Ex. No. 10	Creating Payload using Metasploit
Date of Exercise	8/11/23

Aim:

The objective of this experiment is to:

Nmap: Discover your network. Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Using Nmap find the vulnerable ports and then using metasploit framework exploit it and list it.

Lab Environment:

To carry out the Experiment, you need:

- Penetration testing operating system [Kali Linux / parrot]
- Web browser with Internet access
- Administration privileges to run the tools

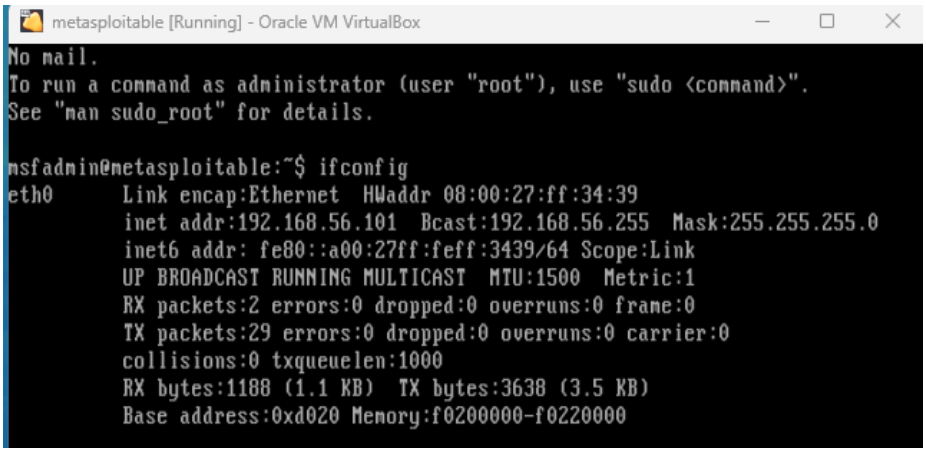
Description:

The Metasploit Framework is a widely used penetration testing and exploitation tool that includes a variety of tools and utilities for finding, exploiting, and managing security vulnerabilities in computer systems and networks. The Metasploit Framework has a database

component known as the Metasploit database or MSF database. This database is an integral part of the Metasploit Framework.

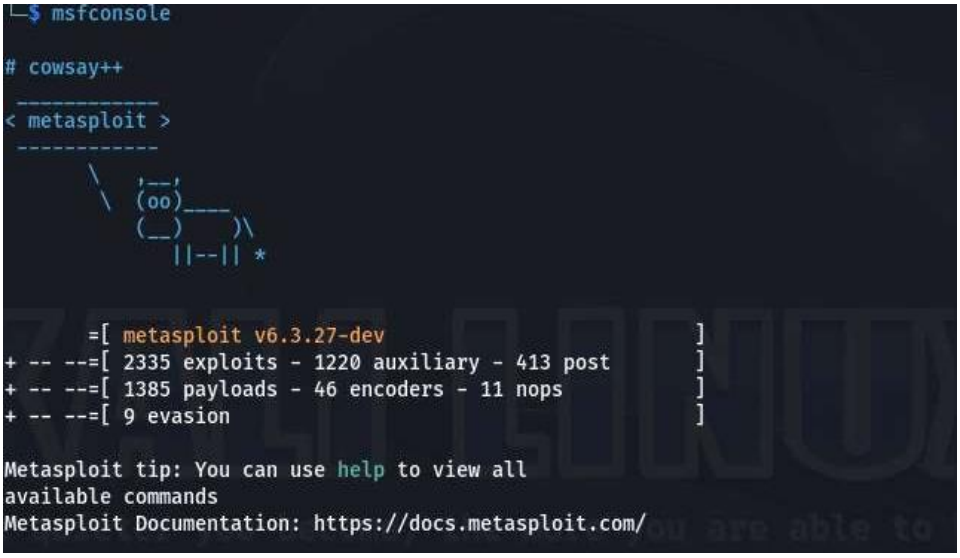
Implementation:

1. Set Up Metasploitable2 VM and get its IP address.

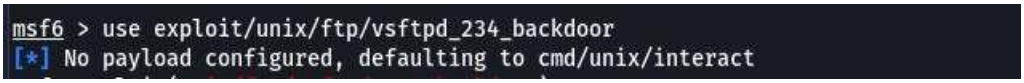


2. Open kali terminal and run nmap to find vulnerabilities in metasploitable vm

3. Fire up Metasploit using msfconsole



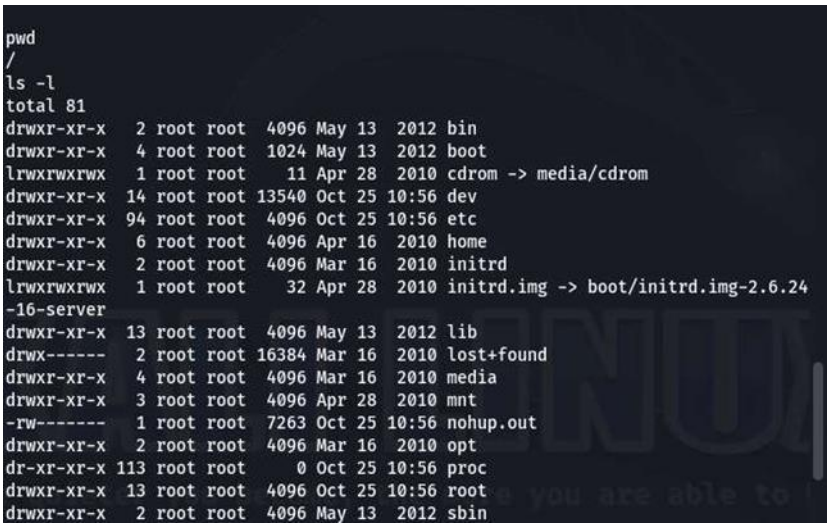
4. Use vsftpd exploit to gain access to the victims file system.



5. Set RHOST

6. Start the exploit to open the command shell.

7. List the files present in the root directory.



Result:

The objective of creating payload using Metasploit was done successfully.