

Understanding SSL/TLS Information Results

The SSL/TLS Information section provides a detailed overview of the SSL/TLS certificates used by the subdomains of the scanned domain. SSL/TLS certificates are crucial for securing data transmitted between a user's browser and the server, ensuring data integrity, confidentiality, and authenticity. The scan results include key information such as the SSL grade, certificate issuer, version of SSL/TLS in use, and expiration dates. This information helps assess the security posture of the domain and identify areas that may need improvement.

Overview of SSL/TLS Information:

This section lists each subdomain with details about its SSL/TLS configuration:

1. **SUBDOMAIN URL:**

The URL of the subdomain using SSL/TLS, such as `https://portal.demodata.com`. This URL indicates the specific subdomain for which the SSL/TLS certificate is being evaluated.

2. **SSL GRADE:**

A grade indicating the quality of the SSL/TLS configuration for the subdomain. Grades typically range from A+ (excellent) to F (poor), with considerations such as encryption strength, supported protocols, and presence of security vulnerabilities.

3. **ISSUED BY:**

Information about the Certificate Authority (CA) that issued the SSL/TLS certificate. This includes the common name (CN) and organization (O) of the issuer, such as "Let's Encrypt" or "DigiCert Inc." Reputable CAs enhance the trustworthiness of the certificate.

4. **ISSUED TO:**

Details about the entity to which the certificate was issued. This includes the common name (CN) and, if applicable, the organization (O) that owns the certificate. The common name usually matches the domain name, indicating that the certificate is valid for that specific subdomain.

5. **SELF SIGNED?:**

Indicates whether the certificate is self-signed (`YES`) or issued by a trusted Certificate Authority (`NO`). Self-signed certificates are less secure because they are not validated by a trusted third party and may be vulnerable to man-in-the-middle attacks.

6. **VERSION NAME:**

Specifies the version of SSL/TLS in use, such as `TLSv1.2` or `TLSv1.3`. Newer versions (e.g., TLSv1.3) offer improved security features and should be preferred over older versions,

which may have known vulnerabilities.

7. EXPIRATION TIME (UTC):

The date and time when the SSL/TLS certificate will expire. An expired certificate can result in security warnings in users' browsers and may expose the subdomain to potential security risks. It's important to renew certificates before they expire to maintain secure communication.

Example Analysis:

Here are some example analyses based on the SSL/TLS scan results:

- **Subdomain:** `https://rdp.demodata.com`
 - **SSL Grade:** A+
 - **Issued By:** Let's Encrypt
 - **Issued To:** `rdp.demodata.com`
 - **Self Signed?:** NO
 - **Version Name:** TLSv1.3
 - **Expiration Time:** 11/04/2023, 06:49 AM
 - **Analysis:** This subdomain has an excellent SSL grade (A+), indicating a secure SSL/TLS configuration. The certificate is issued by a reputable CA (Let's Encrypt) and supports TLSv1.3, the latest version with enhanced security features. The certificate is not self-signed and is valid until April 2023, ensuring secure communication for the subdomain.
- **Subdomain:** `https://soc.demodata.com`
 - **SSL Grade:** T
 - **Issued By:** COMODO CA Limited
 - **Issued To:** `*.oversig.ht`
 - **Self Signed?:** NO
 - **Version Name:** TLSv1.2
 - **Expiration Time:** 18/04/2019, 11:59 PM
 - **Analysis:** This subdomain has a low SSL grade (T), which indicates potential issues with its SSL/TLS configuration. The certificate is outdated, having expired in April 2019, which can lead to browser security warnings and expose the subdomain to security risks. Additionally, the certificate was issued for `*.oversig.ht` rather than the subdomain itself, suggesting a possible misconfiguration. Immediate action is required to renew the certificate and ensure it matches the subdomain correctly.
- **Subdomain:** `https://webconf.demodata.com`
 - **SSL Grade:** B
 - **Issued By:** DigiCert Inc
 - **Issued To:** `*.demodata.com`
 - **Self Signed?:** NO
 - **Version Name:** TLSv1.2
 - **Expiration Time:** 30/11/2023, 11:59 PM

- **Analysis:** This subdomain has a moderate SSL grade (B), indicating a decent but not perfect SSL/TLS setup. The certificate is issued by a reputable CA (DigiCert Inc) and is valid until November 2023. However, it uses TLSv1.2, which, while secure, can be updated to TLSv1.3 for enhanced security. Some improvements may be needed to achieve a higher grade, such as reviewing the supported ciphers and protocols.

Importance of SSL/TLS Monitoring:

Regularly monitoring SSL/TLS configurations is crucial to maintaining a secure environment. Properly configured SSL/TLS certificates ensure encrypted data transmission, protect against man-in-the-middle attacks, and provide users with confidence when accessing your services. Identifying and addressing issues such as expired certificates, outdated protocols, or weak encryption is key to strengthening the overall security posture of your domain.

Revision #2

Created 16 September 2024 12:00:35 by Raphael

Updated 16 September 2024 12:40:55 by Raphael