El ataque informatico

Las fases suelen ser:

- Descubrimiento de los sistemas que componen el objetivo (por ejemplo, la red en la que se haya).
- Exploración de las vulnerabilidades de los sistemas
- Explotación de las vulnerabilidades detectadas, mediante herramientas específicamente construidas para tal fin, que se denominan exploits
- Compromiso del sistema
- Ocultamiento o eliminación de los rastros que prueban el ataque

Vulnerabilidades del sistema

Vulnerabilidad: probabilidad de que una amenaza se materialice en un daño

¿Qué hace que un sistema operativo o aplicación sea vulnerable?

- Errores de instalación o configuración
- Errores de programación (bugs)
- Retraso en la publicación de parches
- Descarga de programas desde fuentes poco fiables

Es muy importante actualizar los sistemas (S.O. y aplicaciones) tan pronto como sea posible, para estar el mínimo tiempo posible expuestos a un ataque.

Las actualizaciones de software vienen justificadas por diferentes motivos:

- Reparar las vulnerabilidades detectadas
- Proporcionar nuevas funcionalidades o mejoras respecto a las versiones anteriores

El proceso de actualización consiste en descargar de la página web del fabricante del programa los ficheros necesarios

Es posible realizar actualizaciones manuales y automáticas (el propio sistema las busca, descarga e instala sin intervención humana).

Actualización automática del sistema operativo:

- Sistemas Microsoft
  - Publica actualizaciones (service packs, actualizaciones de versión, actualizaciones de drivers,…) los segundos martes de cada mes
  - Windows update: servicio de actualizaciones automáticas de Windows
  - En versiones antiguas podíamos elegir entre:
    - No buscar actualizaciones ni instalarlas (no recomendable)
    - Comprobar si hay actualizaciones, pero no descargarlas ni instalarlas. Esto solo tienen sentido en equipos con poco disco o acceso limitado a internet

        - Descargar actualizaciones, pero no instalarlas. En algunos sistemas podemos tener una configuración muy sensible a cambios en el sistema operativo
        - Descargar e instalar siempre. Es lo mas habitual en los puestos de usuario.
    - En Windows 10 se descargan y actualizan siempre, aunque en las ultimas versiones se permiten detener la actualización 7 días.

Actualización automática del sistema operativo:

Sistemas Linux en UBUNTU:

- Es posible configurar la actualización automática desde el menú de configuración del sistema
- Otra opción es programar en cron (tareas programadas) una línea de comandos que actualice la lista de repositorios y luego ejecute la actualización de aplicaciones que tengan disponible nueva versión.

Seguridad activa: Definición

> La **seguridad activa** es el conjunto de medidas que previenen o intentan evitar los daños en un sistema informático, minimizando los riesgos. Se trata de estudiar qué mecanismos de protección podemos utilizar en nuestro equipo para evitar accesos indeseados de intrusos (personas o programas).

Objetivos:

- Restringir el acceso al arranque, al sistema operativo, programas y archivos.
- Asegurar que los usuarios puedan trabajar sin una supervisión minuciosa y que no puedan modificar los programas y los archivos que no correspondan
- Asegurar que se estén utilizando los datos, archivos y programas correctos, por le procedimiento correcto y actualizando periódicamente los mismos.

La defensa en profundidad

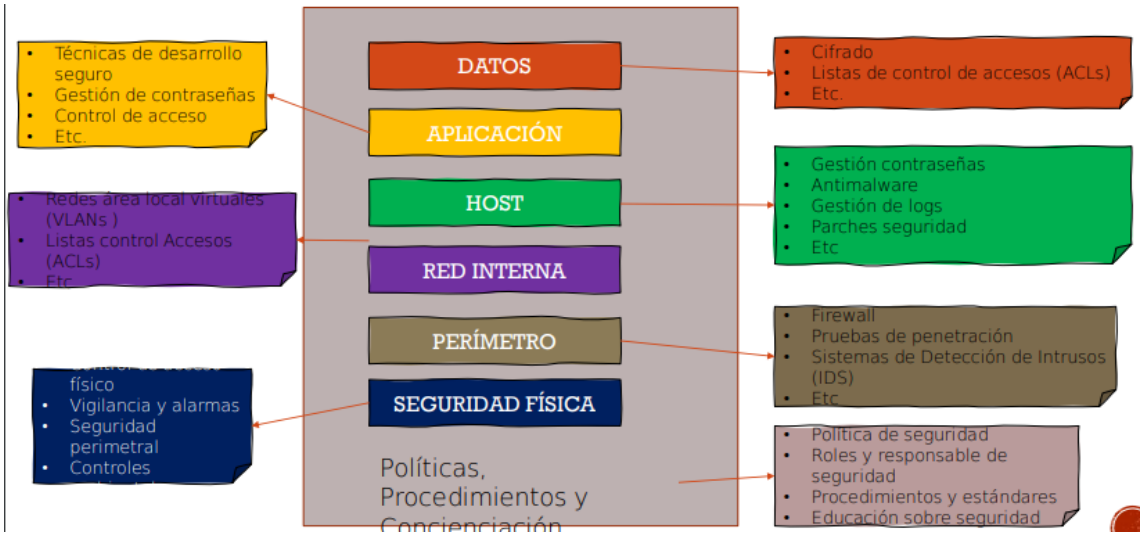
La seguridad de los sistemas debe organizarse según las propuestas de una defensa en profundidad, es decir, proveyendo múltiples barreras con seguridad integrada en cada una de ellas.

