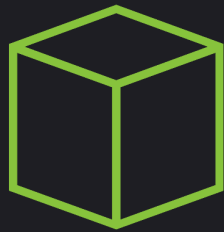


# Hack The Box - Sherlocks - Defensive Security



**Hack The Box**  
PEN-TESTING LABS

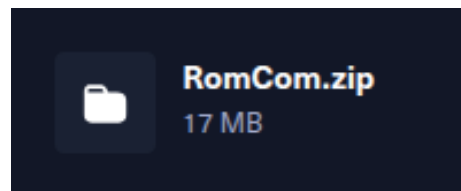


**RomCom**

Very Easy

Este sherlock es de dificultad muy fácil, ya que trataremos con un sistema que fue víctima de un exploit en la aplicación de Winrar.

Podemos empezar descargando el archivo comprimido en Kali:



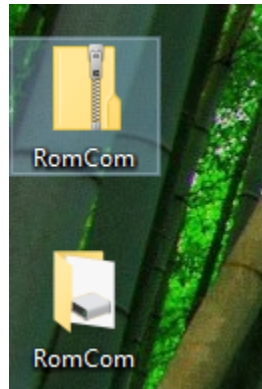
Una vez lo tengamos descargado, lo descomprimos para ver qué contiene.

Parece ser que es un archivo con extensión '**vhdx**'. Este tipo de archivos funcionan como discos duros virtuales que actúan como discos duros físicos, almacenan información que puede ser un sistema operativo completo, aplicaciones, registros del sistema, etc.

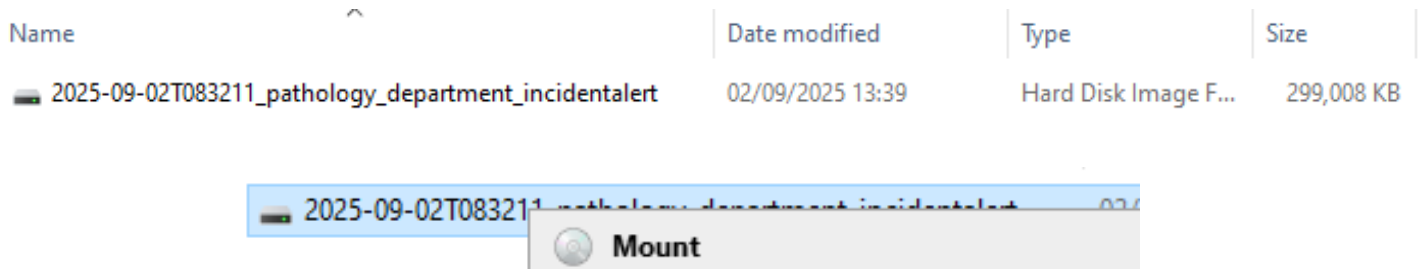
```
(d4rkonus@kali)-[~/Desktop]
$ ls
2025-09-02T083211_pathology_department_incidentalalert.vhdx
```

Este tipo de archivos funcionan en sistemas operativos Windows de forma nativa, aunque hay comandos en Linux que pueden funcionar también.

En este caso, nos creamos una máquina virtual de Windows para proseguir con la resolución, y hacemos lo mismo con el archivo comprimido, es decir, lo descargamos y lo descomprimimos.



Para montar la unidad, tenemos que seleccionarla y con el click derecho en 'Montar':



En este punto, vamos a empezar a responder las preguntas para resolver el sherlock, la primera es esta:

Task 1

What is the CVE assigned to the WinRAR vulnerability exploited by the RomCom threat group in 2025?

CVE-\*\*\*\*-\*\*\*\*

Solo hay que buscar esto en Internet para conseguir la respuesta correcta '*winrar romcom cve*'.

What is the CVE assigned to the WinRAR vulnerability exploited by the RomCom threat group in 2025?

CVE-2025-8088


Después tenemos la siguiente pregunta, la cual se trata de decir la naturaleza de la vulnerabilidad, es decir, que tipo de vulnerabilidad se trata:

What is the nature of this vulnerability?

\*\*\*\* \*

Responder esto es simple, basta con buscar el CVE en Internet y al mismo tiempo veremos la respuesta:

CVE-2025-8088

**CVE-2025-8088** is a high-severity, actively exploited **path traversal vulnerability** in the Windows versions of the WinRAR archive management tool (and related UnRAR components) that allows attackers to execute arbitrary code. 

What is the nature of this vulnerability?

