

Gestión de Red

Ejercicio práctico con RANCID

=====

Notas

- * Los comandos precedidos por el signo de pesos "\$", deben ser ejecutados como un usuario general - y no como superusuario (root).
- * Los comandos precedidos por el signo de número "#", deben ser ejecutados por el superusuario (root).
- * Los comandos precedidos por líneas de comando más específicas (e.g. "rtr>" or "mysql>") deben ser ejecutados en equipos remotos, dentro de otras aplicaciones.
- * Si la línea de comandos termina con una barra invertida "\", quiere decir que el comando continua en la próxima línea y todas líneas deben ser tratadas como un comando de sola línea.
- * Referencias a "N", representan su número de grupo.

Ejercicios

1. Ingrese en su PC con ssh
2. Conviértase en root, e instale el sistema de control de versiones Subversion:

Además de Subversion, instalaremos telnet y el cliente de correo Mutt. Puede que ambos paquetes ya hayan sido instalados en un ejercicio previo. En tal caso, no se preocupe. El comando apt-get simplemente no los instalará.

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

3. Instalar Rancid

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

- Le mostrará una advertencia. Seleccione <Ok> y oprima ENTER para continuar.
- Le mostrará otra advertencia sobre la necesidad de hacer una copia de sus datos en Rancid. Como no tenemos datos, simplemente seleccione <YES> y oprima ENTER para continuar.

4. Agregue un "alias" para el usuario rancid en el archivo de alias:

```
# editor /etc/aliases
```

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

Grabe y salga. Luego ejecute:

```
# newaliases
```

5. Edite la configuración de Rancid

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

Busque esta línea:

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

Y debajo de ésta, agregue:

```
LIST_OF_GROUPS="all"
```

Sin el carácter "#" al comienzo de la línea, y alineada hacia la izquierda.

Vamos a usar Subversion con nuestro sistema de control de versiones, y no CVS, así que busque la línea con el parámetro RCSYS:

```
RCSYS=cvs; export RCSYS
```

Y cámbiela a:

```
RCSYS=svn; export RCSYS
```

también busque la línea con CVSR00T:

```
CVSR00T=$BASEDIR/CVS; export CVSR00T
```

y cámbiela a:

```
CVSR00T=$BASEDIR/svn; export CVSR00T
```

Asegúrese de que "svn" esté en minúscula. Grabe y salga del editor.

6. Cambie el usuario rancid

MUY IMPORTANTE:

Ponga mucha atención a cuál ID de usuario (userid) está usando durante el resto de los ejercicios. Si no está seguro, simplemente ejecute "id" en la línea de comandos en cualquier momento.

Desde una línea de comandos de root ("#"), cambie su identidad para convertirse en el usuario 'rancid':

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

Confirme que es el usuario rancid ahora:

```
$ id
```

Debería ver algo similar a esto (puede que los números no concuerden):

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

***** SI NO ES RANCID AHORA, NO SIGA *****

7. Configure el script para iniciar sesiones (logins) automáticas:

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

Agregue las siguientes dos líneas:

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

La primera línea indica que debe usarse el nombre de usuario "cisco". En la segunda línea, el primer y segundo "cisco" son los passwords de acceso y modo privilegiado (enable) para para el enrutador. El asterisco "*" en los nombres es un comodín, lo cual indica que Rancid deberá usar estas credenciales para todos los dispositivos cuyos nombres terminen en .ws.nsrc.org

Grabe y salga.

Ahora proteja este archivo para que no pueda ser leído por otros usuarios:

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

8. Compruebe que puede iniciar sesiones hacia el enrutador de su grupo

Ingrese a su enrutador con clogin. La primera vez probablemente recibirá una advertencia de SSH sobre la clave pública. Confirme con "y". Pero no debería tener que escribir la contraseña del enrutador. Debería ser automático.

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

(reemplace X con su número de grupo. Por ejemplo, si usted es grupo 1, el nombre sería rtr1.ws.nsrc.org)

Debería ver algo como esto:

```
spawn ssh -c 3des -x -l cisco rtr2.ws.nsrc.org
The authenticity of host 'rtr2.ws.nsrc.org (10.10.2.254)' 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 rtr1.ws.nsrc.org added to the list of known hosts.
yes
Warning: Permanently added 'rtr1.ws.nsrc.org' (RSA) to the list of known hosts.
Password:

rtr1>enable
Password:
rtr1#
```

Termine la conexión al enrutador:

```
rtr2#exit
```

9. Inicialize el repositorio SVN para Rancid:

Asegúrese de ser rancid antes de continuar:

```
$ id
```

Si no ve algo como

```
"uid=108(rancid) gid=113(rancid) groups=113(rancid)"
```

NO CONTINUE hasta haberse convertido en el usuario rancid. Vea el paso 6

para más detalles.