La definición formal que proporciona el centro criptológico nacional español es que:

> "La **defensa en profundidad** es una estrategia consistente en introducir múltiples capas de seguridad que permitan reducir la probabilidad de compromiso en caso de que una de las capas falle y en el peor de los casos minimizar el impacto." (Guía STIC 400 2006)

Esta organización en niveles permite dividir el problema global de la seguridad en otros mas pequeños y manejables con soluciones especializadas, contribuyendo en de este modo a mejorar la calidad del plan de seguridad

Niveles de una defensa en profundidad



Medidas de defensa

A modo de ejemplo, se enumeran algunas características más importantes de las medidas de defensa que se utilizan en los sistemas asegurados con defensa en profundidad.

Defensa en políticas, procedimientos y concienciación

Establecen el tono de seguridad en toda la organización en relación a la protección de activos informáticos, definen los objetivos y actividades de control y proveen un criterio para la realización de auditorias

Para mejorar su efectividad, las políticas deben ser comunicadas a todo el personal de la empresa, ya que la concienciación es un elemento clave

Debe exigirse a todo el personal un compromiso serio con la seguridad

Algunas técnicas de concienciación pueden ser: carteles, salvapantallas de advertencia, alertas generadas por ordenador, mensajes de correo electrónico a toda la empresa, conferencias o sesiones dirigidas por un instructor en persona

Defensa en cortafuegos

Es la primera línea de defensa de la red, que se analiza las conexiones entre las redes interna y externa de una organización y restringe el acceso de acuerdo a una política de seguridad

Actualmente, al cortafuegos se le han añadido otras funciones de seguridad

Es muy importante que este correctamente configurado y actualizado

Defensa en sistemas de detección de intrusos

Intrusión detection system (IDS) es un sistema que monitoriza el trafico de la red y alerta de cualquier actividad sospechosa en tiempo real

Son sistemas que generar una gran cantidad de falsos positivos, es decir, detectan algunas actividades legitimas como si fueran maliciosas, lo que supone vigilar constantemente para minimizarlos

Algunos IDS también pueden implantar procesos específicos de intervención para atajar algunos problemas de seguridad detectados

Defensa en el control de acceso a la red

Network access control (NAC)

Es un concepto de ordenador en red y conjunto de protocolos usados para definir como asegurar los nodos de la red antes de que estos accedan a la red

Por ejemplo, podría establecerse que cualquier ordenador que se conecte a la red tenga un antivirus actualizado y el cortafuegos personal activado. Si no cumpliese con estos requisitos se le puede denegar el acceso

Defensa contra malware

Las tecnologías antimalware (que protegen de amenazas como virus, troyanos y malware) continúan avanzando para ofrecerse a los usuarios como suites de seguridad

Algunas defensas contra el malware son:

- Actualizar el antivirus
- Sistema operativo actualizado
- Utilizar un firewall
- Realizar análisis regulares en el equipo
- Practica una navegación segura por la web
    - Elegir contraseñas seguras
    - No acceder a sitios sospechosos
    - Cuidado con el phishing y spam
    - Utilizar bloqueador de ventanas emergentes
    - Cuidado con los ficheros que se descargan

Las tecnologías antimalware (que protegen de amenazas como virus, troyanos y malware) continúan avanzando para ofrecerse a los usuarios como suites de seguridad

