Domain Name Security Extensions

ESIR - TP DNSSEC

2025

TOUJOURS VÉRIFIER QUE VOUS UTILISEZ DU MATÉRIEL EN ÉTAT.
Ne jamais supposer que les personnes vous ayant précédés ont fait le ménage !

1. Vérifiez que votre machine a eth0 câblées correctement
2. En démarrant VirtualBox, vérifiez qu'il ne traîne pas de machines virtuelles, sinon supprimez les (bouton effacer tous les fichiers).
3. Si vous utilisez le switch, vérifiez que sa conf est "vide" (show run, show vlan)
4. Si vous utilisez le routeur, vérifiez que sa conf est "vide"
5. Si vos configurations ne sont pas "vides", passez à l'étape nettoyage en fin de TP pour y remédier
6. Vérifiez l'ordre de vos interfaces physiques en fonction de leurs adresses MAC

1 Objectif

L'objectif de ce TP est de vous donner tous les outils et toutes les compétences nécessaires pour sécuriser une zone DNS. Nous procéderons donc par étape, tout d'abord la création et la sécurisation de la zone locale **mXX**. Puis nous rattacherons cette zone à la zone parente **i207**. Tout au long du processus, nous vérifirons l'existence d'une chaîne de confiance lors de la résolution de noms.

Rappel : toutes vos connaissances sur le DNS, protocole, création de zone, délégation, fonctionnement sont bien sûr nécessaires.

2 Création de la zone mXX

Pré-requis d'installation :
— VM debian ;
— `bind9` (nom du service associé : `named`).

2.1 Rappels

Pour ce TP, une zone DNS spécifique à la salle a été créée. Il s'agit de la zone **i207**. Vous allez être une zone fille de cette zone. Si vous avez la machine 1, vous serez la zone **m01.i207.** ; si vous avez la machine 10, vous serez la zone **m10.i207.** ; etc.

Vérifiez que votre fichier `/etc/bind/named.conf` contient bien la directive
`include /etc/bind/named.conf.local`

C'est ce fichier en `.local` que nous modifierons. Pour la suite vous pourrez vous inspirez des fichiers présent dans le répertoire `/etc/bind`, notamment les fichiers `.conf.default-zone` ou `db.local`.

Question 1. Dans le fichier `/etc/bind/named.conf.local`, ajoutez un bloc indiquant que vous gérez la zone `mXX.i207.` et que la description de cette zone se trouve dans le répertoire `/etc/bind/master/mXX.i207`.

Question 2. Créez le répertoire master s'il n'existe pas ainsi que le fichier `mXX.i207` en vous inspirant du fichier `db.local` par exemple. Si elle n'existe pas, ajoutez en début de fichier la ligne `$ORIGIN mXX.i207.` et en fin de fichier ajoutez la ligne :

```
$GENERATE 0-999 machine${0,3,d} CNAME aliasmachine${0,3,d}
```

Vous pouvez vérifier que vos configurations sont syntaxiquement correctes en utilisant les commandes : `named-checkconf` et `named-checkzone`.

Comme vous avez modifié les configurations du serveur, il faut redémarrer le service pour les prendre en compte.

`sudo systemctl restart named`

Question 3. Faites une résolution de nom pour vérifiez que votre zone est fonctionnelle. Pour être sûr d'interroger votre serveur DNS soit vous modifiez le fichier `/etc/resolv.conf` soit vous précisez à la commande `dig` d'interroger votre serveur avec l'option `@localhost`.

Si votre zone est fonctionnelle passez à la suite, sinon débugguez pour qu'elle le soit. Si la zone DNS ne fonctionne pas ce n'est pas la peine de poursuivre, ça ne fonctionnera pas non plus en DNSSEC !

3 Signature de la zone mXX

3.1 Génération des clés de chiffrement

La commande utilisée pour générer les clés de chiffrement que ce soit une KSK ou une ZSK est `dnsec-keygen`, un petit tour rapide du manuel ne sera pas inutile.

Nous allons commencer par générer une ZSK :

```
sudo dnssec-keygen -a <algorithm> -b <taille> -n ZONE <nom-de-la-zone>
```

Sur un serveur de production où on préférera des KSK de 2048 bits et des ZSK de 1024 bits minimum ! Deux fichiers ont été créé le répertoire à partir duquel vous avez tapé la commande, un fichier `.key` et un fichier `.private`. Il faut maintenant dire à votre serveur où trouver la clé à utiliser.

