Requisitos básicos que rige la seguridad

Confidencialidad

La información de un sistema informático sólo debe ser accesible para lectura para aquellas partes que estén autorizadas. `impresión, mostrado de datos`

Integridad

Los contenidos de un sistema informático solo pueden ser modificados por quien esté autorizado. `escritura, cambio, modif. estado, borrado y creacion`

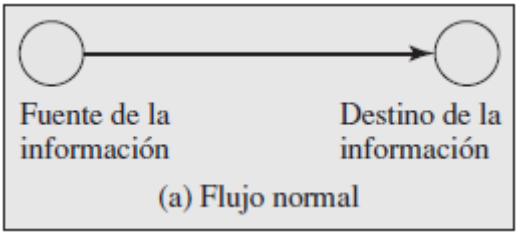
Disponibilidad

Los componentes de un sistema informático deben estar disponibles para las partes autorizadas.

Autenticación

El sistema informático debe ser capaz de verificar la identidad de los usuarios.

Tipos de peligros



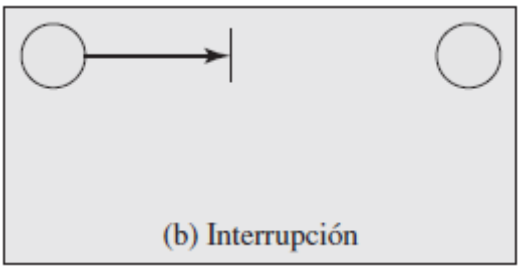
(a) Flujo normal

Interrupción

Se destruye un componente del sistema o se encuentra no disponible o utilizable.

Es un ataque centrado en la **disponibilidad**.

> Destrucción de una pieza de hardware, interrupción de un canal de comunicación o la eliminación del sistema gestor de ficheros

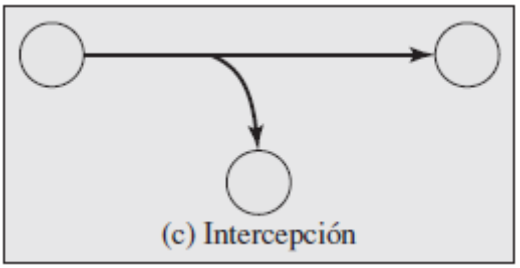

(b) Interrupción

Intercepción

Una parte no autorizada consigue acceso a un componente.

Es un ataque dirigido hacia la **confidencialidad**.

> Escucha en un canal de comunicación o la copia ilícita de ficheros o programas

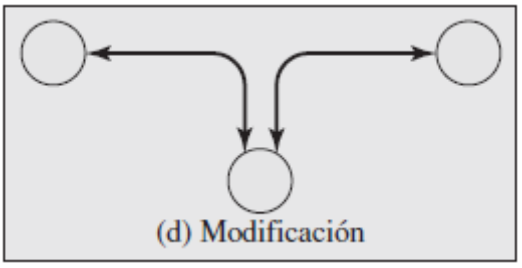


Modificación

Un elemento no autorizado no sólo tiene acceso a un componente sino que también es capaz de modificarlo.

Es un ataque dirigido hacia la **integridad**.

> Cambiar valores de un fichero, alterar un programa, modificar mensajes transmitidos por la red

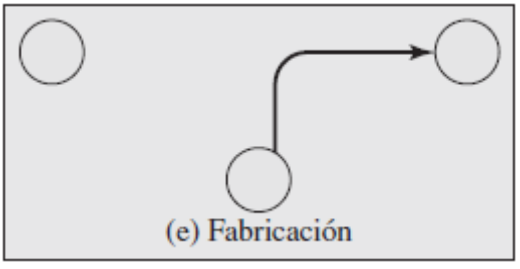


Fabricación

Un elemento no autorizado inserta objetos extraños en el sistema.

Es un ataque contra la **autenticación**.

> Inserción de mensajes externos en la red o incluir un registro en un fichero



Componentes de un sistema informático

Se pueden clasificar en hardware, software, datos y líneas de comunicación y red.

Tabla 16.1. Peligros de seguridad y componentes.

