Cybersecurity Internship – Task 1

Network Port Scanning using Nmap

Name :- Bogi Arun

Date :- 04/08/2025

Introduction

In today's digital landscape, understanding network exposure is a critical aspect of cybersecurity. One of the foundational skills in this area is network reconnaissance, which involves identifying devices, services, and vulnerabilities within a network. This task focuses on performing a basic port scan of the local network using **Nmap**, a powerful open-source network scanner.

The objective is to detect live hosts and open ports within a specified IP range, helping to reveal what services are running on each machine. This provides insight into potential security risks that can arise from improperly secured or unnecessary services. By completing this task, I gained hands-on experience with Nmap and a better understanding of how attackers might scan networks to find weaknesses — a crucial step toward building defensive security skills.

Tools Used

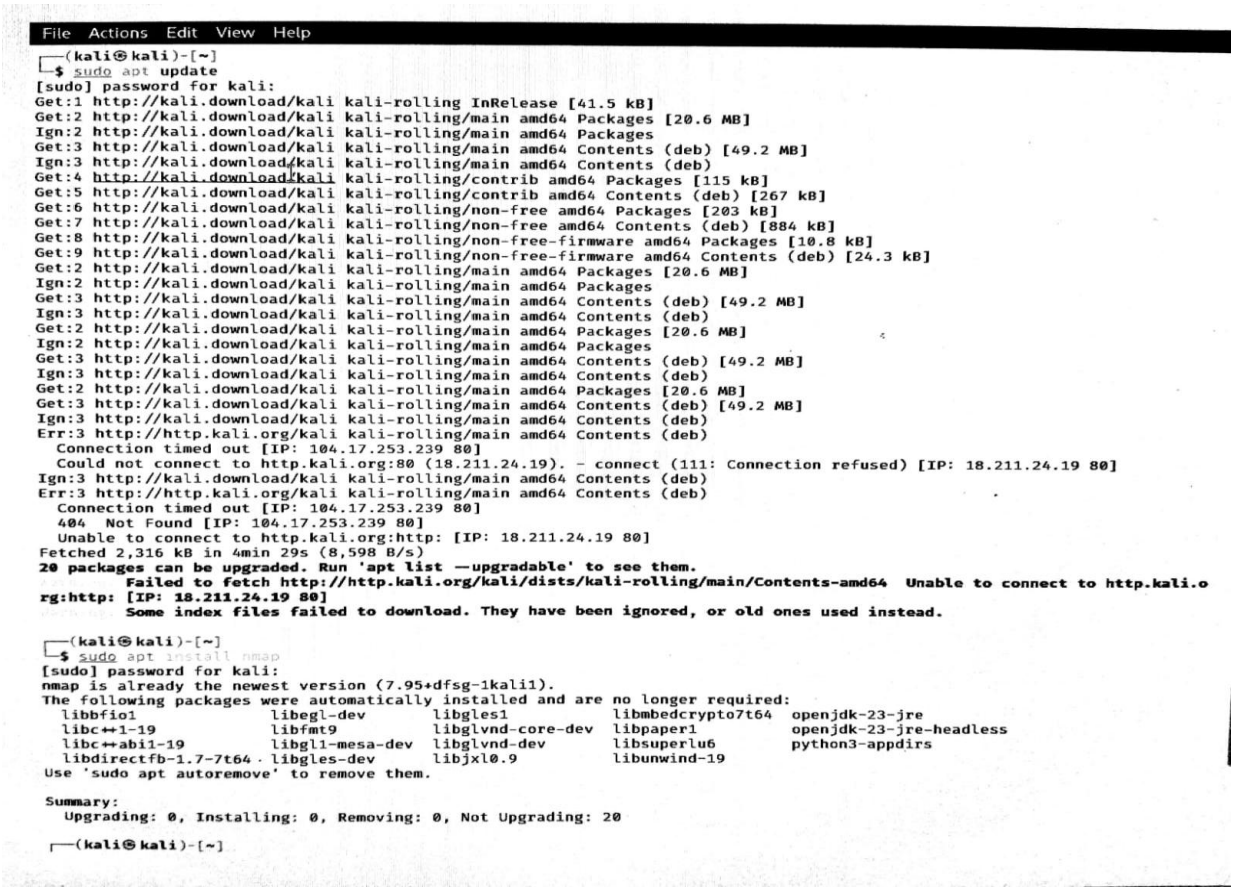
- **Kali Linux**
  A Debian-based Linux distribution used for penetration testing and cybersecurity tasks. It comes with a wide range of security tools pre-installed, including Nmap.
- **Nmap (Network Mapper)**
  An open-source network scanning tool used to discover hosts and services on a computer network by sending packets and analyzing the responses.
- **Terminal (Command Line Interface)**
  Used to execute Nmap commands and interact with the operating system.
- **(Optional) Wireshark**
  A network protocol analyzer used to capture and inspect data packets in real-time. It can help understand how Nmap scans appear at the packet level.
- **Text Editor (e.g., nano, VS Code, or built-in editor)**
  Used for writing the README file and reviewing scan results.
- **GitHub**
  A web-based platform for version control and code sharing. Used to upload and submit the completed task along with results and documentation.

Step 1: Update Kali Linux

sudo apt update

Step 2: Install Nmap

sudo apt install nmap



Step 3: Find Local IP Range

ifconfig

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.189.129  netmask 255.255.255.0  broadcast 192.168.189.255
        inet6 fe80::20c:29ff:fee1:45a0  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:e1:45:a0  txqueuelen 1000  (Ethernet)
        RX packets 14259  bytes 16233238 (15.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4299  bytes 1105801 (1.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 24  bytes 1440 (1.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1440 (1.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$
```

Step 4: Perform TCP SYN Scan

nmap –sS 192.168.189.129/24

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.189.129/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-04 11:57 IST
Nmap scan report for 192.168.189.2 (192.168.189.2)
Host is up (0.00053s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE    SERVICE
53/tcp filtered domain
MAC Address: 00:50:56:F4:88:7A (VMware)

Nmap scan report for 192.168.189.254 (192.168.189.254)
Host is up (0.00082s latency).
All 1000 scanned ports on 192.168.189.254 (192.168.189.254) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E2:CC:F6 (VMware)

Nmap scan report for 192.168.189.129 (192.168.189.129)
Host is up (0.0000030s latency).
All 1000 scanned ports on 192.168.189.129 (192.168.189.129) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (3 hosts up) scanned in 6.23 seconds

┌──(kali㉿kali)-[~]
└─$
```

Step 5 : IP addresses and open ports

1. Host: 192.168.189.2

- **Status**: Host is up
- **Open Port**:
  - 53/tcp → **Filtered** (Service: domain, typically DNS)
- **MAC Address**: 00:50:56:F4:88:7A (VMware)

2. Host: 192.168.189.254

- **Status**: Host is up
- **Open Ports**:
  - **None detected**
  - All 1000 ports are in **filtered state (no response)**
- **MAC Address**: 00:50:56:E2:CC:F6 (VMware)

3. Host: 192.168.189.129 (Your Machine)

- **Status**: Host is up
- **Open Ports**:
  - **None detected**
  - All 1000 ports are **closed**

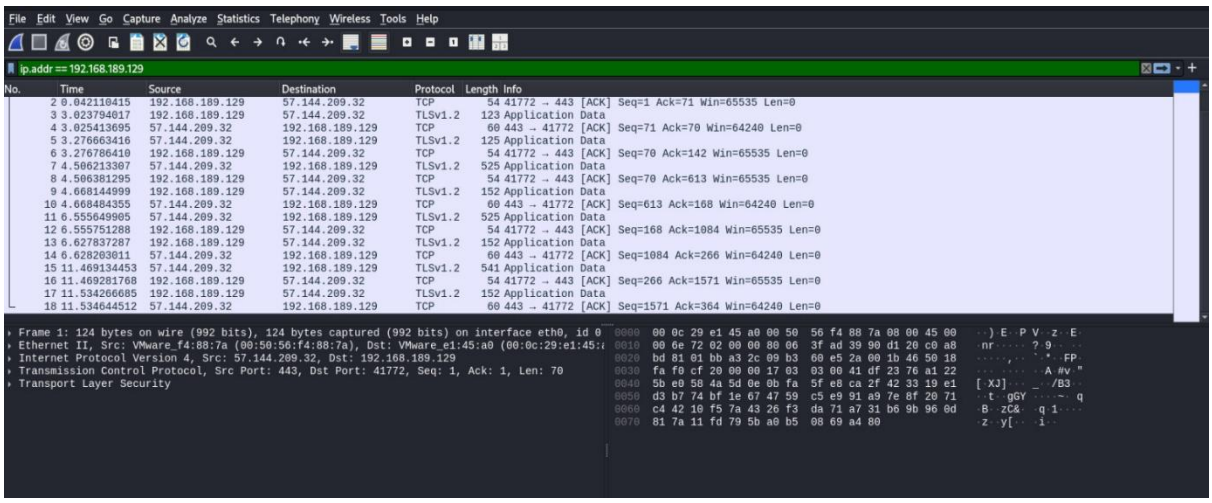
Step 6 : Install wireshark in kali linux

Sudo wireshark

ip.addr == 192.168.189.129

It’s a Wireshark display filter that tells Wireshark to only show packets where:

- The source IP is 192.168.189.129,



Port	Protocol	Service Name	Description
20	TCP	FTP (Data)	Transfers files from server to client
21	TCP	FTP (Control)	Command/control for FTP sessions
22	TCP	SSH	Secure Shell for remote login/command execution
23	TCP	Telnet	Remote login (insecure; outdated)
25	TCP	SMTP	Sending email (Simple Mail Transfer Protocol)
53	UDP/TCP	DNS	Domain Name System (resolves domain names to IPs)
67/68	UDP	DHCP	Dynamic Host Configuration Protocol (IP assignment)
80	TCP	HTTP	Web traffic (unsecured)
110	TCP	POP3	Email receiving (Post Office Protocol)
143	TCP	IMAP	Email access protocol (more modern than POP3)
443	TCP	HTTPS	Secure web traffic (SSL/TLS encryption)
445	TCP	SMB	File sharing in Windows networks
3389	TCP	RDP	Remote Desktop Protocol (Windows remote access)
3306	TCP	MySQL	MySQL database service
8080	TCP	HTTP-alt / Proxy	Alternate HTTP or web proxy service

Analysis of Common Ports and Potential Security Risks

Port	Protocol	Service	Description
21	TCP	FTP	File Transfer Protocol (unencrypted)
22	TCP	SSH	Secure Shell for remote access
23	TCP	Telnet	Unencrypted remote shell access
53	UDP/TCP	DNS	Domain Name System
80	TCP	HTTP	Unsecured web traffic
443	TCP	HTTPS	Secure web traffic via SSL/TLS
445	TCP	SMB	Windows file and printer sharing
3306	TCP	MySQL	Database service

---

3. Potential Security Risks

Port 21 - FTP:

- Data and credentials are transmitted in plaintext.
- Vulnerable to sniffing, brute-force attacks, and command injection.
- **Mitigation:** Replace with SFTP or disable the service if not needed.

Port 22 - SSH:

- Commonly targeted for brute-force login attempts.
- **Mitigation:** Use key-based authentication, change default port, disable root login.

Port 23 - Telnet:

- Data is unencrypted; high risk of interception.
- **Mitigation:** Disable and replace with SSH.

Port 53 - DNS:

- Can be abused in DNS amplification attacks or poisoned for redirecting traffic.
- **Mitigation:** Restrict external queries, monitor for abnormal activity.

Port 80 - HTTP:

- No encryption means sensitive data can be intercepted.
- **Mitigation:** Enforce redirection to HTTPS.

Port 443 - HTTPS:

- Secure by design, but still at risk if SSL/TLS versions are outdated.
- **Mitigation:** Regularly update libraries, enforce strong ciphers.

Port 445 - SMB:

- Used in ransomware attacks like WannaCry.
- **Mitigation:** Disable if not used, patch vulnerabilities, block external access.

Port 3306 - MySQL:

- If exposed externally, attackers can access databases.
- **Mitigation:** Restrict access, use strong credentials, and monitor queries.