TP2 : Installation et administration d'un serveur DNS

Préambule : *Administration d'un serveur DNS, avec Bind.*

Consignes pour le TP :

- **Rédiger seul·e ou en binôme un rapport tout au long de la séance**, qui contient les configurations et commandes utilisées, vos explications et vos réponses aux éventuelles questions. Ce rapport au format texte brut ou PDF, devra être envoyé par mail à l'intervenant·e, avec le sujet suivant : « *[SSSR][TP2] Nom1 Nom2* ».

- **Remettre la machine en état avant de partir**, en rétablissant la configuration par défaut du réseau, en désinstallant les services inutiles, et en la redémarrant. **Penser à copier auparavant les fichiers** qui ont été modifiés/générés au fil des questions.

- Hormis pour utiliser Firefox et Wireshark, tout le TP doit exclusivement se faire **en utilisant des commandes non-graphiques**, dans un ou plusieurs terminaux (permettant ainsi de se rapprocher des conditions réelles de l'administration de serveurs). Utiliser *vim* ou *emacs* pour éditer les fichiers de configuration est fortement conseillé (en prenant un peu de temps pour suivre un tutoriel, à la fois pour comprendre comment les utiliser, et saisir pourquoi tant de professionnel·le·s ne jurent que par leur utilisation).

Partie I : Jouer avec un client DNS

1. Observer avec Wireshark les requêtes DNS qui sont produites, lorsque vous consulter un site web avec Firefox. Expliquer à quoi sert le protocole DNS et à quel niveau du modèle TCP/IP il se situe.

2. Déterminer quel est le serveur DNS récursif qui est actuellement utilisé par votre ordinateur. À votre avis, comment l'ordinateur a-t-il pris connaissance de l'adresse de ce serveur ?

3. Afin de pouvoir modifier manuellement les serveurs DNS récursifs à utiliser, stopper le service *resolvconf*, qui est en charge de la mise à jour du fichier */etc/resolv.conf*. Ce fichier contient les adresses des serveurs DNS récursifs utilisés par votre ordinateur. Modifier le contenu de ce fichier pour qu'il utilise désormais les serveurs DNS récursifs publics de Lorraine Data Network[1] :

```
nameserver 2001:913::8
nameserver 80.67.188.188
```

1 Uniquement la seconde ligne, si votre machine ne peut pas sortir sur Internet en IPv6.

4. Vérifier avec Wireshark que votre ordinateur utilise bien désormais un des serveurs DNS récursifs que vous avez définis.

5. Utiliser la commande *dig* (installer le paquet *dnsutils* si la commande n'est pas disponible) avec le domaine *arn-fai.net*, pour déterminer :

   a) Les adresses IPv6 et IPv4 du site web qui est associé au domaine.
   b) Le nom des serveurs mails qui sont associés au domaine.
   c) L'adresse reverse (PTR) associée à l'IPv6 trouvée en *a)*.

Partie II : Installer et configurer un serveur DNS

1. Quelle est la différence entre un serveur DNS récursif et un serveur DNS qui fait autorité ?

2. Afin de créer votre propre serveur DNS récursif, installer le paquet *bind9*. Bind est le logiciel de serveur DNS le plus utilisé dans le monde (et il est libre). Les fichiers de configuration de Bind sont situés dans */etc/bind/*.

3. Démarrer le service de Bind. Par défaut, Bind écoute sur le port 53 de toutes les IPv6 et IPv4 de votre ordinateur (il est possible de vérifier avec *netstat -pnat | grep 53*) et a un comportement de serveur DNS récursif. Configurer votre ordinateur pour qu'il utilise ce nouveau serveur (en utilisant l'adresse locale *::1*), et vérifier qu'il est effectivement bien utilisé.

4. Ce serveur va également être utilisé pour faire autorité sur votre propre zone DNS (équivalente au nom de domaine choisi pour votre site web lors du TP1, e.g. *mylittle.pony*). Dans le fichier *named.conf* de Bind, ajouter un appel au fichier */etc/bind/myzones*.

5. S'inspirer de la définition de la zone *localhost* dans *named.conf.default-zones*, pour créer la zone *mylittle.pony* dans le fichier *myzones*. Il faudra également créer le fichier db correspondant, en s'inspirant de celui utilisé pour *localhost*.

6. Demander à votre binôme de vérifier que son fichier */etc/hosts* ne contient plus d'information à propos de votre nom de domaine (suite au TP1). En configurant son ordinateur pour qu'il utilise uniquement votre serveur DNS récursif, vérifier qu'il est en capacité de 1) naviguer correctement sur Internet et 2) accéder à votre site web *mylittle.pony.*

Partie III : Pirater votre binôme

1. Ajouter une zone pour *www.google.fr* dans *myzones*, qui pointe sur les adresses IP de votre propre serveur web. Redémarrer Bind, et demander à votre binôme de vérifier les IP de *www.google.fr* avec dig.

2. Créer le site web de google.fr sur votre serveur web (en HTTP **et** HTTPS), en utilisant la page *index.php* suivante :

```
Vous recherchez : <?= $_GET['q'] ?>
```

3. Demander à votre binôme d'aller sur http://www.google.fr avec son navigateur (il faut qu'ille ait fermé toutes les pages de ce site depuis au moins 1 minute, avant d'essayer). Que voit-ille ?

4. Félicitations, vous avez fait du DNS menteur ! Cette possibilité est utilisée dans toutes les bonnes dictatures du monde. Ainsi qu'en France, pour bloquer certains sites de téléchargements illégaux.

5. Demander à votre binôme de faire une recherche Google avec la barre de recherche de Firefox. Quelles sont les différences avec la tentative précédente ?

6. Citer deux moyens d'améliorer votre falsification du site de Google.

7. En utilisant les mots *phishing* et *cookies*, donner des exemples d'attaques concrètes qui sont à portée de votre main. Indiquer quel en serait le but, et ce qu'il faudrait mettre en place pour y parvenir.

8. **BONUS EXPERT·E·S :** Réussir à mettre en place les deux propositions qui ont été citées à la question *6)*, en les faisant valider auparavant par votre enseignant·e.