Penetration Test Report

Robert A. Kalka Metropolitan Skyport
November 11, 2023
Finals-XX

Notice of Confidentiality: This document is confidential and intended only for Robert A. Kalka Metropolitan Skyport. It contains privileged information about the company's infrastructure that must not

be shared or distributed without the company's explicit permission. Doing so may compromise the company's security and expose it to risks.

Disclaimer of Warranty and Limitation of Liability: This report presents the results of a penetration test conducted within a limited scope and timeframe. The publisher and authors are not responsible for any consequences of using or relying on this report. Any external sources or works cited or referenced in this report are not endorsed by the publisher and authors. Readers should also note that cybersecurity standards and practices may change over time and that this report reflects the information available at the time of writing.

Warning: This report is for Robert A. Kalka Metropolitan Skyport only and should not be altered. The customer is advised to address all the findings in this report and not claim any resolution until audited by qualified experts.

Table of Contents

4. Strategic Recommendations

5. Findings

5. Appendix

1. Executive Summary

1.1 Purpose:

Finals-XX conducted a security reassessment of Robert A. Kalka Metropolitan Skyport (RAKMS) infrastructure, specifically the corporate, user, train, and guest networks, on January 12th,

The engagement aims to achieve the following:

- Assess changes in RAKMS security posture between the current engagement and the engagement conducted on November 11th ,2023
- Find and exploit vulnerabilities in RAKMS infrastructure within the agreed upon scope
- Assess compliance with TSA, PCI DSS, and GDPR standards
- Document exploitation methods and results
- Recommend solutions and actions to fix and reduce vulnerabilities and risks.

1.2 Scope of Evaluation:

During the engagement, Finals-XX remained within a defined scope and ensured that actions taken during the evaluation did not interfere with business operations. The scope for this engagement encompasses all hosts within the following four subnets:

- Corporate Network: 10.0.0.0/24
- User Network: 10.0.1.0/24
- Train Network: 10.0.20.0/24
- Guest Network: 10.0.200.0/24

During the engagement, Finals-XX identified 27 hosts, including the Sky Control server, the baggage claim system, the flight monitor, trams, guest wifi and etc.[1]

[1] See Appendix A for a detailed diagram of the network topology with the discovered hosts)

1.3 Assumptions

Activities performed during the engagement were conducted in a manner that simulated an adversary that was able to gain internal access to RAKMS's network. No access credentials were provided prior to engagement.

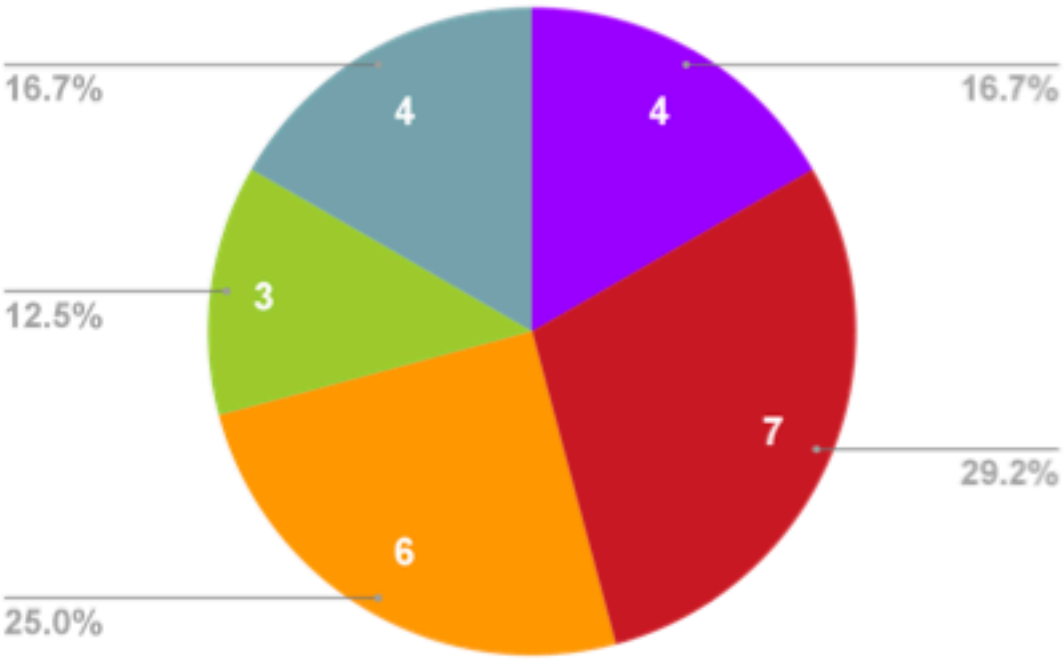
1.4 Limitations

Despite the team's efforts, certain systems remained untested due to their resilient security features, preventing the assessment team from gaining access for thorough evaluation. Additionally, certain networks and specific attacks, such as social engineering, were limited by our provided scope and at the request of RAKMS.

1.5 Summary of Findings:

Finals-XX's assessment identified a total of **24** vulnerabilities, which consisted of **4** critical severity vulnerabilities.

The chart below illustrates the distribution of identified risks and vulnerabilities.



** See Section 2.2: Severity and Risk Level Classifications for a high-level overview of the vulnerability severity categories* and *see Section 5: Findings for more details on findings and discovered vulnerabilities*

1.6 Reassessment Summary:

A primary goal of this assessment was to assess changes in RAKMS security posture between the current engagement and the engagement previously conducted on November 11th. The reassessment reveals that the vulnerabilities identified in the November 11th, 2023 assessment persist, underscoring the need for further remediation measures to be taken. Finals-XX's

findings indicate that a substantial portion of previous remediation recommendations remained unimplemented, emphasizing the opportunity for collaborative improvement. Acknowledging the ongoing nature of addressing security concerns, Finals-XX is prepared to assist RAKMS in implementing effective measures to improve their overall security posture.

Another focus of the present engagement was social engineering, where a notable observation was made regarding the awareness and training levels of RAKMS personnel in defending against social engineering attacks. To evaluate this vulnerability, Finals-XX conducted a targeted vishing attack specifically directed at RAKMS IT helpdesk staff. The assessment resulted with the successful acquisition of credentials from employees, underscoring the critical need for enhanced cybersecurity education within the organization.

In the assessment, Finals-XX emphasizes a crucial point: RAKMS's recognized risk tolerance in the commercial aviation sector, which also falls under critical infrastrucuture is notably high, posing potential implications for national security and public safety. While current risk mitigation strategies are in place, it is imperative to bolster them to safeguard critical assets, preserve brand integrity, and ensure the smooth flow of business operations at airports. This reassessment aims to enhance RAKMS's overall security posture and align it with the heightened standards necessary for critical infrastructure, addressing the pressing concerns identified in the reassessment.

** See Section 5.2: Residual Risk Details for more information on addressed and unaddressed risks*

1.7 Overall Risks & Impacts

The assessment uncovered noteworthy risks that could have substantial impacts on crucial aspects of the airport's operations. These risks extend to compliance, customer data, various facets of RAKMS business operations (such as baggage claim and people mover systems), and the overall brand image. Non-compliance poses legal and financial risks for RAKMS in addition to risking the airport's reputation in the industry.

These risks have the potential to result in significant consequences, including substantial financial penalties.

1.8 Key Strengths:

The assessment team identified the following strengths in security during the evaluation of RAKMS infrastructure:

- **Hashing —** Finals-XX observed secure hashing practices in RAKMS infrastructure. This was identified in the windows account hashes of employees,

protecting their accounts from being compromised by Finals-XX penetration testers..

- **Account Lockout Policy —** Finals-XX observed strong account lockout policies **in** RAKMS infrastructure, preventing them from being able to brutefoce logins. This was identified in when attempting to log into employee accounts. This measure contributes to the overall robustness of the security posture.

- **Phishing Awareness —** In the phishing exercise requested, Finals-XX found that the sent phishing email did not result in a succesful compromise. This is likely a sign of proper phishing awareness and training.

1.9 Strategic Recommendations

Team 4 recommends the following measures be prioritized for implementation to improve RAKMS overall security posture and remediate identified vulnerabilities:

- **Strong Authentication Measures Implementation —** It is recommended to enforce the implementation of Multi-Factor Authentication (MFA) across all systems and portals in RAKMS infrastructure to enhance security. This action should be prioritized for immediate implementation to address the associated vulnerabilities or risks related to unauthorized access and credential-based threats.

- **Social Engineering Mitigation —** It is recommended to implement Employee Awareness Training across the organization in order to enhance the understanding of social engineering tactics and promote a culture of security awareness. This action should be prioritized for immediate implementation to address the vulnerabilities associated with phishing and unauthorized access attempts.

** See Section 4: Strategic Recommendations for more details*

1.10 Final Notes

RAKMS's commitment to revolutionizing travel and pioneering an era of seamless, sustainable, and personalized aviation while prioritizing security and safety is commendable. Following our initial assessment, it is evident that RAKMS has taken strides in enhancing the security of its systems, marking a pivotal step forward in supporting its mission. The progress RAKMS has made demonstrates the company's dedication and proactive approach to ensuring a secure aviation landscape.

Finals-XX values RAKMS' partnership in this journey towards a more secure and innovative aviation landscape. We encourage RAKMS to leverage the insights provided in this report to stay vigilant and to continuously enhance its security posture, helping it carry out its mission to create unparalleled journeys for every traveler.

Finals-XX would be proud to offer our services again for any future security evaluations or support that RAKMS may require to uphold its mission of ensuring a seamless and secure traveling experience for all passengers.

2. Introduction

2.1 Methodology

2.1.1 Penetration Testing Execution Framework

To ensure a thorough evaluation of RAKMS security, Finals-XX conducted the security assessment following the Penetration Testing Execution Standards (PTES), a standardized and widely recognized framework that provides a structured approach to conducting penetration tests and security assessments. Finals-XX also incorporated the MITRE ATT&CK Framework to map findings to real-world threat techniques, which increased the depth and effectiveness of the assessment by providing a structured method to categorize, analyze, and develop responses to attack techniques.

2.2 Severity and Risk Level Classifications

Finals-XX used two measures to assess the urgency of a vulnerability. The main measure is the severity level, which is scored using the Common Vulnerability Scoring System v3.1 (CVSS), an industry-standard framework for measuring the severity of vulnerabilities that ensures a consistent and reliable approach to assessing their potential impact. CVSS measures severity based on several factors, such as exploitability, extent, impact, and complexity. Finals-XX also provides the CVSS base vector string to give a concise representation of the characteristics and impact of a vulnerability.

The secondary measure, risk level, ranks vulnerabilities based on their impact and the likelihood of the vulnerability being exploited in the context of the organization, following the approach recommended in NIST SP-800-30.

These two measurements will help prioritize remediation and mitigation measures for vulnerabilities based on their overall impact, considering violations of confidentiality, integrity, and availability, as well as business impacts such as financial loss, brand damage, and legal action against the organization.

Severity Level Explanations		
Severity Rating	**Base Score**	**Explanation**
Critical	9.0-10.0	Vulnerability poses an immediate and significant threat, capable of causing extensive system compromise. Has the potential to lead to significant data breaches and severe operational disruption
High	7.0-8.9	Vulnerability poses substantial risk, potentially resulting in partial system compromise or significant data exposure, impacting operations and security
Medium	4.0-6.9	Vulnerability has moderate potential impact, causing moderate disruption or exposing some sensitive information, affecting operational continuity to a certain extent.
Low	0.1-3.9	Vulnerability has limited impact or limited potential for exploitation They might lead to minimal disruption or have low potential for data exposure.
Informational	0	Finding does not pose immediate threat, but provides useful information for improving overall security posture.

Risk Level Explanations	
Rating	**Explanation**
Critical	Vulnerability poses severe threat with a high probability of exploitation. Potential for severe data breaches, operation disruptions, financial loss, and considerable compromise to the organization's systems and reputation
High	Vulnerability poses significant threat with a significant probability of exploitation, potentially leading to substantial data exposure, financial risk, or operational disruption.
Medium	Vulnerability has a moderate probability of exploitation, potentially causing moderate disruption or sensitive information exposure

Low	Vulnerability has a lower probability of exploitation and pose minimal risk to operations or security. It has the potential to cause minimal disruption or have little potential for data exposure or system compromise.
Informational	Vulnerability has an extremely low probability of exploitation with minimal impact if exploited. Poses negligible risk to operations and security. It is highly unlikely to be exploited or cause any significant disruption or data exposure.

** See Appendix D for a detailed explanation of the severity and risk level classifications used during this engagement*

3. Assessment Results

Finals-XX has provided below a risk analysis, listings of the company's compliance with the TSA Cybersecurity Requirements for Airport and Aircraft Operators, GDPR, and PCI-DSS standards, as well as a recommended remediation plan. **[let me know what you think to put in the risk analysis section cuz I think it can get easily repetitive, but then I'm like it can be a good overview was on the fence of how to approach writing it]**

3.1 Risk Analysis

The vulnerabilities outlined in the report introduce a substantial level of business risk for RAKMS. The primary concern is operational risk stemming from cyber vulnerabilities. This risk manifests as a potential for external fraud, encompassing theft resulting from compromised confidentiality and integrity.

This scenario could lead to the misappropriation of intellectual property and other assets through illicitly obtained credentials. Any disruptions that compromise the availability of RAKMS's services, resulting from the exploitation of these vulnerabilities, also fall under the classification of external fraud, posing a significant operational risk to the organization.

Furthermore, some of the vulnerabilities found may qualify as violations of PCI-DSS. Should such violations be found and remain unmitigated, they may pose regulatory risks to RAKMS as well as financial risks due to the possibility of significant monetary penalties. Additionally, if the same violations are publicized through a Notice of Penalty posted on the PCI-DSS website, they may also pose a reputational risk to the company. With the company only recently having gone public, this risk also amounts to potential financial risk if investors lose trust in the company.

3.2 Compliances & Regulations

3.2.1 TSA Cybersecurity Requirements for Airport and Aircraft Operators

RAKMS is an airport facility in the US that is subject to the regulations and security programs set by the US Transportation Security Administration (TSA). Evaluation of RAKMS's compliance with these regulations were therefore an essential part of the engagement.

The TSA announcement for the TSA Cybersecurity Requirements for Airport and Aircraft Operators does not provide a documented security directive specifically for airports and airport carriers but references SD-1580/82-22-01, cybersecurity measures issued to passenger and freight railroad carriers. Finals-XX will use the cybersecurity requirements referenced in SD-1580/82-22-01 to supplement implementation details for TSA Cyber

Finals-XX conducted a penetration assessment that considered the compliance risks of RAKMS to SD-1580/82-22-01. This is a standard that applies to passenger and freight railroad carriers. However, on March 9, 2023, the TSA issued a new cybersecurity amendment, TSA Cybersecurity requirements for Airport and Aircraft Operators on an emergency basis for some TSA-regulated airport and aircraft operators. This followed similar measures announced in October 2022 for passenger and freight railroad carriers. Therefore, our findings also evaluated the compliance with SD-1580.82.

Finals-XX's evaluation considered only those standards subject to enforcement as of November 11, 2023, and those that could be assessed within the stipulated timeframe and the limited digital access provided.

Title	Reference
TSA Cybersecurity Requirements for Airport and Aircraft Operators	***https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft***
SD-1580/82-22-01	***https://www.tsa.gov/sites/default/files/sd-1580-82-2022-01.pdf***

**References for each section of the TSA Cybersecurity Requirements referenced by Finals-XX are provided in Appendix E*

3.2.2 General Data Protection Regulation

RAKMS is an international airport in the US that handles data of EU passengers. Therefore, it must comply with the data protection standards set by national and international authorities, including GDPR. GDPR is a European regulation that also regulates international data transfers, which RAKMS often performs as an international airport. RAKMS can face significant financial penalties and legal consequences if it does not comply with GDPR

Finals-XX's analysis focused on the GDPR standards that were in force as of November 11, 2023. However, RAKMS should be aware of any future enforcement requirements that the analysis did not cover.

For more information on GDPR regulations, please refer to the link below.

Title	Reference
GDPR	***https://gdpr-info.eu/***

**References for each article of GDPR referenced by Finals-XX are provided in Appendix F.*

3.2.3 Payment Card Industry Data Security Standard

RAKMS is an airport that is part of the critical infrastructure. This means that it has to follow the regulatory standards set by national organizations to protect its business operations and customer information from attacks. One of these standards is PCI-DSS, which applies to RAKMS because it is a Payment Card provider that handles cardholder data. RAKMS can face significant financial penalties from regulatory authorities if it does not comply with PCI-DSS.

Finals-XX's analysis only covered the standards that were enforceable as of November 11, 2023. Finals-XX strongly recommends RAKMS to also consider the standards that will be enforced in the future, even though they were not part of Finals-XX's analysis.

For more information on PCI-DSS, please refer to the link below

Title	Reference
PCI DSS	***https://listings.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf***

**References for each section of PCI-DSS referenced by Finals-XX are provided in Appendix F.*

3.3 Compliance to TSA Cybersecurity Requirements for Airport and Aircraft Operators

Below we will detail what compliances were met. Compliances met are indicated with "Y" located in the green cells. Compliances that violated are indicated with "N" located in the red cells.

Resultant Compliance with TSA Cybersecurity Requirements for Airport and Aircraft Operators		
Y/N	**Ref #**	**Requirements**
	III.B	Develop network segmentation policies and controls to ensure that operational technology systems can continue to safely operate in the event that an information technology system has been compromised and vice versa
	III.C	Create and access control measures to secure and prevent unauthorized access to critical cyber systems;
	III.C.1.a	Policy for memorized secret authenticator resets that includes criteria for when resets must occur
	III.C.2	Multi-factor authentication or other logical and physical security controls that supplement password authentication. If not applied, the owner/operator must specify what compensating controls are used
	III.D	Implement continuous monitoring and detection policies and procedures to defend against, detect, and respond to cybersecurity threats and anomalies that affect critical cyber system operations; and
	III.F	Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers, and firmware on critical cyber systems in a timely manner using a risk-based methodology

3.4 Compliance to GDPR

Below we will detail what compliances were met. Compliances met are indicated with "Y" located in the green cells. Compliances that violated are indicated with "N" located in the red cells.

Resultant Compliance to GDPR		
Y/N	**Ref #**	**Requirements**
	12	1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. 2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.
	15	1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations; (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; (f) the right to lodge a complaint with a supervisory authority; (g) where the personal data are not collected from the data subject, any available information as to their source; (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. 2. Where personal data are transferred to a third country or to an international organization, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.
	17	1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the

		controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).
	24	1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary. 2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller. 3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.
	32	1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

	82	1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.
		3. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. 2The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. 4. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3.5 Compliance to PCI DSS

Below we will detail what compliances were met. Compliances met are indicated with "Y" located in the green cells. Compliances that violated are indicated with "N" located in the red cells.

Resultant Compliance to PCI DSS		
Y/N	**Ref #**	**Requirements**
	1.1.7	Install and maintain a firewall configuration to protect cardholder data. Install a firewall at each internet connection(every device). Configure your firewalls with a description of groups responsible for network components and business justifications for all services/protocols/ports in the configuration.
	2.1	Do not use vendor-supplied defaults for system passwords and other security parameters. Identify a sysadmin to be responsible for system components. Document policies to change vendor-supplied default passwords, default wireless settings and remove default accounts before installing a system on your network. Maintain an inventory list of all system components in scope for PCI DSS.
	3.1	Protect stored cardholder data. Make sure the stored data and data in transit are unreadable. Use a data discovery tool to find misplaced sensitive data in your environment
	4.1	Encrypt transmission of cardholder data across open public networks. Identify where you send cardholder data and ensure your policies are not violated in the journey and only trusted keys or certificates are used.
	5.1.1	Protect all systems against malware and regularly update antivirus software or programs. Regularly update anti-virus software on your commonly affected systems

		and evaluate whether additional systems are at risk of needing an antivirus. Automate anti-virus scans and maintain antivirus audit logs for your systems. Document procedures for protecting against malware
	6.2	Develop and maintain secure systems and applications. Establish a process to keep up-to-date with the latest security vulnerabilities and identify the risk level. Use strict development processes and secure coding guidelines (outlined in DSS) when developing software in-house
	7.2	Restrict access to cardholder data by business need to know. Create a list of roles with access to the CDE that includes the definition of each role, their privilege level, and what permissions are required for each role to function. Create a least-privilege policy for all employees and a default "deny-all" setting on all access control settings
	8.2	Identify and authenticate access to system components. Define and document procedures for user identification and authentication on all system components. Assign unique IDs to all users, test those privilege controls, and revoke access on inactive/terminated users. Follow best practice guidelines outlined in DSS for password setting – including strong password composition, encrypting credentials, verifying ID before reset, and mandatory resets every 90 days.
	9.1.1	Restrict physical access to cardholder data. Document process for physical access to CDE systems and a list of all devices, limiting access to roles that require it and monitoring all with authorization tokens and surveillance. .
	10.8	Track and monitor all access to network resources and cardholder data. Track all admin actions, login attempts, account changes, and pauses in the audit trail. Ensure each audit log captures user ID, event type, date and time, event success or failure, where the event originated from, and what resources are affected.
	11.1	Regularly test security system and process

4. Strategic Recommendations

4.1 Key Security Strengths

P1: Network Segmentation

Description

We commend RAKMS for implementing secure security practices and establishing distinct networks for specific groups. The creation of four separate subnets in our pentest network enhances the overall safety of your network. In the event that one subnet is infected with malicious malware, the impact remains contained within that specific network.

P2: Account Lockout Policy

Description

We applaud RAKMS for maintaining a robust Account Lockout Policy. This policy acts as a critical defense measure by limiting the number of unsuccessful login attempts, mitigating the risk of unauthorized access due to brute force attacks. This proactive approach significantly reduces the potential impact of credential-based threats, enhancing overall security.

P3: Hashing

Description

We want to commend RAKMS once again for implementing robust encryption and hashing algorithms. During the penetration testing conducted by Finals-XX on the RAKMS network, we encountered instances where sensitive information was effectively encrypted or hashed. This demonstrates a commendable attention to detail and significantly enhances the security posture, making it more challenging for an attacker to compromise sensitive information. We appreciate this commitment to maintaining a high level of security.

5. Findings

5.1 Overview

Finals-XX performed a penetration test on RAKMS and discovered <X> significant vulnerabilities in the company's network. Finals-XX also found [x number] informational finding that could further improve RAKM's overall security posture if addressed. The table below shows a summary of the findings by their severity level.

Findings Count					
Severity Rating	**Critical**	**High**	**Medium**	**Low**	**Informational**
Vulnerabilities	2	4	3	1	2

The chart below illustrates the distribution of identified risks and vulnerabilities

Include a bar graph of vulnerabilities showing how many vulnerabilities are found of each category (How many are Critical, High, Medium, Low, etc.)

The following is a brief overview of each finding found during testing. Section 5.3 of this report, the Technical Findings Details section, provides more details about these findings.

Finding ID	Severity Level	Finding Name
C1	Critical	Pass-the-Hash
C2	Critical	Exposed API Endpoint
H1	High	AWS Access Control
H2	High	Credentials in LDAP
H3	High	Unauthenticated Access to Sensitive Employee Data
H4	High	Passenger PII sent over Unencrypted Channels
M1	Medium	Use of external email address for business
M2	Medium	Kerberos Pre-authentication Disabled
M3	Medium	LFI in Picture System of Baggage Check-in
L1	Low	Internal Information Disclosure using Hidden NTLM Authentication
L2	Low	XSS in Employee DB
I1	Informational	Internal Information Disclosure using Hidden NTLM Authentication
I2	Informational	Exposed UUID

5.3 Technical Findings Details

This section presents the key technical findings from the security assessment, following a structured approach. Vulnerabilities are categorized by severity levels, presented in order of severity: critical, high, medium, and low, in alignment with predefined definitions. Subsequently, informational findings are documented and discussed. Each technical finding includes a severity and risk level graphic, a brief vulnerability overview, a business impact analysis, reproducible attack replication documentation, systems affected, recommended remediation, and references for further information.

