{{CLIENT CORPORATE LOGO}}

**{{CLIENT}}**

Security Assessment Findings Report

# 

# 

# 

# 

# 

*Date: November 11th, 2023*

*Project: {{CLIENT}}-001*

*Version 1.0*

# Table of Contents

[**Table of Contents 2**](#_heading=h.up3w853b9aj8)

[**Confidentiality Statement 4**](#_heading=h.hdp6uqg93060)

[**Disclaimer 4**](#_heading=h.asg94zfc92xr)

[**Document History 4**](#_heading=h.n2zhs7ul4sjk)

[**Executive Summary 5**](#_heading=h.bas8ly96g9w3)

[**Assessment Overview 6**](#_heading=h.shqd34eaz8sm)

[Purpose of the Assessment 6](#_heading=h.3zo8o6m0khzx)

[Approach 6](#_heading=h.hxsl6mmzvl1a)

[Targets and Scope 7](#_heading=h.5pfy11cp2mmf)

[Network Topology 8](#_heading=h.kwyb031y4sy7)

[Testing Methodology 9](#_heading=h.g1lxuv6olsw2)

[Finding Severity Ratings 10](#_heading=h.6g8hy0l77gdi)

[Risk Factors 11](#_heading=h.wslw7tc2u0dn)

[Key Findings 12](#_heading=h.vqhlnffcxl48)

[Finding 1 12](#_heading=h.50y0zilmxnhn)

[Finding 2 12](#_heading=h.hiku7krkzdu1)

[Finding 3 12](#_heading=h.lqlxtn69jk0e)

[Finding 4 12](#_heading=h.xni25ybmwpc4)

[Finding 5 12](#_heading=h.m7et57j9nv6l)

[Prioritized Remediations 12](#_heading=h.ipb9wnh8kqo6)

[Remediation 1 12](#_heading=h.ftodghcvsm9q)

[Remediation 2 12](#_heading=h.hkri4dz0etlw)

[Remediation 3 12](#_heading=h.cv34ht48guu1)

[Remediation 4 12](#_heading=h.5byq5hatd0oj)

[Remediation 5 12](#_heading=h.8pgv7nlujmiy)

[Business Impacts 12](#_heading=h.iw2h6xsy702a)

[**Compliance Assessment 13**](#_heading=h.1lhkkpt7efeh)

[Regulatory and Compliance Remediations 15](#_heading=h.9qpzfe9sxdxa)

[**Attack Narrative 15**](#_heading=h.jns4zf4h0iic)

[**Technical Findings 17**](#_heading=h.4t4k8e63gp6v)

[Critical Severity 17](#_heading=h.w6eirggh7da5)

[Finding 1 17](#_heading=h.1rc7kgy9rg3f)

[Finding 2 17](#_heading=h.27ijv0feigqr)

[Finding 3 17](#_heading=h.4yf0rcyek4aa)

[Finding 4 17](#_heading=h.ont9dlkz3vu9)

[Finding 5 17](#_heading=h.ge81szxt0aal)

[High Severity 17](#_heading=h.6t54z2wgo6in)

[Finding 1 17](#_heading=h.dwbr02svh8i8)

[Finding 2 17](#_heading=h.3ngzhuz2zk8p)

[Finding 3 17](#_heading=h.hpvzn0uwy8b)

[Finding 4 17](#_heading=h.gv6jtgguvzet)

[Finding 5 17](#_heading=h.c1656i6nht06)

[Medium Severity 17](#_heading=h.3s4arqvsxsh8)

[Finding 1 17](#_heading=h.k1eihlp785it)

[Finding 2 17](#_heading=h.gu9pziu4y7v)

[Finding 3 17](#_heading=h.2l3evge18yd8)

[Finding 4 17](#_heading=h.nb5xa74pxvh5)

[Finding 5 17](#_heading=h.kgbkbv7n4zfm)

[Low Severity 18](#_heading=h.qpsa0q9rnnkz)

[Finding 1 18](#_heading=h.bro47voxrv4q)

[Finding 2 18](#_heading=h.yb4hak44drzi)

[Finding 3 18](#_heading=h.7tjr6qr4dbvg)

[Finding 4 18](#_heading=h.fa5vxym3pnk5)

[Finding 5 18](#_heading=h.v2exkmppyoib)

[Informational 18](#_heading=h.nn56srowf204)

[Finding 1 18](#_heading=h.o9ntcgu9ibt)

[Finding 2 18](#_heading=h.d4vnmh5phpoo)

[Finding 3 18](#_heading=h.5u8j38l6cjkw)

