VAPT CAPSTONE PROJECT REPORT

Assessment Type

Vulnerability Assessment and Penetration Testing (VAPT)

Methodology

The assessment was conducted following industry best practices and aligned with the Penetration Testing Execution Standard (PTES).

1. Executive Summary

A security assessment was performed to evaluate the overall security posture of the target system. The testing identified a critical vulnerability in the web server that could allow an unauthenticated attacker to execute commands remotely. Additional weaknesses related to outdated services increased the overall attack surface and risk level.
If exploited, these vulnerabilities could lead to full system compromise, unauthorized access to sensitive data, and service disruption. No evidence of malicious exploitation was observed during the engagement. Immediate remediation is recommended, followed by verification testing to ensure that applied security fixes are effective.

2. Scope and Methodology

Scope

The assessment focused on the following in-scope assets and services:

- Target IP Address: 192.168.1.150
- HTTP (Apache Web Server)
- HTTPS
- SSH

Methodology

The assessment followed a structured approach consisting of:

- Reconnaissance and discovery
- Vulnerability identification and prioritization
- Controlled exploitation
- Limited post-exploitation validation
- Evidence collection and integrity validation
- Reporting and remediation guidance

3. Reconnaissance Summary

Initial reconnaissance identified multiple exposed services running outdated software versions.

Open services discovered during testing include:

Port 22 – SSH (OpenSSH 2.9p2)

Port 80 – HTTP (Apache 1.3.20)

Port 443 – HTTPS (Apache SSL)

The presence of outdated services significantly increases the likelihood of exploitable vulnerabilities.

4. Technical Findings

Finding ID: F001

Title: Apache Remote Code Execution

Severity: Critical

CVSS Score: 9.1

Affected Service: Apache HTTP (Port 80)

Description:

The Apache web server is running an outdated version vulnerable to remote code execution. This vulnerability can be exploited remotely without authentication, allowing an attacker to execute arbitrary system commands on the target server.

Impact:

Successful exploitation could allow an attacker to gain unauthorized access to the system, execute commands, access sensitive data, and potentially compromise the entire server.

Evidence:

Controlled exploitation confirmed the ability to execute system-level commands through the web service. User context was verified post-exploitation. Evidence was collected, documented, and hashed to maintain integrity.

Remediation:

- Upgrade Apache to the latest supported version
- Apply all relevant security patches
- Restrict unnecessary services
- Implement network-level access controls and secure configurations

5. Post-Exploitation Summary

Post-exploitation activities were limited strictly to verification of impact. The current user context and privilege level were identified and documented. No persistence mechanisms were created, and no sensitive data was accessed or retained. All actions adhered to least-access and least-impact principles.

6. Evidence Handling and Chain of Custody

The following evidence was collected and preserved according to professional chain-of-custody procedures:

Item: System Proof

Description: User context verification

Collected By: VAPT Analyst

Date: 2025-08-25

Integrity: SHA-256 hash generated

Item: Traffic Log

Description: Limited HTTP traffic capture

Collected By: VAPT Analyst

Date: 2025-08-25

Integrity: SHA-256 hash generated

All evidence was securely stored and protected from modification.

7. Recommendations

- Immediately patch and upgrade all outdated services
- Apply secure configuration baselines
- Conduct regular vulnerability assessments and penetration testing
- Perform a re-assessment after remediation to confirm fixes

8. Conclusion

The assessment confirmed the presence of a critical vulnerability that could allow full system compromise if exploited. Prompt remediation and follow-up testing are essential to reduce risk and improve the overall security posture of the environment.

Final Management Briefing

The security assessment identified a critical weakness in the web server that could allow an external attacker to gain unauthorized control of the system. Although no malicious activity was observed during testing, the vulnerability presents a serious business risk due to its ease of exploitation and potential impact. Immediate remediation is strongly recommended, including patching affected services and validating fixes through retesting. Addressing these issues promptly will significantly reduce the likelihood of system compromise and improve operational security.