**NMAP SCAN**

**Ex no:1**

**Aim:**

To install and perform Nmap scan (note :- you may use ip address or website name)

**Procedure:**

Step 1: Open Nmap from Kali Linux (Goto Applications->select Information Gathering>select

Nmap)

Step 2: Perform different types of scan

(Tcp, Udp, Ack, Syn, Fin, Null, Xmas, Rpc, Idle)- scan types

**Scanning Techniques**

|  |  |  |
| --- | --- | --- |
| **Flag** | **Use** | **Example** |
| **-sS** | **TCP syn port scan** | **nmap -sS 192.168.1.1** |
| **-sT** | **TCP connect port scan** | **nmap -sT 192.168.1.1** |
| **–sU** | **UDP port scan** | **nmap –sU 192.168.1.1** |
| **–sA** | **TCP ack port scan** | **nmap –sA 192.168.1.1** |

Step 3:-

**To perform host discovery**

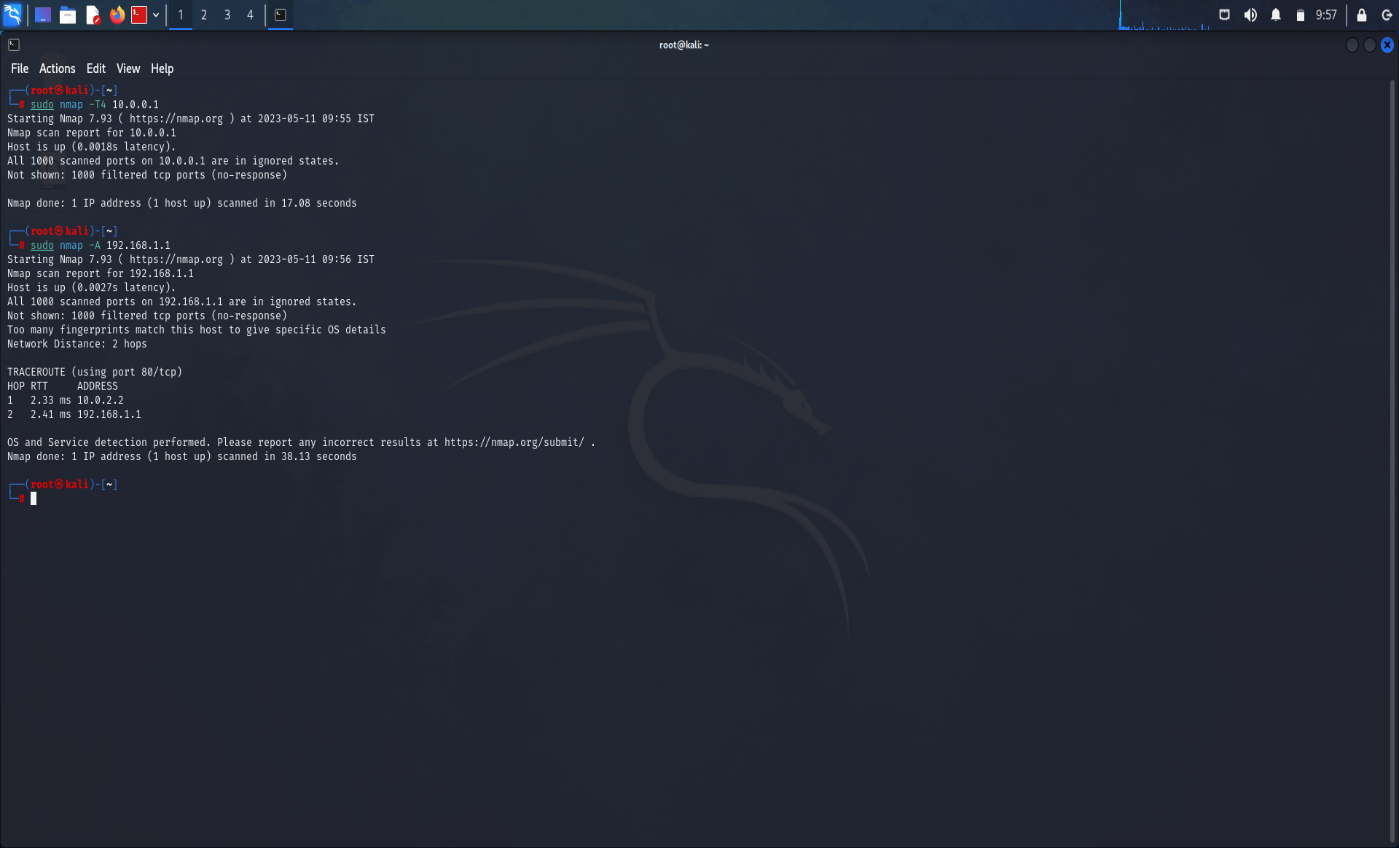
|  |  |  |
| --- | --- | --- |
| -Pn | only port scan | nmap -Pn192.168.1.1 |
| -sn | only host discover | nmap -sn192.168.1.1 |
| -PR | arp discovery on a local network | nmap -PR192.168.1.1 |
| -n | disable DNS resolution | nmap -n 192.168.1.1 |

