**PRACTICAL: 4**

**AIM:**

Port scanning is a method for determining open ports and services available on a network or a host. It involves connecting with TCP and UDP ports on the system once you find the IP addresses of a target network or host using the Footprinting technique. You have to map the network of this targeted organization. Nmap (Network Mapper) is a powerful, flexible, open- source, easy-to-use port scanning tool available for both Linux and Windows-based operating systems. Study practical approaches to implementing scanning and enumeration techniques using Nmap.

**THEORY:**

Nmap ("Network Mapper") is a free and open-source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).

Nmap is ...

**Flexible:** Supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers, and other obstacles. This includes many port scanning mechanisms (both TCP & UDP), OS detection, version detection, ping sweeps, and more. See the documentation page.

**Powerful:** Nmap has been used to scan huge networks of literally hundreds of thousands of machines.

**Portable:** Most operating systems are supported, including Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, and more.

**Easy:** While Nmap offers a rich set of advanced features for power users, we can start out as simply as "nmap -v -A targethost". Both traditional command line and graphical (GUI) versions are available to suit your preference. Binaries are available for those who do not wish to compile Nmap from source.

**Free:** The primary goals of the Nmap Project are to help make the Internet a little more secure and to provide administrators/auditors/hackers with an advanced tool for exploring their networks. Nmap is available for free download, and also comes with full source code that you may modify and redistribute under the terms of the license.

**Well Documented:** Significant effort has been put into comprehensive and up-to-date man pages, whitepapers, tutorials, and even a whole book! Find them in multiple languages here.

**CODE:**

|  |
| --- |
| * nmap -v * nmap localhost * nmap 172.16.3.129 --disable-arp-ping * nmap -v 172.16.3.129 --disable-arp-ping * nmap -sA 172.16.3.129 * nmap -Pn 172.16.3.129 * nmap -F 172.16.3.129 * nmap –iflist * nmap -o 172.16.3.129 * nmap -A 172.16.3.129 * nmap 172.16.3.1-255 * nmap charusat.edu.in * nmap -sS 172.16.3.129 * nmap 172.16.3.129/24 --disable-arp-ping |

