UNIVERSIDAD AUTONOMA DEL ESTADO DE HIDALGO

INSTITUTO DE CIENCIAS BÁSICAS E INGENIERÍA

“SEGURIDAD EN REDES”

M O N O G R A F Í A

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

PRESENTA:

RUBÉN BUSTAMANTE SÁNCHEZ

ASESOR:

ISC. SANDRA LUZ HERNÁNDEZ MENDOZA

AGRADECIMIENTOS.

A MI FAMILIA:

Por brindarme su apoyo, confianza y sabiduría, compartiendo tanto alegrías como tristezas, pero que siempre han estado, están y estarán Conmigo... por siempre.
Son los únicos que realmente me conocen.
Los quiero de corazón.

A MI PADRE:

Que he aprendido mucho de él, Hemos hecho cosas juntos y creé en mí. Me ha ayudado en todo este transcurso de mi vida y todo lo bueno que venga, será por ti.

A MI MADRE:

Que siempre se ha preocupado por mi, me ha dado mucho cariño y amor, me ha inculcado valores que no he olvidado. Y deja de hacer sus cosas por mí.

A MIS HERMANOS:

Han sido parte fundamental en mi vida, he crecido con ustedes y parte de mi carácter y forma de ser, es igual que ustedes. Gracias por enseñarme ver más allá de lo superficial.

INDICE

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

En la vida siempre ha existido la evolución, donde ella ha servido y debe servir para mejorar el nivel de vida de la humanidad, tanto espiritual, tecnológica, en las comunicaciones, etc. Donde el hombre, por naturaleza necesita interactuar con las demás personas, esto para intercambiar ideas, pensamientos o documentos que sean de utilidad a un individuo, a un grupo o una organización. Todo esto se resume a lo que es la información, y esta puede ser pública o privada.

Cuando la información es privada siempre existe la preocupación de que alguien pueda robársela, utilizándola para fines lucrativos para sí mismo o para perjudicar a sus semejantes, es por eso que se debe buscar la seguridad en el traslado de la información. Esta seguridad no es mas que tomar medidas preventivas, para evitar en su mayor totalidad de la intromisión de terceros no autorizados a la documentación.

Este trabajo se enfoca en la seguridad en redes de computadoras, donde las organizaciones pueden confiar que su información valiosa, puede estar protegida ante distintas amenazas.

La seguridad en redes se da en dos tipos: física y lógica. En la primera, se debe estar atento y tomar medidas preventivas como son los desastres naturales, inundaciones, terremotos, incendios, así, como también de las instalaciones eléctricas, etc. En la segunda se debe tener cuidado con aquellas personas que no están autorizadas para el acceso de la información, y es aquí donde entran los piratas informáticos, un ejemplo de ellos son los hackers, crackers, etc. Que buscan algo que les interesa y después puedan poseerlo, o también para probarse a sí mismos hasta donde pueden llegar, aprovechándose de las vulnerabilidades de la víctima, como por ejemplo de los sistemas operativos o de la ingenuidad de los trabajadores al recibir archivos desconocidos y abrirlos, infectando el sistema por medio de virus u otra especie de herramientas.

Es por eso que se deben tener medidas preventivas para combatir estos ilícitos, ya sea con políticas de seguridad de la organización, de herramientas de seguridad para los sistemas operativos y también, dar capacitación al personal, que es fundamental para tener una buena seguridad.

Es cierto que la seguridad no se da en toda su totalidad, pero, si se puede tener en su mayoría, ya que para una persona muy capaz, siempre habrá otra que este por arriba de ella. Haciendo que esto sea un ciclo de nunca acabar, porque no existe una conciencia social, algunos para atacar y otros que hacen un monopolio para aprovecharse de los demás con sus productos.

Lo mejor sería trabajar en conjunto, pero en vista de que no es posible, y siempre hay intereses de por medio, entonces, las víctimas, tienen que recurrir a los recursos que se ofrecen en el mercado para protegerse. Y he ahí la información que se transmitirá en esta investigación.

JUSTIFICACIÓN.

Como la inseguridad se da en muchas maneras en nuestro entorno social, en las redes no es la excepción. Las organizaciones, empresas, universidades, etc. buscan tener la mayor seguridad en sus esquemas, para no tener perdidas en su economía, de su privacidad y de su confidencialidad.

Para no tener que preocuparse demás, esto se puede hacer simplemente si se tiene una buena planeación, organización y prevención de lo que realmente se requiere para la infraestructura que queremos proteger.

En vista que la información, es el factor primordial por el cual muchos usuarios malintencionados hacen actos ilícitos, de los cuales utilizan diferentes métodos que muchos de nosotros ni siquiera nos habíamos imaginado, con tal de conseguir la valiosa información, aunque por otro lado también hay quienes no están de acuerdo con la monopolización que hacen algunas empresas, entonces lo que buscan es hacer notar de dichas fallas que pueden tener sus productos, dando las posibilidad de conocer otros mercados que puedan contener mejor seguridad, y mejores precios, pero como siempre, los más afectados son aquellos que no tienen nada que ver con todo lo que pase, y es por ello que las “víctimas” tienen que recurrir y confiar en los diferentes productos.

Y para que se puedan tomar medidas preventivas es importante que nos preguntemos ¿contra qué nos defendemos?, ¿Por qué nos defendemos?, y ¿con que nos podemos defender?

OBJETIVO GENERAL

Describir y analizar los factores que intervienen en la seguridad en redes, a partir de los usuarios que buscan la mayor protección y confidencialidad de información en su red, utilizando herramientas y políticas de seguridad, para alcanzar ese fin. Pero para poder lograrlo se debe conocer contra quien debe protegerse y como son los medios en los que operan los atacantes, ya que con el paso de los años, las herramientas tanto de seguridad, como las herramientas para hackear, se van haciendo más potentes, destructivas y con una alta calidad. Y es importante saber en donde está esa evolución en nuestra actualidad, para el cuidado de las redes.

OBJETIVOS ESPECÍFICOS

- Orientar sobre las aplicaciones de barrera físicas y procedimientos de control como medidas de prevención.

- Identificar las vulnerabilidades que existen en las redes, tanto del equipo como los firewalls, como de los sistemas operativos.

- Utilizar políticas de seguridad, como protección y conocer los modelos que existen para su elaboración.

- Describir los piratas informáticos y la forma en que operan para restringir lo más posible su acceso.

- Analizar algunas herramientas de seguridad a las que se puede recurrir.

CAPITULO

1

INTRODUCCIÓN A LA SEGURIDAD EN REDES.

RESUMEN.

En este capítulo hablaremos de la seguridad en las redes, los diferentes tipos de seguridad, medidas de prevención contra desastres naturales que pueden en algún momento perjudicar a las instalaciones, mencionaremos como hay que controlar el acceso y las limitaciones de los usuarios a los datos, ya sea de forma interna o externa, así como también, analizaremos los diferentes niveles de seguridad de la información.

Por último se detallarán las vulnerabilidades que se presentan en los sistemas operativos, como en un esquema de seguridad en redes.

1.1 CONCEPTO DE SEGURIDAD EN LAS REDES

La definición y el objetivo de la seguridad en redes es mantener la integridad, disponibilidad, privacidad (sus aspectos fundamentales) control y autenticidad de la información manejada por computadora, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo adecuado.[1]

En la Fig. 1.1 muestra de manera global las amenazas que existen en la seguridad en redes.

Fig. 1.1 Amenazas en la seguiridad.

1.2 TIPOS DE SEGURIDAD

Podemos clasificar a la seguridad en redes en 2 tipos, y de ellos se subdividen en la siguiente tabla donde más adelante se definirán.

1. SEGURIDAD FÍSICA.	2.SEGURIDAD LÓGICA
Desastres	Controles de acceso
Incendios	Identificación
Equipamiento	Roles
Inundaciones	Transacciones
Picos y ruidos electromagnéticos	Limitación a los servicios
Cableado	Control de acceso interno

TABLA1. TIPOS DE SEGURIDAD

1.2.1 SEGURIDAD FÍSICA.

La seguridad física es la “aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial”.[2]

La seguridad física se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de computo así como los medios de acceso remoto del mismo; implementados para proteger el hardware y medios de almacenamiento de datos. Es muy importante, que por más que nuestra organización sea la más segura desde el punto de vista de ataques externos, hackers, virus, etc; la seguridad de la misma será nula si no se ha previsto como combatir un incendio.
La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos tratados a continuación se prevén, otros, como la detección de un atacante interno a la empresa que intenta acceder físicamente a una sala de operaciones de la misma. Esto puede derivar en que para un atacante sea mas fácil lograr tomar y copiar una cinta de la sala, que intentar acceder vía lógica a la misma.[2]

1.2.1.1 TIPOS DE DESASTRES

Está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro.
Las principales amenazas que se prevén en la seguridad física son:
1.- Desastres naturales, incendios accidentales tormentas e inundaciones.
2.- Amenazas ocasionadas por el hombre.
3.- Disturbios, sabotajes internos y externos deliberados.

A continuación se analizan los peligros más importantes que ocurren en un centro de procesamiento; con el objetivo de mantener una serie de acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos. [2]

1.2.1.2 INCENDIOS

Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.

Los diversos factores a contemplar para reducir los riesgos de incendio a los que se encuentra sometido un centro de cómputo son:

1. El área en la que se encuentran las computadoras debe estar en un local que no sea combustible o inflamable.
2. El local no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.
3. Las paredes deben hacerse de materiales incombustibles y extenderse desde el suelo al techo.
4. Debe construirse un “falso piso” instalado sobre el piso real, con materiales incombustibles y resistentes al fuego.
5. No debe estar permitido fumar en el área de proceso.[2]

1.2.1.3 SEGURIDAD DEL EQUIPAMIENTO.

Es necesario proteger los equipos de computo instalándolos en áreas en las cuales el acceso a los mismo solo sea para el personal autorizado. Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados.

Para protegerlos se debe tener en cuenta que:

- La temperatura no debe sobrepasar los 18° C y el límite de humedad no debe superar el 65% para evitar el deterioro.

- La red debe estar provisto de equipo de para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.
- Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores).[2]

1.2.1.4 INUNDACIONES

Se define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial. Esta es una de las causas de mayores desastres en las redes.

Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior.

Para evitar este inconveniente se pueden tomar las siguientes medidas: construir un techo impermeable para evitar el paso de agua desde un nivel superior y acondicionar las puertas para contener el agua que bajase por las escaleras.[2]

1.2.1.5 INSTALACIÓN ELÉCTRICA

Trabajar con computadoras implica trabajar con electricidad. Por lo tanto esta es una de las principales áreas a considerar en la seguridad física, ya que es una problemática que abarca desde el usuario hogareño hasta la gran empresa.
En la medida que los sistemas se vuelven más complicados, se hace más necesaria la presencia de un especialista para evaluar riesgos particulares y aplicar soluciones que estén de acuerdo con una norma de seguridad industrial.[2]

1.2.1.5.1 CABLEADO

Los cables que se utilizan para construir las redes locales, van desde el cable telefónico normal al cable coaxial o la fibra óptica. Algunos edificios de oficinas ya se construyen con los cables instalados para evitar el tiempo y el gasto posterior, y de forma que se minimice el riesgo de un corte, rozadura u otro daño accidental.

Los riesgos más comunes para el cableado se pueden resumir a continuación:

1. **Interferencia**: estas modificaciones pueden estar generadas por cables de alimentación de maquinaria pesada o por equipos de radio o microondas. Los cables de fibra óptica no sufren el problema de alteración (de los datos que viajan a través de él) por acción de campos eléctricos, que si sufren los cables metálicos.
2. **Corte del cable**: la conexión establecida se rompe, lo que impide que el flujo de datos circule por el cable.
3. **Daños en el cable**: los daños normales con el uso pueden dañar el apantallamiento que preserva la integridad de los datos transmitidos o dañar al propio cable, lo que hace que las comunicaciones dejen de ser fiables.

En la mayor parte de las organizaciones, estos problemas entran dentro de la categoría de daños naturales. Sin embargo, también se pueden ver como un medio para atacar la red si el objetivo es únicamente interferir en su funcionamiento.

El cable de red ofrece también un nuevo frente de ataque para un determinado intruso que intentase acceder a los datos. Esto se puede hacer:

1. Desviando o estableciendo una conexión no autorizada en la red: un sistema de administración y procedimiento de identificación de acceso adecuados hará difícil que se puedan obtener privilegios de usuarios en la red, pero los datos que fluyen a través del cable pueden estar en peligro.

2. Haciendo una escucha sin establecer conexión, los datos se pueden seguir y pueden verse comprometidos.

Luego, no hace falta penetrar en los cables físicamente para obtener los datos que transportan.[2]

1.2.2 SEGURIDAD LÓGICA

Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para hacerlo.

Después de ver como nuestra red puede verse afectado por la falta de seguridad física, es importante recalcar que la mayoría de los daños que puede sufrir un sitio de computo, no será sobre los medios físicos, sino, contra información por él almacenada y procesada.

Así, la seguridad física, solo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la seguridad lógica.[3]

Los objetivos que se plantean para la seguridad lógica son:

1. Restringir el acceso a los programas y archivos.
2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
3. Asegurar que se estén utilizando los archivos y programas correctos en y por el procedimiento correcto.
4. Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
5. Que la información recibida sea la misma que ha sido transmitida.

6. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
7. Que se disponga de pasos alternativos de emergencia para la transmisión de información.

1.2.2.1 CONTROLES DE ACCESO.

Estos pueden implementarse en el sistema operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados. Así mismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso.

Al respecto, el National Institute for Standars and Technology (NIST)[1] ha resumido los siguientes estándares de seguridad que se refieren a los requisitos mínimos de seguridad en cualquier sistema:

1.2.2.1.1 IDENTIFICACIÓN Y AUTENTICACIÓN.

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

[1] NIST: Instituto Naional para Estandares y Tecnologias.

