CAP - Writeup HTB

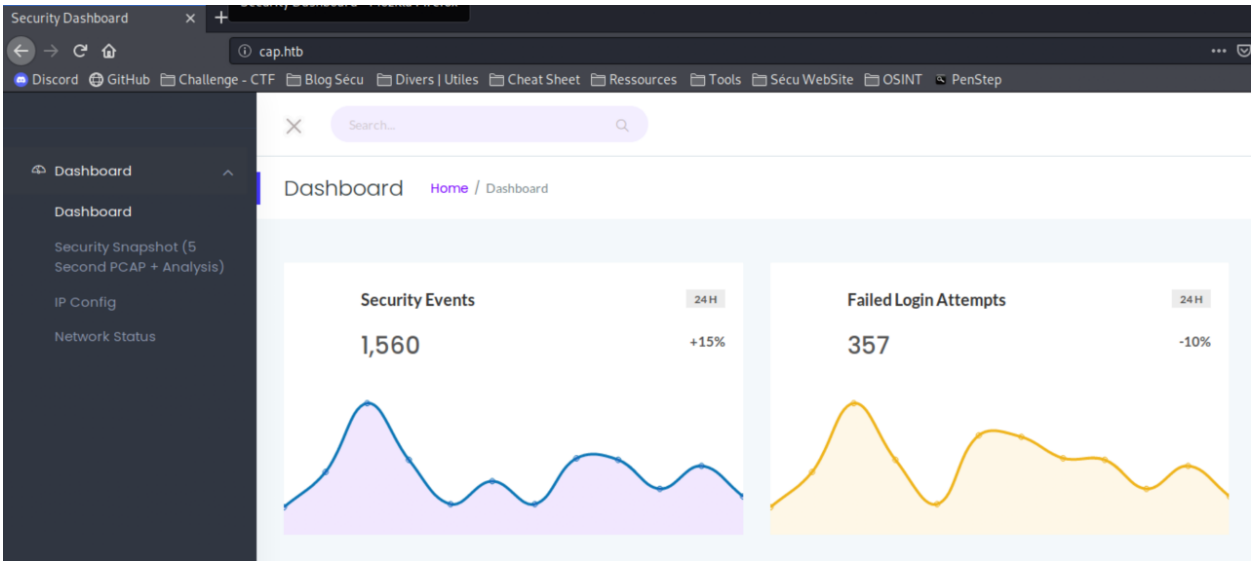
Author : PierreAD

I) Enumeration :

```
nmap -sV -A -O cap.htb
```

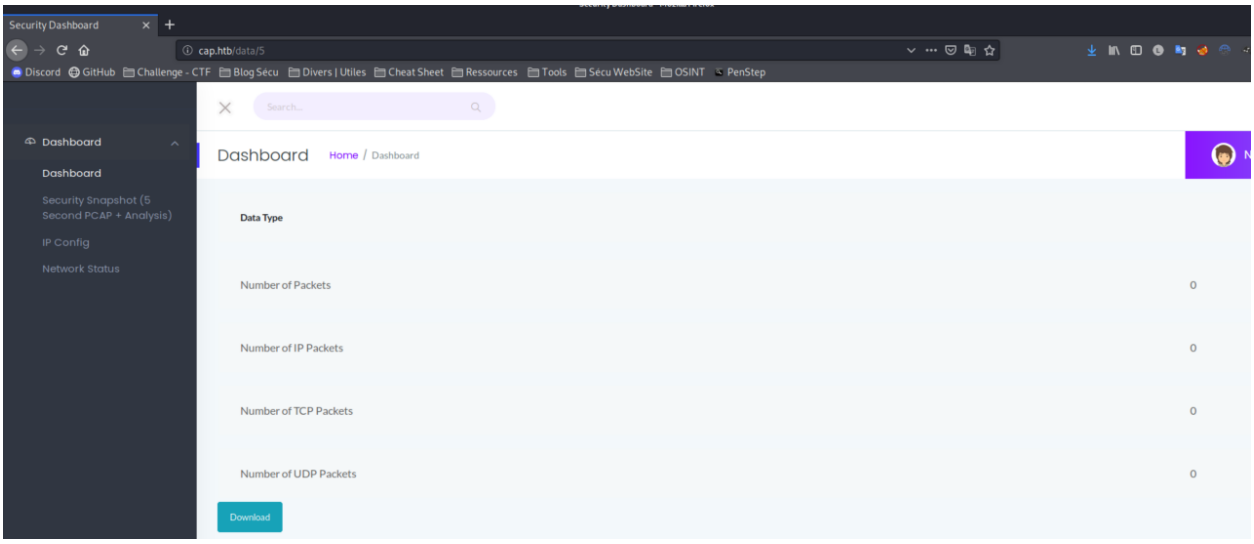
> Nothing interesting with nmap enumeration

```
firefox http://cap.htb
```



