****



**{date}**

**{title} Penetration Test Report**

 **Public scope Pentest**

**Cyber Security Institute**

Table of Contents

[**DOCUMENT PROPERTIES** 4](#_Toc96491213)

[ABOUT US 5](#_Toc96491214)

[INTELLECTUAL PROPERTY RIGHTS 5](#_Toc96491215)

[LIMITATIONS ON DISCLOSURE AND USE OF THIS REPORT 5](#_Toc96491216)

[ASSUMPTIONS AND CONSTRAINTS 6](#_Toc96491217)

[REPORT STRUCTURE 6](#_Toc96491218)

[EXECUTIVE SUMMARY 7](#_Toc96491219)

[INTRODUCTION 7](#_Toc96491220)

[SCOPE OF WORK 8](#_Toc96491221)

[METHODOLOGY 8](#_Toc96491222)

[OVERVIEW OF FINDINGS 9](#_Toc96491223)

[DETAILED FINDINGS 11](#_Toc96491224)

1. {#critical} {title} ……………………………………………………………………………………………………………. {/critical}
2. {#high } {title} ……………………………………………………………………………………………………………. {/high}
3. {#medium} {title} ……………………………………………………………………………………………………………. {/medium}
4. {#low} {title} ..……………………………………………………………………………………………………………. {/low}

[**Notes** 44](#_Toc96491242)

[ We limited our test to the Red-Team 44](#_Toc96491243)

[ We found other vulnerabilities at internal 44](#_Toc96491244)

[ Telephone Systems exposed from access wifi not separated 44](#_Toc96491245)

[APPENDIX A: OUR CONSULTANT'S TOOLBOX 44](#_Toc96491246)

[APPENDIX B: RISK SCORING 45](#_Toc96491247)

[CALCULATING THE RISK RATING 45](#_Toc96491248)

[CVSS 45](#_Toc96491249)

[REMEDIATION TIMELINES 46](#_Toc96491250)

# **DOCUMENT PROPERTIES**

|  |  |
| --- | --- |
| Title | {title} |
| Version | {version} |
| Report ID | {id} |
| Prepared for | {client name} |
| Prepared By | {org name} |
| Release date | {release date} |
| Document classification | Confidential |

|  |  |
| --- | --- |
| Team | |
| Name | Level |
| {#users} {user name} | {user type} {/users} |

|  |  |
| --- | --- |
| Report Distribution List | |
| Name | Organization |
| Cyber Security Institute | {org name} CIO / {org name} CTIO |

# ABOUT US

**{org name} Cyber Security Institute** is managed by a team of experts in cyber defense field. We are a service-oriented organization specialized in technical security consultancy services for unlimited scale of business to help maintain your resources secure with high level of professionalism and precision such as IT risk management and information security advisory. By using the latest techniques, methodologies, and attack simulation from malicious perspective. We make sure that your organization is approaching the best practice to mitigate the risk at the lowest cost. We approach our cyber defense services from a holistic approach. Our aim is to contribute to the efforts of our customers in securing the critical IT infrastructure and crown jewels within their IT landscape.

# INTELLECTUAL PROPERTY RIGHTS

This document contains valuable trade secrets and confidential information of {org name} Cyber Security Institute and its partners. Any content shall not be disclosed to any person, organization, or entity unless such disclosure is subject to the provisions of a written non-disclosure agreement and proprietary rights agreement, or intellectual property license agreement approved by {org name}. The distribution of this document does not grant any license or rights in whole or in part to the content, the product(s), technology, or intellectual property described herein.

# LIMITATIONS ON DISCLOSURE AND USE OF THIS REPORT

This report contains information concerning potential vulnerabilities of the project's in-scope targets and methods of exploiting them. It is recommended that special precautions be taken to protect the confidentiality of both this document and the information contained in it. A copy of the report has been retained and secured for customer reference.

Our opinion provided in this report is valid for the period during which the assessment was carried out, and it is based on the information provided for the assessment and does not constitute a pre-certification or certification audit in accordance with the attainment of any accreditation/certification. Projection of any conclusions based on our findings for future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to or the failure to make the changes required for the network, applications, or systems. Furthermore, the findings in this report reflect the conditions found during the assessment, and do not necessarily reflect current conditions.

