Arquitectura de Comunicaciones

Lic. Pablo Lena
Ing. Anibal Pose

INTRODUCCION EN SEGURIDAD EN REDES

INDICE

1. Requisitos y tipos de ataques en la seguridad de la red.
2. Causantes de los ataques.
3. Ejemplos de ataques y soluciones.

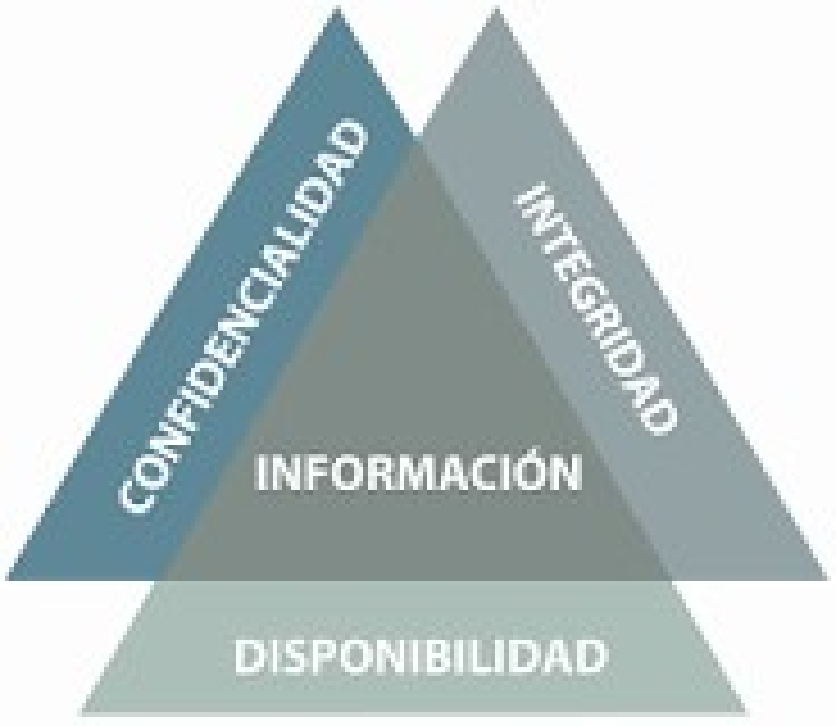
Requisitos de la seguridad en la red

La seguridad en ordenadores y en redes implica tres exigencias:

Confidencialidad

Integridad.

Disponibilidad.



Seguridad: Línea de Tiempo

Los *ataques* comenzaron en la década del '50. Los primeros atacantes eran personas cercanas a los sistemas (¿ y hoy?.....).

1960 HW de protección de memoria: VM.
1962 Mecanismos de control de acceso a los archivos.
1967 Funciones One-Way (passwords).
1968 Seguridad en kernels (Multics).
1969-89 ARPANET (Admin. Centralizada), Intemet TCP/IP en 1977.

Seguridad: Línea de Tiempo (2)

1975 UNIX-UNIX copy protocol (UUCP) y puertas trampa en mails,
1976 Criptografia de clave pública y firma digital.
1978 RSA (clave pública).
1978 Estudio de contraseñas (inteligente).
1978 Primer protocolo de e-cash.
1983 DNS distribuido (vulnerable al spoofing).
1984 Los Virus empiezan a investigarse.
1985 Esquemas de contraseñas avanzados.
1988 Intemet Worm (6000 computadoras (10% Intenet)).
1988 Autentificación distribuida (Kerberos).
1989 Pretty Good Privacy (PGP) y Privacy Enhanced Mail (PEM).

Seguridad: Línea de Tiempo (3)

1990 Remailers anónimos.
1993 Spooling, sniffing, firewalls.
1994 SSL v 1.0 (Netscape).
1996 Java (Web hacking),
1997 DNSSec.
1998 Programas de barrido de redes.
1998 Ipsec.
1999 Primer ataque DDoS.
2000 I LoveYou (VBscript) (.5 a 8 millones de infecciones). B02k.
2001 Red Code, Nimbda (infección de servidores MS IIS).
2002 Mas I-Worms (en general explotan fallas en Intemet Explorer).

Tipos de ataques a la seguridad en la red

Interrupción: ataque de disponibilidad.

Intercepción: ataque a la confidencialidad.

Modificación: ataque a la integridad.

Fabricación: ataque a la autenticidad.

Ataques pasivos

La meta del oponente es obtener información que está siendo transmistida.

Divulgación del contenido de un mensaje (un correo electrónico, un fichero con datos importantes)**.**

Análisis del tráfico (cuando se usan sistemas de cifrado, el oponente se dedica a observar la frecuencia y longitud de los mensajes e intentará a partir de estos datos descifrarlos).

