Title

“Local Network Port Scanning Using Nmap”

**What is Nmap**

Nmap is an open-source tool used for network discovery and security auditing. Discover live hosts on a network Scan open ports on devices Identify services running on those ports Detect operating systems and versions Perform vulnerability scanning (with scripts)

**How to use Nmap**

In Linux we can use command called

>> nmap --help to view all available options and usage instructions

**The basic command used in nmap**

|  |  |
| --- | --- |
| nmap -sn 192.168.1.0/24 | Ping scan – list live devices |

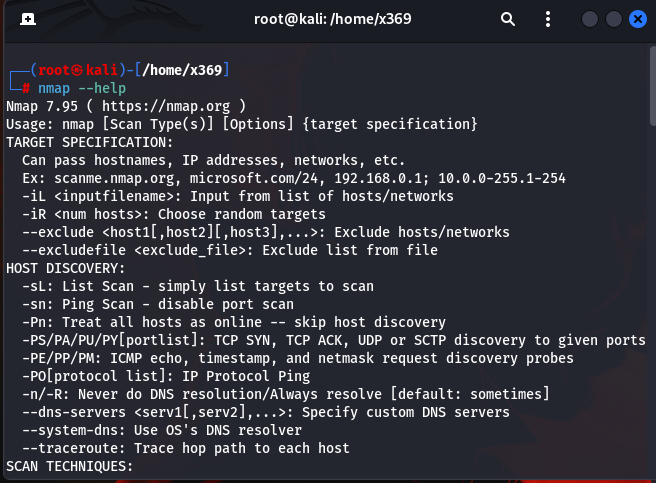
|  |  |
| --- | --- |
| nmap -sS 192.168.1.5 | scan – find open TCP ports |

|  |  |
| --- | --- |
| nmap -sV 192.168.1.5 | Detect service versions |

|  |  |
| --- | --- |
| nmap -O 192.168.1.5 | OS detection |

|  |  |
| --- | --- |
| nmap -A 192.168.1.5 | Aggressive scan (OS, services, traceroute) |

**Practical task on Nmap:**

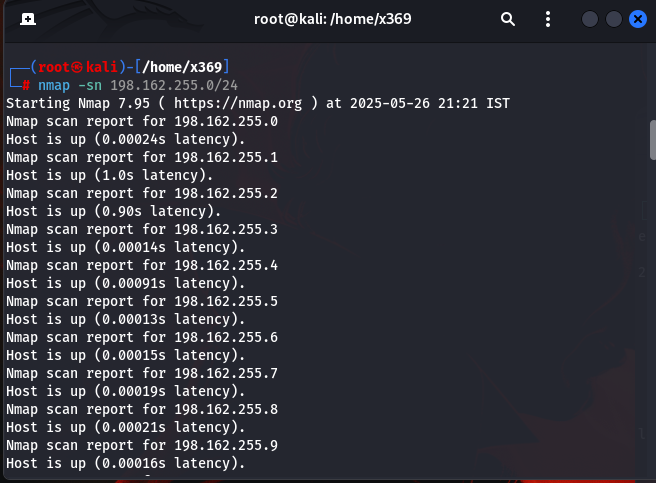


>> nmap –help

nmap --help provides a manual guide (or help message) that shows how to use Nmap commands, available options, and how to combine them for different specific tasks like scanning hosts, detecting operating systems, services, ports, and more.

**>> nmap -sn <ip address/24>**

The nmap -sn <address>/24 command performs a ping scan to find all active IP addresses in a /24 network. It helps identify how many devices are currently connected and online in that network



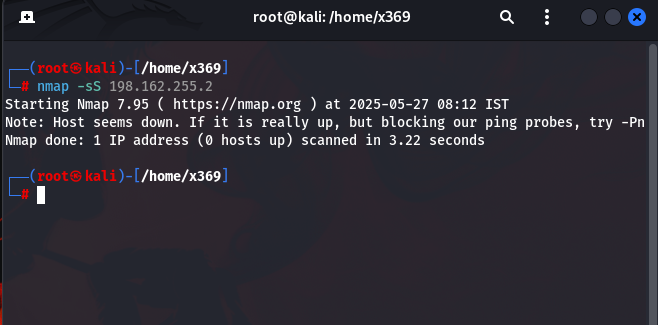
**Note** : It gives you all the devices which are active and connected to network if the device which is not connected to network is not show

From this devices select the device you want to scan for open ports

I have selected **192.168.255.2**

**>> nmap -sS 192.168.255.2**

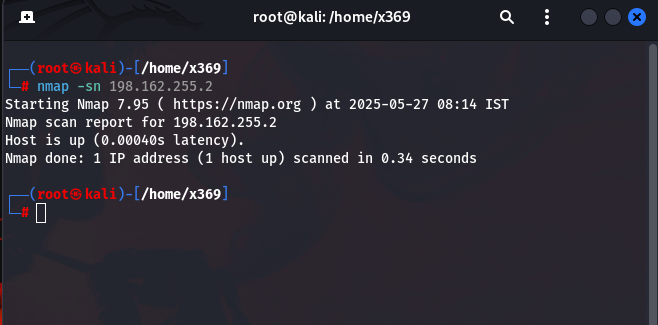
It is a specific scan technique to find the open port on device



In this case, I wasn't able to find open ports because most systems block port scanning. The requests might be blocked by a firewall or built-in security mechanisms on the target systems.

To check the host is active or down use the command

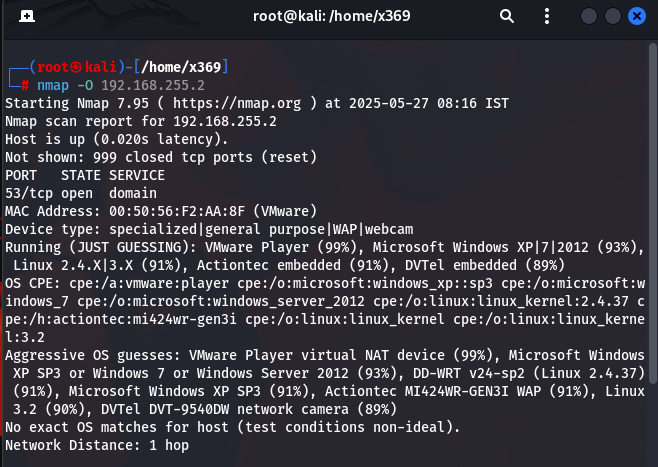
>> nmap -sn 192.168.255.2



Host is up but blocks the port scan

And continue the basic scan techniques to find more about device. like OS scan

>> nmap -O 192.168.255.2



Nmap can detect the operating system with high accuracy (up to 99%) when the target responds to all probe packets and there are no firewalls or filtering, but its accuracy decreases significantly if the system is behind a firewall, NAT, or uses a virtual machine with generic network settings.

This document covers basic Nmap usage for beginners. Advanced techniques such as full-port scanning, UDP scanning, script-based enumeration, and evasive scans — will be covered in future lessons

Thank you