CPTC Report Template

**Penetration Test Report Template**

For the []

Penetration Testers

Region: So Cal

Team #??

**BUSINESS CONFIDENTIAL**

Table of Contents

Table of Contents 2

Confidentiality Statement 3

Disclaimer 3

Contact Information 3

Assessment Overview 4

Assessment Components 4

Internal Penetration Test 4

Finding Severity Ratings 5

Risk Factors 5

Likelihood 5

Impact 5

Scope 6

Scope Inclusions 6

Executive Summary 7

Scoping and Time Limitations

Testing Summary

Tester Notes and Recommendations

Key Weaknesses

Vulnerability Summary and Report Card

Internal Penetration Test Findings

Technical Findings

Internal Penetration Test Findings

IPT001:

IPT002:

IPT003:

IPT004:

IPT005:

IPT006:

IPT007:

IPT008:

**Confidentiality Statement**

This document is the exclusive property of **Team Name**. This document contains proprietary and confidential information. The duplication, redistribution, or use in whole or in part, in any form whatsoever, requires consent of both **Team Name** and company name.

**Team 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. Therefore, the findings and recommendations in this report reflect the information gathered during the assessment and not any changes or modifications made outside that period.

Time-limited engagements do not allow for a full evaluation of all security controls. **Team name** prioritized the assessment to identify the weakest security controls a threat actor would exploit. **Team name** recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

**Executive Summary**

(Explain our most pressing findings and urgent recommendations. )

**Team name** evaluated [Organizer]s internal security posture through penetration testing **Insert Date**. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

**Assessment Overview**

Phases of internal network penetration testing activities include the following steps.

* Planning: Customer goals are gathered, and the rules of engagement (RoE) document is obtained.
* Discovery: Performing scanning and enumeration to identify potential vulnerabilities/weak areas within the network to exploit.
* Attack: Confirming potential vulnerabilities through exploitation and performing additional discovery upon new access
* Reporting: Documenting all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses

A diagram of a flowchart

Description automatically generated

**Assessment Components**

**Internal Penetration Test**

An internal penetration test emulates the role of a threat actor from inside the network. A penetration tester will scan the network to identify vulnerabilities and perform common and advanced internal network attacks. The penetration tester will seek to gain access to hosts through various exploitation techniques.

**CVSS (Common Vulnerability Scoring System)**

CVSS scoring involves how much impact the vulnerability has on a system (severity level) and how much of a compromised system's threat is toward a client (risk level). They are assessed using the table below via CVSS v3.1:

| Rating | Score | Description |
| --- | --- | --- |
| Critical | 9.0-10.0 | Vulnerability poses a severe and immediate threat to the organization and needs immediate remediation |
| High | 7.0-8.9 | Vulnerability poses a major threat to the organization and needs to be prioritized in remediation |
| Moderate | 4.0-6.9 | Vulnerability poses a moderate threat to the organization and will need to be remediated |
| Low | 0.1-3.9 | Vulnerability may pose a threat to the organization and needs further investigation for remediation |
| Informational | \*.\* | Informational finding |

*(Source:* [*https://www.first.org/cvss/v3.1/specification-document*](https://www.first.org/cvss/v3.1/specification-document)*,* [*https://www.sentinelone.com/cybersecurity-101/cybersecurity/cvss-common-vulnerability-scoring-system/*](https://www.sentinelone.com/cybersecurity-101/cybersecurity/cvss-common-vulnerability-scoring-system/)*)*

**Likelihood**

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the publicly available tools, the attacker skill level, and the client environment.

**Impact**

Impact measures the potential vulnerability’s effect on business operations, up to and including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

**Scope**

| **Assessment** | **Details** |
| --- | --- |
| Internal Penetration Test | Insert IPs here |

**Scope Exclusions**

Per client request, 5th Pin Security did not perform any of the following attacks during testing:

* Denial of Service (DoS)
* Social engineering (aside from the phishing exercise)
* All other attacks not specified above were permitted by [Organizers]

**Scoping and Time Limitations**

Scoping during the engagement did not permit denial of service attacks.

Time limitations were also in place for testing. Internal network penetration testing was permitted for 1 business day.

**Testing Summary**

**Tester Notes and Recommendations**

**Key Weaknesses**

The following identifies the key weaknesses identified during the assessment:

**Vulnerability Summary and Report Card**

The following tables illustrates the vulnerabilities found by impact and recommended remediations.

**Internal Penetration Test Findings**

| **0** | **0** | **0** | **0** | **0** |
| --- | --- | --- | --- | --- |
| **Critical** | **High** | **Moderate** | **Low** | **Informational** |

| **Finding** | **Severity** | **Recommendation** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Technical Findings**

**Internal Penetration Test Findings**

**Finding IPT-001**

| **Description** |  |
| --- | --- |
| **Risk** |  |
| **System** |  |
| **Tools Used** |  |
| **References** |  |

**Evidence**

**Remediation**

**Internal Penetration Test Findings**

**Finding IPT-002**

| **Description** |  |
| --- | --- |
| **Risk** |  |
| **System** |  |
| **Tools Used** |  |
| **References** |  |

**Evidence**

**Remediation**

**Internal Penetration Test Findings**

**Finding IPT-003**

| **Description** |  |
| --- | --- |
| **Risk** |  |
| **System** |  |
| **Tools Used** |  |
| **References** |  |

**Evidence**

**Remediation**

**Internal Penetration Test Findings**

**Finding IPT-004**

| **Description** |  |
| --- | --- |
| **Risk** |  |
| **System** |  |
| **Tools Used** |  |
| **References** |  |

**Evidence**

**Remediation**

**Internal Penetration Test Findings**

**Finding IPT-005**

| **Description** |  |
| --- | --- |
| **Risk** |  |
| **System** |  |
| **Tools Used** |  |
| **References** |  |

**Evidence**

**Remediation**

**Internal Penetration Test Findings**

**Finding IPT-006**

| **Description** |  |
| --- | --- |
| **Risk** |  |
| **System** |  |
| **Tools Used** |  |
| **References** |  |

**Evidence**

**Remediation**

**Internal Penetration Test Findings**

**Finding IPT-007**

| **Description** |  |
| --- | --- |
| **Risk** |  |
| **System** |  |
| **Tools Used** |  |
| **References** |  |

**Evidence**

**Remediation**

**Internal Penetration Test Findings**

**Finding IPT-008**

| **Description** |  |
| --- | --- |
| **Risk** |  |
| **System** |  |
| **Tools Used** |  |
| **References** |  |

**Evidence**

**Remediation**