

Robert A. Kalka Metropolitan Skyport

Internal Penetration Test

New England Team 3

11/11/2023

CONFIDENTIAL

Disclosure Statement

All information contained in this document is confidential and only to be viewed by authorized entities associated with Robert A Kalka Metropolitan Skyport. The viewing or distribution of this report to unauthorized personnel is strictly prohibited.

**Table of Contents**

[**Executive Summary 4**](#_t5zav9ozwvs)

[**Engagement Overview 5**](#_cvfk1ozen55h)

[Network Topology 5](#_wykzbj9yspit)

[Scope 5](#_deoevgjd821q)

[Open Source Intelligence (OSINT) 5](#_c2fedxuyghjq)

[Social Engineering 5](#_29a7khcuf44c)

[Objectives 5](#_utu377qj4dgy)

[Methodology 5](#_8ukfkopq5mhj)

[Compliance 5](#_izqh6wmbrfqb)

[Assessment Results 5](#_71j2jgjouf6p)

[**Technical Findings 6**](#_c9ffj55l0q88)

[Critical Severity Vulnerabilities 6](#_f8eera32o739)

[High Severity Vulnerabilities 7](#_t5shifimmnzz)

[Medium Severity Vulnerabilities 8](#_bnpox4wk5rpu)

[Low Severity Vulnerabilities 9](#_1nz22cyjviht)

[Informational Severity Vulnerabilities 10](#_34q2xxxel98k)

[**Appendix 11**](#_wd4pa5gbmcjb)

[Tools 11](#_kf5b58a5cymu)

# Executive Summary

Robert A. Kalka Metropolitan Skyport engaged our services to assess the security of their corporate, user, train, and airport guest networks. The security evaluation involved both an internal penetration test conducted by our team as well as preliminary analysis of the company's operational security.

Before commencing the penetration test, our team, operating under the name new-england-03, procured information about the Skyport through open-source intelligence (OSINT) gathering. Throughout the engagement phase, this information was strategically utilized in conjunction with various exploits to uncover potential vulnerabilities within the infrastructure of Robert A. Kalka Metropolitan Skyport.

Executed on November 11th, 2023, the penetration test simulated the actions of a potential threat actor, mirroring the steps a real-life adversary might take. The approach adopted was black-box, meaning that our team relied solely on information available on the internet, without any additional data provided.

The assessment revealed NUMBER critical vulnerabilities and several lower severity issues within the four Metropolitan Skyport subnets. Immediate attention is strongly recommended to address these vulnerabilities promptly and mitigate the risk of substantial harm to company assets.

To enhance overall security measures, new-england-03 suggests that Robart A. Kalka Metropolitan Skyport prioritizes the remediation of these vulnerabilities in a logical sequence, starting with the critical findings before addressing less urgent issues. Additionally, it is advisable for the company to implement employee training programs, focusing on password reuse and complexity, alongside regularly scheduled sessions addressing the awareness and prevention of social engineering attacks. These proactive steps will contribute to strengthening the overall security posture of Robert A. Kalka Metropolitan Skyport.

## 

# Engagement Overview

## Network Topology

## Scope

## Open Source Intelligence (OSINT)

## Social Engineering

## Objectives

## Methodology

## Compliance

United States Transportation Security Administration’s cybersecurity requirements for airport and aircraft operators

<https://www.tsa.gov/for-industry/surface-transportation-cybersecurity-toolkit>

## Assessment Results

## 

# Technical Findings

## Critical Severity Vulnerabilities

Title:

CVSS Score:

Scope:

Description:

Steps to Recreate:

Impact:

Remediation:

## High Severity Vulnerabilities

## Medium Severity Vulnerabilities

## Low Severity Vulnerabilities

## Informational Severity Vulnerabilities

# **Appendix**

## Tools

1. **Metasploit:**

Open Source Pentesting framework which contains modules for running exploits, post-exploitation, and the Meterpreter shell payload.

1. **Burp Suite:**

Web Application Pentesting tool which can provide a proxy to intercept and modify website requests, perform fuzzing on web endpoints, and create scope map of the victim website

1. **Nmap:**

Port scanning tool that can be used to enumerate vulnerable services. Contains a scripting engine for checking misconfigurations and vulnerabilities.

1. **Chisel:**

Network Tunneling executable that provides a Client-Server functionality to pivot into internal subnets

1. **Dirbuster:**

Web enumeration tool used to discover unknown files and directories by bruteforcing paths in a wordlist

1. **MSFVenom:**

Versatile payload generator that provides executables for gaining remote code execution through a bind or reverse shell