Task 1 – Local Network Port Scanning (Anonymized)

Task 1 – Local Network Port Scanning (Anonymized)

Objective
The goal of this task was to identify devices in my local network and discover which ports are open. This exercise helps in understanding how exposed services can introduce potential security risks.

Steps Followed

1. Installed Nmap
Downloaded and installed the latest stable version of Nmap from the official site.

2. Found Local IP Range
Determined the local network range by checking the system network configuration. IP addresses have been anonymized in this report.

3. Performed TCP SYN Scan
Ran the following command in terminal:

```
nmap -sS
```

This scanned all active hosts in the subnet for open TCP ports.

4. Recorded Results (Anonymized)
The scan returned several devices (router, workstation, mobile device, IoT device) along with their open ports.
Example findings (anonymized):
- [Router] : Ports 53 (DNS), 80 (HTTP), 443 (HTTPS) open
- [Workstation] : Ports 22 (SSH), 135 (RPC), 445 (SMB), 3389 (RDP) open
- [Mobile] : No open TCP ports detected
- [IoT Device] : Port 1900 (UPnP) open

5. (Optional) Checked with Wireshark
Captured live packets during the scan to see the SYN/ACK exchanges. This confirmed how Nmap detects open ports without completing the full TCP handshake.

Analysis

- Common Services Identified
- Port 80/443 → Web interface (likely router admin)
- Port 53 → DNS service
- Port 135/445 → Windows RPC and file-sharing services
- Port 1900 → UPnP service (commonly used by smart devices)

- Risks

Open ports increase attack surface. For example:
- Exposed HTTP/HTTPS without strong authentication can allow brute force or misconfig exploitation.
- RPC and SMB services may be abused for lateral movement.
- UPnP can expose internal services to remote manipulation if misconfigured.

Key Learnings

- Understood how to enumerate devices and ports in a subnet.
- Learned that not all detected services are dangerous, but each open port must be justified and secured.
- Realized the importance of firewalls and service hardening in minimizing network exposure.

Securing Open Ports

- Disable unnecessary services.
- Restrict access with firewall rules.
- Keep router and OS firmware updated.
- Monitor network traffic for suspicious connections.

Repository Contents

- scan_results_anonymized.txt → Anonymized Nmap output
- README.md → Documentation (this file)

- Screenshots → Evidence of running scans and results (with sensitive data redacted)

Outcome: Gained hands-on experience in network reconnaissance and developed awareness of how attackers can use port scanning as a first step before exploitation.