task 1 - scan your local network for open ports

*Step 1 - In Cmd use ipconfig command and take the ip address.
*Step 2 - After that we are perform nmap scan using command: nmap -sS 172.90.10.0/24 for TCP SYN scan.

Scanned Devices

Device 1: 172.90.10.15

Port	Service	Risk Level	Recommendation
21/tcp	FTP	High	Disable if not needed. Use SFTP/FTPS. Enforce strong authentication, restrict access, patch regularly. FTP transmits data in plaintext, making credentials easily interceptable by attackers.
53/tcp	Domain (DNS)	Moderate-High	Ensure DNS server is properly secured. Disable zone transfers, restrict recursion, apply latest security patches, and monitor logs. Exposed DNS can be targeted for exploits, amplification attacks, or information gathering.

Explanation:
- **Port 21 (FTP):** Standard FTP is highly insecure as it transmits credentials unencrypted. Open FTP ports are frequently targeted for anonymous access or brute-forcing.
- **Port 53 (TCP DNS):** Legitimate for DNS servers, but attackers often exploit DNS services for reconnaissance, denial of service, or data exfiltration if not properly configured.

Device 2: 172.90.10.25

Port	Service	Risk Level	Recommendation
135/tcp	MSRPC	High	Block externally if not required. Apply latest security patches. Segregate network, limit access to trusted hosts. Port used for Microsoft RPC; often abused in malware propagation and lateral movement.
139/tcp	NetBIOS-SSN	High	Should not be accessible from untrusted networks. Disable if not in use, segment network, block on perimeter firewalls. NetBIOS can expose file sharing and authentication vulnerabilities.
445/tcp	Microsoft-DS	High	Critical to secure. Restrict access, patch, and disable SMBv1. Used for SMB file and printer sharing; frequent vector for ransomware and worms (e.g., EternalBlue, WannaCry)

Explanation:
- **Ports 135, 139, 445:** All associated with Windows networking, remote management, and file sharing.

- Exposure to untrusted networks creates a high risk for exploitation, as seen in past widespread attacks.
- These should not be open to the wider internet, and network segmentation and firewall rules are essential.

General Recommendations:

- Limit exposure of these ports/services to internal/trusted networks only.
- Regularly patch operating systems and related services.
- Use encryption and secure protocols where possible (e.g., SFTP instead of FTP).
- Monitor network traffic for suspicious activity on these ports.
- Disable unused services to minimize attack surface.