Cybersecurity Internship – Task 1 Report

Introduction

The very first step in defending any network is knowing what's exposed to the outside world. For this task, I explored my local network using **Nmap** to identify open ports and the services running behind them. The goal was simple: to understand what my devices are "advertising" to anyone who decides to look.

This exercise not only taught me of **network reconnaissance** but also highlighted the importance of securing seemingly small details like unused ports.

Approach

Here's how I went about it:

1. **Getting the tools ready**
   I installed **Nmap** (the industry-standard port scanner) and prepared my system for scanning. I also kept **Wireshark** handy to peek into the packets for a deeper understanding.
2. **Discovering the network**
   I found my local IP range (`xxx.xxx.xxx.0/24` in my case) — essentially the digital "neighbourhood" of all devices connected to my router.
3. **Running the scan**
   Using a **TCP SYN scan** (stealthy and efficient), I ran:
   sudo nmap -sS xxx.xxx.xxx.x/24.

1. This revealed active hosts and their open ports.
2. **Digging into the results**
   I noted down IPs, open ports, and the corresponding services. To verify what was happening behind the scenes, I also looked at some packet traces in **Wireshark**.

Findings

The scan identified several devices with commonly used open ports. For example:

- **Port 80 (HTTP)** – Hosting web services
- **Port 443 (HTTPS)** – Secure web traffic
- **Port 22 (SSH)** – Remote administration
- **Port 445 (SMB)** – File sharing across the network

While these services are normal, each open port is also a potential **doorway**. For example:

- **SSH (22)** could be brute-forced if not secured properly.
- **SMB (445)** has a history of being abused in ransomware attacks.

This made me realize that even a home or small office network isn't immune — if it's connected, it's discoverable.

Analysis & Reflection

At first, the results looked harmless. After all, I *expect* my router and devices to have services like HTTP and HTTPS open. But then it hit me: if I can see these ports so easily, so can an attacker.

- An **open port = an invitation** (unless you specifically guard it).
- Attackers often use port scans as a **reconnaissance step** before exploiting vulnerabilities.
- Tools like Wireshark help validate and monitor traffic, giving defenders visibility that attackers hope you don't have.

This task gave me more than technical output — it gave me perspective: **security is about awareness first, then defence.**

Recommendations

If this were a real-world environment, I would suggest:

1. **Close unused ports** – Don't leave unnecessary doors open.
2. **Use firewalls effectively** – Restrict access to sensitive services.
3. **Keep systems patched** – Vulnerabilities in old versions are low-hanging fruit for attackers.
4. **Enable monitoring** – Regular scans and network monitoring tools can help spot unusual activity early.

Key Takeaways

- Port scanning is like "shaking the doorknobs" of a network harmless in practice, but dangerous in the wrong hands.
- Even simple tools like Nmap reveal **a lot of valuable information**.
- Network security starts with **visibility**: you can't defend what you don't know exists.

Interview Prep

- **What's an open port?**
  Think of it as a door to your system. If it's open, people can knock — and sometimes walk in.
- **How does a TCP SYN scan work?**
  It half-opens a connection (SYN → SYN/ACK → no final ACK) to quietly check if a port is listening, without completing the full handshake.
- **Why are open ports risky?**
  They expose services, and if those services are misconfigured or outdated, attackers can exploit them.
- **TCP vs UDP scanning?**
  TCP is like calling someone and waiting for a hello. UDP is like dropping a letter in a mailbox — you're not sure it was received unless you get a response.
- **How to secure open ports?**
  Shut the ones you don't need, restrict access, and secure the ones you do.
- **Firewall's role?**
  It's the guard at the door, deciding who gets in and who doesn't.
- **Why do attackers scan?**
  To map out the target — before breaking in, they need to know where the doors are.
- **Wireshark's role?**
  It's like CCTV for your network traffic, showing you what's happening in real-time.

Conclusion

This task was a hands-on introduction to **network reconnaissance**. It taught me how quickly a simple scan can map out a network, and why defenders must always assume attackers are watching.