**OUTPUT:**

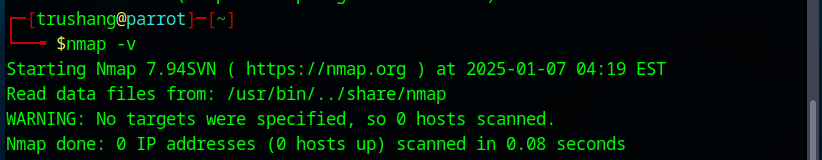
****

Figure 1:Check the version of Nmap

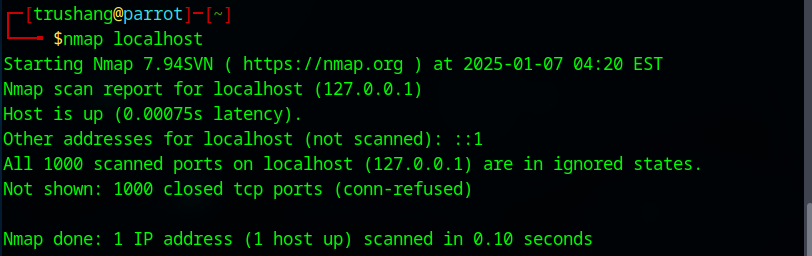


Figure 2:Scan using Nmap

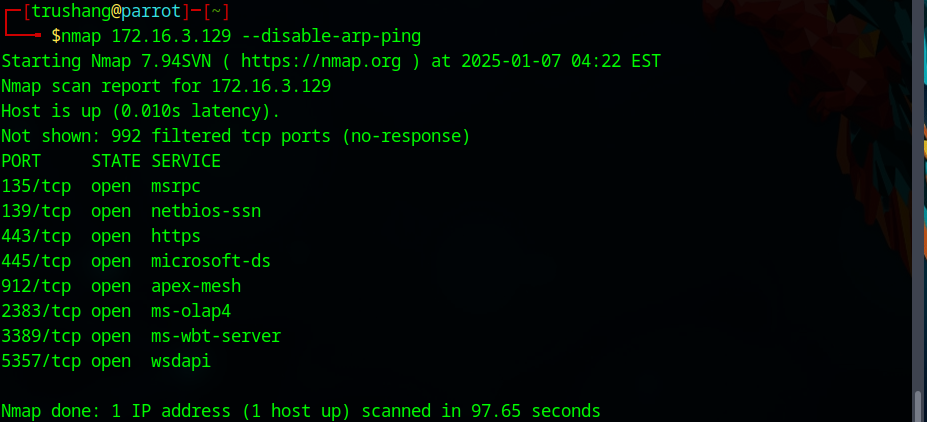


Figure 3:Scan using ip address

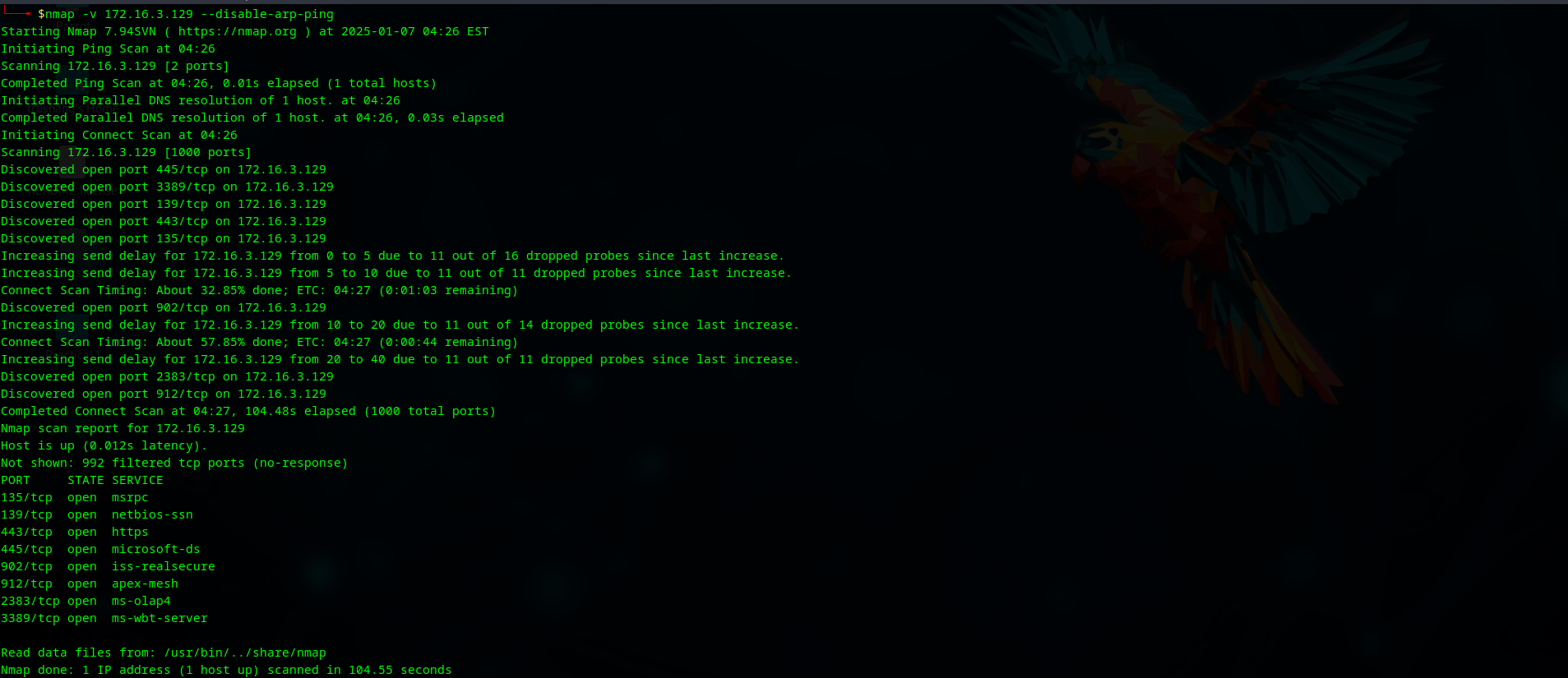
****

Figure 4:Get a more detailed output of the scan, such as status updates on scanning the host and ports

