[CLIENT]

Security Assessment Findings Report

Business Confidential

Date: May 8th, 2024
Project: ALT
Version 1.0

Table of Contents

Confidentiality Statement

This article is the sole property of [CLIENT] and [CONSULTANT]. This document includes private and confidential information. Duplication, dissemination, or use, in whole or in part, in any form, requires the permission of both [CLIENT] and [CONSULTANT].

[CLIENT] may share this material with auditors under non-disclosure agreements to verify compliance with penetration testing requirements.

Disclaimer

A penetration test is viewed as a snapshot in time. The findings and recommendations are based on the information obtained during the evaluation and do not include any changes or revisions made beyond that period.

Time-limited engagements do not allow for a comprehensive assessment of all security controls. [CONSULTANT] prioritized the evaluation to find the most vulnerable security controls an attacker may exploit. [CONSULTANT] suggests that similar assessments be conducted on an annual basis by internal or third-party assessors to verify that the controls remain effective.

Contact Information

[CLIENT]		
Name	Title	Contact Information

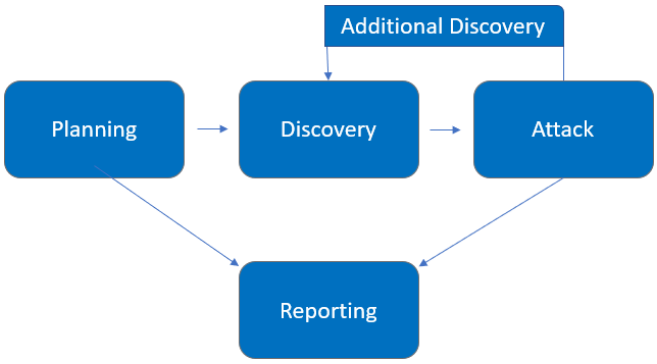
[CONSULTANT]		
Name	Title	Contact Information
Zandro Dadulla Jr.	Penetration Tester	zandro@techwithz.com

Assessment Overview

[CLIENT] engaged [CONSULTANT] from [START DATE], to [END DATE], to assess the security status of its infrastructure in relation to the latest industry standards, which involved conducting an internal network penetration test. The testing conducted is based on the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and tailored testing frameworks.

Phases of penetration testing activities include the following:

- Planning – Customer goals are identified, and rules of engagement are established.
- Discovery – Perform scanning and enumeration to identify possible vulnerabilities, weak points, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation, then conduct additional discovery with new access.
- Reporting – Document all discovered vulnerabilities and exploits, unsuccessful attempts, and company strengths and weaknesses.



Assessment Components

Internal Penetration Test

An internal penetration test simulates the actions of an attacker from within the network. An engineer will scan the network for possible host vulnerabilities and carry out common and sophisticated internal network attacks, including LLMNR/NBT-NS poisoning and other man-in-the-middle attacks, token impersonation, kerberoasting, pass-the-hash, golden ticket, and others. The engineer will attempt to acquire access to hosts via lateral movement, compromise domain user and admin accounts, and exfiltrate sensitive data.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Risk Factors

Risk is measured by two factors: Likelihood and Impact:

Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, the attacker's skill level, and the client environment.

Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

Scope

Assessment	Details
Internal Penetration Test	172.16.1.0/24

Scope Exclusions

As per the client's request, [CONSULTANT] did not conduct any of the following attacks during testing:

- Denial of Service (DoS)
- Phishing/Social Engineering

Client Allowances

[CLIENT] did not provide any allowances to assist with the testing.

Executive Summary

Between [START DATE] and [END DATE], [CONSULTANT] conducted penetration testing to assess [CLIENT]'s internal security posture. The parts that follow offer a high-level summary of the vulnerabilities discovered, successful and unsuccessful attempts, as well as strengths and weaknesses.

Scoping and Time Limitations

Throughout the engagement, scoping prohibited denial of service or social engineering in any testing components.

Testing was limited in duration. Internal network penetration testing was approved for two (2) days.

Testing Summary

The internal network security posture of [CLIENT] was analyzed as part of the network evaluation. To analyze the network's overall patching condition, the [CONSULTANT] team performed vulnerability assessments across every IP address provided by [CLIENT]. The group also carried out common Active Directory-based attacks, such as [ATTACK 1], [ATTACK 2], [ATTACK 3], [ATTACK 4], and [ATTACK 5].

The [CONSULTANT] team discovered that SMB signing was enabled on the workstations (Finding IPT-001), allowing the team to intercept and relay user hashes over the network, which then allows the team to dump local account hashes. These hashes were taken offline and cracked using dictionary attacks, indicating a poor password policy (Finding IPT-005). Using the cracked passwords, the [CONSULTANT] team gained access to multiple devices on the network, indicating overly permissive user accounts.

