

PenTest Prospecting

Evaluation Summary

SAMPLE

Example Company

October 01, 2026

Copyright

© TRU Solutions. 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 This is unpublished material and contains trade secrets and other confidential information and is subject to a confidentiality agreement.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 TRU Solutions and may not be disclosed without written permission from TRU Solutions. TRU Solutions gives permission to copy this report for the purpose of disseminating information within your organization, or any regulatory agency.

Confidentiality

This document contains organization 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. TRU Solutions treats the contents of a security audit as organization 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:	TRU Solutions
Title:	PenTest
Office:	+4(031) 405-6677
Email:	pentest@tru.ro

SAMPLE

Introduction

This report provides an evaluation of your organization's network security using our pentest methodology. It is not a full penetration test and cannot be used to meet compliance or cyber insurance requirements.

Engagement Scope of Work

Prior to beginning the assessment, TRU Solutions and Example Company 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 Prospecting Test	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. → **Reputational Threat Exposures** - Using information available on the public Internet (e.g. search engines, social media, etc.), TRU Solutions attempted to discover information that could potentially harm Example Company'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.

SAMPLE

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. Exploiting these vulnerabilities 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 leads to access to multiple systems and/or several pieces of sensitive information.
	High	A high threat ranking requires immediate remediation or mitigation. Exploiting these vulnerabilities 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 leads to access to a single system 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 do 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.

SAMPLE

Discovered Threats

DISCOVERED THREATS	THREAT SEVERITY RANKINGS	
External Network Prospecting Test (5)		
Insecure Protocol - FTP		Medium
Insecure Protocol - POP3		Medium
Insecure Protocol - SMTP		Medium
Misconfigured DMARC Record		Medium
Missing DNSSEC Configuration		Informational

SAMPLE

MEDIUM

Insecure Protocol - FTP

Observation

The File Transfer Protocol (FTP) is commonly employed by client systems for the purpose of connecting to, storing, and retrieving files on server(s). A significant vulnerability inherent to FTP is its lack of encryption for the data exchanged between the client and server, which renders all transmitted information visible in cleartext format. Although FTP has the capability to establish a secure connection through TLS, the current configuration of the affected server(s) does not initiate or negotiate this secure protocol. Consequently, any sensitive data transferred over FTP is susceptible to interception.

Security Impact

The absence of encryption in FTP exposes all communications between client(s) and server(s) in an unprotected manner. This vulnerability creates opportunities for attackers to execute man-in-the-middle attacks, where they can capture sensitive user credentials and the contents of files being transmitted. The retrieved information could subsequently facilitate further attacks within the network environment, thereby increasing the overall risk of data breaches and unauthorized access.

Recommendation

If the FTP service is not essential for business operations, disabling it is strongly recommended to minimize risk exposure. For environments where file transfers are necessary, transitioning to Secure FTP (SFTP) is advised. SFTP employs encryption protocols to secure communication channels between client(s) and server(s), thereby enhancing the security posture and protecting sensitive data during transmission.

SAMPLE

MEDIUM

Insecure Protocol - POP3

Observation

The Post Office Protocol (POP) is widely utilized by email client(s) to facilitate the retrieval of emails associated with user account(s). However, a default configuration on certain POP server(s) may employ an insecure protocol, which can lead to the exchange of email data in plaintext. In scenarios where email client(s) pull email content over this unencrypted channel, sensitive information may be exposed, depending on the user account configuration.

Security Impact

The deployment of POP3 over a plaintext protocol renders all traffic transmitted between the client(s) and server(s) vulnerable to interception. This situation significantly increases the risk of man-in-the-middle attacks, where an adversary could capture sensitive user credentials and email contents. The harvested information can also facilitate additional targeted attacks against the organization's network infrastructure.

Recommendation

It is advisable to disable the POP3 service if it is not essential for business functions. In cases where email retrieval is required, implementing Secure POP3 (POP3S) is recommended. POP3S employs encryption, ensuring that communications between email client(s) and server(s) are secured against unauthorized access.

