

{{Customer Name}}

{{Type of Test}}

Confidential

{{Test Date}}

Contents

[1. Test Details 3](#_Toc105523909)

[1.1. Scope 3](#_Toc105523910)

[1.2. Technical Team 3](#_Toc105523911)

[1.3. Caveats 3](#_Toc105523912)

[1.4. Test Limitations 3](#_Toc105523913)

[2. Finding Information 4](#_Toc105523914)

[2.1. Common Vulnerability Scoring System (CVSS) 4](#_Toc105523915)

[2.2. Severity Ratings 4](#_Toc105523916)

[2.3. Determining Risk 4](#_Toc105523917)

[3. Executive Summary 5](#_Toc105523918)

[3.1. Key Recommendations 5](#_Toc105523919)

[4. Finding Summary 6](#_Toc105523920)

[5. Network Vulnerabilities 7](#_Toc105523921)

[5.1. 7](#_Toc105523922)

[6. Document Control 7](#_Toc105523923)

[7. Appendices 8](#_Toc105523924)

[7.1. Port Scans 8](#_Toc105523925)

1. Test Details

A {{Type of Test}} test was requested for {{Business Name}}.

The network houses server and desktop computers and a test was requested to identify weaknesses.

The web application requires a test to was requested to identify weaknesses.

The mobile application requires a test to was requested to identify weaknesses.

## Scope

All computers in the range {{range}} were in scope for this test.

The web application at the domain {{domain name}} was in scope for this test

The aim was to assess the security of the network, where an attacker could be an external actor gaining access, or an internal employee with malicious intent.

The test was performed between {{Start Date}} and {{End Date}}, taking {{Number of Days}} days in total.

## Technical Team

|  |  |  |
| --- | --- | --- |
| Author Name | Role | Email |
| {{TesterName}} | {{TesterRole}} | {{TesterEmail}} |
|  |  |  |

## Caveats

{{Caveats}}

## Test Limitations

This was a time bound test, meaning that a fixed amount of time was given to perform it. Attackers are not constrained in this way and so may be able to find additional vulnerabilities.

The test results are an indication of the vulnerabilities present at the time of the test. New vulnerabilities arise on an ongoing basis, so keeping systems updated and performing regular penetration tests are recommended.

Testing was limited to technical vulnerabilities, so additional testing, for example social engineering was not performed.

Denial of Service (DoS) testing is not typically performed and was specifically excluded from the scope of this test due to the potential problems it could cause.

# Finding Information

## Common Vulnerability Scoring System (CVSS)

Where relevant, findings in this report come with attached CVSS scores. This communicates characteristics and severity of a vulnerability by detailing various metrics. Links are provided to those calculations to assist with transparency of the severity rating given.

## Severity Ratings

Where CVSS scores are present, severity ratings are directly related to them, based on the following table:

|  |  |
| --- | --- |
| Severity Rating | CVSS Score |
| None / Informational | 0.0 |
| Low | 0.1 – 3.9 |
| Medium | 4.0 – 6.9 |
| High | 7.0 – 8.9 |
| Critical | 9.0 – 10.0 |

Not all findings fit within the CVSS scoring system. If CVSS scores are not present then severity ratings are based on the testers understanding of the issue.

Further information:

* [Common Vulnerability Scoring System User Guide](https://www.first.org/cvss/v3.1/user-guide)

## Determining Risk

A commonly used calculation for risk is:

Risk = Impact \* Likelihood

Impact and likelihood scores will be supplied to give an overall risk score for a vulnerability. These scores are indicative of risk to the business.

Scores are given from 1 – 3 (low to high) for both impact and likelihood, meaning all risks are assessed to be between 1 (very low risk) and 9 (very high risk)

An example would give a finding a medium impact (2) and a high likelihood (3), making the calculation:

Risk = 2 \* 3 = 6

# Executive Summary

During the test, it was possible to:

* {{Bullet List of Key Vulnerabilities}}

{{Detail Chained Attacks / detail Key Vulnerabilities}}

## Key Recommendations

#### Patching Policy

Patching is of critical importance on a network, requiring a structured approach to ensure operating systems and services are patched in a timely manner.

#### Password Hygiene

Weak passwords, especially for high privileged accounts are also critical to the defensive posture of a network. Passwords for all accounts should be strong, with an even greater importance being placed on privileged accounts.

#### Excessive File Share Access

Network shares should be used carefully, with strict access control being applied if confidential information is stored on them. Additionally, credentials should never be stored as plaintext within documents. Software such as password managers can be used to effectively store and even share credentials if a small pool of people require access to them.

# Finding Summary

Below is an overview of the findings in this report:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Title | CVSS Score | CVSS Rating | Indicative Risk |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Below is a graph to indicate the spread of findings by CVSS rating:

Figure 1 Penetration test – vulnerability totals

# Network Vulnerabilities

## 

# Document Control

|  |  |  |
| --- | --- | --- |
| Name | Date | Comments |
|  |  | Initial draft |
|  |  |  |
|  |  |  |

# Appendices

## Port Scans

Port scanning was performed using the tool [nmap](https://nmap.org/).

The following command was used to scan the environment:

|  |
| --- |
| nmap -sSV {{IpRange}} |

This resulted in the following open ports discovered on the network:

|  |  |  |  |
| --- | --- | --- | --- |
| IP Address | Port | Service | Version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |