1. Ip address - Host: 10.0.2.2

Open Ports:

1. 135/tcp (msrpc)

Threat: Common in Windows. Can be exploited by malware (e.g., Blaster worm), used in lateral movement and privilege escalation.

Mitigation: Disable if not needed, use firewall rules to restrict access.

1. 445/tcp (microsoft-ds)

Threat: SMB protocol. Vulnerable to exploits like EternalBlue (used by WannaCry).

Mitigation: Patch the system, disable SMBv1, restrict to trusted IPs.

1. 3306/tcp (MySQL)

Threat: If exposed, attackers could brute-force credentials or exploit known MySQL vulnerabilities.

Mitigation: Never expose MySQL externally, use strong credentials, limit access by IP.

2. Ip address-Host: 10.0.2.3

Open Port:

1. 53/tcp (domain)

Threat: Usually DNS. If misconfigured, could be abused for DNS amplification DDoS attacks or data exfiltration.

Mitigation: Restrict to internal use, monitor traffic, disable recursion if not required.

3. Ip address-Host: 10.0.2.15

All 1000 ports closed / ignored

Threat: None currently visible, but the system could be stealthy or behind a firewall.

---