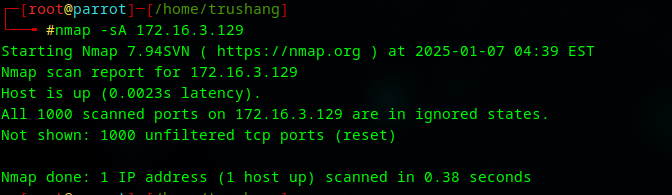


Figure 5:TCP ACK port scan

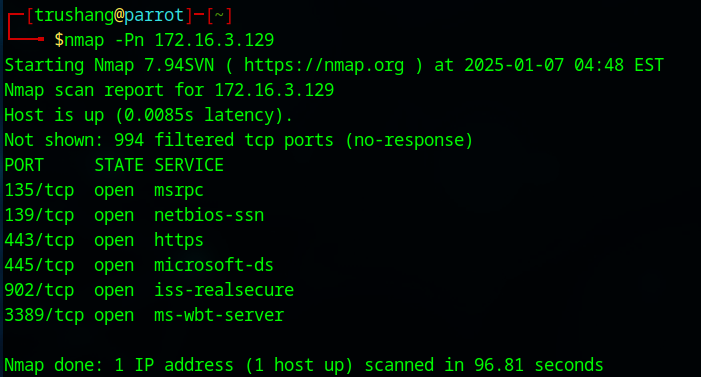


Figure 6:Scan a host to detect firewall

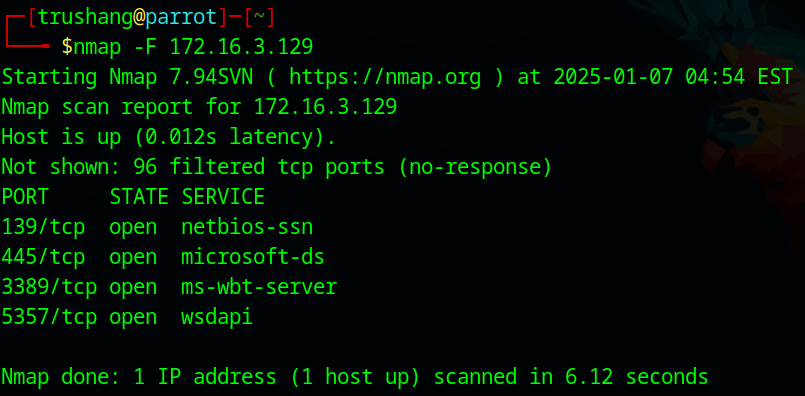


Figure 7:Perform fast scan

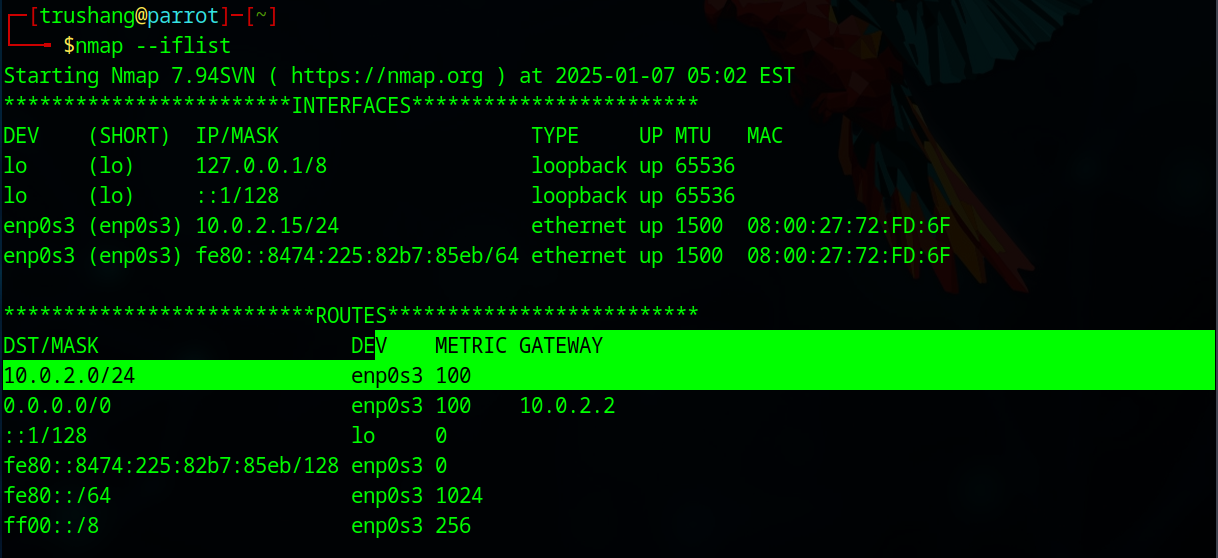


