****

CLIENT-NAME  
(CLIENT-ABV)   
Penetration Test Report

Prepared by:

TEAM-IDENTIFIER

DAY MONTH, YEAR

A red rectangle with black background

Description automatically generated

# Document Information

## Confidentiality

This document and all the information contained within are confidential and proprietary to TEAM-IDENTIFIER and CLIENT-NAME. The utmost care should be exercised when handling, referring to, or copying this document. TEAM-IDENTIFIER authorizes CLIENT-NAME to view and communicate this document as they see fit in accordance with CLIENT-NAME’s data handling policies.

## Legal Disclaimer

No warranties are provided by TEAM-IDENTIFIER for this penetration test report with respect to the accuracy, reliability, or correctness of the information in this document. This report is delivered “as is” with findings and recommendations reflecting only the information obtained during the assessment. TEAM-IDENTIFIER does not assume liability from any damages, indirectly or directly, related to the reliance of information provided in this report, and it is highly recommended to thoroughly evaluate the business impact of changes before the implementation of them.

## Contact Information

|  |  |
| --- | --- |
| **TEAM-IDENTIFIER** | |
| **Name** |  |
| **Role** |  |
| **Email** |  |
| **CLIENT-NAME** | |
| **Name** |  |
| **Role** |  |
| **Email** |  |

# Table of Contents

[Document Information 2](#_Toc147356205)

[Confidentiality 2](#_Toc147356206)

[Legal Disclaimer 2](#_Toc147356207)

[Contact Information 2](#_Toc147356208)

[Table of Contents 3](#_Toc147356209)

[Executive Summary 5](#_Toc147356210)

[Assessment Overview 5](#_Toc147356211)

[Findings Count 5](#_Toc147356212)

[Scope 5](#_Toc147356213)

[Dates 5](#_Toc147356214)

[Key Findings 5](#_Toc147356215)

[Key Strengths 5](#_Toc147356216)

[Strategic Recommendations 5](#_Toc147356217)

[Governance and Regulatory Compliance 6](#_Toc147356218)

[Payment Card Industry Data Security Standard (PCI DSS) 6](#_Toc147356219)

[Testing Details 7](#_Toc147356220)

[Methodology Overview 7](#_Toc147356221)

[Scope 7](#_Toc147356222)

[Open-Source Intelligence (OSINT) 8](#_Toc147356223)

[Network Reconnaissance 8](#_Toc147356224)

[Network Map 8](#_Toc147356225)

[Exploitation 8](#_Toc147356226)

[Post-Exploitation 8](#_Toc147356227)

[Attack Chains 8](#_Toc147356228)

[Finding Classifications 9](#_Toc147356229)

[Business Impact 9](#_Toc147356230)

[CVSS Score 9](#_Toc147356231)

[Naming Schema 9](#_Toc147356232)

[Findings Summary 10](#_Toc147356233)

[Critical Risk Findings 11](#_Toc147356234)

[Description 11](#_Toc147356235)

[High Risk Findings 12](#_Toc147356236)

[Description 12](#_Toc147356237)

[Moderate Risk Findings 13](#_Toc147356238)

[Description 13](#_Toc147356239)

[Low Risk Findings 14](#_Toc147356240)

[Description 14](#_Toc147356241)

[Informational Findings 15](#_Toc147356242)

[Description 15](#_Toc147356243)

[Conclusion 16](#_Toc147356244)

[Appendix A: Testing Methodology 17](#_Toc147356245)

[Appendix B: Tools Used 18](#_Toc147356246)

[Appendix C: OSINT Findings 19](#_Toc147356247)

[Appendix D: Reconnaissance Findings 20](#_Toc147356248)

[Appendix E: Categorized Findings Tables 21](#_Toc147356249)

# Executive Summary

## Assessment Overview

TEAM-IDENTIFIER was contacted by CLIENT-NAME (hereafter referred to as CLIENT-ABV) to conduct a penetration test on their network after responding to CLIENT-ABV’s RFP. The penetration test simulated an attack starting within CLIENT-ABV’s network as well as [ADDITIONAL ENGAGEMENT ACTIVITIES]. The purpose of the penetration test was to assess CLIENT-ABV to identify opportunities to enhance the protection of information across CLIENT-ABV’s terminal and operational departments.

In total, TEAM-IDENTIFIER identified XX total findings during our assessment with XX of the findings being critical. It is recommended that CLIENT-ABV takes the necessary steps to evaluate and remediate these findings in order of severity. Leaving these systems in their current state can expose them to not only risk of intrusion – which can disrupt business operations, require a costly response to cover impacted parties, and lead to a loss of trust from customers and partners – but also significant regulatory jeopardy – which can result in monthly fines up to $XXX,XXX until resolved.

### Goals

Assess adherence to industry best practices and mitigating risks across the following domains:



## Findings Count

Critical Risk Findings: ***X***

High Risk Findings: ***X***

Moderate Risk Findings: ***X***

Low Risk Findings: ***X***

Informational Findings: ***X***

## Scope

* Subnet 1X.X.X.X/24
* Subnet 2X.X.X.X/24
* Subnet 3X.X.X.X/24
* Subnet 4X.X.X.X/24
* Subnet 5X.X.X.X/24

## Dates

XX/XX/XX -

## Key Strengths

## Key Findings

## Strategic Recommendations

# Governance and Regulatory Compliance

## Payment Card Industry Data Security Standard (PCI DSS)

### PCI DSS Compliance Business Impact

### PCI DSS Compliance Findings

# Testing Details

## Methodology Overview

To assess CLIENT-ABV’s internal network, TEAM-IDENTIFIER utilizes the Penetration Testing Execution Standard (PTES) as it provides a comprehensive framework, covering all stages involved in an internal penetration test. For more details on the PTES methodology, please consult Appendix A.

## Scope

### Authorized Assets

TEAM-IDENTIFIER was authorized by CLIENT-ABV to assess the following internal subnets during the requested penetration test:



### Approach

TEAM-IDENTIFIER’s penetration test was performed with initial internal network access from provided Windows 10 and Kali Linux virtual machines under a “black-box” penetration testing approach where penetration testers had limited knowledge of network assets from the initial RFP posted from CLIENT-ABV, the network scope provided, and additional information supplied from CLIENT-ABV throughout the penetration testing period.

### Timeframe

TEAM-IDENTIFIER was allotted one day, X, to perform an assessment over the authorized assets mentioned above where our engagement started at X and ended at X. After the assessment, our team worked diligently to deliver this report of our findings before X.

## Open-Source Intelligence (OSINT)

## Network Reconnaissance

## Network Map

## Exploitation

## Post-Exploitation

## Attack Chains

# Finding Classifications

TEAM-IDENTIFIER utilized a two-dimensional matrix, see below, consisting of the business impact and Common Vulnerability Scoring System v4.0 (CVSS)[[1]](#footnote-2) score of each finding to categorize it within one of five overall security risk categories: informational, low, moderate, high, and critical. These categories were organized to prioritize the remediation of findings that would cause CLIENT-ABV financial loss, non-compliance with governance requirements, and reputational impact.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Business Impact** | | | | |
| **CVSS Score** | **N/A (1)** | **Low (2)** | **Moderate (3)** | **High (4)** | **Critical (5)** |
| **N/A – 0.0 (a)** | 1a | 2a | 3a | 4a | 5a |
| **0.1 – 3.9 (b)** | 1b | 2b | 3b | 4b | 5b |
| **4.0 – 6.9 (c)** | 1c | 2c | 3c | 4c | 5c |
| **8.0 – 8.9 (d)** | 1d | 2d | 3d | 4d | 5d |
| **9.0 – 10.0 (e)** | 1e | 2e | 3e | 4e | 5e |
| **Overall Risk Key: ◼ Informational ◼ Low ◼ Moderate ◼ High ◼ Critical** | | | | | |

## Business Impact

TEAM-IDENTIFIER incorporates business impact into the result for the categorization of a finding to help prioritize mitigation efforts and allocate resources effectively to address the most critical issues. We base our qualitative measurement on the ability of a finding to impact CLIENT-ABV’s ability to conduct business, ensure public safety and security, protect customer information, or stay in compliance with government regulations and business standards. As TEAM-IDENTIFIER is operating under limited knowledge of the business operations of CLIENT-ABV, we would recommend CLIENT-ABV to review the business impact of these findings to provide a better understanding of the overall risk of said findings.

