# PENETRATION TESTING REPORT TEMPLATE

REVIEWED BY: Nathan Reynolds

APPROVED BY: AeroTech

VERSION: 1.1 DATE: 09/22/2025

## Change history

| Date | Version | Owner | Change Description |
|---|---|---|---|
| | | | |
| | | | |

## Table of contents

## 1. Purpose

The purpose of this penetration test is to identify vulnerabilities that exist on AeroTech's in scope devices.

## 2. Executive Summary

A penetration test was conducted on AeroTech's infrastructure to identify vulnerabilities, weaknesses, and potential areas of improvement in their cybersecurity posture. The primary objective was to simulate real-world cyber-attacks in a controlled environment and provide actionable insights to bolster AeroTech's defenses.

After completing the penetration test there was a high severity vulnerability that allowed us to gain root access to the target machine. This vulnerability was due to the use of an outdated FTP version that was vulnerable to the exploit/unix/vsftpd_234_backdoor Metasploit payload.

## 3. Project Details / Scope

This engagement was set to take place from October 1st – October 7th. The only in-scope device for this penetration test is the Metasploitable VM that AeroTech has on their network. The IP address for this in-scope device is 192.168.57.129

## 4. Reference documents

- Rapid7 Metasploit Documentation

## 5. Results From Port Scan

| Port | State | Service | Version | Vulnerable? |
|---|---|---|---|---|
| 21 | Open | FTP | vsftpd 2.3.4 | Yes |
| 139 | Open | Smb | Samba | Yes |

## 6. Findings

| Description | Details | Severity | Recommendations |
|---|---|---|---|
| **The penetration testers were able to gain access through the FTP service** | This was achieved using the exploit/unix/ftp/vsftpd_234_backdoor payload from Metasploit | Critical | **We need to update this service so it is no longer using a vulnerable version** |

## 1. DISCLAIMER

This document is confidential and only for use by the company receiving this information from AeroTech