“***ELEVATE LABS CYBERSECURITY INTERNSHIP PROJECT WORK***”

“PROJECT-Scanning local network for open ports”

- *Name- Gajanand Prasad*
- *Institution –Elevate labs*
- *Date – 23-06-2025*
- *Email-ID – gajanandprasad482@gmail.com*

#-TABLE OF CONTENT:-

Section no	Title
1	Introduction
2	objective
3	Tools & Technologies used
4	Methodology
5	Findings
6	Risk-analysis
7	Recommendations
8	Conclusion
9	references

1-INTRODUCTION:- In cybersecurity, understanding how networks are exposed to threats is a crucial first step toward securing them. One of the foundational techniques for this is **port scanning** — the process of probing a device or network to discover **open ports** and the services running on them. Open ports can act as potential entry points for attackers if not properly secured.

This project focuses on performing **network reconnaissance** using **Nmap**, a powerful and widely-used network scanning tool. The goal is to identify active devices in a local network, determine their **IP addresses**, and detect which ports are open and listening for connections. Specifically, the project uses a **TCP SYN scan**, which is a fast and stealthy scanning method that sends only the initial packet of the TCP handshake to detect open ports without completing the full connection.

By scanning an **IP range** (e.g., 192.168.1.0/24), we aim to map the network's attack surface and understand its **exposure level**. This process highlights how real attackers might gather information in the early phases of an attack. It also builds a foundational understanding of **network security basics**, helping us analyze and secure systems by identifying unnecessary or risky services.

Through this task, we develop hands-on skills in **reconnaissance**, one of the most important phases of ethical hacking and penetration testing.

2-OBJECTIVES;-

The objective of this project is to scan the local network using Nmap to identify live hosts and open ports. It aims to build basic skills in network reconnaissance, understand service exposure, and highlight the importance of securing open ports in cybersecurity.

3-TOOLS & TECHNOLOGIES USED:-

Tool used	Nmap
OS used	windows

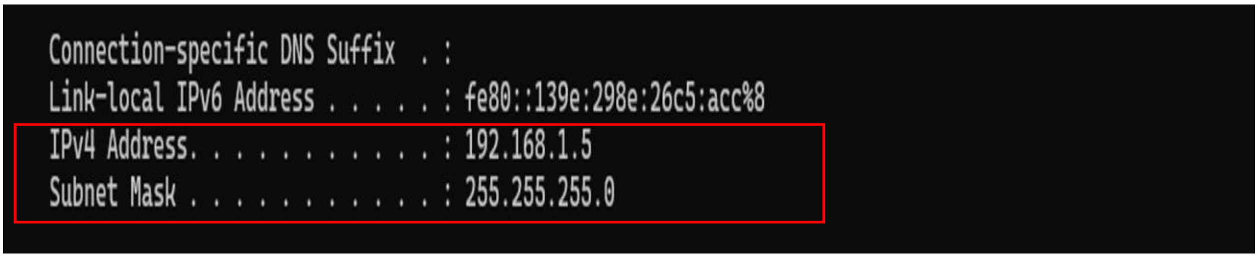
4-METHODOLOGY:-

- **Commands used**

commands	What it does?
ipconfig	Network configuration

nmap –sS <target ip range>	Tcp syn scan (stealty and fast)

- Finding local ip address & subnet mask -“ipconfig”



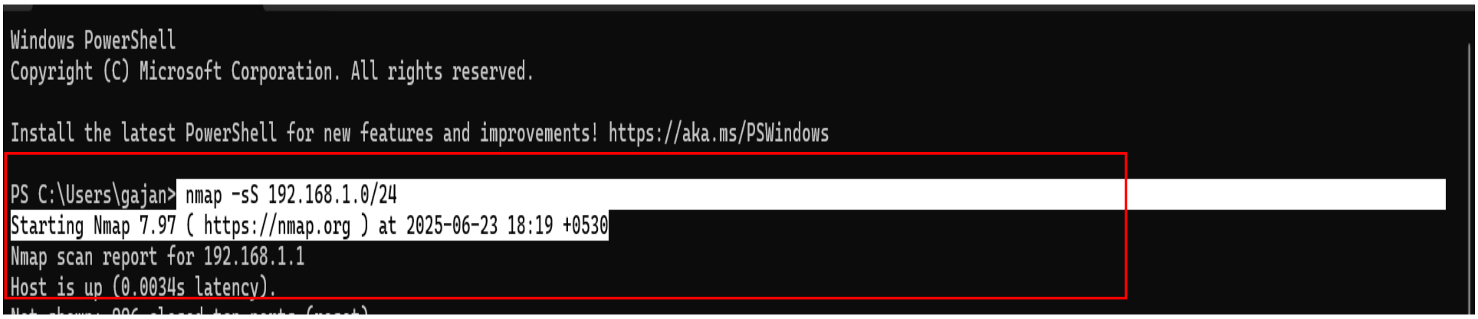
```
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::139e:298e:26c5:acc%8
   IPv4 Address. . . . . . . . . . . : 192.168.1.5
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
```

- Ipv4 address -192.168.1.5

- Subnet mask-255.255.255.0

- Finding local ip range------[192.168.1.0/24]

#**performing TCP SYN SCAN** :-

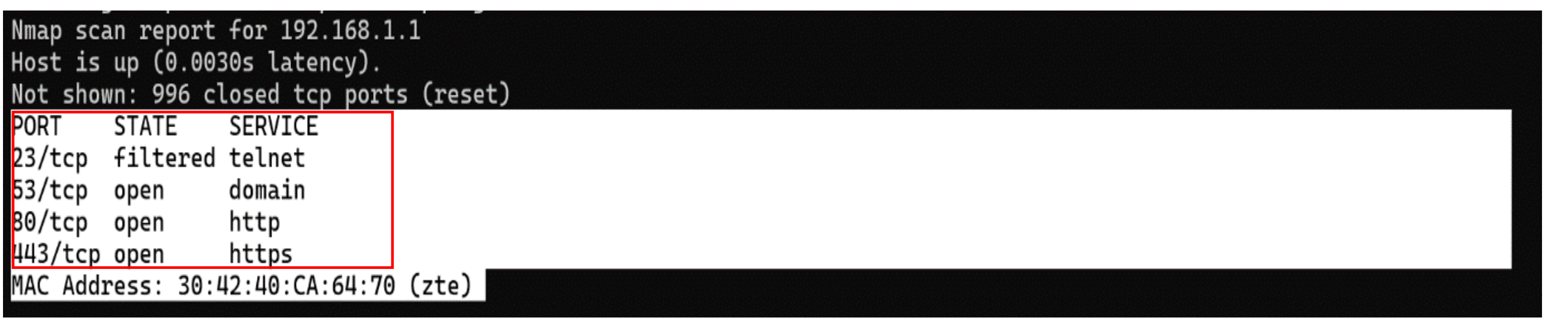


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\gajan> nmap -sS 192.168.1.0/24
Starting Nmap 7.97 ( https://nmap.org ) at 2025-06-23 18:19 +0530
Nmap scan report for 192.168.1.1
Host is up (0.0034s latency).
Not shown: 996 closed tcp ports (reset)
```

- This scan sends SYN packets to each port and records responses without completing the TCP handshake, making it stealthy and efficient.

5-FINDINGS:-

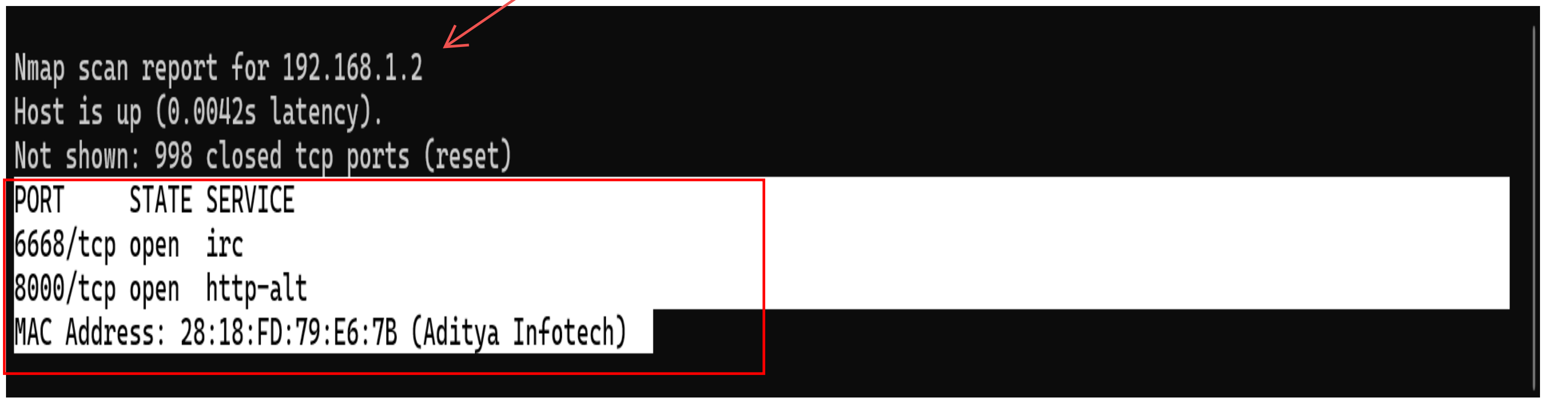
1-



