Vulnerability Scanning Lab Report

Title: Critical Web Vulnerabilities Assessment
Target Host: 192.168.43.131
Environment: Metasploitable2 (Lab)
Tools Used: Nmap, OpenVAS, Nikto

1. Executive Summary

A vulnerability assessment was conducted against the target host **192.168.43.131** to identify security weaknesses that could lead to system compromise. The assessment revealed multiple **critical and high-risk vulnerabilities**, including default database credentials, exposed backdoor services, outdated operating systems, and remote code execution flaws in Apache Tomcat.

The system is highly vulnerable and can be compromised with minimal effort. Immediate remediation is required to prevent unauthorized access, data leakage, and full system takeover.

2. Scope and Methodology

Scope

- Single target IP: **192.168.43.131**
- Web services, database services, OS-level vulnerabilities

Methodology

The assessment followed **PTES-aligned vulnerability scanning** steps:

1. Service discovery using **Nmap**
2. Web vulnerability scanning using **Nikto**
3. Authenticated and unauthenticated vulnerability detection using **OpenVAS**
4. CVSS-based risk prioritization
5. Documentation and remediation planning

3. Tools Used

Tools	Purpose
Nmap	Port scanning and service/version detection
Nikto	Web server misconfiguration and vulnerability detection
OpenVAS	Automated vulnerability scanning and CVSS scoring

4. Scan Results Summary (Table)

Scan ID	Vulnerability	CVSS Score	Priority	Host
001	SQL Injection	9.1	Critical	192.168.43.131
002	Open Port 445	6.5	Medium	192.168.43.131
003	MySQL Default Credentials	9.8	Critical	192.168.43.131
004	Apache Tomcat RCE	9.8	Critical	192.168.43.131
005	Possible Backdoor (Ingreslock)	10.0	Critical	192.168.43.131
006	OS End of Life	10.0	Critical	192.168.43.131

5. Detailed Findings

5.1 Open Ports and Services (Nmap)

Nmap scan revealed multiple unnecessary and insecure services, including FTP, Telnet, SMB, MySQL, PostgreSQL, and Tomcat.

Key Risks:

- Telnet transmits credentials in plaintext
- SMB (445) exposed to network attacks
- MySQL accessible remotely
- Backdoor service running on port 1524

Impact:

Attackers can enumerate services, brute-force credentials, and exploit known vulnerabilities.

5.2 Web Server Vulnerabilities (Nikto)

- Nikto identified severe web misconfigurations:
- Directory indexing enabled
- `phpinfo()` exposed
- phpMyAdmin publicly accessible
- HTTP TRACE method enabled (XST attack)
- Apache 2.2.8 (EOL)

Impact:

Sensitive system information disclosure and increased attack surface for exploitation.

5.3 MySQL Default Credentials (OpenVAS)

CVSS: 9.8 (Critical)

Finding: Login possible as `root` with empty password

Impact:

Complete database compromise, data theft, and privilege escalation.

5.4 Apache Tomcat Ghostcat Vulnerability

CVE: CVE-2020-1938
CVSS: 9.8 (Critical)

The AJP connector allows unauthorized access to internal configuration files such as `/WEB-INF/web.xml`.

Impact:
Remote Code Execution (RCE) and full server compromise.

5.5 Possible Backdoor – Ingreslock

CVSS: 10.0 (Critical)
Port: 1524

The service responds to system commands and returns **root-level output**.

Impact:
Attackers can execute arbitrary commands as root, resulting in total system takeover.

5.6 Operating System End of Life

OS: Ubuntu 8.04 (EOL since 2013)
CVSS: 10.0 (Critical)

Impact:
No security patches available, exposing the system to all known exploits.

6. Risk Prioritization (CVSS-Based)

- **Immediate (Critical):** Backdoor, Tomcat RCE, MySQL default credentials, OS EOL
- **High:** Web misconfigurations, phpMyAdmin exposure
- **Medium:** SMB open ports

7. Remediation Recommendations

Immediate Actions

- Rebuild system to remove backdoors
- Upgrade OS to a supported version
- Patch Apache and Tomcat
- Disable AJP connector
- Enforce strong database credentials

Hardening

- Close unused ports (FTP, Telnet, SMB)
- Restrict phpMyAdmin access
- Disable directory indexing
- Implement firewall rules

8. Conclusion

The vulnerability assessment confirms that the target system is **critically insecure** and vulnerable to complete compromise. Multiple high-impact vulnerabilities allow attackers to gain root access with minimal effort. Immediate remediation and system hardening are strongly recommended before deploying such a system in any production environment.

9. Escalation Email to Developers (100 Words)

Subject: Critical Security Vulnerabilities Identified on 192.168.43.131

Dear Development Team,

During a recent vulnerability assessment, multiple **critical security issues** were identified on host **192.168.43.131**. These include default MySQL root credentials, Apache Tomcat Ghostcat RCE (CVE-2020-1938), an active backdoor service providing root access, and an end-of-life operating system. Proof of concept confirms successful command execution and unauthorized access.

Immediate remediation is required, including OS upgrade, service hardening, credential enforcement, and removal of unauthorized services. Failure to address these issues could result in complete system compromise and data loss.

Regards,
VAPT Analyst