Name: Vinit Kumar Sharma

Email: [vinitkumar261995@gmail.com](mailto:vinitkumar261995@gmail.com)

Subject: Cyber Security Essentials Batch-1, Day-6 Assignment

**Day-6 Assignment**

**Question 1.**

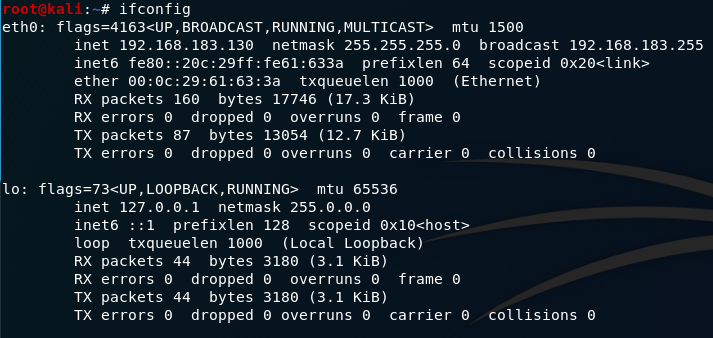
● Create payload for windows.

● Transfer the payload to the victim's machine.

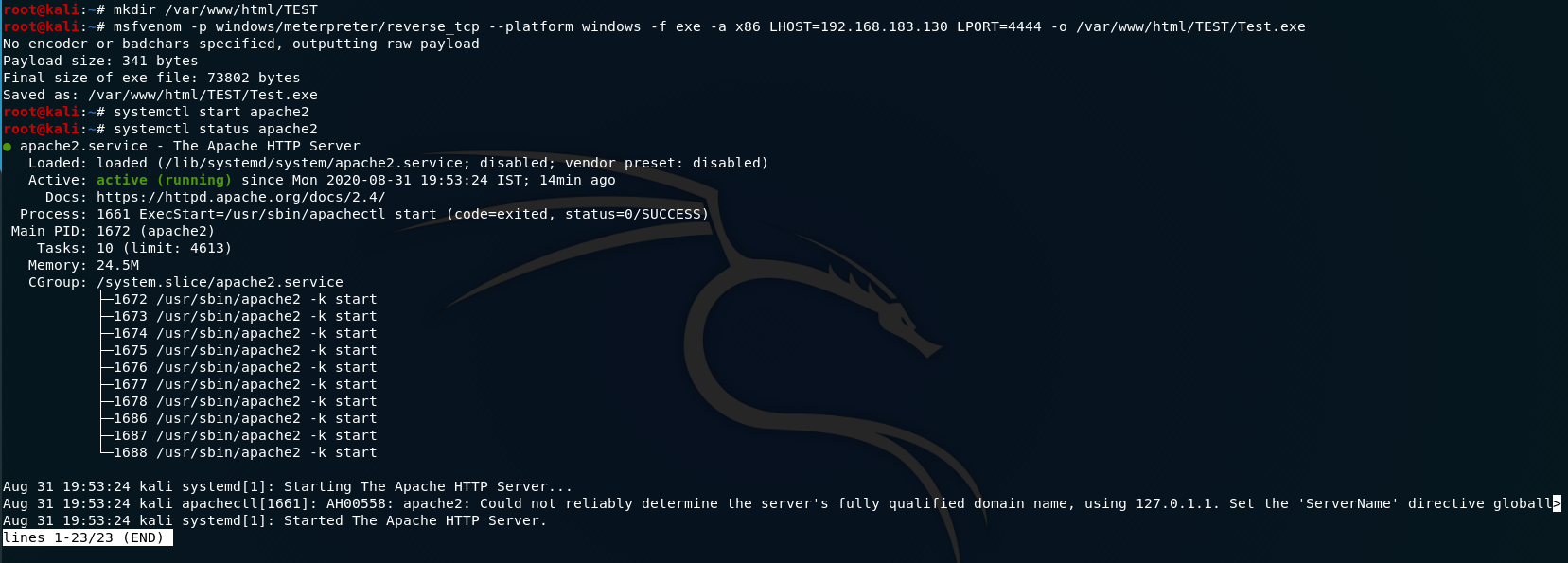
● Exploit the victim's machine.

**Answer 1:**

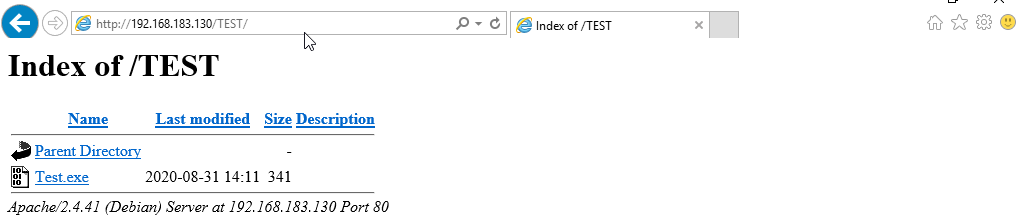
Steps: Check your IP using ifconfig command.