[Finding 4 18](#_heading=h.pyzk21k845cf)

[Finding 5 18](#_heading=h.s0jgxoulvryy)

[**Future Testing Recommendations 18**](#_heading=h.b2b3hc79ul4k)

[**Appendix 20**](#_heading=h.qsyihya01k0f)

[Vulnerability Rating System 20](#_heading=h.khftnga36c2y)

[Evidence and Artifacts 20](#_heading=h.yz6kz4gd41od)

[Regulatory and Compliance Sources 20](#_heading=h.tgy1e1oi6kb8)

# 

# Confidentiality Statement

This document remains the sole property of {{CLIENT}} and {{VENDOR}}. It encompasses proprietary and confidential data. Any form of reproduction, dissemination, or utilization, whether in entirety or in segments, necessitates the authorization of both {{CLIENT}} and {{VENDOR}}.

{{CLIENT}} is permitted to divulge this document to auditors under sealed confidentiality agreements to validate penetration test adherence.

# Disclaimer

A penetration test epitomizes a momentary insight. The conclusions and suggestions correspond to the data obtained during the examination, excluding any alterations or adjustments made beyond this interval.

The limited timeframe of engagements precludes a comprehensive appraisal of all security safeguards. {{VENDOR}} accentuated the review to pinpoint the most vulnerable security mechanisms a perpetrator could leverage. {{VENDOR}} advocates for the execution of supplementary evaluations annually, by in-house or external evaluators, to uphold the enduring efficacy of its safeguards.

# Document History

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Description** |
| 0.1 | 10/26/2023 | Initial document template |
| 0.5 | 11/11/2023 | Assessment findings added post-engagement |
| 0.9 | 11/11/2023 | Final draft released for internal review |
| 1.0 | 11/12/2023 | Final report released to client |

**Contact Information**

|  |  |  |
| --- | --- | --- |
| **Name** | **Title** | **Contact Information** |
| Michael Crawford | Team Lead | {{COMPETITION EMAIL}} |
| {{CLIENT POC}} | Director, Security and Technology | {{CLIENT EMAIL}} |

# Executive Summary

The {{CLIENT}} underwent a penetration test to meticulously evaluate the security posture of its digital infrastructure on {{DATE}}. This assessment was diligently conducted by {{VENDOR}}, following established frameworks including the NIST SP 800-53 revision 5, 800-115, OWASP Testing Guide (V4.2), and PCI DSS Requirement 11.3.

The focus of the assessment was particularly on identifying network vulnerabilities, scrutinizing vulnerabilities within the {{SYSTEM CATEGORIES}}, and ensuring the secure handling of customer information in adherence to {{COMPLIANCE STANDARD}}.

During this comprehensive examination, {{VENDOR}} successfully identified a multitude of vulnerabilities across varying levels of severity, detailed as follows:

* **Critical**: {{CRITICAL #}}
* **High:** {{HIGH #}}
* **Medium:** {{MEDIUM #}}
* **Low:** {{LOW #}}
* **Informational:** {{INFORMATIONAL #}}

Noteworthy findings among these include {{NOTEWORTHY FINDINGS}}. The critical and high-severity vulnerabilities signify areas requiring immediate attention to prevent potential exploitation and subsequent adverse impact on operations and customer trust and safety.

On a positive note, the {{POSITIVE MEASURES}} implemented at {{CLIENT}} showcased a proactive approach toward minimizing the {{TYPES OF RISK MITIGATED}}, should a breach occur.

Given the findings, it's imperative for {{CLIENT}} to engage in a collaborative effort with cybersecurity professionals to devise and implement a robust remediation plan. Recommendations include but are not limited to:

* {{REMEDIATION 1}}
* {{REMEDIATION 2}}
* {{REMEDIATION 3}}
* {{REMEDIATION 4}}
* {{REMEDIATION 5}}

Addressing the identified vulnerabilities will not only significantly enhance the security posture of {{CLIENT}} digital infrastructure but also reinforce the trust and safety of its patrons and stakeholders, aligning with {{COMPLIANCE FRAMEWORKS}}.

