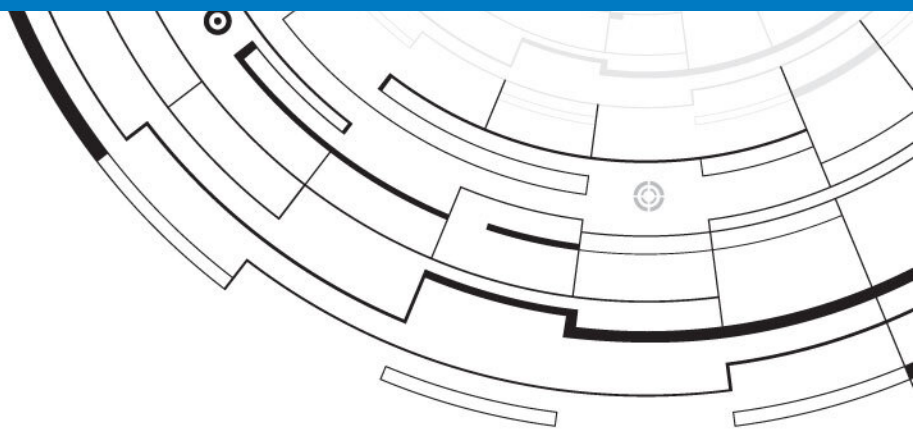
Sample Report

Customer

Consolidated Vulnerability & Penetration Scanning Report



Customer

Date

tpx.com

Executive Summary

{client} has requested the assistance of TPx Communications 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, TPx Communications 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
External Network Security Assessment	During this phase, Open Source Intelligence (OSINT) Gathering is researched to identify valuable information that may contribute to a successful attack against the external network environment. Additionally, a penetration test and vulnerability assessment is conducted to identify and exploit security weaknesses. → **Reputational Threat Exposures** - Using information available on the public Internet (e.g. search engines, social media, etc.), TPx Communications attempted to discover information that could potentially harm {client}'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. → **Vulnerability Assessment** - 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.

Engagement Results Charts

To help {client} understand the severity of the threats identified during testing, TPx Communications has included an over-all summary chart below that displays a comparison of the report findings as well as the vulnerabilities that were discovered.

External 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.

0	CRITICAL	1	HIGH	0	MEDIUM
0	LOW	0	INFO		

As part of the penetration test, TPx Communications 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

0 TOTAL

0	CRITICAL	0	HIGH	0	MEDIUM	0	LOW	0	INFO

Technical Report Details

Threat Severity Rankings

To assist the organization with prioritizing findings, the findings and observations have been categorized with threat severity rankings based on the following guidelines:

SEVERITY		DESCRIPTION
	Critical	A critical threat ranking requires immediate remediation or mitigation. Exploitation of these vulnerabilities typically require a minimal amount of effort by the adversary, but poses a significant threat to the confidentiality, integrity, and/or availability of the organization's systems and data. A successful compromise of findings of this ranking lead to access to multiple systems and/or several pieces of sensitive information.
	High	A high threat ranking requires immediate remediation or mitigation. Exploitation of these vulnerabilities typically require a minimal amount of effort by the adversary, but poses a significant threat to the confidentiality, integrity, or availability of the organization's systems or data. A successful compromise of findings of this ranking lead to access to a single access or limited sensitive information.
	Medium	A medium threat ranking requires remediation or mitigation within a short and reasonable amount of time. These findings typically lead to a compromise of non-privileged user accounts on systems and/or applications or denote a denial-of service (DoS) condition of the host, service, or application.
	Low	A low threat ranking requires remediation or mitigation once all higher prioritized findings have been remediated. These findings typically leak information to unauthorized or anonymous users and may lead to more significant attacks when combined with other attack vectors.
	Informational	An informational threat ranking does not pose a significant threat to the environment and may just be findings that could potentially disclose valuable information, but does not expose the organization to any technical attacks. Findings rated as informational may be useful for an attacker performing information gathering on the organization to leverage in other attacks, such as social engineering or phishing.

For a full sample report, contact us at
https://www.tpx.com/contact-sales/