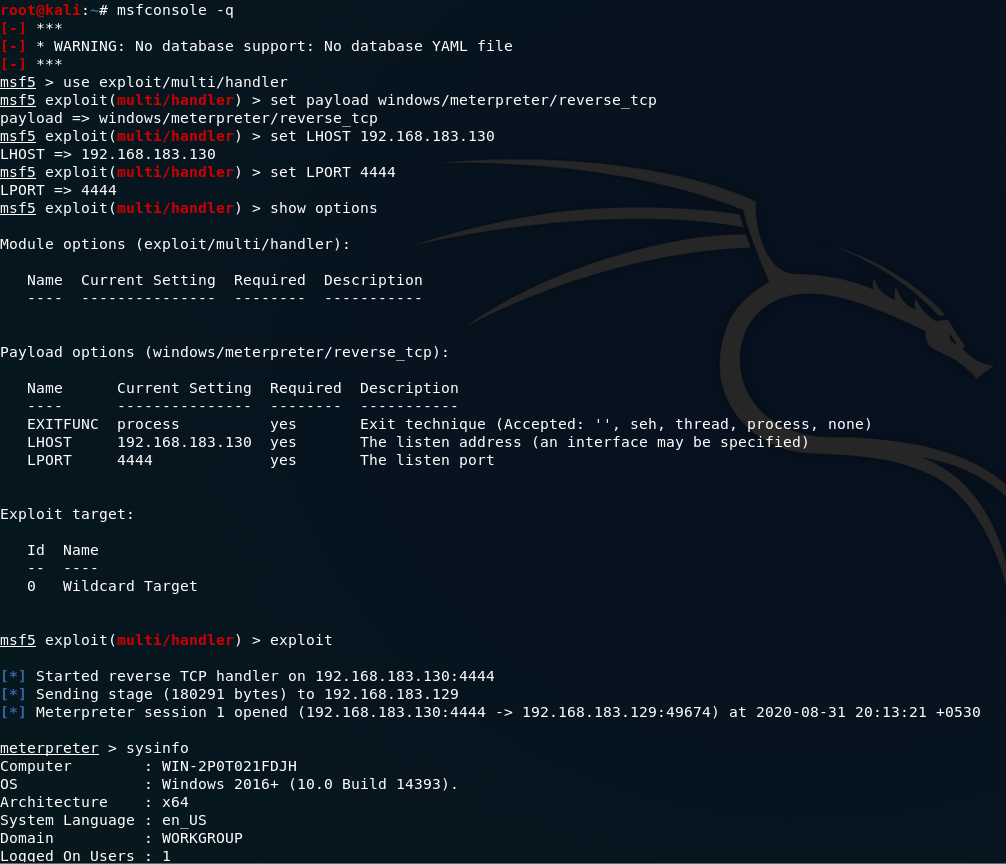
* Create a Payload.
* And Start web server.



Download Payload in Victim machine using machine attacker machine webpage.



* Open Metasploit console and set multi handler.
* Set payload that you created using set command.
* Set LHOST and LPORT.
* Exploit using exploit command.



**Question 2.**

● Create an FTP server

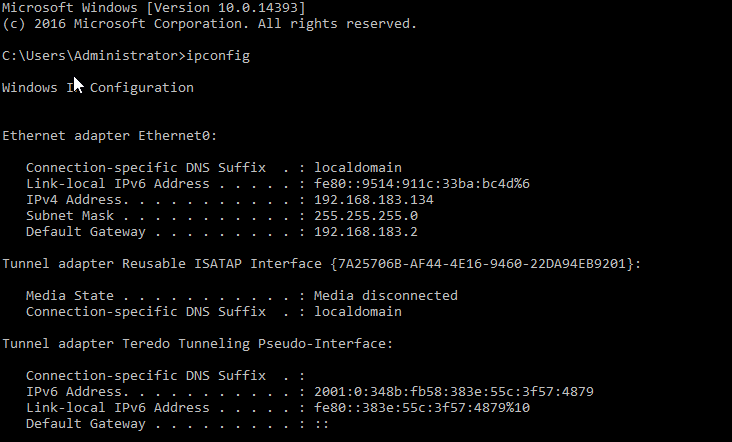
● Access FTP server from windows command prompt

● Do a mitm and username and password of FTP transaction using wireshark and dsniff.