# 

# Assessment Overview

The primary objective of this penetration testing engagement was to comprehensively evaluate the cybersecurity strength and resilience of {{CLIENT}}'s digital infrastructure within the airport environment. Recognizing the unique challenges airports face, from the intricate integration of various technologies to the safety and operational implications of potential breaches, this assessment was of paramount importance. To ensure a meticulous and structured approach, our assessment was carried out based on established frameworks, including NIST SP 800-53 revision 5, 800-115, OWASP Testing Guide (V4.2), and PCI DSS Requirement 11.3

## Purpose of the Assessment

Based on the RFP document from {{CLIENT}}, the purpose of this assessment was as follows:

1. Identify potential vulnerabilities in {{CLIENT}}’s infrastructure that could be exploited by adversaries, affecting both airport operations and passenger safety.
2. Assess the effectiveness of current security measures in place, especially those that cater to the specialized needs of an airport environment.
3. Ensure that {{CLIENT}}’s digital infrastructure is in compliance with general cybersecurity standards and {{COMPLIANCE STANDARD}} regulations.
4. Provided insights into areas of improvement to safeguard against potential threats unique to airports.
5. Recommend a detailed remediation plan based on highest priority vulnerabilities and a follow up plan for {{CLIENT}}.

## Approach

{{VENDOR}}’s team employed a multi-faceted methodology that combined both automated scanning tools and manual penetration testing techniques. Given the criticality of airport systems, this blend was essential to uncover vulnerabilities that could have severe operational impacts and might be missed if solely relying on one approach.

Airports are prime targets for cyber threats due to their strategic importance and the potential catastrophic consequences of security breaches. The myriad risks range from disruptions in flight schedules and air traffic control systems to breaches in passenger data and safety systems, staying ahead of threats is not just a matter of compliance but of utmost public safety and national security. This evaluation for {{CLIENT}} underscores the airport’s commitment to maintaining robust security measures that protect its passengers, staff, and assets from the increasingly sophisticated cyber threats evolving. The potential implications of a security breach – from financial losses to reputational damage – show that assessments have become an imperative for organizations such as {{CLIENT}}.

## Targets and Scope

The scope of this assessment encompassed the network range {{NETWORK RANGE}} and the domain {{DOMAIN NAME}}. Within this scope, {{TECHNOLOGY 1}}, {{TECHNOLOGY 2}}, {{TECHNOLOGY 3}}, and critical infrastructure were included. For a thorough understanding and clarity, the full scope is detailed in the table below:

|  |  |  |
| --- | --- | --- |
| **IP Range (CIDR)** | **Hostname/URL** | **Description** |
| {{IP RANGE 1}} | {{HOSTNAME 1}} | {{DESCRIPTION 1}} |
| {{IP RANGE 2}} | {{HOSTNAME 2}} | {{DESCRIPTION 2}} |
| {{IP RANGE 3}} | {{HOSTNAME 3}} | {{DESCRIPTION 3}} |
| {{IP RANGE 4}} | {{HOSTNAME 4}} | {{DESCRIPTION 4}} |
| {{IP RANGE 5}} | {{HOSTNAME 5}} | {{DESCRIPTION 5}} |
| {{IP RANGE 6}} | {{HOSTNAME 6}} | {{DESCRIPTION 6}} |

### 

### Network Topology

Understanding the network topology is crucial in an airport environment due to the interconnectedness of systems, ranging from passenger processing to air traffic control. A clear view of this layout aids in pinpointing potential chokepoints and high-value targets for adversaries.

The following network topology details the systems identified during the engagement. Below is a visual representation of the identified network topology, illustrating the interconnections and relationships of the various systems.

The topology also highlights key zones such as the {{ZONE 1}}, {{ZONE 2}}, which were of special focus during our assessment due to their critical nature.

For accuracy, the presented topology is based on the combination of initial inputs from {{CLIENT}} and discoveries made during the assessment. This comprehensive representation ensures a holistic view, capturing both expected and unexpected network components.

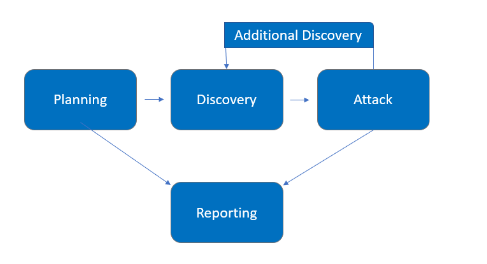
{{IMAGE OF NETWORK TOPOLOGY}}

## Testing Methodology

For this engagement, {{VENDOR}} closely followed the NIST SP 800-115 framework for penetration testing. NIST SP 800-115 provides a proven methodology for penetration testing, recognized for its thoroughness amongst cybersecurity professionals. Given the significance of airport infrastructure, {{VENDOR}} wanted to adhere to a framework that brings rigor and depth to the testing process.