## CVSS Score

The Common Vulnerability Scoring System (CVSS) is a widely recognized industry standard used to evaluate and communicate the severity of security vulnerabilities in computer systems and software. It provides a structured framework for assessing a vulnerability's potential impact, exploitability, complexity, and privileges required for exploitation, assigning it a numeric score from 0 to 10, with higher scores indicating greater risk. CVSS assists organizations in prioritizing and addressing security flaws by considering their impact on confidentiality, integrity, and availability. In our security assessments, we adhere to the CVSS framework, which allows us to accurately gauge the severity of vulnerabilities and effectively communicate their potential risks.

## Naming Schema

# Findings Summary

|  |  |  |  |
| --- | --- | --- | --- |
| **Critical Risk Findings** | | | |
| **Unique ID** | **Finding Name** | **CVSS Score** | **Page Number** |
| **{%tr for finding in findings | filter\_severity([“Critical”]) %}** | | | |
| **XX-C-{{ “%02d” | format( loop.index | int ) }}** | **{{ finding.title }}** | **{{ finding.cvss\_score }}** |  |
| **{%tr endfor %}** | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **High Risk Findings** | | | |
| **Unique ID** | **Finding Name** | **CVSS Score** | **Page Number** |
| **{%tr for finding in findings | filter\_severity([“High”]) %}** | | | |
| **XX-H-{{ “%02d” | format( loop.index | int ) }}** | **{{ finding.title }}** | **{{ finding.cvss\_score }}** |  |
| **{%tr endfor %}** | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Moderate Risk Findings** | | | |
| **Unique ID** | **Finding Name** | **CVSS Score** | **Page Number** |
| **{%tr for finding in findings | filter\_severity([“Medium”]) %}** | | | |
| **XX-M-{{ “%02d” | format( loop.index | int ) }}** | **{{ finding.title }}** | **{{ finding.cvss\_score }}** |  |
| **{%tr endfor %}** | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Low Risk Findings** | | | |
| **Unique ID** | **Finding Name** | **CVSS Score** | **Page Number** |
| **{%tr for finding in findings | filter\_severity([“Low”]) %}** | | | |
| **XX-L-{{ “%02d” | format( loop.index | int ) }}** | **{{ finding.title }}** | **{{ finding.cvss\_score }}** |  |
| **{%tr endfor %}** | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Informational Findings** | | | |
| **Unique ID** | **Finding Name** | **CVSS Score** | **Page Number** |
| **{%tr for finding in findings | filter\_severity([“Informational”]) %}** | | | |
| **XX-I-{{ “%02d” | format( loop.index | int ) }}** | **{{ finding.title }}** | **{{ finding.cvss\_score }}** |  |
| **{%tr endfor %}** | | | |

# Critical Risk Findings

{% for finding in findings | filter\_severity([“Critical”]) %}

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **XX-C-{{ “%02d” | format( loop.index | int ) }}** | {{ finding.title }} | | |
| **Findings Categorization** | | | | |
| **Business Impact** | | {{ finding.impact | strip\_html }} | **CVSS v4.0 Score** | {{ finding.cvss\_score }} |
| **CVSS Attack Vector** | | {{ finding.cvss\_vector }} | | |

Description

{{ finding.description | strip\_html }}

Affected Systems

Potential Compliance Violations

Mitigations

References

{{ finding.references | strip\_html }}

Steps for Reproduction

{{ finding.replication\_steps | strip\_html }}

{% endfor %}

# High Risk Findings

{% for finding in findings | filter\_severity([“High”]) %}

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **XX-H-{{ “%02d” | format( loop.index | int ) }}** | {{ finding.title }} | | |
| **Findings Categorization** | | | | |
| **Business Impact** | | {{ finding.impact | strip\_html }} | **CVSS v4.0 Score** | {{ finding.cvss\_score }} |
| **CVSS Attack Vector** | | {{ finding.cvss\_vector }} | | |

Description

{{ finding.description | strip\_html }}

Affected Systems

Potential Compliance Violations

Mitigations

References

{{ finding.references | strip\_html }}

Steps for Reproduction

{{ finding.replication\_steps | strip\_html }}

{% endfor %}

# Moderate Risk Findings

{% for finding in findings | filter\_severity([“Medium”]) %}

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **XX-M-{{ “%02d” | format( loop.index | int ) }}** | {{ finding.title }} | | |
| **Findings Categorization** | | | | |
| **Business Impact** | | {{ finding.impact | strip\_html }} | **CVSS v4.0 Score** | {{ finding.cvss\_score }} |
| **CVSS Attack Vector** | | {{ finding.cvss\_vector }} | | |

