**Seguridad: Tema 5**

1. La seguridad activa en los sistemas
   1. **Introducción**

Una vez sufrido un ataque es importante conocer qué quiere el atacante y cómo lo quiere conseguir con el objetivo de organizar una buena defensa.

* 1. **El ataque informático**

El atacante lleva a cabo un proceso organizado para realizar dicho ataque, fases de un ataque:

* Descubrir los sistemas que componen la red la cual se quiere atacar
* Exploración de las vulnerabilidades en los sistemas
* Explotación de las vulnerabilidades detectadas
* Compromiso del sistema
* Ocultamiento o eliminación de los rastros del ataque

Las herramientas utilizadas para aprovecharse de vulnerabilidades se conocen como “exploits”.

La corrupción del sistema consiste en modificar el SW o los datos de un sistema para que sean explotados remotamente por el atacante.

Para la eliminación de pruebas habrá que borrar los ficheros log o procesos que revelan la actividad del sistema.

**Tipos de ataques**

Existen números tipos de ataques posibles, y cada vez existen más formas de atacar, por lo que el administrador tiene que estar prevenido de la mejor forma posible, vigilando comportamiento de usuarios y aplicaciones sospechosos. Principales ataques ante un sistema informático:

* Acciones de reconocimiento y descubrimiento de sistemas
* Detección de vulnerabilidades
* Robo de información mediante la interceptación de tráfico (sniffing)
* Cifrado de información con rescate económico (ransomware)
* Modificación de contenidos en los mensajes enviados por la red
* Alteración de los números de secuencia en los mensajes transmitidos
* Análisis de tráfico de red.
* Suplantación de la identidad
* Alteración de las tablas de enrutamiento o tablas de direcciones físicas
* Conexión no autorizada a los sistemas de la red para introducir malware
* Denegaciones de servicio
* Propagación de malware
* Alteración o destrucción de información.

**Herramientas utilizadas en un ataque**

Los atacantes utilizan herramientas apropiadas y de última generación para realizar los ataques y usualmente tienen altos conocimientos en ocultación, suplantación y criptografía.

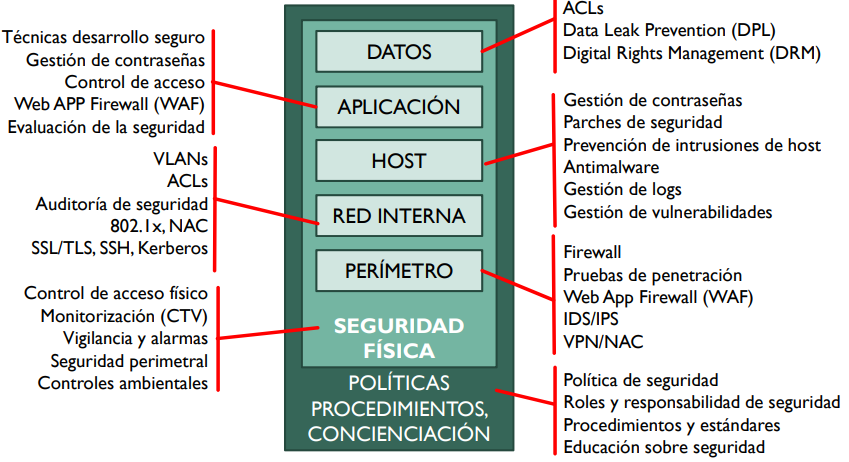
1. La defensa en profundidad

**2.1. Introducción**

La defensa en profundidad es una estrategia que consiste en proteger los sistemas con varias capas para que en caso de que una falle, los sistemas no se vean comprometidos y el ataque tenga el menor impacto posible.

De esta forma se puede dividir el problema de la seguridad en ámbitos más pequeños y con soluciones más manejables y especializadas

Las contramedidas puedes ser pasivas o activas. También pueden ser físicas o lógicas



**Medidas de defensa**

* **Defensa en políticas, procedimientos y concienciación:** definen los objetivos y actividades para el control de la seguridad, además de proveer un criterio para realizar auditorías. Estas políticas deben ser comunicadas a todo el personal.
* **Defensa en cortafuegos:** El firewall es la primera línea de defensa de la red ya que gestiona la conexión entre la red interna y la externa.
* **Defensa en el sistema de detección de intrusos (IDS):** Monitorizan el tráfico de la red para detectar cualquier actividad sospechosa. Generan muchos falsos positivos por lo que hay que gestionarlo de forma correcta para que no interrumpa la actividad de la empresa.
* **Defensa en el control de acceso a la red (NAC):** determinan si los equipos que se conectan a la red cumplen con las políticas de seguridad requeridas por el administrado. Es decir, antivirus y SO actualizados, etc.…
* **Defensa contra malware:** Utilizar y gestionar adecuadamente SW antimalware.
* **Defensa mediante cifrado:** utilizar técnicas criptográficas para proteger la integridad, confidencialidad y autenticidad de los mensajes. Es muy importante custodiar de manera correcta la claves.
* **Defensa de los equipamientos físicos:** mantener controles de seguridad física (cámaras, alarmas, etc…) Especialmente para el CPD.

