VII Défi n°1 : scan des algorithmes de chiffrement d'une application web

Le premier défi est le scan d'un serveur web afin de lister les technologies de chiffrement configurées afin d'apprécier leur pertinence dans le cadre d'un audit.

1 Outils et documents

Documents à utiliser :

- document 1 : Recommandations de sécurité relatives à TLS de l'ANSSI ;

- document 2 : Le protocole TLS-1.0 et les cartes de paiement.

Le programme sslscan :

L'outil sslscan permet de détecter la configuration SSL/TLS d'un site et de connaître les dates de création et de péremption des certificats. Les configurations SSL/TLS sont détectées et affichées avec les algorithmes utilisés ainsi que leur version.

Installation sous Linux :

Il faut installer le paquet sslscan depuis les dépôts.

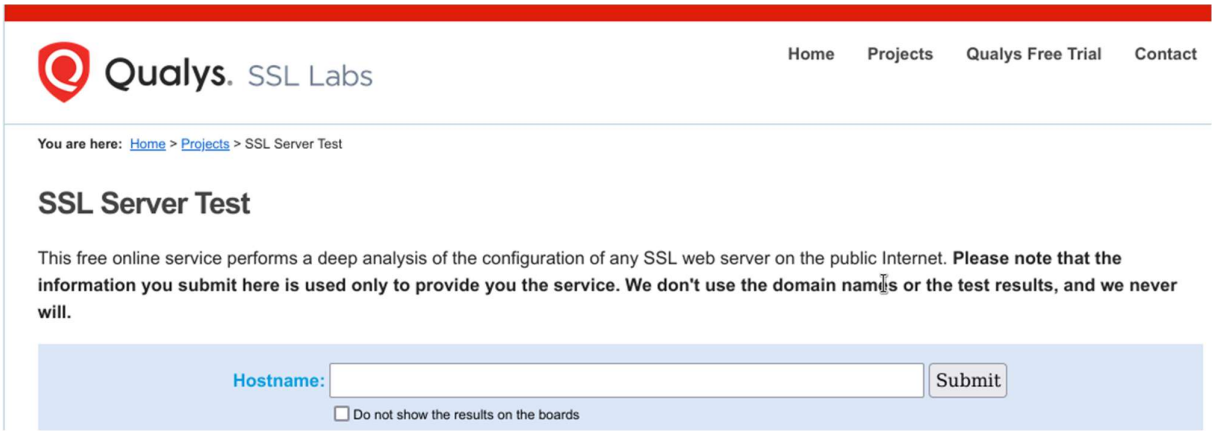
```
#sudo apt install sslscan
```

```
prof@host555:~$ sslscan -h
                _
 ___ ___| |___ ___ __ _ _ __
/ __/ __| / __|/ __/ _` | '_ \
\__ \__ \ \__ \ (_| (_| | | | |
|___/___/_|___/\___\__,_|_| |_|

           2.0.7
           OpenSSL 1.1.1n  15 Mar 2022

Command:
  sslscan [options] [host:port | host]

Options:
  --targets=<file>      A file containing a list of hosts to check.
                        Hosts can  be supplied  with ports (host:port)
  --sni-name=<name>     Hostname for SNI
  --ipv4, -4            Only use IPv4
  --ipv6, -6            Only use IPv6

  --show-certificate    Show full certificate information
  --show-client-cas     Show trusted CAs for TLS client auth
  --no-check-certificate  Don't warn about weak certificate algorithm or keys
  --ocsp                Request OCSP response from server
  --pk=<file>           A file containing the private key or a PKCS#12 file
                        containing a private key/certificate pair
  --pkpass=<password>   The password for the private  key or PKCS#12 file
  --certs=<file>        A file containing PEM/ASN1 formatted client certificates
```

Utilisation en ligne :

L'outil peut s'utiliser en ligne depuis le lien suivant :

