****

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

[1. Document Information 2](#_Toc155198101)

[1.1. Confidentiality 2](#_Toc155198102)

[1.2. Legal Disclaimer 2](#_Toc155198103)

[1.3. Contact Information 2](#_Toc155198104)

[2. Table of Contents 3](#_Toc155198105)

[3. Executive Summary 6](#_Toc155198106)

[3.1. Assessment Overview 6](#_Toc155198107)

[3.2. Engagement Timeline 6](#_Toc155198108)

[3.3. Findings Count 6](#_Toc155198109)

[3.4. Scope 6](#_Toc155198110)

[3.5. Key Strengths 6](#_Toc155198111)

[3.6. Key Findings 6](#_Toc155198112)

[3.7. Strategic Recommendations 6](#_Toc155198113)

[4. Reassessment Summary 7](#_Toc155198114)

[5. Governance and Regulatory Compliance 8](#_Toc155198115)

[5.1. Payment Card Industry Data Security Standard (PCI DSS) 8](#_Toc155198116)

[5.1.1. PCI DSS Compliance Findings 8](#_Toc155198117)

[5.1.2. Prioritized Approach for PCI DSS 8](#_Toc155198118)

[5.2. Other Regulatory Compliance 9](#_Toc155198119)

[5.3. Other Other Regulatory Compliance 9](#_Toc155198120)

[5.4. Other Other Other Regulatory Compliance 9](#_Toc155198121)

[6. Testing Details 10](#_Toc155198122)

[6.1. Methodology Overview 10](#_Toc155198123)

[6.2. Scope 10](#_Toc155198124)

[6.2.1. Assessment Access Assets 10](#_Toc155198125)

[6.2.2. Authorized Engagement Assets 10](#_Toc155198126)

[6.3. Approach 10](#_Toc155198127)

[6.4. Timeframe 10](#_Toc155198128)

[6.5. Network Map 11](#_Toc155198129)

[7. Attack Narrative 12](#_Toc155198130)

[7.1. Pre-Engagement 12](#_Toc155198131)

[7.2. Day X 12](#_Toc155198132)

[7.3. Day X 12](#_Toc155198133)

[7.4. Day X 12](#_Toc155198134)

[8. Finding Classifications 13](#_Toc155198135)

[8.1. Business Impact 13](#_Toc155198136)

[8.2. CVSS Score 13](#_Toc155198137)

[8.3. Naming Schema 13](#_Toc155198138)

[9. Finding Details 14](#_Toc155198139)

[9.1. Findings Summary 14](#_Toc155198140)

[9.2. Critical Risk Findings 16](#_Toc155198141)

[9.2.1. {{ finding.title }} 16](#_Toc155198142)

[9.3. High Risk Findings 17](#_Toc155198143)

[9.3.1. {{ finding.title }} 17](#_Toc155198144)

[9.4. Moderate Risk Findings 18](#_Toc155198145)

[9.4.1. {{ finding.title }} 18](#_Toc155198146)

[9.5. Low Risk Findings 19](#_Toc155198147)

[9.5.1. {{ finding.title }} 19](#_Toc155198148)

[9.6. Informational Findings 20](#_Toc155198149)

[9.6.1. {{ finding.title }} 20](#_Toc155198150)

[10. Conclusion 21](#_Toc155198151)

[11. Appendix A: Non-Compliance Findings 22](#_Toc155198152)

[11.1. Payment Card Industry Data Security Standard (PCI DSS) 22](#_Toc155198153)

[11.2. Other Regulatory Compliance 22](#_Toc155198154)

[11.3. Other Other Regulatory Compliance 22](#_Toc155198155)

[11.4. Other Other Other Regulatory Compliance 23](#_Toc155198156)

[12. Appendix B: Testing Methodology 24](#_Toc155198157)

[12.1. Penetration Testing Execution Standard (PTES) 24](#_Toc155198158)

[12.2. OWASP Top 10 25](#_Toc155198159)

[13. Appendix C: Findings Legend 26](#_Toc155198160)

[14. Appendix D: Logical Systems 27](#_Toc155198161)

