

Gestion de privilegios y root

- El usuario root (UID 0) es el administrador total
- Best practice: no logearse directamente como root. Usar sudo para auditoria y seguridad
- Combinación de identidad: (Su vs Sudo)

2) Base de datos de usuarios

Lista almacenada idénticamente en archivos de texto en /etc/. Se pueden consultar con cat, grep o getent

A) /etc /passwd (definición de usuario)

legible por todos. Estructura de campo (separador por ':')

1 usernone (sysadmin)

2) password placeholder (\rightarrow incluye que estén en shadow)

3) UID : User ID (0 = root, 1 - 999 = sistema, 1000+ = usuarios)

4) GID : Group ID principal

5) Comentarios (nombre real)

6) home Directory (/home /sysadmin)

7) Shell : /bin/bash o /sbin/nologin
(eventos de servicios /demonios)

B /etc /shadow

Solo legible por root. Contiene la política de contraseñas. Campos claros para auditoria

- hash del password : algoritmo + salt + salt + hash (si hay * o !, la cuenta esté bloqueada / sin password)
- Last Change : días desde "the epoch" until now calculados en segundos

Credenciales con panchos

- aging : mínimos / máximos de días para Cambio , días de advertencias , inactividad y expiración
- /etc/group Define membership secundarios
Formato ; nombre_grupo :x:gid:
usuari1, usuari2
- importante para Compartir recursos entre equipos