UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO

INSTITUTO DE CIENCIAS BÁSICAS E INGENIERÍA
LICENCIATURA EN SISTEMAS COMPUTACIONALES

CENTRO DE INVESTIGACIÓN EN TECNOLOGÍAS DE INFORMACIÓN Y SISTEMAS

“El hacking y técnicas de contra-ataques a la seguridad de información”

M O N O G R A F Í A

QUE PARA OBTENER EL TÍTULO DE
LICENCIADO EN SISTEMAS COMPUTACIONALES

P r e s e n t a

PLSC: Rosa María Ponce Pérez

ASESOR
M. EN C. GONZALO ALBERTO TORRES SAMPERIO

Pachuca de Soto Hidalgo, 2008
México.

Índice

Capítulo III: Ataques típicos efectuados por un hacker

Capítulo IV: Herramientas utilizadas por el hacker

Capítulo V: Como ingresa el Hacker en el sistema operativo Unix

Capítulo VI: Seguridad del hacking

ÍNDICE DE FIGURAS

Capítulo III: Ataques típicos efectuados por un hacker

Capítulo IV: Herramientas utilizadas por el hacker

Capítulo VI: Seguridad del hacking

ÍNDICE DE TABLAS

Capítulo I: Hacking

Capítulo III: Ataques típicos efectuados por un hacker

Capítulo V: Como ingresa el Hacker en el Sistema Operativo Unix

1.- Introducción

Todos hemos escuchado el término "Hacker" alguna vez, los que contamos con una computadora en casa, el sólo hecho de escuchar el término nos asusta, lo relacionamos con virus y espías peligrosos que pueden causar graves daños a la computadora.

En éste trabajo se aborda la definición de “Hacker” y lo que este término lleva consigo, que es más de lo que podría imaginar al comenzar esta investigación.

La Internet está llena de sitios y consejos que sirven a los hackers para hacer sus fechorías, tanto jóvenes, como criminales y terroristas tienen acceso a ella, lo que significa que un mayor número de intrusos está tocando las puertas. A pesar de una mayor seguridad en la web y de castigos más severos; los ataques de los hackers están a la orden del día.

La mayoría de las compañías no aceptan dichos ataques con el fin de evitar un impacto negativo en la publicidad. Las estadísticas cubren desde las interrupciones en las redes locales (que le dan acceso al hacker a los archivos con la información), hasta el vandalismo en los sitios Web, (los ataques de negación de servicios y el robo de la información). Los riesgos que se corren aquí son personales y profesionales. Los hackers se pueden robar las contraseñas y los números de cuentas bancarias de la computadora o pueden apoderarse de los secretos comerciales desde la red local de la compañía.

Este fenómeno también representa un riesgo contra la seguridad nacional, porque los terroristas más conocedores o los gobiernos más hostiles, pudieran interrumpir los sistemas satelitales, llevar a cabo una guerra económica interfiriendo en las transferencias financieras o incluso crear problemas en el control de tráfico aéreo.

Pero no todos los hackers tienen malas intenciones. Algunos se encargan de la seguridad de los sistemas de las compañías y otros contribuyen a la protección avisándoles a los fabricantes de software, si encuentran algo vulnerable.

La ética del “Hacker”, que es un episodio aún sin escribir y que gobierna el mundo de la piratería, dice que un “Hacker” no hará daño. Pero esto no se puede comprobar, así que mientras esté en la red, es un peligro latente.

Si una persona tiene motivos políticos contra alguna empresa "X" y decide estropear la página Web, tiene que entrar en línea y aprender cómo hacerlo. En el transcurso de la investigación se relacionarán conocimientos acerca de la comunicación que existe dentro de una sociedad mundial intercambiando múltiples datos, así como la importancia; además de la seguridad que involucra cada uno de estos sistemas de comunicación.

2.- Justificación

En la actualidad la gran mayoría de la población que tiene una computadora personal y tiene conexión a Internet, corre el gran riesgo de ser atacado por el mayor problema Informático: " LOS HACKERS ". Los conocimientos que se pueden adquirir sobre los ataques de hackers son importantes, para la seguridad del equipo y más aun la de la información.

De acuerdo a estas ideas, la presente investigación refiere en analizar y diagnosticar los recursos que aplica el usuario a la computadora para poder evitar el acceso de visitantes indeseados.

3.- Objetivos

3.1.- Objetivo general

Mostrar las principales técnicas que puede dañar a un sistema de prevención de fácil manejo y bajo costo para el usuario además detectar y repare los ataques de Hackers contra los computadores domésticos.

3.2.- Objetivos específicos

- Estudiar y analizar un sistema contra los ataques de hacker.
- Diagnosticar el nivel de seguridad en los computadores personales.
- Detectar las necesidades de actualización educativa del usuario en el área de Informática.

Capítulo

I

Hacking

1.1.- Concepto de Hacking

Son las técnicas y procedimientos utilizados por un *"Hacker"* para un determinado objetivo. Normalmente son procedimientos ilegales.

Hacker: Es un pirata informático o persona con altos conocimientos sobre informática (o también otros sistemas como la telefonía, etc.) y usa sus conocimientos con un determinado objetivo (no necesariamente maligno). Cuando realiza una determinada tarea como *"Hacker"* se denomina hackeo, es decir, está haciendo *"Hacking"*. A veces lo que anima a hacer hackeo no es obtener dinero, sino la satisfacción de saber que pudo cumplir un objetivo. Por lo general no se quedan con un triunfo, sino buscan retos más difíciles y diferentes **[21]**.

1.2.- Seguridad en la Web

Para proteger la red ante accesos no deseados, un sistema operativo de red cuenta con la opción siguiente:

Detección y cierre de la red ante intrusos

Los usuarios de la red han de estar identificados ante el sistema. Éste permitirá acceder a los datos a aquellos que cuenten con autorización. Para ello, se proporciona al usuario un nombre que el sistema reconoce y una contraseña (password).Si se desconoce cualquiera de las dos el sistema no deja acceder a ninguno de los datos.

Pero puede haber usuarios que, para intentar acceder a la red, hagan pruebas de introducción de nombres y o contraseñas.

Para incrementar la seguridad de la red, puede hacer que la red controle el número de intentos incorrectos al introducir la contraseña de acceso.

Después de especificar el número de intentos fallidos, puede hacer que la red cierre la entrada al usuario durante un tiempo determinado. Esta estrategia detiene a los intrusos que conectando con el nombre de un usuario (por ejemplo, el supervisor) intentan introducir varias contraseñas con la esperanza de conseguir la correcta.

Para ello, se dispone de las siguientes opciones:

Detectar intrusos. Al marcar en este campo, se establece la detección de intrusos.

En el bloque límites de detección de intruso se encuentra los siguientes apartados:

Intentos de entrada incorrectos. Indica el número de intentos de entrada fallidos que se permite a los usuarios (por defecto es 7).

Restablecimiento de intrusión. Indica el período de tiempo durante el cual se está contando los intentos de conexión erróneos para que se contabilicen (por defecto es 30 minutos).

Si marca en bloquear cuenta después de detección está indicando que una vez se hayan dado el número de intentos de entrada fallidos en el período de tiempo indicado, se debe bloquear la cuenta durante el tiempo indicado en restablecimiento de bloqueo de intrusos (por defecto es 15 minutos) durante el cual no se permitirá la entrada a ese usuario.

> El bloqueo de intrusos sólo se ha activado para los usuarios cuyo contexto es el objeto contenedor indicado, el resto no tiene ningún tipo de bloqueo de intrusión.

Así como ha ido avanzado día con día el Internet, se permiten cada vez mas las formas de ataque a la seguridad de red, como pueden ser los "*virus"*, "*Caballos de Troya"* y penetración de las redes internas. Algunos usuarios o departamentos individuales se conectan a Internet sin la "*autorización*" de algún servidor.

Puede ser difícil saber si se está o no conectado a la red del Internet. El entrar al Internet es como abrir las cortinas en las ventanas de la oficina y dejar la claridad completa del sol del mediodía **[8]**.

1.2.1.- La navegación por Internet

Al navegar por la red, no escribir formularios con los datos, dejando múltiples rastros de identidad, de una manera inconsciente es recogida de forma oculta por los servidores y pueden ser utilizados para diversas finalidades ya sea para un mejor funcionamiento de la página Web, para objetivos comerciales o quizá hasta para metas malignas **[8]**.

Muchos consumidores adoptaron las redes inalámbricas en casa. Los fabricantes, al querer ofrecer una experiencia positiva, lanzan productos que casi no requieren de configuración alguna. Conectarse a una red inalámbrica es tan fácil como encender la computadora.

Mientras esté en su red inalámbrica, es posible que su vecino (o peor aún, un pirata casual). También lo esté. Por lo general, los intrusos inalámbricos sólo quieren una parte de su ancho de banda. Algunos consejos ayudarán a proteger red inalámbrica. Primero, active todas las características de seguridad que incluya el hardware. Todos los productos inalámbricos ofrecen soporte para el protocolo.

Proteja el correo electrónico

Hay muchos programas gratuitos o muy económicos que alejan a los intrusos. Las soluciones más sencillas y completas son los servicios de correo Web ultraseguros, que incluyen opciones de codificación, firmas digitales y acceso con claves públicas. No obstante, si va a cafés Internet, usa terminales en bibliotecas u otras computadoras públicas, la PIP es indispensable. Sin ella, deja atrás contraseñas, su historial de

navegación, archivos temporales y otra clase de información personal en cada máquina que usa.

PIP copia su cuenta de correo electrónico en el dispositivo, creando una identidad portátil. Conecte el dispositivo a una computadora compatible, abra PIP y podrá trabajar con su correo electrónico, teniendo acceso total a sus carpetas y su libreta de direcciones desde el dispositivo.

La navegación privada en la Web de PIP protege artículos personales como favoritos, historial, archivos temporales, cookies y URL capturados almacenándolos en el dispositivo. También puede usar PIP para elaborar perfiles de carpetas y archivos que va a guardar en el dispositivo y sincronizarlos con otra computadora.

Una advertencia: como todo el acceso se realiza a través del dispositivo desmontable, dé cuenta de que el envío de e-mail o la navegación se vuelven más lentos por medio de PIP. Recuerde apagar el dispositivo antes de desconectarlo para no perder información.

Navegación Anónima

La navegación en el Web permite tener la ilusión del anonimato, pero no necesariamente es una realidad. Los sitios Web pueden registrar su dirección IP, determinar la página desde la que llegó e incluso elaborar un perfil suyo por medio de cookies. Además un administrador de red o un pirata puede revisar el tráfico sin codificar para saber hacia dónde va. Las herramientas y servicios de navegación anónima pasan sus peticiones a través de servidores proxy para cubrir su identidad y, en algunos casos, codificar incluso su propia información.

Mensajería instantánea segura

La mensajería instantánea no sólo es gratificante al instante, sino que también es insegura. Cualquiera que tenga las herramientas y acceso a la red puede leer los mensajes. Asimismo, los mensajes son vulnerables durante el procesamiento en el servidor, o por más tiempo, si se archivan. Asimismo, se pueden interceptar, alterar o retransmitir.

1.2.2.- Seguridad en Internet

Hoy en día, nadie confía en la seguridad del Internet, ya que alguien pueda conseguir el número de la tarjeta de crédito mediante el uso de la red. Se teme que a descubrir códigos de acceso de la cuenta del banco y entonces transfieran fondos a la *"cuenta"* de un usuario donde tiene acceso sin *"autorización".*

Las agencias de gobierno, los bancos, las corporaciones, entre otros, no dar información confidencial a personas no autorizadas, empleados que no están autorizados al acceso de esta, o hasta quienes traten de curiosear sobre una persona o empleado. Las organizaciones se preocupan porque los competidores tengan conocimiento sobre información patentada que pueda dañarlos. La seguridad es guardar algo seguro. "Algo"

puede ser un objeto, tal como un secreto, mensajes, aplicaciones, archivos, sistemas o una comunicación interactiva. Seguramente los medios son protegidos desde el acceso, el uso o alteración no autorizada **[8]**.

Para guardar objetos seguros, es necesario:

- Se garantice quien firma un mensaje es realmente quien dice ser.
- La "*autorización*".
- La privacidad o confidencialidad, una información solamente puede ser conocida por individuos autorizados.
- La integridad de datos, la integridad se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc., durante el proceso de transmisión o en el propio equipo de origen. Es un riesgo común que el atacante no puede descifrar un paquete de información y, saber qué es importante o que simplemente lo intercepte y borre.
- La disponibilidad de la información, trata de la seguridad, la información pueda ser recuperada en el momento se necesite, esto es, evitar la pérdida o bloqueo, ya sea por alguna mala operación accidental o situaciones de fuerza mayor.
- No rechazo (la protección contra alguien que niega que ellos originaron la comunicación o datos) **[8]**.

En la tabla 1.1, se presenta una relación de los intereses se deben proteger y los requerimientos relacionados:

Intereses	Requerimientos
Fraude	Autentificación
Acceso no autorizado	Autorización
Curiosidad	Privacidad
Alteración de Mensaje	Integridad de datos
Desconocido	No-Rechazo

Tabla 1.1.- Relación de los intereses que se deben proteger y sus requerimientos.

Estos intereses no son exclusivos de Internet. La "*autentificación"* y el asegurar los objetos es una parte de la vida diaria. La comprensión de los elementos de seguridad y como ellos trabajan en el mundo físico, puede ayudar para explicar cómo estos requerimientos se encuentran en el universo de la red y dónde se sitúan las dificultades **[8]**.

1.2.3.- La Web y los secretos

La página Web: Hay dos tipos de página (dos protocolos diferentes) visualmente se diferencian por empezar con "*http"*: o por https: (notar la *s* del último caso) y por un candado cerrado o una llave que aparece en la parte inferior del navegador. La diferencia fundamental es que en el primer caso toda la transmisión se hace en claro y la segunda se hace cifrada. En el primer caso, los datos transmitidos pueden ser interceptados y pueden apoderarse de la información transmitida.

La segunda la utilizan los servidores para hacer transacciones seguras (por ejemplo ventas, operaciones bancarias, etc.) la información transmitida es cifrada. Ejemplo, debe asegurarse siempre que se vaya a dar la tarjeta de crédito, ya que lo está haciendo mediante un servidor seguro. Dentro de la categoría de servidores seguros hay unos más seguros que otros, dependiendo del nivel de cifrado ofrecen (por ejemplo los hay de 56 bits, inseguros, y de 128 bits, seguros).

Al navegar por Internet se debe tener la seguridad que la página que se esté visitando corresponde a quien debe pertenecer. Acceder a las páginas Web a través de enlaces, una página estafadora puede enlazar con una página falsa que solicita por ejemplo datos de un individuo. Primero sería comprobar en el navegador en qué URL se encuentra y si de verdad corresponde a quien dice ser.

Si está en un servidor seguro, debe comprobar el Certificado de Autoridad (quien realmente certifica que es quien dice ser) Se puede comprobar en Internet a quien pertenece un "*dominio"* en http://www.whois.net/ (para los tipos com., org y net) o en http://www.nic.es/ (para .es) algunas veces puede encontrar un mismo nombre de "*dominio"* **[8]**.

Cookies: Los "*cookies"* son pequeños archivos de texto, se guardan en el navegador a petición del servidor. Como puede ser el usuario y clave de acceso a ella. Al ser un archivo de texto, no es potencialmente peligroso y como tal no es ejecutable (no se puede introducir ni "*virus"*, ni ejecutar programas, etc.), solo es eso, un texto.

Aunque en un principio los "*cookies"* eran utilizados por un servidor para ayudarle a sobrellevar la carga del sistema, ahora es muy usado como fuente de información sobre los hábitos al navegar, ejemplo los anunciantes, para llevar un mejor control del perfil. Cuando se habla del perfil, no se dice el nombre, teléfono, etc., sino de qué es lo interesante, que es y lo que no se le presta atención.

Otro problema de los "*cookies"* es precisamente que se almacenan en el disco duro, por lo que si alguien tiene acceso a él (físicamente a través de una red) puede conocer esos datos y utilizarlos (por ejemplo si hay usuarios y contraseñas).Los navegadores modernos tienen la posibilidad de desactivar a voluntad los "*cookies"* (en Opciones de seguridad) **[3]**.

Normas de Seguridad para una clave perfecta en Internet: Es de gran importancia la seguridad en Internet para proteger la información para una empresa, hay que tener una clave difícil para ladrones informáticos.

Por la computadora personal alguien tiene acceso a las cuentas bancarias, el banco le da a un usuario su clave personal para realizar movimientos en las *"cuentas",* el banco le recomienda modificar la clave para su mayor protección.

Esto es importante porque la mayoría de las personas ponen claves fáciles como pueden ser: fechas de nacimiento, aniversarios, etc., como consecuencia pueden acceder a los datos no autorizados. Tener una mala elección para un *"clave"* en un "*correo electrónico*" donde cualquier intruso puede entrar en los datos de entrada y salida, el pirata obtiene posibles presupuestos, clientes, y pudiera dejar los datos de la empresa **[8]**.

Las normas para una clave segura de los datos, las cuales son usadas en servidores Web, "correo electrónico", accesos bancarios, etc.:

A) Jamás usar claves como palabras, ejemplo nombres comunes, ni del usuario, personajes famosos (políticos, deportistas, etc.), miembros de la familia o nombres de marcas, ciudades, lugares turísticos o vacaciones.

B) Jamás usar claves completamente numéricas que se relacionen con usted.

Ejemplos: teléfonos tanto personales como de empresa, fechas de aniversarios o nacimiento, números de seguridad social, números de la matrícula de el automóvil, todo lo relacionado con usted puede ser de mala elección.

C) Modelo de clave perfecta es que se contenga y mezcle caracteres alfanuméricos, puede escoger caracteres del teclado, seleccionar al azar. Ejemplo: Bn45p$.su9.

D) Debe tener un mínimo de ocho caracteres, si es usada en una llave de programas de encriptación.

E) Jamás compartir las claves.

F) Es recomendable usar claves distintas para cada uno de los correos, o cuentas de bancos, si un individuo obtiene alguna clave de forma ilícita puede ser usada fácilmente la misma clave tanto para cuenta de banco y "*correo electrónico*".

G) Modificar las claves tras un periodo de tiempo, cada 3 meses, algunos bancos fuerzan a los clientes a realizarlo para tener una mejor seguridad para los clientes.

Las Normas que fueron mencionadas con anterioridad son para tener más seguro los pequeños datos personales o de empresa de esos individuos que pueden usar los datos ilegalmente. Es importante poner buenas cerraduras a la casa para que no pueda ser tan fácilmente atacadas por intrusos **[8]**.

A la hora de plantearse en qué elementos del sistema se deben de ubicar los servicios de seguridad se distinguen dos tendencias principales**:**

- **Protección de los sistemas de transferencia o transporte:** El administrador de un servicio, tiene la responsabilidad de garantizar la transferencia segura de la información de forma bastante clara a un usuario final. Ejemplo: el establecimiento de un nivel de transporte seguro, instalación de un "*cortafuego*" *("firewall"),* que defiende el acceso a una parte protegida de una red.

- **Aplicaciones seguras extremo a extremo**: Por ejemplo un "*correo electrónico*" consistiría en construir un mensaje en el cual el contenido ha sido asegurado mediante un procedimiento de encapsulado previo al envío, de forma que este mensaje puede atravesar sistemas diversos y poco fiables, sin por ello perder la

validez de los servicios de seguridad provistos. Aunque el acto de proteger el mensaje cae bajo la responsabilidad del usuario final, es razonable pensar que dicho usuario deberá usar una herramienta aceptable, proporcionada por el responsable de seguridad de la organización.

En el caso de "*claves secretas*" el problema mayor consiste en mantener la privacidad durante la distribución, en caso de que sea inevitable el envío de un punto a otro. Cuando es una "*clave pública"*, los problemas tienen que ver con la garantía de que pertenecen al titular y la confianza en la vigencia (que no haya caducado o sido revocada) **[8]**.

1.2.4.- Virus a través de Internet

Un *"virus"* solamente puede entrar en el equipo de cómputo cuando interactúa con otro equipo. Cuando uno descarga software gratuito en Internet, comparte archivos con amigos o incluso transfiera archivos desde el trabajo a casa, es importante tomar las precauciones indicadas, tanto el equipo y los datos deben permanecer seguros.

En Internet, saber un origen significa descargar sólo archivos de los sitios "*Web*" que se conocen que son seguros. Esto se da a los archivos de programa o a las aplicaciones, ya que los "*virus*" se suelen esconder frecuentemente dentro de programas y se activan sólo al ejecutar dichos programas. Sin embargo, los archivos ejecutables pueden adjuntar archivos "*Web*" de uso especial, archivos de vídeo y agentes activos de software, etc. Aparecerá un mensaje de advertencia en la pantalla siempre que se vaya a descargar una aplicación.

Cuando descargue un archivo, se presentará la opción de abrirlo o guardarlo en disco. Si no está seguro de que la aplicación es segura o no sabe si puede confiar en el sitio del que procede, puede que usted quiera cancelar la transferencia en esa ocasión.

Los antivirus disponibles funcionan, como vacunas virtuales contra "*virus*" conocidos. Es importante tener un programa antivirus actualizado en el equipo y utilizarlo. Tomar en cuenta que constantemente se están desarrollando nuevos "*virus*", de modo que se deben actualizar los programas antivirus con gran frecuencia.

Cualquier información que va por la red pasa realmente por muchas computadoras durante todo el transcurso, existe la posibilidad de que alguien pueda robar la información confidencial. Los piratas o hackers interrumpen para robar datos almacenados. Nadie sabe con qué frecuencia realmente lo hacen.

Es importante utilizar la tecnología de codificación**.** El software de codificación actúa como una caja decodificadora en la televisión. Se mezclan los datos en un código secreto, de manera que nadie lo entienda mientras se está transmitiendo. Los datos llegan al destino, el mismo software decodifica la información. Los códigos pueden ser violados por personas que se burlan de los sistemas de seguridad de computadoras.

Si alguien tiene acceso a Internet a través de una cuenta telefónica, las oportunidades de que alguien irrumpa en la computadora son remotas. Un objetivo de la mayoría de los intrusos es llegar hasta las computadoras del gobierno y las empresariales. Para proteger los sistemas se construye el llamado "*cortafuego*" o "*firewall*", es una capa extra de seguridad ubicada entre las computadoras internas y la Internet **[8]**.

1.2.5.- Seguridad Informática

Cualquier organización debe estar al tanto de los procesos de cambio. Donde se dispone de información continua, confiable y en tiempo, constituye una ventaja fundamental "*Información es poder*", una información se reconoce como:

- Crítica, indispensable para garantizar la continuidad operativa de la organización.
- Valiosa, es un activo corporativo que tiene valor en sí mismo.
- Sensitiva, es conocida por las personas que necesitan los datos.

Identificar los riesgos de la información es de vital importancia, para garantizar la seguridad de la información:

- La Disponibilidad de los sistemas de información.
- La recuperación rápida y completa de los sistemas de información.
- La Integridad de la información.
- La Confidencialidad de la información.

Propuesta:

- Implementación de políticas de Seguridad Informática.
- Identificación de problemas.
- Desarrollo del Plan de Seguridad Informática.
- Análisis de la seguridad en los equipos de computación.
- Auditoria y revisión de sistemas.

Daños que se pueden causar "*virus"* al sistema:

- Software.
- Modificación de programas para que ya no funcionen.
- Modificación de programas para que funcionen con errores.
- Modificación sobre los datos.
- Eliminación de programas y/o datos.
- Acabar con el espacio libre en un disco rígido.
- Hacer que un sistema funcione más lentamente.
- Robo de una información confidencial.
- Hardware.
- Borrado del BIOS: Quemado de un procesador por una falsa información del sensor de temperatura.

- Rotura del disco rígido al hacerlo: Leer repetidamente sectores específicos que fuercen el funcionamiento mecánico **[8]**.

Los "*virus"* se pueden encontrar en:

- Disquetes u otro medio de almacenamiento removible.
- Software pirata en disquetes o CDS.
- Redes de computadoras.
- Mensajes de "*correo electrónico"*.
- Software bajado de Internet.
- Discos de demostración y pruebas gratuitas.

Señalamientos indican la presencia de "*Virus"*:

- Cambios en la longitud de los programas.
- Cambios en la fecha y/u hora de los archivos.
- Retardos al cargar un programa.
- Operación más lenta del sistema.
- Reducción de la capacidad en memoria y/o disco rígido.
- Sectores defectuosos en los disquetes.
- Mensajes de error inusuales.
- Actividad extraña en la pantalla.
- Fallas en la ejecución de los programas.
- Escrituras fuera de tiempo en el disco **[8]**.

1.2.6.- Virus informático

Un "*virus"* informático es un programa de computadora, tal y como puede ser un procesador de textos, una hoja de cálculo o un juego. Un "*virus"* informático ocupa una cantidad mínima de espacio en un disco, se ejecuta sin conocimiento del usuario y se dedica a autorreplicarse, es decir, hace copias de sí mismo e infecta archivos, tablas de partición o sectores de arranque de los discos duros y disquetes para que pueda expandirse lo más rápidamente posible.

Qué son los virus informáticos:

- Son programas de computadora.
- La principal cualidad es la de poder autorreplicarse.
- Intentan ocultar la presencia hasta el momento de la explosión.
- Producen efectos dañinos en el *"huésped"* **[8]***.*

1.2.7.- Tipos de Virus que existen en computación por el efecto de infección

Infectores de archivos ejecutables: Afectan archivos de extensión EXE, COM, BAT, SYS, PIF, DLL, DRV

Infectores directos: Un programa infectado tiene que estar ejecutándose para que un "*virus"* pueda funcionar (seguir dañado y ejecutar las acciones destructivas)

Infectores residentes en memoria: El programa infectado no necesita estar ejecutándose, el "*virus"* se aloja en la memoria y permanece residente infectando cada nuevo programa ejecutado y practicando la rutina de destrucción

Infectores del sector de arranque: Los discos rígidos como los disquetes contienen un *"Sector"* de Arranque, el cual contiene información específica relativa al formato del disco y los datos almacenados en él. Contiene un pequeño programa llamado Boot Program que se ejecuta al bootear desde ese disco y que se encarga de buscar y ejecutar en el disco los archivos del "*sistema operativo*". Este programa es el que muestra el famoso mensaje de "Non-system Disk or Disk Error" en caso de no encontrar los archivos del "*sistema operativo*". Este es el programa afectado por los "*virus"* de *"sector"* de arranque.

Una computadora se infecta con un "*virus"* de *"sector"* de arranque al intentar bootear desde un disquete infectado. En ese momento el "*virus"* se ejecuta e infecta el *"sector"* de arranque del disco rígido, infectando luego cada disquete utilizado en la computadora. Por eso es de gran importancia destacar que como cada disco posee un *"sector"* de arranque, es posible se infecte la computadora con un disquete contenga sólo datos **[8]**.

1.2.8.- Medidas antivirus

Un programa antivirus con el tiempo ya no es de gran utilidad por eso es importante estar actualizado:

- Desactivar el arranque desde disquete en el setup para que no se ejecuten "*virus de boot*".
- Desactivar compartir archivos e impresoras.
- Analizar con el antivirus todo archivo recibido por e-mail antes de abrirlo.
- Actualizar antivirus.
- Activar la protección contra macrovirus del Word y Excel.
- Sea cuidadoso al bajar archivos de Internet.
- No envíe la información personal ni financiera a menos sepa quién la solicita.
- No comparta discos con otros usuarios.
- No entregue a nadie las claves, incluso si lo llaman del servicio de Internet u otro.
- Enseñe a los niños las prácticas de seguridad, sobre todo la entrega de información **[8]**.

1.2.9.- Internet de una forma segura

El Internet es una herramienta increíble, pero oculta ciertos peligros. Se descubren entre 10 y 15 nuevos "*virus"* y "*gusanos*" al día y los hackers están constantemente intentando encontrar nuevas vulnerabilidades puedan ser explotadas. Hay en la actualidad más de 60,000 "*virus*" conocidos y los ataques de los hackers se están convirtiendo en algo común.

Primer Consejo

El peligro: Los “virus” ocasionan daños o eliminan archivos, o incluso borran todo el disco duro. El software de protección contra virus si no está actualizado muestra una protección muy débil contra nuevos virus.

Hacer: Instalar un software de antivirus fiable y analizar regularmente el sistema para comprobar que no existe algún virus. Es importante actualizar las definiciones de “virus” del software de forma frecuente. A diario se descubren nuevos “virus”.

Si se pasa demasiado tiempo conectado, se debe emplear software antivirus que actualice automáticamente las definiciones de “virus”.

Segundo Consejo

El peligro: incluso amigos pueden enviarse sin darse cuenta en virus adjuntos a los mensajes de “correo electrónico”.

Hacer: Es importante se haga una doble revisión antes de hacer doble clic. Si hay un mensaje de “correo electrónico” con un archivo adjunto sospechoso, no se abra – incluso se conoce al emisor. Jamás abrir archivos adjuntos de fuentes desconocidas o archivos adjuntos que no se están esperando y desactivar la apertura automática de archivos adjuntos de “correo electrónico”. No caer en la trampa de creer averiguar o conocer qué es el archivo adjunto.

Windows tiene múltiples extensiones y bastantes programas de correo, sólo se muestra la primera. Ejemplo, puede ver un archivo llamado wow.jpg cuando de hecho el nombre completo es wow.jpg.vbs, y al abrir este archivo adjunto puede activar un VBScript malicioso. Se elimina el mensaje y el archivo adjunto y se contacta con la persona que envió el mensaje **[8]**.

Tercer Consejo

El peligro: Los hackers para tener información o hacerle daño a los archivos, tratan de entrar en la computadora. Cada minuto la computadora está conectada a la red, es vulnerable a intrusiones y al robo de información. Sin importar qué tipo de conexión de Internet tenga.

Hacer: Instalar un “firewall” personal y software de detección de intrusos en la computadora. Con las complejas amenazas que existen hoy en día, la detección de intrusos, se integran a otra capa de seguridad al examinar el contenido del tráfico de Internet para detectar códigos maliciosos y ataques, es determinante.

Cuarto Consejo

El peligro: Las amenazas y vulnerabilidades están evolucionando rápidamente. Es difícil estar al día en los cambios.

Hacer: Es necesario una revisión de la computadora para detectar vulnerabilidades. Si se hace regularmente se puede administrar la seguridad en Internet y protegerlo contra las amenazas.

Quinto Consejo

El peligro: El "navegador Web" puede decirse que se recuerda la contraseña o número de tarjeta de crédito para un uso en el futuro en el mismo sitio. Si se acepta, los datos serán almacenados en la computadora, donde será accesible para los hackers.

Hacer: Jamás debe permitirse que los programas pidan las contraseñas o números de tarjetas de crédito. Es recomendable cambiar las contraseñas constantemente, y no compartirlas con otros. Las contraseñas son una de las primeras líneas de defensa que se tienen para proteger los sistemas.

Una buena contraseña es una combinación de alrededor de seis o más caracteres, que contenga letras aleatorias (mayúsculas y minúsculas), números y símbolos especiales. Jamás usar palabras del diccionario y nombre **[8]**.

Sexto Consejo

El peligro: Los archivos pueden perderse o dañarse debido a la eliminación accidental, problemas con sistemas o el robo de el equipo.

Hacer: Ordenar los archivos regularmente en un disco u otra computadora. Para una mayor protección, guárdalos en un lugar distinto.

Séptimo Consejo

El peligro: En Internet, los niños pueden estar expuestos a material inadecuado o revelar accidentalmente información confidencial.

Hacer: Vigilar a los niños menores de cerca en las actividades de Internet. También, instalar software como un "firewall" personal en la computadora que permita bloquear el acceso a sitios Web cuestionables y servicios potencialmente peligrosos.

Los firewalls personales, también, pueden evitar la información confidencial sea enviada por medio de Internet, "correo electrónico" o mensajes instantáneos.

Octavo Consejo

El peligro: En una conversación por medio de Internet, el individuo con que se esté comunicando puede no ser quien parece ser.

Hacer: Jamás dar información personal a extraños en chats, mensajería instantánea, "correo electrónico", u otros servicios se presente en Internet.

Noveno Consejo

El peligro: Los programas que son gratuitos como protectores de pantalla y juegos que se descarguen de sitios Web a menudo son fuentes de "virus".

Hacer: Jamás descargar programas a menos que sepa que el sitio Web sea de fiar. Es importante asegurar que los servidores que hospedan el sitio están protegidos contra "virus".

Décimo Consejo

El peligro: La información de tipo personal puede ser vendida a empresas de Marketing por medio de los sitios Web en los que uno se registra.

