**Security Blue Team**

*2024 Security Assessment Report Template*

[Company Name]

By:[Insert Name]

Report Issue: <TEST DATE>

## Confidentiality Notice

*This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. Publication of this report may cause reputational damage to [Insert Company Name] or facilitate attacks against [Insert Company Name]. [Company Name] shall not be held liable for special, incidental, collateral or consequential damages arising out of the use of this information.*

## Disclaimer

*Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope of the engagement. This report is a summary of the findings from a “point-in-time” assessment made on [Insert Company Name] environment. Any changes made to the environment during the period of testing may affect the results of the assessment.*

**TABLE OF CONTENTS**

[**EXECUTIVE SUMMARY**](#_heading=h.tyjcwt) **4**

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

**RISK CLASSIFICATIONS 5**

Exploitation Likelihood

**PROCEDURE STEPS 6**

Phases 6

[**SCOPE**](#_heading=h.44sinio) **7**

[Networks](#_heading=h.2jxsxqh) 7–8

**TOOLS & CONFIGS USED 9**

**REPORTING AND MONITORING 10**

[**ENGAGEMENT INFORMATION**](#_heading=h.147n2zr) **11**

[Client Information](#_heading=h.3o7alnk) 11

[Version Information](#_heading=h.23ckvvd) 11

[Contact Information](#_heading=h.ihv636) 11

**FINDINGS** **12–39**

# 

# EXECUTIVE SUMMARY

[Company Name] performs a security assessment of the internal corporate network of *[Insert Company Name]* on a monthly basis. [Company Name]’s vulnerability test attempts to expose vulnerable access to systems within the *[Insert Company Name]’* corporate network. The purpose of this assessment was to discover and identify vulnerabilities in *[Insert Company Name]* infrastructure and suggest methods to remediate the vulnerabilities. [Company Name] identifies vulnerabilities within the scope of the engagement which are broken down by the critical severity.

The highest severity vulnerabilities give potential attackers the opportunity to steal sensitive data such as documentation of business processes and trade secrets or contact or contact information for employees and customers. Data breaches can cause employee productivity issues, regulatory fines, customers abandoning your business, and loss in revenue. In order to ensure data confidentiality, integrity, and availability, security remediations should be implemented as described in the security assessment findings.

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope. Any changes made to the environment during the period of testing may affect the results of the assessment.

## Risk Classifications

| **Level** | **Score** | **Description** |
| --- | --- | --- |
| **Critical** | **10** | The vulnerability poses an immediate threat to the organization. Successful exploitation may permanently affect the organization. Remediation should be immediately performed. |
| **High** | **7-9** | The vulnerability poses an urgent threat to the organization, and remediation should be prioritized. |
| **Medium** | **4-6** | Successful exploitation is possible and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible. |
| **Low** | **1-3** | The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible. |
| **Informational** | **0** | These findings have no clear threat to the organization, but may cause business processes to function differently than desired or reveal sensitive information about the company. |

## Exploitation Likelihood Classifications

| **Likelihood** | **Description** |
| --- | --- |
| **Likely** | Exploitation methods are well-known and can be performed using publicly available tools. Low-skilled attackers and automated tools could successfully exploit the vulnerability with minimal difficulty. |
| **Possible** | Exploitation methods are well-known, may be performed using public tools, but require configuration. Understanding of the underlying system is required for successful exploitation. |
| **Unlikely** | Exploitation requires deep understanding of the underlying systems or advanced technical skills. Precise conditions may be required for successful exploitation. |

# 

# **Procedure Steps**

Discovery Phase:

● **Vulnerabilities identified across all in scope devices**

1. Launch Nessus by testing each port on a computer

2. Identify open ports and services running on scanned systems

3. Correlate system information with known vulnerabilities

Prioritization Phase:

● **Discovered vulnerabilities and assets are reviewed, prioritized, and assessed**

**using results from technical and risk reports.**

1. After vulnerabilities are identified, they will need to be evaluated so the risks posed

by them are dealt with appropriately.

Planning Phase:

● **Mitigation efforts are devised.**

1. Keep software/hardware updated.

2. Eliminate unwanted hardware and software.

3. Restrict access to protected information.

Remediation Phase:

● **Vulnerabilities are addressed after they have been validated and deemed a**

**risk. Different ways to treat the vulnerability will be examined.**

1. Remediation: Fully fixing or patching a vulnerability so it can’t be exploited.

2. Mitigation: Lessing the likelihood and/of impact of a vulnerability being exploited.

3. Acceptance: Taking no action to fix or otherwise lessen the likelihood/impact of a

vulnerability being exploited.

