Metasploit

Metasploit is an open-source penetration testing framework used for developing, testing, and executing exploits against remote targets. It is widely regarded as a powerful tool for cybersecurity professionals, ethical hackers, and penetration testers to identify, validate, and exploit vulnerabilities in a network or system.

Key Functionalities

- **Exploitation**: Automates the process of exploiting known vulnerabilities in various systems.
- **Post-Exploitation**: Facilitates further exploitation and information gathering after initial access is gained.
- **Payload Generation**: Generates custom payloads that can be used with exploits to control the compromised system.
- **Auxiliary Tools**: Offers tools for network discovery, fingerprinting, brute-forcing, and vulnerability scanning.
- **Database Integration**: Supports integration with databases like PostgreSQL to store scan results, information about targets, and track the progress of penetration testing engagements.

How to Use Metasploit

1. **Install Metasploit**: It can be installed on various operating systems, including Kali Linux, Ubuntu, and Windows.
2. **Start the Framework**: Use msfconsole, the command-line interface of Metasploit, to start the framework.
3. **Search for Exploits**: Use the search command to find exploits for specific vulnerabilities.
4. **Configure the Exploit**: Set the necessary options, such as the target IP address and payload.
5. **Run the Exploit**: Use the run or exploit command to execute the exploit against the target.
6. **Post-Exploitation Activities**: Perform further actions like privilege escalation, data exfiltration, or maintaining access.

Advantages

- **Comprehensive**: Contains a large number of pre-built exploits and payloads.
- **Extensible**: Users can write and integrate their modules.
- **Community-Driven**: Regularly updated by a large community of contributors.
- **Cross-Platform**: Works on different operating systems and targets.

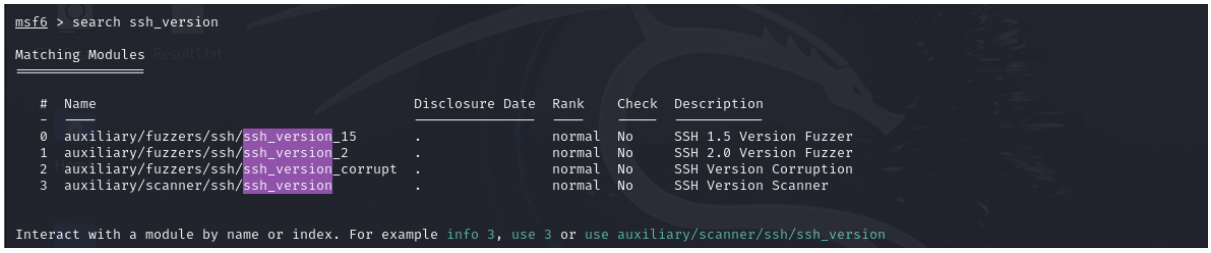
Disadvantages

- **Risk of Misuse**: Can be used by malicious actors for unethical purposes.
- **Resource-Intensive**: Some operations may consume significant system resources.
- **Requires Expertise**: Understanding the framework and its modules requires a good grasp of cybersecurity concepts.

Commands:

- Command: ***search ssh_version***

This command searches for the ssh versions available in Metasploit



use auxiliary/scanner/ssh/ssh_version

used to identify the version of the SSH server running on a remote system.

- **Options**

  if we look at **options** then we can see the module options.

Since RHOST is not set, we set the Ip of the target machine.

```
msf6 auxiliary(scanner/ssh/ssh_version) > set RHOSTS 192.168.80.133
RHOSTS ⇒ 192.168.80.133
```

Setting **THREADS** to 100 means that the module will use 100 concurrent threads to perform its operations (like scanning or exploiting).

When **'run'** command is given, it starts performing the actions defined by that module — such as scanning for vulnerabilities, gathering information, or exploiting a target.