# UNIVERSIDAD NACIONAL DE LA AMAZONÍA PERUANA


## FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA


# "METODOS DE ATAQUE INFORMATICOS"

## INFORME DE TRABAJO PRÁCTICO DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

**INGENIERO DE SISTEMAS E INFORMÁTICA**

PRESENTADO POR EL BACHILLER:

**PERCY JOEL PLAZA TORRES**

ASESOR:
**ING. LUIS HONORATO PITA ASTENGO**

**IQUITOS – PERÚ**
**2014**

**INFORME TÉCNICO DE EXÁMEN DE SUFICIENCIA PREVIA ACTUALIZACIÓN ACADÉMICA APROBADO EN SUSTENTACIÓN PÚBLICA EL DIA 13 DE SETIEMBRE DEL 2014 POR EL JURADO EXAMINADOR DESIGNADO POR EL DECANO DE LA FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA DE LA UNIVERSIDAD NACIONAL DE LA AMAZONÍA PERUANA.**

……..
Dr. Luis Benjamín Irigoin Sánchez
Presidente

……..
Lic. Adm Angel Ildefonso Catashunga Torres
Primer Miembro

……..
Ing. Rafael Vilca Barbaran
Segundo Miembro

……..
Ing. Luis Honorato Pita Astengo
Asesor

## DEDICATORIA

A Dios por darme vida, salud y alegría, al mismo tiempo mi agradecimiento profundo y sincero a mis queridos padres, quienes me orientaron y respaldaron con mucho amor mi educación, haciendo posible mi formación profesional como ingeniero de sistemas e informática.

## PRESENTACION

En los años recientes el uso de las redes de computadoras han crecido de manera asombrosa. Hoy en día, empresas y usuarios que interactúan con el internet, hacen sus compras, pagan sus cuentas o realizan negocios.

El avance que ha tenido la tecnología ha posibilitado que las actividades efectuadas en una entidad se realicen en forma más rápida, y se tenga disponible en las bases de datos del los servidores y en los archivos de los usuarios, información muy importante que pueda ser vulnerada.

Como ya es conocido, las redes entre computadoras se encuentran muy expuesta a los ataques informáticos, por lo cual, es importante contar con mecanismos de seguridad para proteger los recursos informáticos.

En el presente trabajo se hace una recopilación de información sobre los métodos de ataque informáticos, especificando los actores del mismo, que método de ataques existen y cuáles son los mecanismos de prevención frentes a estas amenazas en la red.

## RESUMEN

En la actualidad la detección de ataques informáticos juega un papel muy importante en la seguridad del procesamiento de datos en los sistemas informáticos.

Hay de todo tipo de ataques informáticos que se aprovechan de las vulnerabilidades que los sistemas de información han ido presentando durante estos últimos años, todo esto es ocasionado por personas que poseen conocimientos avanzados de la tecnología y que muchas veces atacan por diferentes ideologías ya sean políticas económicas o religiosas.

Por lo cual es importante crear y establecer políticas de seguridad, además se deben estudiar las herramientas que se utilizan para fortalecer un sistema informático, de los cuales existen varios tipos dependiendo de la seguridad la seguridad que requiere el usuario.

# ÍNDICE DE CONTENIDOS

# ÍNDICE DE FIGURAS

## I. JUSTIFICACION:

En la actualidad, con la masificación del uso del internet para efectuar diversas actividades en una organización, trajo consigo muchos beneficios aportando sustancialmente en el ámbito de la investigación y demás fines, pero adicionalmente a ello aparecieron diversas amenazas, entre ellas la posibilidad que otra persona con ciertos conocimientos de informática pueda causar perjuicio a una organización a través de los diversos ataques informáticos que existen en la actualidad, es por ello que es muy importante conocer los método de ataque informáticos a que estánexpuestos los activos informáticos de una organización, para que apartir de ahí podamos establecer mecanismos que prevengan oen todo caso mitiguen la materialización de dichos ataques, evitando así grandes pérdidas económicas e incluso de prestigios en la entidad.

## II. OBJETIVO

Objetivo general:

Dar a conocer un marco teórico completo referente a los métodos de ataques informáticos, incluyendo clasificación, anatomía y método de prevención para un ataque Informático.

Objetivos específicos:

- Definir los métodos de ataque informático.
- Diferenciar los tipos de ataques informáticos que existen en la actualidad así mismo el papel que desempeñanlos atacantes y cómo actuar frente a ellos.
- Comprender la importancia en la seguridad de la información y saber qué mecanismo de prevención utilizar frente a un tipo específicode ataque Informático.
- Implementar un ejemplo de ataque y defensa informático, vulnerando la seguridad de un sistema operativo.

# III. DESARROLLO DEL TEMA:

## 1. ¿QUE ES UN ATAQUE INFORMATICO?

Un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización.

## 2. CLASIFICACIÓN DE LOS ATAQUES SEGÚN LOS OBJETIVOS:

Planteamos el escenario de una comunicación entre dos o más equipos. Un ataque a un sistema concebido de esta forma se lleva a cabo generalmente por alguno de los siguientes métodos:

### 2.1 Interrupción.

Consiste en que un recurso del sistema es destruido o se vuelve no disponible. Es un ataque contra la disponibilidad de los recursos de sistema. Ejemplos de este tipo de ataque son: la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros.

### 2.2 Intercepción.

En este caso, un usuario no autorizado consigue acceder a un recurso incluso antes del verdadero destinatario. Es un ataque contra la confidencialidad. Cuando hablamos de usuario entendemos que podría ser una Entidad, Organización, persona física, un programa o un ordenador. Ejemplos de este tipo de ataque son:

Hacer click una línea para hacerse con datos que circulen por la red; hacer copia ilícita de ficheros o programas (intercepción de datos), o bien leer las cabeceras de paquetes, para desvelar la identidad de uno o más usuarios implicados en la comunicación ilegalmente intervenida (intercepción de identidad).

2.3 Modificación

El intruso, que así llamaremos a la entidad no autorizada, no solo consigue el acceso a un recurso, sino que es capaz de manipularlo. Este es el caso de un ataque contra la integridad. Ejemplos de este ataque podrían ser: el cambio de valores en un archivo de datos, alteración de un programa para modificar su funcionamiento y corromper el contenido de mensajes que están siendo transferidos por la Red

2.4 Generación

Un usuario no autorizado introduce objetos, elementos, parámetros falsificados en el sistema, originando un ataque contra la autenticidad de los recursos. Ejemplos de este tipo de ataque son: insertar mensajes corruptos en una red, o añadir registros a un archivo.

