Task 1: Network Port Scanning with Nmap - Internship Submission

For this task, I got hands-on experience using Nmap to scan my local network and understand how open ports can affect system security.

What I Did:

I started by installing Nmap and finding my local IP range (mine was something like 192.168.1.0/24). Then, I ran a TCP SYN scan using the command:

```
nmap -sS 192.168.1.0/24 -oN scan_results.txt
```

This helped me identify which devices were connected to my network and which ports were open on them.

Scan Results (Simplified):

- 192.168.1.1 - Port 80 open (likely my router's admin page)
- 192.168.1.3 - Port 22 open (SSH service)
- 192.168.1.5 - Port 139 open (Windows file sharing / SMB)

What I Learned:

- Open ports can expose a system to potential attacks if not properly secured.
- Services like SSH and HTTP are commonly targeted by attackers if left unprotected.
- Tools like Wireshark can be used alongside Nmap to see how packets behave during a scan (I tried this and found it super interesting!).

- Overall, this task taught me how attackers gather basic info about a network-and how we can prevent that from happening by securing or closing unused ports.

Takeaway:

This was my first time using Nmap, and it was eye-opening to see how easy it is to scan a network. It also made me more aware of how important it is to manage open ports and monitor services running on a system. Definitely a useful and practical start to cybersecurity!