	Disponibilidad	Privacidad	Integridad/Autenticación
Hardware	Equipamiento robado o deshabitado, por lo tanto denegación de servicio.		
Software	Borrado de programas, denegación de acceso a los usuarios.	Copia no autorizada de software.	Modificación de un programa, bien para hacer que falle durante la ejecución o para que realice una tarea diferente.
Datos	Borrar ficheros, denegación de acceso a los usuarios.	Lectura no autorizada de datos. Un análisis estadístico de los datos que revele la información subyacente.	Modificación de los ficheros existentes o creación de nuevos ficheros.
Líneas de comunicación	Borrado o destrucción de mensajes. Las líneas de comunicación o redes no se encuentran disponibles.	Lectura de mensajes. Observación de los patrones de tráfico de mensajes.	Modificación, borrado, reordenación o duplicación de mensajes. Fabricación de mensajes falsos.

Tipos de ataques

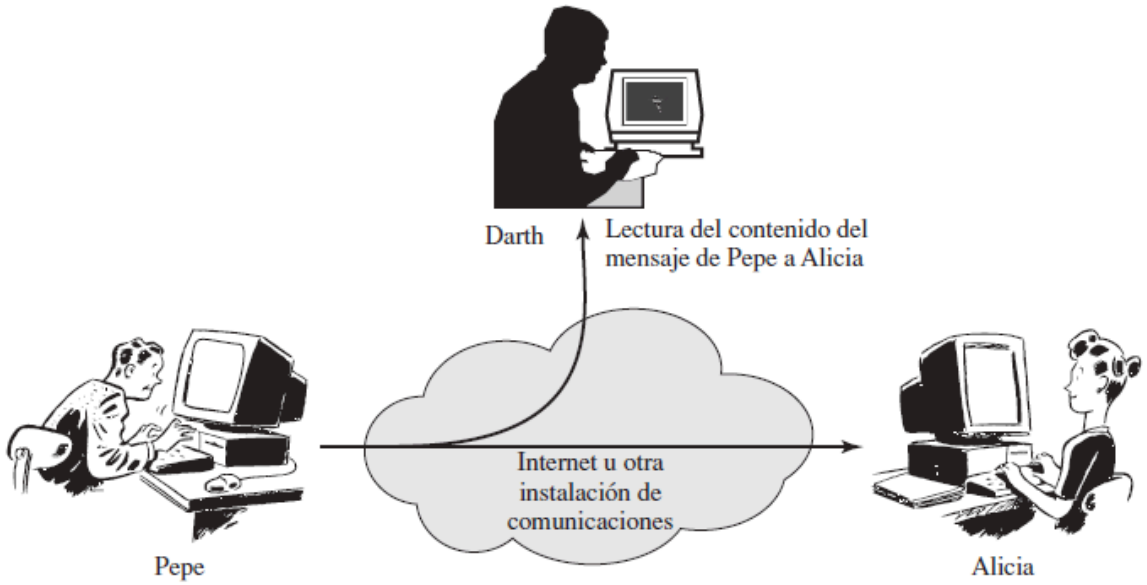
Ataques pasivos

Intenta aprender o hacer uso de la información del sistema, pero no afecta a los recursos del mismo.

Difíciles de detectar.

> Espionaje o monitorización de las transmisiones

Lectura de los contenidos de los mensajes

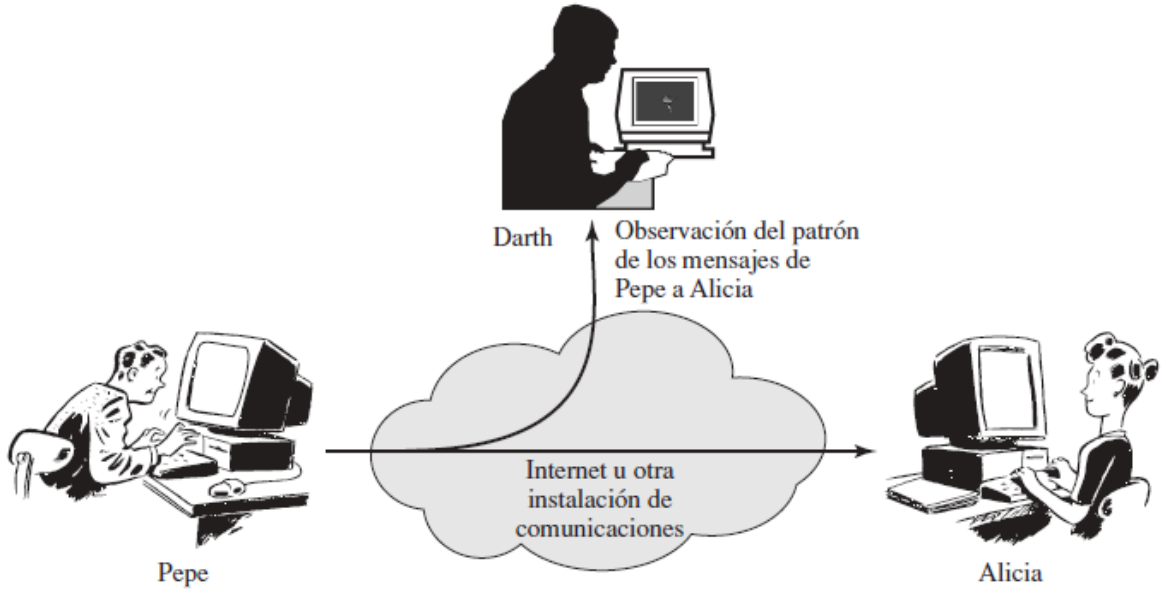


(a) Lectura de los contenidos de los mensajes

> Una conversación telefónica, un mail o la transferencia de un fichero

Análisis de tráfico

Se pueden usar mecanismos de cifrado para ocultar los contenidos de los mensajes, pero se basa en aprender de patrones.



(b) Análisis de tráfico

Ataques activos

Intenta alterar los recursos del sistema o afectar a su operativa.

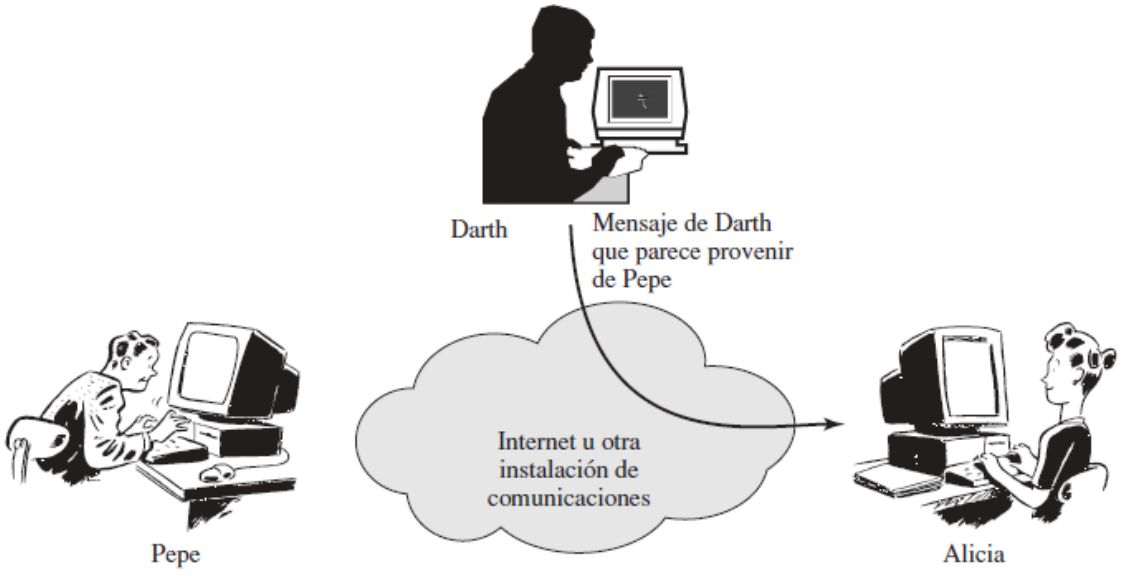
Implican modificaciones en el flujo de datos o la creación de flujos de datos falsos.

Difíciles de prevenir de forma completa.

Enmascaramiento

El elemento intenta hacerse pasar por otro diferente.

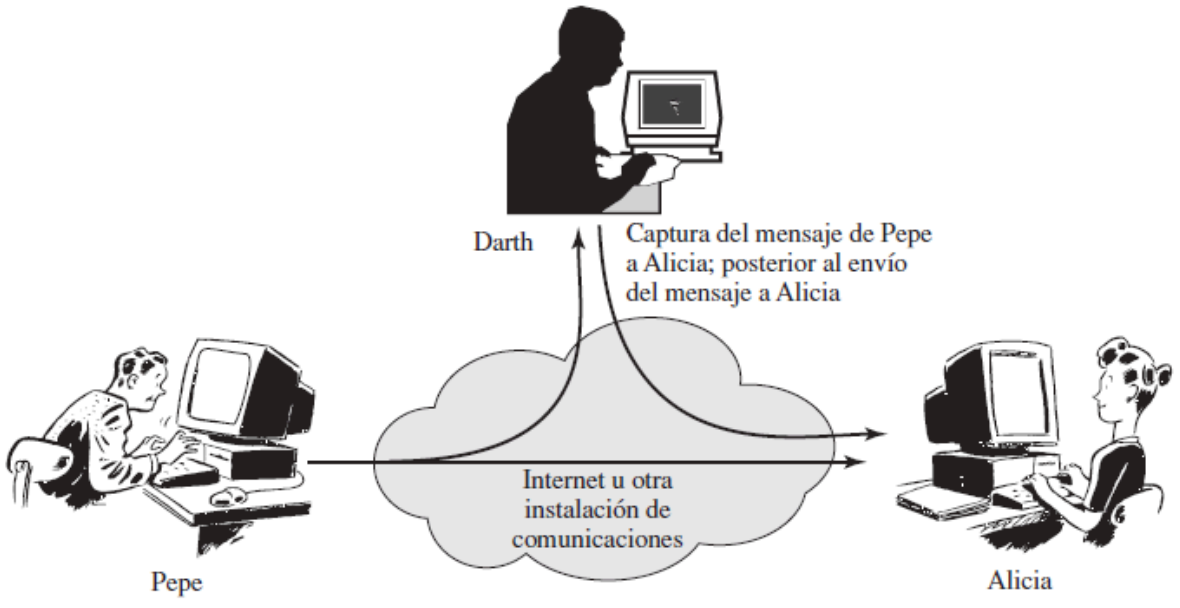
Habitualmente incluye otras formas de **ataques activos**.



(a) Enmascaramiento

Reenvío

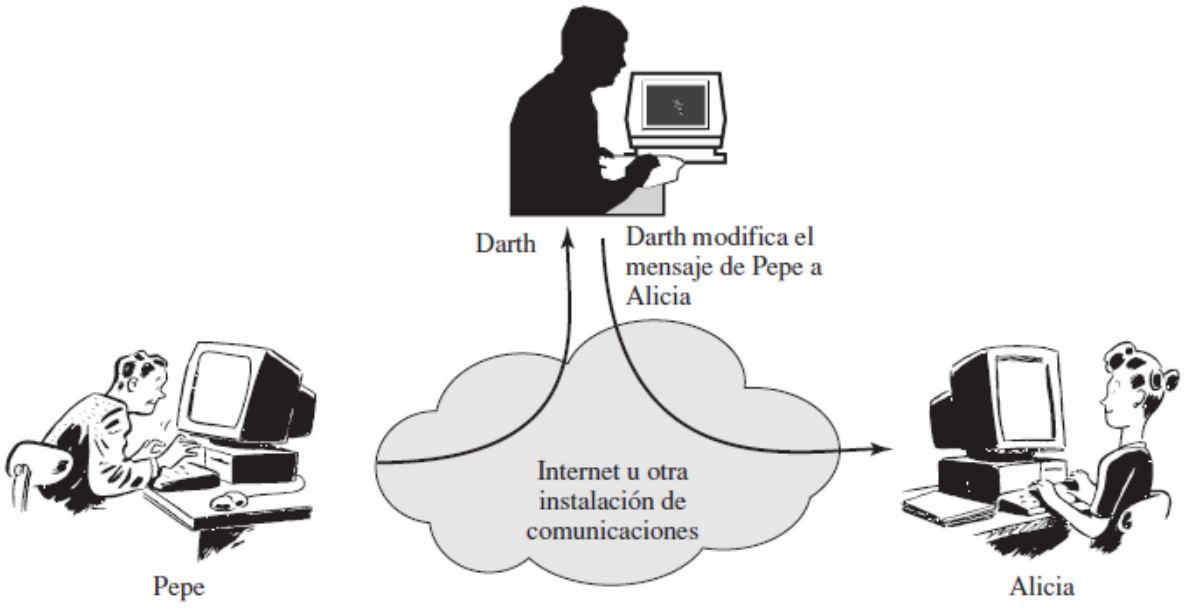
Captura pasiva de una unidad de datos y su posterior retransmisión.



(b) Reenvío

Modificación de mensajes

Una parte de un mensaje válido se altera o se borran/reordenan mensajes.

