

{name}

Network Penetration Test

Confidential

{date | convertDateLocale: 'us': 'full'}

Contents

[1. Test Details 3](#_Toc104729603)

[1.1. Scope 3](#_Toc104729604)

[Technical Team 3](#_Toc104729605)

[1.2. Test Limitations 3](#_Toc104729606)

[2. Finding Information 4](#_Toc104729607)

[Common Vulnerability Scoring System (CVSS) 4](#_Toc104729608)

[2.1. Severity Ratings 4](#_Toc104729609)

[2.2. Determining Risk 4](#_Toc104729610)

[3. Executive Summary 5](#_Toc104729611)

[3.1. Key Recommendations 5](#_Toc104729612)

[4. Finding Summary 6](#_Toc104729613)

[5. Network Vulnerabilities 7](#_Toc104729614)

[5.1. {title} 7](#_Toc104729615)

[5.1.1. Vulnerability Description 7](#_Toc104729616)

[5.2. Vulnerability Detail 7](#_Toc104729617)

[5.2.1. Remediation Advice 7](#_Toc104729618)

# Test Details

A network penetration test was requested for the Carved Rock Fitness internal network. The network houses server and desktop computers and a test was requested to identify weaknesses.

## Scope

All computers in the range {-w:p scope}{name}{/scope} were 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 {date\_start | convertDateLocale} and {date\_end | convertDateLocale}.

## Technical Team

|  |  |  |
| --- | --- | --- |
| Author Name | Role | Email |
| {creator.firstname} {creator.lastname} | Penetration Tester | {creator.email} |
|  |  |  |

## 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 the network, 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

{#executivesummary.text}

{@text | convertHTML}

{#images}

{%image}

Image 1 – {caption}

{/images}

{/executivesummary.text}

## Key Recommendations

{#executivesummary.recommendations}

{@text | convertHTML}

{#images}

{%image}

Image 1 – {caption}

{/images}

{/executivesummary.recommendations}

# Finding Summary

Below is an overview of the findings in this report:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Title | CVSS Score | CVSS Rating | Indicative Risk |
| {#findings}{#cvss.baseSeverity == 'Critical'}{identifier} | {title} | {#cvss} {baseMetricScore} | {baseSeverity} {/cvss}  {/cvss.baseSeverity == 'Critical'} {/findings} |  |
| {#findings}{#cvss.baseSeverity == 'High'}{identifier} | {title} | {#cvss} {baseMetricScore} | {baseSeverity} {/cvss}  {/cvss.baseSeverity == 'High'} {/findings} |  |
| {#findings}{#cvss.baseSeverity == 'Medium'}{identifier} | {title} | {#cvss} {baseMetricScore} | {baseSeverity} {/cvss}  {/cvss.baseSeverity == 'Medium'} {/findings} |  |
| {#findings}{#cvss.baseSeverity == 'Low'}{identifier} | {title} | {#cvss} {baseMetricScore} | {baseSeverity} {/cvss}  {/cvss.baseSeverity == 'Low'} {/findings} |  |
| {#findings}{#cvss.baseSeverity == 'None'}{identifier} | {title} | {#cvss} {baseMetricScore} | {baseSeverity} {/cvss}  {/cvss.baseSeverity == 'None'} {/findings} |  |

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

Graph

# Network Vulnerabilities

{#findings}

## {title}

{#cvss}

**Severity**: {baseSeverity} **CVSS Score**: {baseMetricScore}

**CVSS Calculation**: {vectorString}

**Likelihood** : Calculate **Impact** : Calculate **Risk**: Calculate

{/cvss}

### Vulnerability Description

{#description}

{@text | convertHTML}

{#images}

{%image}

Image 1 – {caption}

{/images}

{/description}

### Vulnerability Detail

{#observation}

{@text | convertHTML}

{#images}

{%image}

Image 1 – {caption}

{/images}

{/observation}

### Remediation Advice

{#remediation}

{@text | convertHTML}

{#images}

{%image}

Image 1 – {caption}

{/images}

{/remediation}

Further information:

{#references}

* {.}

{/references}

{/findings}

Document Control

|  |  |  |
| --- | --- | --- |
| Name | Date | Comments |
| {creator.firstname} {creator.lastname} | {date | convertDateLocale} | Initial draft |
|  |  |  |
|  |  |  |