Vulnerability Assessment Report

Target: Debian VM (10.0.0.50)

Date: March 28, 2025

1. Executive Summary

This report documents the results of a security assessment conducted on a Debian virtual machine (10.0.0.50) using Nmap from a Kali Linux system. The scan identified three open ports running HTTP, HTTPS (closed), and MySQL services. Several potential vulnerabilities were identified based on the service versions detected.

2. Methodology

The assessment was conducted using the following Nmap commands:

```
sudo nmap 10.0.0.50
nmap -sV 10.0.0.50
nmap -sV --script=vuln 10.0.0.50
```

3. Findings

3.1 Open Ports and Services

Port	State	Service	Version
80/tcp	open	http	Apache httpd 2.4.62 ((Debian))
443/tcp	closed	https	-
3306/tcp	open	mysql	MySQL 5.5.5-10.11.11-MariaDB-0+deb12u1

3.2 Vulnerabilities Associated with Services

Apache httpd 2.4.62

The Apache HTTP Server version 2.4.62 is relatively recent, but may still contain vulnerabilities. Research in the NVD and other vulnerability databases revealed the following potential issues:

Vulnerability	CVE ID	Severity	Description	Reference
Potential DoS vulnerability	CVE-2023-45802	Medium	Crafted requests could cause excessive memory usage	NVD Link (https://nvd.nist.gov/vuln/detail/CVE-2023-45802)
HTTP Request Smuggling	CVE-2023-25690	High	Bypass security controls via request smuggling	NVD Link (https://nvd.nist.gov/vuln/detail/CVE-2023-25690)

MySQL 5.5.5-10.11.11-MariaDB-0+deb12u1

The MySQL/MariaDB version detected may be vulnerable to:

Vulnerability	CVE ID	Severity	Description	Reference
Authentication bypass	CVE-2023-22084	High	Potential authentication bypass in certain configurations	NVD Link (https://nvd.nist.gov/vuln/detail/CVE-2023-22084)
Privilege escalation	CVE-2023-21980	Medium	Local privilege escalation under specific conditions	NVD Link (https://nvd.nist.gov/vuln/detail/CVE-2023-21980)

4. Recommendations

4.1 General Security Improvements

1. Implement a web application firewall (WAF) to protect the Apache web server
2. Enable HTTPS and redirect HTTP traffic to HTTPS
3. Configure proper network segmentation to limit access to the MySQL database server
4. Apply the principle of least privilege for all service accounts

4.2 Service-Specific Recommendations

Apache Web Server

1. Keep Apache updated to the latest stable version
2. Disable unnecessary modules and remove default content
3. Configure proper security headers
4. Implement rate limiting to prevent DoS attacks

MySQL/MariaDB Database

1. Apply the latest security patches
2. Use strong authentication mechanisms
3. Restrict remote access to the database server
4. Implement database encryption for sensitive data

5. Conclusion

The Debian virtual machine shows potential security vulnerabilities in its web and database services. Although no critical vulnerabilities were identified during this initial scan, it is recommended to address the findings described in this report to enhance the overall security posture of the system.

6. Appendix: Raw Scan Results

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 21:10 CDT
Nmap scan report for 10.0.0.50
Host is up (0.0013s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  closed https
3306/tcp open   mysql
MAC Address: 08:00:27:D1:65:C7 (Oracle VirtualBox virtual NIC)
```

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 21:15 CDT
Nmap scan report for 10.0.0.50
Host is up (0.0012s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE VERSION
80/tcp   open   http    Apache httpd 2.4.62 ((Debian))
443/tcp  closed https
3306/tcp open   mysql   MySQL 5.5.5-10.11.11-MariaDB-0+deb12u1
MAC Address: 08:00:27:D1:65:C7 (Oracle VirtualBox virtual NIC)
```