Automated Vulnerability Report

>> Port 135 (msrpc) [!][!][!][!][!]

1. Explanation: Port 135 is used by Microsoft's Remote Procedure Call (RPC) service, which allows communication between processes on remote servers.

2. Security Risk: The msrpc service on port 135 is often targeted by attackers due to its history of vulnerabilities, including buffer overflows and remote code execution flaws.

3. Remediation: To secure Port 135, you should:

   - Patch your system with the latest updates provided by Microsoft.

   - Implement proper firewall rules to restrict access to this port.

   - Consider using network segmentation to isolate critical servers from direct exposure to the internet.

>> Port 445 (microsoft-ds) [!][!][!]

1. Explanation: Port 445 is used by Microsoft-DS (Directory Services) for file sharing and printer services on Windows systems.

2. Security Risk: This service is prone to attacks like the infamous EternalBlue exploit, allowing remote code execution and lateral movement in a network.

3. Remediation: To enhance the security of Port 445:

   - Ensure that systems are patched with the latest security updates from Microsoft.

   - Disable SMBv1 if not required and implement SMB signing.

   - Restrict access to this port to only trusted IP addresses.

>> Port 3306 (mysql) [!][!][!]

1. Explanation: Port 3306 is commonly used by MySQL database servers for data storage and retrieval.

2. Security Risk: Running MySQL on this port could expose sensitive data to unauthorized access or potential SQL injection attacks if not properly configured.

3. Remediation: To secure Port 3306:

   - Implement strong passwords and user authentication for MySQL.

   - Regularly update MySQL to the latest version and apply security patches.

- Utilize network security measures like VPNs or SSH tunnels for remote access to the MySQL server.