# Vulnerability Scanning Lab

## 1. Executive Summary

Host **192.168.0.16 (Metasploitable2)** exposed multiple critical vulnerabilities including outdated services, remote command execution vectors, directory indexing, PHP info disclosure, and misconfigured Apache/PHP modules. The system is highly exploitable and must not be exposed to any production network.

## 2. Lab Environment Setup

**Attacker Machine:**

- **Kali Linux** (VMware)
- Tools: Nmap, OpenVAS, Nikto

**Target Machine:**

- **Metasploitable2** (IP: 192.168.0.16)

Both machines were placed in the same Bridged network.

## 3. Scanning Activities

### 3.1 Nmap Scan

Command run:

nmap -sV  192.168..16

**Results (Summary):**

- Multiple open ports: 21, 22, 23, 25, 80, 139, 445, 3306
- Detected vulnerable services:
    - vsftpd 2.3.4 (Backdoor vulnerability)
    - Apache 2.2.8 (CVE-2021-41773 path traversal)
    - SMB (MS08-067 vulnerability)

### 3.2 OpenVAS Scan

A full and fast scan was executed.

**Findings:**

- Critical: Apache Path Traversal (CVE-2021-41773)
- High: SMB Remote Code Execution (MS08-067)
- Medium: Open Port 445 (Unrestricted access)
- Medium: Weak FTP service

### 3.3 Nikto Scan

Command:

nikto -h http://192.168.0.16

Findings:

- Apache outdated version (2.2.8)
- Directory traversal risk
- Default files and banners exposed

### 4. Vulnerability Prioritization Table

**Host: 192.168.0.16(metasploitable2)**

| Priority | CVSS Range | Vulnerabilities Found |
|---|---|---|
| **Critical (9.0–10.0)** | **10.0 – 9.8** | • TWiki XSS + Command Execution (10.0)<br>• rexec service running (10.0)<br>• MySQL/MariaDB default credentials (9.8)<br>• vsftpd backdoor (9.8)<br>• PHP multiple vulnerabilities (9.8)<br>• Apache Tomcat Ghostcat RCE (9.8 |
| **High (7.0–8.9)** | **8.9-1.0** | • DistCC RCE (9.3)<br>• UnrealIRCd authentication spoof (8.1)<br>• rlogin service (7.5)<br>• UnrealIRCd backdoor (7.5)<br>• FTP brute force / default creds (7.5)<br>• rsh cleartext login (7.5)<br>• OpenSSL CCS MITM (7.4) |
| **Medium (4.0–6.9)** | **6.9 – 4.0** | • TWiki CSRF (6.8)<br>• STARTTLS plaintext injection (6.8)<br>• Anonymous FTP login (6.4)<br>• TWiki < 6.1.0 XSS (6.1)<br>• jQuery < 1.9 XSS (6.1)<br>• Samba trans2 RCE (6.0)<br>• Weak SSL/TLS ciphers (5.9)<br>• Deprecated SSLv2/SSLv3 (5.9)<br>• TRACE/TRACK enabled (5.8)<br>• phpinfo() exposed (5.3)<br>• TLS renegotiation DOS (5.0)<br>• Directory Browsing (/doc) (5.0)<br>• QWikiwiki path traversal (5.0)<br>• phpMyAdmin XSS (4.3)<br>• Apache httpOnly cookie info disclosure (4.3)<br>• Deprecated TLSv1.0/1.1 (4.3)<br>• LogJam DHE_EXPORT MITM (4.3) |
| **Low (< 4.0)** | **3.9 – 0.0** | • SSLv3 CBC info leak (3.4)<br>• ICMP Timestamp Reply (2.1) |

### 5. Detailed Findings (Based on OpenVAS Scan for 192.168.0.16)

### 5.1 Critical Severity Findings (CVSS 9.0 – 10.0)

#### 5.1.1 TWiki XSS and Command Execution Vulnerabilities

**CVEs:** CVE-2008-5304, CVE-2008-5305
**CVSS Score:** 10.0
**Affected Host:** 192.168.0.16
**Description:**
TWiki contains multiple vulnerabilities allowing attackers to perform XSS attacks and execute system commands remotely.