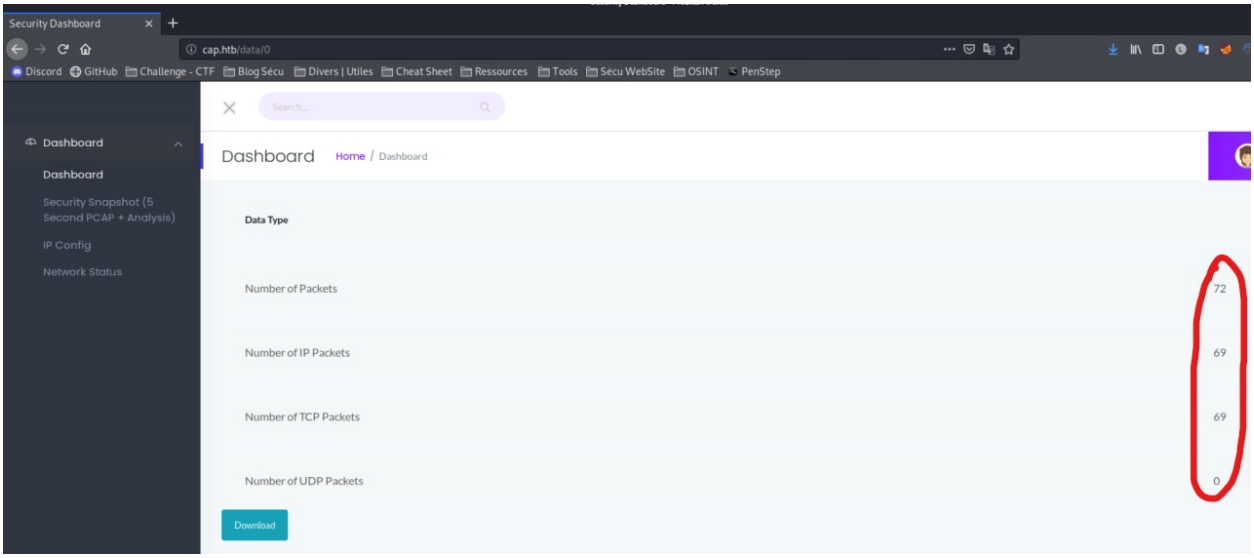
> Web server offers possibility to have network capture (open by wireshark)

```
firefox http://cap.htb/data/5
```

