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 "rtrX" 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 -s
   # apt-get install mutt telnet subversion mutt
   ```

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'avions 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 le nom 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).

    (Note: il est également possible d'utiliser des adresses IP, et on
     pourrait alors écrire: add user 10.10.* cisco
                            add password 10.10.* nsrc+ws nsrc+ws)

    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

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 un message du type :

```
spawn ssh -c 3des -x -l cisco rtrX.ws.nsrc.org
The authenticity of host 'rtrX.ws.nsrc.org (10.10.X.254)' 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 rtrX.ws.nsrc.org added to the list of known hosts.
Warning: Permanently added 'rtrX.ws.nsrc.org' (RSA) to the list of known hosts.
Password:

rtrX>enable
Password:
rtrX#
```

Quittez le routeur

```
rtrX# exit
```

9. Initialiser le dépôt SVN pour rancid :

Assurez-vous que vous êtes l'utilisateur rancid avant de continuer :

```
$ id
```

Si vous ne voyez pas quelque chose similaire à:
"uid=108(rancid) gid=113(rancid) groups=113(rancid)"
... ne PAS CONTINUER avant que vous ayez réussi à devenir l'utilisateur rancid.

Voir l'étape 6 pour plus de détails.

```
$ /usr/lib/rancid/bin/rancid-cvs
```

Vous devriez obtenir ce type d'informations :

```
Committed revision 1.
```

```
Checked out revision 1.
At revision 1.
A         configs
Adding         configs

Committed revision 2.
A         router.db
Adding         router.db
Transmitting file data .
Committed revision 3.
```

*** La section suivante n'est valable que SI vous avez eu des problèmes cités ci-dessus ***

Si cela ne fonctionne pas, alors il vous manque le paquet subversion, ou bien quelque chose n'a pas été correctement configuré au cours des étapes précédentes. Vous devez vérifier que subversion est installé puis, avant de lancer à nouveau la commande cvs-rancid, effectuer l'opération suivante :

```
$ exit
# apt-get install subversion
# su - /bin/bash rancid
$ cd /var/lib/rancid
$ rm -rf all
$ rm -rf svn
```

Maintenant, essayez d'exécuter à nouveau la commande rancid-cvs :

```
$ /usr/lib/rancid/bin/rancid-cvs
```

*** Fin de section ***

10. Créez router.db

```
$ vi /var/lib/rancid/all/router.db
```

Ajoutez cette ligne :

```
rtrX.ws.nsrc.org:cisco:up
```

(N'oubliez pas de remplacer X comme convenu)

11. Lancez rancid !

```
$ /usr/lib/rancid/bin/rancid-run
```

(Ceci devrait prendre environ 30 secondes)

Lancez-le à nouveau, étant donné qu'il pourrait ne pas fonctionner correctement la première fois :

```
$ /usr/lib/rancid/bin/rancid-run
```

12. Consultez les journaux :

```
$ cd /var/lib/rancid/logs
$ ls -l
```

... Visualisez le contenu du/des fichier(s) :

```
$ less all.*
```

13. Regardez les configs

```
$ cd /var/lib/rancid/all/configs
$ less rtrX.ws.nsrc.org
```

... en remplaçant "X" avec le numéro de votre groupe.

Si tout s'est bien déroulé, vous voyez maintenant le fichier config du routeur.

14. Modifions maintenant une description d'interface sur le routeur :

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

... en remplaçant "X" avec le numéro de votre groupe.

À l'invite "rtrX#", saisissez la commande :

```
rtrX# conf term
```

Vous devriez voir le message suivant :

```
Enter configuration commands, one per line.  End with CNTL/Z.
rtrX(config)#
```

Saisissez :

```
rtrX(config)# interface LoopbackXX (remplacez XX par le numéro de
                                    votre PC)
```

par exemple

```
rtrX(config)# interface Loopback17 (si votre PC porte le numéro 17)
```

Vous obtenez l'invite suivante :

```
rtrX(config-if)#
```

Saisissez :

```
rtrX(config-if)# description <put your name here>
rtrX(config-if)# end
```

Vous obtenez maintenant l'invite suivante :

```
rtrX#
```

Pour enregistrer la configuration en mémoire :

```
rtrX# write memory
```

Vous devriez voir le message suivant :

```
Building configuration...
[OK]
```

Sortez ensuite en tapant :

```
rtrX# exit
```

Vous devriez maintenant vous retrouver à l'invite système,
en tant qu'utilisateur rancid.

15. Exécutons de nouveau rancid :

```
$ /usr/lib/rancid/bin/rancid-run
```

Examinez la configuration et les journaux

```
$ ls /var/lib/rancid/logs/
```

16. Observons les différences :

```
$ cd /var/lib/rancid/all/configs
$ ls -l
```

Vous devriez voir tous les fichiers de config routeur

