

Nmap Port Scanning

Nmap port scanning is a fundamental feature of Nmap used to identify open ports and services running on a target host or network. Port scanning helps network administrators, security professionals, and ethical hackers discover the various entry points into a system, assess the security posture of a network, and identify potential vulnerabilities.

Port scanning works by sending packets to specific ports on a target and analyzing the responses to determine the state of each port. Ports can be in various states such as open, closed, or filtered, indicating whether a service is listening, no service is present, or the port is being blocked by a firewall, respectively.

Port scanning with Nmap can be customized further with options to specify port ranges, set timing and performance parameters, and employ advanced techniques like version detection (-sV) and script scanning (-sC) to gather more detailed information about running services and potential vulnerabilities. This comprehensive approach makes Nmap an invaluable tool for network security assessments and management.

Examples: -

1. This command will scan port scan for defined port x.

```
(root@kali)-[/home/kali]
# nmap 192.168.1.1 -p 21
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-14 02:04 EDT
Nmap scan report for 192.168.1.1
Host is up (0.011s latency).

PORT      STATE SERVICE
21/tcp    open  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.51 seconds
```

2. This command will scan ports scan for defined range of port x.

```
(root@kali)-[/home/kali]
# nmap 192.168.1.1 -p 21-30
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-14 02:04 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0021s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    filtered ssh
23/tcp    filtered telnet
24/tcp    filtered priv-mail
25/tcp    filtered smtp
26/tcp    filtered rsftp
27/tcp    filtered nsw-fe
28/tcp    filtered unknown
29/tcp    filtered msg-icp
30/tcp    filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 1.46 seconds
```

3. This command is for port scan for multiple TCP and UDP ports.

```
(root@kali)~[/home/kali]
# nmap 192.168.1.1 -p U:53,T:21-25,80
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-14 02:05 EDT
WARNING: Your ports include "U:" but you haven't specified UDP scan with -sU.
Nmap scan report for 192.168.1.1
Host is up (0.0032s latency).

PORT      STATE      SERVICE
21/tcp    open      ftp
22/tcp    filtered  ssh
23/tcp    filtered  telnet
24/tcp    filtered  priv-mail
25/tcp    filtered  smtp
80/tcp    filtered  http

Nmap done: 1 IP address (1 host up) scanned in 1.47 seconds
```

4. This will scan for all the available 65535 ports. You can't be able to see the result below as I have stop the scan as it is going to scan all the ports which is very time consuming.

```
(root@kali)~[/home/kali]
# nmap 192.168.1.1 -p-
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-14 02:05 EDT

zsh: suspended  nmap 192.168.1.1 -p-
```

5. This will do a fast port scan for 100 ports.

```
(root@kali)~[/home/kali]
# nmap 192.168.1.1 -F
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-14 02:06 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0015s latency).
Not shown: 99 filtered tcp ports (no-response)
PORT      STATE      SERVICE
21/tcp    open      ftp

Nmap done: 1 IP address (1 host up) scanned in 2.09 seconds
```

6. Here port scanning is done from service name.

```
(root@kali)~[/home/kali]  
* nmap 192.168.1.1 -p http,https  
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-14 02:07 EDT  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 3.17 seconds
```