



Internal Network Penetration Test

# EXECUTIVE SUMMARY

**Demo Client**

June 06, 2021

[app.vpentest.io](https://app.vpentest.io)

## Copyright

© vPenTest Partner. 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 This is unpublished material and contains trade secrets and other confidential information and is subject to a confidentiality agreement.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 vPenTest Partner and may not be disclosed without written permission from vPenTest Partner. vPenTest Partner 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. vPenTest Partner 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 on 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	
<b>Name:</b>	Demo Consultant
<b>Title:</b>	Consultant
<b>Mobile:</b>	+1(504) 507-0558
<b>Office:</b>	+1(844) 866-2732
<b>Email:</b>	altonjx@gmail.com

## Executive Summary

Demo Client has requested the assistance of vPenTest Partner 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

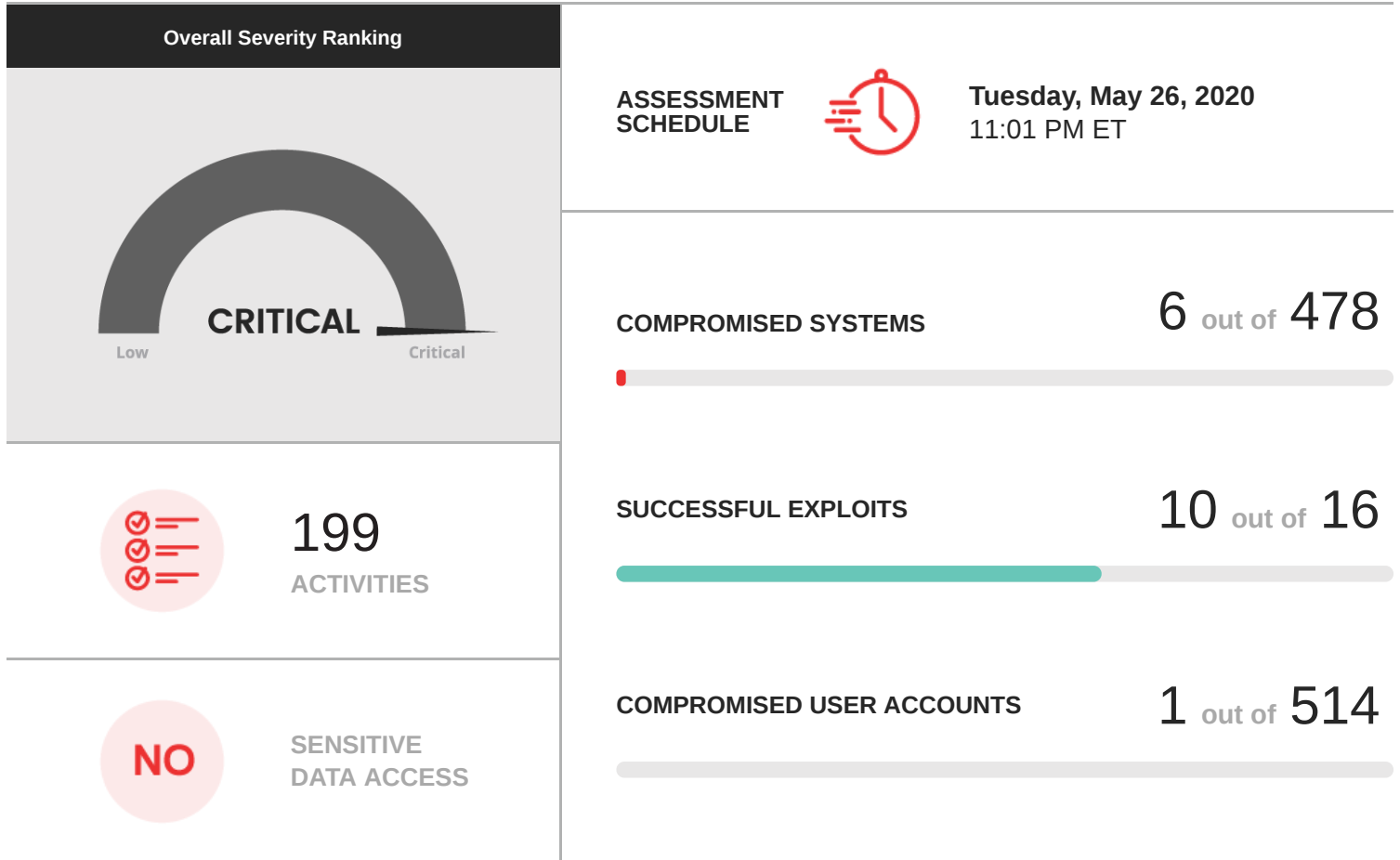
Prior to beginning the assessment, vPenTest Partner and Demo Client agreed to a scope of work to define the specific assessment phases. The table below outlines the engagement scope of work and details entailed within each assessment phase that was conducted as part of this engagement.

Assessment Component	Assessment Phases
<b>Internal Network Security Assessment</b>	<p>During this phase, security weaknesses within the internal network environment are identified to attempt discovering sensitive and/or valuable information within the environment. This phase includes man-in-the-middle attacks, as well as exploitation of patching, authentication, as well as configuration deficiencies. Additionally, a penetration test and vulnerability assessment is conducted to identify and exploit security weaknesses.</p> <ul style="list-style-type: none"><li>→ <b>Internal Network Penetration Test</b> - 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 phases.</li><li>→ <b>Vulnerability Assessment</b> - A vulnerability assessment was also performed against the list of systems provided for the scope for testing. This vulnerability assessment attempted to identify, but not exploit, security vulnerabilities that exist within the environment.</li></ul>

## Engagement Statistics

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

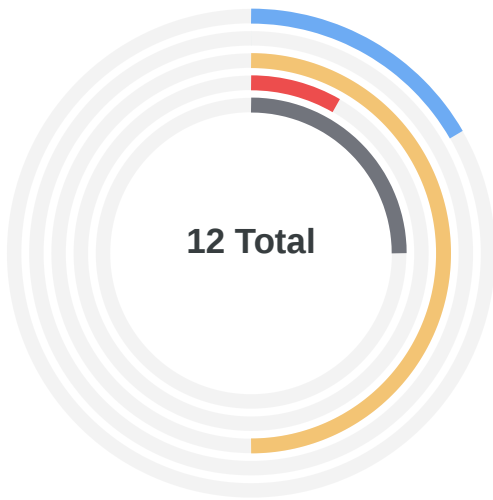
### Internal Network Security Assessment



## Engagement Results Charts

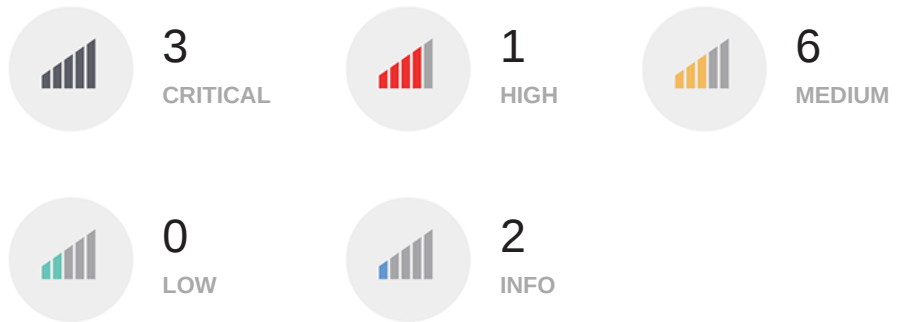
To help Demo Client understand the severity of the threats identified during testing, vPenTest Partner has included an over-all summary chart below that displays a comparison of the report findings as well as the vulnerabilities that were discovered.

### Internal Network Security Assessment Results



#### PenTest Findings

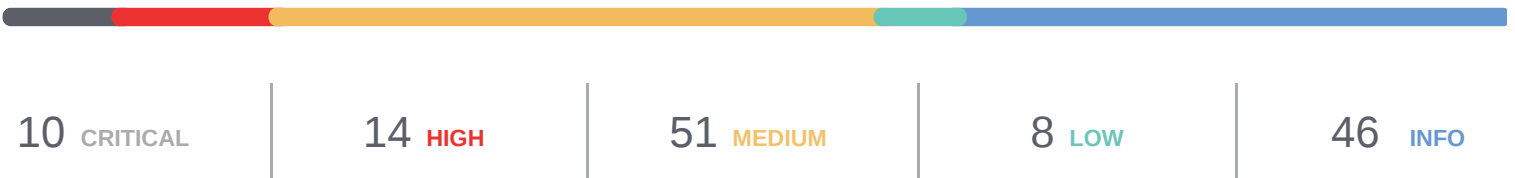
The following chart displays the overall severity of the report findings that were documented as part of the penetration testing efforts.



As part of the penetration test, vPenTest Partner also performed a vulnerability assessment to provide additional value and insight as to the vulnerabilities that were identified by our vulnerability scanner. This vulnerability scan included the discovery of common security vulnerabilities that are publicly documented with Common Vulnerabilities and Exposures (CVE) scores.

#### VULNERABILITY ASSESSMENT FINDINGS

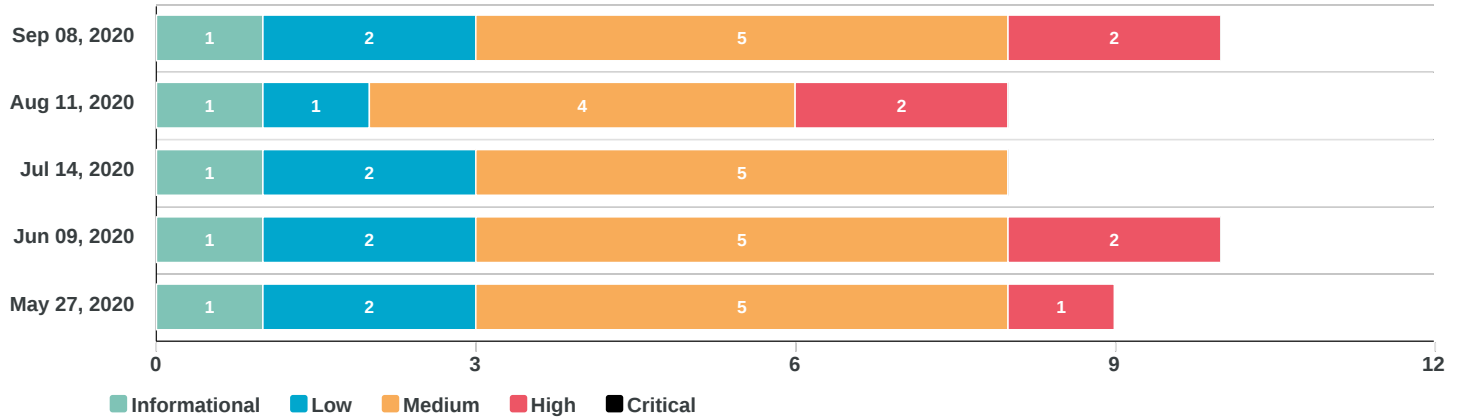
129 TOTAL



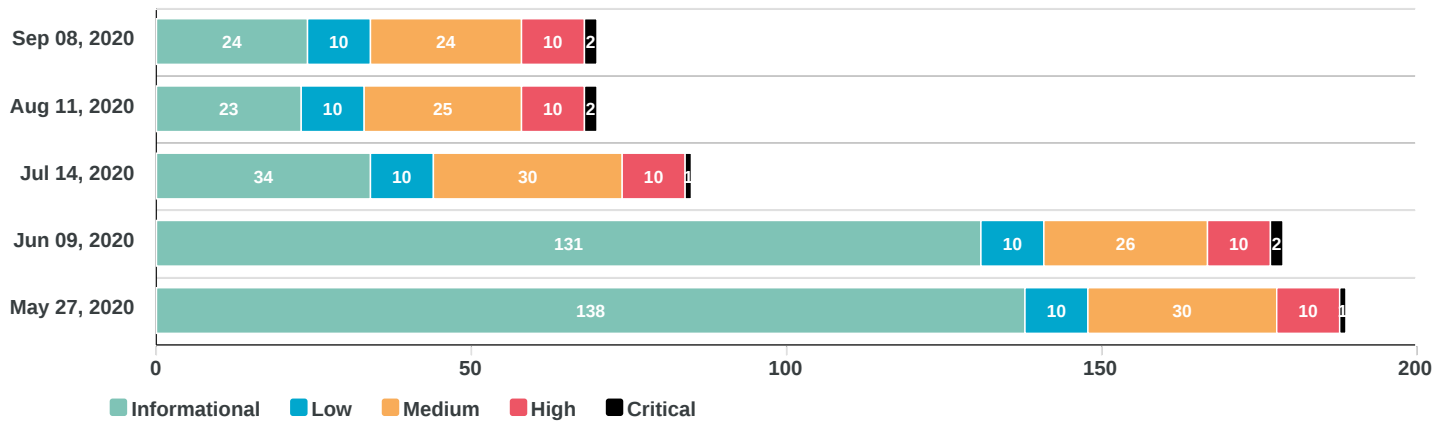
## Comparison Charts

To help Demo Client understand the trend of the PenTest Findings and vulnerabilities discovered in the past as part of this on-going engagement, vPenTest Partner has provided trend data in this section of the report.

### History of PenTest Findings



### History of Vulnerability Assessment Findings



## Engagement Results Summary

To summarize the results, vPenTest Partner 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, Demo Client's security posture would be greatly reduced.

### Identified Threats - Internal Network Security Assessment

#### 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.

#### 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.

#### 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.

#### EGRESS FILTERING DEFICIENCIES

Testing identified that excessive services are accessible on the public Internet from the internal network environment. This could allow for an attacker to circumvent security controls by using alternative communication channels. Furthermore, a compromised system may be able to use such alternative communication channels to exfiltrate sensitive information.

## Remediation Roadmap

For each assessment conducted, vPenTest Partner provided a remediation roadmap to help Demo Client 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.

### Internal Network Security Assessment

Issue	Remediation Strategy
<b>Patching Deficiencies</b>	<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>
<b>Configuration Deficiencies</b>	<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>
<b>Egress Filtering Deficiencies</b>	<p>Ensure that the organization's network firewalls restrict outbound access to the public Internet to services that are required for business operations. For services that are required for business operations, the organization should document these in a policy and procedure 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.</p>
<b>Insecure Protocols</b>	<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>