TEMA 5: SEGURIDAD EN REDES

0. INTRODUCCIÓN

Seguridad en una red informática se define como la garantía de integridad de los datos con los que se trabaje en esa red.

Integridad de los datos es la característica de dichos datos de no haber sido manipulados por agentes no autorizados.

1. TIPOS DE ATAQUE INFORMÁTICO

Vamos a realizar una pequeña clasificación de los tipos de acciones más comunes que suponen una agresión a la integridad de la información:

- VIRUS Y TROYANOS
- PHISING
- CHILD GROOMING
- CRACKING
- MAN IN THE MIDDLE

2. VIRUS Y TROYANOS

Virus: programa informático que viene oculto en el interior de otro programa informático, normalmente de origen dudoso. Dicho

programa se instala junto al programa huésped sin nuestro conocimiento, de forma oculta, y hace copias por su cuenta de sí mismo en distintos puntos del disco duro.

El programa huésped se define como **infectado**.

El objetivo principal de un virus es propagarse y causar daños en el sistema (borrar datos, modificarlos, etc..)

El funcionamiento de un antivirus estándar consiste en localizar rutinas de instalación ajenas al objetivo que dicho programa crea que estamos persiguiendo (carpetas de instalación distintas, etc…), o copias o borrados automáticos dentro del disco duro que no constaban la tabla de tareas del sistema operativo.

Cuando en la instalación de un programa aparece alguno de esos comportamientos, el algoritmo de trabajo es:

a) El antivirus consulta dicho comportamiento con su base de datos.

b) Si dicho comportamiento coincide con el de un virus de su base de datos, interrumpe la instalación, y dependiendo de si está configurado en modo automático o no,

borra el programa (desinfecta)

c) Si dicho comportamiento no aparece en su base de datos, propone al usuario la cuarentena de dicho archivo (aislarlo en una carpeta sin permisos de lectura/escritura)

Gusano: al igual que un virus, es un programa con objetivos maliciosos que trata de instalarse en nuestro ordenador sin nuestro conocimiento, haciendo copias de sí mismo en distintas partes del disco duro. Al contrario que un virus, no trata de dañar el equipo, sino de mantenerse oculto el mayor tiempo posible para realizar cualesquiera tarea para la que esté programado.

Según el tipo de tarea que realice, podemos distinguir entre gusanos de tipo **TROYANO** y **BACKDOOR**. También puede tomar la forma de un **ROOTKIT**

3. TROYANOS, BACKDOORS Y ROOTKITS

Troyano: por definición, es un programa de tipo gusano (worm) que granjea el acceso externo a un programador malintencionado (cracker) (no confundir con el hacker, que es el aficionado investigador compulsivo)

Backdoor: es una puerta trasera que un gusano deja abierta en nuestro ordenador para posibilitar accesos externos posteriores. Mientras que un troyano está más pensado para permitir el control directo por el cracker de nuestro ordenador, el backdoor simplemente deja pasar a un pirata o a un programa.

Rootkit: viene a ser un programa que oculta a sí mismo o a otro programa al administrador de tareas. Así, el usuario no puede localizar manualmente a dicho proceso "fantasma" que sin embargo está residente en memoria.

4. SPYWARE Y DERIVADOS

SPYWARE: por definición, se refiere a cualquier tipo de software que recaba información de mi equipo de forma maliciosa.

Los datos que suele recabar un programa de spyware son:

- Cookies, direcciones de internet y de e-mail, y datos introducidos en formularios en páginas web
- Dirección IP, DNS, características de router, y otros datos relativos a la conexión del equipo.

ADWARE: Cualquier programa que mientras está residente en memoria, ejecuta

automáticamente o me redirecciona a páginas web de corte publicitario. Su funcionamiento más común consiste en mostrar de forma intrusiva ventanas (pop-up) publicitarias mientras el usuario navega por Internet.

HIJACKING: técnicas de programación orientadas a la manipulación de nuestro programa navegador, normalmente. Entre otras tareas, un hijacker puede cambiar nuestra página de inicio, o redireccionar nuestro buscador a resultados que le interesen al programador (páginas de pago, normalmente).

PHARMING: técnica consistente en cambiar nuestro servidor DNS, para redireccionarnos a espacios web predeterminados.

5. OTRAS TÉCNICAS DE CARÁCTER MALICIOSO.

PHISING: Técnicas de ingeniería social consistentes en ponerse en contacto con un internauta, diciendo representar a una entidad financiera, y pidiéndole los datos a dicho usuario con cualquier excusa. Parte del engaño pasa por redireccionar al usuario a una web falsa que emula a una institución de confianza para el usuario.

KEYLOGGER: Es un programa que registra

absolutamente todo lo que un usuario teclea y lo guarda en un archivo.

STEALER: Es un programa que busca en determinadas carpetas información referente a contraseñas, trata de desencriptarlas y las envía al cracker.

DIALER: Es un programa que, en los tiempos antiguos de Internet y líneas telefónicas, conectaba la línea del usuario con líneas telefónicas de pago, de altas tarifas por minuto.

6. ATAQUES DISTRIBUIDOS. SPAM, ZOMBIES Y BOTNETS.

SPAM: Todo tipo de correo de corte publicitario no deseado.

ORDENADOR ZOMBI O BOTNET: Ordenador de usuario infectado por algún tipo de gusano que se dedica a enviar correo spam a espaldas de dicho usuario. En realidad, el ordenador es el zombi, y se habla de BOTNET refiriéndonos a la red de ordenadores zombies.

Los métodos de recolección de direcciones de mail son muy variados:

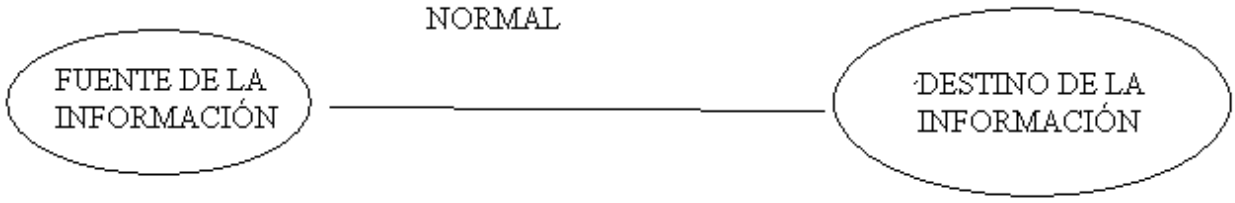
- Cartas encadenadas: la mayoría de la gente reenvía este tipo de correos a todos sus

contactos, sin utilizar la herramienta CCO:

- Infección del equipo por Spyware (stealers, hijackers, etc...)
- Uso de redes sociales (Tuenti, Facebook...) mediante técnicas legales o ilegales.

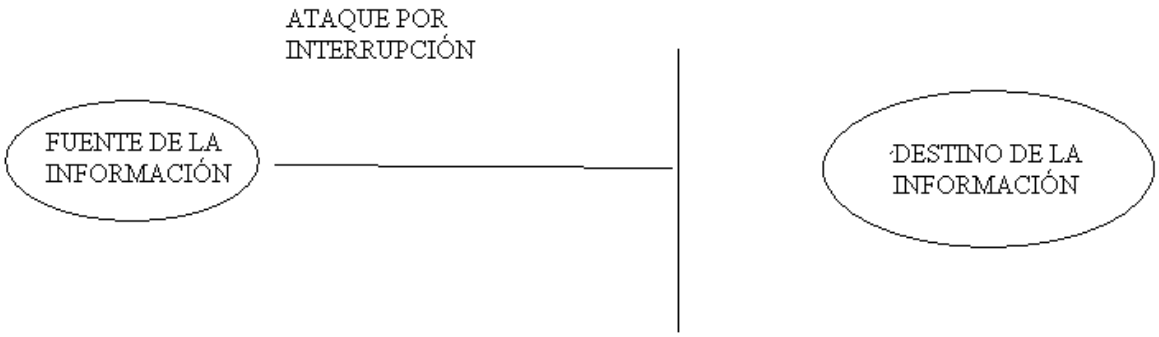
En una BOTNET cada ordenador infectado contacta con un canal IRC (de chat) donde recibe las instrucciones a cumplir.