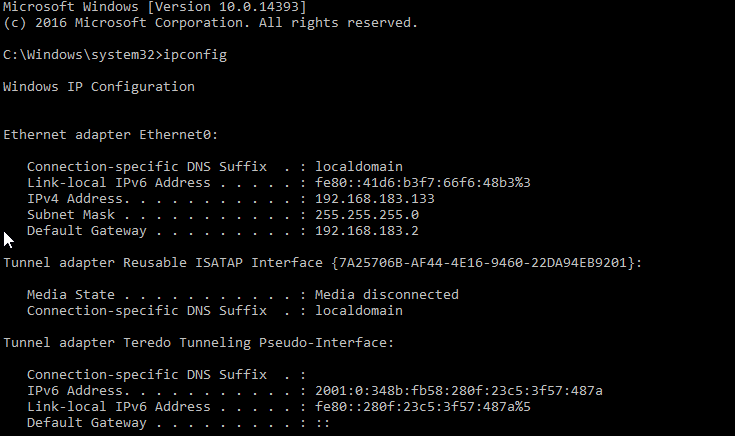
**Answer 2:**

Made an ftp server using manage and tools option in the windows server manager.

Checked the ips of the ftp machine and the machine which was supposed to be connected to it as shown in images below.

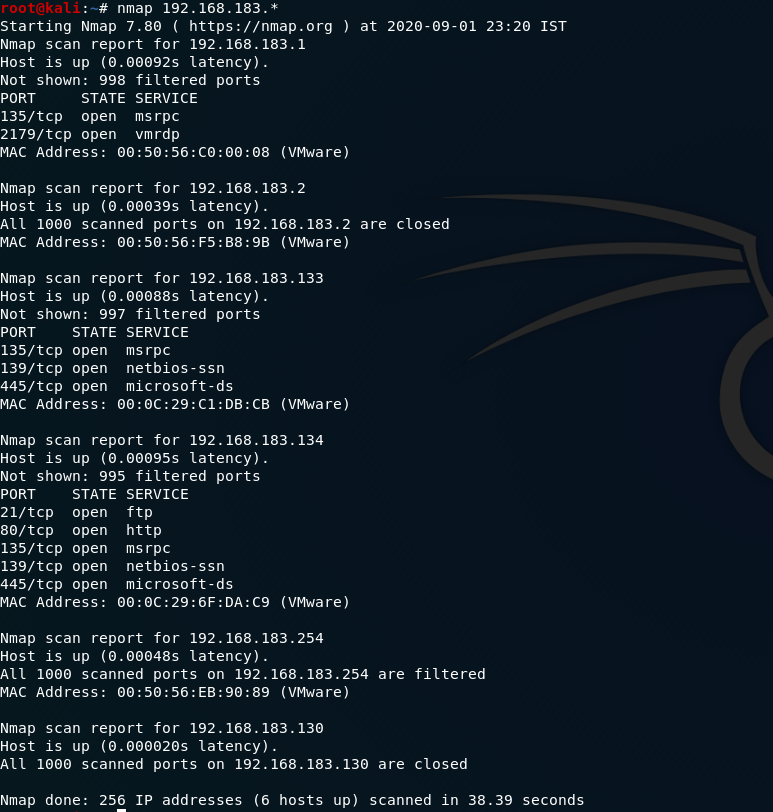


**FTP Server**



**Machine that was connected**

Nmap the full network using nmap 192.168.183.\*.



From nmap scan I got the target ip on which ftp is open that is 192.168.183.134 and the ip which is going to connect it is 192.168.183.133

**Configured the kali machine to forward the packet through it using commands:**

echo 1 > /proc/sys/net/ipv4/ip\_forward

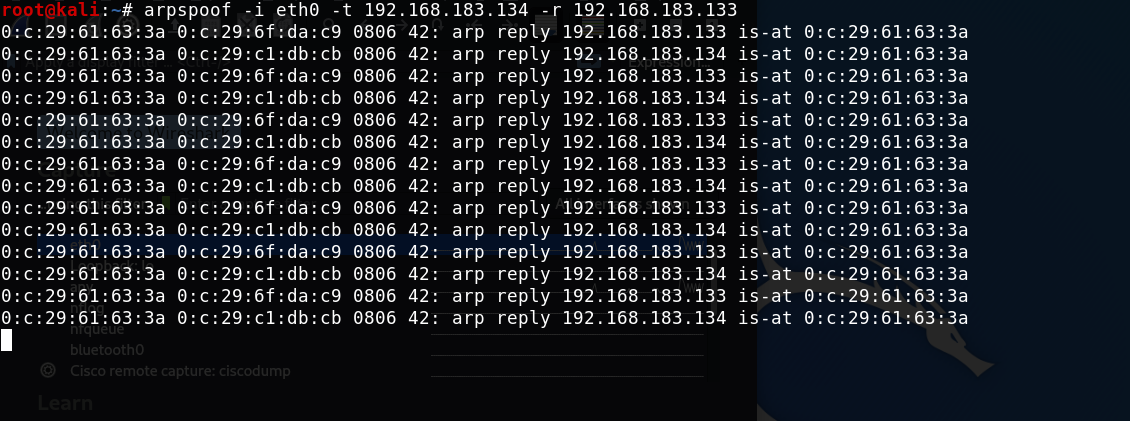
sysctl -w net.ipv4.ip\_forward=1

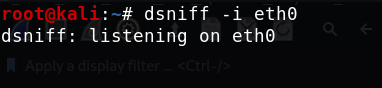
C:\Users\lokes\AppData\Local\Packages\Microsoft.Office.Desktop_8wekyb3d8bbwe\AC\INetCache\Content.Word\packet.png

