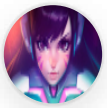


Belen_Dominguez
www.wuolah.com/student/Belen_Dominguez

Apuntes-TAI-Tema-1.pdf

? Apuntes TAI ?

3° Tecnologías Avanzadas de la Información

Grado en Ingeniería Informática - Tecnologías Informáticas

Escuela Técnica Superior de Ingeniería Informática
Universidad de Sevilla

APUNTES TAI

TEMA 1 - INTRODUCCIÓN A LA SEGURIDAD EN REDES DE COMPUTADORES

PARTE 1 - SEGURIDAD INFORMÁTICA

Seguridad informática: Conjunto de sistemas, métodos, herramientas, procedimientos y actuaciones encaminados a conseguir la protección de la información y la garantía de funcionamiento de los sistemas informáticos, alertando la detección de actividad ajena.

Definiciones básicas:

- Vulnerabilidad: Debilidad.
- Amenaza: La posibilidad de que una vulnerabilidad sea aprovechada.
- Ataque: Llevar a cabo una amenaza.
- Riesgo: Posibilidad de que ocurra un ataque.

Principios de la seguridad informática:

- ❏ Acceso más fácil: siempre se intentará atacar por el eslabón más débil del sistema (este definirá el nivel de seguridad de nuestro equipo).
- ❏ Caducidad de la información: tiempo durante el que se deba tener protegido una información (no tendrá sentido seguir protegiendo algo si ya se descubrió).
- ❏ Eficiencia: las medidas de control deben funcionar cuando se les necesite sin provocar molestia al usuario (deben ser transparentes) y siempre optimizando los recursos del equipo.

Objetivos de la seguridad informática:

Se buscará proteger activos (información, equipos o usuarios). Debemos evitar el robo de documentos, la manipulación, la entrada de bugs, fallos que dañen los equipos, olvido de contraseñas, etc.

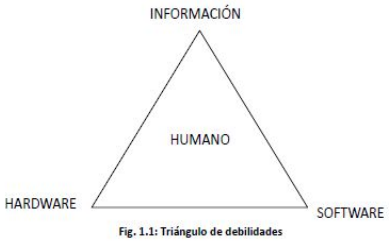


Fig. 1.1: Triángulo de debilidades

- Autenticidad: verificar la identidad de los usuarios.
- Confidencialidad: poder encubrir la información a usuarios no autorizados.
- Integridad: modificación de la información solo a usuarios autorizados.
- Disponibilidad: Información siempre disponible para las partes autorizadas.

Clasificación de ataques:

- ❏ Según el origen: distinguimos entre **externos** (exterior a la organización) e **interior** (dentro de la organización, no siempre puede ser intencionados y son los más probables).
- ❏ Según la complejidad: distinguimos entre **No estructurados** (no se han preparado, suelen ser fácilmente reconocibles) y **Estructurados** (dirigidos a un objetivo muy concreto, estudiando detalles y debilidades de este).

- Según el objetivo: distinguimos entre **Interrupción** (hacer inaccesible un elemento, ya sea de software o hardware), **Interceptación** (conseguir permisos para leer y supervisar una información, de los más difíciles de interceptar), **Modificación** (igual que la interceptación pero consiguiendo además modificar la información) y **Invención o Generación** (insertar objetos falsos en un sistema, delito de falsificación y suplantación de identidad).

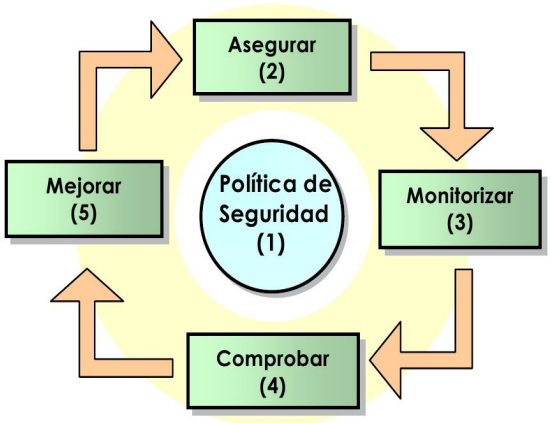
Gestión de la seguridad:

Conjunto de requisitos que indican que está y que no está permitido. Esta puede ser **prohibitiva** (todo lo no permitido expresamente se deniega) o **permisiva** (todo lo no permitido expresamente se permite).

La normativa estándar **ISO-27001** define las líneas de actuación de Seguridad de la organización, Seguridad del personal (formación, confidencialidad, etc), Controles de acceso (contraseñas, monitorización de accesos, etc), Requisitos legales (cumplir la normativa del país), etc.

La representación de una metodología que verifique que hemos implementado las medidas y que funciona es la rueda de la seguridad.

