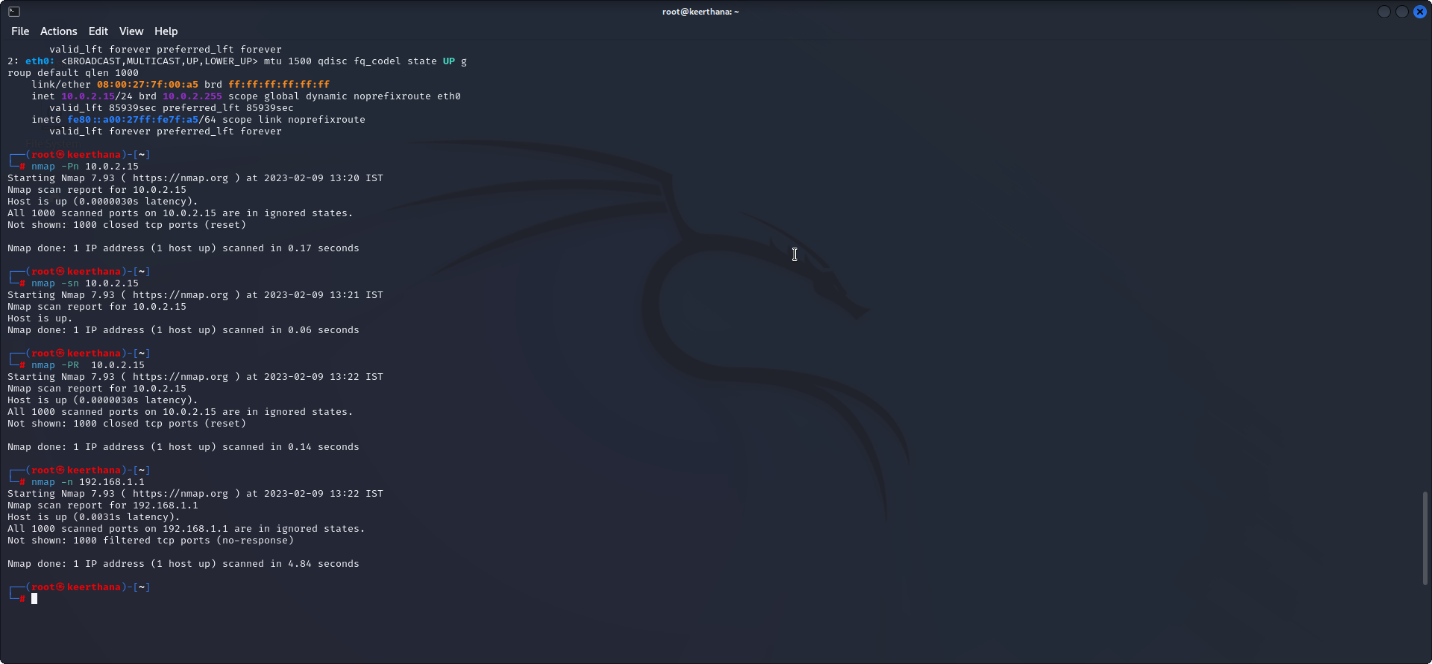
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Exercise No 1:Nmap Scan    Aim:    To install 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 | Example | | -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 |     Step 5:-    Service Version and OS Detection   |  |  |  | | --- | --- | --- | | Flag | Use | Example | | -sV | detect the version of services running | nmap -sV 192.168.1.1 | | -A | aggressive scan | nmap -A 192.168.1.1 | | -O | detect operating system of the target | nmap -O 192.168.1.1 |     Step 6:-    Timing and Performance   |  |  |  | | --- | --- | --- | | Flag | Use | Example | | -T0 | paranoid IDS evasion | nmap -T0 192.168.1.1 | | -T1 | sneaky IDS evasion | nmap -T1 192.168.1.1 | | -T2 | polite IDS evasion | nmap -T2 192.168.1.1 | | -T3 | normal IDS evasion | nmap -T3 192.168.1.1 | | -T4 | aggressive speed scan | nmap -T4 192.168.1.1 | | -T5 | insane speed scan | nmap -T5 192.168.1.1 | |

Output:



Result:

Hence the map scan performed suscessfully.