Ahora inicialize el repositorio SVN:

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

Verá algo como:

```
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.
```

***** Sólo haga lo siguiente si tiene problemas *****

Si esto no funciona, entonces puede que le falte el paquete subversion, o que algo no se configuró apropiadamente durante los pasos anteriores. Debe verificar que Subversion está instalado, así que antes de ejecutar rancid-cvs, haga lo siguiente:

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

Ahora intente de nuevo:

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

10. Cree el archivo que contendrá la lista de dispositivos

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

Agregue esta línea:

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

Grabe y salga

11. Vamos a probar rancid!

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

Esto tardará unos momentos.

Pruébalo de nuevo porque la primera vez puede que no registre correctamente:

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

12. Revise los registros de eventos (logs) de Rancid:

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

... Inspeccione el contenido de los archivos:

```
$ less all.*
```

NOTA! Al usar "less" - para ver el siguiente archivo presione ":n".
Para ver el archivo anterior, presione ":p". Salga con "q".

13. Mire las configuraciones

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

Si todo salió bien, debería ver la configuración del enrutador.

14. Vamos a cambiar la descripción de una interfaz en el enrutador

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

En la línea de comandos "rtrX#" escriba:

```
rtrX# conf term
```

Verá:

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

Ingrese:

```
rtrX(config)# interface LoopbackXX (sustituya XX con el # de su PC)
```

Verá lo siguiente:

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

Ingrese:

```
rtr2(config-if)# description <escriba su nombre aquí>
rtr2(config-if)# end
rtrX# write memory
rtrX# exit
```

15. Ejecutemos Rancid de nuevo:

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

Mire los registros de eventos

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

Debería ver un nuevo archivo de eventos indicando la última ejecución de Rancid con la fecha y hora como parte del nombre.

16. Veamos las diferencias

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

Debería ver el archivo del enrutador de su grupo:

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

Fíjese en las revisiones. Veamos las diferencias entre las dos versiones:

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

... ¿Puede ver los cambios?

Note que svn es el comando del sistema de control de versiones para manejar repositorios de información. Si escribe:

```
$ ls -lah
```

Verá un directorio escondido llamado ".svn" - este contiene toda la información sobre los cambios entre las configuraciones de los enrutadores recogidos cada vez que se ejecuta rancid.

Nunca, nunca toque o edite el directorio .svn a mano!

17. Revise su correo

Ahora saldremos del shell de rancid para volver a el shell de root, y de ahí saldremos a el shell de "sysadmin". Vamos a usar el programa "mutt" para ver si rancid nos ha estado enviando correos:

```
$ exit                (salir del shell de rancid)
# exit                (salir del shell de root)
$ id
... comprobar que somos sysadmin de nuevo;

... si no, salga e ingrese de nuevo a su PC como sysadmin.

$ mutt
```

(Cuando se le pregunte sobre crear el directorio "Mail", diga Yes)

Si todo sale como está planificado, debería poder leer los e-mails enviados por Rancid. Puede seleccionar el e-mail enviado por "rancid@pcX.ws.nsrc.org" y ver qué tiene dentro.

Note que será la descripción de su enrutador y cualquier diferencia que se haya registrado desde la última vez que se ejecutó rancid-run.

Salga de mutt.

(use 'q' para salir al índice, y 'q' de nuevo para salir de mutt)

18. Hagamos que Rancid se ejecute cada 30 minutos por medio de Cron

cron es un sistema disponible en Linux para automatizar la ejecución de tareas. Primero debemos convertirnos de nuevo en root:

```
$ sudo bash
```

Ahora crearemos una nueva tarea para el usuario rancid:

```
# crontab -e -u rancid
```

Le preguntará por su opción de editor. Indique el editor que haya estado usando hasta ahora en clase

Agregue esta línea al final del archivo (COPIE Y PEGUE):

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

... Y salga.

Ya está. El comando "rancid-run" se ejecutará automáticamente cada 30 minutos a partir de ahora, todos los días.

19. Ahora agregue todos los enrutadores

Conviértase en el usuario rancid y edite el archivo siguiente:

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

Agregue los otros enrutadores de la clase en el archivo.

Si hay más o menos enrutadores en clase, incluya el número correcto (esto es sólo un ejemplo):

COPIE Y PEGUE:

```
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
```

Note que "cisco" significa que estos son equipos Cisco. Esta información ayuda a Rancid a identificar cómo debe comunicarse con el equipo. Rancid también soporta muchos otros fabricantes, tales como Juniper, HP, etc.

