**EXPERIMENT NUMBER 3**

| Name of Student: Sangeet Agrawal | PRN: 21070122140 | Section: CS-B |
| --- | --- | --- |

**Title:** Metasploit Framework for client and server exploitation

**Aim:** Demonstration of Network Security tools/frameworks like Metasploit.

**Objective:** To demonstrate scanning and exploitation of vulnerable OS using the Metasploit framework.

**Theory: [Source:** [**https://www.varonis.com/blog/what-is-metasploit**](https://www.varonis.com/blog/what-is-metasploit)**]**

Using pen-testing tools, white hats, and DevSec professionals are able to probe networks and applications for flaws and vulnerabilities at any point along the production and deployment process by hacking the system.

One such penetration testing aid is the Metasploit Project. This Ruby-based open-source framework allows testing via command line alterations or GUI. It can also be extended through coding to act as an add-on that supports multiple languages.

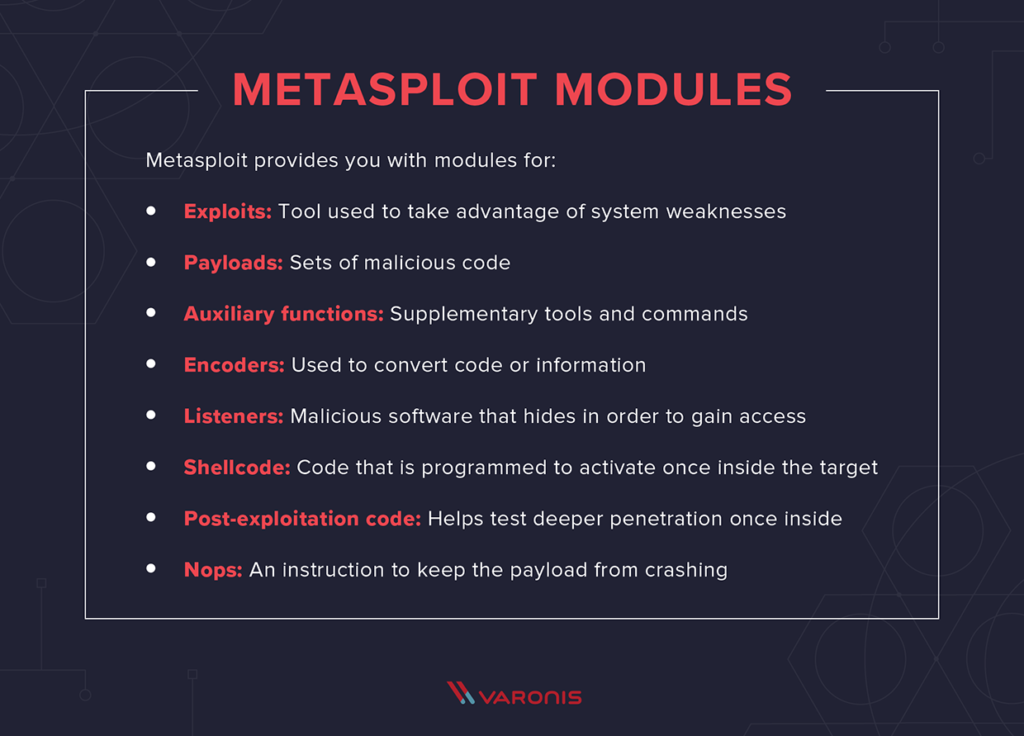
The Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers. Because it’s an open-source framework, it can be easily customized and used with most operating systems.

With Metasploit, the pen testing team can use ready-made or custom code and introduce it into a network to probe for weak spots. As another flavor of threat hunting, once flaws are identified and documented, the information can be used to address systemic weaknesses and prioritize solutions.

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:

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

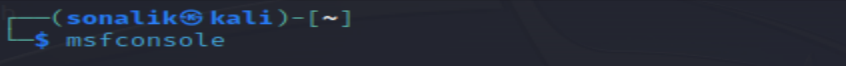
The below diagram shows details of various Metasploit modules.