```
Nmap scan report for 192.168.1.1
Host is up (0.0030s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE    SERVICE
23/tcp   filtered telnet
53/tcp   open     domain
80/tcp   open     http
443/tcp  open     https
MAC Address: 30:42:40:CA:64:70 (zte)
```

- Host -192.168.1.1
- Open Port & services- 80(HTTP),443(HTTPS)

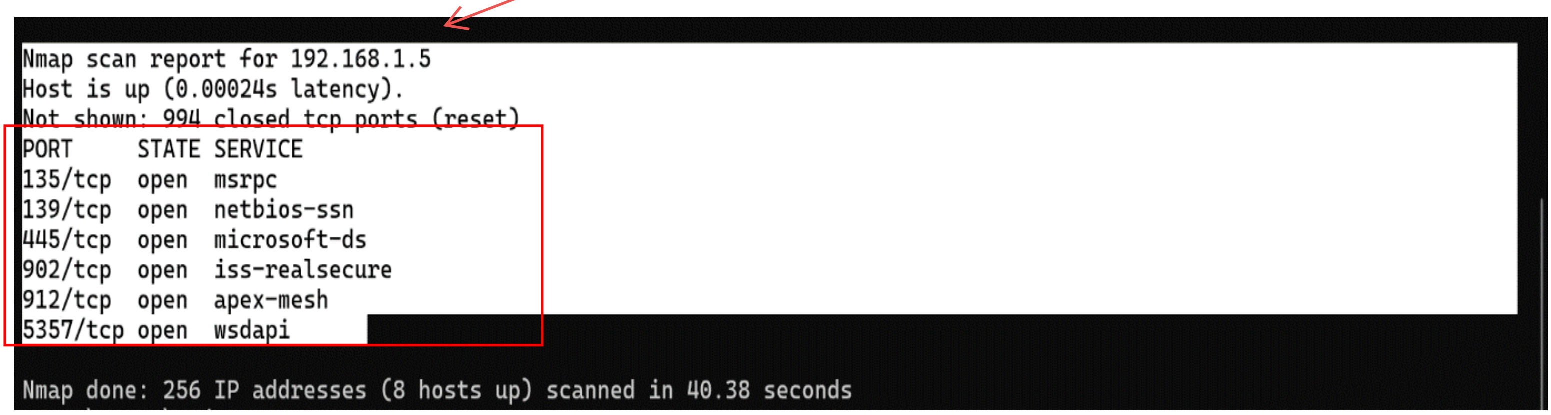
2-



```
Nmap scan report for 192.168.1.2
Host is up (0.0042s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
6668/tcp open  irc
8000/tcp open  http-alt
MAC Address: 28:18:FD:79:E6:7B (Aditya Infotech)
```

- Host -192.168.1.2
- Open ports & services -6668 (IRC), 8000 (http-alt)

3-



```
Nmap scan report for 192.168.1.5
Host is up (0.00024s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
5357/tcp open  wsdapi

Nmap done: 256 IP addresses (8 hosts up) scanned in 40.38 seconds
```

- Host-192.168.1.5
- Open ports & services-135(msrpc),139(netbios-ssn),445(microsoft-ds),902(iss-realsecure)

#-<u>DETAIL ANALYSIS OF SERVICES RUNNING IN THESE PORTS</u>:-

Service	Description
HTTP	Web server (unsecured web traffic)
HTTPS	Secure web server (SSL/TLS encrypted)

IRC	Internet Relay Chat (can be abused by malware)
HTTP-ALT	Alternate web traffic port (often custom apps)
MSRPC	Microsoft RPC (used for DCOM, Windows services)
NetBIOS-SSN	NetBIOS session (file/printer sharing on Windows)
Microsoft-DS	SMB over TCP (Windows file sharing, vulnerable often)
ISS-Realsecure	Used by VMware or intrusion detection systems

6-RISK-ANALYSIS:-

Open-ports	risk
80	**Moderate risk** – Unencrypted; vulnerable to session hijacking, sniffing, and downgrade attacks.
443	**Low risk** if configured securely. If outdated SSL/TLS versions are used, it can be

	vulnerable to attacks like POODLE or BEAST
6668	**High risk** – IRC is often used as a control channel in botnets. If unmonitored, can be exploited.
8000	**Depends on usage** – If it's a web app, risks include XSS, SQLi, or outdated server software.
135	**Moderate to high risk** – Can be used in DCOM or SMB-based exploits (e.g., CVE-2017-0144 - EternalBlue).
139	**High risk** – Can be exploited for information gathering and lateral movement. Often targeted by malware.
445	**Critical risk** – Commonly exploited (EternalBlue, WannaCry). Used for lateral movement.
902	**Low to moderate** – If related to VMware services, ensure restricted access.

7-RECOMMENDATIONS:-

- **Disable unused ports/services** like Telnet (23), NetBIOS (139), and SMB (445) if not needed.

- **Use HTTPS** instead of HTTP and enforce strong SSL/TLS settings.
- **Restrict access** to sensitive ports using firewalls
- **Keep systems updated** to patch known vulnerabilities.
- **Monitor traffic** using tools like Wireshark or IDS.

8-CONCLUSION:-

This project helped identify open ports and services using Nmap, highlighting possible security risks in a local network. It enhanced understanding of basic network reconnaissance, scanning techniques, and the importance of securing exposed services.

9-REFERENCES:-

- Download and install **Nmap-** https://nmap.org/download.html