Se denomina **identificación** al momento en que el usuario se da a conocer en el sistema; y **autenticación** a la verificación que realiza el sistema sobre esta identificación.

Al igual que se consideró para la seguridad física, y basada en ella, existen 4 tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

1. Algo que solamente el individuo conoce: por ejemplo una clave secreta de acceso password, una clave criptográfica, un numero de identificación personal o PIN, etc.
2. Algo que la persona posee: por ejemplo una tarjeta magnética.
3. Algo que el individuo es y que lo identifica unívocamente: por ejemplo las huellas digitales o la voz.
4. Algo que el individuo es capaz de hacer: por ejemplo los patrones de escritura.

Para cada una de estas técnicas vale lo mencionado en el caso de la seguridad física en cuanto a sus ventajas y desventajas. Se destaca que en los dos primeros casos enunciados, es frecuente que las claves sean olvidadas o que las tarjetas o dispositivos se pierdan, mientras que por el otro lado, los controles de autenticación biométricos serian los mas apropiados y fáciles de administrar, resultando ser también, los mas costosos por lo dificultosos de su implementación eficiente.

Desde el puntos de vista de la eficiencia, es conveniente que los usuarios sean identificados y autenticados solamente una vez, pudiendo acceder a partir de ahí, a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota. Esto se denomina “single log-in” o sincronización de passwords.

Una de las posibles técnicas para implementar esta única identificación de usuarios sería la utilización de un servidor de autenticaciones sobre el cual los usuarios se identifican, y que se encarga luego de autenticar al usuario sobre los restantes equipos a los que éste pueda acceder. Este servidor de autenticaciones no debe ser necesariamente un equipo independiente y puede tener sus funciones distribuidas tanto geográfica como lógicamente, de acuerdo con los requerimientos de carga de tareas. [4]

La seguridad informática se basa, en gran medida, en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos. Esta administración abarca:

1. Proceso de solicitud, establecimiento, manejo, seguimiento y cierre de las cuentas de usuarios. Es necesario considerar que la solicitud de habilitación de un permiso de acceso para un usuario determinado, debe provenir de su superior y de acuerdo con sus requerimientos específicos de acceso, debe generarse el perfil en el sistema de seguridad, en el sistema operativo o en la aplicación según corresponda.
2. Además, la identificación de los usuarios debe definirse de acuerdo con una norma homogénea para toda la organización.
3. Revisiones periódicas sobre la administración de las cuentas y los permisos de acceso establecidos. Las mismas deben encararse desde el punto de vista del sistema operativo, y aplicación por aplicación, pudiendo ser llevadas a cabo por el personal de auditoría o por la gerencia propietaria del sistema; siempre sobre la base de que cada usuario disponga de mínimo permiso requiera de acuerdo con sus funciones.
4. Las revisiones deben orientarse a verificar la adecuación de los permisos de acceso de cada individuo de acuerdo con sus necesidades operativas, la actividad de las cuentas de usuarios o la autorización de cada habilitación de acceso. Para esto, deben analizarse las cuentas en busca de periodos de inactividad o cualquier otro aspecto anormal que permita una redefinición de la necesidad de acceso.

5. Detección de las actividades no autorizadas. Además de realizar auditorias o efectuar el seguimiento de los registro de transacciones (pistas), existen otras medidas que ayudan a detectar la ocurrencia de actividades no autorizadas. Algunas de ellas se basan en evitar la dependencia hacia personas determinadas, estableciendo la obligatoriedad de tomar vacaciones o efectuando rotaciones periódicas a las funciones asignadas a cada una.
6. Nuevas consideraciones relacionadas con cambios en la asignación de funciones del empleado. Para implementar la rotación de funciones, o en caso de reasignar funciones por ausencias temporales de algunos empleados, es necesario considerar la importancia de mantener actualizados los permisos de acceso.
7. Procedimientos a tener en cuenta en caso de desvinculaciones de personal con la organización, llevadas a cabo en forma amistosa o no. Los despidos del personal de sistemas presentan altos riesgos ya que en general se trata de empleados con capacidad para modificar aplicaciones o la configuración del sistema, dejando “bombas lógicas” o destruyendo sistemas o recursos informáticos. No obstante, el personal de otras áreas usuarias de los sistemas, también puede causar daños, por ejemplo, introduciendo información errónea a las aplicaciones intencionalmente.

Para evitar estas situaciones, es recomendable anular los permisos de acceso a las personas que se desvincularán de la organización, lo antes posible. En caso de despido, el permiso de acceso debería anularse previamente a la notificación de la persona sobre la situación.[4]

1.2.2.1.2 ROLES

El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso. Algunos ejemplos de roles serían los siguientes: programador, líder de proyecto, gerente de un área usuaria, administrador del sistema, etc. En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usurarios.[4]

1.2.2.1.3 TRANSACCIONES.

También pueden implementarse controles a través de las transacciones, por ejemplo solicitando una clave al requerir el procesamiento de una transacción determinada.[4]

1.2.2.1.4 LIMITACIÓN A LOS SERVICIOS.

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema. Un ejemplo podría ser que en la organización se disponga de licencias para la utilización simultanea de un determinado producto de software para cinco personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario.

1.2.2.1.5 MODALIDAD DE ACCESO

Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información. Esta modalidad puede ser:

- **Lectura:** el usuario puede únicamente leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.
- **Escritura**.: este tipo de acceso permite agregar datos, modificar o borrar información.
- **Ejecución**: este acceso otorga al usuario el privilegio de ejecutar programas.
- **Borrado**: permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación.

Además existen otras modalidades de acceso especiales, que generalmente se incluyen en los sistemas de aplicación:

- **Creación**: permite al usuario crear nuevos archivos, registros o campos.
- **Búsqueda**: permite listar los archivos de un directorio determinado.

1.2.2.2 CONTROL DE ACCESO INTERNO.

1.2.2.2.1 PALABRAS CLAVE. (PASSWORDS)

Generalmente se utilizan para realizar la autenticación del usuario y sirven para proteger los datos y aplicaciones. Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo, sin embargo, cuando el usuario se ve en la necesidad de utilizar varias palabras clave para acceder a diversos sistemas, encuentra dificultoso recordarlas y probablemente las escriba o elija palabras fácilmente deducibles, con lo que se ve disminuida la utilidad de está técnica.

Se podrá, por años, seguir creando sistemas altamente seguros, pero en última instancia cada uno de ellos se romperá por este eslabón: la elección de passwords débiles.[4]

- **Sincronización de passwords:** consiste en permitir que un usuario acceda con el mismo password a diferentes sistemas interrelacionados y a su actualización automática en todos ellos en caso de ser modificada. Podría pensarse que esta es una característica negativa para la seguridad de un sistema, ya que una vez descubierta la clave de un usuario, se podría tener acceso a los múltiples sistemas a los que tiene acceso dicho usuario. Sin embargo, estudios hechos muestran que las personas normalmente suelen manejar un solo password para todos los sitios a los que tengan acceso, y que si se le hace elegir diferentes passwords tienden a guardarlas escritas para no olvidarlas, lo cual significa un riesgo aún mayor. Para implementar la sincronización de passwords entre sistemas es necesario que todos ellos tengan un alto nivel de seguridad.

- **Caducidad y control:** este mecanismo controla cuando pueden y/o deben cambiar sus passwords los usuarios. Se define el periodo mínimo que debe pasar, para que los usuarios puedan cambiar sus passwords y un periodo máximo que puede transcurrir para que éstos caduquen.

1.2.2.2.2 ENCRIPTACIÓN.

La información encriptada solamente puede ser desencriptada por quienes posean la clave apropiada. La encriptación puede proveer de una potente medida de control de acceso.[4]

1.2.2.2.3 LISTAS DE CONTROL DE ACCESOS

Se refiere a un registro donde se encuentran los nombres de los usuarios que obtuvieron el permiso de acceso a un determinado recurso del sistema, así como la modalidad de acceso permitido. Este tipo de listas varían considerablemente en su capacidad y flexibilidad.[4]

1.2.2.2.4 LIMITES SOBRE LA INTERFASE DE USUARIO.

Estos límites, generalmente, son utilizados en conjunto con las listas de control de accesos y restringen a los usuarios a funciones específicas. Básicamente pueden ser de tres tipos: menús, vistas sobre la base de datos y límites físicos sobre la interfase de usuario. Por ejemplo, los cajeros automáticos donde el usuario solo puede ejecutar ciertas funciones presionando teclas específicas.[4]

1.2.2.2.5 ETIQUETAS DE SEGURIDAD.

Consiste en designaciones otorgadas a los recursos (como por ejemplo un archivo) que pueden utilizarse para varios propósitos como control de accesos, especificación de medidas de protección, etc., estas etiquetas no son modificables.[4]

1.2.2.3 CONTROL DE ACCESO EXTERNO.

1.2.2.3.1 DISPOSITIVOS DE CONTROL DE PUERTOS.

Estos dispositivos autorizan el acceso a un puerto determinado y pueden estar fácilmente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un MODEM.[4]

1.2.2.3.2 FIREWALL O PUERTAS DE SEGURIDAD.

Permiten bloquear o filtrar el acceso entre dos redes, usualmente una privada y otra externa (por ejemplo internet). Los firewalls permiten que los usuarios internos se conecten a la red exterior al mismo tiempo que previenen la intromisión de atacantes o virus a los sistemas de la organización. Este tema será abordado posteriormente.[4]

1.2.2.3.3 ACCESO DE PERSONAL CONTRATADO O CONSULTORES.

Debido a que este tipo de personal en general presta servicios temporarios, debe ponerse especial consideración en la política y administración de sus perfiles de acceso.[4]

1.3 NIVELES DE SEGURIDAD INFORMÁTICA.

El estándar de niveles de seguridad más utilizado internacionalmente es el TCSEC Orange Book[2], desarrollo en 1983 de acuerdo a las normas de seguridad en computadoras del departamento de los Estados Unidos.

[2] TCSEC Orange Book: Criterios de evaluación de la seguridad de los sistemas de computación.

Los niveles describen diferentes tipos de seguridad del sistema operativo y se enumeran desde el mínimo grado de seguridad al máximo.

Estos niveles han sido la base de desarrollo de estándares europeos (ITSEC/ITSEM)[3] y luego internacionales (ISO/IEC)[4].

Cabe aclarar que cada nivel requiere todos los niveles definidos anteriormente: así el subnivel B2 abarca los subniveles B1, C2, C1, y el D.[5]

1.3.1 NIVEL D

Este nivel contiene solo una división y está reservada para sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad. Sin sistemas no confiables, no hay protección para el hardware, el sistema operativo es inestable y no hay autenticación con respecto a los usuarios y sus derechos en el acceso a la información. Los sistemas operativos que responden a este nivel son MS-DOS y System 7.0 de macintosh.[5]

1.3.2 NIVEL C1: PROTECCIÓN DISCRECIONAL.

Se requiere identificación de usuarios que permite el acceso a distinta información. Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene control total de acceso.

Muchas de las tareas cotidianas de administración del sistema sólo pueden ser realizadas por este “super usuario”; quien tiene gran responsabilidad en la seguridad del mismo. Con la actual descentralización de los sistemas de cómputos, no es raro que en una organización encontremos dos o tres personas cumpliendo este rol. Esto es un problema, pues no hay forma distinguir entre los cambios que hizo cada usuario.[5]

[3] ITSEC: Criterios de Evaluación de la Seguridad en las Tecnologías de la Información.
[4] IEC: Comisión Electrotécnica Internacional.

A continuación se enumeran los requerimientos mínimos que debe cumplir la clase C1:

- **Acceso de control discrecional**: distinción entre usuarios y recursos. Se podran definir grupos de usuarios (con los mismos privilegios) y grupos de objetos (archivos, directorios, disco) sobre los cuales podrán actuar usuarios o grupos de ellos.
- **Identificación y autenticación**: se requiere que un usuario se identifique antes de comenzar a ejecutar acciones sobre el sistema. El dato de un usuario no podrá ser accedido por un usuario sin autorización o identificación.

1.3.3 NIVEL C2: PROTECCIÓN DE ACCESO CONTROLADO.

Este subnivel fue diseñado para solucionar las debilidades del C1. cuenta con características adicionales que crean un ambiente de acceso controlado. Se debe llevar una auditoria de accesos e intentos fallidos de acceso a objetos. Tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitir o denegar datos a usuarios en concreto, con base no sólo en los permisos, sino también en los niveles de autorización

Requiere que se audite el sistema. Este auditoria es utilizada para llevar registros de todas las acciones relacionadas con la seguridad, como las actividades efectuadas por el administrador del sistema y sus usuarios. La auditoria requiere de autenticación adicional para estar seguros de que la persona que ejecuta el comando es quien dice ser. Su mayor desventaja reside en los recursos adicionales requeridos por el procesador y el subsistema de discos.

Los usuarios de un sistema C2 tienen la autorización para realizar algunas tareas de administración del sistema sin necesidad de ser administradores. Permite llevar mejor cuenta de las tareas relacionadas con la administración del sistema, ya que es cada usuario quien ejecuta el trabajo y no el administrador del sistema.[5]

1.3.4 NIVEL B1: SEGURIDAD ETIQUETADA.

Este subnivel, es el primero de los tres con que cuenta el nivel B. Soporta seguridad multinivel, como la secreta y ultra secreta. Se establece que el dueño del archivo no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio. A cada objeto del sistema (usuario, dato, etc). Se lo asigna una etiqueta, con un nivel de seguridad jerárquico (alto secreto, secreto, reservado, etc). Y con unas categorías (contabilidad, nominas, ventas, etc).