Asegúrese de que las entradas están alineadas hacia la izquierda del archivo.

20. Ejecute rancid otra vez:

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

Tomará un minuto o más, espere.

21. Revise los registros:

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

... Busque el último archivo y mírelo

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

Este debería ser el último archivo en la lista producida por "ls -l"

Debería haber un número de entradas indicando que los enrutadores se han agregado a Subversion, y otras informaciones.

22. Revise las configuraciones

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

Use la barra espaciadora para continuar a los demás archivos, o también:

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

Y oprima la barra espaciadora para desplazarse hacia abajo en la página y luego presione ":n" para ver el próximo archivo. Recuerde que en ambos casos puede salir con "q".

Si todo salió bien, debería ver las configuraciones de todos los enrutadores.

23. Ejecute Rancid de nuevo para ver si alguien ha cambiado la configuración de su enrutador.

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

23. Juegue con clogin:

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

Qué puede observar?

Y lo que es mas interesante es que podemos sacar provecho de esta herramienta y escribir un script sencillo para hacer cambios en múltiples dispositivos rápidamente:

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

... en este archivo escriba (o COPIE Y PEGUE):

```
configure terminal
username pc<número_de_PC> secret 0 NewPassword
exit
write
```

Guarde, salga y ejecute lo siguiente:

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

Su línea de comandos cambiará a ">". Continúe escribiendo:

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

Ahora su línea de comandos volverá a ser "\$" y el comando clogin de Rancid

se ejecutará y enviará los comandos que acaba de escribir a los enrutadores rtr1, rtr2, rtr3 y rtr4. Esto es programación en shell sencilla en Linux, pero es muy poderosa.

Q. Cómo verificaría que esto se ha ejecutado correctamente ?

Pista: "show run | inc <patrón>"

A. Conéctese a rtr1, rtr2, rtr3 y rtr4. Escriba "enable" y luego "show run | inc username" para verificar que el nuevo usuario NewUser existe. Salga con "exit". Naturalmente esto lo podríamos automatizar de la misma manera.

24. Agregar el repositorio Subversion de Rancid a WebSVN

Si todavía está como usuario rancid, salga para volver a ser root. Recuerde que puede ejecutar "id" para comprobar qué usuario es efectivamente.

```
$ exit
#
```

Instale WebSVN:

```
# apt-get install websvn
* Responda <Yes> para configurar WebSVN ahora y oprima ENTER
* Responda <Ok> a la siguiente pregunta sobre soporte para servidores
  y presione ENTER
* Cuando se le pregunte sobre "svn parent repositories" cambie el camino
  a:

/var/lib/rancid/svn

Diga <Ok> y oprima ENTER. Haga lo mismo para "svn repositories" en
la siguiente pantalla. O sea, use el camino:

/var/lib/rancid/svn

y no lo que se muestra por defecto. <Ok> y luego ENTER.
* Diga <Ok> a la pregunta de permisos y luego ENTER.
```

25. Repare los permisos. El servidor web debe poder leer la carpeta svn (Subversion)

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

26. Ahora puede ver los archivos de Rancid desde su navegador!

<http://pcX.ws.nsrc.org/websvn>

Vaya al directorio 'all/configs'.
Puede ver todas las configuraciones de sus enrutadores ahí.

27. Compruebe las revisiones

WebSVN le permite ver con facilidad las diferencias entre versiones.

```
* Navegue a http://pcXXX.ws.nsrc.org/websvn de nuevo y vaya a all/configs.
* Vaya al enlace de su enrutador (rtrX.ws.nsrc.org) name. Verá otra pantalla.
* Oprima "Compare with Previous" al comienzo de la pantalla.
```

* Ahora podrá ver los últimos cambios.

Oprima "REPOS 1" para volver a la página principal:

- * Oprima "all/" bajo "Path"
- * Oprima "configs/"
- * Seleccione dos enrutadores contiguos. Ej. rtr1 y rtr2, rtr3 y rtr4.
- * Oprima Compare Paths

Esto le mostrará las diferencias entre dos configuraciones de enrutadores distintos.

WebSVN es una manera conveniente de ver las diferencias rápidamente en una interfaz gráfica entre múltiples archivos de configuración. Note que esto es un potencial problema de seguridad, así que debería restringir el acceso al URL <http://<host>/websvn> usando contraseñas (y SSL), y listas de control de acceso.

+----

Rev. 18 Oct 2012