Ataques activos

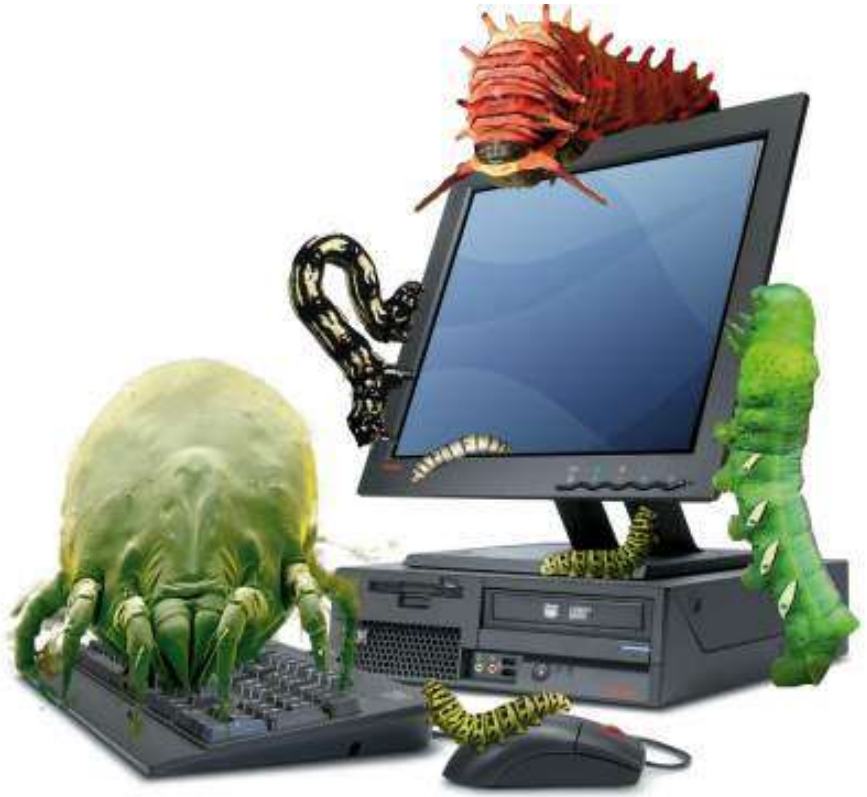
Consisten en la modificación del flujo de datos o la creación de flujos falsos.

Enmascaramiento.

Repetición.

Modificación de mensajes.

Denegación de un servicio.



Causantes de los ataques

HACKER

¿Qué es?

Un **hacker** es alguien que descubre las debilidades de un computador o de una red informática, aunque el término puede aplicarse también a alguien con un conocimiento avanzado de computadoras y de redes informáticas.

A los hackers a menudo se refiere a la cultura *underground* de computadoras, pero ahora es una comunidad abierta

Gente apasionada por la seguridad informática. Una comunidad de entusiastas programadores y diseñadores de sistemas originada en los sesenta.

En la actualidad se usa de forma corriente para referirse mayormente a los criminales informáticos, debido a su utilización masiva por parte de los medios de comunicación desde la década de 1980

CRACKER

Es una persona que mediante ingeniería inversa realiza: seriales, keygens y cracks.

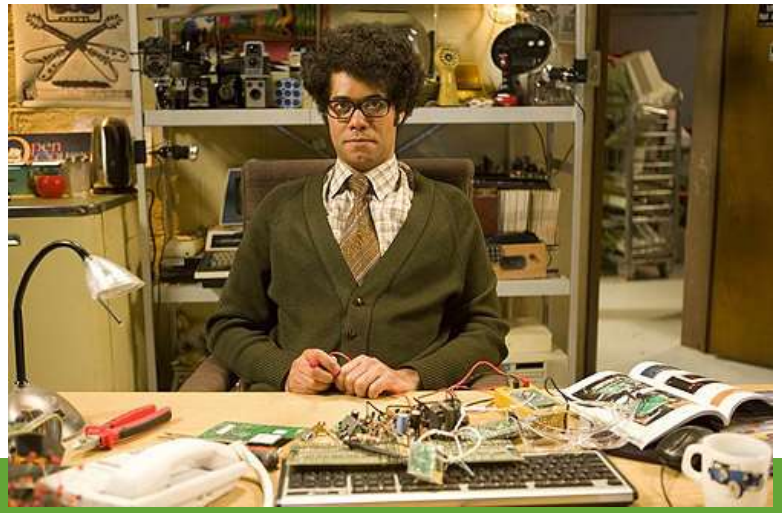
Es cualquier persona que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño.

En ocasiones el *cracking* es la única manera de realizar cambios sobre software para el que su fabricante no presta soporte.

LAMER

Es el nombre estándar para aquellos considerados **incompetentes** frente a otras personas que sí presentarían realmente más habilidades o conocimientos sobre un tema en específico

Un lamer se considera a un aficionado al tema que se jacta de poseer grandes conocimientos que realmente no posee y que no tiene intención de aprender.



Correos electrónicos en cadena

ABSOLUTAMENTE TODOS esos e-mails que piden que hagas un re-envío SON FALSOS.

Hay que borrar esos mails y tirarlos a la papelera.

Phising

Es un tipo de delito cibernético, en el que el estafador, conocido como *phisher*, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un e-mail, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.

De: BBVA <bbva@rec.info>
Asunto: **aviso Segurid bbva net**
Fecha: 16 de septiembre de 2009 11:28:25 GMT+02:00
Para: [redacted]
Responder a: BBVA <bbva@rec.info>

Estimado cliente de BBVA:

Grupo **BBVA**

Grupo BBVA siempre trata de encontrar sus expectativas mas altas. Por eso usamos la ultima tecnologia en seguridad para nuestros clientes.
Por lo tanto nuestro departamento de antifraude ha desarrollado un nuevo sistema de seguridad que elimine cualquier posibilidad del acceso de la tercera persona a sus datos, cuentas ni fondos.

Es obligatorio para todos los clientes de **BBVA** en Linea usar este sistema de seguridad.

Nuestro consejo para usted es que introduzca sus datos se acceso para pasar La Verificacion Del Sistema. Si el registro no es realizado dentro de 48 Horas su cuenta sera suspendida temporalmente hasta que su registro sea completado.

Esto solo le va a costar unos minutos de su tiempo y va a tener una seguridad mucho mas estable.
Para comenzar el registro por favor pinche aqui:

Aceptar

RE: Portal de administración

TS

Tutorias Sociales

To Tutorias Sociales

"Estimado usuario de correo electrónico de la universidad

Estamos actualizando nuestro servicio de correo web para aumentar la velocidad y el

Utilice el siguiente enlace para actualizar su correo electrónico

Haga clic aquí

Gracias
Portal de administración - Universidad Nacional de La Matanza

Tutorias Sociales -

Nombre de usuario

Dirección de correo electrónico

Contraseña

Entrar

De: [redacted]
Asunto: **Trabajo remoto, los salarios de 500 a 1500 euros por semana.**
Fecha: 28 de octubre de 2009 11:58:21 GMT+01:00
Para: [redacted]

Nos gustaria ofrecerle la cooperacion y un ingreso adicional decente.
Usted puede ganar dinero sin salir de casa.Pagado cada semana.

Para ello es necesario:
1. 2-8 horas de tiempo de ocio por dia de tiempo libre.
2. Casilla de correo personal en Internet.
3. Mobile o por telefono.

Si desea saber acerca de esto mas informacion o una pregunta Escriba a nuestros empleados. en: Kennith@west-eur.net

Por favor, en su carta de nombre y edad.
Nuestro Manager respondera dentro de 5-6 horas.

Antes de la conexion.

Soluciones Anti-Phishing

Respuesta social: no fiarse de nada ni de nadie.

Respuesta técnica: hay varios programas informáticos anti-phishing disponibles, aparte de los programas anti-spam.

Respuesta legislativa o judicial: son muchos los países que ya cuentan con leyes anti-phishing.

Agujeros de seguridad

¿Qué son?

Son un tipo de bug (errores de programación) que no se suelen detectar ya que no están asociados a disfunciones del sofware.

Muchos programadores los buscan con el objeto de invadir ordenadores ajenos.

¿Cómo protegernos?

Realizar copias de seguridad o backups de forma sistemática para prevenir posibles pérdidas de información.

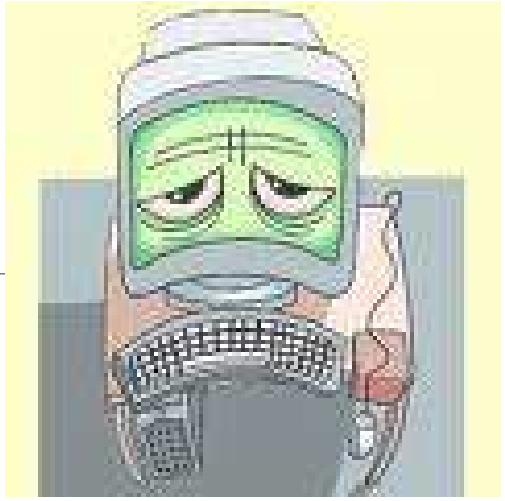
Utilizar los servicios de actualización automática de los fabricantes o, en su defecto, asegurarse de tener instalados los últimos parches o actualizaciones.

