Boletín ejercicios sencillos de Administración de usuarios y grupos

Nota: para crear los usuarios que se indican en los siguientes ejercicios utiliza UID's 500 en adelante.
Objetivo: el objetivo de esta práctica es trabajar con todo lo relacionado con la gestión de los usuarios. Así vamos a crear y configurar las cuentas de usuarios utilizando varios métodos. Es interesante que aprecies las diferencias y equivalencias de los diferentes métodos así como la importancia de los siguientes puntos:

- UID y GID's de la cuenta, y forma de asignación.
- La contraseña y su política de envejecimiento, longitud, etc.
- El directorio HOME y sus ficheros asociados.
- Los ficheros relacionados con la gestión de usuarios.

Tienes que realizar todos los ejercicios en una máquina virtual para evitar dañar el sistema. Como en este caso hay que realizar algunos ejercicios con la interfaz gráfica, utilizaremos la máquina Ubuntu que tenéis en la carpeta compartida. Por favor al responder a los ejercicios indicar todos los pasos que realizáis para resolverlos.

Ejercicios

1. Crea el usuario aso1 con la interfaz gráfica y comprueba si puede entrar en el sistema. Una vez creado el usuario, resuelve las siguientes cuestiones sobre la herramienta gráfica de creación de usuarios (no te limites a contestar a las preguntas, indica también lo que has hecho para averiguar la respuesta):
   1.1. ¿Crea el directorio HOME?
   Sí, lo comprobamos en un terminal con ls /home y vemos que se ha creado el directorio /home/aso1
   1.2. ¿Qué grupo primario le asigna?
   Crea un nuevo grupo aso1 y se lo asigna como grupo primario.
   tail /etc/passwd
   tail /etc/group
   Vemos las últimas líneas de cada uno de estos ficheros, observando primero el gid que le asigna (cuarto campo de la línea) y después vemos en /etc/group el nombre del grupo al que pertenece dicho gid.
   1.3. ¿Copia los ficheros de inicialización al directorio home del usuario?
   Sí, ls -a /home/aso1 nos muestra todos los ficheros del directorio home del usuario y vemos que si ha copiado los ficheros de inicialización.
   1.4. Finalmente, observa lo que ha escrito en /etc/passwd y /etc/shadow
   Abrimos un terminal y ejecutamos tail /etc/passwd y sudo tail /etc/shadow (si no lo ejecutamos con sudo no nos deja ver el contenido, solo el usuario root puede ver el contenido) tambien puede ser less/etc/passwd obteniendo la última línea de cada fichero:
   Última línea del fichero /etc/passwd:
   aso1:x:1001:1001:aso1,,,,:/home/aso1:/bin/bash
   Última línea del fichero /etc/shadow:
   aso1:6yW1Y6Zn7$PVGt8rm7BuE55Ok1ORXo5p1Xu4QyRksQaLlbLxWCelaVOWUFjdyHMqLBNns25yNYVtUm/AXys.C6dJS8zzrVe/:15662:0:99999:7:::
2. Crea el usuario aso2 con la orden adduser sin utilizar ningún parámetro y contesta a las siguientes preguntas:
   2.1. ¿Crea el directorio HOME?
   En este caso para contestar a todas las preguntas lo único que hace falta es observar la salida del comando por pantalla, ya que indica todo lo que hace:
   sudo adduser aso2
   Añadiendo el usuario `aso2' ...
   Añadiendo el nuevo grupo `aso2' (1002) ...
   Añadiendo el nuevo usuario `aso2' (1002) con grupo `aso2' ...
   Creando el directorio personal `/home/aso2' ...
   Copiando los ficheros desde `/etc/skel' ...
   Introduzca la nueva contraseña de UNIX:
   Vuelva a escribir la nueva contraseña de UNIX:
   passwd: contraseña actualizada correctamente
   Cambiando la información de usuario para aso2
   Introduzca el nuevo valor, o presione INTRO para el predeterminado
   Nombre completo []: aso2

Número de habitación []:
Teléfono del trabajo []:
Teléfono de casa []:
Otro []:
¿Es correcta la información? [S/n] s
¿Qué grupo primario le asigna?
Contestada en el apartado anterior
¿Copia los ficheros de inicialización al directorio home del usuario?
Contestada en el apartado anterior
Finalmente, observa lo que ha escrito en /etc/passwd y /etc/shadow
aso2:x:1002:1002:aso2,,,:/home/aso2:/bin/bash
aso2:6FNd71TGc$Jl6UdiQI5uYiGpWt8UrBi/lHhlZi5rgvh5AJOYZQwy/eEM2XrVC.C086QzXneWPx9PJoKgO6REyIfdJJFBxEc.:15662:0:99999:7:::

3. Crea el usuario aso3 con la orden useradd sin utilizar ningún parámetro y contesta a las siguientes preguntas:
   3.1. ¿Crea el directorio HOME?. En caso negativo, ¿qué habría que hacer para que se cree?.
   No. Tendríamos que utilizar la opción -m.
   3.2. ¿Qué grupo primario le asigna?
   Igual que en los ejercicios anteriores, crea un nuevo grupo con el nombre del usuario.
   3.3. ¿Copia los ficheros de inicialización al directorio home del usuario?. En caso negativo, ¿qué habría que hacer para que se cree?
   No, si no crea el directorio home es imposible que copie los ficheros de inicialización, con la opción -m vista en el primer punto de este ejercicio también copia dichos ficheros.
   3.4. Finalmente, observa lo que ha escrito en /etc/passwd y /etc/shadow.
   Igual que antes
   3.5. Elimina el usuario con userdel y vuelve a crearlo con las opciones pertinentes para que se cree su home y se copien los ficheros de inicialización al mismo.
   sudo userdel aso3
   sudo useradd -m -s /bin/bash aso3

   NOTA: no asignes contraseña al usuario con la opción “-p”, ya que useradd espera recibir la contraseña encriptada. Por ello, al crear un usuario no se le asigna contraseña y se deja la cuenta bloqueada.
4. Usando la orden **passwd** asígnale una contraseña al usuario aso2.
   Hay una errata, debería poner aso3:
   sudo passwd aso3
5. En el directorio **/etc/skel** están los ficheros de configuración iniciales que se copian a los directorios HOME de los usuarios cuando se crean sus cuentas. Realiza las modificaciones que sean oportunas para que:
   5.1. Al crear un usuario, se le copie a su HOME un fichero llamado “horario” que contenga lo siguiente “Las salas de prácticas están abiertas todos los días”. (Este fichero se copiará de forma automática al home de los usuarios que creemos a partir de ahora pero no se mostrará ni nada por el estilo).
   sudo nano /etc/skel/horario y añadimos el contenido que nos dice.
   5.2. Cada vez que el usuario entre en el sistema se ha de añadir al fichero inicios en el home del usuario la fecha de conexión. (Recordad que mediante >> podemos añadir la salida de un comando a un fichero y que si el fichero no existe se crea automáticamente).
   sudo nano /etc/skel/.profile → y añadimos la siguiente línea al final del fichero:
   date >>$HOME/inicios
   5.3. Cada vez que el usuario abra un terminal, se le dará la bienvenida con el mensaje “Bienvenido **nombre_de_usuario**” donde **nombre_de_usuario** será el nombre del usuario (Pista: busca la variable de entorno que contiene el nombre del usuario). Y además se ejecutará la orden who, que mostrará quien está conectado al sistema).
   sudo nano /etc/skel/.bashrc → y añadimos las siguientes líneas al final del fichero:
   echo “Bienvenido $USER”
   who
6. Crea el usuario aso4, con useradd asegurándote de usar los parámetros adecuados para que el usuario:
   - Utilice la shell de comandos /bin/bash
   - Se cree su directorio home y se copien los ficheros de inicialización.

   Una vez creado, comprueba que ha funcionado correctamente lo realizado en el ejercicio anterior, es decir, se ha copiado el fichero horario a su home, cada vez que el usuario entra en el sistema se añade al fichero inicios

la fecha de conexión y cada vez que el usuario abre un terminal se le da la bienvenida y se muestran los usuarios conectados.
sudo useradd -m -s /bin/bash aso4
sudo passwd aso4
Las comprobaciones os las dejo a vosotros.

7. Borra los usuarios aso1, aso2 y aso3, el primero con la herramienta gráfica, el segundo con deluser y el tercero con userdel y contesta a las siguientes preguntas :
   7.1. ¿Tienen el mismo efecto? (Comprueba si en todos los casos se borra el directorio HOME del usuario)
   En ningún caso lo borra automáticamente, pero en el caso de la interfaz gráfica, nos pregunta si queremos borrarlo o no.
   7.2. En caso de que con alguno de los comandos no se borre el directorio HOME, indica la opción que hay que indicar para que se borre dicho directorio.
   Con deluser tenemos que utilizar la opción –remove-home. También tenemos la opción –remove-all-file que eliminaría todos los ficheros que pertenezcan al usuario. (Delante de ambas opciones van 2 guiones, pero el procesador lo transforma automáticamente en un guión más largo).
   Con userdel tenemos que utilizar la opción -r.
8. En el campo “password” del fichero **/etc/shadow** podemos encontrar diferentes valores que indican distinto comportamiento del sistema o de la cuenta. Responde a las siguientes cuestiones:
   8.1. Si hay una cadena encriptada, es la contraseña y por tanto significa que:
   La cuenta está activa, tiene contraseña.
   8.2. Si encontramos “!!” o “*” o “!” significa que:
   La cuenta está bloqueada
   8.3. Para este último caso:
      a) ¿Es posible hacer un login?
      No
      b) ¿Pueden esos usuarios ejecutar procesos?
      Sí, solo hay que hacer un ps -aux y ver como hay usuarios con cuenta bloqueada que tienen procesos en marcha
      c) ¿Y poseer archivos?
      Sí, por ejemplo en el directorio /etc podemos encontrar algún fichero que posee algún usuario bloqueado.
   8.4. Una “x” en el campo “password” del fichero **/etc/passwd** significa que:
   Las shadow están activas, es decir, que la información sobre la contraseña se guarda en el fichero /etc/shadow.
   8.5. Si encontramos la contraseña encriptada en el campo “password” del fichero **/etc/passwd** significa que:
   Las shadow están desactivadas, es decir, que la información sobre la contraseña se guarda en /etc/passwd
9. La orden chfn permite que un usuario cambie la información que se tiene guardada sobre él en el fichero **/etc/passwd**. Estos datos se presentan cuando se usa la herramienta finger, por ejemplo al ejecutar “finger joadelvia” obtendremos:

Login: joadelvia	Name: Joaquín Delhom Viana
Directory: /home/joadelvia	Shell: /bin/bash
Office: 1, 555757575	Home Phone: 555676767

   9.1. Entra al sistema con el usuario aso4 y cámbiale esta información.
   chfn aso4
   9.2. Comprueba que en qué campo del fichero **/etc/passwd** se almacenan los datos introducidos y que formato se sigue para guardarlos.
   cat /etc/passwd
   Se guardan en el campo gecos separados por “,”.

   NOTA: la orden finger pertenece al paquete llamado también finger. Si no está instalado, hazlo con “apt-get install finger”.
10. Para el usuario aso4 establece los siguientes parámetros de tiempo (envejecimiento de la cuenta):
   10.1. El mínimo número de días entre cambios de contraseña es de 2 días.
   10.2. El usuario debe mantener, como mucho, 60 días una contraseña.
   10.3. Una semana antes de que su contraseña expire el sistema debe empezar a informarle.
   10.4. Si 15 días después de haber expirado la contraseña no ha sido cambiada, la cuenta se debe bloquear.
   10.5. La cuenta no debe ser accesible a partir del 12 de junio del presente año.

Se puede hacer todo con la siguiente línea:
sudo chage -m2 -M60 -W7 -I15 -E2012-06-12 aso4

11. Como usuario aso4, intenta cambiar la contraseña asignada. Cumpliendo las restricciones de tiempo, el sistema no te lo debe permitir.
Si lo hacemos todo como dice el enunciado, no nos deja ni utilizar la cuenta, ya que hemos puesto que la cuenta caducaba el 12 de junio y ya ha pasado.
12. Crea, usando la herramienta useradd, un nuevo usuario, apagar, que, haciendo uso de la orden /**sbin/halt**, apague el sistema. Asígnale una contraseña y comprueba si se apaga la máquina. Si no funciona como se esperaba, es muy probable que te estés equivocando al asignarle el UID a ese usuario. Piensa qué usuario es el único que puede ejecutar la orden halt.
sudo useradd -o -u 0 -s /sbin/halt apagar
Es imprescindible utilizar -o, ya que si no nos deja asignar un uid que ya existe.
sudo passwd apagar
su apagar
13. Haz uso de la herramienta **/usr/sbin/newusers** y crea tres usuarios a la vez, por ejemplo: aassoo1,aassoo2,aassoo3. Esta herramienta recibe como entrada un fichero, con el mismo formato que **/etc/passwd**, con el listado de todos los usuarios que se desean añadir. En este caso, se puede asignar una contraseña a los nuevos usuarios, indicándola en texto plano en el fichero correspondiente. Los usuarios deber tener la shell **/bin/bash** y contraseña **usuario**. Por último, comprueba si se crea o no el directorio HOME de los usuarios y si se copian los ficheros de inicialización.
Creamos un fichero (yo lo voy a llamar nuevos, pero podríamos poner el nombre que queramos).
nano nuevos
Y le añadimos las siguientes líneas:
aassoo1:usuario:1010:1010::/home/aassoo1:/bin/bash
aassoo2:usuario:1011:1011::/home/aassoo2:/bin/bash
aassoo3:usuario:1012:1012::/home/aassoo3:/bin/bash
Ahora ejecutamos newusers seguido del fichero para que añada los 3 usuarios al sistema:
sudo newusers nuevos
Utilizando ls podemos ver como si que crea los homes de los usuarios pero no les copia los ficheros de inicialización.
14. La orden chsh permite que un usuario cambie la shell que tiene asignada. Por otro lado, el fichero /etc/shells indica las shells que están permitidas en el sistema, es decir, que pueden ser asignada a un usuario. Ten en cuenta que prohibir un intérprete de órdenes significa que a partir de ese momento no se podrá seleccionar, pero los usuarios que previamente la tenían asignada, podrán seguir usándola sin problemas. Según esto, resuelve los siguientes ejercicios:
    14.1. Como administrador, “prohíbe” el uso de la shel **/bin/csh** y habilita el uso de **/bin/rbash**.
    /bin/rbash ya está habilitado (existe una línea que contienes /bin/rbash)
    Para prohibir /bin/csh podemos o borrar la línea o añadirle delante el símbolo “#”
    14.2. Como usuario aso4, intenta cambiarte la shell, seleccionando como nueva **/bin/csh**.
    chsh -s /bin/csh → no lo permite
    14.3. Como aso4, selecciona como nueva shell **/bin/ksh**. A continuación, entra al sistema con este usuario, y comprueba si te ha asignado el nuevo terminal.
    Chsh -s /bin/ksh → me dice que es un intérprete inválido, pero mirando en /etc/shells vemos que está permitida, el problema es que dicha shell no está instalada, para ello :
    sudo apt-get install ksh
    Repetimos el primer comando y ahora si que nos deja.
15. Shell restringida.
    15.1. Comprueba si existe el fichero /bin/rbash. En caso de que no exista, créalo como enlace simbólico al fichero **/bin/bash**.
    Sí que existe.
    15.2. Permite que la shell restringida pueda ser usada.
    Ya está permitida /bin/rbash
    15.3. Crea el usuario restringido (que no estreñido) y comprueba que acciones puede o no realizar. En la página de manual de bash (man bash), en la sección RESTRICTED SHELL, encontrarás una descripción detallada de lo que está prohibido para este nuevo tipo de shell.
    sudo useradd -m -s /bin/rbash restringido

16. Con la herramienta gráfica crea un nuevo grupo, aso, y haz que el usuario aso4 pertenezca al mismo.
    Trivial
17. Haciendo uso de la herramienta groupadd, crea un nuevo grupo llamado ssoo. Usando la herramienta usermod, haza que el usuario aso4 pertenezca a este nuevo grupo. ¡OJO! Tienes que hacer esto sin que deje de pertenecer al aso.
    groupadd ssoo
    usermod -a -G ssoo aso4 → La opción -a es imprescindible para que añada el usuario aso4 al grupo ssoo, si no la ponemos, el usuario aso4 perdería todas las pertenencias a grupos secundarios y pasaría a pertenecer solo al grupo ssoo.
18. Por defecto, useradd crea un grupo para el usuario con el mismo nombre. Crea un usuario aso5 con useradd asignándole como grupo primario el grupo aso y que además pertenezca a los grupos: ssoo y users.
    useradd -m -s /bin/bash -g aso -G ssoo,users aso5
19. Las órdenes id y groups permiten conocer los grupos a los que pertenece un usuarios. Entra al sistema como el usuario aso5 y realiza los siguientes ejercicios:
    19.1. Comprueba, con groups e id, cuál es el grupo activo del usuario.
    Trivial
    19.2. Crea un fichero ejecutando “touch prueba” y comprueba cuál es su grupo propietario.
    Trivial
    19.3. ¿Cómo será el comportamiento si estuviera activado el bit sgid del directorio donde se crea el fichero? Por ejemplo, si tenemos el usuarios aso5 que pertenece a los grupos users, aso y ssoo, y tenemos el siguiente directorio:
    drwxrwsr_x 7 aso5 root 4096 ene 27 10:15 synroot (Esto sería la salida del comando ls -l)
    Sabiendo que el usuario aso5 no pertenece al grupo root, si crea un fichero en el interior de ese directorio, ¿qué grupo es el propietario del fichero creado?
    NOTA: Esto todavía no lo hemos visto en clase, busca información sobre el bit sgid y resuelve el ejercicio.
    El bit sgid si está activo en un directorio hace que todos los ficheros y directorios que se creen en su interior se creen con el grupo propietario del directorio que lo tiene activado, por lo tanto, en este caso el grupo propietario será root.
    19.4. Con la orden **newgrp** haz que el nuevo grupo activo sea users. Comprueba con **groups** o **id** que ha cambiado el grupo activo. Crea un fichero y observa cuál es el grupo asignado al mismo.
    newgrp users (daría error porque nosotros no pertenecemos al grupo users) para ver el ejercicio podemos usar adm, un grupo al que si pertenecemos
    newgrp adm
    touch prueba
    ls -l
    Vemos que el grupo propietario del fichero es adm.
    19.5. Comprueba que **newgrp** realmente lo que hace es lanzar un nuevo intérprete de órdenes (shell). Al ejecutar exit finalizará ese intérprete y volverá a tener como grupo activo su grupo principal.
20. Deshaz todo lo que has hecho en esta sesión de prácticas: borra todos los usuarios creados, y todos sus directorios, borra también todos los grupos creados.

Ejercicios complementarios (sí, también hay que hacerlos)

1. Tenemos dos usuarios contratados a media jornada. Uno, llamado matutino, viene sólo por las mañanas, y el otro, vespertino, que viene sólo por la tarde, continúa el trabajo de matutino.

   El jefe quiere que, aunque sean personas diferentes, y cada uno use su propio login, en realidad sea el mismo usuario efectivo y tenga los mismos permisos, de forma que de cara al sistemas sean en realidad uno sólo. ¿Cómo podemos realizar esto?. Resuelve las siguientes cuestiones:

   1.1. ¿Qué UID y directorio HOME le asignarás a cada uno de ellos?

   Tenemos que asignarle a los dos usuarios el mismo uid y el mismo directorio home, por ejemplo:

   uid=1020 HOME=/home/turnos

   1.2. ¿Cómo se consigue que compartan todos los ficheros?

Creando los dos usuarios con el mismo uid y mismo home para el sistema son el mismo usuario, por lo que todos los ficheros que pertenezcan a uno pertenecerán al otro.

2. Si no deseo tener dos usuario con el mismo identificador, ¿puedo hacer que compartan el mismo directorio HOME? ¿Es posible conseguir que compartan los ficheros que hay dentro de ese directorio?

   Los dos usuarios deben pertenecer al mismo grupo como grupo principal y el grupo propietario de dicho directorio debe ser dicho grupo.