This report may not be used for any other purpose without CORELIA prior, written approval. Any references to {org name} Cyber Security Institute or our report(s) in marketing or promotional literature or any material to be disseminated to the public must be approved in advance in writing by {org name}.

# ASSUMPTIONS AND CONSTRAINTS

Please note that the penetration test/vulnerability assessment may not help identify all issues in the targeted systems and applications. The assessment can only indicate the security posture of the assessed target at the time of the test. Therefore, security testing should be considered as a process, not a silver bullet. Continuous execution of security assessments is recommended.

# REPORT STRUCTURE

This report contains the information gathered during the vulnerability assessment exercise performed on {client name}. This report is divided into three sections:

* Executive Summary.
* Detailed Findings.
* Conclusion and Way Forward.

The executive summary provides an overview of the security testing exercise, followed by Detailed Findings of the security gaps discovered during the engagement, and the Conclusion and Way Forward.

# EXECUTIVE SUMMARY

## INTRODUCTION

{org name} creates correlations between our customers' data, IT and business lines, correlates the highest levels of expertise with the growing complexity of projects, intelligence, and technology. CORELIA DNA is Data at the heart of all projects, at the heart of all our expertise, is the cross-functionality of our offers and our innovations. Correlating it engages us in each of our actions, from simple migration to the highest level of complexity of data management, powered by our Data Science Institute. This same correlation of data commits us to its performance, its integrity, its structuring, its homogenization, its conformity, its sovereign location and just as much to its criticism of security and its ability to homogenize it. CORELIA tames data, for the benefit of its customers. To carry out one such review, {client name} had engaged {org name} to perform penetration test on ‘All {client name} External Domains and IPs' web and network penetration test. The following activities were performed as part of the vulnerability assessment exercise:

* Identification of the vulnerabilities related to {client name} all external assets.
* Prioritization of the vulnerabilities depending upon the risk exposure.
* Exploitation of vulnerabilities.
* Development of recommendations to mitigate the vulnerabilities.

## SCOPE OF WORK

The scope of the engagement involved a Grey Box penetration test for {client name}. The assessment was performed with no prior knowledge of the target systems some technical and architectural details were shared i.e., VLANS.

The target assets analyzed as part of the assessment are summarized below:

**Grey Box:**

|  |  |
| --- | --- |
| No. | Asset |
|  | {#assets} {asset value} {/assets} |

## METHODOLOGY

Assessment methodology includes structured review processes based on recognized best practices as defined by such methodologies as the ISECOM's Open-Source Security Testing Methodology Manual (OSSTMM), Penetration Testing Execution Standard (PTES) and the Open Web Application Security Project (OWASP). In general, {org name}’s Cyber Security Institute are following a cyclical process while performing security assessments.

Gathering

Information

Cleaning Up

and Reporting

Enumeration

Post-

Exploitation

Vulnerability

Identification

Vulnerability

Exploitation

{org name}’s Cyber Security Institute are highly experienced in web application assessments so that our proprietary methodology is supported by contextual analysis and testing that helps in uncovering the most obscure vulnerabilities while also ensuring coverage at all levels.

1. Information Gathering Reconnaissance.
2. Configuration and Deploy Management Testing.
3. Authentication Testing.
4. Authorization Testing.
5. Business Logic Testing.
6. Data Validation Testing.

## OVERVIEW OF FINDINGS

The vulnerabilities and corresponding risks identified as part of the tests are categorized into the following severity levels:

* Critical – Severe impact on the affected system/application (identified issues which, if not addressed, could potentially pose a significant security threat to DFI IT infrastructure. Controls/countermeasures must be implemented immediately to address the gaps.).
* High – High impact on the affected system/application that would pose a direct threat to the confidentiality and integrity of very sensitive information or availability of critical systems. The issue identified could harm the organization either financially or legally, and could potentially create a loss of image.
* Medium – Moderate impact on the affected system/application that poses a direct threat to the confidentiality and integrity of (a subset of) sensitive information or availability of non-critical systems; or the issue gives an attacker access to systems or other means that provide an advanced platform for further attack.
* Low – Limited impact on the affected system/application that leads to technical information disclosure or increases the chance of successful attacks. This issue does not directly lead to unauthorized access, nor poses a direct threat to the confidentiality and integrity of sensitive information.

