

# Ethical Hacking Package

## Hogwarts Heist - Writeup

22PC02: Abhinivesh

22PC23: Navya

22PC26: Praveshini S B

All the machines are on the NAT Network.

Kali VM: 10.0.2.15

NMap is used to find active hosts on the network. It finds a host with the IP - 10.0.2.16.

The information from the application service versions suggest that it is an Ubuntu Machine.

There are 3 open ports:

FTP: Port 21

SSH: Port 22

HTTP: Port 80

```
[root@kali3 ~]# nmap -A -sT 10.0.2.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-11 11:17 EDT
Nmap scan report for 10.0.2.16
Host is up (0.0027s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
20/tcp    closed  ftp-data
21/tcp    open   ftp     vsftpd 3.0.5
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-nlst: Can't get directory listing: TIMEOUT
|_ftp-syst: 
|_STAT: 
|_FTP server status:
|_Connected to ::ffff:10.0.2.15
|_NDI: 
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_At session startup, client count was 1
|_vsFTPD 3.0.5 - secure, fast, stable
|_End of status
22/tcp    open   ssh     OpenSSH 8.9p1 Ubuntu 0.4 (Ubuntu; protocol 2.0)
|_ssh-hostkey:
|_256 b0:9a:98:e9:3f:ad:80:5e:42:70:83:8e:02:ea:c7 (ED25519)
|_89/100%  Apache/2.4.41 (Ubuntu)
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Apache2 Debian Default Page: It works
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.0.2.15
Host is up (0.0025s latency).
All 1008 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1008 closed tcp ports (conn-refused)
```

```
Nmap scan report for 10.0.2.16 [re/dirs/wordlists/common.txt]
Host is up (0.0027s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
20/tcp    closed  ftp-data
21/tcp    open   ftp     vsftpd 3.0.5
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-nlst: Can't get directory listing: TIMEOUT
|_ftp-syst: 
|_STAT: 
|_FTP server status:
|_Connected to ::ffff:10.0.2.15
|_NDI: 
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_At session startup, client count was 1
|_vsFTPD 3.0.5 - secure, fast, stable
|_End of status
22/tcp    open   ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
|_3072 92:c9:63:10:b8:c4:ad:35:80:e2:93:0c:0:ea:1:07:bb (RSA)
|_256 b3:ee:ee:e2:1b:ca:64:73:4a:c9:c8:b3:e2:cd:8:e1:9e (ECDSA)
|_256 de:37:be:16:64:65:6:a:f:a:f:4:d5:98:54:8:f:2:44 (ED25519)
|_80/tcp    open   http   Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works at 10.0.2.16 Port 80</address>
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

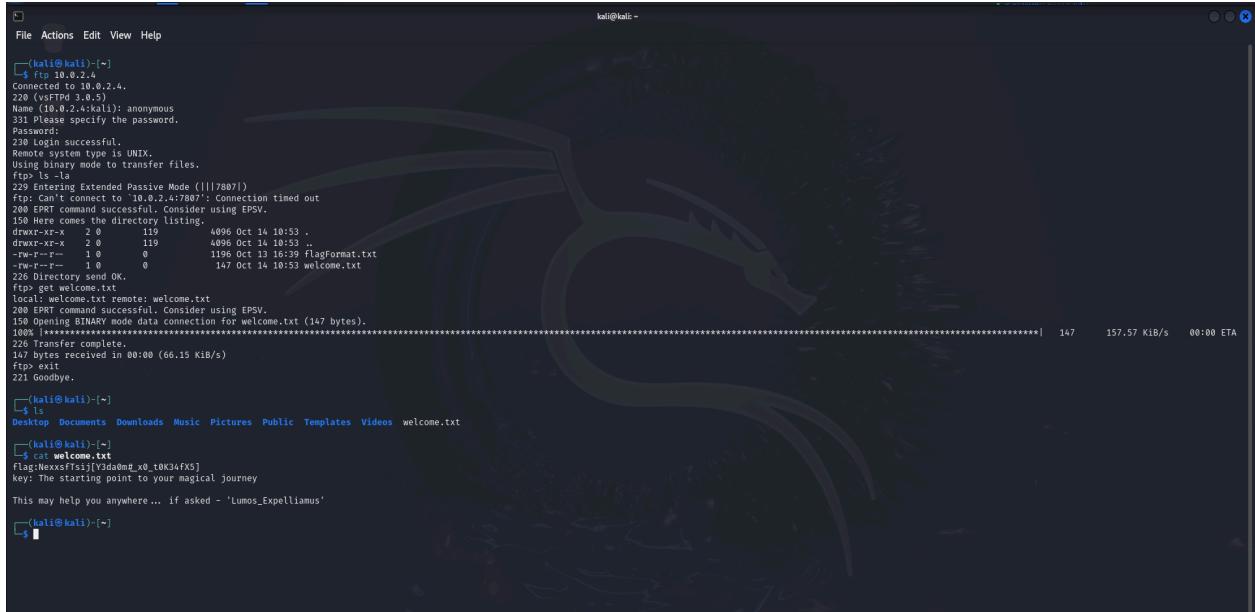
Service detection performed. Please report any incorrect results at https://nmap.org/submit/. 
Nmap done: 256 IP addresses (4 hosts up) scanned in 45.30 seconds
```

It is seen that anonymous login is allowed on the FTP Port.

There is a file containing the flag format and another rule.

```
Flag Format: PotterHead[flag]
Passwords for files(if any): all lowercase letters
```

In ftp another file welcome.txt is there



```
(kali㉿kali)-[~]
$ ftp 10.0.2.4
Connected to 10.0.2.4.
220 (vsFTPd 3.0.5)
Name (10.0.2.4:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
100% 147 157.57 Kib/s 00:00 ETA
$ ls -la
drwxr-xr-x 2 0 119 4096 Oct 14 10:53 .
drwxr-xr-x 2 0 119 4096 Oct 14 10:53 ..
-rw-r--r-- 1 0 0 1196 Oct 13 16:39 flagformat.txt
-rw-r--r-- 1 0 0 147 Oct 14 10:53 welcome.txt
221 Directory send OK.
ftp> get welcome.txt
local: welcome.txt remote: welcome.txt
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for welcome.txt (147 bytes).
100% 147 157.57 Kib/s 00:00 ETA
226 Transfer complete.
167 bytes received in 00:00 (66.15 KiB/s)
ftp> exit
221 Goodbye.

(kali㉿kali)-[~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos welcome.txt

(kali㉿kali)-[~]
$ cat welcome.txt
flag:Nexxxttsij[V3d4m#_x0_t0K34Fx5]
key: The starting point to your magical journey
This may help you anywhere ... if asked - 'Lumos_Exploriamus'

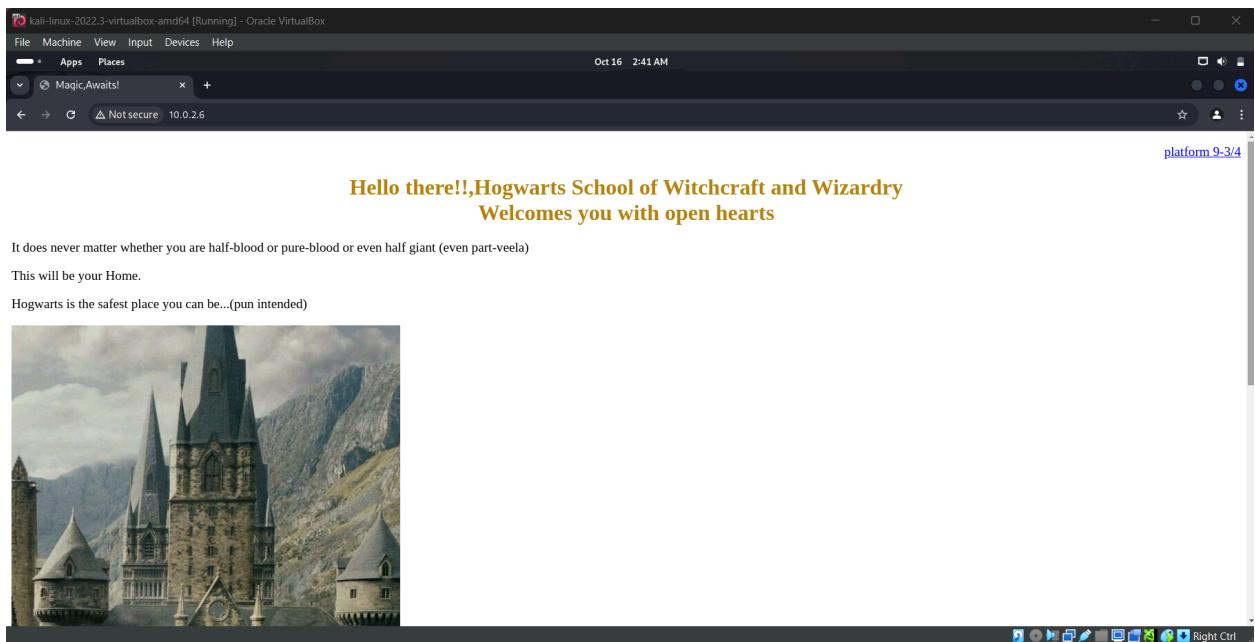
(kali㉿kali)-[~]
$
```

