**Name : ADARSH M. MENDHE**

**Assignment : 2**

**Question 1:**

● Create payload for windows .

● Transfer the payload to the victim's machine.

● Exploit the victim's machine.

**Answer:**

Open kali machine

Open terminal

#apt install apache2

#cd /var/www/html/

#mkdir counterstrike

#cd counterstrike

in the directory create payload for windows system

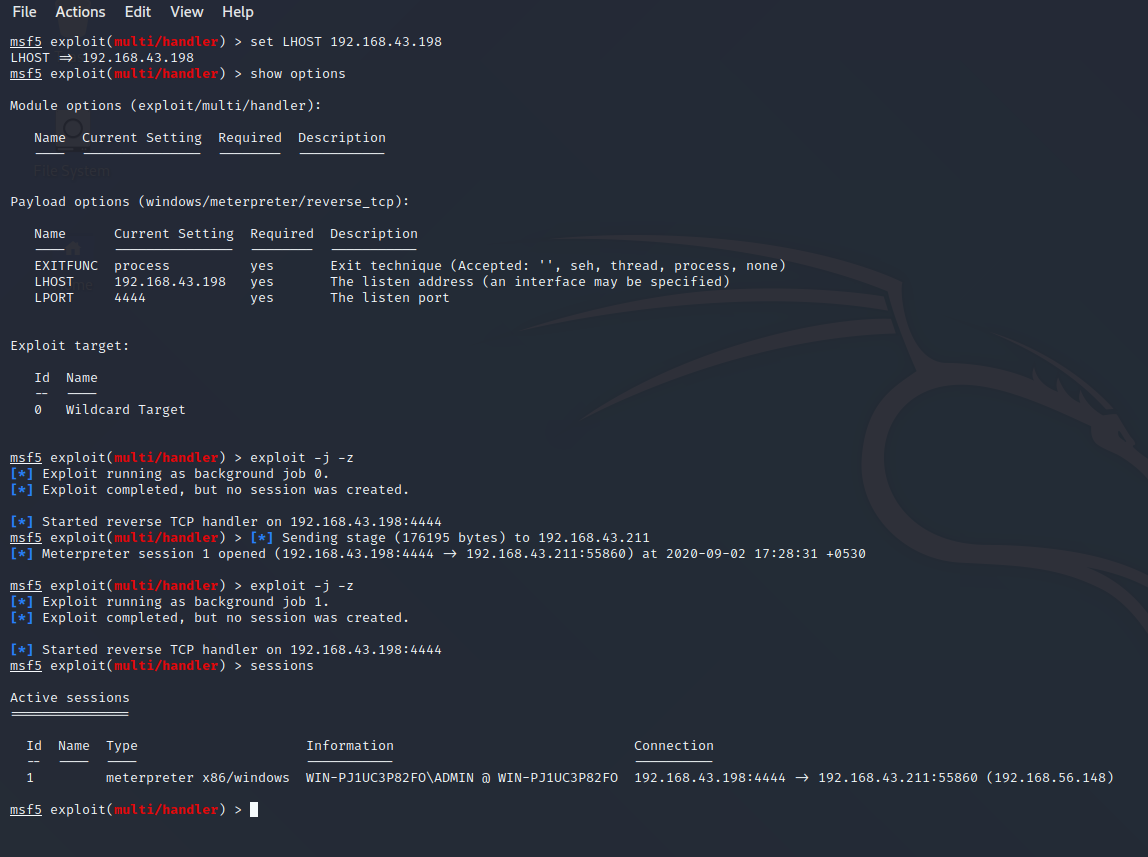
#systemctl enable apache2

#systemctl start apache2

On target system

Open browser type: #http://<ipadd>/counterstrike

#msfconsole

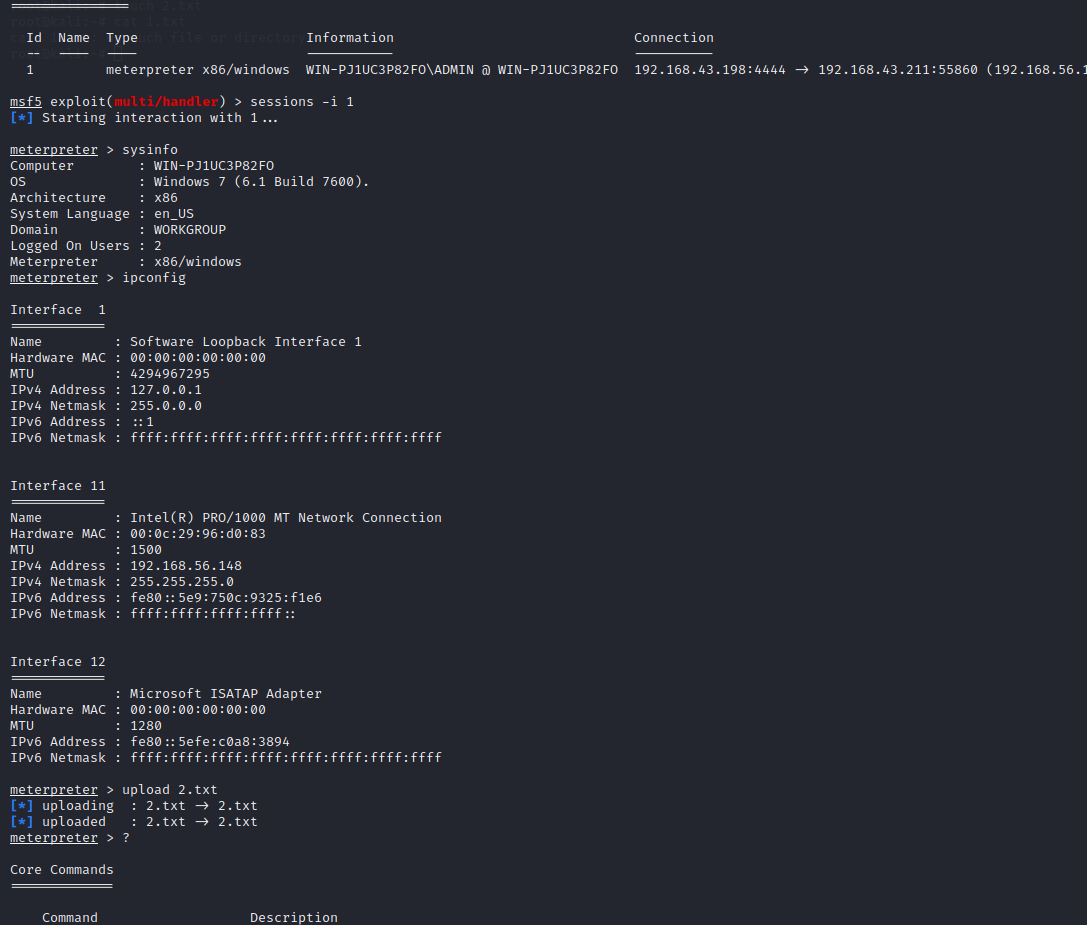


#Use multi/handler

#set payload

#exploit

#sessions



**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:

Create FTP server on WINDOWS server