**Impact:**

- Remote command execution
- Compromise of full server
- Lateral movement

**Evidence:**
Detected by OpenVAS with severity 10.0.

### 5.1.2 Rexec Service Running

**CVE:** CVE-1999-0618
**CVSS Score:** 10.0
**Affected Host:** 192.168.0.16
**Description:**
The *rexec* service is enabled, which allows remote command execution using plaintext authentication.
**Impact:**

- Full remote command execution
- Credential compromise (cleartext)

**Evidence:**
OpenVAS detected the rexec service enabled and accessible.

### 5.1.3 MySQL / MariaDB Default Credentials

**CVEs:** Multiple (incl. CVE-2001-0645 … CVE-2024-22901)
**CVSS Score:** 9.8
**Affected Host:** 192.168.0.16
**Description:**
The MySQL server on this host is using **default or weak credentials**, allowing unauthorized access.
**Impact:**

- Full database compromise
- Data extraction or deletion
- Remote code execution via SQL functions

**Evidence:**
OpenVAS authenticated using default credentials over the MySQL protocol.

### 5.1.4 vsftpd 2.3.4 Backdoor Vulnerability

**CVE:** CVE-2011-2523
**CVSS Score:** 9.8
**Affected Host:** 192.168.0.16
**Description:**
vsftpd 2.3.4 contains a backdoor where typing a username ending with ":)" spawns a remote shell.

**Impact:**

- Unauthenticated remote shell
- Complete system takeover

**Evidence:**
OpenVAS detected vulnerable version and backdoor pattern.

### 5.1.5 PHP Multiple Vulnerabilities (Pre-5.3.13)

**CVEs:** CVE-2012-1823, CVE-2012-2335, etc.
**CVSS Score:** 9.8
**Affected Host:** 192.168.0.16
**Description:**
Several PHP vulnerabilities allow remote code execution, information leakage, and bypasses.
**Impact:**

- Code execution on server
- Information disclosure
- Web application compromise

**Evidence:**
Version check by OpenVAS showed PHP <5.3.13/5.4.3.

### 5.1.6 Apache Tomcat AJP (Ghostcat RCE)

**CVE:** CVE-2020-1938
**CVSS Score:** 9.8
**Description:**
Ghostcat allows attackers to read or include arbitrary files using the AJP connector.
**Impact:**

- RCE through JSP upload
- Webroot file access

**Evidence:**
AJP port detected and confirmed by OpenVAS script.

### 5.1.7 DistCC Remote Code Execution

**CVE:** CVE-2004-2687
**CVSS Score:** 9.3
**Description:**
DistCC service allows unauthenticated remote commands.
**Impact:**

- Server takeover
- Botnet recruitment

**Evidence:**
Service fingerprinting by OpenVAS.

### 5.2 High Severity Findings (CVSS 7.0 – 8.9)

#### 5.2.1 UnrealIRCd Authentication Spoofing

**CVE:** CVE-2016-7144
**CVSS Score:** 8.1
**Description:**
UnrealIRCd contains an authentication bypass flaw allowing attackers to spoof identity.
**Impact:**

- Unauthorized admin access
- Data leakage

#### 5.2.2 rlogin Service Running

**CVE:** CVE-1999-0651
**CVSS Score:** 7.5
**Description:**
rlogin transmits all data in plaintext and is unsafe.
**Impact:**

- Credential theft
- Remote execution

#### 5.2.3 UnrealIRCd Backdoor

**CVE:** CVE-2010-2075
**CVSS Score:** 7.5
**Description:**
This backdoored version allows remote shell execution.
**Impact:**

- Automatic root compromise

#### 5.2.4 FTP Default Credential Brute-Force Success

**CVEs:** Multiple legacy FTP CVEs
**CVSS Score:** 7.5
**Description:**
FTP server accepts common default credentials or weak passwords.
**Impact:**

- Attackers gain access to file system

#### 5.2.5 rsh Cleartext Login

**CVE:** CVE-1999-0651
**CVSS Score:** 7.5
**Description:**
rsh allows logins without encryption.

**Impact:**

- Credential interception
- Remote execution

**5.2.6 OpenSSL CCS Injection MitM**

**CVE:** CVE-2014-0224

**CVSS Score:** 7.4

**Description:**

A flaw in OpenSSL enables man-in-the-middle attacks.