7. AMENAZAS DE SEGURIDAD. ATAQUES ACTIVOS Y PASIVOS.

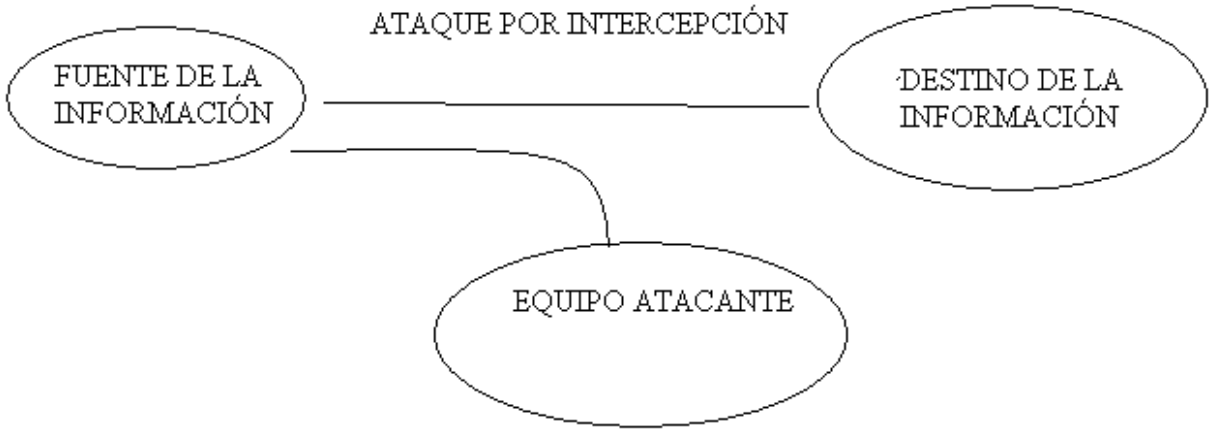


Normalmente, el flujo de la información en un sistema seguro se produce desde el ordenador fuente al ordenador cliente (destino).

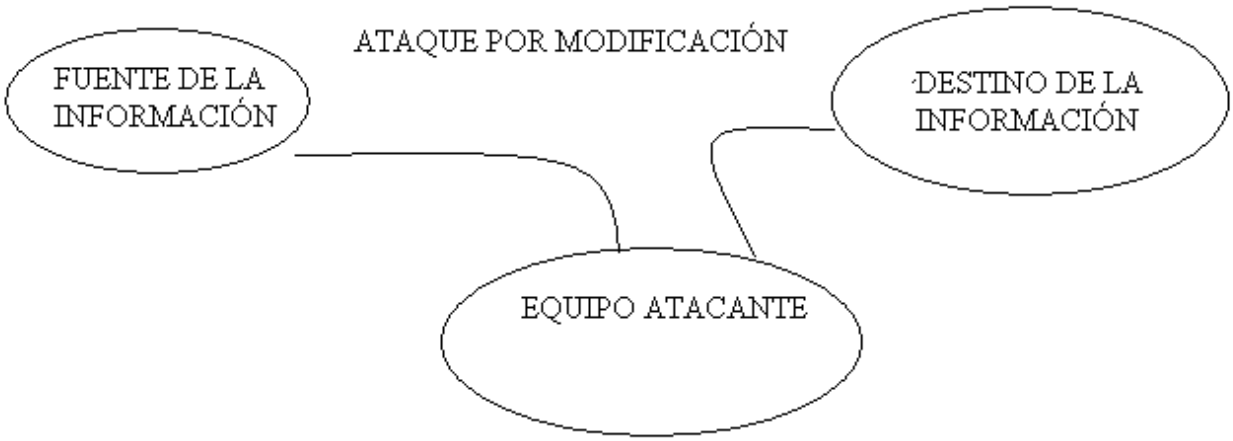
Las **amenazas de seguridad** se pueden plantear por interrupción, por intercepción, por modificación y por fabricación



Ataque por interrupción: se interrumpe el flujo normal de la información, y el cliente no se puede conectar al ordenador servidor.



Ataque por intercepción: no se interrumpe el flujo de la información, pero el atacante recibe la misma información a la que accede el cliente legal.



