

Protección

• Protección de la memoria

• Control de acceso orientado a usuario → Identificación Usuario/password.

→ Arquitectura Single sign on

• Control de acceso orientado a datos → Permisos específicos para determinados usuarios.

→ Matriz de acceso.

→ Sujeto

→ Objeto

→ Derecho de acceso.

→ Lista de control de acceso

→ Tickets de capacidades.

Intrusos

→ Enmascarado

→ Un individuo que no está autorizado a utilizar un ordenador y que penetra en los controles de acceso del sistema para aprovecharse de una cuenta de usuario.

→ Trasgresor

→ Usuario legítimo que accede a datos, programas o recursos para los cuales dicho acceso no está autorizado, o si está autorizado usa los recursos de forma maliciosa.

→ Usuario Clandestino

→ Un usuario que sobrepasa el control de supervisión del sistema y usa dicho control para evadir la auditoría y el control de acceso o para suprimir la recogida de registros de acceso.

Técnicas de intrusión

• Formas de protección de ficheros de contraseña

→ Cifrado Unidireccional

→ Control acceso.

• Estrategias de selección de contraseñas

→ Educación de los usuarios

→ Contraseñas generadas por ordenador

→ Verificación reactiva

→ Verificación proactiva.

Detección de Intrusos

→ Bitácoras (registros de sucesos y logs)

→ Detección de anomalías

→ por umbral

→ Basado en el perfil.

→ Prevención.