**Impact:**

- Traffic hijacking

**5.3 Medium Severity Findings (CVSS 4.0 – 6.9)**

(Only main ones summarized)

**5.3.1 TWiki CSRF / XSS / Directory Issues**

- CVSS 6.8, 6.1, 6.0
- Multiple TWiki flaws including CSRF, XSS, and directory traversal.

**Impact:**

- Session hijacking
- Privilege escalation

**5.3.2 Anonymous FTP Login**

**CVSS:** 6.4

**Impact:**

- Attackers can browse FTP directories

**5.3.3 Samba Remote Command Execution (CVE-2007-2447)**

**CVSS:** 6.0

**Impact:**

- Remote system compromise

**5.3.4 Weak/Deprecated SSL Protocols**

**CVSS:** 5.9–5.0

Includes:

- SSLv2/SSLv3 enabled
- Weak cipher suites
- RSA_EXPORT / DHE_EXPORT

**Impact:**

- MITM attacks
- Encrypted traffic downgrade

**5.3.5 phpinfo() Exposure**
**CVSS:** 5.3
**Impact:**

- Information leakage
- Sensitive configuration exposure

**5.3.6 Directory Browsing Enabled (/doc)**
**CVSS:** 5.0
**Impact:**

- Leakage of internal files

**5.3.7 phpMyAdmin XSS**
**CVSS:** 4.3
**Impact:**

- Session hijacking

**5.4 Low Severity Findings (CVSS < 4.0)**

**5.4.1 SSLv3 CBC Information Disclosure (POODLE related)**
**CVSS:** 3.4
**Impact:**

- Traffic decrypted under certain conditions

**5.4.2 ICMP Timestamp Disclosure**
**CVSS:** 2.1
**Impact:**

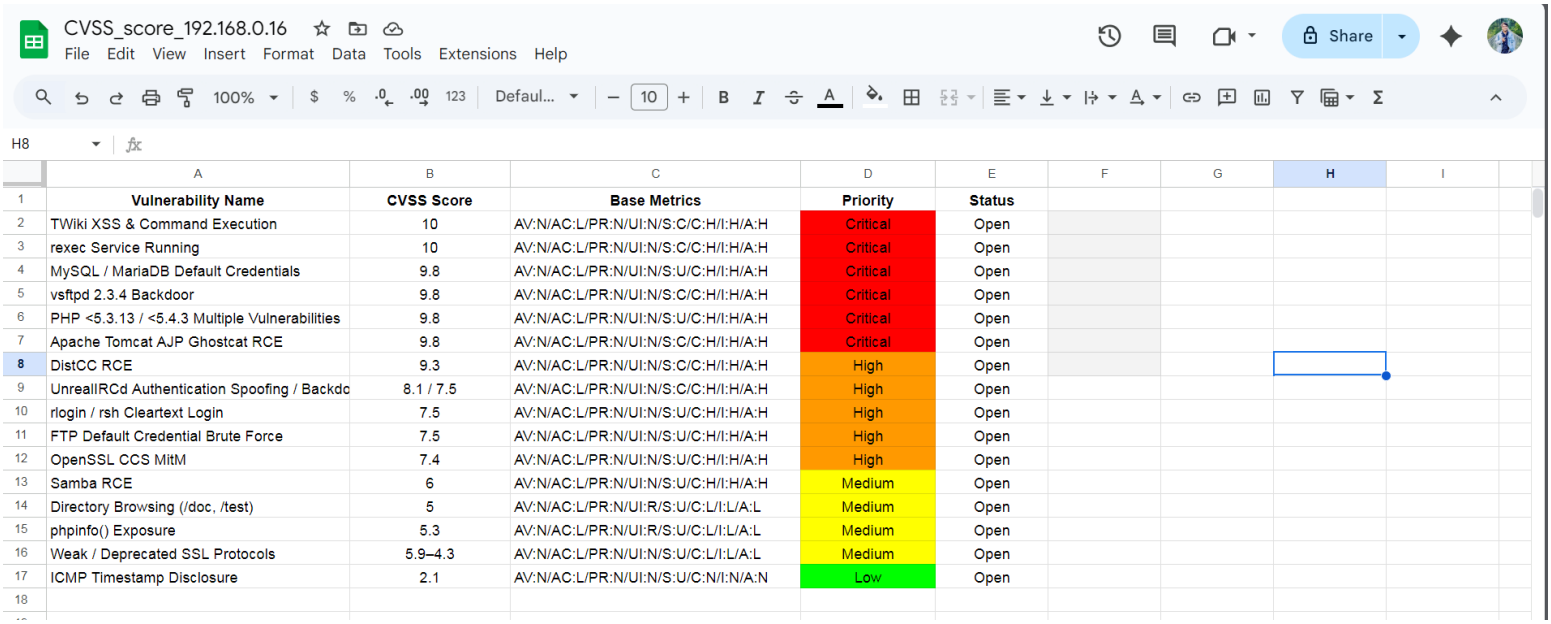
- Reveals system uptime for reconnaissance

## 6. Remediation Recommendations

| Vulnerability | CVSS Score | Recommended Fix |
|---|---|---|
| TWiki XSS & Command Execution (CVE-2008-5304, CVE-2008-5305) | 10.0 | Upgrade TWiki to the latest secure version. Apply patches, remove test content, and disable unsafe scripting features. Restrict admin access. |
| rexec Service Running (CVE-1999-0618) | 10.0 | Disable the rexec service entirely. Use SSH with key-based authentication for remote commands. |
| MySQL / MariaDB Default Credentials (Multiple CVEs) | 9.8 | Change default credentials immediately. Enforce strong passwords and restrict remote root login. Enable SSL for connections. |
| vsftpd 2.3.4 Backdoor (CVE-2011-2523) | 9.8 | Remove or upgrade vsftpd to a secure version. Disable anonymous login. Block FTP access from untrusted networks. |
| PHP < 5.3.13 / < 5.4.3 Multiple Vulnerabilities | 9.8 | Upgrade PHP to the latest supported version. Apply all security patches. Disable unused modules and phpinfo() in production. |
| Apache Tomcat AJP Ghostcat RCE (CVE-2020-1938) | 9.8 | Disable the AJP connector if not required. Apply the latest Tomcat patches and restrict access to trusted hosts. |
| DistCC RCE (CVE-2004-2687) | 9.3 | Disable the DistCC service or restrict it to localhost only. Apply updates if required. |
| UnrealIRCd Authentication Spoofing / Backdoor (CVE-2016-7144 / CVE-2010-2075) | 8.1 / 7.5 | Upgrade UnrealIRCd to the latest secure version. Restrict IRC access and monitor logs for unauthorized connections. |
| rlogin / rsh Cleartext Login | 7.5 | Disable rlogin and rsh. Use SSH with key-based authentication. |
| FTP Default Credential Brute Force | 7.5 | Enforce strong passwords. Disable anonymous logins. Implement account lockout policies. |
| OpenSSL CCS MitM (CVE-2014-0224) | 7.4 | Update OpenSSL to latest version. Disable SSLv2/SSLv3. Use TLS 1.2+ only. |
| Samba RCE (CVE-2007-2447) | 6.0 | Upgrade Samba to latest supported version. Restrict access and disable SMBv1. |
| Directory Browsing Enabled (/doc, /test) | 5.0 | Disable directory indexing in Apache (Options -Indexes). Restrict access to sensitive directories. |
| phpinfo() Exposure | 5.3 | Remove or restrict access to phpinfo.php. Only allow admin/internal access if needed. |
| Weak / Deprecated SSL Protocols (SSLv2, SSLv3, TLS1.0/1.1) | 5.9–4.3 | Disable weak protocols and ciphers. Enforce TLS 1.2+ with strong cipher suites. |
| ICMP Timestamp Disclosure | 2.1 | Disable ICMP timestamp responses in firewall or kernel settings. |

## 7. Prioritization Using CVSS

A Google Sheet was created to calculate and sort vulnerabilities based on **CVSS Base Scores**, which helps prioritize remediation effectively.




| | A | B | C | D | E | F | G | H | I |
|---|---|---|---|---|---|---|---|---|---|
| 1 | **Vulnerability Name** | **CVSS Score** | **Base Metrics** | **Priority** | **Status** | | | | |
| 2 | TWiki XSS & Command Execution | 10 | AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H | Critical | Open | | | | |
| 3 | rexec Service Running | 10 | AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H | Critical | Open | | | | |
| 4 | MySQL / MariaDB Default Credentials | 9.8 | AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | Critical | Open | | | | |
| 5 | vsftpd 2.3.4 Backdoor | 9.8 | AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H | Critical | Open | | | | |
| 6 | PHP <5.3.13 / <5.4.3 Multiple Vulnerabilities | 9.8 | AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | Critical | Open | | | | |
| 7 | Apache Tomcat AJP Ghostcat RCE | 9.8 | AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H | Critical | Open | | | | |
| 8 | DistCC RCE | 9.3 | AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H | High | Open | | | | |
| 9 | UnrealIRCd Authentication Spoofing / Backdc | 8.1 / 7.5 | AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H | High | Open | | | | |
| 10 | rlogin / rsh Cleartext Login | 7.5 | AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | High | Open | | | | |
| 11 | FTP Default Credential Brute Force | 7.5 | AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | High | Open | | | | |
| 12 | OpenSSL CCS MitM | 7.4 | AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | High | Open | | | | |
| 13 | Samba RCE | 6 | AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | Medium | Open | | | | |
| 14 | Directory Browsing (/doc, /test) | 5 | AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L | Medium | Open | | | | |
| 15 | phpinfo() Exposure | 5.3 | AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L | Medium | Open | | | | |
| 16 | Weak / Deprecated SSL Protocols | 5.9–4.3 | AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L | Medium | Open | | | | |
| 17 | ICMP Timestamp Disclosure | 2.1 | AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N | Low | Open | | | | |
| 18 | | | | | | | | | |

# 8. Escalation Email for 192.168.0.16

**Title:** Critical Web Vulnerabilities

**Findings:**

- **Host:** 192.168.0.16
- **Critical Vulnerabilities:**
  - TWiki XSS & Command Execution (CVE-2008-5304, CVE-2008-5305)
  - vsftpd 2.3.4 Backdoor (CVE-2011-2523)
  - Apache Tomcat Ghostcat AJP RCE (CVE-2020-1938)
  - MySQL / MariaDB Default Credentials (Multiple CVEs)
  - rexec Service Running (CVE-1999-0618)

**Remediation:**

- Update all affected software to latest secure versions.
- Remove or disable vulnerable services (vsftpd, rexec).
- Restrict access to sensitive directories and admin panels.
- Apply all security patches and disable unused ports/services.

**Subject:** Critical Vulnerabilities Identified on Host 192.168.0.16

Dear Team,

During a vulnerability assessment on **192.168.0.16**, several critical issues were found, including **TWiki XSS/Command Execution**, **vsftpd backdoor**, **Ghostcat Tomcat AJP RCE**, and **MySQL default credentials**. PoC testing confirms attackers can execute arbitrary commands, access sensitive data, and compromise the system.

Immediate action is required: update vulnerable software, remove backdoors, disable unused services, and apply security patches. These steps are critical to prevent potential exploitation and protect system integrity.

Regards,
Arabi Basnet
Security Analyst (VAPT)