Comprobación de permisos. (Objetivo 104.7 del examen 101)

Puno de los permisos que podrían crear fallos de seguridad es el de escritura de un directorio para todos los usuarios. Podríamos buscarlo con:

```
find / -type d -perm -002
```

Permisos especiales. (Objetivo 104.5 del examen 101)

- **SetUID** (El programa se ejecutará con los permisos del usuario propietario)
- **SetGID**: Igual que setUID pero con los permisos del grupo. En caso de ser directorio los elementos creados pertenecerán al grupo del directorio.

Los podemos buscar con: `find / -perm /6000`

Ficheros en uso.

- **lsof**: Lista los fichero abiertos en el sistema. Podemos filtrar por:
  - ✓ `ruta`, -u `usuario`, -p `PID`, -c `nombre_proceso`, -i (IP)
- **fuser**: Muestra los procesos que están usando un fichero o directorio. Con la opción `-k` se le pueden enviar señales a los procesos implicados, `-v` nos muestra más detalles
- **iotop**: Muestra en tiempo real los procesos que están escribiendo en el disco

Usuarios y contraseñas. (Objetivo 107.1)

Con el comando `chage` podemos establecer una política segura para la gestión de las contraseñas por parte de nuestros usuarios.

Sudo

El comando `sudo` permite ejecutar ordenes con permisos de administrador.

```
sudo cat /etc/shadow
```

Para gestionar los permisos que concede sudo usaremos: `visudo /etc/sudoers`

Este comando lanza el editor por defecto y al guardar comprueba la sintaxis.

Reglas de acceso en sudoers

La sintaxis es: `usuario_destino host=(usuario:grupo) comando/s`

Podemos usar diversos alias para agrupar usuarios, grupos, comandos, etc.

Si queremos hacer referencia a "todos" usamos ALL.

Su

El comando `su` cambia a otro usuario. Si no se indica ningún parámetro cambia al usuario root. Para que se inicie el entorno de ejecución del usuario al que cambiamos hay que poner `su -`

Información sobre logins

- **who**: indica quién está identificado en el sistema
- **w**: muestra quién hay y qué está ejecutando
- **last**: lista los últimos accesos que ha tenido el sistema.

Limitar el uso del sistema

En el fichero `/etc/security/limits.conf` podemos establecer diversos límites de uso del sistema a usuarios o grupos de usuarios. Cada fila es una limitación y tiene el formato:

```
domain    type    item      value
```

- **domain**: es quién se verá afectado por la restricción
- **type**: puede ser hard (dura) o soft (blanda).
- **Item**: a qué recurso afecta la limitación
- **value**: el valor límite

El comando **`ulimit`** sirve para poner límites a nivel de todo el sistema

Comandos de red

- **netstat / ss**: Mostrar puertos abiertos y conexiones establecidas
  (Objetivo 109.3)
- **nmap**: escaneo de puertos y otro tipo de comprobaciones
  - ✓ `nmap 192.168.0.50`
  - ✓ `nmap -sP 192.168.0.0/24`
  - ✓ Puedo usar rangos de puertos o IP's: `nmap -p 20-40 192.168.0.10-80`

    https://www.comparitech.com/net-admin/nmap-nessus-cheat-sheet/

  - ✓ Se pueden hacer escaneo muy avanzados con script

    https://www.hacking4badpentesters.com/2017/04/scripts-nmap-para-tener-mano-si-sos.html