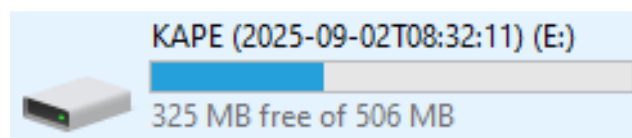
Path Traversal

La siguiente pregunta trata de encontrar el nombre de un archivo comprimido dentro de la carpeta de Documentos de un usuario llamado Susan, dicho archivo ejecuta la vulnerabilidad al abrir el archivo comprimido.

Task 3

What is the name of the archive file under Susan's documents folder that exploits the vulnerability upon opening the archive file?

Para encontrar el archivo tenemos que dirigirnos a la montura que tenemos en Windows:



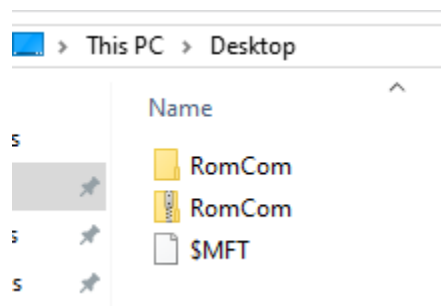
Debemos buscar dentro de la montura hasta encontrar este archivo:



Este archivo '*MFT*' se le conoce también como '*Master File Table*', es una base de datos maestra interna de Windows, tienen la función de guardar toda la información que se conoce sobre los archivos que tiene Windows, desde fechas de creación hasta los permisos que tienen.

Lo malo de este archivo es que no se puede leer directamente porque Windows no lo permite, aunque podemos volcar el contenido que tenga este archivo a un archivo tipo '.csv'.

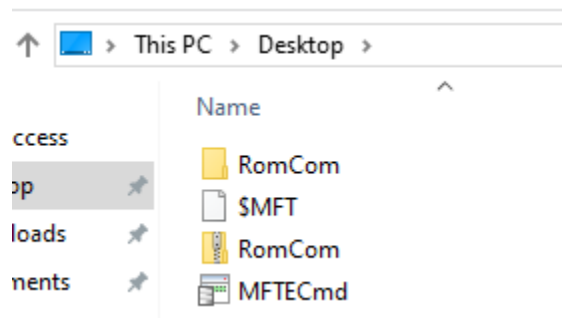
Para ello primero, movemos este archivo al escritorio:



Despues no dirigimos a este repositorio de GitHub, donde encontraremos una herramienta que nos permitirá hacer el volcado de datos:



Y al igual que con la MFT, movemos este nuevo archivo al escritorio:



Para hacer el volcado de datos, abrimos una powershell y ejecutamos este comando:

```
PS C:\Users\d4rkonus\Desktop> .\MFTECmd.exe -f '.\$MFT' --csv C:\Users\d4rkonus\Desktop\
```

Cuando termine la ejecución, tendremos este resultado:

```
FILE records found: 139,533 (Free records: 0) File size: 136.5MB  
CSV output will be saved to C:\Users\d4rkonus\Desktop\20251015091752_MFTECmd_$MFT_Output.csv
```

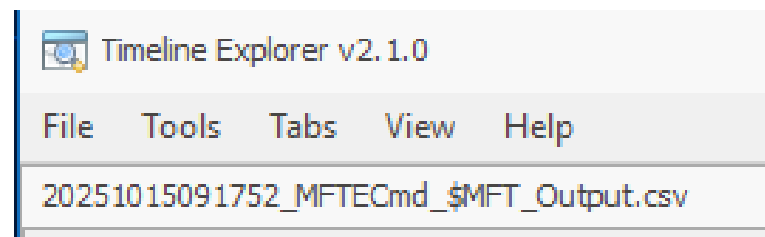
Ya tenemos los datos en el archivo 'csv', para poder leerlo, nos descargamos otra herramienta del mismo repositorio que antes:

```
ericzimmerman.github.io
```

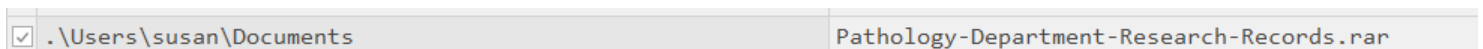
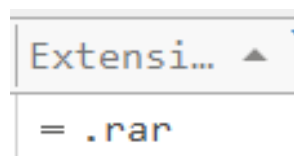
Timeline Explorer

- | [2.0.0.1](#) | [2.1.0](#)

Ahora es tan sencillo como instalar el programa y abrir el archivo '.csv' con dicho programa:



Para encontrar el archivo, la propia pregunta nos ofrece una pista, filtrar por la extensión '*.rar*' y que se encuentre dentro de '*Documentos*':





La siguiente pregunta que se nos presenta es:

When was the archive file created on the disk?

