Vulnerability Assessment Report - Metasploitable2

1. Executive Summary

This assessment identifies high-risk services exposed on a deliberately vulnerable system using Nmap. It is part of a home lab security portfolio project and simulates attacker behavior for learning purposes.

2. Scope

Target: 192.168.176.4

Tool Used: Nmap

Tester: Prince Solanki

Date: 2025-06-07

3. Methodology

A network scan was conducted using Nmap with service and script detection enabled. The goal was to identify open ports, running services, and potential vulnerabilities.

4. Findings

Port	Service	Version	Risk	Notes
21	FTP	vsftpd 2.3.4	High	Known backdoor vulnerability
23	Telnet	Open	High	Unencrypted login
3306	MySQL	5.x	Medium	Possible default credentials
139/445	Samba	3.x	Medium	Potential EternalBlue vector
8180	Tomcat	7.x?	Medium	Likely admin panel

5. Recommendations

- Disable insecure services such as FTP and Telnet
- Apply security patches and use updated OS images
- Implement network segmentation and firewall rules
- Use strong authentication on all exposed services

6. Conclusion

This scan highlights real risks of using default configurations and outdated services. Regular scanning,

patching, and basic hardening measures are essential to maintain security.