**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.

**Clasificación de atacantes por su actividad:**

* Hacker: experto en seguridad informática que conoce en profundidad los sistemas de cifrado y como aprovecharse de vulnerabilidades de seguridad. Los hackers contratados por empresas para reforzar su seguridad se conocen como hackers de sombrero blanco.
* Cracker: experto en programación cuya finalidad es atacar sistemas y destruirlos
* Bucanero: comerciante ilegal de la red. Utiliza sus amplios conocimientos en negocios para realizar fraudes.
* Lammer: persona que desea convertirse en un hacker, pero posee pocos conocimientos. Utiliza programas creados por otros los cuales no dominan a la perfección. Los principiantes en la materia reciben el nombre de newbie
* Copyhacker: falsificador de hardware, su motivación es simplemente económica
* Phreaker: elevados conocimientos de telefonía para realizar actividades ilegales
* Kiddie: usuario con bajos conocimientos que descarga y ejecuta cualquier programa, infectando su equipo y los de la red

**Clasificación de atacantes según su relación con el ataque:**

* Sniffers: escuchar el tráfico de la red para descifrar los mensajes
* Spammers: envío masivo de correo no solicitado que colapsa buzones y servidores
* Programadores de malware: expertos en programación que construyen virus.
* Personal interno a la organización: empleados que por despiste o malicia causan daños a la empresa
* Antiguos empleados: aprovechan sus cuentas no canceladas para atacar a su antigua empresa
* Intrusos remunerados: expertos en informática para sabotear una empresa desde dentro

**La motivación del atacante**

* Motivos económicos
* Ideología (terrorismo)
* Compromisos con ciertas personas o empresas
* Reconocimiento social y autorrealización
* Diversión

**Riesgos asociados con las personas**

La ignorancia de los usuarios es el mayor peligro, pero se puede combatir con formación. También existen otros peligros:

* Atacantes que utilizan ingeniería social para averiguar contraseñas
* Configuración incorrecta de las cuentas (o no eliminarlas cuando ya no están en uso)
* Incumplimiento de las políticas de seguridad
* Errores en la documentación y su comunicación a los usuarios.
* Empleados descontentos
* Equipos erráticos no controlados
* Contraseñas inseguras
* Usuarios que habilitan puertas traseras
* No desechar bien los medios de almacenamiento
* Contraseñas escritas en papel
  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 numerosos 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. Herramientas más comunes:

* Escáneres de puertos: detectar los servicios instalados en un sistema local o remoto
* Sniffers: programas que escuchan la red para capturar los paquetes que circulan por ella
* Exploits: programas que se aprovechan de vulnerabilidades en los sistemas
* Backdoors: aplicaciones que permiten abrir agujeros de seguridad, dejando puertos abiertos
* Rootkits: tener privilegios de administrador y ocultar malware con el fin de despistar los sistemas de seguridad
* Auto-rooters: herramientas para automatizar ataques
* Password-crackers: aplicaciones que permiten averiguar las contraseñas gracias a diccionario o fuerza bruta.
* Generadores de malware: aplicaciones que generan virus u otro tipo de malware

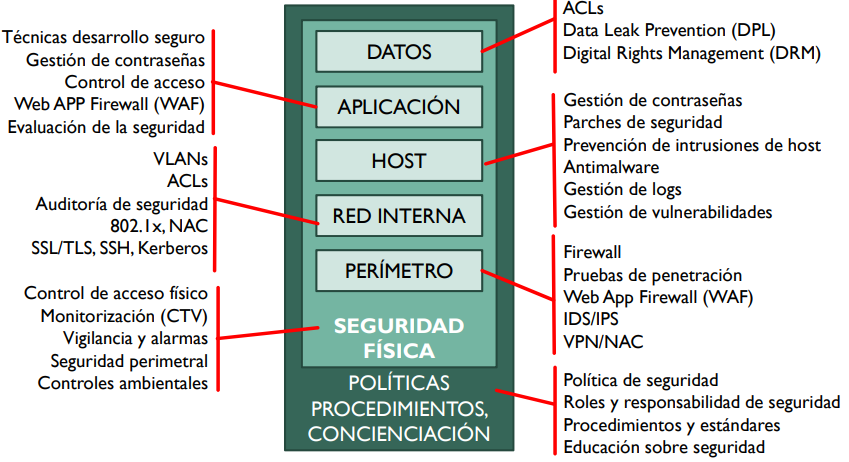
1. La defensa en profundidad

**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 pueden 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 administrador. 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 las claves.
* **Defensa de los equipamientos físicos:** mantener controles de seguridad física (cámaras, alarmas, etc.…) Especialmente para el CPD.