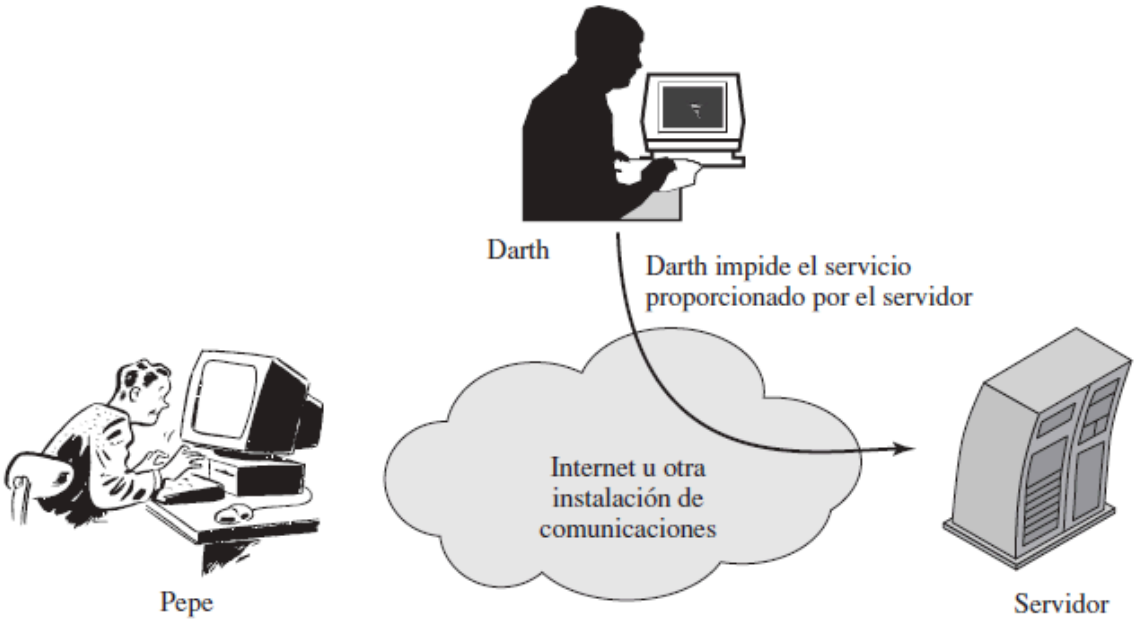


(c) Modificación de mensajes

Denegación de servicio (DOS)

Previene o imposibilita el uso normal o gestión de las instalaciones de comunicaciones.

> Suprimir todos los mensajes dirigidos a la auditoría de seguridad, desarticulación de toda la red (tirarla)



(d) Denegación de servicio

Protección

La multiprogramación trajo la posibilidad de compartir recursos entre usuarios, como:

- Memoria
- Dispositivos de E/S
- Programas
- Datos

La posibilidad de compartir estos recursos introduce la necesidad de la protección.

El sistema operativo debe ofrecer niveles de protección a lo largo del siguiente rango *(orden creciente de dificultad según su implementación y el nivel de protección)*:

Sin protección alguna

Apropiado por los procedimientos sensibles de ejecutar en instantes diferentes.

Aislamiento

Cada proceso opera de forma separada con otros procesos. Sin compartición ni comunicación.

Cada proceso tiene su propio espacio de direcciones, ficheros, etc.

Compartición completa o sin compartición

El propietario del objeto declara si es público o privado.

Público: Cualquier proceso puede acceder al objeto.

Privado: Sólo los procesos del propietario pueden acceder a dicho objeto.

Compartición vía limitaciones acceso

El sistema operativo verifica la permisibilidad de cada acceso por parte de cada usuario específico sobre cada objeto. Actúa como un guardián o vigilante.

Acceso vía capacidades dinámicas

Permite la creación dinámica de derechos de acceso a los objetos.

Uso limitado de un objeto

No sólo limita el acceso a un objeto sino que también el uso que se puede realizar de dicho objeto.

> Un usuario puede ver un documento sensible, pero no imprimirlo

Protección de la memoria

Los aspectos importantes son la seguridad y el correcto funcionamiento de procesos activos.

