Cyber Teen Camp 2025

Security Assessment Findings Report

Team XXX

Copyright © 2022 Cyber Teen Camp Ltd. All rights reserved.

No part of this publication, in whole or in part, may be reproduced, copied, transferred or any other right reserved to its copyright owner, including photocopying and all other copying, any transfer or transmission using any network or other means of communication, any broadcast for distant learning, in any form or by any means such as any information storage, transmission or retrieval system, without prior written permission from Cyber Teen Camp.

## Table of Contents

Contents

[Business Confidential 2](#_heading=h.46r0co2)

[Table of Contents 3](#_heading=h.30j0zll)

[Confidentiality Statement 4](#_heading=h.3znysh7)

[Disclaimer 4](#_heading=h.3dy6vkm)

[Contact Information 4](#_heading=h.4d34og8)

[Assessment Overview 5](#_heading=h.3rdcrjn)

[Assessment Components 5](#_heading=h.lnxbz9)

[Internal Penetration Test 5](#_heading=h.44sinio)

[Finding Severity Ratings 7](#_heading=h.z337ya)

[Risk Factors 7](#_heading=h.1y810tw)

[Likelihood 7](#_heading=h.2xcytpi)

[Impact 7](#_heading=h.3whwml4)

[Scope 8](#_heading=h.qsh70q)

[Scope Exclusions 8](#_heading=h.1pxezwc)

[Client Allowances 8](#_heading=h.2grqrue)

[Executive Summary 9](#_heading=h.3o7alnk)

[Significant Findings and Business Impact 9](#_heading=h.5d2wbc3qla0m)

[Scoping and Time Limitations 9](#_heading=h.m9rihdy3ul1)

[Testing Summary 9](#_heading=h.ihv636)

[Tester Notes and Recommendations 9](#_heading=h.ihv636)

[Key Strengths and Weaknesses 10](#_heading=h.1hmsyys)

[Vulnerability Summary & Report Card 10](#_heading=h.2grqrue)

[Penetration Test Findings 10](#_heading=h.3fwokq0)

[Informational Findings 11](#_heading=h.xd7tib9qgiks)

[Company Preparedness to Accept Penetration Test 11](#_heading=h.d2rgptub4vk1)

[Technical Findings 11](#_heading=h.xd7tib9qgiks)

[External Penetration Test Findings 11](#_heading=h.2u6wntf)

[Internal Penetration Test Findings 13](#_heading=h.nmf14n)

[Additional Scans and Reports 17](#_heading=h.1mrcu09)

# Confidentiality Statement

This document is the exclusive property of Cyber Teen Camp (CTC). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of CTC and XXXXX.

XXXXX may share this document with auditors under non-disclosure agreements to show 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. CTC prioritized the assessment to identify the weakest security controls an attacker would exploit. CTC recommends conducting similar assessments annually by internal or third-party assessors to ensure the continued success of the controls.

# Contact Information

|  |  |  |
| --- | --- | --- |
| **Name** | **Title** | **Contact Information** |
| CyberTronics Inc. | | |
| XXXXXX | XXXXXX | Email: xxxxx |
| Cyber Teen Camp | | |
| XXXXXXX | Lead Penetration Tester | Email: xxxxxxx |

# Assessment Overview

**Goals**

The penetration test assessed the security posture of CyberTronics Inc.’s external and internal networks. The goal was to identify vulnerabilities, evaluate the risk associated with each, and recommend mitigations to enhance overall security. The testing was performed against:

**Details**

* Web Application: http://<IP>
* Internal Network: 172.18.0.4

**Testing Objectives**

* Identify security weaknesses within CyberTronics' infrastructure.
* Exploit identified vulnerabilities to demonstrate their potential impact.
* Simulate an attacker’s ability to maintain persistence within the network.
* Provide actionable remediation steps.

# Executive Summary

From XXXX XX, 20XX to XXXX XX, 20XX, CTC engaged XXXX to assess its security posture through internal network penetration testing based on the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and other customized frameworks. The objectives of the test aligned with the following business objectives, \_\_\_\_. During the assessment, Cyber Teen Camp identified critical vulnerabilities that \_\_\_\_. These weaknesses were easily detected through basic reconnaissance and required minimal effort to exploit. Subsequent sections offer a detailed overview of the discovered vulnerabilities, attempts made, and the overall strengths and weaknesses.

### Significant Findings and Business Impact

* First significant finding and how it impacts the business (ex. Password Policies, changes to tech, org structure - xxxx)
  + Revising and/or creating a strict password policy would have prevented the active directory and network from being compromised so easily.
* Second significant finding and how it impacts the business
* Third significant finding and how it impacts the business
* Fourth significant finding and how it impacts the business
* Fifth significant finding and how it impacts the business
* Sixth significant finding and how it impacts the business

### 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. Penetration testing was permitted for one (1) business day (June 2nd, 2022, to June 7th, 2022)

### Summary of Recommendations

Many of the findings discovered are vulnerabilities within XXXXXX. We recommend …

During testing, we discovered multiple vulnerabilities such as …

# 

# 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. We provide additional information 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. We give ratings based on the difficulty of the attack, the 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

|  |  |
| --- | --- |
| **Assessment** | **Details** |
| Internal Penetration Test | XXX.XXX.XXX.X/24 |
| External Penetration Test | XXX.XXX.XXX.X/24 |

### Scope Exclusions

Per client request, CTC did not perform any of the following attacks during testing:

* Denial of Service (DoS).
* Phishing/Social Engineering.

# Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

### Penetration Test Findings

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ? | ? | ? | ? | ? |
| Critical | High | Moderate | Low | Informational |

|  |  |  |
| --- | --- | --- |
| **Finding** | **Severity** | **Recommendation** |
| IPT-001: XXXX | High |  |
| IPT-002: XXXX | Critical |  |
| IPT-003: XXXX | Moderate |  |

# Technical Findings

### External Penetration Test Findings

**Finding IPT-001:** (Example) Weak Password

|  |  |
| --- | --- |
| Description: | Upon scanning the system, there was an exposed webserver that displayed a username and password. Using scanning tools, the login screen was easily bypassed due a weak password. |
| Risk: | High |
| System: | 172.18.0.3 |
| Tools Used: | Burpsuite, Hydra |
| References: |  |

**Evidence**

*Figure X: XXX*

*Figure X: XXX*

**Remediation**

Use stronger passwords and develop a password policy that has at least 12 characters, upper and lower case, along with special characters.

**Finding IPT-002:** XX

|  |  |
| --- | --- |
| Description: |  |
| Risk: | Likelihood:  Impact: |
| System: |  |
| Tools Used: |  |
| References: |  |

**Evidence**

*Figure X:*

**Remediation**

**Finding IPT-003:**

|  |  |
| --- | --- |
| Description: |  |
| Risk: | Likelihood:  Impact: |
| System: |  |
| Tools Used: |  |
| References: |  |

**Evidence**

*Figure X:*

*Figure X:*

**Remediation**

### Internal Penetration Test Findings

**Finding IPT-004:**

|  |  |
| --- | --- |
| Description: |  |
| Risk: | Likelihood:  Impact: |
| System: |  |
| Tools Used: |  |
| References: |  |

**Evidence**

*Figure X:*

*Figure X:*

**Remediation**

**Finding IPT-005:**

|  |  |
| --- | --- |
| Description: |  |
| Risk: | Likelihood:  Impact: |
| System: |  |
| Tools Used: |  |
| References: |  |

**Evidence**

*Figure X:*

*Figure X:*

**Remediation**

**Finding IPT-006:**

|  |  |
| --- | --- |
| Description: |  |
| Risk: | Likelihood:  Impact: |
| System: |  |
| Tools Used: |  |
| References: |  |

**Evidence**

*Figure X:*

**Remediation**

**Finding IPT-007:**

|  |  |
| --- | --- |
| Description: |  |
| Risk: | Likelihood:  Impact: |
| System: |  |
| Tools Used: |  |
| References: |  |

**Evidence**

*Figure X:*

**Remediation**

**Finding IPT-008:**

|  |  |
| --- | --- |
| Description: |  |
| Risk: | Likelihood:  Impact: |
| System: |  |
| Tools Used: |  |
| References: |  |

**Evidence**

*Figure 16: Windows screen with IP and Username*

**Remediation**

**Finding IPT-009:**

|  |  |
| --- | --- |
| Description: |  |
| Risk: | Likelihood:  Impact: |
| System: |  |
| Tools Used: |  |
| References: |  |

**Evidence**

**Remediation**

**Finding IPT-10:**

|  |  |
| --- | --- |
| Description: |  |
| Risk: | Likelihood:  Impact: |
| System: |  |
| Tools Used: |  |
| References: |  |

**Evidence**

*Figure X:*

**Remediation**

### 

### Additional Scans and Reports

Last Page