Hacer: La próxima vez que se acceda a Internet para adquirir un producto o registrarse para un servicio asegurarse de leer la política de privacidad del sitio Web. Algunos sitios venden información personal a terceros, lo que puede dar como resultado que se empezará a recibir infinidad de correos electrónicos no deseados ("SPAM") **[8]**.

Décimo primero Consejo

El peligro: Las brechas existentes en el software o aplicaciones son el modo más fácil y rápido de irrumpir en una computadora. Es lo primero que intentará un "hacker".

Hacer: Descargar las actualizaciones relevantes de seguridad suministradas por los fabricantes de software de seguridad. Es recomendable estar al tanto de futuras actualizaciones.

Décimo segundo Consejo

El peligro: Mientras se observa toda la información interesante en Internet, otros pueden estar observando los movimientos y la información que se está viendo.

Hacer: Lo primero debe hacer es desactivar la capacidad de la computadora para recibir "cookies" dando clic sobre la opción "preferencias" del "navegador". Esto va a prevenir que los sitios Web registren los movimientos en Internet **[8]**.

1.2.10.- Agujeros de seguridad

Agujeros de Seguridad Físicos: Cuando el problema es potencial, es por el hecho de dar a personas, sin *"autorización",* acceso físico a la computadora, siempre esto pueda permitir hacer cosas que no deberían ser capaces de efectuar.

Un ejemplo puede ser una sala pública, con estaciones de trabajo, donde sería facilísimo

reiniciar una computadora en modo mono-usuario y revolver con los archivos de la estación de trabajo, si no se hubieran tomado precauciones.

Un segundo ejemplo sería la necesidad de restringir el acceso a cintas backup confidenciales, de otro modo pueden ser leídas por cualquier usuario que tenga una unidad lectora, independientemente de que tenga o no permiso **[28]**.

Agujeros de Seguridad en el Software: El software (daemons, cronjobs) pueden estar comprometidos a realizar tareas que no deberían **[28]**.

Agujeros de Seguridad por Incompatibilidades: Es por falta de experiencia, o por descuido, el administrador del sistema hace funcionar software sobre un hardware para el que no está optimizado, dando lugar a posibles resultados inesperados y fallos pueden dañar seriamente la seguridad del sistema. Es la incompatibilidad entre software y hardware la que crea agujeros de seguridad.

Problemas como este son difíciles de encontrar una vez que un sistema está montado y funcionando, de manera que es muy conveniente leer atentamente la documentación del software y del hardware que se va a montar (o que pretenda atacar) y estar muy atento a cualquier noticia o actualización **[28]**.

Elección y Mantenimiento de la Filosofía de Seguridad: El cuarto problema de seguridad es el de la percepción y el entendimiento. Software perfecto, hardware protegido, y componentes compatibles no funcionan a menos que se haya elegido una política de seguridad correcta y que se hayan puesto en marcha las partes del sistema que la refuerzan.

Teniendo el mejor mecanismo de "*password*" del mundo es inútil si los usuarios creen que la última parte del nombre del login es un buen "*password*". La seguridad está relacionada con una política (o conjunto de políticas/normas) y el funcionamiento del sistema conforme a dicha política.

1.3.- Perfil de un hacker:

"Hacker" es un individuo compulsivo y obsesivo por almacenar conocimientos. Es comunicativo e investiga lo que tenga relación con la electrónica y la informática. Es el tipo de individuos que suelen abrir todos los aparatos de consumo de casa o lee los ficheros de la computadora hasta modificarlos para ver que pasa. Un buen "*Hacker"* prueba y pasa muchas horas pensando en ello. Hay dos tipos de Hackers, Hackers en si y los Hardware Hackers.

El primero practica con las computadoras, el segundo con la electrónica. Pero uno y otro conocen bastante ambos extremos, ya que le son útiles tener conocimientos electrónicos e informáticos. El "*Hacker"* conoce los terrenos en los que reposa la actual tecnología. Un buen "*Hacker"* es alguien que tiene ansias por saber todo, la investigación le gusta y lo que

resulta más difícil de descifrar. Ello se refiere a sistemas de cifrado o sistemas de codificación.

En la actualidad los sistemas de cifrado y codificación están a la orden del día, ejemplo los canales de televisión de pago o cualquier soporte de grabación de datos, así como el CD o DVD. Estos dispositivos se basan en un estándar de codificación de datos, al igual que ocurre con el protocolo de comunicaciones de Internet "*TCP/IP*".

En la actualidad y más en el futuro, la tecnología se fundamenta en protocolos y datos ordenados en cadena. El entendimiento de estas cadenas de datos tratará una superioridad de control sobre cualquier tecnología. Este entendimiento permitirá modificar la información, es un reto para un "*Hacker"*. El "*Hacker"* busca principalmente el entendimiento del sistema tanto de Hardware como de software y descubrir el modo de codificación de las órdenes. En segundo lugar, busca modificar la información para usos propios y de investigación del funcionamiento total del sistema.

Un auténtico "*Hacker"* aprende y trabajan solos y jamás se forman a partir de las ideas de otros, aunque es verdad que las comparten, si estas son interesantes **[28]**.

1.3.1.- Perfil de un cracker

"Cracker" es un usuario informático que invade en secreto la computadora de otro usuario para inspeccionar, alterar o incluso dañar la información y programas que se encuentre en él. También se puede denominar así a un experto en la eliminación de las diversas protecciones de un programa que impiden la copia o uso después de una determinada fecha.

1.3.2.- Diferencias entre hackers y crackers

El "*hacker"* jamás está conforme, no sabe pensar en un mundo con limitaciones, le entusiasma investigar, no permanece callado, no tolera los abusos de los gobiernos, la limitación de la información, de la tecnología, etc. En este sentido el "hacker", le hace un favor a la sociedad violando sistemas informáticos porque si lo hace un espía o enemigo puede causar graves daños.

El "*cracker"* tiene como intención destruir, el *"hacker"* lo contrario. El "*cracker"* realiza fraudes con tarjetas de crédito, el hacker no. A lo máximo puede hacer un "*hacker"* es violar algún servidor o una página Web, lo que hace es dejar constancia de que ese sitio es vulnerable, para que el dueño cambie la seguridad del mismo.

Ejemplo, una empresa se dedica a vender productos, esos artículos pueden ser adquiridos vía Web con el uso de una tarjeta de crédito; ingresa un "*cracker"* y se roba los números de tarjetas de todos los individuos que han comprado en ese sitio, la víctima es la persona que depositó la confianza en ese sitio, y el "*cracker"* goza felizmente la valiosa información que halló en ese lugar, y piensa en cuánto puede vender esos números, y si usted fuese el

"*hacker*" impide que pase eso, y al siguiente día lee los diarios, y nota lo acusan de ladrón **[12]**.

1.3.3.- Normas para evitar el hacking

Lograr una seguridad adecuada en el sistema, es necesario tomar en cuenta diversos aspectos que son de suma importancia; a continuación 10 normas que son las más importantes de manera general:

- No hay que crear acciones que perjudiquen a terceras personas. Ejemplo, quitar el contenido de un directorio de inicio de un usuario no sabe de nada.
- No hay que dar jamás los datos personales en ningún sitio, nada más a las personas que conozca y tenga confianza en ellas.
- No hay que hackear en sistemas gubernamentales. Se encontrarían fácilmente. Las pequeñas empresas y las universidades muchas veces no admiten el lujo de buscar en el caso que no deje la *"IP"* en el sistema.
- No hay que proporcionar datos del sistema en el que esta hackeando a ninguno. Otro *"hacker"* es el que roba el trabajo que se lleva hecho.
- Sólo se destruye aquella información que afecte o dañe algún individuo, no se va destruir nada si no se tiene ningún buen motivo para hacerlo.
- Se cambian solamente los archivos que borren las huellas y los que permitan un futuro acceso.
- Si se detienen es porque han hecho algo mal, siempre haya dejado intacto el sistema no tienen nada que alegar en contra de uno, a no ser haya tenido acceso a información muy privada, de sistemas muy importantes como FBI y NASA. Entonces hay que contactar con un abogado. A un buen *"hacker"* no le caen nunca condenas grandes.
- No hay que permanecer más de dos horas conectado a un sistema cuando se es "*root*".
- No se podrán utilizar nukes, mail bombs, ni cosas por el estilo para molestar a otros individuos, a no ser que se tengan buenos motivos para hacerlo. Es decir, no utilizar esos programas por simple diversión **[3]**.

Hoy en día es muy difícil poder hackear computadoras de proveedores de Internet, ya no suelen tener el *"telnet"* jamás abierto.

Cuando se esté hackeando se tiene que conocer siempre las posibilidades sobre un fichero determinado.

Capítulo

II

Principales formas en como operan los hackers

2.1.- Exploración de un sistema informático

Para ingresar a una computadora de la que se conoce el nombre de una "*cuenta"* (como "*root"* en "*UNIX"*) pero no el "*password"*, una posibilidad es probar todas y cada una de las combinaciones para obtenerla. El método se conoce como fuerza bruta y no es nada sencillo. Si el sistema admite letras de la A a la Z, mayúsculas y minúsculas, igualmente de números del 0 al 9, y un largo de 8 caracteres, las posibilidades de comparación son 218.340.105.584.896, sin contar teclas especiales y todos los passwords son de ocho dígitos.

Lograr un millón de combinaciones por segundo se tardarían unos siete años. Varios sistemas obligan al usuario a esperar unos segundos entre cada intento de login erróneo, es fácil sospechar que tal vez no se conozca del acercamiento más práctico a la solución.

Las personas usan sistemas, no por abstracciones matemáticas. Eso admite pensar caminos más cortos: Poca gente, ejemplo, eligen recordar un "*password"* como "Hks4Ijdh"; usualmente se eligen claves como "Gustavo", "Mnemonic", "aeiou" o cualquier otro fácil de detener en la memoria. Es bastante común usar el mismo nombre de *"login"* como "*password"*: un usuario ingresa "pepe", entonces la clave puede ser "pepe". Por lo regular escogen el nombre para un "*password"*.

Se acostumbra el uso de una sola letra, las posibilidades se reducen a cincuenta y dos, tomando en cuenta mayúscula y minúscula. Un usuario elige el nombre del sistema para una contraseña o hasta la palabra "*password*". Nombre de lugares, personas, marcas con elecciones muy comunes.

En un programa, el password Cracker, admite comprobar automáticamente los password corrientes. Es raro que se use hacia un sistema en tiempo real: la totalidad de las veces se consigue el archivo encriptado de passwords y se verifica contra el programa. Las claves quedan encriptadas con un algoritmo de una sola dirección, aquel que admite *"encriptar"* un texto pero no *"desencriptarlo".*

Esto quiere decir, no existe forma de conseguir "*password"* a partir de un archivo. Para verificar si el "*password"* ingresado por el usuario es correcto, el sistema encripta la clave que ingresa y la compara con el archivo. Un "*hacker"* tiene un archivo de contraseñas obtiene una palabra, encriptarla y ver si está en el archivo. En *"Unix"* el archivo de passwords es legible por cualquiera y en numerosos sistemas a través del "*FTP"* anónimo se obtiene.

Los programas chequeadores logran comprobar setecientos "*password"* por segundo si una computadora es una 486: El término es encriptado en un diccionario (preparado por el "*hacker"*) y revisan contra todos los passwords del archivo. Las claves se pueden adivinar en determinadas horas o, si en un día usan diccionarios grandes. Este método no descubrirá contraseñas tal "PdejkK", descubre las más comunes. La defensa más usada para impedir esta técnica es admitir algunos intentos y si no hay un *"password"* correcto desconectar la computadora.

Otra forma seria buscar cuentas sin passwords, o passwords default. Cuando los hackers conocen un sistema determinado el usuario "admin." Viene configurado con password "admin", es lo principal que prueban **[15]**.

Sucede con los que no son demasiado usados, como una cuenta para mantenimiento de emergencia, suele llamarse "admin2" y no tener "*password"* por default. El "*administrador"* puede haber olvidado corregirlo y puede ignorar que existe.

Además los procesos automáticos pueden aprovecharse. En la red puede existir un usuario "backup" sin "*password"*, o con una obvia como "backup", se utilice para realizar una copia de seguridad al ingresar. Debe permitir a todos los archivos; es apetecible hacia un "*hacker"* puede usarlo si se conecta con ese nombre, aborta el backup y logra permanecer en el shell de comandos.

Ningún sistema muestra en pantalla el "*password"*, una vista rápida puede seguir el movimiento de los dedos y descubrir las letras que marcó el usuario: la técnica se denomina shoulder surfing y consiste en el antiguo truco de mirar discretamente por sobre el hombro del otro. Numerosos hackers disimulados saben obtener interesantes datos frente a teléfonos públicos ejemplo: claves de servicios de llamadas de larga distancia.

Los programas de comunicaciones son una fuente de passwords. Varios Terminate, permiten guardar la clave del usuario junto con el teléfono del sistema. Otros dejan realizar *"Scripts",* programas que facilitan la comunicación con diversos lugares, donde está el "*password"* sin "*encriptar"*. Obtener una contraseña de esa manera requiere acceso físico a la computadora o, a través de una red, donde se encuentre el directorio **[28]**.

2.2.- El atacante

Los Troyanos pueden utilizarse para extraer información confidencial o para hacer daño. Un "*Troyano"* suele ser más utilizado para espiar y robar información delicada (espionaje industrial). El interés del atacante podría incluir pero no estar limitado a:

- Información de Tarjetas de crédito (utilizadas a menudo para registro de dominios o compras).
- Cualquier dato de cuentas (contraseñas de correo, contraseñas de acceso telefónico, contraseñas de servicios Web, etc.).
- Documentos confidenciales.
- Direcciones de *"correo electrónico"* (ejemplo, detalles de contacto de clientes)
- Diseños o fotografías confidenciales.
- Información de calendario relativa al paradero de los usuarios.
- Utilización del equipo para propósitos ilegales, como "*hacking"*, scan, flood o infiltrarse en otros equipos de la red o de Internet **[15]**.

2.2.1.- Tipos de Troyanos

Un troyano es un programa que modifica su función habitual para conseguir algún objetivo que nos interese. En principio, una de las utilidades más importantes de los troyanos es dejar backdoors con los típicos troyanos del login, telnetd, fingerd y demás.

En principio hay muchos administradores que entran con una cuenta de usuario normal y cuando necesitan hacer algo que requiere que sean root, ejecutan el comando su que permite cambiar el usuario a root. Esto se hace ya que no es conveniente ser root en la computadora (sobretodo a altas horas de la mañana) y si por ejemplo haces un rm sobre un fichero importante y no eres root, no pasa nada en general ya que no tendrás permisos para hacerlo.

Para usar este sistema, hay que buscar quien usa su. Esto se puede hacer viendo en el /var/adm/messages (si tienes permisos para leerlo), el su log u otros archivos de log dependiendo del sistema en el que estés, o bien entrar en los directorios HOME (si tienes permisos) y ver los history (que son distintos dependiendo del shell que se usa.. están explicados en el apartado de borrar huellas) ya que en esos archivos se ven todos los comandos ejecutados por el usuario.

Es decir, con esta técnica también tenemos que obtener un passwd de administrador, pero hay que tener en cuenta que si por ejemplo es una computadora con dos users con id=0 y que además cada uno de ellos entra con una cuenta normal para hacer luego su, hay 4 cuentas de “root” por lo que pasando unos cuantos diccionarios es fácil que caiga alguna de las cuatro.

En fin, suponiendo que tenemos la cuenta de ese user que luego hace su root, se ha de cambiar la variable path a un directorio donde pongamos el su troyano, es decir, el código del su, lo compilamos y lo introducimos en un directorio cualquiera. Ese directorio lo ponemos en el path de manera que este antes que el directorio por defecto donde esta el su verdadero. Por ejemplo, si el path es:

PATH=/bin/:/sbin/....

Tendría que ponerse si el directorio donde esta el troyano de su, se llama /.troyano:
PATH=/.troyano:/bin:/sbin.....

Así, si el administrador que no ha entrado con la cuenta de root hace su, entrara el troyano que lo que hace pedirle el passwd y le dice que es un passwd incorrecto con lo que el pensara que se ha equivocado introduciendo el dato y guarda el passwd en un fichero determinado. Tras esto, el su troyano se borra automáticamente por lo que pierde el rastro.

Los troyanos están agrupados en categorías principales. Es difícil clasificar un "*troyano"* en un solo grupo ya que a menudo tiene atributos donde lo sitúan en ciertas categorías se pueden clasificar en: **[27].**

2.2.2.1.- Troyanos de acceso remoto

Los troyanos de acceso remoto son los más conocidos, porque proporcionan al atacante un control total del equipo de la víctima. Ejemplos: Troyanos Back Orifice y Netbus. Es dar al atacante acceso completo al equipo de alguien, un acceso total a archivos, conversaciones privadas, datos de cuentas, etc.

Actúan como un servidor y a menudo manejan un puerto que no está disponible para atacantes de Internet. Un equipo se sitúa detrás de un *"cortafuego",* es imposible que un hacker remoto pueda conectar con el "*troyano"* (los puertos han sido cerrados por usted). Un "*hacker"* interno (se encuentra detrás de los cortafuegos) puede conectar con esta clase de troyanos sin ningún problema **[27]**.

2.2.2.2.- Troyanos que envían datos (contraseñas, pulsaciones de teclado, etc.)

Los Troyanos envían datos al "*hacker"* con información como contraseñas (ICQ, "*IRC"*, *"FTP", "HTTP"*) o alguna información confidencial como puede ser tarjetas de crédito, registros de conversaciones, listas de direcciones, etc. El "*troyano"* puede buscar información específica de cierto lugar en particular, o puede instalar un recogedor de pulsaciones de teclado y enviar las teclas pulsadas al "*hacker"* (el cual puede extraer las contraseñas de los datos).

Los datos que son capturados se envían a la dirección del correo del atacante, se encuentra en algún servicio de correo Web gratuito. Los datos que son capturados se envían mediante la conexión al sitio Web del *"hacker"* – utilizando un proveedor de *"Web"* gratuito – y enviando los datos vía formulario Web. Ambos métodos no se notarían y pueden hacerse desde cualquier equipo de la red con acceso a correo e Internet.

Hacker internos y externos utilizan troyanos envían datos para tener acceso a información confidencial sobre la empresa **[27]**.

2.2.2.3.- Troyanos destructivos

Los troyanos destructivos se encargan de acabar y eliminar archivos. Pueden eliminar automáticamente todos los archivos principales del sistema del equipo ejemplo: archivos .ini o .exe y .dll. Los troyanos pueden ser activados por el atacante o trabajar como una "*bomba lógica"* se inicia a una fecha y hora específica.

El "Troyano" destructivo es un peligro para cualquier equipo de la red. Es similar a un "*virus"*, con el "*troyano"* destructivo la intención es atacar y en consecuencia no puede ser detectado por el software anti-virus **[27]**.

2.2.2.4.- Troyanos del ataque denegación de servicio (DoS)

Estos Troyanos dan al atacante el poder de iniciar un ataque de denegación de servicio (DoS) si hay suficientes víctimas. La idea principal es que si tiene 200 usuarios aDSL infectados y se ataca a la víctima simultáneamente desde cada uno, esto generará un TRAFICO PESADO (más de lo que el ancho de banda de la víctima puede soportar, en la mayoría de los casos), haciendo el acceso a Internet se venga abajo.

Otra variación de los Troyanos DoS es un Troyano bomba de correo, cuya principal meta es infectar tantos equipos como sea posible y simultáneamente atacar direcciones de correo concretas con asuntos aleatorios y contenidos que no pueden ser filtrados.

De nuevo, un Troyano DoS es similar a un virus, puede crearse con el propósito de atacarle y, en consecuencia, no puede ser detectado por su software anti-virus **[27]**.

2.2.2.5.- Troyanos Proxy

Estos Troyanos convierten el equipo de la víctima en un servidor proxy, haciéndolo disponible para todo el mundo o solo para el atacante. Se utiliza para hacer Telnet, ICQ, IRC, etc. anónimo, para hacer compras con tarjetas de crédito robadas, y para otras actividades ilegales. Esto proporciona al atacante un completo anonimato y la oportunidad de hacer cualquier cosa desde su equipo, incluyendo la posibilidad de lanzar ataques desde su red.

Si las actividades del atacante son detectadas y rastreadas, esto no los llevará al atacante sino a usted - lo que podría poner en aprietos legales a su organización. Estrictamente hablando, usted es responsable de su red y de los ataques lanzados desde ella **[27]**.

2.2.2.6.- Troyanos FTP

FTP(File Transfer Protocol) (Protocolo de transferencia de archivos). Es una aplicación de Internet que permite transferir archivos de una computadora a otra. Las siglas FTP también pueden hacer referencia al propio protocolo. Estos Troyanos abren el puerto 21 (el puerto para transferencias FTP) y permite al atacante conectar al equipo vía FTP.

2.2.2.7.- Deshabilitadores de software de seguridad

Estos son Troyanos especiales, diseñados para parar/eliminar programas como software anti-virus, cortafuegos, etc. Una vez estos programas son deshabilitados, el hacker puede atacar su equipo más fácilmente.

Los deshabilitadores de software de seguridad son habitualmente diseñados para software concreto de usuario final como cortafuegos personales, y en consecuencia menos aplicables a entornos corporativos **[27].**

2.3.- Diferencia entre un Virus y un Troyano

SISTEMA ANTIVIRUS

Los antivirus son programas cuya función es detectar y eliminar virus informáticos y otros programas maliciosos (a veces denominados malware).

Básicamente, un antivirus compara el código de cada archivo con una base de datos de los códigos de los virus conocidos, por lo que es importante actualizarla periódicamente a fin de evitar que un virus nuevo no sea detectado. También se les ha agregado funciones avanzadas, como la búsqueda de comportamientos típicos de virus (técnica conocida como heurística) o la verificación contra virus en redes de computadoras.

Normalmente un antivirus tiene un componente que se carga en memoria y permanece en ella para verificar todos los archivos abiertos, creados, modificados y ejecutados en tiempo real. Es muy común que tengan componentes que revisen los adjuntos de los correos electrónicos salientes y entrantes, así como los scripts

y programas que pueden ejecutarse en un navegador Web (ActiveX, Java, JavaScript).

Un *"virus"* daña los archivos y programas, un *"troyano"* es un programa que permite a quien te lo envía o quien tiene la habilidad de encontrar y usar para ingresar a la computadora y hacer dueño de "todo" lo que se tenga en la PC.

TROYANO

Se denomina troyano (o caballo de Troya, traducción más fiel del inglés Trojan horse aunque no tan utilizada) a un virus informático o programa malicioso capaz de alojarse en computadoras y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de socavar la información.

Suele ser un programa pequeño alojado dentro de una aplicación, una imagen, un archivo de música u otro elemento de apariencia inocente, que se instala en el sistema al ejecutar el archivo que lo contiene. Una vez instalado parece realizar una función útil (aunque cierto tipo de troyanos permanecen ocultos y por tal motivo los antivirus o antitroyanos no los eliminan) pero internamente realiza otras tareas de las que el usuario no es consciente, de igual forma que el Caballo de Troya que los griegos regalaron a los troyanos.

Habitualmente se utiliza para espiar, usando la técnica para instalar un software de acceso remoto que permite monitorizar lo que el usuario legítimo de la computadora hace y, por ejemplo, capturar las pulsaciones del teclado con el fin de obtener contraseñas u otra información sensible.

Los Troyanos acceden a datos privados y confidenciales, como direcciones "*IP"*, nombres de usuario y passwords, etc. La mayoría de ellos tienen la capacidad de enviar datos son recogidos al autor del *"virus".* A diferencia de otros códigos maliciosos, los troyanos tienen

la particularidad de que no se reproducen infectando a otros ordenadores, la capacidad de propagación que tienen es muy limitada **[7].**

GUSANO

Es un virus o programa autoreplicante que no altera los archivos sino que reside en la memoria y se duplica a sí mismo. No necesita un programa huésped donde alojarse. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.

Es algo usual detectar la presencia de gusanos en un sistema cuando, debido a su incontrolada replicación, los recursos del sistema se consumen hasta el punto de que las tareas ordinarias del mismo son excesivamente lentas o simplemente no pueden ejecutarse.

El 18 de enero, un gusano llamado Storm comenzó a llegar como anexo a mensajes de e-mail cuyo asunto tenía frases como 230 muertos en una tormenta que azota Europa.

Más de 42.000 variaciones distintas del programa malicioso se diseminaron en un período de 12 días, dice la compañía de seguridad Commtouch. El violento ataque estaba diseñado para evadir la detección tradicional de virus, que se basa en firmas y debe reconocer un pedazo específico del programa malicioso para atraparlo.

El gusano de Storm es un ejemplo de cómo los escritores de virus tratan de mantenerse un paso delante de los programas antivirus produciendo nuevas variaciones exitosas de programas maliciosos. Los malhechores también intentan ocultar sus actividades (y mantenerse fuera de la base de datos de firmas) con ataques localizados que envían un pequeño grupo de programas maliciosos a una sola compañía u organización. Estos ataques suelen tener un diseño más avanzado que el promedio; por ejemplo, usan direcciones de origen falsificadas de empleados de compañías reales para enviar e-mail con virus.

Para contraatacar, las compañías de seguridad están agregando la protección anticipatorio, cuya eficacia no depende de una firma de virus. Hoy, esta protección es, absolutamente necesaria, una analista de seguridad trata de protegerse de los peligros desconocidos y localizados, dice ella.

Un enfoque anticipatorio emplea lo que se conoce como técnicas heurísticas para examinar la programación de un virus y detectar segmentos de código o instrucciones sospechosos.

Este método frecuentemente puede detectar una nueva variante de programa malicioso por ejemplo, uno de los muchos gusanos Storm-. En tanto que la técnica heurística examina el interior de un programa malicioso, el análisis de comportamiento, otra técnica de protección anticipatorio, lo examina desde afuera mientras ejecuta su trabajo. Las acciones sospechosas, como la ejecución desde un directorio temporal, pueden hacer que el programa antivirus marque un archivo como software malicioso potencial.

MYDOOM

Es un gusano de correo electrónico muy conocido, el cual venía adjunto en un mensaje de correo, cuando se abría el correo, se mostraba el bloc de notas el cual tenía caracteres aleatorios. El gusano busca en los archivos posibles direcciones de correo electrónico para poder esparcirse.

Otra de sus funciones era la de abrir un backdoor con la que se podían generar ataques a la computadora afectada.

2.4- Los hackers y ataques

Los *"piratas"* tienen pocas armas (computadora y una línea telefónica) tienen un cerebro desarrollado, un "*hacker"* tarda meses en vulnerar un sistema ya que cada vez son más sofisticados.

Los que se introducen en los sistemas de aeropuertos produciendo un desconcierto en los vuelos y en los horarios de los aviones. Pero aquí hay una diferencia. Los crackers viene de crack= destruir, son individuos buscan molestar a otros, piratear software protegido por leyes, destruir sistemas muy complejos mediante la transmisión de poderosos *"virus",* etc. Se diferencian con los hackers porque no poseen ningún tipo de ideología cuando realizan los "trabajos". El objetivo principal de los hackers es no convertirse en delincuentes sino "pelear contra un sistema injusto" utilizar como arma el sistema **[7]**.

Los hackers se consideran como chicos son capaces de violar sistemas informáticos de grandes empresas y del gobierno.

El "*hacker"* puede realizar dos tipos de actividades: acceder a un sistema informático, o explorar y aprender a utilizar un sistema informático.

Una vez que se ha conseguido acceder al sistema cuando se ha obtenido una clave de acceso. El sistema ha sido utilizado sin autorización, el "*hacker"* no suele tener, términos generales, acceso a los manuales de operación y recursos disponibles para los usuarios legítimos para conocer el uso se da al sistema.

La totalidad de los hackers no destruyen y no dañan los datos. El hacerlo iría en contra de la intención de mezclarse con el usuario normal y atraería la atención sobre su presencia, haciendo la *"cuenta"* se está usando sea borrada. Gastar tiempo en conseguir la cuenta, el *"hacker"* coloca una alta prioridad para que él no sea descubierto.

Un "*hacker"* es un individuo tiene la capacidad, habilidad y deseo de explorar un sistema informático. Conseguir el acceso, es decir, adivinando la clave no es suficiente para conseguir la denominación. Debe existir una ambición de explotar y usar el sistema después de haber accedido a él. Una vez que los intrusos lograr acceder al sistema algunos no mantienen el interés.

Las claves de acceso y las cuentas suelen intercambiarse y ponerse a disposición de un uso general. Conseguir el acceso es una parte “fácil”, por aquellos que utilizan y exploran los sistemas que tienen un mayor prestigio **[7]**.

2.4.1.- Ataques a la información y amenazas

Los ataques sirven a varios objetivos incluyendo fraude, robo de información, extorsión, venganza o simplemente el desafío de penetrar un sistema. Esto puede ser realizado por empleados internos que abusan de los permisos de acceso, o por atacantes externos acceden remotamente o interceptan el tráfico de la red.

Los genios informáticos, lanzan desafíos para quebrar tal o cual programa de seguridad, captar las claves de acceso a computadoras remotas y utilizar las cuentas para poder viajar por el ciberespacio, ingresar a redes de datos, sistemas de reservas aéreas, bancos.

Los administradores de todos los sistemas, disponen de herramientas para controlar “todo vaya bien”, si los procesos son los normales o si existe algún movimiento sospechoso, ejemplo un usuario esté recurriendo a vías de acceso para las cuales no está autorizado o alguien intente ingresar varias veces con claves equivocadas que esté probando. Los movimientos del sistema son registrados en archivos, revisan diariamente los operadores **[16]**.

2.4.2.- Firma digital

Para garantizar la integridad de un mensaje, se añade a un conjunto de caracteres asociados solamente pueden generar el remitente a través del uso de la “*clave privada*” pero esto puede ser confirmado por el destinatario. Un mínimo cambio en el mensaje, puede ser descubierto. De forma similar, se procede en una generación de firma digital. Se puede decir que todos estos procedimientos están basados en la posibilidad de que una de las partes tiene la capacidad de generar códigos que ninguna persona puede hacer, pero sí pueden descifrar o verificar.

El cifrado con “*clave pública”* admite crear firmas digitales hacen posible certificar la procedencia de un mensaje, en otros términos, afirmar que proviene de quien dice. De esta forma se puede evitar alguien substituya a un usuario y envíe mensajes falsos a otro usuario, como un impedimento de falsificar la firma. También, garantizan la integridad del mensaje, es decir, que no ha sido alterado durante la transmisión. La firma se aplica a un mensaje completo o puede ser algo añadido al mensaje.

Las firmas son especialmente de gran utilidad cuando la información debe pasar por las redes sobre las que no se tiene control directo y, en resultado, no existe posibilidad de comprobar de otra manera la procedencia de los mensajes.

Existen varios métodos para hacer uso de la firma digital, uno de ellos es el siguiente: "quien envía el mensaje lo codifica con la “*clave privada”*. Para descifrarlo, sólo puede hacerse con la *“clave pública”* correspondiente a dicha persona o institución.

Si efectivamente con dicha clave se descifra es señal de quien dice envió el mensaje, realmente lo hizo" **[27]**.

Hay diversos métodos para hacer uso de la firma digital, como el siguiente: "La persona envía el mensaje lo codifica con la *"clave privada".* Para descifrarlo, Firma Digital y "*Autentificación"*:

E: "*Encriptar"* / D: "*Desencriptar"*.

KP: Encriptación utilizando la "*Clave Privada"*.

KV: Encriptación utilizando la "*Clave Pública"*.

M: Mensaje.

2.4.3.- Puerto

Cuando se conecta a otra computadora, para gestionar la información, lo crea a través de algunos "puertos". Éstos vendrían a ser "puertas" a un ordenador. Saber entender el ordenador como si fuera ya que, para salir de la casa, lo hace por algunas "puertas" (serían los puertos del ordenador).

También, se pueden recibir visitas en la casa (ordenador). Por tanto aparecerá alguien y pretenderá entrar por una determinada "puerta" (puerto). Si tiene esa puerta cerrada, queda claro el otro individuo no puede entrar, pero si queda abierta, si puede pasar. Es decir, en un ordenador sabe establecer:

- **conexiones de salida**: Al salir de alguna de las puertas (puertos en lenguaje informático) y entrar por una de las puertas del otro ordenador.
- **conexiones de entrada**: Un individuo salió por un puerto en un ordenador remoto y entra en el ordenador por un puerto en concreto **[27]**.

Entran los intrusos: Para que un atacante consiga controlar tu ordenador, primeramente ha tenido entrar en él por una puerta abierta, es decir, por un puerto de comunicaciones no estaba convenientemente asegurado. Igual en tu casa no dejas las ventanas y las puertas abiertas de par en par, en tu equipo debes tener cuidado para evitar intrusiones siempre que estés conectado a la Red.

