**EXPERIMENT – 07**

**AIM – To implement different commands using Metasploit.**

**Theory**

The Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers. Because it’s an open-source framework, it can be easily customized and used with most operating systems.

Metasploit now includes more than 1677 exploits organized over 25 platforms, including Android, PHP, Python, Java, Cisco, and more. The framework also carries nearly 500 payloads, some of which include:

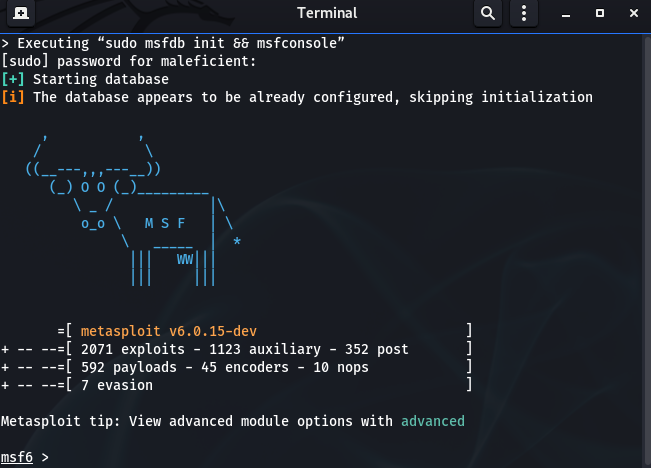
* Command shell payloads that enable users to run scripts or random commands against a host
* Dynamic payloads that allow testers to generate unique payloads to evade antivirus software
* Meterpreter payloads that allow users to commandeer device monitors using VMC and to take over sessions or upload and download files
* Static payloads that enable port forwarding and communications between networks.

**Steps to perform basic commands**:

1. First of all, open the Metasploit console in Kali. You can do so by following the path: Applications → Exploitation Tools → Metasploit.



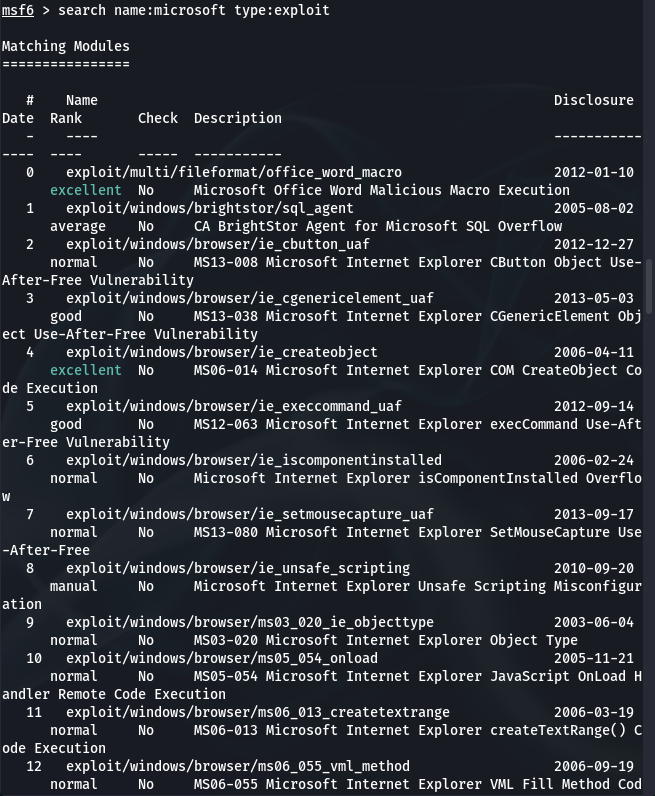
1. Once you open the Metasploit console, you will get to see the following screen. Highlighted in red underline is the version of Metasploit.