[14.1. Logical System Findings: XX 27](#_Toc155198162)

[14.2. Logical System Findings: XX 27](#_Toc155198163)

[14.3. Logical System Findings: XX 27](#_Toc155198164)

[14.4. Logical System Findings: XX 27](#_Toc155198165)

[15. Appendix E: Tools Used 29](#_Toc155198166)

[15.1. Reconnaissance Tools 29](#_Toc155198167)

[15.2. Exploitation Tools 33](#_Toc155198168)

[15.3. Post-Exploitation Tools 34](#_Toc155198169)

[16. Appendix F: OSINT Assessment 36](#_Toc155198170)

[16.1. OSINT Findings 36](#_Toc155198171)

[17. Appendix G: Phishing Assessment 37](#_Toc155198172)

[17.1. 37](#_Toc155198173)

[18. Appendix H: Assessment Artifacts 38](#_Toc155198174)

# Executive Summary

## Assessment Overview

TEAM-IDENTIFIER was contacted by CLIENT-NAME (hereafter referred to as CLIENT-ABV) to conduct a security reassessment on their network after an initial penetration test was performed in Q3 2023. This reassessment focused on assessing CLIENT-ABV current security posture across the following contexts:

* W
* W
* W
* W
* W

In total, TEAM-IDENTIFIER identified XX total findings during our assessment with XX% of the findings from the previous assessment being resolved. 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 or an fine of $XXX,XXX if a data breach occurs within this period.

## Engagement Timeline

* A
* A
* A
* a
* a

## 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

## Key Strengths

## Key Findings

## Strategic Recommendations

# Reassessment Summary

During the prior engagement conducted on October 14, 2023, TEAM-IDENTIFIER a total of XX vulnerabilities within the network. Subsequent to this discovery, proactive measures were taken to address the issues, resulting in the resolution of XX vulnerabilities. Additionally, efforts were made to partially resolve XX vulnerabilities, while XX vulnerabilities remained unresolved. A distribution of the resolution of these findings are as follows:

|  |  |  |
| --- | --- | --- |
| **Finding Title** | **Finding Severity** | **Remediation Status** |
| FINDING TITLE | **Critical** | **Resolved** |
| FINDING TITLE | **High** | **Resolved** |
| FINDING TITLE | **Moderate** | **Resolved** |
| FINDING TITLE | **Low** | **Resolved** |
| FINDING TITLE | **Informational** | **Resolved** |
| FINDING TITLE | **Critical** | **Partially Resolved** |
| FINDING TITLE | **High** | **Partially Resolved** |
| FINDING TITLE | **Moderate** | **Partially Resolved** |
| FINDING TITLE | **Low** | **Partially Resolved** |
| FINDING TITLE | **Informational** | **Partially Resolved** |
| FINDING TITLE | **Critical** | **Unresolved** |
| FINDING TITLE | **High** | **Unresolved** |
| FINDING TITLE | **Moderate** | **Unresolved** |
| FINDING TITLE | **Low** | **Unresolved** |
| FINDING TITLE | **Informational** | **Unresolved** |

[Add notes based on results]

# Governance and Regulatory Compliance

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

The Payment Card Industry Data Security (PCI DSS)[[1]](#footnote-2) is a twelve (12) requirement actionable framework to ensure data security when processing, transmitting, and storing cardholder data. This standard was created collaboratively by major credit card companies such as Visa, MasterCard, and American Express to reduce the risk of data breaches and fraud. Companies that are looking to process credit cards are required to continuously adhere to PCI DSS to ensure the security of payment card data. Failure to comply can lead to monthly fines (which can range from $XX,XXX to $XX,XXX based on TEAM-IDENTIFIER classifying CLIENT-ABV as a Level X or Level X merchant from preliminary data), increased auditing requirements, inability to process credit cards, loss of public trust, lawsuits, and data breaches. In addition, data breaches that occur during periods of non-compliance can result in fines ranging from $50 to $90 per customer, which can equate to a total of $XXX,XXX.