Using the acquired hashes, the [CONSULTANT] team found that local account hashes were being reused among devices, allowing machine access via pass-the-hash attacks (Finding IPT-002). The [CONSULTANT] team leveraged a compromised domain user-level account to acquire a service account via a Kerberoasting attack (Finding IPT-007), which was then taken offline, and the team was able to crack the service account hash.

Lastly, the [CONSULTANT] team discovered that the compromised service account had domain admin privileges, which allowed the team to access the domain controller and compromise the whole domain. Please see Finding IPT-008 for a detailed guide on acquiring Domain admin access.

In addition to the aforementioned compromise, the [CONSULTANT] team also discovered that LLMNR was enabled on the network, allowing them to intercept user hashes via LLMNR poisoning (Finding IPT-006). The team also determined that delegation attacks could be used to impersonate users (Finding IPT-004), and IPv6 traffic was not restricted potentially leading

to LDAPS relaying and domain compromise (Finding IPT-003). For further details on the findings, please see the Technical Findings section.

Tester Notes and Recommendations

[CONSULTANT] discovered numerous vulnerabilities within Active Directory that are enabled by default, namely LLMNR, IPv6, and Kerberoasting.

During testing, two things stood out: a poor password policy and overly permissive accounts. The weak password policy resulted in an initial compromise of accounts and is typically one of the first footholds an attacker seeks to employ in a network. The presence of a weak password policy is supported by the fact that our testing team cracked over 5 user account passwords, including Domain Administrator accounts, using basic dictionary attacks.

We advised that [CLIENT] review its current password policy and consider a policy of 15 characters or more for regular user accounts and 30 characters or more for Domain Administrator accounts. We also urge that [CLIENT] look into password blacklisting and will provide a list of cracked user passwords for the staff to review. Finally, a Privilege Access Management solution should be considered.

We recommend that the [CLIENT] team review the accounts with domain admin privileges and make sure to implement least privilege and avoid assigning domain and local admin privileges to service and user accounts.

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

1. Strength
2. Strength

The following identifies the key weaknesses identified during the assessment:

1. Weakness
2. Weakness

Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

Internal Penetration Test Findings

6	1	0	0	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
IPT-001: Insufficient Hardening – SMB Signing Disabled	Critical	Enable SMB signing on all [CLIENT] domain computers.
IPT-002: Security Misconfiguration – Local Admin Password Reuse	Critical	Utilize unique local admin passwords and limit local admin users via least privilege.
IPT-003: Security Misconfiguration – IPv6	Critical	Restrict DHCPv6 traffic and incoming router advertisements in Windows Firewall via GPO.
IPT-004: Insufficient Hardening – Token Impersonation	Critical	Restrict token delegation.
IPT-005: Insufficient Password Complexity	Critical	Implement CIS Benchmark password guidelines / PAM solution.
IPT-006: Insufficient LLMNR Configuration	Critical	Disable multicast name resolution via GPO.
IPT-007: Insufficient Privileged Account Management – Kerberoasting	High	Utilize Group Managed Service Accounts (GMSA) for privileged services.
IPT-008: Steps to Domain Admin (Informational)	Informational	Review action and remediation steps.

Technical Findings

Internal Penetration Test Findings

Finding IPT-001: (Critical)

Description	
Risk	
System	
Tools Used	
References	

Evidence

[SCREENSHOT]

Figure 1: [CAPTION]

Remediation

Finding IPT-00X: (Critical)

Description	
Risk	
System	
Tools Used	
References	

Evidence

[SCREENSHOT]

Figure 2: [CAPTION]

Remediation

Finding IPT-00X: Steps to Domain Admin (Informational)

The steps below describe how the penetration tester obtained domain administrator access. Each step also provides remediation recommendations to help mitigate risk.

Step	Action	Remediation
1	Discovered that SMB signing is enabled on the workstations and utilized that to capture NetNTLMv2 hash and dump local user hashes from the machines.	Enable SMB Signing. Disable NTLM authentication.
2	Cracked the captured NetNTLMv2 hash of a domain user account called “bsmith”.	Increase password complexity. Implement a Privileged Account Management (PAM) solution. Utilize a password filter
3	Leveraged the password of “bsmith” to retrieve the hash of a service account via Kerberoasting and was able to crack the hash.	Increase password complexity for service accounts. Implement a Privileged Account Management (PAM) solution.
4	Found that the compromised service account has Domain Admin privileges which allowed access to the Domain Controller.	Implement least privilege or account tiering.
5	Utilized the compromised service account to dump the hashes stored in the Domain Controller.	

Remediation

Review action and remediation steps.

Additional Scans and Reports

[CONSULTANT] provides all clients with the report data gathered during testing. This includes Nessus files and comprehensive vulnerability scans in detailed formats. These reports include raw vulnerability scan results as well as other vulnerabilities that [CONSULTANT] did not attempt to exploit.

The reports indicate hygiene concerns that require attention but are less likely to result in a breach, such as defense-in-depth opportunities. For further information, please refer to the papers in the folder named "*Additional Scans and Reports*".

LAST PAGE