PenTest Sample - Internal Assessment

EXECUTIVE SUMMARY

PenTest Client - Sample

January 10, 2024

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. ENS 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 Points of Contact	
Name:	Mark Weigand (ENS President) --- or Paul Herring (CISO)
Cell:	Mark: 916-517-6250 --- Paul: 949-873-4074
Email:	mark.weigand@ens.us.com / paul.herring@ens.us.com

Executive Summary

Client has requested the assistance of ENS 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, ENS and 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
Internal Network Penetration Test	This assessment attempted to identify security threats that are exposed on the internal network environment. Threats identified within the internal environment are usually less severe than those of the external environment due to the limited exposure. ▯ **Internal 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.

Engagement Statistics

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

Internal Network Penetration Test

Overall Severity Ranking

ASSESSMENT SCHEDULE

Friday, December 08, 2023
07:00 PM CT

277
ACTIVITIES

YES
SENSITIVE DATA ACCESS

COMPROMISED SYSTEMS 7 out of 276

SUCCESSFUL EXPLOITS 7 out of 10

COMPROMISED USER ACCOUNTS 3 out of 346

Engagement Results Charts

To help Client understand the severity of the threats identified during testing, ENS has included a summary chart below that displays a comparison of the report findings as well as the vulnerabilities that were discovered.

Internal Network Penetration Test Results

PenTest Findings

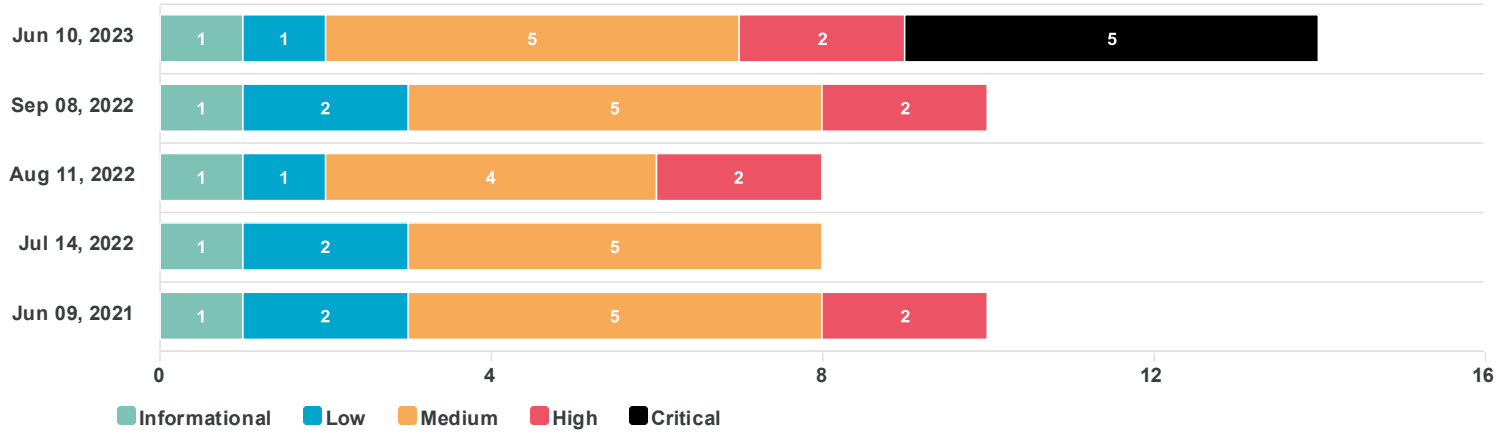
The following chart displays the overall severity of the report findings that were documented as part of the penetration testing efforts.

5	CRITICAL	2	HIGH	5	MEDIUM
1	LOW	1	INFO		

Comparison Charts

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

History of PenTest Findings



Engagement Results Summary

To summarize the results, ENS 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, Client's security posture would be greatly reduced.

Internal 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.
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, ENS provided a remediation roadmap to help 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 Penetration Test

Issue	Remediation Strategy
Patching Deficiencies	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. 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.
Configuration Deficiencies	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.
Egress Filtering Deficiencies	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.
Insecure Protocols	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.