### PCI DSS Compliance Findings

TEAM-IDENTIFIER chose to assess CLIENT-ABV compliance utilizing version 4.0[[2]](#footnote-3) of PCI DSS as version 3.2.1 of PCI DSS is set to retire after March 2024. During our assessment, TEAM-IDENTIFIER discovered XX potential PCI DSS violations.

[Summary of findings w/ Distribution]

A detailed list of the PCI DSS compliance findings can be found in Appendix A.

### Prioritized Approach for PCI DSS

The Prioritized Approach for PCI DSS[[3]](#footnote-4) is a roadmap of six risk-based security milestones provided by PCI DSS to help organizations incrementally protect against the highest risk factors while working to become PCI DSS compliant.

[Additional info]

|  |
| --- |
| **Prioritized Approach for PCI DSS Milestones** |
| 1. Do not store sensitive authentication data and limit cardholder data retention. |
| 1. Protect systems and networks and be prepared to respond to a system breach. |
| 1. Secure payment applications. |
| 1. Monitor and control access to your systems. |
| 1. Protect stored cardholder data. |
| 1. Complete remaining compliance efforts, and ensure all controls are in place. |

## Other Regulatory Compliance

## Other Other Regulatory Compliance

## Other Other Other Regulatory Compliance

# Testing Details

## Methodology Overview

To assess CLIENT-ABV’s internal network, TEAM-IDENTIFIER utilizes the Penetration Testing Execution Standard (PTES)[[4]](#footnote-5) 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 B.

## Scope

### Assessment Access Assets

CLIENT-ABV requested TEAM-IDENTIFIER to assess CLIENT-ABV’s network using jump hosts that were to be utilized by a VPN connection. The details of these assets are as follows:



### Authorized Engagement Assets

TEAM-IDENTIFIER was authorized by CLIENT-ABV to assess the following internal subnets during the 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 X days, 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.

## Network Map

# Attack Narrative

## Pre-Engagement

## Day X

## Day X

## Day X

# Finding Classifications

TEAM-IDENTIFIER utilized a two-dimensional matrix, see below, consisting of the business impact and Common Vulnerability Scoring System v4.0 (CVSS)[[5]](#footnote-6) 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, safety risks, non-compliance with governance requirements, and reputational impact. A detailed explanation of each section of the finding structure can be found at Appendix C.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Business Impact** | | | | |
| **CVSS Score** | **Informational (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 |
| **7.0 – 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 quantitatively gauge the severity of vulnerabilities.

## Naming Schema

TEAM-IDENTIFIER utilizes a three-part structure for creating our findings’ unique identifiers which includes: a logical system abbreviation, a risk categorization abbreviation, and a numeric index within the risk categorization. For instance, a finding could be named “AD-H-05” to identify a finding within the active directory logical system (AD), that has been categorized as high based on our two-dimensional matrix (H), when it was the fifth finding within the high categorization. A list of all logical systems and their respective findings can be found at Appendix D.

# Finding Details

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 Vector** | | {{ finding.cvss\_vector }} | | |

Technical Description

{{ finding.description | strip\_html }}

Business Impact Description

Affected Systems

[LIST OF IPs]

* [PORT]
  + [FUNCTION]

Potential Compliance Violations

PCI DSS:

[OTHER]:

Mitigations

References

{{ finding.references | strip\_html }}

Steps for Reproduction

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



|  |  |
| --- | --- |
|  |  |



**END OF FINDING BLOCK**

{% 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 Vector** | | {{ finding.cvss\_vector }} | | |

Technical Description

{{ finding.description | strip\_html }}

Business Impact Description

Affected Systems

[LIST OF IPs]

* [PORT]
  + [FUNCTION]

Potential Compliance Violations

PCI DSS:

[OTHER]:

Mitigations

References

{{ finding.references | strip\_html }}

Steps for Reproduction

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



|  |  |
| --- | --- |
|  |  |



**END OF FINDING BLOCK**

{% 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 Vector** | | {{ finding.cvss\_vector }} | | |

Technical Description

{{ finding.description | strip\_html }}

Business Impact Description

Affected Systems

[LIST OF IPs]

