**1) Crea el usuario iso2 con la orden useradd y contesta a las siguientes preguntas**

**a) ¿Crea el directorio HOME?**

No, el fichero home tenemos que crearlos nosotros con el comando mkdir

**b) ¿Qué grupo primario le asigna?**

Se le asigna el grupo 1001

**c) ¿Copia los ficheros de inicialización al directorio de trabajo del usuario? Si lo creó, entra en su directorio y teclea ls -l**

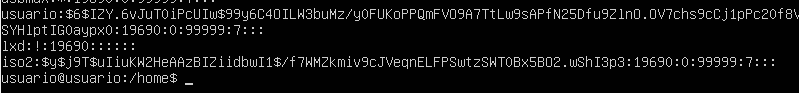
Si

**d) A continuación, observa lo que ha escrito en /etc/passwd y /etc/shadow. Haz una captura de pantalla.**

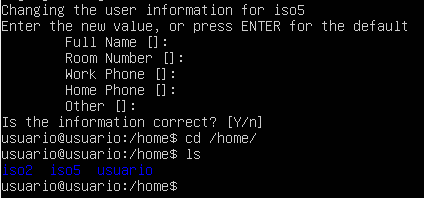
Con el comando etc/passwd nos muestra el directorio de iso2



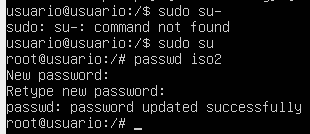
Con el comando etc/shadow nos muestra la contraseña de las cuentas de usuario



**e) Realiza los mismo pasos con la orden adduser y usuario iso5 y responde a las mismas preguntas anteriores**



**2) Usando la orden passwd, asígnale una contraseña al usuario iso2**



**3) 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 con adduser. Realiza las modificaciones que sean oportunas para que:**

* Queremos que al crear un nuevo usuario, se le copie a su directorio HOME, un fichero llamado “horario” que contenga lo siguiente ‘‘Las salas de prácticas están abiertas todos los días’’.





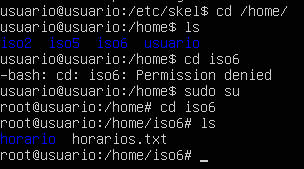
(Este fichero se copiará al HOME del usuario, pero no se mostrará ni nada por el estilo).

* Realiza las modificaciones necesarias sobre la carpeta /etc/skel

**4) Crea el usuario iso3, con useradd con la opción para que cree automáticamente su**

**directorio HOME, y comprueba que lo hecho en el ejercicio anterior funciona, (se le ha**

**copiado el fichero “horario”)**



**5) Borra el usuario iso3 creado anteriormente, con la orden userdel. Responde a las**

**siguientes preguntas:**



*a) Borra el directorio home del usuario*

No

*b) ¿Qué opción de userdel habría que emplear para que lo haga? (consulta la ayuda: man userdel)*

Deberíamos usar el comando: *userdel -r iso6*

**6) En el campo “password” del fichero /etc/shadow podemos encontrar diferentes valores que indican distinto comportamiento del sistema o de la cuenta. Responde las siguientes cuestiones:**

**Si hay una cadena encriptada, es la contraseña, y por tanto significa que:**

**Si encontramos “!!” o “\*” significa que:**

**Para este último caso:**

* *1) ¿Es posible hacer un login?*

No, ya que esto significa que la cuenta está deshabilitada

* *2) ¿Pueden esos usuarios ejecutar procesos?*

Tampoco podrá ejecutar ningún proceso

* *3) ¿Y poseer archivos?*

Si, poseer archivo si podría, solo que al no tener iniciada la cuenta no podrá verlos

* *4) Una “x” en el campo “password” del fichero /etc/passwd significa que:*

Significa que la autenticación del usuario se maneja de manera diferente y generalmente está vinculada a configuraciones específicas del sistema en uso.

**7) 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 pilar” obtendremos:**

**Login: pilar**

**Directory: /home/pilar**

**Oce: 3.45, 868 88 76 58**

**Name: Pilar Gonzalez Ferez**

**Shell: /bin/bash**

**Home Phone: 555555**

**(debes instalar antes la utilidad finger: sudo apt-get install finger)**

**Puedes consultar la ayuda: man chfn**

**Por ejemplo, este comando:**

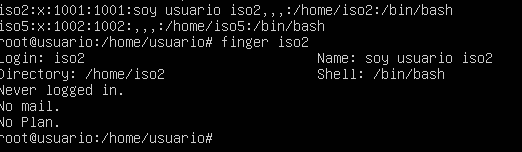
**chfn -r 24 usuario modifica la habitación (room) de usuario a la 24**

*a) Entra al sistema con el usuario iso2 y cambiale su información.*

*b) Comprobar en qué campo del fichero /etc/passwd se almacenan los datos*

*introducidos y qué formato se sigue para guardarlos. Por ejemplo, modifica su shell a /bin/sh*

*c) Compruebalo con la orden finger*

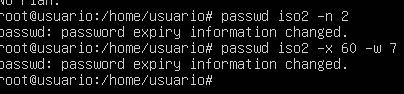
****

**8) Para el usuario iso2 establece los siguientes parámetros de tiempo:**

*a) El mínimo número de días entre cambios de contraseña es 2 días*

*b) El usuario debe mantener, como mucho, 60 días una contraseña.*

*c) Una semana antes de que su contraseña expire el sistema debe empezar a informarle.*

****

*d) Si 15 días después de haber expirado la contraseña aún no ha sido cambiada, la cuenta se debe bloquear.*

*e) La cuenta no debe ser accesible a partir del 12 de junio del presente año.*

****

**9) Como usuario iso2, intenta cambiar la contraseña asignada. Cumpliendo las**

**restricciones de tiempo, el sistema no te lo debe permitir.**

**10) Haz uso de la herramienta /usr/sbin/newusers y crea dos usuarios a la vez, por**

**ejemplo:iso6, iso7.**

*Esta herramienta recibe como entrada un fichero, con el mismo formato*

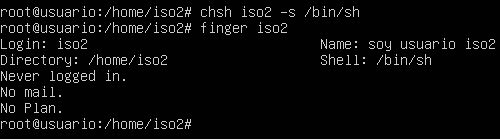
*que /etc/passwd, con el listado de todos los usuarios que se desean añadir. En este caso se puede asignar una contraseña a los nuevos usuarios, en texto plano en el fichero correspondiente.*

NO SE HACE

**11) 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 asignadas a un usuario. Ten en cuenta que prohibir un intérprete de las órdenes significa que a partir de ese momento no se podrá seleccionar, pero los usuarios que previamente lo tenían asignado seguirán usándolo sin problemas. Según esto, resuelve los siguientes ejercicios:**

*a) Como usuario iso2, intenta cambiarte la shell, seleccionando como nueva /bin/sh.*

*b) A continuación, en un terminal entra al sistema con este usuario, y comprueba si te ha asignado la nueva shell. (orden finger iso2)*



**12) Haciendo uso de la herramienta groupadd, crea un nuevo grupo llamado iso.**

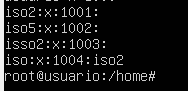
a) Usando la herramienta usermod, haz que el usuario iso3 pertenezca a este nuevo grupo.



b) Usando la herramienta gpasswd, haz que el usuario iso2 pertenezca a este nuevo grupo.



c) Visualiza ahora el contenido del fichero /etc/group



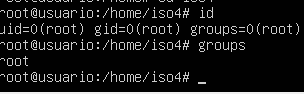
**13) Por defecto, useradd crea un grupo para el usuario con el mismo nombre. Crea un**

**usuario iso4 con adduser, y luego con usermod asígnale como grupo primario el grupo iso y que además pertenezca a los grupos: adm y users.**

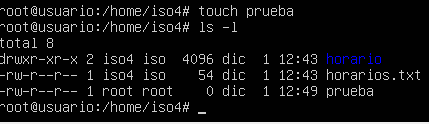


**14) Las órdenes id y groups permiten conocer los grupos a los que pertenece un usuario. Entra al sistema como el usuario iso4 y realiza los siguientes ejercicios:**

a. Comprueba, con groups e id, cuál es el grupo activo del usuario.



b. Crea un fichero ejecutando “touch prueba” y comprueba cuál es su grupo propietario. (ls -l)



c. Con la orden newgrp (newgrp grupo) y 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.

d. Comprueba que newgrp realmente lo que hace es lanzar un nuevo intérprete de órdenes.

e. Al ejecutar exit finalizará ese intérprete y volverá a tener como grupo activo su grupo primario.