Critical Risk Findings

C1: Pass-the-Hash **CRITICAL**

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	Critical		Score	9.1	
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N				
Risk Matrix					
Risk Level	Critical	Impact	Critical	Probability	High

Affected Systems			
IP Address	Port	Service	Version
10.0.0.0/24	n/a	NTLM	2

Overview:

Pass-the-Hash vulnerability was found within the Windows network of the RAKMS airport infrastructure, specifically in the domain controller, allowing attackers to exploit hashed credentials and escalate privileges. This compromise affects RAKMS Confidentiality and Integrity by potentially compromising sensitive user credentials and compromising the integrity of the entire network.

Finals-XX identified a vulnerability within the domain controller. The vulnerability involves the exploitation of hashed credentials, violating security standards and risking unauthorized access to critical systems. This violation is particularly significant in the context of [Relevant Compliance Standard or Requirement], which mandates strict controls over credential management and access.

Finals-XX successfully accessed the domain controller using Pass-the-Hash techniques, allowing them to escalate privileges and potentially compromise sensitive user credentials. This action violates confidentiality, posing a high level of risk to the security posture of RAKMS airport infrastructure. The details of this vulnerability, including evidence and steps to reproduce, are thoroughly documented in the Attack Replication.

Immediate remediation is essential to address this vulnerability, prevent unauthorized access, and ensure compliance with security standards, safeguarding the confidentiality and integrity of our network.

Business Impact:

The discovery of a Pass-the-Hash vulnerability in the Windows network of RAKMS airport infrastructure poses critical risks to our organizational security.

An attacker exploiting this vulnerability could potentially:

• Compromise sensitive data stored within the network.
• Disrupt critical operations, leading to potential service outages.
• Escalate privileges to the domain controller, compromising the entire network integrity.

These risks could lead to severe consequences, including legal liabilities, financial losses, and reputational damages. Immediate remediation is imperative to safeguard our airport infrastructure and ensure compliance with security standards.

Addressing this vulnerability promptly is crucial to maintaining the trust of our stakeholders, protecting sensitive information, and preserving the operational resilience of RAKMS airport.

Attack Replication:

1. crackmapexec smb <IP> -u <user> -H <LM>

2. evil-winrm –i <IP> -u <user> -H <LM>

3. secretsdump.py <user>@<IP> -hashes <NTLM>

Please refer to bleepingcomputer "Pass-the-Hash explained and How to Prevent" in References for more comprehensive Attack Replication.

Recommended Remediation:

Finals-XX recommends that RAKMS IT operations team implement the following actions to mitigate the risk associated with pass-the-hash attacks:

1. Avoid Logging into Workstations with Privileged Accounts"
- Establish dedicated management workstations for privileged operations, minimizing the risk of pass-the-hash attacks on regular workstations.

2. Enable Windows Defender Credential Guard:
- Activate Windows Defender Credential Guard on Windows 10 and 11 systems to utilize hardware-level virtualization, enhancing resistance against pass-the-hash attacks.

3. Apply the Principle of Least User Access:
- Implement the Principle of Least User Access, restricting user permissions to the minimum necessary for their roles. While not preventing pass-the-hash attacks, it minimizes potential damage in case of compromise.

4. Use Firewalls to Block Unnecessary Traffic:

- Configure firewalls to block workstation-to-workstation traffic, limiting an attacker's lateral movement and hindering the success of pass-the-hash attacks.

5. Leverage Specops Password Auditor:
- Employ Specops Password Auditor to assess password health, identifying at-risk accounts before they are compromised and preventing the initial points of entry for attackers.

In summary, RAKMS IT operations should establish dedicated management workstations, enable Credential Guard, follow the Principle of Least User Access, utilize firewalls to block unnecessary traffic, and leverage Specops Password Auditor for proactive identification of at-risk accounts. These measures collectively enhance the organization's security posture against pass-the-hash attacks.

References

Tenable CVSS
- https://www.tenable.com/plugins/nessus/63478

Pass-the-Hash commands
- https://viperone.gitbook.io/pentest-everything/everything/everything-active-directory/lateral-movement/alternate-authentication-material/wip-pass-the-hash

Pass-the-Hash explained and How to Prevent
- https://www.bleepingcomputer.com/news/security/pass-the-hash-attacks-and-how-to-prevent-them-in-windows-domains/

C2: Exposed API Endpoints **CRITICAL**

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	Critical	Score	9.8		
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H				
Risk Matrix					
Risk Level	high	Impact	High	Probability	high

Affected Systems			
IP Address	Port	Service	Version
S3://rakmstoolrequisition20240111034801124200000007		AWS api	

Overview:

Three API endpoints, three internal websites was found, allowing attackers to **manipulate employee tools requsition enabling attacker request tools with founding**, expose the airport map and api, and compromising confindentialty of tools requistion granting all use right to request for all tools. This attack poses **critcial level as it abuse the right of all tool requisition**. This attack carries the potential cause to significant financial lose and portiental unauthorzied purchase used unintended and illegal usage that can leads rand damages and unlawful acts

Business Impact:

The discovery of exposed s3 buckets endpoints poses critical risks to employee internal websites and company budget .This vulnerability allows all user who visit the website to have right to purchase any items with company's founding. An attacker exploiting this vulnerability could potentially cause significant finanial damages from unauthorized ordering Moreover the unauthorized purchased can be illegal items or unintended items that can cause portiental damage. In a scenario, an unauthorized person can use the application to purchase items that can be used for harmful purposes under the company's supervision. This will cause financial damage and ilegal violation

Attack Replication:

1. Login with AWS access key and secret access key with a profile , then check s3 buckets. To do this, run the following command: cli "aws s3 ls –profile"
2. Check the http address and API endpoint input into browser, upload the pictures of the item you like to purchase


Welcome to the RAKMS Tool Requisition System Beta!
ealous of a coworker's tool? Upload a photo here to order one!
Choose File
No file chosen
Submit
Welcome to the RAKM
Beta!
Jealous of a coworker's tool? Upload a photo here to order one!
Requisition ID
Tool Name
Tool Description
Tool Weight
Tool Price
Quantity Requested (min: 1, max: 5)
1
Total Price
Submit

Recommended Remediation:

Finals-XX recommends that **RAKMS implement access control, update bucket policy to restrict public access, monitor and log the request from the s3 bucket to mitigate the risk associated with exposed s3 bucket endpoints**. This includes **[implementing strong access control in s3 bucket methods, update s3 bucket policy disable public access , enforcing logging and MFA for each purchase** .. Additionally, it is advised to enable aws config rule restricting from unauthorized person to view s3 bucket resources to enhance the overall security posture.

C3: Improper Authorization to Tram Admin Controls **CRITICAL**

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	Medium		Score	6.5	
Vector	AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H				
Risk Matrix					
Risk Level	High	Impact	High	Probability	High

Affected Systems			
IP Address	Port	Service	Version

10.0.20.101-103	8088/tcp	http	Werkzeug/3.0.1 Python/3.10.12

Overview:

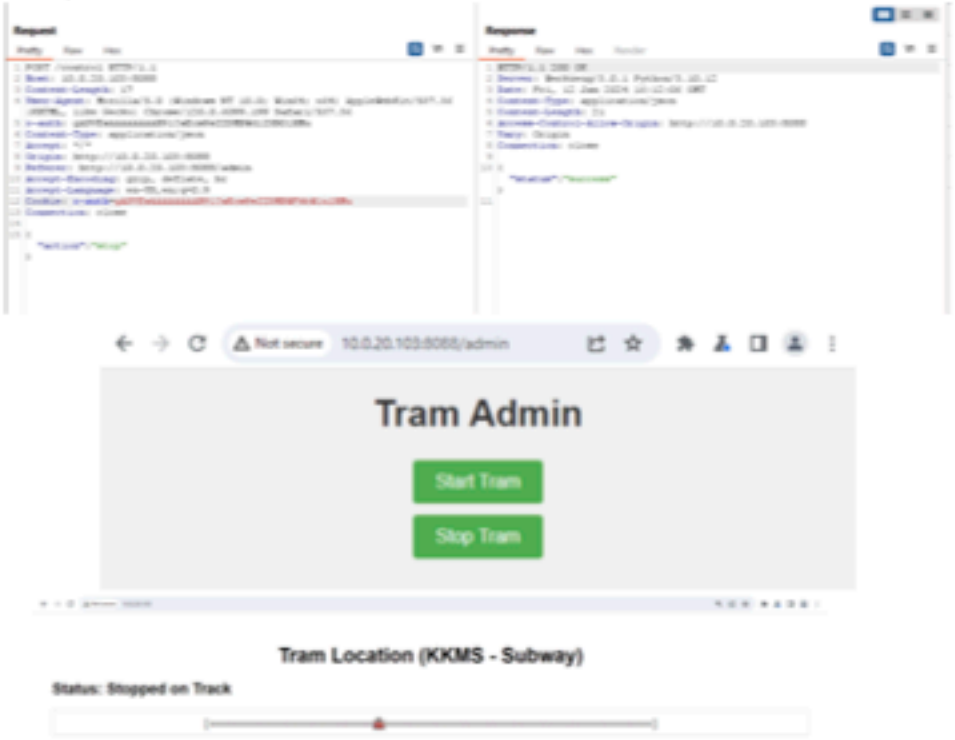
[redacted] discovered weak authorization for the tram admin pages, potentially allowing attackers to stop trams compromising accessibility of the tram system.

Business Impact:

This attack poses a significant risk to the trams. An attacker exploiting this vulnerability could potentially disrupt operations and create new fake trams to cause confusion.

Attack Replication:

- Fuzz port 8088 on any tram to discover /admin
- Receive guest cookie from server
- Decode base64 cookie and replace "guest" with "admin"
- Send new request for /admin



Recommended Remediation:

Finals-XX recommends that RAKMS implement stronger authorization methods to mitigate the risk associated with this vulnerability. This could be as simple as swapping to

a signed jwt token instead of the base64 cookie in order to verify that the server sent the admin cookie.

CRITICAL

C4: EC2 key pair exposure CRITICAL

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	Critical		Score	9.1	
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N				
Risk Matrix					
Risk Level	Moderate	Impact	High	Probability	Low

Affected Systems			
IP Address	Port	Service	Version
10.0.5.75	3306/tcp	MySQL	5.5.5 MariaDB

Overview:

The exposure of EC2 key pairs in the AWS environment poses a significant risk, allowing attackers unintended access to these critical components. This threat jeopardizes the confidentiality, integrity, and availability of the key pairs. The severity of the issue stems from the attacker's ability to view and exploit the exposed key pair, paving the way for unauthorized activities. The potential consequences include the creation of malicious Amazon Machine Images (AMIs) with the capacity for substantial and far-reaching damage. Swiftly addressing this vulnerability is imperative to safeguard the security and integrity of the AWS environment.

Business Impact:

The identification of the exposed EC2 key pair vulnerability poses a severe risk to RAKMS' business operations and reputation. If exploited by attackers, it could lead to significant disruptions, compromise sensitive data, and potential violations of compliance standards. The unauthorized access to key pairs creates a pathway for malicious activities, putting RAKMS at risk of legal liabilities, financial losses, and reputational damages. Immediate attention and remediation are essential to mitigate these potential adverse impacts.

Attack Replication:

- First use the given user policy to list ec2 key pairs run (aws ec2 describe-key-pairs)
- Second use the existed key id to create new ec2 run (aws ec2 run-instances --image-id ami-xxxxxxxxxxxx --instance-type t2.micro --key-name YourKeyPairName --security-group-ids)

Recommended Remediation:

Finals-XX recommends that [Affected Company/Organization] swiftly address the compromised EC2 key pair by initiating a key rotation process. This involves generating a new key pair, updating associated instances to use the new key, and reinforcing a proactive key management strategy. Additionally, consider implementing strict access controls and regular key rotation practices to enhance security. Ensuring that only authorized personnel have access to key pairs is crucial. Implementing encryption protocols for data transmission and regularly reviewing and updating access policies will contribute to a more secure IT environment.

