**Assignment 7**

Lavanya Bhambure MITU20BTCS0150 LY ISA 1

**Problem Statement**: Use nmap to scan open ports, services, OS and version information of Target IP

**Theory:**

Nmap is a versatile and powerful open-source utility designed for network discovery and security auditing.

1. Nmap Overview:

Nmap is a command-line tool that allows you to probe a target IP address or range of IP addresses to gather information about the hosts and services running on the network. It operates by sending packets to the target and analyzing the responses to determine the status of ports, the services they are running, and even the operating system and version information.

2. Scanning Open Ports:

To scan for open ports on a target IP, you can use the `-p` option followed by the port range or specific ports you want to scan. For example, to scan common ports, you can use:

nmap -p 1-1024 <Target\_IP>

Nmap will send packets to the specified ports on the target IP and report back which ones are open, closed, or filtered. This information is essential for understanding the network's configuration and potential vulnerabilities.

3. Identifying Services:

Nmap not only detects open ports but also attempts to identify the services running on those ports. It does this by sending various probes and analyzing the responses. The service names are usually associated with well-known port numbers and can give you insights into the applications and software running on the target system.

To display service information, simply run Nmap without any specific options for service detection:

nmap <Target\_IP>

4. OS and Version Detection:

Nmap can go a step further and attempt to identify the operating system and version of the target system. This is done through a series of tests and comparisons with known OS and application fingerprints.

To enable OS and version detection, use the `-O` option:

nmap -O <Target\_IP>

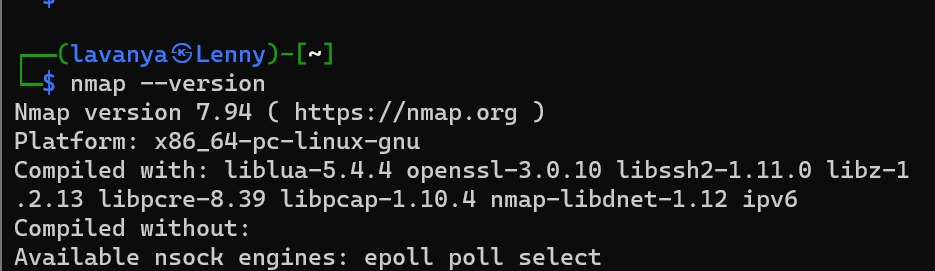
Nmap will provide information about the possible OS and application versions running on the target, based on the responses it receives.

5. Output and Analysis:

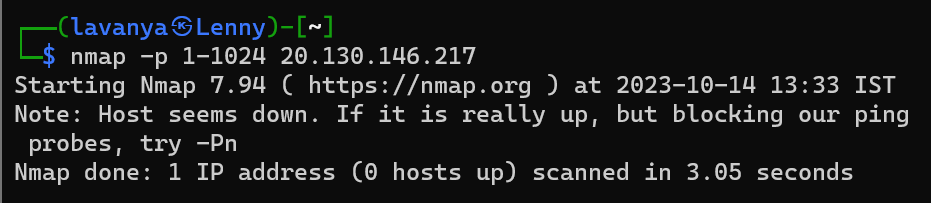
Nmap provides detailed output about the results of the scan, including open ports, service information, and OS details. Analysts can use this information to assess the security of the network, identify potential vulnerabilities, and plan appropriate security measures.

