DNS

Genma

24 septembre 2014

But de cette présentation

Cette présentation est une vulgarisation (et donc une simplification) sur le thème du DNS. Elle se veut accessible à tous et peut de ce fait contenir des approximations.

Quelques principes

Principes

- Les machines connectés à un réseau IP, comme Internet, possèdent une adresse IP.
- Ils envoient et recoivent des "paquets" (comme des colis) qui transitent sur le réseau vers une destination dont l'adresse finale est l'adresse IP du serveur ou celle de la machine.
- Les machines utilisent des adresses IP (des nombres) car cela est plus facile à utiliser dans le cadre de traitement informatisé.

L'humain lui préfère mémoriser du texte qu'une série de nombre abstraits.

Qu'est ce que le DNS ?

Principes

- Les sites webs sont associés à des noms de domaines et se trouvent sur des serveurs (qui ont une adresse IP).
- Un serveur DNS est un annuaire qui fait la correspondance nom de domaine - adresse IP.

Comment ça marche ?

Version simplifiée - vulgarisée

- Quand on tape une adresse url dans le navigateur, par exemple http ://genma.free.fr, l'ordinateur va demander au serveur DNS quel est l'adresse IP du serveur où se trouve le site web demandé.
- L'ordinateur connait alors l'adresse IP du site web.
- Il peut alors envoyer des paquets ("Envoi moi la page d'accueil que je l'affiche", "Tiens voilà les login et mots de passe") et communiquer avec le site web.

Qu'est ce que le blocage par le DNS ?

Principe du blocage

- On enlève la correspondance nom de domaine - adresse IP de l'annuaire DNS.
- Quand une machine demande à ce serveur DNS l'adresse IP d'un site web dont on souhaite bloquer l'accès aux utilisateurs `http://www.piratebay.com`, le serveur DNS ne renvoit rien.

Conséquence : le site web ne s'affiche pas.

Comment le contourner et limites du blocage ?

Deux façons simples

- Connaitre l'adresse IP du serveur et se connecter au site web via une url du type `http://123.456.789.012:80`
- Changer de serveur DNS pour en utiliser un qui contient la correspondance. En effet, par défaut, on utilise les serveurs DNS de son fournisseur d'accès (Free, SFR etc.) qui sont tenues d'appliquer la loi et de "bloquer" l'accès à des sites des jeux en lignes.

Utiliser le DNS de Google ?

Google fourni un DNS

- Google fourni des serveurs DNS aux adresses très simples : 8.8.8.8 et 8.8.4.4
- En les utilisant, Google sait quels sont les sites que l'on consulte...

Rq : en utilisant le DNS du FAI, il en est de même. De même si on cherche le nom d'un site web via Google et que l'on clique sur le résultat proposé...

DNS et Tor

Quand on utilise TOR

- Les requêtes DNS (les demandes de correspondances IP/nom de domaine) ne passent par TOR.
- C'est l'IP de la machine (et non celle de "TOR") qui fait la demande DNS.
- "On" sait donc quel site vous allez consulter (mais le site lui-même ne connaitra pas votre vraie adresse IP, vu que la communication se fait via les adresses IP et via Tor).

C'est ce que l'on appelle le DNS Leak.

Qu'est ce que DNSSec ?

Présentation de DNSSec

- DNSSEC permet de sécuriser les données envoyées par le DNS.
- DNSSEC signe cryptographiquement les enregistrements DNS et met cette signature dans le DNS.
- Ainsi, un client DNS méfiant peut récupérer la signature et, s'il possède la clé du serveur, vérifier que les données sont correctes.

On valide que la correspondance "url-IP" que l'on reçoit est bien celle qui a été certifiée-validée et n'a pas été changée entre temps.