Ataque por modificación: la información pasa primero por el equipo atacante, que la modifica a voluntad antes de pasarla al cliente.

Ataque por fabricación: el equipo atacante genera directamente la información que llega al cliente.

Los ataques de un equipo pirata a una red pueden ser de tipo **ACTIVO** o **PASIVO**

ATAQUES PASIVOS: El atacante no altera la comunicación (sólo está a la escucha). Algunos ejemplos de ataque pasivo son:

- Obtención del origen y el destinatario de la comunicación
- Control del volumen de tráfico en la red
- Control de horarios

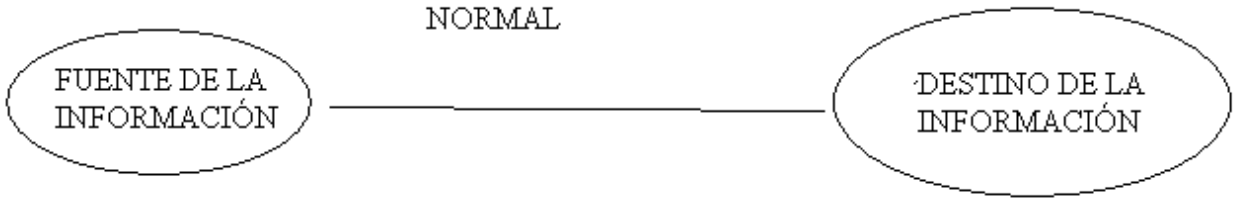
ATAQUES ACTIVOS: en estos ataques, el equipo agresor puede modificar la información que fluye por la red. Ejemplos de estos ataques pueden ser:

- Suplantación de identidad
- Reactuación (capturar la información, por ej, de una transacción bancaria, y modificarla a nuestro favor).
- Modificación de mensajes
- Denegación de servicio: impedir que el ordenador atacado acceda a un servicio de la red.

Los ataques de denegación de servicio están a la

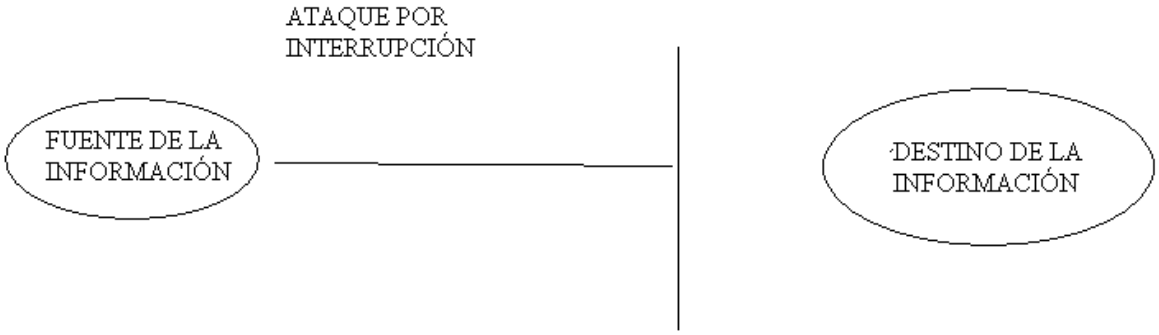
orden del día, como modo de chantaje a multinacionales o de ciber-guerra fría.

