TEMA 7 →ATAQUES Y CONTRAMEDIDAS

Seguridad activa en el sistema

- **Seguridad en el acceso de un ordenador**:
  - Colocar candados: Kensington, con detector que se graba en la BIOS la fecha y hora de apertura.
  - Asegurar arranque con contraseña:
    - BIOS
    - GRUB
    - CIFRAR PARTICIONES
    - CUOTAS DE DISCO
- **Autenticación de usuarios:**
  - Algo que el usuario sabe (contraseña)
  - Usuario posee(tarjetas)
  - Características propias del usuario: Huellas dactilares y reconocimiento Biométrico.
  - Combinaciones de diferentes métodos.
- **Políticas de contraseñas:**
  - Tener en cuenta las características que deben cumplir las contraseñas.
  - Las contraseñas deben ser:
    - Cadenas de caracteres compuestas por mayúsculas, minúsculas y caracteres especiales.
    - La longitud oscila entre 8 y 14 caracteres.
    - En general se debe intentar cumplir todas las características vistas anteriormente.
- **Sistemas biométricos**
- **Tarjetas:**
  - Las tarjetas son de dos tipos:
    - Sencillas→Magnéticas.
    - Complejas (CHIP)→Estas son más seguras, pero de coste más alto.
- **Evaluación de privilegios**:
  - Consiste en pedirle al sistema ejecutar un determinado programa con permisos de administrador.
- **Listas de control de acceso (ACL):**
  - Mejorar seguridad de archivos
  - Define privilegios que tiene el usuario de forma individual
  - Permite limitar acceso a ficheros
  - Las ACL son tablas que dicen al S.O. que y quienes pueden acceder:
    - Son exclusivas de formato NTFS
    - Para acceder a las tablas se debe utilizar: un comando especifico
  - Tienen asociados parámetros de seguridad que se llaman descriptores:
    - Quien es el propietario
    - A que grupo de usuarios pertenece
    - Quien tiene acceso
    - Que permisos de accesos

- Los descriptores son metadatos no están en ninguna carpeta; estos datos se describen otros datos que describen otros datos y sirven para suministrar información sobre los datos producidos.
- **Cuotas de disco:**
    - Definición: Para aplicar una cuota en el sistema se establece que cada usuario pueda ocupar un número determinado de bytes (y otras capacidades) cuando se excede ese límite se puede configurar de forma que en sistema no pueda extenderse hay que asignar cuotas teniendo espacial cuidado en que no sean ni bajas ni muy altas.
- **Actualizaciones y parches:**
    - Las actualizaciones son paquetes de software donde se introducen mejoras y se corrigen defectos, para configuran las actualizaciones se realizan desde panel de control y las opciones depende del sistema.
- **Vulnerabilidades del sistema:**
    - Para evitaras hay que mantener el sistema actualizado.
    - En Linux:
        - **Last:** Con este comando podemos ver los últimos que se han logeado y los últimos reinicios del sistema.
        - **Lastb**: Muestra los intentos fallidos del login en el sistema.
        - **Lastlog**: Información reciente de los login de todos los usuarios.
- **Monitorización:**
    - Para vigilar que todo esta correcto revisar los ficheros log (que es donde queda anotado cualquier suceso anómalo)
    - Activar las copias sincronizadas del log
    - Revisar la ocupación del sistema
    - Suscribirse a las newletters de los fabricantes de nuestro hardware
    - Participar en foros de usuarios
    - La monitorización del log consiste en diferenciar que es un problema y que no lo es, el texto del fichero del log suele tener identificador de gravedad.

ATAQUES Y CONTRAMEDIDAS→ POWER POINT

- **Vulnerabilidad:**
    - **Bug**: Fallo de seguridad en el software que puede hacer el programa funcione incorrectamente.
    - Frente a esto los fabricantes de software publican:
        - Fix , Hotfix: programas que eliminan los bug.
        - Patch: programas que resuelven las consecuencias del bug.
        - Service Pack: son nuevas versiones de un programa.
    - **Exploits:** Errores por parte del desarrollador o en el proceso del desarrollo del software que suponen brechas de seguridad aprovechan los ciberdelincuentes.
    - Solución: Mantener el software actualizado y estar al corriente de las URL de las siguientes vulnerabilidades de las aplicaciones.
- **Hackers:**
    - Experto en seguridad informática con buenas o malas intenciones que interviene o realiza con unas intenciones se clasifican en sombrero negro, gris y blanco.
- **Ataques**:

    - Los ataques se producen porque aprovechan las vulnerabilidades y estos ataques pueden ser intercepción, modificación y fabricación.
- **Malware:**
    - Software malicioso que daña el sistema con el objetico de obtener información del mismo.
- **Escaneo:**
    - Búsqueda de información.
- **Técnicas:**
    - Footprinting: En busca de información pública depende de la seguridad.
    - Spidering: Funciona inspeccionado páginas web para almacenar información irrelevante como direcciones de correos y registros de páginas.
    - Fingerprinting: Consiste en recopilar información sobre el sistema de una organización identificando puerto, sistemas operativos etc.
- **Ataque DoS**: Son ataques que interrumpen un servicio.
    - Sniffing: Son análisis del tráfico de red con fines malicioso con la intención con obtener datos personales etc.
    - Spoofing: Suplantación de identidad.
    - Man in the middle: El atacante se sitúe entre las dos partes que intentan comunicarse interceptando los mensajes.
- **Ingeniería social:** Utilizando los hackers para obtener información intentan conseguir ofreciendo correos, formularos maliciosos para que compartan información.
- **Botnets**: Red de ordenadores infectados controlados por un ciberdelincuente.
    - Que hacen: Recopilar información tales como capturas de contraseñas y datos personales que después se venden en la DEEP WEB , envían spam, manipulan encuestas etc.