Internal Penetration Test

Report of Findings

Lead Penetration Tester: TODO Lead Penetration Tester Name

TODO Customer, Inc.

November 19, 2025

Version: 1.0

Table of Contents

1 Statement of Confidentiality

The contents of this document have been developed by ISP Security LLC. ISP Security LLC considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from ISP Security LLC. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of ISP Security LLC.

The contents of this document do not constitute legal advice. ISP Security LLC's offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect ISP Security LLC external or internal infrastructure.

2 Engagement Contacts

TODO Customer Contacts		
Contact	**Title**	**Contact Email**
TODO Customer Contact 1	Chief Executive Officer	TODO EMAIL
TODO Customer Contact 2	Chief Technical Officer	TODO EMAIL

Assessor Contact		
Assessor Name	**Title**	**Assessor Contact Email**
TODO Lead Penetration Tester Name	TODO Lead Penetration Tester Title	TODO Lead Penetration Tester Email

3 Executive Summary

TODO Customer, Inc. (“TODO Customer” herein) contracted TODO Lead Penetration Tester Name to perform an **Internal Penetration Test** of TODO Customer’s environment to identify security weaknesses, determine impact on TODO Customer’s critical infrastructure, document all findings in a clear and repeatable manner, and provide remediation recommendations.

3.1 Approach

TODO Lead Penetration Tester Name performed testing under a “Grey Box” approach from November 19, 2025, to November 19, 2025 with no credentials and minimal advance knowledge of TODO Customer’s internal network. The goal was to evaluate the security posture of their infrastructure, identify misconfigurations, vulnerabilities, and attack paths, and determine their potential impact. Testing was performed remotely from TODO Lead Penetration Tester Name’s personal machine, focusing on critical systems such as Domain Controllers, Exchange Servers, Backup Servers, Network Printers, Copiers, Switches, Routers, and other infrastructure within the confines of TODO Customer's private network. Each identified weakness was documented and manually analyzed to determine exploitation possibilities, privilege escalation potential, and lateral movement opportunities. TODO Lead Penetration Tester Name sought to demonstrate the full impact of each vulnerability, up to and including domain-wide compromise. If TODO Lead Penetration Tester Name gained a foothold in the environment, TODO Customer authorized additional testing to include lateral movement, horizontal/vertical privilege escalation, and validation of implemented security controls, such as antivirus solutions and infrastructure updates, to demonstrate the potential consequences of a complete compromise.

3.2 Scope

The scope of this assessment included TODO SUBNETS internal network ranges, the **TODO PRIMARY DOMAIN** Active Directory domain, any additional Active Directory domains owned by TODO Customer, Inc. that were discovered during the engagement, and any additional internal hosts such as network printers, routers, switches, or private-facing servers. Internal access was provided by the client, and VPN access was provided by TODO Lead Penetration Tester Name to facilitate the assessment.

In Scope Assets

Host/URL/IP Address	Description
TODO X.X.X.X	TODO FILL IN DESCRIPTION
TODO DOMAIN NAME	TODO FILL IN DESCRIPTION

3.3 Assessment Overview and Recommendations

During the Internal Penetration Test of TODO Customer, Inc., TODO Lead Penetration Tester Name identified 1 findings that pose risks to the confidentiality, integrity, and availability of TODO Customer’s information systems. The findings were categorized by severity level, with TODO SEVERITY RATINGS HERE 0 of the findings being assigned a critical-risk rating, 0 high-risk, 0 medium-risk, and 0 low risk. There were also 1 informational finding related to improving security monitoring capabilities within the internal network.

TODO EXECUTIVE SUMMARY HERE

TODO Customer should create a remediation plan based on the Remediation Summary section of this report, addressing all high-risk findings as soon as possible according to the needs of the business. Given the comprehensive nature of this in-depth Active Directory penetration test, TODO Customer should focus on implementing the recommendations provided to address misconfigurations, privilege escalation paths, and

lateral movement opportunities. To maintain a robust security posture, TODO Customer should also consider scheduling periodic Active Directory security assessments and penetration tests to validate improvements and identify emerging vulnerabilities. Continuous monitoring and proactive hardening of the Active Directory environment will make it increasingly challenging for attackers to compromise the network and will improve TODO Customer's ability to detect and respond to suspicious activity effectively.