Un PC necesita para comunicarse con el resto de ordenadores conectados a Internet tener una dirección electrónica y poder identificarse con los demás. Si haces una petición, por ejemplo, de una página Web, el servidor tiene que saber a quién se la envía. Esa dirección electrónica es la dirección IP (número de 4 grupos de cifras de la forma xxx.xxx.xxx.xxx).

Pero eso no es suficiente, ya en Internet se pueden utilizar muchos y diversos servicios y es necesario poder diferenciarlos. La forma de hacerlo es mediante los puertos.

Imagina un edificio de oficinas: éste tiene una puerta de entrada al edificio (sería la IP) y muchas oficinas dan servicios (los puertos). Eso nos lleva a la dirección completa de una oficina viene dada por la dirección postal y el número de la oficina. En el caso de Internet viene dado por la dirección IP y por el número de puerto. Así por ejemplo, un servidor Web escucha las peticiones le hacen por el puerto 80, un servidor FTP lo hace por el puerto 21, etc.

Es decir, los puertos son los puntos de enganche para cada conexión de red que realizas. El protocolo TCP (el utilizado en Internet) identifica los extremos de una conexión por las direcciones IP de los dos nodos (ordenadores) implicados (servidor y cliente) y el número de los puertos de cada nodo.

Como hemos indicado al principio, cuando te conectas a Internet tu proveedor te da, para esa conexión, una dirección IP te identifica para que puedas comunicarte con el resto de Internet. Cuando solicitas un servicio, por ejemplo una página Web, ésta también tiene asignada una dirección IP.

De esta forma tenemos identificados el origen y destino del flujo de información. Pero este flujo tiene muchos caminos alternativos, por lo que dependiendo del tipo de servicio o información deseas intercambiar, se han establecido las vías pertinentes. Estos caminos son los puertos de comunicaciones. De forma cuando haces tu petición de información o servicios, se lleva a cabo mediante un puerto específico de tu ordenador a un puerto del servidor Web igualmente predeterminado. Esta es la forma en que la información navega por Internet, estableciendo el punto de partida, el punto de llegada y la ruta a seguir.

Existen más de 65.000 puertos diferentes usados para las conexiones de Red. Si en tu ordenador se pasa a través del correo electrónico un virus capaz de abrir alguno de estos puertos, el resultado es que la puerta de tu casa quedará abierta.

Puedes estar seguro de que cualquier puerto abierto que tú no controles (en ocasiones es posible que ni tan siquiera sepas que existe) es una invitación para que puedan observar en tu equipo, robarte información confidencial y ocasionarte multitud de problemas **[27]**.

Combatirlos. Antes de entrar, hay que llamar: La posibilidad de que alguien entre en tu ordenador y pueda ver todo lo que allí guardas, desde archivos poco relevantes hasta datos de gran importancia como números de cuentas bancarias, resulta perturbadora. Afortunadamente, colarse en un PC no es tan sencillo si se ponen las barreras suficientes para que esto no ocurra.

Una medida básica de seguridad es conocer qué puertos tiene tu equipo, cuáles están abiertos y por qué lo están. Entre estos últimos, además, debes tener en cuenta cuáles no estás utilizando y los que pueden ocasionar un problema de seguridad.

Existen dos formas básicas de combatir a los intrusos una vez que ya hemos recabado toda la información acerca de los puertos. La primera de ellas consiste en bloquear los puertos, es decir, cerrar aquellos que no quieras utilizar.

Otro método, mucho más efectivo, es cerrarlos todos e instalar un firewall o cortafuegos. Este programa sólo permite el tráfico con Internet que tú aceptes, haciendo una consulta cada vez necesita abrir un puerto para que algo salga o entre en el equipo **[27]**.

"High ID" y "Low ID"

- **High ID (ID Alta):** Es un usuario sabe conectarse a otro y, lo importante, es cualquier otro pueda conectarse a él. Ser un "High ID" cede, en general, más fluidez en las conexiones y mayor velocidad de bajada.

- **Low ID (ID Baja):** Es un usuario no sabe recibir conexiones exteriores ya que posee el "clientport" cerrado (Por alguna razón, en ese puerto no sabe escuchar si hay intentos de conexiones exteriores). Para lograr bajar o subir, constantemente debe establecer él la conexión con el otro cliente.

Con las definiciones anteriores se puede notar un cliente High ID no se puede conectar directamente a un cliente Low ID (no admite la conexión).

Para remediar este problema, lo que se hace es el cliente High ID se conecta al servidor al que el cliente Low ID está conectado y le exige al servidor que pretende bajar un archivo del cliente Low ID. Así que el cliente Low ID se conectó activamente al servidor, el servidor le dice: "Tal cliente High ID quiere tal archivo". En ese instante el dciho Low ID se conecta al High ID y empieza a enviarle el archivo. Este proceso, sin embargo, crea una sobrecarga importante a los servidores, debe tomar ciertas medidas para que no pase esto.

Lo que se extrae de este proceso es que dos clientes Low ID nunca pueden conectarse. Nadie de los dos puede aceptar conexiones directas de diferentes clientes. **[27]**

Capítulo

III

Ataques típicos efectuados por un hacker

3.1.- Ataques más utilizados por los hackers

Los ataques más usuales de los hackers se dividen en categorías generales que se relacionan entre sí, el uso de un método en una categoría admite el uso de diferentes métodos en otras. Ejemplo: después de crackear un *"password"*, un intruso realiza un *"login"* como legítimo usuario para que navegue entre los archivos y explotar vulnerabilidades del sistema.

El atacante puede adquirir derechos a lugares fueran dejar "*virus"* y "*bombas lógicas"* para paralizar todo un sistema antes de huir **[26]**.

3.1.1.- Eavesdropping y packet sniffing

Numerosas redes son vulnerables al eavesdropping, también conocido como la intercepción pasiva (sin modificación) del tráfico de red. En Internet esto se realiza por packet sniffers, son programas que monitorean los paquetes de red están direccionados a la computadora donde están instalados.

El "*sniffer"* es colocado tanto en una estación de trabajo conectada a red, como a un equipo router o a un *"gateway"* de Internet, esto es realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías.

El método se utiliza para capturar loginIDs y passwords de usuarios, viajan claros (sin encriptar) al ingresar a sistemas de acceso remoto (RAS). Además se utilizan para capturar números de tarjetas de crédito y direcciones de e-mail entrante y saliente. El análisis de tráfico se utiliza para establecer relaciones entre organizaciones e individuos **[26]**.

3.1.2.- Snooping y downloading

Snooping y Downloading igual que el sniffing se encarga obtener la información sin modificarla y se diferencia básicamente en el tráfico de red, el atacante ingresa a los documentos, mensajes de e-mail y cualquier información esté guardada, realizando un downloading de la información de una computadora. En el Snooping la finalidad es el robo de información o software **[26]**.

Figura 3.1.- Mensajes de E-mail

El snooping tiene como objetivo obtener información de una red a la que están conectados sin modificarla, similar al sniffing ([[packet sniffer]]). Además de interceptar el tráfico de red, el atacante accede a documentos, mensajes de e-mail y otra información privada guardada en el sistema, guardando en la mayoría de los casos esta información en su equipo.

Aunque el resultado es en muchos aspectos similar al sniffing, técnicamente poco tiene que ver con éste: en ningún momento se capturan datos que circulan por la red, la tarjeta no trabaja en modo promiscuo (es más, ni siquiera es necesario un [[interfaz de red]]), etc; simplemente, la información que un usuario introduce en un terminal es clonada en otro, permitiendo tanto la entrada como la salida de datos a través de ambos.

El snooping se puede realizar por simple curiosidad, pero también se realiza con fines de espionaje y robo de información o software. Los casos más resonantes de este tipo de ataques fueron: el robo de un archivo con más de 1.700 números de tarjetas de crédito desde una compañía de música mundialmente famosa, y la difusión ilegal de reportes oficiales reservados de las [[Naciones Unidas]], acerca de la violación de derechos humanos en algunos países europeos en estado de guerra.

3.1.3.- Tampering o data diddling

En Tampering O Data Diddling el ataque trata de modificar desautorizadamente a los datos, o al software instalado en un sistema, mediante el borrado de archivos. La persona que realiza el ataque tiene derechos de supervisor o administrador, con una capacidad de disparar y borrar cualquier información puede terminar en la baja total del sistema en forma deliberada. Para recuperar la información ha sido alterada o borrada es necesario el administrador dé: dar de baja las horas o días.

Esto puede ser realizado por insiders u outsiders, con un fraude o dejar fuera de servicio un competidor.En los fraudes bancarios crean falsas cuentas para derivar fondos en otras cuentas, las calificaciones de exámenes son modificados por los estudiantes, también los contribuyentes pagan para que la deuda sea anulada por algún impuesto en el sistema municipal **[26]**.

3.1.4.- Spoofing

El Spoofing es utilizado por otros usuarios, para realizar tareas de snoofing o tampering. Spoofing consigue el nombre y "*password"* de un usuario legítimo cuando se ingresa al sistema, toma acciones en nombre de él, como puede ser el envío de falsos e-mails.

El intruso utiliza un sistema para conseguir información e ingresar en otro, y luego utiliza este para entrar en otro, y en otros. Este proceso se llama Looping, la finalidad es evaporar la identificación y la ubicación del atacante. Puede tener muchas estaciones el camino que es tomado desde el origen hasta el destino, que exceden, obviamente, a los límites de un país.El envío de falsos e-mails es otra forma de spoofing permitida por las redes. Es donde el atacante envía a nombre de otra persona e-mails con otros objetivos **[26].**

3.1.5.- Jamming o flooding

Satura los recursos del sistema de la víctima dejándola sin memoria, sin espacio libre en el disco duro.

Por ejemplo el atacante satura el sistema con peticiones de conexión. En lugar de enviar la *"IP"* verdadera de emisor, envía una falsa. El sistema no encuentra una respuesta de la *"IP"* falsa, se mantendrá el buffer abierto esperando información pero bloqueando la comunicación con la *"IP"* verdadera. Los ataques frecuentes a proveedores son usando el ping de la muerte (bloquea el equipo) **[26].**

3.1.6.- Net flood (inundación de la red)

El Net Flood es un ataque dañino y tiene poca defensa en la red atacada. En estos casos, la red víctima no puede hacer nada. Aunque filtre el tráfico en los sistemas, las líneas estarán saturadas con tráfico malicioso, incapacitándolas para cursar tráfico útil. Un ejemplo habitual es el de un teléfono: si alguien quiere molestar, sólo tiene que llamar, de forma continua.

Si se descuelga el teléfono (para que deje de molestar), tampoco se puede recibir llamadas de otras personas. Este problema es habitual, por ejemplo, cuando alguien intenta mandar un fax empleando el número de voz: el fax insiste durante horas y sin que el usuario llamado pueda hacer nada al respecto **[26]**.

3.1.7.- Mail bombing-mail spamming-junk mail

El Mail Bombing se encarga del envío indiscriminado y masivo de un mensaje idéntico a una misma dirección, saturando el correo electrónico (mailbox) del destinatario.

El Mail Spamming es un bombardeo publicitario que se encarga de enviar un Emilio a miles de usuarios, si hayan o no solicitado el mensaje. Es utilizando en las empresas para publicar los productos.

El junk mail o correo basura. Es una propaganda indiscriminada y masiva a través de emilios. No se puede diferenciar del spamming

El mail spamming y el junk mail no se consideran como ataques DoS auténticos, mucho que moleste no están orientados a saturar ningún sistema, aunque en ocasiones se utiliza para que éste se produzca **[26]**.

3.2.- Ataques que aprovechan las vulnerabilidades de los sistemas

Los ataques a los servidores se ejecutan con otros servidores que trabajan como "zombies" esto significa los servidores zombie; en los que instala un programa automático (daemon) pasa desapercibido para el propietario del servidor. Al recibir la orden de ataque, a los zombies comienza a disparar peticiones contra la víctima.

Con esta técnica el atacante hace más difícil la localización. Si se investiga la procedencia del tráfico, se llega a un inocente servidor de una universidad.

Para enviar un número suficiente de peticiones y saturar una computadora en un corto espacio de tiempo es necesario el ataque se dé por un número enorme de computadoras conectadas a la red y sincronizadas entre sí.

La operación se realiza basándose en el control de decenas de servidores a lo largo y ancho de Internet, el programa tiene instalado, comienza a enviar como zombies las peticiones al servidor especificado.

Para tener el control de las computadoras zombies los atacantes van en busca de servidores vulnerables para eso exploran Internet. Para hacer esto es necesario un software especializado que escanea los puertos abiertos del servidor víctima en busca de puntos débiles.

El puerto está en un servidor que se encarga de dar un servicio particular en Internet, la *"www"* es un servicio con un puerto asignado, un *"correo electrónico"* tiene otro, el *"ftp"* otro, etc. Más servicios de un servidor tiene más posibilidades de ser vulnerable; cada puerto es una puerta de entrada. Si existen más puertas que proteger más difícil será evitar que alguien se infiltre por una de ellas. Un servidor tiene un programa informático se encarga de gestionar cada uno de los servicios al que se asigna un puerto.

Estos programas, al igual que cualquier otro, tienen errores de programación que los hace vulnerables para quien los conozca bien. El atacante descubre un puerto que está congestionado por un programa del que conoce un error de programación por el cual pasarse, se implanta por él, el control del servidor lo toma e instala el programa lo convierte un zombie.

Por la inexperiencia del "administrador", tiene programas antiguos que son vulnerables puede ser atacado. Por esta razón los administradores de un sistema informático conectado a Internet deben tener actualizados los programas que gestionan los diversos servicios que administra **[6]**.

3.2.1.- Vulnerabilidad de los sistemas

Las vulnerabilidades son errores de programación y/o diseño a nivel de software y/o hardware permiten que un tercero se aproveche de estas para realizar acciones tales como ataques, intrusiones o cualquier otro uso indebido.
La *"dirección IP"* es el método de identificación de los computadores. Es una vulnerabilidad que afecta tanto a los servidores como a los usuarios.

3.2.1.1.- Pasos para esconder una IP

Paso 1 - Determinar la dirección IP: Cualquier computadora conectada a Internet tiene un número de identificador para la *"dirección IP".* En la totalidad de las redes la dirección IP de una computadora siempre es la misma. Esta se asigna cuando una computadora se conecta a la red. Si la *"IP"* es dinámica va a ser distinta cada vez que se conecte **[25]**.

Paso 2 - Lograr navegar anónimamente.

Método 1: Anonymizer: Anonymizer presta el servicio de "acercar" las páginas Web lejanas, ejemplo, si una página se encuentra en Japón y hay problema de enlace no permite conectar rápidamente (esto quiere decir: no se puede ver), decirle a Anonymizer que entre a ella y la muestre luego.

Anonymizer tiene un mejor enlace con Japón entonces solucionaría el problema. Algunos sitios muestran distinta información de acuerdo al lugar geográfico desde el cual entra. Ejemplo: El sitio de la Enciclopedia Británica (se dedica a "enviar el pedido de compra") ofrece un listado de representantes en cada país, si entra como Anonymizer aparece en el lugar otra página donde se puede apreciar los precios que tienen en USA (hogar de Anonymizer). Los precios de los representantes son mayores que los precios en USA.

Anonymizer es una de las herramientas más populares donde puede navegar anónimamente **[25]**.

Método 2: Servidores Proxy: También pueden lograr el anonimato en la navegación interponiendo un servidor Proxy. Este servicio es parecido al de Anonymizer, donde las páginas son solicitadas por el *"Proxy"* en lugar del individuo que está navegando. Hay algunas diferencias: Los proxies no filtran los *"cookies",* applets ni código malintencionado. Se encargan de ocultar la posición geográfica.

Todos los servidores Proxy tienen el acceso restringido a los usuarios del proveedor en el cual se encuentra. El *"Proxy"* ofrece los servicios al público en general **[25]**.

3.2.2.- Proxy realmente anónimo

Los Servidores Proxy Anónimos ocultan la *"dirección IP"* y por lo tanto lo previenen de acceso no autorizado a la computadora a través de Internet. No le proveen a nadie la *"dirección IP"* y ocultan de manera efectiva cualquier información que tenga y los intereses de lectura. Aparte de eso, no dejan que nadie sepa que alguien está navegando a través de un servidor proxy. Los Servidores Proxy Anónimos pueden ser utilizados para cualquier tipo de servicio Web, tales como Correo - Web (MSN Hot Mail, Yahoo mail), salas de chat, servidores *"FTP",* etc.

Anonymizer es la mejor solución para muchos de los usuarios de Internet. Protección extrema de la privacidad - nadie puede saber donde está navegando.

Si recibes un mensaje “Proxy Server is detected” significa que hay un agujero de seguridad en el *“Proxy”* que se está usando y los servidores Web tienen la habilidad para saber cual es la *“IP”.* En la página Web aparece la *“IP”.* Si recibes un mensaje “Proxy Server not detectet” significa que navegas anónimamente. Es importante realizar otras pruebas para saber si el navegador es anónimo **[25]**.

3.3.- Ataques a los sistemas informáticos

Modos de Ataque I

Los modos de ataques como directos e indirectos, pero realmente creo que podemos simplificar y enfocar de una forma más directa en simples componentes que son:

1. Ataque al Usuario

Este es el ataque mas frecuente, debido al potencial de la información que se puede obtener mediante este tipo de agresión, ya que dependiendo del nivel de ingenio del atacante puede obtener información importante de un usuario victima extrayendo sus cookies y consiguiendo información almacenada en ellas o robando su sesión de usuario en un sitio Web especifico.

Dentro de las diversas formas de ataque veremos dos de las más comunes.

Ataque vía correo electrónico:

Se basa en el envió de un correo electrónico a un usuario con un script oculto en un link a una dirección Web, el atacante buscando motivar a su victima a seguir el enlace le ofrece un premio, regalo u oferta si visita dicho vinculo, al verse atraído por la información en el correo electrónico el usuario hace click en el vinculo sin darse cuenta de que esta activando una secuencia de comandos que se ejecutaran en su equipo local, que podrían extraer sus cookies, eliminar archivos y en el caso mas fatal formatear su disco duro, mediante la invocación de programas con parámetros aleatorios.

Ataque vía publicación en Sitios Vulnerables:

Esta segunda forma se basa en la publicación datos en blogs, foros, libros de visitas o sitios que permiten reflejar información enviada por un usuario y que no es validada por el servidor, donde podremos esconder secuencias de comandos detrás de un vinculo o imagen, este ataque tiene la misma finalidad que el anterior, pero con un mayor alcance de usuarios afectados.

Bien, como desarrolladores posiblemente tendremos o hemos tenido que crear sitios en donde los usuarios puede costear información que se vera reflejada en el sitio y podrá ser accedida por otros usuarios, ya sea blogs, foros o libros de visitas como se explico antes, pero que tal una bolsa de empleo donde puedo agregar mi currículo, o un sitio para comentarios de visitantes entre otras muchas opciones.

Si no tenemos una validación debida de las entradas por parte del usuario, se pueden enviar cadenas con comandos ocultos en vínculos que se almacenaran y reflejaran en nuestro sitio.

Los ataques son acciones que se suponen con una violación a la seguridad de un sistema (confidencialidad, integridad o disponibilidad). Las acciones se clasifican de modo genérico según los efectos causados:

Interrupción*:* Es destruido un recurso del sistema o se vuelve no disponible. Ejemplo los Nubes, ocasiona se queden sin servicio los equipos. También la destrucción, como suspender una línea de comunicación.

Intercepción: Es un ataque contra la confidencialidad. Por ejemplo la obtención de datos mediante el empleo de programas troyanos o la copia ilícita de archivos.

Modificación: Es un ataque contra la integridad, ejemplo la modificación de cualquier tipo en archivos de datos, para alterar un programa funciona de forma distinta y modifica el contenido de la información ha sido transferida por la red.

Fabricación: Es un ataque contra la autenticidad. Por ejemplo la inserción de mensajes falsos en una red o para añadir datos a un archivo. Estos ataques se dividen en pasivos y activos.

- **Ataques activos:** Son activos que implican algún tipo de modificación de los datos o la creación de falsos datos: Suplantación de identidad, Modificación de mensajes, Web Spoofing Etc.

- **Ataques pasivos:** Los pasivos son la comunicación que no se altera por el atacante, solamente la escucha o monitoriza, para que tenga información que ha sido transmitida. Los ataques pasivos no tienen alteración en los datos es por eso que es difícil de detectar **[1]**.

3.3.1.- Algoritmo

Cuando se establece una estrategia de seguridad. El algoritmo Productor/Consumidor. En este algoritmo, existen dos entidades: una es la encargada de producir la información; la otra es el consumidor de la información y la, llamada precisamente “otros”. Entre el productor y el consumidor, se define una relación tiene como objetivo una transferencia de “algo” entre ambos, sin otra cosa que intervenga en el proceso. Si esto se logra llevar a cabo y se mantiene a lo largo del tiempo, se estará en presencia de un sistema seguro.

En la realidad, existen entidades y/o eventos provocan alteraciones a este modelo. El estudio de la seguridad, en pocas palabras, se basa en la determinación, análisis y soluciones de las alteraciones a este modelo**.**

En una observación y planteo del modelo, determinar que sólo existen cuatro tipos de alteraciones en la relación producción-consumidor. Definir el concepto de “recurso” **[17]**.

Se menciona como recurso a cualquier cosa, ya sean bienes específicos o que permitan la subsistencia de la organización como tal.

Debido a ello, es diferenciar claramente tres tipos de recursos **[20]**:

- Físicos
- Lógicos
- Servicios

Los recursos físicos son, por ejemplo, las impresoras, los servidores de archivos, los *"routers",* etc. Los recursos lógicos son, por ejemplo, las bases de datos de la cual obtiene la información que permite trabajar en la organización. Los servicios son, por ejemplo, de correo electrónico, de página WEB, etc. Todas las acciones correctivas se lleven a cabo con el fin de respetar el modelo estarán orientadas a atacar uno de los cuatro casos. A continuación se explican y se muestran ejemplos de cada uno.

El caso número uno es el de *"Interrupción"* (ver Tabla 3.1). Este afecta la disponibilidad del recurso (tener en cuenta la definición de: físico, lógico y servicio.

Por ejemplo:

Recurso afectado	Nombre	Causa	Efecto
Servicio	Correo electrónico	Alguien dio de baja el servidor (por algún método)	No poder enviar mail
Físico	Impresora	Falta de alimentación eléctrica	No imprime

Tabla 3.1.- Interrupción.

El segundo caso es el de Intercepción (ver Tabla 3.2), en el cual se pone en riesgo la privacidad de los datos.

Recurso afectado	Nombre	Causa	Efecto
Lógico	Datos sobre cuentas en el banco	Se ha puesto un dispositivo que permite monitorear los paquetes en la red y sacar información de ellos.	Conseguir datos privados sobre montos de cuentas corrientes
Servicio	Correo electrónico	Se ha implantado un programa que duplica los mensajes (mails) salen de una sección y los envía a una dirección.	Leer información

Tabla 3.2.- Intercepción.

El tercer caso, modificación (ver Tabla 3.3) afecta directamente la integridad de los datos que le llegan al consumidor.

Recurso afectado	Nombre	Causa	Efecto
Lógico	Base de datos de pagos en cuentas corrientes.	Se ha implantado un programa que redondea en menos los pagos y carga éstos redondeos a una cuenta corriente.	Incrementar el crédito de una cuenta corriente en base al redondeo realizado en los pagos.
Servicio	Servidor de página WEB	Alguien logró ingresar como WEBMASTER y ha cambiado los contenidos de la página.	Los datos mostrados en la página no son reales.

Tabla 3.3.- Modificación

El cuarto y último es el de la producción impropia de información (ver Tabla 3.4). En éste, el consumidor es directamente engañado.

Recurso afectado	Nombre	Causa	Efecto
Lógico	Datos de deudores	Se ha generado una base de datos falsa, la que ante el pedido de informes, responde ella con sus datos.	Hacer pasar a los deudores como que no lo son.
Servicio	Servidor WEB	Alguien se ha apropiado del password del WEBMASTER y, modificando el direccionamiento, logra que se cargue otra página WEB.	Redireccionar la página WEB hacia otro sitio.

Tabla 3.4.- Producción impropia de Información.

Una vez enterados de que hay sólo cuatro posibles casos de problemas. Hay que identificar los recursos dentro de la organización.

Los recursos deben ser considerados al estimar las amenazas a la seguridad son solamente seis **[20]**:

- *Hardware:* procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, cableado de la red, servidores de terminal, routers y bridges.

- *Software:* programas fuente, programas objeto, utilerías, programas de diagnóstico, sistemas operativos, programas de comunicaciones.

- *Datos:* durante la ejecución, almacenados en línea, archivados fuera de línea, back-up, bases de datos, en tránsito sobre medios de comunicación.

- *Gente:* usuarios, personas para operar los sistemas.

- *Documentación:* sobre programas, hardware, sistemas, procedimientos administrativos locales.

- *Accesorios:* papel, formularios, cintas, información grabada.

Luego de haber visto lo anterior, es cómo proteger ahora los recursos. Según el del que se trate, será el modo de protegerlo.

Primero, hay que tener en cuenta qué es lo que hay que proteger. Si se trata de los problemas ocasionados por el personal propio o de intromisiones clandestinas que puedan afectar la operación de la organización.

Una aproximación acerca de cómo proteger los recursos de los problemas originados por el cliente interno consiste en la identificación del uso correcto de los mismos por parte de éstos.

Pero primero, saber quiénes son los que van a hacer uso de los recursos. Es decir, se debe poseer, previamente, con un conocimiento cabal de todos los usuarios que tiene en el sistema.

Esta lista no es obligatoriamente individual, sino que puede ser, en efecto, una lista por grupos de usuarios y las necesidades en el sistema. Esta es, con seguridad, la práctica más extendida pues, definida la necesidad de un grupo de usuarios, lo más efectivo es englobarlos a todos en un mismo grupo.

El otro problema se presenta, es el de las intromisiones clandestinas. Aquí, es preciso tener en cuenta el tipo de recurso a proteger. Con base en ello, estará dada la política de seguridad **[20]**.

Ejemplos acerca de a qué se está enfrentando:

- Asegurar no se ingresa al sistema por un puerto desprotegido o mal configurado.
- Asegurarse de que no se estén usando programas propios del sistema operativo o aplicaciones para ingresar al sistema en forma clandestina.
- Asegurar que, ante un corte de energía eléctrica, el sistema seguirá funcionando.
- Asegurar de que los medios de transmisión de información no son susceptibles de ser monitoreados.
- Actúa la organización frente al alejamiento de uno de los integrantes.
- La respuesta a estos interrogantes reside en la posibilidad de conseguir dicha seguridad por medio de herramientas de control y seguimiento de accesos, utilizando check-lists para comprobar puntos importantes en la *"configuración"* y/o funcionamiento de los sistemas y por medio de procedimientos que hacen frente a las distintas situaciones **[17]**.

Ejemplo de procedimiento de verificación de eventos en el sistema:

Diariamente: Extraer un logístico sobre el volumen de correo transportado. Extraer un logístico sobre las conexiones de red levantadas en las últimas 24 horas.

Semanalmente:

1.- Extraer un logístico sobre los ingresos desde el exterior a la red interna.
2.- Extraer un logístico con las conexiones externas realizadas desde la red.
3.- Obtener un logístico sobre los downloads de archivos realizados y quién los realizó.
4.- Obtener gráficas sobre tráfico en la red.

Lograr logísticos sobre conexiones realizadas en horarios no normales (desde dónde, a qué hora y con qué destino).

Mensualmente: Realizar un seguimiento de todos los archivos logísticos a fin de detectar cambios.

Cabría resaltar que, en gran parte, este procedimiento puede ser automatizado por medio de programas que realicen las tareas y sólo informen de las desviaciones con respecto a las reglas dadas **[20]**.

3.3.2.- Escaneo de puertos

Se encarga de buscar puertos abiertos y fijarse en los que puedan ser de utilidad. Cuando se hace una llamada a un número telefónico y la señal se escucha conoce el estado de ese teléfono en ese preciso momento. Después hace una llamada a otro número y así continuamente. El escaneo se encarga de seleccionar el rango de las IPs y hacer esas "llamadas" a unas direcciones *"IP"* consecutivamente, aunque también se puede hacer un escaneo a una *"IP"* concreta. Los firewall actuales reconocen el escaneo y la llamada a puertos consecutivos **[26]**.

3.3.3.- Tipos de escaneo

Escaneo de conexión TCPconnect (): Es el sistema más fácil de escaneo de puertos TCP. Si el puerto escaneado está abierto y a la escucha, regresará una respuesta de éxito; cualquier otra respuesta conlleva el puerto no está abierto o no puede establecer conexión con él.

Se realiza con una gran velocidad que no es necesario tener privilegios especiales. Tiene la facilidad de ser detectable. Existe un gran número de conexiones y mensajes de error con una computadora se conecta y desconecta continuamente.

FTP bounce attack: El protocolo *"ftp"* admite la conección proxy ftp. Es decir, conectarse a un *"ftp"* desde un servidor proxy y al hacer esto establece una conexión y envía un archivo a cualquier parte del Internet. Con esto los atacantes se aprovechan para hacer escaneos,

se ejecutan detrás de un *"firewall"* (el del *"proxy"*) con dificulta para rastrear el origen del escaneo. Es lento y poco usado.

Escaneo de fragmentación: En lugar de enviar paquetes completos de sondeo, se parten en pequeños fragmentos IP. De esta manera es difícil de monitorizar por los filtros que puedan estar ejecutándose en el sistema atacado.

Se pueden producir caídas de rendimiento como en sistema del cliente y en el servidor, por lo que es detectable.

Snooping-Downloading*:* Es semejante al sniffing en el sentido de que obtienen información sin modificarla, el sistema que emplean es distinto pues el sistema se basa en copiar la información y bajarla a la computadora en forma de archivos.

Es la suplantación de un individuo con autorización por parte del atacante. Se da de dos maneras: Obtener el nombre y contraseña del atacado **[26]**.

3.3.4.- Técnicas al realizar ataques

Simulación de Identidad: El atacante instala un programa que recrea la pantalla de entrada al sistema, cuando el usuario intenta entrar en él escribiendo el *"login"* y *"password",* el programa los captura y los muestra en la pantalla de "error en el acceso" al usuario. El usuario vuelve a escribir el *"login"* y *"password",* sin tener problemas al entrar. El usuario al teclear se equivoca entonces el atacante captura el *"login"* y el *"password".*

Spoofing. Engaño: Se encarga de sustituir la fuente de origen de una serie de datos (ejemplo un usuario) adoptando una identidad falsa para engañar a un "*firewall"* o filtro de red. Los ataques spoofing más conocidos son el *"IP Spoofing"*, el Web Spoofing y el fake-mail.

IP Spoofing: Sustituir una *"IP".* El atacante se identifica con una *"IP"* que no le pertenece, una tercera persona es el agresor no tiene nada que ver con el asunto en vez de ser el atacante.

Web Spoofing: El atacante establece un sitio Web falso es parecido al de la víctima que desea entrar. Los accesos a este sitio están dirigidos por el atacante, admitirle monitoriza todas las acciones de la víctima: datos, números de tarjeta de créditos, contraseñas. Cuando se transmite a un servidor original cualquier dato el atacante puede modificarlo.

Eso se da en Internet es un ataque peligroso y difícilmente detectable. Las medidas preventivas se muestran a continuación:

- Desactivar la opción de JavaScript en el navegador.
- La barra de navegación cerciorarse que este siempre activa.

- Tener atención a las URL que se enseñan en la barra de estado, asegurándose que siempre apuntan al sitio que se quiere conectar.

Fake-mail: Se encarga del envío de e-mails (correos electrónicos). Es donde el atacante envía e-mails en nombre de otra persona con cualquier motivo y objetivo. Estos ataques se inician utilizando la Ingeniería Social para hacerse con el nombre y contraseña de una víctima **[26]**.

3.3.5.- Negación de servicio (denial of service)

Denial of service es un ataque con la finalidad de negar el acceso del atacado a un recurso determinado o a los propios recursos. Ejemplos de este tipo de ataque son:

- Tentativas de "floodear" (inundar) una red, evitando de esta manera el tráfico legítimo de datos en la misma.
- Tentativas de interrumpir las conexiones entre dos computadoras evitando, de esta manera, el acceso a un servicio.
- Tentativas de evitar que una determinada persona tenga acceso a un servicio.
- Tentativas de interrumpir un servicio específico a un sistema o a un usuario.

