TP 01 – DNSSEC
R411 – Cyber - Sécurisation de services réseaux

Il vous est demandé un compte-rendu (en PDF) précisant les commandes, les résultats (capture de texte principalement) et **le contenu des fichiers de configuration** (e.g. `/etc/bind`).
Déposer le compte-rendu sur l'ENT de l'IUT ou l'envoyer par mail à christophe.borelly@umontpellier.fr.

1. Serveur DNS personnel simple

1. Préparer un serveur DNS de type *master* pour une zone simulant un domaine portant **votre nom**, associé aux adresses IPv4 `192.168.1.0/24` et IPv6 `2001:db8:1234::/64` (Pour l'étudiant `John DOE`, le domaine pourrait être `DOE.FR`). Ajouter au moins les noms `dns`, `mail` et `www` et utiliser des champs A, AAAA, NS, MX, CNAME.
2. Créer également les zones inverses.
3. Vérifier vos fichiers avec `named-checkconf` et `named-checkzone`.
4. Démarrer votre serveur en mode « foreground » (`named -g`) et tester celui-ci en local et à distance avec `dig` (sur une autre machine : celle de votre voisin par exemple).
5. Tester la résolution inverse avec `host` puis `dig`.
6. Utiliser la directive `allow-query` pour autoriser ou interdire les requêtes vers votre serveur (de façon globale ou pour une zone particulière).
7. Définir une ACL (Access Control Lists) pour simplifier l'écriture de la directive précédente.
8. Ajouter un nom ou modifier une adresse dans une zone « master » et recharger la configuration (`rndc reload`, voir aussi `rndc --help`). Qu'indique le serveur si on a pas pris soin de changer le numéro de version de la zone ?
9. Ajouter le support de DNSSEC (Signature NSEC) à votre zone.
10. Que faudrait-il faire pour valider entièrement un enregistrement (voir `delv`) ?

2. Transfert de zones

1. Créer sur votre serveur DNS, une zone secondaire pour la zone « maître » du serveur de l'un de vos voisins (ou bien créer un second serveur sur une machine virtuelle). Vérifier que le transfert de zone à bien fonctionné.
2. Utiliser la commande `tsig-keygen` pour créer une clé TSIG de type HMAC-SHA256 :

```
tsig-keygen cleXFR
```

3. Utiliser cette clé pour sécuriser le transfert de zone. Vérifier que le transfert est interdit tant que le « slave » n'utilise pas la même clé.

3. Mises à jour dynamiques :

1. Utiliser la directive `allow-update` sur votre zone « maître » pour qu'un client utilisant DHCP par exemple, puisse indiquer son adresse au serveur DNS avec la commande `nsupdate -d nsupdate.conf`. Voici un exemple de fichier de configuration pour `nsupdate` :

```
server x.x.x.x
update add nom.DOE.FR 300 IN A 10.1.2.3
send
```

2. Sur le serveur maître, afficher le contenu du fichier de journalisation qui a été créé avec l'outil `named-journalprint`.
3. Quelle adresse est utilisée si on n'utilise pas la commande `server` dans le fichier .conf ?
4. Utiliser une clé TSIG pour sécuriser maintenant la mise à jour.
5. Comment automatiser la mise à jour quand le client utilise `dhclient` (ou `dhcpcd`) pour obtenir son adresse IP ?
6. Utiliser les commandes `prereq` et `delete` de `nsupdate` pour effacer un enregistrement si seulement il existe.
7. Mettre en place une mise à jour SIG(0).