Si se busca aislar los espacios de memoria: El sistema operativo debe asegurar que sólo el proceso puede acceder a sus páginas/segmentos. `que no entradas duplicadas en la tabla de páginas/segmentos`

Si se desea permitir la compartición: El mismo segmento/página puede aparecer en más de una tabla. Es más fácil de alcanzar en sistemas con segmentación o la combinación de segmentación con paginación.

Control de acceso orientado a usuario

Suele dominarse a través de la autenticación.

La técnica más común es el registro o conexión de usuario. `user log on (id y contraseña)`

Se puede llevar a cabo de forma centralizada o descentralizada.

Centralizada: La red proporciona un servicio de conexión, que determina quien puede hacer uso de la red y con quién se puede conectar.

Descentralizada: La red es un enlace de comunicación transparente y el mecanismo de acceso lo realiza el ordenador destino.

Control de acceso orientado a datos

Puede existir un perfil asociado a un usuario que especifique las operaciones permitidas en los accesos a ficheros. Aplicar reglas por perfiles, no por usuario.

Matriz de acceso: Modelo que tiene como elementos al **sujeto, objeto, derechos**.

En la práctica, estas matrices se descomponen las columnas en **listas de control de acceso (ACL)** `ls -l + chmod`. Por cada objeto hay una *lista de control de acceso* que muestra los usuarios y los permisos.

Las filas de las matrices se definen en **tickets de capacidades**. Estos especifican objetos y operaciones autorizadas para un determinado usuario. El usuario tiene un número de tickets y puede cederlos. No deben ser falsificables.

Intrusos

Generalmente se los denomina *hackers* o *crackers*.

Tipos de intrusos

Enmascarado

Individuo que no está autorizado a utilizar un ordenador y penetra en controles de acceso del sistema para aprovecharse de una cuenta de usuario legítimo.

Suele ser un usuario externo.

Trasgresor

Usuario legítimo que accede a datos, programas o recursos a los cuales no está autorizado o, estando autorizado, aprovecha sus privilegios de forma maliciosa.

Suele ser un usuario interno.

Usuario clandestino

Usuario que sobrepasa el control de supervisión del sistema y evade la auditoría o suprime la recogida de registros de acceso.

Puede ser un usuario interno o externo.

Técnicas de intrusión

El objetivo de un intruso es ganar acceso a un sistema o incrementar el rango de sus privilegios de acceso al sistema.

El fichero de contraseñas se puede proteger con

Cifrado unidireccional

El sistema almacena únicamente una forma cifrada de la contraseña de usuario.

Control acceso

El acceso al fichero que contiene las contraseñas se encuentra limitado a pocas cuentas.

Técnicas

- Probar contraseñas `predeterminadas, cortas o de una lista`
- Recolectar información de los usuarios. **Ingeniería social**.
- Troyanos
- Pinchar la línea entre el usuario y el sistema.

Protección de contraseñas

Técnicas básicas

Educación de los usuarios

Decirle a los usuarios la importancia de usar contraseñas difíciles de adivinar y proporcionar referencias de estas contraseñas.

Los usuarios suelen ignorar estas recomendaciones.

Contraseñas generadas por el ordenador

Si la contraseña es muy aleatoria, los usuarios no la recordarán.

Verificación reactiva de las contraseñas

El sistema, de forma periódica, ejecuta su propio programa de adivinación para encontrar posibles contraseñas adivinables.

Requiere un uso intensivo de recursos.

Verificación proactiva de las contraseñas

A los usuarios se les permite seleccionar su propia contraseña, y al momento de la selección, el sistema prueba a ver si la contraseña está permitida.

Detección de intrusos

Detección estadística de anomalías

Implica la recolección de datos relativos al comportamiento de los usuarios legítimos durante un período de tiempo. Luego se aplican tests estadísticos en un nuevo comportamiento para determinar si el comportamiento es o no del usuario legítimo.

Intenta definir un comportamiento normal o esperado.

Detección por umbral

Implica la definición de umbrales, independientes del usuario, para la frecuencia de determinados eventos.

Basado en el perfil

Se desarrolla un perfil de actividad por cada uno de los usuarios y se lo utiliza para detectar cambios en el comportamiento.

Detección basada en reglas

Implica un intento de definir un conjunto de reglas que se puedan utilizar para decidir si un comportamiento es o no de un intruso.

Intenta definir un comportamiento sospechoso.

Detección de anomalías

Reglas desarrolladas para detectar la desviación de los patrones de usos previos.

Identificación de penetración

Un sistema experto que busca comportamiento sospechoso.