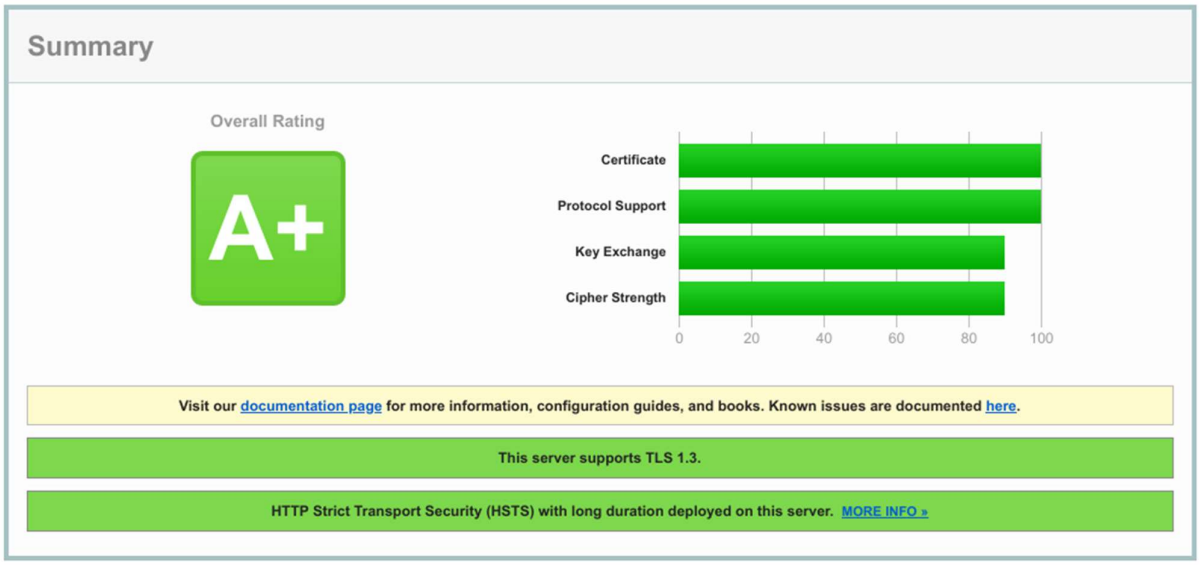
https://www.ssllabs.com/ssltest/



Cet outil teste les éléments suivants :

- Émetteur du certificat, validité, algorithme utilisé pour signer ;
- Détails du protocole, suites de chiffrement, simulation de prise de contact.

Les résultats des tests fournissent des informations techniques détaillées ainsi que des conseils à destination de l'administrateur système, de l'auditeur ou de l'ingénieur de sécurité Web pour connaître et corriger les paramètres faibles.



D'autres outils en ligne existent comme :

- SSL checker :

https://www.thesslstore.com/ssltools/ssl-checker.php

- Geekflare :

https://geekflare.com/fr/tools/tls-test

2 À vous de jouer

Travail à faire 1

Q1. Définir le protocole TLS. Expliquer la différence entre TLSv1.2 et TLSv1.3 en terme de performance et de sécurité.

Q2. Qu'est ce qu'un certificat de sécurité SSL ?. Quel est son rôle dans la sécurisation d'une application web ?

Q3. Qu'est ce qu'une autorité de certification ? Quelle différence entre une autorité privée et une autorité publique. Retrouver la liste des autorités publiques sur votre navigateur.

Q4. Tester la sécurité SSL/TLS des applications suivantes en utilisant les outils de scan :

- Google Gruyere

https://google-gruyere.appspot.com/start

-BWAP (noter le résultat du test de vulnérabilité Heartbleed)

http://itsecgames.com/

- Une application de votre choix développée en atelier de professionnalisation.

Reporter les résultats observés sur votre compte-rendu puis conclure.

Q5. A l'aide de vos recherches sur internet, expliquer ce qu'est la vulnérabilité Heartbleed. Quelles peuvent être les conséquences de cette vulnérabilité ?