A green chameleon logo

Description automatically generated

**SSL SCAN**

​​

TABLE OF CONTENTS

1-Summary

2- Introduction

3- Tools Used

4-Scope of testing

5-Results

6-Conculsions

7-References

**EXECUTIVE SUMMARY**

A diagram of a computer network

Description automatically generated

In summary, SSL scanning is a crucial aspect of web security, providing insights into the strength of a website's SSL/TLS security measures. Regular scans help organizations maintain a secure and up-to-date cryptographic configuration, ensuring the protection of sensitive data during communication.

**INTRODUCTION**

SSL scanning, also known as SSL/TLS scanning, refers to the process of evaluating the security configuration and implementation of the SSL/TLS protocols on a web server or network. The goal is to identify potential vulnerabilities and weaknesses that could be exploited by attackers. SSL scans are conducted using specialized tools and services to assess the strength of cryptographic protocols, cipher suites, certificate configurations, and overall security settings.

Here's an introduction to SSL scanning:

SSL scanning aims to assess the security of the SSL/TLS implementation on a website or server.

It helps identify and mitigate potential vulnerabilities that could compromise the confidentiality and integrity of data transmitted over the network.

**TOOLS USED**

Tools and Services:

SSL scans are performed using dedicated tools and online services designed to analyze the SSL/TLS configuration of a target.

Popular SSL scanning tools include Qualys SSL Labs, SSLyze, testssl.sh, and others.

**SCOPE OF TESTING**

The scope of SSL scanning, like any security testing activity, should be well-defined to ensure that it aligns with organizational goals and meets security objectives. Here are key considerations for defining the scope of SSL scanning:

Authorized Testing:

Ensure that SSL scanning is conducted with explicit authorization from the owner or administrator of the target system or network.

Define Testing Objectives:

Clearly articulate the objectives of SSL scanning. Understand whether the focus is on a specific website, a range of IP addresses, or an entire network.

Scope Inclusions:

Identify the systems, servers, and websites that fall within the scope of SSL scanning. Specify whether the testing includes external-facing servers, internal servers, or both.

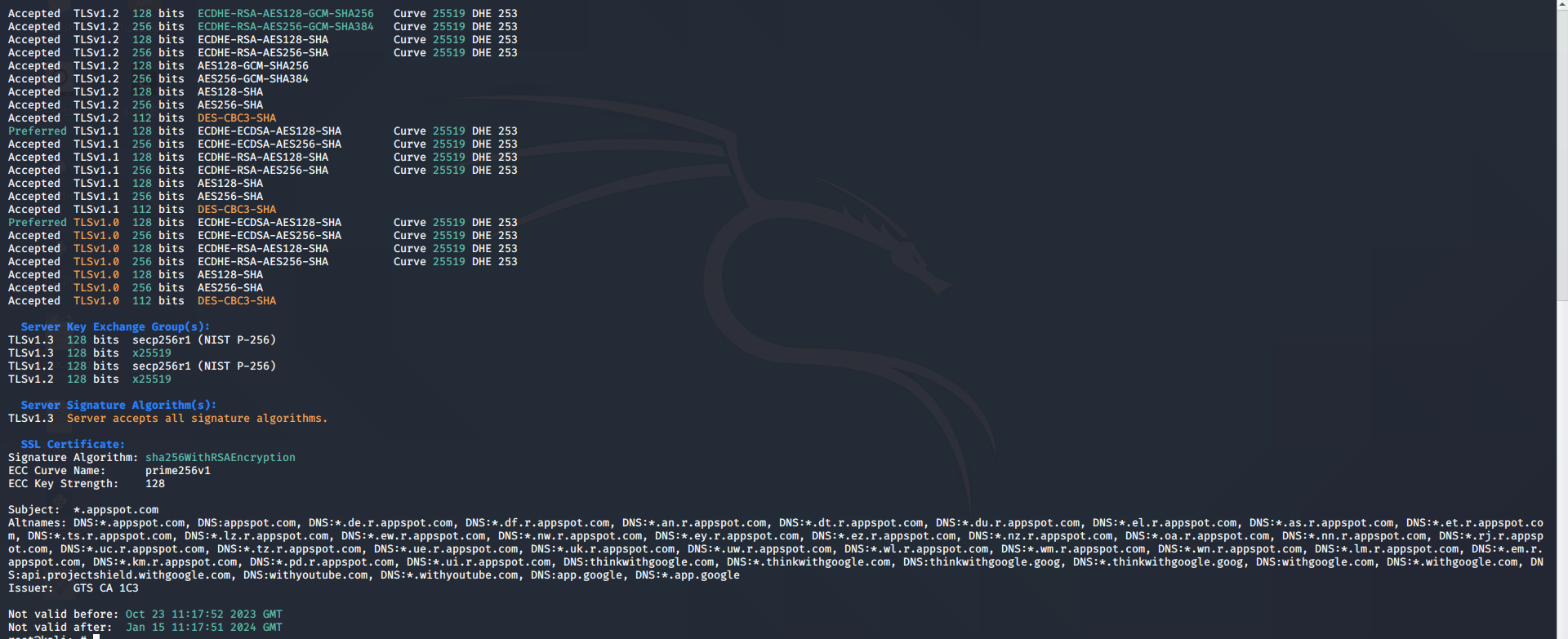
Exclusions:

Clearly define any systems or components that are excluded from SSL scanning. For example, certain critical systems might be excluded to prevent disruption to essential services.

Specific Protocols and Ciphers:

Specify which SSL/TLS protocols (e.g., TLS 1.2, TLS 1.3) and cipher suites are within the scope of testing. This helps ensure that the scanning aligns with the organization's security standards

**RESULTS**



A computer screen shot of a bird

Description automatically generated

**CONCLUSION**

Though this process is tedious and complex, the pinning SSL certificate is worth the effort as it decreases the risk of data leaks and serves as countermeasures against MITM attacks..

References:

1-Team, T.R. (2016). *SSL Scanning and Application Control*. [online] Redscan. Available at: https://www.redscan.com/news/ssl-scanning-and-application-control/ [Accessed 10 Dec. 2023].

‌2-Indusface. (n.d.). *What is SSL Pinning? – A Quick Walk Through| Indusface Learning*. [online] Available at: https://www.indusface.com/learning/what-is-ssl-pinning-a-quick-walk-through/ [Accessed 10 Dec. 2023].

‌