SAMPLE

MEDIUM

Insecure Protocol - SMTP

Observation

The penetration test identified that the Simple Mail Transfer Protocol (SMTP) server(s) were configured to accept plaintext authentication over port 25/tcp. This configuration is problematic because it allows credentials to be transmitted unencrypted, presenting a significant risk during data exchange. Under conditions where network traffic can be intercepted, such as in open or poorly secured networks, malicious actors can exploit this vulnerability to capture sensitive information.

Security Impact

The lack of encryption for user credentials exposes sensitive data to potential interception during transit, making it susceptible to man-in-the-middle (MitM) attacks. As a result, an attacker could gain unauthorized access to the SMTP server, potentially compromising email accounts and accessing sensitive content within end users' mailboxes.

Recommendation

To mitigate this vulnerability, it is strongly recommended to implement SSL/TLS encryption for all authentication processes on the SMTP server(s). While port 25/tcp is essential for interoperability with other mail servers, enforcing encryption for user credential transmission will significantly enhance security. Additionally, the use of secure alternatives, such as port 587/tcp for submission of emails, should be considered to minimize the risk of unauthorized access.

SAMPLE

MEDIUM

Misconfigured DMARC Record

Observation

The penetration test identified that the organization has a misconfigured DMARC (Domain-based Message Authentication, Reporting, and Conformance) record for its domain(s). DMARC is critical for verifying the authenticity of emails sent from the organization, serving as a vital barrier against email spoofing and phishing attacks. Without proper configuration, DMARC fails to instruct receiving mail servers on how to treat email messages from the organization's domain, thereby increasing vulnerability to attack.

Security Impact

A misconfigured DMARC record poses serious security risks to the organization. If the DMARC policy is set to "none" or is inadequately defined, it creates an opportunity for malicious actors to impersonate the organization's domain. This not only heightens the likelihood of successful phishing attacks but also exposes the organization to potential data breaches, financial losses, and reputational damage as fraudulent emails proliferate.

Recommendation

To mitigate these risks, it is essential for the organization to promptly review and rectify its DMARC record configuration. The DMARC policy should be explicitly defined, ideally set to "quarantine" or "reject," which directs receiving mail servers on the proper handling of unauthenticated messages. Proper DMARC configuration will significantly bolster the organization's email security posture, diminish the risk of phishing attacks, and safeguard sensitive data. Additionally, effective configuration will facilitate the receipt of reports regarding email authentication failures, enabling the organization to proactively monitor and respond to emerging threats.

SAMPLE

INFORMATIONAL Missing DNSSEC Configuration

Observation

The penetration test identified in-scope, primary domains that do not have DNSSEC (Domain Name System Security Extensions) configured. DNSSEC is a set of DNS protocol extensions that cryptographically sign DNS records, allowing resolvers to verify that responses have not been forged or tampered with in transit. When a zone is signed and the parent zone publishes the corresponding Delegation Signer (DS) record, validating resolvers can detect and reject manipulated DNS responses. Without DNSSEC, DNS responses for the domain are served unsigned and cannot be cryptographically validated.

Security Impact

The absence of DNSSEC does not directly expose the domain to exploitation, but it removes a layer of defense against a class of DNS integrity attacks. Specifically, unsigned zones remain susceptible to DNS cache poisoning, off-path spoofing, and on-path manipulation of DNS responses, which could redirect users or systems to attacker-controlled infrastructure. While modern resolvers and transport protections (such as DNS over TLS and source-port randomization) reduce the likelihood of these attacks, DNSSEC provides the only end-to-end cryptographic assurance that DNS data has not been altered between the authoritative nameserver and the resolver.

Recommendation

To strengthen the organization's DNS integrity posture, consider the following steps to configure DNSSEC:

1. Enable DNSSEC signing at the authoritative DNS provider for each primary domain, using current recommended algorithms (e.g., ECDSAP256SHA256 / type 13).
2. Publish the corresponding Delegation Signer (DS) record at the domain registrar to establish the chain of trust to the parent zone.
3. Validate the configuration end-to-end using a DNSSEC validation tool to confirm that the chain of trust is complete.
4. Establish a key rotation and monitoring process so that key or signature expirations do not cause resolution outages.

SAMPLE