* [PORT]
  + [FUNCTION]

Potential Compliance Violations

PCI DSS:

[OTHER]:

Mitigations

References

{{ finding.references | strip\_html }}

Steps for Reproduction

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



|  |  |
| --- | --- |
|  |  |



**END OF FINDING BLOCK**

{% 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 Vector** | | {{ finding.cvss\_vector }} | | |

Technical Description

{{ finding.description | strip\_html }}

Business Impact Description

Affected Systems

[LIST OF IPs]

* [PORT]
  + [FUNCTION]

Potential Compliance Violations

PCI DSS:

[OTHER]:

Mitigations

References

{{ finding.references | strip\_html }}

Steps for Reproduction

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



|  |  |
| --- | --- |
|  |  |



**END OF FINDING BLOCK**

{% 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 Vector** | | {{ finding.cvss\_vector }} | | |

Technical Description

{{ finding.description | strip\_html }}

Business Impact Description

Affected Systems

[LIST OF IPs]

* [PORT]
  + [FUNCTION]

Potential Compliance Violations

PCI DSS:

[OTHER]:

Mitigations

References

{{ finding.references | strip\_html }}

Steps for Reproduction

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



|  |  |
| --- | --- |
|  |  |



**END OF FINDING BLOCK**

{% endfor %}

# Conclusion

# Appendix A: Non-Compliance Findings

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

|  |  |
| --- | --- |
| **PCI DSS Requirements** | **Related Findings** |
| **Build and Maintain a Secure Network and Systems** | |
| Requirement 1: Install and Maintain Network Security Controls |  |
| Requirement 2: Apply Secure Configurations to All System Components |  |
| **Protect Account Data** | |
| Requirement 3: Protect Stored Account Data |  |
| Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks |  |
| **Maintain a Vulnerability Management Program** | |
| Requirement 5: Protect All Systems and Networks from Malicious Software |  |
| Requirement 6: Develop and Maintain Secure Systems and Software |  |
| **Implement Strong Access Control Measures** | |
| Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know |  |
| Requirement 8: Identify Users and Authenticate Access to System Components |  |
| Requirement 9: Restrict Physical Access to Cardholder Data |  |
| **Regularly Monitor and Test Networks** | |
| Requirement 10: Log and Monitor All Access to System Components and Cardholder Data |  |
| Requirement 11: Test Security of Systems and Network Regularly |  |
| **Maintain an Information Security Policy** | |
| Requirement 12: Support Information with Organizational Policies and Programs |  |

## Other Regulatory Compliance

|  |  |
| --- | --- |
| **Other Regulation Requirements** | **Related Findings** |
| Requirement 1: |  |
| Requirement 2: |  |
| Requirement 3: |  |
| Requirement 4: |  |

## Other Other Regulatory Compliance

|  |  |
| --- | --- |
| **Other Other Regulation Requirements** | **Related Findings** |
| Requirement 1: |  |
| Requirement 2: |  |
| Requirement 3: |  |
| Requirement 4: |  |
| Requirement 5: |  |
| Requirement 6: |  |
| Requirement 7: |  |
| Requirement 8: |  |
| Requirement 9: |  |
| Requirement 10: |  |
| Requirement 11: |  |
| Requirement 12: |  |
| Requirement 13: |  |
| Requirement 14: |  |

## Other Other Other Regulatory Compliance

|  |  |
| --- | --- |
| **Other Other Other Regulation Requirements** | **Related Findings** |
| Requirement 1: |  |
| Requirement 2: |  |
| Requirement 3: |  |
| Requirement 4: |  |
| Requirement 5: |  |
| Requirement 6: |  |

# Appendix B: Testing Methodology

Penetration Testing Execution Standard (PTES)

For the assessment of CLIENT-NAME’s internal network, TEAM-IDENTIFIER utilized the Penetration Testing Execution Standard (PTES)[[6]](#footnote-7) 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.

