HPKP

Comprendre HPKP

HPKP est une en-tête HTTPS permettant d'indiqué au client pendant une durée déterminé quel seront les certificats HTTPS qui pourront lui être présenté.

Les problèmes pouvant être rencontrées sont les suivants :

- C'est une méthode TOFU, donc si la personne n'est jamais venu sur site ou après l'expiration de la durée indiqué dans l'en-tête depuis sa dernière visite , on ne pourra assuré quel n'est pas de MITM sur la communication.
- Très casse gueule, si la moindre erreur la personne ne pourra pas accéder au site jusqu'à l'expiration de son en-tête.
- Un changement de certificat se doit d'être réalisé en 3 étapes qui prennent la durée minimum indiqué dans l'en-tête.

Voici les recommandations officiels :

- Toujours avoir une paire de clé/certificat de secours dans l'en-tête en cas de compromissions du serveur.
- La durée de rétention est de 60 jours

Compatibilité avec Let's Encrypt

HPKP est tout comme DANE_TLSA, nativement pas compatible avec **certbot**. Mais avec un peu de rigueur, et les bons arguments, on peut faire en sorte de garder ses clés publiques et donc permettre de garder ses empreintes **HPKP**. N'oubliez pas de faire un deuxième certificat non signé pour la backup.

Générer une entrée HPKP

Pour obtenir le **HASH** du certificat, il faut taper la commande :

```
# openssl req -pubkey < /etc/letsencrypt/wiki.virtit.fr/live/cert.csr |
openssl pkey -pubin -outform der | openssl dgst -sha256 -binary | base64
```

et il suffira d'ajouter une entêtes suivante dans votre serveur WEB, par exemple pour apache :

```
Header always set Public-Key-Pins "max-age=5184000; pin-
sha256=\"JOLIE_PETIT_HASH_ACTIF\"; pin-sha256=\"JOLIE_PETIT_HASH_BACKUP\"; "
```