Malware

La palabra malware proviene de la composición de las palabras inglesas **malicious software**, es decir, programas maliciosos.

Se entiende por malware cualquier programa, documento o mensaje que puede resultar perjudicial para un ordenador, tanto por pérdida de datos como por pérdida de productividad.

Ejemplos de Malware



VIRUS

Los virus son programas que se introducen en los ordenadores de formas muy diversas: a través del correo electrónico, Internet, disquetes, etc.

Tienen dos características diferenciales:

- Se reproducen infectando otros ficheros o programas.
- Al ejecutarse, realizan acciones molestas y/o dañinas para el usuario.

BACKDOORS

Programa que se introduce en el ordenador de manera encubierta, aparentando ser inofensivo. Una vez ejecutado, establece una "puerta trasera" a través de la cual es posible controlar el ordenador afectado.

Acciones:

- Eliminación de ficheros o la destrucción de la información del disco duro.
- Pueden capturar y reenviar datos confidenciales a una dirección externa o abrir puertos de comunicaciones, permitiendo que un posible intruso controle nuestro ordenador de forma remota.

TROYANOS

Un troyano llega al ordenador como un programa aparentemente inofensivo. Sin embargo, al ejecutarlo instalará en nuestro ordenador un segundo programa, el troyano en sí.

Acciones:

- Capturar todos los textos introducidos mediante el teclado.
- Registrar las contraseñas introducidas por el usuario.

Ataques y técnicas de intrusión

Una técnica de intrusión es un conjunto de actividades que tienen por objetivo violar la seguridad de un sistema informático.

Que puedo utilizar investigar sitio

- Ingenieria social
- Verificar DNS
- Verificar proveedores
- Analisis de vulnerabilidad
- Analisis de Puertos

SPYWARE

Son aplicaciones informáticas que recopilan datos sobre los hábitos de navegación, preferencias y gustos del usuario. Los datos recogidos son transmitidos a los propios fabricantes o a terceros, en forma directa o después de ser almacenados en el ordenador.

Se puede instalar a través de:

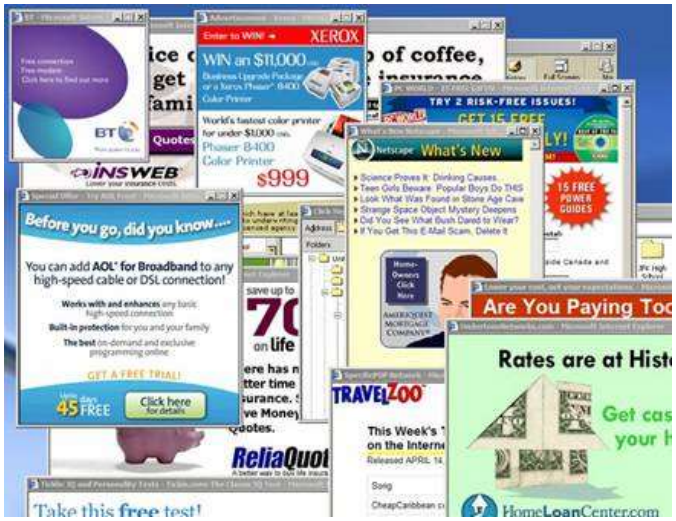
- Un troyano.
- Visitas a páginas web que contienen determinados controles ActiveX o código que explota una determinada vulnerabilidad.
- Aplicaciones con licencia de tipo shareware o freeware descargadas de Internet, etc.

Solución: instalar un Anti-spyware.

ADWARE

Adware es una contracción de las palabras Advertising Software, es decir, programas que muestran anuncios.

Se denomina adware al software que muestra publicidad, empleando cualquier tipo de medio: ventanas emergentes, banners, cambios en la página de inicio o de búsqueda del navegador, etc.



PACKET SNIFFER

¿Qué es?

En informática, un **packet sniffer** es un programa de captura de las tramas de red.

Es algo común lo que ocurre, el medio de transmisión (cable coaxial, UTP, fibra óptica etc.) es compartido por varias computadoras y dispositivos de red, lo que hace posible que un ordenador capture las tramas de información no destinadas a él.

USOS

Tienen diversos usos como monitorizar de redes para detectar y analizar fallos. Detección de intrusos, con el fin de descubrir hackers.

También es habitual su uso para **fines maliciosos**, como robar contraseñas, interceptar mensajes de correo electrónico, espiar conversaciones de Chat, etc..

Pasos de las practicas