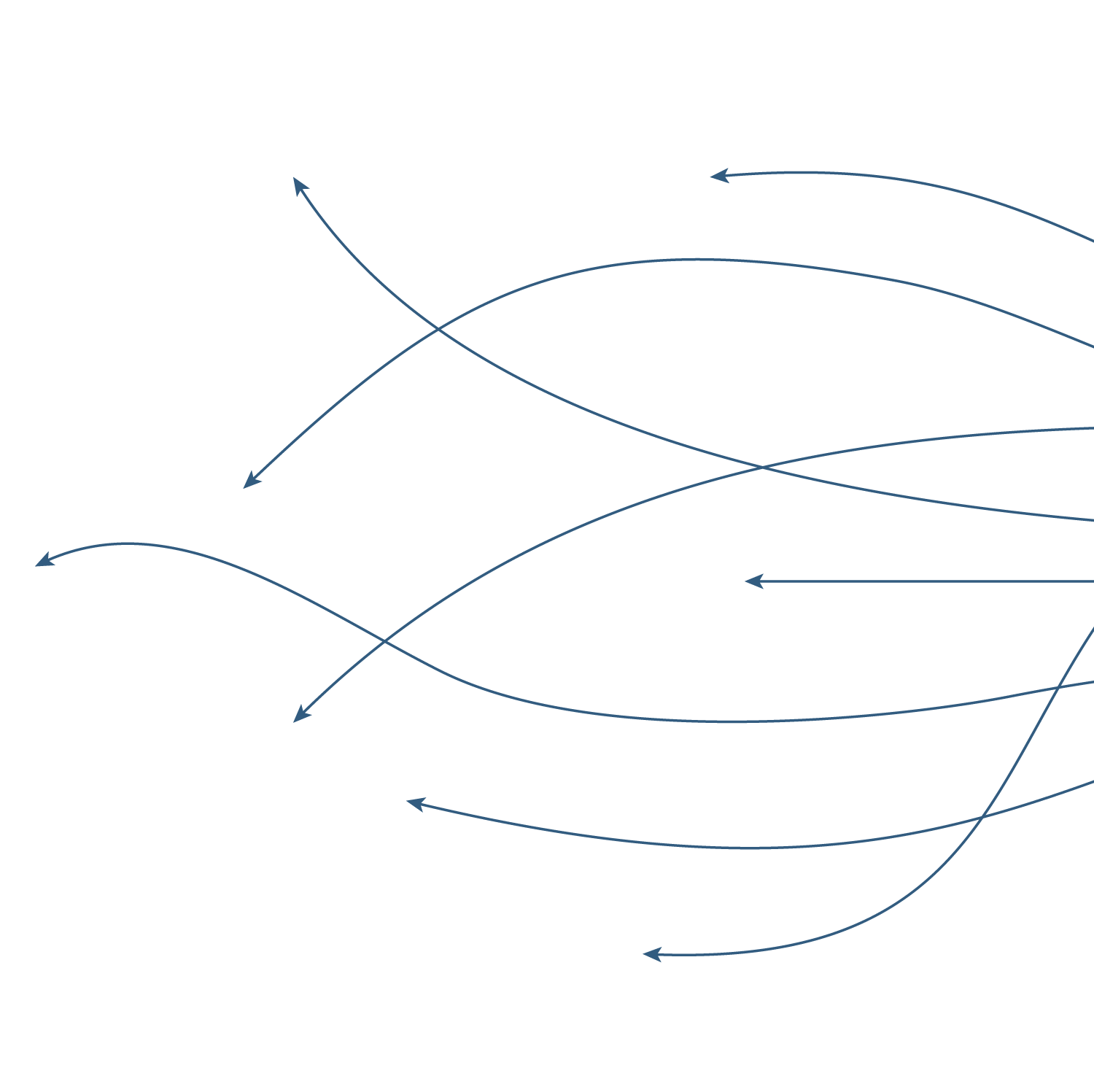


**{{NOMECLIENTE}} and DEMO SEC Confidential**

**Vulnerability Assessment Report**

***{{NOMEINFRASTRUTTURA}}***

***{{NOMECLIENTE}}***



Demo Security

Date:

Document Control

Confidentiality Statement

This document is the exclusive property of **{{NOMECLIENTE}}** and Demo Security. This document contains proprietary and confidential information.

Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both **{{NOMECLIENTE}}** and Demo Security.

Demo Security may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Document Tracking

Data Classification: **DEMO Security AND {{NOMECLIENTE}} CONFIDENTIAL**

Authors

|  |  |  |
| --- | --- | --- |
| Name | Title | Email Address |
| John Doe | Security Expert |  |
| Mario Rossi | Security Expert |  |

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Number | Revision Date | Author | Summary of changes |
| 1.0 |  | John Doe | Release to client |

Table of Contents

[Document Control 3](#_Toc126923741)

[Assessment Overview 5](#_Toc126923742)

[Scope Exclusions 5](#_Toc126923743)

[Executive Summary 6](#_Toc126923744)

[Summary of Findings 6](#_Toc126923745)

[Main Remediations 8](#_Toc126923746)

[Methodology 9](#_Toc126923747)

[Overview 9](#_Toc126923748)

[Tools 10](#_Toc126923749)

[Risk Parameter Criteria 10](#_Toc126923750)

[Findings and Remediations 11](#_Toc126923751)

[Demo Security Team 12](#_Toc126923752)

Tables & Images

Assessment Overview

**{{NOMECLIENTE}}** hired Demo Security to perform a Vulnerability Assessment on its **{{NOMEINFRASTRUTTURA}}** infrastructure.

The testing activity began on **{{data\_inizio}}** and ended on **{{data\_fine}}.**

The identified vulnerabilities, if discovered by a malicious user, would create a VALUABLE risk of compromise of all data on all systems in scope.

Out Of Scope

1. Per client request, Demo Security did not perform any Denial of Service attacks during testing.

Executive Summary

**{{NOMECLIENTE}}** hired Demo Security to perform a Vulnerability Assessment on its **{{NOMEINFRASTRUTTURA}}** infrastructure.

The testing activity began on **{{data\_inizio}}** and ended on **{{data\_fine}}.**

Summary of Findings

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Vulnerability** | **Risk** | **N°Host Impacted** | **N°CVE** | **Solution** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

*Table 1 – Summary of Findings*

{{CHART}}

*Figure 1 – Vulnerability x Impact*

Main Remediations

These are the main remedial actions recommended to fix the major vulnerabilities detected and, in some of the cases, exploited:

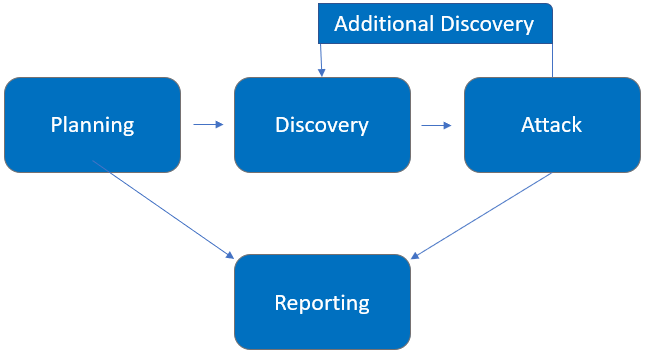
Methodology

Overview

All testing performed is based on the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks*.

Phases of penetration testing activities include the following:

* **Planning** – Customer goals are gathered and rules of engagement obtained.
* **Discovery** – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
* **Attack** – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
* **Reporting** – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Tools

Tools utilized for the activity:

1. Tenable Nessus (description).
2. ....

Risk Parameter Criteria

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

|  |  |
| --- | --- |
| **CVSS Score Range** | **Severity** |
| Da 9.0 a 10.0 | CRITICAL |
| Da 7.0 a 8.9 | HIGH |
| Da 4.0 a 6.9 | MEDIUM |
| Da 0.1 a 3.9 | LOW |

Findings and Remediations

The following are all the vulnerabilities found with information about the systems on which they were found and the corresponding countermeasures to be taken to resolve them.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Index** | **Item** | **ID** | **Risk** | **Name** | **CVE** | **System** | **Description** | **CVSS Base Score** | **CVSS Temporal Score** | **Solution** |
| {%tr for item in table\_contents %} | | | | | | | | | | |
| {{item.Index}} | {{item.Item}} | {{item.ID}} | {{item.Risk}} | {{item.Name}} | {{item.CVE}} | {{item.System}} | {{item.Description}} | {{item.CVSS\_Base\_Score}} | {{item.CVSS\_Temp\_Score}} | {{item.Solution}} |
| {%tr endfor %} | | | | | | | | | | |

Demo Security Team

**John Doe** Security Expert

**Mario Rossi** Security Expert

**-END OF DOCUMENT-**