



External Pen Test 5-1-2024

EXECUTIVE SUMMARY

Demo Customer C

May 31, 2024

www.vonahi.io

Copyright

© Vonahi Security. All Rights Reserved. This is unpublished material and contains trade secrets and other confidential information and is subject to a confidentiality agreement. The unauthorized possession, use, reproduction, distribution, display, or disclosure of this material or the information contained herein is prohibited.

The methodology used to audit the computer systems is considered proprietary intellectual information of Vonahi Security and may not be disclosed without written permission from Vonahi Security. Vonahi Security gives permission to copy this report for the purpose of disseminating information within your organization, or any regulatory agency.

Confidentiality

This document contains company confidential information of a proprietary and sensitive nature. As such, this document should be afforded the security and handling precautions that a confidential document warrants. This document should have a controlled distribution to relevant parties only and should not be copied without written permission. Vonahi Security treats the contents of a security audit as company confidential material and will not disclose the contents of this document to anyone without written permission.

Assessment Project Team

Below is a list of contacts that were involved in this engagement. Should you have any questions pertaining to the content of this document or any project and non-project-related items, please feel free to reach out to the necessary project contacts.

| Primary Point of Contact | |
|--------------------------|---------------------|
| Name: | Vonahi Security |
| Title: | Security Consultant |
| Office: | |
| Email: | support@vpentest.io |

Executive Summary

Vonahi Security (test account) has requested the assistance of Vonahi Security to perform a comprehensive security assessment to assist with evaluating the cyber risks presented within the tested environment(s). The objective of this engagement was to determine if any identified threats could be used to mount an attack against the organization that could lead to the disclosure of sensitive information or access to critical information systems.

Included in this Executive Summary report is a high-level overview of the results that were observed during this assessment. A copy of more specific information pertaining to technical findings and remediation details are documented within the Technical Report as well as the Vulnerability Tracking Report.

Engagement Scope of Work

Prior to beginning the assessment, Vonahi Security and Vonahi Security (test account) agreed to a scope of work to define the specific assessment phases. The table below outlines the engagement scope of work and details entailed within each assessment phase that was conducted as part of this engagement.



| Assessment Component | Assessment Phases |
|--|--|
| External Network Penetration Test | <p>This assessment includes performing a security assessment from the perspective of a malicious attacker from public Internet environments. Threats exposed to users on the public Internet are higher severity than those of the internal environment due to the increased exposure.</p> <ul style="list-style-type: none">→ Reputational Threat Exposures - Using information available on the public Internet (e.g. search engines, social media, etc.), Vonahi Security attempted to discover information that could potentially harm Vonahi Security (test account)'s reputation. This includes publicly disclosed information that may or may not be useful for an attack.→ External Network Penetration Test - A penetration test was conducted to identify the potential impact of exploiting any identified vulnerabilities. Only exploits that are deemed safe were executed during this phase. Information obtained from within the Reputational Threats Exposure phase were used as part of this penetration test. |

Engagement Statistics

The information below displays overall statistics that were recorded as part of this engagement. Following the statistics, Vonahi Security has summarized all of the threats identified.

External Network Penetration Test

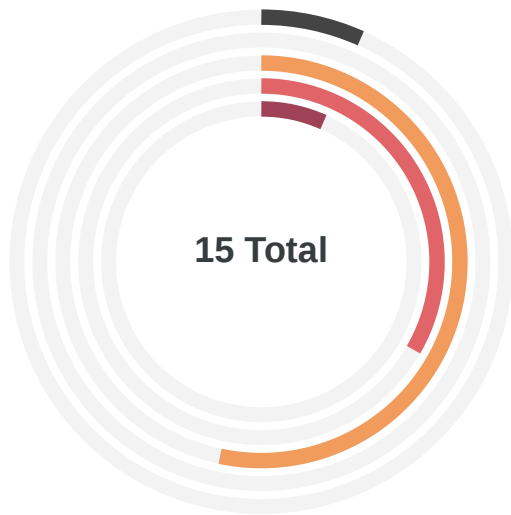
The information below provides a high-level overview of the assessment results recorded as part of this engagement. Following this section is a summary of all the threats identified and their potential risk to your organization.

| Overall Severity Ranking | |
|---|--|
|  <p>Low CRITICAL Critical</p> | <p>ASSESSMENT SCHEDULE  Thu, May 30, 2024 10:05 PM ET</p> <p>Immediate remediation or mitigation is required. Exploitation of identified vulnerabilities require minimal effort from an attacker and pose a significant threat. A successful attack could result in unauthorized access to systems and/or valuable data.</p> |

Engagement Results Charts

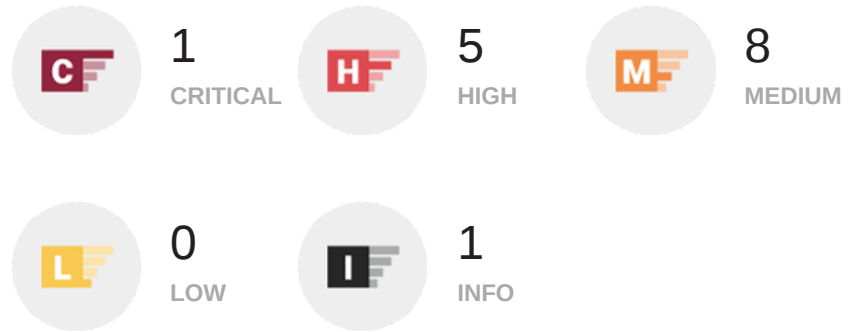
To help Demo Customer C understand the severity of the threats identified during testing, Vonahi Security has included an overall summary chart below that displays a comparison of the report findings as well as the vulnerabilities that were discovered.

External Network Penetration Test Results



PenTest Findings

The following chart displays the overall severity of the report findings that were documented as part of the penetration testing efforts.



Engagement Results Summary

To summarize the results, Vonahi Security has grouped all of the findings from the penetration test into rollup findings. These rollup findings can be used to quickly determine the root cause of the issues identified in the technical report. By implementing a remediation strategy for the findings based on the rollup issues identified below, Vonahi Security (test account)'s security posture would be greatly reduced.

External Network Penetration Test

| Category | Summary |
|---------------------------------------|--|
| Insecure Protocols | Testing identified instances of insecure protocols, which are essentially communication protocols that can potentially expose sensitive/confidential data in cleartext communications. A successful compromise against this weakness could lead to escalated privileges within the environment and could provide additional access to critical information systems and/or resources. |
| Patching Deficiencies | The tested environment contains patching deficiencies amongst systems and services. These issues could potentially result in a successful compromise as each vulnerability contain multiple security weaknesses that an attacker may be able to take advantage of. Successful access may lead to confidential data and/or systems. |
| Configuration Deficiencies | Configuration weaknesses were identified that could potentially lead to a successful compromise of systems and/or data within the tested environment. Although some of the configuration weaknesses may be exploitable in limited circumstances, the potential impact of a successful attack could be relatively high. |
| Ingress Filtering Deficiencies | The organization's network firewalls allow an excessive amount of access to services within the internal, trusted network environment. This excessive access could potentially expose the organization to attacks that are accessible due to unnecessary or misconfigured access. Services on the internal network should only be accessible to individuals and computer systems that are considered "trusted" such as through a Virtual Private Network (VPN) along with appropriate access controls. |

Remediation Roadmap

For each assessment conducted, Vonahi Security provided a remediation roadmap to help Vonahi Security (test account) understand the issues within the respective environment and the overall remediation strategies that should be implemented to resolve the issues identified during the penetration test. It should be noted that the remediation strategies below apply to multiple issues identified within the technical report and can greatly reduce the overall attack surface once successfully implemented.

External Network Penetration Test

| Issue | Remediation Strategy |
|---------------------------------------|--|
| Patching Deficiencies | <p>A patch management program should be implemented to ensure that both native and third-party services are up-to-date. Given today's threat landscape and the frequency in which security updates are released for systems and services, patches should be applied on a weekly basis at minimum.</p> <p>If the organization currently has a patch management program, it should be evaluated to determine where gaps may exist that resulted in the patching deficiencies identified during testing.</p> |
| Configuration Deficiencies | <p>Implement or improve a security configuration baseline that adheres to security best practices and industry standards such as National Institute of Standards and Technology (NIST). This security configuration baseline should ensure that no services and/or systems are deployed within the environment until a thorough configuration review has been performed.</p> |
| Insecure Protocols | <p>Implement and/or improve a security configuration baseline within the organization that addresses the use of secure protocols. Insecure protocols pose a significant risk as the data being communicated is exposed in cleartext, allowing an attacker to discover potentially sensitive information. The organization should regularly perform scans that attempt to identify the use of insecure protocols to ensure that the configuration baseline is effective.</p> |
| Ingress Filtering Deficiencies | <p>Ensure that the organization's network firewalls restrict inbound access to the trusted internal network environment to services that are required for business operations. For services that are required for business operations, the organization should document these so that business justifications are communicated and understood within the organization. Any adjustments to these configurations should be documented in a change management program to establish an audit trail. Lastly, the organization may consider implementing a Virtual Private Network (VPN) to ensure that only authorized users can communicate with services that are deemed sensitive.</p> |