Figure 8:Print Host interface and route

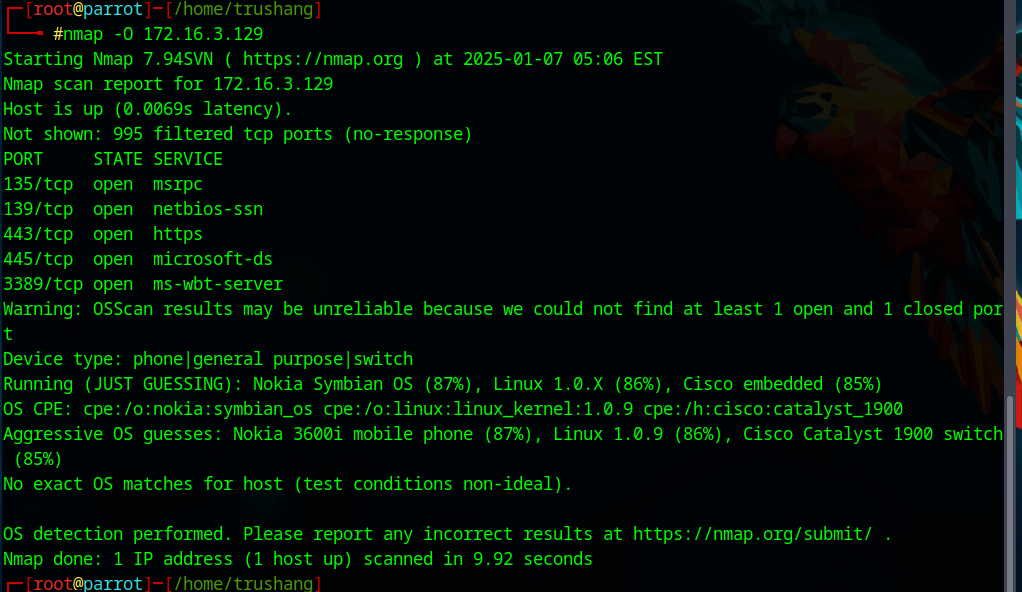


Figure 9:Remote OS detection using TCP/IP stack fingerprinting

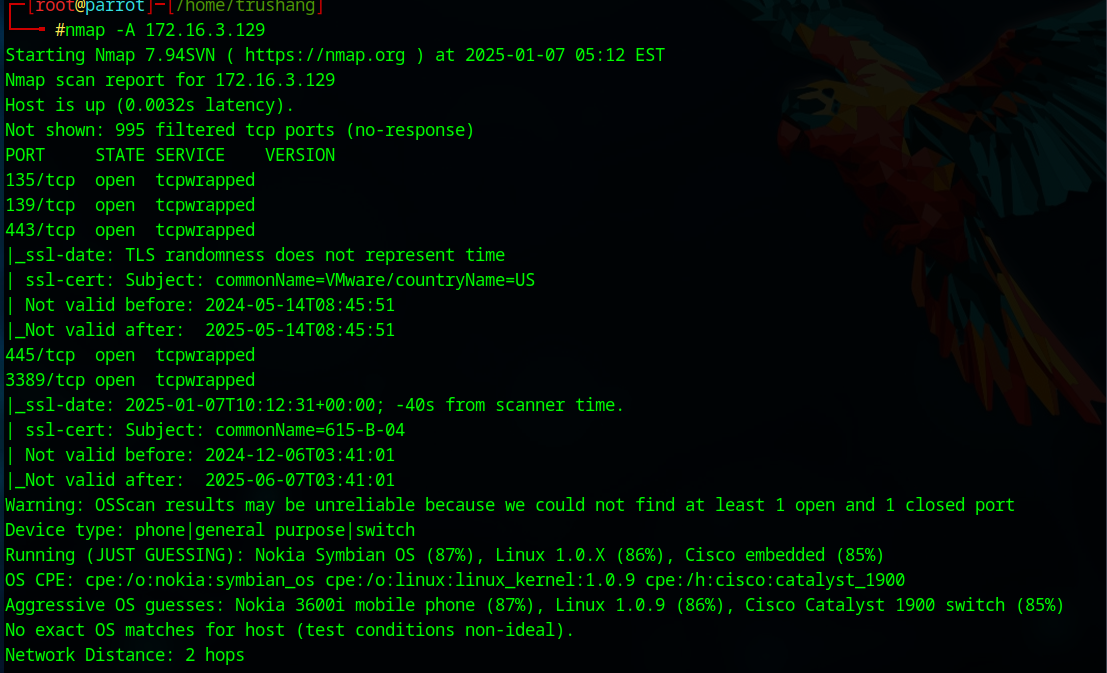


Figure 10: Enables OS detection, version detection, script scanning, and traceroute