OWASP Top 10

TEAM-IDENTIFIER utilizes the OWASP Top 10[[7]](#footnote-8) as a foundational framework for evaluating Web Applications, focusing on identifying common vulnerabilities and misconfigurations. The overarching goal of the project is to establish a consensus among experts in web application security regarding the most prevalent issues in modern applications. The 2021 edition of the OWASP Top 10, which if the most recent, specifies the following web application security flaws:

|  |  |
| --- | --- |
| **OWASP Top 10** | |
| 1. Broken Access Control | 1. Cryptographic Failures |
| 1. Injection | 1. Insecure Design |
| 1. Security Misconfiguration | 1. Vulnerable and Outdated Components |
| 1. Identification and Authentication Failures | 1. Software and Data Integrity Failures |
| 1. Security Logging and Monitoring Failures | 1. Server-Side Request Forgery |

This structured approach empowers security professionals to comprehensively assess and address the most critical aspects of web application security based on the collective insights of the industry.

# Appendix C: Findings Legend

To enhance clarity, TEAM-IDENTIFIER has included this legend of our findings. This serves as a helpful reference guide to understanding the background behind each of the sections of our findings.

|  |  |
| --- | --- |
| **Section** | **Description** |
| **Unique ID** | The unique ID serves as an easy way to identify a specific finding as it is composed of the abbreviation of the relevant logical system, a risk categorization abbreviation, and a numeric index within the risk categorization. Additional information of the logical systems can be found in Appendix D. |
| **Finding Title** | The finding title is a short description of finding that can be utilized to understand the contents of the finding at a high-level overview. |
| **Business Impact** | TEAM-IDENTIFIER utilizes a qualitative business impact rating based on the ability of the finding to impact the confidentiality of the business or customer data, the integrity of said data, the availability of business operations, the legal and regulatory compliance of the business, or the safety of employees and customers. The business impact is rated across one of five categories, Critical, High, Moderate, Low, Informational, and is used in tandem with the Common Vulnerability Scoring System (CVSS) v4.0 score to achieve the overall finding categorization. |
| **CVSS v4.0 Score** | The CVSS v4.0 score is a standardized numerical rating that quantifies the severity of a security vulnerability. It considers various factors, including the vulnerability's impact and how easy it is to exploit. A higher score indicates a more critical and potentially harmful vulnerability, aiding organizations in prioritizing and addressing security issues effectively. |
| **CVSS Vector** | The CVSS vector is an abbreviated string representation of the metrics utilized to calculate the CVSS score. This metric can be useful to identify reoccurring issues or understand the technical impact of the vulnerability at a brief glance. |
| **Technical Description** | The technical description gives a detailed explanation of a technical aspect of the finding, breaking down how the vulnerability exists and could be exploited. It helps technical teams understand fix the vulnerability more effectively. |
| **Business Impact Description** | The business impact description outlines the potential consequences of a finding on the organization’s operations, assets, and overall business continuity. |
| **Affected Systems** | The affected systems section includes all assets that are impacted by the specified finding. |
| **Potential Compliance Violations** | Potential compliance violations refer to aspects of regulatory, industry, or legal requirements that might be violated with respect to the contents of the findings. |
| **Mitigations** | The mitigations section offers practical strategies and recommendations to address and reduce the impact of identified findings. |
| **References** | The references section includes and references that might be helpful for resolving, reproducing, or understanding the finding. |
| **Steps for Reproduction** | Steps for reproduction are a clear and concise set of instructions to allow CLIENT-ABV to verify findings and test potential solutions for remediation. |

# Appendix D: Logical Systems

During assessments, TEAM-IDENTIFIER groups assets together logically based on their purpose as well as their relationship with other assets. This helps spot larger issues that might affect multiple devices as well as to understand the extent of a vulnerability. By organizing assets this way, we not only streamline the identification of problems but also provide valuable support to the teams managing these assets. A table of the logical systems, their abbreviation, and a description of said systems is as follows:

|  |  |  |
| --- | --- | --- |
| **Logical System** | **Abbreviation** | **Description** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Following this organization, our findings are presented in tables corresponding to each logical system by descending order of their severity. These tables provide a targeted and efficient remediation process, allowing teams to address issues specific to their areas of responsibility and enhance the overall security of the network.

