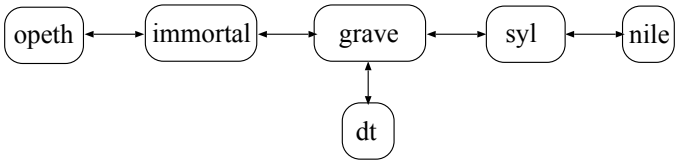
Université de Bordeaux — année 2019-2020

Master CSI/Master Info. — Sécurité des réseaux

TD - Premiers pas avec IPSec

Le but de ce TP est de mettre en place un tunnel IPSec entre deux machines distantes afin d'assurer la confidentialité des données échangées. Ce mécanisme sera mis en place entre les machines immortal et syl de la plate-forme décrite ci-dessous :



La topologie réseau correspondante peut être obtenue en lançant le script de démarrage `/net/stockage/aguermou/SR/TP/7/qemunet.sh` en lui fournissant la description de la topologie réseau à l'aide de l'option `-t` ainsi que l'archive contenant la configuration initialte des machines à l'aide de l'option `-a`. Ceci revient à lancer les commandes suivantes :

```
cd /net/stockage/aguermou/SR/TP/7/; ./qemunet.sh -x -t topology -a archive_tp7.tgz
```

1. Configurer le réseau pour que toutes les machines puissent communiquer les unes les autres (j'ai été gentil, je l'ai déjà fait ;-)).
2. Pour la suite, nous allons utiliser le démon *racoon* ainsi que les outils fournis par le paquet *ipsec-tools*. Les machines sur lesquelles nous allons configurer IPSec seront immortal et syl. La première opération à effectuer sera la création des clés qui seront utilisées pour pour chiffrer les communications (nous allons utiliser la méthode simple dans un premier temps, une méthode plus sophistiquée serait l'utilisation des certificats X509). Utilisez la commande suivante pour générer la clé :

   ```
   dd if=/dev/random count=24 bs=1 | xxd -ps
   ```

   Il faut ensuite que la clé générée par cette commande soit placée sur les extrémités de notre tunnel (à savoir immortal et syl) dans le fichier /etc/racoon/psk.txt comme suit :

   sur syl

   ```
   @publique d'immortal     clé
   ```

   et sur immortal

   ```
   @publique de syl     clé
   ```

   Attention, il faut ajouter un 0x avant la clé pour spécifier que c'est une valeur hexadécimale.
3. Il faut maintenant configurer `racoon`. Cette dernière étape se fait par le biais du fichier `/etc/racoon/racoon.conf`. Par exemple sur immortal (il faut faire un traitement symétrique sur syl), ce fichier doit contenir :

   ```
   remote  @ip_syl{
           proposal {
                   encryption_algorithm aes;
                   hash_algorithm sha1;
                   authentication_method pre_shared_key;
                   dh_group modp1024;
           }
   ```

```
        verify_identifier on;
        peers_identifier address;
        exchange_mode main;
}

sainfo address @reseau_immortal/masque[any] any address @reseau_syl/masque[any] any {
        pfs_group modp1024;
        encryption_algorithm aes,3des;
        authentication_algorithm hmac_sha1,hmac_md5;
        compression_algorithm deflate;
}
```

En ajoutant ces deux blocs, on configure à la fois la négociation faite lors de l'établissement de la connexion ainsi que ce qui doit être fait lorsqu'une machine appartenant au réseau "interne" doit communiquer via le tunnel (le deuxième bloc).

4. Il faut maintenant configurer le mode IPSec qu'on veut utiliser entre les deux points de notre tunnel. Tout comme pour les parties précédentes, il faut effectuer cette opération sur tous les deux extrémités de notre tunnel. Nous allons donc éditer le fichier `/etc/ipsec-tools.conf` pour y ajouter une description des connexions à chiffrerr. Par exemple sur immortal :

   ```
   flush;
   spdflush;

   spdadd @reseau_immortal/masque[any] @reseau_syl/masque[any] any -P out ipsec
           esp/tunnel/@ip_immortal-@ip_syl/unique;

   spdadd @reseau_syl/masque[any] @reseau_immortal/masque[any] any -P in ipsec
           esp/tunnel/@ip_syl-@ip_immortal/unique;
   ```

   Il faut remarquer que dans notre cas, on utilise un tunnel esp. Attention, il ne faut pas oublier de mettre "yes" dans `/etc/default/setkey`.

5. Démarrez les démons concernés par vos modifications :
   `/etc/init.d/racoon restart; /etc/init.d/setkey restart`
   et testez les communications entre opeth et nile. Faites un tcpdump au niveau de grave pour voir la nature du trafic généré.
6. En vous inspirant de ce qui a été fait précédemment, mettre un en place un tunnel utilisant ah entre immortal et syl.
7. Pour finir, faites pareil, mais cette fois-ci en utilisant le mode transport.