BIND SÉCURISATION DU TRANSFERT

Sécurité à base de clé TSIG

Au lieu d'utiliser des adresses IP, nous allons maintenant utiliser des clés cryptographiques pour authentifier le transfert de zone - celui-ci utilise TSIG, un mécanisme par lequel la communication entre le maître et le serveur esclave sera authentifié en utilisant cette clé.

1. Éxécuter:

```
$ cd /tmp/
$ sudo dnssec-keygen -a HMAC-MD5 -b 128 -n HOST mydomain.key
```

(Pensez bien sûr à remplacer 'mydomain' avec le nom de votre domaine!)

Vous verrez quelque chose de similaire à ceci:

Kmydomain.key.+157+32373   (le dernier nombre sera différent)

Deux fichiers auront été créés:

```
$ ls -l K*
```

Kmydomain.key.+157+32373.key
Kmydomain.key.+157+32373.private

2. Afficher le contenu de la clé privée

```
$ cat Kmydomain.key.+157+32373.private
```

Vous verrez quelque chose de similaire à:

Private-key-format: v1.2
Algorithm: 157 (HMAC_MD5)
Key: tHTRSKKrmyGmPnzNCf2IRA==
Bits: AAA=

... la "Key:" est la chose importante ici, donc copier "tHTRSKKrmyGmPnzNCf2IRA==" (mais bien sûr pas celui ci-dessus! celle dans VOTRE fichier!)

Nous allons l'utiliser dans les étapes suivantes.

3. Modifiez votre named.conf

```
$ cd /etc/namedb/
```

Editez le fichier named.conf et modifier la déclaration allow-transfer, afin qu'elle ressemble à ceci:

```
options {
        ...
        allow-transfer { 127.0.0.1; ::1; };  // myslaves est enlevé!
        ...
};
```

Note: Nous avons supprimé "myslaves"

Maintenant, après la fin de la section options (ou à la fin du fichier),
ajouter une nouvelle déclaration pour la clé:

```
key "mydomain-key" {
        algorithm hmac-md5;
        secret "tHTRSKKrmyGmPnzNCf2IRA==";  // Coller ici VOTRE clé!

};
```

N'oubliez pas de changer "mydomain" et remplacer avec le nom de
votre domaine.

Modifier la définition de votre zone:

```
zone "MYTLD" {
        type master;
        file "/etc/namedb/master/mytld";

        allow-transfer { key mydomain-key; };   // <-- Ajouter ceci!
};
```

Comme vous pouvez le voir ci-dessus, nous avons ajouté une déclaration
"allow-transfer" permettant le transfert de la zone pour les détenteurs
de la clé "mydomain-key".

Note: allow-transfer est désormais placé à l'INTERIEUR de
la définition d'une zone, et non pas globalement à l'intérieur de
la section options - BIND permet de limiter le transfert de zone soit
globalement, soit par zone. Nous aurions pu choisir de permettre
les transferts globalement (pour toutes les zones), en laissant le
la déclaration allow-transfer dans la section "options" principale.

4. Redémarrez named

```
    $ sudo service named
```

5. Essayez de faire un transfert de zone à partir d'une AUTRE machine
  - demandez à vos voisins de faire:

```
    $ dig @10.10.XX.1 MYTLD axfr
```

Regardez le fichier /etc/namedb/log/general et /etc/namedb/log/transfers

    Q: Que remarquez-vous?

6. Ensuite, demandez-leur d'essayer à nouveau avec la clé:

```
    $ dig @10.10.XX.1 axfr mydomain -y mydomain-key:tHTRSKKrmyGmPnzNCf2IRA==
```

Q: Qu'est-ce qui se passe maintenant?

Vérifiez les journaux de nouveau, en particulier /etc/namedb/log/transfers

7. Sur l'hôte ESCLAVE de votre partenaire (votre secondaire - encore une
   fois, cela peut être l'instructeur si ils offrent un service secondaire

pour votre domaine).

Commencez par demander à votre partenaire de supprimer leur copie de votre zone:

- Demandez-leur de supprimer la zone de /etc/namedb/slave/MYTLD -

Rappelez-vous, c'est sur la machine de votre partenaire SLAVE:

- Demandez-leur de redémarrer nommé

```
$ sudo rm /etc/namedb/slave/MYTLD
```

Vérifiez avec eux que la zone a disparu et que leur serveur n'a pas pu la recharger.

Q: Que voyez-vous dans les journaux MASTER (auth1) (transfers et general) ?

Q: Qu'est-ce que vous voyez dans les journaux de l'ESCLAVE (transfers et general) ?

8. Toujours sur l'ESCLAVE (si l'instructeur fournit un service secondaire, ce sera eux qui effectueront cette partie)

Trouvez la déclaration de la zone:

```
zone "MYTLD" {
        type slave;
        masters { 10.10.XX.1; };
        file "slave/mydomain.dns";
};
```

... et ajouter la clé, et une déclaration pour dire quelle clé utiliser quand on parle a "10.10.XX.1." (le maître):

```
key mydomain-key {
        algorithm hmac-md5;
        secret "tHTRSKKrmyGmPnzNCf2IRA==";
};
server 10.10.XX.1 {      // mettre ici l'IP du master de la zone
        keys { mydomain-key; };
};
```

9. Redémarrez named

```
$ sudo service named restart
```

Sur le serveur ESCLAVE:

Q: Est ce que la zone "MYTLD" est réapparue dans le répertoire slave/ ?

Q: Que voyez-vous dans les journaux de l'ESCLAVE (transfers et general)?

Sur le serveur MAITRE:

Q: Que voyez-vous dans les journaux MASTER (auth1) (transfers et general)?

Pouvez-vous voir un avantage général à l'utilisation de clés au lieu d'ACL à base d'IP?