**Potential Security Risks From Open Ports:**

**Port 135 (TCP) – Microsoft RPC (Remote Procedure Call)**

* Used for: DCOM services like remote administration and management.
* Risks:
  + Exploitable by malware (e.g., Blaster worm, Sasser worm).
  + Can be used for remote code execution if unpatched.
  + Often targeted in DDoS attacks or information gathering.

**Port 139 (TCP) – NetBIOS Session Service**

* Used for: File and printer sharing on older Windows systems.
* Risks:
  + Allows enumeration of shares, users, and machines in a network.
  + Null sessions can be exploited for unauthenticated access.
  + Attackers can perform SMB relay attacks, which impersonate users.

**Port 445 (TCP) – Microsoft-DS (SMB over TCP)**

* Used for: File sharing, printer sharing, Windows authentication.
* Risks:
  + High-value target for ransomware (e.g., WannaCry, NotPetya).
  + Vulnerable to EternalBlue and SMBGhost (CVE-2020-0796) exploits.
  + Can be used for lateral movement and privilege escalation in a network.

**Mitigation Recommendations:**

1. Block Ports 135, 139, and 445 from external access (firewall or router).
2. Use firewalls to restrict traffic to only necessary systems.
3. Apply all patches and updates—especially for SMB vulnerabilities.
4. Disable unused services if not required .
5. Use network segmentation to isolate high-value systems.
6. Monitor with IDS/IPS tools for exploitation attempts.