Validation Phase:

● **Successful remediation measures are determined by subsequent analysis.**

1. Observe the changes in policy to determine your security posture score and act

accordingly.

2. A security posture is the overall security status of a company's network.

# SCOPE

All testing was based on the scope as defined in the Request For Proposal (RFP) and official written communications. The items in scope are listed below.

## Networks

| **Network** | **Note** |
| --- | --- |
| [Enter Client’s IP] | [Location/Site] |
| [Enter Client’s IP] | [Location/Site] |
| [Enter Client’s IP] | [Location/Site] |
| [Enter Client’s IP] | [Location/Site] |
| [Enter Client’s IP] | [Location/Site] |
| [Enter Client’s IP] | [Location/Site] |
| [Enter Client’s IP] | [Location/Site] |
| [Enter Client’s IP] | [Location/Site] |
| [Enter Client’s IP] | [Location/Site] |
| [Enter Client’s IP] | [Location/Site] |
| [Enter Client’s IP] | [Location/Site] |
| [Enter Client’s IP] | [Location/Site] |
| [Enter Client’s IP] | [Location/Site] |
| [Enter Client’s IP] | [Location/Site] |
| [Enter Client’s IP] | [Location/Site] |
| [Enter Client’s IP] | [Location/Site] |
| [Enter Client’s IP] | [Location/Site] |
| [Enter Client’s IP] | [Location/Site] |
| [Enter Client’s IP] | [Location/Site] |
| [Enter Client’s IP] | [Location/Site] |
| [Enter Client’s IP] | [Location/Site] |
| [Enter Client’s IP] | [Location/Site] |
| [Enter Client’s IP] | [Location/Site] |
| [Enter Client’s IP] | [Location/Site] |
| [Enter Client’s IP] | [Location/Site] |

# APPENDIX A - TOOLS USED

| **TOOL** | **DESCRIPTION** |
| --- | --- |
| **XXXX** | [Enter Description] |
| **XXXX** | [Enter Description] |

***Table A.1:*** *Tools used during assessment*

APPENDIX A - Tool Configurations

| **Configurations - XX/XX/XXXX** |
| --- |
| [Enter Configuration] |
| [Enter Configuration] |
| [Enter Configuration] |
| [Enter Configuration] |
| [Enter Configuration] |

**Reporting and Monitoring**

The main aspect of reporting is to keep in mind that it must be easy to read

and logically set up so that the sequence of testing flows. The list of

remedial actions should be clearly defined. A standard documentation of

vulnerability format usually includes the following:

● The scope of the report: This explains what needed to be tested and how it was

tested.

● Risk: The probability of exposure or loss resulting from a cyber-attack or data breach

on your organization.

● Host: This is any hardware device that has the capability of permitting access to a

network via a user interface, specialized software, network address, protocol stack,

or any other means.

● Port: A software-defined number associated with a network protocol that receives or

transmits communication for a specific service.

● Vulnerability Name: A flaw or weakness in a computer system, its security

procedures, internal controls, or design that can be exploited.

● Device: A thing made for a particular purpose.

● Summary: A brief statement or account of the main points of something

● Solution: A means of solving a problem or dealing with a difficult situation.

**[Note to reporter: Feel free to delete this page before sending this to the client. It is an reminder for you on the reporting process. Do forget to edit the TOC! ]**

# ENGAGEMENT INFORMATION

## Client Information

| **Client** | [Insert Company Name] |
| --- | --- |
| **Primary Contact** | [Insert Name] (Insert Role) (XXX) XXX-XXX  [Enter Client Email] |
| **Approvers** | The following people are authorized to change the scope of engagement and modify the terms of the engagement   * [Insert Name] * [Insert Name]] |

## Version Information

| **Version** | **Date** | **Description** |
| --- | --- | --- |
| 1.0 | <DATE HERE> | Initial report to client |

## Contact Information

| **Name** | [Company Name] |
| --- | --- |
| **Address** | [Enter Address] |
| **Phone** | (XXX) XXX-XXX |
| **Email** | [Enter Contact Email] |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |

**Location:** <Example>



| **RISK** |  |
| --- | --- |
| **HOST** |  |
| **PORT** |  |
| **VULN NAME** |  |
| **DEVICE** |  |
| **SUMMARY** |  |
| **SOLUTION** |  |