**Control de acceso al sistema**

Para diseñar un sistema de acceso seguro a las instalaciones hay que plantearse las siguientes cuestiones

* ¿Qué salas deben ser protegidas y qué salas tiene sistemas críticos?
* ¿Qué formas de acceso tiene un intruso?
* Definir los horarios para cada usuario
* Instrucción de los empleados sobre el sistema de acceso
* Métodos de autenticación permitidos por la organización
* Auditorías del sistema de seguridad
* Cambio frecuente en las contraseñas
* Creación de un plan de seguridad y de respuesta

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 diferentes caracteres (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: cuentas creadas por defecto por el SO, deben ser eliminadas o renombradas para que un atacante no las pueda encontrar (cuenta admin, root, o guest)
* Restricciones en el logon de los usuarios: horarios de uso, tiempo máximo de uso por día, restringir el uso solo a ciertas IPs y establecer un numero máximo de intentos fallidos en el inicio de sesión
* Política de contraseñas para el usuario: largas y complejas, cambios frecuentes.
* Otros medios de control de acceso: tarjetas inteligentes (utilizan técnicas criptográficas), sistemas biométricos…

**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)

1. Seguridad en la red corporativa

No es suficiente con garantizar la seguridad en un equipo, debe extenderse a proteger la red corporativa

Las amenazas más frecuentes sobre la red son:

* Interrupción: ataques de denegación de servicio que produce una falta de disponibilidad
* Interceptación: un atacante consigue hacer una copia de la información a la que no debería tener acceso
* Modificación: una vez interceptado, el mensaje puede ser modificado y reenviado, provocando un fallo en la integridad.
* Generación, creación o fabricación: el atacante fabrica un mensaje recibido por el receptor, pero suplantando la identidad, provocando un fallo en la autenticidad

**Vulnerabilidades en la arquitectura TCP/IP**

* Capa de subred (1 y 2 de OSI): acceso físico a los equipos o el cableado. Se pueden generar problemas de suplantación o sniffers. Para asegurar la capa de red:
  + Confidencialidad: datos disponibles solo para usuarios autorizados
  + Autenticidad: verificar la identidad digital de los agentes
  + Integridad: evitar alteraciones en la información
* Capa de Internet (3 de OSI): escuchas no autorizadas a paquetes IP, suplantación de IP o envenenamiento de las tablas de ARP.
* Capa de transporte (4 de OSI): interceptación de puertos TCP y UDP, importante disponer de un firewall que gestione que puertos están abiertos
* Capa de aplicación (5, 6 y 7 de OSI): problemas relacionados con los servicios de la red y autenticación de datos
  + Deficiencias en los servicios de nombres de dominio
  + Envenenamiento de las cachés del DNS
  + Suplantación del servidor DNS
  + Inseguridad de protocolos no cifrados (telnet, ftp)
  + Vulnerabilidades con el protocolo http

**Ataque de ingeniería social, web y whois**

La ingeniería social consiste en persuadir a un usuario para que revele información confidencial que pueda comprometer los sistemas. También se puede obtener información a través de una sede web o el servicio “whois” para conocer el propietario de un dominio

**Ataque de denegación de servicio**

El objetivo principal de DoS es impedir el uso de un servicio, esto se logra colapsando el servidor a través de un gran número de peticiones.

Cuando el ataque está formado por una red de atacantes (botnet) coordinados se conoce como denegación distribuida del servicio (DDoS).

Para evitar un ataque DoS basta con bloquear una IP, pero es más difícil bloquear un ataque DDoS puesto que utilizan diferentes IPs

**Cracking de contraseñas, mail bombing, spamming**

El objetivo principal del atacante es descubrir la cuenta del administrador. Deshabilitando o cambiando el nombre de esta cuenta se logra que sea más difícil identificar la cuenta. Dos métodos para crackear contraseñas:

* Diccionario: utilizar palabras del diccionario hasta encontrar la contraseña
* Ataques por fuerza bruta: probar todas las combinaciones posibles de caracteres.

El mail bombing consiste en enviar muchas veces el mismo mensaje, provocando un ataque DoS. El más perjudicado es el cliente.

El mail spamming consiste en enviar el mismo correo (no deseado) a muchos equipos diferentes. El más perjudicado es el servidor.

**Escaneo de puertos y sniffers**

El escaneo de puertos permite a los atacantes conocer que puertos están abiertos para buscar vulnerabilidades en estos. Almacenan la información en ficheros log. Algunos firewalls son capaces de detectar el escaneo.

A través de los sniffers se puede obtener información sin cifrar y conocer la estructura lógica de la red.

Para que un sniffer funcione la información debe pasar por el equipo que está siendo atacado, por eso los hub son una mala elección ya que reenvían la información a todas sus conexiones, es preferible utilizar switches.

**Riesgos potenciales en los servicios de red**

* El firewall solo debe abrir sus puertos a aquellos servicios que utilice
* Utilizar solo los servicios necesarios
* Instalar solo los servicios que se vayan a utilizar
* Intentar utilizar siempre protocolos cifrados
* Intentar utilizar protocolos que admitan autenticación

**Seguridad en redes inalámbricas**

La seguridad en medios no guiados es más compleja ya que los mensajes llegan a todos los dispositivos que alcance la red, por lo que se eleva ampliamente el riesgo de escucha no autorizada. Se han desarrollado varios protocolos

* Protocolo WEP (Wired Equivalent Privacy): primer protocolo creado, utiliza contraseñas para autenticar a los clientes la cual solo debe ser conocida por los usuarios autorizados. Cifrado AES
* Protocolo IEEE 802.IIi y 802.IIn: la red decide si el cliente se puede conectar a la propia red
* WPA y WPA2: más seguro que WEP, menos que 802. Se cifra con RC4

**Seguridad perimetral**

Un sistema de detección de intrusos (IDS) detecta manipulaciones no deseadas en los equipos o ataques no detectados por los cortafuegos en base a la monitorización de eventos. Existen tres tipos de IDS:

* HIDS (Host IDS): vigila un único sistema
* NIDS (Network IDS): basado en la red, detectando ataques
* DIDS (Distributed IDS): basado en cliente-servidor, utiliza múltiples NIDS

**DMZ o red perimetral**

Una zona desmilitarizada es una red aislada dentro de una red interna de la organización, en esta se encuentran principalmente los servidores. Siempre se deberá conectar a través de Internet, una red local nunca podrá conectar directamente con una DMZ

**Seguridad de la red interna**

La mayoría de los ataques que sufre una organización viene de su interior (fugas de información, confidencialidad, etc…). Puntos a destacar en la seguridad de una red interna:

* Antimalware y firewall. Buscar un equilibrio entre lo permitido, pero sin ser una defensa excesiva
* Realizar una defensa en profundidad con todas las capas
* Realizar auditorías constantes sobre cada capa
* Subdividir la red mediante switches y router y VLANs
* Cuidar la política de contraseñas
* Deshabilitar o renombrar cuentas por defecto
* Implementar la seguridad perimetral
* Actualizar y administrar los sistemas correctamente
* Disponer de un sistema de detección de intrusos

**Seguridad de la red perimetral**

* Está en contacto con el exterior por lo que sufre una gran cantidad de ataques
* Sus principales vulnerabilidades son los puertos TCP y UDP
* La seguridad perimetral no sirve si no se cuida la seguridad de la red interna
* Los ataques con éxito a la red perimetral desprestigian a la empresa

**Tecnologías para la seguridad perimetral**

El administrador debe conocer la arquitectura de seguridad. Además de las políticas, son necesarios dispositivos físicos que proporcionen seguridad. Los elementos HW o SW que proporcionan seguridad son: Routers, Firewalls, IDS, VPN, Software y servicios, DMZ y subredes.