Algunas defensas contra el malware son:

- Actualizar el antivirus
- Sistema operativo actualizado
- Utilizar un firewall
- Realizar análisis regulares en el equipo
- Practica una navegación segura por la web
    - Elegir contraseñas seguras
    - No acceder a sitios sospechosos
    - Cuidado con el phishing y spam
    - Utilizar un bloqueador de ventanas emergentes
    - Cuidado con los ficheros que se descargan

Defensa mediante cifrado

El cifrado de datos protege de muchos ataques, especialmente los de confidencialidad, integridad y autenticidad

la seguridad del cifrado depende de la custodia de la clave o contraseña, por lo que habrá que protegerla con mucho cuidado

defensa de los equipamientos físicos

aunque se tenga un buen sistema de defensa lógica, de nada servirá si no se cuida la seguridad física

por tanto, es imprescindible disponer de cámaras, alarmas, vigilancia, etc. Especialmente en lugares críticos como el centro de proceso de datos

Defensa en profundidad

Hay dos analogías comunes que se utilizan para describir un enfoque de defensa en profundidad

Cebolla de seguridad

- Una analogía común utilizada para describir un enfoque de defensa en profundidad se llama "la cebolla de seguridad".
- Como se ilustra en la figura, un actor de amenazas tendría que despegar las defensas de una red capa por capa de una manera similar a pelar una cebolla. Solo después de penetrar cada capa, el actor de amenazas alcanzaría los datos o el sistema de

Nota: La cebolla de seguridad descrita es una forma de visualizar la defensa en profundidad. Esto no debe confundirse con el conjunto de herramientas de seguridad de red Security Onion.

Alcachofa de seguridad

- El panorama cambiante de las redes, como la evolución de las redes sin fronteras, ha cambiado esta analogía a la "alcachofa de seguridad", que beneficia al actor de amenazas.
- Como se ilustra en la figura, los actores de amenazas ya no tienen que quitar cada capa. Solo necesitan quitar ciertas "hojas de alcachofa". La ventaja es que cada "hoja" de la red puede revelar datos confidenciales que no están bien protegidos.
- Por ejemplo, es más fácil para un actor de amenazas comprometer un dispositivo móvil que comprometer una computadora o servidor interno que está protegido por capas de defensa. Cada dispositivo móvil es una hoja. Y hoja tras hoja, todo lleva al hacker a obtener más datos. El corazón de la alcachofa es donde se encuentran los datos más confidenciales. Cada hoja proporciona una capa de protección al mismo tiempo que proporciona un camino para atacar.
- No es necesario quitar todas las hojas para llegar al corazón de la alcachofa. El hacker socava la armadura de seguridad a lo largo del perímetro para llegar al "corazón" de la empresa.
- Si bien los sistemas orientados a Internet suelen estar muy bien protegidos y las protecciones de límites suelen ser sólidas, los piratas informáticos persistentes, ayudados por una combinación de habilidad y suerte, eventualmente encuentran una brecha en

Identificación y autenticación

es la primera línea de defensa de sistemas computerizados, previniendo el ingreso de persona no autorizadas

- Identificación: momento en que el usuario se da a conocer en el sistema
- Autenticación: verificación que realiza el sistema sobre la identificación. "autenticar: dar seguridad de que alguien o algo es lo representa o parece". Según la RAE

- Técnicas de autenticación
    - Algo que solamente el individuo conoce: PIN, clave secreta, nº identificación
    - Algo que la persona posee: tarjeta magnética
    - Algo que el individuo es y que lo identifica unívocamente: huellas digitales, voz, … (medidas biometricas).
- Estas técnicas se pueden / deben combinar

Identificación y autenticación: USUARIO / PASSWORD

Es el mecanismo más utilizado que utiliza la estrategia algo que sabes

Una pantalla inicial del sistema espera que la persona introduzca un usuario y la contraseña asociada

Se impide la entrada al sistema o aplicación hasta que el par usuario/contraseña sea verificado

Ante una equivocación algunos sistemas ofrecen pistas sobre la contraseña

Casi todos los sistemas tienen un número máximo de intentos, tras los cuales se bloquea

No debemos escribir la contraseña en ningún sitio

No debemos enviar una contraseña por correo electrónico ni comunicarla por teléfono

Debemos limitar el número de intentos fallidos.

