Masscan

Masscan is a network port scanner, similar in many ways to the well-known Nmap command. The goal of Masscan, however, is to enable security researchers to run port scans on large swathes of the Internet as quickly as possible.

It is the fastest network port scanner. It can scan the whole internet under 6 minutes with 25 millions per second data transmitting speed.

Masscan uses it’s own custom TCP/IP stack. Anything other than a simple port scan may cause conflict with the local TCP/IP stack.

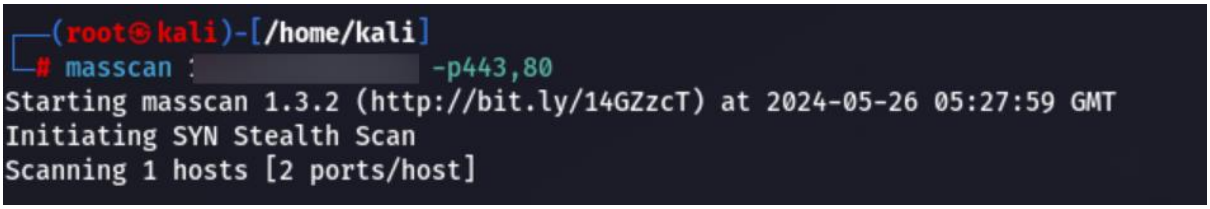
Usecase: -

- **Network Mapping and Inventory**: Organizations use Masscan to quickly map their networks, identifying live hosts and open ports. This helps in maintaining an accurate inventory of network devices and services.
- **Vulnerability Assessment**: Security professionals use Masscan to identify potentially vulnerable services that are exposed on the internet or within a network. This can be the first step in a more detailed vulnerability assessment process.
- **Compliance Audits**: Compliance requirements often necessitate regular scans of networked assets to ensure there are no unauthorized or unsecured services running. Masscan can perform these scans efficiently.
- **Research and Internet Measurement**: Researchers and organizations conducting large-scale internet measurements or studies on the deployment of internet services can use Masscan due to its ability to scan vast address spaces quickly.

Example: -

1. If you want to scan for a particular port then use -p flag along with that port number. Here I have scanned for the port 443.

2. Now we are going to scan for more than one port to do so we will use , in between two ports.



3. In order to scan for a range of ports we can use – in between two ports.

4. Scanning ports can take too long time as it sends various packets at a default speed of 100 packets per second. In order to do fast scanning I have set the sending speed at 2500000 packets per second by using –rate flag.