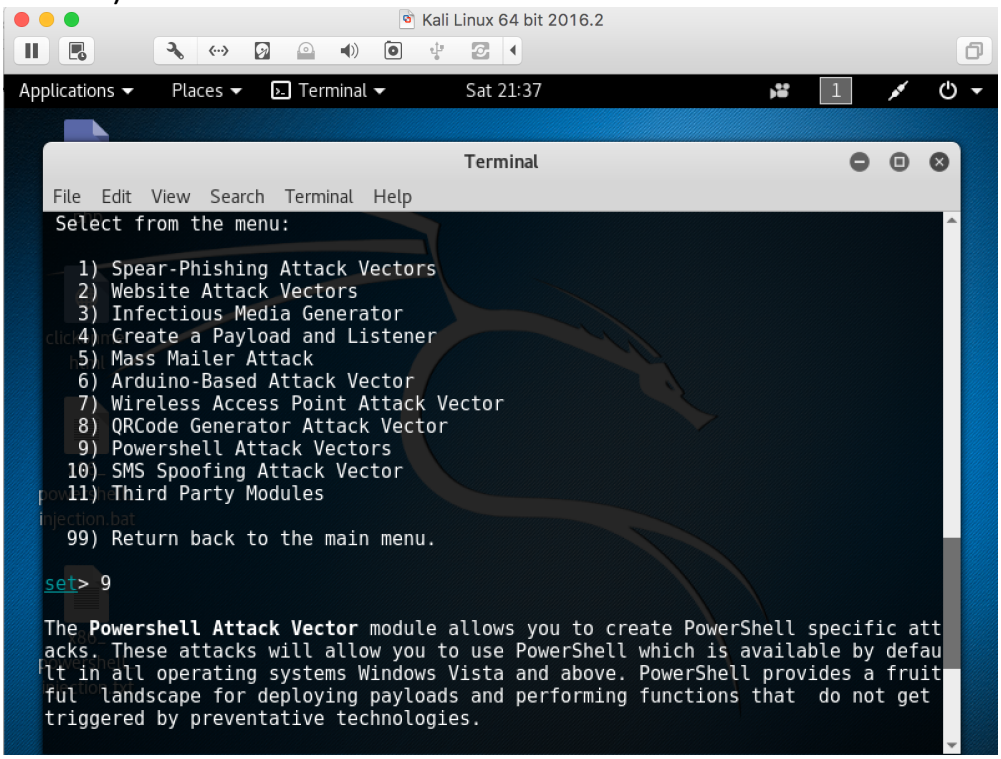
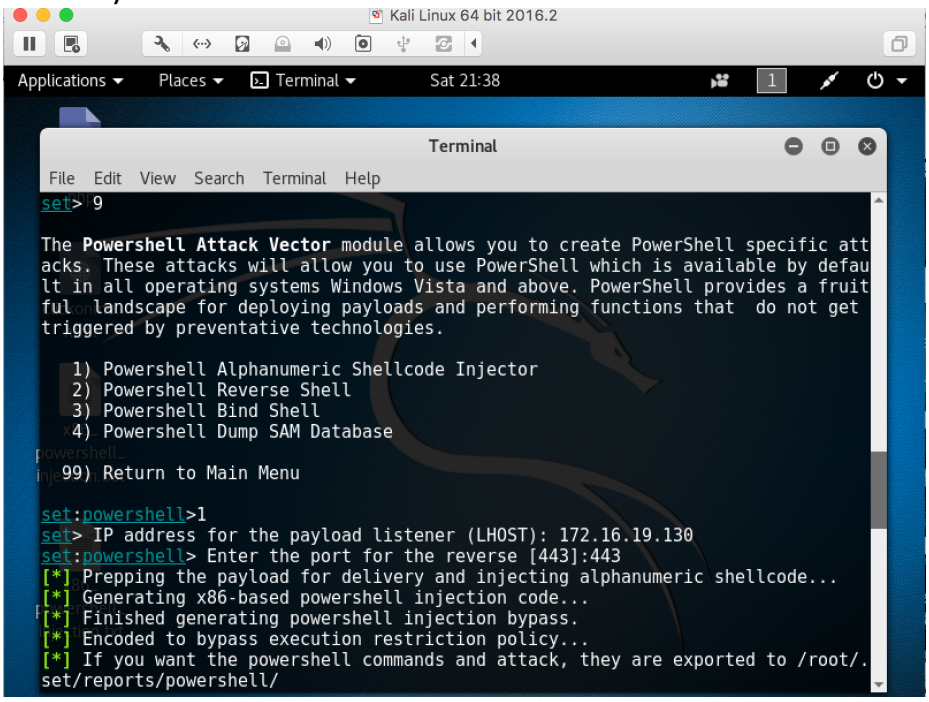
Powershell Attack Vectors