Logical System Findings: XX

|  |  |  |
| --- | --- | --- |
| **Unique ID** | **Finding Name** | **Page Number** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Logical System Findings: XX

|  |  |  |
| --- | --- | --- |
| **Unique ID** | **Finding Name** | **Page Number** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Logical System Findings: XX

|  |  |  |
| --- | --- | --- |
| **Unique ID** | **Finding Name** | **Page Number** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Logical System Findings: XX

|  |  |  |
| --- | --- | --- |
| **Unique ID** | **Finding Name** | **Page Number** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Appendix E: Tools Used

## Reconnaissance Tools

|  |  |
| --- | --- |
| **AWS CLI** | |
| **Description** | The AWS Command Line Interface (AWS CLI) is a unified tool to manage your AWS services. Attackers can use the CLI to look into publicly exposed S3 buckets and more. |
| **Source** | <https://aws.amazon.com/cli/> |

|  |  |
| --- | --- |
| **BloodHound** | |
| **Description** | BloodHound is an Active Directory (AD) reconnaissance tool that can reveal hidden relationships and identify attack paths within an AD environment. |
| **Source** | <https://www.kali.org/tools/bloodhound/>  <https://github.com/SpecterOps/BloodHound> |

|  |  |
| --- | --- |
| **Enum4linux** | |
| **Description** | Enum4linux is a tool for enumerating information from Windows and Samba systems. |
| **Source** | <https://www.kali.org/tools/enum4linux/> |

|  |  |
| --- | --- |
| **Eyewitness** | |
| **Description** | EyeWitness is designed to take screenshots of websites, provide some server header info, and identify default credentials if possible. |
| **Source** | <https://www.kali.org/tools/eyewitness/>  <https://github.com/RedSiege/EyeWitness> |

|  |  |
| --- | --- |
| **Feroxbuster** | |
| **Description** | Feroxbuster is a tool designed to perform forced browsing. Forced browsing is an attack where the aim is to enumerate and access resources that are not referenced by the web application but are still accessible by an attacker. |
| **Source** | <https://www.kali.org/tools/feroxbuster/>  <https://github.com/epi052/feroxbuster> |

|  |  |
| --- | --- |
| **Gobuster** | |
| **Description** | Gobuster is a tool used to brute-force URIs including directories and files as well as DNS subdomains. |
| **Source** | <https://www.kali.org/tools/gobuster/>  <https://github.com/OJ/gobuster> |

|  |  |
| --- | --- |
| **NBTscan** | |
| **Description** | NBTscan is a program for scanning IP networks for NetBIOS name information. It sends NetBIOS status query to each address in supplied range and lists received information in human readable form. For each responded host it lists IP address, NetBIOS computer name, logged-in user name and MAC address (such as Ethernet). |
| **Source** | <https://www.kali.org/tools/nbtscan/>  <https://salsa.debian.org/pkg-security-team/nbtscan> |

|  |  |
| --- | --- |
| **Nikto** | |
| **Description** | Nikto is a web server scanner which performs comprehensive tests against web servers for multiple items, including potentially dangerous files/programs, checks for outdated versions of servers, and version specific problems. |
| **Source** | <https://www.kali.org/tools/nikto/>  <https://github.com/sullo/nikto> |

|  |  |
| --- | --- |
| **Onesixtyone** | |
| **Description** | Onesixtyone is a simple SNMP scanner which sends SNMP requests for the sysDescr value asynchronously with user-adjustable sending times and then logs the responses which gives the description of the software running on the device. |
| **Source** | <https://www.kali.org/tools/onesixtyone/>  <https://github.com/trailofbits/onesixtyone> |

|  |  |
| --- | --- |
| **Sharphound** | |
| **Description** | SharpHound is the official data collector for BloodHound. It is written in C# and uses native Windows API functions and LDAP namespace functions to collect data from domain controllers and domain-joined Windows systems. |
| **Source** | <https://github.com/BloodHoundAD/SharpHound> |