YYYY-MM-DD hh:mm:ss

En este caso, la respuesta es simple de encontrar, en la propia tabla donde encontramos el nombre del archivo, encontraremos la fecha.

Created0x10

2025-09-02 08:13:50

La siguiente pregunta que se nos presenta es:

When was the archive file opened?

YYYY-MM-DD hh:mm:ss

En este caso, la respuesta es la siguiente:

Last Record Change0x10

2025-09-02 08:14:04

Al parecer hay un archivo que parece ser legítimo, pero que resulta ser falso y tiene la función de distraer al usuario, porque la siguiente pregunta trata de encontrar este mismo archivo:

What is the name of the decoy document extracted from the archive file, meant to appear legitimate and distract the user?

filename without path

Para encontrarlo, simple, nos dirigimos a esta barra de búsqueda de la esquina superior derecha, y filtramos por *'susan\Documents'*:

. \Users\ <b>susan\Documents</b>	Genotyping_Results_B57_Positive.pdf	.pdf
. \Users\ <b>susan\Documents</b>	Pathology-Department-Research-Records.rar	.rar

Podemos ver que hay un archivo PDF junto al .rar, este PDF es el archivo que buscábamos y la respuesta a la pregunta anterior.

Parece ser que el atacante dejó un archivo de backdoor en caso de que quisiera volver a atacar, ya que la siguiente pregunta trata de encontrar este archivo:

Task 7

What is the name and path of the actual backdoor executable dropped by the archive file?

full path of file, starting with drive letter

Estuve analizando el archivo de la 'MFT' y no encontré nada para poder responder, decidí investigar con detalle la montura para ver si podría encontrar algo de información útil.

Encontré este archivo que a primera vista parece igual que la 'MFT' por el formato del nombre del archivo:

> This PC > KAPE (2025-09-02T08:32:11) (E:) > C > \$Extend		
Name		Date modified
SJ		01/09/2025 21:10

Para volcar los datos de este archivo a un archivo '.csv', ejecutamos este comando:

```
PS C:\Users\d4rkonus\Desktop> .\MFTECmd.exe -f '.\SJ' --csv C:\Users\d4rkonus\Desktop\
```



Tras la ejecución del comando, tenemos este archivo donde encontraremos los datos requeridos:

 20251015095047\_MFTECmd\_\$J\_Output.csv

Usamos el programa usado anteriormente para analizar este archivo, y filtramos por extensión de archivo **‘.exe’**:

187531	<input type="checkbox"/>	2025-09-02 08:14:28	ApbxHelper.exe
187530	<input type="checkbox"/>	2025-09-02 08:14:28	ApbxHelper.exe
187504	<input type="checkbox"/>	2025-09-02 08:14:18	ApbxHelper.exe

Encontramos este archivo ejecutable y es la respuesta a la pregunta, lo único que hay que añadir la ruta completa:

Parent Path	File Name
	
.\Users\susan\AppData\Local	ApbxHelper.exe

Además el exploit también dejó un archivo de persistencia en el equipo para que el atacante pueda seguir teniendo acceso al sistema:

The exploit also drops a file to facilitate the persistence and execution of the backdoor. What is the path and name of this file?

full path of file, starting with drive letter

Por algún motivo no encontré nada en el segundo archivo '.csv', así que decidí volver al primero, y tras analizarlo, encontré esto:

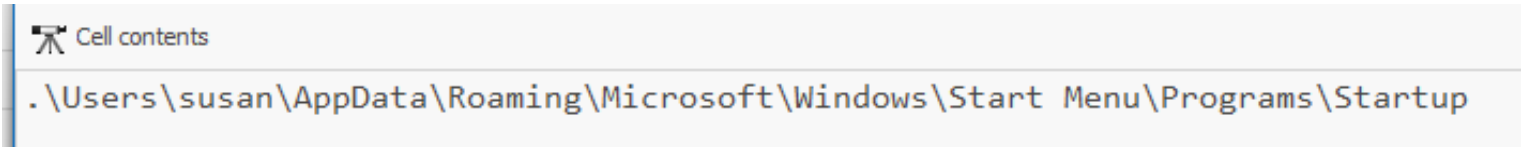


Display Settings.lnk

Encontré este archivo ya que tiene una fecha de creación similar a la de los anteriores archivos, ya que se creó de forma simultánea

Los archivos con este tipo de extensión suelen ser usados por los atacantes para apuntar a un programa ejecutable malicioso usando el propio '.lnk', este tipo de archivos se suelen incluir en la carpeta 'Startup' de Windows para que se inicie automáticamente cuando el usuario inicie sesión.

