

Metasploit- Auxiliary Scan

An auxiliary scan in the context of Metasploit refers to the process of using auxiliary modules to gather information about a target network or system without exploiting vulnerabilities. Unlike exploit modules, which are designed to exploit vulnerabilities and gain unauthorized access, auxiliary modules perform a variety of tasks such as network scanning, service enumeration, vulnerability assessment, and information gathering. These modules help security professionals and penetration testers to map out the network, identify active hosts, determine the services and versions running on those hosts, and uncover potential security issues that need attention. For example, an auxiliary scan can be used to detect open ports, identify operating system versions, discover network shares, and even check for weak passwords. This information is crucial for understanding the target environment and planning further penetration testing activities. Auxiliary scans are a fundamental part of the reconnaissance phase in a security assessment, providing a comprehensive overview of the target's security posture without causing disruption or alerting the target.

Example: -

1. Firstly, open the msfconse inside the terminal.

[illegible]

2. Now we will list all the auxiliary by using show auxiliary command.

[illegible]

3. Now out of list we have to choice scanner/portscan/tcp option.

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

Name: TCP Port Scanner
Module: auxiliary/scanner/portscan/tcp
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
  hdm <x@hdm.io>
  kris katterjohn <katterjohn@gmail.com>

Check supported:
  No

Basic options:


| 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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a> |
| THREADS     | 1               | yes      | The number of concurrent threads (max one per host)                                                                                                                             |
| TIMEOUT     | 1000            | yes      | The socket connect timeout in milliseconds                                                                                                                                      |



Description:
  Enumerate open TCP services by performing a full TCP connect on each port. This does not need administrative privileges on the source machine, which may be useful if pivoting.
```

4. Now we have to define our target.

```
msf6 auxiliary(scanner/portscan/tcp) > set RHOST 192.168.172.135
[-] Unknown datastore option: RHOST. Did you mean RHOSTS?
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.172.135
RHOSTS => 192.168.172.135
msf6 auxiliary(scanner/portscan/tcp) > set THREADS 50
THREADS => 50
```

5. At last use run command to perform the scan.

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

[*] 192.168.172.135: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) > =
```