Dans votre fichier de zone après la ligne contenant la directive `$TTL` ajoutez la ligne :

```
$INCLUDE <macle>.key
```

On procède de même pour générer une KSK, en passant en plus à la commande `dnssec-keygen` l'option `-f KSK`. Créez votre KSK et n'oubliez pas de l'inclure dans votre fichier de zone.

3.2 Signature de la zone

La commande utilisée pour signer un fichier de zone est `dnssec-signzone`, un petit tour rapide du manuel ne sera pas inutile. Maintenant que vos clés sont créées et incluses dans votre fichier de zone vous pouvez la signer.

```
dnssec-signzone -t -g -o <nom de domaine> -k <ma KSK> <fichier de zone> <ma ZSK>
```

Si tout se passe bien vous avez un fichier `mXX.i207.signed` qui a été créé. Vous pouvez donc dire à votre serveur BIND d'utiliser ce fichier plutôt que celui de la zone non signée. Vous pouvez aussi éditez le fichier `.signed` pour vérifier que votre commande `$GENERATE` a bien fonctionné.

N'oubliez pas aussi de dire à votre serveur qu'il sait faire du DNSSEC en ajoutant la ligne dnssec-enable yes ; dans le fichier named.conf.options.

Question 4. Faites une résolution de nom pour vérifiez que votre zone est fonctionnelle en DNSSEC.

4 Sécurisation de la délégation

Lors de la signature de votre zone, l'outil a créé un fichier `dsset`. C'est ce fichier qu'il faut transmettre à votre zone parente pour sécuriser la délégation.

Transmettez-moi votre fichier dsset ainsi que l'adresse IP de votre machine (`ip -c a`) afin que je crée la délégation sécurisée.

5 Mise en place d'un cache sur la deuxième machine

Passer sur la seconde machine de votre table. Modifier le fichier `/etc/bind/named.conf.options` pour qu'il contienne les options :

```
recursion yes;
dnssec-enable yes;
dnssec-validation yes;
forward first;
forwarders{148.60.12.25;};
```

et

```
logging{
    channel "security-channel" {
        file "/var/log/named/dnssec";
        severity debug 3;
        print-category yes;
        print-severity yes;
        print-time yes;
    };
    category "dnssec" {
        "security-channel";
    };
    channel "general-channel" {
        file "/var/log/named/general";
        severity debug 3
        print-category yes;
        print-severity yes;
        print-time yes;
    };
    category "general" {
        "general-channel";
    };
};
```

N'oubliez pas de créer les fichiers `dnssec` et `general` dans le répertoire indiqué derrière la directive `directory` et de donner à bind les droits en écriture dessus.

N'oubliez pas que pour faire une résolution DNSSEC, il faut établir une chaîne de confiance et donc avoir un *Secure Entry Point*. Que manque-t-il à votre serveur cache pour pouvoir valider des enregistrements DNSSEC ?

Mettez en place le SEP grâce au bloc :

```
trusted-keys {
    <nom de zone> 257 3 5 "la KSK en base64";
};
```

Ce bloc sera le premier du fichier avant même les options. Note importante : `5` correspond à l'algorithme utilisé pour la génération de la clef et doit donc être adapté selon le contenu du fichier `.key`.

Question 5. Pourquoi ne met-on pas de ZSK en SEP ?

Question 6. Configurez votre client pour qu'il interroge votre cache. Faites une résolution de nom pour vérifiez dans les logs ce que votre serveur cache a fait des signatures. Dessinez la chaîne de confiance prise par votre cache.

6 Bonus : s'il vous reste du temps

1. Montez un serveur secondaire
2. Sécurisez votre transfert de zone avec TSIG

7 Nettoyage

Pour remettre la salle en état. **Si** vous avez utilisé le routeur :

```
Router#erase startup-config
```

Éteindre le routeur.
Si vous avez utilisé le switch :

```
Switch# delete flash:vlan.dat si vous avez fait des vlan
Switch# erase startup-config
```

Éteindre le switch.
Recâbler correctement, si nécessaire le câble d'eth0.
Supprimer vos machines vituelles via VirtualBox