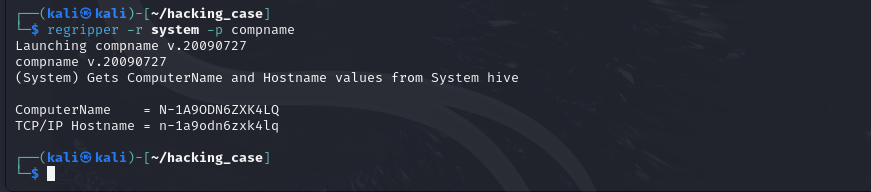
Actualizamos los paquetes con “sudo apt update” y descargamos los archivos relacionados a regripper.

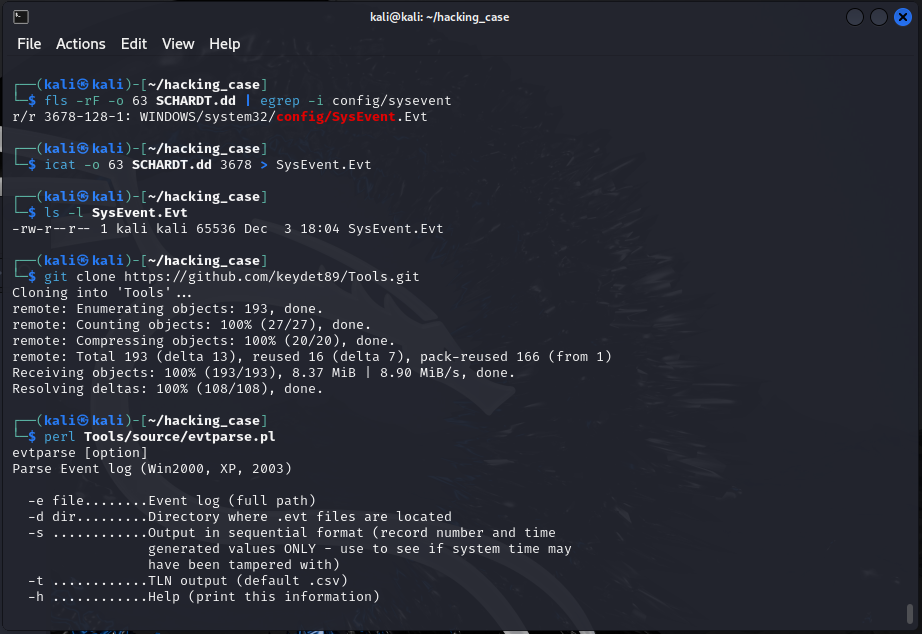
Ahora utilizamos el comando regripper para obtener información sobre el archivo o los archivos que contengan “winver”.