In Kali Linux, goto Applications -> Social Engineering -> SET.
Enter 9)

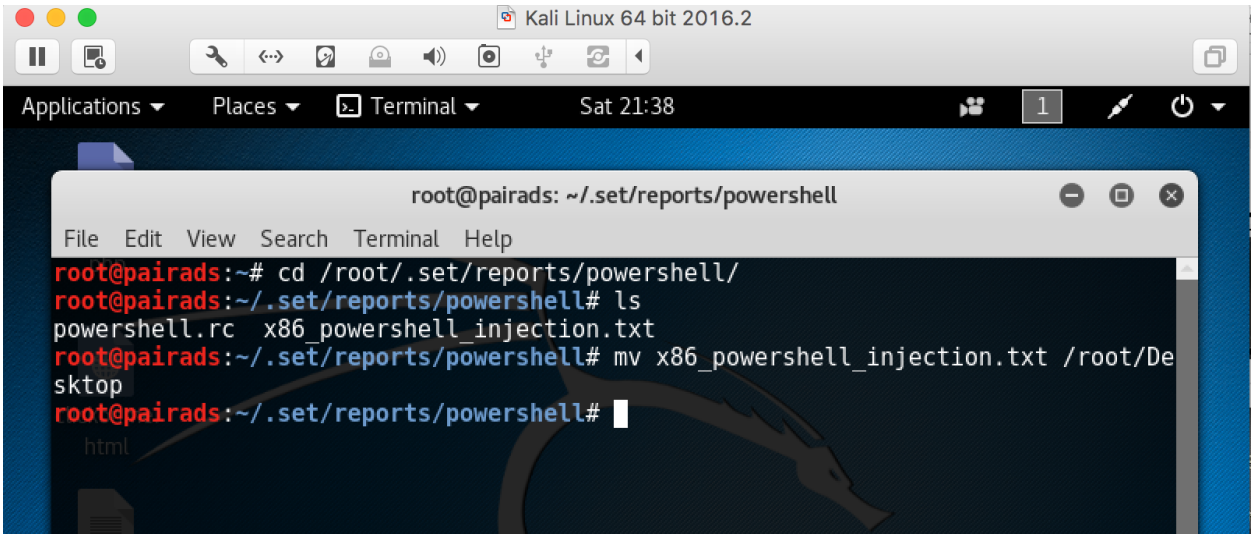


Enter 1)