High Risk Findings

H1: AWS access control

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	High		Score	7.6	
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H				
Risk Matrix					
Risk Level	Moderate	Impact	High	Probability	Low

Affected Systems			
IP Address	Port	Service	Version
		IAM cloud trail EC2	V1

Overview:

Access control issues were found in the AWS environment, affecting IAM policies, databases, CloudTrails, and System Manager, allowing attackers to access resources and credentials. This compromise jeopardizes the confidentiality and integrity of metadata and user data. The attack poses a high level of risk as it grants access to sensitive credentials. Additionally, this attack carries the potential to expose confidential data and violates compliance standards

Business Impact:

The discovery of a lack of access control poses a high-level risk to AWS credentials and user data. An attacker exploiting this vulnerability could potentially compromise sensitive data, violate compliance standards, and expose the system to further targeted attacks based on the information collected. The attacker not only jeopardizes the confidentiality, integrity, and availability of critical data but also introduces the possibility of subsequent security breaches. These risks could lead to data breaches, regulatory penalties, and damage to the organization's reputation and trust.

Attack Replication:

First identify account iam policy (aws iam list-attached-user-policies --user-name)
aws iam get-policy-version --policy-arn
<arn:aws:iam::975426262029:policy/list_apigateways> --version-id <VERSION_X>
Now we can run cli commands such as (aws iam list-access-keys –user-name)

References

https://aws.amazon.com/iam/

https://aws.amazon.com/identity/attribute-based-access-control/

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_aws-services-that-work-with-iam.html

H2: Credentials in LDAP **HIGH**

er

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	High	Score	8.6		
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L				
Risk Matrix					
Risk Level	High	Impact	High	Probability	High

Affected Systems			
IP Address	Port	Service	Version
10.0.0.5-6	389	http	n/a

Overview:

Credentials exposed in 10.0.0.5-6 LDAP for RAKMS pose a high-risk threat. Attackers gaining unauthorized access compromise user credentials, risking confidentiality, integrity, and availability. The potential fallout includes unauthorized system access, service disruptions, financial losses, and brand damage. Urgent action is needed to secure the LDAP server and prevent unauthorized access.

Business Impact:

The exposure of credentials in LDAP presents significant risks to the organization. If exploited, this vulnerability could have severe consequences impacting RAKMS's operations, financial standing, and overall reputation.

Potential impact scenarios:

1. Unauthorized System Access: The compromise of credentials raises the risk of unauthorized access, potentially leading to the misuse of privileged accounts and compromising critical systems.

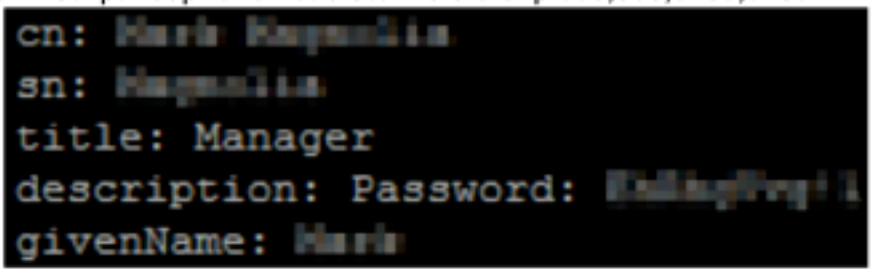
2. Service Disruptions: The exposed credentials may result in disruptions to RAKMS services, affecting the availability and reliability of the infrastructure, impacting the organization's operational efficiency.

3. Financial Implications: Unauthorized access and service disruptions carry the potential for financial losses, impacting the financial health of RAKMS and the success of the contracted project.

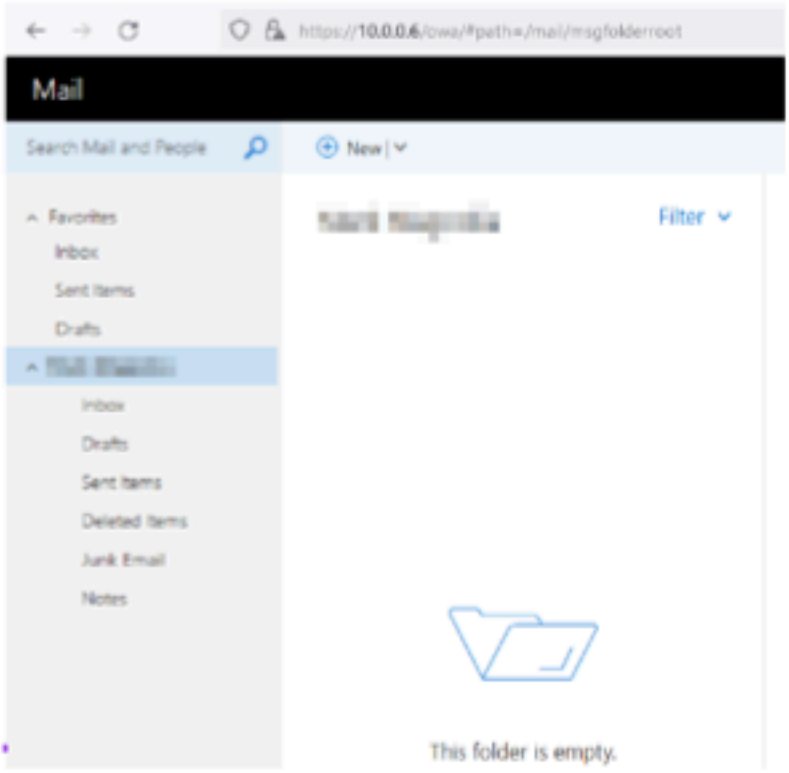
These risks could lead to adverse consequences such as legal liabilities, financial setbacks, and damage to RAKMS's reputation. Immediate remediation is essential to fulfill the contracted responsibilities and maintain a secure environment.

Attack Replication:

1. nmap -n -sV --script "ldap* and not brute" 10.0.0.5 -p 389,636,3268,3269



2. Log into Outlook Mail at https://10.0.0.6/owa/#path=/mail/msgfolderroot with credentials



Recommended Remediation:

Finals-XX recommends that RAKMS implement the following actions to mitigate the risk associated with plaintext password exposure in LDAP, specifically addressing the use of Nmap LDAP scripts:

1. Implement Secure LDAP (LDAPS): Transition from unsecured LDAP to LDAPS, which encrypts the communication between clients and the LDAP server, preventing the interception of plaintext passwords.
2. Update LDAP Configuration: Modify the LDAP server configuration to disable plaintext password storage or transmission, making it more resistant to scripts that attempt to extract such information.
3. Strong Authentication Policies: Enforce strong authentication policies, including the use of hashed or encrypted password storage mechanisms, to enhance the overall security of LDAP credentials.

Compliances & Regulations

1. PCI-DSS:

- Access Controls (PCI-DSS Requirement 7): Inadequate management of LDAP credentials may lead to violations of PCI-DSS access control requirements, risking unauthorized access to payment card data.
- Encryption (PCI-DSS Requirement 4): Failure to secure LDAP communication with encryption may result in non-compliance with PCI-DSS encryption requirements, jeopardizing the protection of sensitive payment information.

2. GDPR:

- Security of Processing (GDPR Article 32): Insufficient protection of LDAP credentials may result in violations of GDPR's requirement to implement appropriate technical and organizational measures to ensure the security of personal data processing.
- Data Protection by Design and Default (GDPR Article 25): Failure to integrate secure LDAP credential management into data processing systems may be seen as non-compliance with GDPR's principle of data protection by design and default.

References

LDAPS Setup Guide

- https://techcommunity.microsoft.com/t5/sql-server-blog/step-by-step-guide-to-setup-ldaps-on-windows-server/ba-p/385362

LDAP Enumeration

- https://www.geeksforgeeks.org/ldap-enumeration/

END OF FINDING BLOCK

H3: Unauthenticated Access to Sensitive Employee Data **HIGH**

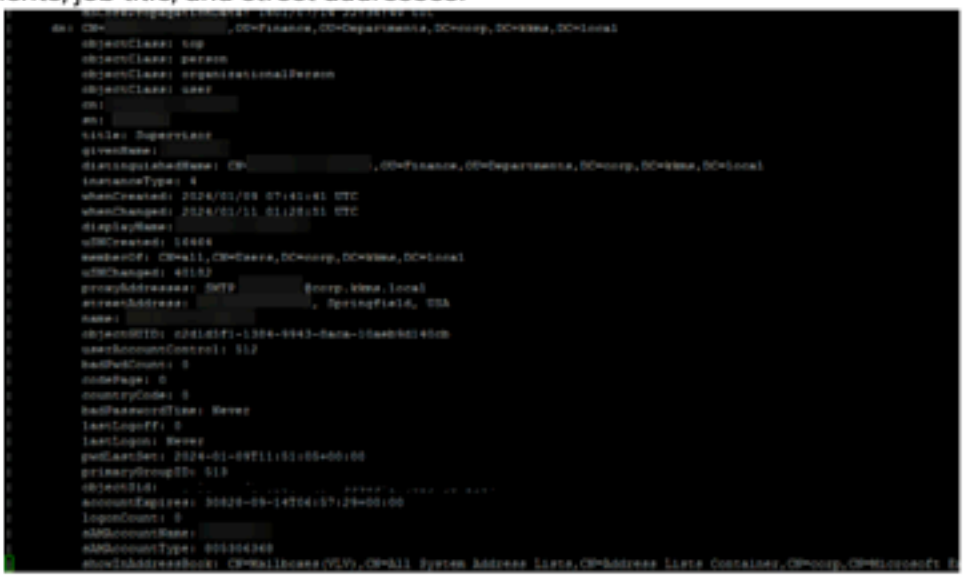
Common Vulnerability Scoring System (CVSS v3.1)					
Severity	High	Score	8.2		
Vector	AV:A/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N				
Risk Matrix					
Risk Level	High	Impact	High	Probability	High

Affected Systems			
IP Address	Port	Service	Version

10.0.0.5	3268/tcp	ldap	Microsoft Windows Active Directory LDAP

Overview:

Unauthenticated access to the active directory data was found on SkyControl01, allowing attackers to view sensitive data pertaining to employees such as: employee names, departments, job title, and street addresses.



This attack poses a high potential for risk as it involves sensitive personal information of employees and is not a difficult vulnerability to exploit.

Business Impact:

These risks would not only impact the privacy of the employees but could result in reputation damage to the RAKMS brand and security. Remediation is strongly recommended.

Attack Replication:

- With a linux device on the network and ldapsearch installed, use the command "ldapsearch -x –H ldap://10.0.0.5:3268"

Recommended Remediation:

Finals-XX recommends that **IT modify the LDAP permissions of unauthenticated users only allow authorized LDAP queries to be executed**. Ideally, use a zero trust model for sensitive information such employee data.

References

Aa

- What Is LDAP & How Does It Work? - https://www.okta.com/identity-101/what-is-ldap/

H4: Passenger PII sent over Unencrypted Channels **HIGH**

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	High	Score	7.3		
Vector	AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N				
Risk Matrix					
Risk Level	High	Impact	High	Probability	High

Affected Systems			
IP Address	Port	Service	Version
10.0.0.33	80/tcp	http	unknown

Overview:

Team[redacted] discovered that the baggage check-in website was using HTTP instead of HTTPS. This means any information sent in between the client and the server such as the passenger info that is requested is unencrypted when sent and are at risk of being captured by an attacker. This includes data such as passengers: social security number, date of birth, and names.

Business Impact:

This sort of security risk leaves RAKMS at risk of reputation damage and fines given the use of HTTP does not insure safety of passenger's information.

Recommended Remediation:

Finals-XX strongly recommends that the baggage check-in website only be hosted using HTTPS in the future and that the service be switched over immediately.

References

- CWE-311: Missing Encryption of Sensitive Data - https://cwe.mitre.org/data/definitions/311.html

H5: SMB Signing Disabled

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	Medium	Score	4.7		
Vector	AV:A/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N				
Risk Matrix					
Risk Level	High	Impact	High	Probability	High

Affected Systems			
IP Address	Port	Service	Version
10.0.0.6, 10.0.0.201-203	445/tcp	smb	Microsoft Windows Active Directory LDAP

Overview:

[redacted] were able to discover multiple hosts with SMB signing disabled. The lack of SMB signing can lead into further attacks, such as man in the middle attacks against your SMB server.

Business Impact:

The discovery of the lack of SMB signing poses a high risk to the network's confidentiality. An attacker exploiting this vulnerability can not only disrupt operations, but also log onto and access sensitive server information, further compromising the integrity of company data.

Attack Replication:

- crackmapexec smb 10.0.0.5-6
- crackmapexec smb 10.0.0.201-203

Attack Remediation

- Finals-XX highly recommend that RAKMS enables signing on all computers with port 445 open and furthermore disable NTLM authentication following least privilege policy.

H6: Improper Certificates **HIGH**

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	High		Score	7.1	
Vector	AV:A/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N				
Risk Matrix					
Risk Level	High	Impact	High	Probability	High

Overview:

While we did notice an adoption of HTTPS since our last engagement on websites such as Employee DB and the Wifi Portal, we noticed some issues with the use of certificates including the use of self-signed certificates and an abuse of the subject alternative names. While the use of self-signed certificates with wide subject alternative names may save time, it introduces some potential security risks.

Business Impact:

Access to the private keys for a certificate can provide an attacker with the ability to modify and traffic from the server and clients or even impersonate the server entirely. This breaches the confidentiality and integrity of any service effected which would be many with the wide use of subject alternative names.

Attack Scenarios:

- An attacker could create their own self-signed certificate to impersonate the server
- An attacker could breach a server and obtain a certificate private key to use on the other subject alternative names

Recommended Remediation:

Finals-XX recommends that **RAKMS: avoid using self-signed certificates for any production environment systems, implement HSTS to protect from changed certificates, and to avoid subject alternative names shared across services and servers.**

H7: Lack of Multi-Factor Authentication **HIGH**

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	High		Score	7.6	
Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:X/RL:O/RC:X				
Risk Matrix					
Risk Level	High	Impact	Critical	Probability	Medium

Overview:

Finals-XX conducted a thorough asssesment of the AWS environment and observed a consistent lack of Multi-Factor Authentication (MFA). This is a fundamental security control that strengthens password security accross the board. Over the past five years, Multi-Factor Authentication (MFA) has progressively solidified its status as an industry-wide standard, emerging as a pivotal enhancement to operational security protocols

Business Impact:

Industry standard have began to mandate implementation of MFA as security best practice. It is in RAKMS' best interest to adhere to compliance standards. Most importantly, a security breach due to the absence of MFA can be detrimental to organizational reputation. As MFA is becoming more wide-spread with everyday mobile applications, the lack of aforementioned features can result in a loss of customer trust.

Recommended Remediation:

Implement a double factor authentication by software or hardware to increase the protection level of the resources authentication.

Medium Risk Findings

M1: Lack of Host Based Defenses MEDIUM

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	Medium		Score	N/A	
Vector	N/A				
Risk Matrix					
Risk Level	Moderate	Impact	High	Probability	High

Affected Systems			
IP Address	Port	Service	Version
10.0.0.5-6 10.0.0.201-203	3389	Windows Defender	N/A

Overview:

Finals-XX found that all windows hosts did not have Windows Defender real time protection on and were not equipped with antiviruses. This led the team to be able to

deploy post-exploitation tools and payloads without requiring stealth and evasion techniques.

Business Impact:

Without antivirus protection, RAKMS will be more susceptible to malware and viruses. As there are new trojans, viruses, ransomware, and worms coming out daily, having an antivirus is crucial to mitigating risks. New threats come out daily and one of the best ways to deter systems being compromised is having antivirus software. Additionally, the vulnerability is also noncompliant with PCI as user data is poorly processed and stored.

Attack Replication:

- Open up Windows Defender and see if Real Time Protection is On
- Can also run .\Seatbelt.exe -group=user

Recommended Remediation:

- We recommend RAKMS turn on Real-Time Protection to detect incoming threats. If there are conflicts with existing software, Finals-XX recommends utilizing antivirus software and setting up on all hosts.

M2: Improper Access Controls

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	Critical		Score		
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H				
Risk Matrix					
Risk Level	Moderate	Impact	High	Probability	Low

Affected Systems			
IP Address	Port	Service	Version
10.0.0.201-203	3389	RDP	Windows Server 2016

Overview:

As the team carried out the engagement, Finals-XX noticed some accounts had access to multiple workstations. mmagnolia and two service accounts, svc_ATC, and EDR_TEST had access to all three corporate workstations and the windows team was able to effectively use the same credentials to access all three computers. The same goes for the same service accounts with easily crackable hashes.

Business Impact:

The discovery of user accounts that have too many privileges poses a high risk to the network as a whole. An attacker could abuse one of these accounts to jump from one host to another. This lowers internal network security as one compromised account can easily lead to a compromised network. Compliance states that corporations should follow the principle least privilege.

Attack Replication:

- python3 ldapdomaindump.py Skyport01.corp.kkms.local:389
- Outputs html files concerning various domain information such as users, trusts, policies, computers, and groups.

Recommended Remediation:

Finals-XX recommends that test accounts be disabled after use, especially since the EDR_TEST account is primarily used to test EDR Deployment. For the service accounts, RAKMS needs to adhere to the principle of least privilege, granting only the specific permissions necessary for their intended functions.

END OF FINDING BLOCK

M3: Use of external email address for business MEDIUM

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	Medium		Score	5.0	
Vector	AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L				
Risk Matrix					
Risk Level	Moderate	Impact	High	Probability	Moderate

Affected Systems			
IP Address	Port	Service	Version
10.0.0.5	636/tcp	ssl/ldap	Microsoft Windows Active Directory LDAP

Overview:

We found many official corporate emails throughout the engagement that used outlook as the email service. This includes a user account with an external outlook email address was found through enumerating the Active Directory LDAP service on 10.0.0.5 as well as a list of outlook emails for employees in IT found on one of the SkyDesktop machines. This compromises existing security policies and management of corporate email accounts; by not being an RAKMS email account, RAKMS no longer has control over the security of the email in regards to password policy, spam protection, confidentiality, and transparency.

Business Impact:

Without access to control over the email account, it is greater at risk for abuse by attackers who manage to gain access, the service it is hosted on, as well attackers who wish to attack the owner of the email account through spam.

• If the owner of the email account chooses to use a weak password or an old password, RAKMS will not be able to check that password against its password policy and will leave the account at risk of being compromised by attackers.
• Any information sent to or from this email address may no longer meet confidentiality standards given that it is hosted on external servers not managed by RAKMS. This sort of breach of confidentiality may break data compliances in the aviation industry.
• Any information sent to or from this email address can not be checked by RAKMS for information that would break company policies.
• The use of an external email account means that any systems in place to prevent spam will not be maintained on this account since it is not managed by RAKMS

Recommended Remediation:

Finals-XX recommends that RAKMS implement a strict policy for Active Directory and business emails that only allows internally managed email accounts for official RAKMS business to mitigate the risk associated with this finding. Additionally, it is advised to check the email account that was being used to ensure that no breaches have already taken place and to be aware of what information may have been at risk.

Compliances & Regulations

TSA Cybersecurity Requirements for Airport and Aircraft Operators

This finding breaks a lot of the recommendations of TSA Cybersecurity Requirements for Airport and Aircraft Operators such as the TSA's requirements for "continuous monitoring and detection policies and procedures to defend against, detect, and respond to cybersecurity threats and anomalies that affect critical cyber system operation," as well as "capabilities to defend against malicious email, such as spam and phishing emails, to preclude or mitigate against adverse impacts to operations."

References

- Transportation Security Administration Security Directive 1580/82-2022-01
https://www.tsa.gov/sites/default/files/sd-1580-82-2022-01.pdf
- TSA issues new cybersecurity requirements for airport and aircraft operators
https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft

END OF FINDING BLOCK

M4: Kerberos Pre-authentication Disabled MEDIUM

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	Medium	Score	idk		
Vector	idk				
Risk Matrix					
Risk Level	Moderate	Impact	High	Probability	Low

Affected Systems			
IP Address	Port	Service	Version
10.0.0.5	88	Kerberos	n/a

Overview:

Disabling Kerberos pre-authentication for a user in the RAKMS environment exposes a security vulnerability. Without pre-authentication, attackers can exploit weaknesses in the Ticket Granting Ticket (TGT) generation process, allowing them to perform a krbtgt dump. This can lead to unauthorized access, compromise of sensitive information, and potential

lateral movement within the network. To mitigate this risk, RAKMS should enforce Kerberos pre-authentication for all users to enhance the overall security posture.

Business Impact:

The discovery of Kerberos pre-authentication being disabled in the RAKMS airport environment poses a critical security risk with high severity. An attacker exploiting this vulnerability could potentially disrupt airport operations, compromise sensitive passenger and flight data, and violate regulatory compliance standards.

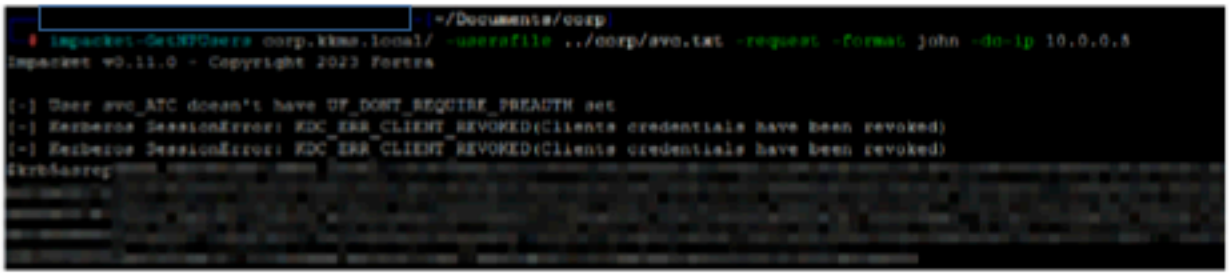
Potential Impact Scenarios:

1. Unauthorized access to critical systems may disrupt flight scheduling and airport services.
2. Compromise of passenger data could lead to privacy breaches and reputational damage.
3. Violation of compliance standards, such as TSA cybersecurity requirements, may result in legal liabilities.

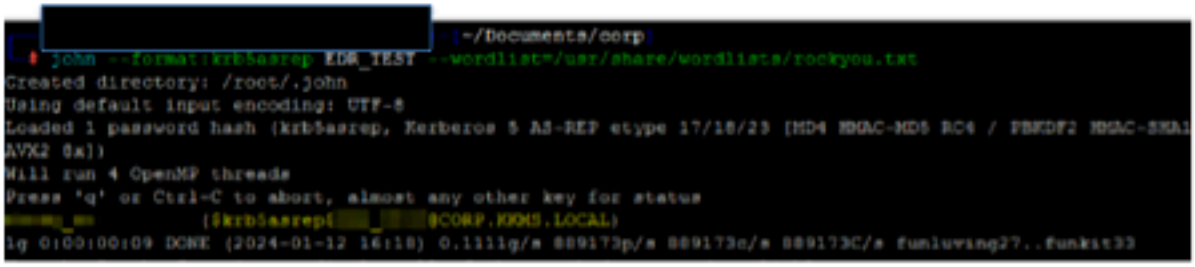
These risks could lead to significant consequences for RAKMS, including financial losses, legal repercussions, and damage to the airport's reputation. Immediate remediation is imperative to safeguard airport operations, protect passenger information, and ensure compliance with industry regulations. Management should prioritize addressing this vulnerability to mitigate potential business and operational impacts.

Attack Replication:

1. Sudo apt install impacket
2. impacket-GetNPUsers corp.kkms.local/ -usersfile <user .txt file> -request -format john -dc-ip 10.0.0.5



3. john --format:krb5asrep EDR_TEST --wordlist=/usr/share/wordlists/rockyou.txt



Recommended Remediation:

1. Enable Kerberos Pre-Authentication:
    - Reconfigure the Kerberos authentication settings to enforce pre-authentication for all users, preventing potential krbtgt dumps.
2. Implement Strong Authentication Methods:
    - Integrate multi-factor authentication (MFA) to enhance user authentication, adding an additional layer of security beyond passwords.
3. Regularly Monitor Kerberos Traffic:
    - Implement continuous monitoring of Kerberos traffic to detect and respond to any suspicious activities, providing proactive threat detection.
4. Review and Enforce Access Controls:
    - Review and strengthen access controls to restrict unauthorized access and limit lateral movement within the network.

References

Tenable

- https://www.tenable.com/blog/how-to-stop-the-kerberos-pre-authentication-attack-in-active-directory

END OF FINDING BLOCK

M5: Unauthorized Access to Baggage Check-in API MEDIUM

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	Medium		Score	4.3	
Vector	AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N				
Risk Matrix					
Risk Level	High	Impact	Medium	Probability	Medium

Affected Systems

IP Address	Port	Service	Version
10.0.0.33	80/tcp	http	unknown

Overview:

Finals-XX identified a vulnerability within the **Baggage Check-In Website at http:// baggagecheckin.corp.kkms.local**. The vulnerability involves **the register endpoint of the API**. Through testing for possible API endpoints in the same web directory as the ones used for check-in, we were able to find an API call that allowed us to add individuals to a flight within the baggage check-in service.

Business Impact:

An attacker exploiting this vulnerability could potentially effect the integrity of the passenger data for fligts and disrupt flight operations. This could cause reputational damage as well as financial damage as passengers could be added and cause disruptions if flights needed to be cancelled due to false passengers.

Recommended Remediation:

Finals-XX recommends that all API endpoints not necessary for unauthenticated use of any website be authenticated. The register option is not necessary for the public to check-in their baggage and should either be removed from the website or require authorization in the future.

Compliances & Regulations

TSA Cybersecurity Requirements for Airport and Aircraft Operators

- The TSA recommends in it's Cybersecurity Requirements for Airport and Aircraft Operators, that the aviation sector implement "access control measures to secure and prevent unauthorized access to critical cyber systems."

M6: LFI in Picture System of Baggage Check-in MEDIUM

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	Low		Score	3.8	
Vector	AV:A/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N				
Risk Matrix					
Risk Level	Low	Impact	Low	Probability	Medium

Affected Systems			
IP Address	Port	Service	Version
10.0.0.33	80/tcp	http	unknown

Overview:

Finals-XX discovered a local file inclusion vulnerability in the photo parameter of the register endpoint on the baggage check-in website. This vulnerability breaches the confidentiality of the baggage check-in filesystem and could be used to obtain information that would allow them to leverage access.

Attack Replication:

By setting the photo parameter of a register API call to a local filepath such as /var/log/auth.log or /etc/passwd, the results of the API call will return the contents of the local file encoded in base64.

Business Impact:

An attacker could theoretically obtain sensitive information off of the baggage check-in server using this vulnerability and possibly even use the local file inclusion vulnerability to find credentials that would give them more access. This would not only damage reputation, but could result in fines for not securing passengers information.

Recommended Remediation:

Finals-XX recommends that the code for the baggage check-in system be rewritten to avoid local file inclusion especially of system files.p

Low Risk Findings

L1: Reflected XSS in Employee DB LOW

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	Low	Score	3.2		
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H				
Risk Matrix					
Risk Level	Low	Impact	Low	Probability	Moderate

Affected Systems			
IP Address	Port	Service	Version
10.0.0.43	443/tcp	http	nginx

Overview:

Finals-XX identified a cross-site scripting vulnerability within the **Employee DB website**. Improper sanitization of employee names can result in an attacker gaining script execution in the context of the website and exfiltrating information such as user sessions.

Business Impact:

This vulnerability places a low risk given that the Employee DB does not look used currently, but could result in an attack in the future that could cause a loss of integrity in employee timesheets hosted on the employee database if an attacker were to gain access to an admins session through this vulnerability

Attack Replication:

- An attacker could send a specially crafted link designed to check the timesheet of an employee with the a name included script tags and javascript and send that link to an admin. One example of a script to include would be to set the location of the browser to an attacker controlled website alongside a GET parameter of the admin's browser cookies.

Recommended Remediation:

Finals-XX recommends RAKMS implement sanitization on the names shown in the employee database. Furthermore, Finals-XX recommends RAKMS implement common cross-site scripting preventions such as Content-Security Policy headers and HTTP cookies.

References

- Cross Site Scripting (XSS) - https://owasp.org/www-community/attacks/xss/

END OF FINDING BLOCK

L2: Internal Information Disclosure using Hidden NTLM Authentication INFORMATIONAL

Affected Systems			
IP Address	Port	Service	Version
10.0.0.6	25/tcp	smtp	N/A

Overview:

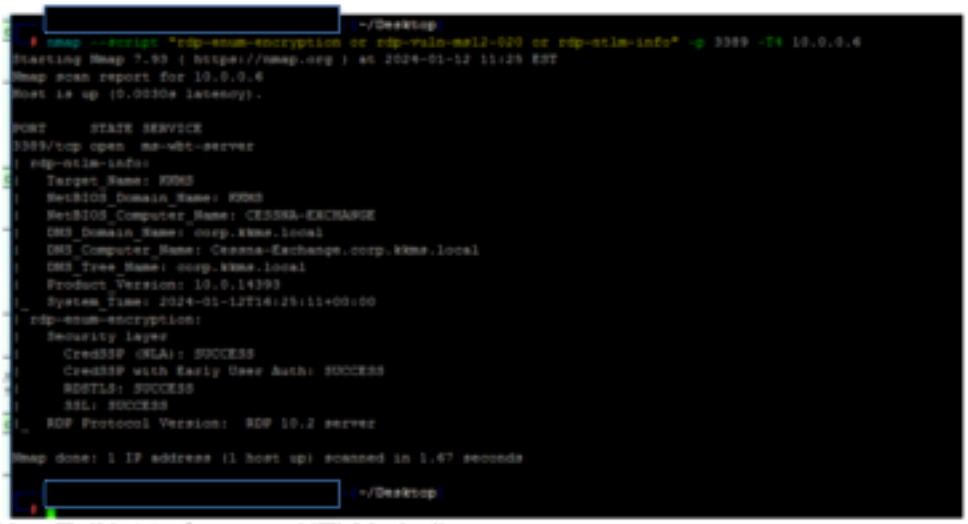
- **Finals-XX was able to enumerate sensitive systems information that allowed the team to understand the basic information of the domain. This resulted in Finals-XX being able to perform initial reconnaissance on the host and its connected systems**

Business Impact:

As system information is easily accessible, an attacker would be able to perform basic reconnaisance and further understand the network easily. A hacker, with domain name information, can leverage this information to further understand the company's infrastructure or even attempt to send out phishing emails.

Attack Replication:

Run built-in nmap scripts to query information



Use TelNet to force an NTLM challenge response

Recommended Remediation:

Aa

- Finals-XX recommends that Robert A. Kalka Metropolitan Skyport disables NTLM authentication over HTTP through the IIS Manager.

L3: Poor Password Policy nevermind INFORMATIONAL

Affected Systems			
IP Address	Port	Service	Version
10.0.0.6	25/tcp	smtp	N/A

Overview:

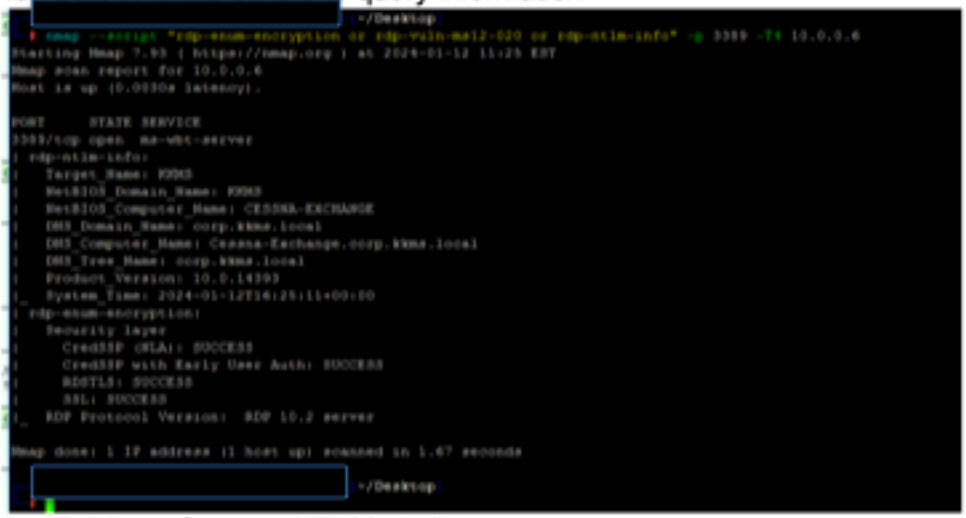
- **Finals-XX noticed password policies on the Domain Controller were not completely up to PCI-DSS standards**

Business Impact:

Team-XX recommends that RAKMS adjust their password policies on the domain controller to meet industry standards. The password policy is partly up to standard. The minimum of seven characters, enforced complexity, max password age, and password history information is up to PCI DSS standard. However, to fully comply with all regulations, the following underlined below must be properly adjusted.

Attack Replication:

- Run built-in nmap scripts to query information



- Use TelNet to force an NTLM challenge response

Recommended Remediation:

- Finals-XX recommends that Robert A. Kalka Metropolitan Skyport disables NTLM authentication over HTTP through the IIS Manager.

END OF FINDING BLOCK

L4: Exposed UUID **INFORMATIONAL**

Affected Systems			
IP Address	Port	Service	Version
10.0.0.6	135/tcp	msrpc	N/A

Overview:

Finals-XX identified a msrpc vulnerability within the Corp subnet. The vulnerability involves the exposure of two UUIDs through the "rpc auditor" tool, allowing unauthorized access to specific RPC interfaces without the need for authentication. This exposes critical functionalities associated with the IID_IObjectExporter and RPC interface for IObjectExporter.

This violates security best practices and the principle of least privilege, as unauthorized access is granted without proper authentication. Access controls and confidentiality principles are violated, as sensitive interfaces are exposed without proper authentication.

Finals-XX successfully accessed the airport RAKMS using the "rpc auditor" tool, leading to the following consequences: This unauthorized access allows for the enumeration of information associated with the IID_IObjectExporter and RPC interface for IObjectExporter. The compromise involves potential disclosure, manipulation, or exploitation of sensitive data within the RAKMS.

The risk assessment is informational [could change!!!!!]

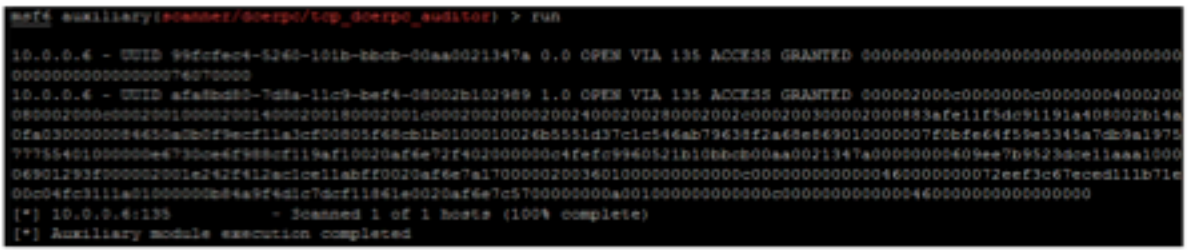
This attack carries the potential to compromise sensitive information within the RAKMS, potentially leading to reconnaissance for further sophisticated attacks. [LEVEL] remediation is advised to mitigate the identified vulnerabilities and enhance the overall security posture of the airport RAKMS.

