PTES Penetration Testing Report

Executive Summary

A controlled penetration test was conducted against a deliberately vulnerable Metasploitable VM (target IP: 192.168.1.200) to evaluate exposure to known service-level and API-related weaknesses. The assessment followed the Penetration Testing Execution Standard (PTES) methodology. A critical remote code execution (RCE) vulnerability was identified in the FTP service (VSFTPD 2.3.4), demonstrating how outdated services can lead to full system compromise. Limited API testing using Burp Suite focused on identifying common authorization and input-handling issues. Overall, the test confirmed that unpatched services and weak security controls significantly increase attack surface.

Attack Timeline

- Reconnaissance & Enumeration: Service discovery identified an exposed FTP service running VSFTPD 2.3.4 and multiple web/API endpoints.
- Vulnerability Analysis: Publicly known backdoor behaviour in VSFTPD 2.3.4 was confirmed as applicable. API endpoints were reviewed for improper input handling and authentication gaps.
- Exploitation:
  - 2025-08-30 15:00:00 | 192.168.1.200 | VSFTPD RCE | Exploitation
  - Successful exploitation resulted in unauthorized command execution, demonstrating complete loss of system integrity.
- Post-Exploitation (High-Level): Impact analysis showed potential for privilege escalation, data access, and persistence due to weak service isolation.
- Reporting: Findings were documented with risk ratings and remediation guidance.

Remediation Plan

- Patch & Upgrade: Remove or upgrade VSFTPD 2.3.4 to a supported, secure version.
- Service Hardening: Disable unused services; restrict FTP access or replace with SFTP.
- Least Privilege: Enforce minimal permissions for service accounts and file access.
- Input Validation & API Security: Implement strict server-side validation, authentication, and authorization checks.
- Network Controls: Apply firewall rules and network segmentation to limit service exposure.
- Verification: Perform a rescan using OpenVAS to confirm remediation effectiveness and establish a baseline.