We should decode the affine cipher with key 9,39

We get the flag = **PotterHead[W3lc0m#\_t0\_h0G34rT5]**

With the flag format we have a first flag - that is encoded and encrypted  
With hint

Next we have http port that can be visited



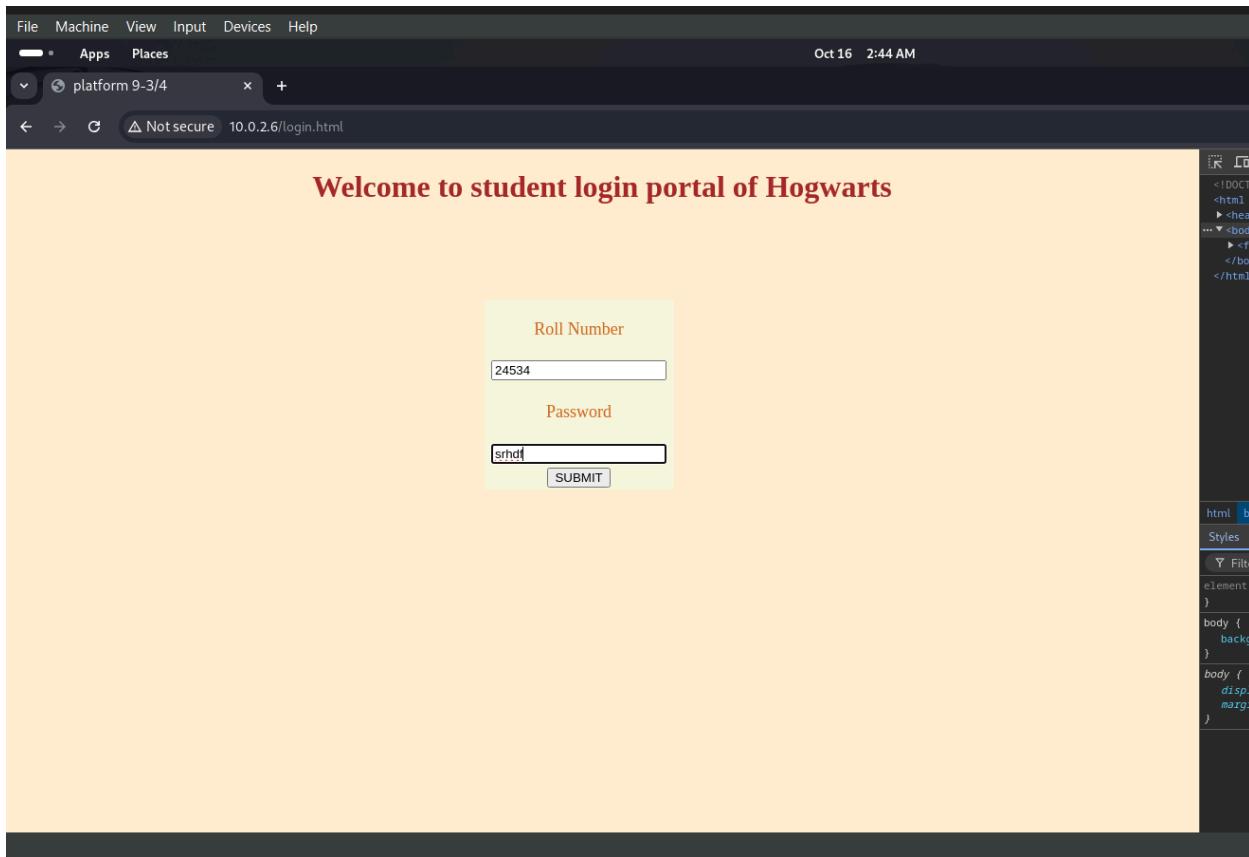
We inspect this page and find 2 parts of a single flag

The screenshot shows the Chrome DevTools Elements tab with the following details:

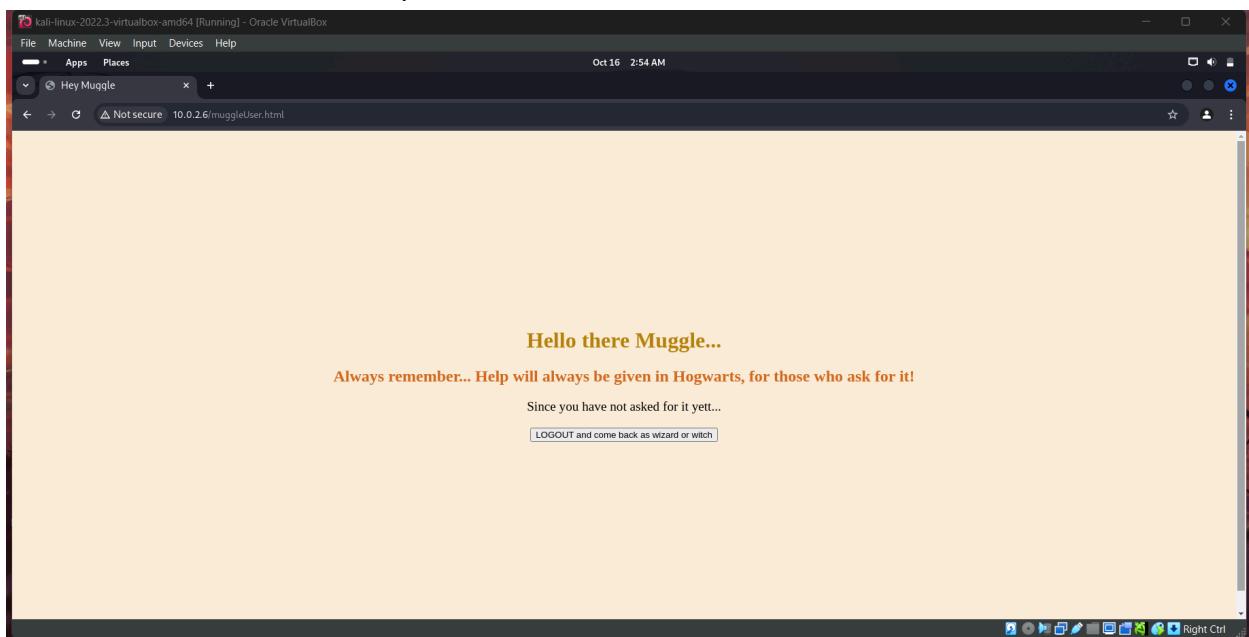
- DOM Tree:** The page structure is as follows:
  - <h1>Platform 9 3/4</h1>
  - </div>
  - <p> "It does never matter whether you are half-blood or pure-blood or even half giant (even part-veela)"</p>
  - <p>This will be your Home.</p>
  - <p>Hogwarts is the safest place you can be...(pun intended)</p>
  - <div>
    - 
  - </div>
  - <center>
    - <h2> Never forget Albus Dumbledore's words.. </h2>
    - <h2>
    - <div>
      - <b> == \$0
      - ""Happiness can be found in the darkest of times, if only one remembers to turn on the light""
      - <!-- last part of flag.. 4\_x1z4r6\_h4rr7-->
  - </div>
- Selected Element:** A **div** element containing a **b** element is selected.
- Styles Tab:** The Styles tab is active, showing the following CSS rules:

  - element.style {  
}
  - b {  
 font-weight: bold;  
}
  - Inherited from **h2**
    - h2 {  
 color: #8B4513;  
}
    - h2 {  
 font-size: 1.5em;  
 font-weight: bold;  
}

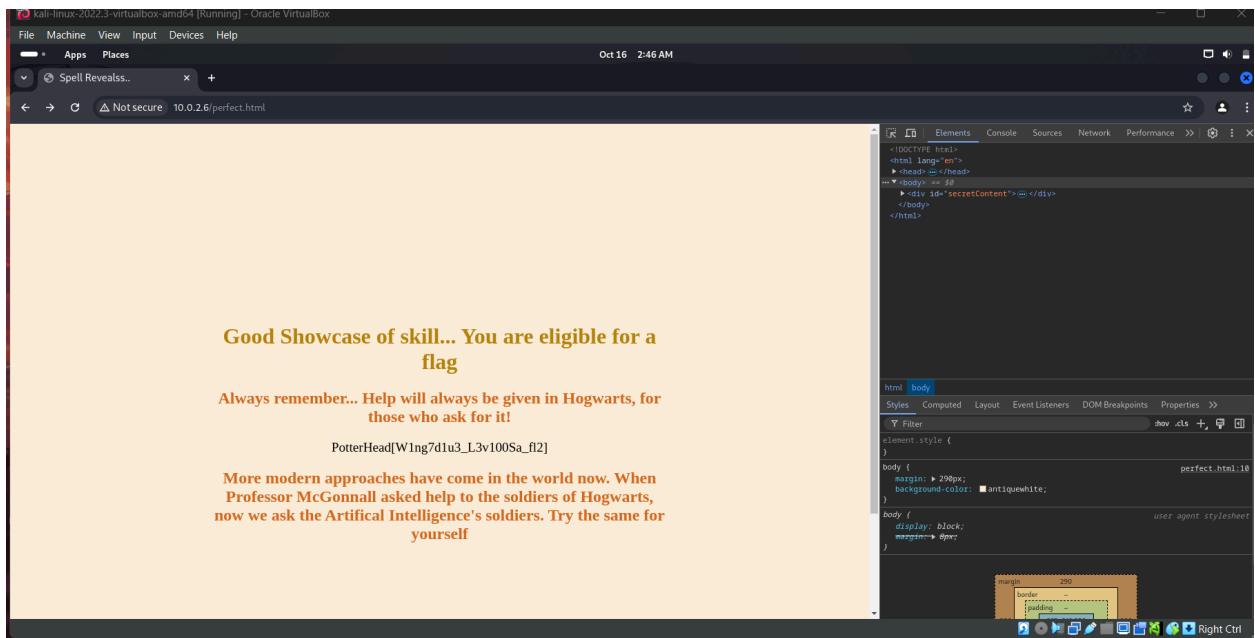
Next we have a link, platform 9 ¾  
We go into it,



And submit random rollno and password



So we understand that special username password or cookie needs to be given.. So we use the welcome.txt hint "Lumos\_Expelliamus" as cookie



With the obtained ssh credentials, access is gained by using curl 10.0.2.4 and the username and password are obtained

```

File Actions Edit View Help
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>Magic,awaits!</title>
<!-- username = pureblood
     password = alohomora
-->
</head>
<style>
.login{
    text-align: right;
}
h1 {
    color: darkgoldenrod;
}
p {
    color: black;
    font-size: larger;
}
h2 {
    color: chocolate;
}
</style>
<body>
    <div id="login"><a href="login.html">platform 9-3</a></p>
        <h1>Hello there!! Hogwarts School of Witchcraft and Wizardry </center>
        <center>welcomes you with open hearts</center>
    </h1>
    <p>It does never matter whether you are half-blood or pure-blood or even half giant (even part-veela)</p>
    <p>This will be your Home.</p>
    <p>Hogwarts is the safest place you can be... (pun intended)</p>
    
    <div>
        <center>
            <h2>Never Forget Albus Dumbledore's words.. </h2>
            <h2>        <div>Happiness can be found in the darkest of times, if only when one remembers to turn on the light!<!-- last part of flag.. 4_x1z4r6_h4rz7]--><b> </div>
        </center>
    </div>
</body>
</html>

```

Username: pureblood

Password: alohomora

```

File Actions Edit View Help
(groot101㉿kali)-[~] 10.0.2.16/ —
$ ssh pureblood@10.0.2.16
pureblood@10.0.2.16's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-196-generic x86_64)

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

System information as of Fri 11 Oct 2024 03:48:22 PM UTC

System load: 0.0          Processes:           134
Usage of /: 42.5% of 11.21GB   Users logged in:  0
Memory usage: 5%           IPv4 address for enp0s3: 10.0.2.16
Swap usage: 0%

```

In the home folder, the draco folder is searched through. There are a few files found.

```
pureblood@hogwarts:~$ cd ..
pureblood@hogwarts:/home$ ls
draco pureblood
pureblood@hogwarts:/home$ cd draco
pureblood@hogwarts:/home/draco$ ls
conversations
pureblood@hogwarts:/home/draco$ cd conversations
pureblood@hogwarts:/home/draco/conversations$ ls -a
. .. ffltlzhzhragh.zip hint.txt hiss.py translate.py
pureblood@hogwarts:/home/draco/conversations$
```

A python file called hiss.py is found. Another zipped file called ffltlzhzhragh.zip is present which is password protected.

The hint mentions that only parselmouths understand the conversation. The hint also suggests that the password lies in the conversation.

On opening the python file, there are certain comments and strings in the print statements that don't look normal.

```
for i in range(3):
    print("A piece of the puzzle falls into place...")

print("Harry's understanding of the Horcruxes grows.")
print("nzhzhraghziizhnzhizh. iizhtth mzhzhraktheezhssss uuzhssss vzhuzhlzhnzheezhrzhzraksslzheezh. wzheezh mzhuzhsssstth")
f print_harry_returns_to_life():
    print("Harry Potter returns to the world of the living, his spirit and determination driving him back to the mortal realm, where he will fa
    print("The warmth of life returns to Harry's body...")
    time.sleep(1) # pause for 1 second
    print("He opens his eyes, ready to face whatever comes next.")

f print_voldemort_final_death():
    print("Lord Voldemort is killed by his own Killing Curse, which rebounds back to him, a fitting end to a life of evil and tyranny, and a te
    print("The curse turns back on Voldemort, striking him down...")
    for i in range(5):
        #print(" mzhizh ffthrzhiiizhheezhnhdzh, mzhuzhsssstth sssstthzrayizh tthlzhoohzsseeezh ")
```

On collecting such statements and arranging them, the conversation is found.

```
tthhsseezh kssoozyizh hsszhrassss dzhiizhsssstthoozhvzheezhrzheezhdzh oozhuuzhrzh sssseeztthrzheezhtth,
nzhzhraghziizhnzhizh. iizhtth mzhzhraktheezhssss uuzhssss vzhuzhlzhnzheezhrzhzraksslzheezh. wzheezh mzhuzhsssstth
|dzheezhptlzhoozyizh zhralzhlzh oozhuuzhrzh ffthoozhrzhttheezhssss nzhoozwhz tthoozh ffthiizhnhdzh hssizhmzh. zhranhdzh yizhoozhuuzh,
| mzhizh ffthrzhiiizhheezhnhdzh, mzhuzhsssstth sssstthzrayizh tthlzhoohzsseeezh|
```

