

TLP: WWWWW

[Enter Assessment Title here.] (Draft)

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’s organization 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.

High Value Asset

ADD SERIAL NUMBER

February 26, 2024

[Enter Assessment Title here.]

High Value Asset

ADD SERIAL NUMBER

February 26, 2024

Table of Contents

[Background and Testing 3](#_Toc81231021)

[Results 5](#_Toc81231022)

[Recommendations 9](#_Toc81231023)

[Appendix A: Findings 10](#_Toc81231024)

[Appendix B: Services and Scope 14](#_Toc81231025)

[Appendix C: Penetration Testing Technical Overview 15](#_Toc81231026)

[Appendix D: Abbreviations and Acronyms 17](#_Toc81231027)

Tables

[Table 1: Applicable ATT&CK Matrix Tactics and Techniques 16](#_Toc81231028)

Figures

[Figure 1: HVA Logistics 3](#_Toc81231029)

[Figure 2: Assessment Scenarios 3](#_Toc81231030)

[Figure 3: HVA Targets 3](#_Toc81231031)

[Figure 5: Scan Results 4](#_Toc81231032)

[Figure 6: Scenario Testing Results 5](#_Toc81231033)

[Figure 7: Phishing Attack Path 5](#_Toc81231034)

[Figure 8: Most Frequently Cited NIST Controls 6](#_Toc81231035)

[Figure 9: NIST Cybersecurity Framework Controls 6](#_Toc81231036)

[Figure 10: Risk Assessment Matrix 7](#_Toc81231037)

[Figure 11: Access Summary 8](#_Toc81231038)

[Figure 12: CIS Controls Based Recommendations 9](#_Toc81231039)

[Figure 13: Findings Breakdown 10](#_Toc81231040)

[Figure 14: Findings Summary 11](#_Toc81231041)

[Figure 13: Services and Scope 14](#_Toc81231042)

# Background and Testing

The security team conducted an assessment for a High Value Asset at the request of the {Stakeholder Long Name} ({Stakeholder Initials}). Specific HVA logistics are provided in Figure 1.

|  |  |
| --- | --- |
| {Stakeholder Initials} Testing Details | |
| Customer | {Stakeholder Long Name} ({Stakeholder Initials}) |
| Customer POC | {Customer Name}, {Customer Email} |
| Security Team Lead | {Fed lead Name}, {Fed lead Email} |
| {Stakeholder Initials}’s Business Goal for the HVA | {GET A BUSINESS GOAL FROM POC} |
| Target HVA | {HVA System Name} |
| Testing – External | |
| Dates | {External Start Date} to {External End Date} |
| Test Location | {External Test Location} |
| Scope | {Short business level external scope – tech scope is in appendix.} |
| Services | {Must be consistent with external Service Catalog} |
| Testing – Internal | |
| Dates | {Internal Start Date} to {Internal End Date} |
| Test Location | {Internal Test Location} |
| Scope | {Short business level internal scope – tech scope is in appendix.} |
| Services | {Must be consistent with internal Service Catalog} |

Figure 1: HVA Logistics

Details on the scope, services performed, and testing timeframes are in [Appendix B](#AppB_ServicesandScope). All penetration testing scenarios listed below were executed with the intent of gaining access to sensitive data protected by the targeted High Value Assets (HVA) listed below.

{Table: Assessment Scenarios}

Figure 2: Assessment Scenarios

{Table: HVA Targets}

Figure 3: HVA Targets

Figure 4 shows a summary of the numbers of Internet Protocol (IP) addresses scanned and hosts identified.

|  |  |  |
| --- | --- | --- |
|  | EXTERNAL Scan | INTERNAL Scan |
| IP Addresses Scanned | {Number of External Addresses Scanned} | {Number of Internal Addresses Scanned} |
| Active Hosts Identified | {Number of External Hosts Identified} | {Number of Internal Hosts Identified} |

Figure 4: Scan Results

# Results

The security team uses a variety of tools and significant security expertise to conduct an HVA. The results presented in this section are an overview of the team’s findings based on the scope, scenarios defined, and resources available. A technical overview of the penetration testing is in [Appendix C](#AppC_PenTestTechOverview). Detailed findings and recommended mitigations are in [Appendix A](#AppA_Findings)**.**

Figure 5 is a summary of results for each of the scenarios tested during the engagement. Validated critical findings were immediately reported to the {Stakeholder Initials} POC.

