Universidad de Buenos Aires
Facultad de Ingeniería

Seguridad en Redes
TP – Fundamentos de Unix/Linux

Objetivo

El objetivo de este trabajo práctico es proporcionar los elementos básicos del SO Unix/Linux para que el alumno pueda trabajar en los trabajos prácticos posteriores de la materia.

Tópicos Principales:

1. Comandos Básicos del Unix
2. Conocimiento del Ambiente, Sistema de Archivos, Configuraciones de red

1. Línea de comandos / Ayuda

1.1. Manual de Unix: comando man. Ejecutar man man. (Para desplazarse utilizar los cursores, para salir la tecla q).

1.2. Utilizando el manual de UNIX, leer las descripciones de:

- ls, pwd, cd, mkdir
- ps, top
- df, du
- cat, more, less, touch

1.3. Búsquedas en el manual: (Comando "**`apropos`**" o "***man –k***"): averiguar qué comandos permiten crear o eliminar usuarios.

2. Usuarios

2.1. Ingresar el comando **`id`** para conocer información de la sesión actual.

2.2. Consultar la lista de usuarios del sistema ingresando **`cat /etc/passwd`**. El comando cat permite visualizar el archivo indicado.

2.3. Crear el usuario "alf" mediante el comando **`useradd`**. ¿Qué UID le asigno?

2.4. Consultar nuevamente la lista de usuarios.

2.5. Explicar cada entrada de un usuario en el archivo /etc/passwd (man /etc/passwd).

2.6. Utilizando **`usermod`**, agregarle la descripción "Gordon Shunway". Usar comilla doble (") para delimitar un argumento que contiene espacios.

2.7. Consultar nuevamente la lista de usuarios.

2.8. Asignarle una clave mediante **`passwd`**.

2.9. Ejecutar el comando **`login alf`** para iniciar una sesion con el nuevo usuario.

2.10. Con el comando **`logout`**, volver a la sesión anterior.

2.11. Consultar la lista de grupos mediante **`cat /etc/group`**

2.12. Agregar el grupo melmac con el comando **`groupadd`**

2.13. Consultar nuevamente la lista de grupos.

3. Filesystem

3.1. Crear una carpeta (mkdir) hija de /tmp

3.2. Crear un archivo (arch_etc) en ese directorio con el listado de archivos en el directorio /etc.

3.3. Crear un archivo vacío en el directorio (touch).

3.4. Copiar el archivo **`/etc/hosts`** al directorio utilizando **`cp`**

3.5. Listar el contenido del directorio

3.6. eliminar el archivo vacío

3.7. Renombrar el archivo **`hosts`** por **`prueba`**. Utilice **`apropos`** para hallar el comando.

3.8. Eliminar el directorio con rmdir. (¿Qué pasa?)

3.9. Ingrese el comando **`find / -name shadow`** para buscar el archivo shadow.

4. Directorios / archivos especiales

Dado que dispositivos, archivos de configuración, aplicaciones, son representados como archivos en el filesystem, estos se encuentran organizados de manera tal que su ubicación en el árbol nos da información de su función.

4.1. Consultar las particiones existentes con **`df`**

4.2. Ir al directorio raiz (/) y listar el contenido

4.3. Qué contienen los siguientes directorios?
`/etc` **`/usr`** **`/var`** **`/proc`** **`/bin`** **`/tmp`** **`/sbin`** **`/dev`** **`/mnt`**
`/etc/init.d` **`/etc/rc.d`** **`/home`**

4.4. ¿Que contienen los siguientes archivos?
`/etc/hosts` **`/etc/passwd`** **`/etc/group`**
`/etc/shadow` **`/etc/services`** **`/etc/fstab`**

5. PROCESOS

Existen diversos comandos para conocer información del sistema, como procesos, usuarios activos, estadísticas. También es posible interactuar con el sistema para controlar estos elementos, siempre que se disponga de los permisos adecuados.

5.1. Ejecutar el comando **ps** (process snapshot) para conocer los procesos activos del usuario actual.

- Ejecutar **ps –e** para ver los procesos activos del sistema
- Ejecutar **ps –u** usuario, para ver los procesos de un usuario.
- Modificador **f**: información ampliada Ejecutar **ps –ef**
- En la columna PID (Process ID) ver el ID de proceso.
- Modificador x: ver el estado de cada proceso. Ejecutar **ps -ex**

5.2. Ejecutar el comando **top**. para ver en forma online los procesos activos.

SEÑALES

5.3. En otra ventana, finalizar el proceso anterior con el comando **kill**, seguido de su PID. (cierra "gentilmente" el proceso).

5.4. Comando **kill –9**, seguido del PID: forzará la salida de memoria del proceso.

5.5. Con un usuario distinto de root (alf), hacer un kill de un proceso de otro usuario.(Buscar entre los procesos del sistema con **ps –ef**). Esto no es posible porque no se tienen permisos suficientes

6. Permisos

6.1. Analizar los permisos de los directorios dentro del directorio **/home** (Listarlo con **ls –l)**.

6.2. Analizar los permisos de los siguientes directorios:
/etc /usr /var /proc /bin /tmp /sbin /dev /mnt
/etc/init.d /etc/rc.d /home

6.3. Crear un archivo "prueba" con el comando **touch prueba** y analizar sus permisos.

6.4. Analizar la representación de permisos mediante los valores en octal.

6.5. Dado el siguiente directorio Unix, y teniendo en cuenta los permisos indicados:

ls –al /directorio

```
drwxrwxrwx  47 jperez informatica 2560  Jun 22 21:48 .
drwxrwxrwx  57 root   wheel       1024  Jun  8 01:47 ..
-rw-------   1 jperez informatica 213   Sep 16  1998 .Xauthority
-rw-------   1 jperez informatica 9425  Nov 27  1997 .Xdefaults
-rw—w--r—-   1 jperez informatica 32223 Oct 21 21:47 usd.tar.gz
```

Ejecutando los comandos indicados a continuación, qué usuarios pueden leer, borrar, modificar, ejecutar el Archivo usd.tar.gz:

Comando	Read	Write	eXecute	Delete
chmod 123 usd.tar.gz				
chgrp melmac usd.tar.gz				

chmod +r usd.tar.gz				
chmod 711 usd.tar.gz				
chown alf usd.tar.gz				
chmod -r usd.tar.gz				
chmod 777 /directorio				

6.6. Qué es y para que sirve el bit de set-user-ID. ¿Por qué el comando passwd tiene el suid puesto?

6.7. Que es y para que sirve el bit de set-group-ID.

6.8. Generar un script que permita recibir por argumento un directorio y lo liste.

7. Configuración y Pruebas de red

7.1. Consultar el nombre del sistema con el comando **hostname**

7.2. Pedir mas información del sistema con **uname –a**

7.3. Con **ifconfig**:

- Listar los dispositivos de red (**ifconfig –a**)
- Ejecutar **ifconfig eth0 down** para deshabilitar el adaptador eth0
- Listar los dispositivos de red (**ifconfig –a**)
- Ejecutar **ifconfig eth0 up** para habilitar nuevamente
- Configurar una IP con **ifconfig eth0** ***IP*** **netmask** ***MÁSCARA***.
- Consultar nuevamente el adaptador con **ifconfig eth0**
- ¿Qué es el adaptador loopback (127.0.0.1)? Efectuar un **ping** a dicha ip para ver si es alcanzable.

7.4. Consultar la tabla de ruteo (comando **route)**

7.5. Consultar los puertos en uso mediante el comando **netstat**.

7.6. Ejecutar **netstat –a** para conocer todos los puertos en uso o en escucha.

7.7. Ver que proceso esta usando el puerto 22. (con **netstat –nap**)

7.8. Hacer un **traceroute** a proxy.fi.uba.ar

7.9. Ver el tráfico que pasa por la interfaz principal. (con **tcpdump** y con **ethereal**)

8. Configuración Sistema

8.1. Abrir el archivo /etc/host e incorporar un alias

8.2. Comparar la salida del comando mount con el archivo /etc/fstab

8.3. Comparar los archivos /etc/passwd, /etc/shadow y /etc/group