Penetration Test

CPTS Exam Report

Alexander Chin-Lenn
HTB Candidate
alex@chin-tech.org
2025-06-07

InlaneFreight

Draft

Contents

1. Statement of Confidentiality
2. Engagement Contacts

Inlanefreight		
Name	Title	Email
John Doe	CEO	jDoe@inlanefreight.htb

Assessor		
Name	Title	Email
Alexander Chin-Lenn	HTB Candidate	alex@chin-tech.org

3. Overview
4. Executive Summary
4.1. Approach
4.2. Scope
4.3. Assesment Overview
5. Network Penetration Test Assessment Summary
5.1. Detailed Walkthrough
6. Internal Network Compromise
6.1. Detailed walkthough
7. Remediation Summary
7.1. Quick Fixes
7.2. Medium-Term
7.3. Long-Term
8. Detailed Technical Findings

This section contains detailed technical findings of the assessment ordered by Common Vulnerability Scoring System (CVSS) Rating. The CVSS rating is a measure of how severe a vulnerability is or could be. It is not indicative of the risk that these vulnerabilties may have to your organization. Meaning, we can have a a vulnerability that has a critical

rating of 9.8 because it is exploitable over the internet and doesn't need authentication. However, that could be an isolated system without exposure to any customer facing data. To mitigate this confusion, there will be notes included to draw your attention to particular findings.

Below will be all of the findings by the finding, the CVSS Score, a high-level definition of the vulnerability for reference, and the specific example found during the assessment.

8.0.1. SQL Injection

CVSS 7.1 blah

SQL Injection

A method of providing input to database that allows for remote code execution

8.0.2. Insecure Passwords

CVSS 3.0 this is not so bad

CVSS 6.0 Okay probably bad

CVSS 9.5 Holy shit, fix this

9. Appendix

9.1. Severities

9.2. Host & Service Discovery

9.3. Subdomain Discovery

9.4. Exploited Hosts

9.5. Compromised Users

9.6. Alterations / Host Cleanup

9.7. Flags