

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**

[**1. Team ### Summary and Contact Information 4**](#_d1zn4cugywqn)

[1.1 Contact Information 4](#_79wr1mu1brfz)

[1.2 Timeline 4](#_t8pe3qjnevy3)

[1.3 Team Summary 4](#_x3l3nm9m0as)

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

[**3. Engagement Overview 6**](#_cvfk1ozen55h)

[3.1 Scope 6](#_wykzbj9yspit)

[3.2 Network Topology 6](#_deoevgjd821q)

[3.3 AWS 6](#_vxezs26fi9uh)

[3.4 Open Source Intelligence (OSINT) 6](#_c2fedxuyghjq)

[3.5 Social Engineering 7](#_29a7khcuf44c)

[3.6 Objectives 7](#_utu377qj4dgy)

[**4. Assessment Results 7**](#_wmcat3jpcqg0)

[4.1 Remediations 7](#_ho98senewpw)

[4.2 Key Strengths 8](#_m0p37c2t9kc1)

[4.3 Key Areas of Improvement 8](#_75zny1x7i6ue)

[4.3.1 test 8](#_2w36tpjc3ame)

[4.4 Assessment Summary 8](#_wo6vsho4gptf)

[**5. Compliance 8**](#_92qbnvz4d8nn)

[5.1 PCI-DSS 8](#_184beph63r6a)

[5.2 COMPLIANCE THINGY 8](#_q5zk55lxvl7s)

[5.3 COMPLIANCY THINGY 8](#_zbp3utip44ih)

[**6. Technical Findings 9**](#_a2x9i5bi5ewc)

[6.1 Critical Findings 9](#_g7nxusxs9iwh)

[**7. Appendix 10**](#_wd4pa5gbmcjb)

[7.1 Pentest Methodology - MITRE ATT&CK 10](#_fgan01qemco4)

[7.2 Pentest Methodology - OWASP 11](#_nxwa4hufyd7k)

[7.3 Vulnerability Classification - CVSS v3 12](#_ca7adngvyfzs)

[7.2 Artifacts 13](#_3lm73g1sklko)

[7.3 Tools 13](#_t9wpcjc14oup)

* use bold in table of contents, space it out more so sections are more defined

# **1. Team ### Summary and Contact Information**

## 1.1 Contact Information

**Company Contact:**

| **Email Address** |  |
| --- | --- |
| **Phone Number** |  |

**Project Lead Contact:**

| **Project Lead** |  |
| --- | --- |
| **Email Address** |  |
| **Phone Number** |  |

## 

## 1.2 Timeline

| **Dates** | **Description** |
| --- | --- |
| 11/11/23 | Initial Security Assessment |
| 1/12/24 - 1/13/24 | Follow Up Security Assessment |

## 

## 1.3 Team Summary

Overall, TEAM # provided a team of six experienced penetration testers with domain knowledge in Network, Web, and Cloud security. Five of the six team members in this engagement are the same from the initial assessment. Each team member was given access to the environment for 16 hours over the dates (1/12/24 - 1/13/24).

# **2. Executive Summary**

Summarized in this report are the findings from the penetration test on Robert A. Kalka Metropolitan Skyport’s NETWORKS. Conducted on January 12th-13th, 2024, this engagement served as a follow-up to the previous assessment performed on November 11th, 2023.

The goal of this simulated cyber-attack test is to identify and exploit vulnerabilities in the RAKMS infrastructure in order to assess the strength and weaknesses of the infrastructure's security.

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

Several of the security issues that are detailed in this report are in violation of the TSA’s cybersecurity requirements for airports and aircraft operators. CONSEQUENCES OF NOT FULFILLING?

To enhance overall security measures, TEAM NAME 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.

# 

# **3. Engagement Overview**

## 3.1 Scope

As instructed by RAKMS, the following subnets were in scope for the engagement:

| **Name** | **IP Range (CIDR)** |
| --- | --- |
| Corporate Network |  |
| User Network |  |
| Train Network |  |
| Guest Network |  |

## 

## 3.2 Network Topology

TEAM NAME used standard enumeration tools, such as Nmap, to discover and map numerous hosts on the in-scope subnets. The resulting scans allowed us to compile a network topology map of the RAKMS network.