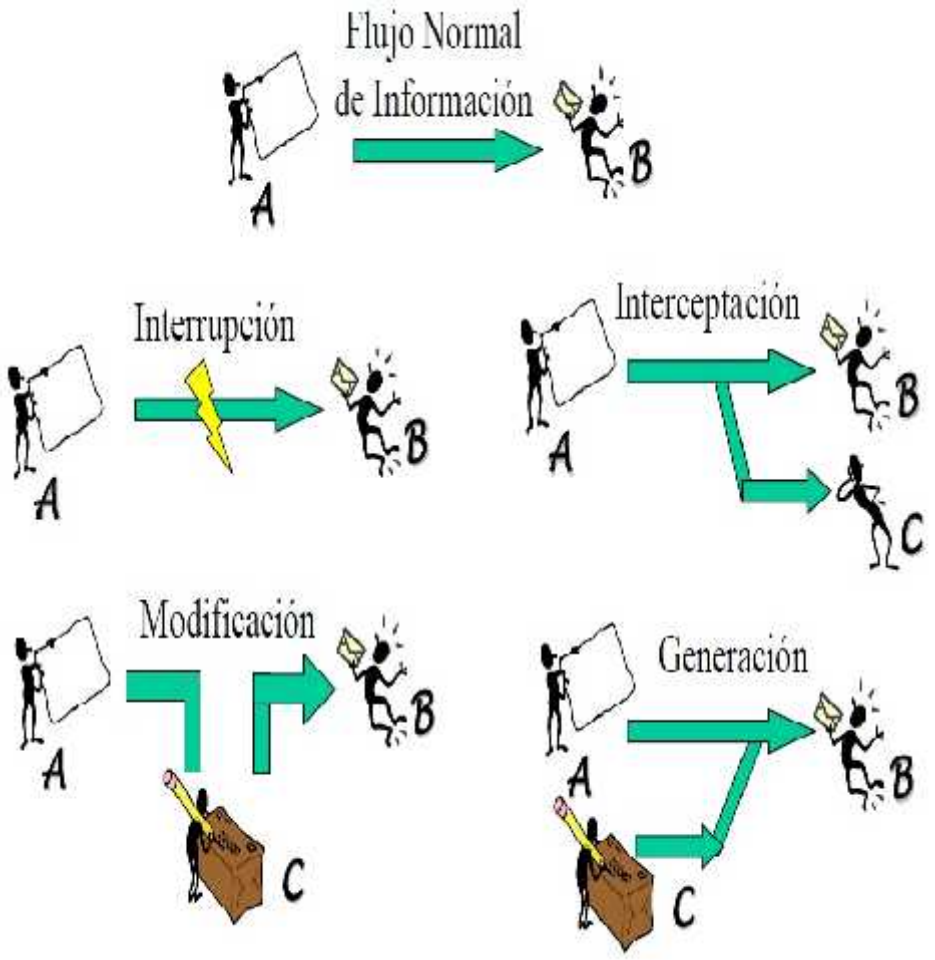


Figura 1: Distintos tipos de ataques en una red de Computadoras

## 3. FASES DE UN ATAQUE INFORMÁTICO

Conocer las diferentes etapas que conforman un ataque informático brinda la ventaja deaprender a pensar como los atacantes y a jamás subestimar su mentalidad. Desde laperspectiva del profesional de seguridad, se debe aprovechar esas habilidades para comprender y analizar la forma en que los atacantes llevan a cabo un ataque.

Fase 1: Reconnaissance (Reconocimiento). Esta etapa involucra la obtención deinformación (*InformationGathering*) con respecto a una potencial víctima que puede ser unapersona u organización.

Por lo general, durante esta fase se recurre a diferentes recursos de Internet como Google, entre tantos otros, para recolectar datos del objetivo. Algunas de las técnicas utilizadas en este primer paso son la Ingeniería Social, el *DumpsterDiving*, el *sniffing*.

Fase 2: Scanning (Exploración). En esta segunda etapa se utiliza la información obtenida en la fase 1 para sondear el blanco y tratar de obtener información sobre el sistema víctima como direcciones IP, nombres de host, datos de autenticación, entre otros.
Entre las herramientas que un atacante puede emplear durante la exploración se encuentra el *networkmappers*, *portmappers*, *networkscanners, portscanners*, y *vulnerabilityscanners*.

Fase 3: Gaining Access (Obtener acceso). En esta instancia comienza a materializarse el ataque a través de la explotación de las vulnerabilidades y defectos del sistema (*Flaw exploitation*) descubiertos durante las fases de reconocimiento y exploración.

Algunas de las técnicas que el atacante puede utilizar son ataques de *Buffer Overflow,* de*Denial of Service (DoS), DistributedDenial of Service (DDos), Passwordfiltering y Sessionhijacking*.

Fase 4: Maintaining Access (Mantener el acceso). Una vez que el atacante ha conseguido acceder al sistema, buscará implantar herramientas que le permitan volver a acceder en el

futuro desde cualquier lugar donde tenga acceso a Internet. Para ello, suelen recurrir a utilidades backdoors, rootkits y troyanos.

Fase 5: CoveringTracks (Borrar huellas). Una vez que el atacante logró obtener y mantener el acceso al sistema, intentará borrar todas las huellas que fue dejando durante la intrusión para evitar ser detectado por el profesional de seguridad o los administradores de la red. En consecuencia, buscará eliminar los archivos de registro (log) o alarmas del Sistema de Detección de Intrusos (IDS).

La siguiente imagenmuestra las cinco etapas por las cuales suele pasar un ataque informático al momento de ser ejecutado:

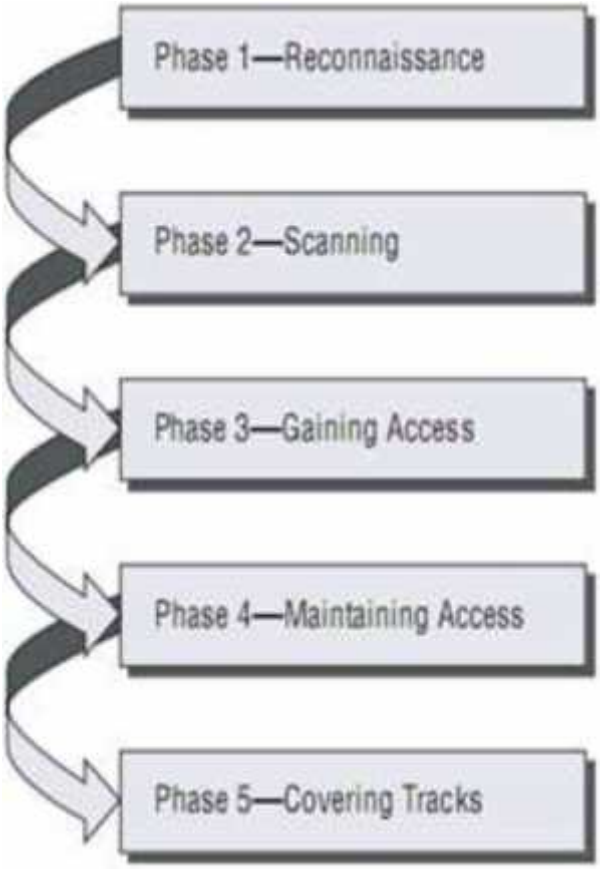


Figura 2. Fases comunes de un ataque informático

# 4. CLASIFICACIÓN DE LOS INTRUSOS EN LAS REDES

## 4.1 Hacker

Los hackers son intrusos que se dedican a estas tareas como pasatiempo y como reto técnico: entran en los sistemas informáticos para demostrar y poner a prueba su inteligencia y conocimientos de los entresijos de Internet, pero no pretenden provocar daños en estos sistemas.

Sin embargo, hay que tener en cuenta que pueden tener acceso a información confidencial, por lo que su actividad está siendo considerada como un delito en bastantes países de nuestroentorno.

El perfil típico de un hacker es el de una persona joven, con amplios conocimientos de informática y de Internet (son auténticos expertos en varios lenguajes de programación, arquitectura de ordenadores, servicios y protocolos de comunicaciones, sistemas operativos, etcétera), que invierte un importante número de horas a la semana a su afición. En la actualidad muchos “hackers” defienden sus actuaciones alegando que no persiguen provocar daños en los sistemas y redes informáticas, ya que sólo pretenden mejorar y poner a prueba sus conocimientos. Sin embargo, el acceso no autorizado a un sistema informático se considera por sí mismo un delito en muchos países, puesto que aunque no se produzca ningún daño, se podría revelar información confidencial.

Por otra parte, la actividad de un “hacker” podría provocar otros daños en el sistema: dejar “puertas traseras” que podrían ser aprovechadas por otros usuarios maliciosos, ralentizar su normal funcionamiento, etc. Además, la organización debe dedicar tiempo y recursos paradetectar y recuperar los sistemas que han sido comprometidos por un “hacker”.

4.2 Crackers (“blackhats”)

Los crackers son individuos con interés enatacar un sistema informático para obtener beneficios de forma ilegal o, simplemente, para provocar algún daño a la organización propietaria del sistema, motivada por intereses económicos,políticos, religiosos, etc.
A principios de los años setenta comienzana producirse los primeros casos de delitos informáticos,provocados por empleados queconseguían acceder a las computadoras de susempresas para modificar sus datos: registros deventas, nóminas.

4.3 Phreakers.

Los phreakers son intrusos especializadosen sabotear las redes telefónicas para poder realizar llamadas gratuitas. Los phreakers desarrollaronlas famosas “cajas azules”, que podíanemitir distintos tonos en las frecuencias utilizadaspor las operadoras para la señalización internade sus redes, cuando éstas todavía erananalógicas.

4.4 Lamers.

Los “lamers”, también conocidos por “script kiddies” o “clickkiddies” , son aquellas personas que han obtenido determinados programas o herramientas para realizar ataques informáticos (descargándolos generalmente desde algún servidor de Internet) y que los utilizan sin tener conocimientos técnicos de cómofuncionan.

A pesar de sus limitados conocimientos, son los responsables de la mayoría de los ataques que se producen en la actualidad, debido a la disponibilidad de abundante documentación técnica y de herramientas informáticas que se pueden descargar fácilmente de

Internet, y que pueden ser utilizadas por personas sin conocimientostécnicos para lanzar distintos tipos de ataques contra redes y sistemas informáticos.

# 5 METODO DE ATAQUES y ESPIONAJE INFORMATICO.

## 5.1 Códigos Maliciosos (Malware)

Los códigos maliciosos, establecen la mayor amenaza de seguridad para cualquier Institución en la cual puede ocasionar destrozos económicos. Dentro de esta categoría se incluyen los programas troyanos, gusanos, xploit, spyware, backdoors, rootkits, keyloggers, entre otros. Los códigos maliciosos se expanden por dos formas, el primero por medio de la llamada ingeniería social ya que en esta opción interviene mucho el engaño a usuarios, y el segundo es por medio de las aplicaciones y dispositivos digitales.

[Mieres, 2009]

## 5.2 Virus Informáticos

Los virus informáticos son como pequeñas aplicaciones creados con la finalidad de ocasionar desastres en nuestros sistemas informáticos, destruyendo o modificando muchas veces la información que tenemos alojado en nuestros sistemas.

Los virus una vez que se instalan empiezan hacer sus funciones por la cual fueron creados.

En un principio solo se transmitan a través de dispositivos removibles, pero con el auge del internet se transfirieron en ficheros y de documentos a través de las redes (principalmente vía correo electrónico). Pueden crear copias de sí mismos, replicar mensajes de correo y en general, dañar los datos y los recursos del sistema atacado.

[Pardo, 1993]

- Características de los virus Informáticos :

Cuando el virus se instala en la computadora, es en ese instante, que se ejecuta y realizan cualquier acción por el cual fue programado, esto lo hace muchas veces sin que el usuario se dé cuenta de este mal.
Los virus que se alojan en los registros de arranque de las máquinas, infectan archivos o se ejecutan cuando se ocupa una unidad de disco o dispositivo de memoria, a estos tipos de virus se les conoce como residentes. Los otros tipos de virus solo realizan acciones cuando el archivo infectado es utilizado.
Todo virus tiene su ciclo de vida la clasifica en tres puntos:

1. Fase de creación: El programador utiliza sus conocimientos para crear el virus.

2. Fase de incubación/propagación: El creador del virus o en muchas ocasiones es el propio virus que hacen una exploración, también es posible que el virus pueda albergar en el ordenador que será infectado y así permanecer en estado de lactancia (suma de retardos temporales en una red), esto se hace con el objetivo de también poder propagarse hacia demás programas o computadoras.

3. Fase de destrucción: Después de que se ha superado las dos fases anteriores procede a ejecutarse y perjudicar los activos o provocar un mal funcionamiento de las tareas de una computadora, todo esto muchas veces hasta llegar a deteriorar por completo los ordenadores.
Los virus informáticos están compuestos de funciones de estructuras o rutinas, estas rutinas componen la base de los virus que tienen dos funciones importantes.

[Marroquí , 2010]

La función de búsqueda y la función de copia, nos platica de esto:

La función de búsqueda consiste en localizar un archivo o un territorio en el ordenador para infectarlo. Según se localice en uno o en otro espacio, el virus será más rápido o más lento, podrá infectar a muchos discos o a uno solo, mientras más complejo sea el mecanismo de búsqueda más espacio ocupa.

La función de copia necesita pasar desapercibido para no ser detectada, y por eso los más pequeños son más efectivos. Un virus que solo afecta archivos COM (ficheros ejecutables), puede obtenerse con una copia más pequeña que las que infecta con archivo EXE (ejecutable), puesto que la estructura de este es más compleja. Con el fin de evitar de ser capturados, algunos virus están dotados de una función de anti detección, que pueden formar parte de las funciones de búsqueda o de copia. Con el fin de burlar los sistemas de detección, los virus pueden activarse solo en ciertas fechas determinadas o a en la unidad de memoria de una computadora y desde allí operan sus acciones.

1. Virus residentes: Albergan en la unidad de memoria de una computadora y desde allí operan sus acciones.

2. Virus de acción directa: Van haciéndose copias de ellos mismos.

3. Virus de sobre escritura: Se sobrescriben en el interior de los archivos atacados.

4. Virus boot: Estos atacan particularmente a los discos duros de la computadora.

5. Virus Macro: Infectan a archivos de escritura como archivos de texto, base de datos o presentaciones.

## 5.3 Bombas Lógicas

Una bomba lógica es un programa con un conjunto de instrucciones, para que en un tiempo determinado se ejecuten automáticamente desencadenando el borrado o la destrucción de información almacenada en el computador, distorsionando el funcionamiento del sistema o paralizaciones intermitentes.

Este tipo de ataques son retardados en tiempo para hacerse funcionar, pues primero entran a la red y después para activarse pasan cierto tiempo para que hagan su efecto y destruyan parte de un sistema.

[Beekman, 1998]

## 5.4 Captura de Cuentas y Contraseñas

Es posible reemplazar la identidad de clientes o usuarios, esto se hace mediante diferentes herramientas que permitan apresar sus contraseñas, Tal como los programas de software espía o los dispositivos hardware especializado que permitan registrar todas las pulsaciones en el teclado. Entre estos están:

### 5.4.1 Caballo de Troya

> Caballo de Troya es denominado así en recuerdo del regalito que Ulises le hizo a los troyanos por aquel asunto de Helena, que tanto dio que hablar.
>
> Es un programa que disimula su efecto negativo en programas aparentemente inofensivos. Este también puede estar compuesto por un virus incorporado a un programa normal.
>
> [Royer, 2004]
>
> Son programas que realizan cualquier acción común a la cual aparentemente es normal y no dañina, pero al mismo tiempo ejecuta tareas destructivas, por lo general las bombas lógicas se encuentran en anuncios de noticias de dominio público con nombres de juegos información cultural entro otros.
>
> [Beekman, 1998]
>
> Los males que incorporan los troyanos son tareas destructivas para el disco duro que viene ocasionando la eliminación de archivos, copia de las pulsaciones del teclado, monitora el trafico de la red, hasta pueden monitorear los mensajes que enviamos y recibimos.
>
> Los troyanos por simple apariencia son inofensivos, pero tiene dos caras ya que cuando ejecutamos la aplicación se instalaran en la computadora el programa que es en realidad y el cual causara destrozos en nuestras maquinas.

Los ataques troyanos funcionan como los virus normales de una computadora, a diferencia que este no se reproduce.

Es muy fácil pero a la vez muy complejo como actúan estos programas, los troyanos proceden como un servidor alojado en la máquina de la víctima. Cuando la víctima se conecte a Internet, el troyano actuara informando al creador del troyano de que la víctima se encuentra en línea.

Posteriormente el atacante enviara ordenes para hacer un control remotamente, su principal objetivo es robar información confidencial.

Los ordenadores controlados se denominan zombies, el cual es un equipo que está infectado y permite que el equipo pueda ser utilizado por otro.

En resumen un programa troyano tiene como objetivo abrir un puerto de red o puede cumplir la función parecida a la de un servidor, el cual estando oculto, el pirata puede tomar el control de la máquina. Entre los programas que son sub categorías de los programas troyanos se encuentran los conocidos espías Keylogger, que se encargan de transmitir la información por medio del teclado.

[Marañón, 2009]

### 5.4.2 keylogger

Es un programa que registra en secreto los golpes de tecla de un usuario y los envía a un hacker. Es una forma de código malicioso llamado caballo de Troya o troyano.

Un keylogger es un software que se encarga de vigilar y de registrar en un archivo cada pulsación de teclado. Un keylogger tiene la capacidad registrar mensajes de correos electrónicos, y de cualquier información escrita en cualquier ocasión durante la utilización del teclado. El archivo creado por el keylogger puede ser enviado a un receptor especificado. Algunos programas también registran cualquier dirección de correo electrónico usada y las direcciones urls (Localizador de Recurso Uniforme) que se visitan.

Los keyloggers los podemos clasificar en dos tipos: en hardware y software, los keyloggers hardware son los que se encuentran entre la computadora y el teclado y registran la actividad de éste en la memoria interna. Los keylogger hardware están diseñados para trabajar con cualquier tipo de teclados. Los programas o software keylogger se puede utilizar, para iniciar ciertos programas mediante combinaciones de teclas. Se pueden encontrar en cualquier tipo de programas que están en la red, al igual estos también pueden ser de ayuda para los administradores de redes, pues pueden saber que están haciendo sus empleados en sus horas laborales.

Hoy en día los keyloggers se usan principalmente para robar información relacionada a varios sistemas de pago en línea.

Existen novedosos keylogger que suelen comunicar el archivo autentificado a una cuenta de correo electrónico mediante Internet. Esto generalmente se consigue de ciertas formas que a continuación se presentan.

1- Por el envío de correo electrónico del archivo autentificado, esto se hace en cada cierto número de horas.

2- Envío de correo electrónico del archivo autentificado cada cierta cantidad de bytes.

3- Transmitido por FTP cada cierto tiempo.

4- Envió de las contraseñas a una paginaphp que los guarda y más tarde pueden ser visualizados.

[Parsons , 2009]

### 5.4.3 Spyware

Un spyware como “un tipo de programa que recopila en secreto información personal sin conocimiento de la víctima, por lo general para propósitos de publicidad y comerciales”. Una vez que esté instalado el programa comienza a vigilar el comportamiento de navegación y de compras en la web, después envía un tipo informe a otra computadora que manipula dicho programa.

[Parsons, 2009]

En un artículo Enter@te (2012) muestra diferentes casos de spyware. Por ejemplo, en el 2005 un periodista americano descubrió después de haber instalado un juego de la empresa de juguetes Mattel en la computadora de su hija, una pieza de software conocida como “Broadcast” que sin saberlo conectaba directamente la computadora de su hija hacia el servidor Web de Mattel, hecho que la compañía señala que se hacía únicamente con el propósito de proporcionar software de seguridad a sus usuarios. Como consecuencia de este suceso, algunos grupos de defensa de las garantías individuales y los derechos de la privacidad alrededor del mundo, señalaron que el software de Mattel contenía capacidades técnicas adicionales que permitían invadir de manera flagrante los derechos de privacidad de los usuarios. Otro curioso hecho que tiene que ver con spyware y la interceptación de comunicaciones electrónicas, sucedió en el año 2005 donde se suscito un problema cuando la esposa de un señor con domicilio en el estado de Florida, instaló un programa spyware de nombre “Spector” en la computadora de su esposo a sabiendas de que este último le era infiel, con el objeto de poder intervenir y conocer las comunicaciones que su esposo realizaba con la susodicha y, de esa forma, tener pruebas suficientes para solicitar la disolución del vínculo matrimonial. Los atacantes suelen utilizar troyanos de manera combinada junto a otros tipos de códigos maliciosos. Si bien cualquier persona con conocimientos básicos de computación puede crear un troyano y combinar su virus con

programas benignos a través de aplicaciones automatizadas y diseñados para esto, los troyanos poseen un requisito particular que debe ser cumplido para que logren el éxito, necesitan la intervención del factor humano, en otras palabras, tienen que ser ejecutados por el usuario.

Este tipo de ataques se riegan por medio de diferentes tecnologías como las dispositivos de memoria, correos electrónicos, mensajes instantáneos, aparentando ser inofensivos, puesto que se esconden en programas como juegos, tipos de archivos o cualquier otra aplicación, en realidad no ocasionan daños en nuestro ordenador pero si, en nuestra privacidad como usuarios, ya que es como si tuviéramos a alguien a las espaldas observando que actividades realizamos.

## 5.5 Fraudes Engaños y Extorsiones

El delito informático es un acto ocasionado por un ser humano, que causa un daño a otra persona, a veces sin que le traiga algún beneficio, es un fraude como “cualquier acción encaminada a eludir las disposiciones legales, siempre que con ello se produzca un perjuicio contra el estado o terceros.”

[Da Costa, 1992]

Los fraudes y estafas financieras a través de internet se han hecho muy frecuentes en estos últimos años. Existe un gran numerode ataques queriendo extorsionar nuestras cuentas bancarias o información personal,entre los las utilizados se encuentran:

### 5.5.1 Spam

> El spam también conocido como corroe basura, estos correos suelen ser no solicitados y su contenido puede variar, se envían de forma masiva.
>
> Suelen proceder de remitentes desconocidos o de direcciones conocidas pero que han sido suplantadas. El contenido del mensaje puede ser de toda índole como de anuncios publicitarios de bancos, empresas privadas y en ocasiones políticos, se envían en cadenas o incluso falsos spam destinados a introducir malware (cuando lleva un archivo adjunto) o a robar información confidencial.
>
> [Gris, 2010].

Estas cadenas de correos inundan de correos electrónicos indeseados porque a veces hasta pornografía se suele encontrar en estos mensajes. Esta es una herramienta muy utilizada por los cyberdelicuentes, pues ya no solo se envían anuncios publicitarios para engañar a la gente para que ingrese sus datos, sino que ahora se pueden enviar correos con virus, troyanos, bombas lógicas entre otros ocasionando destrozos en las computadoras. Aunque los filtros antispam han ido mejorando, este mal sigue siendo un dolor de cabeza para cualquier organización o para un simple usuario.

### 5.5.2.Phishing

El Phishing consiste en el envío de mensajes (anzuelos) a una o varias personas, recurriendo a la suplantación de la identidad de una empresa o entidad pública con el objetivo de persuadir a la futura víctima para revelar sus datos personales o financieros que involucran nombres de usuario y contraseñas. Una vez obtenida esta información es utilizada con fines maliciosos para realizar acciones como transferencias de fondos a cuentas bancarias y

compras con tarjetas de crédito entre otras acciones delictivas que afectan económicamente a la víctima.

En la actualidad la actividad de phishing utiliza principalmente el correo electrónico enviando correos falsos por parte del atacante. En estos correos se solicitan contraseñas o detalles de las cuentas bancarias argumentando comúnmente situaciones como problemas técnicos, procesos de actualización y revisión de datos buscando aprovecharse de la ingenuidad de los usuarios para obtener información. En algunos casos se emplean técnicas más sofisticadas como el uso de sitios web falsos, instalación de caballos de Troya, key-loggers, screen-loggers, envíos de mensajes de SMS, mensajes en contestadores automáticos y llamadas telefónicas.

Se define como “un robo de identidad digital para obtener un lucro indebido. Se trata de un cyberataque en el cual un atacante se hace pasar por una compañía o institución financiera de reconocido prestigio, enviando mensajes habitualmente através de correo electrónico o en documento en Word o pdf”.

[Álvarez ,2009]

El objetivo es obtener los datos, cuentas bancarias, número de tarjeta de crédito, identidades, de un usuario para usarlo con fines fraudulentos.

[Romero, 2010]

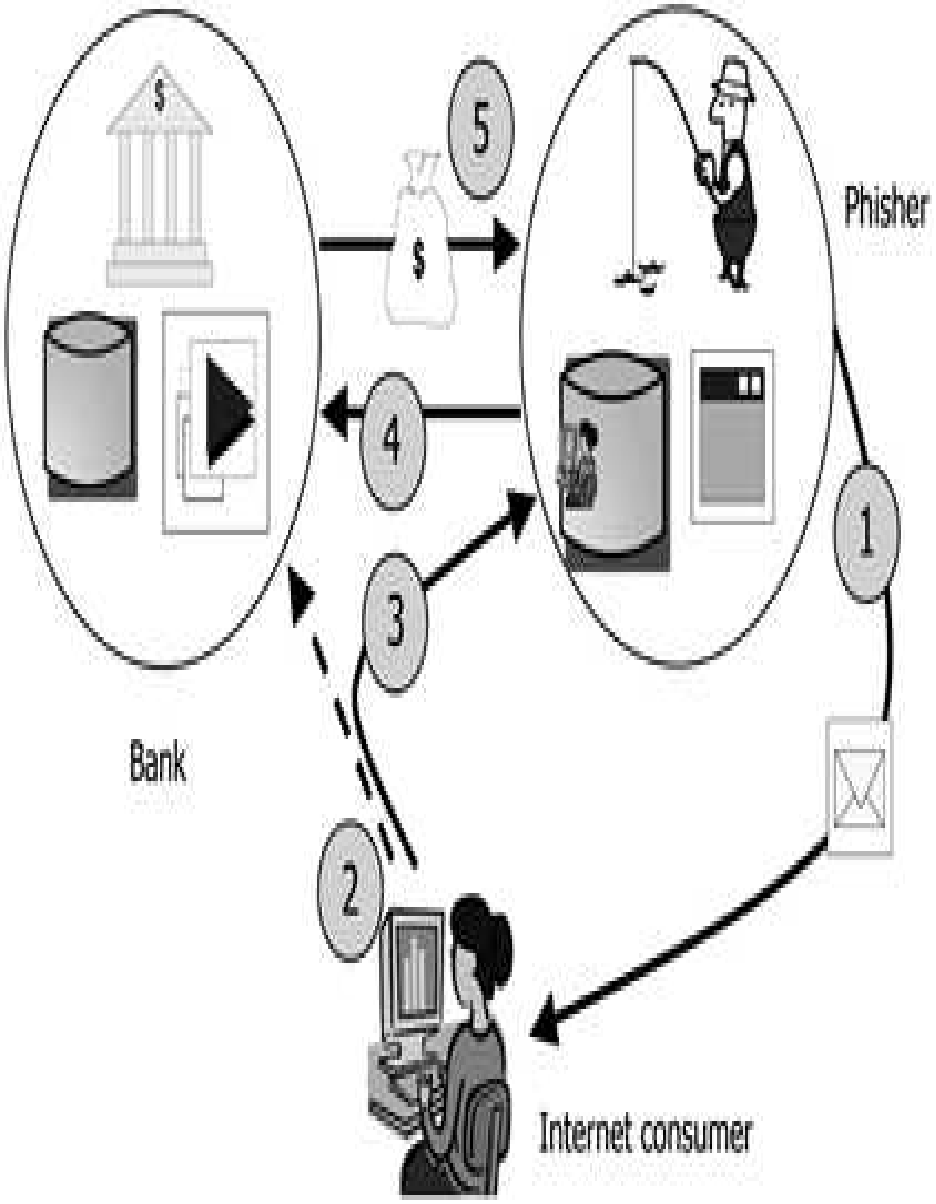


Figura 3: fases de Phishing

### 5.5.3 Pharming

El pharming consiste en manipular direcciones DNS para engañar al usuario y cometer fraude.
Para entender mejor y con mayor claridad el pharming, debemos entender exactamente en qué consiste la manipulación de las direcciones DNS.
Cuando se teclea una dirección web determinada (URL) en el navegador de Internet, para poder acceder a ella, esta URL debe convertirse a la dirección IP real de la página que se quiere visitar.

El formato IP es: 000.000.000.000.

Obviamente, esto se hace porque sería extremadamente complejo poder recordar secuencias de números que identificasen todas las webs que visitamos. Por lo tanto, es más sencillo escribir en nuestro navegador, por ejemplo, www.cajamadrid.es, y luego convertirlo a la numeración correspondiente a su IP real. Ahora bien, normalmente el navegador no puede realizar esta conversión, por lo que se necesita un servidor DNS para que realice esta acción.A modo de ejemplo, al teclear cajamadrid.es estamos enviando este nombre a un servidor DNS.

Éste tiene un registro que administra esos nombres y les otorga su correspondiente secuencia numérica, para conducir finalmente al usuario a la página deseada.

El pharming realiza su ataque sobre estos servidores DNS. Su objetivo es cambiar la correspondencia numérica a todos los usuarios que lo utilicen. Al

cambiar esta correspondencia, usted escribe en su navegador cajamadrid.es, pero el DNS le otorga otra correspondencia numérica distinta a la original y real, llevando al usuario a una página idéntica a la de cajamadrid, pero que en realidad ha sido creada por los delincuentes. A partir de aquí, el usuario ve en su navegador que está en www.cajamadrid.es y realiza sus movimientos con total tranquilidad. El delincuente informático tan sólo tiene que utilizar las claves que el usuario escribe.

Otro tipo de pharming, aún más peligroso y efectivo es el que se realiza a nivel local, es decir, en cada equipo individualmente. Tan sólo es necesario modificar un archivo denominado “HOSTS”, y que contiene cualquier ordenador que funciona bajo el sistema operativo Windows y que utilice Internet Explorer para navegar por Internet.

El fichero hosts actúa de tal forma que no es necesario acceder al servidor DNS para reconducirnos a la web deseada. Éste almacena una pequeña tabla con las direcciones de servidores y direcciones IP que más suele utilizar el usuario.

Al modificar este fichero, por ejemplo, con falsas direcciones de bancos online sucederá como en el caso anterior, es decir, en el navegador se escribirá el nombre, pero nos enviará a una página que no corresponde con la real.

Suponemos que a estas alturas la pregunta que nos formulamos todos es: ¿Cómo modifica una tercera persona en un ordenador personal un fichero concreto? Esto puede hacerlo directamente el delincuente entrando en el ordenador de forma

remota a través de alguna vulnerabilidad del sistema, o bien mediante un código malicioso (virus o troyanos). Algunos ejemplos de troyanos reconocidos con la capacidad de realizar estos cambios en el fichero hosts son los de las familias Bancos, Banker o Banbra. Estos troyanos suelen ser malwares disfrazados que suelen esconderse en ficheros adjuntos, o bien se descargan al acceder a páginas falsas creadas con este objetivo.

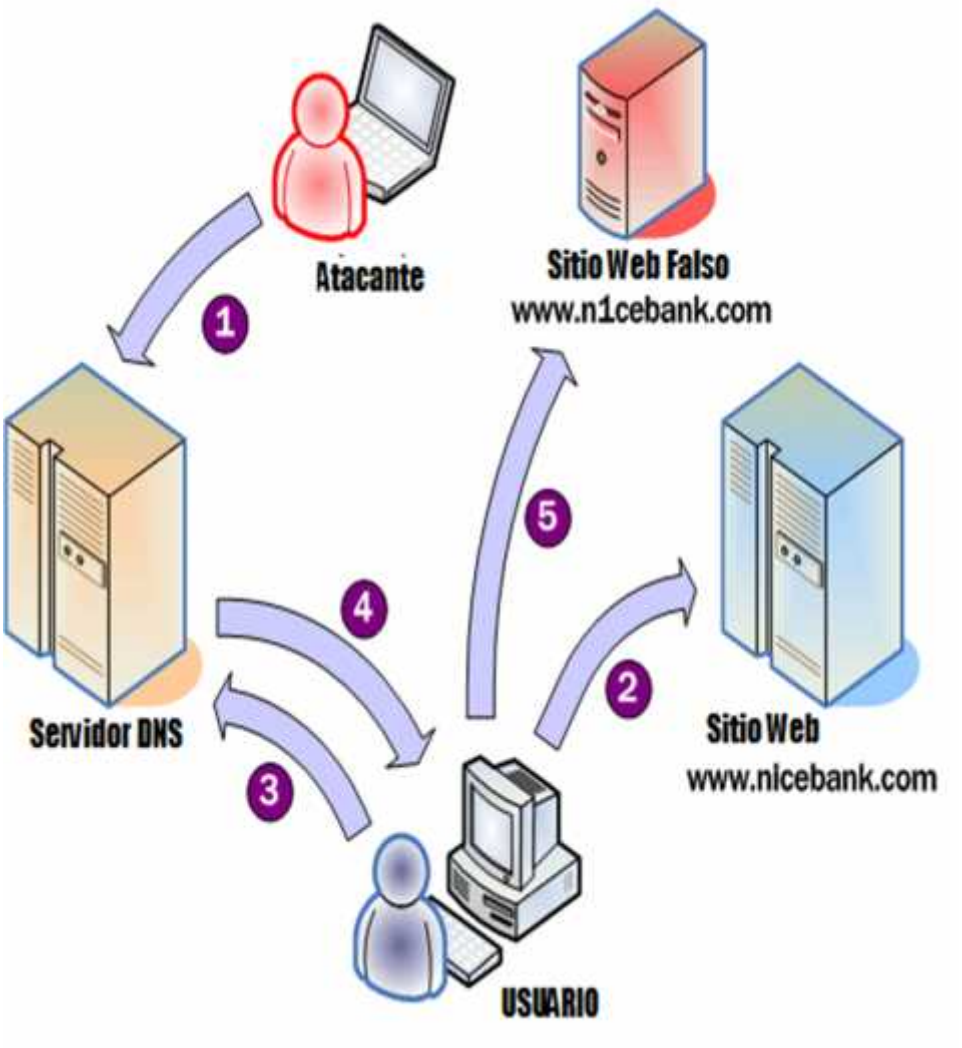


Figura 4 : fases de Pharming

## 5.6 Inyección SQL

Inyección SQL es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar consultas a una base de datos.

El origen de la vulnerabilidad radica en el incorrecto chequeo y/o filtrado de las variables utilizadas en un programa que contiene, o bien genera, código SQL. Es, de hecho, un error de una clase más general de vulnerabilidades que puede ocurrir en cualquier lenguaje de programación o script que esté embebido dentro de otro.

Se conoce como Inyección SQL, indistintamente, al tipo de vulnerabilidad, al método de infiltración, al hecho de incrustar código SQL intruso y a la porción de código incrustado.

Se dice que existe o se produjo una inyección *SQL* cuando, de alguna manera, se inserta o "inyecta" código SQL invasor dentro del código SQL programado, a fin de alterar el funcionamiento normal del programa y lograr así que se ejecute la porción de código "invasor" incrustado, en la base de datos.

Este tipo de intrusión normalmente es de carácter malicioso, dañino o espía, por tanto es un problema de seguridad informática, y debe ser tomado en cuenta por el programador de la aplicación para poder prevenirlo. Un programa elaborado con descuido, displicencia o con ignorancia del problema, podrá resultar ser vulnerable, y la seguridad del sistema (base de datos) podrá quedar eventualmente comprometida.

La intrusión ocurre durante la ejecución del programa vulnerable, ya sea, en computadores de escritorio o bien en sitios Web, en éste último caso obviamente ejecutándose en el servidor que los aloja.

La vulnerabilidad se puede producir automáticamente cuando un programa "arma descuidadamente" una sentencia SQL en tiempo de ejecución, o bien durante la fase de desarrollo, cuando el programador explicita la sentencia SQL a ejecutar en forma desprotegida. En cualquier caso, siempre que el programador necesite y haga uso de parámetros a ingresar por parte del usuario, a efectos de consultar una base de datos; ya que, justamente, dentro de los parámetros es donde se puede incorporar el código SQL intruso.

Al ejecutarse la consulta en la base de datos, el código SQL inyectado también se ejecutará y podría hacer un sinnúmero de cosas, como insertar registros, modificar o eliminar datos, autorizar accesos e, incluso, ejecutar otro tipo de código malicioso en el computador.

## 5.7 Denegación del Servicio (Denial of Service)

Este ataque es una agresión a un sistema o red que causa la pérdida de servicio a los usuarios, típicamente la pérdida de conectividad con la red consumiendo el ancho de banda o sobrecargando los recursos del sistema de la víctima. Principalmente se inhabilitan las funciones de un equipo en la red, se puede utilizar un sin fin de herramientas, llegando a afectar a equipos y servicios muy sofisticados.

[Corrales, 2006]

Es un tipo de ataque se produce cuando un atacante intenta ocupar la mayoría de los recursos de una red, esta puede ser inalámbrica, impidiendo a los usuarios legítimos de esta, disponer de dichos servicios o recursos. Por lo cual se suele modificar parámetros del estándar que permitan enviar mensajes sin ni siquiera esperar los intervalos necesarios no importa que no se procesen en el destino, el ataque consiste en bombardear la red y hacerla inaccesible.

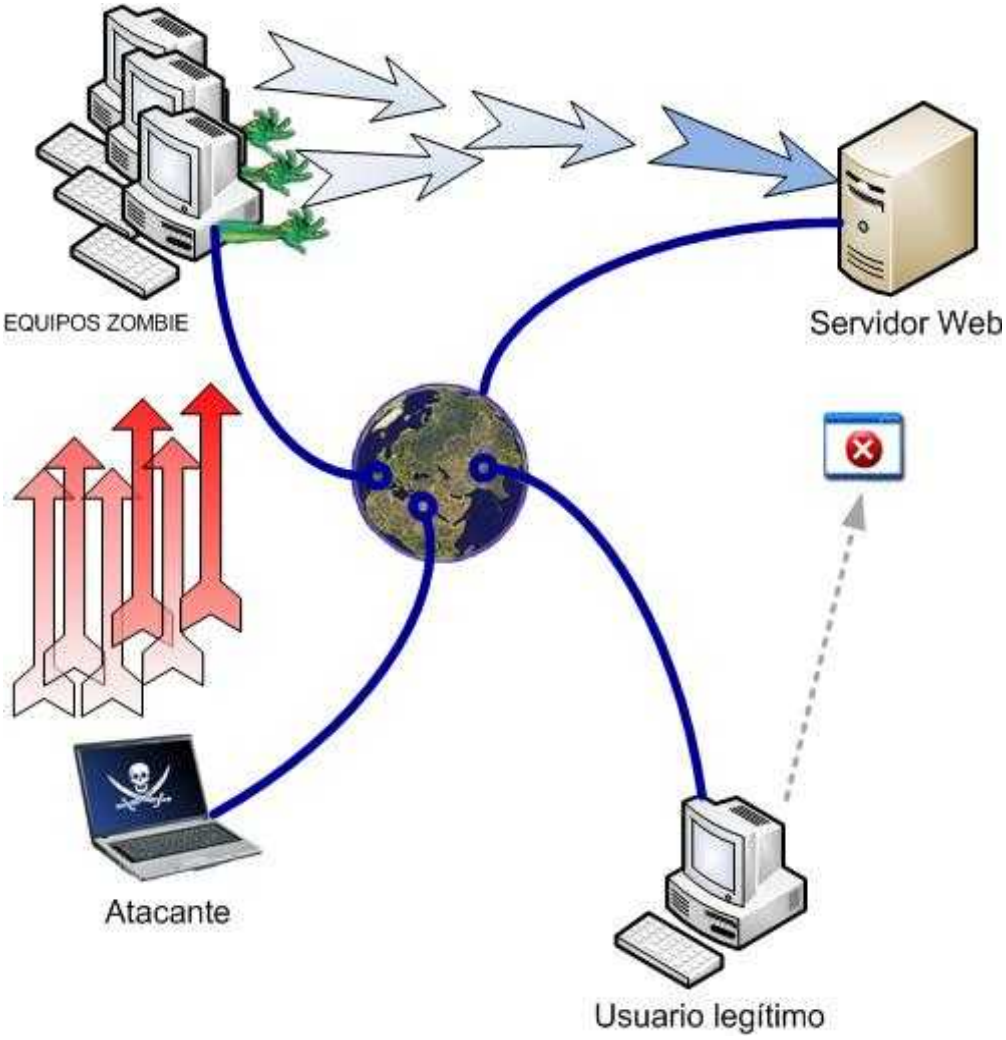


Figura 5 : fases de Denegación de Servicios

A continuación se realiza una clasificación de los ataques de denegación de servicio atendiendo al tipo de objetivo elegido. Para cada uno de ellos se detallaran los mecanismos que pueden ser efectuados por el atacante para llevar a cabo el ataque. Por lo cual los ataques se pueden categorizar dentro de los siguientes tipos.

• Ataques de vulnerabilidad:

Consiste en la transmisión de paquetes, construido y dirigido hacia algún sector, aprovechándose de las vulnerabilidades del servicio obteniendo como consecuencias dañar el servicio que se presta.