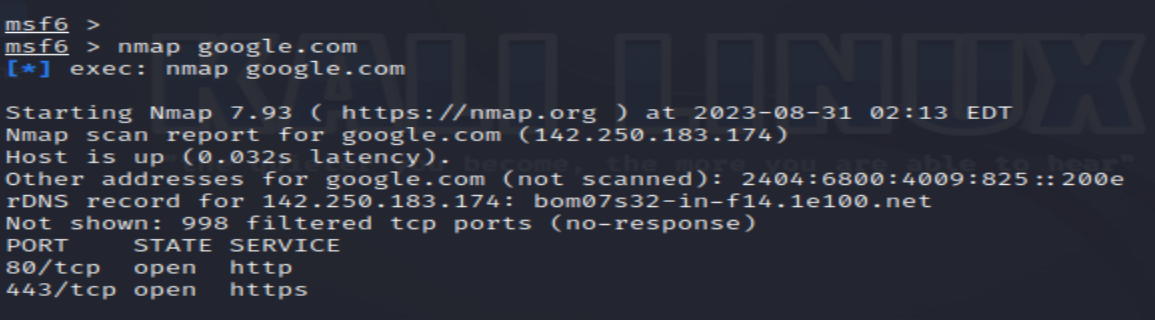
**Demonstration:**

For demonstration, KAli or Parrot OS is used as attacker while Metasploitable2 OS is used as victim.

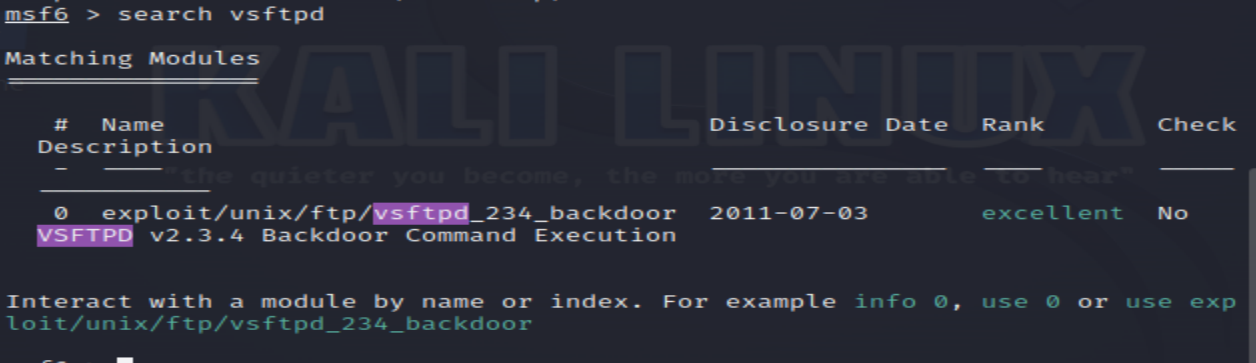
1. Start Metasploit using below command on attacker machine:



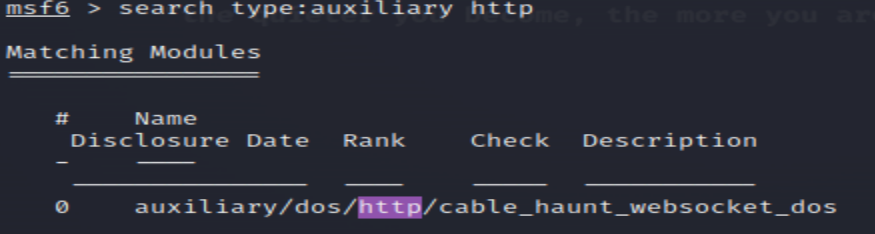
1. nmap command on msfconsole for domain scanning



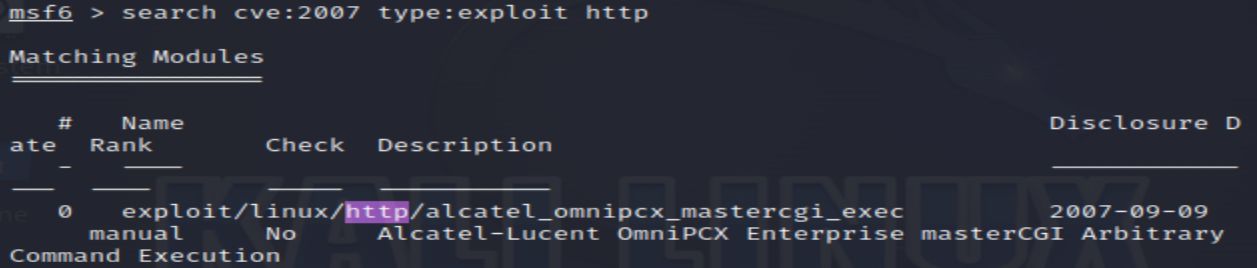
1. search command to find auxiliary and exploits