{Table: HVA Scenario Testing Results}

Figure 5: Scenario Testing Results

## External Results

{external results business desc}

## Phishing Results

The phishing tests included both user and systems testing. During a phishing attack (Figure 6), an attacker sends an email that must successfully pass through any protections presented by both the network border and the host system that receives the email. After the email passes through those protections, the social engineering aspect of having the user interact with the email takes place.

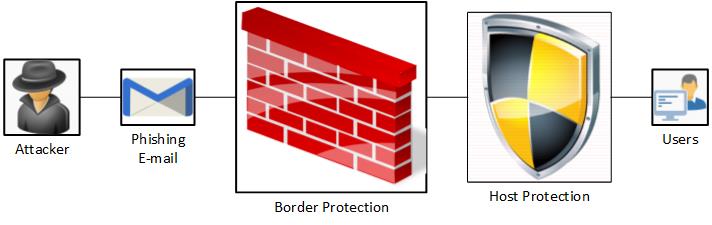


Figure 6: Phishing Attack Path

{phishing results business desc}

{phishing results susceptibility}

## Web Application Assessment

{web application}

## Internal Assessment

{internal results business desc}

## Internal Threat Emulation

{internal threat emulation}

## Data Exfiltration

{data exfiltration}

## Comparison Results

{Comparison results}

## NIST-Based Summary

The security team mapped all of the findings (see [Appendix A](#AppA_Findings)) to applicable National Institute of Standards and Technology (NIST) controls as described in NIST Special Publication (SP) 800-53. Figure 7 illustrates the most common control families cited based on the number of findings. [Appendix A](#AppA_Findings) provides the complete mapping and the detailed technical description for each finding. Note that some findings may be mapped to multiple applicable NIST controls.

{NIST 800-53 Controls}

Figure 7: Most Frequently Cited NIST Controls

## NIST Cybersecurity Framework

HVAs are also mapped to the NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February 12, 2014, commonly called the Cybersecurity Framework.

Figure 8 illustrates the most common controls cited based on the number of findings. [Appendix A](#AppA_Findings) provides the complete mapping and the detailed technical description for each finding. Note that some findings may be mapped to multiple applicable NIST controls.

{NIST CSF}

Figure 8: NIST Cybersecurity Framework Controls

## Risk Assessment

The security team uses a risk matrix to present a visualization of {Stakeholder Initials}’s risks as determined by the threat emulation scenarios performed during the assessment. The level of risk is determined by considering the likelihood of the emulated threat against its demonstrated impact during the assessment. The results of the risk assessment are evident in the severity ascribed to individual findings. A greater risk score (calculated as the product of probability and impact) results in a higher severity. The security team recommends that higher severity findings be addressed quicker to reduce the associated risks.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Impact of Risk  (Consequence) | Major | {MajLow} | {MajMed} | {MajHigh} |
| Moderate | {ModLow} | {ModMed} | {ModHigh} |
| Minor | {MinLow} | {MinMed} | {MinHigh} |
| Seriousness of Risk =  Probability x Impact | | Low | Moderate | High |
| Probability of Risk | | |

Figure 9: Risk Assessment Matrix

## Noted System Strengths

In addition to observing and assessing the technical components, the security team noted the following business and administrative components that augmented the network security posture of the tested environment.

{noted system strengths}

## Access Summary Conclusion

{access summary conclusion}

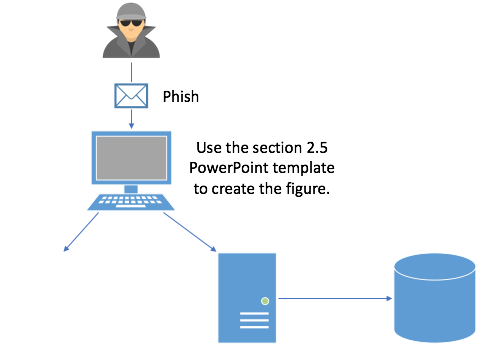


Figure 10: Access Summary

# 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 Critical Infrastructure Security (CIS) controls for mitigating the risks discovered. Figure 11 represents a high-level summary of prioritized recommended remediations and the associated findings. As always, {Stakeholder Initials} has a much deeper understanding of its business and technical environment standards that should be balanced in determining implementation.

To ensure compliance with Binding Operational Directive (BOD) 18-02, HVA stakeholders are required to remediate or submit a SAORM approved remediation plan for all critical and high findings within (30) days of receipt of the final HVA report. The stakeholders are to provide notification to DHS that each identified vulnerability was addressed.