Cada usuario que accede a un objeto debe poseer un permiso expreso para hacerlo y viceversa. Es decir que cada usuario tienes sus objetos asociados. También se establecen controles para limitar la propagación de derecho de accesos a los distintos objetos.[5]

1.3.5 NIVEL B2: PROTECCIÓN ESTRUCTURADA.

Requiere que se etiquete cada objeto de nivel superior por ser parte de un objeto inferior. La protección estructurada es la primera que empieza a referirse al problema de un objeto a un nivel mas elevado de seguridad en comunicación con otro objeto a un nivel inferior. Así, un disco será etiquetado por almacenar archivos que son accedidos por distintos usuarios.
El sistema es capaz de alertar a los usuarios si sus condiciones de accesibilidad y seguridad son modificadas, y el administrador es el encargado de fijar los canales de almacenamiento y ancho de banda a utilizar por los demás usuarios.[5]

1.3.6 NIVEL B3: DOMINIOS DE SEGURIDAD.

Refuerza a los dominios con la instalación de hardware: por ejemplo el hardware de administración de memoria, se usa para proteger el dominio de seguridad de acceso no autorizado a la modificación de objetos de diferentes dominios de seguridad. Existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite o las deniega según las políticas de acceso que se hayan definido.

Todas las estructuras de seguridad deben ser lo suficientemente pequeñas como para permitir análisis y testeos ante posibles violaciones. Este nivel requiere que la terminal del usuario se conecte al sistema por medio de una conexión segura.
Además, cada usuario tiene asignado los lugares y objetos a los que pueda acceder.[5]

1.3.7 NIVEL A: PROTECCIÓN VERIFICADA.

Es el nivel más elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales (matemáticos) para asegurar todos los procesos que realiza un usuario sobre el sistema.
Para llegar a este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse. El diseño requiere ser verificado de forma matemática y también se deben realizar análisis de canales encubiertos y de distribución confiable. El software y el hardware son protegidos para evitar infiltraciones ante traslados o movimientos de equipamiento.[5]

1.4 VULNERABILIDAD EN REDES.

Una vulnerabilidad es toda condición que permite un atentado a la seguridad dentro de las redes.[6]

Existen diferentes formas en las que se puede encontrar vulnerabilidades tanto en hardware como software.

1.4.1 VULNERABILIDADES EN LOS NAVEGADORES.

Generalmente las fallas de los navegadores, no se dan por fallos intrínsecos, sino que fallan las tecnologías que implementan, aunque en este punto analizaremos realmente fallos intrínsecos de los navegadores, como pueden ser los “Buffer Overflow”

Los “Buffer Overflows” consisten en explotar una debilidad relacionada con los buffers que la aplicación usa para almacenar las entradas de usuario. Por ejemplo, cuando el usuario escribe una dirección en formato URL, ésta se guarda en un buffer para luego procesarla. Si no se realizan las oportunas operaciones de comprobación, un usuario podría manipular estas direcciones.

El protocolo usado puede ser http, pero también otro menos conocidos, internos de cada explorador, como el “res:” o el “mk:”. Precisamente existen fallos de seguridad del tipo “Buffer Overflow” en la implementación de estos dos protocolos.

También se puede citar el fallo de seguridad descubierto por Cybersnot Industries relativo a los archivos “.lnk” y “url” de windows 95 y NT respectivamente. algunas versiones de Microsoft Internet Explorer podían ser utilizadas para ejecutar la aplicación que se deseara siempre que existiera en la computadora de la víctima.[6]

1.4.2 VULNERABILIDAD EN UN ESQUEMA DE SEGURIDAD.

En las redes existe la vulnerabilidad en la seguridad, y en la figura 1.2 muestra dicha vulnerabilidad en un esquema de seguridad:[6]

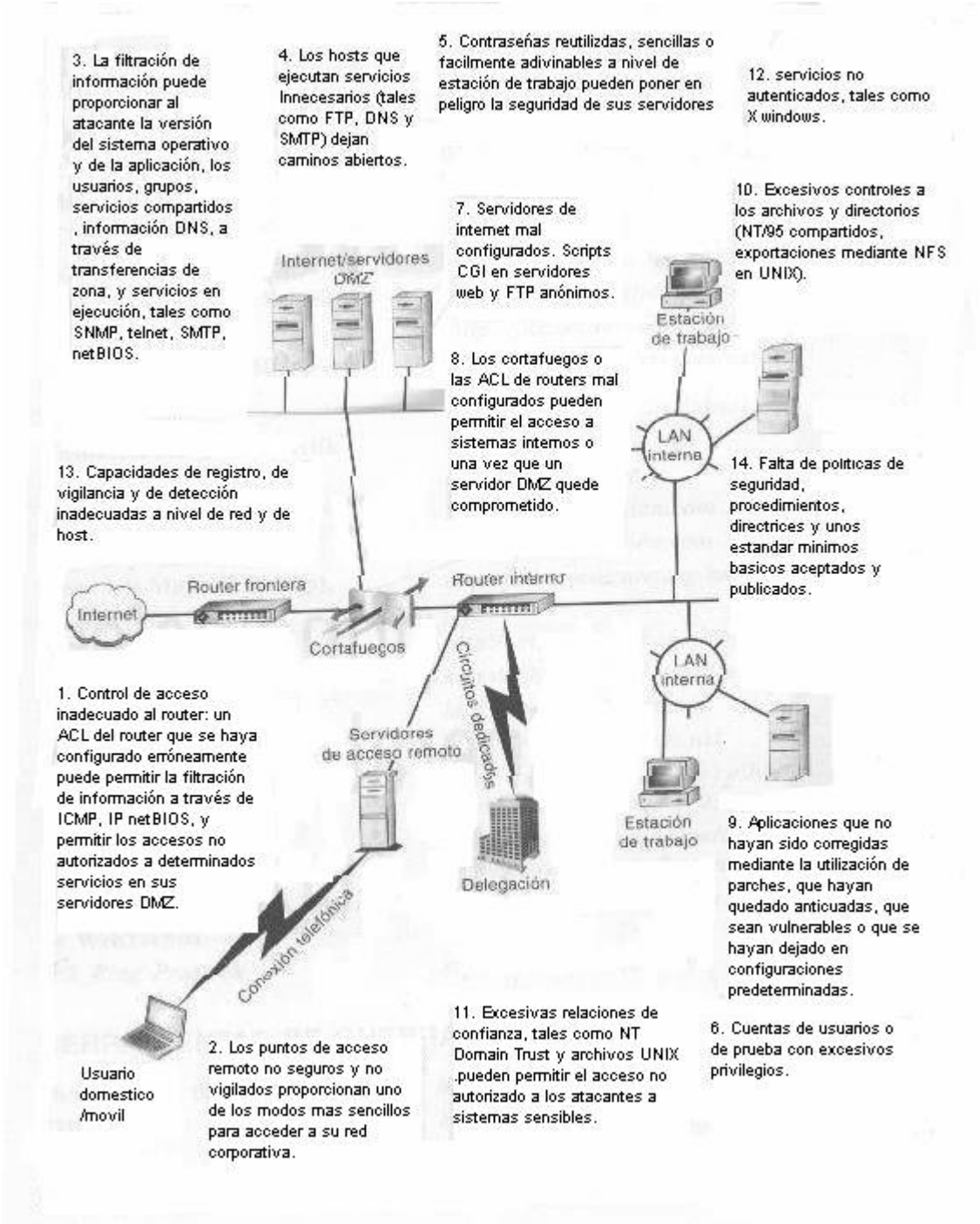

Fig. 1.2 Esquema de la vulnerabilidad en redes

1.5 RIESGOS EN LA INFORMACIÓN.

Estos riesgos provocan acciones hostiles como el robo, fraude y sabotaje de información.

En la Fig. 1.3 aparece un desglose de las perdidas que obtienen las organizaciones anualmente.

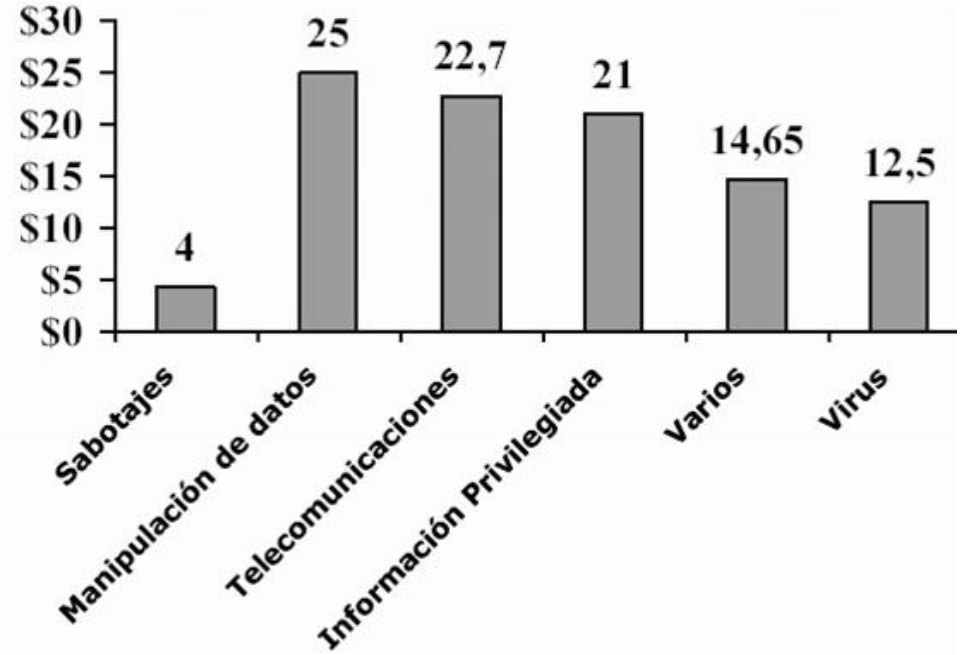

Fig. 1.3 Perdidas monetarias de las organizaciones.

1.5.1 ROBO.

Las computadoras son posesiones valiosas de las empresas y están expuestas, de la misma forma que lo están las piezas de stock e incluso el dinero. Es frecuente que los operadores utilicen la computadora de la empresa para realizar trabajos privados o para otras organizaciones y, de esta manera, robar tiempo de máquina. La información importante o confidencial puede ser fácilmente copiada. Muchas empresas invierten millones de dólares en programas y archivos de información, a los que dan mejor protección que la que otorgan a una máquina de escribir o una calculadora. El software, es una propiedad muy fácilmente sustraíble y las cintas y discos son fácilmente copiados sin dejar ningún rastro.[7]

1.5.2 FRAUDE.

Cada año, millones de dólares son sustraídos de empresas y en muchas ocasiones, las computadoras han sido utilizadas como instrumento para dichos fines. Sin embargo, ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.), tienen algo que ganar, sino que más bien pierden en imagen, no se da publicidad a este tipo de situaciones.[7]

1.5.3 SABOTAJE.

El peligro más temido en los centros de procesamiento de datos, es el sabotaje. Empresas que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos mas duros. Este puede ser un empleado o un sujeto ajeno a la propia empresa.[7]

Físicamente, los imanes son las herramientas a las que se recurre, ya que con una ligera pasada, la información desaparece, aunque las cintas estén almacenadas en el interior de su funda de protección. Una habitación llena de cintas puede ser destruida en pocos minutos y los centros de procesamiento de datos pueden ser destruidos sin entrar en ellos. Además, suciedad, partículas de metal o gasolina pueden ser introducidos por los conductos de aire acondicionado. Las líneas de comunicaciones y eléctricas pueden ser cortadas, etc.[7]

1.6 TIPOS DE DELITOS INFORMÁTICOS.

La Organización de las Naciones Unidas (ONU) reconocen los siguientes tipos de delitos informáticos:

1. **Fraudes cometidos mediante manipulación de computadoras**
   - ♠ **Manipulación de los datos de entrada**: este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común, ya que es fácil de cometer y difícil de descubrir.
   - ♠ **La manipulación de programas**: consiste en modificar los programas existentes en el sistema o en insertar nuevos programas o rutinas. Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente tiene conocimientos técnicos concretos de informática y programación.
   - ♠ **Manipulación de los datos de salida**: se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude del que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.
   - ♠ **Fraude efectuado por manipulación informática**: aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina “técnica del salchichón” en la que “rodajas muy finas” apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra. Se basa en el principio de que 10,66 es igual a 10,65 pasando 0,01 centavos a la cuenta del ladrón “n” veces.

2. **Manipulación de los datos de entrada.**
   - ♠ **Como objeto**: cuando se alteran datos de los documentos almacenados en forma computarizada.
   - ♠ **Como instrumento**: las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial.

3. Daños o modificaciones de programas o datos computarizados.

- **Sabotaje informático**: es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.
- **Acceso no autorizado a servicios y sistemas informáticos**: estos acceso se pueden realizar por diversos motivos, desde la simple curiosidad hasta el sabotaje o espionaje informático.
- **Reproducción no autorizada de programas informáticos de protección legal**: esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de estas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, se considera, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

Adicionalmente a estos delitos, existen otros como los siguientes:

- Fraude en el campo de la informática.
- Falsificación en materia informática.
- Sabotaje informático y daños a datos computarizados.
- Acceso no autorizado.
- Espionaje informático.
- Tráfico de claves informáticas obtenidas por medio ilícito.
- Distribución de virus o programas delictivos.[7]

CAPITULO

2

ATAQUES A LA SEGURIDAD EN REDES

RESUMEN.

En este capítulo se refiriere a las distintas personas que tratan de manera ilegal, la obtención de datos o información, también, aquellos que tratan de atacar a una organización con fines de destrucción de la misma, o de aquellos que solo por gusto y curiosidad quieren probar sus habilidades contra ellas, estos pueden ser los hackers, crackers, y otros habitantes del ciberespacio, donde cada uno de ellos se describirán. Se conocerán las diferentes técnicas, ataques y herramientas que utilizan para alcanzar su objetivo, ya sea de controlar la pc de la víctima, o el robo de passwords, etc.

Se informará de que es un virus, como se propaga en la computadora, los daños que pueden causar, las diferentes partes donde residen, los tipos de virus y también el como prevenirlos, las medidas que se tienen para su obstrucción y la eliminación de ellos.

.1 DEFINICIÓN DE HACKER.

Un hacker es una persona que está siempre en una continua búsqueda de información, vive para aprender y todo para él es un reto; no existen barreras, y lucha por la difusión libre de información, distribución de software sin costo y la globalización de la comunicación.[8]

El concepto de hacker, generalmente es confundido erróneamente con los mitos que existen acerca de este tema:

- ♠ Un hacker es pirata. Esto no es así, ya que los piratas comercian con la información que obtienen, entre otras cosas, y un verdadero hacker solo obtiene esa información para su uso personal.
- ♠ Un hacker es el que entra en los sistemas ajenos y se dedica a destruir la información almacenada en ellos. El error consiste en que el destruye información y sistemas ajenos, no es el hacker sino el cracker.

Entonces un hacker se describe de la siguiente forma:

1. Un verdadero hacker es curioso y paciente. Si no fuera así, terminarían por hartarse en el intento de entrar en el mismo sistemas una y otra vez, abandonando el objetivo.
2. Un verdadero hacker no se mete en el sistema para borrarlo todo o para vender lo que consiga. Quiere aprender y satisfacer su curiosidad. Esa el única finalidad de introducirse en el sistema. Buscan dentro de un lugar en el que nunca han estado, exploran todos los pequeños rincones de un mundo diferente del que ya conocen y que les aburre. ¿Por qué destruir algo y perderse el placer de decir a los demás que hemos estado en un lugar donde ellos no han estado?
3. un hacker es inconformista, ¿por qué pagar por una conexión que actualmente cuesta mucho dinero, y además es limitada?¿por qué pagar por una información que solo utilizaran una vez?

4. Un hacker es discreto, es decir, que cuando entra en un sistema es para su propia satisfacción, no van por ahí cantándolo a los cuatro vientos. La mayoría de los casos de “hackers” escuchados son en realidad “fantasming”. Esto quiere decir, que si un amigo se entera que ha entrado en cierto sistema ; “el ruido de los canales de comunicación” hará que se termine sabiendo que se ha entrado en un sistema cinco veces mayor, que había destruido miles de ficheros y que había inutilizado el sistema.
5. Un hacker disfruta con la exploración de los detalles de los sistemas programables y aprovecha sus posibilidades; al contrario de la mayoría de los usuarios, que prefieren aprender sólo lo imprescindible.
6. Un hacker programa de forma entusiasta (incluso obsesiva), rápido y bien.
7. Un hacker es experto en un programa en particular, o realiza trabajos frecuentemente usando cierto programa. Por ejemplo “ un hacker de unix programador en C”.
8. Los hackers suelen congregarse. Tienden a connotar participación como miembro en la comunidad global definida como “ La Red”.
9. Un hacker disfruta del reto intelectual de superar o rodear las limitaciones de forma creativa.
10. Antiguamente en esta lista se incluía: persona maliciosa que intenta descubrir información sensible: contraseñas, acceso a redes, etc. Pero para este caso en particular los verdaderos hackers han optado por el término cracker y siempre se espera (quizás inútilmente) que se los diferencie.

11. 2.1.1 HABILIDADES BÁSICAS EN UN HACKER.

El conjunto de habilidades cambia lentamente a lo largo del tiempo a medida que la tecnología crea nuevas tecnologías y descarta otras por obsoletas. Por ejemplo, hace tiempo, se incluía la programación en lenguaje de máquina y Assembler, y no se hablaba de HTML. Un buen hacker incluye las siguientes reglas en su itinerario:

1. Aprender a programar. Esta es, por supuesto, la habilidad fundamental del hacker. Se deberá aprender como pensar en los problemas de programación de una manera general, independiente de cualquier lenguaje. Se debe llegar al punto en el cual se pueda aprender un lenguaje nuevo en días, relacionando lo que está en el manual con lo que ya se sabe de antes. Se debe aprender varios lenguajes muy diferentes entre sí. Es una habilidad compleja y la mayoría de los mejores hackers lo hacen de forma autodidacta.
2. Aprender Unix. El paso más importante es obtener un Unix libre, instalarlo en una máquina personal y hacerlo funcionar. Si bien se puede aprender a usar internet sin saber Unix, nunca se podrá ser hacker en internet sin conocerlo. Por este motivo, la cultura hacker está centrada fuertemente en Unix[5].[8]

2.2 CRACKERS.

Los crackers, en realidad, son hackers cuyas intenciones van más allá de la investigación. Es una persona que tiene fines maliciosos o de venganza, quiere demostrar sus habilidades pero de manera equivocada o simplemente personas que hacen daño solo por diversión. Los hackers opinan que ellos son “hackers mediocres, no demasiados brillantes, que buscan violar un sistema.[8]

[5] UNIX: Sistema operativo multiusuario independiente del tipo de ordenador

2.3 PHREAKERS

El phreaker, son personas que tienen ciertos conocimientos y utilizan herramientas de hardware y software, para engañar a las compañías telefónicas y éstas no les cobren las llamadas que hacen.

La realidad indica que los phreakers son crackers de las redes de comunicación. Personas con amplio (a veces mayor que el de los mismos empleados de las compañias telefónicas) conocimientos en telefonía.

Se dice el phreaking es el antecesor del hacking ya que es mucho más antiguo. Comenzó en los albores de la década de los 60's cuando un tal Mark Bernay descubrió como aprovechar un error de seguridad de Bell basaba en la utilización de los mecanismos para la realización de llamadas gratuitas. Lo que Bernay descubrió, fue que dentro de Bell existían unos números de prueba que servían para que los operarios comprobaran las conexiones. Hasta aquí todos eran simples adolescentes que hacían llamadas gratuitas a sus padres en otro estado.

La situación cambió cuando se descubrió que Bell era un universo sin explorar y al que se le podría sacar más partido que el de unas simples llamadas. Se comenzaron a utilizar ciertos aparatos electrónicos, los cuales son conocidos como "boxes" (cajas). La primera fue la "blue box" que fue hallada en 1961 en el Washington State College, y era un aparato con una carcasa metálica que estaba conectada al teléfono. Estas boxes lo que hacían era usar el nuevo sistema de Bell (lo tonos) para redirigir las llamadas. Cuando se marcaba un número, Bell lo identificaba como una combinación de notas musicales que eran creadas por seis tonos maestros, los cuales eran los que controlaban Bell y por lo tanto eran secretos (al menos eso pretendían y creían los directivos de Bell).

El cómo los phreakers llegaron a enterarse del funcionamiento de estos tonos fue algo muy simple: Bell, orgullosa de su nuevo sistema, lo público detalladamente en revistas que iban dirigidas única y exclusivamente a los operarios de la compañía telefónica. Lo que sucedió es que no cayeron en la cuenta de que todo suscriptor de esa revista recibió también en su casa un ejemplar que narraba el funcionamiento del nuevo sistema.

Al poco tiempo hubo en la calle variaciones de la blue box inicial, que fueron llamadas red box y black box, las cuales permitían realizar llamadas gratis desde teléfonos públicos.

Las blue boxes no solo servían para realizar llamadas gratuitas, sino que proporcionaban a sus usuarios los mismo privilegios que los operadores de Bell.

Lo realmente curioso y desastroso para Bell, es que algunas personas eran capaces de silbar 2600 ciclos (lo cual significa que la línea está preparada para recibir una llamada) de forma completamente natural.

Hoy, el hacking y el phreacking viven en perfecta armonía y en pleno auge con las nuevas tecnologías existentes. Es difícil delimitar el terreno de cada uno, ya que un hacker necesitaría, tarde o temprano, hacer phreacking si desea utilizar la línea telefónica mucho tiempo en forma gratuita y de la misma forma un phreaker necesitará del hacking si desea conocer en profundidad cualquier sistema de comunicaciones.[8]

2.4 CARDING – TRASHING.

Entre las personas que dedicaban sus esfuerzos a romper la seguridad como reto intelectual hubo un grupo (con no tan buenas intenciones) que trabajan para conseguir una tarjeta de crédito ajena. Así nació:

1. El carding, es el uso (o generación) ilegítimo de las tarjetas de crédito (o sus números), pertenecientes a otras personas con el fin de obtener los bienes realizando fraude con ellas. Se relaciona mucho con el hacking y el cracking mediante los cuales se consiguen los números de las tarjetas.
2. El trashing, que consiste en rastrear en las papeleras en busca de información, contraseñas o directorios.[9]

2.5 DIFERENTES HABITANTES DEL CIBERESPACIO.

2.5.1 GURÚS.

Son considerados los maestros y los encargados de “formar” a los futuros hackers. Generalmente no están activos pero son identificados y reconocidos por la importancia de sus hackeos, de los cuales sólo enseñan las técnicas básicas.[10]

2.5.2 LAMERS O SCRIPT – KIDDERS

Son aficionados jactosos. Prueban todos los programas (con el título “como ser un hacker en 21 días) que llegan a sus manos. Generalmente son los responsables de soltar virus y bombas lógicas en la red sólo con el fin de molestar y que otros se enteren que usa tal o cual programa. Son aprendices que presumen de lo que no son, aprovechando los conocimientos del hacker y lo ponen en práctica sin saber.[10]

2.5.3 COPYHACKERS.

Literalmente son falsificadores sin escrúpulos que comercializan todo lo copiado (robado).[10]

2.5.4 BUCANEROS.

Son comerciantes sucios que venden los productos crackeados por otros. Generalmente comercian con tarjeta de crédito, de acceso y compran a los copyhackers. Son personas sin ningún (o escaso) conocimiento de informática y electrónica.[10]

2.5.5 NEWBIE.

Son los novatos del hacker. Se introducen en sistemas de fácil acceso y fracasan en muchos intentos, sólo con el objetivo de aprender las técnicas que puedan hacer de él, un hacker reconocido.[10]

2.5.6 WANNABER.

Es aquella persona que desea ser hacker pero estos consideran que su coeficiente no da para tal fin. A pesar de su actitud positiva, difícilmente consiga avanzar en sus propósitos.[10]

2.5.7 SAMURAI.

Son los más parecidos a una amenaza pura. Sabe lo que busca, donde encontrarlo y cómo lograrlo. Hace su trabajo por encargo y a cambio de dinero. Estos personajes, a diferencia de los anteriores, no tienen conciencia de comunidad y no forman parte de los clanes reconocidos por los hackers. Se basan en el principio de que cualquiera puede ser atacado y saboteado, solo basta que alguien lo desee y tenga el dinero para pagarlo.[10]

2.5.8 PIRATAS INFORMÁTICOS.

Este personaje (generalmente confundido con el hacker) es el realmente peligroso desde el punto de vista del copyright, ya que copia soportes audiovisuales (discos compactos, cassettes, DVD, etc.) y los vende ilegalmente.[10]

2.6 IDENTIFICACIÓN DE LAS AMENAZAS.

La identificación de amenazas requiere conocer los tipos de ataques, el tipo de acceso, la forma operacional y los objetivos.[11]

Las consecuencias de los ataques se podrían clasificar en:

- ♠ Data corruption: la información que no contenía defectos pasa a tenerlos.
- ♠ Denial of service (DoS): servicios que deberían estar disponibles no lo están.
- ♠ Leakage: los datos llegan a un destino donde no deberían llegar.

Desde 1990 hasta nuestros días, el CERT (computer emergency response team) que es un grupo de seguridad internacional especializado en dar respuesta a las empresas y organizaciones que denuncian ataques informáticos a sus sistemas de información, viene desarrollando una serie de estadísticas que demuestran que cada día se registran más ataques informáticos y estos son cada vez más sofisticados, automáticos y difíciles de rastrear.

En la figura 2.1 detalla el tipo de atacante, las herramientas utilizadas, en que fase se realiza el ataque, los tipos de procesos atacados, los resultados esperados y/u obtenidos y los objetivos perseguidos por los intrusos.

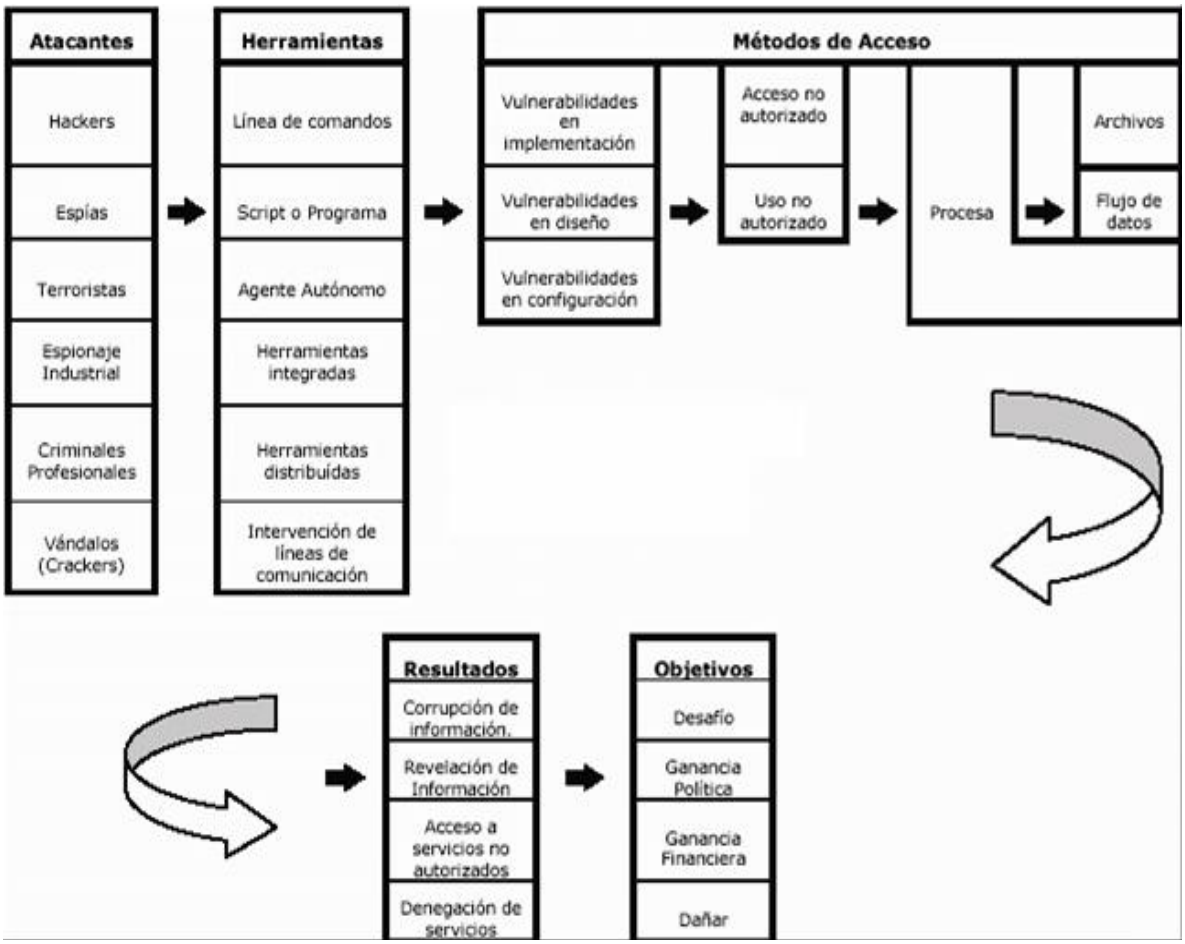

Fig. 2.1 Detalles de ataques

Cualquier adolescente de 15 años (script kiddies), sin tener grandes conocimientos, pero con una potente y estable herramienta de ataque desarrollada por los gurús, es capaz de dejar fuera de servicio cualquier servidor de información de cualquier organismo en Internet, simplemente siguiendo las instrucciones que acompañan la herramienta. [11]

2.7 TIPOS DE ATAQUES.

A continuación se expondrán diferentes tipos de ataques perpetrados, principalmente, por hackers. Estos ataques pueden ser realizados sobre cualquier tipo de red, sistema operativo, usando diferente protocolos, etc.

En los primeros tiempos, los ataques involucraban poca sofisticación técnica. Los insiders (operadores, programadores, data entrys) utilizaban sus permisos para alterar archivos o registros. Los outsiders ingresaban a la red simplemente averiguando una password válida. A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar “agujeros” en el diseño, configuración y operación de los sistemas.

Al describir los tipos de ataques, no se pretende dar una guía exacta ni las especificaciones técnicas necesarias para su uso. Solo se pretende dar una idea de la cantidad y variabilidad de los mismos, así como que su adaptación (y aparición de nuevos) continúa paralela a la creación de nuevas tecnologías.

Cada uno de los ataques abajo descriptos serán dirigidos remotamente. Se define Ataque remoto como “un ataque iniciado contra una maquina sobre la cual el atacante no tiene control físico”. Esta máquina es distinta a la usada por el atacante y será llamada víctima.[12]

2.7.1 INGENIERÍA SOCIAL (IS).

Es la manipulación de las personas para convencerlas de que ejecuten acciones o actos que normalmente no realizan para que revele todo lo necesario para superar las barreras de seguridad. Si el atacante tiene la experiencia suficiente (generalmente es así), puede engañar fácilmente a un usuario (que desconoce las mínimas medidas de seguridad) en beneficio propio. Esta técnica es una de las más usadas y efectivas a la hora de averiguar nombres de usuarios y passwords.

Por ejemplo suele llamarse a un usuario haciéndose pasar por administrador del sistema y requerirle el password con alguna excusa convincente. O bien, podría enviarse un mail (falsificando la dirección origen a nombre del administrador) pidiendo al usuario que modifique su password a una palabra que el atacante suministra.[12]

Para evitar situaciones de IS es conveniente tener en cuenta estas recomendaciones:

- ♠ Tener servicio técnico propio o de confianza.
- ♠ Instruir a los usuarios para que no respondan ninguna pregunta sobre cualquier característica del sistema y derivan la inquietud a los responsables que tenga competencia para dar esa información.
- ♠ Asegurarse que las personas que llaman por teléfono son quien dicen ser. Por ejemplo si la persona que llama se identifica como proveedor de internet lo mejor es cortar y devolver la llamada a forma de confirmación.

2.7.2 INGENIERÍA SOCIAL INVERSA (ISI).

Consiste en la generación por parte de los intrusos, de una situación inversa a la originada en Ingeniería social.

En este caso el intruso publicita de alguna manera que es capaz de brindar ayuda a los usuarios, y estos lo llaman ante algún imprevisto. El intruso aprovechará esta oportunidad para pedir información necesaria para solucionar el problema del usuario y el suyo propio (la forma de acceso al sistema).

La ISI es más difícil de llevar a cabo y por lo general se aplica cuando los usuarios están alertados de acerca de las técnicas de IS. Puede usarse en algunas situaciones especificas y después de mucha preparación e investigación por parte del intruso:

1. Generación de una falla en el funcionamiento normal del sistema. Generalmente esta falla es fácil de solucionar pero puede ser difícil de encontrar por los usuarios inexpertos (sabotaje). Requiere que el intruo tenga un mínimo contacto con el sistema.
2. Comunicación a los usuarios de que la solución es brindada por el intruso (publicidad).
3. Provisión de ayuda del intruso encubierto como servicio técnico.[12]

2.7.3 TRASHING (CARTONEO)

Generalmente, un usuario anota su login y password en un papelito y luego, cuando lo recuerda, lo arroja a la basura. Este procedimiento por más inocente que parezca es el que puede aprovechar un atacante para hacerse de una llave para entrar al sistema..."nada se destruye, todo se transforma".

El trashing puede ser físico (como el caso descrito) o lógico, como analizar buffers de impresora y memoria, bloques de discos, etc. El trashing físico suele ser común en organizaciones que no disponen de alta confidencialidad, como colegios y universidades.[12]

2.7.4 ATAQUES DE MONITORIZACIÓN.

Este tipo de ataque se realiza para observar a la víctima y su sistema, con el objetivo de obtener información, establecer sus vulnerabilidades y posibles formas de acceso futuro.[12]

2.7.4.1 SHOULDER SURFING

Consiste en espiar físicamente a los usuarios para obtener el login y su password correspondiente. El surfing explota el error de los usuarios de dejar su login y password anotadas cerca de la computadora (generalmente en post-it adheridos al monitor o teclado). Cualquier intruso puede pasar por ahí, verlos y memorizarlos para su posterior uso. Otra técnica relacionada al surfing es aquella mediante la cual se ve, por encima del hombro, al usuario cuando teclea su nombre y password.[12]

2.7.4.2 DECOY (SEÑUELOS)

Los decoy son programas diseñados con la misma interface que otro original. En ellos se imita la solicitud de un login y el usuario desprevenido lo hace. Luego, el programa guardará esta información y dejará paso a las actividades normales del sistema. La información recopilada será utilizada por el atacante para futuras "visitas".

Una técnica similar es mediante un programa, donde se guardan todas las teclas presionadas durante una sesión. Y después estudiar el archivo generado para conocer nombre de usuarios y claves.[12]

2.7.4.3 SCANNING (BÚSQUEDA)

El scaneo, como método de descubrir canales de comunicación susceptibles de ser explotados, lleva en uso mucho tiempo. La idea es recorrer (scanear) tantos puertos de escucha como sea posible, y guardar información de aquellos que sean receptivos o de utilidad para cada necesidad en particular. Muchas utilidades de auditoria también se basan en este paradigma.

Scanear puertos implica las técnicas de fuerza bruta. Se envía una serie de paquetes para varios protocolos y se deduce que servicios están “escuchando” por las respuestas recibidas o no recibidas.[12]

Existen diversos tipos de Scanning según las técnicas, puertos y protocolos explotados:

2.7.4.3.1 TCP CONNECT SCANNING

Esta es la forma básica del scaneo de puertos TCP. Si el puerto está escuchando, devolverá una respuesta de éxito; cualquier otro caso significará que el puerto no está abierto o que no se puede establecer conexión con él.

Las ventajas que caracterizan esta técnica es que no necesita de privilegios especiales y su gran velocidad.

Su principal desventaja es que este método es fácilmente detectable por el administrador del sistema. Se verá un gran número de conexiones y mensajes de error para los servicios en los que se ha conseguido conectar una máquina, que lanza el scanner y también se verá su inmediata desconexión.[12]

2.7.4.3.2 TCP SYN SCANNING

Cuando dos procesos establecen una comunicación usan el modelo Cliente/servidor para establecerla. La aplicación del servidor “escucha” todo lo que ingresa por los puertos.

La identificación del Servidor se efectúa a través de la dirección IP del sistema en el que se ejecuta y del número de puerto del que depende para la conexión. El cliente establece la conexión con el servidor a través del puerto disponible para luego intercambiar datos.

La información de control de llamada Handshake /saludo) se intercambia entre el cliente y el servidor para establecer un dialogo antes de transmitir datos. Los “paquetes” o segmentos TCP tienen banderas que indican el estado del mismo.

El protocolo TCP de internet, sobre el que se basa la mayoría de los servicios (incluyendo el correo electrónico, el web y el IRC) implica esta conexión entre dos máquinas.

La principal ventaja de esta técnica de escaneo es que poco sitios están preparados para registrarlos. [12]

2.7.4.3.3 FRAGMENTATION SCANNING.

Esta no es una nueva técnica de escaneo como tal, sino una modificación de las anteriores. En lugar de enviar paquetes completos de sondeo, los mismos se particionan en un par de fragmentos IP. Así, se logra partir una cabecera IP en distintos paquetes para hacerlo más difícil de monitorizar por los filtros que pudiera estar ejecutándose en la máquina objetivo.

Sin embargo, algunas implementaciones de estas técnicas tienen problemas con la gestión de este tipo de paquetes tan pequeños, causando una caída de rendimiento en el sistema del intruso o en el de la víctima. Problemas de esta índole convierte en detectables a este tipo de ataque.[12]

2.7.4.4 EAVESDROPPING – PACKET SNIFFING (husmeo de paquetes)

Muchas redes son vulnerable al eavesdropping, o a la pasiva intercepción (sin modificación) del tráfico de red.

Esto se realiza con Packet Sniffers, los cuales son programas que monitorean los paquetes que circulan por la red. Los sniffers pueden ser colocados tanto en una estación de trabajo conectada a la red, como a un equipo Router a un Gateway de internet y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías.

Cada máquina conectada a la red (mediante una placa con una dirección única) verifica la dirección destino de los paquetes TCP. Si estas direcciones son iguales asume que el paquete enviado es para ella, caso contrario libera el paquete para que otras placas lo analicen.

Un sniffers consiste en colocar a la placa de red en un modo llamado promiscuo, (el cual desactiva el filtro de verificación de direcciones) y por lo tanto, todos los paquetes enviados a la red llegan a esta placa (computadora donde está instalado el sniffer).

Inicialmente este tipo de software, era únicamente utilizado por los administradores de redes locales, aunque con el tiempo llegó a convertirse en una herramienta muy usada por los intrusos.

Actualmente existen sniffers para capturar cualquier tipo de información específica. Por ejemplo passwords de un recurso compartido o de acceso a una cuenta, que generalmente viajan sin encriptar al ingresar a sistemas de acceso remoto. También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mails entrantes y salientes. El análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones e individuos.

Para realizar estas funciones se analizan las tramas de un segmento de red y presentan al usuario solo las que interesan.

Normalmente, los buenos sniffers no se pueden detectar, aunque la inmensa mayoría y debido a que están demasiado relacionados con el protocolo TCP/IP, si pueden ser detectados con algunos trucos.[12]

2.7.4.5 SNOOPING – DOWNLOADING

Los ataques de esta categoría tienen el mismo objetivo que el sniffing: obtener la información sin modificarla.

Sin embargo, los métodos son diferentes. Aquí, además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de correo electrónico y otra información guardada, realizando en la mayoría de los casos un downloading (copia de documentos) de esa información a su propia computadora, para luego hacer un análisis exhaustivo de la misma.

El snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software.[12]

2.7.5 ATAQUES DE AUTENTIFICACIÓN.

Este tipo de ataque tiene como objetivo engañar al sistema de la victima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y password.[13]

2.7.5.1 SPOOFING – LOOPING.

Spoofing puede traducirse como “hacerse pasar por otro” y el objetivo de esta técnica, justamente, es actuar en nombre de otros usuarios.

El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y así sucesivamente. Este proceso se le llama Looping, tiene la finalidad de “evaporar” la identificación y la ubicación del atacante.

El camino tomado desde el origen hasta el destino puede tener muchas estaciones, que exceden obviamente los límites de un país. Otra consecuencia del looping es que una compañía o gobierno pueden suponer que están siendo atacados por un competidor o una agencia de gobierno extranjera, cuando en realidad están seguramente siendo atacados por un insider, o por un estudiante a miles de kilómetros de distancia, pero que ha tomado la identidad de otros.

La investigación de procedencia de un looping es casi imposible, ya que el investigador debe contar con la colaboración de cada administrador de cada red utilizada en la ruta.[13]

2.7.5.2 SPOOFING.

Este tipo de ataques (sobre protocolos) suele implicar un buen conocimiento del protocolo en el que se va a basar el ataque. Los ataques de tipo spooning más conocidos son el IP spoofing, el DNS spooning y el web Spoofing.[13]

2.7.5.2.1 IP SPOOFING

Con el IP spoofing, el atacante genera paquetes de internet con una dirección de red falsa en el campo From, pero que es aceptada por el destinatario del paquete. Su utilización más común es enviar los paquetes con la dirección de un tercero, de forma que la víctima "ve" un ataque proveniente de esa tercera red, y no la dirección real del intruso.[13]

En la figura 2.2 se observa un esquema con dos puentes.

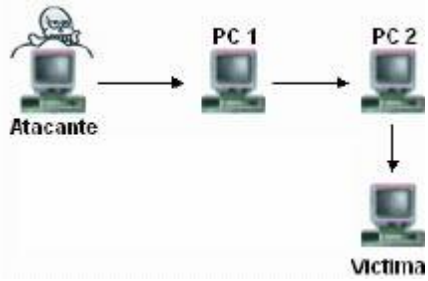

Fig. 2.2 Ataque IP spoofing.

Nótese que si la víctima descubre el ataque, verá a la PC2 como su atacante y no el verdadero origen.

2.7.5.2.2 DNS SPOOFING

Este ataque se consigue mediante la manipulación de paquetes UDP pudiéndose comprometer el servidor de nombres de dominio (Domain Name Server – DNS) de windows NT. Si se permite el método de recusión en la resolución de "Nombre↔Dirección IP" en el DNS, es posible controlar algunos aspectos del DNS remoto. La recursión consiste en la capacidad de un servidor de nombres para resolver una petición de dirección IP a partir de un nombre que no figura en su base de datos. Este es el método de funcionamiento por defecto.[13]

2.7.5.2.3 WEB SPOOFING.

En el caso web spoofing el atacante crea un sitio web completo (falso) similar al que la víctima desea entrar. Los accesos a este sitio están dirigidos por el atacante, permitiéndole monitorear todas las acciones de la víctima, desde sus datos hasta los passwords, números de tarjeta de crédito, etc.

El atacante también es libre de modificar cualquier dato que se esté transmitiendo entre el servidor original y la víctima o viceversa[13]

2.7.5.3 UTILIZACIÓN DE BACKDOORS

"Las puertas traseras son trozos de código en un programa que permiten a quien las conoce, saltarse los métodos usuales de autentificación para realizar ciertas tareas. Habitualmente son insertados por los programadores del sistema para agilizar la tarea de probar código durante la fase de desarrollo".

Esta situación se convierte en una falla de seguridad si se mantiene, involuntaria o intencionalmente, una vez terminado el proyecto ya que cualquiera que conozca el agujero o lo encuentre en su código podrá saltarse los mecanismos de control normales.[14]

2.7.5.4 UTILIZACIÓN DE EXPLOITS

Es muy frecuente ingresar a un sistema explotando agujeros en los algoritmos de encriptación utilizados, en la administración de claves por parte de la empresa, o simplemente encontrando un error en los programas utilizados.

Los programas para explotar estos "agujeros" reciben el nombre de exploits y lo que realizan es aprovechar la debilidad, fallo o error hallado en el sistema (hardware o software) para ingresar al mismo.

Nuevos exploits (explotando nuevos errores en los sistemas) se publican cada día por lo que mantenerse informado de los mismos y de las herramientas para combatirlos es de vital importancia. [14]

2.7.5.5 OBTENCIÓN DE PASSWORDS

Este método comprende la obtención por “Fuerza Bruta” de aquellas claves que permiten ingresar a los sistemas, aplicaciones, cuentas, etc, atacados.

Muchos passwords de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario y además, esta nunca (o rara vez) se 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.[14]

2.7.5.5.1 USO DE DICCIONARIOS

Los diccionarios son archivos con millones de palabras, las cuales pueden ser posibles passwords de los usuarios. Este archivo es utilizado para descubrir dicho password en pruebas de fuerza bruta.

El programa encargado de probar cada una de las palabras, encripta cada una de ellas, mediante el algoritmo utilizado por el sistema atacado y compara la palabra encriptada contra el archivo de passwords del sistema atacado. (previamente obtenido). Si coinciden se ha encontrado la clave de acceso al sistema, mediante el usuario correspondiente a la clave hallada.

Actualmente es posible encontrar diccionarios de gran tamaño, orientados incluso a un área específico de acuerdo al tipo de organización que esté atacando.[14]

2.7.6 ATAQUES DE MODIFICACIÓN – DAÑO

2.7.6.1 TAMPERING O DATA DIDDLING

Esta categoría se refiere a la modificación desautorizada de los datos o el software instalado en el sistema víctima, incluyendo borrado de archivos. Son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que se puede incluso terminar en la baja total del sistema.

Aun así, si no hubo intenciones de bajar por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada.

Como siempre, esto puede ser realizado por insiders u outsiders, generalmente con el propósito de fraude o de dejar fuera de servicio a un competidor.

Son innumerables los casos de este tipo: empleados bancarios (o externos) que crean falsas cuentas para derivar fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes, o contribuyentes que pagan para que les anule una deuda impositiva.[15]

2.7.6.2 BORRADO DE HUELLAS

El borrado de huellas es una de las tareas más importantes que debe realizar el intruso después de ingresar en un sistema, ya que, si se detecta su ingreso, el administrador buscará como conseguir “tapar el hueco” de seguridad, evitar ataques futuros e incluso rastrear al atacante.

Las huellas son todas las tareas que realizó el intruso en el sistema y por lo general son almacenadas en Logs (archivos que guarda la información de lo que se realiza en el sistema) por el sistema operativo.[15]

2.7.6.3 ATAQUES MEDIANTE JAVA APPLETS.

Java es un lenguaje de programación interpretado, desarrollado inicialmente por la empresa SUN. Su mayor popularidad la merece por su alto grado de seguridad. Los más usados navegadores actuales, implementan Máquinas Virtuales Java (MVJ) para ser capaces de ejecutar programas (Applets) de java.

Estos applets, al fin y al cabo, no son más que código ejecutable y como tal, susceptible de ser manipulado por intrusos. Sin embargo, partiendo del diseño, java siempre ha pensado en la seguridad del sistema. Las restricciones a la que somete a los Applets son de tal envergadura (imposibilidad de trabajar con archivos a no ser que el usuario especifique lo contrario, imposibilidad de acceso a zonas de memoria y disco directamente, firma digital, etc.) que es muy difícil lanzar ataques. Sin embargo, existe un grupo de expertos especializados en descubrir fallas de seguridad en las implementaciones de las MVJ[6].[15]

2.7.6.4 ATAQUES CON JAVASCRIPT Y VBSCRIPT.

Son dos lenguajes usados por los diseñadores de sitios Web para evitar el uso de Java. Lo programas realizados son interpretados por el navegador. Aunque los fallos son más numerosos en versiones antiguas de java, actualmente se utiliza para explotar vulnerabilidades específicas de navegadores y servidores de correo.[15]

[6] MVJ: Máquinas Virtuales Java

2.7.6.5 ATAQUES MEDIANTE ACTIVEX.

Activex es una de las tecnologías más potentes que ha desarrollado Microsoft. Mediante Activex es posible reutilizar código, descargar código totalmente funcional de un sitio remoto, etc. Esta tecnología es considerada la respuesta de Microsoft a java. Activex soluciona los problemas de seguridad mediante certificados y firmas digitales. Una Autoridad Certificadora (AC) expide un certificado que acompaña a los controles activos y a una firma digital del programador.

Cuando un usuario descarga una página con un control, se le preguntará si confía en la AC que expendió el certificado y/o en el control Activex. Si el usuario acepta el control, éste puede pasar a ejecutarse sin ningún tipo de restricciones (sólo las propias que tenga el usuario en el sistema operativo). Es decir, la responsabilidad de la seguridad del sistema se deja en manos del usuario, ya sea este un experto cibernauta consciente de los riesgos que puede acarrear la acción o un perfecto novato en la materia. Esta última característica es el mayor punto débil de los controles Activex, ya que la mayoría de los usuarios aceptan el certificado sin siquiera leerlo, pudiendo ser esta la fuente de un ataque con un control dañino.

Así, un conocido grupo de hackers alemanes, desarrollo un control Activex maligno que modificaría el programa de Gestión Bancaria Personal Quicken 95, de tal manera que si un usuario aceptaba el control, éste realizaba la tarea que supuestamente tenía que hacer y además modificaba el Quicken, para que la próxima vez que la víctima se conectara a su banco, se iniciara automáticamente una transferencia a una cuenta del grupo alemán.

Otro control Activex muy especialmente “malévolo” es aquel que manipula el código de ciertos exploradores, para que este no solicite confirmación al usuario a la hora de descargar otro control activo de la Web. Es decir, deja totalmente descubierto el sistema de la víctima, a ataques con tecnología Activex.[15]

2.8 ERRORES DE DISEÑO, IMPLEMENTACIÓN Y OPERCIÓN

Muchos sistemas están expuestos a “agujeros” de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades ocurren por variadas razones, y miles de “puertas invisibles” son descubiertas cada día en sistemas operativos, aplicaciones de software, protocolos de red, browsers de internet, correo electrónico y toda clase de servicios informáticos disponibles.

Los sistemas operativos abiertos (como unix y linux) tienen agujeros más conocidos y controlados que aquellos que existen en sistemas operativos cerrados (como Windows). La importancia y ventaja del código abierto radica en miles de usuarios analizan dicho código en busca de posibles bugs[7] y ayudan a obtener soluciones en forma inmediata.[15]

2.8.1 PREVENCIONES DE ESTOS ATAQUES.

La mayoría de los ataques mencionados se basan en fallos de diseño inherente a Internet (y sus protocolos) y a los sistemas operativos utilizados, por lo que no son solucionables en un plazo breve de tiempo.

La solución inmediata en cada caso es mantenerse informado sobre todos los tipos de ataques existentes y las actualizaciones pertinentes de software, principalmente a los sistemas operativos.[15]

[7] BUGS: Error en el hardware o en el software.

Las siguientes son medidas preventivas que toda red y administrador deben conocer y desplegar:

1. Mantener las máquinas actualizadas y seguras físicamente.
2. Mantener personal especializado en cuestiones de seguridad.
3. No permitir el tráfico “broadcast” desde fuera de nuestra red. De esta forma evitamos ser empleados como “multiplicadores” durante un ataque Smurf.
4. Filtrar el tráfico IP Spoof.
5. Auditorias de seguridad y sistemas de detección.
6. Mantenerse informado constantemente sobre cada una de las vulnerabilidades encontradas y parches lanzados. Para esto es recomendable estar suscrito a listas que brinden este servicio de información.
7. La capacitación continua del usuario.

2.9 VIRUS INFORMÁTICOS.

Es un pequeño programa, invisible para el usuario (no detectable por el sistema operativo) y de actuar específico y subrepticio, cuyo código incluye información suficiente y necesaria para que, utilizando los mecanismos de ejecución que le ofrecen otros programas a través del microprocesador, puedan reproducirse formando réplicas de sí mismos (completas, en forma discreta, en un archivo, disco u computadora distinta a la que ocupa), susceptibles de mutar; resultando de dicho proceso la modificación, alteración y/o destrucción de los programas, información y/o hardware afectados (en forma lógica).[16]

2.9.1 DESCRIPCIÓN DE UN VIRUS

Dado que el virus tiene como característica propia su autoreproducción, no necesita de mucha ayuda para propagarse rápidamente. Existen distintos tipos de virus, como aquellos que infectan archivos ejecutables (.exe, .com, .dll, etc.) los sectores de Boot y la tabla de partición de los discos. Actualmente los que causan mayores problemas son los macro-virus y script-virus, que están ocultos en simples documentos, planillas de cálculo, correo electrónico y aplicaciones que utiliza cualquier usuario de PC. Y además son multiplataforma, es decir, que no dependen de un sistema operativo en particular, ya que un documento puede ser procesado tanto en windows 95/98/NT/2000,XP, como en una macintosh u otras.[17]

2.9.1.1 TÉCNICAS DE PROPAGACIÓN.

Las técnicas son muy variadas para su propagación como se lista a continuación:

1. **Disquetes y otros medios removibles.** A la posibilidad de que un disquete contenga un archivo infectado se une el peligro de que integre un virus de sector de arranque (boot). En este segundo caso y si el usuario lo deja en la disquetera, infectará el ordenador cuando lo encienda, ya que el sistema intentará arrancar desde el disquete.

2. **Correo electrónico.** El usuario no necesita hacer nada para recibir mensajes que en muchos casos ni siquiera ha solicitado y que pueden llegar de cualquier lugar del mundo. Los mensajes de correo electrónico pueden incluir archivos, documentos o cualquier objeto ActiveX – java infectado que, al ejecutarse, contagian la computadora del usuario. En las últimas generaciones de virus se envían e-mails sin mensajes pero con archivos adjuntos (virus) que al abrirlos proceden a su ejecución y posterior infección del sistema atacado. Estos virus poseen una gran velocidad de propagación, ya que se envían automáticamente a los contactos de la libreta de direcciones del sistema infectado.

3. **IRC O CHAT.** Las aplicaciones de mensajería instantánea (ICQ, AOL, MSN, etc) o Internet Relay Chat (IRC), proporcionan un medio de comunicación anónimo, rápido, eficiente, cómodo y barato. Sin embargo, también son peligrosas, ya que los entornos de chat ofrecen por lo general, facilidades para la transmisión de archivos, que conllevan un gran riesgo en un entorno de red.
4. **PAGINAS WEB Y TRANSFERENCIA DE ARCHIVOS VÍA FTP.** Los archivos que se descargan de internet pueden estar infectados y pueden provocar acciones dañinas en el sistema en el que se ejecutan.
5. **GRUPOS DE NOTICIAS.** Sus mensajes e información (archivos) pueden estar infectados y por lo tanto, contagiar al equipo del usuario que participe en ellos.

2.9.1.2 TIPOS DE VIRUS.

Un virus causa daño lógico (generalmente) o físico (bajo ciertas circunstancias y por repetición) de la computadora infectada. Para evitar la intervención del usuario los creadores de virus debieron inventar técnicas de las cuales valerse para que su “programa” pudiera ejecutarse.[18] Estas son algunas:

2.9.1.2.1 ARCHIVOS EJECUTABLES (VIRUS EXEVIR)

El virus se adosa a un archivo ejecutable y desvía el flujo de ejecución a su código, para retornar al huésped y ejecutar las acciones esperadas por el usuario. Al realizarse la acción el usuario no se percata de lo sucedido. Una vez que el virus es ejecutado se aloja en memoria y puede infectar otros archivos ejecutables que sean abiertos en esa máquina.

En este momento su dispersión se realiza en sistema de 16 bits (DOS) y de 32 bits (WINDOWS) indistintamente, atacando programas .COM, .EXE, .DLL, .PIF, etc, según el sistema infectado.[18]

La figura 2.3 muestra las técnicas de infección en archivos ejecutables, algunos ejemplos de ellos son : chernovil, darth vader, PHX

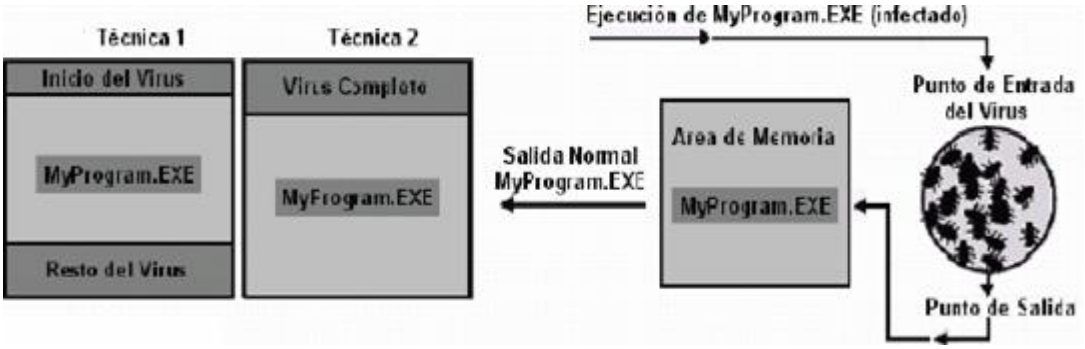

Fig. 2.3 Técnicas de infección en archivos ejecutables.

2.9.1.2.2 VIRUS EN EL SECTOR DE ARRANQUE (VIRUS ACSO ANTERIOR A LA CARGA DEL SO).

En los primeros 512 bytes de un disquete formateado se encuentran las rutinas necesarias para la carga y reconocimiento de dicho disquete. Entre ellas se encuentra la función invocada si no se encuentra el sistema operativo. Es decir, que estos 512 bytes se ejecutan cada vez que se intenta arrancar (bootear) desde un disquete (o si se dejó olvidado uno en la unidad y el orden de booteo de la PC es A: y luego C:). Luego, esta área es el objetivo de un virus de booteo.

Se guarda la zona de booteo original en otro sector del disco (generalmente uno muy cercano o los más altos). Luego el virus carga la antigua zona de booteo. Al arrancar el disquete se ejecuta el virus (que obligatoriamente debe tener 512 bytes o menos) quedando residente en memoria; luego ejecuta la zona de booteo original, salvada anteriormente. Una vez más el usuario no se percata de lo sucedido ya que la zona de booteo se ejecuta iniciando el sistema operativo (si existiera) o informando la falta del mismo.[18]

La figura 2.4 muestra la técnica de infección en la zona de booteo, y algunos ejemplos son el: 512, stoned, michelangelo, diablo.

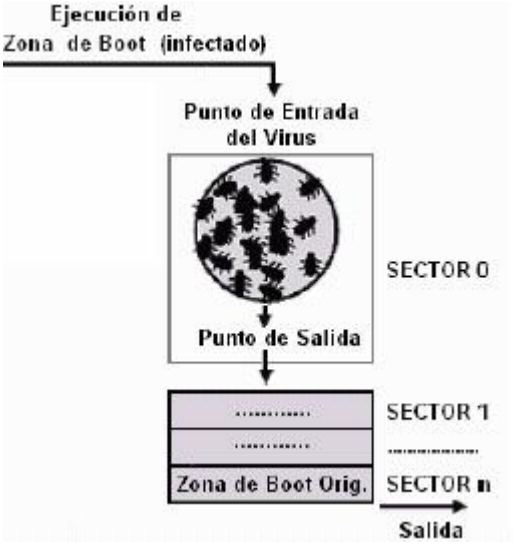

Fig. 2.4 Técnica de infección en zona de booteo.

2.9.1.2.3 VIRUS RESIDENTE.

Un virus puede residir en memoria. El objetivo de esta acción es controlar los accesos a disco realizados por el usuario y el sistema operativo. Cada vez que se produce un acceso, el virus verifica si el disco o archivo objetivo al que se accede, está infectado y si no lo está procede a almacenar su propio código en el mismo. Este código se almacenará en un archivo, tabla de partición, o en el sector de booteo, dependiendo del tipo de virus que se trate.[18]

Ejemplo: 512, avispa, michelangelo, dir II.

2.9.1.2.4 MACROVIRUS.

Estos virus infectan archivos de información generados por aplicaciones de oficina que cuentan con lenguajes de programación de macros. Últimamente son los más expandidos, ya que todos los usuarios necesitan hacer intercambio de documentos para realizar su trabajo. Los primeros antecedentes de ellos fueron con las macros de lotus 123 que ya eran lo suficientemente poderosas como permitir este tipo de implementación. Pero los primeros de difusión masiva fueron desarrollados a principios de los 90's para el procesador de texto Microsoft word, ya que este cuenta con el lenguaje de programación word basic.

Su principal punto fuerte fue que terminaron con un paradigma de la seguridad informática: "los únicos archivos que pueden infectarse son los ejecutables" y todas las tecnologías antivirus sucumbieron ante este nuevo ataque.

Su funcionamiento consiste en que si una aplicación abre un archivo infectado, la aplicación (o parte de ella) se infecta y cada vez que se genera un nuevo archivo o se modifique uno existente contendrá el macrovirus.[18]

En la figura 2.5 se observa una infección de múltiples documentos, como por ejemplo:

De Microsoft word: cap I, cap II, concept, wazzu.

De Microsoft excel: laroux.

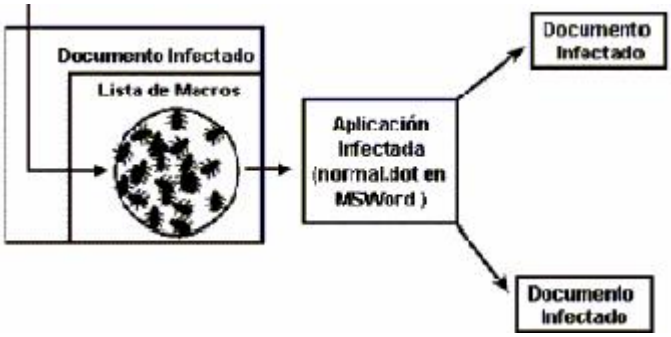

Fig. 2.5 Infección de múltiples documentos.

2.9.1.2.5 VIRUS DE MAIL.

El “último grito de la tecnología” en cuestión de virus. Su modo de actuar, al igual que los anteriores, se basa en la confianza excesiva por parte del usuario: a este le llega vía mail un mensaje con un archivo comprimido (.ZIP por ejemplo), el usuario lo descomprime y al terminar esta acción, el contenido (virus ejecutable) del archivo se ejecuta y comienza el daño.

Este tipo de virus tomó relevancia estos últimos años con la explosión masiva de internet y últimamente con el virus Melissa y I love you. Generalemente estos virus se auto envían a algunas de las direcciones de la libreta. Cada vez que uno de estos usuarios recibe el supuesto mensaje no sospecha y lo abre, ocurriendo el mismo reenvío y la posterior saturación de los servidores al existir millones de mensajes enviados.[18]

2.9.1.2.6 VIRUS DE SABOTAJE.

Son virus construidos para sabotear un sistema o entorno específico. Requieren de conocimientos de programación pero también una acción de inteligencia que provea información sobre el objetivo y sus sistemas.[18]

2.9.1.2.7 VIRUS DE APPLETS JAVA Y CONTROLES ACTIVEX.

La práctica demuestra que es posible programar virus sobre ellas. Este tipo de virus se copian y se ejecutan a si mismos mientras el usuario mantiene una conexión a internet[18]

2.9.1.2.8 REPRODUCTORES – GUSANOS.

Son programas que se producen constantemente hasta agotar totalmente los recursos del sistema huésped y/o recopilar información relevante para enviarla a un equipo al cual su creador tiene acceso.[18]

2.9.1.2.9 CABALLOS DE TROYA.

De la misma forma que el antiguo caballo de troya de la mitología griega, escondía en su interior algo que los troyanos desconocían, y que tenian una función muy diferente a la que ellos podían imaginar; un caballo de troya es un programa que aparentemente realiza una función útil pero además realiza una operación que el usuario desconoce y que generalmente beneficia al autor del troyano o daña el sistema huésped.

Consisten en introducir dentro de un programa una rutina o conjunto de instrucciones, no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto.

Los ejemplos más conocidos de troyanos son el back oriffice y el net bus que, si bien no fueron desarrollados con ese fin, son una poderosa arma para tomar el control de la computadora infectada. Estos programas pueden ser utilizados para la administración total del sistema atacado por parte de un tercero, con los mismos permisos y restricciones que el usuario de la misma.[18]

2.9.1.2.10 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 o dado algún evento particular en el sistema, bien destruye y modifica la información o provoca la baja del sistema.[18]

2.9.1.3 MODELO DE VIRUS INFORMÁTICO.

Un virus está compuesto por su propio entorno, dentro del cual pueden distinguirse tres módulos principales:

1. Módulo de reproducción. Es el encarado de manejar la rutinas de parasitación de entidades ejecutables con el fin de que el virus pueda ejecutarse subrepticiamente, permitiendo su transferencia a otras computadoras.
2. Módulo de ataque. Es el que maneja las rutinas de daño adicional al virus. Esta rutina puede existir o no y generalmente se activa cuando el sistema cumple alguna condición. Por ejemplo el virus chernovil se activa cada vez que el reloj del sistema alcanza el 26 de cada mes.
3. Módulo de defensa. Este módulo, también optativo, tiene la misión de proteger al virus. Sus rutinas tienden a evitar que faciliten o provoquen la detección o remoción del virus.[18]

La figura 2.6 muestra los diferentes módulos de los virus informáticos.

Fig.2.6 Módulos de virus informáticos.

2.9.3 TIPOS DE DAÑOS OCASIONADOS POR LOS VIRUS.

Los virus informáticos no afectan (en su mayoría) directamente al hardware sino a través de los programas que lo controlan; en ocasiones no contienen código nocivo, o bien, únicamente causan daño al reproducirse y utilizar recursos escasos como el espacio en el disco duro, tiempo de procesamiento de memoria, etc. En general los daños que pueden causar los virus se refieren a hacer que el sistema se detenga, borrado de archivos, comportamiento erróneo de la pantalla, despliegue de mensajes, desorden en los datos del disco, aumento del tamaño de los archivos ejecutables o reducción de la memoria total.[18]

2.10 PROGRAMA ANTIVIRUS

Un antivirus es una gran base de datos con la huella digital de todos los virus conocidos para identificarlos y también con las pautas que más contienen los virus. Los fabricantes de antivirus avanzan tecnológicamente casi en la misma medida que lo hacen los creadores de virus. Esto sirve para combatirlos, aunque no para prevenir la creación e infección de otros nuevos.

Actualmente existen técnicas, conocidas como heurísticas, que brindan una forma de “adelantarse” a los nuevos virus. Con esta técnica el antivirus es capaz de analizar archivos y documentos y detectar actividades sospechosas. Esta posibilidad puede ser explotada gracias a que de los 6–20 nuevos virus diarios, sólo aparecen unos cinco totalmente novedosos al año.[19]

Debe tenerse en cuenta que:

• Un programa antivirus forma parte del sistema y por lo tanto funcionará correctamente si es adecuado y está bien configurado.

• No será eficaz el 100% de los casos, no existe la protección total y definitiva. Las funciones presentes en un antivirus son:

1. **Detección:** se debe poder afirmar la presencia y/o accionar de un VI en una computadora. Adicionalmente puede brindar módulos de identificación, erradicación del virus o eliminación de la entidad infectada.
2. **Identificación de un virus:** existen diversas técnicas para realizar esta acción:

a).**Scanning**: técnica que consiste en revisar el código de los archivos (fundamentalmente archivos ejecutables y de documentos) en busca de pequeñas porciones de código que puedan pertenecer a un virus (sus huellas digitales). Estas porciones están almacenadas en una base de datos del antivirus. Su principal ventaja reside en la rápida y exacta que resulta la identificación del virus. En los primeros tiempos (cuando los virus no eran tantos ni su dispersión era tan rápida), esta técnica fue eficaz, luego se comenzaron a notar sus deficiencias. El primer punto desfavorable es que brinda una solución a posteriori y es necesario que el virus alcance un grado de dispersión considerable para que llegue a mano de los investigadores y estos lo incorporen a su base de datos (este proceso puede demorar desde uno a tres meses). Este modelo reactivo jamás constituirá una solución definitiva.

b. **Heurística***:* búsqueda de acciones potencialmente dañinas perteneciente a un virus informático. Esta técnica no identifica de manera certera el virus, sino que rastrea rutinas de alteración de información y zonas generalmente no controlada por el usuario (MBR, Boot Sector, FAT, y otras). Su principal ventaja reside en que es capaz de detectar virus que no han sido agregados a las base de datos de los antivirus (técnica proactiva). Su desventaja radica en que puede “sospechar” de demasiadas cosas y el usuario debe ser medianamente capaz de identificar falsas alarmas.

3. **Chequeadores de Integridad**: Consiste en monitorear las actividades de la PC señalando si algún proceso intenta modificar sectores críticos de la misma. Su ventaja reside en la prevención aunque muchas veces pueden ser vulnerados por los virus y ser desactivados por ellos, haciendo que el usuario se crea protegido, no siendo así.

Es importante diferenciar los términos **detectar:** determinación de la presencia de un virus e **identificar:** determinación de qué virus fue el detectado. Lo importante es la detección del virus y luego, si es posible, su identificación y erradicación.

2.10.1 MODELO DE UN ANTIVIRUS.

Un antivirus puede estar constituido por dos módulos principales y cada uno de ellos contener otros módulos.

La figura 2.7 se observa cual es el modelo de un antivirus.

