Gestion et surveillance de réseau

Utilisation de RANCID

Notes :

* Les commandes précédées de "$" signifient que vous devez exécuter la commande en tant qu'utilisateur général - et non en tant qu'utilisateur root.
* Les commandes précédées de "#" signifient que vous devez travailler en tant qu'utilisateur root.
* Les commandes comportant des lignes de commande plus spécifiques (par exemple "RTR-GW>" ou "mysql>") signifient que vous exécutez des commandes sur des équipements à distance, ou dans un autre programme.

Exercices

1. Connectez-vous à votre PC en utilisant ssh

2. Devenez utilisateur root et installez Subversion, le système de versionnage.

   En plus de Subversion, on installera telnet et le client mail mutt.

   Ces deux paquetages doivent déjà être installés par les labos précédents. Sinon, pas de problème - la command apt-get ne les réinstallera pas.

```
$ sudo bash
# apt-get install mutt telnet subversion
```

3. Installez l'application Rancid proprement dite

```
# apt-get install rancid
```

   - Un message d'avertissement "Really continue?" (voulez-vous vraiment continuer) s'affichera. Sélectionnez <OK> puis ENTREE pour continuer.

   - Un second avertissement apparaîtra pour vous recommander de faire une sauvegarde de vos données Rancid. Nous n'avins pas de données, donc sélectionnez <YES> et ENTREE pour

continuer.

4. Créez un alias pour l'utilisateur rancid dans le fichier /etc/aliases

```
# editor /etc/aliases

rancid-all:     sysadm
rancid-admin-all:   sysadm
```

Enregistrez le fichier, puis exécutez :

```
# newaliases
```

5. Modifiez /etc/rancid/rancid.conf

```
# editor /etc/rancid/rancid.conf
```

Recherchez la ligne suivante dans rancid.conf:

```
#LIST_OF_GROUPS="sl joebobisp"
```

Et, en dessous ajoutez la ligne suivante :

```
LIST_OF_GROUPS="all"
```

(Sans "#" en début de ligne)

En outre nous voulons utiliser Subversion, et non CVS, donc recherchez
la ligne contenant le paramètre RCSSYS:

```
RCSSYS=cvs; export RCSSYS
```

et modifiez-la comme suit :

```
RCSSYS=svn; export RCSSYS
```

Ainsi que la ligne contenant CVSROOT :

```
CVSROOT=$BASEDIR/CVS; export CSVROOT
```

Et remplacez la par:

```
CVSROOT=$BASEDIR/svn; export CSVROOT
```

Notez bien le "svn" en *minuscules*. Sauver, et quitter le fichier.

6. Devenez utilisateur rancid

```
**********************************
*           ATTENTION !!!          *
**********************************
```

Faites très attention au compte utilisateur avec lequel vous agirez pour le reste de ce labo! Si vous êtes dans le doute, il suffit de taper la commande "id" sur la ligne de commande, à tout moment.

Depuis une invite root, changez d'identité pour devenir l'utilisateur "rancid" :

```
# su -s /bin/bash rancid
```

Vérifiez que vous êtes BIEN l'utilisateur rancid :

```
$ id
```

Vous devriez voir quelque chose de similaire (les chiffres peuvent être différents):

```
uid=104(rancid) gid=109(rancid) groups=109(rancid)
```

```
*********************************************************************
*    SI VOUS N'ÊTES PAS UTILISATEUR RANCID APRÈS AVOIR TAPÈ "id"   *
*                        NE CONTINUEZ PAS                           *
*********************************************************************
```

7. Créez /var/lib/rancid/.cloginrc

```
$ editor /var/lib/rancid/.cloginrc
```

Ajoutez les lignes suivantes:

```
add user *.ws.nsrc.org cisco
add password *.ws.nsrc.org nsrc+ws nsrc+ws
```

(Le premier "cisco" correspond au nom d'utilisateur, le deuxième et le troisième "nsrc+ws" sont le mot de passe et le mot de passe enable utilisé pour se connecter à votre routeur. L'astérisque dans l'IP signifie que Rancid va essayer d'utiliser ce nom d'utilisateur et ce mot de passe pour tous les routeurs dont le

nom finit en .ws.nsrc.org).

Quitter et sauver ce fichier.

Protégez maintenant ce fichier afin qu'il ne puisse pas être lu par d'autres utilisateurs :

```
$ chmod 600 /var/lib/rancid/.cloginrc
```

En réalité, vous voulez créer un utilisateur RANCID supplémentaire sur le réseau Cisco, doté de droits limités.

8. Testez l'ouverture de session sur le routeur de votre groupe

Connectez-vous à votre routeur avec clogin. Il se peut que vous ayez à répondre "oui" (yes) au premier message d'avertissement alerte, mais vous ne devriez pas avoir besoin d'entrer un mot de passe, ceci devrait être automatique.

```
$ /var/lib/rancid/bin/clogin rtrX.ws.nsrc.org
```

(Remplacez le X par votre n° de groupe. Par exemple, Groupe 1 = rtr1)

Vous devriez voir s'afficher un message du type :

```
spawn ssh -c 3des -x -l cisco 10.10.0.X
The authenticity of host '10.10.0.X (10.10.0.X)' can't be established.
RSA key fingerprint is 73:f3:f0:e8:78:ab:49:1c:d9:5d:49:01:a4:e1:2a:83.
Are you sure you want to continue connecting (yes/no)?
Host 10.10.0.X added to the list of known hosts.
Warning: Permanently added '10.10.0.X' (RSA) to the list of known hosts.
Password:

rtr2>enable
Password:
rtr2#
```

Quittez le routeur

```
rtr2# exit
```