1. To search auxiliary having some particular keyword



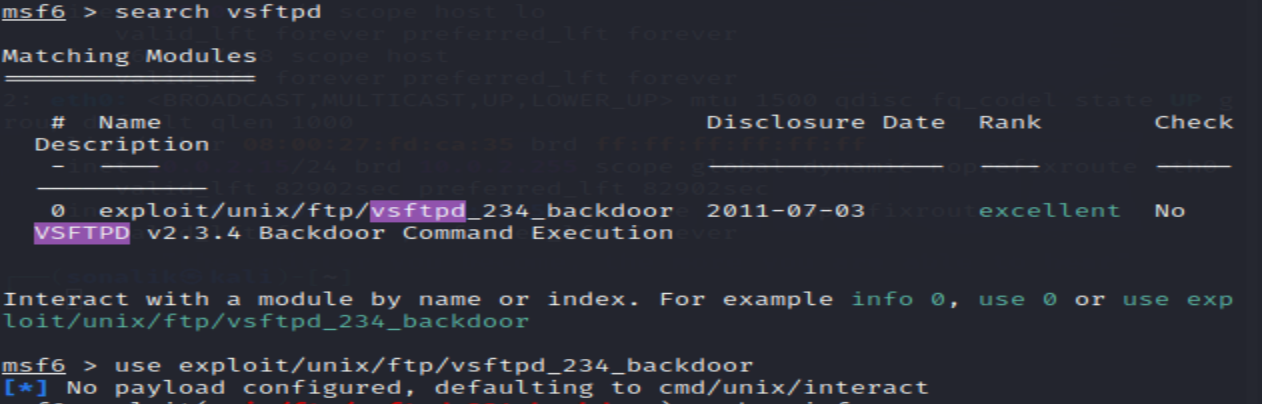
1. To search any exploit using cve id

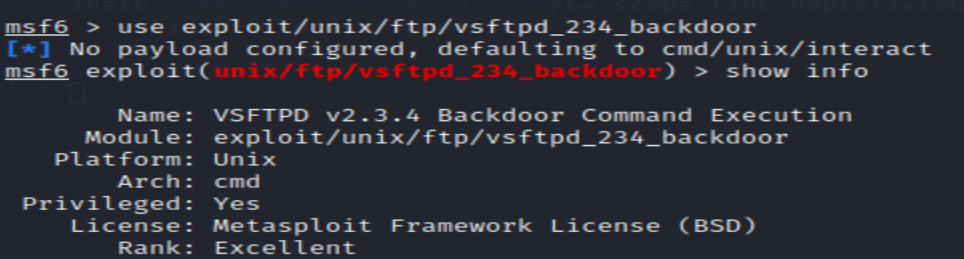


1. To use vsftpd exploit for exploiting victim machine

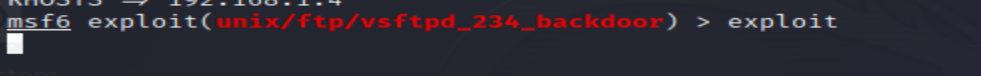
* Here, **search** command is used to find exploit
* **use** command is used for working with the exploit.
* **show info** command gives details about the auxiliary or exploit.
* **show options** command will give mandatory options
* **show missing**  will show the details of missing options which is mandatory to provide
* **SET RHOSTS 192.168.1.4** - sets host value to victim ip address. Here it is 192.168.1.4

This will establish session with the vulnerable OS and attacker can access details of the victim machine.









**Reference Book:** <https://www.researchgate.net/publication/327572223_Metasploit_Penetration_Testing_Cookbook_-_Third_Edition>

**Documentation:** <https://docs.metasploit.com/>

**Conclusion:**

**Implementation question:**

1. Refer to Chapter 3 from the above-mentioned reference book and perform Linux server Exploitation. Paste screenshots to demonstrate all required commands used.
2. Refer to Chapter 7 from the above-mentioned reference book and perform Client-side Exploitation. Paste screenshots to demonstrate all required commands used.

**Implementation Screenshots:**

