Ejercicios Dia 1: Taller CEDIA

29 de Febrero, 2004

1.) Cambiar el Teclado. Reinicializar al nivel 3 (texto)

Primero, login como:

Por favor, no cambia la contraseña de usuario root en ningun caso.

usuario: root
clave: espe2004

Primero, cambiamos el teclado para usar el teclado en Español. Abrimos una ventana de terminal, y en el terminal haz lo siguiente:

```
cd /etc/X11
vi XF86Config
:65
```

Deberias ver una linea asi:

"Option "XkbLayout" "us"

> Mueve su "cursor" a la "u" y apreta "x" dos veces.
> Ahora, apreta "i" para cambiar el modo de editar a "insertar"
> Tipea "es"
> Apreta el teclado "Esc"
> Tipea ":wq" y

Ahora, cambiamos al modo de no GUI. Tipea:

```
/sbin/telinit 3
```

2.) Practicar con comandos basico

Ten cuidado en este ejercicio. Corriendo como root significa que se puede arruinar su sistema facilmente. Si no estas seguro de un comando pregunta al instructor o a los ayudantes.

El primer comando que vamos a usar es "man", es corto por "man"ual. Lea sobre cado comando para ver el rango de opciones que hay. Haz esto asi:

```
man cp
man cd
man ls
man mv
man rm
```

Despues haz lo mismo, pero ahora usa "info" asi:

```
info cp
info cd
info ls
info mv
info rm
```

Y, si tienes problems para quitar "man" apreta "q". Tambien, se puede usar las flechas para mover en cada descripcion.

Ahora, estamos listos para practicar un poco con los comandos:

```
cd /
ls
ls -la
cd /tmp
cd ..
cd tmp
```

Que paso aqui? Si no entiendes pregunta.

```
touch texto.txt
cp texto.txt nuevo.txt
mv texto.txt nuevo.txt
```

Que pasa ahora. Responde "si" o "y".

```
cp texto.txt /root/.
cd ../root
```

Entiendes que se puede hacer "cd /root", o "cd .." y despues "cd root" o "cd /root", y al fin llegarias al mismo directorio?

Ahora, juega con el uso del teclado "tab". Por ejemplo, en /root empieza tipea el primer parte del comando "cp texto.txt texto.txt.bak" - entonces, tipea:

```
cp te
cp texto.txt te
```

```
cp texto.txt texto.txt.bak
```

El teclado tab te hace mucho mas facil la vida. Ahora tipea:

```
mkdir tmp
mv text.* tmp/.
ls
```

Finalmente, vamos a remover el directorio donde hay los dos archivos.

```
cd tmp
rm *
cd ..
rmdir tmp
```

Se puede forzar esto con un comando asi:

```
rm -rf tmp
```

El uso de "rm -rf" es **supremamente peligroso!**, y, naturalmente, muy util de repente. Por ejemplo, si tu eres "root" y tipeas "rm -rf /*" esto seria el fin de tu servidor. El comando dice "remover, forzar, recursivamente, todo" - O, empezando en el directorio base, remueve todo los archivos y directorios *sin preguntar*. Si quieres usar el "rm -rf *" siempre toma una pausa y tipea:

```
pwd
```

primero. Esto te dice en que directorio estas. Si equivocas tendras la oportunidad de not remover archivos que, tal vez, realmente necesitas.

3.) Practicar con mas comandos

Como se puede ver hay un monton de comandos. Si te vas a los directorios /bin, /usr/bin, /sbin, /usr/sbin/, /usr/local/bin, etc. se puede ver cientos de archivos que son programas que actuan como comandos. El directorio /bin tiene los comandos criticos por el sistema operativo. En /sbin vas a encontrar los comandos que, en general, solo root corre, or que root puede correr con afecto. Haz lo siguiente:

```
cd /bin
ls
```

Y, ahora, lea sobre estes comandos. Por ejemplo:

```
man dmesg
```

Con cuidado juega con los comandos que hay en la presentacion, y/o con los camandos que encuentras.

4.) Buscar mas informacion sobre tu sistema

Si quieres var que hay en un archivo hay tres maneras tipicas para hacer esto:

cat
less
more

El comando "less" tiene mas funcionalidad, pero no siempre funciona. El comando "cat" casi simpre te permite ver un archivo si tienes el permiso. Y, el "more" es como "cat" pero un poco menos poderoso.

prueba usando los trez veando que hay en los archivos de informacion:

```
cd /etc
cat motd
more services
less services (sale con "q")
```

Si no entiendes de que se trata uno de los archivos usa "man" - Por ejemplo, se puede tipear:

```
man modules.conf
man XF86Config
man fstab
```

Si tienes una pregunta asi pregunta al instructor o a uno de los ayudantes.