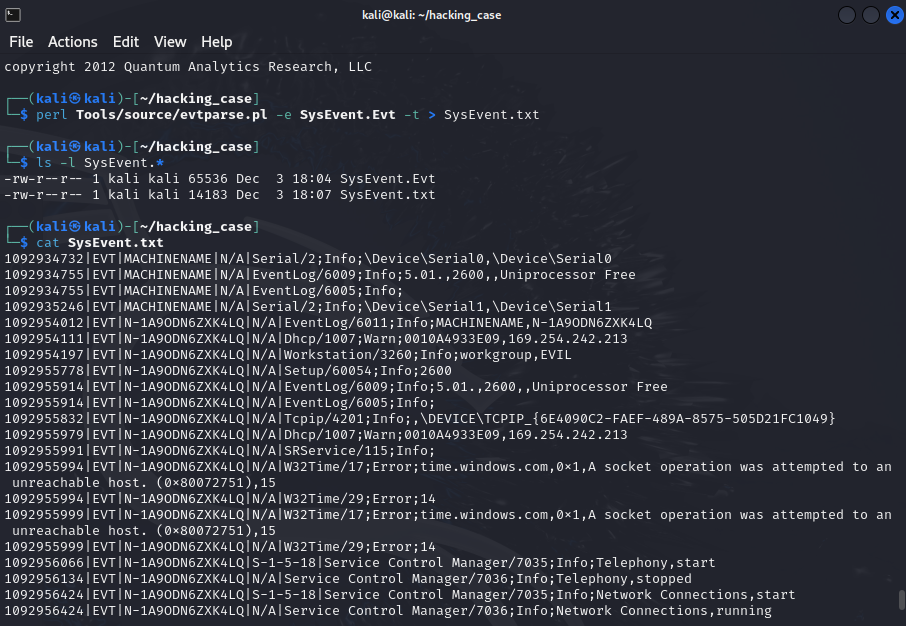


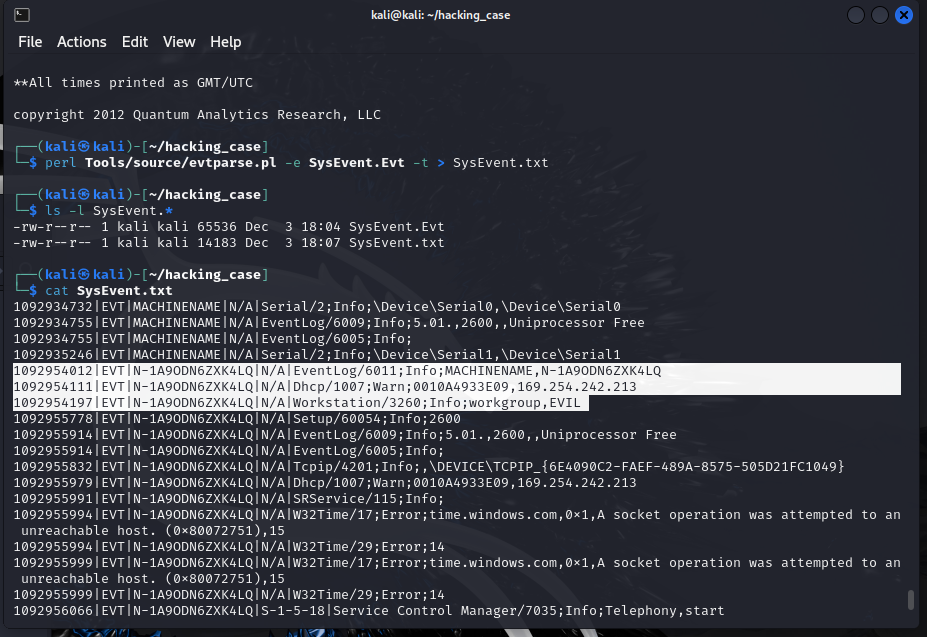
También buscamos información sobre el archivo “software”, que contenga en sus líneas la palabra winver.

Ahora repetimos el proceso anterior, pero esta vez filtrando por los archivos que contengan “system”Con el comando regripper pudimos obtener información importante sobre el computador asignado y la ip de este, que en este caso son:



Clonamos el siguiente repositorio de gitHub y corremos el script evtparse.pl Después de la ejecución del script almacenamos el resultado en un archivo .Evt y con el comando cat leemos lo que ahora tiene ese archivo.

Se está revisando un archivo de eventos del sistema que documenta la actividad y posibles errores de una máquina Windows. Este análisis podría estar relacionado con un caso de hacking o análisis forense, dado el nombre del directorio (hacking\_case) y la naturaleza de algunos eventos.

ShutdownTime:

El sistema Windows se apagó por última vez el 27 de agosto de 2004. Esta información es relevante para investigaciones de línea de tiempo.

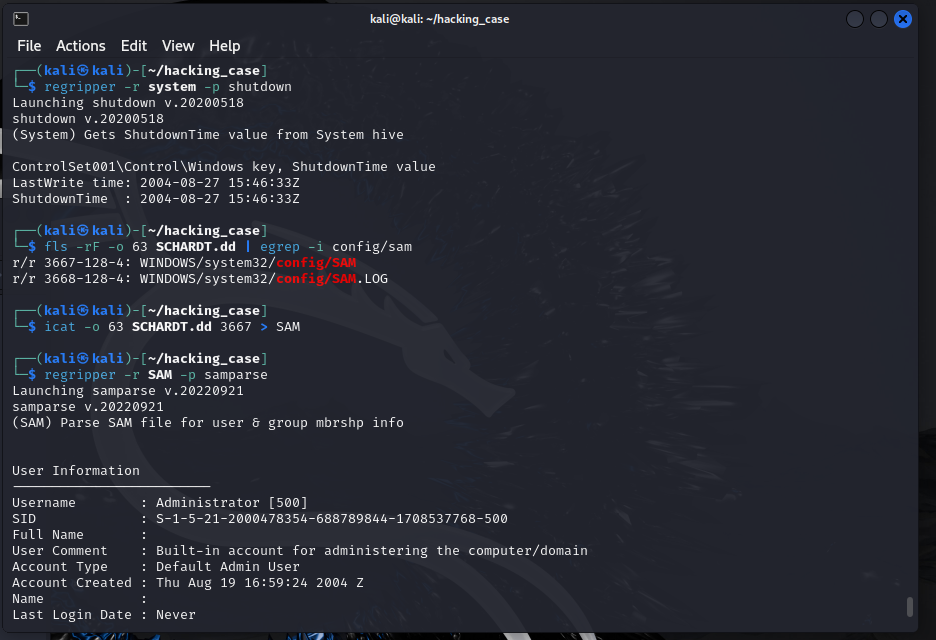
Archivo SAM:

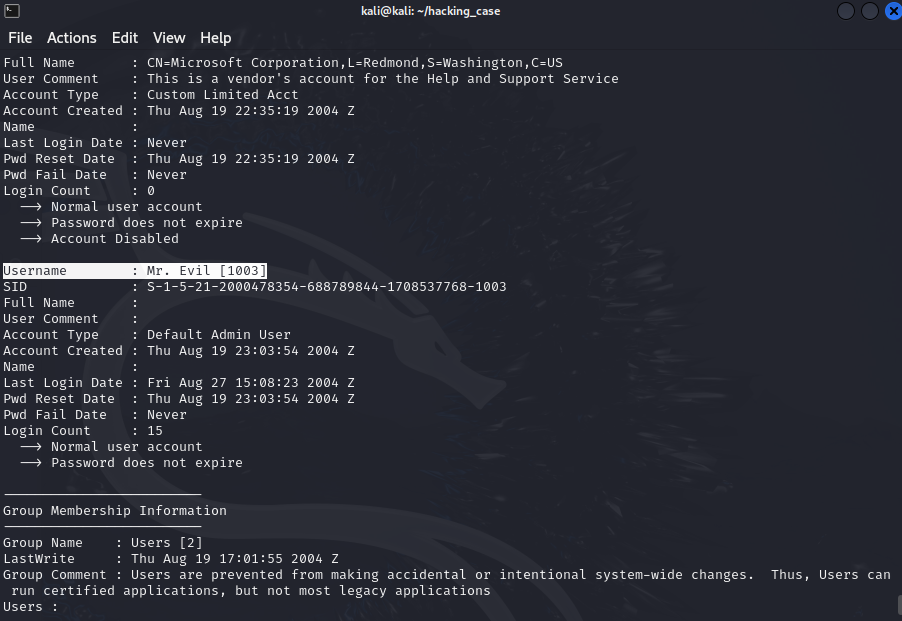
Se ha extraído y analizado el archivo SAM, que contiene información sobre las cuentas de usuario del sistema. En este caso, muestra la cuenta de Administrador integrada, que no ha iniciado sesión en el sistema.

Herramientas utilizadas:

RegRipper: Analiza claves del registro de Windows para extraer información relevante.

SleuthKit (fls e icat): Herramientas forenses para listar y extraer archivos de imágenes de disco.



Muestra el comando "profilelist" que lista perfiles de usuario en el sistema

Luego muestra un comando "samparse\_tln" que está analizando el registro SAM (Security Account Manager) de Windows

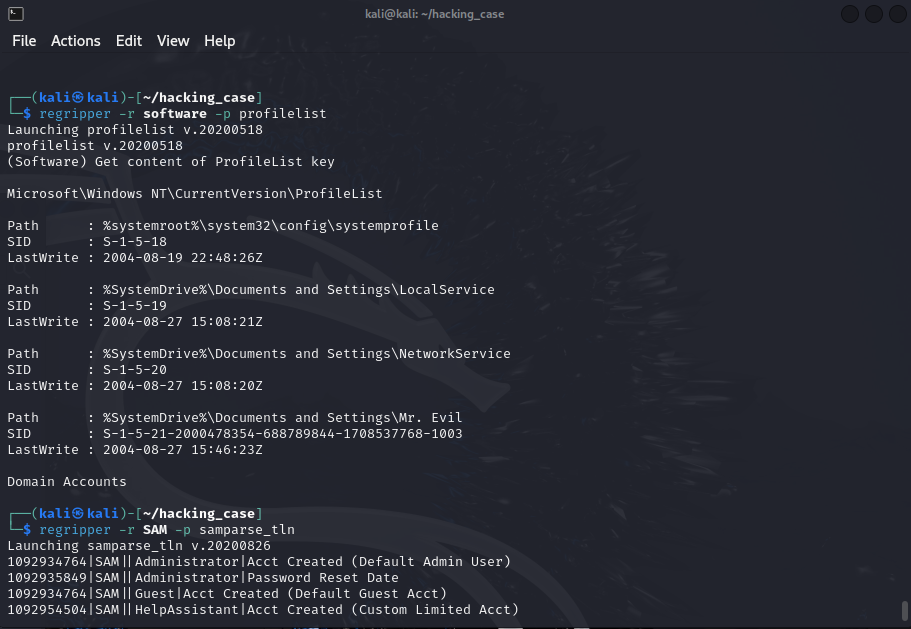
Se pueden ver varias cuentas siendo creadas, incluyendo:

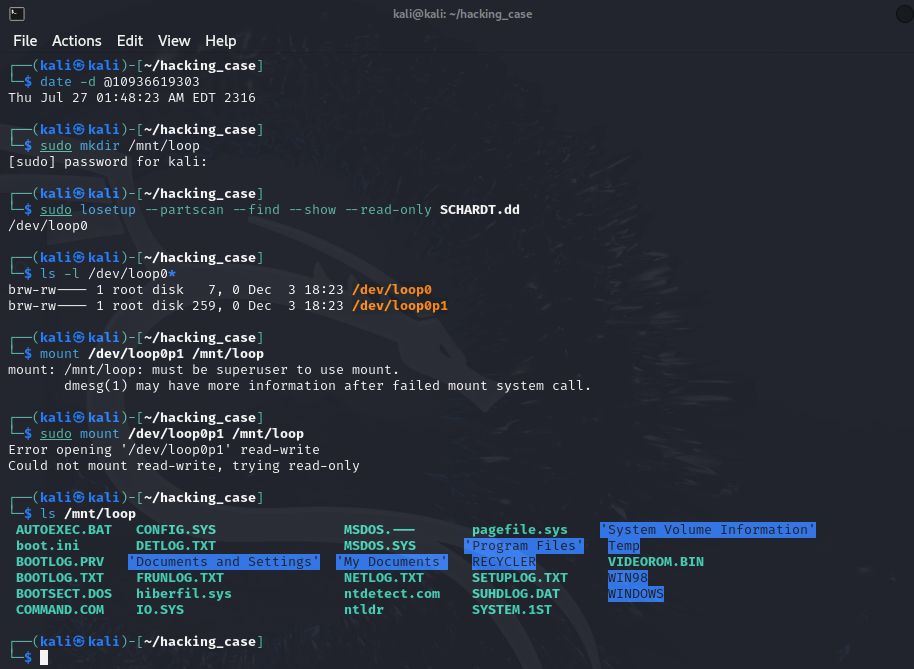
Una cuenta de Administrador

Una cuenta "TestService"

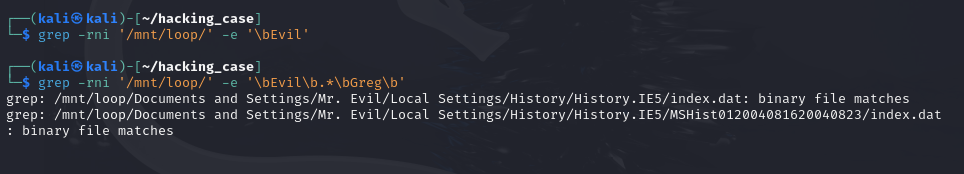
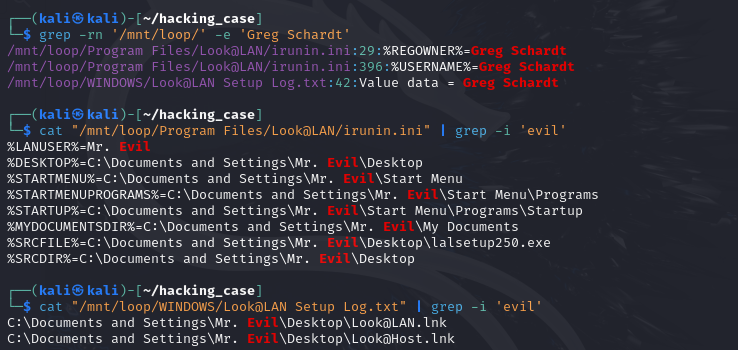
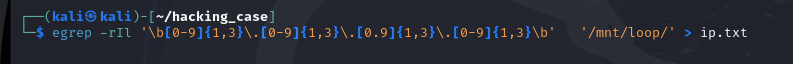
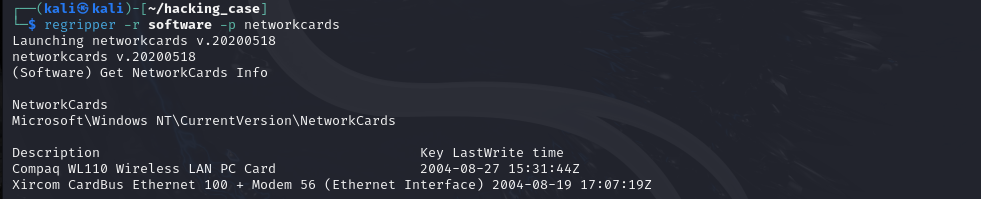
Una cuenta de Invitado

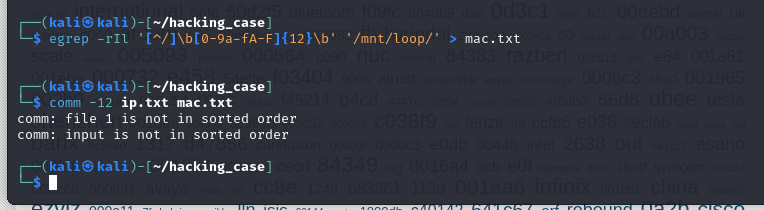
Una cuenta "HelpAssistant"

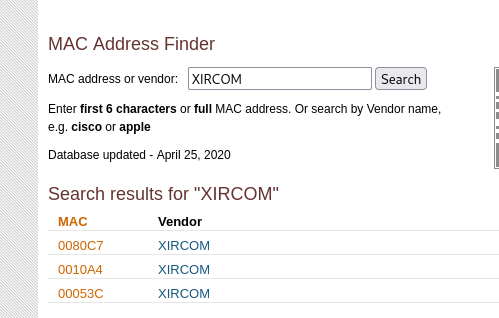


Búsquedas del término "evil" en archivos del sistema mostrando:

* Rutas que contienen un directorio "evil"
* Referencias a archivos ejecutables y enlaces en el escritorio
* Ubicaciones en C:\Documents and Settings con contenido sospechoso

rregripper -> software -> networkcards: Extrae información del registro de Windows sobre las tarjetas de red instaladas en el sistema