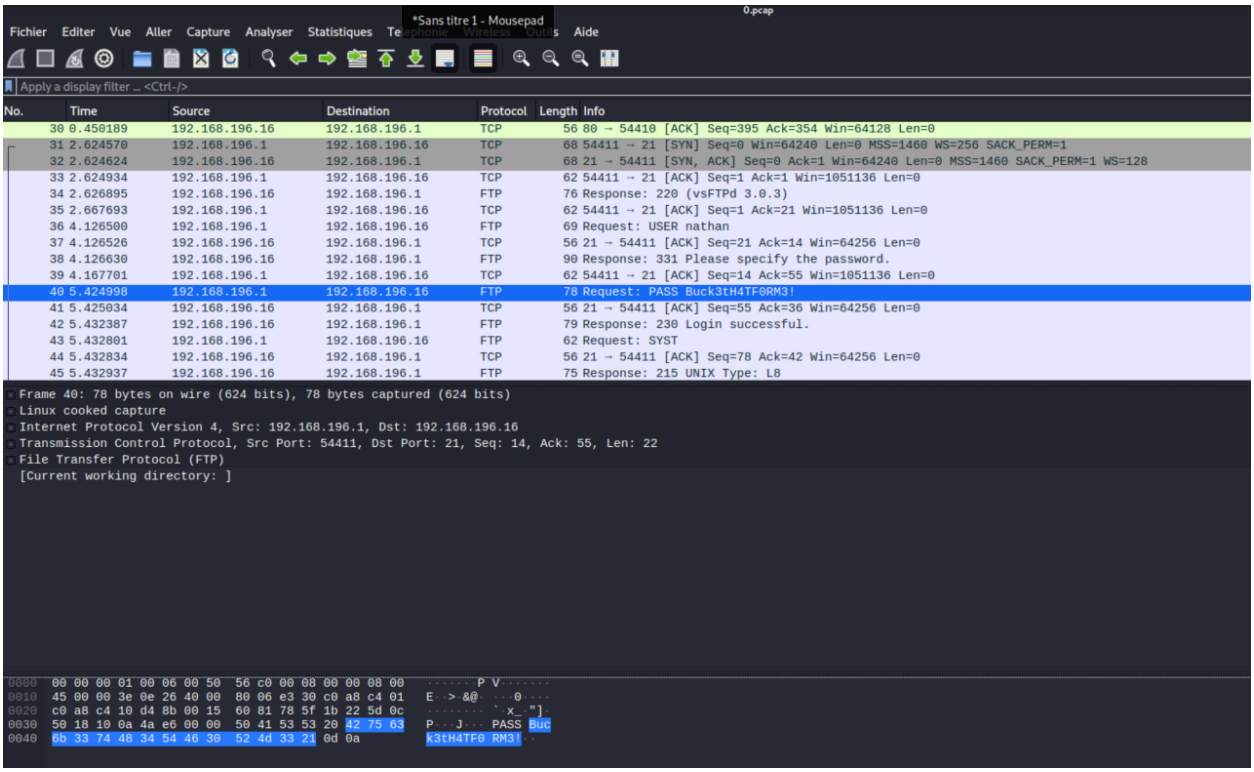


II) Exploitation :

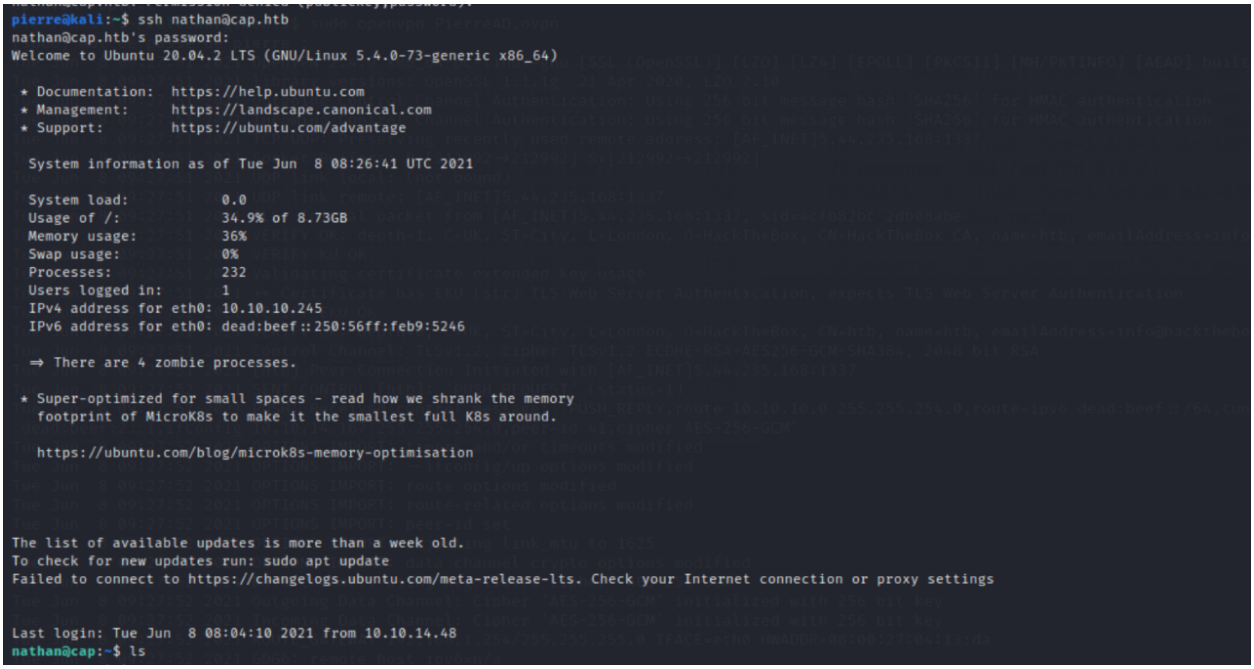
> If the url is changed, we can have access to old captures



> If we inspect the traffic we can see ftp credentials :



> We can now log in ssh with the creds found (User Nathan)