1. Help command



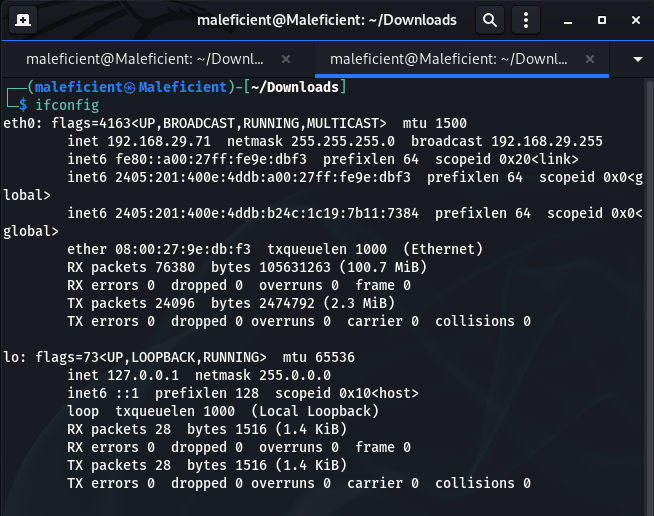
1. Search Command



1. Info Command

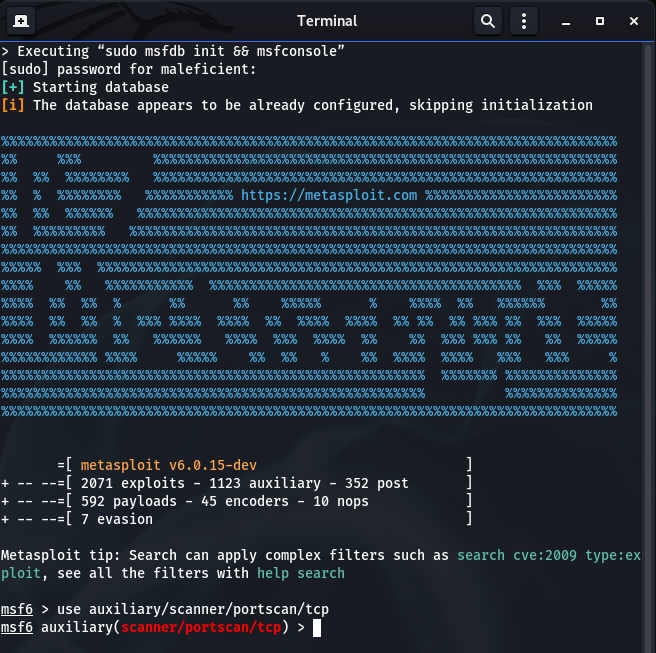


**Steps to Perform Scanning for open ports on the client machine with Metasploit**:



1. We start by launching Metasploit and using the port scanner module.

Msf5 > use auxiliary/scanner/portscan/tcp

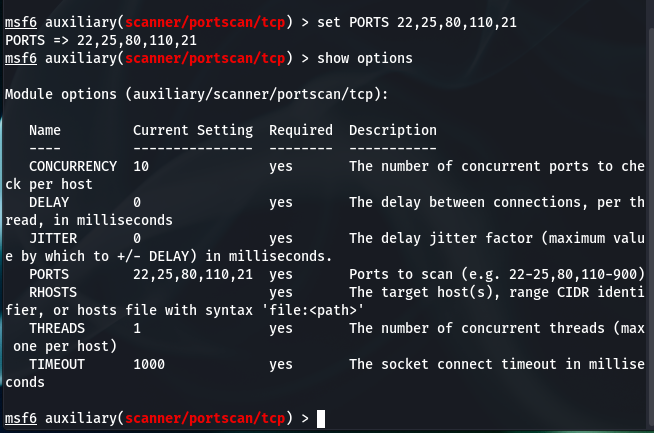


1. We set the options for this module with ‘show option’.



1. We set the RHOSTS with the IP/IP(s) of our client machine and if we want to customize the scan for specific ports we can do that by changing ports.

Msf5> set PORTS 22,25,80, 110, 21

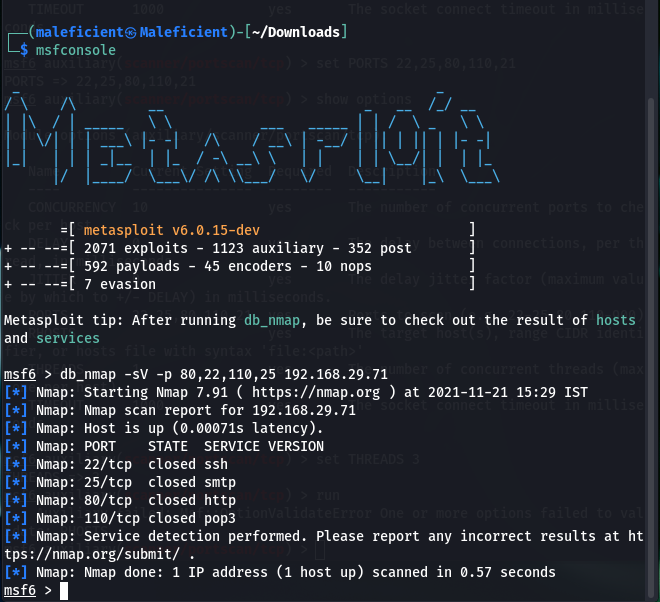


1. After running scan we will have an output displaying the open ports on the target client machine we specified earlier.

**Combining NMAP with Metasploit for a more detailed and in- depth scan on the client machine**:

We can start enumerating the ports to see and fine the running services alongside their version.

Msf5> db\_nmap -sV -p 80,22,110, 25 IP address.



**Scanning for vulnerabilities with Nmap and Metasploit**:

Msf5> dp\_nmap -sV -A -p 80,22,110,25 IP address.