There is also a function voldemort\_talks\_to\_nagini() which prints the whole conversation when called.

```
def voldemort_talks_to_nagini():
    print('tthhsseezh kssoozyizh hsszhrassss dzhiizhsssstthoozhvzheezhrzheezhdzh oozhuuzhrzh sssseeztthrzheezhtth,
nzhzhraghziizhnzhizh. iizhtth mzhzhraktheezhssss uuzhssss vzhuzhlzhnzheezhrzhzraksslzheezh. wzheezh mzhuzhsssstth
|dzheezhptlzhoozyizh zhralzhlzh oozhuuzhrzh ffthoozhrzhttheezhssss nzhoozwhz tthoozh ffthiizhnhdzh hssizhmzh. zhranhdzh yizhoozhuuzh,
| mzhizh ffthrzhiiizhheezhnhdzh, mzhuzhsssstth sssstthzrayizh tthlzhoohzsseeezh')
```

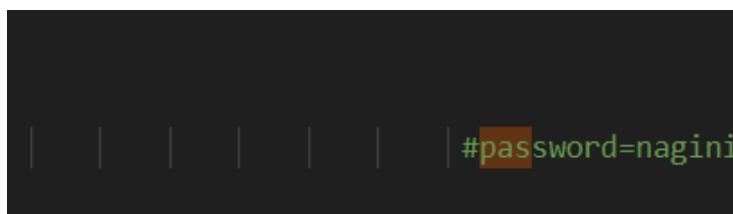
Also a translator file - translate.py is present which accepts language as the parameter and asks the language of the text that is needed to be converted. Parselmouths only understand Parseltongue.

On giving the obtained text as input to the program, the output is obtained as follows:

“che boy has discovered our secrec,  
nagini. ic makes us vulnerable. we musc  
deploy all our forces now co find him. and you,  
my friend, musc scay close”

The password protected file - ffhlzhzragzh.zip - turns out to be ‘flag’.(encoded in parseltongue).

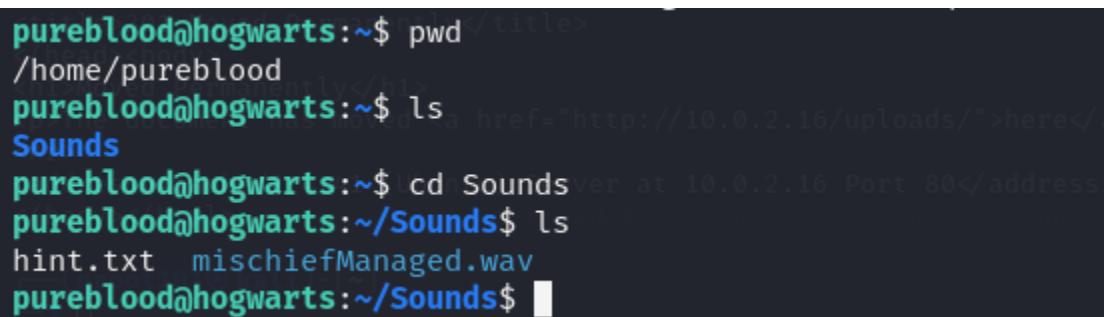
Now the password is guessed as nagini as the file name is hiss.py.  
Also a comment in the python file is found revealing the password.



A terminal window showing a portion of a Python script. The line '#password=nagini' is highlighted in green, indicating it is a comment.

On opening the flag.txt file, a flag is found - **PotterHead[N@g1n1\_th3\_H0rC#ux]**.

A folder called Sounds is found navigating through the home folder. The files are transferred to the local machine - Kali VM.



A terminal window showing directory navigation and listing. The user is in their home directory (~) and lists the contents of the Sounds folder, which contains 'hint.txt' and 'mischiefManaged.wav'.

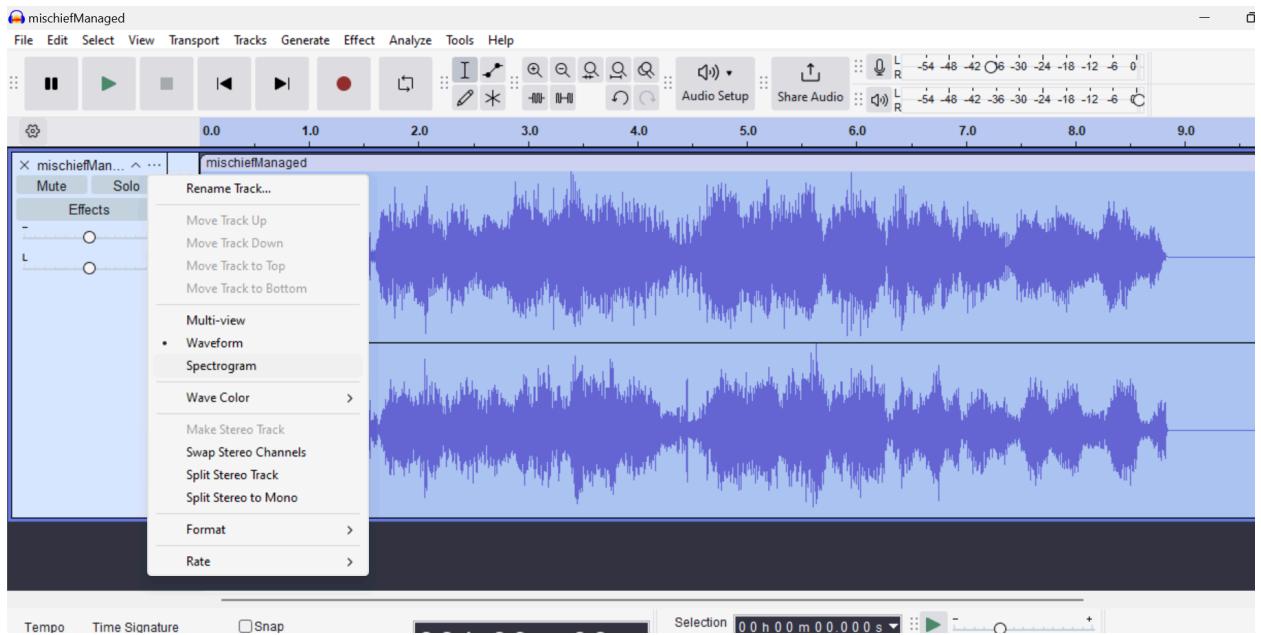
There is an audio file - mischiefManaged.wav - it runs for 8s.

But the audio is heard as a random noise.

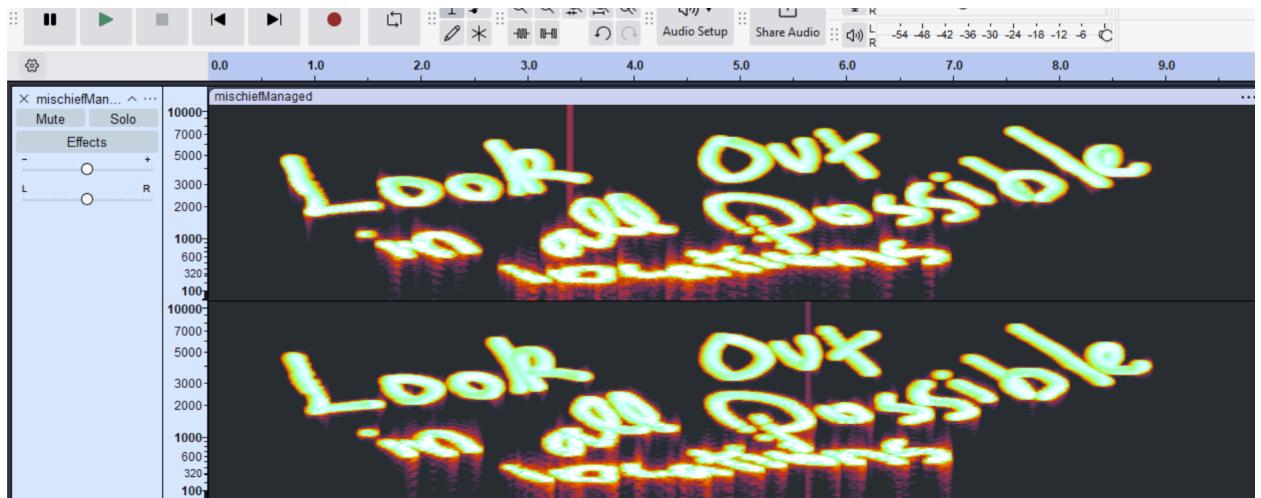
The hint suggests that the sound isn't audible as it isn't in the ghosts' SPECTRUM.

So a steganography technique called - Spectrogram Analysis can be tried.

For this the wav file is opened in Audacity.



The audio should be viewed as spectrograms.



A clue - "Look out in all possible locations" - is obtained.

So the hidden files are explored and a text file- hexicallyDumpedImage.txt is found.  
It appears to have some hexdump values as its name suggests.

```

hexicallyDumpedImage.txt
0A1A0A000000D49484452000005280000003320800000004B67709300010004944154789CECFDD
0D97C0CC3D00C4D51144288240982C0710CE33CF8253C52525F86BDBBE770269A56499971F170375F
7FA945FF39E73FC7F8cff17FFF8B78325FFFB35E93FC77F8EFF1CFF7F7FC3BA212DFFCF53FC77
03FE839BC91E837010C733EB19FFE681A3F61EBFA195EC2F88FD15DFBCEE6B3FEEF1F7D38FC6668
10FC414079DB9677DBB693496F48F9E79386F7C19ABFF8E79B8776D0F76EFDBB66D070F29FD84FF
1E193E3493CFCF29B04C0F1C63BB07DF54E1B5EDFE9D5B35E29C5A1DBF6920FB98104E3FBED24022
2CEE593772E6626CFBEFE9A03FE0B86DED1B92F8AB33F5DDE376D6BFF1E92F1FBF83D3FEDA5DDE1
LF88D78F06F791CE74767167FDA5429C3F406D8FB81937F47A7FBFF69187080FFCAA0FFAB40F93B9E
37FD57A0F5771EBF6E8ABFA64FBF9441CA7F9FF01F3FD5FA6187F82A4F0B56D36FEBAA1579E94370
0EE1D71FF1781F2F7CC821D287FF92AEE14A2B2CF12CC1968C4ADE9E1FFE70CF3D7FDF3BAB5AFC4A7
5F4E9B115078A07A7CD32747D05F0BE76EAAF99B2FD94FFB05FCBA912CEE9F542E7A18B0DF751CFBE
7AABF08E0D6FE17F6FFCB687E015FB1954657BFB3704CC7938B9DE65982FBF6461BF7938FA3BFA3B
DE5DBEEFD75E5FB2DD38F3E328D0FB98B7E7EB9F788369D62733FD5398AD9A1DDC349BFA1556
33BD3DFC3DB83BDC337C81D0F5A59B7C2F996C27DBDA2191B0F15EBB0F078FCCED38C86FB6FF
9555BDA25FF0250FE5FC7C9F2826498A7E065FE107C052C6FAB8D2108D4EFF6C633471ED7FE64D5E
1770042127037737712D806E41AA618E0859695A620A78A19400DA6CB7A0030877761E1AFCDBBDE
79CB0F01DF36034314B87969114B537BCFD0D67533004E50047418DCE04E10100ADDCCB0C4B57370
LDEA5AD19666EE6660094F0ECA42A72763046A5396839B94C41CD1C6079634FEE04DD9D14F19C0D20
37733A7C1CA71471980F6C224C286BE3BDC68C0AD76CDBB3A6CF8897619C932890ECF44334065A4C
7EF2984E3ED38F9F66E42D1B4011DE8CE8A036BCBAF9D97A88238B2FAFE839E297F7A9D69C35975
E52A0F3FFEE50C3338C5856ED90CA24144CCB66D4DDE1A7CDFEF7270F9FFF2E944334000BA79765

```

Using an online tool, the hex is converted to a grayscale image of The Marauders' Map. Now in the hidden files, there is another python file called spellEncoded.py. In spellEncoded.py it is seen that a QR Code is hidden behind the image that was found. Also the comments - bitplanes and lsb - give clues about the encoding techniques.

The screenshot shows a web-based tool for converting hex data into images. At the top, it says "... Cracking the MITAC...". Below that is a toolbar with TOOLS, PLAY, WRITE, EDIT, and PUBLISH buttons. The main area has a title "Hex to Image Converter". Under "Input:", there is a large text area containing the hex dump provided above. Below the input area are dropdown menus for "Convert From:" (set to "Hexadecimal") and "Convert To:" (set to "PNG"). A "Download" button is located next to the "Convert To:" dropdown. At the bottom, there is an "Image Preview" section showing a grayscale image of the Marauders' Map.

```

from PIL import Image
import numpy as np

# Convert cover image to gray-scale
cover = Image.open("coverPhoto.png").convert('L')

data_c = np.array(cover)

# Convert image to 1-bit pixel, black and white
secret = Image.open("qrFrame.png").convert('1')
secret = secret.resize(cover.size)

data_s = np.array(secret, dtype=np.uint8)

# Rewrite LSB
res = data_c & ~1 | data_s

new_img = Image.fromarray(res).convert("L")
new_img.save("cover-secret.png")
new_img.show()

#bitplanesbitplanesbitplanes
#lsblsblsblsb

```

A script is written to extract the actual Least Significant Bits and the QR code is obtained as a PNG image.

```
from PIL import Image
import numpy as np

# Open the encoded image
encoded = Image.open("cover-secret.png").convert('L')
data_e = np.array(encoded)

# Extract the LSBs to reveal the hidden message
hidden_bits = data_e & 1

# Scale bits back to pixel values (0 or 255)
hidden_image = Image.fromarray(hidden_bits * 255).convert('1')

# Save and show the hidden image
hidden_image.save("decoded-secret.png")
hidden_image.show()
```



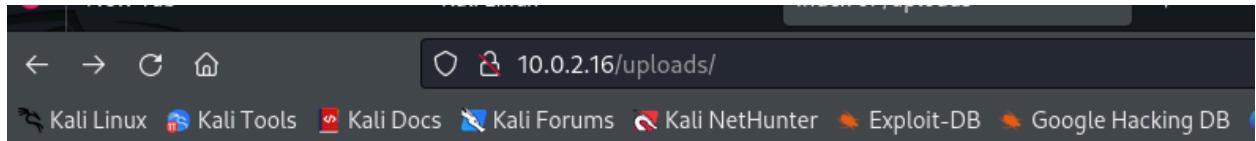
On scanning the QR, a flag is found.

PotterHead[!S0lemnly%Sw3ar\_I^am\_Up!to#N0\_G00d]

To look for possible hidden directories and other directories in the web server at the target machine, dirb is used. The subdirectory /uploads is found

```
[(groot101㉿kali)-[~]]$ dirb http://10.0.2.16
Updates is more than a week old.
To check for new updates run: sudo apt update
DIRB v2.22
By The Dark Raver
Last login: Fri Oct 11 14:09:59 2024
START_TIME: Fri Oct 11 09:56:54 2024
URL_BASE: http://10.0.2.16/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
[!] Threads: 10000 [!] Timeout: 10s [!] Threads: 10000 [!] Timeout: 10s
[!] Threads: 10000 [!] Timeout: 10s [!] Threads: 10000 [!] Timeout: 10s
pureblood@kali:~/Desktop$ pwd
/home/pureblood
GENERATED WORDS: 4612 $ ls
Sounds
--- Scanning URL: http://10.0.2.16/
+ http://10.0.2.16/index.html (CODE:200|SIZE:10918)
+ http://10.0.2.16/server-status (CODE:403|SIZE:274)
⇒ DIRECTORY: http://10.0.2.16/uploads/
pureblood@kali:~/Desktop$ cd http://10.0.2.16/uploads/
--- Entering directory: http://10.0.2.16/uploads/
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
pureblood@kali:~/Desktop$ ls
END_TIME: Fri Oct 11 09:57:01 2024
DOWNLOADER: /612 FOUND: 2
```

2 text files are found.

