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:

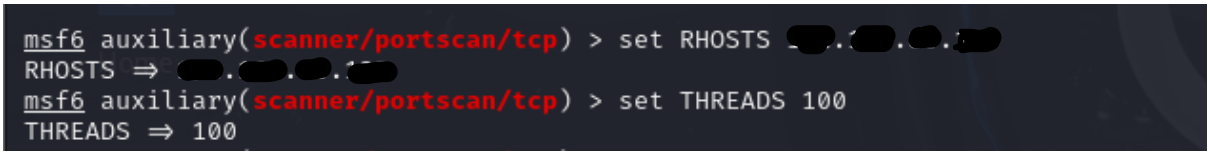
- **use auxiliary/scanner/portscan/tcp**

  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.

- **Options**

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

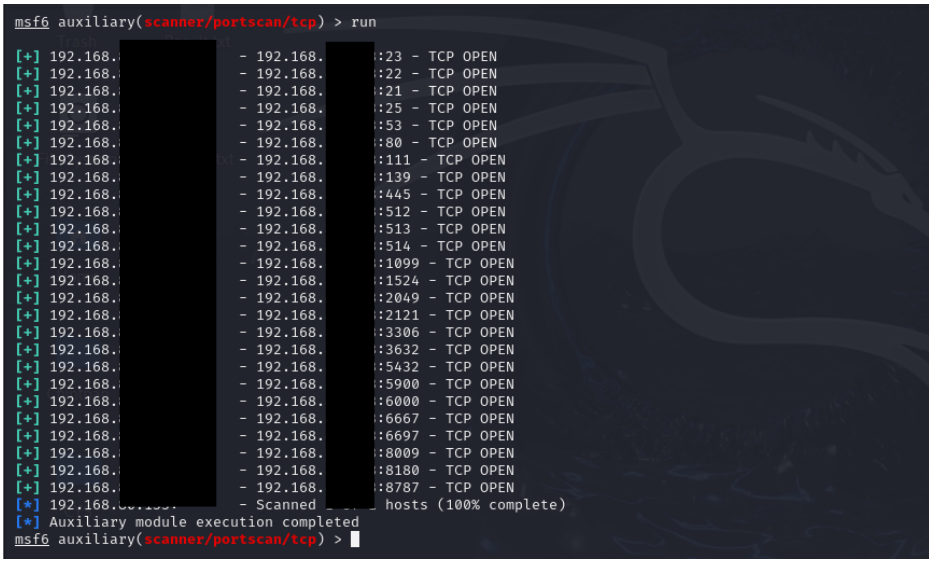
  Since RHOST is not set, we set the Ip of the target machine.



  (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.



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.