**Code output windows**

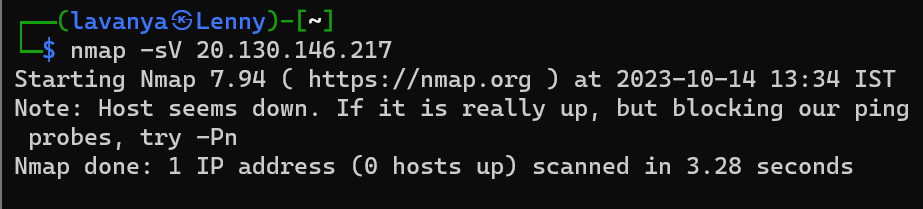
N map version



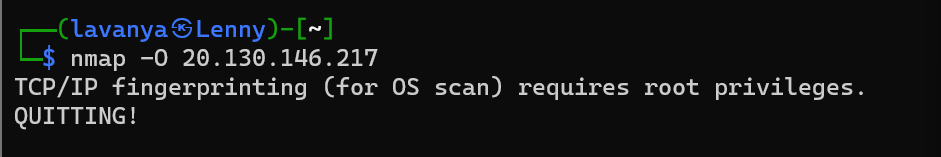
Scanning Open ports



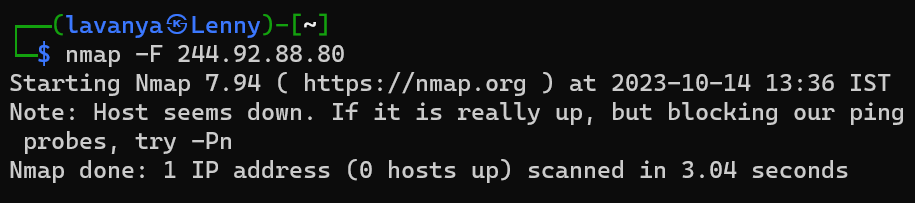
Identifying services



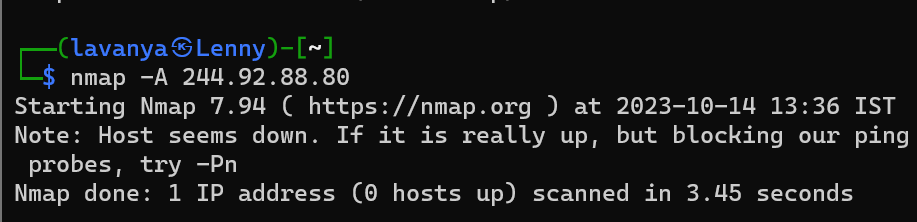
OS and version detection



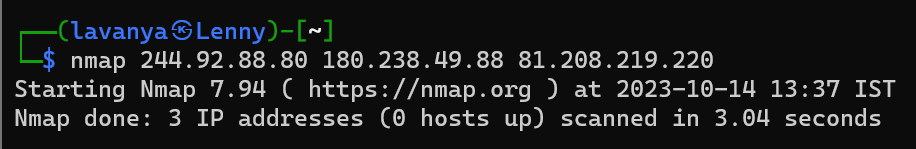
Scanning Files



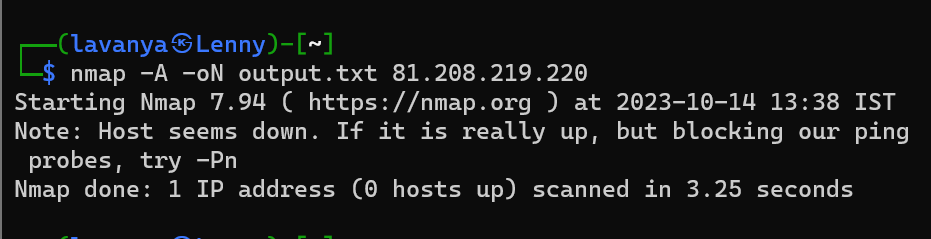
Scanning aggressively files



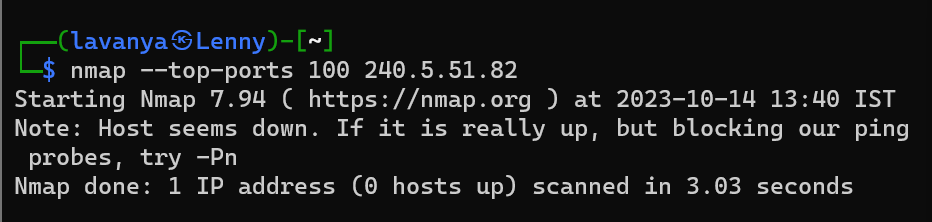
Scanning multiple IP’s



Output text



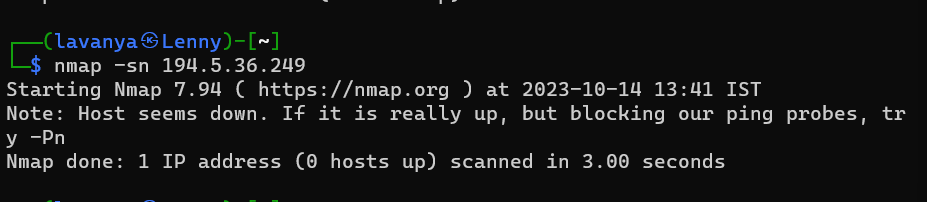
Fast Scan



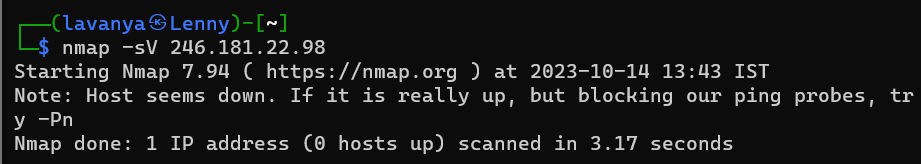
Scanning IPv6 Target



Ping Scan



Service version enumeration



Note: random IP addresses have been used

**Conclusion:**

We have successfully completed implementing Nmap and its code in Kali Linux software.