Tener en cuenta que, el uso ilegítimo de recursos puede también dar lugar a la negación de un servicio. Ejemplo, un *"hacker*" puede utilizar un área del *"FTP"* anónimo para salvar archivos, consumiendo, de esta manera, espacio en el disco y generando tráfico en la red.

Como consecuencia, los ataques de negación de servicio pueden esencialmente dejar sin funcionamiento a una computadora o una red. De una manera, toda una organización durante un tiempo determinado puede quedar fuera de Internet **[26]**.

3.3.5.1.- Modos de ataque

Los ataques del rechazo de servicio entran una variedad de formas y apuntan a una variedad de servicios. Hay tres tipos básicos de ataque **[26]**:

A.- Consumo de recursos escasos, limitados, o no renovables: Las computadoras y las redes para el funcionamiento necesitan ciertos recursos: ancho de banda de la red, espacio de memoria y disco, tiempo de CPU, estructuras de datos, acceso otras computadoras y redes, y ciertos recursos medioambientales como energía, el aire fresco, o incluso agua. Los ataques de Negación de servicio frecuentemente se ejecutan contra la conectividad de la red. La finalidad del hacker es evitar las computadoras se comuniquen en la red.

Un ejemplo de este tipo de ataque es el "SYN flood": En este tipo de ataque, el *"hacker"* empieza el proceso de establecer una conexión *"TCP"* a la computadora de la víctima, pero lo hace de manera tal que evita que la conexión se complete. En este tiempo, la computadora de la victima ha reservado uno entre un número limitado de estructuras de los datos que se exigió para completar la conexión inminente. El resultado es que las

conexiones legítimas se rechazan mientras que la computadora del atacado se queda esperando para terminar esas falsas conexiones "medio abiertas".

Si haces una conexión mediante telnet por ese puerto a un servidor que disponga de ese servicio, el programa reaccionará a esta conexión enviando una cadena de caracteres que verás repetidos en la ventana de tu programa de telnet. Todo lo que necesitas hacer es conectar a ese servicio.

El resultado es, que los dos servicios consumen todo el ancho de banda de red entre ellos. Así, la conectividad para todas las computadoras en la misma red desde cualquiera de las computadoras atacadas se ve afectada.

Consumo de ancho de banda Un *"hacker"* puede, también, consumir todo el ancho de banda disponible en la red generando una gran cantidad de paquetes dirigidos a la misma. Típicamente, estos paquetes son de generación de eco de ICMP (ping), pero pueden ser cualquier otra cosa. Además, en el *"hacker"* no es necesario opere en una sola computadora; él puede coordinar varias computadoras en diversas redes para alcanzar el mismo efecto **[1]**.

Otros recursos consumidos: Además del ancho de banda de la red, los hackers pueden consumir otros recursos el sistema necesite para funcionar. Por ejemplo, en muchos sistemas, un número limitado de las estructuras de datos en el kernel está disponible para almacenar información de procesos (identificadores, entradas en tablas de procesos, slots, etc.).

Un *"hacker"* puede consumir estas estructuras de datos escribiendo un programa o un script no haga nada pero que realice en varias ocasiones copias de sí mismo. La mayoría de sistemas operativos modernos, tienen curiosidad para protegerse contra este problema. Aunque no se llenen las tablas de procesos, se consume CPU para la gran cantidad de procesos y conmutación entre los mismos **[1]**.

Un hacker consume el espacio en disco de otras maneras, ejemplo:

- Generar miles de e-mails (Spam, Bombing).
- Utilizar el proceso syslog de la víctima para que registre eventos de otra computadora, llenando el espacio en disco con el archivo de syslog.
- Colocar archivos en el disco, utilizando *"ftp"* anónimo. En general, se puede utilizar cualquier cosa permita que los datos sean escritos en el disco para ejecutar un ataque de negación de servicio si no hay límites en la cantidad de datos que se pueden escribir (quotas) **[26]**.

La mayoría de los sitios tiene esquemas de "lockout" de cuenta después de un cierto número de logins fallados. Un setup típico bloquea el *"login"* después de 3 o 5 tentativas falladas. Un *"hacker"* puede utilizar este esquema para evitar que los usuarios legítimos entren. En algunos casos, incluso las cuentas privilegiadas, tales como *"root"* o "*administrador",* pueden ser víctimas de este tipo de ataque.

Un *"hacker"* puede hacer caer el sistema o ponerlo inestable, enviando datos que no se esperaban. Un ejemplo de tal ataque es el "ping flood" o pings de tamaño demasiado grande. Si el sistema está experimentando caídas frecuentes sin causa evidente, puede deberse a este tipo de ataque. Hay otros componentes que pueden ser vulnerables a la negación de servicio y que deben vigilarse. Como son:

- Impresoras
- Unidades de cinta
- Conexiones de red
- Otros recursos limitados importantes para la operación del sistema.

B.- Destrucción o alteración de la información de configuración: Una computadora que no esté bien configurada, no puede funcionar bien. Un *"hacker"* puede alterar o destruir la información de *"configuración"* del *"sistema operativo",* evitando de esta forma usar la computadora o red.

Algunos ejemplos: Si un *"hacker"* puede cambiar la información de ruteo de los routers, la red puede ser deshabilitada. Si un *"hacker"* puede modificar el registro en una computadora Windows NT, ciertas funciones pueden ser imposibles de utilizar, o directamente el sistema puede no volver a bootear **[1]**.

C.- Destrucción o alteración física de los componentes de la red: Es importante la seguridad física de la red. Se debe resguardar contra el acceso no autorizado a las computadoras, los *"routers",* los racks de cableado de red, los segmentos del *"backbone"* de la red, y cualquier otro componente crítico de la red. **[1]**

3.3.5.2.- Prevención y respuesta

Los ataques de negación de servicio puede ocasionar pérdidas significativas de tiempo y dinero para varias organizaciones, es recomendable una serie de medidas, las cuales se mencionan a continuación:

- Coloque access lists en los routers. Esto reducirá la exposición a ciertos ataques de negación de servicio.

- Instale *"patches"* al *"sistema operativo"*. Esta acción permite reducir sustancialmente la exposición a estos ataques aunque no pueda eliminar el riesgo en forma definitiva.

- Quitar cualquier servicio de red innecesario o no utilizado. Esto puede limitar la capacidad de un *"hacker"* de aprovecharse de esos servicios para ejecutar un ataque de negación de servicio.

- Es recomendable utilizar configuraciones de red redundantes y fault-tolerant (tolerante a fallos/fallas) **[1]**.

3.3.5.3.- Descubrir un password

Un *"password"* esta encriptado, no se puede desencriptar. Esto no garantiza la seguridad del *"password",* significa que el *"password"* no se pueda averiguar.
Existe un mecanismo para descubrir (no desencriptar) los passwords consiste en efectuar encriptaciones de palabras (posibles passwords) y comparar estas encriptaciones con el original.

Hay éxito dependiendo de la calidad que tenga el diccionario (archivo que contiene un conjunto de posibles passwords), del programa que utilice, CPU y la paciencia. Los programas buscadores de contraseñas son fácilmente de diseñar.

Si mediante un *"bug"* se obtiene el archivo /etc/passwd, se puede iniciar un ataque al diccionario contra el mismo obteniéndose, de este modo, los passwords.

Long. En caracteres	**26 letras (minúsculas)**	**36 letras y dígitos**	**52 (mayúsculas y minúsculas)**	**96 Todos los caracteres**
6	50 minutos	6 horas	2.2 días	3 meses
7	22 horas	9 días	4 meses	23 años
8	24 días	10.5 meses	17 años	2287 años
9	21 meses	32.6	881 años	219.000 años
10	45 años	1159 años	45.838 años	21 millones de años

Tabla 3.5.- Tiempo de búsqueda de un password.

Otro tipo de ataque es el de "fuerza bruta", se encarga de realizar todas las combinaciones posibles de caracteres hasta encontrar el *"password".* En la tabla 3.5 se muestra el tiempo de búsqueda de un *"password"* de acuerdo a la longitud y tipo de caracteres utilizados. Con una velocidad de búsqueda de 100.000 passwords por segundo**.**

Es importante utilizar más de ocho caracteres y si tiene más símbolos, hay menos probabilidad de encontrar un *"password"* **[1]**.

Capítulo

IV

Herramientas utilizadas por el hacker

4.1.- Criptoanálisis

Es necesario un usuario tenga un *"password"* para conectarse a Internet, esto se da cuando hay un contrato con el proveedor. La clave de conexión a la red es la misma que se utiliza al recibir el correo con el cliente habitual o para actualizar las páginas *"Web"* personales a través del *"ftp".* Si una persona con mala intención quiere acceder a la cuenta de correo, no es necesario saber la *"clave"* se utiliza para leer e-mail, con el *"password"* grabado en un cliente de *"ftp"* es necesario para tener las puertas abiertas a los mensajes privados de la víctima.

La debilidad de los sistemas de cifrado utiliza algunos de los programas que los almacenan. Se trata de algoritmos propietarios que basan la seguridad en no difundir el código. Estos sistemas no tienen nada que ver con la *"criptografía".*

Por esto, huir de los sistemas de cifrado propietarios, en realidad no facilitan el algoritmo que usan y que, normalmente, resulta sencillo descubrirlo. En la mayoría de las ocasiones suele bastar la ingeniería inversa; empleando un número finito de pares *"password"/*password cifrada, se localiza con el procedimiento de encriptación. Hallar una contraseña específica de forma inmediata es bastante con invertir los algoritmos **[24]**.

Desencriptación de una clave: La labor primordial de un *"administrador"* es realizar una auditoria de seguridad que se basa en recopilar información, la tarea principal al igual el hacker que está investigando la vulnerabilidad de un sistema o un atacante. Es fundamental lo anterior en el se basan todos los procesos siguientes. Es importante comprobar en qué archivos guarda la información cada aplicación, en un .ini, .dat, o en el mismo directorio.

Bases criptográficas: Todo *"hacker"* o experto en seguridad debe familiarizarse con las técnicas y algoritmos criptográficos. Es importante familiarizarse con los métodos clásicos de cifrado, como el de César, donde se realiza una sustitución de carácter a carácter del texto. Ejemplo la A se sustituye por la D, la B por la E, la C pasaría a ser una F y así con todo el abecedario **[24]**.

Ejemplo:
ESTO ES UNA PRUEBA.
Sustitución:
HVWR HV XPD SUXHED

El método es bastante antiguo, ejemplo, el carácter H el cual se repite en el cifrado, correspondería a la E, la vocal que más se utiliza en el castellano. Para saber los caracteres originales se tiene que atrasar tres posiciones en el abecedario, las que se encuentran entre la H y la E. Al utilizar esta regla, modificar tres lugares en todas las posiciones, lograra un texto original. Lo principal para evitar que se encuentre el texto original, no es definitivo, una misma letra puede ser cifrada con distintos pares. Ejemplo, sumar una posición en los lugares impares y dos en los pares. Así, la letra A se sustituye por B, la B por la D, la C por D y así sucesivamente **[24]**.

Ejemplo:
Texto claro:
ESTO ES UNA PRUEBA
Sustitución:
FUUQ GT VOB QTVGCC

Las letras se repiten más en el cifrado son la U, la T y la C, es muy diferente al primer ejemplo, no se logra realizar una correspondencia tan directa para tener una solución. La transposición es un método clásico se encarga de aplicar cambios de posición entre los elementos del texto. Se puede llevar a cabo una transposición muy básica cuando se intercambian las posiciones de los caracteres por parejas. Es decir, el primer carácter por el segundo, el tercero por el cuarto, etc.

Ejemplo:
Texto claro:
ESTO ES UNA PRUEBA
Transposición:
SEOTE SNU ARPEUAB

Al fortalecer el cifrado, se utiliza una combinación de diversos métodos. Aplicar en primer lugar, una sustitución con el método Cesar y al texto cifrado resultante se realiza una transposición.

Ejemplo:
Texto claro:
ESTO ES UNA PRUEBA
Sustitución:
HVWR HV XPD SUXHED
Transposición:
VHRWH VPX DUSHXDE

Para recuperar el texto solamente con realizar la inversa, como primer lugar la transposición y posteriormente de la sustitución.

4.1.1.- Realizar un criptoanálisis

Los programas utilizan métodos de cifrado para ocultar los passwords son bastante evolucionados tratan de poner bastantes trabas. A pesar de esto, los sistemas implementados presentan debilidades y logran ser atacados mediante un *"criptoanálisis"* apropiado.

En muchas ocasiones, el problema surge solamente que haya un texto cifrado y no tomar en cuenta el algoritmo empleado para ello. Si el método lo conoce, solamente con saber la clave se puede efectuar un ataque apropiado, bien invirtiéndolo el algoritmo con el texto cifrado para obtener la clave.

El *"hacker"* tiene al alcance una copia del programa que desee realizar. Debe emplearlo para almacenar diferentes contraseñas o textos y comprobar de qué forma almacena cada uno de ellos. Si primero se guarda el *"password"* <<pepe>> y después escribir <<Carmen>> como clave. Los pasos que se realizan no son sencillos, en lo que se refiere a la recopilación de toda la información necesaria para afrontar el *"criptoanálisis"* adecuadamente. Es decir grabar diferentes passwords y guardar los datos sobre la forma en que éstas se almacenan.

Es más difícil encontrar el fichero donde se guardan, entonces introducir un *"password"* a través del programa y observar los archivos que se han modificado a raíz de esa operación. Introducir una cuenta nueva de *"ftp",* para que la almacene y observando cómo se cifra la clave. Con F4 abre la ventana de administrador de servidores *"FTP".* Añadir un servidor, como nombre <<PRUEBA>> y como contraseña <<aaaaaaaaaa>>.

Los datos introducidos en cuenta: nombre de la cuenta, dirección del servidor, nombre de usuario y a continuación 10 caracteres iguales, <<®®®®®®®®®®>>, diferentes al *"password"* introducido. El carácter <<a>> corresponde al número 97 del código *"ASCII".* Se trata de un cifrado basado en el método de sustitución simple. Restando los códigos *"ASCII"* obtiene 72, que parece ser el número que suma a los caracteres del texto original para lograr el cifrado.

Introducir otra *"cuenta",* el nombre de usuario será <<OTRA>> y la clave <<ABCDE>>. Editando el fichero <<tree.dat>>, encontrar al final los datos introducidos y, junto al nombre de usuario, los caracteres <<ëèìîì>>, corresponden a los códigos *"ASCII"* 137, 138, 139, 140, 141. Si resta 72, obtendrá los números 65, 66, 67, 68 y 69, que corresponden a los caracteres *"ASCII"* de <<ABCDE>>>.

El programa CuteFtp almacena las contraseñas en el fichero <<tree.dat>>. Utiliza un método de cifrado basado en sustitución, sumar 72 posiciones y tener como conjunto de elementos el código *"ASCII"* de 1 a 255, de manera cíclica. Al hacer las operaciones de sustitución, se supera la cifra 255, se continuara por el 1. Tener esta información resulta insignificante diseñar un programa que lea el fichero <<tree.dat>> y como salida tenga las cuentas de servidores *"ftp"* con los nombres de usuarios y los passwords descifrados al realizar el método de sustitución a la inversa **[10]**.

4.1.2.- Criptografía

La *"criptografía"* da los siguientes servicios de seguridad al sistema operativo y las aplicaciones.

Confidencialidad: La confidencialidad garantiza las entidades autorizadas tienen acceso a la información. Este servicio se encarga para almacenar datos sensibles en ubicaciones vulnerables como ordenadores portátiles o transmitirlos a través de redes vulnerables, como Internet o una *"WAN"* obtenida del exterior. La *"criptografía"* convierte grandes secretos (los datos) en pequeños secretos (claves criptográficas). Las claves son secretos más sencillos de administrar, ante todo porque pueden intercambiarse por adelantado.

Autentificación de entidades: *"Autentificación"* de entidades se encargan de comprobar la identidad de una entidad ante otra e implementa habitualmente manifestando la posesión de un secreto. La *"criptografía"* mantiene el secreto en privado durante el proceso de *"autentificación".*

Integridad de los datos: La integridad o el servicio de *"autentificación"* de datos aseguran que el bloque se originó en una entidad y permanece inalterado. La *"criptografía"* ayuda a vincular los datos con el creador.

No rechazo: El no rechazo permite a los usuarios que los documentos electrónicos se firmen digitalmente y establecen un vínculo legal con las firmas. La *"criptografía"* puede proporcionar pruebas de que un usuario firmó un documento, pero deben cumplir muchas condiciones para un tribunal considere que hay una vinculación legal **[10]**.

4.1.3.- Algorítmica

La algorítmica estudia el desarrollo de soluciones computacionales de diversos problemas que se plantean en el desarrollo de un programa. Las soluciones son independientes del lenguaje de programación utilizado, ya que son resueltos en nivel de una abstracción mayor. Varias soluciones algorítmicas se encargan de diferente estructura de datos como apoyo fundamental a la hora de resolver problemas. Es importante saber las diferentes estructuras con el objetivo de aplicar la más adecuada al tipo de problema con el cual enfrenta **[24]**.

4.1.3.1.- Estructura de datos y algoritmos

Una programación estructurada y eficiente, es un elemento básico consiste en la elaboración de los datos de una forma adecuada y el posterior desarrollo de algoritmos para el acceso y modificación. La estructura de datos es la organización de la información que admite un determinado lenguaje de programación. Tiene propias características de almacenamiento y recuperación de los datos de cada estructura.

Los algoritmos se componen de la resolución de los problemas computacionales basándose en un lenguaje de programación. Los algoritmos también permiten mediante los lenguajes de programación se pueda resolver los problemas computacionales. Por ejemplo hay dos que son los más usuales:

- *Divide y Vencerás:* Se encarga de descomponer un problema en subproblemas, resolver cada subproblema y combinar las soluciones. El resultado, es la solución del problema original. Cuando los subproblemas son demasiado grandes, utiliza la misma táctica es decir dividirlos también, utilizando un algoritmo recursivo que vaya diciendo más el subproblema hasta que la solución sea trivial.

- *Backtracking o esquema:* El Backtracking o esquema, el esquema que da forma sistemática y organizada, genera y recorre un espacio que tiene todas las posibles secuencias y decisiones. El espacio se llama espacio de búsqueda del problema, y

se representa como un árbol sobre el algoritmo que hace un recorrido en profundidad empezando desde la raíz. El orden que se va generar se conoce y recorre los *"nodos"* y se va continuando en recorre el árbol mientras se cumplan las restricciones. Éste método tiene tres esquemas: encontrar una solución factible, en todas las posiciones posibles es lo más apropiado **[24]**.

4.1.3.2.- Tecnologías de clave pública

Los Sistemas Operativos de Microsoft introducen una completa infraestructura de *"clave pública"* (PKI) a la plataforma de Windows. La infraestructura amplía los servicios criptográficos de *"clave pública"* (PK) se basan en Windows en el pasado, aportando un conjunto integrado de servicios y herramientas administrativas para crear, implantar y gestionar aplicaciones basadas en *"clave pública"* **[24]**.

Infraestructura de clave pública: La infraestructura de *"clave pública"* es el estudio de las aplicaciones cliente y servidor para aumentar la confianza en las credenciales de "*autentificación"* de uno y otro de modo altamente escalable. Las aplicaciones pueden utilizar esas credenciales para realizar una autentificación robusta y emplear servicios de confidencialidad e integridad de un extremo a otro **[10]**.

Algoritmos criptográficos simétricos: La criptografía simétrica funciona transformando (cifrado) el texto sin cifrar (datos originales) el texto cifrado (datos protegidos) de una manera que impide invertir el proceso sin conocer a fondo la función de transformación, la modificación secreta se divide en una parte constante, el algoritmo criptográfico, y una parte variable, la clave criptográfica. El algoritmo implementa ampliamente en software o dispositivos que utilizan la *"criptografía"* y no asume que sea secreto. De manera la seguridad debe mantenerse a toda costa en la clave.

Las claves simétricas son bloques aleatorios de datos o se generan de contraseñas de usuario y tienen una longitud de 40 a 128 bits. Los algoritmos simétricos utilizan claves y un algoritmo de bloque para cifrar y descifrar datos sin procesar **[10]**.

Algoritmos criptográficos asimétricos: La criptografía asimétrica o de *"clave pública"* convierte el texto sin cifrar en texto cifrado utilizando el algoritmo y la clave. La diferencia es en el uso de la clave de descifrado diferente, de ahí el nombre de asimétrico. La clave de descifrado (privada) y la clave de cifrado (pública) la segunda es necesaria al estar en secreto porque se da a conocer. Los usuarios de claves públicas en una clave determinada deben confiar en ella y si pertenece a un propietario en particular. La seguridad mantiene en secreto la *"clave privada".*

Las claves asimétricas se eligen de manera aleatoria de entre un grupo que tiene determinadas propiedades que son específicas al algoritmo asimétrico, de manera que es imposible que dos usuarios generen las mismas claves. El tamaño de la clave puede variar entre 512 y 4.096 bits.

Algoritmos de firma asimétricos: También se puede invertir la relación de una dirección entre las claves asimétricas para firmar datos con una *"clave privada"* y comprobar la firma con la *"clave pública".* Esto se da ya que la firma sólo puede haberse generado con la clave privada asociada. Las claves criptográficas asimétricas manejan firmas digitales y la autenticación Desafío-Respuesta **[10]**.

4.1.3.3.- La importancia de los números primos

El objetivo principal de los números primos es generar un número que sirva para cifrar mensajes y que luego sea muy complicado descifrarlos.

Se puede cifrar un mensaje en función de un número primo. Cada letra en un mensaje tiene un número asociado que nunca cambia. El número se da con el código *"ASCII".* El conjunto de caracteres *"ASCII"* define cada carácter con un número que va desde el 0 al 255. Ejemplo, la letra "A" mayúscula corresponde al código 65, la "z" minúscula corresponde al código 122, etc. Cualquier texto escrito en un ordenador se puede trasladar a notación "ASCII". Ejemplo, en código "ASCII" la palabra "antivirus" es **[10]**:

97 110 116 105 118 105 114 117 115

La *"cadena"* de números (es como realmente se transmite la información digitalmente) se multiplican por un número sea la multiplicación de dos números primos. Por ejemplo, 14 (multiplicando 2 y 7), la *"cadena"* de números quedaría así:

1358 1540 1624 1470 1652 1470 1596 1638 1610

La persona quiera leer lo que pone primero deberá averiguar cuál es el número que utiliza para cifrar la información. Es necesario adivinar cuáles son los dos factores que utiliza para cifrar la información. Ejemplo es muy fácil, 14 es 7 por 2. El problema es difícil cuando los números son grandes. Ejemplo, si el número 2.591.372.723, la descomposición en dos factores primos ya no es tan inmediata. A pesar de eso, en muy poco tiempo verá que es el producto de 97.453 y 26.591.

La longitud de estos números (lo que se llama el "tamaño de la clave") es primordial para que un cifrado sea más o menos efectivo. En el primer ejemplo, si una notación binaria el número 14 se escribe 1110, un número de 4 bits. El segundo ejemplo, 2.591.372.723, se escribe en binario como 10011010011101010011010110110011, 32 bits. Y en los sistemas de cifrado actuales en una clave de menos de 400 ó 500 bits se considera ridícula. Lo más normal es utilizar, como poco, 1.024 bits de longitud de clave **[10]**.

4.1.3.4.- Ventajas y problemas del cifrado

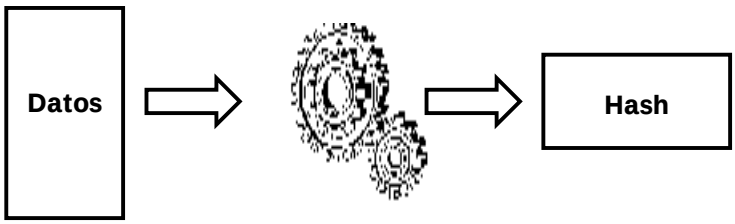
El enviar un correo electrónico cifrado aporta indudables ventajas tanto al emisor como al receptor del mensaje. La confidencialidad está prácticamente asegurada, nadie conoce las claves, entonces no sabrá lo que tiene el correo. Así al mandar todo tipo de información con la tranquilidad de que estará a salvo de teóricas intercepciones de la comunicación.

Los sistemas de cifrado son una herramienta que aumenta la seguridad de las comunicaciones, pero ocultan *"virus"* a los antivirus perimetrales que no estén preparados. Una solución para evitar que los virus cifrados entren en la empresa, debe ser una protección perimétrica efectiva que bloquee los elementos cifrados no autorizados antes de que puedan alcanzar los servidores y las estaciones de trabajo de la empresa **[10]**.

4.1.4.- Algoritmos

En la *"Criptografía"* de *"Clave Pública"* se utilizan los siguientes algoritmos, funciones matemáticas, para trasformar la información.

Algoritmo Hash (ver Figura 4.1): Se encarga de pasar los datos por un algoritmo Hash, el cual obtiene un resumen único de esos datos, pero a partir del resumen no se pueden obtener los datos **[23]**.



Algoritmo Hash

Figura 4.1.- Algoritmo Hash.

Algoritmo de clave Pública: Función matemática es fácil de resolver en un sentido, pero prácticamente imposible de realizar en forma inversa, a menos que conozca la *"clave privada".*

Par de Claves: La *"Criptografía"* de *"Clave Pública"* se encarga en la tenencia por cada usuario de un par de claves asimétricas asociadas (diferentes):

- La *"clave privada",* está en poder del usuario y no de otra copia.
- La *"clave pública",* es conocida por todos **[23]**.

Una clave puede verificar y *"desencriptar"* lo que la otra ha firmado y encriptado.

4.1.5.- Seguridad del software

Hoy en día aparecen errores y problemas de seguridad que afectan algún software al estar utilizándolo. Necesariamente estos *"bugs"* son los que se pueden aprovechar en un intruso para poder entrar en el ordenador o crear cualquier otro tipo de problema "informático". Por lo tanto, es más que recomendable que mantenga al día la computadora para evitar estos problemas **[23]**.

4.1.6.- Defensa-bloqueo de puertos

Una vez de haber determinado los puertos abiertos se pone el remedio a los problemas que ha encontrado. Para ello, dispone de la siguiente forma para hacerlo:

- Bloqueo de Puertos e Instalar un Firewall (cortafuegos)

Un cortafuego o firewall en inglés, es un equipo de hardware o software utilizado en las redes para prevenir algunos tipos de comunicaciones prohibidos por las políticas de red, las cuales se fundamentan en las necesidades del usuario. El bloqueo de puertos se encarga de cerrar el paso a los puertos (se tienen abiertos) querer tener cerrados, el *"firewall"* o *"cortafuegos"* es más seguro tenerlos todos cerrados y abrir sólo aquellos que se permitan el bloqueo, ya que sólo permite el tráfico desde Internet que se acepte.

Para bloquear puertos del ordenador; utilizar otro programa que se llama pblocki.exe**.** La diferencia entre éste programa y un *"firewall"* es que a éste programa se le dice que puertos bloquear y a un *"firewall"* lo que se dice es que puertos están permitidos **[23]**.

4.1.6.1.- Usando el Sistema Operativo

Windows, como *"Linux",* ofrece una herramienta va a mostrar conexiones de red que se tienen en cada momento. Esa herramienta es el programa **netstat** (que permite ver qué puertos se está atendiendo), y para ejecutarla, en ambos casos, necesita abrir una Consola. En Windows abrir MS-DOS y escribir: netstat –an.

Para saber qué conexiones están abiertas, lo mejor es que antes de ejecutar dicha orden cerrar todos los programas a excepción de MS-DOS, e ir desde el principio comprobando que conexiones tiene y cuáles se van abriendo. Una vez ejecutada la orden, aparecerá una pantalla de este tipo en MS-DOS (ver Figura 4.2) **[23]**.

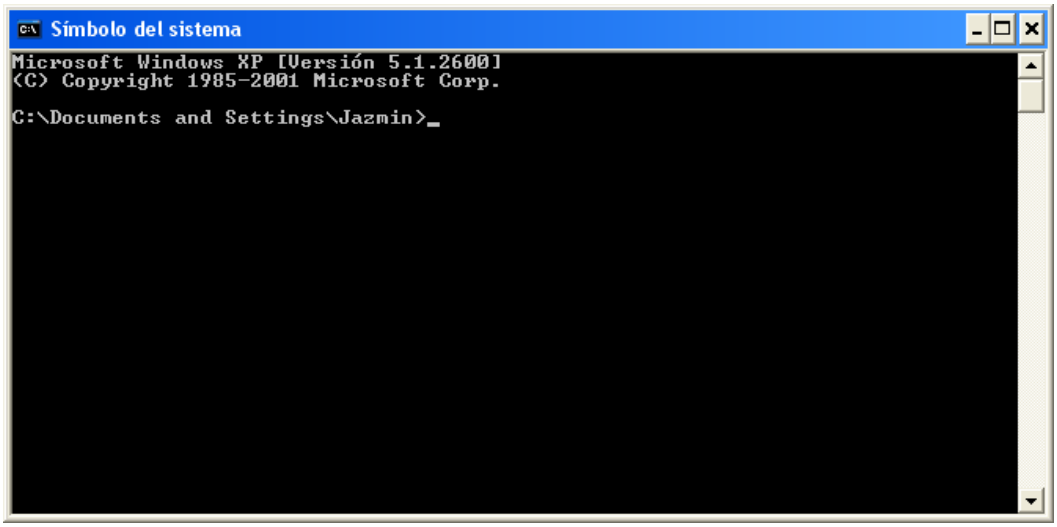


Figura 4.2.- Pantalla de MS-DOS.

1.- Detección de puertos - Escáner Puertos Online

> **Escáner de Puertos:** *El "Escáner de puertos",* se encarga de realizar algunos de los principales puertos de llegada a la computadora desde el servidor. Sólo se comprueban si están abiertos (columna de Estado) o si están cerrados o no existen (recuadro OK en columna de Estado). La ventaja de este *"escáner"* es que detectarán si se está detrás de un *"Proxy"* o *"router"* y poder comprobar realmente qué puertos son accesibles desde el exterior, que no necesariamente son los que se han detectado con el *"escáner de puertos"* desde el propio ordenador **[2]**.

2.- Iniciar el Escáner

> **Encriptar datos en un PDA:** Siglas de "Personal Digital Assistant" (Asistente Digital personal). Son ordenadores de bolsillo que, en muchas ocasiones ni siquiera tienen teclado y se manejan con un pequeño lápiz. Se utilizan sobre todo como bloc de notas y como agendas de teléfonos y direcciones, pero pueden llegar a tener otras funciones como enviar y recibir correo electrónico, enviar faxes o conectarse a Internet.

La importancia de tener datos a salvo de miradas extrañas. Los PDAs son muchas veces usados como pequeñas oficinas portátiles, donde se guardan datos de gran valor y de gran importancia para tener estos datos protegidos. Bastantes usuarios de PDAs por comodidad no protegen el acceso de inicio con una clave; en caso de pérdida del aparato o descuido puede dejar estos datos confidenciales en manos ajenas. Para solucionar este problema o tener un cierto grado de seguridad, es muy importante poder encriptar **[2]**.

4.2.- Obtención de Passwords, Códigos y Claves

Este método (usualmente denominado cracking), comprende la obtención "por fuerza bruta" de aquellas claves que permiten ingresar a servidores, aplicaciones, cuentas, etc. Muchos passwords de acceso son obtenidos, fácilmente, porque involucran el nombre u otro dato familiar del usuario, que además nunca la cambia. En este caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles claves hasta encontrar el password correcto.

Es muy frecuente crackear una *"password"* explotando agujeros en los algoritmos de encriptación utilizados, o en la administración de las claves por parte de la empresa.

Por ser el uso de passwords la herramienta de seguridad más cercana a los usuarios, es aquí donde hay que poner énfasis en la parte "humana" con políticas claras (*"password"* sería, el autorizado para revelarlo) y una administración eficiente (cada cuánto van cambiando).No muchas organizaciones están exentas de mostrar passwords escritas y pegadas en la base del monitor de los usuarios, u obtener simplemente preguntando al responsable de cualquier PC, seria el *"password"* **[10]**.

1.- Las Redes necesitan centinelas cada vez más Atentos: La seguridad de una red se hace cada vez más difícil. A pesar de que las herramientas se mejoran día con día, los hackers también se aumenta el nivel de conocimientos técnicos y de modernidad. En general, las empresas y las organizaciones son cada vez más conscientes de los riesgos y permanentemente tratan de aumentar los niveles de protección **[10]**.

2.- Vulnerar para Proteger (checarlo más al fondo: Los hackers utilizan diversas técnicas para violar los sistemas de seguridad de una red. Básicamente, buscan los puntos débiles del sistema para poder apoderarse de ella.

Mientras que los hackers penetran en las redes para dañar o robar información, un testers o verificador lo hace para poder mejorar los sistemas de seguridad. Al conjunto de técnicas que se utilizan para evaluar y probar la seguridad de una red se le conoce como Penetration Testing, uno de los recursos más poderosos con los que se cuentan hoy para generar barreras cada vez más eficaces. En cuanto a las barreras de seguridad, un testers se explica que: Están totalmente relacionadas con el tipo de información que se maneja en cada organización.

Por consiguiente, según la información que deba ser protegida, se determinan la estructura y las herramientas de seguridad y no a la inversa. Pero las herramientas no son sólo técnicas. El software y el hardware utilizados son una parte importante, pero no la única. A ella se agrega lo que se denomina "políticas de seguridad internas", que cada empresa u organización debe generar **[10]**

Capítulo

V

Como ingresa el hacker en el sistema operativo Unix

5.1.- Hackear computadoras con sistema operativo Unix

Hackear computadoras con sistema operativo unix aparte de *"unix"* hay otros sistemas operativos como mainframes y miniordenadores.

Pasos para hackear en sistema (ver Tabla 5.1):

1	Ingresar en sistema que tenga como objetivo.
2	Al momento de conseguir el acceso, conseguir privilegios de root (administrador del sistema).
3	Borrar huellas.
4	Instalar un sniffer (programa que monitoriza la red consiguiendo logins y passwords) para poder acceder a otros sistemas.

Tabla 5.1.- Hackear un sistema.

"Linux" empieza como *"root",* porque ya está creada la cuenta de *"root".* Al ingresar como *"root"* y al quedar dentro, no ingresar ningún *"password".* Cuando esté adentro, establecer un *"password"* para que nadie pueda ingresar como *"root".*

Para no ser "*lamer"* y encontrar un *"password"* verdaderamente difícil de *"desencriptar",* la palabra no sea sola sino una serie de letras y números que no tengan sentido. Un buen *"root"* pone un *"password"* de este tipo ya que un *"hacker"* utiliza programas de desencriptación asociados a diccionarios para "*desencriptar"* el *"password"*, solamente hay que teclear **[22]**:

 # Passwd root

Y luego introducir el *"password"* se tiene en mente.

El *"sistema operativo"* con más fuerza para redes es *"Unix".* Es tan completo y complejo que para él no existen los *"virus"* porque el usuario controla todo. Existe el *"Linux"* el cual es igual al *"Unix"* es gratuito, el sistema operativo de los hackers.

Unix es excelente para llevar redes, e Internet es una red. En *"unix"* los comandos son diferentes a los de MS-DOS, así dir es ls, copy es cp. La forma de la ruta de los directorios es distinta. En MS-DOS escribe \programas. Unix es /programas.

"Unix" se utiliza en redes, tiene que lograr que varios usuarios se controlen. Ejemplo: todos no pueden acceder a diversos datos que no le corresponden, y no todos logran tomar el mando de un ordenador central.

El usuario obtiene total acceso a la mayoría de los recursos del servidor en el *"root",* es decir, el superusuario, da la autorización al resto de los usuarios. Hay usuarios que son los Daemons, dichos procesos siempre están en marcha de un ordenador, ejemplo, conectado a Internet con algunos Daemons pueden ser el *"http"* (páginas Web), el ftp (servidor de

ficheros), etc. Es necesario entrar en el servidor remotamente es decir haciendo *"telnet".* El proceso a realizar en el servidor es el siguiente **[13]**:

> **1º. Pedir un *"login"* (nombre de usuario):** si el nombre no es el correcto, y no muestra ningún error el sistema para impedir que el individuo sepa qué accesos se encuentran dados de alta y cuáles no.
>
> **2º. Pedir un *"password"* (contraseña o palabra clave):** si concuerda con el que tiene asignado el *"login"*, permite el acceso al sistema.

Los usuarios estén dados de alta, así como los passwords que utilizan, se localizan en el fichero passwd. Algunos usuarios no necesitan la clave, como el usuario *"anonymous"* (anónimo) o gues (invitado), tienen la misma palabra como *"login"* y *"password"*. En *"Unix"* el usuario "Rosy" no es lo mismo que "rosy", en *"unix"* hace la diferencia de mayúsculas de las minúsculas **[13]**.

5.1.1.- Ingresar en el sistema.

Los fallos de seguridad que se benefician para conseguir entrar en el sistema por lo regular se basan en protocolos *"TCP/IP",* en servicio de red como el NFS o NIS o en los comandos "r" de *"Unix".*

TCP/IP
TCP = Transport Control Protocol
IP = Internet Protocol

Los protocolos que se basan en *"TCP/IP"* que realmente suelen aprovechar son *"Telnet", "FTP",* SMTP, *"HTTP",* SMTP, TFTP. Los protocolos tienen los propios agujeros de seguridad que van parcheando con nuevas versiones de estos protocolos, constantemente aparecen nuevos *"bugs"* **[5]**.

5.1.2.- Conseguir privilegios de root una vez conseguido el acceso

Los fallos de seguridad que explota son del propio sistema operativo Unix, a diferencia de saber cuando ingresar en el sistema; explotaban los agujeros de seguridad de los protocolos o servicios de red.

Aunque exploten los *"bugs"* de los protocolos *"TCP/IP",* no significa que los *"bugs"* funcionen con cualquier *"sistema operativo".* Al contrario, *"bugs"* funcionan con el sistema operativo Unix. Los sistemas operativos tienen propios *"bugs"* relacionan los protocolos *"TCP/IP"***,** obtiene dos cosas cuando se introduce en el sistema:

> **1 - Conseguir privilegios de root:** Se obtiene mediante varios "bugs" dependiendo del tipo de "Unix" en que se mueve ("aix", "sun", "Solaris", "hp-ux", etc.) y también la configuración de dicho sistema.

Hay varias fuentes de información en Internet para conocer bugs, que no indican la existencia del "bug" que funciona en "unix" y algunos casos para explotarlos publican en la red programas **[13]**.

2.- Mantener los privilegios de root: Para mantener los privilegios de "root" se encargan de asegurar en casi en la próxima vez que se entre al sistema con la cuenta de un usuario que tenga privilegios normales, obtener privilegios de "root" de forma fácil y sin ninguna complicación.

La forma para conseguir esto es que una vez alcanzado los privilegios de "root", copia un shell (el fichero /bin/sh) a un directorio público es decir un usuario normal que pueda ejecutar los ficheros y cambiar el nombre al que uno quiera. El shell copiado tenga como owner (propietario del fichero) al "root" y los permisos del fichero con las cifras 4755 que sean cambiados.

El 4, significa cualquier usuario ejecute dicho fichero y lo ejecuta con los privilegios del owner. El owner es el "root" y el fichero en cuestión es un shell, el sistema abre un shell con privilegios del "root".

La siguiente vez que se acceda al sistema con una cuenta de usuario normal, hay que cambiar al directorio donde haya copiado el shell, ejecutarlo y entonces será "root" sin tener complicaciones que explota un "bug" **[13]**.

5.1.3.- Borrar las huellas

Borrar las huellas es importante, haber introducido en el sistema y haber conseguido el nivel de *"root"* si al siguiente día el acceso lo han suspendido porque han dejado huellas en todas partes.

El sistema operativo Unix guarda diversos registros (*"logs"*) de las conexiones de los usuarios al sistema. Hay varios ficheros y comandos que auxilian al administrador a conocer todos los detalles sobre las conexiones de los usuarios. Estos ficheros y comandos, constan de diversas facilidades y aplicaciones que ejecutan un registro continuado y profundo sobre las actividades tiene un usuario dentro del sistema **[13]**:

BUSCANDO LA MÁQUINA OBJETIVO Y ALGO SOBRE UNIX ORIENTADO AL HACKING.

Lo primero que se ha de hacer, como es lógico es determinar la maquina objetivo. Esta decisión se puede hacer en base a distintos criterios como pueda ser que es una maquina especialmente interesante para ti o que es una maquina que sabes o te han dicho que el rOOt no es una lumbrera. Bien, sea como fuere, se ha determinado la maquina objetivo.

Tras esto, se ha de recopilar la mayor información sobre esa maquina. Lo mejor es empezar haciendo un escaneo de puertos a la maquina, esto consiste en ir haciendo telnet's a todos los puertos de la maquina (normales 1-6000) para ver que programas

contestan en cada puerto y su versión, o si el puerto esta cerrado. Por ejemplo: con un telnet normal (puerto 23) determinaremos el sistema operativo, con un telnet 79 (finger) para obtener información, entrar por el netstat (puerto 15) si lo tiene abierto (poco usual), mirar si tiene pagina Web y que demonio de http usa (puerto 80), mirar la versión del sendmail (puerto 25), ver si esta el systat abierto, ver si tiene ftp anónimo en el 21, ver si ofrece nfs o nis, etc. Para esto se necesita un escaneador de puertos de los que hay muchísimos en la red (strobe, portscan, nmap, etc.)

Además, en caso de que quieras hackear victima1.microsoft.com, en caso de que veas que no puedes hacer nada en esta máquina victima1, puedes plantear hackear otra del dominio microsoft.com, ya que si consigues root y colocas un sniffer en victima2.microsoft.com (o quizá con un poco de suerte con el hosts.equiv o el .rhosts) seguramente podrás conseguir cuentas en victima1.microsoft.com.

El fichero hosts.equiv es un fichero que hay en los sistemas unix que indica que maquinas pueden ejecutar comandos remotos en esta maquina sin pedir ni login ni password, es decir, indica las maquinas que son confiables.

Igualmente, el fichero .rhosts es un fichero que hay en el HOME de cada usuario que indica las maquinas a las que permite ejecutar un comando remoto sin pedir password. Además, el comando host puedes obtener una lista de maquinas pertenecientes a un dominio dado y que el comando traceroute muchas veces puede ayudar (recuerdo que el traceroute muestra el recorrido que hacen los paquetes hasta llegar a la máquina destino).

5.1.4.- Instalar un sniffer

Para tener acceso a otros sistemas a partir del *"host"* que es hackeado existen diversas técnicas. La más entendida es el consultado en los ficheros .rhosts de los usuarios e intentando acceder a los sistemas incluidos mediante rlogin o rsh.

Existen diversas formas más o menos confusas permita conseguir información desde un sistema en el se encuentra y permita acceder a otros de la red. El método más famoso y más eficiente es la colocación de un *"sniffer".*

El *"sniffer"* es un programa monitoriza la red consultando los diversos paquetes de información que van circulando en ella. Cumple cierto requisito alguno de los paquetes ejemplo: sea un paquete correspondiente a un proceso de *"login",* guarda dicho paquete en un fichero es decir, guarda un *"log".*

Un *"hacker"* puede consultar dicho fichero le aporte información sobre que usuario y se conecte a un determinada computadora, y que *"password"* utilizó **[13]**.

- Funcionamiento de un sniffer

La red Internet es un conjunto de subredes comunicadas entre sí mediante computadoras llamadas *"gateways", "bridges"* o *"routers"*. Una subred está dividida en varias subredes.

Las computadoras están organizadas en una red de tipo *"ethernet"*, y dicha red está conectada a Internet o a una subred de Internet mediante los correspondientes *"routers"* o *"gateways"* pueden ser un *"router"* si no diversos para poder comunicarse con el exterior, que serán las computadoras que mantengan a dicha red ethernet en contacto con el resto de la red.

Las redes ethernet trabajan mandando los paquetes de información por un canal que comparte a todas las computadoras. En la cabecera para cada paquete de información está la dirección de cada computadora a la cual va destinado el paquete de información. Solamente lo recibe la computadora a la cual va destinado. Las computadoras reciben cualquier paquete de información aunque no estén destinados a ella, se dice están en modo promiscuo.

Un *"hacker"* pone en modo promiscuo la computadora (si es que no lo está ya en el momento de hackearla) y capturar los paquetes va por la red, aunque no vengan de la computadora y aunque no estén destinados a ella. Usualmente se capturan paquetes cumplan algún requisito como aquellos incluyan el momento de acceso de un usuario a una computadora.

Tomando en cuenta que el *"login"* y el *"password"* del usuario se Los ficheros manejan el "sniffer" para guardar la información, crecen muy rápido por lo que si no se tiene cuidado pueden hacerse enormemente grande y alertar al administrador del sistema, al examinar los ficheros se dará cuenta de que hay un *"hacker"*. Por lo tanto, es aconsejable consultar los *"logs"* en cada momento y abandonar los ficheros a cero **[13]**.

5.1.4.1.- Servicios de red

NFS (Network File System): Es un servicio de red donde varias computadoras nombran clientes y comparten uno o diversos directorios se encuentran físicamente en una computadora llamada servidor. Una computadora cliente, a pesar de no tener físicamente dichos directorios, puede instalarlos de tal manera que pueda acceder a ellos como si los tuviera. Lo que se puede hacer con los ficheros incluidos en dichos directorios (si pueden borrar, modificar, alterar los permisos, etc.), lo cual depende de la configuración del NFS.

Mandan en modo un texto, el *"hacker"* puede leer con todo agrado el fichero de registro que genera el *"sniffer"* qué *"password"* maneja el usuario y en qué computadora lo maneja **[13]**.

Puede sniffar información si el sistema no está en modo promiscuo, por lo tanto la computadora sólo aceptará información esté destinada a ella, y los paquetes de información que monitorizará el sistema serán los paquetes destinados a él, y los paquetes que desciendan del sistema.

Mala configuración del NFS es donde están siempre los fallos de seguridad.

NIS (Network Information Service): Es un servicio donde varias computadoras comparten "mapas". Los mapas son ficheros como passwd, hosts, etc. Ejemplo, el usuario puede entrar con una misma cuenta todas las computadoras compartan un mismo mapa de passwords. Los mapas son consultados por los clientes a las computadoras tengan mapas, que son los servidores **[13]**.

Comandos "r": Son comandos exclusivos del sistema operativo Unix. En el sistema existe un fichero de nombre host.equiv y cada usuario tiene en el directorio home (es el reservado a cada usuario para el uso propio del sistema) un fichero de nombre .rhosts. Dependiendo de la configuración de estos dos ficheros se puede o no acceder a dicho ordenador desde otro sistema Unix sin necesidad de password con los comandos rlogin o rsh **[13]**.

Hay 2 maneras de introducirse en el sistema:

- Se puede entrar directamente sin tener cuenta en el sistema objetivo. Ejemplo, comandos "r" o algún *"bug"* (alterar el fichero passwd del ordenador por rsh, alterar el fichero .rhosts de algún usuario por NFS, etc.)

- Obtener el fichero passwd del sistema objetivo y crackearlo. El fichero passwd tiene los logins de los usuarios y el adecuado password encriptadas. Para saber el *"password"* de cada usuario se utiliza un programa *"crackeador"* como el crack, para MS-DOS encripta cada palabra de un diccionario y las compara con la cadena encriptada del fichero passwd, cuando las cadenas encriptadas coinciden entonces la palabra del diccionario que el programa ha encriptado en ese instante es el *"password"* buscado **[22]**.

5.1.4.2.- Tipo de agujeros

Agujeros de Seguridad Físicos: El problema potencial, es debido al hecho de otorgar a personas, sin autorización, acceso físico a la computadora, siempre y cuando permita realizar cosas que no deben ser capaces de hacer.

Ejemplo: Una sala pública, con estaciones de trabajo, donde puede ser fácil reiniciar una computadora en modo mono-usuario y "trastear" con los archivos de la estación de trabajo, si no se han tomado precauciones.

Otro ejemplo: Es la necesidad de restringir el acceso a cintas backup confidenciales, que de otra forma pueden ser leídas por cualquier usuario que tenga una unidad lectora, independientemente de si tiene permiso o no **[13]**.

Agujeros de Seguridad en el Software: Es cuando el problema se presenta por una mala escritura de partes "privilegiadas" de software (daemons, cronjobs) que están comprometidos a realizar tareas que no deben.

Agujeros nuevos que aparecen todos los días, los mejores métodos para prevenir son los siguientes:

- Tratar de estructurar el sistema de manera que el menor software trabaje con privilegios *"root"/*daemon/bin corra en la computadora, el individuo que lo haga que sea con una seguridad.
- Para tener información sobre los problemas y/o *"parches"* suscribirse a listas de correo y actuar en cuanto esté disponible.

No confiar en los *"scripts"/*programas de instalación. Tales utilidades tienden a instalar/cargar lo que existe en el paquete sin exigir confirmación. **[13]**.

Agujeros de Seguridad por Incompatibilidades: Se da por algún descuido, el administrador del sistema hace funcionar software sobre un hardware para el que no está optimizado, da lugar a resultados imprevistos y errores pueden dañar seriamente la seguridad del sistema. Es la incompatibilidad de un software y hardware la que va creando agujeros de seguridad.

Problemas de este tipo son difíciles de encontrar una vez que el sistema está instalado y funcionando, de manera que es muy favorable el leer cuidadosamente la documentación del software y del hardware que se va a instalar (o que pretenda atacar) y estar al día con la actualización **[13]**.

Capítulo

VI

Seguridad del hacking

6.1.- Seguridad, cifrado y firma electrónica

Para impedir ataques informáticos contra un servidor, se puede encontrar con diversos sistemas técnicos, como los *"firewalls",* protegen a una computadora de posibles accesos por parte de personas no autorizadas, aunque este sistema de seguridad quiebra ya que existen usuarios que saben esquivarlos.

Una IP a través de un e-mail recibido: Cuando te envían un e-mail al correo y necesita saber de que *"IP"* viene, tienes que ver el *"Header"* (encabezado) del mail. De esta manera obtiene la *"IP"* tenía la computadora del emisor en el momento en que se envió el mail y no garantiza que ese individuo aún esté bajo esa misma *"IP".*

Para ver el encabezado de un mensaje en Outlook Express se da click con el botón derecho del mouse en el e-mail y luego en "Propiedades/Detalles". Los servicios webmail suelen dar la opción de ver encabezamiento. Por ejemplo en Hotmail.com hay que configurar Opciones -> Configuración de pantalla de correo -> Encabezados de mensajes -> Avanzado **[19]**.

La seguridad es la principal defensa que puede tener una organización si desea conectarse a Internet, dado expone la información privada y arquitectura de red a los intrusos de Internet (Crakers). El *"Firewall"* ofrece esta seguridad, mediante: (Choke Point), monitoreos y políticas de seguridad, determinando que servicios de la red pueden ser accesados y quienes pueden utilizar estos recursos, manteniendo al margen a los usuarios no-autorizados y en caso de un ataque genera alarmas de seguridad **[11]**.

La preocupación principal del administrador de red, son los múltiples accesos a Internet, porque se desconoce lo que pasa en la transmisión de datos, si son *"virus",* intrusos, espías. Entonces este sistema protege la red de la otra red Internet, mediante el uso de filtros están equipados para que automáticamente eviten un usuario no-autorizado ataque al equipo, ya sea en forma remota por Internet o por traidores internos de la red.

Las políticas es el apoyo de este sistema, informar a los usuarios de las responsabilidades, normas de acceso remoto o local, políticas de los recursos de la red, reglas de encriptación, normas de protección de virus y entrenamiento.

El administrador del *"Firewall"* puede definir el choke-point o (embudo), para mantener al margen a los usuarios no-autorizados (hackers, crakers y espías).

El *"Firewall"* ofrece un punto de seguridad monitoreada y si aparece alguna actividad sospechosa para generar una alarma ante la posibilidad de que ocurra un ataque **[11]**.

6.1.1.- Firewall

Un "*firewall"* se compone de equipos y programas, estos quedan un poco lejos para el usuario doméstico.

El funcionamiento de los tipos de programas se basa en el "*filtrado de paquetes"* todo dato o información que circule en la computadora y la red será analizado por el programa ("*firewall"*) con la misión de permitir o negar el paso en ambas direcciones (Internet-->PC ó PC--->Internet).

El entender dicho proceso es muy importante, ya que si autoriza un determinado servicio o programa, el *"firewall"* no va a decir cual es correcto o incorrecto, o incluso, que al ser correctos los paquetes están entrando o saliendo, éstos contienen datos dañinos para el sistema o la red, por lo que hay que tener el cuidado en las autorizaciones que otorga.

Ejemplo de esto último es el "*Correo Electrónico"*. Si autoriza el *"firewall"* en un determinado programa de correo y al recibir un mensaje contiene un archivo adjunto con un "*virus"*, por ejemplo tipo "*gusano*", el "*firewall"* no se va a defender de ello, ya se ha autorizado a que ese programa acceda a la red.

Lo que si va a hacer es si al ejecutar el archivo adjunto, el "*gusano*" intenta acceder a la red por algún puerto que no esté previamente aceptado por alguien, no lo va a dejar propagarse. Si hace uso por ejemplo del mismo cliente de correo, si va a propagarse. La misión del "*firewall"* es la de aceptar o negar el tráfico, pero no el contenido del mismo. En este caso, la misión de protegerse es (además del sentido común de no ejecutar sin más un adjunto) con un programa Antivirus.

Un "*firewall"* funciona, en principio, negando cualquier camino que se produzca cerrando todos los puertos de la computadora. En el momento que un determinado servicio o programa intente tener acceso a Internet o a la computadora lo hará saber. En ese momento se puede aceptar o negar dicho tráfico, asimismo hacer (para no tener que repetir la operación cada vez) "permanente" la respuesta hasta que no se cambie la política de aceptación **[3]**.

Reglas de un Correo electrónico:

- Jamás enviar información confidencial de la empresa a terceros. Puede ocasionar una violación de la buena fe contractual, una sanción o el despido.
- Si la empresa dispone de dos cuentas de correo, una para uso personal y la otra para asuntos de trabajo, se utiliza la primera para las comunicaciones privadas.
- El correo es usado para comunicarse con los representantes de labor.
- Cuidado con los "*virus"*. No confiar en los archivos adjuntos y antes de ejecutarlos asegurarse de quién lo envía y de si lo ha hecho voluntariamente (muchos "*virus"* se auto reenvían sin conocimiento del usuario). Las posibilidades de que se extienda el daño por la red interna de la empresa deben procurar ser especialmente cuidadoso. Borrar dicho mensaje del buzón.
- Aunque la palabra abuso es algo ambiguo, es importante, para no caer en él se consideraron algunas cuestiones de sentido común a la hora de utilizar el correo.
- Jamás enviar mensajes o ficheros adjuntos de gran tamaño ya que puede tener problemas el servidor.
- No es recomendable hacer envíos generales a demasiados usuarios.

- Respetar los derechos de los destinatarios de los correos: los contenidos de los mensajes deben sujetarse a la ley y no contener declaraciones ofensivas.

El patrón puede exigir que se incluya una cláusula de no responsabilidad cuando los empleados comuniquen de manera interna y externa, especificando que los puntos de vista expresados son aquéllos del autor y no de la empresa **[3]**.

6.1.2.- Las fases de un firewall

- Fase I consiste en presentar el funcionamiento del *"Firewall"* como sistema de seguridad de una red.
- Fase II comprende los componentes del sistema Firewall.
- Fase III relaciona las características y ventajas del *"Firewall".*
- Fase IV es el diseño de decisión de un Firewall de Internet y el ultimo tema Limitaciones del *"Firewall".*

FASE I: Funcionamiento del Firewall como sistema de seguridad de una red: Un *"Firewall"* se conecta entre la red interna confiable y la red externa no confiable, (ver Figura.6.1).

Los *"Firewalls"* en Internet administran los accesos posibles del Internet a la red privada. Si no cuenta con un *"Firewall",* cada uno de los servidores del sistema se exponen al ataque de otros servidores en Internet.

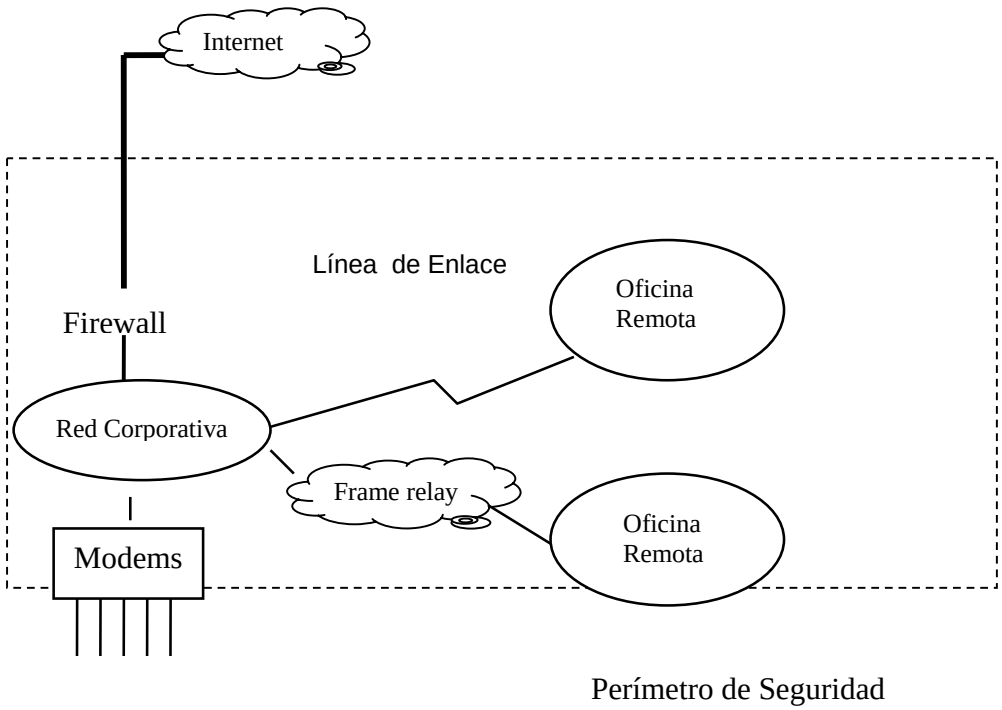


Figura 6.1.- Funcionamiento del Firewall.

El sistema Firewall opera en las capas superiores del modelo OSI y tienen información sobre las- funciones de la aplicación en la que basan las decisiones. Los *"Firewalls"* también operan en las capas de red y transporte en cuyo caso examinan los encabezados *"IP"* y *"TCP",* (paquetes entrantes y salientes), y rechazan o pasan paquetes con base a reglas de filtración de paquetes programados **[11]**.

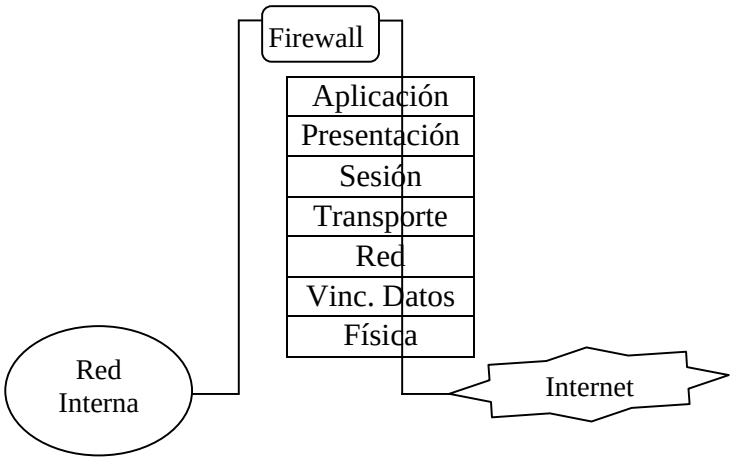


Figura 6.2.- Firewall opera en las capas del Modelo OSI.

El *"firewall"* actúa como un punto de cierre que monitorea y rechaza el tráfico de red a nivel de aplicación, (Ver Figura. 6.2).

Los *"Firewalls"* son filtros que bloquean o permiten conexiones transmisiones de información por Internet, los filtros están diseñados para evitar un usuario irreconocible ataque al equipo por Internet y al mismo tiempo puede ser inmune a la penetración **[11]**.

FASE II: Componentes del sistema Firewall: Un *"Firewall"* típico se divide (ver Figura 6.3) en:

- Ruteador Filtra-paquetes.
- *"Gateway"* a nivel-aplicación.
- *"Gateway"* a nivel-circuito.

Ruteador Filtra-paquetes: El ruteador toma las decisiones de rehusar y permitir el paso de cada uno de los paquetes que son recibidos. Este sistema se basa en el examen de cada *"datagrama"* enviado y cuenta con una regla de revisión de información de los encabezados *"IP",* si estos no corresponden a las reglas, se descarta o desplaza el paquete **[11]**.

Gateways a nivel-aplicación: Los *"Gateways nivel-aplicación"* permiten al administrador de red la implementación de una política de seguridad estricta que le permite un ruteador filtra-paquetes. Es mejor depender de una herramienta genérica de filtra-paquetes para administrar la circulación de los servicios de Internet a través del *"firewall"*, se instala en el *"gateway"* un código de propósito-especial (un servicio Proxy) para cada aplicación deseada **[11]**.

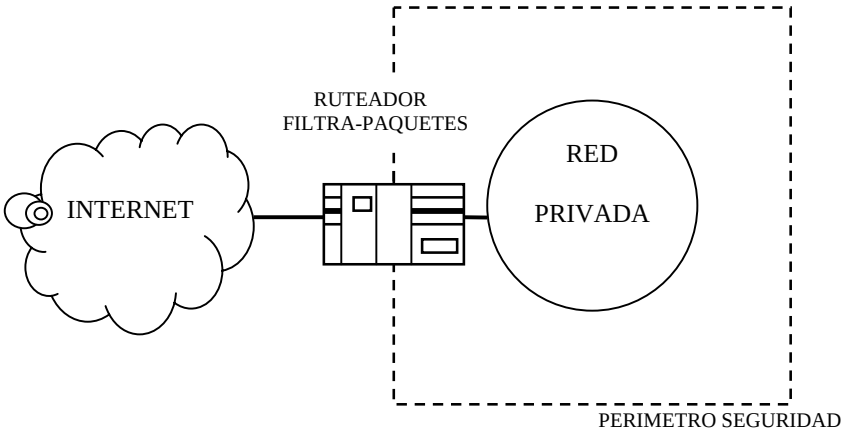


Figura 6.3.- Sistema Firewall.

Gateway a nivel-circuito: Un *"Gateway a nivel-circuito"* es en función que puede ser perfeccionada en un *"Gateway a nivel-aplicación"*. A nivel-circuito simplemente trasmite las conexiones *"TCP"* sin cumplir cualquier proceso adicional en filtrado de paquetes.

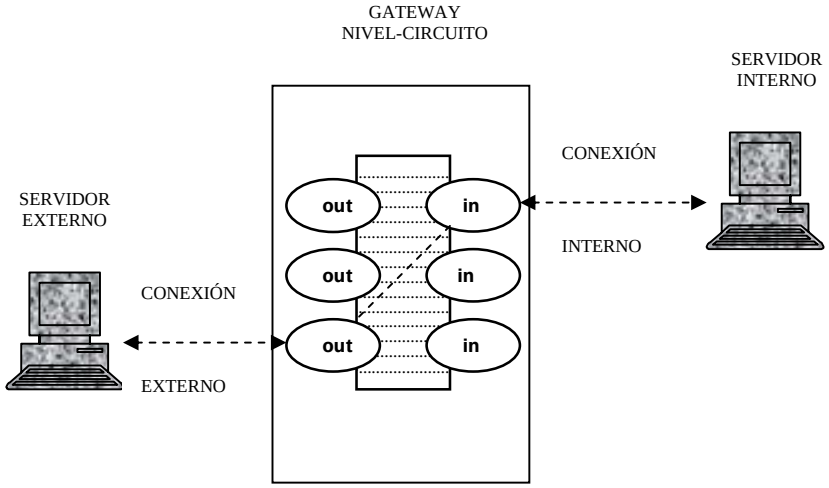


Figura 6.4.-Operación de una conexión típica de telnet.

La figura 6.4.- Muestra la operación de una conexión típica *"Telnet"* a través de un *"gateway a nivel-circuito"*.

Como se menciona anteriormente, este *"gateway"* simplemente trasmite la conexión por el *"firewall"* sin examinarlo adicionalmente, filtrarlo, o dirigiendo el protocolo de *"Telnet".*

El *"gateway a nivel-circuito"* acciona como un cable copiando los bytes antes y después entre la conexión interna y la conexión externa **[11]**.

FASE III: Características y ventajas del Firewall

Protección de la Red: Mantiene alejados a los piratas informáticos (crackers) de la red al mismo tiempo permite acceder a todo el personal de la oficina.

Control de acceso a los recursos de la red: Al encargarse de filtrar, en primer nivel antes que lleguen los paquetes al resto de las computadoras de la red, el *"firewall"* es idóneo para implementar en el los controles de entrada.

Control de uso de Internet: Permite bloquear el material no- adecuado, determinar qué sitios puede visitar el usuario de la red interna y llevar un registro.

