Práctica 4.3

Seguridad lógica	
OBJETIVOS	Practicar el uso de los bits SUID/SGID y el registro de accesos al sistema
TAREAS	Uso de SUID / GUID Probar **chmod +s**, ejecutar archivos SUID, **find -perm** Probar las órdenes **last**, **lastb**, **lastlog** Usar sumas de control para vigilar archivos: MDA5, SHA...
DOCUMENTACIÓN	Diapositivas del Tema 4 «Seguridad lógica»; páginas de manual
TIEMPO ESTIMADO	1 hora en laboratorio

Tareas propuestas

1. Bit SUID/GUID

- Ejemplos de uso de SUID y GUID
- ¿qué programas hay en **/bin** y **/usr/bin** con el bit SUID activado?
- Actívale el SUID al programa **useradd** y observa cómo un usuario no privilegiado puede crear otras cuentas. ¡Cuando lo hayas probado, regrésalo a su estado original!

2. Registro de accesos

Estas son las principales órdenes y ficheros relacionados con el registro de accesos al sistema:

Información	**Herramienta (orden)**	**Ficheros de registro**
Último acceso de los usuarios	lastlog	/var/log/lastlog
Registro de accesos	last	/var/log/wtmp
Registro de intentos fallidos	lastb	/var/log/btmp
Registro de seguridad (incluye todos los intentos de acceso)	---	/var/log/secure

Con ellas podemos saber quién ha accedido al sistema, o quién ha intentado acceder sin éxito.

Prueba a abrir sesiones con varios usuarios, algunas de ellas fallidas. Observa el registro con **lastlog**, **last** y **lastb**. Observa el contenido de **/var/log/secure**.

¿Podrías saber con facilidad si alguien intentó entrar en el sistema sin éxito el día 9/11/2016?

¿Podrías saber cuántas sesiones ha abierto la semana pasada un usuario dado?

3. *Sumas de control*

Con **md5sum**, **sha1sum**, **shasum** podemos obtener *sumas de control* a partir del contenido de un fichero o de la entrada estándar. Estas sumas de control nos pueden servir para comprobar con bastante seguridad si un fichero ha sido modificado.

Ejemplo. Obtener sumas de control para unos ficheros:

```
$ md5sum /etc/passwd /etc/group
10e0c324eb557a113a5af3ee24ccd939  /etc/passwd
0861cb62b29e3f68f94de2609f67e9fd  /etc/group
```

Ejemplo. Obtener una suma de control para un texto:

```
$ echo "me vas a firmar este mensaje" | md5sum
5d31e58cac8b2d33fe1d690cdd69cafc  -
```

Tarea: obtén la suma de control de algún fichero del sistema (ej. /etc/passwd o un binario). Cambia el contenido del fichero y vuelve a obtener una suma de control. Verás que la suma cambia sensiblemente.