A blue and white airplane with white text

Description automatically generated

Robert A. Kalka Metropolitan Skyport

Security Assessment Findings Report

Business Confidential

Date: 12/14/2023

Project: RAKMS23

Version 1.0



Table of Contents

[Confidentiality Statement 4](#_Toc147681065)

[Disclaimer 4](#_Toc147681066)

[Executive Summary 5](#_Toc147681067)

[Purpose 5](#_Toc147681068)

[Findings 5](#_Toc147681069)

[Compliance 6](#_Toc147681070)

[Assessment Overview 7](#_Toc147681071)

[Assessment Components 7](#_Toc147681072)

[Open-Source Intelligence 7](#_Toc147681073)

[Internal Penetration Test 7](#_Toc147681074)

[<Last Part> 8](#_Toc147681075)

[Scope 8](#_Toc147681076)

[Scope Exclusions 8](#_Toc147681077)

[Client Allowances 8](#_Toc147681078)

[Network Diagram 9](#_Toc147681079)

[Risk Factors 10](#_Toc147681080)

[Likelihood 10](#_Toc147681081)

[Impact 10](#_Toc147681082)

[Compliance Summary 10](#_Toc147681083)

[TSA Security Directive 1580/82-2022-01 and TSA Security Directive 1582-21-01A 10](#_Toc147681084)

[NIST SP 800-82 Rev. 3 12](#_Toc147681085)

[Finding Severity Ratings 13](#_Toc147681086)

[Vulnerability Report Card 14](#_Toc147681087)

[Technical Findings 16](#_Toc147681088)

[Finding RAKMSXXX: Vulnerability Name 16](#_Toc147681089)

[Appendix A: Social Engineering Overview 18](#_Toc147681090)

[Appendix B: Methodologies 19](#_Toc147681091)

[Penetration Testing Phases 19](#_Toc147681092)

[OWASP Top 10 19](#_Toc147681093)

[Appendix C: Attack Paths 20](#_Toc147681094)

[Appendix D: Technical Findings Legend 21](#_Toc147681095)

# Confidentiality Statement

This document is the property of Robert A. Kalka Metropolitan Skyport and <Team-#>. This document contains sensitive information including proprietary and confidential information. This document shall not be distributed outside of Robert A. Kalka Metropolitan Skyport or the <Team-#> without the express consent of both parties involved.

# Disclaimer

This document contains information regarding the overall network and system security of Robert A. Kalka Metropolitan Skyport. While <Team-#> maintains the highest standards of quality in their work, this document should not be construed as an exhaustive list of all possible vulnerabilities. We have intentionally focused on the areas with the highest risk and greatest vulnerability to attack to maximize the value of our services.

Due to the changing nature of the computer systems and networks, security vulnerabilities and risks will change over time; <Team-#> recommends annual testing to maintain a good security posture in response to evolving threats.

# Executive Summary

## Purpose

Robert A. Kalka Metropolitan Skyport enlisted the help of <<REGIONALS/FINALS-#>>’s penetration testing services to evaluate their corporate, customer user, transport train, and guest networks. This test was a reassessment of previous vulnerabilities as well as an assessment for new vulnerabilities present in Robert A. Kalka Metropolitan Skyport’s networks. The penetration test encompassed two workdays.

## Findings

Among the findings from our assessment, a few were particularly noteworthy due to their significant risk to Robert A. Kalka Metropolitan Skyport’s airport operations safety. <<Finding 1 business impact>>, <<Finding 2 business impact>>, and <<Finding 3 business impact>> are detrimental consequences from the reported vulnerabilities. It is imperative to remediate these vulnerabilities in this report to mitigate risk to airport operations safety customer privacy. This will help protect the company from disruptions to business operations, damage to business reputation, and an erosion of trust between the business and the consumer.

Figure 1: Chart of Found Vulnerabilities

While this test was designed to find system and business process vulnerabilities, it was also a test of the security posture of Robert A. Kalka Metropolitan Skyport’s networks. Based on our testing, we found RAKMS excelled in the areas of <<AREA1, AREA2, AREA3>>. <<Details for Area 1 explaining why they did well>>. <<Details for Area 2 explaining why they did well>>. <<Details for Area 3 explaining why they did well>>. We commend the RAKMs staff for excelling in these areas of the business’ security posture.

## Compliance

Understanding that Robert A. Kalka Metropolitan Skyport falls under the TSA’s standards for safety and security compliance, the three highest priority standards requiring re-evaluation are the <<LISTOFCOMPLIANCEAREAS>> areas of security compliance. As understood by RAKMS, a failure to meet these standards can result in safety violations, legal fees and fines, reputational damage, loss of consumer trust, operational disruption, and more. Our firm recommends analyzing the following findings and correcting them and the vulnerabilities described earlier: <<FINDING1COMPLIANCE and details, etc.>>. Following the recommendations will assist RAKMS in maintaining security compliance standards and the business will improve the airport operations safety and information security posture critical to protecting consumer data.

