Team XX

Penetration Test Executive Briefing

1/15/2022

Our Team

Presentation Overview

01
Method & Scope

02
Findings

03
Remediations

04
Conclusion & Questions

Scope

Corporate Network

10.0.0.0/24

- Hotel reservations
- Rewards system
- Employee workstations

Guest Network

10.0.200.0/24

- Guest kiosks

Assessing Risk (CRS)

Severity

Inherent magnitude of the vulnerability

Ease of Exploitation

Expertise required to exploit vulnerability

Effort to Fix

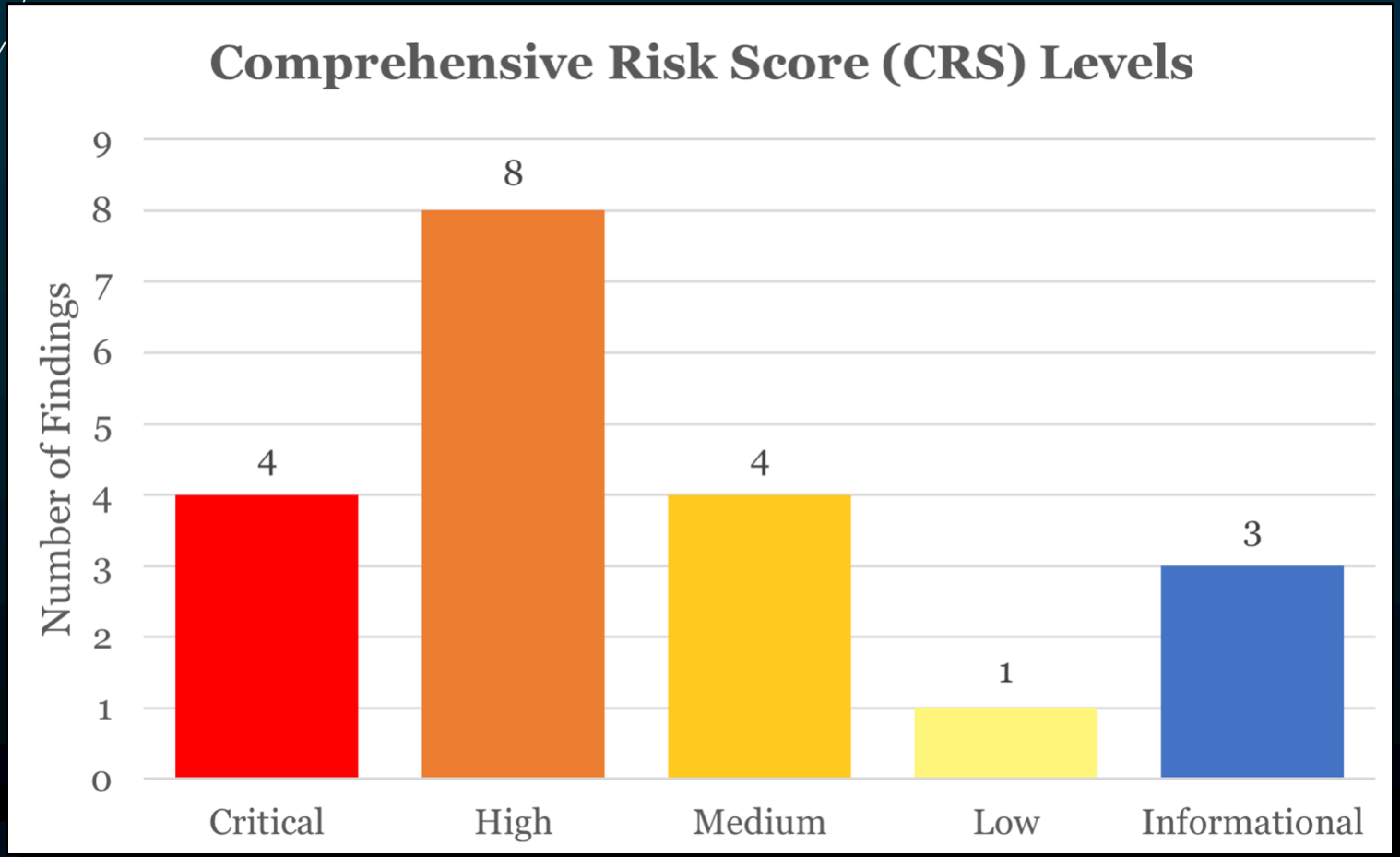
Time, effort, and resources required to remediate

Degree of Exposure

Degree vulnerability is exposed in the infrastructure

Business Impact

Impact to business, reputation, and compliance


Comprehensive Risk Score (CRS) Levels
Number of Findings
0
1
2
3
4
5
6
7
8
9
4
8
4
1
3
Critical
High
Medium
Low
Informational


40%
of previous findings remediated

Unencrypted Password Storage and Exposure

Vector:
Unencrypted employee and user passwords stored in directory service and other easily accessible locations

Impact:
Attackers can use easily guess password to directory service allowing access to passwords and sensitive PII for employees and guests

Weak Database Passwords

Vector:
Logins to databases used in business-critical applications

Impact:
Attacker can easily guess logins for databases, yielding access to sensitive customer PII including credit card numbers and CVVs, phone numbers, home addresses, and emails

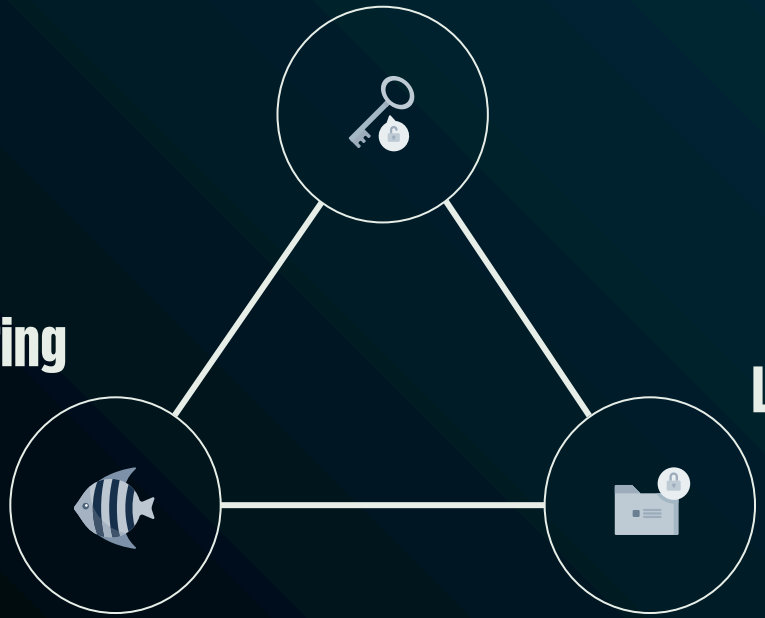
Kiosks Grant Trivial Access to Corporate Domain

Vector:
Given access to the kiosks on the guest network, attackers can escape out of the kiosk system and penetrate the corporate network

Impact:
Attacker can elevate access to disrupt confidentiality, integrity, and availability of internal corporate computing services

Key Remediations

Password Policies



Social Engineering Training

Principle of Least Privilege

Regulatory Compliance

PCI-DSS

Nevada Revised Statute 603a

Regulatory Compliance

PCI-DSS

Nevada Revised Statute 603a

Observed Strengths

1. Up-to-date Services
2. Lockout Policies
3. Network Segmentation
4. Activity Logging

Thank you!

Questions?

<insert-team-email>