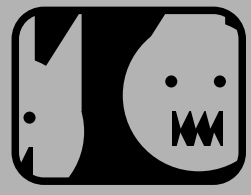
LAS AMENAZAS INFORMÁTICAS: PELIGRO LATENTE PARA LAS ORGANIZACIONES ACTUALES



AUTOR
Carlos Alberto Parra Correa
Ingeniero de Sistemas
Ms(c) en Informática
GEOMÁTICA
Gestión y Optimización de Sistemas
Universidad Industrial de Santander
Carlospacorr@yahoo.com
COLOMBIA

AUTOR
Hernán Porras Díaz
Ingeniero Civil
Magíster en Gestión Tecnológica
Magíster en Informática
Doctor en Ingeniería Telemática
ProfesorTitular
Escuela de Ingeniería Civil
Universidad Industrial de Santander
COLOMBIA

Fecha de Recepción: Octubre 12 de 2007
Articulo Tipo 3

Fecha de Aceptación: Noviembre 1 de 2007

RESUMEN.

Este artículo tiene como propósito mostrar el estado del arte de las diferentes amenazas que pueden afectar la seguridad informática de cualquier organización actual, presenta estadísticas acerca de incidentes de seguridad ocurridos a nivel mundial y local, como también hace una descripción de las diversas amenazas informáticas que pueden afectar actualmente a cualquier organización, con el fin de llamar la atención de las empresas y en especial la Universidad Industrial de Santander UIS, acerca de la importancia de proteger la información mediante esfuerzos completos e integradores, enfocados hacia la búsqueda de un modelo de seguridad informática, objeto final de esta investigación, que obtuvo como principales resultados, Primero: el análisis y evaluación del estado de la seguridad de la red de datos institucional de la UIS, segundo, proponer un modelo de seguridad para la mitigación de la vulnerabilidad de la red de datos, basado en la indagación de los pilares fundamentales de la seguridad informática a escala mundial, que permitió postular una serie de políticas, estándares y procedimientos, y por último, la estimación del presupuesto de implantación de dicho modelo. Como conclusión, las empresas actualmente no están exentas de sufrir algún ataque informático, por lo tanto deben preocuparse por conocer tales amenazas y trabajar en la construcción de una muralla protectora, teniendo en cuenta que esta no se elabora parcial o aisladamente, sino por el contrario, en forma conjunta e integradora, respaldando siempre los objetivos del negocio. Además las políticas, estándares y procedimientos de seguridad que deban ser implantados deben ser apoyados absolutamente por las directivas de la organización.

PALABRAS CLAVE

amenazas
seguridad informática
clasificación de amenazas informáticas
intrusos
virus.

ABSTRACT

This article has as purpose to show the state of the art of the different threats that can affect the computer security of any current organization, it presents statistical about incidents of security happened at world and local level, as well as makes a description of the diverse computer threats that can affect at the moment any organization, with the purpose of getting the attention of the companies and especially the Industrial University of Santander UIS, about the importance of protecting the information by means of complete and integrative efforts, focused toward the search of a model of computer security, final object of this investigation that obtained as main results, first: the analysis and evaluation of the state of the security of the institutional net of data of the UIS, second, to propose a model of security for the mitigation of the vulnerability of the net of data, based on the inquiry of the fundamental pillars from the computer security to world scale that allowed to postulate a series of politics, standards and procedures, and lastly, the estimate of the budget of installation of this model. As conclusion, the companies at the moment are not exempt from suffering some computer attack, therefore they must worry and get to know such threats and to work in the construction of protections, keeping in mind that this it is not elaborated partial or scatteredly, but on the contrary, in combined and integrative form, always supporting the objectives of the business. The politics, standards and procedures of security that should be implanted should also be leaning absolutely for the directive of the organization.

KEYWORDS:

threatens
informatic security
classification of informatic threatens
hackers
virus

INTRODUCCIÓN:

Con la aparición y masificación del uso de las redes informáticas y en especial de la red de redes, Internet, las organizaciones abrieron los ojos y notaron enormes ventajas y posibilidades, convirtiendo a la información procesada, almacenada o transmitida en un activo de suma importancia para cualquier organización [1][2]. Dentro de las ventajas destacables por las cuales las organizaciones, incluidas las universidades, decidieron acceder a estas tecnologías es su ubicuidad, es decir, la posibilidad de estar en todas partes, como también el intercambio de conocimientos tecnológicos tanto a nivel local como mundial, con gran facilidad y velocidad.

Desafortunadamente surgieron individuos que realizaban actividades ilegales que tenían como objetivo irrumpir en flujos de información privados y confidenciales, haciendo que las redes y en particular Internet se convirtiera en un entorno inseguro para cualquier organización. Ninguna organización está exenta de esta grave problemática, ya que puede estar siendo blanco de ataques y presentar debilidades potenciales con respecto a su seguridad informática sin saberlo. Por tal motivo, se han orientado esfuerzos en procura de investigar acerca de las diversas amenazas informáticas que pueden afectar a cualquier organización hoy en día, con el ánimo de alertarlas y motivar esfuerzos en la búsqueda de una protección integral contra la latente, sigilosa y peligrosa amenaza informática.

1. ESTADÍSTICAS IMPORTANTES RELACIONADAS CON INCIDENTES DE SEGURIDAD INFORMÁTICA OCURRIDOS A NIVEL MUNDIAL Y NACIONAL.

Como en [3] se menciona, la sociedad se ha vuelto cada vez más dependiente de las computadoras, y esto ha provocado que los crímenes informáticos vayan cada vez en aumento, sean más desastrosos, impactantes y llamativos para los criminales. Según el CSI (Computer security institute) de San Francisco el 90% de las empresas entrevistadas detectaron ataques a sus computadoras, el 70% reportó que los más comunes fueron virus, robo de laptops y ataques de abuso de la red de sus empleados [4]. Las estadísticas de seguridad en cómputo indican que cerca del 80% de los fraudes relacionados con las computadoras provienen de los usuarios internos[5][6], por esto las intranets son las más vulnerables a ataques de ésta índole.

Las pérdidas estimadas en 3 años consecutivos superaron los 100 millones de dólares [7].

En Colombia los reportes de violaciones de seguridad muestran la siguiente tendencia como puede observarse en la figura 1.

Analizando los informes anteriores, tanto a nivel mundial como local, se observa un incremento acelerado de factores que afectan la seguridad de la información de las organizaciones, provocando la necesidad de investigación tanto de empresas tecnológicas como de la academia, conformando lo que hoy en día se conoce como seguridad informática[9][10].

2.LAS AMENAZAS INFORMÁTICAS Y SUS DIVERSAS CLASIFICACIONES

Amenaza:

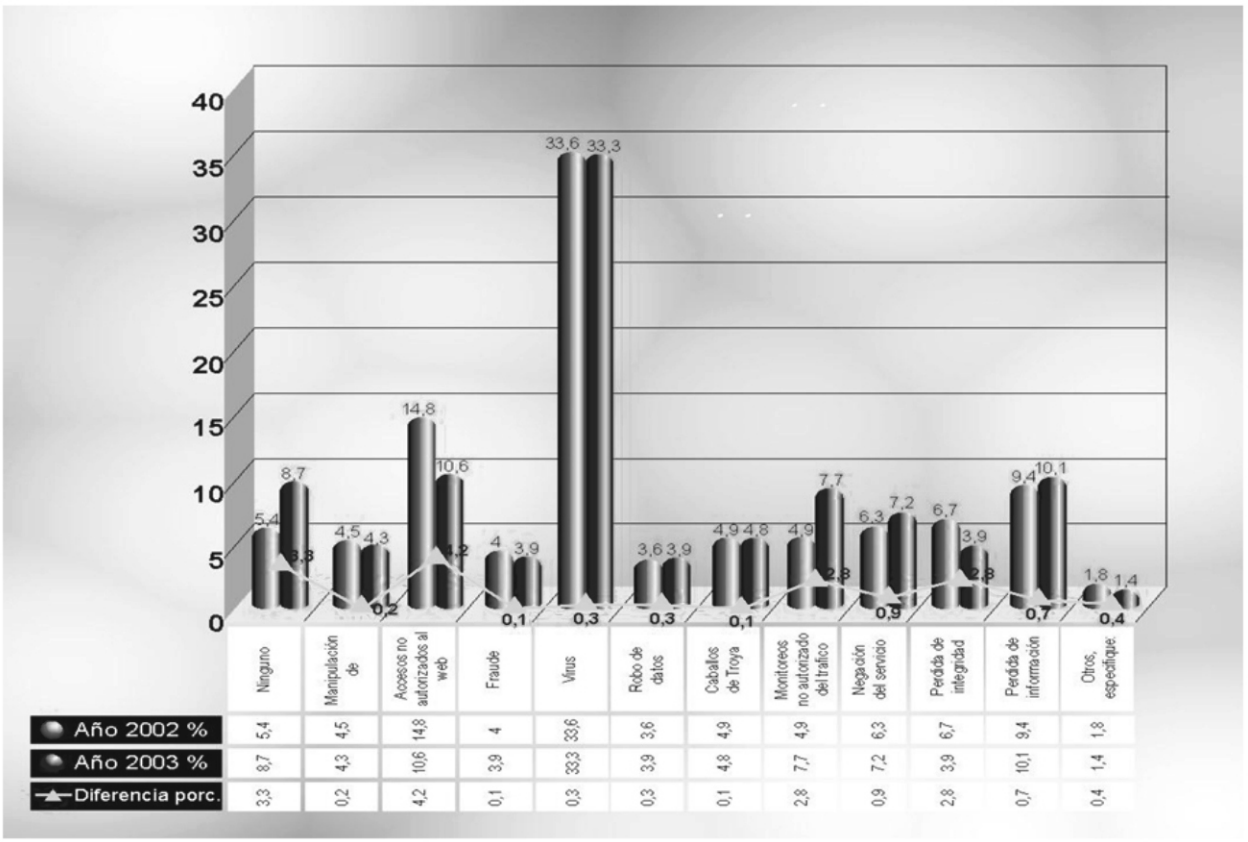
Se refiere a cualquier hecho natural o maniobra de tipo técnico o humana que puede modificar, interrumpir, interceptar o destruir la información de una organización [11]. [12] la define como un acceso no autorizado a una red o dispositivo de red. Existen diversos tipos de clasificaciones respecto a las amenazas informáticas[13], las cuales guardan alguna relación unas con otras, como se muestra en la figura 2, en la cual los diferentes colores mostrados en cada ítem, resaltan la relación entre las diferentes clasificaciones.

De acuerdo al área donde se produzcan las amenazas se pueden clasificar en:

- **Amenazas externas:** Se originan fuera de la organización dentro de las cuales podemos encontrar los virus, gusanos, caballos de Troya, intentos de ataques de piratas informáticos, retaliaciones de ex-empleados o espionaje industrial.

- **Amenazas internas:**Son las que provienen del interior de la organización y pueden ser muy costosas debido a que el infractor por ejemplo un empleado descontento, conoce muy bien la entidad objeto de ataque, tiene mayor capacidad de movilidad dentro de la misma, por lo tanto tiene mayor acceso y perspicacia para saber donde reside la información sensible e importante[14]. Dentro de estas también se incluyen el uso indebido del acceso a Internet por parte de los empleados, así como los problemas que

Figura 1. Violaciones de Seguridad Informática en Colombia.



podrían ocasionar los empleados al enviar y revisar material ofensivo a través de Internet.

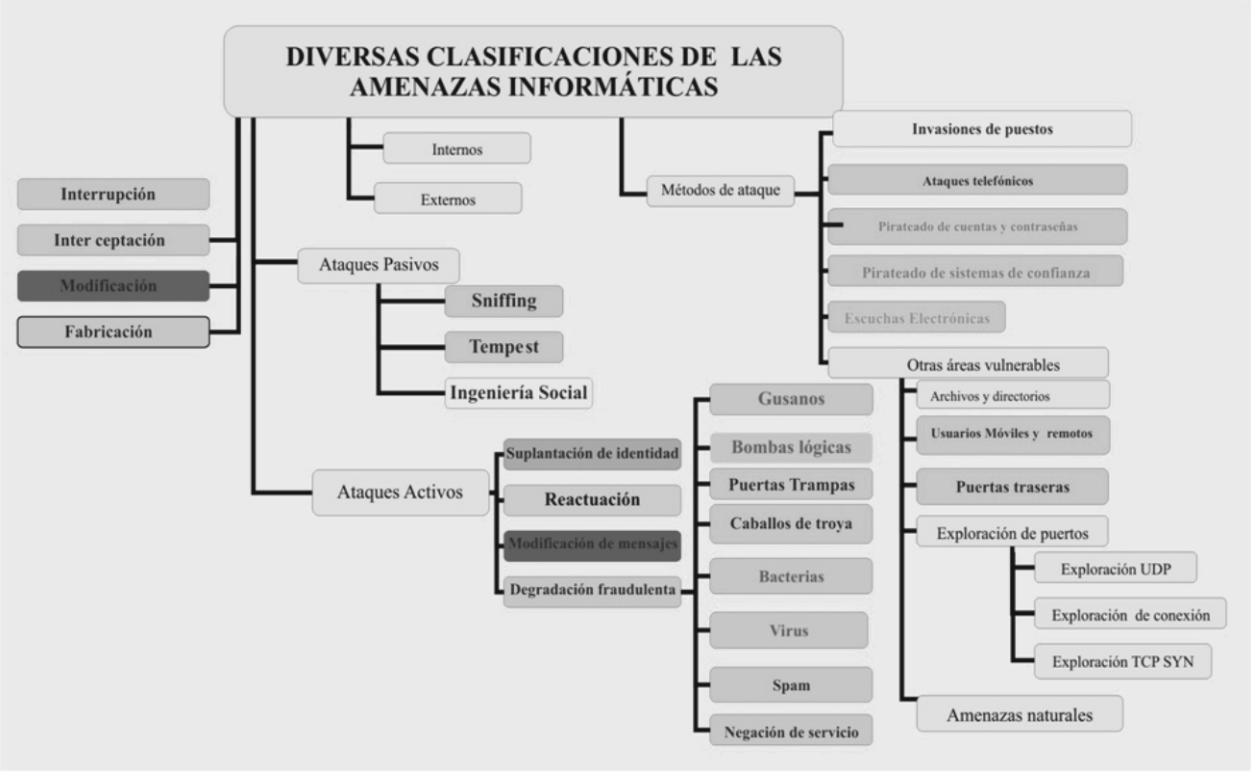
Cuando la amenaza, ya sea externa o interna, se hace efectiva, se convierte en un ataque y estos pueden presentar efectos tanto activos como pasivos:

- **Ataques Pasivos:** Son aquellos en los cuales el atacante recopila información sin que nadie de la organización sepa que se está produciendo [15]. Tiene como objetivo la interceptación y el análisis de tráfico [16]. Dentro de las técnicas más sutiles para obtener información se tienen:
  - Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitorizados.
  - Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.
  - Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los periodos de actividad.

Son ejemplos de estos ataques, las escuchas y los pinchazos electrónicos (sniffing), tempest, lo mismo que ataques propiciados por la llamada ingeniería social, cuyas características se exponen a continuación:

Sniffing: Un sniffer es un programa que permite escuchar o monitorizar todo el tráfico de la red, puede colocarse en una estación de trabajo de la LAN, en un gateway o en un router. El sniffer va leyendo los mensajes que atraviesan la estación de trabajo, gateway o router donde esta instalado y graba la información en un fichero. Esto es posible porque la mayoría de las tarjetas de red ethernet tienen un modo llamado promiscuo, que les permite aceptar todos los datos de la red. En los primeros mensajes de conexión se encuentran los passwords sin cifrar [17].

Figura 2. Diversas Clasificaciones de las Amenazas Informáticas.



Fuente. Los autores

Tempest: Todo equipo electrónico realiza emanaciones eléctricas y magnéticas. Es posible captar estas emanaciones y de ellas obtener información, esta tecnología es utilizada por agencias gubernamentales [18][19]. Actualmente se fabrican equipos con filtro anti- tempest.

Ingeniería Social: Mediante esta denominación no se pretende entrar en controversia con otras ramas del saber en donde su definición varía totalmente, sólo que en seguridad informática, la "ingeniería social" se ha utilizado para denominar una serie de técnicas sicológicas que pueden permitir la obtención de información de manera engañosa o fraudulenta [20]. Es el arte de convencer a la gente de entregar información sensible, como claves de acceso, y de esta forma colaborarle al atacante quien se hace pasar generalmente por el administrador de la red [21]. Es altamente efectiva y difícil de controlar (Educación de usuarios).

- **Ataques Activos:** Se refieren a modificaciones del flujo de datos que el atacante propicia en los datos almacenados o transmitidos. Estos cambios pueden consistir en el borrado, alteración, el retraso o interrupción en las transmisiones. Son difíciles de detectar, porque suelen camuflarse como eventos accidentales en la organización. Pueden dividirse en cuatro categorías:

    - **Suplantación de Identidad:**El intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, esto es posible al sustraer la contraseña de acceso a una cuenta.
    - **Reactuación:** Uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.
    - **Modificación de Mensajes:**Una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje "Consigne 10 millones de pesos en la cuenta X" pudiera modificarse por "Consigne 10 millones de pesos en la cuenta Y".
    - **Degradación fraudulenta del servicio:** Impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o podría interrumpir el servicio de una red inundándola con mensajes triviales. Entre estos ataques se encuentran los de negación de servicio, consistentes en paralizar temporalmente el servicio de un servidor que puede ser de correo, Web, FTP, etc. Son ejemplos de estos tipos de ataques los siguientes:

1) Gusanos (Worms)

Estas piezas de código se propagan por sus propios medios, absorbiendo en forma creciente recursos del sistema, hasta saturarlos causando efectos dañinos como el bloqueo a los sistemas. Son ejemplos de estos:

MELISSA: cuya propagación se hacía a través de correo electrónico.

NIMDA: consumía gran parte del canal de acceso a internet.

GUSANO DE INTERNET: se propagaba con gran facilidad en máquinas UNIX.

2) Bombas Lógicas (Logic Bombs)

Este código dañino se activa al producirse un hecho predeterminado, como por ejemplo una fecha, un número de encendidos del sistema, determinada secuencia de teclas, etc.

3) Puertas Trampa

Son puntos de entrada secretos en un programa, creados para facilitar la depuración sin pasar por el segmento de autenticación pueden ser instalados en el código fuente para suministrar accesos ilegales. Un ejemplo son los Easter Egg[22].

4) Caballos de Troya (Trojan Horses)

Son códigos dañinos anexados en programas de uso autorizado[23], que al ser ejecutados permiten que dicho código nocivo tome el control del sistema. Parece llevar a cabo una función cuando en realidad hace otra cosa[24][25].

5) Bacteria

No realiza daños a sí mismo, su propósito es replicarse a sí misma, puede hacer sólo dos copias de sí misma. Su efecto nocivo es el de consumir todo el espacio en memoria y en disco negando el acceso de los usuarios a los recursos.

6) Virus

Son programas, rutinas o instrucciones desarrolladas para provocar la destrucción o alteración de información importante en un sistema

[26]. Tanto el código ejecutable, como el código no ejecutable son susceptibles de ser infectados, pero sólo adquiere capacidad de auto reproducirse cuando infecta código ejecutable [27][28].

Características de los Virus:

- Se crean y programan intencionalmente.
- Se introducen en equipos de cómputo en diferentes formas.
- Deben ser activados para que realicen su función nociva, debido a que dependen de un archivo ejecutable que los carga en memoria.
- Se camuflan en programas o archivos de apariencia normal.
- Algunos virus tienen la capacidad auto-encriptarse[29] para evitar ser detectados por los Antivirus.

Medios de Infiltración de los virus

Los medios comúnmente utilizados por los virus para su infiltración son:

- Unidades externas de almacenamiento: unidades de discos extraíbles, Disquetes, CD Rom u otros formatos extraíbles.
- Conexiones externas de datos: el hecho de conectar equipos a redes informáticas incrementa las posibilidades de resultar infectado por virus informáticos. Existen tres principales vías de entrada que son la descarga de archivos, el correo electrónico y los sitios web.

En la tabla 1 se presenta una reseña histórica de los virus desde su aparición hasta nuestros días.

1939-1949:	John Louis Von Neumann, colaborador en la construcción de las célebres computadoras ENIAC y UNIVAC, demuestra la posibilidad de crear pequeños programas con capacidad para tomar a su vez el control de otros programas. Nadie sospechó en un principio las consecuencias....
1959:	En los laboratorios AT&T Bell, se inventa el juego "Guerra Nuclear" (Core Wars)[30]. Consistía en una batalla entre los códigos de dos programadores, en la que cada jugador desarrollaba un programa cuya misión era la de acaparar la máxima memoria posible mediante la reproducción de sí mismo.
1970:	El Creeper es difundido por la red ARPANET. El virus mostraba el mensaje "SOY CREEPER...ATRAPAME SI PUEDES!". Ese mismo año es creado su antídoto: el antivirus Reaper cuya misión era buscar y destruir al Creeper.
1980:	La red ARPANET (fue la red precursora de Internet) es infectada por un "gusano" y queda 72 horas fuera de servicio. La red, que utilizaba UNIX como sistema operativo se vio afectada en 6.000 servidores.
1983:	El juego Core Wars, salió a la luz pública. Ese mismo año aparece el termino virus tal como lo entendemos hoy.
1986:	Un programador llamado Ralf Burger se dio cuenta de que un archivo podía ser creado para copiarse a sí mismo, adosando una copia de él a otros archivos. VIRDEM podía infectar cualquier archivo con extensión .COM. Aparecen, pues, en escena los primeros virus capaces de infectar archivos .EXE y .COM.
1987:	Se da el primer caso de contagio masivo de computadoras a través del MacMag Virus, sobre computadoras Macintosh. El virus contaminó el disco maestro del nuevo software Aldus Freehand que fue enviado a la empresa fabricante que comercializó su producto infectado por el virus.
1988:	El virus Brain creado por los hermanos Basit y Alvi Amjad de Pakistán aparece en Estados Unidos. El primer virus destructor y dañino plenamente identificado que infecta muchos PCs fue creado en 1986 en la ciudad de Lahore, Pakistán, y se le conoce con el nombre de BRAIN. Este virus infectaba el sector de arranque de los disquetes. Sus autores vendían copias pirateadas de programas comerciales como Lotus, Wordstar, etc por sumas bajísimas. Los turistas que visitaban Pakistán, compraban esas copias y las llevaban de vuelta a los EE.UU. Las copias pirateadas llevaban un virus. Fue así, como infectaron más de 20,000 PCs.
1989:	Año de efervescencia viral. Virus como el "Fu manchú", "Jerusalem", "Datacrime", "Stoned", ponen en alerta a usuarios y empresas del peligro real y el coste económico que conlleva la infección de virus.

1991:	Aparición del primer virus polimórfico. Symantec comercializa "Norton Antivirus". Los macro virus aparecen en escena, familia de virus con capacidad para infectar documentos y replicarse infectando otros documentos sin ser archivos ejecutables. Alerta mundial frente al virus "Michelangelo".
1998:	El año del Back Orifice, primer virus Troyano diseñado para la administración remota de equipos.
1999:	Aparecen los virus con la más terrible capacidad de difusión: Los virus adjuntos a mensajes de correo (Melissa, Magister, Chernobyl, Sircam, BubbleBoy...)
2000:	El virus I Love you fue detectado el Jueves 4 de mayo de 2000 cuando infecto a miles de ordenadores en todo el mundo. Este código ha sido considerado como uno de los más rápidos de todos los tiempos en propagarse e infectar ordenadores.
2001:	El virus Sircam (2001): Llegaba oculto dentro del contenido de un mensaje de correo electrónico, fue considerado muy peligroso por el gran número de infecciones que produjo. Combinaba características de troyano y gusano de Internet y también fue conocido por la frase que encabeza el mensaje: ¿Hola como estas?
2002:	El virus Klez , el más persistente, en su momento causó estragos por su capacidad para aprovecharse de vulnerabilidades en aplicaciones como los navegadores de Internet o los clientes de correo electrónico, con el fin de autoejecutarse simplemente con la vista previa del mensaje de email en el que llegan.
2003:	Blaster apareció en septiembre del 2003, atacaba básicamente el sitio de Microsoft. Este gusano se propagó rápidamente a través de computadoras con Windows 2000 y XP.
2004:	El gusano MyDoom.A, se propaga a través del correo electrónico en un mensaje con características variables y a través del programa de ficheros compartidos (P2P) KaZaA
2005:	El virus informático más molesto del 2005 fue el Elitper.D, por impedir él sólo la ejecución de hasta noventa aplicaciones comunes, como Word, Excel o Winzip. El titulo más moderno los ostenta ComWar.A, el primer virus para teléfonos móviles capaz de enviarse a sí mismo en mensajes MMS, de la misma manera en que lo hacen los del correo electrónico. El troyano Bancos.NL, fue el más observador, ya que espía al usuario a la espera de que éste entre en la Web de entidades bancarias para robarles los datos.
2006:	A partir del 2006, se pronostica una proliferación de virus cada vez más compleja y más oculta con un objetivo lucrativo, como los troyanos, keyloggers, phishing [31] y pharming. Las amenazas saltarán a plataformas nuevas como las de 64 bits o los dispositivos móviles.

7) Spam

No es un código dañino, pero si bastante molesto. Se trata de un programa que ejecuta una orden repetidas veces. Normalmente en el correo electrónico. Así un mensaje puede ser enviado varios cientos de veces a una misma dirección. En cualquier caso existen programas anti-spam, ya que los spam son empleados normalmente por empresas de publicidad directa.

8) Negación de Servicio (DoS)

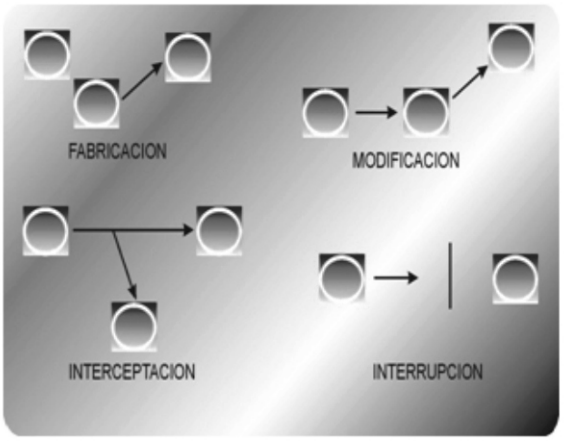
En este tipo de ataque el pirata informático mediante maniobras técnicas busca negar completamente un servicio requerido ya sea por un usuario, red sistema o recurso legítimo [33][34]. Las consecuencias en costos económicos son muy altas y corresponden al lapso de tiempo de indisponibilidad que el sistema haya estado, junto con todo el esfuerzo necesario realizado para identificar y corregir este ataque. Ejemplos de estos ataques los efectuados en febrero del 2000 a algunos sitios web como yahoo.com, Buy.com, CNN.com los cuales fueron dejados sin funcionamiento por dos días.

Formas de Ataque a la Seguridad Informática

Un ataque puede presentarse en diversas formas clasificadas en cuatro categorías[35], como se

observa en la figura 3

Figura 3. Formas de Ataque a la Seguridad Informática



a) Fabricación

Se refiere a aquella maniobra técnica o de engaño humana que es elaborada o diseñada para actuar contra un objetivo definido, por ejemplo los virus.

b) Modificación

Este ataque persigue alterar o cambiar ya sea información o sistemas sensibles para la organización. Por ejemplo la alteración de un servidor que contiene las notas de los estudiantes de una Universidad.

c) Interceptación

Se refiere a aquella estrategia técnica o de engaño humano, que permite enterarse sin que nadie lo note de información pertinente exclusivamente a la organización. Ejemplo de esto pudiera ser un pinchazo electrónico o la utilización de un "sniffer" en la red de la empresa objetivo de ataque.

d) Interrupción

Este tipo de amenaza persigue cortar la transmisión de información, como sucede cuando un servidor deja de funcionar debido a un ataque de negación de servicio.

Métodos de Ataque.

Las anteriores formas de ataque han originado diversos métodos que los atacantes usan para intentar penetrar las organizaciones, como por ejemplo: las contraseñas, escuchas en las líneas, instalar cámaras ocultas o hasta revisar las cestas de la basura para conseguir la información objetivo. Dentro de sus objetivos importantes pueden estar los sistemas de archivos, ya que pueden ejecutar programas de administración y obtener permisos, también son conocedores de los archivos de registro porque les permite borrar los rastros de su intrusión[36], y así entrar las veces que deseen sin que nadie se entere[37]. Dentro de los métodos más comunes y efectivos de atacar tenemos:

1) Invasiones del puesto :Consiste en espiar a las personas aprovechando que han dejado su puesto de trabajo libre durante el cual se instala, extrae, engaña o revisa información sensible. Ejemplo de este ataque lo relata el analista de seguridad Bill Hancock, en un artículo de abril de 1996 llamado "Can you Social Engineer your way Into Your Network" publicado en la revista Network Security (Oxford, UK). Dice que en una ocasión creó una tarjeta falsa con el logotipo de la compañía y un trozo de cinta magnética para simular la banda magnética. A pesar de que esta estrategia no le sirvió totalmente, pudo acceder a áreas reservadas de la compañía esperando que alguien autorizado entrara, sosteniendo la puerta tras él. Una vez adentro logró el puesto de las copias de seguridad y lo utilizó para romper el 50 por ciento de las contraseñas.

2) Ataques Telefónicos: Este tipo de ataques es perpetrado por personas que sacan ventaja del sistema de telecomunicaciones, efectuando llamadas telefónicas de larga distancia gratis, pueden también escuchar conversaciones privadas, acceder otros sistemas a través del sistema violado, acceder a sistemas internos[38]. Por lo tanto son personas expertas en conmutadores telefónicos, redes, equipos de redes, sistemas PBX, armarios telefónicos, cuartos de telecomunicaciones, poseen manuales de fabricantes de equipos de telecomunicaciones, dentro de sus maniobras, está el hacer una llamada a una empresa, transferir la llamada a un operador, para luego simular que es un empleado importante de la empresa y que necesita una llamada al exterior, la llamada es ahora de la compañía que es la que paga y lo peor es que puede aparecer como responsable de otros ilícitos. Otra técnica empleada es la guerra telefónica (wardialing), esta consiste en utilizar un programa de automarcado telefónico, con el fin de encontrar los números telefónicos de computadoras conectadas por modem, para luego tomar tales números y marcar a cada uno de los teléfonos guardados intentando penetrar el sistema. Herramientas con las que se puede desarrollar estos tipos de ataques están ToneLoc y THC- Scan, son totalmente gratuitos y pueden

bajarse de internet, también existe una comercial llamada PhoneSweep[39].

3) Pirateado de cuentas y contraseñas: Obtener el nombre y las contraseñas de las cuentas de los usuarios es una de las primeras prioridades de los atacantes, porque de lograrlo el siguiente paso sería mejorar los privilegios, además los nombres de usuarios son fáciles de adquirir, pues en muchas organizaciones los usuarios internos tienen fácil acceso a listas de nombres de usuarios, además los sistemas de correo electrónico en una empresa pueden suministrar este tipo de listas, por lo tanto se debe asegurar que estas listas no sean legibles.

Si el atacante llega a obtener un nombre de cuenta de usuario, procedería a romper la contraseña, para romperla se apoyan en contraseñas comunes y fáciles de adivinar que muchos usuarios utilizan como el nombre de sus hijos, mascotas, fechas de nacimiento entre otras. Muchas personas utilizan la misma contraseña que en otros sistemas como los cajeros electrónicos, un atacante podría robar la contraseña observando a larga distancia con unos binóculos, también pudiera intentar romper la contraseña mediante un ataque de fuerza bruta, esto consiste en un programa que intenta sucesivamente miles de contraseñas diferentes hasta que logra el acceso. Un ataque de diccionario, es muy similar al anterior sólo que utiliza un diccionario completo con contraseñas comunes en varios idiomas. Otro método para romper las contraseñas consiste en instalar programas de captura o lector de teclas de teclado siempre y cuando se tenga acceso a la estación de trabajo, estos programas son llamados en inglés keyloggers.

4) Pirateado de sistemas de confianza: Los atacantes adoran las relaciones de confianza, ya que un programa de una computadora puede acceder a información almacenada en otra computadora, permitiéndoles acceder a otros sistemas y más si dichas relaciones son transitivas (una relación de confianza es transitiva si un sistema X mantiene su relación de confianza con un sistema Y, y este sistema hace lo mismo con el sistema Z, y se puede extender la relación de confianza de X a Z a través de Y).

5) Escuchas electrónicas y rastreadores de conexiones (Sniffing):Se refiere a un dispositivo o software que instala el atacante en un punto ya sea externo o interno de una organización con el objeto de capturar, almacenar paquetes para posteriormente extractar la información de interés, que son habitualmente los inicios de sesión, esta técnica de escucha es difícil de detectar, estos rastreadores generalmente se conocen con el nombre de sniffers, y uno de los más famosos es el "snort" (disponible gratuitamente en http://www.snort.org).

6) Otras Áreas Vulnerables: Los piratas informáticos hacen uso de una variedad de herramientas y técnicas para atacar. Usualmente se aprovechan de falencias conocidas, dentro de estas tenemos:

Archivos y directorios

Existen sistemas operativos con debilidades en sus sistemas de archivos que pueden permitir arrancar equipos con DOS para acceder a archivos de cualquier directorio, por ejemplo en Windows NT uno de sus sistemas de archivos: el FAT permite arrancar una computadora desde DOS permitiendo acceder a cualquier archivo de un directorio, estas debilidades son comúnmente llamadas agujeros de seguridad.

Usuarios Móviles y Remotos

El hecho de permitir inicio de sesión a un usuario móvil remoto nos puede ocasionar serios inconvenientes de seguridad, como por ejemplo:

- Alguien puede ver el inicio de sesión del usuario remoto de la compañía, ya sea directamente o utilizando dispositivos de vigilancia cercanos.

- El usuario remoto realiza los inicios de sesión sobre líneas públicas, que pueden no tener la seguridad adecuada, permitiendo el espionaje de piratas informáticos que tengan en la mira nuestra compañía.

- Un equipo portátil puede ser fácilmente objeto de robo. La información valiosa de la organización queda a merced del ladrón como: contraseñas almacenadas en el disco, nombre de las cuentas de usuario listadas en las direcciones de correo electrónico, información confidencial [40] de la compañía entre otras.

Puertas traseras.

Conocidas en inglés con el nombre de backdoors. Son generadas por los piratas informáticos al abrir puertos utilizando características tanto de las redes, como de los

sistemas operativos, que les permiten ejecutar funciones remotas sobre equipos, blanco de ataque. También los programadores habitualmente dejan en sus programas puertas de escape, con el fin de saltarse procesos que ahorran pasos de verificación y control, pero olvidan muchas veces cerrarlos, provocando serios problemas cuando al hallarlos los piratas informáticos, logran aumentar los privilegios hasta acceder a una organización.

Exploración de Puertos

Uno de los pasos que realiza un atacante informático para determinar si los sistemas individuales están activos, es llevar a cabo un barrido ping automatizados por ejemplo en un rango de direcciones IP y bloques de red [41]. La instrucción Ping se utiliza habitualmente para enviar paquetes ICMP ECHO (Tipo 8) al sistema objetivo de ataque, si el sistema responde un ICMP ECHO_REPLY (Tipo 0) indicará que el sistema destino está activo. Por lo tanto una exploración de puertos es el proceso de conexión a puertos (UDP y TCP) del sistema destino que constituyen nuestro objetivo para determinar qué servicios están activos o si se encuentran un estado de escucha (LISTENING).

Los objetivos de este ataque denominado exploración de puertos son los siguientes:

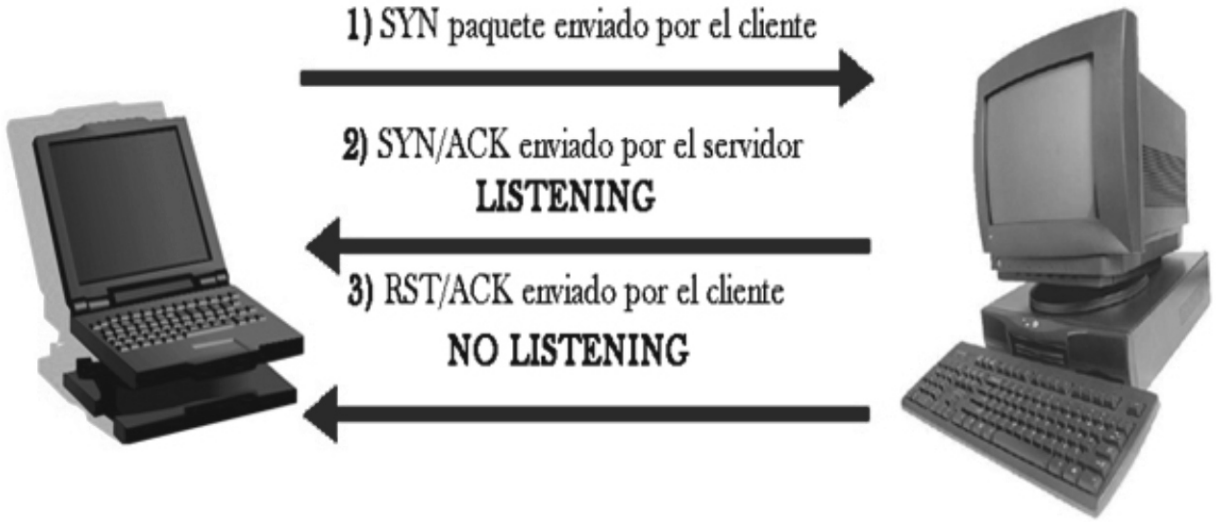
- La identificación de servicios UDP y TCP que se están ejecutando en el sistema objeto de ataque.
- La identificación del sistema operativo.
- La identificación de las versiones o aplicaciones específicas de un determinado servicio.

Tipos de Exploración

Existe una herramienta desarrollada por Fyodor llamada Nmap, en esta se han desarrollado varios tipos de exploración de puertos dentro de las cuales destacamos:

1.)Exploración de conexión TCP:Esta busca conectar con el puerto objeto de ataque e intentar un acuerdo o conexión de tres vías (SYN, SYN/ACK Y ACK). Tiene como gran desventaja que es fácilmente detectable por el sistema atacado [42]. Este tipo de exploración se ilustra en la Figura 4.

Figura 4. Exploración de Conexión TCP Completa.

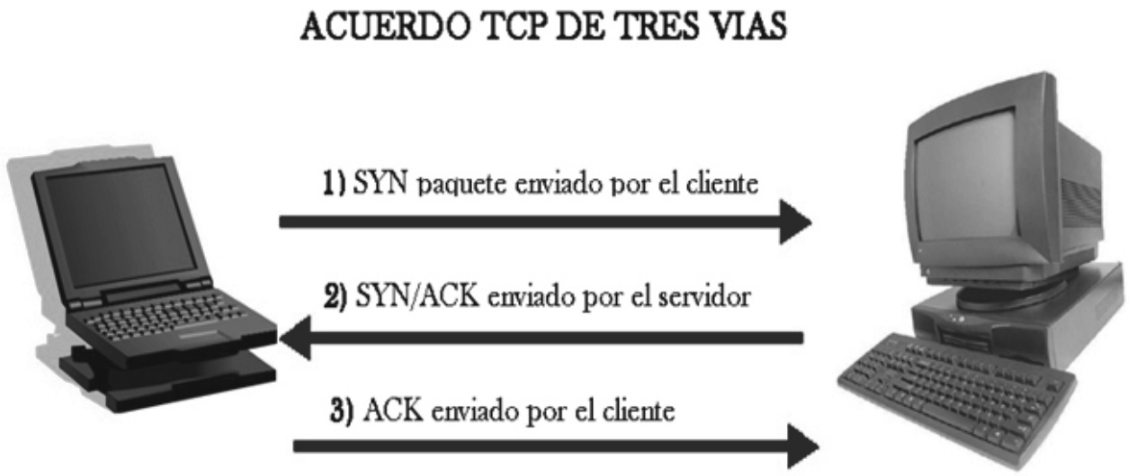


Fuente. Los autores

2) Exploración TCP SYN

Este ataque que se muestra en la Figura 5, se caracteriza porque no se realiza una conexión TCP completa, también es conocida como exploración semiabierta. Se envía un paquete SYN al puerto objetivo. Si retorna un SYN/ACK del puerto explorado, se puede deducir que está a la escucha. Si por el contrario, se recibe un RST/ACK esto indicará que el puerto no está a la escucha. Luego el sistema que está llevando a cabo la exploración de puertos enviará un RST/ACK para que no establezca una conexión completa, siendo una técnica más cautelosa y difícil de detectar.

Figura 5. Exploración TCP SYN.

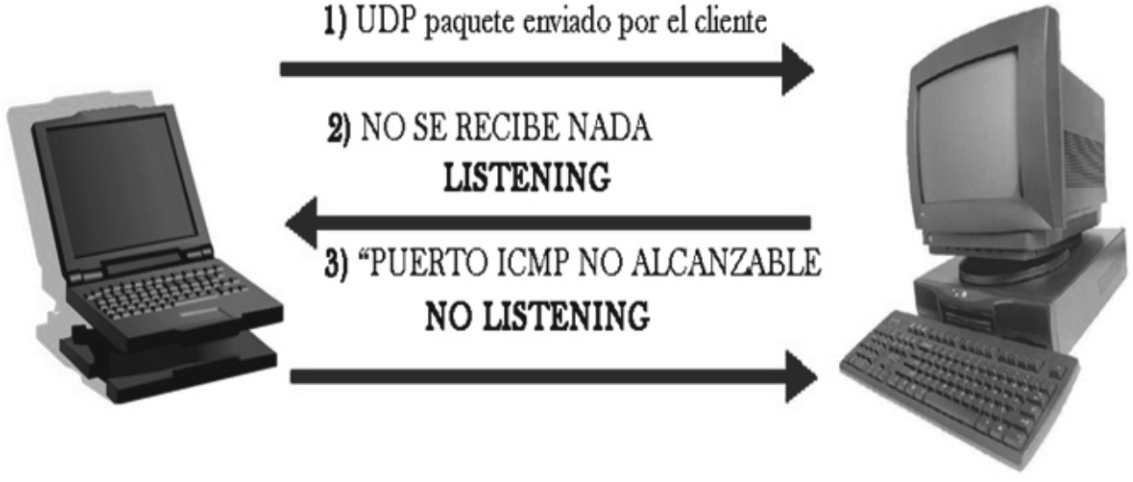


Fuente. Los autores

3) Exploración UDP

En esta envía un paquete UDP al puerto atacado. Si el puerto responde con un mensaje similar a "puerto ICMP no alcanzable" obviamente el puerto está cerrado, en caso contrario, si recibimos un mensaje diferente al de "puerto ICMP no alcanzable", se puede deducir que el puerto está abierto. Como UDP es conocido como un protocolo sin conexión depende de factores relacionados con tráfico y recursos de red,

Figura 5. Exploración TCP SYN.



Fuente: Los autores

convirtiendo la exploración UDP en un proceso bastante lento. Un esquema de este tipo de ataque se muestra en la Figura 6.

Amenazas Naturales

Es erróneo pensar que todas las amenazas a la seguridad de una red informática provienen del talento humano, también fallos en la alimentación eléctrica, incendios [43], fallos en los componentes, y otras problemáticas pueden arruinar sistemas y provocar enormes pérdidas económicas. Dentro de las amenazas naturales podemos considerar las siguientes:

- Fallos de hardware pueden ocasionar pérdidas en la disponibilidad de los datos, es por eso que los sistemas redundantes y las copias de seguridad son imprescindibles.

- Las interrupciones en la energía eléctrica pueden ocasionar indisponibilidad de la información. Las fuentes de alimentación para copias de seguridad son indispensables.

- Las inundaciones, el fuego, los temblores de tierra y otros desastres obligan a la necesidad de sistemas de copia de seguridad, centros alternativos de datos y plantas de recuperación ante catástrofes.

3. CONCLUSIONES

Las redes informáticas han aportado grandes beneficios para las organizaciones, convirtiendo la información en un activo muy importante y valioso para cualquier empresa en la actualidad. Las estadísticas mundiales y locales muestran la aparición de múltiples maniobras conocidas como amenazas informáticas, que han permitido modificar, interrumpir, interceptar o destruir la información de las empresas tanto a nivel mundial como local.

Las amenazas son efectuadas entre otros por empleados descontentos o por individuos con conocimentos informáticos, que toman como reto propio el vulnerar los sistemas mediante diversos mecanismos técnicos o no técnicos y así poder acceder a información confidencial de las empresas de manera prohibida.

Existen gran diversidad de amenazas informáticas, de acuerdo al área de la empresa donde se produzcan pueden ser: internas o externas, siendo las más frecuentes las internas. Cuando las amenazas se hacen efectivas pueden manifestarse en ataques pasivos o activos. En el primero, el atacante intenta tomar la información, sin que la organización sepa que se está produciendo sin alterarla, en el segundo,el atacante intenta alterar, borrar o retrasar la transmisión. Para las empresas actuales los virus son las amenazas mas frecuentes y molestas.

En Colombia, apenas algunas organizaciones empiezan a comprender y tomar conciencia de la importancia de conocer y controlar la amenaza informática, ya que muchas ignoran el tema motivo de este artículo, cuyo primer propósito es el de convocar a las empresas, para que descubran, analicen y evalúen la amenaza informática y sus efectos nocivos para las organizaciones. El segundo propósito, impulsar investigación acerca de los pilares fundamentales de la seguridad informática que puedan permitirle controlar la amenaza, y el tercero, por buscar un modelo de seguridad informática realista e integrador, que permita armar una muralla sólida contra el monstruo de mil cabezas en que se convirtió la amenaza informática en estos tiempos.

4. REFERENCIAS

[1]FISHER, R.P. Seguridad en los Sistemas Informáticos.1 ed.: Díaz de Santos, 1988, p.1-3.

[2]AFZAL, A. Introducción a Unix. 1 ed. Madrid: Prentice may, 2000. p. 394-399.

[3]AMOROSO, E.G. Fundamentals of Computer Security Technology ,Prentice Hall, 1994. p.1-4.

[4]http://www.corporate intranet.com/treasury/articles/art04.html, http://www.cert.com, http://www.gocsi.com/prelea_000321.htm

[5]COMMER, D,E. Internetworking with TCP/IP. 2 ed. E.E.UU: Prentice Hall, 1991.p.100-250

[6]TACKETT, J y GUNTER, D. Utilizando Linux. 2 ed. E.E.U.U: Prentice may, 1991. p. 50-250.

[7]VICENTE, C.A y MENDOZA M. Las políticas como una forma de reglamentación a la falta de Legislación informática. URL: http://seguridad.internet2.ulsa.mx. 08/2003

[8]Fuente: III Encuesta Nacional de Seguridad Informática ACIS 2003.

[9] RAMIÓ, J. Seguridad informática y criptografía. URL: http://www.criptored.upm.es/ . 02/2002

[10]HEWLEWTT PACKARD COMPANY. Servicios HP de seguridad: servicios y soluciones para garantizar la seguridad y disponibilidad de su entorno de IT. URL: http: www//hp.es/serviciosdeseguridad y http://www.hp.es/serviciosdesoporte. UE. 06/2002

[11]COWAN,C., WAGLE, P., PU, C. , BEATTIE, S and WALPOLE,J. Buffers Overflows: Attacks and Defenses for the Vulnerability of the Decade. In Proceedings of the sans 2000 Conference. The sans Institute, 2000.

[12]KISKENDALL,K.R y LIÚ, D. Fundamentos de Seguridad de Redes-Academia Networking de CISCO System- Especialista en Firewall CISCO, Madrid : Pearson, 2005.p. 832.

[13]APARICIO, J. Seguridad Informática, la importancia de conocer las amenazas. SekureIT, Consultores en Seguridad Informática. URL: http.//www.sekureit.com. 11/10/2001

[14]GONZALEZ, J. Seguridad profesional en windows NT. 1 ed. Madrid: Alfaomega-rama, 2002.p 16-25

[15]SCHNEIER,B El rootkit del DRM de SONY: La verdadera historia. URL:http://www.kriptopolis.org/node/1467. p.1-5. 18/11/2005

[16]GARFINKEL, S and SPAFFORD, E. Practical Unix & Internet Security. 2 ed. O'Reilly & Associates 1996.p. 34-250

[17]KLEIN, D. Foiling the cracker: A survey of, and improvements to, password security. In Unix Security Workshop, pages 514. The USENIX Association, 1990.

[18]RANADE,J. Computer & Comunications Security Strategies for the 1990s , Singapur: McGrawHill,1989.p.1-3.

[19]NICHOLS, R,K y LEKKAS, P,C. Seguridad para comunicaciones inalámbricas. 1 ed. Madrid: McGraw-Hill, 2003.p 73-83.

[20]SCAMBRAY,J., MCCLURE, S. and KURTZ, G. Hackers 2 Secretos y soluciones para la seguridad de redes. 1 ed. México: McGrawHill, 2001. p.115, 171, 626-629.

[21]CHESWICK,W,R and BELLOVIN, S,M. Firewalls and Internet Security. 1 ed. USA: Addinson Wesley, 1994.p.13.

[22]http://www.eggheaven2000.com . Egg Heaven 2000. Available from Internet

[23]GEORGIA INSTITUTE OF TECHNOLOGY. Georgia Institute of Technology Computer and Network Usage Policy. URL: http://www.educause.edu/ . 09/10/2002

[24]PARSONS, J.J.Conceptos de Computación, 2 ed. México, D.F: Internacional Thomson Editores, 1999.p. G-6.

[25]CERT. CERT Advisory CA9902. Trojan Horses. Technical report, Computer Emergency Response Team.03/1999

[26]WHITTINGTON, R y PANY, K. Auditoría un enfoque integral. 12 ed. Madrid: McGraw-Hill, 2000.p. 218.

[27]GUERRERO, C.D y VELAZQUEZ, G.A. IX Semana Técnica Internacional: Seguridad Informática. 1 ed. Bucaramanga: Armonía Impresores, 2002, p.

[28]DU, Tom . Experience with viruses on UNIX systems. In USENIX Computing Systems, volumen 2, 1989

[29]SCHNEIER, B. Applied Cryptography. 1 ed. E.E.U.U: John Wiley & Sons, 1994.

[30]GONZALEZ, G y .MAS, J. El libro de los Virus y la Seguridad Informática, 1 ed. Madrid : Ra-ma, 1990. p. 41-42.

[31]VIRUSPROT.COM. Ataque de phishing a clients de Santander Central Hispano. El mail es un truco de los hackers para conseguir contraseñas. URL: //www.virusprot.com/security-Santander_Hispano_News010906.htm 01/09/2006

[32]GUILLEN, Anellie, Boletín No.19.

www.gcpglobal.com.

[33]CHAPMAN, D.B. y ZWICKY, E.D. Construya Firewalls para Internet, 1ed. México, D.F: McGrawHill, 1997. p.7-10.

[41]DEPARTAMENTO DE SEGURIDAD DE CÓMPUTO UNAM-CERT. Guía de seguridad para Windows 2000. URL: http://www.seguridad.unam.mx,http://wwww.unam-cert.unam.mx p. 11-13.

[42] NORTHCUTT, S y NOVAK, J. Detección de Intrusos. 2 ed. Madrid: Prentice Hall, 2001. p. 115-132.

[43]BLAKE, R,P. Seguridad Industrial. 1 ed. México. D.F: Diana, 1970.p. 424-427.