The NIST SP 800-115 methodology proceeds as follows:

1. Planning: Initial phase where the objectives, boundaries, and rules of engagement are clearly defined in consultation with {{CLIENT}}. This ensures alignment with the client’s needs and establishes the groundwork for the testing process.
2. Discovery: In this phase, both passive and active techniques are employed to identify systems, services, and potential vulnerabilities within the in-scope targets.
3. Attack: Utilizing the vulnerabilities discovered, our team actively tried to exploit them to understand their real-world impact on {{CLIENT}}’s digital infrastructure. This also helped determine the feasibility for an attacker leveraging the same vulnerabilities for malicious intent.
   1. Post-Attack Discovery: After the initial attack phase, a secondary discovery phase was undertaken. This was crucial to identify any changes or new vulnerabilities that might have surfaced as a result of our attack actions.
4. Reporting: All findings from the assessment, positive and negative, were meticulously documented. This report not only details vulnerabilities found but also provides actionable recommendations on how to remediate them.



Throughout the entire process, regular communication was maintained between {{CLIENT}}’s IT and security teams and {{VENDOR}}. This approach facilitated real-time feedback and adaptations, ensuring the safety and operational integrity of the airport’s systems at every step.

## Finding Severity Ratings

In this assessment, vulnerabilities are rated based on their severity, which is derived from the Common Vulnerability Scoring System (CVSS). CVSS scores are calculated using the official NIST CVSS v3.1 Calculator ([NVD NIST CVSS v3 Calculator](https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator)). This quantitative measure evaluates the severity of vulnerabilities based on factors such as Confidentiality, Integrity, and Availability (CIA triad).

We also utilize Common Weakness Enumeration (CWE) identifiers for each finding, which are sourced from the official CWE database ([CWE MITRE](https://cwe.mitre.org/data/index.html)). CWE provides a standardized framework for identifying the root cause or underlying weakness of a vulnerability, assisting in both immediate and long-term remediation efforts.

|  |  |  |
| --- | --- | --- |
| **Severity** | **CVSS v3.1 Score Range** | **Definition** |
| **Critical** | 9.0-10.0 | Vulnerabilities in this category are extreme and present immediate and severe risks to the system or network. Exploitation is often trivial and can lead to complete compromise of the target's confidentiality, integrity, and availability. Immediate action is required to remediate. |
| **High** | 7.0-8.9 | These vulnerabilities are high-risk but may not be immediately exploitable. Nonetheless, they could lead to significant damage if left unaddressed. Remediation should be conducted as soon as feasibly possible to prevent potential escalation. |
| **Medium** | 4.0-6.9 | Medium-severity vulnerabilities carry potential future risks. While not immediately dangerous, they could be leveraged in more complex attack scenarios and therefore should be addressed. Remediation can be scheduled but should not be indefinitely postponed. |
| **Low** | 0.1-3.9 | Low-severity vulnerabilities have minimal impact and pose limited risk. While they are generally not priorities for immediate action, addressing them can improve the overall security posture. Remediation can be deferred but should still be executed. |
| **Informational** | N/A | These are findings that may not have a direct security impact but provide valuable information for improving security awareness, compliance, or system configurations. No immediate action is typically required, but they should be considered for future security enhancements. |

Each finding in this report will carry a CVSS score and a corresponding CWE identifier to ensure a comprehensive understanding of both the severity and the nature of the vulnerability.

## Risk Factors

In our assessment, we utilize a 5x5 risk matrix to determine risk levels. Risk is evaluated based on a combination of the likelihood of an event occurring and its resulting severity.

## Key Findings

### Finding 1

### Finding 2

### Finding 3

### Finding 4

### Finding 5

## Prioritized Remediations

### Remediation 1

### Remediation 2

### Remediation 3

### Remediation 4

### Remediation 5

## Business Impacts

# Compliance Assessment

This test also includes an evaluation of {{CLIENT}}’s adherence to the Payment Card Industry Data Security Standard (PCI DSS). It is important to secure cardholder data in order to prevent potential data breaches. Our evaluation is based on the standards set out in the PCI DSS version 3.2.1. Please note that changes to the PCI DSS will be made in version 4.0 which will take effect on March 31st, 2024.

Purpose of the PCI DSS Assessment

1. Identify and mitigate vulnerabilities: Discover and address any vulnerabilities in {{CLIENT}}’s systems that would potentially expose cardholder data to unauthorized users.
2. Evaluate security controls: Assess the effectiveness of existing security controls in place to safeguard against unauthorized access. Secure data storage and ensure the integrity of payment card transactions.
3. Ensure compliance: Verify that {{CLIENT}}’s processes and systems align with the PCI DSS.
4. Recommend improvements: Provide insight into areas that are in need of improvement to meet PCI DSS standards.
5. Develop remediation plan: Propose a detailed remediation plan that prioritizes the resolution of the identified non-compliance items.

