Logotipo

Descripción generada automáticamente

{{ corp\_name }}

Security Assessment

Findings Report

Business Confidential

* Date of the project: {{ project\_date }}
* Version of the project: {{ project\_version }}
* Project name: {{ project\_name }}

# Table of Contents

[Table of Contents 4](#_Toc138088042)

[Confidentiality Statement 5](#_Toc138088043)

[Disclaimer 5](#_Toc138088044)

[Contact Information 5](#_Toc138088045)

[Assesment overview 6](#_Toc138088046)

[Assessment Components 6](#_Toc138088047)

[Internal Penetration Test 6](#_Toc138088048)

[Finding severity ratings 7](#_Toc138088049)

[Risk factors 7](#_Toc138088050)

[Likelihood 7](#_Toc138088051)

[Impact 7](#_Toc138088052)

[Scope 8](#_Toc138088053)

[Hosts analyzed 8](#_Toc138088054)

[Scope Exclusions 8](#_Toc138088055)

[Client Allowances 8](#_Toc138088056)

[Executive summary 9](#_Toc138088057)

[Scoping and time limitations 9](#_Toc138088058)

[Testing summary 9](#_Toc138088059)

[Tester Notes and Recommendations 9](#_Toc138088060)

[Vulnerability summary & report card 10](#_Toc138088061)

[Internal Penetration Test Findings 10](#_Toc138088062)

# Confidentiality Statement

This document is the exclusive property of {{ corp\_name }} and {{ team\_name }} ({{ team\_abbreviature }}).

This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both {{ corp\_name }} and {{ team\_abbreviature }}).

{{ corp\_name }} may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

# Disclaimer

|  |  |  |
| --- | --- | --- |
| **Name** | **Title** | **Contact Information** |
| {{ corp\_name }} | | |
| John Smith | Global Information Security Manager | Email: {{ corp\_email }} |
| {{ team\_name }} | | |
| {{ pentester\_name }} | Penetration Tester | Email: {{ pentester\_email }} |

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. {{ team\_abbreviature }} prioritized the assessment to identify the weakest security controls an attacker would exploit. {{ team\_abbreviature }} recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

# Contact Information

# Assesment overview

From {{ start\_date }} to {{ project\_date }}, {{ corp\_name }} engaged {{ team\_name }}, from now on, {{ team\_abbreviature }}, to evaluate the security posture of its infrastructure compared to current industry best practices that included an internal network penetration test. 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 vulnerabilitie**s through exploitation and **perform additional discovery** upon new access.
* **Reporting** – **Document** all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.

# Assessment Components

## Internal Penetration Test

An internal penetration test emulates the role of an attacker from inside the network. An engineer will scan the network to identify potential host vulnerabilities and perform common and advanced internal network attacks, such as: LLMNR/NBT-NS poisoning and other man- in-the-middle attacks, token impersonation, kerberoasting, pass-the-hash, golden ticket, and more. The engineer will seek to gain access to hosts through lateral movement, compromise domain user and admin accounts, and exfiltrate sensitive data.

# Finding severity ratings

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

|  |  |  |
| --- | --- | --- |
| **Severity** | **CVSS V3**  **Score Range** | **Definition** |
| **Critical** | 9.0–10.0 | Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately. |
| **High** | 7.0 – 8.9 | Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible. |
| **Moderate** | 4.0 – 6.9 | Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved. |
| **Low** | 0.1 – 3.9 | Vulnerabilities are non-exploitable but would reduce an organization’s attack surface. It is advised to form a plan of action and patch during the next maintenance window. |
| **Informational** | N/A (Informational data) | No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation. |

# Risk factors

Risk is measured by two factors: Likelihood and impact.

## Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

## Impact

Impact measures the potential vulnerability’s effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

# Scope

## Hosts analyzed

|  |  |  |  |
| --- | --- | --- | --- |
| Host | {% colspan port\_context\_columns|count %}Information about the host | | |
| {%tc for col in port\_context\_columns %} | {{ col }} | {%tc endfor %} |
| **{%tr for item in port\_context\_rows %}** | | | |
| **{{ item.label }}** | **{%tc for col in item.cols %}** | {{ col }} | {%tc endfor %} |
| **{%tr endfor %}** | | | |

## Scope Exclusions

Per client request, {{ team\_abbreviature }} did not perform any of the following attacks during testing:

* Denial of service (DoS)
* Phishing/Social Engineering

All other attacks not specified above were permitted by {{ corp\_name }}.

## Client Allowances

{{ corp\_name }} provided {{ team\_abbreviature }} the following allowances:

* Internal access to network via TBD.

# Executive summary

{{ team\_abbreviature }} evaluated {{ corp\_name }}’s internal security posture through penetration testing from {{ start\_date }} to {{ project\_date }}. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

{{ executive\_summary }}

## Scoping and time limitations

Scoping during the engagement did not permit denial of service or social engineering across all testing components.

Time limitations were in place for testing. Internal network penetration testing was permitted for {{ scope\_ptt\_days }} days.

## Testing summary

he network assessment evaluated {{ corp\_name }}’s internal security posture. From an internal perspective, the {{ team\_abbreviature }} performed vulnerability scanning against the IP addresses provided by {{ corp\_name }} to evaluate the overall patching health of the network.

TBD

## Tester Notes and Recommendations

TBD overall security (good/regular/bad).

TBD constants that stood out in the process

TBD reccomendations.

We recommend that the {{ corp\_name }} team reviews the patching recommendations made in the TBD section of the report along with reviewing the provided scans for a full overview of the items to be patched. We also recommend that Demo corp improve their patch management policies and procedures to help prevent potential attacks within their network.

TBD alerts triggered.

Overall, the {{ corp\_name }} network performed as expected for the penetration test. **We recommend that the {{ corp\_name }} team thoroughly review the recommendations made in this report, patch the findings, and re-test annually to improve their overall security posture.**

# Vulnerability summary & report card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

## Internal Penetration Test Findings

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| {{ critical\_vulns }} | {{ high\_vulns }} | {{ moderate\_vulns }} | {{ low\_vulns }} | {{ informational\_vulns }} |
| Critical | High | Moderate | Low | Informational |

{%p for f in finding\_dictionary %}

# Finding {{ f.finding\_counter }}

### Affected IP: **{{ f.ip }}**

### Affected port and service: **{{ f.port }}** (service **{{ f.service }}**)

### Related CVE: **{{ f.cve }}**

### Severity score: **{{ f.cvss }} ({{ f.severity }} severity)**

## **Public exploits related to this finding**

{% for exploit in f.exploits %}

#### Exploit ID: {{ exploit.id }}.

Description: {{ exploit.description }}

Download URL: {{ exploit.url }}

{% endfor %}

## Severity rationale

{{ f.severity\_rationale }}

## Description of the finding

{{ f.description }}

## Mitigation steps

{{ f.mitigation }}

{%p endfor %}