Concentra la seguridad: El *"firewall"* facilita la labor a los responsables de seguridad, dado la máxima preocupación de encarar los ataques externos y vigilar, mantener un monitoreo.

Control y estadísticas: Permite controlar el uso de Internet en el ámbito interno y conocer los intentos de conexiones desde el exterior y detectar actividades sospechosas.

Choke-Point: Permite al administrador de la red definir un (embudo) manteniendo al margen los usuarios no-autorizados fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques.

Genera Alarmas de Seguridad: El administrador del *"firewall"* puede tomar el tiempo para responder una alarma y examina regularmente los registros de base.

Audita y registra Internet: Permite al administrador de red justificar el gasto que implica la conexión a Internet, localizando con precisión los cuellos de botella potenciales del ancho de banda **[11]**.

FASE IV: Diseño de decisión de un Firewall de Internet: Cuando se diseña un firewall de Internet, se toma algunas decisiones pueden ser asignadas por el administrador de red:

Las políticas propone el Firewall: Posturas de la políticas "No todo lo específicamente permitido esta prohibido" y "Ni todo lo específicamente prohibido esta permitido".

- La primera postura asume un *"firewall"* puede obstruir todo el tráfico y cada uno de los servicios o aplicaciones deseadas necesariamente y ser aplicadas caso por caso.
- La segunda propuesta asume el *"firewall"* puede desplazar todo el tráfico y cada servicio potencialmente peligroso necesitara ser aislado básicamente caso por caso.

La Política interna propia de la organización para la seguridad total: La política de seguridad se basará en una conducción cuidadosa analizando la seguridad, la asesoría en caso de riesgo **[11]**.

FASE V: Limitaciones de un Firewall: Un *"firewall"* no puede protegerse contra aquel ataque se efectúen fuera del punto de operación, en este caso:

- Conexión dial-out sin restricciones permita entrar a la red protegida, el usuario puede hacer una conexión SLIP o PPP al Internet. Este tipo de conexiones derivan de la seguridad provista por firewall construido cuidadosamente, creando una puerta de ataque.
- El *"firewall"* no puede protegerse de las amenazas a que está sometido por traidores o usuarios inconscientes.
- El *"firewall"* no puede protegerse contra los ataques de la ingeniería social, en este caso, un *"cracker"* quiera ser un supervisor o aquel persuade a los usuarios menos sofisticados.
- El *"firewall"* no puede protegerse de los ataques posibles a la red interna por virus informativos a través de archivos y software.
- Tampoco puede protegerse contra los ataques en la transferencia de datos, estos ocurren cuando aparentemente los datos son enviados o copiados a un servidor interno y son ejecutados despachando el ataque. Por ejemplo, una transferencia de datos podría causar un servidor modificara los archivos relacionados a la seguridad haciendo más fácil el acceso de un intruso al sistema.

El *"Firewall"* le proporcionara la mayoría de las herramientas para complementar la seguridad en la red, mediante la imposición de políticas de seguridad, en el acceso a los recursos de la red y hacia la red externa, es importante establecer que un monitoreo constante del registro base, permitirá detectar un posible intruso y así proteger la información. Es inevitable proteger la red de crackers cuando dentro de la organización existe personal traidor y puede sabotear el sistema **[11]**.

La falta de medidas de seguridad en las redes es un problema está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día con día habilidades más especializadas les permiten obtener mayores beneficios. Tampoco deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización.

La propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad van apareciendo. En medio de esta variedad, han ido aumentando las acciones poco respetuosas a la privacidad y de la propiedad de recursos y sistemas. Hackers, crackers, entre otros, han hecho su aparición en el vocabulario ordinario de los usuarios y de los administradores de las redes. Además de las técnicas y herramientas criptográficas, es importante recalcar un componente muy importante para la protección de los sistemas consiste en la atención y vigilancia continua y sistemática por parte de los responsables de la red.

A la hora de plantearse con qué elementos del sistema se deben de ubicar los servicios de seguridad y distinguirse dos tendencias principales:

Protección de los sistemas de transferencia o transporte: En este caso, el administrador de un servicio asume la responsabilidad de garantizar la transferencia segura al usuario final de la información de forma lo más transparente posible.

Ejemplos de este tipo de planteamientos serían el establecimiento de un nivel de transporte seguro, de un servicio de mensajería con *"MTAs"* (Mail Transport Agents) seguros, o la instalación de un *"firewall",* defiende el acceso a una parte protegida de una red.

Aplicaciones seguras de extremo a extremo: Por ejemplo, en el *"correo electrónico",* consistiría en construir un mensaje en el cual el contenido ha sido asegurado mediante un procedimiento de encapsulado previo al envío. De esta forma, el mensaje puede atravesar sistemas heterogéneos y poco fiables, sin por ello perder la validez de los servicios de seguridad provistos.

Aunque el acto de asegurar el mensaje cae bajo la responsabilidad del usuario final, es razonable pensar dicho usuario deberá usar una herramienta amigable proporcionada por el responsable de seguridad de la organización. Esta misma operación, puede usarse para abordar el problema de la seguridad en otras aplicaciones tales como videoconferencias, acceso a bases de datos, etc. En ambos casos, un problema de capital importancia es la gestión de passwords **[19]**.

La obtención sin autorización de los datos que son almacenados, en un fichero informático, a través de diferentes mecanismos, siempre y cuando el fichero tenga un valor económico.

Otro riesgo hay en Internet es el acceso, en un determinado momento de la comunicación, a datos se envían a través de esta red. Existe un riesgo en la intimidad de los datos.

Hay dos mecanismos técnicos van a garantizar la integridad de los mensajes que marchan a través de las redes abiertas de comunicación. Es la *"criptografía"* de clave simétrica o cifrado simétrico.

Esta técnica consiste en el cifrado de algunos datos con una clave y el posterior descifrado de los mismos se lleva a cabo por la misma clave. Tanto en ventajas e inconvenientes.

Como ventajas es la velocidad de los algoritmos que utilizan son los más apropiados para el cifrado de amplias cantidades de datos. Si alguien obtuviera la clave tendría descifrar el mensaje.

La segunda técnica es la *"criptografía"* de clave asimétrica o cifrado asimétrico. Donde existan un par de claves, una pública donde es conocida por todos los usuarios y una privada donde solamente el usuario la conoce. Esta técnica se encarga de cifrar un mensaje con la *"clave pública"* de un usuario y ese mismo mensaje solo puede ser descifrado con una *"clave privada"* de tal usuario.

Con una clave se cifra, y solamente se puede descifrar con la otra. La ventaja es si se conoce una *"clave pública"* no quiere decir pueda descifrar el mensaje y la desventaja operación de cifrado y descifrado es más lenta que en la criptografía simétrica.

La *"criptografía"* de clave asimétrica existe un elemento en el cual cobra especial trascendencia, el llamado certificado digital va a garantizar una *"clave pública"* corresponde a una persona en concreto.

El cifrado de clave asimétrica va a garantizar el autor de un mensaje no haya sido desplazado al enviarlo a través de redes abiertas de comunicaciones como el Internet; el mensaje no sea alterado durante la transmisión; el receptor del mensaje asegurar haberlo recibido y el contenido del mensaje sea leído por un individuo autorizado **[9]**.

6.1.3.- Siete grandes mitos en seguridad

Al navegar en Internet, se realizan compras y operaciones bancarias en línea sin comprender realmente, salir al mundo desde la computadora del hogar, es un gran logro; y poner a prueba los conocimientos de la seguridad informática del hogar, tener algunos conocimientos equivocados se sorprenderán sobre eso **[18]**:

Mito No. 1: Tener un software antivirus: Este es el mito de Internet más común. Aunque la protección antivirus es importante y necesaria, no basta con tenerla. Nuevos virus surgen todo el tiempo, por lo cual usted necesita actualizar periódicamente las definiciones de virus para garantizar estén actualizadas, y lo más importante, para utilizar el software que lo hace automáticamente por usted.

Además, el software antivirus sólo ofrece un tipo de seguridad (evitar los virus infecten su sistema) cuando usted esté en línea. Sin embargo, los hackers también son una amenaza y el software antivirus no puede desviar a un hacker decidido (ver Mito No. 4). Usted necesita un firewall para que los hackers no ingresen a su sistema y para asegurarse de que su información personal no sale sin su autorización.

Mito No. 2: No existe nada en la computadora que pueda querer un hacker: La mayoría de nosotros creemos que esto es verdad. No obstante, un hacker podría querer la información privada que existe en su computadora.

Los hackers podrían buscar la información personal que usted guarda en el sistema - por ejemplo su número de la seguridad social o de la cuenta bancaria - las puede llegar a utilizar para hacer compras fraudulentas a nombre suyo. El robo de identidad es el delito administrativo de más rápido crecimiento en Estados Unidos hoy en día. Incluso si usted no lleva cuentas financieras en su computadora del hogar, podría tener su currículum vitae en el disco duro de su computadora en un archivo de escritorio que convenientemente guardaría con este mismo nombre y tendría su nombre, dirección, escuela donde estudió y experiencia laboral. Este es exactamente el tipo de información se necesita para solicitar una tarjeta de crédito o préstamo bancario. Una vez los hackers se apoderan de su

información personal, especialmente del número de seguridad social, pueden hacer toda clase de daños.

Mito No. 3: Sólo las grandes compañías son objetivo de los hackers, jamás los usuarios particulares del hogar: Los hackers generalmente buscan presas fáciles y su computadora personal es más fácil de violentar una gran red corporativa. Los hackers pueden infiltrar su sistema mediante el uso de una cantidad de herramientas están disponibles en línea. Las conexiones de banda ancha son especialmente vulnerables porque tienen una dirección IP estática, "siempre conectada", a la que se puede acceder más fácilmente, lo que le tomaría más tiempo a usted para darse cuenta ha sido atacado por los hackers. Si su computadora del hogar siempre está conectada, pero no la analiza con frecuencia, podría ser un objetivo ideal.

Por otra parte, las grandes compañías han invertido mucho en los departamentos de tecnología de la información. Tienen enormes programas antivirus en el gateway y firewall muy efectivos. En otras palabras, son más difíciles de atacar.

Mito No. 4: Se necesita tener conocimientos tecnológicos para ser un "hacker": Contrario a la creencia popular, no se necesita ser genio para *"piratear"* una computadora. Para *"piratear"* una computadora realmente se necesita muy poco conocimiento porque cualquier motor de búsqueda listará sitio tras sitio de las "herramientas para la piratería informática", las cuales están disponibles y se pueden descargar en pocos minutos; incluso traen las instrucciones.

Mito No. 5: Mi proveedor de Internet me ofrece protección (antivirus y/o "firewall") cuando está en línea: Rara vez los proveedores de Internet brindan protección total, aunque por alguna razón los usuarios piensen que sí. Por lo tanto, usted debería verificar con su proveedor de Internet y preguntarle por el nivel de seguridad que tiene contra virus y hackers. Aún si su proveedor de Internet le proporciona alguna protección, debería instalar un buen software antivirus en su computadora.

Cuando está en línea es vulnerable a los virus descargados porque es probable que su proveedor de Internet únicamente analice el correo electrónico. Esto no lo protege de un virus que usted podría descargar inadvertidamente.

Mito No. 6: Utilizo la conexión de acceso telefónico, entonces no debe preocuparse por los hackers: Es verdad los usuarios de banda ancha son más vulnerables a ser atacados. En una conexión de alta velocidad (banda ancha) usted tiene una dirección IP (Protocolo de Internet), de forma que una vez los hackers saben donde encontrarlo, pueden volver porque saben donde vive.

Con una conexión de acceso telefónico mucho más lenta, su dirección IP cambia todo el tiempo. Esta dirección de acceso aleatorio les permite a los usuarios de conexión telefónica disfrutar de un falso sentido de seguridad, aunque esto no significa que los hackers no los puedan encontrar.
Si usted tiene una conexión de acceso telefónico, un hacker que viole su sistema, podría instalar un caballo de Troya de acceso furtivo para verlo cada vez que se conecte. El

caballo de Troya manda una señal que dice: "oye, aquí estoy, ven por mi"- para que el hacker sepa que usted está en línea y es vulnerable. También es posible contagiarse de un Caballo de Troya por un virus de correo electrónico o al descargarlo en un archivo infectado de Internet. Cuando se contagia con un Caballo de Troya, no importa si su conexión es de banda ancha o de acceso telefónico.

Mito No. 7: Tengo un equipo de computo Macintosh: Con frecuencia los usuarios de Mac se sienten seguros porque la mayoría de virus están diseñados para las plataformas basadas en Windows. Sin embargo, eso no importa para un hacker; una computadora es una computadora, y no les interesa qué plataforma se utilice, sólo buscan puertos abiertos.

Muchas herramientas de piratería informática específicas para Mac están disponibles en Internet. El nuevo SO X también está basado en Unix. Las computadoras Unix han estado en el mercado durante tanto tiempo que muchas de las herramientas de piratería informática a que tienen acceso los usuarios de Unix ahora son aplicables a las PC Macintosh.

6.2.- Políticas de seguridad de la información

Política de seguridad: Disponer de acceso a los servicios de la red de una empresa y acceso al mundo exterior a través de la organización, da al personal e institución bastantes beneficios. A mayor acceso se provea, más es el peligro de que alguien explote lo que resulta del incremento de debilidad.

Cada vez se añade un nuevo sistema, acceso de red o aplicación se agregan debilidades potenciales y aumenta la mayor dificultad y complejidad de la protección. Si se está dispuesto a enfrentar realmente los riesgos, es posible cosechar los beneficios de mayor acceso mientras se minimizan las dificultades. Para lograr esto, se necesitará un plan complejo, así como los recursos para ejecutarlo. También se debe tener un conocimiento detallado de los riesgos que pueden ocurrir en todos los lugares posibles, así como las medidas pueden ser tomadas para protegerse.

Para asegurar una red adecuadamente, no solamente se necesita un profundo entendimiento de las características técnicas de los protocolos de red, sistemas operativos y aplicaciones son accesadas, sino también lo relativo al planeamiento. El plan es el primer paso y es la base para asegurar que todas las bases sean cubiertas **[20]**.

Definición de una política de uso aceptable:

- Las herramientas y aplicaciones forman la base técnica de la política de seguridad.

Por ejemplo, los derechos y responsabilidades de los usuarios:

- Si los usuarios están restringidos, y cuáles son las restricciones.
- Si los usuarios pueden compartir cuentas o dejar otros usuarios utilicen las cuentas.
- Cómo deberían mantener las contraseñas los usuarios.
- Con qué frecuencia deben cambiar las contraseñas.
- Si se facilitan copias de seguridad o los usuarios deben realizar las que tienen **[20]**.

Políticas generales de seguridad (PSI): Las Políticas de seguridad informática se encargan de comunicarse con los usuarios y los gerentes. Las PSI constituyen el canal de forma de actuación del personal, en relación con los recursos y servicios informáticos, importantes de la organización.

No es una técnica de mecanismos de seguridad, tampoco una expresión legal que involucre sanciones a conductas de los empleados. Es una descripción de lo que se desea proteger y el porqué de ello **[20]**.

6.2.1.- Elementos de una política de seguridad informática

En el PSI las decisiones se toman en relación con la seguridad deben orientarse. Pues se requiere de una disposición por parte de cada uno de los miembros de la empresa para tener como finalidad una visión conjunta de lo que es de gran importancia.

PSI considera los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual se aplica. Es una invitación de la organización a cada uno de los miembros a reconocer la información como uno de los principales activos así como, un motor de intercambio y desarrollo en el ámbito de los negocios.

- Objetivos de la política y descripción clara de los elementos involucrados en la definición.

- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.

- Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.

Definición de violaciones y consecuencias del no cumplimiento de la política.

- Responsabilidades de los usuarios con respecto a la información a la que se tiene acceso.

Las PSI deben ofrecer explicaciones comprensibles acerca de por qué deben tomarse ciertas decisiones, transmitir por qué son importantes estos u otros recursos o servicios.

De igual forma, las PSI establecen las expectativas de la organización en relación con la seguridad y lo que ella puede esperar de las acciones que la materializan en la compañía. Deben mantener un lenguaje común libre de tecnicismos y términos legales que impidan una comprensión clara de las mismas, sin sacrificar la precisión y formalidad dentro de la empresa **[14]**.

Proposición de una forma de realizar el análisis para llevar a cabo un sistema de seguridad Informática: En la Figura 6.5 se muestran todos los elementos intervienen para el estudio de una política de seguridad.

Se inicia realizando una evaluación del factor humano participativo - tomando en cuenta que éste es el punto más vulnerable en toda la cadena de seguridad, de los mecanismos con que se cuentan para llevar a cabo los procesos necesarios (mecanismos técnicos, físicos ó lógicos), luego, con el medio ambiente en que se desempeña el sistema, las consecuencias que puede traer aparejado defectos en la seguridad (pérdidas físicas, pérdidas económicas, en la imagen de la organización, etc.), y cuáles son las amenazas posibles.

Una vez evaluado todo lo anterior, se origina un programa de seguridad, que involucra los pasos a tomar para asegurar el umbral de seguridad que se desea. Luego, se pasa al plan de acción, es cómo se va a llevar a cabo el programa de seguridad. Finalmente, se redactan los procedimientos y normas que permiten llegar a buen destino.

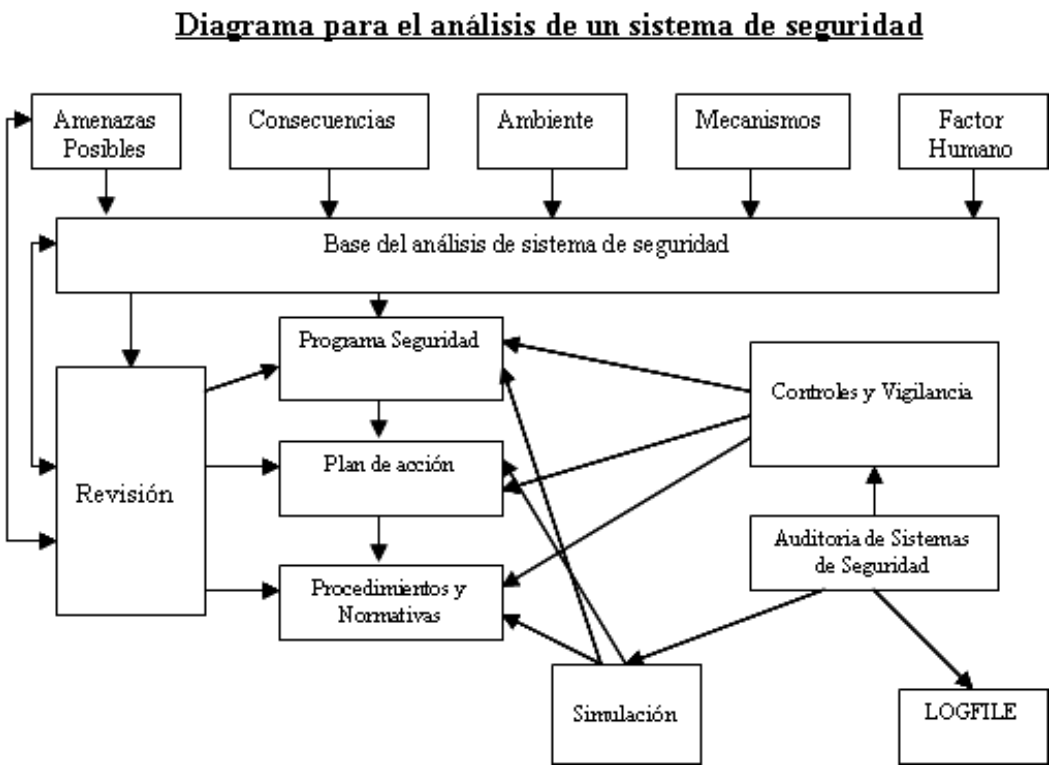


Figura 6.5.- Diagrama para el análisis de un sistema de seguridad.

Con la finalidad de asegurar el cumplimiento de todo lo anterior, se realizan los controles y la vigilancia aseguran el fiel cumplimiento de los tres puntos anteriores. Para asegurar un marco efectivo, se realizan auditorias a los controles y a los archivos logísticos se generen en los procesos implementados (de nada vale tener archivos logísticos si nunca se analizan o se verifican cuando ya ha ocurrido un problema).

Con el objeto de confirmar el buen funcionamiento de lo creado, se procede a simular eventos que atenten contra la seguridad del sistema. Como el proceso de seguridad es un paso dinámico, es necesario realizar revisiones al programa de seguridad, al plan de acción y a los procedimientos y normas.

Es claro que el establecimiento de políticas de seguridad es un momento preciso sobre el que hay que estar actuando permanentemente, de manera tal que no quede desactualizado; cuando se le descubran debilidades, éstas sean corregidas y, finalmente, la práctica por los integrantes de la organización no caiga en desuso.

La mayoría de las veces, las organizaciones realizan grandes esfuerzos para definir las directrices de seguridad y concretarlas en documentos orienten las acciones de las mismas, con relativo éxito.

En particular, la gente debe conocer las consecuencias de las decisiones, incluyendo lo mejor y lo peor pueda ocurrir. Una intromisión o una travesura pueden convertir a las personas no entendieron, en blanco de las políticas. Luego, para que las PSI logren abrirse espacio en el interior de una organización deben integrarse a las estrategias del negocio, a la misión y visión, con el propósito de que los que toman las decisiones reconozcan la importancia e incidencias en las proyecciones y utilidades de la compañía.

De igual forma, las PSI deben ir acompañadas de una visión de negocio que promueva actividades que involucren a las personas en el hacer diario, donde se identifiquen las necesidades y acciones que materializan las políticas. En este contexto, entender la organización, los elementos culturales y comportamientos que debe llevar a reconocer las pautas de seguridad necesaria y suficiente asegure confiabilidad en las operaciones y funcionalidad de la compañía **[20]**.

6.2.2.- Algunos parámetros para establecer políticas de seguridad

Las características de las PSI que se han indicado hasta el momento, dan una perspectiva de las implicaciones en la formulación de estas directrices, revisar a continuación, algunos aspectos generales recomendadas para la formulación de las mismas.

- Efectuar un ejercicio de análisis de riesgos informático, a través del cual los activos, el cual le permitirá afinar las PSI de la organización.

- Involucrar a las áreas propietarias de los recursos o servicios, que poseen la experiencia y son fuente principal para establecer el alcance y las definiciones de violaciones a la PSI.

- El personal esté involucrado en el desarrollo de las PSI comunicarle los beneficios y riesgos estén relacionados con los recursos y bienes, y los elementos de seguridad.
- Identificar quién tiene la autoridad para la toma de decisiones, ellos son los responsables de proteger los activos críticos de la funcionalidad del área u organización.

- Desarrollar un proceso de monitoreo constante de las directrices en el hacer de la organización, que permitan una actualización oportuna de las mismas.

Último consejo: no dé por hecho algo que es obvio. Haga claro y preciso los alcances y propuestas de seguridad, con el propósito de evitar sorpresas y malos entendidos en el momento de establecer los mecanismos de seguridad que respondan a las PSI trazadas **[17]**.

6.2.3.- Las políticas de seguridad informática como base de la administración de la seguridad integral

Las políticas de seguridad informática conforman el conjunto de lineamientos que una organización debe seguir para asegurar la confiabilidad de los sistemas. En razón de lo anterior, son parte del engranaje del sistema de seguridad que la organización posee para proteger los activos.

Las PSI constituyen las alarmas y compromisos compartidos en la organización, que le permiten actuar proactivamente ante situaciones que comprometan la integridad. Efectivamente, deben constituir un proceso continuo y retroalimentado que observe la concientización, los métodos de acceso a la información, el monitoreo de cumplimiento y la renovación, aceptación de las directrices y estrategia de implantación, lleven a una formulación de directivas institucionales que logren la aceptación general.

Las políticas semejantes no constituyen una garantía para la seguridad de la organización. Ellas deben responder a intereses y necesidades organizacionales establecidas en la visión de negocio, lleven a un esfuerzo conjunto de los actores por administrar los recursos y a reconocer en los mecanismos de seguridad informática factores que facilitan la normalización y materialización de los compromisos adquiridos con la organización **[17].**

La seguridad tiene varios estratos:

- El marco jurídico adecuado.
- Medidas técnico-administrativas, como la existencia de políticas y procedimientos o la creación de funciones, como administración de la seguridad o auditoria de sistemas de información interna.

Ambas funciones han de ser independientes y nunca una misma persona puede realizar las dos ni existir dependencia jerárquica de una función respecto de otra.

En cuanto a la administración de seguridad pueden existir, además, coordinadores en las diferentes áreas funcionales y geográficas de cada entidad, especialmente si la dispersión, la complejidad organizativa o el volumen de la entidad así lo demandan.
En todo caso, debe existir una definición de funciones y una separación suficiente de tareas. No tiene sentido que una misma persona autorice una transacción, la introduzca, y revise después los resultados (ejemplo, un diario de operaciones), porque puede planificar un fraude o encubrir cualquier anomalía; por ello deben intervenir funciones / personas

diferentes y existir controles suficientes. La seguridad física, como la ubicación de los centros de procesos, las protecciones físicas, el control físico de accesos, los vigilantes, las medidas contra el fuego y el agua, y otras similares.

La llamada seguridad lógica, como el control de accesos a la información exige la identificación y autentificación del usuario, o el cifrado de soportes magnéticos intercambiados entre entidades o de respaldo interno, o de información transmitida por línea. Puede haber cifrado de la información por dispositivos físicos o a través de programas, y en casos más críticos existen los dos niveles **[17]**.

6.2.3.1.- Riesgos

La *"autentificación"* suele ejecutarse mediante una contraseña, aún cuando sería más lógico - si bien los costes resultan altos para la mayoría de sistemas - se puede combinar con características biométricas del usuario para impedir la suplantación. Entre éstas pueden estar: la realización de la firma con reconocimiento automático por ordenador, el análisis del fondo de ojo, la huella digital u otras.

Al margen de la seguridad, parece que el mayor riesgo, aún teniendo un entorno muy seguro, es que la Informática y la Tecnología de la Información en general no cubran las necesidades de la entidad; o que no estén alineadas con las finalidades de la organización.

Definir a la seguridad propiamente dicha, los riesgos pueden ser múltiples. Primero es conocer y segundo es tomar decisiones al respecto; conocer y no tomarlos no tiene sentido y debiera de establecerse una situación de preocupación. Las medidas tienen un costo, a veces, los funcionarios se preguntan cuál es el riesgo máximo que puede soportar la organización.

La respuesta no es fácil porque depende de la vulnerabilidad del sector y de la entidad misma, de la dependencia respecto de la información, y del impacto que la no disponibilidad pueda tener en la entidad. Si se fundamenta en el impacto nunca debería aceptarse un riesgo que lograra llegar a poner en peligro la propia continuidad de la entidad, pero este riesgo es demasiado alto **[17]**.

Por debajo de ello hay daños de menores consecuencias, siendo los errores y omisiones la causa más frecuente - normalmente de poco impacto pero frecuencia muy alta - y otros, como por ejemplo:

- El acceso indebido a los datos (a veces a través de redes).
- La cesión no autorizada de soportes magnéticos con información crítica (algunos dicen "sensible").
- Los daños por fuego, por agua (del exterior como puede ser una inundación, o por una tubería interior).
- La variación no autorizada de programas, la copia indebida, y tantos otros, persiguiendo el propio beneficio o causar un daño, a veces por venganza. Otra figura es la del *"hacker",* intenta acceder a los sistemas sobre todo para demostrar

(a veces, para demostrarse a sí mismo/a) qué es capaz de hacer, al superar las barreras de protección se hayan establecido **[17]**.

Alguien puede preguntarse por qué no se citan los virus, cuando han tenido tanta incidencia.

Afortunadamente, este riesgo es menor en la actualidad comparando con años atrás. Existe, de todas maneras, un riesgo constante porque de forma continua aparecen nuevas modalidades, no son detectadas por los programas antivirus hasta que las nuevas versiones los contemplan.

Un riesgo adicional es que los *"virus"* pueden llegar a afectar a los grandes sistemas, sobre todo a través de las redes, pero esto es realmente difícil - no imposible- por las características y la complejidad de los grandes equipos y debido a las características de diseño de los sistemas operativos.

En definitiva, las amenazas hechas realidad pueden llegar a afectar los datos, en las personas, en los programas, en los equipos, en la red y algunas veces, simultáneamente en varios de ellos, como puede ser un incendio.

Las personas resultan el punto más crítico y el valor de una vida humana no se puede comparar con las computadoras, las aplicaciones o los datos de cualquier entidad. Ahora bien, por otra parte, puede determinar los datos son aún más críticos si se centra en la continuidad de la entidad.

Como consecuencia de cualquier incidencia, se pueden producir unas pérdidas que pueden ser no sólo directas (cubiertas por los seguros) más fácilmente, sino también indirectas, como la no recuperación de deudas al perder los datos, o no poder tomar las decisiones adecuadas en el momento oportuno por carecer de información.

Saber que se producen casos similares en gran parte de entidades, pero en general no conoce a cuáles han afectado (o lo sabe pero no puede difundirlo), porque por cuidar una imagen estos no se hacen públicos y el hecho de que se conozcan muchos más referidos a Estados Unidos y a otros puntos lejanos que respecto de los países no significa esté a salvo, sino que el interés empresarial es mayor y lo oculta siempre que puede **[18]**.

6.2.3.2.- Niveles de trabajo

Confidencialidad: Consiste en proteger la información contra la lectura no autorizada explícitamente. Incluye no sólo la protección de la información en la totalidad, sino también las piezas individuales pueden ser utilizadas para inferir otros elementos de información confidencial.

Integridad: Es necesario proteger la información contra la modificación sin el permiso del dueño. Ser protegida incluye no sólo la que está almacenada directamente en los sistemas

de cómputo sino que también se deben considerar elementos menos obvios como respaldos, documentación, registros de contabilidad del sistema, tránsito en una red, etc.

Autenticidad: En cuanto a telecomunicaciones se refiere, la autenticidad garantiza que quien dice ser "X" es realmente "X". Es decir, se deben implementar mecanismos para verificar quién está enviando la información.

No–repudio: Ni el origen ni el destino en un mensaje pueden negar la transmisión. Quien envía el mensaje debe probar que, en efecto, el mensaje fue enviado y viceversa.

Disponibilidad de los recursos y de la información: De nada sirve la información si se encuentra intacta en el sistema pero los usuarios no pueden acceder a ella. Por tanto, se deben proteger los servicios de cómputo de manera que no se degraden o dejen de estar disponibles a los usuarios de forma no autorizada **[20]**.

Consistencia: Se trata de asegurar que el sistema siempre se comporte de la forma esperada, de tal manera los usuarios no encuentren variantes inesperadas.

Control de acceso a los recursos: Consiste en controlar quién utiliza el sistema o cualquiera de los recursos que ofrece y cómo lo hace.

Auditoria: Consiste en contar con los mecanismos para poder determinar qué es lo que sucede en el sistema, qué es lo que hace cada uno de los usuarios y los tiempos y fechas de dichas acciones.

Resulta de extrema importancia, cuando se trata de los derechos de los usuarios, diferenciar entre “espiar” y “monitorear” a los mismos.

Todos estos servicios de seguridad deben ser tomados en cuenta en el momento de elaborar las políticas y procedimientos de una organización para evitar pasar por alto cuestiones importantes como las que señalan dichos servicios.

De esta manera, es posible sentar de forma concreta y clara los derechos y límites de usuarios y administradores. Sin embargo antes de realizar cualquier acción para lograr garantizar estos servicios, es necesario asegurar de que los usuarios conozcan los derechos y obligaciones (es decir, las políticas), de tal forma que no se sientan agredidos por los procedimientos organizacionales **[20]**.

6.2.3.3.- Tipos de procedimientos para la conexión de red

Procedimiento de alta de cuenta de usuario: Cuando un elemento de la organización requiere una cuenta de operación en el sistema, debe llenar un formulario que contenga, al menos los siguientes datos:

1. Nombre y Apellido.
2. Puesto de trabajo.

3. Jefe inmediato superior que avale el pedido.
4. Descripción de los trabajos que debe realizar en el sistema.
5. Consentimiento de que las actividades son susceptibles de ser auditadas en cualquier momento y de que conoce las normas de "buen uso de los recursos" (para lo cual, se le debe dar una copia de tales normas).
6. Explicaciones breves, pero claras de cómo elegir un *"password".*

Asimismo, este formulario debe tener otros elementos que conciernen a la parte de ejecución del área encargada de dar de alta la cuenta, datos como:

1. Datos referentes a los permisos de acceso (por ejemplo, tipos de permisos a los diferentes directorios y/o archivos) Si tiene o no restricciones horarias para el uso de algunos recursos y/o para el ingreso al sistema.
2. Tipo de cuenta.
3. Fecha de caducidad.
4. Fecha de expiración **[17]**.

