[FORT] Tema 3: Securizando el Sistema de Ficheros

Tenemos dos aproximaciones al uso de discos y particiones en linux:

- **Sistema de archivos en particiones**: Considerada la aproximación tradicional, el sistema de archivos se crea en cada dispositivo físico. Cada dispositivo físico debe ser montado para ser accesible. Las particiones no pueden ser cambiadas de tamaño fácilmente. Este tipo de sistema puede ser cifrado
- **LVM**: Sistema de volúmenes lógicos. Es más flexime que la aproximación tradicional ya que se puede añadir espacio dinámicamente. Es más fácil de administrar y aca volúmen lógico puede ser cifrado. No es recomendable para la partición /boot. Para usar esta aproximación en sistemas debian se debe instalar el paquete lvm2
    - Volúmenes Físicos: Son discos duros o particiones configuradas como tales.

Posibles amenazas para el sistema de archivos

- Acceso No Autorizado: Para prevenirlo se puede hacer lo siguiente:
    - Todos los directorios home deben tener el permiso 700 y podemos establecer el umask para que sea 077
    - Los archivos de configuración de diferentes daemons no deben ser legibles.
    - Algunas distros tienen programas que revisan y establecen periódicamente los permisos de los archivos en el sistema de archivos
- Que el sistema de ficheros sea llenado a tope y nadie pueda escribir en el
- Corrupción del sistema de archivos haciéndolo inutilizable
    - Usar un sistema de archivos fiable y probado
    - Mantener la máquina en un ambiente estale.
    - Tener cuidado con los permisos de archivos
- Ganar acceso a archivos maliciosos con privilegios altos.
    - Usar ACL (Listas de Control de Acceso)