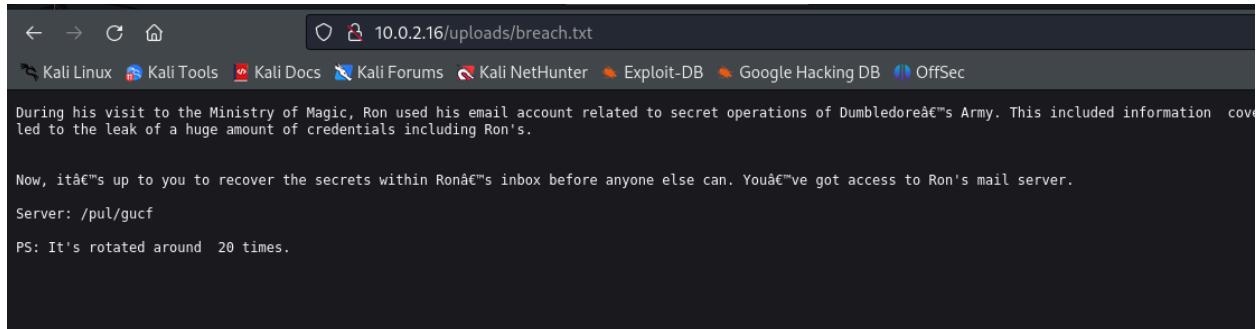


## Index of /uploads

Name	Last modified	Size Description
<a href="#">Parent Directory</a>	-	
<a href="#">breach.txt</a>	2024-10-11 12:42	495
<a href="#">wall.txt</a>	2024-10-11 13:51	627

Apache/2.4.41 (Ubuntu) Server at 10.0.2.16 Port 80

breach.txt turns out to be a clue for flags.



The server path is shifted 20 times. The actual path: /var/mail

On navigating to the folder, folders minuteOfMeeting and sortingHat are present.

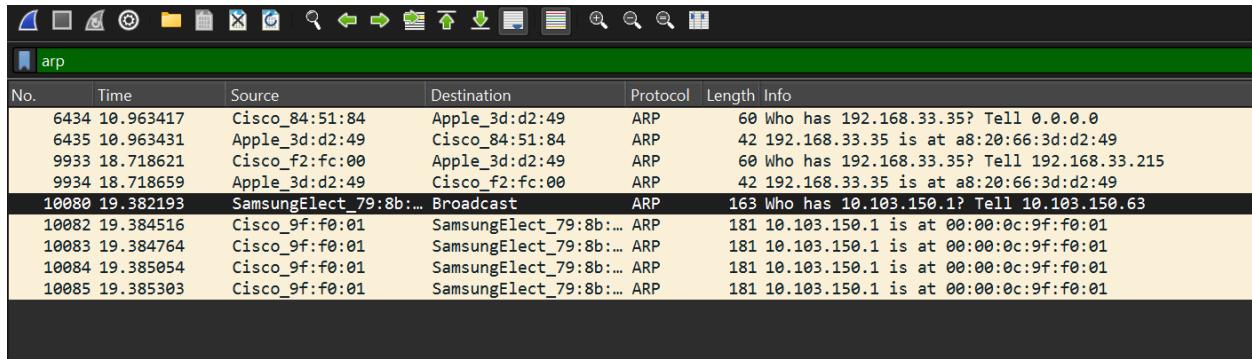
```
pureblood@hogwarts:/home$ cd .. /var/mail
pureblood@hogwarts:/var/mail$ ls
minuteOfMeeting  sortingHat
pureblood@hogwarts:/var/mail$ cd minutesOfMeeting
-bash: cd: minutesOfMeeting: No such file or directory
pureblood@hogwarts:/var/mail$ cd minuteOfMeeting
pureblood@hogwarts:/var/mail/minuteOfMeeting$ ls
hint.txt  protectUs.pcapng
pureblood@hogwarts:/var/mail/minuteOfMeeting$ cat hint.txt
When Harry, Hermione, and Ron decide to form Dumbledore's Army, they gather a group of like-minded students with Dark Arts skills, especially with Voldemort's return. He emphasizes the importance of being prepared to agree to learn from him.

Harry has (arp)BROADCASTED an important spell to all that gives protection from the Dementors. He sends them to the world.

Harry has created a site for the spell. When another person tried to access it in his system, the person
```

minuteOfMeeting contains a pcapng file.

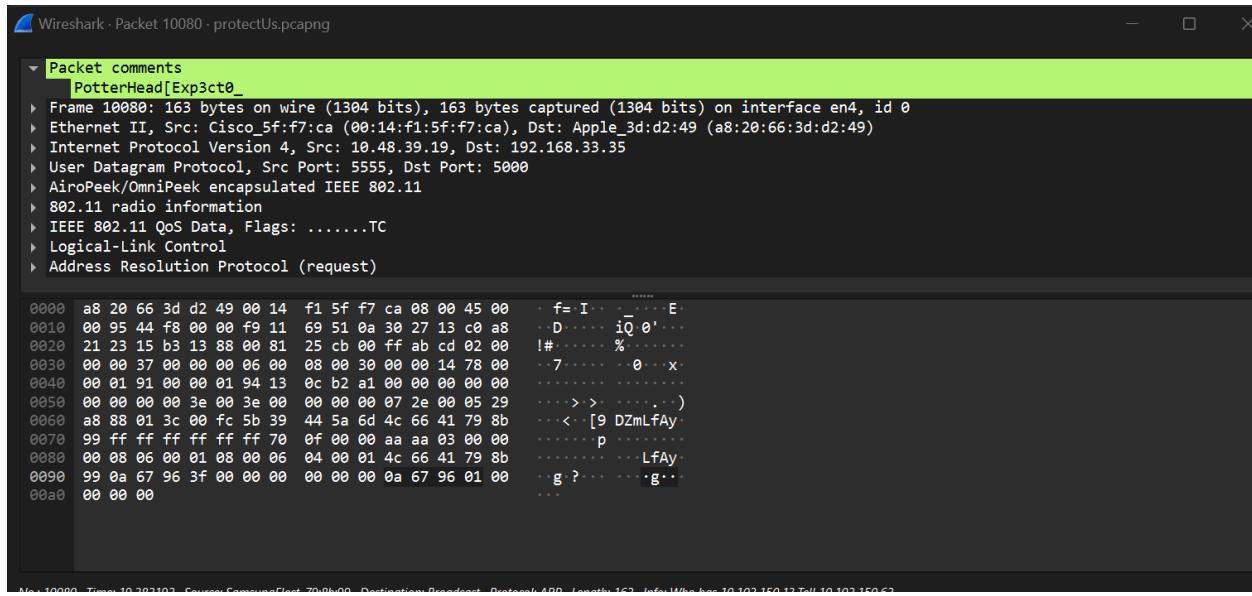
protectUs.pcapng is opened using Wireshark. It has over 10000 packets.  
hint.txt has the information that the spell is in 2 parts. So ,the flag is in 2 parts.  
One of the clues in hint.txt is that the spell has been (arp)BROADCASTED.



