Security Assessment Findings Report

[Company Name]

For internal use only.

[Company Name]
Email: email@email.com
Web: http://www.example.com

Date:	Sep 5, 2022
Project:	0
Version:	0.1

Table of Contents

Confidential Statement

This document is the exclusive property of [Company Name] and [Company Name]. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both [Company Name] and [Company Name]. [Company Name] may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Disclaimer

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. [Company Name] prioritized the assessment to identify the weakest security controls an attacker would exploit. Ibex Security recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

Name	Title	Contact Information
Pentester	Lead Penetration Tester	email@email.com
Name	Title	email@email.com

Assessment Overview

From [Date] to [Date], [Company Name] engaged [Company Name] 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 vulnerabilities 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.

Findings Severity Ratings

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 loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Medium	4.0 - 6.9	Vulnerability exists 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 path during the next maintenance window.
Information	N/A	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

Scope	Details
Internal Penetraion Test	10.x.x.x/8

Scope Exclusion

Client Allowances

Executive Summary

Ibex Security evaluated [Company Name] internal security posture through penetration testing from [Date] to [Date]. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

Scoping and Time Limitations

Testing Summary

Tester Notes and Recomendations

Key Strengths and Weaknesses

Vulnerability Summary

Finding	Severity	Recommendations
Example	Critical	Example recommendation.

Technical Findings

[Name]

Description:	Example description.
Risk:	Likelihood: Low – An attacker can discover these vulnerabilities with basic tools. Impact: High – If exploited, an adversary gains code execution, leading to lateral movement across the network.
System:	Example system identified.
Tools Used:	Example tool.
References:	CVE-000-2022

Evidence

Example evidence.

Remediations

Example remediations.

Additional Scans and Findings