# Assessment Overview

On 10/14/2023, <Team-#> conducted a penetration test to evaluate the overall security posture of Robert A. Kalka Metropolitan Skyport. This test was conducted in accordance with industry standard best practices. The phases of the penetration test are as follows:

* Planning – Customer expectations and rules of engagement are obtained.
* Enumeration – Open-source intelligence and scanning are done to identify common vulnerabilities and weak areas.
* Exploitation – Confirm vulnerabilities by successfully completing an exploit and then perform more discovery based on new information.
* Reporting – Record all vulnerabilities, findings, successful exploits, and organizational strengths and weaknesses.

A diagram of an enumeration

Description automatically generated

# 

# Assessment Components

## Open-Source Intelligence

Before the beginning of the internal penetration test, Open-Source Intelligence on RAKMS will be performed. As much information about the company will be gathered using only public facing and freely accessible sources. This will both give our team more insight and context for performing the rest of the engagement as well as give valuable information on how well RAKMS is protecting the data about their company that gets out on the internet.

## Internal Penetration Test

The internal penetration test will simulate how an attacker would operate inside of the internal network. Members of the team will enumerate the network for vulnerabilities as well as carry out internal network attacks. The goal of this portion of the engagement is to find as many vulnerabilities as possible across RAKMS for the purposes of reporting. The hope is that with the help of our team, RAKMS can remediate much of their technical risk. The team will also assess the business risk each vulnerability possesses so that RAKMS can accurately decide what risk is acceptable and which is not. This will be a large portion of the assessment and will utilize information found during the Open-Source Intelligence part.

## <Last Part>

<fill in later>

# Scope

|  |  |
| --- | --- |
| Assessment | Details |
| Corporate Network | 10.0.0.0/24 |
| User Network | 10.0.10.0/24 |
| Train Network | 10.0.20.0/24 |
| Guest Network | 10.0.30.0/24 |

## Scope Exclusions

The team will not conduct any testing on any externally facing systems or IP addresses. No disruptive or destructive testing will be allowed on any systems. Social engineering will not be permitted except in a specific scenario designated directly by RAKMS. Any other social engineering is strictly prohibited.

Testing will be limited to the assigned subnets. The VPN client as well as all computers provided to the testers for the engagement will be out of scope for security testing.

## 

## Client Allowances

The client will provide a Windows and Kali Linux system for each tester; these will be used as an entry point to other systems.

## Network Diagram

Insert network diagram here

# Risk Factors

Risk is measured by two factors, likelihood and impact, with impact being further categorized into technical impact and business impact.

## Likelihood

Likelihood measures the probability of a vulnerability being exploited. Severity ratings are used for scoring based on how difficult the attack was, the tools available, the skill level of the attacker, and the environment of the client.

## Impact

Technical impact measures the potential damage a vulnerability could have on operations in the corporation. This includes the confidentiality, integrity, and availability of client-side systems and data, harm to software and/or hardware.

Business impact is a measure of the overall impact to the business, including financial loss, operational impact in potential downtimes, loss of reputation, and compliance violations.

# Compliance Summary

## TSA Security Directive 1580/82-2022-01 and TSA Security Directive 1582-21-01A

The Robert A. Kalka Metropolitan Skyport is an airport that deals with public transportation. Due to this, RAKMS must adhere to Transportation Security Administration (TSA) security directives. TSA security directives are a set of mandatory measures that public transportation businesses must follow to ensure national security and public safety. Failure to adhere to security directives may result in penalties such as fines, additional security restrictions, or suspension of flights across the United States resulting in a loss of business and credibility. This assessment fulfills the requirement found in “Security Directive 1580/82-2022-01” related to penetration testing as a part of “The Cybersecurity Assessment Program.”

The below table includes overall security objectives as well as the actions required to maintain compliance. Any vulnerabilities discovered during the assessment will be mapped to specific requirements if applicable. While all aspects of the security directives are important and mandatory, there are some that our team is unable to test due to the nature of the engagement. These directives should still be carefully tested to ensure full compliance. The table will not include these untestable portions.