|  |  |
| --- | --- |
| **Smbmap** | |
| **Description** | SMBMap allows users to enumerate samba share drives across an entire domain. List share drives, drive permissions, share contents, upload/download functionality, file name auto-download pattern matching, and even execute remote commands. |
| **Source** | <https://www.kali.org/tools/smbmap/>  <https://github.com/ShawnDEvans/smbmap> |

|  |  |
| --- | --- |
| **Smtp-user-enum** | |
| **Description** | Smtp-user-enum is a username guessing tool primarily for use against the default Solaris SMTP service. |
| **Source** | <https://www.kali.org/tools/smtp-user-enum/> |

|  |  |
| --- | --- |
| **Sslscan** | |
| **Description** | SSLScan queries SSL services, such as HTTPS, in order to determine the ciphers that are supported. SSLScan is designed to be easy, lean and fast. The output includes preferred ciphers of the SSL service, the certificate and is in text and XML formats. |
| **Source** | <https://www.kali.org/tools/sslscan/>  <https://github.com/rbsec/sslscan> |

|  |  |
| --- | --- |
| **Wappalyzer** | |
| **Description** | Wappalyzer is an extension for browsers which allows you to graphically and simply visualize the technologies that are using an individual web page you visit, from the programming language used on the client and server side, to detect the CMS and more. |
| **Source** | <https://www.wappalyzer.com/> |

## Exploitation Tools

|  |  |
| --- | --- |
| **Burp Suite** | |
| **Description** | Burp Suite is a tool for testing web applications for security vulnerabilities through inspection and manipulation of their requests. |
| **Source** | <https://portswigger.net/burp> |

|  |  |
| --- | --- |
| **Certify / Certipy** | |
| **Description** | Certify/Certipy is an offensive tool for enumerating and abusing Active Directory Certificate Services (AD CS). |
| **Source** | <https://github.com/r3motecontrol/Ghostpack-CompiledBinaries>  <https://www.kali.org/tools/certipy-ad/> |

|  |  |
| --- | --- |
| **Kerbrute** | |
| **Description** | Kerbrute is an open-source tool to quickly bruteforce and enumerate valid Active Directory accounts through Kerberos Pre-Authentication |
| **Source** | <https://github.com/ropnop/kerbrute> |

|  |  |
| --- | --- |
| **Netexec** | |
| **Description** | Netexec formerly known as CrackMapExec is a network service exploitation tool that helps automate assessing the security of large networks. |
| **Source** | <https://github.com/Pennyw0rth/NetExec> |

|  |  |
| --- | --- |
| **Rubeus** | |
| **Description** | Rubeus is a C# toolset for raw Kerberos interaction and abuses. |
| **Source** | <https://github.com/r3motecontrol/Ghostpack-CompiledBinaries>  <https://github.com/GhostPack/Rubeus> |

|  |  |
| --- | --- |
| **Sqlmap** | |
| **Description** | sqlmap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. |
| **Source** | <https://www.kali.org/tools/sqlmap/>  <https://github.com/sqlmapproject/sqlmap> |

## Post-Exploitation Tools

|  |  |
| --- | --- |
| **Hashcat** | |
| **Description** | Hashcat supports five unique modes of attack for over 300 highly-optimized hashing algorithms. |
| **Source** | <https://www.kali.org/tools/hashcat/>  <https://hashcat.net/hashcat/> |

|  |  |
| --- | --- |
| **John The Ripper** | |
| **Description** | John the Ripper is a tool designed to help systems administrators to find weak (easy to guess or crack through brute force) passwords, and even automatically mail users warning them about it, if it is desired. |
| **Source** | <https://www.kali.org/tools/john/>  <https://github.com/openwall/john> |

|  |  |
| --- | --- |
| **Mimikatz** | |
| **Description** | Mimikatz uses admin rights on Windows to display passwords of currently logged in users in plaintext. |
| **Source** | <https://www.kali.org/tools/mimikatz/> aa |

|  |  |
| --- | --- |
| **Peass-ng** | |
| **Description** | Privilege Escalation Awesome Scripts SUITE. These scripts assist a penetration tester is identifying potential privilege escalation vulnerabilities as a part of their post-exploitation procedures. |
| **Source** | <https://www.kali.org/tools/peass-ng/>  <https://github.com/carlospolop/PEASS-ng> |