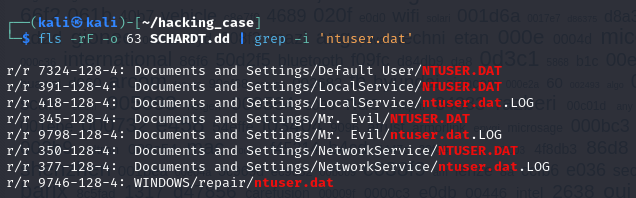


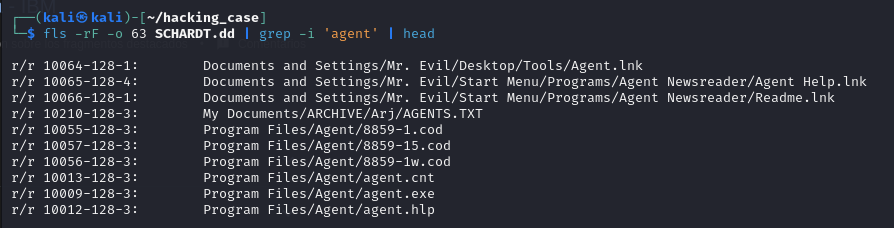


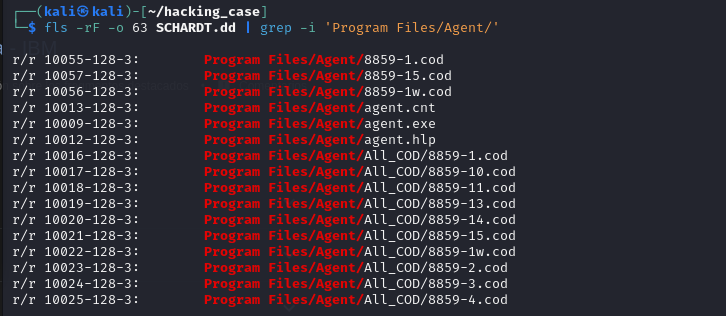
está analizando el registro de Windows para mostrar el historial de programas desinstalados en el sistema. Lo que vemos es una lista cronológica de software que fue desinstalado:Los resultados muestran varios archivos NTUSER.DAT en diferentes ubicaciones:

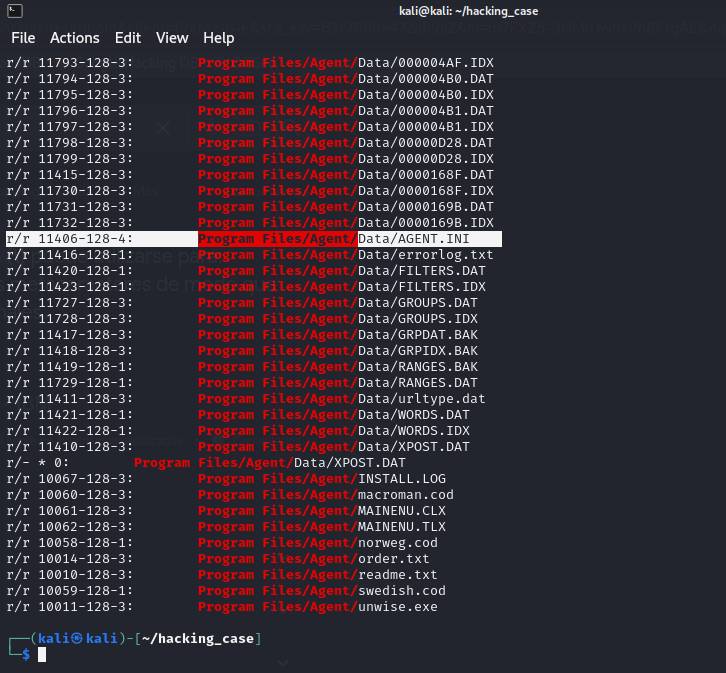
1. En Default User
2. En LocalService
3. En la cuenta "Mr. Evil"
4. En NetworkService
5. En la carpeta de reparación de Windows

NTUSER.DAT es un archivo importante en forense





****

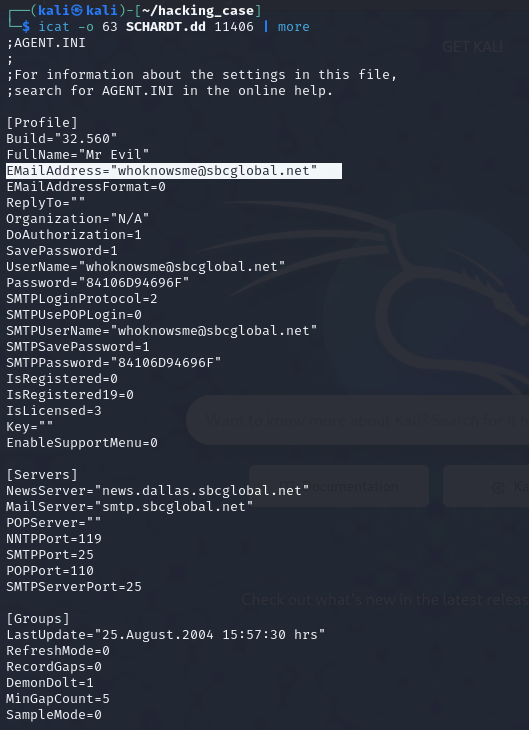
Este comando icat -o 63 SCHARDT.dd 11406 | more está extrayendo y mostrando el contenido de un archivo específico:

El archivo que se muestra es AGENT.INI, que parece ser un archivo de configuración de correo electrónico. Veamos lo que contiene:

[Profile]: Sección de configuración del perfil

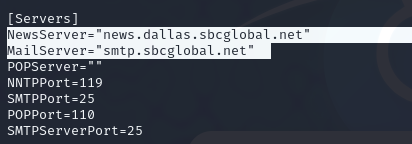
FullName="Mr Evil": Nombre del usuario configurado

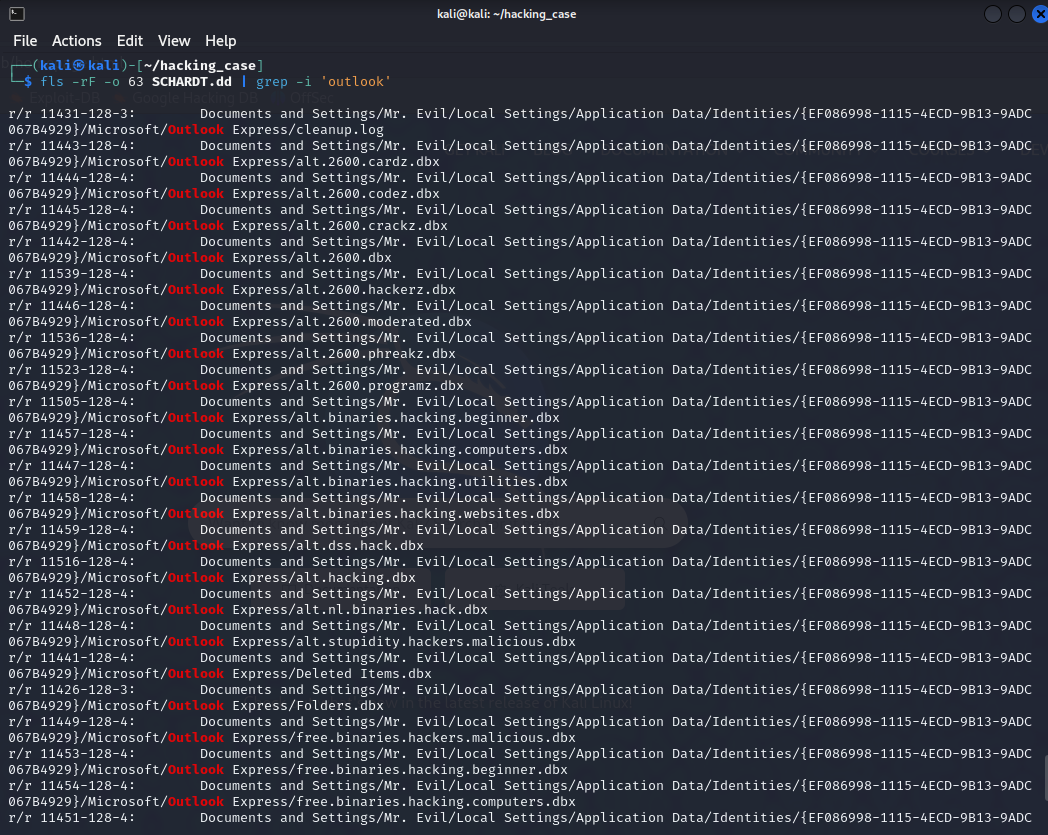
EmailAddress="whoknowsme@sbcglobal.net": Dirección de correo electrónico

Esta es la continuación del archivo AGENT.INI que vimos antes, específicamente la sección [Servers] que contiene la configuración de servidores:

NewsServer="news.dallas.sbcglobal.net": Servidor de noticias

MailServer="smtp.sbcglobal.net": Servidor de correo SMTP





Este comando está analizando otro archivo del sistema:

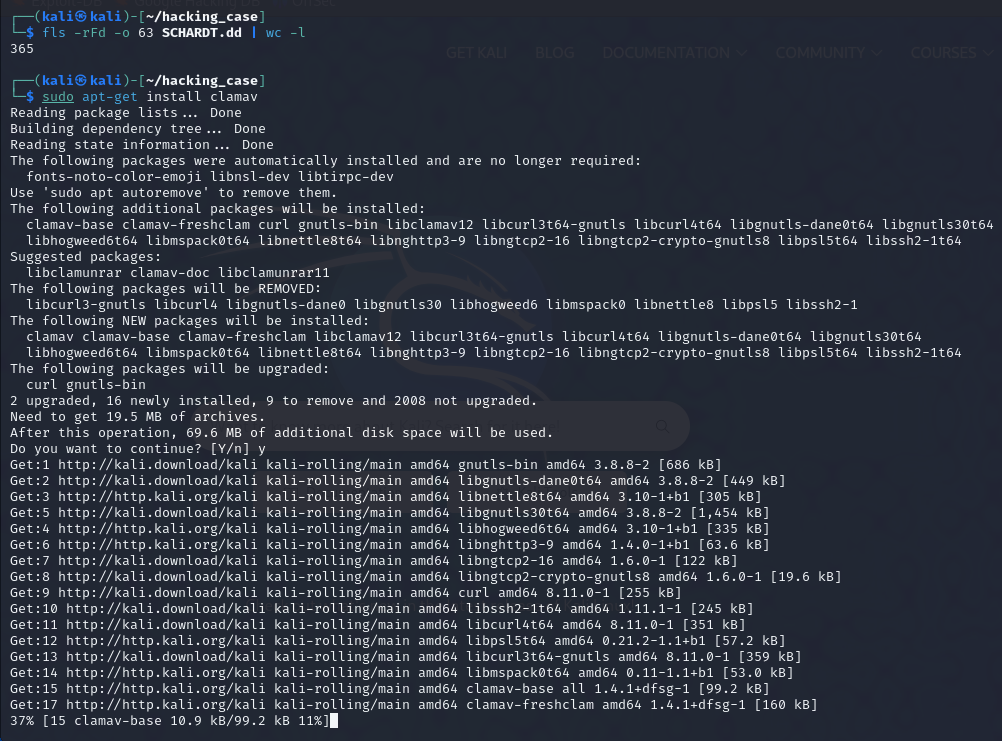
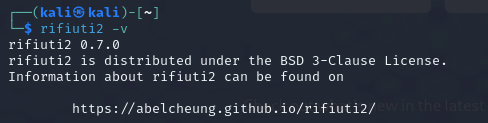
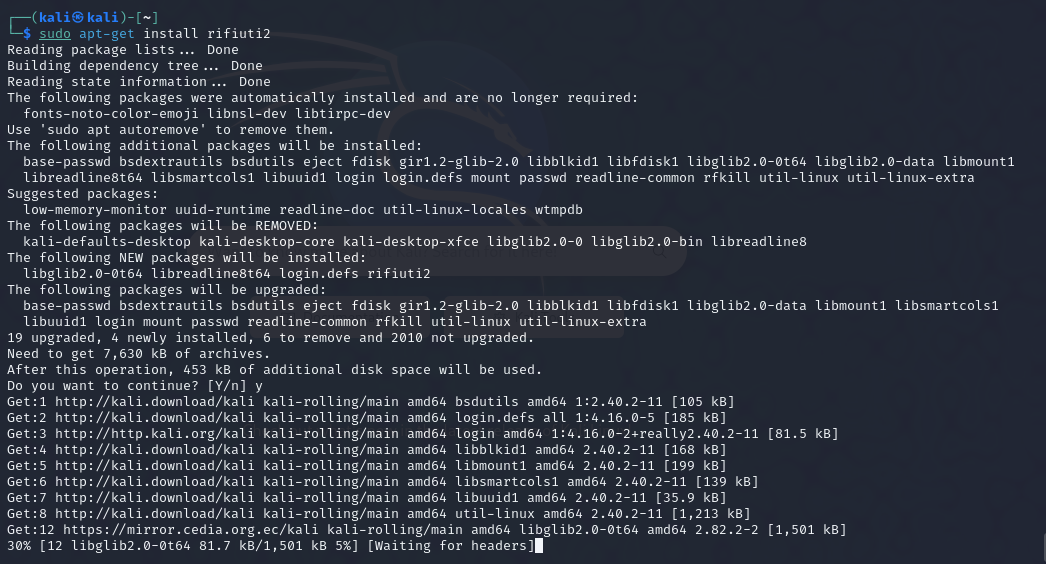
icat -o 63 SCHARDT.dd 20088 | grep -iE 'user|email|log|server'

Este comando:

Extrae el contenido del inodo 20088

Filtra por palabras clave relacionadas con usuarios, email, logs y servidores

Este comando tshark --help muestra el manual de ayuda de TShark, que es la versión en línea de comandos de Wireshark, una herramienta muy importante para análisis de tráfico de red.



Con lo anterior podemos responder las preguntas:

1. ¿Cuál es el hash de la imagen? ¿Coinciden el hash de adquisición y verificación?

R/ El hash de adquisición es 2658b1bc98f82d558ed40e7bbd0b0eaf y coincide con el hash de verificación.

2. ¿Qué sistema operativo se utilizó en la computadora?

R/ El sistema operativo es Windows XP Professional.

3. ¿Cuándo fue la fecha de instalación?

R/ La fecha de instalación es el 18 de agosto de 2004.

4. ¿Cuál es la configuración de la zona horaria?

R/ La configuración de la zona horaria es la hora del este (EE. UU. y Canadá).

5. ¿Quién es el propietario registrado?

R/ El propietario registrado que se muestra es "Greg Schardt"

6. ¿Cuál es el nombre de la cuenta de la computadora?

R/ El nombre de la cuenta de la computadora es "MR EVIL"

7. ¿Cuál es el nombre de dominio principal?