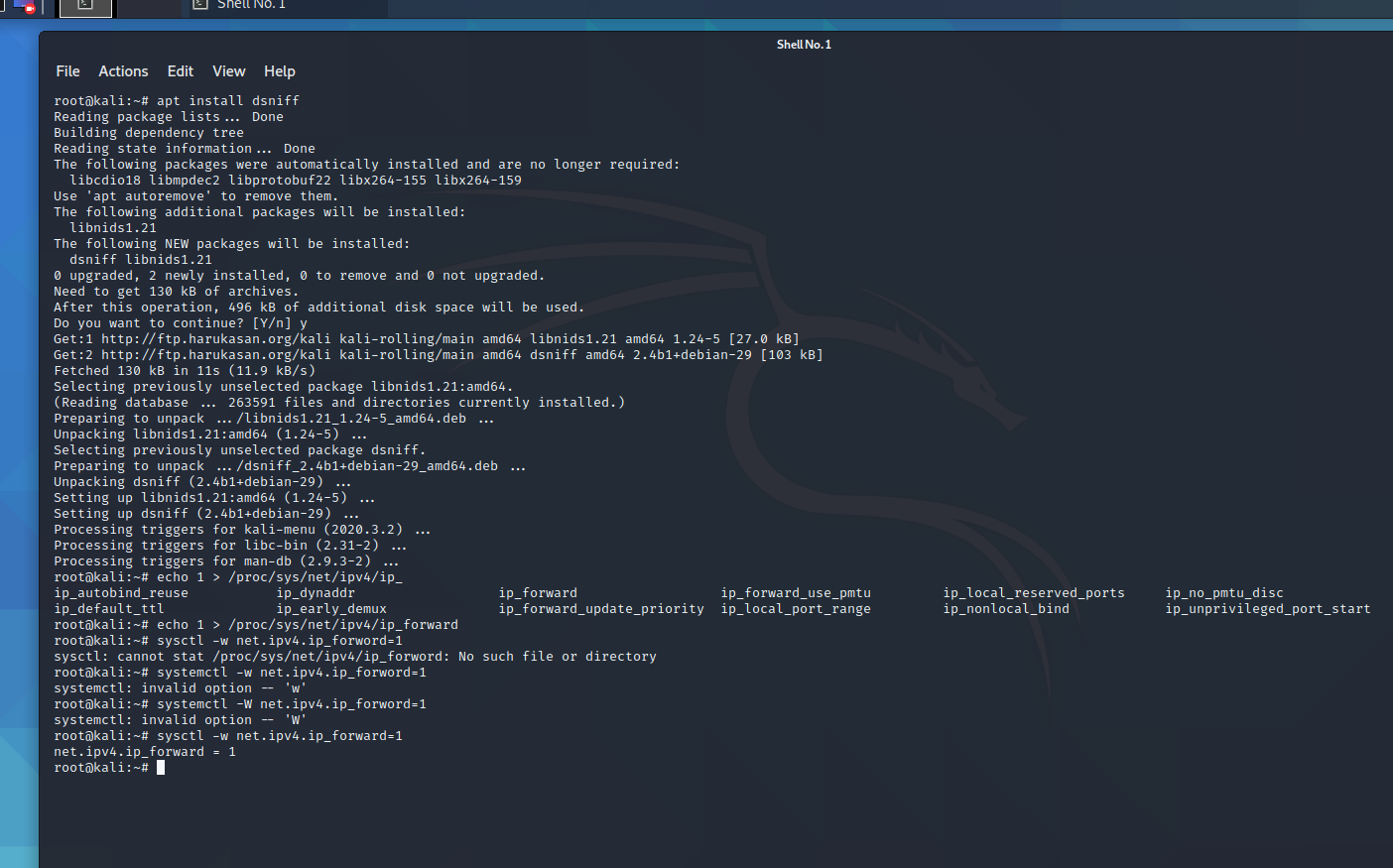
Create user

On another windows machine open terminal

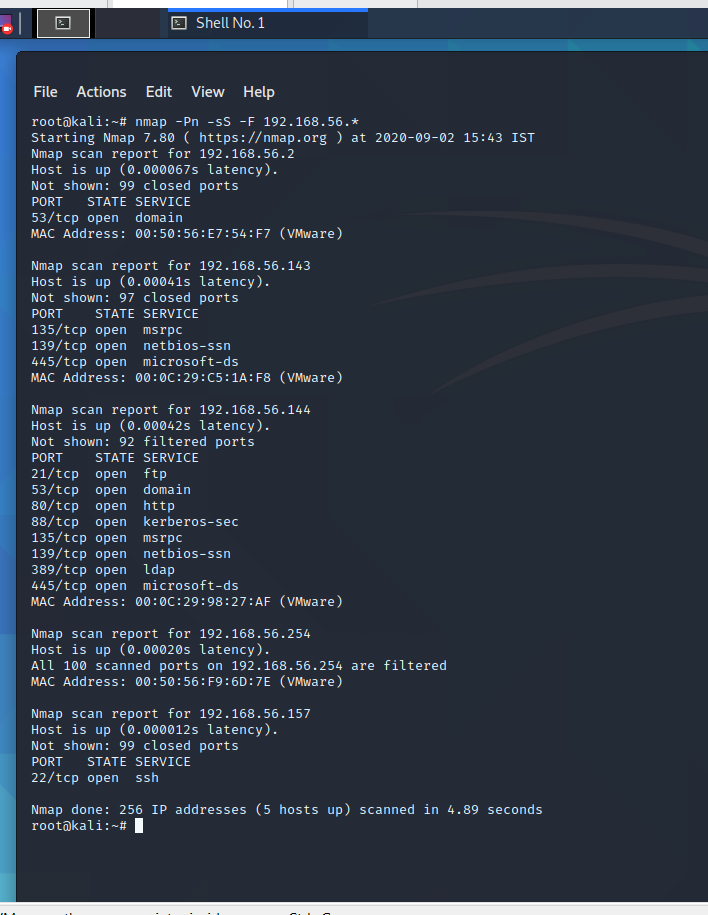
#ftp <ip add>

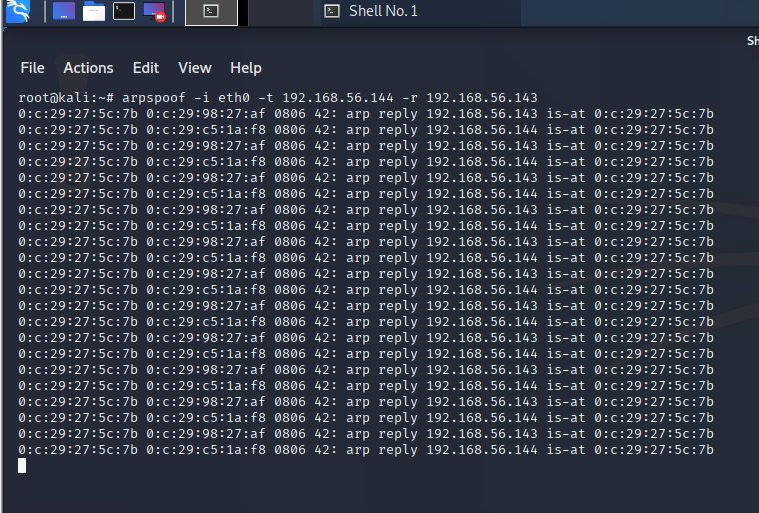
Open kali machine

Install dsniff



**Here we are scanning the network**





Here we get the username & password

