Rapport de laboratoire #4

CRY - Mise en place d’une PKI

Alexis Martins

22 juin 2023

1 Questions

1.1 Pourquoi devons-nous transmettre une chaine de certificats dans les deux applications (email et TLS) ?

Cela permet à l'application de vérifier que le certificat utilisé, ainsi que l'ensemble des certificats menant à la racine sont valides et de confiance. Ainsi, on peut s'assurer que le certificat qui nous est donné par le serveur est bien valide, car il a bien été signé par la bonne autorité intermédiaire, qui elle-même a été signée par la bonne autorité racine.

1.2 Comment avez-vous configuré nginx ? Donnez votre fichier de configuration.

Voir le fichier **`default`** qui se situe dans le dossier `webserver_config`.

1.3 Fournissez le résultat du scan de testssl sur votre serveur ainsi que des commentaires, si nécessaire.

Il n'y a pas grand chose de particulier à dire, les seuls points qui ne sont pas "OK" sont liés à l'ordre des cipher suites et à l'OCSP, ce qui est normal. Il a aussi trouvé une vulnérabilité potentielle qui est `BREACH (CVE-2013-3587)`, c'est possible de retirer ce warning en modifiant légèrement la configuration NGINX comme ça :

```
    location / {
        index  index.html;
        gzip off;
    }
```

J'ai réalisé au total 2 scans différents, le premier était avec la version "stable" de testssl qui est la 3.0.8. Cette version n'avait pas la note en fin d'analyse, mais on pouvait y voir ce qui était bien ou non. Le second scan est fait avec la version 3.1 qui est une version "dev", mais on voit en fin de scan la note attribuée par l'outil (je trouvais ça un peu plus sympa).

1.4 Quelle durée de validité avez-vous choisie pour le certificat du serveur TLS ? Pourquoi ?

J'ai choisi une durée de validité de 395 jours (soit environ 1 an et 1 mois) afin de m'aligner sur la durée des certificats comme vu en classe. Cela permet d'améliorer la sécurité par exemple en réduisant le temps d'exposition en cas de compromission d'un certificat.