Security Assessment Findings Report

**Haigh**

**Test**

Date: 10th of March 2024

Version: 1.0

# Table of Contents

Right-click to update field.

# Confidentiality Statement

This document is the exclusive property of Haigh. This document contains proprietary and confidential information. Duplication, redistribution, or use in whole or in part in any form requires consent of both Haigh and Test. Test 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. Haigh prioritized the assessment to identify the weakest security controls an attacker would exploit. We recommend 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 |
|  |  |  |
|  |  |  |

# Assessment Overview

From 10th of March 2024 to 15th of March 2024, Haigh evaluated the security posture of Test's 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:

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

# 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 | No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation. |

# Scope

|  |  |
| --- | --- |
| Assessment | Details |
| Internal Penetration Test | 10.x.x.x/8 |

## Scope Exclusions

Per client request, {self.company\_name} did not perform any of the following attacks during testing:  
Denial of Service (DoS)  
Phishing/Social Engineering

## Client Allowances

{self.client\_name} provided {self.company\_name} the following allowances:  
Internal access to network via dropbox and port allowances

# Executive Summary

Haigh evaluated Test's internal security posture through penetration testing from 10th of March 2024 to 15th of March 2024. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

## 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 ten business days.

# Testing Summary

The network assessment evaluated {self.client\_name}'s internal network security posture. From an internal perspective, {self.company\_name} performed vulnerability scanning against all IPs provided by {self.client\_name} to evaluate the overall patching health of the network. The team also performed common Active Directory based attacks such as Link-Local Multicast Name Resolution (LLMNR) Poisoning, SMB relaying, IPv6 man-in-the-middle relaying, and Kerberoasting. Beyond vulnerability scanning and Active Directory attacks, {self.company\_name} evaluated other potential risks such as open file shares, default credentials on servers/devices, and sensitive information disclosure to gain a complete picture of the network’s security posture.

The {self.company\_name} team discovered that LLMNR was enabled in the network (Finding IPT-001) which permitted the interception of user hashes via LLMNR poisoning. These hashes were taken offline and cracked via dictionary attacks which signals a weak password policy (Finding IPT-005). Utilizing the cracked passwords, the {self.company\_name} team gained access to several machines within the network which indicates overly permissive user accounts.

With machine access and the use of older operating systems in the network (Finding IPT-009), the team was able to leverage WDigest (Finding IPT-003) to recover cleartext credentials to accounts. The team was also able to dump local account hashes on each machine accessed. The {self.company\_name} team discovered that the local account hashes were being re-used across devices (Finding IPT-002) which lead to additional machine access through pass-the-hash attacks.

Ultimately, the {self.company\_name} team was able to leverage accounts captured through WDigest and hash dumps to move laterally throughout the network until landing on a machine that had a Domain Administrator credential in cleartext via WDigest. The testing team was able to achieve domain admin rights and fully compromise the network.

# Vulnerability Summary & Report Card

A brief summary of the identified vulnerabilities, including their severity and status.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Vulnerability ID | Description | Severity | Status | Notes |
| SQL Injection | Vulnerability in user login form | High | Open | Remediation in progress |
| Cross-Site Scripting (XSS) | Reflected XSS on search page | Medium | Open | Remediation in progress |
| Insecure Direct Object References (IDOR) | Unauthorized access to user profiles | High | Open | Remediation in progress |

# Internal Penetration Test Findings

## SQL Injection - High

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| CWE | Vulnerability in user login form |
| CVSS 3.1 Score | 9.8 |
| Description (Incl. Root Cause) | 2024-06-01 |
| Security Impact | Open |
| Affected Domain | John Doe |
| Remediation | Sanitize inputs and use parameterized queries |
| External References | 2024-06-15 |

### Finding Evidence:

## Cross-Site Scripting (XSS) - Medium

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| CWE | Reflected XSS on search page |
| CVSS 3.1 Score | 6.5 |
| Description (Incl. Root Cause) | 2024-06-02 |
| Security Impact | In Progress |
| Affected Domain | Jane Smith |
| Remediation | Encode output and validate inputs |
| External References | 2024-06-20 |

### Finding Evidence:

## Insecure Direct Object References (IDOR) - High

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| CWE | Unauthorized access to user profiles |
| CVSS 3.1 Score | 8.6 |
| Description (Incl. Root Cause) | 2024-06-05 |
| Security Impact | Open |
| Affected Domain | Mark Lee |
| Remediation | Implement access controls and proper authorization |
| External References | 2024-06-25 |

### Finding Evidence: