**Name of Implementation Tool**: - Nmap

**Functionalities implemented: -**

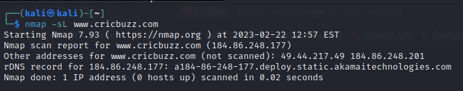
1.Host Discovery in Nmap Network Scanning

2.Port Scanning Techniques by Using Nmap

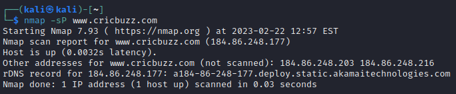
3.OS Detection in Nmap

**. 1. The function of Host discovery in Nmap:**

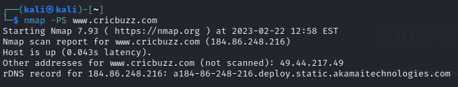
* **List Scan:** A list scan generally lists the possible host without sending any packets to the targeted host.

****

* **Ping Sweep:** Ping sweep discovers on the basis the host is powered on.



* **TCP SYN Ping:** Nmap checks whether a host is online.

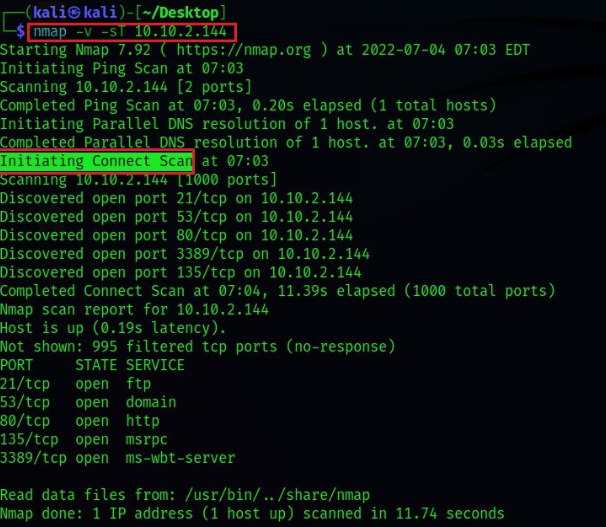
****

* **Traceroute:** Traceroute helps to discover the following hops or pathways to the targeted host.



**2. Different Port Scanning Techniques in Nmap:**

* **TCP Connect Scan (-sT):** TCP Connect scan uses the concept of a full three-way handshake to discover whether a given port is open, filtered, or closed according to the response it receives. Nmap sends a TCP request packet to each and every port specified and determines the status of the port by the response it receives.
* **TCP SYN Scan (-sS):** SYN scans are often called “Half-open” or “Stealth” scans. SYN scan works the same way as TCP Connect scan with closed and filtered ports i.e receives a RST packet for closed port and no response for filtered ports. The only difference is in the way they handle the open ports.
* **UDP Scan (-sU):** UDP unlike TCP, doesn’t perform a handshake to establish a connection before sending data packets to the target port but rather sends the packets hoping that the packets would be received by the target port.



**3. OS Detection in Nmap**

* **Step 1:** Getting the IP of the System
* **Step 2:** Finding List of active devices in the Network
* **Step 3:** Now we perform an Aggressive scan To guess the OS

