EL GHORFI Rabii

TP6 : Configurer un serveur NIS

Le service `NIS` (Network Information System),
permet de centraliser les connexions sur un réseau local

D'après Wikipedia (encyclopédie libre) : "Son but est de distribuer les informations contenues dans des fichiers de configuration contenant par exemple les noms d'hôte (/etc/hosts), les comptes utilisateurs (/etc/passwd), etc. sur un réseau.

Un serveur NIS stocke et distribue donc les informations administratives du réseau et qui se comporte ainsi comme un ensemble cohérent de comptes utilisateurs, groupes, machines, etc.

A l'origine, NIS est sorti sous le nom de « Yellow Pages » (YP) ou Pages jaunes mais le nom étant déposé par la compagnie anglaise British Telecom, Sun a renommé son protocole NIS. Cependant, les commandes NIS commencent toutes par yp.

NIS est réputé pour être faible en termes de sécurité." voir :

- LDAP
- Kerberos
- RADIUS

1. Installation du Serveur

Nous partirons du principe que votre serveur et les clients disposent d'adresses IP statiques. NIS en adresses IP dynamiques présente un sérieux risque en terme de sécurité. Lisez la section "Sécurité", plus loin, elle aborde les problèmes inhérents de sécurité liés à NIS et comment les éviter.

- (Optionnel) Ajoutez chaque nom de client et les adresses IP dans le fichier "**/etc/hosts**". L'adresse IP du serveur devrait déja être présente. Je ne parle pas de 127.0.0.1, mais de l'adresse IP réelle visible de l'extérieur. Cela assurera le fonctionnement de NIS même si le DNS est planté. Vous pouvez également relayer vers le DNS, c'est vous qui voyez.
- Ajoutez la ligne suivante dans le fichier "**/etc/hosts.allow**":

```
portmap ypserv ypbind : "liste d'addresses IP"
```

Où "liste d'addresses IP" sera la liste de toutes les adresses IP des clients ainsi que celle du serveur. Mettez uniquement des adresses IP ceci étant rendu obligatoire suite à une limitation de portmap qui ne supporte pas les noms d'hôtes.

- Installez NIS:

```
sudo apt-get install portmap nis
```

Il vous sera demandé le nom de votre domaine NIS. Cela peut-être n'importe quoi ; assurez vous juste qu'il soit identique entre le serveur et les clients.

- Editez "**/etc/default/nis**" et définissez la ligne NISSERVER à :

```
NISSERVER=master
```

- Editez "**/etc/yp.conf**" et ajoutez une ligne de serveur sous la forme:

```
ypserver 127.0.0.1
```

- Editez "**/var/yp/Makefile**" et lisez les instructions. Il n'y aura probablement pas besoin de faire beaucoup de modifications. La seule chose à changer c'est la ligne MINGID qui définit si l'appartenance au groupe doit être propagée à travers le domaine. On l'a définie à 1.

```
MINGID=1
```

MINxID définit la plus petite valeur (MIN) de UID ou GID à propager au travers de NIS. Définir ce dernier à 1 est une aberration : les groupes et utilisateurs dont l'ID est inférieur à 1000 sont généralement utilisateurs ou groupes systèmes. Il est bien plus rationnel de laissé MINxID à 1000.

- Editez "**/etc/ypserv.securenets**" et ajoutez les lignes qui restreindront l'accès aux membres du domaine. On utilisera lignes pour des hôtes spécifiques:

```
host 192.168.1.1
host 192.168.1.2
etc…
```

Commentez la ligne 0.0.0.0 . Sinon tout le monde aura accès. (Lisez dans "Sécurité" pourquoi c'est mauvais).

"One can use the word "host" instead of a netmask of 255.255.255.255. Only IP addresses are allowed in this file, not hostnames." C'est-à-dire, chez Molière, On peut utiliser le mot "host" pour remplacer 255.255.255.255 (ou 32) comme masque de sous-réseau. Pour les profanes, généralement, on utilise le masque 255.255.255.0 (ou 24) avec nos petites "box internet". Et de même que pour portmap, ne donnez que des adresses IP, pas de noms d'hôtes.

- Construisez la base de données pour la première fois, lancez:

```
sudo /usr/lib/yp/ypinit -m
```

Puis suivez les instructions. Cela engendrera certainement des messages d'erreurs disant que le programme n'est pas en mesure de contacter certaines choses. Ce n'est pas grave. (Les autres erreurs le sont probablement).

- Redémarrez tout:

```
sudo /etc/init.d/portmap restart
```

Préférez l'utilisation de la commande interne *service* comme suit :

```
sudo service portmap restart
```

Note : Si vous avez des problèmes avec l'arrêt de portmap. Il va falloir l'arrêter en faisant un kill -9.

- Si vous changez quoique ce soit (ajouter un utilisateur, etc.), assurez-vous de faire:

```
sudo make -C /var/yp
```

2. Sécurité

NIS est quelque chose de dangereux. N'importe qui pouvant accéder au démon peut récupérer vos listes de mots de passe. Si ils peuvent le faire alors ils ont vos mots de passe. Peu importe qu'ils soient cryptés; ils sont l'équivalent des mots de passe clairs, depuis que l'authentification s'effectue à l'aide de mots de passe cryptés vous n'avez pas besoin du mot de passe clair, il faut juste écrire une application qui présentera correctement la version cryptées au système d'authentification. Aussi assurons-nous que cela n'arrive pas. Comment? Et bien, d'abord en restreignant les accès:

- N'autorisez que certains membres du domaine à contacter les services appropriés dans le "**hosts.allow**". Ceci implique que le "**hosts.deny**" est paramétré à **ALL** afin que cela fonctionne.
- Limitez les clients à qui le serveur répondra en mettant les membres du domaine dans "**/etc/securenets**".

Bien, nous avons restreint l'accès à des adresses IP spécifiques, on est doué quand même, non ? Et bien, pas tant que ça. Que se passe-t-il si quelqu'un éjecte une de vos machines du réseau, lui pique son adresse IP et récupère le fichier de mot de passe ? Vous êtes mort. **Solution: IPSec** (Allez voir le **IPSecHowTo**). Vous pouvez paramétrer tous les membres de votre domaine à ne communiquer que sur IPSec ce qui permettra de vérifier que vos clients sont bien qui ils affirment être. Comment? Et bien, le client crypte le trafic à destination du serveur avec la clé du serveur, et le serveur répond à chaque demande en cryptant avec la clé du client. Le trafic est décrypté avec les clés respectives. Ainsi, un client ne disposant pas des clés qu'il est supposé avoir ne pourra ni envoyer ni recevoir de données. Le fichier contenant les clés et raisonnablement protégé (lisible que par root), vous ne pouvez obtenir les clés sans compromettre le client. Si vous compromettez le client, vous pouvez tout de même obtenir la liste de mots de passe, ainsi l'attaquant vous aura tout de même (ce qui est une faille dans la plupart des systèmes d'authentification de domaine).

3. Configuration du Client NIS

Une note concernant l'administration: Etant donné que le compte root est désactivé, assurez vous que celui qui administre la machine est présent dans le fichier "/etc/sudoers" du client. C'est également une bonne idée de définir ces utilisateurs en tant qu'utilisateurs locaux avec **les mêmes UID** que dans la liste de mot de passe du domaine. Cela permet de garder les choses propres et cohérentes, et s'il venait à y avoir un problème, vous pourriez avoir besoin d'un compte local afin d'accéder à la machine.

- Ajoutez le serveur à "/etc/hosts". Cela permettra de toujours résoudre l'adresse du serveur même en cas de panne du DNS.
- Installez les programmes dont vous avez besoin

```
sudo apt-get install portmap nis
```

Il vous sera demandé votre nom de domaine NIS. Entrez le nom de votre domaine NIS. C'est probablement une bonne idée d'ajouter une ligne portmap dans "**/etc/hosts.allow**" pour des raisons de sécurité:

```
portmap : <adresse IP>
```

Où "Serveur NFS" sera le nom de votre serveur NFS et "adresse IP" son adresse IP

- Définir les noms des services qui utiliseront NIS:

Editez "**/etc/passwd**" afin d'ajouter ceci à la fin:

```
+::::::
```

Editez "**/etc/group**" afin d'ajouter ceci à la fin:

```
+:::
```

Editez "**/etc/shadow**" afin d'ajouter ceci à la fin:

```
+::::::::
```

Cela définit les services qui doivent inclure des entrées NIS si une correspondance n'est pas trouvée dans le fichier. Vous pourriez changer d'autres services afin qu'ils utilisent NIS en éditant "/etc/nsswitch.conf", mais ceux-ci sont les plus importants.

- Editez "**/etc/yp.conf**" afin d'ajouter la ligne:

```
domain domainname server servername
```

Où domainname sera le nom de votre domaine NIS, et servername sera le nom de votre serveur NIS.

Il se peut que cela ne fonctionne pas en mettant le nom du serveur NIS, car ce sera transposé avec la correspondance contenue dans /etc/hosts donc par 127.0.01. Dans ce cas il faut mettre l'adresse ip du serveur (192.168.9.2 par exemple)

Une solution pratique : Sur le fichier */etc/hosts* du serveur NIS :

```
 127.0.0.1 localhost
   <adresse_du_serveur> <nom_du_serveur>
   <adresse_d'un_client> <nom_d'un_client>
   ...
```

Ce fichier sera retransmis aux clients tel quel, et pourra donc être utilisable quoiqu'il advienne.

- Redémarrez NIS:

```
/etc/init.d/nis restart
```

Note: sshd devra être redémarré afin d'utiliser le nouveau système d'authentification. Juste pour info.