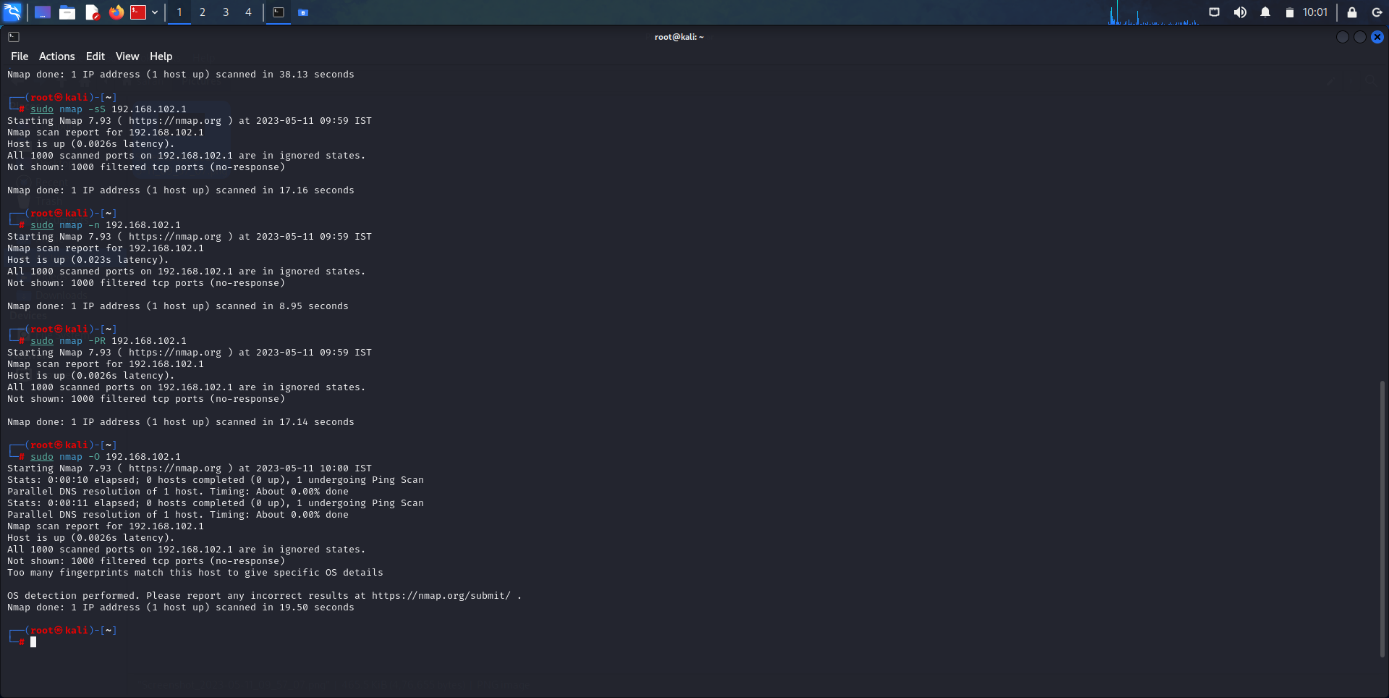
Step4

**port specification**

|  |  |  |
| --- | --- | --- |
| **Flag** | **Use** | **Use** |
| **-p** | **specify a port or port**  **range** | **nmap -p 1-30 192.168.1.1** |
| **-p-** | **scan all ports** | **nmap -p- 192.168.1.1** |
| **F** | **fast port scan** | **nmap -F 192.168.1.1** |

**Output:**





**Result:**  Hence the nmap scan performed successfully