Se deben cambiar las contraseñas de acceso por defecto suministradas por fabricantes

No debemos utilizar la misma contraseña en distintas maquinas o sistemas

Las contraseñas deben caducar, para ser cambiadas cada cierto tiempo

No debemos permitir que las aplicaciones recuerden las contraseñas

Políticas de contraseñas: en los equipos informáticos la autenticación se realiza mediante un identificador de usuario y una contraseña. Por lo tanto, cuanto mejor sea la contraseña elegida, mejor será la seguridad del sistema. Las empresas definen políticas de seguridad estableciendo las características exigidas a esas contraseñas

No deben estar formadas por palabras de algún idioma

No deben usarse solo letras mayúsculas o minúsculas

No deben estar formadas exclusivamente por números

No se debe utilizar información personal: nombre, fechas de nacimiento, números de teléfono, etc.

No se deben invertir palabras conocidas

No se deben repetir los mismos caracteres en la misma contraseña

Conviene combinar letras, números características especiales, mayúsculas y minúsculas

Las contraseñas deben ser cadenas de caracteres (de más de ocho caracteres) que incluyan letras mayúsculas, minúsculas, números y caracteres especiales, sin ningún tipo de lógica.

Identificación y autenticación: tarjetas

Es el mecanismo que utiliza algo que tienes. Requiere de un elemento físico previamente repartido a los usuarios autorizados

Inicialmente se distinguía entre tarjetas sencillas (magnéticas o rfid) o complejas (chip)

Tarjas sencillas:

- Magnéticas: tienden a desaparecer ya que pueden sufrir borrados accidentales
- RFID: utilizan radiofrecuencia para conectar a un cliente y un servidor que contiene la base de datos de usuarios, son más seguras que las magnéticas y resultan igual de baratas

Tarjetas con chip

- De almacenamiento: contienen las claves para que las lea el dispositivo donde introducimos la tarjeta
- De procesamiento: contienen las claves, pero nunca salen de la tarjeta. El chip se limita a cifrar con ellas algún desafío que lanza el dispositivo por donde introducimos la tarjeta

Identificación y autenticación: biometría

Aplica la estrategia <<algo que eres>>, para complementar el mecanismo usuario/contraseña o de tarjeta con un control más: la biométrica

La biométrica consiste en identificar alguna característica física del sujeto: la huella dactilar, el ojo, la voz

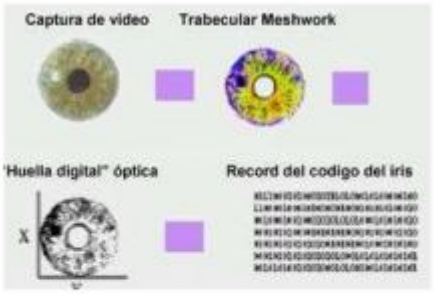
Se recogen una serie de medidas de características especificas que permiten la identificación de personas utilizando dispositivos electrónicos que las almacena. Esta identificación consiste en comparar esas características físicas especificas de cada persona con un patrón conocido y almacenado en una base de datos.

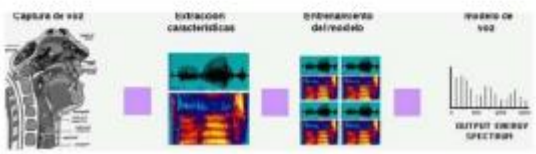
Una de las ventajas de la utilización de la tecnología biométrica es que pueden eliminar la necesidad de utilizar tarjetas de acceso, con todo lo que conlleva de gasto en su creación y sobre todo en su control y administración

Además, los dispositivos biométricos son mas sencillos de mantener ya que solo requieren el mantenimiento propio del dispositivo y el mantenimiento de la base de datos

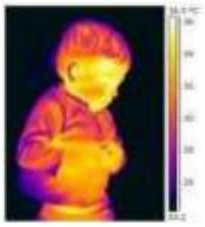
Algunos sistemas biométricos

- Emisión de calor: mide la emisión de calor del cuerpo (termograma) y realiza un mapa de valores sobre la forma de cada persona
- Huella digital: cada huella digital tiene un conjunto de pequeños arcos, ángulos, bucles, remolinos, Etc. (minucias) característicos y la posición relativa de cada una de ellas es lo que se analiza para establecer la identificación de una persona. Esta aceptado que dos personas no tienen mas de ocho minucias iguales y cada una posee mas de 30, lo que hace al metido muy seguro
- Verificación de voz: consiste en grabar la lectura de una o varias frases por parte de los diferentes usuarios y en el momento de intentar accede se comparará la voz con sus diferentes cualidades como entonación, timbre, etc… este sistema es muy sensible a factores externos como el ruido, el estado de animo y enfermedades del tipo afonías u otras que alteren la voz, el envejecimiento, etc.
- Verificación de patrones oculares: sistemas basados en patrones del iris o de la retina y hasta el momento son considerados los más efectivos ya que en 200 millones de personas la probabilidad es casi 0.





