Cyber Security

Tejaswini Sardar

MAY 26 2025

—

CYBER SECURITY

—

INTRODUCTION

Task 1:

Scan Your Local Network for Open Ports.

The objective of this task is to explore and identify open ports on devices within the local network to assess potential network exposure and associated security risks.

THE PROCESS

TOOLS: -

- Nmap (Network Mapper): A free and open-source network scanning tool used for network discovery and security auditing.
- Metasploit (Metasploit is a framework for security testing and vulnerability management Tool)
- Wireshark (A network protocol analyzer used to inspect network traffic.)

These Are the Tools Used While Doing the Task For Scanning Ports.

Procedure

Step 1: Install Nmap

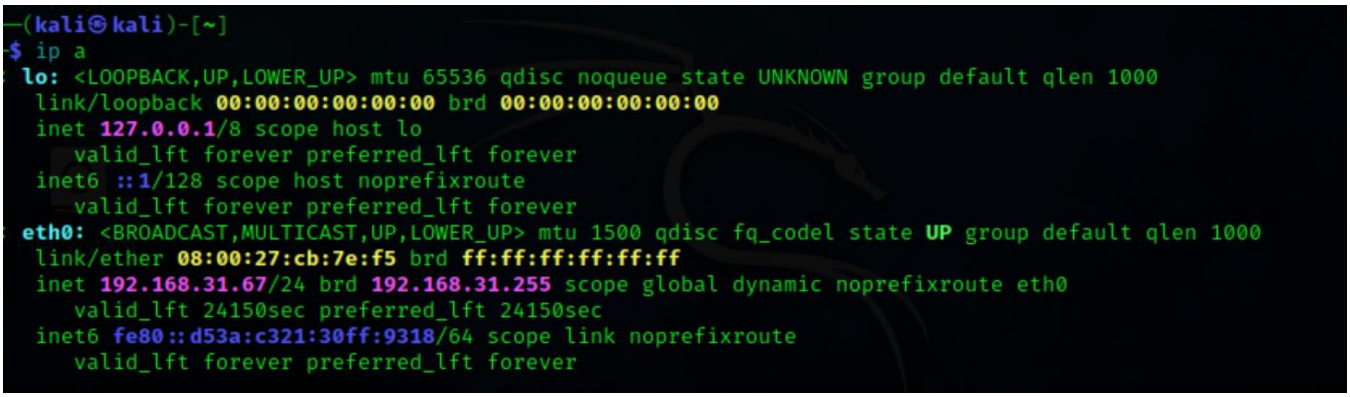
Nmap was downloaded and installed from the official website: https://nmap.org. The installation was performed on a Windows/Linux system.

Step 2: Identify Your Local IP Address Range

Step 1: Open Terminal

Run the following command to view your network configuration:

$ Ip a



Step 3: Perform TCP SYN Scan

A SYN scan was performed using the following Nmap command:

$ Sudo nmap -sS 192.168.31.246

```
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:9f:89:06
          inet addr:192.168.31.246  Bcast:192.168.31.255  Mask:255.255.255.0
          inet6 addr: 2409:40c2:122e:b2a5:a00:27ff:fe9f:8906/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe9f:8906/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:113 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10507 (10.2 KB)  TX bytes:7670 (7.4 KB)
          Base address:0xd010 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:102 errors:0 dropped:0 overruns:0 frame:0
          TX packets:102 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23665 (23.1 KB)  TX bytes:23665 (23.1 KB)
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.31.246
Starting Nmap 7.94 ( https://nmap.org ) at 2025-05-26 08:13 EDT
Nmap scan report for 192.168.31.246
Host is up (0.0019s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:9F:89:06 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
```

Step 4 :- IP addresses and open ports found.

✅ Open Ports & Services

Port	Service	Description
21	FTP	File Transfer Protocol
22	SSH	Secure Shell (remote login)
23	Telnet	Insecure remote login
25	SMTP	Simple Mail Transfer Protocol
53	Domain	DNS service
80	HTTP	Web traffic
111	RPCBind	Remote Procedure Call service
139	NetBIOS-SSN	Windows file/printer sharing
445	Microsoft-DS	SMB over IP
512	Exec	Remote command execution (rsh)
513	Login	Remote login (rlogin)
514	Shell	Remote command shell
1099	RMI Registry	Java Remote Method Invocation
1524	Ingreslock	Often used for backdoors
2049	NFS	Network File System
2121	CCPROXY-FTP	Custom FTP proxy
3306	MySQL	MySQL database
5432	PostgreSQL	PostgreSQL database
5900	VNC	Virtual Network Computing (remote desktop)
6000	X11	X Window System (GUI)
6667	IRC	Internet Relay Chat
8009	AJP13	Apache JServ Protocol
8180	Unknown	Undetermined service

Step 5:- Identify potential security risks from open ports.

⚠️ Security Observations

- Telnet (23): Unencrypted and insecure. Recommend disabling.
- R-services (512, 513, 514): Outdated and insecure; often exploited.
- SMB (139, 445): Common target for ransomware (e.g., Eternal Blue).
- Ingreslock (1524): Frequently left by exploits/backdoors.
- RPC and NFS (111, 2049): Can expose sensitive file systems if misconfigured.
- VNC & X11 (5900, 6000): GUI access points — ensure authentication is enforced.

- IRC (6667): Often used in botnets; ensure it’s necessary.
- Unknown (8180): Needs further investigation — may be a custom or test service.

Step 6 :- Scan results as a text or HTML file.

https://github.com/Travel-Hacker/task-1-cyber-security/blob/main/Nmap%20report.txt

Conclusion:-

The network scan revealed multiple devices with open ports, many running common services. Some of these services (e.g., SMB, HTTP) may expose the network to known vulnerabilities. It is recommended to:

- Disable unnecessary services.
- Secure remote access protocols.
- Keep firmware and software up to date.
- Implement firewall rules to restrict exposure.