7. AMENAZAS DE SEGURIDAD. ATAQUES ACTIVOS Y PASIVOS.

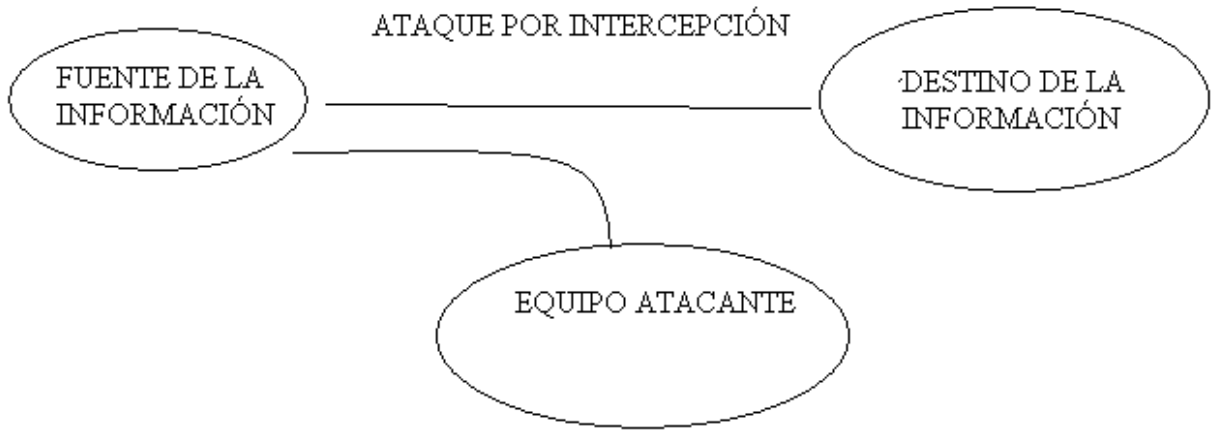


Normalmente, el flujo de la información en un sistema seguro se produce desde el ordenador fuente al ordenador cliente (destino).

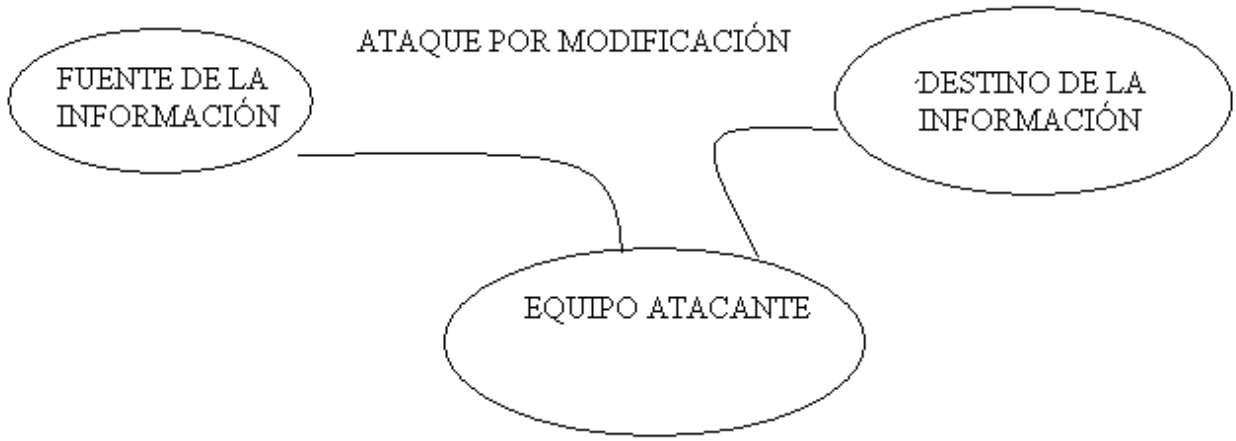
Las **amenazas de seguridad** se pueden plantear por interrupción, por intercepción, por modificación y por fabricación



Ataque por interrupción: se interrumpe el flujo normal de la información, y el cliente no se puede conectar al ordenador servidor.



Ataque por intercepción: no se interrumpe el flujo de la información, pero el atacante recibe la misma información a la que accede el cliente legal.



Ataque por modificación: la información pasa primero por el equipo atacante, que la modifica a voluntad antes de pasarla al cliente.

Ataque por fabricación: el equipo atacante genera directamente la información que llega al cliente.

Los ataques de un equipo pirata a una red pueden ser de tipo **ACTIVO** o **PASIVO**

ATAQUES PASIVOS: El atacante no altera la comunicación (sólo está a la escucha). Algunos ejemplos de ataque pasivo son:

- Obtención del origen y el destinatario de la comunicación
- Control del volumen de tráfico en la red
- Control de horarios

ATAQUES ACTIVOS: en estos ataques, el equipo agresor puede modificar la información que fluye por la red. Ejemplos de estos ataques pueden ser:

- Suplantación de identidad
- Reactuación (capturar la información, por ej, de una transacción bancaria, y modificarla a nuestro favor).
- Modificación de mensajes
- Denegación de servicio: impedir que el ordenador atacado acceda a un servicio de la red.