References:

<https://www.tsa.gov/sites/default/files/sd-1580-82-2022-01.pdf>

<https://www.tsa.gov/sites/default/files/sd-1582-21-01a.pdf>

|  |  |  |
| --- | --- | --- |
| TSA Security Directive Objectives | TSA Requirement | Compliance Violation Findings |
| Network Segmentation | 1. Prevent unauthorized communications between network zones | * RAKMSXXX |
| 1. Prohibit OT & IT services from communicating unless encrypted | * RAKMSXXX |
| Access Control Measures | 1. Enable Multi-factor Authentication | - |
| 1. Enforce Principle of Least Privilege | - |
| Continuous Monitoring and Detection Policies | 1. Defend Against Malicious Emails | - |
| 1. Prevent unauthorized code execution, i.e. macro scripts | - |
| Patch Management | 1. Apply current patches and updates to critical systems | - |

## NIST SP 800-82 Rev. 3

The ability to properly comply with governing standards like the TSA Security Directives requires strong frameworks set by established organizations. NIST, or the National Institute of Standards and Technology, is a non-regulatory federal agency that provides cybersecurity guidance. The NIST SP 800-82 Rev. 3 is a NIST special publication that outlines a cybersecurity framework specific to Operational Technology (OT) Security. The use of this guide will provide RAKMS with a foundation for securing its infrastructure and complying with important standards such as the TSA Security Directives.

Reference: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf>

# Finding Severity Ratings

This section is used to define the severity ratings for any vulnerabilities and measure risk. The severity ratings will follow the corresponding CVSS score range.

|  |  |  |
| --- | --- | --- |
| Severity | CVSS V3  Score Range | Definition |
| Critical | 9.0 – 10.0 | Straightforward exploitation typically results in high-level system access. Vulnerabilities of this category should be  resolved immediately |
| High | 7.0 – 8.9 | Exploitation may involve more steps but could result in gaining elevated privileges and potentially significant downtime or data loss. Vulnerabilities in this category should be resolved as soon  as possible. |
| Medium | 4.0 – 6.9 | Vulnerabilities are present but are not exploitable, involve many extra steps, and/or require social engineering. Vulnerabilities in this category should be resolved after high-priority issues are  resolved. |
| Low | 0.1 – 3.9 | Vulnerabilities may be present but are not exploitable. Resolving these vulnerabilities would help to reduce the organization’s attack surface. Vulnerabilities in this category should be resolved during the next period of planned  maintenance. |
| Informational | N/A | No vulnerability exists. This category is reserved for findings  that do not directly relate to exploitation but may provide an attacker with information that would assist them in an attack. |

# Vulnerability Report Card

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Critical | High | Medium | Low | Informational |
| 2 | 13 | 14 | 2 | 7 |

Vulnerability Summary

|  |  |  |
| --- | --- | --- |
| Severity | Vulnerability | Recommendation |
| Critical | **RAKMSXXX:** Lorum Ipsum |  |
| High |  |  |
| Medium |  |  |
| Low |  |  |
| Info |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

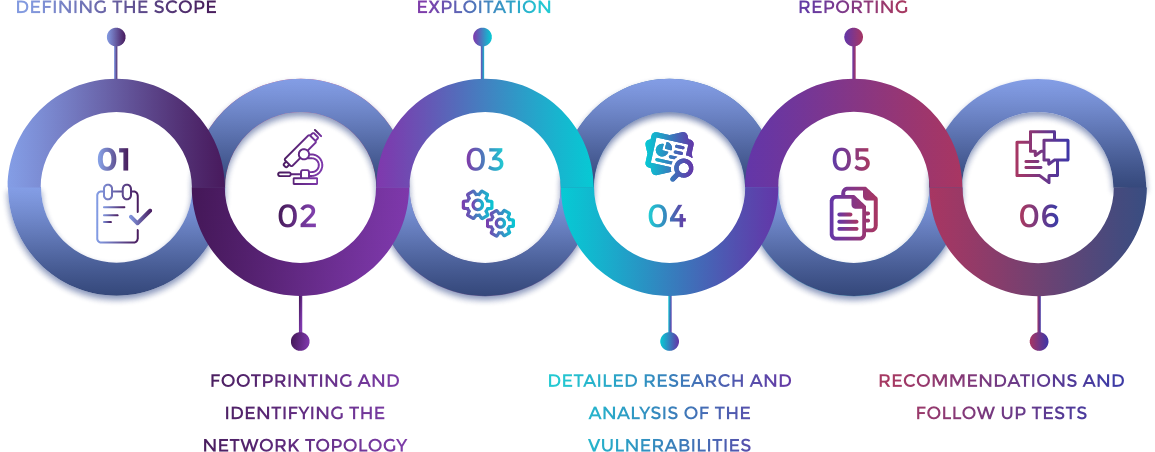
# Technical Findings

|  |  |
| --- | --- |
| Finding RAKMSXXX: Vulnerability Name | |
| **Affected Hosts** | IP Range |
| **CVSS:** #.# | Low, Medium, High, Critical | **Likelihood: Low | Medium | High**  Notes about the likelihood of exploitation, including the difficulty, credentials needed, etc.  **Technical Impact: Low | Medium | High**  Notes about the effect on RAKMS’s systems and infrastructure if this vulnerability is exploited, including access gained, or damage to systems done |
| **Vulnerability Description** | A description of how the vulnerability works and what it allows an attacker to do |
| **Business Impact** | A description of the negative effects to RAKMS from a business standpoint |
| **Requirements to exploit** | A list of requirements that may include tools, credentials needed, internal access, etc. |
| **Remediation** | General steps to correct any deficiencies specific to this instance of the exploit |
| **References** | Optional materials for additional reading |
| **Proof of Concept**  An explanation of what steps were taken as well as what the screenshots are indicating. Be concise while still giving enough details for replication.    Ensure there is a newline before and after a screenshot and that the screenshot is centered and the text is left aligned. In addition, use Blue Accent 1 with 2 ¼ pt thickness for the border and try to leave room around the edges of the screenshot. | |

# Appendix A: Social Engineering Overview

# Appendix B: Methodologies

## Penetration Testing Phases

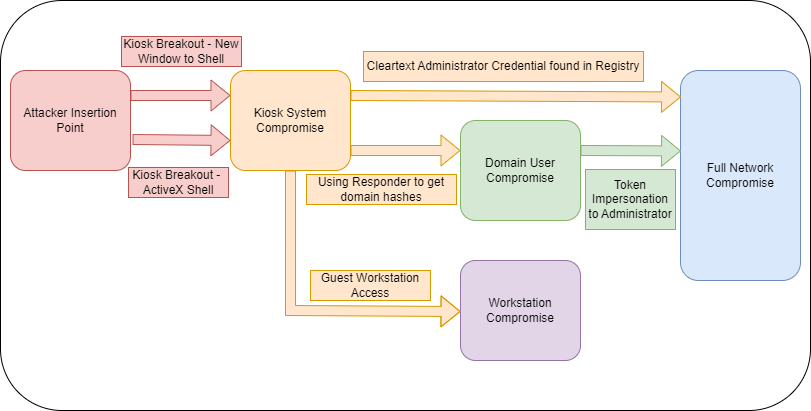
These six phases are the model by which we conduct our penetration tests. They provide accountability and robustness in testing procedures. This ensures that the highest cost to value ratio is achieved while providing an excellent product to the client.

## OWASP Top 10

The OWASP Top 10 are the ten most commonly found vulnerabilities found in web applications. All web applications are tested against these vulnerabilities at a minimum to ensure that the most vulnerabilities are discovered on each system.

|  |  |
| --- | --- |
| OWASP Top 10 - 2022 | |
| 1. Broken Access Control | 2. Cryptographic Failures |
| 3. Injection | 4. Insecure Design |
| 5. Security Misconfiguration | 6. Vulnerable and Outdated Components |
| 7. Identification and Authentication Failures | 8. Software and Data Integrity Failures |
| 9. Security Logging and Monitoring Failures | 10. Server-Side Request Forgery (SSRF) |

# Appendix C: Attack Paths

The following chart shows the most likely attack paths for an adversary based on our findings report. There are two paths discovered to completely compromise the network and another separate vector to compromise the corporate workstations.

# Appendix D: Technical Findings Legend

|  |  |
| --- | --- |
| Finding RAKMSXXX: Vulnerability Name | |
| **Affected Hosts** | *Targets/affected systems* |
| **CVSS:** *#.#* | *Rating* | **Likelihood: *Low | Medium | High***  *Notes about the likelihood of exploitation, including the difficulty, credentials needed, etc.*  **Technical Impact: Low | Medium | High**  *Notes about the effect on RAKMS’s systems and infrastructure if this vulnerability is exploited, including access gained, or damage to systems done.* |
| **Vulnerability Description** | *A description of how the vulnerability works and what it allows an attacker to do.* |
| **Business Impact** | *A description of the negative effects to RAKMS from a business standpoint.* |
| **Requirements to exploit** | *A list of requirements that may include tools, credentials needed, internal access, etc.* |
| **Remediation** | *General steps to correct any deficiencies specific to this instance of the exploit.* |
| **References** | *Optional materials for additional reading.* |
| **Proof of Concept**  *A detailed, concise set of steps to reproduce the vulnerability as proof of exploitation.*  *\*Screenshots go here\** | |

A blue and white airplane with white text

Description automatically generated

**Last Page**