**Task 1: Scan Your Local Network for Open Ports**

**4. Target Network 192.168.88.0/24 (Open ports):**

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

808/tcp open ccproxy-http

902/tcp open iss-realsecure

912/tcp open apex-mesh

55056/tcp closed unknown

**7. Identify potential security risks from open ports:**

| **Port** | **Service** | **Potential Security Risks** | **Recommended Action** |
| --- | --- | --- | --- |

|  |  |  |  |
| --- | --- | --- | --- |
| **135** | msrpc | - Targeted by malware (e.g., **Blaster worm**)  - Can be used for **remote code execution (RCE)** in unpatched systems |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **139** | Netbios ssn | - Supports file/printer sharing – **vulnerable to SMB relay & info disclosure** - Legacy protocol, often exploited |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **445** | microsoft-ds | - Used for **SMB (Server Message Block)** – known for vulnerabilities like **EternalBlue** (used in WannaCry) |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **808** | ccproxy-http | - May expose a **proxy service**  - If open to others, could be abused for **proxy bypass or traffic interception** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **902** | iss-realsecure | - Likely **VMware remote management port** - If exposed, attackers may gain **access to virtual machines** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **912** | apex-mesh | - Uncommon port; could be **IoT device or custom application**  - May run **unauthenticated or vulnerable services** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **55056** | unknown (closed) | - Port is **currently closed**, so **not an immediate risk** - May have been used in past |  |