**Task 1: Scan Your Local Network for Open Ports (Nmap)**

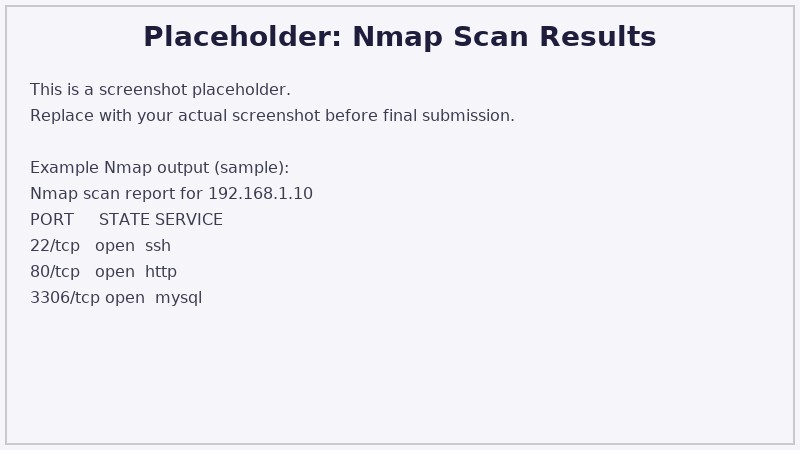
**Objective:** Discover open ports on devices in the local network to assess exposure.

**Tools Used:** Nmap (network scanner), Wireshark (optional), terminal/CLI **Procedure / Steps:**

1. Install Nmap from https://nmap.org/ or use package manager (apt/yum/choco).
2. Identify your local IP range (e.g., on Linux/Mac: `ip addr` or `ifconfig`; on Windows:

`ipconfig`).

1. Run a TCP SYN scan across the subnet: `nmap -sS 192.168.1.0/24` (replace subnet accordingly).
2. For detailed service/version detection: `nmap -sV -p- 192.168.1.0/24` or against a target IP.
3. Save results to file: `nmap -oN scan\_results.txt 192.168.1.0/24` or output as HTML for sharing.
4. (Optional) Capture packets during scanning with Wireshark for deeper analysis.
5. Analyze findings: note IPs with open ports, common services (SSH, HTTP, SMB), and high-riskports.



**Observations:**

* Open ports allow remote services to be reachable; common ports include 22 (SSH), 80/443 (HTTP/HTTPS), 3389 (RDP).
* Exposed management services on default ports increase risk of unauthorized access.
* Services with known vulnerabilities or weak configurations should be prioritized.

**Mitigation Recommendations:**

1. Disable unused services and close unnecessary ports via firewall rules (ufw/iptables/firewalld).
2. Use port forwarding and VPNs for remote admin access rather than exposing services directly.
3. Keep services updated and run vulnerability scans against detected services.
4. Implement network segmentation and apply least-privilege access.