5.) Crear un archivo y usar vi para editarlo

Ahora vamos a abrir un archivo vacio y poner text adentro. El editor vi tiene un modo de entra datos (entrada) y un modo de comando. Tu puedes salir del modo de entrada usando el teclado de ESCape. Ahora hacemos lo siguiente:

```
cd /root
touch taller.txt
vi taller.txt
```

Ahora, estas en vi. Apreta el teclado "i" para entrar en modo de entrada.

Tipea algo, como "Que rico es vi. Creo que voy a usar vi en vez de Microsoft Word desde ahora."

Aprete para agregar lineas. Tipea mas.

Ahora, recordando lo siguiente:

```
Abrir: vi fn, vi -r fn, vi + fn, vi +n fn, vi +/pat fn
Cerrar: :w, :wq, :q, :q!
Movimiento: h,j,k,l y w, W, b, B, :n
Editar: i, o, x, D, dd, yy, p
Buscar: /patron, ?patron, n, N
```

Juega con el moviemento. Mueve tu flecha a una linea con text y vea que pasa con "w" o "W" o "b" o "B" - recuerda, si estas en el modo de entrada apreta "ESC"ape para cambiar al modo de comando.

Ahora apreta "/" y tipea una palabra que hay en tu documento y apreta . Que pasa?

Haz lo mismo, pero apreta "?" al principio. Usa "ESC"ape para empezar de nuevo si es necesario.

Para grabar el archivo apreta el ":" y despues tipea "w" y apreta .

Para salir vi y grabar haz:

:wq

para salir sin grabar nada y perder los cambios que has hecho:

:q!

Pero, trata de grabar algo por mas tarde. Practica grabando, saliendo, entrando vi, etc...

6.) Crear un usuario nuevo

En un terminal tipea:

```
useradd "usuario"
```

Elige el nombre que quieres por el "usuario". Ahora tenemos que dar un clave (password) al usuario. Elige una contraseña buena (mas de 7 caracteres, no palabras, mezclada con simbolos, numeros, y/o letras en mayuscala y menuscala. Para poner la contraseña tipea:

```
passwd "usuario"
```

y sigue las instrucciones en la pantalla.Ahora existe este usuario. Apaga su session como el usuario "root" y entra con tu nuevo usuario. Despues que has hecho un "logout" y un "login" abre un terminal y haz los siguientes comandos:

```
ls -lah
ls -lah /etc/skel
cd ..
ls
man useradd
```

Que viste entre el directorio de tu usuario y del /etc/skel? Viste todo las opciones por correr el comando useradd? Es posible escribir scripts (programas) para crear muchas cuentas rapidas.

7.) Dar privilegios a tu usario

Hay dos maneras para hacer esto. Primero haz lo siguiente:

```
cd /etc
less /etc/passwd
less /etc/shadow
less /etc/group
```

Viste tu entrada por tu usuario en cada uno de estes archivos? Tiene sentido que veas? Si no, pregunta.

Una manera seria poner nuestro usuario en el grupo "wheel" (/usr/sbin/usermod usuario -G wheel), pero el usuario "wheel" no existe, entonces no se puede hacer esto ahora. Mejor, que haces esto por mientras:

```
vi /etc/sudoers
```

Y busca la linea que dice:

```
# User privilege specification

root    ALL=(ALL) ALL
```

Abajo la entrada por root agrega:

usuario ALL=(ALL) ALL

Graba el archivo, y sale de la cuenta root usando "logout" - Entra como tu usuario y prueba si puedes usar "su" en un terminal:

```
su (contraseña de root)
```

Y, si tu session de terminal deberia cambiar por ser una de root.

8.) Comandos - programas - shell - path

Por este ejercicio deberia cambiar su shell por no ser root. Entonces es asi:

```
su – usuario
```

Cuando uno tipea un comando o el nombre de un programa el sistema busca esto usando el variable del shell PATH. Tambien, si el programa es uno de los programas del shell ("built-in"), se lo encuentra. El comando "cd" es un ejemplo de esto. Vea su PATH asi:

```
printenv
```

Pero, si quiere ver solo el variable PATH haz:

```
printenv | grep PATH
```

El variable PATH esta configurado durante inicializacion por los scripts que corren. Para cambiar el PATH por cada shell de bash se puede hacerlo en el archivo /home/usuario/.bash_profile.