4 Internal Penetration Test Assessment Summary

TODO Lead Penetration Tester Name began all testing activities from the perspective of an unauthenticated user on the internal network. TODO Customer provided the tester with internal network access but did not provide additional information such as configuration details.

4.1 Summary of Findings

During the course of testing, TODO Lead Penetration Tester Name uncovered a total of 1 findings that pose a material risk to TODO Customer's information systems. As requested by TODO Customer, this assessment focuses exclusively on findings with medium and high impact, ensuring that all documented vulnerabilities and recommendations are directly relevant to risks that could significantly affect the confidentiality, integrity, and availability of TODO Customer's systems. The below table provides a summary of the findings by severity level.

In the course of this penetration test **1 Info** vulnerabilities were identified:

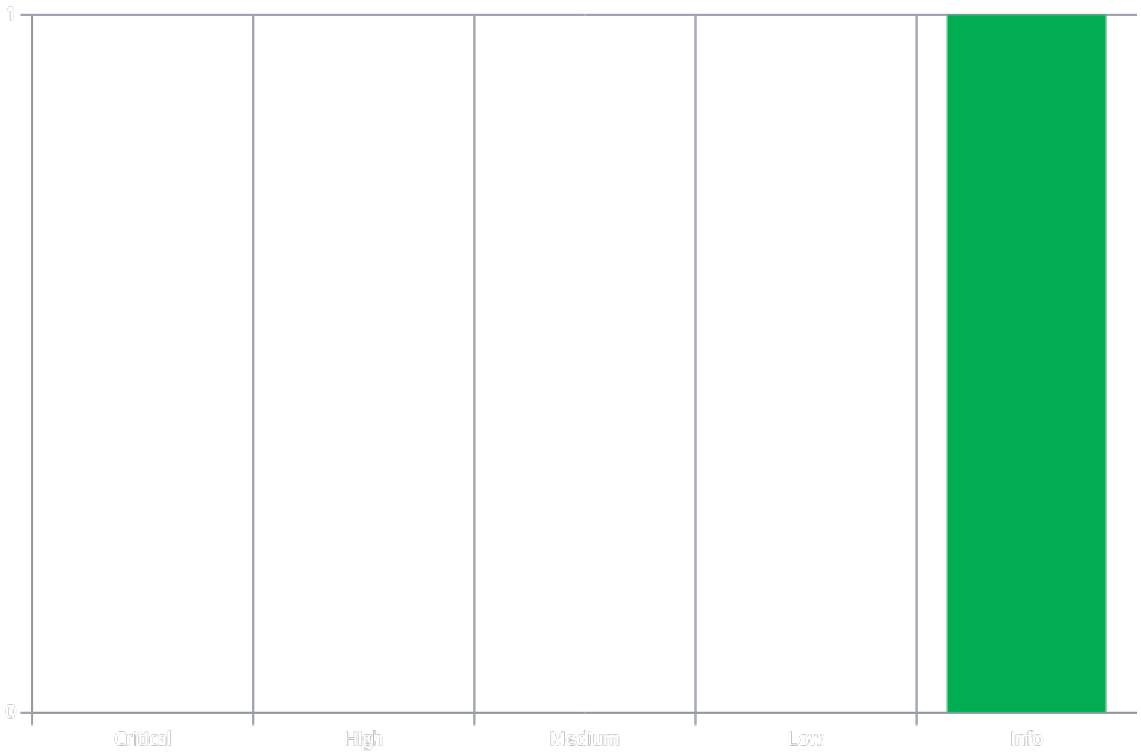

Figure 1 - Distribution of identified vulnerabilities

Below is a high-level overview of each finding identified during testing. These findings are covered in depth in the Technical Findings Details section of this report.

#	Severity Level	Finding Name	Page
1	0.0 (Info)	TODO FINDING TITLE	10

5 Internal Penetration Test Narrative

During the course of the assessment, TODO Lead Penetration Tester Name performed the following series of steps to test TODO Customer's internal network, with the goal of finding as much as possible and taking whatever attack chains may be discovered on whatever hosts in whatever services as far as they can possibly be taken.

