Índice

Objetivo de la práctica

Durante el desarrollo de esta práctica, el alumno provocará varios agujeros de seguridad en sistemas Linux, que un usuario sin privilegios podría aprovechar para tomar el control del sistema. De esta forma podrá comprobar como errores más o menos sutiles pueden convertir un sistema en inseguro.

Además, investigará qué tipo de niveles de acceso puede tener un usario en el sistema y la forma de modificarlos.

Ejercicio 1 : Aprovecha un fallo de seguridad (provocado) en Linux (2 puntos)

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`.

Pistas

- Puedes cambiar la password del root, o bien...
- Puedes añadir usuarios al grupo admin y al grupo sudo, que son especiales para el comando sudo

Ejercicio 2 : Elección de una buena contraseña (1 punto)

- Crea el hash de la contraseña **pass** (por ejemplo con el comando `md5sum` o `sha256sum`). No uses `mkpasswd`, pues utiliza una **sal**.
- Intenta encontrar el *hash* de la contraseña en Internet. Si lo encuentras, es que la contraseña **pass** no es demasiado buena.
- Cambia la contraseña por una mejor, y que no aparezca su *hash* en los buscadores

Ejercicio 3 : Escalada de privilegios en Linux (2 puntos)

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

Ejercicio 4 : Implementa el uso de cuotas de disco en Linux (3 puntos)

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

Ejercicio 5 : Listas de control de acceso (1 punto)

Haz una lista de qué permisos pueden otorgarse/negarse en **Windows** a

- Ficheros
- Procesos (utiliza el programa `procexp.exe`)
- Entradas de registro (utiliza `regedit.exe`)

Ejercicio 6 : Auditoría de accesos en Linux (1 punto)

- Realiza acciones relativas a accesos en **Linux**:
  - Intenta hacer login con un usuario que no existe
  - Intenta hacer sudo con contraseña incorrecta
  - Intenta hacer sudo con un usuario que no tiene acceso a sudo
- Localiza en qué fichero de log (`/var/log`) se han reportado dichos sucesos ¿qué información se obtiene?

Qué se valorará

En la memoria del trabajo se valorará:

- Que cada paso quede bien documentado.
- La corrección técnica (que funcione)
- Que esté correctamente redactado, de forma que nuestro lector lo entienda
- La apariencia profesional:
  - Estética
  - Organización
  - Homogeneidad de formatos y estilos

Instrucciones de entrega

- El ejercicio se realizará y entregará de manera individual.
  - Solo se admiten trabajos en pareja, si en clase es necesario compartir ordenador.
  - En este caso, todos los integrantes del grupo deben subir el trabajo al aula virtual.
- Los trabajos pueden entregarse:
  - En formato **DOC** o **DOCX**.
  - En formato **ODT**.
  - En formato **PDF**.
  - Como una entrada en un **blog**
- La entrega se realizará en la tarea correspondiente del aula virtual. Si se entrega un fichero, este se subirá directamente. Si es una entrada de blog, se subirá un fichero de texto con la URL de dicha entrada.