Name of Individual Conducting Scanning:	Daniel Owen
Nessus Scanner IP (IP of Kali VM):	10.0.2.15
Date &Time Scan Started:	15/05/2024, 9:35
Date &Time Scan Finished:	15/05/2024, 9:45
Security Issues Identified:	47 Vulnerabilities

Overview

The scan returned a total of 47 vulnerabilities, with 96% being info and the other 4% is split evenly across Low and Medium risk.
The scan discovered 4 vulnerabilities within the SSL certificate, with the server's X.509 certificate being rated as Medium risk, found with the plugin ID: 51192, it has a CVSS base score of 6.5.
the remaining 3 vulnerabilities are rated as info.
The version of OpenJDK installed on the remote host is prior to 8. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024-04-16 advisory. This vulnerability was found with the plugin ID: 193405, it has a CVSS base score of 3.7. It is rated as Low risk.

Top 5 Most Serious Security Issues (In priority order - most important first):

>> What are the 5 most critical issues with the scanned system? Talk about each one, and what could happen if an attacker exploits the vulnerability <<

- Security flaw 1 - The most serious issue discovered is the server's X.509 certificate could not be trusted. This situation can occur in 3 different ways:
  (A) The top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

(B) The certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

(C) The certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

This vulnerability could result in an attacker carrying out a man-in-the-middle attacks against the remote host.

- Security flaw 2 - The second most vulnerable issue found was the version of OpenJDK installed on the remote host is prior to 8. the Vulnerability in the Oracle Java SE allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. (CVE-2024-21094)

- Security flaw 3 - The third issue is enumeration of the network interfaces configured with IPv4 addresses by connecting to the remote host via SSH using the supplied credentials.
  Whilst the risk factor is none, this could potentially pose a risk by allowing remote access from an unauthorised user. They could then perform malicious activities, such as stealing sensitive information and data.

- Security flaw 4 - The fourth issue is the Apache HTTP server installed on the remote linux host. Although the risk factor is none, if an attacker is to discover a vulnerability within Apache it could result in various security issues such as remote code execution and scripting.
- Security flaw 5 - The fifth issue is the HTTP server type and version. The reference information is IAVT: 0001-T-093. The risk factor is none. If a vulnerability was to be discovered, an attacker could carry out a Denial-of-service (DOS) attack which could cause the system to crash or become unusable.

Top 5 - Remediations (In priority order - most important first):

- My suggestions to address the issue related to the server's X.509 certificate would be to purchase or generate a proper SSL certificate and configure the server to use the newly aquired certificate.

- In order to resolve this issue, I would suggest upgrading to an OpenJDK version greater than 8u402 / 11.0.22 / 17.0.10 / 21.0.2 / 22.0.0 making sure to apply the patch and that the version is current.

- To resolve the SSH issue it would be wise to disable any unused IPv4 interfaces on the host system.

- To address vulnerabilities related to Apache HTTP make sure the latest patch and updates are installed on the linux host device.
- To address this issue make sure the HTTP server type and version are not disclosed to the public. Also making sure that the latest patches are applied.