```
$ svn log rtrX.ws.nsrc.org
```

(où xxx est le numéro de votre routeur)

Notez les révisions. Observez la différence entre les deux versions :

```
$ svn diff -r 5:7 rtrX.ws.nsrc.org | less
```

... voyez-vous vos modifications ?

Notez que l'outil en ligne de commande svn (Subversion) est utilisé pour gérer le versionnage de l'information. Si vous tapez:

```
$ ls -lah
```

... vous verrez un répertoire caché appelé ".svn". Ceci contient en fait toutes les informations concernant les changements de la configuration de votre routeur, à chaque fois que vous avez lancé rancid via la commande /usr/lib/rancid/bin/rancid-run

Surtout, ne JAMAIS toucher le répertoire .svn à la main!

17. Consultez votre messagerie

Nous allons maintenant quitter le shell de l'utilisateur rancid et celui de l'utilisateur root afin de redevenir utilisateur "sysadm". Ensuite on va exécuter "mutt" pour visualiser les messages que rancid a envoyés :

```
$ exit
# exit
$ id
```

... vérifiez que vous êtes maintenant redevenu l'utilisateur "sysadm". Dans le cas contraire déconnectez-vous avant de vous reconnecter.

```
$ mutt
```

(Au message de sollicitation vous demandant de créer le répertoire courrier (Mail), répondez oui)

Si tout se déroule comme prévu, vous devriez être en mesure de lire les messages envoyés par Rancid. Vous pouvez sélectionner un message envoyé par "rancid@pcX.ws.nsrc.org" et le visualiser pour voir à quoi cela ressemble.

Notez que c'est bien votre routeur, ainsi que tout changement effectué depuis la dernière fois ou la commande rancid-run a été lancée.

Maintenant, quittez mutt.

(tapez une première fois 'q' pour revenir à l'index des messages, et une seconde fois pour quitter mutt)

18. Faisons en sorte que rancid s'exécute automatiquement toutes les 30 minutes au moyen d'une tâche cron

    cron est un système sous UNIX qui gère l'éxécution automatique de tâches.

    On va repasser root:

        $ sudo -s

    Maintenant on va créer une tâche pour l'utilisateur Rancid:

        # crontab -e -u rancid

    Rancid va vous demander votre éditeur favori.

    Ajoutez cette ligne à la fin du fichier (copier & coller)

        */30 * * * * /usr/lib/rancid/bin/rancid-run

    ... puis sauvegardez et quittez.

    C'est tout. La commande "rancid-run" sera éxécutée automatiquement à partir de maintenant, et ce toutes les 30 minutes, tout le temps (tous les jours, semaines, mois)

19. Ajoutez maintenant tous les autres routeurs

    Notez les noms de de machine des routeurs

        rtrX.ws.nsrc.org, où X va de 1 à 9

    Mettez à jour le fichier router.db

        # su -s /bin/bash rancid
        $ editor /var/lib/rancid/all/router.db

    Ajoutez dans le fichier d'autres routeurs de classe. Le résultat devrait ressembler à ce qui suit :

        rtr1.ws.nsrc.org:cisco:up
        rtr2.ws.nsrc.org:cisco:up
        rtr3.ws.nsrc.org:cisco:up
        rtr4.ws.nsrc.org:cisco:up
        rtr5.ws.nsrc.org:cisco:up
        rtr6.ws.nsrc.org:cisco:up
        rtr7.ws.nsrc.org:cisco:up
        rtr8.ws.nsrc.org:cisco:up
        rtr9.ws.nsrc.org:cisco:up

(Notez que "cisco" signifie qu'il s'agit d'un équipement Cisco - cela indique à Rancid que nous nous attendons ici à communiquer avec un dispositif Cisco. Vous pouvez également communiquer avec un dispositif Juniper, HP...)

20. Exécutez de nouveau rancid :

```
$ /usr/lib/rancid/bin/rancid-run
```

(Ceci devrait maintenant prendre une minute ou plus, soyez patient)

21. Consultez les journaux :

```
$ cd /var/lib/rancid/logs
$ ls -l
```

... Choisissez le fichier le plus récent et affichez-le

```
$ less all.YYYYMMDD.HHMMSS
```

C'est à dire le dernier fichier listé par la commande "ls -l"

22. Regardez les configs

```
$ cd /var/lib/rancid/all/configs
$ more *.ws.nsrc.org
```

Utiliser la barre ESPACE pour défiler le contenu de chaque fichier. Ou alors, on peut faire

```
$ less *.ws.nsrc.org
```

Puis, ESPACE pour faire défiler, et ":n" pour passer au fichier suivant. Souvenez-vous, dans les deux cas, vous pouvez appuyer sur "q" pour quitter à tout moment.

Si tout s'est bien déroulé, vous voyez les configs de TOUS les routeurs.

23. Exécutez de nouveau RANCID juste au cas où quelqu'un aurait modifié la configuration sur le routeur

