Cybersecurity Task 1: Port Scanning with Nmap

Objective

To scan the local network and identify active devices, open ports, and potential security risks using Nmap.

Tools Used

- Nmap 7.97

- macOS Terminal

- (Optional) Wireshark

Installation and Setup

- Installed Nmap version 7.97 on macOS from the official website.
- Found local IP range using `ifconfig` command: `192.168.1.0/24`.
- Could not run TCP SYN scan (`-sS`) because it requires root privileges and `sudo` access was denied.
- Used TCP Connect scan (`-sT`) as an alternative without root

Scan Command and Results

bash
CopyEdit

```
nmap -sT 192.168.1.0/24
```

Scan summary:

IP Address	Open Ports	Services

192.168.1.1	80, 1900, 8080	HTTP, UPnP, HTTP-proxy
192.168.1.27	3306, 5000, 7000	MySQL, UPnP, AFS3-fileserver

Analysis of Open Ports and Services

- Port 80 (HTTP): Common web server port. Usually serves websites. Traffic is unencrypted, which can risk data interception.
- Port 1900 & 5000 (UPnP): Universal Plug and Play used for device discovery. Known to have security flaws that allow remote attacks or network exposure.
- Port 8080 (HTTP-proxy): Often used for proxy servers or alternative HTTP services. Can expose internal services if misconfigured.
- Port 3306 (MySQL): Database service. Open exposure can lead to data leakage or unauthorized database access.
- Port 7000 (AFS3-fileserver): Used by Andrew File System, less common but increases attack surface if not secured.

Detailed Device Info

Device 1 — 192.168.1.1

Latency: 0.0055s
Filtered Ports: 996
Visible Ports:

Port	State	Service	Description
23	Closed	Telnet	Telnet is disabled (good — it's insecure)
80	Open	HTTP	Web server (likely a router config page)
1900	Open	UPnP	Universal Plug and Play — risky if exposed

8080	Open	HTTP-proxy	Often used for alternate web services or admin UIs

Device 2 — 192.168.1.27

Latency: 0.00036s
Closed Ports: 997
Visible Ports:

Port	State	Service	Description
3306	Open	MySQL	Database — if exposed without auth, high risk
5000	Open	UPnP	Again, Universal Plug and Play
7000	Open	AFS3 Fileserver	Used for distributed file systems (rare at home)

Security Risk Analysis

IP Address	Port	Service	Risk Description
192.168.1.1	80	HTTP	Might expose router settings, no encryption
192.168.1.1	1900	UPnP	Often targeted for remote access vulnerabilities
192.168.1.1	8080	HTTP-proxy	Could be an alternate admin interface — secure it with a password
192.168.1.27	3306	MySQL	Databases should not be publicly exposed — needs strong password/auth setup
192.168.1.27	5000	UPnP	Same risk as above
192.168.1.27	7000	AFS3 Fileserver	Rarely used in home setups — should be disabled unless intentionally used

Identify Potential Security Risks

IP	Risk Example	Recommendation
192.168.1.1	HTTP, UPnP, HTTP-proxy exposed	Use HTTPS; disable UPnP if not required.
192.168.1.27	MySQL open to network, UPnP exposed, unused port 7000	Allow DB access only locally; disable unused ports.

Scan Results

Starting Nmap 7.97 (https://nmap.org) at 2025-05-26 17:30 +0530
Nmap scan report for 192.168.1.1
Host is up (0.0055s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT STATE SERVICE
23/tcp closed telnet
80/tcp open http
1900/tcp open upnp
8080/tcp open http-proxy

Nmap scan report for 192.168.1.27
Host is up (0.00036s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT STATE SERVICE
3306/tcp open mysql
5000/tcp open upnp
7000/tcp open afs3-fileserver

Nmap done: 256 IP addresses (2 hosts up) scanned in 95.78 seconds