**Started the arp spoffer and dsniff using**

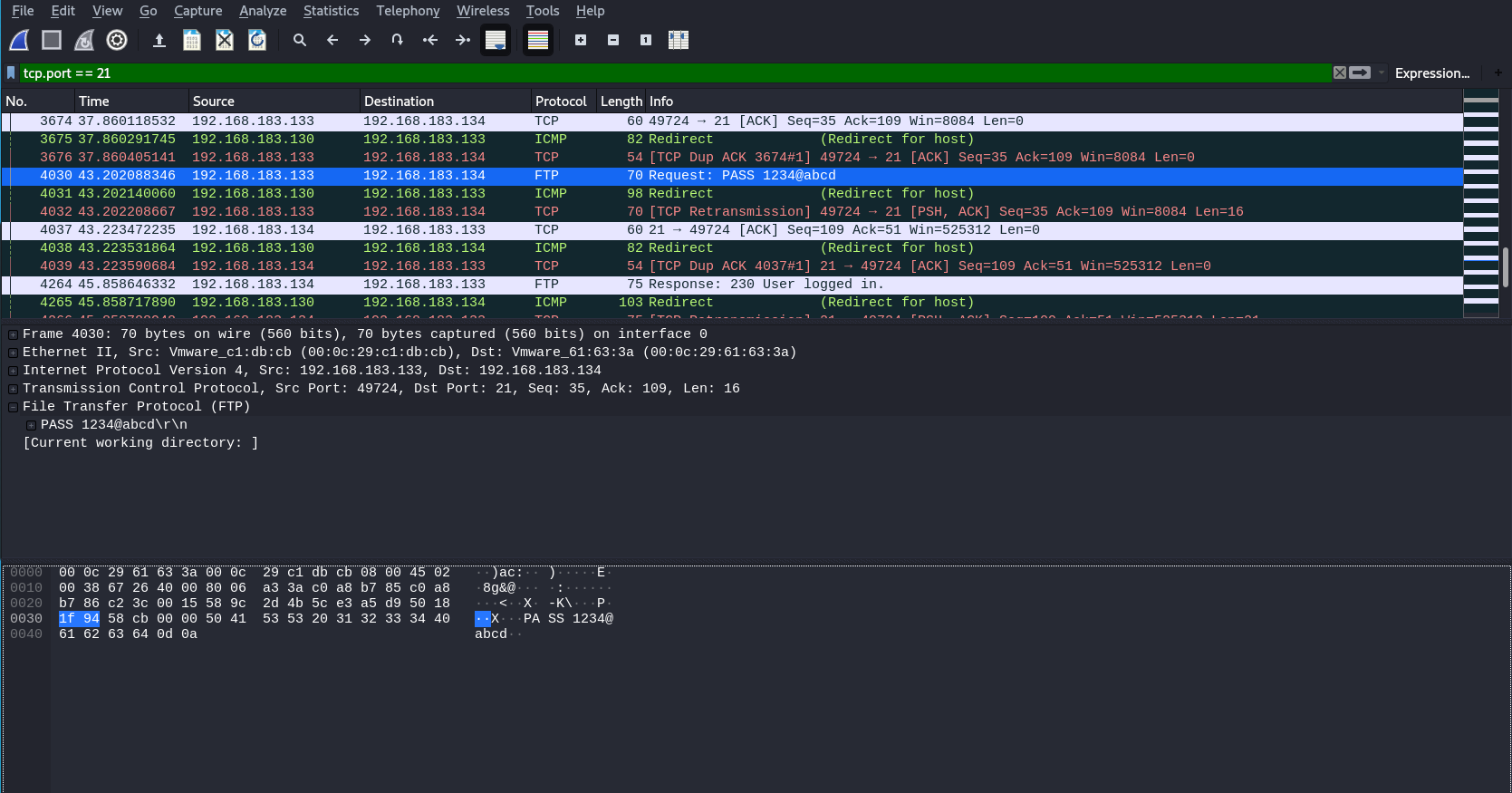
arpspoof -i eth0 -t 192.168.183.134 -r 192.168.183.134

dsniff -i eth0





**Used the wireshark to get the password which is shown in image below**



Got password as 1234@abcd

**Thank You**