Realiza los siguientes ejercicios, respondiendo a todas las preguntas y documentando cada paso (opciones seleccionadas, comandos introducidos, pantallazos de resultados obtenidos,…).

Aprovecha un fallo de seguridad (provocado) en Ubuntu

* 1. Haz que el fichero **/etc/groups** y **/etc/passwd** de un sistema Linux tenga permisos 777. Crea un usuario normal, sin ningún permiso especial, y consigue utilizando ese usuario ser **root**.
     1. Pista: puedes cambiar la password del root, o bien…
     2. Pista: puedes añadir usuarios al grupo **admin** y al grupo **sudo**, que son especiales para el comando **sudo**

Elección de una buena contraseña

* 1. Crea el hash de la contraseña **pass** (por ejemplo con el comando **md5sum** o **sha256sum**)
  2. Intenta encontrar el hash de la contraseña en Internet
  3. Cambia la contraseña por una mejor, y que no aparezca en los buscadores

Escalada de privilegios en Linux

* 1. Consulta información del permiso **s** en el manual de **chmod**
  2. Crea un usuario no administrador de nombre **normal**
  3. Crea una copia de la shell (**/usr/bin/bash**) en el directorio home de **normal** (**/home/normal/shell-de-root**)
  4. Haz que **shell-de-root** tenga como propietario a **root** y tenga el permiso **s**
  5. Ejecuta **shell-de-root** **–p** siendo el usuario **normal**. ¿Qué ocurre?

Implementa el uso de cuotas de disco en linux

* 1. Instala la el sistema de cuotas con **apt-get install quota**
  2. Consulta
     1. <http://www.linuxparatodos.net/portal/staticpages/index.php?page=04-disk-quota&mode=print>
  3. Crea un usuario con una cuota de 1000 KBytes. Llena su cuota (por ejemplo, bajando imágenes de Internet) y observa qué ocurre.

Listas de control de acceso. Haz una lista de qué permisos pueden otorgarse/negarse en Windows a

* 1. Ficheros
  2. Procesos (utiliza el programa **procexp.exe**)
  3. Entradas de registro (utiliza **regedit.exe**)

Utiliza el sistema de auditoría de Ubuntu

* 1. Realiza acciones relativas a seguridad en Ubuntu
     1. Intenta hacer login con un usuario que no existe
     2. Intenta hacer **sudo** con contraseña incorrecta
     3. Intenta hacer **sudo** con un usuario que no tiene acceso a **sudo**
  2. Localiza en qué fichero de log (**/var/log**) se han reportado dichos sucesos ¿qué información se obtiene?