• Ataques de protocolo:

En este ataque se aprovecha de las vulnerabilidades de un protocolo, se inunda de paquetes a los protocolos. Si la víctima tiene algún servicio activado que requiere más tiempo para procesar una petición que el que implica la generación de dicha petición, el atacante puede utilizar dicha asimetría. Esto también es aplicable a los casos en los que el servidor tiene que reservar un recurso limitado para atender a la petición, mientras que la generación de la misma no implica la reserva de ningún recurso.

• Ataques a un recurso físico:

Se puede realizar un ataque contra un recurso físico específico de una maquina, como por ejemplo su CPU, memoria, capacidad de conmutación de un encaminado.

• Ataques de aplicación:

El intruso toma alguna aplicación determinada como su posible víctima, y este le transmite paquetes que exponen ciertos fallos de modo que la aplicación deje de operar ya sea temporalmente o totalmente. Es parecido a los anteriores ataques ya mencionados,

pues se inunda la red con tráfico de paquetes hasta que alcance el límite de peticiones de servicio que sea capaz de procesar.
Las formas de ataques dos más comunes son las siguientes:
Radio Jamming: Interferir el espectro con una señal de alta potencia inhabilitando que el usuario legitimo acceda al servicio.
Wirelles Dos: Es inherente al protocolo IEEE 802.11. Como las tramas de gestión no están protegidas por privacidad, autenticación e integridad.

## 5.8 Ingeniería Social

Existen estrategias de ataque que se basan en el engaño y que están netamente orientadas a explotar las debilidades del factor humano: la Ingeniería Social. Los atacantes conocen de esta metodología y lo integran como una herramienta para realizar sus ataques.
Esta técnica es muy utilizada en diferentes campos pero a lo que se refiere en la tecnología, se utiliza mucho en la obtención de información confidencial de un usuario que tenga accesos a los sistemas de información de una organización, jugando muchas veces con características psicológicas del ser humano.
Las persona es el problema más importante de seguridad para cualquier entidad, pues son estas las que manejan los sistemas tecnológicos, son los que tienen acceso a la información, son los creadores de virus y son el único elemento dentro de un entorno seguro que es capaz de irrumpir con las reglas establecidas en las políticas de seguridad.

La inseguridad empieza desde adentro de una organización pues un ataque para que tenga éxito depende muchas veces de los mismo colaboradores dentro de una entidad, puesto que ya sea por su ignorancia o indolencia puede ser la primera entrada para que las amenazas en principio se conviertan en daños y perdidas. Es por eso que es muy importante a considerar los puntos de confianza, capacitación y responsabilidad, ya que

asegurando estos puntos se empieza dando un primer paso muy importante en lo que se refiere a la seguridad.

[Meires, 2009]

Las formas de ataques por medio de la ingeniería social más usadas a nivel físico según Sandoval (2011) son:

- Ataque por teléfono. El intruso comienza haciendo una llamada telefónica, a otra persona en este caso será la víctima, haciéndose pasar por otro, ejemplo como un técnico de soporte o un empleado de la misma organización.
  Es un método muy efectivo pues la conversación se hace por voz y no de manera presencial por lo cual no podemos ver físicamente los estados de ánimo de las persona.

- Ataque vía Internet. Desde que empezó a tener más auge el internet se ha convertido en uno de los medios de comunicación más importantes, los servicios por este medio aumentaron, por lo cual los ataques también se elevaron. Los ataques que más se realizan son por medio del servicio de correo electrónico, se fomenta mucho el phishing esto es para obtener información privada de usuarios, también es común mandar archivos infectados que dañan a nuestro ordenadores y por ultimo también lo hacen por vía web suplantando la identidad de esta ultimas.

- DumpsterDivingo Trashing (zambullida en la basura). Consiste en buscar información relevante en la basura, como: agendas telefónicas, organigramas, agendas de trabajo, unidades de almacenamiento (CD's, UBS, etc.).

- Ataque vía SMS. Funciona por medio de mensajes hacia celulares, los contenidos de estos mensajes son de promociones o de servicios, si es que la persona cae en estos

engaños suele ingresar información relevante y por ende puede ser víctima de robos.

- Ataque vía correo postal. Se envían correos falsos como son suscripciones a revistas, periódicos, invitación de obtención de tarjetas de crédito, cupones de descuento entre otros. En estos mensajes también contienen secciones donde el usuario debe de ingresar sus datos personales para que sea efectivo.

- Ataque cara a cara. Los que llevan a cabo estos ataques deben de ser personas que tengan conocimientos en cuestión de habilidad social y para manejar cualquier situación que se les presente. Tiene talento para el engaño y para saber persuadir a las personas. Por lo que las personas más susceptibles suelen ser las más inocentes

## 6. - HERRAMIENTAS DE PREVENCION

Tiempo atrás las redes de las computadoras se utilizaban solo para el envío de correos electrónicos y para compartir recursos como carpetas de archivos o impresoras. Por lo cual el peligro era mínimo y no se contaban con muchos mecanismos para proteger sus redes, hoy en día esto no es así, pues con la sistematización de toda la información, los mecanismos de seguridad se han vuelto en una prioridad.

Lo primordial de los mecanismos de seguridad es fortalecer la confidencialidad, integridad y la disponibilidad de un sistema informático.

En una manera sencilla de explicar cómo funciona la seguridad informática es de qué se ocupa de garantizar que los usuarios no puedan leer o modificar mensajes dirigidos a

otros destinatarios. También se ocupa de mecanismos para verificar que el mensaje supuestamente enviado sea para el destinatario correcto.

Son mecanismos de seguridad son todo aquello de naturaleza hardware como software que se utiliza para crear, reforzar y mantener la seguridad informática, este mismo autor clasifica a los mecanismos de seguridad en:

- Mecanismos lógicos: En donde se encuentran barreras de software como lo es los cortafuegos, antivirus, antispam, encriptación de la información .

- Mecanismos hardware o físicos: En donde se vigila o resguarda la protección de los componentes físicos como lo es el control de acceso físico al sistema, controles de acceso con identificación, controlar la temperatura y humedad dentro de la habitación donde se encuentran los equipos informáticos.

Según las funciones de los mecanismos de seguridad los clasifica en:

• Preventivos: Actúan antes de que se produzca un ataque

• Detectores: Evitan que el ataque que se ha producido no cause muchos o ningún daño a los sistemas.

• Correctores: Se ejecutan después de que se haya realizado un ataque y se produzcan los daños de estos. Entonces trata de recuperar a un estado anterior antes de que se hayan desarrollado la amenaza.

La elección de mecanismos de seguridad depende de cada sistema de información, de su función, de las posibilidades económicas, de la organización y de cuáles son los riesgos a los que está expuesto el sistema. A continuación se presentaran una serie de herramientas o mecanismos que se utilizan para combatir cualquier tipo de ataques informáticos.

## 6.1 Criptografía

Este mecanismo protege a cualquier tipo de archivos de datos mediante la utilización del cifrado y códigos en la escritura. Por lo cual se trata de mantener en secreto cualquier información importante.

La criptografía como la herramienta automatizada más importante con diferencia para la seguridad de redes de comunicaciones.

[Stalling, 2004].

La criptografía hace posible que se envie información a través de las redes y que esta al mismo tiempo no pueda ser leídas por cualquier persona salvo el destinatario

[Villacorta, 2005].

## 6.2.- Cortafuegos

El cortafuego es un tipo de software que nos ayuda a proteger nuestros sistemas de intrusos que pretenden causar daños a nuestras computadoras.

El cortafuego como: “un sistema de seguridad desarrollado para ubicarse entre una red pública, que generalmente es el internet, y en una red interna perteneciente a una organización, o bien entre diferentes secciones de una red interna” .

El cortafuego está compuesto de una colección de elementos (equipos y programas), que controlan y filtran el tráfico entre las dos redes autorizando o impidiendo su tránsito de una a otra.

*¿Cómo funciona un Cortafuegos?*

Un firewall es una barrera que protege a todo sistema de cualquier código maliciosos o paquete sospechosos que provenga de la red y que infecte nuestros puertos de comunicación.

El firewall decide qué paquetes deben pasar y cuáles deben ser bloqueados. Muchos tipos de firewalls son capaces de filtrar el tráfico de datos que intenta salir de nuestra red al exterior, evitando así que los diferentes tipos de código malicioso como caballos de Troya, virus y gusanos, entre otros, sean efectivos.

El cortafuegos actúa como un mediador entre un equipo de computo y las redes a las cual está conectado, en este caso sería el internet, depurando el trafico de la red que va hacia ese sistema de computo. Es sabido que la comunicación que se da con el internet es el constante intercambio de paquetes de datos, las direcciones ip (protocolo de internet) y los puertos de comunicación juegan un rol muy importante pues cada paquete que se transmite debe llevar anexado este protocolo, pues así la información que se envié llegara a su correcto destino. Es importante especificar que son los puertos de comunicación, pues son como la puerta de entrada y salida de toda información que se envía entre una computadora y sus diferentes periféricos esto a través de la red.

Sabiendo cómo funciona la comunicación en internet es en donde el cortafuegos juega un rol importante, ya que obstaculiza cada uno de los paquetes que tienen como destino un equipo de computo, siendo este la primera barrera de escaneo antes de que algún otro servicio lo utilice, por lo cual es un tipo de controlador de comunicaciones a través del internet.

Los cortafuegos se encuentran tanto en software como en hardware. Los cortafuegos de software que están más orientados a simples usuarios, es aparentemente fácil de instalarlos pues solo se instalan en cada computadora. En cambio los de hardware son dispositivos externos que se conectan entre la computadora y la red, con un solo cortafuegos hardware se pueden proteger varios ordenadores que compartan la conexión a Internet. Hoy en día muchos de los routers se pueden utilizar como cortafuegos.

Como funciona un cortafuegos

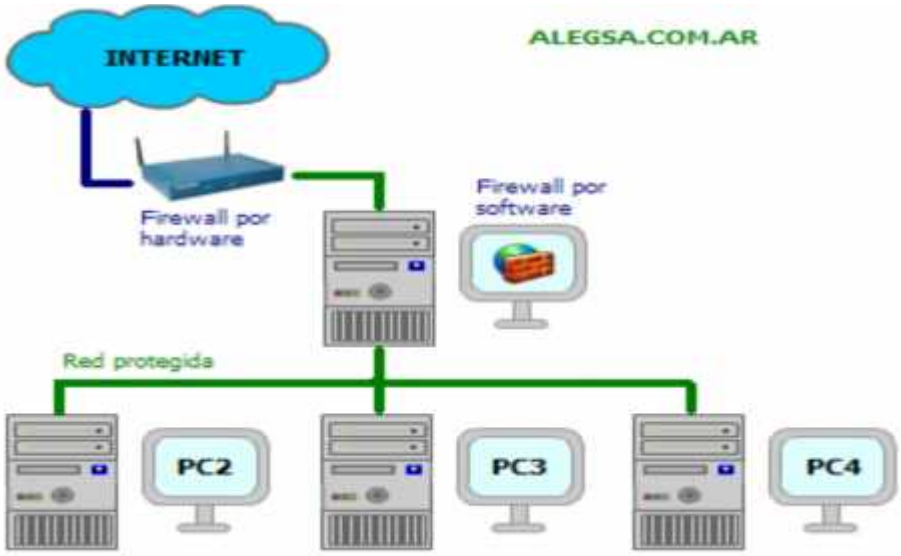


Figura 6: Como funciona un cortafuegos

> El cortafuego es una especie de vigilante de cada puerto de entrada y salida de una computadora. Cada vez que cierto paquete intente entrar o solicitar el paso por medio de un protocolo, el cortafuegos revisa si la información es auténtica y no es dañina para algún sistema.
>
> [Caprani ,2006]
>
> Por lo cual el cortafuego constituye la primera vía de comunicación hacia el internet y redes locales que se tenga acceso. Se encarga de el transporte de datos, solo tenga una solo vía de comunicación permitiéndose así documentar cuando y de qué forma se ha enviado o recibido un determinado tipo de información.
>
> [Dembowski, 1999].

### 6.3.- Anti-spam

El antispam como el mismo nombre lo dice, es un mecanismo el cual ayuda a contrarrestar el spam (correo basura). Es una herramienta muy común que es utilizado por la mayoría de los administradores de red, para salvaguardar el correo electrónico.

El antispam es un software que filtra los mensajes no solicitados o sospechosos de los correos electrónicos, antes de que estos lleguen al buzón, funcionan al inspeccionar los datos del encabezado y el contenido en base a unos métodos.

Como anteriormente se ha visto el spam es empleado, por lo general para el envío de publicidad y avisos de cualquier servicio, aunque también se usa en la propagación de códigos maliciosos como son los virus. Además de los riesgos que representa el spam por el envío de contenidos dañinos, y por la molestia que causa al usuario recibir publicidad no deseada

> La finalidad de esta herramienta es detectar todo aquel correo no solicitado y la mayoría de las veces mal intencionado, de la bandeja de entrada de los correos electrónicos, pero también debe de ser capaz de identificar cuales correos son de nuestro interés y permitirles la entrada a nuestra bandeja. Utiliza muchas técnicas para filtrar los mensajes, entre estas están la utilización de diccionarios, los cuales son consultados para detectar que parámetros o palabras son las que suelen coincidir en un spam, de igual forma el usuario puede configurar manualmente al diccionario con palabras claves que ayuden al cortafuegos a identificar más rápido los correos que no son del interés de este. Otra técnica se basa en la lista de confianza, es decir existen listas llamadas negras y blancas, en la cual las listas blancas se encuentran todas las direcciones de correo que son de confianza, interés y que siempre se desea recibir correos, del otro lado están las listas negras en las cuales se almacena todo tipo de remitente de correos que sea de dudosa procedencia o que sean
>
> [Jamrichoja ,2008]

## CONCLUSIONES

- Conocer el concepto exacto de un ataque informático.

- Se define los tipos de ataques informáticos, describiendo los métodos y herramientas que el atacante emplea para vulnerar un sistema.

- Se muestra la importancia de la seguridad información, permitiendo tomar conciencia de la importancia de la información como un activo másde una organización, permitiendo prevenir ataques utilizando mecanismos de defensa antes mencionados.

- Conocer mediante el ejemplo práctico las vulnerabilidades que hay en un sistema operativo (Windows XP), así mismo que hacer para contrarrestar estos ataques.

## RESULTADOS OBTENIDOS.

- Conocer de manera clara las amenazas que existe en el mundo del ciberespacio y cómo actuar frente a ellos.

- Dar a conocer mediante este trabajo quienes con los principalesactores en cometer ataques informáticos.

## DIFICULTADES ENCONTRADAS.

- Al momento de realizar la práctica y familiarizarse con el sistema operativo Backtrack 5 R3, puesto que este sistema tiene una interfaz totalmente distinta a lo que estamos acostumbrado (Windows - microsoft), así mismo idioma del sistema está en un 100 % .

## REFERENCIAS BIBLIOGRAFICAS.


- Mieres Jorge. (2009). Ataques Informáticos
- Pardo Clemente Ezequiel. (1993). Microinformática de gestión.
- MarroquiNestor. (2010). Tras los pasos de un Hacker. Estados Unidos de Norte América: 1ra Edición.
- Beekman George. (1998). Introducción a la Informática.. 1ra Edición
- Royer Jean-Marc. (2004). Seguridad en la Informática de Empresa: Riesgos,Amenazas, Prevención y Soluciones. España: ENI. 1ra Edición.
- AlvarezMarañon Gonzalo. (2009). Como protegernos de los peligros internetEspaña.
- Parsons Jamrichoja June. (2009). Conceptos de Computación: Nuevas Perspectivas..de C.V. 10 Edición.
- Da Costa Carballo Carlos Manuel. (1992). Fundamentos de Tecnología Documental. 1ra Edición.
- Gris Myriam. (2010). Clave Iniciación a Internet. 1ra Edición
- AlvarezMarañon Gonzalo. (2009). Como protegernos de los peligros internet
- Romero Ma. Del Carmen. (2010). Redes Locales. España: Paraninfo. 1ra Edición.
- Corrales Hermoso (2006). Diseño e Implantación de Arquitecturas Informáticas Seguras.1ra Edición