Penetration Test Report

Date: August 4, 2024
Tester: Peter Banchoff
Target Company: John's Awesome Steakhouse
Target IP Address: 192.168.13.129
Target Operating System: Windows 10
Target Web Server: XAMPP/Apache

Executive Summary

The Penetration test conducted on your network infrastructure aimed to identify and analyze potential security vulnerabilities that could easily be exploited by threat actors. The scope of this test included both external and internal network components, as well as web applications.

Objectives

- To evaluate the security posture of the network's infrastructure.
- Identify the vulnerabilities that could lead to data breaches or unauthorized access.
- Provide recommendations to enhance the security measures.

Key Findings

Critical Vulnerability: The default username and password were found on the web server, making it easy for threat actors to predict and crack those credentials.

Remedy: Change the password immediately, using at least 12 characters with a mix of upper case and lower case letters, numbers, symbols, an avoiding common words and personal information.

Critical Vulnerability: The remote host is running an outdated version of OpenSSL, which is version 3.1.0, and has not been updated to version 3.1.7.

Remedy: Update OpenSSL to the newest version.

Critical Vulnerability: The remote host is running an outdated version of Apache, which is version 2.4.58. This version is affected by multiple vulnerabilities, such as CVE-2024-36387, and CVE-2024-28472.

Remedy: Update Apache to version 2.4.60 or later.

High Vulnerability: The SSL certificate chain uses a weak hashing algorithm, SHA-1. This is vulnerable to collision attacks.

Remedy: Contact the Certificate Authority to have the SSL certificate reissued with a stronger algorithm.

Medium Vulnerability: The SSL certificate cannot be trusted as it has an unknown certificate authority and expired on November 4, 2019.

Remedy: Purchase or generate a proper SSL certificate for this service.

Medium Vulnerability: The remote web server supports TRACE/TRACK methods, allowing threat actors to potentially conduct Cross-Site Tracing (XST) attacks.

Remedy: Disable HTTP TRACE/TRACK methods.

Recommendations

- Implement strong password policies and change the default credentials immediately.
- Regularly update software and apply patches.
- Ensure that the SSL certificates are issues by trusted authority and use stronger hashing algorithms.
- Disable unnecessary HTTP methods to shrink the attack surface.

Overall, this test revealed critical and high severity vulnerabilities that require immediate attention. Addressing these vulnerabilities and implementing the recommended measures will assist John’s Awesome Steakhouse to enhance the security posture and reduce added risk of potential breaches.