# 

# Document Information

**Confidentiality Notice**

This document and the contents thereof are provided in strict confidence for the sole usage of Robert A. Kalka Metropolitan Skyport. As the contents of the document contain strictly confidential and privileged information regarding the infrastructure of Robert A. Kalka Metropolitan Skyport, the document may not be disclosed or redistributed without the sole consent of Robert A. Kalka Metropolitan Skyport, as such actions may expose sensitive information regarding the company and put them at risk.

**Disclaimer of Warranty and Limitation of Liability**

If further professional assistance is required outside the responsibilities of penetration testing, the services of a competent professional person should be sought. Neither the publisher nor the authors shall be liable for damages arising herefrom. The referencing of any external sources or works as a citation or a potential source of further information does not imply the endorsement of the publisher and authors. Further, readers should be aware that standards and practices constantly change within the field of cybersecurity, and that the information in this document is only deemed accurate up to the time the work was written.

**Warning**

The contents of this report are to be provided to Robert A. Kalka Metropolitan Skyport in a format that is not easily modifiable. The customer should not attempt to omit any findings within this report and should take full responsibility for remediating or mitigating any findings herein. The resolution of any of these findings should only be documented once the finding has been remediated and has been validated by another professional competent in the field of cybersecurity, which may be the same as the publishers of this document.

**Document History**

| **Version Number** | **Issue Date** | **Issued By** | **Change Description** |
| --- | --- | --- | --- |
| 0.1 | 22/10/2023 | at-large2 Team | Draft for internal review only |
| 0.2 | 22/10/2023 | at-large2 Team | Quality Assurance |
| 1.0 | 22/10/2023 | at-large2 Team | Released to RAKMS |

**Document Distribution**

| **Name** | **Position** | **Organisation** |
| --- | --- | --- |
| Markiian Chaklosh | Team Captain | at-large2 Team |
| … | … | … |

# 

# How to approach this report

**Executive Summary**

**Technical Details**

**Open-source intelligence (OSINT)**

**Findings Details**

**Social Engineering Campaign**

**Appendixes A-G**

# Table Of Contents

[**Document Information 1**](#_heading=h.eoawv2hc7jrn)

[**How to approach this report 3**](#_heading=h.oru10xe7urs)

[**Table Of Contents 4**](#_heading=h.30j0zll)

[**Executive Summary 6**](#_heading=h.1fob9te)

[1.1 Project Objectives 7](#_heading=h.tyjcwt)

[1.2 Scope, Timeframe and Limitations 9](#_heading=h.3dy6vkm)

[1.3 Summary of Findings 10](#_heading=h.26in1rg)

[1.4 Summary of Business Risks 12](#_heading=h.lnxbz9)

[1.5 High-Level Recommendations 16](#_heading=h.1ksv4uv)

[**Technical Details 17**](#_heading=h.idgppjie6fy)

[2.1 Methodology 17](#_heading=h.z337ya)

[2.2 Security tools used 19](#_heading=h.3j2qqm3)

[**Open-source intelligence (OSINT) 20**](#_heading=h.ivd6nadh0m2l)

[**Findings Details 21**](#_heading=h.4i7ojhp)

[3.1 Critical severity findings 21](#_heading=h.2xcytpi)

[3.1.1 … 21](#_heading=h.1ci93xb)

[3.2 High severity findings 22](#_heading=h.184mhaj)

[3.2.1 … 22](#_heading=h.3s49zyc)

[3.3 Medium severity findings 23](#_heading=h.49gfa85)

[3.3.2 … 23](#_heading=h.2gb3jie)

[3.4 Low severity findings 24](#_heading=h.76qz8ro70t80)

[3.4.1 … 24](#_heading=h.3mj2wkv)

[3.5 Informational severity findings 25](#_heading=h.dscdd07gf94n)

[3.5.1 … 25](#_heading=h.wc55bx7dkbbz)

[**Social Engineering Campaign 27**](#_heading=h.gof1nmli3a2x)

[**Appendix A: Network mapping 28**](#_heading=h.eqy6f2ij82q)

[**Appendix B: MITRE ATT&CK mapping on Findings 29**](#_heading=h.y8dg85wtrwcs)

[**Appendix C: Assessment Artifacts 30**](#_heading=h.ykbytfp8mk7m)

[**Appendix D: Timeline 31**](#_heading=h.7xzjfdc7e7p9)

[**Appendix E: Compliance 32**](#_heading=h.7rlh91yi5baw)

[**Appendix F: Remediation Priority Suggestion 34**](#_heading=h.wa0bv2zgvfa)

[**Appendix G: Used Acronyms 35**](#_heading=h.xxhwa72p29gg)

# Executive Summary

| Scope of assessment | Internal Network Infrastructure |
| --- | --- |
| Security Level | **F** |
| Grade | Unacceptable |

| **Grade** | **Security** | **Criteria Description** |
| --- | --- | --- |
| **A** | Excellent |  |
| **B** | Good |  |
| **C** | Fair |  |
| **D** | Poor |  |
| **F** | Unacceptable |  |

## 1.1 Project Objectives

* Identify risks that organizations could be the victim of ransomware attack
  + Confirmed:
* Identifying network-based threats to and vulnerabilities in the Active Directory
  + Confirmed:
* Check for Cyber hygiene
  + Confirmed:
  + Does not meet:
  + Partially meet:
  + Meets best practices:
* Providing recommendations that RAKMS can implement to mitigate threats and vulnerabilities and meet industry best practices
  + Completed:

## 

## 1.2 Scope, Timeframe and Limitations

**Disclaimer**

.

The following hosts were considered to be in scope for testing.

| **Scope:** | **Description:** |
| --- | --- |
| 10.0.0.0/24 | Corporate network subnet |
| 10.0.10.0/24 | User network subnet |
| 10.0.20.0/24 | Train network subnet |
| 10.0.30.0/24 | Airport guest network subnet |

## 

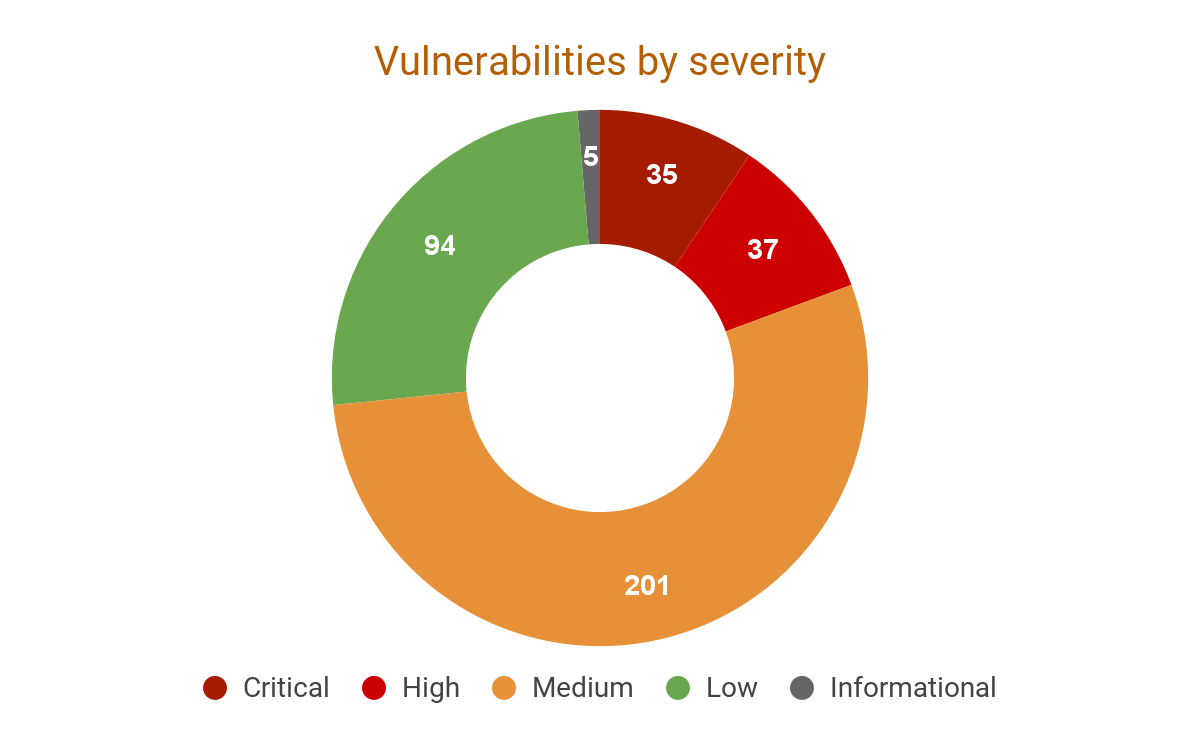
## 

## 

## 

## 1.3 Summary of Findings

Our assessment of the RAKMS internal network revealed the following vulnerabilities:



Conducted security testing demonstrates the following results.

| Severity | Critical | High | Medium | Low | Informational |
| --- | --- | --- | --- | --- | --- |
| Number of issues | 35 | 37 | 201 | 94 | 5 |

Severity scoring:

* Critical:
* High:
* Medium:
* Low:
* Informational:

Example of each severity:

* Critical:
* High:
* Medium:
* Low:
* Informational:

## 1.4 Summary of Business Risks

| **Security controls** | **Business Risks** | | | |
| --- | --- | --- | --- | --- |
| **Operational Disruption** | **Regulatory Compliance** | **Damage to Reputation** | **End User Data Disruption** |
| Insecure Network Architecture | Direct impact | Direct impact | Direct impact | Direct impact |
| Lack of Patching and Software Updates | Direct impact | High risk | High risk | Direct impact |
| Lack of Security Monitoring | High risk | Direct impact | Direct impact | Direct impact |
| Human Related Risks | High risk | High risk | High risk | Direct impact |

**Financial Loss:**

**Operational Disruption:**

**Regulatory Compliance:**

**Data Breaches:**

**Damage to Reputation:**

Critical severity issues can lead to

High severity issues can lead to

Medium severity issues can lead to

Low and Informational severity issues can lead to:

## 

## 1.5 High-Level Recommendations

Taking into consideration all issues that have been discovered, we highly recommend to:

# Technical Details

## 2.1 Methodology

There are seven stages during a penetration test. These seven phases are:

* Phase 1: Intelligence Gathering

Phase 1: Intelligence Gathering

Phase 2: Threat Modelling

Phase 3: Vulnerability Analysis

Phase 4: Exploitation

Phase 5: Post-Exploitation

Phase 6: Reporting

Phase 7: Re-audit

* [*Penetration Testing Execution Standard*](http://www.pentest-standard.org/index.php/Main_Page) *(PTES)*
* [*OWASP Top 10 Application Security Risks*](https://owasp.org/www-chapter-new-zealand/assets/slides/2020-02-09%20-%20Introduction%20to%20the%20OWASP%20Top%20Ten.pdf)
* [*OWASP Web Security Testing Guide*](https://owasp.org/www-project-web-security-testing-guide/stable/)
* [*Open Source Security Testing Methodology Manual (OSSTMM)*](https://www.isecom.org/OSSTMM.3.pdf)

[*Penetration Testing Execution Standard (PTES)*](http://www.pentest-standard.org/index.php/Main_Page)

[*Open Web Application Security Project (OWASP)*](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=Main)

[*The* *Open Source Security Testing Methodology Manual (OSSTMM)*](https://www.isecom.org/OSSTMM.3.pdf)

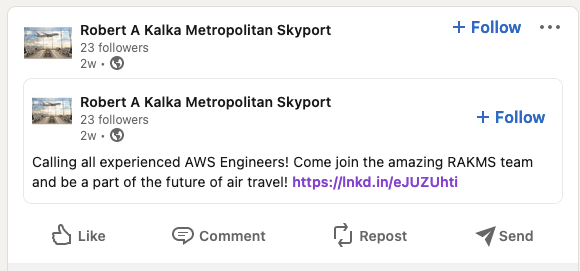
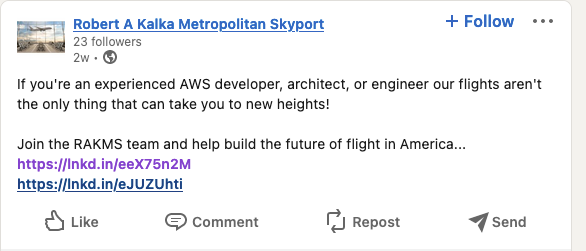
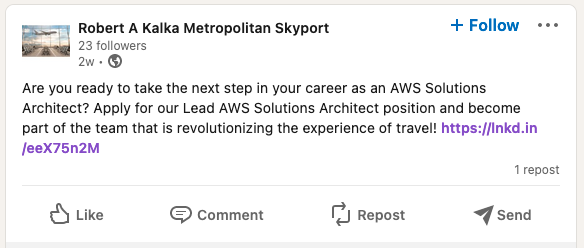
## 2.2 Security tools used

* *Manual testing:* Burp Suite
* *Vulnerability scan:* OpenVAS, nikto, arachni
* *Network scan:* Nmap, masscan, crackmapexec
* *Exploitation:* Metasploit, Inveigh
* *Hash cracking:* hashcat
* *Directory enumeration:* gobuster, dirsearch
* *Injection testing tools:* XSSHunter, SQLmap

# 

# Open-source intelligence (OSINT)

aaa



# 

# Findings Details

| 3.1 Critical severity findings |
| --- |

### 3.1.1 …

Severity: **Critical**

Location:

* All Workstations

Impact:

…

Vulnerability Details:

…

Steps to reproduce:

…

Recommendations:

…

References:

* <https://www.theregister.com/2021/02/15/solarwinds_microsoft_fireeye_analysis/>

### 

| 3.2 High severity findings |
| --- |

### 3.2.1 …

Severity: **High**

Location:

* …

Impact:

…

Vulnerability Details:

…

Proof of Vulnerability:

*…*

Recommendations:

…

References:

* <https://www.theregister.com/2021/02/15/solarwinds_microsoft_fireeye_analysis/>

| 3.3 Medium severity findings |
| --- |

### 3.3.2 …

Severity: **Medium**

Location:

* …

Impact:

…

Vulnerability Details:

…

Proof of Vulnerability:

*gege*

Recommendations:

…

References:

* <https://securiteam.com/windowsntfocus/5ep010kg0g/>

| 3.4 Low severity findings |
| --- |

### 3.4.1 …

Severity: **Low**

Location:

* …

Impact:

…

Vulnerability Details:

…

Recommendations:

…

References:

* <https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-allow-access#why-allow-connections-only-with-network-level-authentication>

| 3.5 Informational severity findings |
| --- |

### 3.5.1 …

Severity: **Informational**

Location:

* …

Impact:

…

Vulnerability Details:

…

Recommendations:

…

References:

* <https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-allow-access#why-allow-connections-only-with-network-level-authentication>

### 

# 

# Social Engineering Campaign

# Appendix A: Network mapping

# Appendix B: MITRE ATT&CK mapping on Findings

| **Vulnerability** | **MITRE ATT&CK Technique** | **Identifier** |
| --- | --- | --- |
| **Critical** | | |
|  |  |  |
| **High** | | |
|  |  |  |
| **Medium** | | |
|  |  |  |
| **Low** | | |
|  |  |  |
| **Informational** | | |
|  |  |  |

# Appendix C: Timeline

| **Time** | **Activity** |
| --- | --- |
| **21st October, 2023** | |
| 9:30 am | All testers have been given permission to access infrastructure |
|  |  |
|  |  |

# 

# Appendix D: Assessment Artifacts

**System Artifacts:**  
These Artifacts consist of scripts / reverse shells that were deployed on the systems in the scope for the penetration testing engagement.

| **Time** | **Artifact Name** | **Host** | **Description** | **Status** |
| --- | --- | --- | --- | --- |
|  | LinPEAS.sh | 10.10.10.10 | Post-exploit enumeration | Present |
|  |  |  |  | Deleted |

**Database Artifacts:**  
These artifacts consist of tables that were created in the database systems for testing purposes.

| **Time** | **Artifact Name** | **Host** | **Description** | **Status** |
| --- | --- | --- | --- | --- |
|  | LinPEAS.sh | 10.10.10.10 | Post-exploit enumeration | Present |
|  |  |  |  | Deleted |

**Web Application Artifacts:**

These artifacts consist of users, … etc that were created in the web application systems for testing purposes.

| **Time** | **Artifact Name** | **Host** | **Description** | **Status** |
| --- | --- | --- | --- | --- |
|  | LinPEAS.sh | 10.10.10.10 | Post-exploit enumeration | Present |
|  |  |  |  | Deleted |

# Appendix E: Compliance

| **TSA Requirement** | **IDs of related findings** | **Potential Monetary Penalty** |
| --- | --- | --- |
| 1. Develop network segmentation policies | | |
| a. Prevent unauthorized communications between logical zones | 1,2,2003 | $3 555,00 |
| b. Control communication between systems, allowing only encrypted or otherwise secured and protected content in transit | 2,2,2003 |  |
| 2. Create access control measures | | |
| a. Memorized secret authenticators should be reset properly | 4,2,2003 |  |
| b. Implement Multi-factor authentication, or other logical and physical security controls that  supplement password authentication | 5,2,2003 |  |
| c. Manage access rights based on the principles of least  privilege and separation of duties. | 6,2,2003 |  |
| d. Limit access to shared accounts using account management that integrates the principles of least privilege and separation of duties | 7,2,2003 |  |
| e. Prevent individuals with revoked access from having knowledge of shared account passwords | 8,2,2003 |  |
| f. Audit existing domain trust connections to ensure their necessity and adopt proper management practices | 9,2,2003 |  |
| 3. Implement continuous monitoring and detection policies | | |
| a. Defend against malicious email (spam and phishing emails) | 11,2,2003 |  |
| b. Block ingress and egress communications with known or suspected malicious IP-addresses | 12,2,2003 |  |
| c. Prevent users and devices from accessing malicious websites | 13,2,2003 |  |
| d. Block and prevent unauthorized code | 14,2,2003 |  |
| e. Monitor and/or block connections from known or suspected malicious C2 servers | 15,2,2003 |  |
| 4. Reduce the risk of exploitation of unpatched systems | | |
| a. Apply all current critical security patches and updates on Critical Cyber Systems | 17,2,2003 |  |

# Appendix F: Remediation Priority Suggestion

| **№** | **Vulnerability Title** | **Severity** |
| --- | --- | --- |
| 1 | … | **High** |
| 2 | … | **Critical** |

# Appendix G: Used Acronyms

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |