VA REPORT

XYZ Corporation – Quarter 1, 2023

Vulnerability Assessor – Avinash Yadav
Phone Number – +91 xxxx-yyyyyy
Email – avinashyadav@protonmail.com

Document Control

Document Version	Owner & Role	Status & comments
v1.0	Avinash Yadav – Penetration Tester	Prepared the Internal Draft

Disclaimer

The content of this report is highly confidential and may include critical information on XYZ-CORPORATION systems, network, and applications. The report should be shared only with intended parties.

Although maximum effort has been applied to make this report accurate, Avinash Yadav cannot be held responsible for inaccuracies or systems changes after the report has been issued since new vulnerabilities may be found once the tests are completed.

Moreover, Avinash Yadav cannot be held responsible on how the report is implemented and changes made to XYZ-CORPORATION systems based on the recommendations of this report. Guidance should be taken from a network and security expert on how best to implement the recommendations.

All other information and the formats, methods, and reporting approaches is the intellectual property of Avinash Yadav and is considered proprietary information and is provided in confidence to XYZ-CORPORATION for the purpose of internal use only.

Any copying, distribution, or use of any of the information set forth herein or in any attachments hereto form outside of XYZ-CORPORATION authorized representatives is strictly prohibited unless XYZ-CORPORATION obtains prior written consent of Avinash Yadav.

Table of Contents

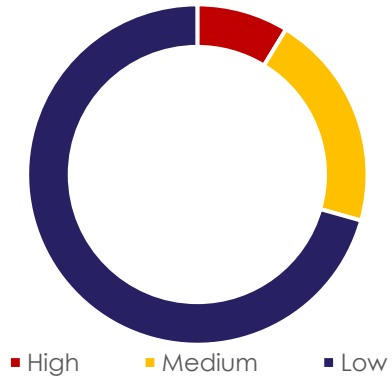
Executive Summary

I was tasked with performing an internal vulnerability assessment on the XYZ-CORPORATION network which revealed a need for Immediate Attention. A grand total of ten machines were assessed over the period from 22 February, 2023 to 24 March, 2023.

My overall objective was to evaluate the network, identify systems, perform automated vulnerability scanning on each system and report the findings back to XYZ-CORPORATION.

These activities were all performed with no prior knowledge of XYZ-CORPORATION state of security for the systems under assessment and I was able to discover major flaws in all of the ten systems, primarily related to outdated patches and poor security configurations.

Some of the vulnerabilities I found in the network are enough to do intrusions, leaking highly sensitive data, making alterations and even damaging the availability of the systems.



It appears that the overall security posture is extremely poor and is mostly due to human related error like patch management issues, and no compliance to best practices. Every vulnerability has been categorized and allocated a risk score, from High/Critical (urgent action needed), Medium (action needed), Low (action needed but not immediately).

In conclusion, based on the results of the tests, I believe that the current internal security defenses are deemed below the expected level of security, therefore the overall assessment was rated as **"Immediate Attention & Action Required".**

Security Posture

The scope was to identify, analyze and rank vulnerabilities on XYZ-CORPORATION systems that may be exploited by malicious attackers, using manual and automated methods.

List of machines included in scope of this vulnerability assessment were as follows:

IP Address	Operating System
192.168.26.40	Microsoft Windows 11
192.168.26.45	Ubuntu 8
192.168.26.50	CentOS 2.6.18
192.168.26.55	Microsoft Windows Server 2012
192.168.26.60	Microsoft Windows 11
192.168.26.65	Ubuntu 8
192.168.26.70	CentOS 2.6.18
192.168.26.75	Microsoft Windows Server 2012
192.168.26.80	Microsoft Windows Server 2012
192.168.26.85	Redhat Enterprise Linux 4.7

Total Findings	High	Medium	Low
1,066	**93**	**220**	**753**

Overall Security Rating – Bad Security Posture – Immediate Attention and Action Required!

Methodology

I utilized a widely adopted approach or process to perform the automated vulnerability assessment to identify as many vulnerabilities as possible on XYZ-CORPORTION systems. Below, a breakdown of the applied methodology is provided.

1. Information Gathering – Passive and active reconnaissance on the given systems.
2. Vulnerability Identification – Finding vulnerabilities by scanners and manual researches.
3. Vulnerability Analysis – Studying the vulnerabilities with their causes, impacts, fixes, etc.
4. Vulnerability Ranking – Giving a severity rating to each vulnerability based on impact.
5. Reporting – Making a final report containing all details of the vulnerability assessment.

Note: No exploitation or intrusive penetration testing tasks were involved in these tests.

Tools Utilized

Only industry grade vulnerability scanners alongside reputed tools & websites were used.

1. Nessus Essentials – Free version of the most popular vulnerability scanner software.
2. Nexpose Trial – Rapid7's on-premises option for vulnerability management software.
3. VEGA – A free web application vulnerability scanner by Subgraph.
4. Faraday CE – A tool for collaborative vulnerability management by FaradaySec.
5. NIST CVSS Calculator – NIST's tool to calculate vulnerability scores based on CVSS.

Specific Hosts & Vulnerabilities

This part of the report deals with vulnerabilities found in specific systems.
It will cover details about each machine involved in this test, one by one.

Details such as vulnerabilities, bugs, errors, exploits and their impact on specific systems.

Detailed Findings

Network Infrastructure Assessment

192.168.26.45

Issue	Impact	CVE	Ease	Recommendation
According to its banner, the version of PHP installed on the remote host is older than 4.4.5. Such versions may be affected by several issues, including buffer overflows, format string vulnerabilities, arbitrary code execution, 'safe_mode' and 'open_basedir' bypasses, and clobbering of super-globals.	High	CVE-2017-010	Easy	Upgrade to PHP version 4.4.5/ 5.1.4 or later.
The remote version of Apache is vulnerable to an off-by-one buffer overflow attack.	High	N/A	Easy	Upgrade to version 2.0.59 or later.
The remote DNS resolver does not use random ports when making queries to third party DNS servers. This problem might be exploited by an attacker to poison the remote DNS server more easily, and therefore divert legitimate traffic to arbitrary sites.	High	N/A	Moderate	Contact your DNS server vendor for a patch The ports used by 81.29.66.2 are not random. An attacker may spoof DNS responses. List of used ports : - 59574 - 59574 - 59574

Recommendations

Recommendations in this report are based on the available findings from the vulnerability assessment. Vulnerability scanning is only one tool to assess the security posture of a network. The results should not be interpreted as definitive measurement of the security posture of the XYZ-CORPORATION network. Other elements used to assess the current security posture would include policy review, a review of internal security controls and procedures, or internal red teaming/penetration testing.

Though mitigation for specific vulnerabilities has already been given previously in this report, we would like to recapitulate some of the most important fixes.

Taking the following actions across all hosts will resolve 93% of the vulnerabilities on the network:

Action To Take	Vulnerabilities	Hosts
Google Chrome < 68.0: Upgrade to Google Chrome version 68.0 or later.	82	3

Additional Items

Appendix A - CVSS Vulnerability Scores:

i. **CVE-2017-0144 (*https://nvd.nist.gov/vuln-metrics/c...*)**

Final Vector: C:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS Base Score: 9.8

Impact Subscore: 5.9

Exploitability Subscore: 3.9

Overall CVSS Score: 9.8

Appendix B - Screenshot Showing Nessus Scan Summary: