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

TBD

# 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 {{ creation\_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 OF THE ASSESSMENT

## 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 %}** | | | |