vapt

(By PRIYANK KUMAR)

Vulnerability Assessment Report

Title : Critical Web Vulnerabilities – Metasploitable2

1. Executive Summary

This vulnerability assessment was conducted on a Metasploitable2 virtual machine to identify security weaknesses using automated and manual scanning techniques. Tools such as **Nmap, OpenVAS, and Nikto** were used to discover open services, outdated software, and misconfigurations. Multiple high and critical vulnerabilities were identified that could allow an attacker to gain unauthorized access, execute remote code, or compromise sensitive data. Immediate remediation is recommended to reduce the attack surface and improve the overall security posture.

2. Scope of Assessment

- **Target Host:** 192.168.79.129
- **Environment:** Local lab (Metasploitable2 VM)
- **Assessment Type:** Vulnerability Scanning (Non-Intrusive)
- **Out of Scope:** Denial of Service (DoS), brute force attacks

3. Tools Used

Tool	Purpose
Nmap	Port scanning & service enumeration
OpenVAS	Vulnerability detection & CVSS scoring
Nikto	Web server vulnerability scanning

4. Methodology

The assessment followed a standard vulnerability assessment workflow:

1. **Discovery** – Identify live host and open ports using Nmap
2. **Enumeration** – Detect running services and versions
3. **Vulnerability Scanning** – Identify known vulnerabilities using OpenVAS and Nikto
4. **Risk Prioritization** – Classify findings using CVSS scoring
5. **Documentation** – Record findings and remediation steps

5. Vulnerability Scan Results (Prioritized)

Scan ID	Vulnerability	CVSS Score	Priority	Host
001	Outdated Apache Web Server	9.1	Critical	192.168.79.129
002	Exposed phpMyAdmin Interface	8.2	High	192.168.79.129
003	Multiple Open Services Detected	7.5	High	192.168.79.129
004	Directory Indexing Enabled	6.5	Medium	192.168.79.129

vapt

(By PRIYANK KUMAR)

6. Detailed Findings

Finding 1: Outdated Apache Web Server

- **Scan ID:** 001
- **Severity:** Critical
- **CVSS Score:** 9.1
- **Affected Host:** 192.168.79.129
- **Tool Used:** OpenVAS / Nikto
- **Related CVE:** CVE-2021-41773

Description:
The Apache web server running on the target system is outdated and vulnerable to known remote path traversal and potential remote code execution attacks.
Impact:
An attacker may exploit this vulnerability to read sensitive files, execute arbitrary commands, or fully compromise the web server.

Finding 2: Exposed phpMyAdmin Interface

- **Scan ID:** 002
- **Severity:** High
- **CVSS Score:** 8.2
- **Affected Host:** 192.168.79.129
- **Tool Used:** Nikto

Description:
The phpMyAdmin interface is publicly accessible without proper access restrictions.
Impact:
Attackers could attempt credential brute forcing or exploit known phpMyAdmin vulnerabilities to gain database access.

Finding 3: Multiple Open Services Detected

- **Scan ID:** 003
- **Severity:** High
- **CVSS Score:** 7.5
- **Affected Host:** 192.168.79.129
- **Tool Used:** Nmap

Description:
Multiple unnecessary services such as FTP, SSH, SMB, and MySQL are exposed, increasing the attack surface.
Impact:
An attacker could exploit vulnerable services to gain unauthorized access or escalate privileges.

vapt

(By PRIYANK KUMAR)

Finding 4: Directory Indexing Enabled

- **Scan ID:** 004
- **Severity:** Medium
- **CVSS Score:** 6.5
- **Affected Host:** 192.168.79.129
- **Tool Used:** Nikto

Description:
Directory listing is enabled on the web server, allowing users to view file structures.
Impact:
Sensitive information disclosure that may assist attackers in further exploitation.

7. Remediation Recommendations

Vulnerability	Recommendation
Outdated Apache	Patch or upgrade Apache to the latest secure version
Exposed phpMyAdmin	Restrict access using authentication or IP whitelisting
Open Services	Disable unused ports and services
Directory Indexing	Disable directory listing in web server configuration

8. Risk Prioritization Summary

- **Critical:** 1
- **High:** 2
- **Medium:** 1
- **Low:** 0

Immediate remediation is required for **Critical and High** severity vulnerabilities.

9. Conclusion

The vulnerability scan identified several serious security weaknesses on the Metasploitable2 system. If exploited, these vulnerabilities could result in full system compromise.
Implementing the recommended remediation steps and performing a follow-up scan will significantly improve the system's security posture.