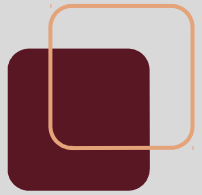
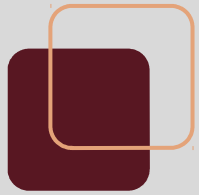


Taller de Infraestructura: Usuarios y Grupos

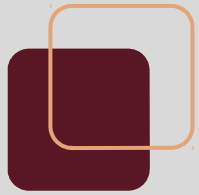
FING – IMM - 2017

Motivación



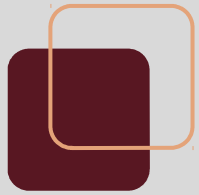
- ¿Por qué utilizar usuarios y grupos?
  - Seguridad:
    - Prevención y detección de acciones no autorizadas
    - Auditoría de las acciones realizadas
    - Aislamiento de acciones en sistemas compartidos

Conceptos Básicos



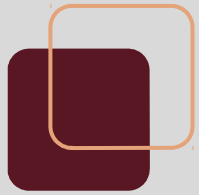
- En sistemas operativos, la información sobre los usuarios se mantiene en cuentas de usuario.
  - Información de autenticación
  - Privilegios
  - Permisos sobre ciertos objetos

Sistemas UNIX



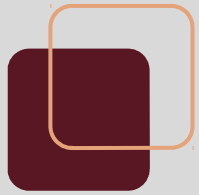
- Usuarios son identificados por un *nombre de usuario* y autenticados con su *contraseña.*
  - Contraseñas guardadas en /etc/passwd
  - Cada línea contiene:
    - Nombre de usuario
    - Contraseña (encriptada)
    - id de usuario (uid)
    - id de grupo (gid)
    - Directorio home
    - Shell a utilizar

Sistemas Unix



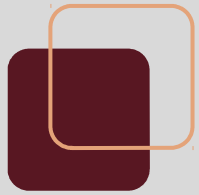
- Modificación de contraseña
  - Comando *passwd*
- Cambio de usuario
  - Comando *su*

Sistemas Unix: Usuarios y superusuarios



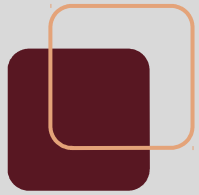
- Usuarios se representan con un nombre de hasta 8 caracteres. Internamente con un identificador de 16 bits. Algunos id’s tienen significados especiales:
  - 0: root
  - 1: demonio
- El usuario root (uid = 0) tiene permiso para realizar casi cualquier acción. Se le denomina ‘superusuario’
  - Problema de seguridad

Sistemas Unix: Grupos



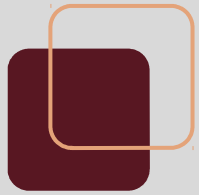
- Usuarios pertenecen a uno o más grupos.
  - Todos los usuarios pertenecen al *grupo primario*
  - Grupos mantenidos en /etc/group con la siguiente información
    - nombre del grupo
    - contraseña
    - id del grupo
    - lista de usuarios

Sistemas Unix:
Cambio de usuario y de grupo



- Programas *suid* y *sgid*
  - Permiten acceso de superusuario a usuarios comunes.
  - *passwd, login, at, su* utilizan esta filosofía

Sistemas Unix: Control de Acceso

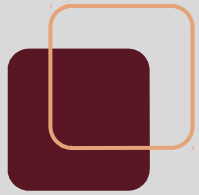


- Permisos de lectura/escritura/ejecución sobre archivos, donde se especifica el control de acceso hacia el mismo por parte del *owner*, de aquellos usuarios del mismo grupo que el archivo y de todos los demás usuarios.

  Ejemplo: -rwx--x---

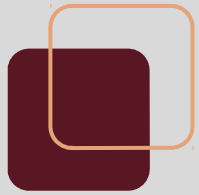
- Cambio de permisos:
  - chmod *absoluto archivo*
  - chmod *[quien] [permisos] archivo*

Sistemas Windows



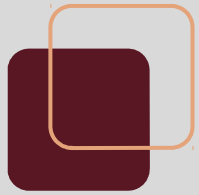
- Autenticación por *usuario* y *contraseña*
- Control de acceso realizado con *listas de control de acceso*

Sistemas Windows: Dominios



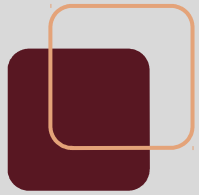
- Los sistemas Windows incluyen la noción de dominio, la cual consiste en una red de computadoras que utilizan una misma base de datos de usuario para realizar el control de acceso y las mismas políticas de seguridad.
  - Base de datos mantenida en 'controlador primario de dominio' (PDC)
  - Si el PDC no está disponible, no se pueden realizar actualizaciones!

Sistemas Windows: Usuarios locales y globales



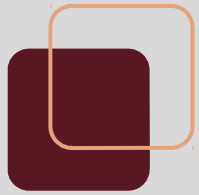
- Los puestos de trabajo pueden mantener sus propias bases de datos de usuarios, generando la noción de usuario ‘local’ (cuando el usuario está autenticado en la máquina local) y usuario ‘global’ (cuando el usuario se autentica en el dominio)

Sistemas Windows: Cuentas de usuario



- En un sistema Windows las cuentas de usuario guardan la siguiente información:
  - nombre de usuario
  - nombre completo
  - contraseñas (encriptadas)
  - horas de trabajo y puestos de trabajo
  - script inicial
  - directorio home

Sistemas Windows: Grupos locales y globales



- Windows define dos tipos diferentes de grupos:
  - Grupos globales: son aquellos definidos sobre el dominio
  - Grupos locales: son aquellos definidos sobre el puesto de trabajo
- Existen algunos grupos por defecto
  - Administradores de dominio
  - Usuarios de dominio
  - Invitados de dominio