|  |  |
| --- | --- |
| Total Number of Vulnerabilities **{finding total count}** | |
| **Critical** | **{critical count}** Vulnerabilities |
| **High** | **{high count}** Vulnerabilities |
| **Medium** | **{medium count}** Vulnerabilities |
| **Low** | **{low count}** Vulnerabilities |

The table below depicts an overview of the identified vulnerabilities and the associated risk classification.

|  |  |
| --- | --- |
| Finding | Risk Score |
| 1. {#critical} {title} | Critical{/critical} |
| 1. {#high} {title} | High{/high} |
| 1. {#medium} {title} | Medium {/medium} |
| 1. {#low} {title} | Low {/low} |

# DETAILED FINDINGS

The below section explains in detail each identified vulnerability, describe its impact, highlight applications affected, and recommend a course of actions to mitigate it.

Graph location

{#critical}

# {title}

|  |  |  |  |
| --- | --- | --- | --- |
| Vulnerable Target(s) | {target} | | |
| Risk | **Critical** | | |
| Finding Type | {finding type} | Root Cause | {root cause} |
| Affected Module | {affected asset} | Impact | {impact type} |
| Finding Status | {finding status} | Likelihood | {likelihood} |

**Description**

{description}

{picture}

**Impact**

{impact}

**References**

{reference}

{#poc}

**Proof of Concept**

{/poc}

{#poc scenarios}

* {scenario}

{#scenario images}

{scenario image}

{/scenario images}

{/poc scenarios}

{#retest}

**Retest**

{/retest}

{#retest scenarios}

* {scenario}

{#scenario images}

{scenario image}

{/scenario images}

{/retest scenarios}

**Recommendation**

**{recommendation}**

{/critical}

{#high}

# {title}

|  |  |  |  |
| --- | --- | --- | --- |
| Vulnerable Target(s) | {target} | | |
| Risk | **High** | | |
| Finding Type | {finding type} | Root Cause | {root cause} |
| Affected Module | {affected asset} | Impact | {impact type} |
| Finding Status | {finding status} | Likelihood | {likelihood} |

**Description**

{description}

{picture}

**Impact**

{impact}

**References**

{reference}

{#poc}

**Proof of Concept**

{/poc}

{#poc scenarios}

* {scenario}

{#scenario images}

{scenario image}

{/scenario images}

{/poc scenarios}

{#retest}

**Retest**

{/retest}

{#retest scenarios}

* {scenario}

{#scenario images}

{scenario image}

{/scenario images}

{/retest scenarios}

**Recommendation**

**{recommendation}**

{/high}

{#medium}

# {title}

|  |  |  |  |
| --- | --- | --- | --- |
| Vulnerable Target(s) | {target} | | |
| Risk | **Medium** | | |
| Finding Type | {finding type} | Root Cause | {root cause} |
| Affected Module | {affected asset} | Impact | {impact type} |
| Finding Status | {finding status} | Likelihood | {likelihood} |

**Description**

{description}

{picture}

**Impact**

{impact}

**References**

{reference}

{#poc}

**Proof of Concept**

{/poc}

{#poc scenarios}

* {scenario}

{#scenario images}

{scenario image}

{/scenario images}

{/poc scenarios}

{#retest}

**Retest**

{/retest}

{#retest scenarios}

* {scenario}

{#scenario images}

{scenario image}

{/scenario images}

{/retest scenarios}

**Recommendation**

**{recommendation}**

{/medium}

{#low}

# {title}

|  |  |  |  |
| --- | --- | --- | --- |
| Vulnerable Target(s) | {target} | | |
| Risk | **Low** | | |
| Finding Type | {finding type} | Root Cause | {root cause} |
| Affected Module | {affected asset} | Impact | {impact type} |
| Finding Status | {finding status} | Likelihood | {likelihood} |

**Description**

{description}

{picture}

**Impact**

{impact}

**References**

{reference}

{#poc}

**Proof of Concept**

{/poc}

{#poc scenarios}

* {scenario}

{#scenario images}

{scenario image}

{/scenario images}

{/poc scenarios}

{#retest}

**Retest**

{/retest}

{#retest scenarios}

* {scenario}

{#scenario images}

{scenario image}

{/scenario images}

{/retest scenarios}

**Recommendation**

**{recommendation}**

{/low}

# APPENDIX A: OUR CONSULTANT'S TOOLBOX

DFI's Cyber Security Team use various free and commercial tools in addition to manual exercises.

However, in many cases our consultants have the ability to develop their own scripts tailored to the assignment. In general, most of the tools used in the engagements are:

|  |  |  |
| --- | --- | --- |
| **Tools** | | |
| Metasploit | BurpSuite Professional | Nessus Professional |
| Netcat | SQLMap | TCPDump |
| Acunetix | John The Ripper | Hydra |
| Nmap | Ettercap | Medusa |
| DnsRecon | Cain Abel | Powersploit |
| Beef | TheHarvester | Microsoft Sysinternal |
| Maltego | SQLNinja | Wireshark |

# APPENDIX B: RISK SCORING

This overview describes the attributes of the risk scoring used by DFI Cyber Security Team.

|  |  |
| --- | --- |
| Likelihood | Impact |
| **High:** The vulnerability is easy to exploit. Little information is required to exploit the issue, or an exploit kit is easy to obtain and use. No effective measures have been taken to prevent the issue from occurring. | **High:** Events that would pose a direct threat to the confidentiality and integrity of very sensitive information or availability of critical systems. The issue identified could harm the organization either financially or legally, and could potentially create a loss of  image |
| **Medium:** The vulnerability is harder to exploit. More information is required, or exploit tools require knowledge, to take advantage of it. Some effective measures have been taken to prevent the issue from occurring. However, the level of measures  taken leaves room for improvement. | **Medium:** Events that pose a direct threat to the confidentiality and integrity of (a subset of) sensitive information or availability of non-critical systems; or the issue gives an attacker access to systems or other means that provide an advanced platform for  further attack. |
| **Low:** The vulnerability is difficult to exploit. Exploitation requires specialist knowledge or detailed knowledge of the specific technical implementation. Alternatively, effective measures have been taken to prevent the issue from occurring. | **Low:** The issue leads to technical information disclosure or increases the chance of successful attacks. This issue does not directly lead to unauthorized access, nor poses a direct threat to the confidentiality and integrity of sensitive  information. |

## CALCULATING THE RISK RATING

The advice for further action for findings made is based on the likelihood and impact rating of the respective finding. This table describes the way the advice for further action is derived from Likelihood and Impact in general.

|  |  |
| --- | --- |
| Risk Rating | Likelihood x Impact |
| Critical | High x High |
| High | Medium x High |
| Medium | Low x High |
| Medium | High x Medium |
| Medium | Medium x Medium |
| Low | Low x Medium |
| Low | High x Low |
| Low | Medium x Low |
| Low | Low x Low |

## CVSS

DFI Cyber Security Team follows the international standard for risk scoring of vulnerabilities to allow clients to track the identified risks better, and easily integrate these with existing vulnerability management systems. DFI Cyber Security Team uses the same CVSS risk calculator that is used by international entities and public vulnerability

databases. This allows adding more granularities to the likelihood vs. impact formula and provides the client with relevant scores. By evaluating the exploitation likelihood and impact of identified security issues, customers can better track their vulnerabilities and prioritize remediation plans.

Following resource links provide background information on the CVSS risk scoring standard: <https://www.first.org/cvss/specification-document>

<https://www.first.org/cvss/user-guide>

The table provides the qualitative severity rating scale for CVSS risk scoring. Une image contenant texte

Description générée automatiquement

## REMEDIATION TIMELINES

|  |  |
| --- | --- |
| Severity risk rating | CVSS score |
| Critical | 9.0 – 10 |
| High | 7.0 – 8.9 |
| Medium | 4.0 – 6.9 |
| Low | 0.1 – 3.9 |

The following table suggests the timelines to implement the recommendations based on the risk rating and level of effort required for the vulnerabilities

|  |  |
| --- | --- |
| Risk Score | Timeline |
| Critical | Implement the recommendations within 1 week |
| High | Implement the recommendations within 1 to 2 weeks of time |
| Medium | Implement the recommendations within 2 - 4 weeks of time |
| Low | Implement the recommendations within 4 - 6 weeks of time |