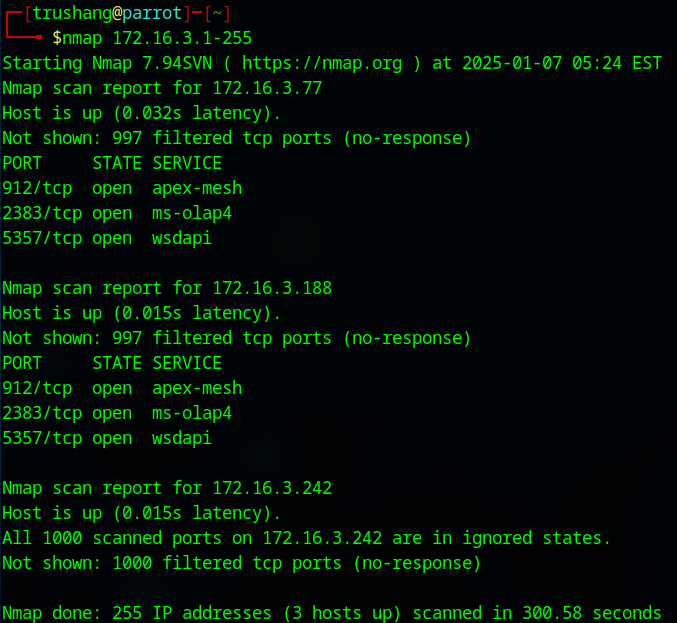


Figure 11:Scan a range of Ip range

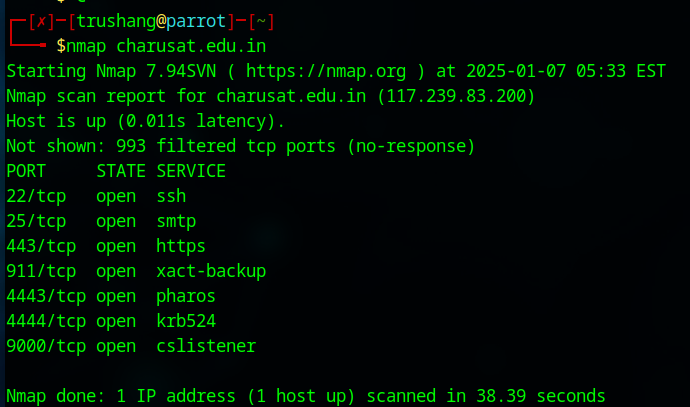


Figure 12:Scan a domain

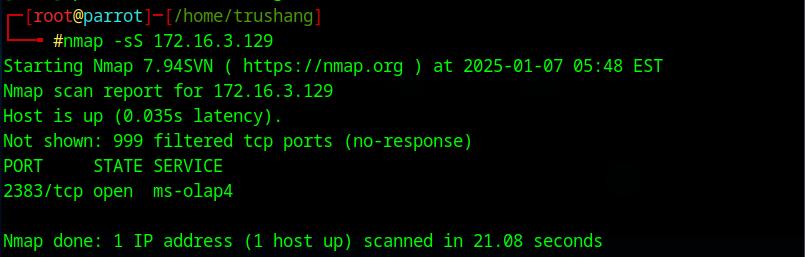


Figure 13:TCP SYN port scan (Default)

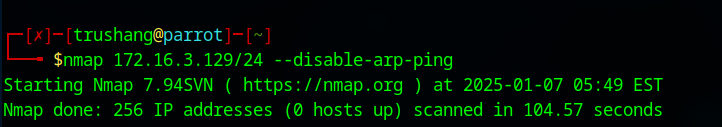
****

Figure 14:Scan using CIDR notation

**LATEST APPLICATIONS:**

* Vulnerability Scanning & Exploitation
* Cloud Security
* IoT Device Discovery and Security
* Automated Network Discovery and Asset Management
* Remote Monitoring and Incident Response
* Automating Network Scans with APIs

**LEARNING OUTCOME:**

In this practical, we learn that port scanning with Nmap is used to identify open ports and services on a network. By combining foot printing and enumeration techniques, Nmap helps security professionals map networks and assess vulnerabilities.

**REFERENCES:**

1. YouTube: <https://www.youtube.com/watch?v=fp1042XK4A8>
2. Nmap: [https://nmap.org/](https://nmap.org/%20)