Project 4: Vulnerability Assessment & Reporting

Summary

A vulnerability assessment was performed against a test machine using **Nessus Essentials**. The scan revealed several security weaknesses, including outdated services, weak cryptographic configurations, and unpatched software. At least one vulnerability was validated manually to confirm the scanner's findings. This report provides details of the assessment, risk evaluation, and remediation recommendations.

Scope

- **Scanner VM:** Ubuntu running Nessus Essentials
- **Target VM:** Ubuntu Server (test environment)
- **Methodology:** Automated vulnerability scanning with Nessus, followed by manual validation of findings

Methodology

1. **Setup:** Nessus Essentials installed and configured on scanner VM
2. **Scanning:** Basic Network Scan performed against target VM's IP
3. **Analysis:** Reviewed Critical/High findings from Nessus report
4. **Validation:** Confirmed at least one vulnerability manually through command-line checks and testing

Findings

1. Outdated OpenSSH Server

- **Description:** The scan identified an outdated OpenSSH version susceptible to known CVEs.
- **Evidence:**
    - Nessus flagged multiple vulnerabilities (CVE references provided in scan).
    - Manual validation:
    - ssh -V
    - OpenSSH_7.2p2 (outdated version)

- **Risk:** High – could allow privilege escalation or remote code execution.
- **Remediation:** Update OpenSSH to the latest stable version using system package manager.

2. Weak SSL/TLS Cipher Suites

- **Description:** The target supports deprecated SSL/TLS protocols (TLS 1.0/1.1) and weak ciphers.
- **Risk:** Medium – may expose encrypted traffic to downgrade and cryptographic attacks.
- **Remediation:** Disable weak ciphers in Apache/Nginx configuration, enforce TLS 1.2 or higher.

3. Outdated Apache Web Server

- **Description:** Apache version is outdated and vulnerable to known exploits.
- **Evidence:**
- apache2 -v
- Server version: Apache/2.4.29
- **Risk:** High – attacker could exploit known RCE vulnerabilities.
- **Remediation:** Update Apache to the latest version available for the OS distribution.

Exploitation & Validation

- **Finding Tested:** Weak SSH password (from Nessus)
- **Method:** Hydra brute-force attack against SSH service
- **Result:** Successful login with weak credentials (user:test123)
- **Impact:** Confirmed Nessus report accuracy and demonstrated potential unauthorized access

Risk Rating

Vulnerability	Severity	Likelihood	Impact	Risk Level
Outdated OpenSSH Server	High	High	High	**Critical**
Weak SSL/TLS Cipher Suites	Medium	Medium	Medium	**Medium**
Outdated Apache Version	High	Medium	High	**High**
Weak SSH Password (validated)	High	High	High	**Critical**

Recommendations

1. Apply all security patches for OpenSSH and Apache.
2. Enforce strong password policies and disable weak SSH authentication.
3. Restrict SSH access with firewall rules (e.g., allow only specific IPs).
4. Reconfigure web server to disable weak SSL/TLS protocols.
5. Implement regular vulnerability scans as part of ongoing security management.

Conclusion

The vulnerability assessment revealed multiple weaknesses in the test environment, including outdated services and weak authentication mechanisms. One vulnerability was validated through successful exploitation of weak SSH credentials, confirming real-world risk. Addressing these findings with timely patching, configuration hardening, and access controls will significantly reduce the attack surface.