*\*Insert image of topology\**

**Machine Summary:**

| **Hostname** | **IP Address** | **Description** | **Operating System** | **Ports Open** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |

## 3.3 AWS

## 3.4 **Open Source Intelligence (OSINT)**

Prior to engagement, TEAM NAME gathered publicly accessible information about RAKMS, including but not limited to information found on the RAKMS website and various social media platforms. As a result, TEAM NAME was able to leverage valuable information to better assess the RAKMS network infrastructure, gain insights about its users, and utilize knowledge for attacks including social engineering attempts.

## 

## 3.5 Social Engineering

## 3.6 Objectives

# **4. Assessment Results**

## 4.1 Remediations

In the previous security assessment, [INSERT NUMBER] findings were reported to Robert A. Kalka Metropolitan Skyport. Of these vulnerabilities, [INSERT NUMBER] have been found to be remediated with [INSERT NUMBER] remediations accurately addressing the vulnerability disclosed in the previous assessment. All vulnerabilities that are unaddressed or addressed incompletely will be included in the vulnerability section of the report as well. Below is a table cataloging the findings from the previous report and how they were addressed by Robert A. Kalka Metropolitan Skyport.

*\*Insert pie chart of remediated/partially fixed/not addressed\**

| **Vulnerability Name** | **CVSS** | **Rating** | **Addressed** | **Notes** |
| --- | --- | --- | --- | --- |
| RCE on Domain Controller | 10.0 | **CRITICAL** | Yes, but can be bypassed. | Only blocked inbound connections from 127.0.0.1 |
|  |  |  |  |  |

## 4.2 Key Strengths

## 4.3 Key Areas of Improvement

### 4.3.1 test

* can place simple stuff (change password regularly, outdated stuff, 2fa)

## 4.4 Assessment Summary

* add more detail in summary of assessment
  + both table of contents for vulns and table of machines?
    - ip, os, hostname, machine description, vuln count

# **5. Compliance**

## 5.1 PCI-DSS

## 5.2 COMPLIANCE THINGY

* look into gdpr stuff/law/compliance stuff/tsa stuff

## 5.3 COMPLIANCY THINGY

# 

# **6. Technical Findings**

## 6.1 Critical Findings

| ***6.0.0*** *Better template* | | | **Risk** | **CVSS** |
| --- | --- | --- | --- | --- |
| **Type of vuln???** | *web, windows, linux, etc* | | ***LOW*** | ***0.0***  ***LOW*** |
| **Likelihood** | *Low-Critical* | |
| **Impact** | *Low-Critical* | |
| **CVSS String** | *Cool Cvss string* | | | |
|
| **Affected Scope** | *10.10.10.10 (name): TCP/1234, service name*  *10.10.10.11 (name)*   * *TCP/1235: service a, service b*   *Users: a.a, b.b, c.c* | | | |
| **Description** | *brief description* | | | |
|
| **Business Impact** | *Business* | | | |
| **Technical Impact** | *Technical* | | | |
| **Remediation** | *steps for remediation* | | | |
| **Steps to Reproduce** | | | | |
| **Step 1 description + captions** | | *relevant images* | | |
| **Proof** | | | | |
| *image* | | | | |

# **7. Appendix**

## 7.1 Pentest Methodology - MITRE ATT&CK

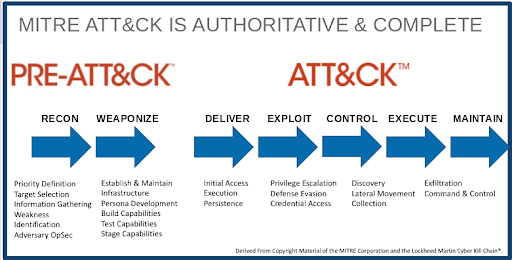
TEAM NAME utilizes the **MITRE ATT&CK framework** as a basis for our pentesting methodology. MITRE ATT&CK is very well known and widely used in the cybersecurity field to identify possible attack vectors that threat actors may use. It includes, but is not limited to: initial access, privilege escalation, credential access, and lateral movement.

**MITRE PRE-ATT&CK:**

PRE-ATT&CK focuses on the stages of the attack lifecycle that occur before a specific adversary actively engages with a target network. It encompasses the initial stages of the cyber kill chain, such as reconnaissance and weaponization.

**MITRE ATT&CK:**

This section covers the tactics, techniques, and procedures (TTPs) employed by adversaries after they have gained initial access to a target network. It is organized into matrices that represent various platforms (e.g., Windows, Linux, macOS) and detail the tactics and techniques associated with each.



