Notes on Using Metasploit

1. Reconnaissance

Before using Metasploit, gather information about the target:

- Use tools like **nmap** to scan for open ports and services.
- Use **whois**, **dig**, and **nslookup** for domain information.
- Identify possible vulnerabilities using tools like **Nessus** or **OpenVAS**.

2. Finding Vulnerabilities

- Use **searchsploit** to find vulnerabilities related to the software and services identified.
- In Metasploit, use the **search** command to look for related exploits.

3. Selecting and Configuring Exploits

- After selecting an exploit with **use**, configure it by setting required options like **RHOST**, **LHOST**, and **PAYLOAD**.
- Use **show targets** to see available targets if the exploit supports multiple ones.

4. Exploitation

- Once configured, launch the exploit using the **exploit** command.
- If the exploit is successful, it will provide you with a session (like a Meterpreter shell).

5. Post-Exploitation

- Explore the target system with commands like **sysinfo**, **ps**, and **hashdump**.
- Maintain access by adding a user or using persistence scripts.

6. Cleanup

- After the session, ensure you clean up by removing any traces of your presence (e.g., deleting logs, closing sessions).

7. Reporting

- Document the vulnerabilities found and the steps taken to exploit them.
- Provide mitigation recommendations for each vulnerability.

---

1. Searchsploit

- **Context**: Command-line tool outside Metasploit.
- **Purpose**: Searches the local Exploit Database (Exploit-DB) for exploits and vulnerabilities related to the software or services you specify.
- **Usage**:

```
searchsploit <keyword>
```

Example:

```
searchsploit apache
```

- **Features**:
  - Allows you to find exploits and proof-of-concept code from the Exploit-DB repository.
  - Provides local access to Exploit-DB without needing an internet connection.
  - Shows details like the type of exploit, platform, and file path.

2. Search (in Metasploit)

- **Context**: Used within the Metasploit Framework (msfconsole).
- **Purpose**: Searches Metasploit's own database for modules (exploits, payloads, auxiliary modules, etc.) related to the keyword you specify.
- **Usage**:

```
search <keyword>
```

Example:

```
search apache
```

- **Features**:
  - Allows you to directly find and use Metasploit modules related to vulnerabilities.
  - Provides an easy way to integrate found exploits into Metasploit workflows.
  - Supports advanced search features like searching by CVE, author, and platform.