Rueda de la seguridad:



- Política de seguridad: definir una política.
- Asegurar: detener y evitar el acceso de los intrusos y las actividades no autorizadas.
- Monitorizar: detección de violaciones en tiempo real (IDS (Intrusión Detection System), Monitor de logs y Honeypots o señuelos).
- Comprobar: asegurar la funcionalidad de lo anterior.
- Mejorar: desarrollar mejoras con la información de las fases anteriores.

MAGERIT:

Metodología estándar española para analizar los riesgos. Ecuación básica del Análisis de riesgo: RIESGO vs CONTROL vs COSTE:

$$B < P \times L$$

B: Coste de implantación
L: Coste en pérdidas tras un ataque
P: Probabilidad de ocurrencia

Si B ≤ P * L: El coste que supone perder el activo es mayor que el coste que supone implantar una medida de prevención. Hay que implementar una medida de prevención o mejorar la existente.

Si B > P * L: No es necesaria una medida de prevención ya que el coste de implantarla es mayor que el coste que supone perder el activo que se quiere proteger.

PARTE 2 - PELIGROS Y MODOS DE ATAQUE

Es improbable que se conozcan todos los tipos de ataques posibles, pero una posible clasificación según el objetivo sería:

- Ataques a la confidencialidad: Se pretende obtener información privilegiada (ya sea según métodos informáticos como de ingeniería social). Varias técnicas observadas son:
    - **Escaneo de puertos**: (recorrer tantos puertos de escucha como sea posible, y guardar información de aquellos que sean receptivos o de utilidad para cada necesidad en particular). Contramedidas usadas son filtrado de puertos, análisis de logs y alarmas.
    - **Sniffing**: escuchar el tráfico de una red de manera pasiva, sin intervenir. Para prevenirlo se usará el cifrado de conexiones.
    - **Snooping downloading**: Obtener documentos, mensajes, correos, etc. Para análisis posterior, por curiosidad espionaje o robo.
- Ataques a la autenticidad: Ingresar al sistema de la víctima como usuario privilegiado.
    - **Spoofing**: actuar en nombre de otros usuarios para realizar otro tipo de acciones maliciosas. Algunos ejemplos son el IP Spoofing (usurpar una IP dentro de la red local), DNS Spoofing (alterar los DNS mediante la manipulación de paquetes UDP), Phishing (envío de e-mails falsos a nombre de otra persona), Web Spoofing (página similar pero falsa a la que la víctima quiere entrar), etc.
    - **HIJACKING**: robar una conexión/sesión después de que la víctima haya superado el proceso de identificación.
    - **BACKDOORS**: trozos de código que permiten saltarse procedimientos si el atacante los conoce.
    - **Fuerza bruta**: probar todas las posibles combinaciones hasta descifrar una clave.
    - **SIM swap**: Duplicado de tarjeta SIM para usarlo en la autenticación en 2 pasos.
- Ataques a la disponibilidad (DoS): Saturar el sistema de la víctima para inhabilitar durante un tiempo los servicios de este. Se dividen entre los que atacan el servicio de aplicación y el servicio de red. De este último vemos:
    - **Flooding / Jamming**: saturar los recursos del sistema (ping de la muerte, emails masivos, etc). Varias modalidades son SYN flooding (dejar un número elevado de conexiones TCP en espera) y UDP (saturación de paquetes UDP).
    - **Fragmentación de paquetes**: aprovechar las vulnerabilidades de la pila TCP/IP al llegarle un paquete fragmentado y pasar desapercibido pero al juntarse conseguir el objetivo.
    - **Smurfing**: inundar de paquetes ICMP el equipo de la víctima.
    - **E-Mail bombing - Spamming**

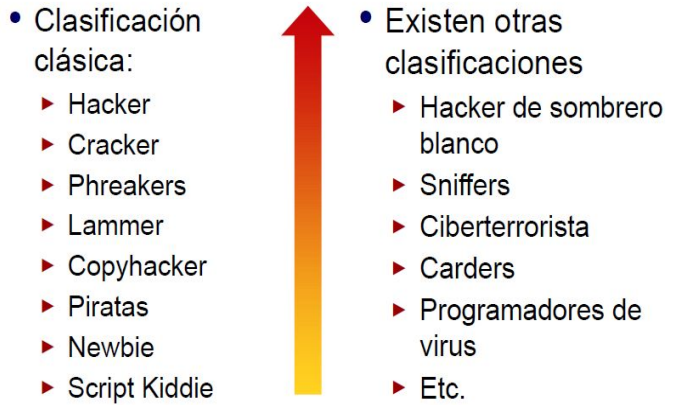
MACARENA
Calle Don Fadrique 19
954 38 51 02 - 636 64 90 58
macarena@couckesacademy.es

- **Denegación de Servicio Distribuida (DDoS)**: capturar sistemas vulnerables, instalarles software malicioso para que operen como "zombies" (llamados también botnets) y a través de estos atacar a la víctima.