The steps below highlight all tests performed, all commands executed, and, if a path to compromise was discovered, all steps taken leading up to said compromise.

The purpose of this narrative is to demonstrate to TODO Customer the potential impact of the vulnerabilities identified in this report and how they interconnect to represent the overall risk to the environment. This approach also helps to prioritize remediation efforts—patching even two critical flaws could disrupt any potential attack chain that this narrative may contain significantly while allowing the organization time to address other reported issues.

5.1 Detailed Narrative

TODO Lead Penetration Tester Name performed the following steps to thoroughly cover all bases within TODO Customer's internal network:

1. TODO BRIEF SINGLE SENTENCE OVERVIEW OF STEP TAKEN DURING NARRATIVE
2. ...

If any systems within TODO Customer's internal network were compromised, the following steps detail how the compromise occurred:

1. TODO LIST STEPS TO ACHIEVE COMPROMISE
2. ...

Detailed reproduction steps for this narrative are as follows: TODO FILL IN FULL NARRATIVE DETAILS, INCLUDING SCREENSHOTS AND COMMAND OUTPUT

6 Remediation Summary

As a result of this assessment there are several opportunities for TODO Customer to strengthen its internal network security. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete. TODO Customer should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

6.1 Short Term

TODO SHORT TERM REMEDIATION:

- Finding Reference 1 - Set strong (24+ character) passwords on all SPN accounts
- Finding Reference 2 - TODO FILL IN AS APPROPRIATE
- Finding Reference 3 - Enforce a password change for all users because of the domain compromise

TODO FILL IN BASED ON FINDINGS, EXAMPLES LEFT FOR REFERENCE

6.2 Medium Term

TODO MEDIUM TERM REMEDIATION:

- Finding Reference 1 - Disable LLMNR and NBT-NS wherever possible
- Finding Reference 2 - TODO FILL IN AS APPROPRIATE

TODO FILL IN BASED ON FINDINGS, EXAMPLES LEFT FOR REFERENCE

6.3 Long Term

TODO LONG TERM REMEDIATION:

- Perform ongoing internal network vulnerability assessments and domain password audits
- Perform periodic Active Directory security assessments
- Educate systems and network administrators and developers on security hardening best practices compromise
- Enhance network segmentation to isolate critical hosts and limit the effects of an internal compromise
- TODO FILL IN AS APPROPRIATE

TODO FILL IN BASED ON FINDINGS, EXAMPLES LEFT FOR REFERENCE

7 Technical Findings Details

1. TODO FINDING TITLE - Info

CWE	CWE-89 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CVSS 3.1	N/A
Root Cause	TODO DESCRIPTION
Impact	TODO IMPACT
Remediation	TODO REMEDIATION
References	-

Finding Evidence

```
ADD COMMAND OUTPUT AS APPROPRIATE
```

TODO ADD SCREENSHOTS AS APPROPRIATE

A Appendix

A.1 Finding Severities

Each finding has been assigned a severity rating of critical, high, medium, low or info. The rating is based off of an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability of TODO Customer's data.

Rating	CVSS Score Range
Critical	9.0 – 10.0
High	7.0 – 8.9
Medium	4.0 – 6.9
Low	0.1 – 3.9
Info	0.0

A.2 Host & Service Discovery

IP Address	Port	Service	Notes
TODO FILL IN AS APPROPRIATE			

A.3 Subdomain Discovery

URL	Description	Discovery Method
TODO FILL IN DISCOVERED VHOSTS/SUBDOMAINS		

A.4 Exploited Hosts

Host	Scope	Method	Notes
TODO FILL IN AS APPROPRIATE	Text	Text	Text

A.5 Compromised Users

Username	Type	Method	Notes
TODO FILL IN AS APPROPRIATE	Text	Text	Text

A.6 Changes/Host Cleanup

Host	Scope	Change/Cleanup Needed
TODO FILL IN AS APPROPRIATE		

End of Report

This report was rendered
by SysReptor with
♥