

Project Title: Vulnerability Assessment

Scope and Objective: The objective of this assessment is to identify, verify, and analyze security vulnerabilities in a Metasploitable2 virtual machine through automated scanning and manual testing within a controlled lab environment. This document includes a prioritized list of findings, manual verification, and remediation guidance, following standard cybersecurity practices.

Executive Summary

A vulnerability scan and manual verification were conducted on a target machine (10.138.16.138) to simulate an internal attacker's perspective. The testing identified several critical and high-risk vulnerabilities including exploitable services, outdated software, and misconfigurations. Immediate remediation is advised to reduce the attack surface.

1. Automated Vulnerability Scan


Tool Used: Nmap

Command:

```
nmap --script vuln -p- -T4 -oN vulnscan.txt 10.138.16.138
```

Findings:

- **vsFTPD 2.3.4 backdoor** – CVE-2011-2523 – Exploitable
- **Anonymous DH TLS cipher** – susceptible to MitM
- **SSL POODLE vulnerability** – CVE-2014-3566
- **Apache HTTP SQL Injection potential** – on multiple endpoints
- **RMI Java registry remote code execution** – default configuration
- **distccd remote code execution** – CVE-2004-2687
- **CSRF vulnerabilities** on several forms
- **Apache Slowloris DoS** – CVE-2007-6750

 Evidence from `vulnscan.txt` (in the repository in the penetration testing folder) confirms vulnerabilities with script references and CVE links.

2. Manual Vulnerability Verification

FTP Anonymous Login:

- **Command:** `ftp 10.138.16.138`
- **Login:** anonymous / blank password
- **Result:** Login successful

```
#ftp 10.138.16.138
Connected to 10.138.16.138.
220 (vsFTPD 2.3.4)
Name (10.138.16.138:user): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

- **Verification:** Confirms weak access control on public service

Apache Banner Grabbing:

- **Command:** `curl -I http://10.138.16.138`
- **Result:** Apache/2.2.8 running with PHP/5.2.4
- **Verification:** Version is outdated and known to contain multiple vulnerabilities

```
#curl -I http://10.138.16.138
HTTP/1.1 200 OK
Date: Wed, 02 Apr 2025 21:05:30 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Type: text/html
```

3. Prioritized Vulnerability Table

| Vulnerability | CVE ID(s) | Risk Level | Justification |
|------------------------------|---------------|------------|----------------------------------------------|
| vsFTPD Backdoor | CVE-2011-2523 | Critical | Allows remote root shell access |
| distccd Command Execution | CVE-2004-2687 | High | Arbitrary command execution |
| RMI Registry RCE | - | High | Java RCE via remote class loading |
| Anonymous FTP Login | - | High | Allows file access without authentication |
| Apache/2.2.8 SQL Injection | - | High | Detected injection points in web app URLs |
| SSL POODLE / Weak DH Ciphers | CVE-2014-3566 | Medium | Allows MitM attacks |
| Apache Slowloris | CVE-2007-6750 | Medium | DoS potential via HTTP connection starvation |
| CSRF on multiple login forms | - | Medium | Exploitable session manipulation |

4. Remediation Recommendations

- **Upgrade or remove vsFTPD 2.3.4** – Use secure alternatives like SFTP.
- **Harden Apache and update to latest stable version.**
- **Patch all services (Apache, PHP, OpenSSL, MySQL, etc.).**
- **Disable anonymous FTP access.**
- **Remove or restrict distccd and RMI registry exposure.**
- **Use strong TLS configurations and disable SSLv3/weak DH ciphers.**
- **Mitigate web application issues:** sanitize inputs, implement CSRF tokens.

5. Testing Evidence

- `vulnscan.txt` includes automated results with CVE IDs and Nmap script output.
- FTP login screenshot confirms anonymous access.
- `curl` screenshot shows Apache and PHP versions.
- Traffic capture file (`capture.pcap`) shows FTP login behavior.