- Ataques a la integridad: Modificar o destruir información o aplicaciones.
  - **Borrado de huellas**: no dejar rastro de las tareas que se realiza.
  - **Ataques a aplicaciones**: aprovecharse de las debilidades de una aplicación. Los más comunes son fallos debidos a una mala configuración, bugs, buffer overflow (aprovechar la falta de controles existente en ciertos programas a la hora de pasarles argumentos) y exploits.
  - **Exploits**: programas con el objetivos de atacar las debilidades de un sistema/ aplicación mediante el desbordamiento de almacenamiento o de la pila.
  - **Ransomware**: secuestro de sistemas y/o datos.
  - **Malware**: Programas que se introducen en nuestro sistema para producir daños (troyanos, gusanos, etc).

PARTE 3 - ATACANTES Y DEFENSAS

Desde la persona Hacker (amplios conocimiento y siempre con ganas de saber más), pasando por Cracker (amplios conocimientos pero con el objetivo de violar la seguridad de los equipos), los típicos Piratas hasta los Newbie (aprendiz de hacker) y los Script Kiddie (aficionados de internet con cero conocimiento).



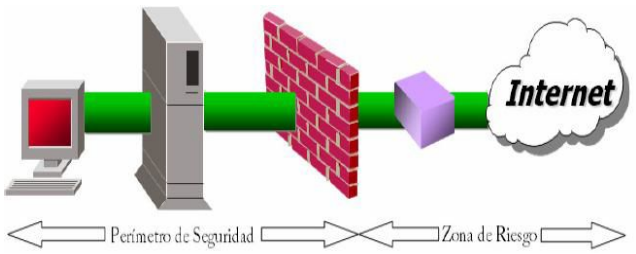
Varios métodos contra ataques son el límite del tráfico mediante el filtrado de paquetes (firewalls) o los servidores proxy. Si no se decide limitar el tráfico deberemos reforzar los métodos de autenticación y evitar los inicios de sesión de partes no autorizadas. Si creemos que vamos a ser víctimas de hijacking o sniffing necesitaremos encriptar la conexión. Tenemos 3 frentes de defensa:

- **Protección perimetral**: Firewalls, VPN's, Sistemas de detección de intrusiones (IDS, IPS, Honeypots,...), etc.
- **Autenticación**: Es el proceso seguido por una entidad para probar su identidad ante otra.
- **Criptografía**: Proteger la información a base de codificarla.

Nos centramos en la seguridad perimetral.

PARTE 4 - SEGURIDAD PERIMETRAL

Conjunto de elementos y sistemas encargados de proteger perímetros físicos o lógicos, controlar el tráfico y monitorizarlo, detectar y bloquear posibles ataques de intrusión, implementar políticas de seguridad, etc. El perímetro protegido se denomina perímetro de seguridad.



Los elementos de una seguridad perimetral son: Router, Firewalls, Sistemas de detección de intrusiones (IDS), Redes privadas virtuales (VPNs), Software y servicios y Zonas desmilitarizadas

Firewall: Sistema capaz de separar una máquina o subred del resto de la red mediante **reglas de filtrado** para la autorización únicamente de paquetes deseados. No puede proteger contra ataques internos, ataques de ingeniería social, virus o fallos en protocolos. Un método para implementar un firewall es el **filtrado de paquetes** estático (no hay relación entre paquetes y se aceptan o rechazan según su cabecera) o dinámico (se considera el estado de los paquetes previos para añadir o eliminar reglas). Tienen un alto rendimiento pero son muy vulnerables.

A parte del filtrado de paquetes también puede usarse el método **Proxy** (programa que realiza una acción en nombre de otro para filtrar, reenviar bloquear, etc). Este puede controlar el inicio y cierre de sesiones, ocultar información, hacer de caché, reducir la complejidad de las reglas de filtrado… Sin embargo, reducen el rendimiento y no siempre es posible usarlo. Se distinguen 4 tipos de Proxy: dedicado (efecto directo en la forma de comunicación), genérico (determina sólo si una conexión es permitida), HTTP directo (Gateway para el navegador cliente) y HTTP inverso (actúa en el back-end de servidores clientes).

Buenas prácticas:

Será importante planificar la seguridad de la red, siendo la monitorización (capacidad de acceder al tráfico que entra y sale) y el control (decidir qué tráfico entra) los ejes de esta.

Otra buena práctica será la separación de servicios según los roles (servidores, clientes, web, etc)