nágenes obtenidas de http://dis.um.es



TÉCNICA	VENTAJAS	DESVENTAJAS
Reconocimiento de cara	Fácil, rápido y barato	La iluminación puede alterar la autenticación
Lectura de huella digital	Barato y muy seguro	Posibilidad de burla por medio de réplicas, cortes o lastimaduras que pueden alterar la autenticación
Lectura de iris/retina	Muy seguro	Intrusivo (molesto para el usuario)
Lectura de la palma de la mano	Poca necesidad de memoria de almacenamiento de los patrones	Lento y no muy seguro
Reconocimiento de la firma	Barato	Puede ser alterado por el estado emocional de la persona
Reconocimiento de la voz	Barato; útil para accesos remotos	Lento; puede ser alterado por el estado emocional de la persona; fácilmente reproducible

Principio de mínimo privilegio: se basa en realizar las tareas necesarias con los minimos privilegios; así cualquier fallo, accidente o vulnerabilidad tiene un impacto mínimo:

- El administrador del sistema tendrá dos cuentas: una con privilegios de administrador (para gestión del sistema e instalación de software) y otra con permisos reducidos (para su uso cotidiano)
- Todo usuario adicional se añadirá como cuenta limitada

Identificación y autenticación: elevación de privilegios

La cuenta limitada:

- No puede acceder a la carpeta Mis documentos de otros usuarios
- No se puede escribir sobre la carpeta del sistema operativo Windows
- No puede instalar un driver
- No puede modificar el registro de Windows

¿Cuando instala programas? Adquiriendo puntualmente privilegios de administrador:

- Cambio rápido de usuario
- “ejecutar como”
- Ejecutar desde la consola del sistema: RunAs.exe

Una vez que estamos autenticados en el sistema operativo y podemos trabajar con el, estaremos limitados a los privilegios asociados al usuario con el que nos hemos presentado

En las empresas, la mayoría de los empleados utilizan usuarios (usuarios limitados) que no tienen permiso para realizar tareas de administración de la maquina: asi se reduce el daño que puedan causar.

Pero en las situaciones en las que un usuario necesite de forma puntual realizar tareas administrativas, solicitara una elevación de privilegios. Consiste en pedirle al sistema ejecutar un determinado programa con permisos de administrador. Se aplica solo a ese programa y solo a esa ejecución

En los sistemas Windows, hasta XP inclusive: una vez entrabamos como administrador, no había ningún control más. Como consecuencia, cualquier virus podía dominar la maquina

Como solución en la versión Vista se añadió UAC (User Access Control) para que el sistema avisara al usuario cuando un programa solicita ejecutar una operación de administración

Introducción

BIOS (Basic Input Output System): es un firmware que se ejecuta al encender el ordenador, y que localiza y reconoce todos los dispositivos necesarios para cargar el sistema operativo en la memoria RAM; es un software muy básico instalado en la placa base que permite que esta cumpla su cometido

La protección con contraseñas para la BOS (o equivalentes al BIOS) y el gestor de arranque, pueden ayudar a prevenir que usuarios no autorizados que tengan acceso físico a nuestros sistemas, arranquen desde medios removibles u obtengan acceso como root a través del modo monousuario

La interación o manipulación de la BIOS puede originar muchos problemas:

- Ataques de denegación de servicio. Por ejemplo, el equipo no arranca del disco adecuado y se impide el acceso al sistema contenido en el
- Ataques de suplantación. Por ejemplo, se puede arrancar de un disco alternativo que simula ser el original pero que contiene software que compromete la privacidad del usuario que piensa que está en su sistema habitual

* Un Live CD o Live DVD, más genéricamente Live Distro, siendo en ocasiones llamado CD vivo o CD autónomo, **es un sistema operativo almacenado en un medio extraíble, tradicionalmente un CD o un DVD (de ahí sus nombres), que puede ejecutarse directamente en una computadora**.