

# Metasploit

learnt,

- What is Metasploit, advantages and disadvantages.
- Learnt how to scan the ssh port and learn / gather information about the target IP address.

## Gathering information about TCP open ports by scanning the target machine:

- **use auxiliary/scanner/portscan/tcp**

Used to perform a TCP port scan on a specified target or range of targets. It scans for open TCP ports by attempting to connect to them, which helps identify which services are running on the target systems.

```
msf6 > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > options

Module options (auxiliary/scanner/portscan/tcp):
```

| Name        | Current Setting | Required | Description   |
|-------------|-----------------|----------|---|
| CONCURRENCY | 10              | yes      | The number of concurrent ports to check per host  |
| DELAY       | 0               | yes      | The delay between connections, per thread, in milliseconds  |
| JITTER      | 0               | yes      | The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.  |
| PORTS       | 1-10000         | yes      | Ports to scan (e.g. 22-25,80,110-900)   |
| RHOSTS      |                 | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| THREADS     | 1               | yes      | The number of concurrent threads (max one per host)   |
| TIMEOUT     | 1000            | yes      | The socket connect timeout in milliseconds  |

View the full module info with the `info`, or `info -d` command.

- **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/portscan/tcp) > set RHOSTS 10.10.10.10
RHOSTS => 10.10.10.10
msf6 auxiliary(scanner/portscan/tcp) > set THREADS 100
THREADS => 100
```

(Hidden IP for Safety)

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.

```
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 192.168.1.1 - 192.168.1.1:23 - TCP OPEN
[+] 192.168.1.1 - 192.168.1.1:22 - TCP OPEN
[+] 192.168.1.1 - 192.168.1.1:21 - TCP OPEN
[+] 192.168.1.1 - 192.168.1.1:25 - TCP OPEN
[+] 192.168.1.1 - 192.168.1.1:53 - TCP OPEN
[+] 192.168.1.1 - 192.168.1.1:80 - TCP OPEN
[+] 192.168.1.1 - 192.168.1.1:111 - TCP OPEN
[+] 192.168.1.1 - 192.168.1.1:139 - TCP OPEN
[+] 192.168.1.1 - 192.168.1.1:445 - TCP OPEN
[+] 192.168.1.1 - 192.168.1.1:512 - TCP OPEN
[+] 192.168.1.1 - 192.168.1.1:513 - TCP OPEN
[+] 192.168.1.1 - 192.168.1.1:514 - TCP OPEN
[+] 192.168.1.1 - 192.168.1.1:1099 - TCP OPEN
[+] 192.168.1.1 - 192.168.1.1:1524 - TCP OPEN
[+] 192.168.1.1 - 192.168.1.1:2049 - TCP OPEN
[+] 192.168.1.1 - 192.168.1.1:2121 - TCP OPEN
[+] 192.168.1.1 - 192.168.1.1:3306 - TCP OPEN
[+] 192.168.1.1 - 192.168.1.1:3632 - TCP OPEN
[+] 192.168.1.1 - 192.168.1.1:5432 - TCP OPEN
[+] 192.168.1.1 - 192.168.1.1:5900 - TCP OPEN
[+] 192.168.1.1 - 192.168.1.1:6000 - TCP OPEN
[+] 192.168.1.1 - 192.168.1.1:6667 - TCP OPEN
[+] 192.168.1.1 - 192.168.1.1:6697 - TCP OPEN
[+] 192.168.1.1 - 192.168.1.1:8009 - TCP OPEN
[+] 192.168.1.1 - 192.168.1.1:8180 - TCP OPEN
[+] 192.168.1.1 - 192.168.1.1:8787 - TCP OPEN
[*] 192.168.1.1 - Scanned 192.168.1.1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) >
```

## Use of Other commands:

- **use auxiliary/scanner/portscan/syn**

This performs a SYN scan (also known as a half-open scan) on a specified target or range of targets which is much more stealthier.

- **Use auxiliary/scanner/portscan/ack**

This command is used to perform ack scan to map out firewall rules and determine which ports are filtered.