III) Privilege Escalation :

> With the machine name as hint, we can run linpeas only for binaries / suid with this command :

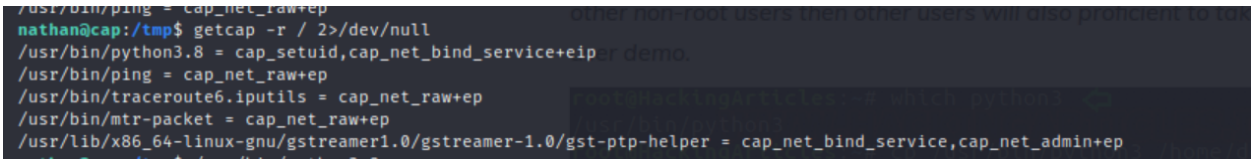
```
./linpeas.sh -o IntFiles
```

> We have a result that interests us on '**linux capabilities**'

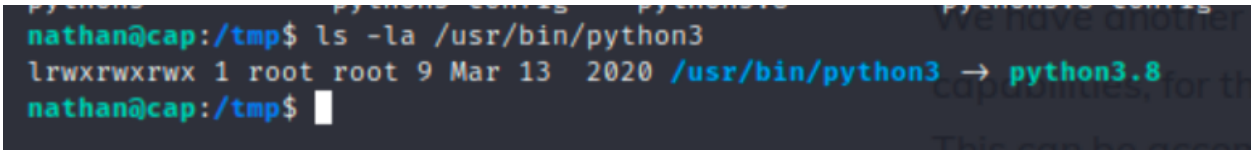
> After some researchs, we can find some article :

https://book.hacktricks.xyz/linux-unix/privilege-escalation/linux-capabilities

> We seach by this command all the binaries with capabilities

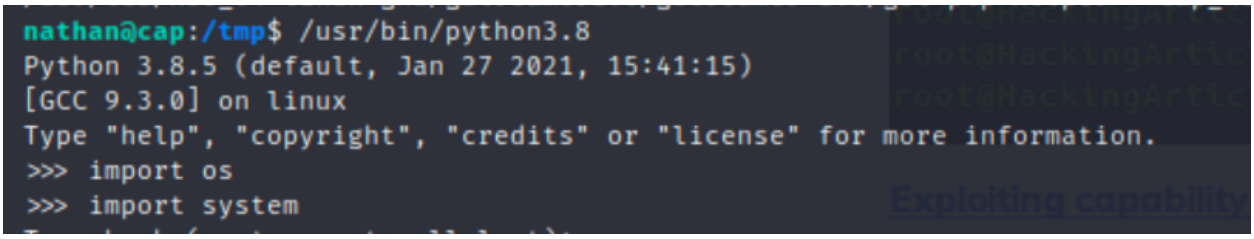


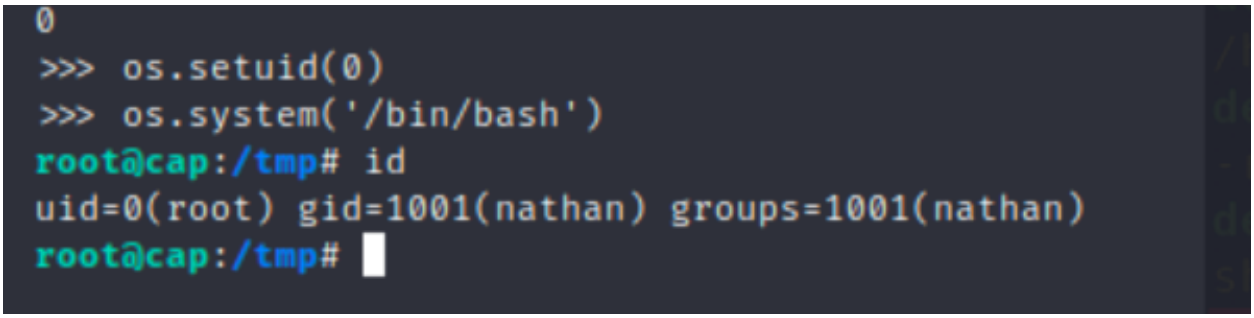
Python 3.8 is displayed on the output, very interesting (the 'cap_setuid+ep' is set, which means all privilege is assigned to the user for that program)



https://www.hackingarticles.in/linux-privilege-escalation-using-capabilities/

> We can launch somme command in python to obtain root shell





anddd we are ROOT !!!