```
$ /usr/lib/rancid/bin/rancid-run
```

(patience)

24. Essayez clogin :

```
        $  /usr/lib/rancid/bin/clogin -c "show clock" rtrX.ws.nsrc.org
```

    ... où "X" est le numéro de votre groupe.

    Que remarquez-vous ?

    Encore mieux, voici la puissance d'un simple script utilisé pour effectuer
    des changements sur plusieurs machines rapidement

```
        $ editor /tmp/newuser
```

    ... dans ce fichier, ajoutez les commandes:

```
configure terminal
username NewUser secret 0 NewPassword
exit
write
```

    Sauvez le fichier, et tapez les commandes suivantes:

```
        $ for r in 1 2 3 4
```

    Votre invite va se transformer en ">". Continuez et tapez:

```
> do
>   /var/lib/rancid/bin/clogin -x /tmp/newuser rtr$r.ws.nsrc.org
> done
```

    Votre invite va redevenir "$" et la commande rancid clogin va
    s'éxécuter et lancer les commandes que vous avez tapés ci-dessus
    sur les routeurs rtr1, rtr2, rtr3, etc. C'est un simple exemple
    de script shell sous Linux, mais très puissant.

    Q: Comment vérifier que la commande a été éxécutée correctement ?
       Indice: "show run | inc"

    A: Connectez-vous à rtr1, 2, 3 et 4 (si actif). Taper "enable"
       et ensuite "show run | inc username" pour vérifier que l'utilisateur
       NewUser existe désormais. Exit pour quitter chaque routeur.

       Évidemment, on peut automatiser ceci comme on l'a fait dans l'exemple
       ci-dessus.

25. Ajoutez le dépôt RANCID SVN dans SVNWeb

    Si vous êtes toujours logué en tant qu'utilisateur rancid,
    reprenez l'identité de root

```
        $ exit
        #
```

Installez SVNWeb :

```
        # apt-get install websvn
```

* Répondez Yes à la question si vous voulez configurer WebSVN maintenant,
  et appuyer sur ENTREE
* Faites OK pour la question suivante concernant la prise en charge
  de différents serveurs web, et appuyer sur ENTREE
* Quand on vous pose la question du "svn parent repositories", remplacer
  le chemin par:

  /var/lib/rancid/svn

  Choisir OK et appuyer sur ENTREE. Faire la même chose quand on vous
  demande le chemin pour "svn repositories". C'est à dire, mettre le
  chemin:

  /var/lib/rancid/svn

  (effacer ce qui est y était sur la ligne avant)

  Choisir OK et appuyer sur ENTREE

* Faites OK pour l'écran suivant relatif aux autorisations, et appuyer sur
  ENTREE

26. Corriger les permissions. Le serveur Web doit pouvoir lire le contenu du dossier svn

```
        # chgrp -R www-data /var/lib/rancid/svn
        # chmod g+w -R /var/lib/rancid/svn
```

27. Parcourez les fichiers avec votre navigateur web

```
        http://pcX.ws.nsrc.org/websvn
```

Parcourez les fichiers du répertoire "all/configs".
Tous vos fichiers de configuration de routeur se trouvent ici.

28. Examinez les révisions

WebSVN vous permet de voire facilement les changements entre les

versions.

* Naviguer sur http://pcX.ws.nsrc.org/websvn de nouveau, cliquer sur "all",
  puis "configs"
* Cliquer sur le fichier avec le nom du routeur (rtrX.ws.nsrc.org). Vous
  allez avoir un nouvel écran
* Cliquer sur "Compare with Previous" en haut de l'écran.
* Vous devriez voir les changements surlignés en couleur.

Cliquer sur "REPOS 1" pour revenir en arrière à la page principale WebSVN:

* Cliquer sur "all/" sous "Path"
* Cliquer sur "configs/"
* Sélectionnez deux des routeurs qui sont côte à côte, par exemple:
  rtr1 et rtr2.
* Cliquer sur "Compare Paths"

Ceci vous montrera les différences de configuration entre deux routeurs distincts.

Note: c'est possiblement un trou de sécurité, donc il vaut mieux restreindre l'accès à http://host/websvn en utilisant des mots de passe (et SSL), ou avec des listes d'accès.

Si vous voulez juxtaposer différentes révisions afin de les comparer, vous pouvez également le faire avec WebSVN.

Accédez de nouveau à http://pcXXX.ws.nsrc.org/websvn, allez à "all configs"
Sélectionnez le fichier de votre routeur (rtrX.ws.nsrc.org) et cliquez sur "Compare with Previous" (comparer avec version précédente)
Vous devriez maintenant voir les dernières modifications côte-à-côte.

Note: En réalité il est préférable dw créer un utilisateur RANCID supplémentaire sur le réseau Cisco, doté de droits limités.