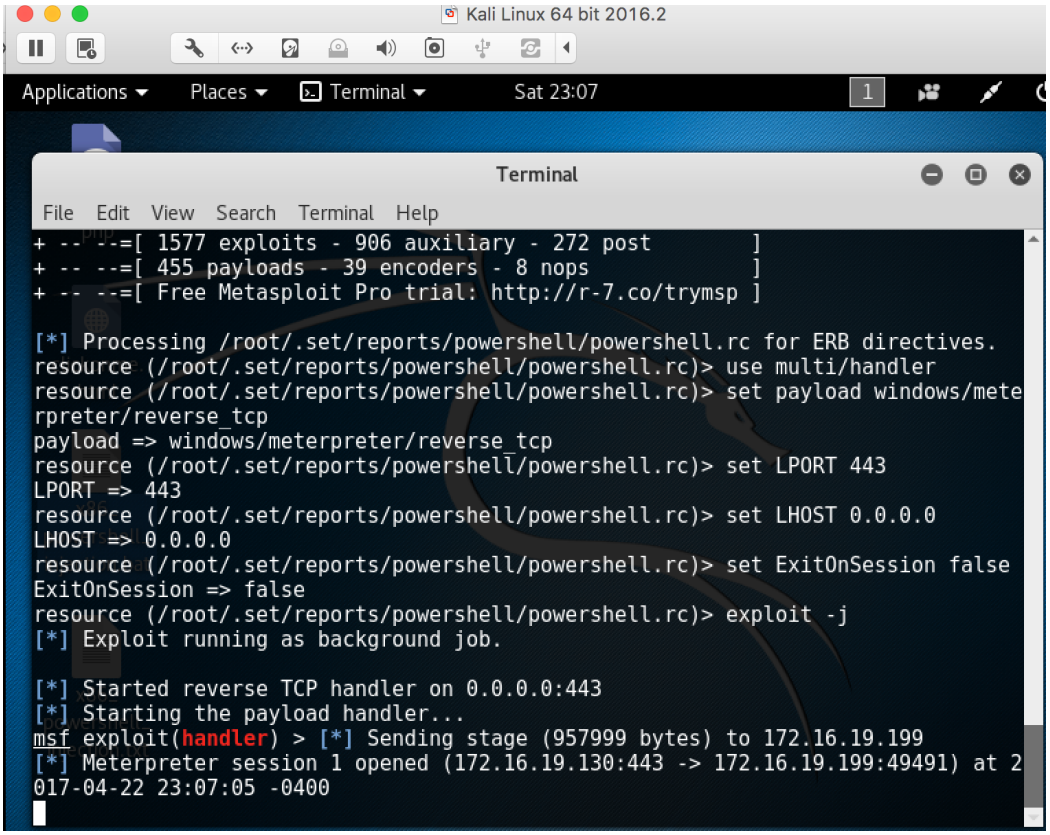


Enter the IP address of your Kali Linux and port as 443 which is the default port.

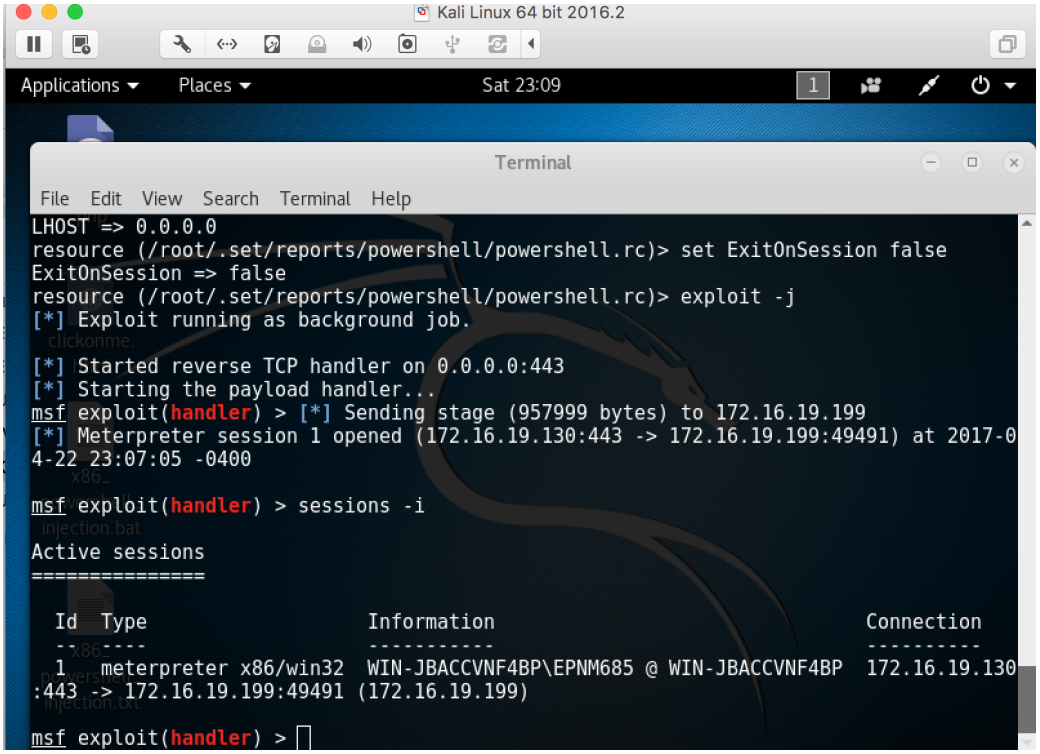
It generates a powershell file at location /root/.set/reports/powershell/ . Copy this file to your desktop. Next copy this file to the victim machine in our case being Windows 7 virtual machine and save it as a batch file. You can use phishing techniques to have this .bat file mailed to the victim and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



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.



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



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.