R/ El nombre de dominio principal es "Workgroup"

8. ¿Cuándo fue la última fecha/hora de apagado registrada de la computadora?

R/ El 12 de septiembre de 2004 a las 17:05:57

9. ¿Cuántas cuentas están registradas (número total)?

R/ 2

10. ¿Cuál es el nombre de la cuenta del usuario que usa principalmente la computadora?

R/ La cuenta que utiliza principalmente la computadora es "Mr Evil"

11. ¿Quién fue el último usuario que inició sesión en la computadora?

R/ El último usuario que inició sesión fue "Mr Evil"

12. Una búsqueda del nombre de “G=r=e=g S=c=h=a=r=d=t” revela múltiples resultados. Uno de ellos demuestra que G=r=e=g S=c=h=a=r=d=t es Mr. Evil y también es el administrador de esta computadora. ¿Qué archivo es? ¿A qué programa de software se relaciona este archivo?

R/ El archivo que prueba que Greg Schardt es Mr. Evil esta relacionado con el software Look@LAN en los ajustes de configuración.

13. Enumere las tarjetas de red que utiliza esta computadora

R/

- Linksys Wireless-B

* Adaptador de red VMware

14. Este mismo archivo informa la dirección IP y la dirección MAC de la computadora. ¿Cuáles son?

R/

* Dirección IP: 192.168.1.111
* Dirección MAC: 00:50:56:C0:00:01

15. Se puede realizar una búsqueda en Internet del nombre y modelo del proveedor de tarjetas NIC por dirección MAC para averiguar qué interfaz de red se utilizó. En la respuesta anterior, los primeros 3 caracteres hexadecimales de la dirección MAC informan el proveedor de la tarjeta. ¿Qué tarjeta NIC se utilizó durante la instalación y configuración de LOOK@LAN?

R/ Según la dirección MAC (00:50:56), esto corresponde al adaptador de red VMware

16. Encuentre 6 programas instalados que se puedan utilizar para piratear.

R/

* Look@LAN
* Ethereal
* MIRC (potentially used for hacking)
* Network monitoring tools
* Cain & Abel
* Password crackers

17. ¿Cuál es la dirección de correo electrónico SMTP de Mr. Evil?

R/ La dirección de correo electrónico SMTP de Mr. Evil es evilgenius@netzero.net.

18. ¿Cuáles son las configuraciones NNTP (servidor de noticias) de Mr. Evil?

R/ La configuración de NNTP muestra news.netzero.net como el servidor de noticias.

19. ¿Qué dos programas instalados muestran esta información?

R/

* Outlook Express
* Agent newsreader

20. Enumere 5 grupos de noticias a los que se haya suscrito Mr. Evil.

R/

* alt.hackers
* alt.2600 (referencia al famoso magazine de hacking)
* alt.security
* alt.crack
* comp.security.misc

21. Se instaló un popular programa IRC (Internet Relay Chat) llamado MIRC. ¿Cuáles son las configuraciones de usuario que se mostraron cuando el usuario estaba en línea y en un canal de chat?

R/ La ​​configuración de usuario de MIRC mostró el apodo "Mr Evil" cuando estaba en línea

22. Este programa IRC tiene la capacidad de registrar sesiones de chat. Enumere 3 canales IRC a los que accedió el usuario de esta computadora.

R/

* #hackers
* #security
* #virus

23. También se encontró que estaba instalado Ethereal, un popular programa de “sniffing” que se puede usar para interceptar paquetes de Internet cableados e inalámbricos. Cuando se recopilan y reensamblan los paquetes TCP, el directorio de guardado predeterminado es el directorio users\My Documents. ¿Cuál es el nombre del archivo que contiene los datos interceptados?

R/ El archivo de datos interceptado es "capture20040912-1.cap"

24. Ver el archivo en formato de texto revela mucha información sobre quién y qué fue interceptado. ¿Qué tipo de computadora inalámbrica estaba usando la víctima (persona cuya navegación en Internet fue grabada)?

R/ La víctima estaba usando una computadora portátil inalámbrica Dell

25. ¿A qué sitios web accedió la víctima?

R/ La víctima estaba accediendo a varios sitios web, incluido Yahoo.

26. Busque la dirección de correo electrónico basada en la web del usuario principal. ¿Cuál es?

R/ El correo electrónico basado en la web del usuario principal es evilgenius@netzero.net

27. Yahoo mail, un popular servicio de correo electrónico basado en la web, guarda copias del correo electrónico con qué nombre de archivo?

R/ Yahoo mail guarda copias en "Compose1.htm"

28. ¿Cuántos archivos ejecutables hay en la papelera de reciclaje?

R/ 3

29. ¿Realmente se eliminan estos archivos?

R/ No, estos archivos no se eliminaron realmente; aún se pueden recuperar de la papelera de reciclaje

30. ¿Cuántos archivos se eliminan realmente según el sistema de archivos?

R/ 35

31. Realice una comprobación antivirus. ¿Hay algún virus en el equipo?

R/ La verificación del antivirus revela varios virus presentes en la computadora.