De hecho la ruta absoluta de este archivo es la siguiente:

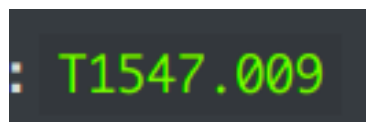


Cell contents

.\Users\susan\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

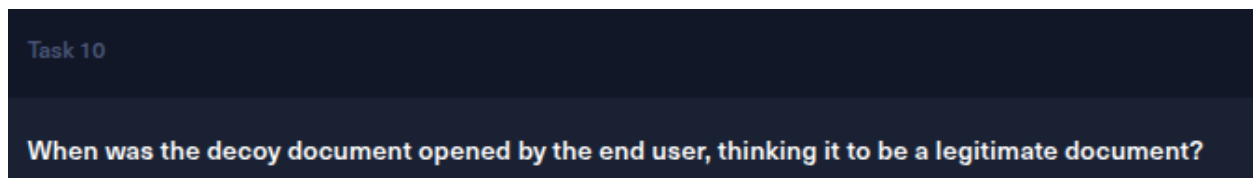
La siguiente pregunta trata de encontrar el ID de técnica que identifica a este tipo de ataque, es decir, *AutoStart/Boot Logon*, que sucede cuando los programas se inician automáticamente una vez el sistema arranca y/o el usuario inicia sesión en el sistema.

En este caso el ID es el siguiente:



```
: T1547.009
```

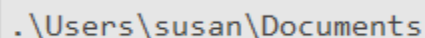
Y para finalizar, la última pregunta que trata de saber cuando fue abierto el documento señuelo por el usuario:



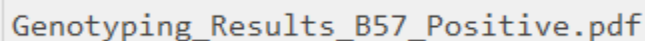
Task 10

When was the decoy document opened by the end user, thinking it to be a legitimate document?

Para esto, nos movemos hacia el archivo señuelo y observamos cuando fue abierto por última vez:



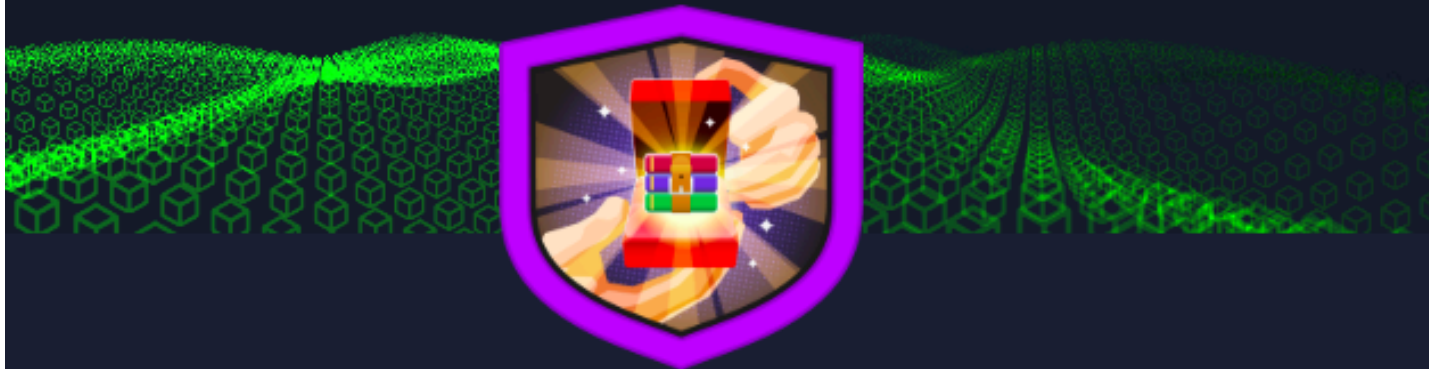
```
.\Users\susan\Documents
```




```
Genotyping_Results_B57_Positive.pdf
```



```
2025-09-02 08:15:05
```



## RomCom has been Solved!

Congratulations  **d4rkonus**, best of luck in capturing flags ahead!

<b>#730</b>	<b>15 Oct 2025</b>	<b>RETIRED</b>
SHERLOCK RANK	SOLVE DATE	SHERLOCK STATE

OK

SHARE