Primero vamos a crear un script en un directorio fuera su PATH que corre un comando.

```
cd /home/usuario
mkdir scripts
cd scripts
vi hola.sh
```

Ahora en el archivo nuevo ponemos estas lineas:

```
#!/bin/bash
#

echo hola
```

Y, para asegurar que puedes ejecutar el archivo usa el comando:

```
chmod u+x hola.sh
```

Vamos a hablar sobre "chmod" y "chown" en Lunes.

Graba el archivo (:wq) y ahora vamos a agregar un directorio a nuestro PATH:

```
cd /home/usuario
vi .bash_profile
```

Ahora busca la linea:

"PATH=$PATH:$HOME/bin"

y cambialo para que se dice:

"PATH=$PATH:$HOME/bin:/home/usuario/scripts

Graba el archivo y en el terminal haz esto:

```
hola.sh
. .bash_profile
hola.sh
```

Que paso? Cambiaste el PATH y el script "hola.sh" no corrio. Pero, despues de ejecutar el archivo ".bash_profile" de nuevo tu PATH cambio, tambien. Ahora, tipiaste "hola.sh" y se corrio el script porque el script estaba en el PATH. Vea esto con "printenv | grep PATH" de nuevo.

Cada vez que tu abres un terminal de bash el archivo ".bash_profile" va a correr, entonces desde ahora el directorio /home/usuario/scripts" va a estar buscado por programas cuando tipeas algo. Nota que se va a buscar en /home/usuario/scripts ultimo, entonces si copias "hola.sh" a /usr/local/bin este version del archivo va a correr y no que esta en el directorio /home/usuario/scripts.

Finalmente, si quieres cambiar algo como el PATH por todos tu puedes cambiarlo en /etc/profile (no es lo mejor idea), o puedes cambiar los archivos que cada usuario nuevo recibe que residen en /etc/skel. Vealos:

Para terminar vamos a cambiar el comando "rm" para ser mas seguro. Haz lo siguiente:

```
vi /home/usuario/.bashrc
```

Y, va al fondo del archivo y tipea "o" para agregar una linea y entrar en el modo de entrad. Agrega un linea que dice:

```
alias rm='rm -i';
```

Y, ahora salir y grabar el archivo (:wq). Despues tipea:

```
touch temp.txt
rm temp.txt
. .bashrc
touch temp.txt
rm temp.txt
```

Y, que paso? Ahora el comando rm te pide antes de borrar un archivo. Si no te gusta, cambia remueve el alias en ".bashrc", pero mi consejo es que esto es una buena idea.

9.) Usar su y sudo un poco mas

Ya has usado su para cambiar su session a ser root. Tambien, si eres otro usuario, pero tienes el derecho de usar su (vea /etc/sudoers de nuevo) se puede cambiar a cualquier usuario. Por ejemplo, desde root se escribe:

```
su usuario
```

Por este ejercicio cambia tu session al usuario que creaste. Y, ahora vamos a correr un comando que es priveligiado pero bajo tu cuenta que no tiene los privelegios para correrlo. Primero el comando sin privilegios:

```
less /etc/shadow
```

Deberias recibir un mensaje, "/etc/shadow: Permission denied". Y, ahora correrlo asi:

```
sudo less /etc/shadow (contraseña de root)
```

despues que has corrido "sudo" con un comando con exito una vez no tendras que usar la contraseña de root de nuevo (mientras que no terminas tu sesion).

10.) Revisamos un paquete de RPM

Los paquetes de software de RPM que ya estan instalado podemos revisar. Por ejemplo, buscamos como se llama el paquete de software por el programa sendamil:

```
rpm -qa | grep sendmail
```

Probablemente viste algo como:

```
sendmail-doc-8.12.8-4
sendmail-cf-8.12.8-4
sendmail-8.12.8-4
sendmail-devel-8.12.8-4
```

Dependiendo que fue instalado vas a ver mas o menos cosas, pero que nos interesa es el paquete principal. Para este caso es "sendmail-8.12.8-4". Entonces, para ver una descripcion y, despues, todo los archivos que fueron instalados haz esto:

```
clear
rpm -qi sendmail-8.12.8-4
clear
rpm -ql sendmail-8.12.8-4 | more
```

Si, por ser caso, tu version de sendmail es diferente, entonces entra la version exactamente como salio despues que hicistes el comando "rpm -qa | grep sendmail"

Si quieres tener una lista, en orden alfabetica, de todo los paquetes de software instalado en tu sistema usando RPM puede hacerlo asi (vamos a /tmp para poner un archivo temporario):

```
cd /tmp
rpm -qa | sort > rpms.txt
less rpms.txt
```

Si quieres mantener el archivo puedes moverlo desde /tmp a tu directorio:

```
mv rpms.txt /home/usuario/.
```

11.) Bajamos y instalamos lynx

Ahora vamos a bajar un paquete de RPM que contiene el Web Browser lynx. Es un Browser que funciona solamente en modo de texto. Lynx puede ser muy util cuando tienes que ver informacion de una pagina de Web y no quieres inicializar todo un Browser como Netscape/Mozilla, Konquerer, Opera, etc. Tambien, si corres tu servidor a nivel de inicializacion 3 no tendras acceso a un Browser grafica.

Vamos a usar FTP para conectarnos a nuestro servidor de NOC (Network Operations Center = Centro de Operaciones de Redes) que tenemos en la sala. La direccion de IP de este servidor es 192.188.58.126. Vamos a conectar usando la cuenta "anonymous" y vamos a bajar el archivo "lynx-2.8.5-11.i386.rpm" al directorio /usr/local/src. Por este ejemplo corre como root.

```
su (si no eres root)
ftp 192.188.58.126
```

Cuando recibes el prompt de servidor responde con:

```
anonymous
usuario@espe (puede ser cualquier correo,
pero algo en este forma)
```

Y, ahora vamos a cambiar directorios por ambos lados y bajar el archivo:

```
cd pub/redhat9/rpms
binary
lcd /usr/local/src
get lynx-2.8.5-11.i386.rpm
quit
```

Ahora instalamos el paquete. Estamos usando el convenio de ponar software que bajamos y instalamos en todo el sistema en /usr/local/src.

```
cd /usr/local/src
rpm -Uvh lynx-2.8.5-11.i386.rpm
lynx 192.188.58.126
q (para salir lynx)
```

No te preocupes si lynx ya era instalado. Deberias ver la pagina principal de taller que tenemos corriendo en nuestro servidor de noc. Juega con lynx veando otros sitios de web. Como se vean?

12.) Apagar y reinicializar

En este ejercicio tiene que ser root. Es mejor si cierres programas que tiene archivos abiertos, por ejemplo Mozilla, vi, etc., pero no es necesario. Antes de continuar lea las paginas de man por shutdown:

```
man shutdown
```

En un terminal haz esto:

```
shutdown -r ahora
```

Ahora tu maquina va a estar reinicializando. Esto demora un poco. Para parar tu maquina puedes usar el comando:

```
halt
```

O, tambien puedes ir al nivel de inicializacion 0, que es equivalente a "halt". Entonces, se escribe:

```
init 0
```

Y, el reinicializar es equivalente al nivel de inicializacion 6, o:

```
init 6
```

Tambien, se puede "logout" y usar el menu que provee Red Hat. Nota que cualquier usuario que tiene acceso a la maquina puede apagar o reinicializara la maquina con el sistema de menus. Es una decision de Red Hat, porque los usuarios normales no puede usar el comando "halt" ni "init" ni "shutdown" ni "reboot".

La idea es que si uno tiene acceso fisico a un servidor es posible reinicializarlo o apagarlo solo desenchufando la maquina. Es mejor, por lo minimo, usar los comandos...

Vamos a hablar mas sobre esto en Miercoles.

13.) Cambiar nivel de inicializacion

Desde entonces vamos a cambiar los PCs no correr XWindows cada vez que se inicializa. Para hacer esto es bastante facil:

```
vi /etc/inittab
```

Busca la linea que dice:

```
id:5:initdefault:
```

Y cambia el "5" por un "3". Graba el archivo y reinicializa tu servidor:

```
shutdown -r ahora
```

Que pasa cuando se prende de nuevo la maquina? Tipea el comando:

```
top
```

y anota cuanto RAM esta usando. Apreta "q" para salir. Puede entrar como root y tipea el comando:

```
init 5
```

si quiere ver el GUI (Graphical User Interface = Interface(?) Grafico de Usuario). No usar KDE, Gnome, el sistema de XWindows ahorra bastante en RAM. Usa el comando "top" ahora en un terminal y vea que diferencia hay.

Si vas a correr un servidor es posible que ni quieres instalar el sistema de XWindows. Este incluye XFree86, Gnome, KDE, etc. Este ahorra espacio, RAM, y si no corres XWindows tu servidor va a estar mas estable.

14.) Apagar, inicializar, y remover un servicio

Abre un terminal como root.

Tipea:

```
/usr/sbin/lsof -i
```

Veas los servicios corriendo y los puertos que usan los servicios. Vas a ver que Red Hat deja corriendo portmap y rpc.statd despues que se instala. Estes servicios se trata con NFS (Network File System = Sistema de Archivo por Redes). El NFS es muy util, y tal vez vamos a jugar un poco con esto esta semana, pero no es seguro. Realmente si tu maquina queda con una direccion de IP publica, o se puede accedirlo desde un red publico, no deberias correr NFS ni rpc.statd ni portmap.

Primero vamos a apagar portmap y inicializarlo de nuevo.

```
cd /etc/rc.d/init.d
ls
./portmap
./portmap stop
```

Fuimos al directorio donde estan los scripts que corren bajo los varios niveles de inicializacion. Se puede correr los scripts usando la herramienta "services", tambien. Por ejemplo desde cualquier directorio:

```
services portmap
services portmap stop
```

Tipeamos "portmap" solo para ver las opciones no mas. Ahora mira al archivo mismo que inicializa portmap:

```
less portmap
```

Veas la linea?:

```
# chkconfig: 345 13 87
```

Esto es muy importante. Esta dicendo que portmap corre en nivels 3, 4, y 5. Que en los niveles donde no se corre se lo para en orden "87" - o mas tarde. Entonce este servicio se apaga despues que los servicios antes "87". Y, tambien, en nivels 3, 4, y 5 se inicializa numero "13", o antes servicios "14" hasta "99". Revisa los directorios /etc/rc.d/rc2.d y /etc/rc.d/rc3.d y busca los archivos "K87portmap" y "S13portmap". Vea bien que son los archivos (desde /etc/rc.d/init.d):

```
ls -la ../rc2.d
ls -la ../rc3.d
```

Tambien, este comentario es por el comando "/sbin/chkconfig" para que se puede configurar bien los niveles. Si el comentario no esta tu tienes que especificar en que niveles va a correr un servicio.

Ahora vamos a remover el servicio portmap de los servicios que se inicializa cada vez que tu servidor se inicializa. Primero corremos chkconfig sin parametros para ver que parametros se accepta:

```
/sbin/chkconfig
./portmap stop
/sbin/chkconfig --list | grep portmap
/sbin/chkconfig --del portmap
/sbin/chkconfig --del | grep portmap
```

Ahora no se vea portmap como servicio que va a correr, pero el script para inicializarlo todovia esta en /etc/rc.d/init.d, que esta bien.

Ahora vamos a especificar en que niveles queremos que corre portmap (temporariamente no mas):

```
/sbin/chkconfig --level 345 portmap on
/sbin/chkconfig --list | grep portmap
```

Y, ahora deberias ver algo asi:

```
portmap         0:off   1:off   2:off   3:on    4:on    5:on    6:off
```

Y, para terminar, vamos a apagar portmap y rpc.statd, y vamos a removerlos como servicios que corren. Primero que servicio corre rpc.statd? No hay un archivo llamado "rpc" ni "statd". Vamos a buscarlo asi:

```
grep statd *
```

Y,parece que el script "nfslock" es el culpable. Si quieres saber mas acerca rpc.statd y portmap lea las paginas man, o:

```
man rpc.statd
man portmap
```

Y, un comentario: uno de los oyos mas grande de seguridad que tiene Microsoft es que todovia Windows corre pedazos de RPC dentro su sistema operativo para comunicar entre procesos. RPC (Remote Procedure Call = Llamadas Remoto de Funciones) es muy inseguro. En el mundo de Linux y Unix los servicios importante dejaron de usar RPC hace varios años por este razon.

Bueno, ahora apagamos portmap (ya hecho), y nfslock, y sacamos ellos de los servicios que se inicializa al initcializar el servidor:

```
./portmap stop
./nfslock stop
/sbin/chkconfig --del portmap
/sbin/chkconfig --del nfslock
/sbin/chkconfig --list | grep nfs
```

Ahora, no estan corriendo dos servicios que no son necesario, por lo minimo, ahora. Revisa esto con:

```
lsof -i
```

Hervey Allen
Febrero 2004