Business Impact:

Finals-XX recommends that **[Affected Company/Organization]** implement **[specific action]** to mitigate the risk associated with **[identified finding]**. This includes **[details on recommended actions – e.g., implementing strong authentication methods, changing weak credentials, enforcing strong password policies, etc.]**. Additionally, it is advised to **[further actions, e.g., implementing access control mechanisms, enforcing encryption protocols, etc.]** to enhance the overall security posture.

Attack Replication:

1. Msfconsole
2. Use scanner/dcerpc/tcp_dcerpc_auditor
3. Set RHOSTS 10.0.0.6
4. run



Recommended Remediation:

Aa

- Target Audience: Engineers / Technical
- Describe how the company's IT operations team can solve the problem.
- Details are fine, but try to be brief.

References

Table of Well-known GUIDs in the DCOM Remote Protocol

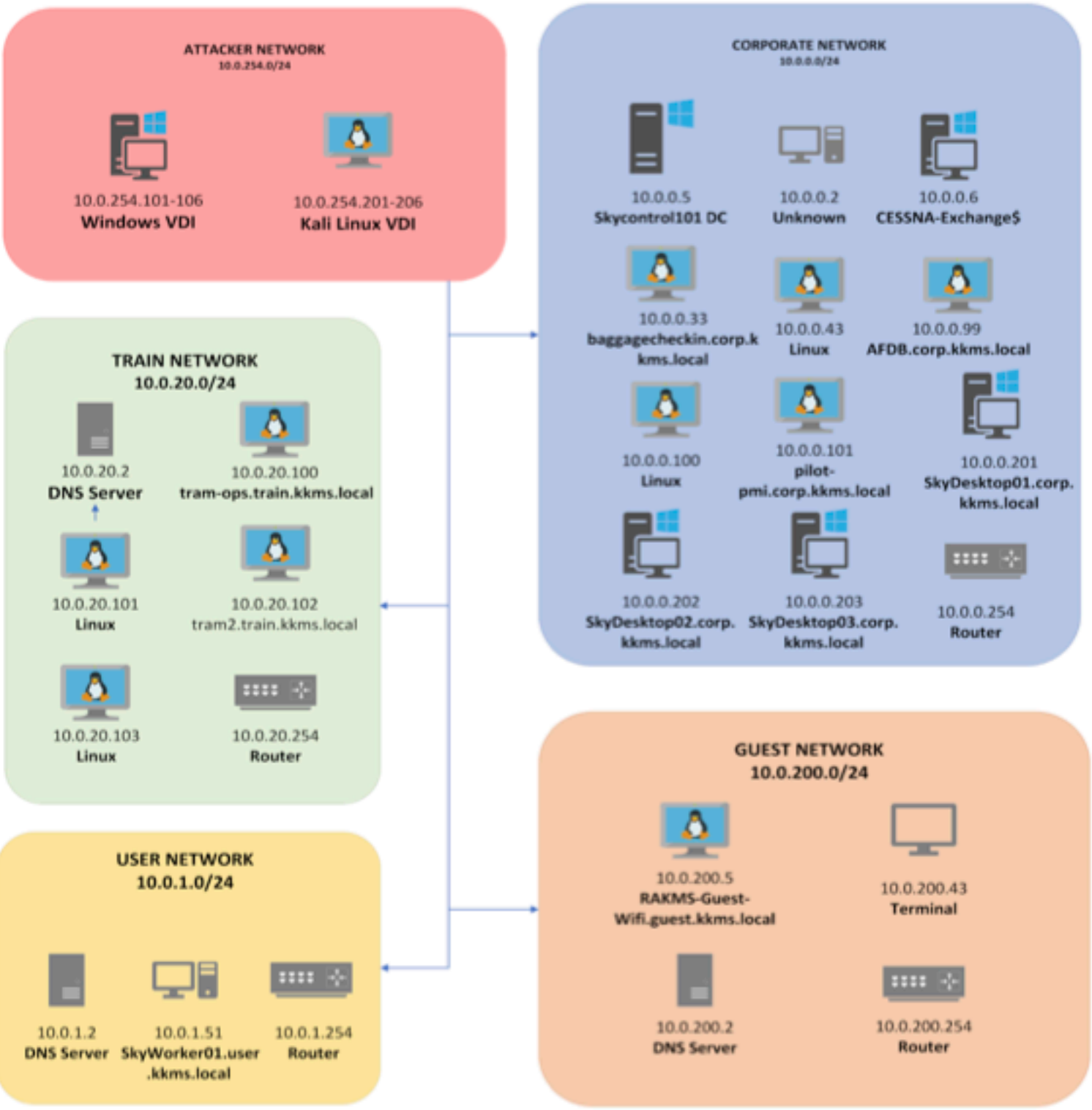
- https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-dcom/c25391af-f59e-40da-885e-cc84076673e4

- https://www.blackhat.com/presentations/win-usa-04/bh-win-04-seki-up2.pdf

Appendix

APPENDIX A: Network Topology Diagram

To maintain an updated list of the targets in scope, Finals-XX made a topology on the RAKMS network. The topology relies on the Nmap scans for precision. During the reconnaissance phase, Finals-XX discovered various systems and interfaces in the company's four subnets. There were multiple databases, admin control panels, and servers in the corporate network. There were several Windows workstations in the guest subnet. The corporate network also contained 3 systems that primarily hosted public-facing information.


ATTACKER NETWORK
10.0.254.0/24
10.0.254.101-106
Windows VDI
10.0.254.201-206
Kali Linux VDI
CORPORATE NETWORK
10.0.0.0/24
10.0.0.5
Skycontrol101 DC
10.0.0.2
Unknown
10.0.0.6
CESSNA-Exchange$
10.0.0.33
baggagecheckin.corp.kkms.local
10.0.0.43
Linux
10.0.0.99
AFDB.corp.kkms.local
10.0.0.100
Linux
10.0.0.101
pilot-pmi.corp.kkms.local
10.0.0.201
SkyDesktop01.corp.kkms.local
10.0.0.202
SkyDesktop02.corp.kkms.local
10.0.0.203
SkyDesktop03.corp.kkms.local
10.0.0.254
Router
TRAIN NETWORK
10.0.20.0/24
10.0.20.2
DNS Server
10.0.20.100
tram-ops.train.kkms.local
10.0.20.101
Linux
10.0.20.102
tram2.train.kkms.local
10.0.20.103
Linux
10.0.20.254
Router
USER NETWORK
10.0.1.0/24
10.0.1.2
DNS Server
10.0.1.51
SkyWorker01.user.kkms.local
10.0.1.254
Router
GUEST NETWORK
10.0.200.0/24
10.0.200.5
RAKMS-Guest-Wifi.guest.kkms.local
10.0.200.43
Terminal
10.0.200.2
DNS Server
10.0.200.254
Router

APPENDIX B: Network Diagram

The following figures show the hosts, services, and ports discovered in the RAKMS internal network during the assessment:

Corporate Network: 10.0.0.0/24

10.0.0.2
53 - tcpwrapped

10.0.0.5
80 - http 81 - http 445 – microsoft-ds 3389 - ms-wbt-server 5060 - 6001 -

10.0.0.6		
25 - smtp 80 - http 81 - http 110 – pop3 135 – msrpc 139 – netbios-ssn 143 – imap 443 – http 444 - http	445 – microsoft-ds 465 – smtp 587 – smtp 593 – ncacn_http 808 – ccproxy-http 993 – imap 995 – pop3 2525 - smtp 3389 – ms-wbt-server	3800 – http 3801 – mc-nmf 3828 – mc-nmf 5060 – sip 6001 – ncacn_http 6566 – msrpc 6567 - msrpc

10.0.0.33
1000 ports replied with: no-response

10.0.0.34
1000 ports replied with: no-response

10.0.0.43
1000 ports replied with: no-response

10.0.0.99
1000 ports replied with: no-response

10.0.0.100
1000 ports replied with: no-response

10.0.0.101
1000 ports replied with: no-response

10.0.0.201
1000 ports replied with: no-response

10.0.0.202
1000 ports replied with: no-response

10.0.0.203
1000 ports replied with: no-response

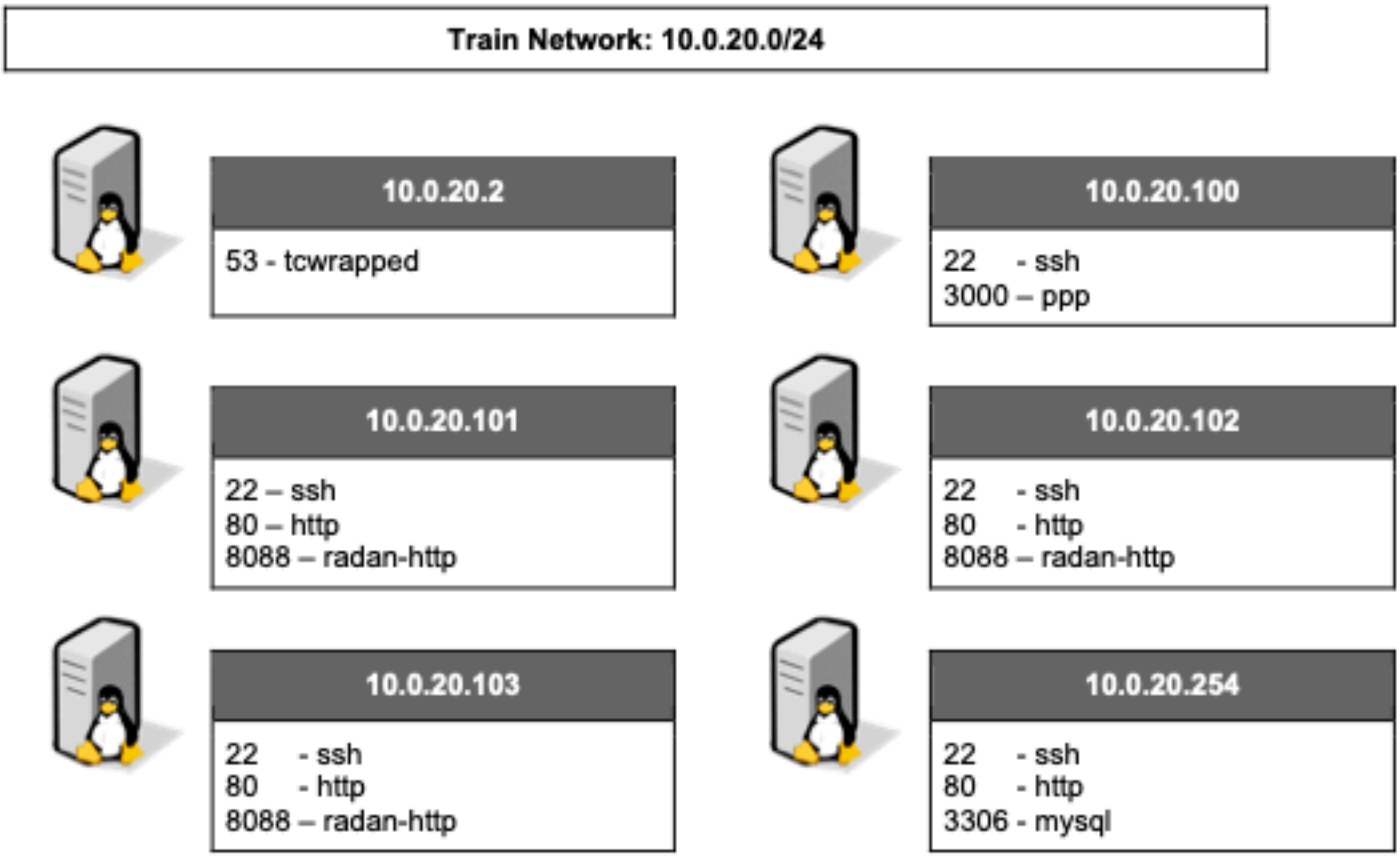
10.0.0.254
1000 ports replied with: no-response

User Network: 10.0.1.0/24

10.0.1.2
53 - tcpwrapped

10.0.1.51
1000 ports replied with: no-response

10.0.1.254
1000 ports replied with: no-response



APPENDIX C: Severity and Risk Level Definitions

Within the report, two main measures are used to evaluate the urgency of a vulnerability. The primary measure used is the severity level, which is scored using the Common

Vulnerability Scoring System v3.1 (CVSS). The secondary measure used is the risk level, using a risk matrix scoring system.

