Web Application Penetration Testing Report

Prepared for: Internal Security Review
Prepared by: Cybersecurity Analyst
Date: 5 June 2025

Confidential – For Internal Use Only

1. Introduction

This document presents the results of a Web Application Penetration Testing exercise conducted against the target host 192.168.152.129. The objective of this test was to identify vulnerabilities that could be exploited by malicious actors to compromise the confidentiality, integrity, and availability of the system. The testing combined automated scanning (OpenVAS) with manual verification to ensure accuracy. Vulnerabilities are categorized based on their severity using the Common Vulnerability Scoring System (CVSS).

2. Background

Web Application Penetration Testing is a proactive approach to evaluating the security of a web application by simulating real-world attacks. It involves reconnaissance, scanning, exploitation, and post-exploitation phases. OpenVAS (Open Vulnerability Assessment System) was chosen for this test due to its comprehensive vulnerability database and proven reliability in detecting a wide range of security flaws.

3. Scope

- Target Host: 192.168.152.129 - Tools Used: OpenVAS, manual verification techniques - Date of Scan: 5 June 2025 - Testing Methodology: Black-box testing approach

4. Methodology

The following methodology was used during the test: 1. Reconnaissance – Identifying live hosts, open ports, and services. 2. Vulnerability Scanning – Running OpenVAS to detect known vulnerabilities. 3. Manual Verification – Confirming findings through manual checks. 4. Risk Assessment – Assigning CVSS scores and prioritizing remediation. 5. Reporting – Documenting all findings with actionable recommendations.

5. Vulnerability Summary

Severity	Count
High	24
Medium	40
Low	6

6. Detailed Findings

Finding: Outdated Ubuntu Linux OS (EOL)

Severity: CVSS 10.0 – Critical
Description: The target host is running Ubuntu Linux 8.04, which reached end-of-life in 2013. No security patches have been released since then.
Impact: An attacker could exploit unpatched vulnerabilities to gain full control of the system.
Recommendation: Upgrade to a supported version of Ubuntu that receives regular security updates.

Finding: Java RMI Server Remote Code Execution (CVE-2011-3556)

Severity: CVSS 7.5 – High
Description: The Java RMI service is configured insecurely, allowing unauthenticated remote code execution.
Impact: An attacker can execute arbitrary code on the server, potentially with elevated privileges.
Recommendation: Disable class-loading in RMI or apply vendor-recommended security patches.

Finding: Apache Tomcat Ghostcat Vulnerability (CVE-2020-1938)

Severity: CVSS 9.8 – Critical
Description: The Apache Tomcat AJP connector is enabled and vulnerable to the Ghostcat file inclusion flaw.
Impact: Attackers can read or include sensitive files from the Tomcat server.
Recommendation: Update Apache Tomcat to version 7.0.100, 8.5.51, or 9.0.31 and disable AJP if not needed.

7. Risk Assessment Matrix

	Low Impact	Medium Impact	High Impact
Low Likelihood	Low	Low	Medium
Medium Likelihood	Low	Medium	High
High Likelihood	Medium	High	Critical

8. Conclusion

The penetration testing exercise revealed multiple critical vulnerabilities that must be addressed immediately to prevent potential exploitation. The presence of outdated software, weak credentials, and misconfigured services significantly increases the attack surface. Implementing the recommended remediations will greatly enhance the system's security posture. Continuous monitoring, patch management, and periodic penetration testing are essential for maintaining a secure environment.