**Control de acceso al sistema**

A la hora de gestionar contraseñas, hay que tener en cuenta:

* Longitud mínima de las contraseñas
* Caducidad de las contraseñas
* Contraseñas diferentes en cada renovación
* Contraseñas que contengan símbolos especiales (mayúsculas, minúsculas, símbolos especiales, números)
* Usar contraseñas junto con tarjetas de identificación
* Monitorizar los accesos al sistema y los cambios de contraseña.

**La seguridad en la BIOS y en los gestores de arranque**

El acceso a la BIOS debe estar protegido siempre con contraseña.

La BIOS también permite proteger el acceso a los discos mediante contraseña, para que solo aquel que la conozca pueda arrancar el sistema.

Cambiar el gestor de arranque para que el ordenador inicie siempre y únicamente con el HDD para evitar programas que copian el Disco duro a un DVD.

Los ataques a la BIOS pueden generar los siguientes problemas:

* Denegación de servicio: evitar que el equipo arranque o deshabilitar parte del HW.
* Ataques de suplantación: arrancar desde un disco alternativo que es una copia del SO original para que el usuario introduzca información confidencial
* Fugas de información: arrancar desde un LiveCD para copiar los datos del SO o formatear las particiones.

**Actualización de sistemas y aplicaciones**

Es muy importante mantener los sistemas actualizados para reducir el número de vulnerabilidades

Nunca realizar una actualización sin una copia de seguridad en caso de que el proceso de actualización falle o la actualización tenga algún fallo de seguridad.

Principales motivos para actualizar el SO y las aplicaciones:

* Eliminar vulnerabilidades detectadas (bugs)
* Mejoras en el Software
* Incorporación de nuevas funcionalidades
* Compatibilidad con nuevas plataformas de SO
* Compatibilidad con el HW más novedoso

También es importante mantener actualizado el firmware del HW, periféricos y la BIOS

Las actualizaciones siempre las deberá hacer el administrador, teniendo en cuenta que no interfiera con el antivirus

**2.2. Seguridad en discos y ficheros**

**Seguridad en el particionado de discos**

Es importante elegir como se configuran las particiones y cada una de estas debe llevar una seguridad específica. Las particiones deben tener el espacio suficiente y admitir seguridad en los ficheros (no utilizar FAT)

Los sistemas de ficheros más seguros son ext4 y NTFS ya que permiten seguridad en los ficheros (contraseñas) y garantizan que las operaciones de escritura no se queden a medias por un fallo del HW.

Además, es importante configurar de manera adecuada los permisos que tiene cada usuario y asignar las operaciones (lectura, escritura, ejecución) oportunas a cada rol. También es conveniente utilizar copias de seguridad.

**Lista de control de acceso (ACL)**

Una ACL indican los usuarios (o equipos) que tendrán acceso a un determinado recurso, el conjunto de reglas que definen el acceso se denomina política.

Los SO disponen de un sistema de permisos para asignar a cada fichero o carpeta, pero debido a que los permisos no son compatibles entre Windows y Linux esto puede suponer una fuente de vulnerabilidades.

**2.3. La autenticación para el acceso al sistema**

Todo usuario deberá tener una cuenta que lo identifique para utilizar los recursos. Esta cuenta tendrá ciertos permisos según la función que realice.

Los administradores deben tener en cuenta:

* Deshabilitar las cuentas conocidas.
* Restricciones en el logon de los usuarios
* Política de contraseñas para el usuario

**2.4. Ataques con software malicioso**

Software malicioso (o malware) es todo aquel programa o código que daña un sistema. Los sistemas de alta seguridad deben tener antivirus con varios motores de análisis

Clasificación general de malware:

* Virus: programa ejecutable que daña un sistema y además se propagan a través del software
* Ransomware: encripta la información del sistema y pide un rescate económico
* Gusanos: programas de autorreplica que se propagan por la red para causar una denegación de servicio.
* Troyanos: código oculto en programas inofensivos que se activa cuando se ejecuta el programa anfitrión.
* Backdoors: forma de acceder al sistema sin medidas de seguridad que utilizan los desarrolladores y pueden ser aprovechadas por los atacantes.
* Spyware: software que espía las actividades de los usuarios
* Adware: software para integrar publicidad no deseada
* Spam: envío masivo de correo no deseado

El objetivo principal del malware es la denegación del servicio y la obtención de privilegios de administrador

**2.5 Seguridad en la conexión de redes públicas**

Cuando un equipo se conecta a una red pública aumenta el riesgo ya que incrementa el número de posibles ataques. Los riesgos más comunes son:

* El cortafuegos no está configurado correctamente
* Las transmisiones no están cifradas
* Conexiones telnet o ftp no cifradas
* Obtención de información sensible a través de foros…
* Sesiones abiertas en servidores de chat (IRC)
* Ataques de denegación de servicio

Estos riesgos se pueden atenuar utilizando las siguientes contramedidas:

* Utilizar un buen antivirus y actualizado
* Activar y configurar de manera correcta el Firewall
* Configurar el antivirus para que proporcione seguridad con antispam, antiphising y detección de vulnerabilidades
* Proteger las conexiones mediante cifrado
* Utilizar redes privadas virtuales (VPN)
* Validar conexiones remotas con sistemas de autenticación (SSH)