Description

{{ finding.description | strip\_html }}

Affected Systems

Potential Compliance Violations

Mitigations

References

{{ finding.references | strip\_html }}

Steps for Reproduction

{{ finding.replication\_steps | strip\_html }}

{% endfor %}

# Low Risk Findings

{% for finding in findings | filter\_severity([“Low”]) %}

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **XX-L-{{ “%02d” | format( loop.index | int ) }}** | {{ finding.title }} | | |
| **Findings Categorization** | | | | |
| **Business Impact** | | {{ finding.impact | strip\_html }} | **CVSS v4.0 Score** | {{ finding.cvss\_score }} |
| **CVSS Attack Vector** | | {{ finding.cvss\_vector }} | | |

Description

{{ finding.description | strip\_html }}

Affected Systems

Potential Compliance Violations

Mitigations

References

{{ finding.references | strip\_html }}

Steps for Reproduction

{{ finding.replication\_steps | strip\_html }}

{% endfor %}

# Informational Findings

{% for finding in findings | filter\_severity([“Informational”]) %}

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **XX-I-{{ “%02d” | format( loop.index | int ) }}** | {{ finding.title }} | | |
| **Findings Categorization** | | | | |
| **Business Impact** | | {{ finding.impact | strip\_html }} | **CVSS v4.0 Score** | {{ finding.cvss\_score }} |
| **CVSS Attack Vector** | | {{ finding.cvss\_vector }} | | |

Description

{{ finding.description | strip\_html }}

Affected Systems

Potential Compliance Violations

Mitigations

References

{{ finding.references | strip\_html }}

Steps for Reproduction

{{ finding.replication\_steps | strip\_html }}

{% endfor %}

# Conclusion

# Appendix A: Testing Methodology

For the assessment of CLIENT-NAME’s internal network, TEAM-IDENTIFIER utilized the Penetration Testing Execution Standard (PTES) due to its coherency and extensive coverage of all stages encountered throughout an internal penetration test. The PTES methodology separates each penetration test into 7 unique phases:

**1. Pre-Engagement Interactions:** This initial phase involves extensive communication and collaboration between the penetration testing team and the client organization. It's during this stage that the objectives, scope, and rules of engagement are defined, and a clear understanding of the target environment is established. By carefully addressing these aspects, the pre-engagement interactions lay the groundwork for a transparent, well-structured, and mutually beneficial penetration testing engagement that aligns with the client's specific security needs and goals.

**2. Intelligence Gathering:** Once pre-engagement interactions have concluded, the next phase of the methodology focuses on collecting information about the target organization and its assets. To collect this information, different techniques are utilized such as Open-Source Intelligence (OSINT), social engineering, and fingerprinting.

**3. Threat Modeling:** The primary goal of this stage is identifying and categorizing a business’s critical assets, mapping each asset to all probable attack vectors, and identifying and modeling the appropriate threat actors based on the nature of the assets.

**4. Vulnerability Analysis:** Next, the methodology then calls for an in-depth analysis of the client’s assets with the goal of discovering flaws in the systems and applications that are within the scope of the assessment. This process can involve the use of banner grabbing to identify services and versions, manual testing to discover vulnerabilities, and automated vulnerability scanners.

**5. Exploitation:** This stage involves revisiting all vulnerabilities gathered during the previous phases of the methodology, with the primary goal of exploiting these targets and gaining access to the client’s assets.

**6. Post-Exploitation:** Upon gaining access, the next step is evaluating the importance of the compromised asset and the risk that it poses, as well as searching for additional vulnerabilities such as privilege escalation or moving laterally within the client’s network.

**7. Reporting:** The final step of this methodology involves gathering all findings from the previous phases and generating a professional report for the client. The main purpose of the report is to convey all findings from the penetration test, as well as remediation techniques so that security is hardened as a result of the assessment.

# Appendix B: Tools Used

# Appendix C: OSINT Findings

# Appendix D: Reconnaissance Findings

# Appendix E: Categorized Findings Tables

1. <https://www.first.org/cvss/v4.0/specification-document> [↑](#footnote-ref-2)