Los ataques de denegación de servicio están a la orden del día, como modo de chantaje a multinacionales o de ciber-guerra fría.

En los próximos apartados distinguiremos entre hacking de sistemas, de redes, de servidores web y de aplicaciones.

8. HACKING DE SISTEMAS

Por hacking de sistemas entenderemos el conjunto de técnicas que analizan un equipo y su sistema operativo, buscan vulnerabilidades (puertos abiertos, bugs...) y tratan de entrar en

dicho equipo aprovechando dichas vulnerabilidades.

Lo más común es escanear los puertos abiertos que hay en un ordenador, normalmente debido a su utilización por parte de diversas aplicaciones y programas. A través de dichos puertos, se puede conectar un equipo externo, y con suerte, obligarle a realizar determinadas tareas.

Un **bug** es un fallo de programación que puede aprovechar un cracker para introducirse en el sistema. Los bugs que van apareciendo en un sistema operativo se van resolviendo a través de las actualizaciones periódicas.

Un **exploit** es un código utilizado por el cracker para entrar o utilizar ilegalmente un equipo aprovechando un **bug**.

Naturalmente, otro modo de hackear un sistema es infectarlo con un virus o un gusano mediante cualquiera de las técnicas comentadas en anteriores apartados.

8.1. Ataques contra contraseñas Windows.

En los sistemas operativos Windows, las contraseñas se almacenan cifradas según una función matemática (**hash**) en una zona llamada **SAM** (Administración de cuentas de seguridad). Este cifrado se realiza según una función aleatoria (en cada equipo, el cifrado ofrecerá un resultado distinto).

Un cracker puede llegar a entrar en las carpetas donde se guardan dichas contraseñas, pero es prácticamente imposible romper dicho cifrado. Una técnica comúnmente utilizada es utilizar unas tablas de referencia (*Rainbow Tables)* en las que se introducen una serie de combinaciones de números y letras comunes, que se van cifrando de acuerdo a dicho algoritmo, comprobando si dicha contraseña se acepta en el sistema en cuestión (es lo que se denomina *ATAQUE POR DICCIONARIO o ATAQUE POR FUERZA BRUTA*).

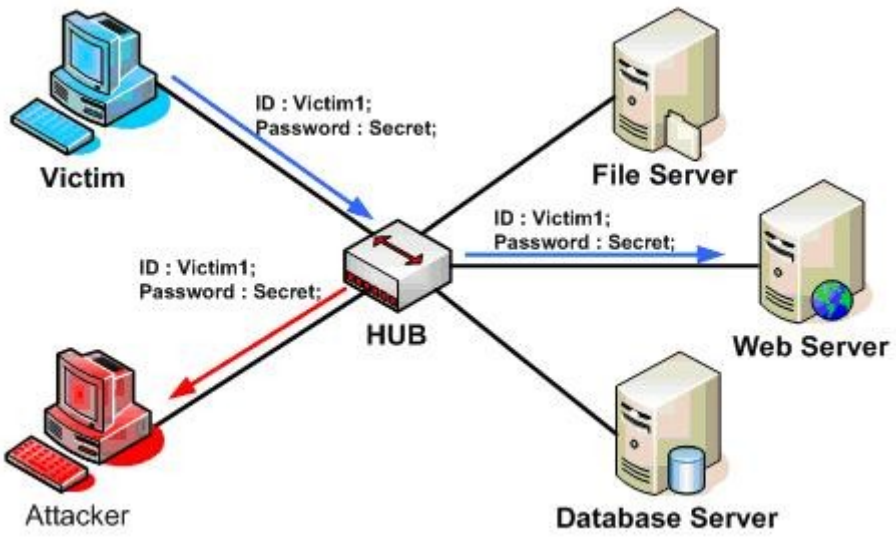
9. HACKING DE REDES

Las técnicas de hacking de redes incluyen todos los procesos que permiten a un usuario irrumpir en una red privada sin tener el permiso necesario para ello.