Though similar, it is important to note that severity and risk are not equivalent. Risk level measures are affected by the likelihood of a vulnerability more than severity levels are. This may lead to negligence of critical severity vulnerabilities of low likelihood. As part of the region's critical infrastructure, the range of potential threat actors anticipated by RAKMS is not limited to unsophisticated, low-level criminals but includes sophisticated, high-caliber, and well-funded threats. Such a threat actor is not limited by low likelihood, as they will search extensively for any vulnerabilities that may compromise the company's systems. Thus, RAKMS can not afford to ignore any high-impact vulnerability merely because of its lower likelihood.

For this reason, Finals-XX has decided to use severity levels as the primary measure to mitigate this issue. Severity levels still take likelihood into consideration in the form of "exploitability", but with reduced effects. However, risk levels are still provided in the report regardless, to give risk analysts and management an alternative measure for evaluating a vulnerability.

Severity Level Measures: To measure severity, the CVSS v3.1 standard is used. The Common Vulnerability Scoring System is an open industry standard for assessing the severity of a computer system security vulnerability. The basic score is used as a simple quantitative measure in collaboration with the score-to-rating chart in Fig 2.2A to provide a qualitative measure of the severity. The base vector string is also shown to give a better technical description of the vulnerability. The breakdown of the vector string is shown in Fig 2.2B.

A.) CVSS v3.1 Score-Rating Table

Severity Rating	Base Score
Critical	9.0-10.0
High	7.0-8.9
Medium	4.0-6.9
Low	0.1-3.9
Informational	0

B.) CVSS v3.1 Base Vector String Breakdown

Exploitability	**Scope (S)**
Attack Vector (AV)	Unchanged (**U**), Changed (**C**)
Network (**N**), Adjacent (**A**), Local (**L**)	**Impact**
Attack Complexity (AC)	Confidentiality (C)
Low (**L**), High (**H**)	None (**N**), Low (**L**), High (**H**)
Privileged Required (PR)	Integrity (I)
None (**N**), Low (**L**), High (**H**)	None (**N**), Low (**L**), High (**H**)
User Interaction (UI)	Availability (A)
None (**N**), Required (**R**)	None (**N**), Low (**L**), High (**H**)

Fig 2.2. A legend for the usage of CVSS 3.1 metrics. (A) shows the qualitative severity ratings w/ the corresponding color depending on base score. (B) shows the breakdown of the CVSS Base

Vector String. The vector string will compose of the field abbreviation (AV for Attack Vector) followed by a colon and the attribute abbreviated (N for Network). Each field is separated by forward slashes.

Risk Level Measures:
Alternatively, to measure risk levels, a simplistic risk matrix is used as defined in Fig 2.3A. The risk matrix will take into account the impact of the vulnerability along with the probability that it will occur. A base impact score is obtained using the impact subscore provided by the CVSS calculator, along with a base probability using the CVSS exploitability subscore. The two scores are then adjusted by Finals-XX's security engineers using their own technical knowledge and by taking the specific context into consideration. The risk score is then obtained by mapping the adjusted impact score and probability to a risk rating using the Probability v Impact Risk Matrix in Fig 2.3A. Finally, all quantitative scores are converted to qualitative ratings using a score-to- rating scale as described in Fig 2.3B.

A.) Probability v Impact, Risk Matrix

Probability	Risk Level				
Very High	Medium	Medium	High	Critical	Critical
High	Low	Medium	High	High	Critical
Medium	Low	Low	Medium	High	High
Low	Informational	Low	Medium	Medium	High
Informational	Informational	Informational	Low	Medium	Medium
Impact	Informational	Low	Medium	High	Very High

B.) Score-to-Rating Chart

Rating	Probability	Impact
Critical	0.9 - 1.00	0.90 - 1.00
High	0.7 - 0.89	0.75 - 0.89
Medium	0.5 - 0.69	0.60 - 0.74
Low	0.3 - 0.49	0.25 - 0.59

Fig 2.3. A legend for the scoring of risk level, probability, and impact. (A) shows the risk matrix for obtaining the qualitative risk level using the qualitative measures of probability and impact. (B) shows the corresponding rating which describes each range of probability, impact, and risk.

Informational	0.0 - 0.29	0.00 - 0.24

It is important to note that the aforementioned scoring process is done throughout the report using the technical knowledge and professional experience of Finals-XX's security engineers. These scores do not reflect the official values found in the National Vulnerability Database (NVD) and should not be treated as such.

APPENDIX D: TSA Cybersecurity Requirements for Airport and Aircraft Operators

Note: The TSA announcement for this cybersecurity amendment does not provide a documented security directive specifically for airports and airport carriers but references SD-1580/82-22-01, cybersecurity measures issued to passenger and freight railroad carriers.

Finals-XX's evaluation considered only those standards subject to enforcement as of November 11, 2023, and those that could be assessed within the stipulated timeframe and the limited digital access provided.

Title	Reference
TSA Cybersecurity Requirements for Airport and Aircraft Operators	***https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft***
SD-1580/82-22-01	***https://www.tsa.gov/sites/default/files/sd-1580-82-2022-01.pdf***

	TSA Cybersecurity Requirements	
References	**Section**	**Required Security Actions and Measures**
TSA Cybersecurity Requirements for Airport and Aircraft Operators	**1**	Develop network segmentation policies and controls to ensure that operational technology systems can continue to safely operate in the event that an information technology system has been compromised and vice versa
TSA Cybersecurity Requirements for Airport and Aircraft Operators	**2**	Create and access control measures to secure and prevent unauthorized access to critical cyber systems;

SD-1580/82-22-01	**III.C.1.a**	Policy for memorized secret authenticator resets that includes criteria for when resets must occur
SD-1580/82-22-01	**III.C.2**	Multi-factor authentication or other logical and physical security controls that supplement password authentication. If not applied, the owner/operator must specify what compensating controls are used
TSA Cybersecurity Requirements for Airport and Aircraft Operators	**3**	Implement continuous monitoring and detection policies and procedures to defend against, detect, and respond to cybersecurity threats and anomalies that affect critical cyber system operations; and
TSA Cybersecurity Requirements for Airport and Aircraft Operators	**4**	Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers, and firmware on critical cyber systems in a timely manner using a risk-based methodology

APPENDIX E: General Data Protection Regulation

For more information on GDPR standards, please refer to the official GDPR website (https://eur-lex.europa.eu/eli/reg/2016/679/oj). It's important to note that while Finals-XX's analysis covered GDPR standards enforceable as of November 11, 2023, RAKMS should remain attentive to future enforcement requirements not covered in the assessment.

The references for the specific GDPR sections considered by Finals-XX during the analysis are as follows:

Title	Reference
GDPR	***https://gdpr-info.eu/***

Relevant GDPR Articles	
Article #	**Requirements**

12	5. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. 2The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. 6. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.
15	3. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: (i) the purposes of the processing; (j) the categories of personal data concerned; (k) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations; (l) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (m) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; (n) the right to lodge a complaint with a supervisory authority; (o) where the personal data are not collected from the data subject, any available information as to their source; (p) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. 4. Where personal data are transferred to a third country or to an international organization, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.
17	2. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

	(g) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (h) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (i) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (j) the personal data have been unlawfully processed; (k) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (l) The personal data have been collected in relation to the offer of information society services referred to in Article 8(1).
24	4. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary. 5. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller. 6. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.
32	2. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (e) the pseudonymisation and encryption of personal data; (f) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (g) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (h) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
34	1. When the personal data breach is likely to result in a high risk to the rights

	and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
40	1. The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. 2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to: 3. In addition to adherence by controllers or processors subject to this Regulation, codes of conduct approved pursuant to paragraph 5 of this Article and having general validity pursuant to paragraph 9 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organizations under the terms referred to in point (e) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.
78	1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them. 2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.
79	1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.
82	2. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.
83	1. Each supervisory authority shall ensure that the imposition of

	administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

APPENDIX F: Payment Card Industry Data Security Standard

PCI DSS constitutes a set of obligatory standards that apply to all entities that store, process, or transmit cardholder data. Non-compliance with these standards can result in substantial financial penalties enforced by regulatory authorities.

Finals-XX's evaluation considered only those standards subject to enforcement as of November 11, 2023, and those that could be assessed within the stipulated timeframe and the limited digital access provided. Finals-XX strongly advises RAKMS also to contemplate standards slated for future enforcement, even though they were not included in Finals-XX's analysis. References for each section of the standard used by Finals-XX are provided below

Title	Reference
PCI DSS	***https://listings.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf***

Relevant PCI-DSS Sections	
Req #	**Requirements**
1.1.7	Install and maintain a firewall configuration to protect cardholder data. Install a firewall at each internet connection(every device). Configure your firewalls with a description of groups responsible for network components and business justifications for all services/protocols/ports in the configuration. Review firewall and router configuration at least every 6 months and confirm all other, non-config traffic (inbound or outbound) is denied.Assign responsibility for someone to check firewall logs daily
2.1	Do not use vendor-supplied defaults for system passwords and other security parameters. Identify a sysadmin to be responsible for system components. Document policies to change vendor-supplied default passwords, default wireless settings and remove default accounts before installing a system on your network. Maintain an inventory list of all system components in scope for PCI DSS.
3.1	Protect stored cardholder data. Make sure the stored data and data in transit are unreadable. Use a data discovery tool to find misplaced sensitive data in your environment

4.1	Encrypt transmission of cardholder data across open public networks. Identify where you send cardholder data and ensure your policies are not violated in the journey and only trusted keys or certificates are used.
5.1.1	Protect all systems against malware and regularly update antivirus software or programs. Regularly update anti-virus software on your commonly affected systems and evaluate whether additional systems are at risk of needing an antivirus. Automate anti-virus scans and maintain antivirus audit logs for your systems. Document procedures for protecting against malware
6.2	Develop and maintain secure systems and applications. Establish a process to keep up-to-date with the latest security vulnerabilities and identify the risk level. Use strict development processes and secure coding guidelines (outlined in DSS) when developing software in-house
7.2	Restrict access to cardholder data by business need to know. Create a list of roles with access to the CDE that includes the definition of each role, their privilege level, and what permissions are required for each role to function. Create a least-privilege policy for all employees and a default "deny-all" setting on all access control settings
8.2	Identify and authenticate access to system components. Define and document procedures for user identification and authentication on all system components. Assign unique IDs to all users, test those privilege controls, and revoke access on inactive/terminated users. Follow best practice guidelines outlined in DSS for password setting – including strong password composition, encrypting credentials, verifying ID before reset, and mandatory resets every 90 days.
9.1.1	Restrict physical access to cardholder data. Document process for physical access to CDE systems and a list of all devices, limiting access to roles that require it and monitoring all with authorization tokens and surveillance.
10.8	Track and monitor all access to network resources and cardholder data. Track all admin actions, login attempts, account changes, and pauses in the audit trail. Ensure each audit log captures user ID, event type, date and time, event success or failure, where the event originated from, and what resources are affected.
11.1	Regularly test security system and process
12.1	Maintain a policy that address information security for all personal

APPENDIX G: Offensive Tools

Tool	Resource
Nmap	https://nmap.org/download.html
Burp Suite	https://portswigger.net/burp
Metasploit	https://www.metasploit.com/
Wfuzz	https://github.com/xmendez/wfuzz

CrackMapExec	https://github.com/byt3bl33d3r/CrackMapExec
Hydra	https://github.com/vanhauser-thc/thc-hydra
Seclist	https://github.com/danielmiessler/SecLists
LinPEAS	https://github.com/carlospolop/PEASS-ng
Netcat:	https://nmap.org/ncat/
Impacket	https://github.com/SecureAuthCorp/impacket