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.

Cada paso está planteado desde el punto de vista de:

Un administrador de sistema  Intentará detectar, evitar o paliar los ataques a la seguridad. También cometerá errores que dejarán el sistema vulnerable.

Un *hacker*  Intentará aprovechar fallos en la seguridad

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

1. Problema de seguridad 

¡El usuario `root` a dejado a `777` los permisos de `/etc/groups` y `/etc/passwd`!

2. Un *hacker* lo aprovecha 

Tienes acceso al usuario `normal`, pero no tiene ningún permiso especial. ¡Aprovecha el problema de seguridad y consigue ser `root`!

- 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)

1. Problema de seguridad 

Un usuario utiliza una contraseña muy débil. Su *hash* md5 se guarda en el fichero `/etc/shadow`, y es `4c882dcb24bcb1bc225391a602feca7c`

2. Un *hacker* lo aprovecha 

- Consigues de un viejo *backup* el fichero `/etc/shadow`, así que conoces el *hash* md5 de la contraseña
- Intenta encontrar el *hash* de la contraseña en Internet. Si lo encuentras, cualquiera puede encontrar la contraseña a partir del *hash*
- Propón una contraseña mejor, e intenta encontrar en Internet su *hash* (calcula el *hash* con el comando `md5sum`).

Ejercicio 3 : Auditoría de accesos en Linux (1 punto)

1. Problema de seguridad 

Alguien está intentando acceder a tu **Linux**, probando usuarios y contraseñas por fuerza bruta

- Intenta hacer *login* con un usuario que no existe (por *ssh* o en una consola de texto)
- Intenta hacer `sudo` con contraseña incorrecta
- Intenta hacer `sudo` con un usuario que no tiene acceso a `sudo`

2. El administrador lo detecta 

Como tienes sospechas de lo que está ocurriendo, decides consultar los ficheros de log (en `/var/log`). ¿En qué ficheros se guardan estos sucesos?. ¿Qué información se obtiene?

Ejercicio 4 : Escalada de privilegios en Linux (2 puntos)

1. Problema de seguridad 

¡El usuario `root` se ha dejado una consola abierta!.
Ahora que lo has visto, quieres aprovechar la posibilidad para poder ser `root` otro día. Tu problema es que si cambias la contraseña **el administrador lo notaría**. Necesitas una forma que no afecte a la configuración del sistema (los ficheros de `/etc`).

2. El *hacker* lo aprovecha 

- Consulta información del permiso `s` en el manual de `chmod`
- Crea el usuario `normal2`
- Crea una copia de la *shell* (`/usr/bash`) en el directorio *home* de **normal2** (`/home/normal2/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 `normal2`. ¿Qué ocurre?

Ejercicio 5 : Implementa el uso de cuotas de disco en Linux (3 puntos)

1. Problema de seguridad

El usuario `normal` está abusando del sistema, ya que se está bajando multitud de archivos de Internet, y no deja sitio libre para el trabajo legítimo de los demás usuarios (es un ataque *Denial of Serivice*).

2. El administrador lo soluciona

- Consulta este enlace para ver cómo manejar las cuotas
- Haz que el usuario `normal2` tenga una cuota de 1000 KBytes, Observa qué ocurre cuando intenta utilizar más de este espacio del disco.

Ejercicio 6 : Listas de control de acceso (1 punto)

1. Problema de seguridad

El administrador tiene ahora un ordenador con **Windows**. Para configurarlo adecuadamente, necesita una lista de qué permisos pueden otorgarse/negarse en **Windows** a cada tipo de *objeto*.

2. El administrador lo soluciona

Consigue una lista de los permisos asignables a:

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

Qué se valorará

El resultado de la práctica debe ser una memoria con los pasos que el alumno ha seguido para seguir los pasos del administrador y el *hacker*. 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.

Créditos