Internal Pentest

Executive Summary

[redacted] Penetration Test | 2026Q1

Abacus Information Technology LLC - Flex -

Apr 16, 2026

ABACUS

Website abacustechnology.com

Email CyberRedTeam@abacustechnology.com

Phone (866) 888-1943

POWERED BY HORIZON3.ai

Summary

Started	**Apr 16, 2026, 5:56 PM UTC**	Initiated by	[redacted]	NodeZero IP	**192.168.40.113**
Completed	**Apr 16, 2026, 7:31 PM UTC**	For client	**Abacus Information Technology LLC - Flex -**	Hosts Assessed	**72**
Duration	**1h 35m**				

0	33	12	0
Attack Paths Exploited	**Weaknesses Found**	**Credentials Compromised**	**Hosts Compromised**

Overall Exposure Level: Medium

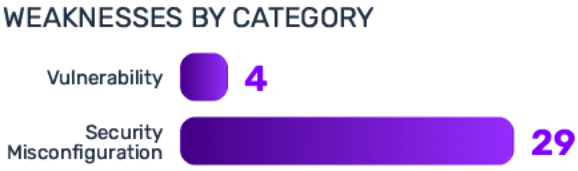
This exposure level stems from finding and exploiting **significant weaknesses** in the network.

Remediate the weaknesses identified to reduce the exposure level.

Top Business Risks and Impacts

33 weaknesses were discovered during the pentest. These weaknesses did not lead to any impacts.

Top Weaknesses



Fixing the following weaknesses will reduce the organization's cyber risk:

1. **H3-2020-** Domain Controller [redacted] and Domain Controller [redacted] Allowing zone transfers to any server provides an attacker with information that can be used to identify target systems. This information may be used to carry out additional attacks.
2. **H3-2022-0069: Web Dir L** ion on [redacted] port 443 and application Application on [redacted] port 80. Directory listings can enable an attacker to gain unauthorized access to sensitive information on the web server, such as source code, configuration files, keys, webserver data, and webserver backup files.

3. **ortname Disclosure** affecting application Microsoft IIS on [redacted] port 80. Remote attackers can discover and read sensitive files hosted by the webserver more easily than with traditional brute-forcing.

Systemic Issues

No Systemic Issues Found

MITRE

This diagram illustrates the actions of NodeZero, as they pertain to MITRE tactics and techniques. Each tile indicates how many attack modules were used for a given technique during the pentest. A total of **1,857 attack modules** employed **34 techniques** across **8 MITRE tactics**.

Reconnaissance

Active Scanning 232 T1595	Gather Victim Network Information 215 T1590	Gather Victim Host Information 191 T1592	Search Victim-Owned Websites 56 T1594

Initial Access

External Remote Services 57 T1133	Valid Accounts 57 T1078	Exploit Public-Facing Application 41 T1190

Credential Access

Brute Force 96 T1110	Exploitation for Credential Access 4 T1212	OS Credential Dumping 4 T1003	Adversary-in-the-Middle 1 T1557	Forced Authentication 1 T1187
Unsecured Credentials 1 T1552				

Discovery

Network Service Scanning 304 T1046	System Information Discovery 131 T1082	Remote System Discovery 117 T1018	Software Discovery 117 T1518	Account Discovery 22 T1087
System Service Discovery 18 T1007	Permission Groups Discovery 8 T1069	Container and Resource Discovery 7 T1613	Network Share Discovery 4 T1135	Password Policy Discovery 2 T1201
File and Directory Discovery 1 T1083				

Lateral Movement

Remote Services 58 T1021	Exploitation of Remote Services 41 T1210	Use Alternate Authentication Material 1 T1550

Collection

Screen Capture 62 T1113	Data from Information Repositories 2 T1213	Adversary-in-the-Middle 1 T1557

Command and Control

Application Layer Protocol 1 T1071	Non-Standard Port 1 T1571	Encrypted Channel 1 T1573

Impact

Data Manipulation 2 T1565		

Top Credentials

1 LOW **ADMIN**

1 LOW **ADMIN**

1 LOW **Administrator**

As illustrated by severity, the pentest discovered **12 credentials** in total. The most impactful credentials likely contribute to the most critical attack paths.