The NIST Special Publication 800-53 rev. 5 *Control Baselines for Information Systems and Organizations* is significant to the {{ CLIENT }}’s controls for safeguarding their airport ecosystem so that it meets industry best practices and mitigating risks. This publication outlines and references security and privacy control baselines for organizations with system, information security, privacy, or risk management, as well as

Purpose of the NIST 800-53 rev. 5 Assessment

1. Identify and mitigate vulnerabilities: Discover and address any vulnerabilities in {{CLIENT}}’s systems that would potentially expose cardholder data to unauthorized users.
2. Evaluate security controls: Assess the effectiveness of existing security controls in place to safeguard against unauthorized access. Secure data storage and ensure the integrity of payment card transactions.
3. Ensure compliance: Verify that {{CLIENT}}’s processes and systems align with the PCI DSS.
4. Recommend improvements: Provide insight into areas that are in need of improvement to meet PCI DSS standards.
5. Develop remediation plan: Propose a detailed remediation plan that prioritizes the resolution of the identified non-compliance items.

Approach

[[VENDOR}}’s team utilized automated tools and manual testing methods to identify and evaluate devices and configurations that relate to the PCI DSS. The use of both automated methods and manual methods ensures a robust evaluation of the current compliance with the PCI DSS.

The PCI DSS

## 

## Regulatory and Compliance Remediations

# Attack Narrative

\*\*Path of least resistance paragraph, black box nature of the test, Known tools used (Nmap, OpenVAS)\*\*

# Technical Findings

## Critical Severity

### Finding 1

### Finding 2

### Finding 3

### Finding 4

### Finding 5

## High Severity

### Finding 1

### Finding 2

### Finding 3

### Finding 4

### Finding 5

## Medium Severity

### Finding 1

### Finding 2

### Finding 3

### Finding 4

### Finding 5

## Low Severity

### Finding 1

### Finding 2

### Finding 3

### Finding 4

### Finding 5

## Informational

### Finding 1

### Finding 2

### Finding 3

### Finding 4

### Finding 5

# Future Testing Recommendations

Given the limited duration of a one-day penetration testing engagement, we recommend planning subsequent, more in-depth assessments to further improve the security posture of {{CLIENT}}. Below are targeted areas that warrant future testing, based on {{VENDOR}}’s findings during the engagement.

## Corporate Network

* Reassess {{IDENTIFIED FIREWALL WEAKNESS}} in internal firewalls and access controls after the initial remediation period. This will ensure that implemented fixes are effective and no new vulnerabilities have been introduced.
* Schedule a more comprehensive examination of the {{CRITICAL/HIGH CORPORATE NETWORK FINDING}}, given the potential for severe impact on business operations and data integrity. This in-depth assessment should include penetration testing and {{POTENTIAL CODE REVIEW}} to validate the security posture.

## User Network

* Perform a follow-up social engineering assessment to evaluate the efficacy of awareness training programs. This will help determine if employees of {{CLIENT}} are aware of the risks and are following best practices.
* Further investigate {{CRITICAL/HIGH USER NETWORK FINDING}}. A thorough review will pinpoint areas needing immediate attention and remediation, ensuring the safety and integrity of user data.

## Train System Network

* Conduct a specialized ICS/SCADA security assessment, particularly focusing on real-time monitoring and incident response capabilities. This will identify vulnerabilities in mission-critical systems, ensuring the safety of passengers and continuity of operations.
* Extensive follow up analysis of {{CRITICAL/HIGH TRAIN NETWORK FINDING}}. A specialized assessment should examine the unique security requirements of the ICS to protect against both conventional and targeted attacks.

## Guest Network

* Run quarterly scans to identify rogue devices and unauthorized access. Frequent checks will make the network more resilient against potential attackers looking to exploit vulnerabilities.
* Consider deployment of an IDS/IPS system to monitor and analyze network traffic for suspicious activities, offering an additional layer of security that is useful in a high-traffic and public environment like {{CLIENT}}.

## Linux and Windows Infrastructure

* {{FILL IN}}
* {{FILL IN}}

## Linux and Windows Infrastructure

* {{FILL IN}}
* {{FILL IN}}

## Linux and Windows Infrastructure

* {{FILL IN}}
* {{FILL IN}}

# Appendix

## Vulnerability Rating System

## Evidence and Artifacts

## Regulatory and Compliance Sources