PENETRATION TESTING REPORT

REVIEWED BY: Idrees Roshan

APPROVED BY: AeroTech

VERSION: 1.1 DATE: 22/02/2024

Change history

Date	Version	Owner	Change Description
22/02/2024	1.1	Idrees Roshan	

Table of contents

1. Purpose

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

2. 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. The vulnerability was due to the use of an outdated FTP version that was vulnerable to the exploit/unix/vsftpd_234_backdoor Metasploit payload.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 February 22nd. The device used for penetration testing was Metasploitable2 VM that AeroTech has on their network. The IP address for this device is 192.169.1.4.

4. Reference documents

- Rapid7 Metasploit Documentation

5. Results From Port Scan

Port	Service	Version	Vulnerable?
21	FTP	Vsftpd 2.3.4	Yes

6. Findings

Findings	Description	Details	Severity	Recommendations
FTP is outdated and vulnerable	Penetration testers were able to gain root access through the FTP service	This was achieved using the exploit/unix/ftp/vsftpd_234_backdoor payload from Metasploit.	Critical (9.8 on cvss)	**Service must be updated so that a vulnerable version is not being used.**

7. DISCLAIMER

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