Entre otras técnicas, estudiaremos los ataques MAN IN THE MIDDLE, DNS SPOOFING, NAVEGACIÓN ANÓNIMA y el uso de SNIFFERS.

9.1. Man in the Middle

Esta técnica de hacking de redes consiste en adquirir la capacidad de leer, insertar y modificar a voluntad la información en juego dentro de una red.



Una de las formas más comunes de este tipo de ataque consiste en engañar a uno de los ordenadores clientes de la red para que crea que nuestro equipo es su puerta de enlace con la red. Así, dicho cliente nos da sus contraseñas de acceso granjeándonos el acceso no sólo a la red, sino a toda la información que dicho equipo envíe o pida a la LAN.

9.2. DNS Spoofing

Esta técnica consiste en suplantar la identidad del servidor DNS de un equipo dentro de una red. Recordemos que el ordenador DNS en una red local es aquél que contiene una base de datos con las correspondencias entre nombres de dominio y sus correspondientes direcciones IP. Así, podemos hacer que cuando el equipo "envenenado" trate de abrir una página web, encuentre otra fabricada por nosotros, o se le redirija a una página de nuestra conveniencia.

9.3. Navegación anónima por Internet.

Cuando se accede a un servidor, éste registra nuestra dirección IP. Si queremos navegar por Internet sin que quede constancia de ello, podemos utilizar servidores proxy anónimos.

Un servidor proxy es un ordenador intermedio que se utiliza en ocasiones para navegar por Internet. Así, cuando realizamos una petición web, se la hacemos al proxy, que busca dicha web, la almacena

en su memoria caché y a continuación nos cede dicha información.

Si encadenamos el uso de diversos servidores proxy, haremos todavía más difícil el que se nos rastree.

9.4. Uso de SNIFFERS

Un SNIFFER es un programa que un cracker utiliza en una red para monitorizar el tráfico de información en la LAN.

Se puede programar un SNIFFER para que detecte un tipo determinado de información, y nos la envíe cuando se produzca en la red. Un caso muy común y popular son los sniffers VoIP (detectan y espían las llamadas telefónicas por Internet).

10. Hacking de servidores web

En este apartado estudiaremos diversos vectores de ataque contra servidore donde se alojan páginas web, entre otros servicios.

La mayoría de los servidores utilizan el

programa de software libre *Apache* para alojar sus sitios respectivos

Los vectores de ataque más conocidos son:

- XSS (Cross Site Scripting)
- RFI (Remote File Includer)
- LFI (Local File Includer)
- Autenticación web
- Inyección SQL

10.1. Ataque XSS (Cross Site Scritping)

Este ataque compromete la seguridad del usuario, y no la del servidor. Consiste en inyectar código HTML o JavaScript en una web, con el objetivo de que el usuario ejecute dicho código malicioso junto con el que genera la página web a la que se ha conectado.

10.2. Remote File Inclusion (RFI) y Local File Inclusion (LFI)

Este ataque consiste en aprovechar una vulnerabilidad del servidor para que él mismo ejecute un código que hemos guardado en otro sitio web distinto.

La forma más común de estos ataques es la de engañar a la página web que estamos visitando para que ejecute un programa que nos granjea acceso a sus carpetas (es lo que se conoce como shell web).

La diferencia entre LFI y RFI es que en el caso del LFI el código que se ejecuta se ha subido al propio servidor, (escondido en mensajes que se envían al foro, etc...)

10.3. Ataque por inyección SQL

El lenguaje SQL (*Structured Query Language*) es un lenguaje de programación para generar y manejar bases de datos en servidores web. La mayor parte de las webs (la del IES Eduardo Valencia, sin ir más lejos) utilizan una base de datos para interactuar con el usuario. Así, por ejemplo, el usuario que está registrado en el sitio web, debe introducir su nombre y contraseña para tener acceso a más contenidos que el usuario no registrado. El servidor comprueba dichos datos en su base de datos SQL, y granjea el acceso que le corresponda.

La unidad básica del lenguaje SQL es la consulta (se pregunta algo a la base de datos). El ataque por inyección SQL consiste en realizar una consulta en este lenguaje, que incluye una serie de instrucciones que tratan de manipular dicha base de datos, extrayendo la información que pueda.