Registros de auditoría

Se utilizan varios registros de las actividades que va realizando el usuario como entrada para los sistemas de detección de intrusos.

Registros de auditoría nativos

Incluido en prácticamente todos los sistemas operativos multiusuarios con el fin de registrar la actividad de los usuarios.

No requiere ningún software adicional para recoger datos.

Pueden no tener la información necesaria o que no esté en el formato conveniente.

Registros de auditoría específicos para detección

Se puede implementar una funcionalidad de recolección de datos que genere registros de auditoría que contienen información pensada únicamente para el sistema de detección de intrusos.

Puede realizarse de forma independiente del vendedor e implantarse en una amplia variedad de sistemas.

Implica tener una sobrecarga extra. Dos paquetes de auditoría ejecutándose en la misma máquina.

Software malicioso ~ *Malware*

Software diseñado para causar daño o utilizar recursos de un ordenador.

Frecuentemente se encuentra escondido dentro de un programa enmascarado como software legítimo.

En algunos casos, se distribuye asimismo a otros ordenadores por medio del correo electrónico.

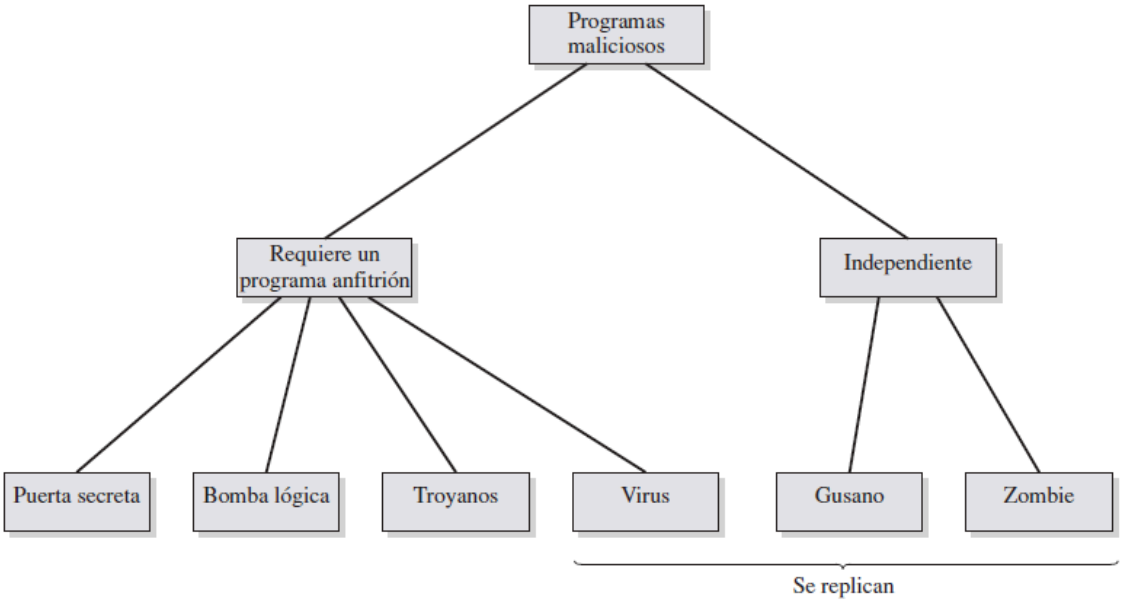


Figura 16.8. Taxonomía de los programas maliciosos.

Puerta secreta

Punto de entrada secreto dentro de un programa que permite a alguien que conoce la existencia de dicha puerta tener el acceso sin utilizar los procedimientos de acceso de seguridad estándar

Bomba lógica

Código insertado dentro de un programa legítimo que explotará bajo ciertas condiciones.

Troyano

Programa útil que, al invocarse, realiza una función no deseada o dañina.

Virus

Programa que puede infectar otros programas modificándolos; las modificaciones incluyen la copia del programa virus.

Gusano

Utilizan las conexiones de red para expandirse de un sistema a otro.

Para replicarse a sí mismo, utiliza algún tipo de vehículo de comunicación:

- Correo electrónico
- Capacidad ejecución remota
- Capacidad de conexión remota

Zombie

Programa que toma el control de otro ordenador conectado a Internet y posteriormente utiliza el mismo para lanzar ataques difíciles de trazar al origen del creador.

Se suelen usar en ataques *DOS* descentralizados.