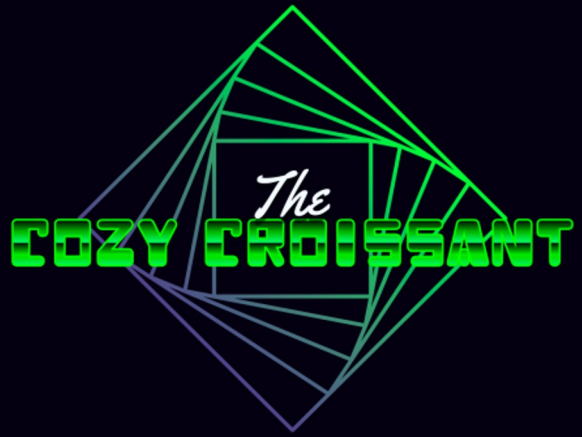


Penetration Testing Debrief

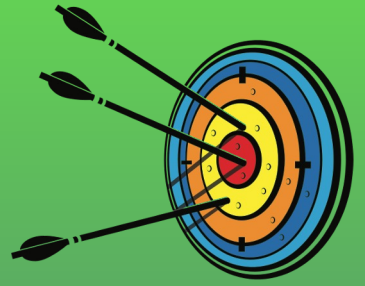
Key Findings

- Domain Controller Missing Critical Patches
- Lack of Authentication for Administrator on Kiosks
- Weak/Default Passwords
- Improper Barriers
- Vulnerable to Social Engineering

Severity of Impact

- Compromise of Sensitive Data
- Unauthorized Access to Company Resources
- Lateral Movement in the Network
- Reputational Damage to the Company
- Possibility of Legal Actions and Fines
- Loss of Customer Trust
- Possibility of Losing (Trust of) All Date

Overview

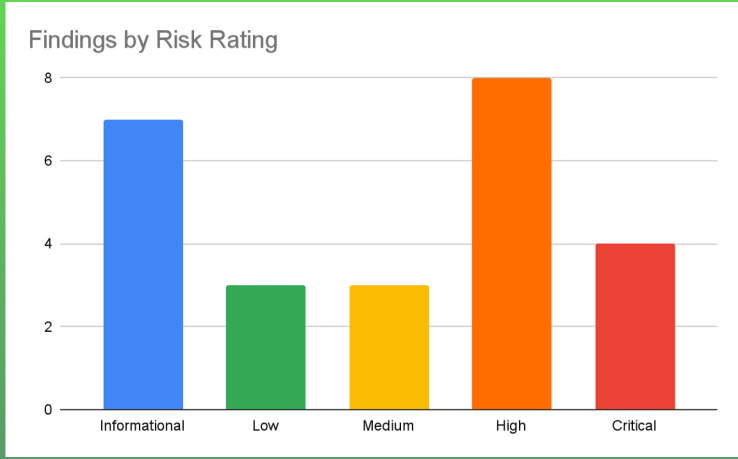


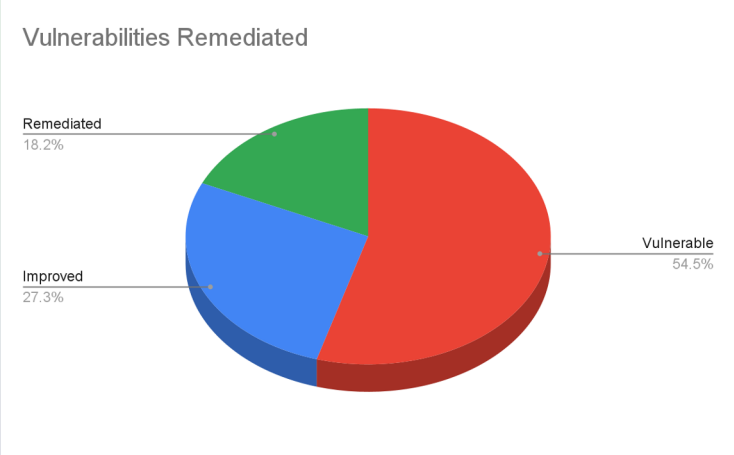
Goals of the Assessment:

1. Identify Potential Vulnerabilities
2. Check if Prior Findings have been Remediated
3. Assess Compliance
    a. Payment Card Industry Data Security Standard (PCI-DSS)
    b. General Data Protection Regulation (GDPR)
4. Improve Resiliency of Business, and Overall Infrastructure
5. Outline Key Remediation to Secure TCC’s Network

Metrics

- 18 Total vulnerabilities
  - 7 Informational
  - 3 Low
  - 3 Medium
  - 8 High
  - 4 Critical
- 18% Remediated






GDPR

GDPR Compliance

Noncompliance:

- 2. Limitation of Purpose, Data and Storage
- 5. Personal Data Breaches
- 10. Awareness and Training


PCI-DSS
COMPLIANCE

PCI-DSS Compliance

Noncompliance:

- 2. Do Not Use Defaults for System Passwords
- 3. Protected Stored Cardholder Data
- 7. Limit Access to Cardholder Data According to Specified Requirements

Recommendations

- Implement Strong Password Policy / Multi-Factor Authentication
- Implement Password Hashing / Encryption
- Proper Storage of Personal Identifiable Information (PII)
- Disable/Restrict WinRM on Kiosks
- Install Updates and Regularly Patch Systems
- Test/Validation Security Measures
- Regular Pen-Testing & Continuous Monitoring