|  |  |
| --- | --- |
| **Sliver** | |
| **Description** | Sliver is an open source cross-platform adversary emulation/red team framework, it can be used by organizations of all sizes to perform security testing. Sliver's implants support C2 over Mutual TLS (mTLS), WireGuard, HTTP(S), and DNS. |
| **Source** | <https://github.com/BishopFox/sliver> |

|  |  |
| --- | --- |
| **XRDP** | |
| **Description** | XRDP provides a graphical login to remote machines using Microsoft Remote Desktop Protocol (RDP). |
| **Source** | <https://github.com/neutrinolabs/xrdp> |

# Appendix F: OSINT Assessment

For the assessment of CLIENT-ABV, TEAM-IDENTIFIER engaged in OSINT (Open-Source Intelligence) prior to the start of the engagement. The primary objective of this Open-Source Intelligence initiative was to comprehensively understand CLIENT-ABV's digital footprint, potential online vulnerabilities, and any publicly available data that could impact the engagement strategy. By seeking information from various publicly accessible sources such as social media, public websites, and public storefronts, TEAM-IDENTIFIER sought to identify potential risks and uncover any relevant trends that might influence CLIENT-ABV's security posture. This proactive approach ensured that the engagement was well-informed, allowing for strategic decision-making and a comprehensive understanding of the external factors that could positively impact CLIENT-ABV during the assessment taking place on XX/XX/2024 through XX/XX/24. The following information is the complete findings of everything found during TEAM-IDENTIFIER's OSINT engagement.

An overview of the OSINT artifacts identified by TEAM-IDENTIFIER are as follows along with a section detailing each finding.

* XXX.XXX
* XXX.XXX
* XXX.XXX
* XXX.XXX
* XXX.XXX

## OSINT Findings

|  |  |  |
| --- | --- | --- |
|  | **OSINT-I-XX** | {{ finding.title }} |

Technical Description

Business Impact Description

Source

Mitigations

References

Steps for Reproduction

|  |  |
| --- | --- |
|  |  |

**END OF FINDING BLOCK**

# Appendix G: Phishing Assessment

# Appendix H: Assessment Artifacts

During our assessments, we occasionally need to create objects such as files or users on a device, referred to as artifacts, to test potential vulnerabilities or gain additional access to a device or network. While our primary goal is to remove these artifacts after the assessment, there are instances where they may persist due to certain limitations in deletion. To mitigate any unintended consequences, we adhere to a standardized naming convention, using "CLIENT-ABV-[Artifact Number].[File Extension]", not only to provide easy identification of these artifacts but also to maintain transparency and accountability, aiming to minimize any lingering impact on the assessed systems. A table of all artifacts created during the assessment is as follows:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Hostname** | **IP** | **Artifact Name** | **Creation Time** | **File Path** | **Deleted?** |
|  |  |  |  |  | Yes/No |
|  |  |  |  |  | Yes/No |
|  |  |  |  |  | Yes/No |
|  |  |  |  |  | Yes/No |
|  |  |  |  |  | Yes/No |
|  |  |  |  |  | Yes/No |
|  |  |  |  |  | Yes/No |
|  |  |  |  |  | Yes/No |
|  |  |  |  |  | Yes/No |

1. <https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI-DSS-v4-0-At-A-Glance.pdf> [↑](#footnote-ref-2)
2. <https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf> [↑](#footnote-ref-3)
3. <https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/Prioritized-Approach-For-PCI-DSS-v4-0.pdf> [↑](#footnote-ref-4)
4. <http://www.pentest-standard.org/index.php/Main_Page> [↑](#footnote-ref-5)
5. <https://www.first.org/cvss/v4.0/specification-document> [↑](#footnote-ref-6)
6. <http://www.pentest-standard.org/index.php/Main_Page> [↑](#footnote-ref-7)
7. <https://owasp.org/www-project-top-ten/> [↑](#footnote-ref-8)