FINALS-XX

Robert A. Kalka

Metropolitan Skyport

Cyber Risk Assessment: Executive Overview

CONFIDENTIAL - DO NOT DISTRIBUTE

Agenda

01. Introduction

02. Engagement Overview

03. Methodology

04. Findings

05. Compliance

06. Recommendations

07. Conclusion

08. Questions & Concerns

Engagement Overview: Objectives

Security

Identify vulnerabilities, assess adherence to security best practices, and evaluate the overall security posture.

Awareness

Assess whether employees follow security practices to prevent social engineering attacks

Compliance

Validate adherence to industry standards and regulatory frameworks, such as PCI-DSS and GDPR.

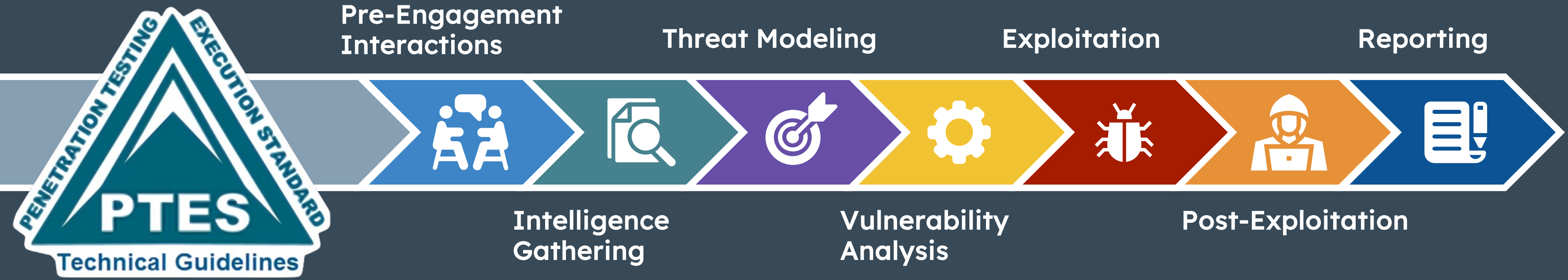
Engagement Overview: Scope

This slide displays some notable hosts found on each network

Corporate Network 10.0.0.0/24	User Network 10.0.200.0/24	Train Network 10.0.20.0/24	Guest Network 10.0.1.0/24
Sky Control Server	SkyWorker01.user.kkms.local	Train Servers	Guest Wifi
Baggage Claim System		Trams	
Employee Time Server			
Cessna-Exchange Server			
Employee DB			
Flight Monitor			
skydesktops			

Methodology: Penetration Testing Framework

Our methodology aligns with PTES, a widely recognized framework, ensuring a systematic and industry-compliant approach to comprehensive cyber risk assessments.



Pre-Engagement Interactions

Intelligence Gathering

Threat Modeling

Vulnerability Analysis

Exploitation

Post-Exploitation

Reporting

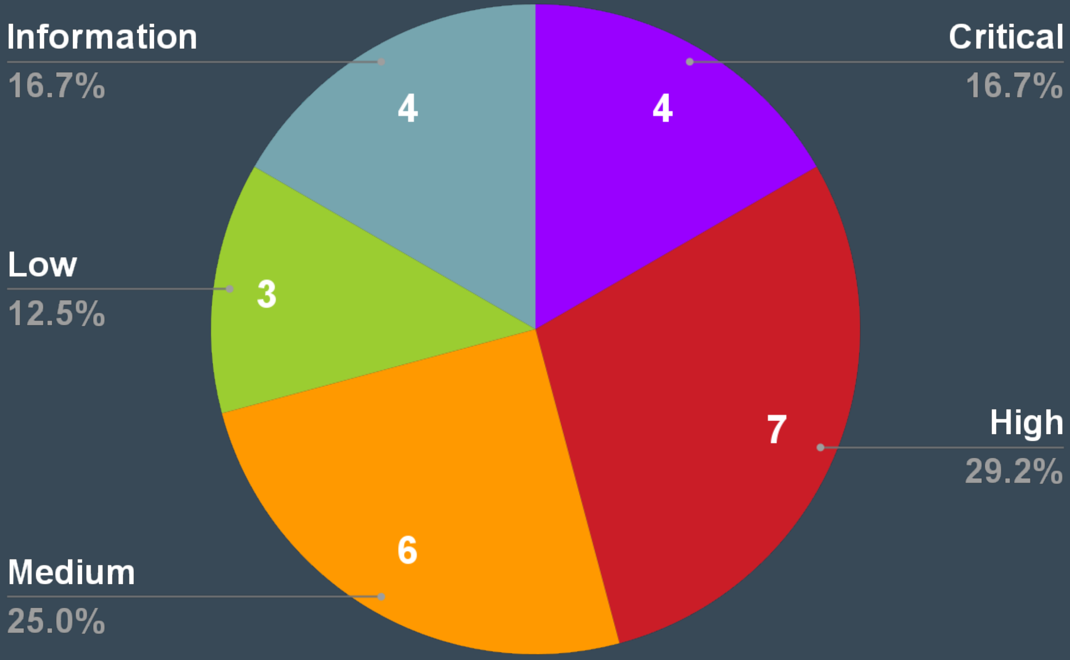
Methodology: Risk Metrics

Impact

Likelihood	Informational	Low	Medium	High	Critical
Critical	Medium	Medium	High	Critical	Critical
High	Low	Medium	High	High	Critical
Medium	Low	Low	Medium	High	High
Informational	Informational	Low	Medium	Medium	High
Informational	Informational	Informational	Low	Medium	Medium

Finals-XX employs a customized framework that considers vulnerability impacts, likelihood, and overall criticalities, complemented by the **Common Vulnerability Scoring System 3.1.** This approach provides comprehensive insights into both technical and business risks for the organization.

Findings: Vulnerabilities Breakdown



Findings: Key Findings

Social Engineering

Successful social engineering, obtaining employee credentials

Lack of Multi Factor Authentication (MFA)

Can lead to higher risk of unauthorized access

Insecure Passenger and Tram Data

Passenger and tram data were exposed and modifiable

Findings: Impact

Critical Infrastructure

Safety

Compliance

Compliance: Standards & Regulations & Violations

SA Cybersecurity Requirements for Airport and Aircraft Operators

III.F - reducing risk by using up to date software
III.C - implement access controls
<u>fine:</u> fees, legal actions

General Data Protection Regulation

32 – encrypting data, ensuring confidentiality integrity and availability of data
<u>Fine:</u> up to $10,000,000

Payment Card Industry Data Security Standard

2.1 - use of default passwords
5.1.1 - use anti-virus software
<u>Fine</u>: $5,000 to $100,000 per month

Recommendations: Key Strengths

Hashes

Great use of strong hashing algorithms

Lockout Policys

Robust defense against password brute force attacks

Strong Access Controls in AWS

Use of principle of least priviledge Role Based access controls

Fast response team

RAKMS staff responded promptly and were quick to detect system changes.

Recommendations: Overview

Employee Awareness Training

Train employees on how to avoid social engineering attacks

Stronger Authentication Measures

Adding an extra layer of authentication for enhanced security.

Routine updates and patches

Perform regular updates to make sure services are up to date

Conclusion

- **Employee awareness training**
- Use of Multi Factor Authentication
- **RAKMS excellent response team**

Questions & Concerns