Penetration Test Report

Executive Summary

Overview

The Penetration Test conducted on your network infrastructure aimed to identify and analyze potential security vulnerabilities that could easily be exploited by threat actors.

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Critical Vulnerability: The remote host is running an outdated version of OpenSSL, which is version 3.1.0, and has not been updated to version 3.1.7.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Critical Vulnerability: The remote host is running an outdated version of Apache, which is version 2.4.58.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.

Overall Risk Rating

9/10

Recommendations

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

Assessment Summary

Scope

Company Name: John's Awesome Steakhouse.
Target Location: Livonia, MI
Target IP Address: 192.168.13.129
Target Operating System: Windows 10
Target Web Server: Apache/XAMPP

Methodology

- Confirmed IP connection via Ping.
- Located the open ports to the server using Nmap.
- Discovered a series of vulnerabilities in the Network with Nessus.
- Obtained knowledge of Web Application's Vulnerabilities through Nikto.
- Tested the Vulnerabilities with Metasploit
- Used Brute Force method to obtain access into the Web Server.

Risk Ratings

9/10

Notes

It is highly recommended that the server is reconfigured to avoid any more potential pitfalls with a default configuration. A suggestion would be for the Firewall to be reconfigured to fit the needs of your business, as well as ensuring that the Web Server and all applications are updated to their latest version. Lastly, updating the password criteria is a must to avoid further attempts of exploitation from threat actors.