Procedimiento de baja de cuenta de usuario: Este procedimiento es el que se lleva a cabo cuando se aleja un elemento de la organización o cuando alguien deja de trabajar por un determinado tiempo (licencia sin goce de sueldo, vacaciones, viajes prolongados, etc.). En base a la explicación anterior hay, entonces, dos tipos de alejamientos: permanente y parcial.

Procedimiento para determinar las buenos passwords: Aunque no lo parezca, la verificación de palabras claves efectivas no es algo frecuente en casi ninguna organización. El procedimiento debe explicar las normas para elegir una *"password"*:

Se debe explicitar:

- La cantidad de caracteres mínimo que debe tener.
- No tiene que tener relación directa con las características del usuario.
- Debe constar de caracteres alfanuméricos, mayúsculas, minúsculas, números y símbolos de puntuación.
- Determinar, si es posible, el seguimiento de las palabras claves (llevar registros de las palabras claves anteriores elegidas por el usuario).

Una vez que el usuario ha elegido el *"password",* se le debe correr un "programa crackeador" para tener idea de que tan segura es, en base al tiempo que tarda en romper la palabra **[20]**.

Procedimientos de verificación de accesos: Debe explicar la forma de realizar las auditorias de los archivos logísticos de ingresos a fin de detectar actividades anómalas. También debe detectar el tiempo entre la auditoria y cómo actuar en caso de detectar desviaciones.

Normalmente, este trabajo es realizado por programas a los que se les dan normativas de qué y cómo comparar. Escanean archivos de *"log"* con diferentes fechas tomando en

cuenta las reglas que se le han dado. Ante la detección de un desvío, generan reportes informando el mismo.

En el procedimiento debe quedar perfectamente indicado quién es el responsable del mantenimiento de estos programas y cómo se actúa cuando se generan alarmas **[17]**.

Procedimiento para el chequeo del tráfico de la red: Permite conocer el comportamiento del tráfico en la red, al detectar variaciones que pueden ser síntoma de mal uso de la misma.

El procedimiento debe indicar el/los programas que se ejecuten, con qué intervalos, con qué reglas de trabajo, quién se encarga de procesar y/o monitorear los datos generados por ellos y cómo se actúa en consecuencia.

Procedimiento para el monitoreo de los volúmenes de correo: Este procedimiento permite conocer los volúmenes del tráfico de correo o la cantidad de "mails" en tránsito. Dicho procedimiento se encuentra realizado por programas que llevan las estadísticas, generando reportes con la información pedida. El conocimiento de esta información permite conocer, entre otras cosas, el uso de los medios de comunicación, y si el servidor está siendo objeto de un "spam".

Como en los casos anteriores, en el procedimiento debe estar explicitado quién es el encargado del mantenimiento y del análisis de los datos generados, y qué hacer cuando se detectan variaciones **[17]**.

Procedimientos para el monitoreo de conexiones activas: Este procedimiento se efectúa con el objeto de prevenir algún usuario deje la terminal abierta y sea posible alguien use la cuenta. El procedimiento es ejecutado por medio de programas que monitorean la actividad de las conexiones de usuarios.

Cuando detecta que una terminal tiene cierto tiempo inactiva, cierra la conexión y genera un *"log"* con el acontecimiento.

Procedimiento de modificación de archivos: Este procedimiento sirve para detectar la modificación no autorizada y la integridad de los archivos y, en muchos casos, permite la traza de las modificaciones realizadas. Al igual en los casos anteriores, debe estar bien determinada la responsabilidad de quién es el encargado del seguimiento y de actuar en caso de alarmas **[17]**.

Procedimientos para el resguardo de copias de seguridad: Este procedimiento debe indicar claramente dónde se deben guardar las copias de seguridad y los pasos a seguir en caso de problemas. Para lograr esto, deben estar identificados los roles de las personas que interactúan con el área, a fin de que cada uno sepa qué hacer ante la aparición de problemas.

Procedimientos para la verificación de las computadoras de los usuarios: Este procedimiento permitirá encontrar programas no deberían estar en las computadoras de

los usuarios y que, por el carácter, pueden traer problemas de licencias y fuente potencial de virus. El procedimiento debe explicitar los métodos que se van a utilizar para la verificación, las acciones ante los desvíos y quién/quiénes lo llevarán a cabo **[17]**.

Procedimientos para el monitoreo de los puertos en la red: Este procedimiento permite saber qué puertos están habilitados en la red, y, en algunos casos, chequear la seguridad de los mismos. El procedimiento deberá describir qué programas se deben ejecutar, con qué reglas, quién estará a cargo de llevarlo a cabo y qué hacer ante las desviaciones detectadas.

Pasos de cómo dar a conocer las nuevas normas de seguridad: Este tipo de procedimiento no siempre es valorado. Sin embargo, en una organización es muy importante conocer las últimas modificaciones realizadas a los procedimientos, de tal manera que nadie pueda poner cómo excusa “que no conocía las modificaciones”. En él, debe describirse la forma de realizar los pasos de las modificaciones: puede ser mediante un mailing, por exposición en transparencias, por notificación expresa, etc.; quién estará a cargo de la tarea y las atribuciones que tiene.

Es fundamental tener en cuenta este último punto ya que un porcentaje de los problemas de seguridad, según está demostrado en estudios de mercado, proviene del desconocimiento de las normas y/o modificaciones a ellas por parte de los usuarios **[17]**.

Procedimientos para la determinación de identificación de usuario y grupo de pertenencia por defecto: Este camino determina la forma de establecer las identificaciones y los grupos a los que pertenecerán los usuarios por defecto en el momento de darlos de alta. En él deben explicarse, concisamente, los pasos a seguir para cambiar los derechos y las identificaciones de los usuarios dados de alta y la manera de documentar los mismos, así también como quién será responsable de la tarea.

Procedimientos para recuperar información: Esta vía sirve para reconstruir todo el sistema o parte de él, a partir de las copias de seguridad. En él, deben explicarse todos los pasos a seguir para rearmar el sistema a partir de los back-up existentes, así como cada cuánto tiempo habría que llevarlos a cabo y quiénes son los responsables de dicha tarea **[17]**.

Afectan a nivel legal informática forense

Para muchos norteamericanos, tanto criminales como inocentes, el primer afectado en la era digital es el derecho a la privacidad.

El FBI(Buró Federal de Investigaciones) reconoció la existencia de Magic Lantern, un programa tipo caballo troyano que ha estado desarrollando y que será capaz de desactivar el proceso de incriptado en la computadora del sospechoso, al registrar la escritura del usuario. Conjuntamente con leyes aprobadas por el congreso de los EE.UU. a raíz de los ataques, Magic Lantern brindará al FBI un acceso sin precedentes a las comunicaciones digitales.

Pero será posible que el gobierno utilice la batalla contra el terrorismo como excusa para ganar poderes de vigilancia anhelados durante mucho tiempo, o está tratando únicamente de mantenerse al mismo nivel de lso criminales experimentados en tecnología.

Magic Lantern permitirá que el agente coloque el registrador de escritura en determinada computadora mediante un programa similar a un virus. Una vez activado, el registrador captará las palabras y los números a medida que el sujeto los escribe en el teclado (antes que comience el proceso de encriptado) y los transmitirá al agente.

Según los partidarios de la privacidad, este programa, que aún no ha sido desplegado, es un intento por parte del gobierno de reunir claves de los fabricantes de software de encriptado, que a su vez permitirá a los oficiales descifrar la información de un sospechoso. El gobierno quiere ser capaz de entrar a las computadoras de las personas, esa es la orden de vigilancia, explica Jim Dempsey, director asistente del centro para la democracia y la tecnología. Cualquier capacidad que le permita a ellos (el gobierno) hacer eso, se hará.

Por su parte, el FBI dice que necesita tales herramientas para luchas contra los criminales. Las organizaciones para el cumplimiento de la ley están tratando de ponerse al día de muchas maneras.

Para nadie es un secreto que los criminales y terroristas están explotando la tecnología en sus crímenes. El FBI no pide más que continuar teniendo la posibilidad de llevar a cabo capturas legales de criminales y terroristas.

La mayoría de los defensores de la privacidad afirman que la tecnología no es lo que les preocupa, sino el descuido judicial en el uso de estos programas.

Los avances en la tecnología requerirán nuevas técnicas en el cumplimiento de la ley. Es posible que estas herramientas funcionen si se utilizan de manera apropiada dentro del sistema de cheques y balances, y entonces podremos aceptarlas. Sin embargo explica, las mismas protecciones de privacidad que regulan todo lo demás también deben regular el mundo digital.

6.3.- Seguridad en redes

6.3.1- Redes IP

Los hackers utilizan varias técnicas para quebrar los sistemas de seguridad de una red. Básicamente buscan los puntos débiles del sistema para poder colarse en ella. El trabajo de los testers no difiere mucho de esto. En lo que sí se diferencia, y por completo, es en los objetivos.

Mientras los hackers penetran en las redes para dañar o robar información, un testers lo hace para poder mejorar los sistemas de seguridad.

Al conjunto de técnicas que se utilizan para evaluar y probar la seguridad de una red se le conoce como Penetration Testing, uno de los recursos más poderosos con los que se cuenta hoy para generar barreras cada vez más eficaces.

> *En cuanto a las barreras de seguridad, un testers explica:* "Están totalmente relacionadas con el tipo de información se maneja en cada organización. Por consiguiente, según la información que deba ser protegida, se determinan la estructura y las herramientas de seguridad. No a la inversa".
>
> *Las herramientas no son sólo técnicas:* El software y el hardware utilizados son una parte importante, pero no la única. A ella se agrega lo que se denomina "políticas de seguridad internas", cada empresa u organización debe generar.

La explicación del porqué viene de un dato de la realidad. Los mismos empleados hackean a la propia organización. Y aquí es donde cobran especial importancia las políticas de seguridad se establezcan, además del aspecto técnico **[20]**.

> *Hacking; Nuevos teléfonos móviles pueden ser hackeados:* Modelos de teléfonos móviles son vulnerables ante ataques externos. Según expertos, las listas de contactos pueden ser robadas y las conversaciones interceptadas.
>
> *Hacking; Google, el favorito de los hackers:* No sólo los usuarios legítimos prefieren a Google. El buscador es una de las herramientas más importantes para hackers buscan sitios Web con seguridad deficiente.

6.3.2.- Redes de Comunicaciones

Figura 6.6.- Seguridad en redes de comunicaciones.

Los principales ataques a los sistemas provienen de la red (ver Figura 6.6). Proteger la misma de intrusiones no deseadas es, por tanto, uno de los objetivos prioritarios un *“administrador”* debe proponerse **[18]**.

Windows IP Security, del Internet Engineering Task Force, proporciona a los administradores de redes un elemento estratégico de defensa para la protección de las redes.

6.3.3.- Redes inalámbricas

Red inalámbrica se encarga que los usuarios puedan conectarse a una red local o a Internet sin estar conectado físicamente, los datos (paquetes de información) se transmiten por el aire.

Al montar un red inalámbrica se necesita una computadora que de un "punto de acceso" y lo demás son "dispositivos de control (ver Figura 6.7)", toda esta infraestructura puede variar dependiendo el tipo de red que se quiera montar en tamaño y en distancia **[17]**.

Figura 6.7.- Dispositivos de control.

Tipos de inseguridades: Si una red inalámbrica está bien configurada no puede pasar por muchos problemas y estar más tranquila.

Las inseguridades de las redes inalámbricas radica en:

- Configuración del propio "servidor" (puntos de accesos).
- La "escucha" (impulsar la comunicación del envió de paquetes).
- "Portadoras" o pisar el radio de onda (no muy común), mandar paquetes al aire, pero dicha posibilidad es real.

Los datos son transmitidos como las ondas que se reciben en la televisión o radio, si alguien tiene un receptor pueden ver los datos o si quiere estropear el radio de transmisión **[20]**.

Consejos de seguridad: Algún intruso tiene que ser *"nodo"* o usuario para que pueda ingresar en la red inalámbrica, el peligro puede ser en escuchar la transmisión. Consejos para la red inalámbrica:

- Cambiar las claves por defecto cuando se instalen el software del Punto De Acceso.
- Control de acceso seguro con autentificación bidireccional.
- Control y filtrado de direcciones "MAC" e identificadores de red para restringir los adaptadores y puntos de acceso que se puedan conectar a la red.
- Configuración "WEP" (muy importante), la seguridad del cifrado de paquetes que se transmiten es fundamental en las redes inalámbricas, la codificación puede ser más o menos segura dependiendo del tamaño de la clave creada y el nivel, la más recomendable es de 128 Bits.

- Crear varias claves “WEP”, para el punto de acceso y los clientes y que varíen cada día.
- Utilizar opciones no compatibles, si la red es de una misma marca escoger esta opción para tener un punto más de seguridad, esto hará que el posible intruso tenga que trabajar con un modelo compatible al que tenga.
- Radio de transmisión o extensión de cobertura, este punto no es muy común en todos los modelos, resulta más caro, pero si se puede controlar el radio de transmisión al círculo de la red puede conseguir un nivel de seguridad muy alto y bastante útil **[19]**.

Afectan los Hackers en las redes inalámbricas

Hay demasiados peligros para seguir sin protección. Las herramientas antivirus detienen virus, gusanos y troyanos conocidos; los muros de fuego pueden evitar una comunicación inapropiada dentro y fuera de computadora y la red.

Un programa antivirus están bueno como actualización más reciente.

Los muros de fuego son clave en la seguridad, puede evitar la comunicación inadecuada dentro y fuera computadora. Con vigilancia del correo electrónico de salida, limpiador de cáche, reglas de muro de fuego para expertos y valores de importación/exportación en una sencilla interfaz, quizá sea intimidante para los usuarios nuevos, pero sus valores predeterminados protegen desde el principio y la interfaz es fácil.

El ruteador/muro de fuego protege su red inalámbrica de piratas y abusivos de ancho de banda.

Firewall facilita a los principiantes la protección de sus máquinas, configurando de manera automática las aplicaciones comunes.

Los ruteadores/muros de fuego de hardware ofrecen mayor conveniencia y seguridad de que sus primos de software cubriendo toda la red, en un lugar de una sola computadora.

Conclusiones

CONCLUSIONES

El desarrollo del tema de Hacking y técnicas de contra ataques a la seguridad de la información se basa en la seguridad que hay en día, y por ello hoy existen diversas causas para protegerse de cualquier situación que se encuentre, como el firewall, es un sistema que protege a una computadora de posibles accesos por parte de usuarios no autorizados.

Hay ataques de gente sin escrúpulos, es por eso que es importante estar al tanto para protegerse en cualquier situación que se presente, para proteger la información es necesario tener una cuenta difícil para ladrones informáticos. En medio de esta variedad han ido aumentando las acciones poco respetuosas con la privacidad y con la propiedad de recursos y sistemas. *Hackers, crakers* y demás han aumentado el vocabulario ordinario de los usuarios y de los administradores de las redes. Hacker se encarga de violar algún servidor sin hacer algún daño en cambio el cracker realiza fraudes con tarjetas de crédito o lo que se le presente, su intención es destruir.

Los ataques a la seguridad, como virus, caballos de troya y otros como pueden ser eavesdropping, packet sniffing, snooping y dowloading, tampering o data diddling,… etc. También existen ataques a los sistemas informáticos como es el escaneo de puertos. Hay que tener cuidado con esto, tener una medida de protección como es el firewall para poder combatir esto, ya se menciono anteriormente de que se encarga.

Un hacker puede ingresar al sistema, mediante el administrador como root es importante borrar huellas y finalizar con un programa que monitoriza la red, consiguiendo login y passwords para acceder a otros sistemas.

Es recomendable llevar a cabo las medidas de protección, para que no surga algún problema con el servidor. La seguridad de la información, es importante debe estar al día con la actualización.

Anexo

1

Hacer hackeo

Hacer hackeo

Listado de recomendaciones para el usuario Windows.

SEGURIDAD

- Instalar y actualizar la última plataforma publicada para usuarios del OS MS-Windows [XP Pro recomendado] ya que es mucho mas estable que sus predecesoras "estando debidamente administrado". No es recomendable dejarlo instalado por defecto.

- Instalar los Service Pack [Paquetes de actualización] de las Plataformas Windows offline, desde un CD luego de haberlo instalado ya que con esto no se correrá el riesgo de conectar la maquina a Internet demasiado vulnerable y exponerla a infecciones de gusanos o diversas instrucciones de terceros.

- Instalarle un firewall.

- Una vez Instalado el firewall actualizar al día de la fecha Windows [gratuitamente y por mas que tu instalación no sea de licencia legal podrás hacerlo] en http://www.windowsupdate.com allí buscar actualizaciones e instalarlas en modo cronológico hasta tenerlas todas aplicadas.

- Instalar Antivirus, actualizarlo, configurarlo y escanear, que monitoree actividad maliciosa en background* (*En tiempo real y files que se ejecutan) e e-mails.

- Instalar Antitroyano, actualizar, configurarlo y escanear, que monitoree en background*. Recomendado The Cleaner www.moosoft.com
  *Ejecutar TCActive! -

Con ello podrás encriptar y firmar e-mails entre amigos, además que ningún admin de ISP o intruso te lea información importante. También podrás borrar información de modo seguro y esta no podrá ser recuperada (wipe).

PERFORMANCE

- Tener como mínimo 512 RAM y un micro medianamente aceptable si se desea implementar la mayoría de estos puntos.

- Para mayor performance de Windows XP vayan a Inicio - Ejecutar: > Ejecutar (copy y paste)SystemRoot\system32\services.msc /s y deshabilitar con click derecho en opciones, todos esos servicios remotos y de sistema inútiles que se cargan al principio, mirar BIEN lo que se cambia y anotar.

- Si el XP funciona lento, se resetea sola o te consume el rígido sin razón aparente, puedes: Deshabilitar Restaurar Sistema (tildando Desactivar desde Propiedades de sistema), destildar Resetear (de Inicio y Recuperación) y defragmentar completo.

PREVENCION Y MANTENIMIENTO

- Implementar una política de backups en CD cada determinado periodo de tiempo, bimensual, semanal o diario, según su trabajo o material.

- Implementar política para el cambiado de claves cada determinado periodo de tiempo, estos suelen viajar en texto plano por la Net y suelen ser capturados por terceros, ya sea casual o intencionalmente, posteriormente usados con fines intrusivos o bien para obtener información de algún tipo, etc.

  Cambia los passwords de sitios, casillas de e-mails y conexión cada cierto tiempo. No solo los administradores de ISP ven tus pass día a día, sino mucha gente externa, amigos de los admins e intrusos varios y amigos de estos. El programa Steganos tiene un agradable y útil administrador de passwords como así también PGP puede usarse para resguardar las mismas.

CONSEJOS VARIOS

- No creas en los e-mails con atachados que vienen de Microsoft o Hotmail o de empresas reconocidas, el SPAM no sirve ni en útil de ninguna manera, TODO mail que te haya llegado sin esperarlo tienes que desecharlo. No abrir tarjetas postales de desconocidos y menos poner la clave Hotmail, Yahoo u otra en el primer sitio de este que se habrá.

- No escribir sobre cosas personales ni dato alguno a desconocidos (pueden serle utiles para futuro hackeo) que aparecen por IRC, MSN, ICQ, E-Mails, Webchat, Teléfono, en la calle, etc... Si los das procurar que sea alguien de confianza y asegúrate de que la seguridad de pc este en buen estado. No aceptes archivos en IRC, ICQ, FTPs, URL, de nadie desconocido que pueden ser un backdoor o troyano. Ya sea sources o binarios.

- Instruir a la persona "de confianza" (Cuidado con el hack local mas que nada por empleados desleales o compañeros de trabajo) que le dejes la PC a cargo: Hermanos, empleados, parientes y amigos, coméntale los riesgos poniéndolo al tanto de estas básicas para que nadie se aproveche de él en la net, más si recién comienza a navegar por la net. Educar principalmente a las secretarias, tanto con el teléfono como la PC y la data que da de la empresa, su entorno o componentes.

- Elegir buenas contraseñas de mas de 8 dígitos alfanuméricas, no usar por ejemplo el mismo login que el password o cosas como nombre de pila o comunes: 123456, " tu birthday " , 111222, "mascota", nataliateamo, admin, tu nick o nombre de hija/o agus32, pablo82, etc.

Glosario

Glosario

Administrador, SYSOP, ROOT: Persona que se encarga del mantenimiento de un sistema informático, generalmente tienen control total sobre el sistema.

Anonymous: Login predeterminado para sistemas que dejan entrar usuarios libremente sin pedir identificación. Esto comporta siempre limitaciones y restricciones.

ASCII: Se trata de un código con el que se codifican los caracteres (texto, números, signos de puntuación,...etc). Cada uno de ellos tendrá asignado un código de 8 bits (bit: unidad mínima de información, 0 o 1).

Autentificación: El proceso de verificar la identidad del usuario que intenta acceder a la red.

Autorización: Proceso de determinar el tipo de actividades permitidas, está estrechamente relacionado con la autentificación puesto que diferentes usuarios pueden tener diferentes permisos de actividad.

Backbone: Nivel más alto en una red jerárquica. Se garantiza que las redes aisladas (stub) y de tránsito (transit) conectadas al mismo eje central están interconectadas.

Bombas Lógicas: Este suele ser el procedimiento de sabotaje más comúnmente utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada destruir o modificar la información, o provocará el cuelgue del sistema.

Bridge (puente): Un bridge se utiliza cuando tiene que conectar dos redes a nivel de capa de enlace. El dispositivo conecta dos o más segmentos de la misma LAN. Las dos LAN's a ser conectadas pueden ser similares o no, por ejemplo, el bridge puede conectar dos Ethernets entre sí o una ethernet y una Token Ring. A diferencia de los routers, los bridges son independientes del protocolo y transparentes para la capa de red (capa 3). Los Bridges realizan funciones de forwarding y filtrado de paquetes sin rutear mensajes, en consecuencia pueden ser más rápidos que los routers, pero son mucho menos versátiles.

Bug: Error en un programa, que produce que este funcione mal. También se aplica a los virus. (Un bug en un virus podría hacer, por ejemplo, que esté infectara mal los EXEs y los destruyera, etc.)

Caballo De Troya: Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones, por supuesto no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa afecte de una forma diferente a como estaba previsto (ejemplo: Formatear el disco duro, modificar un fichero, sacar un mensaje, etc.).

Cadena: es una consecución de caracteres de texto, dígitos numéricos, signos de puntuación o espacios en blanco consecutivos.

Chat: se trata de conversaciones escritas en Internet. Mediante una conexión a la red y un programa

especial, es posible conversar (mediante texto escrito) con un conjunto ilimitado de personas, al mismo tiempo.

Clave (del Registro)*:* el Registro de Windows (Registry) es un elemento en el que se guardan las especificaciones de configuración del ordenador, mediante valores o claves. Estas claves cambiarán de valor, y/o se crearán, cuando se instalen nuevos programas o se altere la configuración del sistema. Los virus pueden modificar estas claves para producir efectos dañinos.

Clave privada: Es la clave que tan sólo una forma conoce y que se utiliza para desencriptar el mensaje que envían encriptado con la clave pública. Este sistema de clave pública y clave privada se conoce como sistema asimétrico.

Clave pública: Es la que hace que se esté al alcance de todo el mundo para que puedan enviar un mensaje encriptado. También con ella se puede desencriptar lo que se le envié encriptado con la clave privada.

Clave secreta: Es el código básico utilizado para encriptar y desencriptar un mensaje. Cuando se utiliza la misma para las dos funciones, se está ante un sistema simétrico.

Cliente: Un sistema o proceso que solicita a otro sistema o proceso que le preste un servicio. Una estación de trabajo que requiere el contenido de un archivo a un servidor es un cliente de este servidor. Ver también: "client-server model", "server".

Configuración: conjunto opciones elegidas por un administrador para un sistema.

Cookie: Procedimiento ejecutado por el servidor que consiste en guardar información acerca del cliente para la posterior recuperación. En la práctica la información es proporcionada desde el visualizador al servidor del Word Wide Web, vía una forma o un método interactivo que puede ser recuperado nuevamente cuando se accede al servidor en el futuro. Es utilizado por ejemplo para el registro a un servicio.

Correo electrónico: equivalente electrónico al correo normal en el que se intercambian mensajes entre dos (o más) personas, a través de una red.

Cortafuego, Firewall, Bastión: Sistema avanzado de seguridad que impide a personas no acreditadas el acceso al sistema.

Crackeador: Programa utilizado para sacar los password encriptados de los archivos de passwords. Bien, desencriptandolos, cuando se puede, o bien probando múltiples combinaciones hasta que encuentra la correcta.

Cracker (intruso): Un "cracker" es una persona que intenta acceder a un sistema informático sin autorización. Estas personas tienen a menudo malas intenciones, en contraste con los "hackers", y suelen disponer de muchos medios para introducirse en un sistema.

Cracker o Crasher: Dentro de redes informáticas son hackers destructivos.

Criptoanálisis: La rama del conocimiento que se encarga de descifrar los mensajes encriptados sin

conocer las llaves. Se dice que determinada clave ha sido “rota” cuando alguien logra descifrar un mensaje sin conocer la clave que le dio origen.

Criptografía: La rama del conocimiento que se encarga de la escritura secreta, originada en el deseo humano por mantener confidenciales ciertos temas.

Cuenta: darle a una persona acceso a una red, a un sistema. Como la homónima en el banco, consiste en los datos personales de un "cliente" (en este caso, cliente de un sistema) que le permiten que use los servicios ofrecidos. Por lo general se identifican con un nombre.

Datagrama: Un paquete de datos más información de entrega asociada a él.

Debug: Programa que permite la edición y creación de otros programas escritos en lenguajes como Ensamblador (no lenguajes de alto nivel). También hace posible la investigación del código interno en cualquier fichero.

Debugger: Un programa para estudiar el funcionamiento de otros programas. (También sirve para estudiar virus).

Decoy: señuelo en inglés. Programa diseñado para que el usuario caiga en un movimiento donde se le pueda robar la password.

Default: si un programa presenta al operador varias opciones y permite que no elija alguna en particular, utiliza una de estas como la respuesta más general. Esto se llama opción default, por defecto, ya que el usuario no eligió nada.

Desencriptar: Decodificar. Recuperación del estado normal y legible de una información previamente cifrada, encriptada o codificado, que es lo mismo.

DES (Data Encryption Standard): un sistema desarrollado a fines de los años 70 y que se basa en el sistema de la llave única.

Dirección de Destino: Dirección en un paquete que especifica el destino último del paquete. En un cuadro de hardware, la dirección destino debe ser una dirección de hardware. En un datagrama IP la dirección destino debe ser una dirección IP.

Dirección de Protocolo: Número asignado a una computadora que se usa como dirección destino en los paquetes enviados a esa computadora. Cada dirección IP es de 32 bits de longitud; otras familias de protocolo usan otros tamaños de dirección de protocolo.

Directorio, Carpeta: Estos dos términos hacen referencia al mismo concepto. Se trata de divisiones (no físicas) en cualquier tipo de disco donde son almacenados determinados ficheros. Forman parte de una manera de organizar la información del disco, guardando los documentos como si de una carpeta clasificadora se tratase.

DNS (Domain Name Service): Base de Datos distribuida que mapea nombres de sistemas con direcciones IP y viceversa.

DNS Spoofing: Suplantar el nombre DNS de otro sistema.

Dominio: Los nombres de dominio se utilizan para simplificar la identificación de las direcciones dentro de Internet. Se compone de varios nombres separados por puntos.

De izquierda a derecha, los nombres identifican la computadora, luego separada por un punto el tipo de organización (com. para empresas, gov para gobiernos, educ. para educativas, net para las relativas a Internet etc.) al final de la dirección puede aparecer la referencia del país a la que pertenece la página (ar para Argentina, cl para Chile, fr para Francia, etc.)

Dorado: CD pirata, cd-rom con programas pirateados. Se llama dorado, por el color que suelen tener lo cd's grabables.

Enchufe: Conexión telefónica, línea, clavija.

Encriptar: codificar un dato de forma que sólo pueda ser leído por el destinatario.

Entrar, Darse Un Paseo o Echar Un Vistazo: Diversas expresiones, que aplicadas a un sistema informático significan, haberlo hackeado. Entrar tiene un significado claro, mientras que los otros dos, se usan, cuando se ha entrado, pero no se ha tocado ni hecho nada dentro.

Escaneo de puertos: Es como si se llamara a un número de teléfono y según la señal que oiga comunicando, llamada, avería,... saber el estado de ese teléfono en ese preciso momento. Después llamar a otro número y así continuamente. El escaneo tradicional consiste en seleccionar un rango de IPs y hacer esas "llamadas" a las direcciones IP consecutivamente, aunque también se puede hacer un escaneo a una IP concreta. Los firewall actuales detectan esa llamada a puertos consecutivos y por lo tanto reconocen el escaneo. Así que se cambia el método y se escanean los puertos de esas IPs de forma no consecutiva. También se puede cambiar el método de comunicación entre ambas máquinas.

Escáner (antivirus): Programa que busca virus en la memoria del PC o en los archivos.

Escáner bajo demanda: Programa escáner antivirus que el usuario ejecuta manualmente cuando lo estima conveniente (Ver Resident Scanner y Heuristic Scanner).

Escáner heurístico: Programa escáner antivirus que busca virus nuevos y desconocidos. También llamado escáner de situaciones sospechosas.

Escáner de puertos: Programa que recorre un rango de Ips pre-establecido de la red e informa del estado de los puertos. Normalmente sólo muestra los puertos abiertos aunque los hay que muestran el estado de todos ellos.

Escáner residente: Programa escáner antivirus que está buscando virus recursivamente en background.

Escoba: ZAPPER, programa encargado de modificar los logs, para evitar ser detectado.

Estamos Dentro: Expresión de júbilo, de alegría. Se usa para celebrar algún éxito en el hacking, no sólo para celebrar el haber entrado en un sistema, sino que también se usa para alegrarse

de cualquier logro o como expresión de ánimo.

TRUCHA, PESCADO o BAKALAO >> Password, clave, o pista importante.

Ethernet: Red de área local (LAN) desarrollada por Xerox, Digital e Intel. Es el método de acceso LAN que más se utiliza (seguido por Token Ring). Ethernet es una LAN de medios compartidos. Todos los mensajes se diseminan a todos los nodos en el segmento de red. Ethernet conecta hasta 1,024 nodos a 10 Mbits por segundo sobre un par trenzado, un cable coaxial y una fibra óptica.

Los tres tipos principales son: (1) 10Base5 Standard Ethernet, que utiliza un cable coaxial grueso en una topología de bus entre nodos con una longitud de segmento máxima de hasta 1,640 pies, (2) 10Base2 Thin Ethernet, también llamado ThinNet y CheaperNet, que utiliza un cable coaxial más delgado de hasta 607 pies por segmento y (3) 10BaseT, que utiliza pares trenzados conectados a una configuración de estrella a través de un centro con una longitud de segmento máxima de 328 pies. Ethernets más rápidas están surgiendo: una Ethernet conmutada da a cada usuario un canal dedicado de 10 Mbps. Una Ethernet rápida corre a 100 Mbps compartidos.

Exploit: Método concreto de usar un bug para entrar en un sistema.
FAT: File Allocation Table. El "mapa" mediante el cual el DOS mantiene registro de que clusters están usados y a que file pertenecen, etc.

Ficheros SCR: son los denominados ficheros de Script. Su extensión es SCR y sirven para determinar los parámetros ("condiciones") con los que se deben ejecutar unos determinados programas. Permiten iniciar con unas pautas fijadas de antemano.

Filtro de Paquetes: Programa que intercepta paquetes de datos, los lee y rechaza los que no estén en un formato predefinido.

Finger (dedo): Programa que muestra información acerca de un usuario específico, o acerca de todos los usuarios, conectado a un sistema o remoto. Habitualmente se muestra el nombre y apellidos, hora de la última conexión, tiempo de conexión sin actividad, línea del terminal y situación de éste. Puede también mostrar archivos de planificación y de proyecto del usuario.

Firewall: un sistema diseñado para evitar accesos no autorizados desde o hacia una red privada. Los Firewalls pueden estar implementados en hardware o software, o una combinación de ambos. Los firewalls son frecuentemente utilizados para evitar el acceso no autorizado de usuarios de Internet a redes privadas conectadas a la misma, especialmente intranets. Todos los mensajes que dejan o entran a la red pasan a través del firewall, el cual examina cada mensaje y bloquea aquellos que no cumplan con determinado criterio de seguridad.

Firewall a nivel de aplicación: Un sistema de firewall en el que los servicios son manejados por procesos que mantienen conexiones TCP completas, a menudo estos sistemas hacen un remapeado de IP para que todo el tráfico interior aparente proceder del firewall (id: screening).

Firewall Cortafuegos: Programa que sirve para filtrar lo que entra y sale de un sistema conectado a una red. Los filtros se pueden hacer por: contenido, es decir, por cantidad de información; por origen: impidiendo lo que llega desde direcciones IP desconocidas o no autorizadas y por tipo de archivos, rechazando los de determinadas extensiones, por tener estas, por ejemplo, la posibilidad de transmitir virus.

Firewall Router: Filtro de paquetes que filtra el tráfico en base a la dirección destino y fuente.

FTP(File Transfer Protocol):
Protocolo parte de la arquitectura TCP/IP utilizado para la transferencia de archivos. Es el puerto 21 de un sistema determinado, que usa un programa servidor de FTP para que otros usuarios entren con un programa cliente de FTP con el fin de poder subir/bajar archivos de/a ese sistema.

Fichero De Password: Fichero en el que el sistema guarda las claves de acceso.

Firewalls: Protegen a las Intranets de los ataques iniciados contra ellas desde Internet. Están diseñados para protegerse del acceso no autorizado a la información de la empresa, y del daño o rechazo de los recursos y servicios informáticos. También están diseñados para impedir que los usuarios internos accedan a los servicios de Internet que puedan ser peligrosos, como FTP.

Gateway: Ordenador o aplicación que actúa de "puente" entre dos sistemas.

Gateway a Nivel de Aplicación:
Programas escritos especialmente que proveen una barrera de seguridad interpretando los datos producidos por aplicaciones tal como pasan por el firewall. (Ver firewall)

Gateway a Nivel de Circuito: Barrera que intercepta sesiones TCP interponiendo aplicaciones especialmente escritas que leen y copian los datos a través del Firewall. (Ver firewall).

Generador de virus: Un programa para hacer virus. Para utilizarlo sólo se necesita un conocimiento muy básico del tema.

Gopher: Un servicio de distribución de información que ofrece colecciones jerarquizadas de información en Internet. Gopher utiliza un protocolo simple que permite a un cliente Gopher acceder a información desde cualquier servidor Gopher que esté accesible, proporcionándole un único "espacio Gopher" (Gopher space) de información.

Gordo: Sistema importante o muy potente.

Gusano: es programa similar a un virus que se diferencia de éste en la forma de realizar las infecciones. Mientras que los virus intentan infectar a otros programas copiándose dentro de ellos, los gusanos solamente realizan copias de ellos mismos.

Hack: Cuando se rompe la seguridad de un sistema para obtener información y se convierte en el administrador de la red.

Hackear Por Fuerza Bruta: No significa nada bestia, ni que necesite mucha fuerza, simplemente es un hacking que

necesita mucho esfuerzo, mucho tiempo de proceso o de intentos. Como es probar distintos passwords hasta encontrar el acertado, usar un crackeador, desencriptar un fichero encriptado, sacar las claves de un archivo de passwords usando las palabras de un diccionario, etc.

Hacker: Persona que hace hacking. Persona muy hábil con los ordenadores. Pirata informático, en cualquiera de los muchos significados.

Hacking: Penetrar en sistemas informáticos ajenos sin el consentimiento, tanto "virtualmente" como físicamente. (Ej. Entrar en una oficina y robar los manuales). Cualquier acción encaminada a conseguir lo primero; como son la ingeniería social, el trashing, etc.

Hackmode: Modo de actuar del hacker. No tiene por qué estar relacionado con los ordenadores, es más bien un modo de interpretar la vida. Consiste en: * No pagar lo que no es estrictamente necesario o pagar de forma "poco corriente" (V. Carding). * Ser un poco "paranoico". :) * Actuar acorde con costumbres rigurosamente calculadas y mil cosas más que se irán ocurriendo.

Header (cabecera): Parte inicial de un paquete, que precede a los datos propiamente dichos y que contiene las direcciones de origen y destino, control de errores y otros campos. Una cabecera es también la porción de un mensaje de correo electrónico que precede al mensaje propiamente dicho y contiene, entre otras cosas, el emisor del mensaje, la fecha y la hora.

Host (sistema central): Computador que permite a los usuarios comunicarse con otros sistemas centrales de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el correo electrónico, Telnet y FTP. Es la manera fácil de leer una IP, ya que está formada por palabras y algunos números. Ejemplo: pp342.redestb.es.

Host-based security: Técnica que protege un sistema individual de un ataque. Esta técnica depende del S. O.

Hoste: Programa parasitado por el virus, programa infectado. (Ver Overwriting y Parasitico).

HTML: Lenguaje de marcado de hipertexto, (Hiper-Text Markup Languaje) es el lenguaje con que se escriben los documentos en el World Wide Web. A la fecha existen tres versiones de HTML. HTML 1, se sientan las bases para la disposición del texto y las gráficas, HTML 2 donde se agregan formas y HTML 3 (llamado también extensiones Netscape) donde se añaden tablas, mapas, etc.

HTTP: Protocolo de Transferencia de Hipertextos (Hiper-Text Transfer Protocol): Es el protocolo usado por el Word Wide Web para transmitir páginas HTML.

Hub: Un punto común de conexión de dispositivos en una red. Los hubs son usados comúnmente para conectar segmentos de una LAN. Un hub contiene múltiples ports. Cuando un paquete llega al port, es copiado a los otros ports, de esta manera los otros segmentos de la LAN pueden ver todos los paquetes.

Un hub pasivo simplemente sirve de conductor de datos entre los diferentes ports. Los hubs inteligentes incluyen servicios adicionales como para permitir a un administrador monitorear el tráfico y configurar cada port del hub. Estos hubs se conocen generalmente como hubs administrables (manageable hubs). Un tercer tipo de hub, llamado switching hub, lee la dirección de destino en cada paquete y lo envía al port correcto.

ID: identificación.

IMAP: Protocolo de Acceso a Mensajes de Internet (Internet Message Access Protocol). Protocolo diseñado para permitir la manipulación de mailboxes remotos como si fueran locales. IMAP requiere de un servidor que haga las funciones de oficina de correos pero en lugar de leer todo el mailbox y borrarlo, solicita sólo los encabezados de cada mensaje. Se pueden marcar mensajes como para ser borrados sin suprimirlos completamente, pues estos permanecen en el mailbox hasta que el usuario confirma su eliminación.

Infection-On-Close: Infectar al cerrar un archivo, en lugar de cuando es corrido.

Integrated Services Digital Network (ISDN): Red Digital de Servicios Integrados. Tecnología en plena evolución. ISDN combina servicios de voz y digitales a través de la red en un solo medio, haciendo posible ofrecer a los clientes servicios digitales de datos así como conexiones de voz a través de un solo "cable".

Interrupción: Es una señal mediante la cual se consigue hacer una pausa momentánea en las labores que se encuentran ejecutando el cerebro del ordenador (el microprocesador). Cuando ésta tiene lugar el micro abandona las operaciones que estaba realizando y pasa a ejecutar las acciones u operaciones que requiere el tipo de interrupción requerida. Respecto a cada una de ellas, existe un nivel de jerarquías para aceptar unas antes que otras o para que unas permitan interrumpir a las otras.

Cuando se han realizado las acciones correspondientes a un tipo de interrupción aceptada, el microprocesador continúa con la tarea que abandonó en el momento.

Intranet: Red privada conectada a Internet, pero generalmente aislada de esta por un cortafuegos. Red privada que usa los mismo protocolos de comunicación que Internet (TCP/IP) y que puede estar aislada o conectada a Internet.

Intranet: Una red privada dentro de una compañía u organización que utiliza el mismo software que se encuentra en Internet, pero que es sólo para uso interno.

Insider attack: Un ataque que se origina dentro de la red protegida.

IP: Es la combinación de números que nuestro proveedor de Internet asigna cada vez que conecta y que identifica. Ejemplo: 194.179.106.2 (xxx.xxx.xxx.xxx). Cada usuario de Internet tiene una distinta. Los sistemas, por supuesto, también tienen la suya, pero es fija y por eso su Host también es fijo. Ciertos usuarios también pueden contratar una IP fija si lo desean en el proveedor.

IP address (Dirección IP): Dirección de 32 bits definida por el Protocolo Internet en STD 5, RFC 791. Se representa usualmente mediante notación decimal separada por puntos.

IP-SPOOFING: Es una técnica, por la cual, el ordenador con el que estas conectado no conoce la verdadera ip, sino que recibe otra. Se ha mitificado mucho, y en realidad tampoco es nada raro. (Aunque si es difícil hacerlo) Por ejemplo, usar un proxy, es un tipo de ip-spoofing, ya que los ordenadores con los que se conecten a través del proxy, recibirán la ip, de este y no la propia.

IP spoofing: Tipo de ataque en el que un sistema asume la dirección IP de otro para suplantarlo.

IRC: es una de las posibilidades que permite Internet. Mediante el IRC se pueden mantener conversaciones escritas, en tiempo real, entre varios usuarios conectados a un canal de comunicaciones disponible en Internet.

Jacking o Destripamiento: Control total sobre algo, o algún sistema. Se usa sobre todo en cracking o desprotección de programas (debugging) cuando se consigue un dominio total sobre el programa en ejecución. Viene de Jack el destripador.

Jefe: Sysop, administrador del sistema.

Lamer: Nombre genérico, para los tontos informáticos, significa tonto, novato, que sabe poco. La palabra viene de los tiempos del spectrum, y se aplicaba a los programadores que copiaban el código de otros y lo firmaban como propio.

Linux: Sistema Operativo multiusuario, versión UNIX de PC.

Listening: Se dice que un ordenador está esperando conexiones, es decir, si acepta conexiones remotas. Cualquier ordenador que esté listening es vulnerable, nunca se debe olvidar.

LLamada anónima: Uno de los nuevos servicios de telefónica, es la posibilidad de evitar que el caller-id sea enviado, mediante la marcación de un código especial antes de llamar. Este código está siendo investigado y posiblemente sea el sujeto de uno de los nuevos expedientes secretos. Aún así, el teléfono al que llama puede que no acepte llamadas anónimas, con lo que el truco no servirá.

Local Area Network (LAN) (Red de Area Local): Red de datos para dar servicio a un área geográfica pequeña, un edificio por ejemplo, por lo cual mejorar los protocolos de señal de la red para llegar a velocidades de transmisión de hasta 100 Mbps (100 millones de bits por segundo).

LOG: Archivo que recoge un registro de actividades en el sistema, almacena información sobre el acceso al mismo.

Login: Nombre de usuario que se usa para entrar en un sistema determinado o procedimiento de identificarse frente a un sistema para luego usarlo.

Logging: El proceso de almacenar información sobre sucesos que ocurren en la red o el firewall.

Mail gateway: Pasarela de correo, Máquina que conecta entre sí a dos o más sistemas (incluso diferentes) de

correo electrónico y transfiere mensajes entre ellos. A veces, la transformación y traducción pueden ser muy complejas.

MAN: Metropolitan Área Network. Red de Área Metropolitana.

MIME: Extensiones de Correo de Internet de Múltiples propósitos (Multipurpose Internet Mail Extensions) Técnica para codificar archivos y anexarlos a un mensaje de correo electrónico. Permite principalmente enviar archivos binarios como parte de un mensaje.

Mochila: Aparato que se conecta al puerto paralelo y que llevan algunos programas comerciales para evitar su copia ilegal.

MTA: Agente para el transporte de correo electrónico (Mail Transport Agent) son programas que se encargan de distribuir los mensajes generados en el sistema. El más popular es el llamado sendmail, distribuido con sistemas UNIX.

Multipartito (o multiparticion): Un virus que es simultáneamente de Boot y de file. Suelen ser más complejos que los contrapartidos solo de file o solo de boot, y la interacción entre la parte de boot y la de file suele ser compleja, y dar mejores resultados en el funcionamiento del virus.

Navegador: Aplicado normalmente a programas usados para conectarse al servicio WWW.

NETIQUETTE: Conjunto de normas de comportamiento que rigen una conducto adecuada en Internet.

Network- Level Firewall: Un firewall en el que el tráfico se examina a nivel de protocolo.

Nodo: Por definición punto donde convergen mas de dos líneas. A veces se refiere a una única máquina en Internet. Normalmente se refiere a un punto de confluencia en una red.

NSA (National Security Agency): Agencia Nacional de Seguridad. Organismo americano para la seguridad, entre otras cosas, informática.

NumeroIP: identificación de la máquina dentro de la red Internet.

Packet Internet Groper (PING) (Búsqueda de Direcciones de Internet): Programa que se utiliza para comprobar si un destino está disponible.

PAP: Password Authentication Protocol. Protocolo de Autentificación por Password. Protocolo que permite al sistema verificar la identidad del otro punto de la conexión mediante password.

Parasitico: Un virus que conserva al programa infectado, para poder correrlo luego como si no lo estuviera.

Password: Clave que tiene cada usuario para entrar en un sistema determinado.

Patch o Parche: Modificación de un programa anterior, con la intención de solucionar un bug, o para crackearlo.

PBX o PABX: Centrales telefónicas privadas, generalmente de empresas, en España no hay muchas.

Pescar o Cazar: Conseguir un password o una clave, o un dato valioso a la hora de hackear. Ser localizado o detenido.

Phreaking: Uso del teléfono, o de las redes y servicios telefónicos, gratis o con un coste menor del normal. Debido al uso intensivo del teléfono por parte de los hackers, es bastante normal que usen el phreackin para ahorrarse unas pelas. Modificación o intervención de las líneas telefónicas, con otros fines distintos del llamar gratis.

Pinchado de Líneas de Datos o Spoofing: Similar al pinchado de líneas telefónicas, en este caso el objetivo son los sistemas de transmisión de datos (Cable telefónico usado por MODEM, cableado de una red local, fibra óptica, TV por cable) con el fin de monitorizar la información que pasa por ese punto y obtener información del sistema.

Pirata Informático: Persona dedicada a la copia y distribución de software ilegal, tanto software comercial crackeado, como shareware registrado, etc., Persona que elimina las protecciones software. Más conocido como cracker. Delincuente informático.

Polimorfismo: Una técnica de ocultamiento que apunta a que sea imposible descubrir al virus mediante scanning, variando de tal forma el código de infección a infección que es imposible extraer una string. Esto se hace encriptando el código del virus y "variabilizando" la rutina de encripcion tanto como sea posible.

POP (Protocolo de Oficina de Correos): Programa cliente que se comunica con el servidor, identifica la presencia de nuevos mensajes, solicita entre los mismos usuarios.

PPP Protocolo Punto a Punto (Point to Point Protocol): Implementación de TCP/IP por líneas seriales (como en el caso del módem). Es más reciente y complejo que SLIP.

PPP, TCP/IP, UDP: Distintos protocolos de comunicación, que usan las grandes redes como Internet.

Protocolo: Descripción formal de formatos de mensaje y de reglas que dos computadores deben seguir para intercambiar dichos mensajes.

Proxy: Una substitución de direcciones, usado para limitar la información de direcciones disponibles externamente.

Proxy Server: Un server que se sitúa entre la aplicación cliente, como por ejemplo un web browser, y un server real. Intercepta todos los requerimientos al server real para ver si las puede resolver él. Si no, envía el requerimiento al server real. Los Proxy servers tienen dos propósitos principales:

Mejorar la perfomance: Los proxy server mejoran la perfomance de un grupo de usuarios, ya que guardan los resultados de los requerimientos de los mismos una determinada cantidad de tiempo. Considérese el caso en que los usuarios A y B acceden a WWW a través de un proxy server. El usuario A accede una determinada página Web, que llama por ejemplo página 1. Algún tiempo después, el usuario B accede a la misma página. En vez de enviar el requerimiento al server en donde reside la página 1, lo cual puede ser una operación lenta, el proxy server retorna la página 1 que había buscado para el

usuario A, la cual fue convenientemente guardada en caché.

Como el proxy server está usualmente en la misma red que el usuario, esta operación es mucho más rápida.

Filtrar requerimientos y/o registrarlos: Los proxy servers pueden además evitar que se accedan a determinados web sites, y registrar en un log los lugares accedidos.

Permitir el acceso seguro de intranets a Internet: En este caso los usuarios de la intranet acceden a Internet a través del proxy, el cual tiene direcciones “reales” de Internet mientras que los usuarios de la intranet están en direcciones privadas, aislados y seguros de la Internet.

Puertas Falsas: Es una práctica acostumbrada en el desarrollo de aplicaciones complejas que los programadores introduzcan interrupciones en la lógica de los programas para chequear la ejecución, producir salidas de control, etc, con objeto de producir un atajo para ir corrigiendo los posibles errores. Lo que ocurre es que en la mayoría de los casos cuando el programa se entrega al usuario estas rutinas no se eliminan del programa y proveen al hacker de accesos o facilidades en su labor si sabe descubrirlas.

RARP: Reverse Address Resolution Protocol. Protocolo de Resolución de Dirección de Retorno. Protocolo de bajo nivel para la asignación de direcciones IP a máquinas simples desde un servidor en una red física.

Rastreadores con topología de red HUB: Capturar el tráfico de una red mediante la instalación de un rastreador (sniffer) genérico, Iris. Posteriormente se utilizarán rastreadores especializados en contraseñas y en espionaje de actividad (dsniff, webspy, urlsnarf). Finalmente, se comprobará la detección de los rastreadores funcionando en la red mediante el uso de técnicas de antisniff (AntiSniff).

Rastreadores con topología de red SWITCH: Secuestro de sesiones y captura de tráfico entre dos estaciones en una topología 28.

Regalo: Fichero interesante, pero camuflado con el nombre de otro. Por ejemplo, si en un sistema unix consigues el fichero de passwords y lo copias a uno de los directorios, pero se le cambia el nombre por otro. Ese segundo fichero es un 'regalo'.

Repeater (repetidor): Un repetidor simplemente reexpide bits de una red hacia otra, haciendo que las dos se vean lógicamente como una sola red. A menudo las redes se dividen en dos o más piezas, como consecuencias de las restricciones de máxima longitud de cable de cada pieza individual. Los repetidores son poco inteligentes (no hay software), sólo copian bits ciegamente.

Residente: Un virus que, cuando es corrido, se carga en memoria y a partir de ahí, queda en el background, hasta que es llamado a la superficie y allí infecta.

Root: Es el super-usuario de un sistema determinado, lo cual quiere decir que puede manipular el ordenador sin ningún tipo de restricción. Esto significa que puede ver/manipular/eliminar cualquier archivo de cualquier directorio

del sistema. El root es, por supuesto, el amo del sistema, pero cualquier usuario que tenga acceso a éste, puede, si sabe cómo, obtener este nivel. Es de hecho en lo que se basa el hacking.

Root: Directorio Raíz, el primer directorio.

Router (direccionador): Dispositivo que distribuye tráfico entre redes. La decisión sobre a dónde enviar se realiza en base a información de nivel de red y tablas de direccionamiento. El router se necesita cuando las dos redes utilizan la misma capa de transporte y tienen diferentes capas de red.

Ruidos en la Línea: Se dice que hay ruidos en la línea, cuando hay alguien oyendo o interceptando la información que pasa por ella. Se puede usar para indicar al otro de que hay alguien escuchando la conversación, para que el que está escuchando no se entere. (Por ejemplo, cuando su madre, espía las conversaciones con la novia) También se usa, cuando el teléfono está intervenido. (Por la policía o por otra persona).
-Un término parecido también se emplea en mensajería para indicar al receptor, que alguien a leído el correo privado. Se suele decir, que el mensaje tiene ruido, o que el mensaje está corrompido. Una manera más sutil de indicar esto es introducir una o dos líneas de caracteres extraños, en el mensaje, para indicar al otro que hay un extraño leyendo el correo privado.

Saco: Lugar donde se almacenan programas o textos interesantes. Puede ser un directorio del disco duro, una caja con disketes, etc. También se puede usar para definir el sitio donde se tiene guardado el material delicado. (Por si no lo sabe no es demasiado sano, tener el material de hacking a la vista de cualquiera).

Salto: El salto es el uso de un ordenador intermedio, para acceder a algo. Es como un puente entre el ordenador y aquel con el que se comunica. Sirve para ocultar la identidad.

SATAN (Security Analysis Tool for Auditing Networks): Herramienta de Análisis de Seguridad para la Auditoria de Redes. Conjunto de programas escritos por Dan Farmer junto con Wietse Venema para la detección de problemas relacionados con la seguridad.

SCRIPT: Sería el equivalente en unix, de los bat's del MS-dos, aunque mucho más potentes y con más opciones, siendo casi un pequeño lenguaje de programación.

Sector: Uno de los "pedazos" en que los discos están divididos. Para el BIOS los sectores son "físicos" y los referencia mediante tres coordenadas;

Lado, pista, sector (lado 0, pista 0, sector 1, por ejemplo.). El DOS utiliza sectores lógicos, que son referenciados mediante un número. (Sector 0)
Y existe la correspondencia (lado 0, pista 0, sector 1 == Sector 0).

Seta: Cabina telefónica.

SFT (System File Table): Una tabla con información referente a un file abierto. Se utiliza para todo tipo de propósitos en los virus, ya que la información que contiene es muy variada y muy valiosa.

Simulación de Identidad:
Básicamente en usar un terminal de un sistema en nombre de otro usuario bien porque se conoce la clave, porque abandonó el terminal pero no lo desconectó y ocupa el lugar. El término también es aplicable al uso de Tarjetas de Crédito o documentos falsos a nombre de otra persona.

Simulación Por Ordenador: Se define asi el uso de la computadora para simular previamente una situación y de esta forma determinar las acciones a probar. En el contexto del hacking se refiere a la simulación en la computadora propia del sistema a atacar con el fin de elaborar estrategias de acción.

Sistema Operativo (S.O.): Existen dos términos muy utilizados en informática. Estos son los conceptos de hardware y software. El primero de ellos se refiere a todo lo que es físico y tangible en el ordenador, como unidades de disco, tarjetas gráficas, microprocesador, memoria,...etc. Por otro lado está el software que se define como el conjunto de programas (o información) con la que se puede trabajar el hardware (ficheros, directorios, programas ejecutables, bases de datos, controladores,...etc.). Pues bien, el sistema operativo pertenece al software y más concretamente es el conjunto de programas (y ficheros o archivos de otro tipo) que permite que se pueda utilizar el hardware.

Sistema Virgen: Sistema que ningún hacker ha descubierto o ha intentado hackear. Sistema que todavía no ha sido hackeado por nadie.

Sniffer: Básicamente es un programa que monitoriza los datos que se envían por la red, cuando un usuario entra en un sistema, tiene que dar login y passwd. Estos datos viajan para ser comprobados con el fichero passwd y ahí es donde el sniffer actúa: intercepta los datos de login y password y los guarda en un fichero de texto que más tarde puede ser examinado por el hacker para conseguir información útil.

Spam o (Correo basura): Cualquier tipo de e-mail no solicitado. Hacer spam es enviar e-mail a usuarios que NO han proporcionado previamente la dirección de correo electrónico.

SSL (Secure Socket Layer): Sistema que permite que la información viaje encriptada evitándose que puede ser leída por sniffers u otros recursos. Es el método que permite garantizar una alta seguridad en el comercio electrónico. Gracias a él, el comerciante ni tan siquiera conoce el número de tarjeta de crédito del comprador online.

String: Cadena que se utiliza para reconocer un file infectado. Es una PARTE del virus, NO todo el virus. Generalmente se hacen strings de las rutinas de infección. Al hacer virus polimorficos, se trata justamente de que no exista una cadena común entre infección e infección.

SUNOS, AIX, HP/UX, IRIX, VMS, UNIX: Varios sistemas operativos que usan los grandes ordenadores.

Superzapping: Se denomina superzapping al uso no autorizado de un programa editor de ficheros para alterar, borrar, copiar, insertar o utilizar en cualquier forma no permitida los datos almacenados en los soportes de un ordenador. El nombre proviene de una utilidad llamada.

SUPERZAP: Diseñada para Mainframes y que permite acceder a cualquier parte del ordenador y modificarlo, el equivalente en un PC serian las Pctools o el Norton Disk Editor.

TCP (Transmission Control Protocol): Uno de los protocolos más usados en Internet. Es un protocolo de capa de transporte.

TCP/IP (Transmission Control Protocol/Internet Protocol): Arquitectura de red desarrollada por la "Defense Advanced Research Projects Agency" en USA, es el conjunto de protocolos básicos de Internet o de una Intranet. La red Internet funciona bajo el protocolo de comunicación tcp-ip, este protocolo se basa en envíos de paquetes de datos, desde el servidor hasta el cliente. Debido a esta estructura, con cualquier ordenador a la que se conecte se intercambian paquetes, y para que esos paquetes puedan llegar al destino, ambos deben conocer la ip, del otro, con lo cual es muy difícil quedar en anonimato, a menos que se usen tipos de ip-spoofing.

Teléfono Limpio: Teléfono que no tiene ninguna relación con el usuario y en el que se está seguro que no localizarán. Tiene que ser una línea telefónica que no tenga nada que ver, no tiene que dar ninguna pista sobre la identidad. (Por ejemplo una cabina de teléfonos, alejada de donde se vive).

Telnet: Telnet es el protocolo estándar de Internet para realizar un servicio de conexión desde un terminal remoto. Está definido en STD 8, RFC 854 y tiene opciones adicionales descritas en muchos otros RFCs.

Telnet: Corresponde al puerto 23 de un sistema determinado. Entrar en él y, dependendiendo del tipo de cuenta que tenga en el sistema puede manipular ese ordenador como si fuera propia, teclea las órdenes como las teclearía en Linux.

Texto plano: Se llama así al documento antes de ser encriptado. (Plain Text).

Timofónica: Telefónica S.A.

Tipo de Llamada: Si la llamada es interprovincia o internacional, la llamada pasará por una o varias centralitas intermedias más, y si la centralita coincide con la del llamado no es necesario pasar por otra. (Esto se nota mucho, porque la llamada es muy rápida y porque el volumen se oye más alto que el normal).

Tirar, Echar Abajo o Hacer Caer: Colapsar un sistema, colgarlo, bloquearlo, generalmente con intenciones malignas.

Token: Dispositivo de autentificación que genera contraseñas de una-vez. Los usuarios que los utilizan son llamados "usuarios autenticados".

Toolkit: Una librería para incluir en un virus, y conferirle a este la potencia de alguna técnica avanzada como polimorfismo o tunneling.

Trashing (Recogida de basura): Rebuscar en la basura, para encontrar algo que pueda ser útil a la hora de hackear.

Trojan Horse (Caballo de troya): programa informático que lleva en el interior la lógica necesaria para que el

creador del programa pueda acceder al interior del sistema que lo procesa.

Troyano: Los troyanos no se pueden considerar virus ya que no se replican o no hacen copias de sí mismos. En realidad son programas que llegan a un ordenador de forma totalmente normal y no producen efectos realmente visibles o apreciables (por lo menos en ese momento). Pueden llegar acompañados de otros programas y se instalan en el ordenador. Al activarse puede dejar huecos en el sistema, a través de los cuales se producen intrusiones.

Tunneling: Una técnica de protección, de tipo anti-anti-virus, que consiste básicamente en pasar "por debajo" de
un paquete perdido no afecta la calidad del sonido.

Uebercracker: Élite (cr/h)acker que es prácticamente imposible mantener fuera de los networks.

UNIX: sistema operativo utilizado por la gran mayoría de máquinas de Internet. El gran éxito se debe a que es abierto, por lo cual existen muchas versiones, y cualquiera puede escribir programas para UNIX.

Virus: Un código ejecutable capaz de reproducirse a sí mismo a través de sistemas y computadoras. Se le clasifica primariamente por el tipo de reproducción (Boot Sector, File, Cluster), y luego por la utilización de técnicas de ocultamiento y protección (Stealth, Polimorfico, etc).

cVirus de boot: Un tipo de virus. Se reproduce poniéndose en el boot sector de los discos, y luego de haberse instalado en memoria, corre el boot sector original.
Los antivirus residentes, que monitorean la actividad "rara". Se obtiene el address original de la int que se piensa puede estar monitoreada, y se usa este address para accederla.

UDP (Protocolo de Datagramas de usuario): Protocolo que no pide confirmación de la validez de los paquetes enviados por la computadora emisora.

Este protocolo es actualmente usado para la transmisión de sonido y vídeo a través de Internet. El UDP está diseñado para satisfacer necesidades concretas de ancho de banda, como
no reenvía los datos perdidos, es ideal para el tráfico de voz digitalizada, pues instalado en memoria, corre el boot sector original.

Virus de cluster: Un tipo de virus relativamente nuevo y oscuro. Para infectar no modifica el file, sino sencillamente la entrada de directorio del archivo. Sólo existe UN virus de este tipo, el celebre Dir-2.

Virus de file: Este tipo de virus se reproduce infectando los files del disco. Se dividen en infectores de COM, de SYS, y de EXE. (y últimamente de EXE de Windows).

Referencias Bibliográficas

Referencias bibliográficas

[1] Dea, Michael, "*Claves Hackers en Windows*", Edit. Mc Graw-Hill Interamericana de España, S.A.

[2] Dora Alba, "*Seguridad en Internet*", Edit. Pearson Educación.

[3] Gutiérrez Gallardo, Juan Diego y López guisado ángel, "*seguridad digital y hackers*", Edit. Anaya multimedia-anaya interactiva.

[4] Harris, Shon; Harper, Allen; Tagle, Chris, "*Hacking Etico*", Edit. Anaya Multimedia, pág. 544.

[5] Himanen Pekka, "Ética del Hacker", Edit. Ediciones destino, S.A.

[6] Horton, Mike, "*Claves Hackers*", Edit. Mc Graw- Hill Interamericana de España, S.A.

[7] Huidobro Moya, José Manuel y Roldan Martínez, "*Seguridad en redes y sistemas informáticos*", Edit. Thomson Paraninfo, S.A.

[8] Jesús de Marcelo rodao, "*Seguridad informática*", Edit. Anaya interactiva.

[9] Jones Joel, "*Hackers*", Edit. Anaya multimedia-anaya interactive.

[10] Jones, Keith, "*Super utilidades Hackers*", Edit. Mc Graw-Hill interamericana de España, S.A.

[11] Kurtz George y Mcclure Stuart, "*Hackers: secretos y soluciones para la seguridad de redes*", Edit. Mc Graw-Hill interamericana España, S.A.

[12] Long, Johny, "*Hacking con Google*", Edit. Anaya Multimedia-Anaya-Interactiva, pág. 600.

[13] Mansfield Richard, "*Defensa contra Hackers: Protección de información privada*", Edit. Anaya Multimedia-anaya interactiva.

[14] Mansfield Richard, "*Sistemas de Seguridad*", Edit. Anaya Multimedia-anaya Interactiva.

[15] Mcnab, Chris, "*Seguridad de Redes*", Edit. Anaya Multimedia-anaya interactiva

[16] Miguel Pérez, Carlos y Ramón Varón, "*Protege tu PC*", Edit. Anaya Multimedia-anaya interactiva

[17] Morant Ramón, José Luís y Ribaforda Garnacho, "*Seguridad y protección de información*", Edit. Thomson Paraninfo, S. A.

[18] Morant Ramón, “Seguridad en Internet”, Edit. Thomson Paraninfo, S.A.

[19] Muñoz Guerrero Julio, “*Sistemas de Seguridad*”, Edit. Thomson Paraninfo, S.A.

[20] Muñoz Ramón, “*Seguridad*”, Edit. Thomson Paraninfo, S.A.

[21] Red invulnerable a los hackers, “*Blindaje de Redes*”, Edit. Anaya Multimedia, pág.- 420.

[22] Sambray Joel y Mcclure, “*Hackers en Windows 2000*”, Edit. Mc Graw-Hill Interamericana de España, S.A.

[23] Scambray, Joel, “*Hacker de sitios Web*”, Edit. MC Graw Hill interamericana de España, S.A.

[24] Schiffman, Mike, “*Hackers*”, Edit. Mc Graw-Hill interamericana de España, S. A.

[25] Shinder, Debra Little John, “Prevención y detección de delitos informáticos”, Anaya Multimedia- Anaya Interactiva.

[26] Strassberg Keith E., “*Firewall*”, Edit. Mc Graw- Hill Interamericana de España, S.A.

[27] Tapiador Mateos Marino y Sigüenza Pizarro, “*Tecnologías Biométricas aplicadas a la seguridad*”.

[28] Zemanek, Jakub, “*Cracking sin secretos, ataque y defensa de software*”, Edit, Anaya interactiva.