[[1]](#footnote-0) MITRE ATT&CK Graphic

## 

## 7.2 Pentest Methodology - OWASP

TEAM NAME uses the **OWASP Web Security Testing Guide (WSTG)** as a guideline for testing security controls in RAKMS web applications outlined in our scope. The WSTG is developed collaboratively by the OWASP community, allowing for continuous improvement and updates based on evolving security challenges. Furthermore, the guide includes practical scenarios, examples, and techniques to simulate real-world attack scenarios and help testers understand how vulnerabilities may be exploited.

The **OWASP Top 10** is also considered when assessing web applications. This list is regularly updated and contains the ten most critical web application security risks. Published by the Open Web Application Security Project (OWASP), this list aims to raise awareness about common vulnerabilities that can be exploited by attackers and to guide organizations in prioritizing their efforts to secure web applications.



[[2]](#footnote-1)OWASP Chart

## 7.3 Vulnerability Classification - CVSS v3

TEAM NAME uses the Common Vulnerability Scoring System (CVSS)[[3]](#footnote-2) during the

engagement to classify the severity level of each vulnerability. The CVSS is a common, industry

standard scale that calculates the severity of a vulnerability based on various factors such as

attack complexity, impact, and scope. More specifically, CVSS v3 is utilized, a standard

that was implemented in 2019 and better evaluates factors better than its predecessors such as feasibility of attack and scope. The score ranges from 5 broad classifications (Critical, High,

Medium, Low, and Informational) based on the mentioned factors and a provides a quantitative

description of a vulnerability’s impact with a number ranging (0.0-10.0). In order to rate the

system, previously assigned CVSS scores given to exploited CVEs or an industry standard calculator was utilized.

**CVSS Chart[[4]](#footnote-3)**

| **Severity** | **CVSS V3 Score Range** | **Definition** |
| --- | --- | --- |
| **Critical** | 9.0-10.0 | Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately. |
| **High** | 7.0-8.9 | Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible. |
| **Moderate** | 4.0-6.9 | Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved. |
| **Low** | 0.1-3.9 | Vulnerabilities are non-exploitable but would reduce an organization’s attack surface. It is advised to form a plan of action and patch during the next maintenance window. |
| **Informational** | N/A | No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation. |

## 7.2 Artifacts

## 7.3 Tools

1. **Metasploit**

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

**Version Number:** 5

**Source:** <https://gitlab.com/kalilinux/packages/metasploit-framework>

1. **Burp Suite**

**Description:** 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

**Version Number:** Community Edition - 2023.10.3.6

**Source:** <https://portswigger.net/burp/communitydownload>

1. **Nmap**

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

**Version Number:** 7.94

**Source:** <https://gitlab.com/kalilinux/packages/nmap>

1. **Chisel**

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

**Version Number:** v1.9.1

**Source:** <https://github.com/jpillora/chisel/releases>

1. **Dirbuster**

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

**Version Number:** 1.0

**Source:** <https://gitlab.com/kalilinux/packages/dirbuster>

1. **WinPEAS and LinPEAS**

Description: Privilege escalation scripts to identify misconfigurations to obtain higher permissions in Windows and Linux systems respectively

Version Number: 20231126-a1ab960a

Source: <https://github.com/carlospolop/PEASS-ng/releases>

1. **SQLMap**

**Description:** Automated tool used to identify exploit SQL Injection vulnerabilities

**Version Number:** 1.7

**Source:** <https://github.com/sqlmapproject/sqlmap/releases>

1. **CrackMapExec**

**Description:** Versatile executable used for pentesting Windows and Active Directory environments

**Version Number:** 5.4.0

**Source:** <https://gitlab.com/kalilinux/packages/crackmapexec>

1. **Hydra**

**Description:** Password bruteforcer utilized for cracking login for multiple protocols including HTTP, FTP, SSH, and more

**Version Number:** 8.6

**Source:** <https://gitlab.com/kalilinux/packages/hydra>

1. **BloodHound**

**Description:** Active Directory enumeration tool used to identify misconfigurations in AD environments using a graph-based visualization

**Version Number:** 4.3.1

**Source:** <https://github.com/BloodHoundAD>

1. https://blogs.infoblox.com/wp-content/uploads/mitre-attack-1.png [↑](#footnote-ref-0)
2. https://evalian.co.uk/wp-content/uploads/2022/04/OWASP-Top-10-Evalian-768x755.png [↑](#footnote-ref-1)
3. https://www.first.org/cvss/v3.0/specification-document [↑](#footnote-ref-2)
4. https://github.com/hmaverickadams/TCM-Security-Sample-Pentest-Report [↑](#footnote-ref-3)