

Risk and vulnerability Assessment Report (Draft)

{REPORT SUBTITLE}

{ DATE }

If {Stakeholder Name}, wishes to create and distribute derivatives of this report (such as summaries of this report or {Stakeholder Name}’s commentary on the report’s recommendations), {Stakeholder Name} should (1) provide notice to the originator before distributing such derivatives; (2) clearly mark derivatives so that it is clear that {Stakeholder Name} created them and so that they cannot be mistaken for documents from the originator’s organization; and (3) refrain from affixing the originator’s logo or proprietary markings to the derivatives, unless {Stakeholder Name} has obtained written permission to do so from the originator’s organization.

Table of Contents

[Executive Summary 3](#_Toc132382702)

[Scope 7](#_Toc132382703)

[Methodology 7](#_Toc132382704)

[Findings 8](#_Toc132382705)

[Attack Paths 12](#_Toc132382706)

[Appendix A: Severity Rating Criteria 12](#_Toc132382707)

[Appendix B: External Port Mapping 13](#_Toc132382708)

[APPENDIX C: Narrative 14](#_Toc132382709)

[Appendix D: Password Analysis 14](#_Toc132382710)

[Appendix E: Abbreviations and Acronyms 15](#_Toc132382711)

Tables

[Table 1: Summary of Findings, Severity, and Mitigation Status 8](#_Toc143177276)

[Table 2: Recommendations Based on CIS Controls 9](#_Toc143177277)

[Table 3: Severity Rating Descriptions 10](#_Toc143177278)

[Table 4: Open Ports and Services on External Systems 11](#_Toc143177279)

Figures

[Figure 1: Risk Score and Findings Breakdown 4](#_Toc131417989)

[Figure 2: Most Frequently Cited NIST Controls 5](#_Toc131417990)

[Figure 3: NIST Cybersecurity Framework Controls 6](#_Toc131417991)

# Executive Summary

## Overview

The security team conducted a Risk and Vulnerability Assessment (RVA) at the request of {Stakeholder Name} ({Stakeholder Initials}). {Team Lead Name} ({Team Lead Email}) led the assessment remotely from {External Start Date} to {External End Date} and on site at {Stakeholder Location} from {Internal Start Date} to {Internal End Date}. This report only covers the targets described within and makes no claims about the security of any system that was deemed out of scope or was not tested during this engagement.

### Significant Findings

During testing, the security team identified the following significant findings:

{SIGNIFICANT FINDINGS}

### Recommendations

Based on the significant findings listed above, the security team recommends the following high-level actions:

{ RECOMMENDATIONS }

### Observed Strengths

In addition to the findings described throughout this report, the security team also observed the following strengths pertaining to the {Stakeholder Name} network and personnel:

{OBSERVED STRENGTHS}

## Risk Score

The security team derives a risk score from each finding based on factors related to impact and likelihood. Together, these factors help determine risk from a technical standpoint and make no assumptions about specific threat actors or the business elements of risk.

From the findings, a **Total Risk Score** is calculated and can be used to measure progress as findings are mitigated. In the event that a finding was mitigated during the assessment timeframe and the security team was able to validate mitigation, the **Mitigated Risk Score** is used to represent the deduction of mitigated findings.

Below are the calculated risk scores and a breakdown of findings by severity:

{Table: Risk Score}

Figure 1: Risk Score and Findings Breakdown

{FINDINGS SUMMARY}

## NIST-Based Summary

The security team mapped all findings to applicable National Institute of Standards and Technology (NIST) controls as described in [NIST Special Publication (SP) 800-53](https://csrc.nist.gov/Projects/risk-management/sp800-53-controls). Figure 2 illustrates the relevant control families cited based on findings. Please refer to NIST SP 800-53 for a full list of control families. The Findings section of this report provides specific mappings of controls to findings and the detailed technical description for each finding. Note that some findings may be mapped to multiple applicable NIST controls.

{NIST CONTROLS}

Figure 2: Number of Findings Mapped to NIST Controls

### Control Family Abbreviations and Definitions

|  |  |  |  |
| --- | --- | --- | --- |
| **AC** | Access Control | **PE** | Physical and Environmental Protection |
| **AT** | Awareness and Training | **PL** | Planning |
| **AU** | Audit and Accountability | **PM** | Program Management |
| **CA** | Assessment, Authorization, and Monitoring | **PS** | Personnel Security |
| **CM** | Configuration Management | **PT** | Personally Identifiable Information Processing and Transparency |
| **CP** | Contingency Planning | **RA** | Risk Assessment |
| **IA** | Identification and Authentication | **SA** | System and Services Acquisition |
| **IR** | Incident Response | **SC** | System and Communications Protection |
| **MA** | Maintenance | **SI** | System and Information Integrity |
| **MP** | Media Protection | **SR** | Supply Chain Risk Management |

## NIST Cybersecurity Framework

RVA findings are mapped to the NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 16, 2018, called the [Cybersecurity Framework](https://www.nist.gov/cyberframework). Figure 3 illustrates the relevant functions and categories cited based on findings. Please refer to the NIST Cybersecurity Framework for a full list of functions and categories. The Findings section of this report provides specific mappings of categories to findings and detailed technical descriptions for each finding. Note that some findings may be mapped to multiple applicable NIST categories.

{NIST CSF}

Figure 3: NIST Cybersecurity Framework Categories

### Function and Category Abbreviations and Definitions

|  |  |  |  |
| --- | --- | --- | --- |
| **DE** | Detect | **PR** | Protect |
| **ID** | Identify | **RS** | Respond |

|  |  |  |  |
| --- | --- | --- | --- |
| **AC** | Identity Management and Access Control | **GV** | Governance |
| **AE** | Anomalies and Events | **IP** | Information Protection Processes and Procedures |
| **AM** | Asset Management | **MA** | Maintenance |
| **AT** | Awareness and Training | **MI** | Mitigation |
| **CM** | Security Continuous Monitoring | **PT** | Protective Technology |
| **DP** | Detection Processes | **RA** | Risk Assessment |
| **DS** | Data Security | **SC** | Supply Chain Risk Management |

# Scope

## Phishing

{PHISHING USERS}

{PHISHING DOMAINS}

## External

{EXTERNAL HOSTS}

{EXTERNAL SCOPE}

## Internal

{INTERNAL HOSTS}

{INTERNAL SCOPE}

# Methodology

The Risk and Vulnerability Assessment consists of several phases detailed in the subsequent sections. At a high level, the RVA methodology involves:

* Gathering relevant information about the target organization and its assets.
* Conducting vulnerability scanning of in-scope assets.
* Manually analyzing in-scope assets and collected data.
* Validating findings, including chaining together multiple vulnerabilities and misconfigurations where possible, in order to elevate privileges and access, or otherwise demonstrate significant impact;
* Providing actionable deliverables to the stakeholder, including an out brief, final report, and raw assessment data

The security team utilizes this methodology from different contexts, dependent on the stakeholder’s interests and accommodations, as well as the security team’s ability to obtain various levels of access. The scenarios by which the security team conducts testing may include:

* External to the stakeholder’s network, with no assumed access to assets or accounts other than what is accessible to the public.
* Leveraging the access of a phished user in a standard phishing campaign.
* Leveraging the credentials of a phished user in a credential harvesting campaign.
* Internal to the stakeholder’s network, with no initial access to the domain.
* Access to the domain via a low privilege account.
* Access to the domain via a privileged account

# Findings

### The security team identified the following findings as potentially exploitable conditions that could lead to compromise of the confidentiality, integrity, and/or availability of the tested environment. Each finding includes a description, supporting details, and recommended steps for mitigation. The {Stakeholder Name} team should review the findings and recommendations for technical weaknesses, shortcomings in processes and procedures, and systemic weaknesses in overall security posture.

### Severity can be used to prioritize mitigation of findings. However, {Stakeholder Name} is best equipped to develop a mitigation strategy based on business impact and priorities. Mitigation Status indicates whether a finding was mitigated during the assessment timeframe and is only adjusted when the security team can confidently validate that the finding was mitigated.

## Findings Summary

{Table: Findings Summary}

Table 1: Summary of Findings, Severity, and Mitigation Status

### See [Appendix A](#APPA) for the criteria used to determine severity (Critical/High/Medium/Low/Informational).

## Detailed Findings

{Table: Detailed Findings}

## General Recommendations

To support the security team’s goal of helping stakeholders improve their security posture, the assessment team identified general recommendations based on the Center for Internet Security’s (CIS) Critical Security Controls for mitigating the risks discovered. Table 1 represents a high-level summary of prioritized recommended remediations and the associated findings. As always, {Stakeholder Name} has a much deeper understanding of its business and technical environment standards that should determine the balance of implementation.

{Table: CIS\_CSC}

Table 2: Recommendations Based on CIS Controls

The security team is available to assist with any follow-up that {Stakeholder Name} may need. For additional information on the security team’s assessment and service offerings, contact ({Team Lead Email}).

{RANSOMWARE RESULTS}

{DATA EXFILTRATION RESULTS}

{PAYLOAD TESTING RESULTS}

{PHISHING CAMPAIGN RESULTS}

# Attack Paths

Attack paths are used to demonstrate impact by chaining together vulnerabilities and misconfigurations to achieve a significant level of access. The sections below provide a high-level overview of attack paths that the security team executed during the engagement and the corresponding MITRE ATT&CK techniques that were leveraged in each attack. A detailed breakdown of each attack path can be found in the corresponding [Appendix D: Narrative](#NAR) section.

{ATTACK PATHS}

# Appendix A: Severity Rating Criteria

The severity selected for each finding during the RVA is determined using the criteria outlined below.

|  |  |
| --- | --- |
| **Severity** | **Description** |
| **• Critical** | Critical findings pose an immediate and severe threat to the environment due to ease of exploitation and significant impact. In most cases, critical findings are reported immediately, and rapid mitigation should be considered. |
| **• High** | An adversary may leverage high findings to obtain full control over a targeted asset. This includes but is not limited to: easily exploitable vulnerabilities that lead to complete compromise of an application, system, or network; significant router/firewall/server misconfigurations; weak password configurations that lead to administrator account compromise; or any vulnerability that can be exploited using readily available tools leading to significant compromise of an asset. |
| **• Medium** | An adversary may leverage medium findings to obtain some control over a targeted asset. This includes but is not limited to: unauthorized disclosure of sensitive customer or user account information; unauthorized read access to sensitive business information; weak anti-virus implementation/configurations; and lack of segmentation between untrusted and trusted networks. |
| **• Low** | Low findings typically encompass items of interest that are not readily exploitable and/or do not result in compromise to confidentiality, integrity, or availability of assets. The raw data and scan reports provided by the security team should be reviewed for additional findings that may have been deemed low severity but were not included in this report based on the minor risk they present. Due to time constraints, the security team prioritizes higher risk findings and may not be able to validate lower severity findings. |
| **• Informational** | Informational findings are potential weaknesses within the environment that cannot be readily exploited. These findings represent areas that should be investigated further, but do not require immediate action or mitigation. |

Table 3: Severity Rating Descriptions

# Appendix B: External Port Mapping

During external testing, the security team identified the following open ports/services on {Stakeholder Name}’s public-facing systems. It is recommended to review the data below, determine if any unnecessary ports/services are publicly accessible, and minimize the external attack surface where possible.

{Table: Port Mapping}

Table 4: Open Ports and Services on External Systems

# APPENDIX C: Narrative

This section highlights key tools and techniques the security team utilized during testing and can be used to replicate the security team’s actions or better understand how a particular finding was identified. These actions should only be replicated by an experienced individual who thoroughly understands the functionality and risks of the tools and techniques.

{NARRATIVE SECTION}

# Appendix D: Password Analysis

The security team obtained the hashed passwords for all the {Stakeholder Name} users during the assessment and attempted to obtain the clear text passwords represented by the hashed values. The following output shows statistical analysis of the clear text passwords recovered by the security team:

{PASSWORD ANALYSIS}

# Appendix E: Abbreviations and Acronyms

{Table: Acronyms}