A screenshot of Wireshark showing an ARP broadcast packet. The packet details are as follows:

No.	Time	Source	Destination	Protocol	Length	Info
6434	10.963417	Cisco_84:51:84	Apple_3d:d2:49	ARP	60	Who has 192.168.33.35? Tell 0.0.0.0
6435	10.963431	Apple_3d:d2:49	Cisco_84:51:84	ARP	42	192.168.33.35 is at a8:20:66:3d:d2:49
9933	18.718621	Cisco_f2:fc:00	Apple_3d:d2:49	ARP	60	Who has 192.168.33.35? Tell 192.168.33.215
9934	18.718659	Apple_3d:d2:49	Cisco_f2:fc:00	ARP	42	192.168.33.35 is at a8:20:66:3d:d2:49
10080	19.382193	SamsungElect_79:8b:..	Broadcast	ARP	163	Who has 10.103.150.1? Tell 10.103.150.63
10082	19.384516	Cisco_9f:f0:01	SamsungElect_79:8b:..	ARP	181	10.103.150.1 is at 00:00:0c:9f:f0:01
10083	19.384764	Cisco_9f:f0:01	SamsungElect_79:8b:..	ARP	181	10.103.150.1 is at 00:00:0c:9f:f0:01
10084	19.385054	Cisco_9f:f0:01	SamsungElect_79:8b:..	ARP	181	10.103.150.1 is at 00:00:0c:9f:f0:01
10085	19.385303	Cisco_9f:f0:01	SamsungElect_79:8b:..	ARP	181	10.103.150.1 is at 00:00:0c:9f:f0:01

Looking at the pcap file,there is only one ARP Broadcast packet.  
On analyzing the packet,one half of a flag is found in the Packet Comments -  
PotterHead[Exp3ct0\_



A screenshot of Wireshark showing the packet comments for the ARP broadcast packet. The comments are as follows:

```
Packet comments
PotterHead[Exp3ct0_
Frame 10080: 163 bytes on wire (1304 bits), 163 bytes captured (1304 bits) on interface en4, id 0
Ethernet II, Src: Cisco_5f:f7:ca (00:14:f1:5f:f7:ca), Dst: Apple_3d:d2:49 (a8:20:66:3d:d2:49)
Internet Protocol Version 4, Src: 10.48.39.19, Dst: 192.168.33.35
User Datagram Protocol, Src Port: 5555, Dst Port: 5000
AiroPeek/OmniPeek encapsulated IEEE 802.11
802.11 radio information
IEEE 802.11 QoS Data, Flags: .....TC
Logical-Link Control
Address Resolution Protocol (request)

0000 a8 20 66 3d d2 49 00 14 f1 5f f7 ca 08 00 45 00 .. f= I .. E
0010 00 95 44 f8 00 00 f9 11 69 51 0a 30 27 13 c0 a8 .. D .. iQ 0' ..
0020 21 23 15 b3 13 88 00 81 25 cb 00 ff ab cd 02 00 !# .. %
0030 00 00 37 00 00 00 06 00 08 00 30 00 00 14 78 00 .. 7 .. 0 .. x
0040 00 01 91 00 00 01 94 13 0c b2 a1 00 00 00 00 00 .. .
0050 00 00 00 3e 00 3e 00 00 00 07 2e 00 05 29 .. > .. )
0060 a8 88 01 3c 00 fc 5b 39 44 5a 6d 4c 66 41 79 8b .. < [9 DZmLfAy
0070 99 ff ff ff ff ff 70 0f 00 00 aa aa 03 00 00 .. p ..
0080 00 08 00 01 08 00 06 04 00 01 4c 66 41 79 8b .. LfAy
0090 99 0a 67 96 3f 00 00 00 00 00 00 0a 67 96 01 00 .. g ? .. g ..
00a0 00 00 00 ..
```

The next clue in hint.txt- The query to Harry's site was DSNied.  
So DNS packets are checked which are 39 in number.Out of the 39 packets , only response packets containing deny messages are checked.

No.	Time	Source	Destination	Protocol	Length	Info
6185	10.164552	10.48.39.33	192.168.33.35	DNS	344	Standard query response 0x1e2c A ccm-ams-07x.cisco.com A 144.254.75.185 NS hkid
6982	12.123336	192.168.33.35	10.48.39.33	DNS	103	Standard query 0x674b AAAA 7.courier-sandbox-push-apple.com.akadns.net
6990	12.147244	10.48.39.33	192.168.33.35	DNS	169	Standard query response 0x674b AAAA 7.courier-sandbox-push-apple.com.akadns.net
7412	13.413718	192.168.33.35	10.48.39.33	DNS	81	Standard query 0xa932 A ucx-em1-gss.cisco.com
7413	13.413838	192.168.33.35	10.48.39.33	DNS	81	Standard query 0xb2b5b AAAA ucx-em1-gss.cisco.com
7420	13.436768	10.48.39.33	192.168.33.35	DNS	344	Standard query response 0xa932 A ucx-em1-gss.cisco.com A 10.61.25.91 NS alln01-
7421	13.437429	10.48.39.33	192.168.33.35	DNS	81	Standard query response 0x2b5b AAAA ucx-em1-gss.cisco.com
9325	17.946556	192.168.33.35	208.67.222.222	DNS	87	Standard query 0xe4c6 TXT 2.DnsCrYpT-CerT.OpenDns.com
18431	20.652012	192.168.33.35	10.48.39.33	DNS	81	Standard query 0xd9a0 A ccm-ams-07x.cisco.com
18432	20.653185	10.48.39.33	192.168.33.35	DNS	344	Standard query response 0xd9a0 A ccm-ams-07x.cisco.com A 144.254.75.185 NS rtp5
18433	20.653948	192.168.33.35	10.48.39.33	DNS	81	Standard query 0x8ac2 AAAA ccm-ams-07x.cisco.com
18436	20.676617	10.48.39.33	192.168.33.35	DNS	81	Standard query response 0x8ac2 AAAA ccm-ams-07x.cisco.com
18828	21996981.52...	10.0.2.15	192.168.1.1	DNS	82	Standard query 0x6375 A flagPart2-PAtro0num.com
18829	21996981.52...	10.0.2.15	192.168.1.1	DNS	82	Standard query 0x2574 AAAA flagPart2-PAtro0num.com
18830	21996981.70...	192.168.1.1	10.0.2.15	DNS	155	Standard query response 0x6375 No such name A flagPart2-PAtro0num.com SOA a.g
18831	21996981.74...	192.168.1.1	10.0.2.15	DNS	155	Standard query response 0x2574 No such name AAAA flagPart2-PAtro0num.com SOA a.g
↓						
Ethernet II, Src: PCSystemtec_59:1f:f7 (52:54:00:12:35:00), Dst: PCSystemtec_59:1f:f7 (08:00:27:59:1f:f7)						
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 10.0.2.15						
User Datagram Protocol, Src Port: 53, Dst Port: 55766						
Domain Name System (response)						
Transaction ID: 0x2574						
> Flags: 0x8183 Standard query response, No such name						
Questions: 1						
Answer RRs: 0						
Authority RRs: 1						
Additional RRs: 0						
Queries						
> flagPart2-PAtro0num.com: type AAAA, class IN						
0000 08 00 27 59						
0010 00 8d 3c 58						
0020 02 0f 00 35						
0030 00 00 00 01						
0040 2d 50 41 74						
0050 00 01 c0 1f						
0060 0c 67 74 6c						
0070 74 00 05 6e						
0080 6e 2d 67 72						
0090 00 03 84 00						

There is a DNS packet - query containing domain name as flagPart2-PAtro0num.com. So, the second part of the spell is obtained.

Flag found: **PotterHead[Exp3ct0\_P@tr0num]**

sortingHat contains an executable file.

```
Help Ron to find the spell.pureblood@hogwarts:/var/mail/warning$ cd ..//sortingHat
pureblood@hogwarts:/var/mail/sortingHat$ ls
hint.txt sortingHat.exe
pureblood@hogwarts:/var/mail/sortingHat$ cat hint.txt
The Great Hall at Hogwarts is a magnificent sight, illuminated by floating candles and enchanted ceiling that reflects the eager faces of the first years. The atmosphere buzzes with anticipation as students whisper and cheer for their house.

As the Sorting Hat is placed on the stool, it begins to sing its traditional song, introducing the qualities of each house. The palpable energy of each name is called, and the students approach the hat, which seems to have a personality of its own.

Ron has received a file that appears to mimic the Sorting Hat. Little does he know that it was actually sent by Hermoine.

He tries to recover the underlying secret by analyzing it.
The HEX of the end file of the application appears to be sus.
```

On running the executable,

```
Ah, another brave soul, I see!
Step forward, and let's see where you'll be.
In this great hall of magic and cheer,
I'll place you in a house, so have no fear.

Courage and daring? That's Gryffindor's way.
Loyal and true? Hufflepuff's here to stay.
Wise and clever? Ravenclaw calls to you.
Ambitious and sly? Slytherin is waiting, too!

So take a seat, and let me decide,
Your heart will reveal where your true self will hide.
Question: What do you value most? (courage, loyalty, intelligence, ambition): loyalty
Welcome to HufflePuff
hi.press enter.
```

Your heart will reveal where your true self will hide.

Question: What do you value most? (courage, loyalty, intelligence, ambition): ambition  
Slytherin is proud to have you.  
hi.press enter.

Your heart will reveal where your true self will hide.

Question: What do you value most? (courage, loyalty, intelligence, ambition): intelligence  
Ravenclaw welcomes you  
hi.press enter.

Question: What do you value most? (courage, loyalty, intelligence, ambition): courage  
FLAGGED AS GRYFFINDOR!!  
hi.press enter.

As seen from the above images, each input gives a different output and the output for the input "courage" seems interesting.

x64dbg is used to analyze the executable.

The references to the string "FLAGGED AS GRYFFINDOR" are searched for.

All Modules (Strings)	Address	Disassembly	String Address	String
	000000000401821	lea rdx,qword ptr ds:[408019]	0000000000408019	"Ravenclaw"
	00000000040184F	lea rdx,qword ptr ds:[408023]	0000000000408023	"Slytherin"
	000000000401986	lea rdx,qword ptr ds:[40822E]	000000000040822E	"courage"
	0000000004019C9	lea rdx,qword ptr ds:[408237]	0000000000408237	"adventuring"
	0000000004019E4	lea rdx,qword ptr ds:[408243]	0000000000408243	"fighting"
	000000000401A27	lea rdx,qword ptr ds:[408003]	0000000000408003	"Gryffindor"
	000000000401A77	lea rdx,qword ptr ds:[40824C]	000000000040824C	"loyalty"
	000000000401A8E	lea rdx,qword ptr ds:[408261]	0000000000408261	"helping others"
	000000000401A91	lea rdx,qword ptr ds:[408263]	0000000000408263	"teamwork"
	000000000401A93	lea rdx,qword ptr ds:[408006]	0000000000408006	"Hufflepuff"
	000000000401B38	lea rdx,qword ptr ds:[40826C]	000000000040826C	"intelligence"
	000000000401B4F	lea rdx,qword ptr ds:[408279]	0000000000408279	"studying"
	000000000401B66	lea rdx,qword ptr ds:[408282]	0000000000408282	"solving puzzles"
	000000000401B9A	lea rdx,qword ptr ds:[408019]	0000000000408019	"Ravenlaw"
	000000000401B9F	lea rdx,qword ptr ds:[408292]	0000000000408292	"ambition"
	000000000401C10	lea rdx,qword ptr ds:[408298]	0000000000408298	"planning"
	000000000401C11	lea rdx,qword ptr ds:[4082A1]	00000000004082A1	"strategy"
	000000000401C6A	lea rdx,qword ptr ds:[408023]	0000000000408023	"Slytherin"
	000000000401C83	lea rdx,qword ptr ds:[4082B0]	00000000004082B0	"Invalid answer. Please answer with the given options.\n"
	000000000401D37	lea rdx,qword ptr ds:[408030]	0000000000408030	"Gryffindor"
	000000000401D67	lea rdx,qword ptr ds:[4082E7]	00000000004082E7	"PotterHead[gRy77!Nd0R_]"
	000000000401D85	lea rdx,qword ptr ds:[4082FE]	00000000004082FE	"FLAGGED AS GRYFFINDOR!!\n"
	000000000401DAA	lea rdx,qword ptr ds:[40800E]	000000000040800E	"Hufflepuff"
	000000000401D8D	lea rdx,qword ptr ds:[408317]	0000000000408317	"Welcome to HufflePuff\n"
	000000000401D96	lea rdx,qword ptr ds:[408019]	0000000000408019	"Ravenlaw"
	000000000401D99	lea rdx,qword ptr ds:[40832E]	000000000040832E	"Ravenlaw welcomes you\n"

			call sortinghat.402380	[rbp+2CF]:???
			lea rdx,qword ptr ss:[rbp+2CF]	
			lea rax,qword ptr ss:[rbp-40]	
			mov r8,rdx	
			lea rdx,qword ptr ds:[4082E7]	00000000004082E7:"PotterHead[gRy77!Nd0R_]"
			mov rcx,rax	
			call sortinghat.402380	[rbp+2CF]:???
			lea rax,qword ptr ss:[rbp+2CF]	
			mov rcx,rax	
			call sortinghat.4023A8	00000000004082E7:"PotterHead[gRy77!Nd0R_]"
			lea rdx,qword ptr ds:[4082FE]	
			mov rcx,qword ptr ds:[&std::cout]	00000000004082FE:"FLAGGED AS GRYFFINDOR!!\n"
			call sortinghat.402328	
			lea rax,qword ptr ss:[rbp-40]	
			mov rcx,rax	
			call sortinghat.402368	

As seen in the above images, the flag's first half - "PotterHead[gRy77!Nd0R\_" is found in the string references.

There is a clue in the hint.txt provided.

"The HEX of the end file of the application appears to be sus."

On opening the binary file with a hex editor, the flag's second part - c4ll5\_y0u] of the flag is found.

55 63 75 72 69 74 79 5F 63 6F 6F 6B 69 65 00 20 00 20 00 63 00 34 00 6C 00 6C 00 35 00 5F mp\_Znwy\_security\_cookie c 4 1 1 5 y 0 u ]

Flag: PotterHead[gRy77!Nd0R\_c4ll5\_y0u]

In wall.txt, another clue is found

The screenshot shows a web browser window with the URL 10.0.2.16/uploads/. The page title is "Index of /uploads". Below the title is a table with three columns: Name, Last modified, and Size Description. The table contains two entries: "breach.txt" and "wall.txt". The "wall.txt" entry has a timestamp of 2024-10-11 13:51 and a size of 627. At the bottom of the page, it says "Apache/2.4.41 (Ubuntu) Server at 10.0.2.16 Port 80".

## Index of /uploads

Name	Last modified	Size Description
------	---------------	------------------

Parent Directory	-	
breach.txt	2024-10-11 12:42	495
wall.txt	2024-10-11 13:51	627

Apache/2.4.41 (Ubuntu) Server at 10.0.2.16 Port 80

The screenshot shows a web browser window with the URL 10.0.2.16/uploads/wall.txt. The page content is a single line of text: "their dark magic surging through the air, hurled their spells at the seemingly invisible WALL around Hogwarts. Yet, their curses bounced off it as if repelled by an unseen force. Even Voldemort's most potent spell, aimed at Harry Potter, was met with a resounding DSNial."

the crowd as the realization dawned upon them. The Death Eaters, with all their power and knowledge, had stumbled upon a hidden WALL, its presence unknown to them. Hermione , her eyes wide with fascination, was determined to unravel the spell used by Voldemort for the future. Find the spell

The hint suggests checking the firewall rules.

The flag: **PotterHead[4vad4\_k3d4vra]** is found.

```
pureblood@hogwarts:~$ sudo ufw status
Status: active

To                         Action      From
--                         --          --
20/tcp                      ALLOW       Anywhere
21/tcp                      ALLOW       Anywhere
22/tcp                      ALLOW       Anywhere
80/tcp                      ALLOW       Anywhere
53                         DENY        Anywhere          # PotterHead[4vad4_k3d4vra]
20/tcp (v6)                 ALLOW       Anywhere (v6)
21/tcp (v6)                 ALLOW       Anywhere (v6)
22/tcp (v6)                 ALLOW       Anywhere (v6)
80/tcp (v6)                 ALLOW       Anywhere (v6)
```