{Table: CIS\_CSC}

Figure 11: CIS Controls Based Recommendations

The security team is available to assist with any follow-up that {Stakeholder Initials} may need. For additional information on the security team’s service offerings, contact the team via email.

Appendix A: Findings

The security team identified the following findings as potentially exploitable vulnerabilities that could compromise the confidentiality, integrity, and availability of the tested environment. Each finding includes a description, supporting details, and recommended steps for mitigation. The following findings are presented for review, validation, and remediation as deemed appropriate. The {Stakeholder Initials} team should review the findings and recommendations for technical weaknesses, shortcomings in processes and procedures, and systemic weaknesses in overall security posture. Additional information from testing and on each specific finding is collected during the HVA, and the entire store of raw data was provided to the {Stakeholder Initials} POC at the conclusion of the test. When appropriate, findings may refer to information available within the raw data. The raw data includes a “README” file with details on the setup of the data store.

## Appendix A.1: Findings Breakdown

{Table: Findings Breakdown}

Figure 12: Findings Breakdown

See [Appendix A.4](#AppA4_Severity) for definitions of each level of severity (Critical/High/Medium/Low/Informational).

## Appendix A.2: Findings Summary and Evidence

{Table: External Findings}

{Table: Internal Findings}

{Table: Social E Findings}

Figure 13: Findings Summary

## Appendix A.3: Detailed Findings

{Table: NCATS Detailed Findings}

## Appendix A.4: Severity Rating Criteria

|  |  |
| --- | --- |
| Severity | Description |
| Critical | Critical vulnerabilities pose an immediate and severe risk to the environment because of the ease of exploit and potential severe impact. Critical items are reported to the customer immediately. |
| High | Intruders may be able to exercise full control on the targeted device.  Examples include:   * Easily exploitable vulnerabilities that can lead to complete application, system, or network compromise, such as an intruder having the ability to remotely administer files on a web server * Severe router/firewall/server misconfigurations * Worm, Trojan, or backdoor detected * Vulnerability that has tools readily available on the Internet to take advantage of it * Weak passwords for remote administration and users |
| Medium | Intruders may be able to exercise some control of the targeted device.  Examples include:   * Disclosure of unauthorized sensitive customer information or user account information * Ability of an intruder to obtain full read access to corporate confidential information * Lack of basic logging and alerting capabilities * Antivirus misconfigurations * Untrusted networks having access to trusted networks |
| Low | The vulnerabilities discovered are reported as items of interest but are not normally exploitable. Many low items reported by security tools are not included in this report because they are often informational, unverified, or of minor risk. |
| Informational | These vulnerabilities are potential weaknesses within the system that cannot be readily exploited. These findings represent areas that the customer team should be cognizant of, but they do not require any immediate action. |

# Appendix B: Services and Scope

{Table: Scope and Services}

Figure 14: Services and Scope

# Appendix C: Penetration Testing Technical Overview

In penetration testing, security engineers test the security of an environment by simulating scenarios an advanced attacker may attempt. Because different components have different vulnerabilities, this type of testing is highly customized. Penetration testing is valuable because it often exploits a chain or path of security vulnerabilities, revealing risks that other activities like security scans and reviews do not detect.

Below is an overview of the penetration testing paths used in this assessment and their results. References to adversarial techniques, described in the ATT&CK for Enterprise threat model, have been inserted as footnotes to applicable steps taken by the security team during the assessment.

Further detail about the techniques used during the assessment are found in Appendix C.1.

{Table: Technical Overview}

## Appendix C.1: ATT&CK Matrix

This ATT&CK Matrix provides a visual representation of the adversarial tactics and techniques used by the security team during the assessment. Click on the associated link for more information about how a technique was used during the assessment.

Tactic categories are listed on the top row, and individual techniques as cells underneath each tactic to denote that technique can be used to accomplish that particular tactic. Techniques can span multiple tactic categories signifying that they can be used for more than one purpose.

More information about the MITRE ATT&CK Matrix for Enterprise can be found at <https://attack.mitre.org/>.

{Table: ATTACK Matrix}

Table 1: Applicable ATT&CK Matrix Tactics and Techniques

# Appendix D: Abbreviations and Acronyms

|  |  |
| --- | --- |
| DHS | Department of Homeland Security |