Fig.2.7 Modelo de antivirus.

• **Módulo de Control:** Este módulo posee la técnica de Verificación de Integridad que posibilita el registro de posibles cambios en los zonas y archivos considerados de riesgo.

• **Módulo de Respuesta:** La función de “Alarma” se encuentra en todos los antivirus y consiste en detener la ejecución de todos lo programas e informar al usuario de la posible existencia de un virus. La mayoría ofrecen la posibilidad de su erradicación si la identificación a sido positiva.[19]

2.10.2 UTILIZACIÓN DE LOS ANTIVIRUS

Como ya se ha descripto un VI[8] es un programa y, como tal se ejecuta, ocupa un espacio en memoria y realiza las tareas para las que ha sido programado. En el caso de instalarse un antivirus en una computadora infectada, es probable que este también sea infectado y su funcionamiento deje de ser confiable. Por lo tanto si se sospecha de la infección de una computadora, nunca deben realizarse operaciones de instalación o desinfección desde la misma. El procedimiento adecuado sería reiniciar el sistema y proceder a la limpieza desde un sistema limpio y seguro.

La mayoría de los antivirus ofrecen la opción de reparación de los archivos dañados. Puede considerarse este procedimiento o la de recuperar el/los archivos perdidos desde una copia de seguridad segura.[19]

[8] VI: virus informáctico.

CAPITULO

3

POLÍTICAS DE SEGURIDAD.

RESUMEN.

En esta parte del documento, se conocerá que es una política de seguridad, para que sirve dicha política dentro de la seguridad en redes, los principios fundamentales, la definición de lo que es un modelo y algunos tipos de ellos que se implementan. Y por último se darán algunas recomendaciones básicas de políticas, que se pueden llevar a cabo para alguna organización, teniéndolas como medidas preventivas para la seguridad de la información y del equipo, ante distintos ataques a los que se expone.

3.1 DEFINICIÓN DE POLÍTICA DE SEGURIDAD

La política de seguridad, en el mundo real, es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad informática dentro de la misma.

La política define la seguridad de la información en el sistema central de la organización, por lo tanto, un sistema central es seguro si cumple con las políticas de seguridad impuestas para esa organización. La política especifica qué propiedades de seguridad el sistema debe proveer. De manera similar, la política define la seguridad informática para una organización, especificando tanto las propiedades del sistema como las responsabilidades de seguridad de las personas.

Una política de seguridad informática debe fielmente representar una política del mundo real y además debe interactuar con la política de recursos, por ejemplo, políticas en el manejo de bases de datos o de transacciones. En ella, se deben considerar las amenazas contra las computadoras, especificando cuáles son dichas amenazas y cómo contraatacarlas. Así mismo debe ser expresada en un lenguaje en el que todas las personas involucradas (quienes crean la política, quienes la van a aplicar y quienes la van a cumplir) puedan entender. [20]

3.2 Principios fundamentales

A través de las leyes, reglas y prácticas que reflejen las metas y situaciones de la organización, ellas también reflejan los principios que se aplican en general, éstos se detallan a continuación:

a) Responsabilidad individual: las personas son responsables de sus actos. El principio implica que la gente que está plenamente identificada debe estar consciente de sus actividades, debido a que sus acciones son registradas, guardadas y examinadas.

b) Autorización: son reglas explícitas acerca de quién y de qué manera puede utilizar los recursos.

c) Mínimo privilegio: la gente debe estar autorizada única y exclusivamente para acceder a los recursos que necesita para hacer su trabajo.

d) Separación de obligaciones: las funciones deben estar divididas entre las diferentes personas relacionadas a la misma actividad o función, con el fin de que ninguna persona cometa un fraude o ataque sin ser detectado. La separación de obligaciones funciona mejor cuando cada una de las personas involucradas tiene diferentes actividades y puntos de vista.

e) Auditoría: el trabajo y los resultados deben ser monitoreados durante su inicio y hasta después de ser terminado. Una revisión de los registros, donde se guardan las actividades, ayuda para realizar una reconstrucción de las acciones de cada individuo.

f) Redundancia: el principio de redundancia afecta al trabajo y a la información. Múltiples copias son guardadas con importantes registros y dichas copias son frecuentemente almacenadas en diferentes lugares.

g) Reducción de Riesgo: Esta estrategia debe reducir el riesgo a un nivel aceptable, haciendo que el costo de la aplicación sea proporcional al riesgo.[20]

3.3 ROLES, PAPELES O FUNCIONES EN EL MUNDO REAL, DE LA POLÍTICA DE SEGURIDAD

La política de seguridad involucra papeles que se repiten en muchas situaciones y también en aplicaciones específicas. Para documentos realizados en papel, se aplican los siguientes roles genéricos:

a) Originador (autor): es la persona que publica un documento, frecuentemente el autor o el director, es el responsable de la unidad.

b) Autorizador: es la persona que tiene el control sobre el documento y quien puede autorizar o denegar el acceso al mismo para editar, copiar, leer, etc. El autorizador puede o no ser el autor.

c) Custodio: es la persona que físicamente guarda el documento y lleva a cabo los propósitos del autorizador sobre la manera de accederlo.

d) Usuario: es la persona que lee y/o modifica el documento.

Si el medio no es un documento pero sí es una transacción comercial, otros roles o funciones entran en acción, incluyendo:

a) Creador: es la persona que diseña la transacción y escribe las reglas sobre los pasos a seguir.

b) Cliente: es la persona que en su nombre se lleva a cabo la transacción.

c) Ejecutor: es la persona que efectivamente realiza la transacción en nombre del cliente, paga un cheque, abre una cuenta, etc.

d) Supervisor: es la persona que verifica que las acciones, resultados y controles se hayan llevado a cabo conforme a lo establecido por el creador.[20]

3.4 POLÍTICAS DE SEGURIDAD EN EL MUNDO REAL DE LA COMPUTACIÓN.

Primero, la política de seguridad debe reflejar fielmente el mundo real. Esto significa que deber ser especificada sin ambigüedades. Segundo, las políticas seleccionadas deben ser hechas sobre la situación actual de los sistemas conectados en red. Una política de seguridad debe estar especificada en un documento especial para tal propósito redactada en un lenguaje natural, claramente y sin ambigüedades posibles. El documento deberá especificar qué propiedades de seguridad se pretenden cubrir con la aplicación de las políticas y la manera de usarlas. [21]

3.5 DEFINICIÓN DE MODELOS

Un modelo de seguridad es la presentación formal de una política de seguridad ejecutada por el sistema. El modelo debe identificar el conjunto de reglas y prácticas que regulan cómo un sistema maneja, protege y distribuye información delicada.

Los modelos de seguridad pueden ser de dos tipos:

1. Modelo abstracto: se ocupa de las entidades abstractas como sujetos y objetos. El modelo Bell LaPadula es un ejemplo de este tipo.

2. Modelo concreto: traduce las entidades abstractas a entidades de un sistema real como procesos y archivos.

Además los modelos sirven a tres propósitos en la seguridad informática:

1. Proveer un sistema que ayude a comprender los diferentes conceptos. Los modelos diseñados para este propósito usan diagramas, analogías, cartas. Un ejemplo es la matriz de acceso.

2. Proveer una representación de una política general de seguridad formal y clara. Un ejemplo es el modelo Bell-LaPadula.

3. Expresar la política exigida por un sistema de cómputo específico.

Es importante mencionar que los modelos formales se basan en métodos de lógica matemática y algunos campos de matemáticas aplicadas, lo cual incluye teoría de información, teoría autómata, teoría compleja y estadística.[21]

3.5.1 CRITERIOS

Al asumir que la política de seguridad es realmente la apropiada, existen criterios que un modelo de seguridad debe seguir a medida que se va desarrollando para considerarse un buen modelo. Por lo tanto, un modelo de seguridad debe:

1. Representar de manera válida y precisa la política de seguridad: los creadores del modelo deben explicar de manera clara cómo el modelo corresponde a la política y deben justificar la validez de las correspondencias.

2. Ayudar a entender a través de expresiones enfocadas y exactas y pruebas de propiedades: un modelo ayuda a la comprensión tras aclarar conceptos y expresarlos de manera precisa, lo cual enfoca la atención sobre lo esencial . Se entiende el problema con lo que se deriva de los axiomas del modelo.

3. Soportar un análisis de seguridad: un modelo debe soportar decisiones sobre seguridad y la pregunta de si existe algún estado del modelo en donde una propiedad específica de seguridad no se mantiene. Desafortunadamente existe una tensión entre la seguridad y la precisión, si el modelo está restringido de manera que la seguridad puede decidirse, no se representará una política de seguridad demasiado precisa.

4. Soportar la creación y verificación del sistema: un sistema basado en un modelo debe ser razonable para construirse y debe trabajar de manera adecuada.

5. Permitir que los sistemas sean modelados en partes y después unirlas: debe ser posible modelar sistemas complejos en partes y después unir estas partes, de esta manera cada parte será más clara y su verificación simple y correcta.[21]

3.5.2 MODELOS DE CONTROL DE ACCESO

Los modelos de control de acceso identifican las reglas necesarias para que un sistema lleve a cabo el proceso que asegura que todo acceso a los recursos, sea un acceso autorizado. Estos modelos refuerzan el principio fundamental de seguridad de autorización, ya que éste protege tanto a la confidencialidad como a la integridad.[21]

Los modelos de control de acceso son:

3.5.2.1 MODELO DE LA MATRIZ DE ACCESO

Este modelo fue desarrollado a principios de los años 70's para los sistemas operativos debido a los problemas de protección presentados en los sistemas multiusuarios. Se trata de un modelo simple e intuitivo y permite expresar varias políticas de protección. El modelo de la matriz de acceso relaciona sujetos, objetos y derechos. Estos elementos se describen a continuación:

a) Objetos: representan los recursos que serán controlados como archivos o áreas de memorias.

b) Sujetos: son las entidades activas del modelo como los usuarios o los procesos ejecutados por el usuario.

c) Derechos: representan un tipo de acceso hacia el objeto como leer, escribir o ejecutar.

La matriz de acceso está formada por un renglón para cada sujeto y una columna para cada objeto, la celda especifica los derechos que el sujeto s tiene sobre el objeto o - la notación empleada es AM[s,o]. Por lo que un renglón de la matriz de acceso corresponde a una lista de capacidad (lista de todos los derechos del sujeto) y una columna corresponde a una lista de control de acceso (lista de todos los derechos que tiene el sujeto sobre el objeto).

Este modelo puede representar muchas políticas de control de acceso que aseguran la confidencialidad (esto se logra controlando la lectura de los objetos) y la integridad (tras controlar las modificaciones a los objetos y la invocación de los programas). Maneja lo que se conoce como DAC[9], ya que la matriz de acceso puede ser cambiada de manera discreta por aquéllos que autorizan. En este modelo se especifica quién eres y con quién estás relacionado además de que el sistema indica lo que te está permitido hacer.

Para que un sistema sea más útil, la matriz de acceso no debe ser estática, entonces los sujetos, los objetos y los derechos suelen ser cambiantes. Esto indica que el modelo debe incluir operaciones para cambiar la matriz de acceso, es decir, ciertas operaciones para crear o destruir sujetos y objetos y para crear o borrar derechos. Sin embargo, debe tomarse en cuenta lo que un cambio en el modelo implica y lo que puede lograr el sujeto con dichos cambios.[21]

3.5.2.2 MODELO HARRISON, RUZZO Y ULLMAN (HRU)

El modelo HRU fue creado por Harrison, Ruzzo y Ullman en 1976 al tratar de mejorar el modelo de la matriz de acceso, debido a que éste era débil con respecto a la seguridad ya que de manera general no toma en cuenta lo que un cambio en el modelo implica.

[9] DAC: control de acceso discreto

El modelo HRU define un sistema de protección que se encuentra constituido por dos elementos:

a) Un conjunto de derechos genéricos: donde ese conjunto representa los tipos de acceso del sujeto hacia el objeto como leer, escribir, borrar, modificar, ejecutar.

b) Un conjunto de comandos: donde un comando cuenta con una parte condicional y una principal, la condicional prueba la presencia de ciertos derechos en la matriz de acceso, si la prueba es exitosa la parte principal se ejecuta realizando una serie de operaciones primitivas que cambian la configuración de protección. Las operaciones primitivas crean y destruyen objetos y sujetos, añaden o borran derechos en la matriz de acceso.

El modelo HRU es sencillo y se encuentra diseñado para contestar preguntas fundamentales. Además, mejora la seguridad puesto que verifica si realmente se trata de un sujeto autorizado y contempla que un cambio en la matriz de acceso no permite a sujetos no autorizados obtener derechos.

El resultado importante del modelo es que no está a discusión si una configuración dada es segura para un determinado derecho. Aún cuando este resultado acerca de la matriz de acceso es fundamental, sólo aplica a un sistema de protección general y no restringido ya que para un sistema restringido monoperacional (donde cada comando se compone de una sola operación primitiva) la seguridad está a discusión pero el procedimiento de decisión es computacionalmente complejo, lo cual no es práctico.

3.5.2.2.1 OTROS RASGOS DEL MODELO DE LA MATRIZ DE ACCESO

Los siguientes rasgos aparecen en diferentes versiones del modelo de la matriz de acceso:

1. Transferencia de derechos: en algunos sistemas los sujetos pueden recibir derechos que son transferibles, es decir, el sujeto puede transferir el derecho a otro sujeto. Esta transferencia es descrita como una copia de bandera, si dicha copia se añade a un derecho en una celda, significa que un sujeto puede copiar ese derecho a otra celda en la columna o, escogiendo si se puede o no copiar la bandera también.

2. El monitor de referencia: algún mecanismo que monitorea todos los accesos a los recursos. Este mecanismo asegura que cada acceso sea autorizado por la matriz.

3. Petición y decisión de acceso: una petición es el evento sobre el cual el monitor de referencia interviene. Esto es, el sujeto s pide acceso de tipo r sobre el objeto o. La decisión permite o niega la petición o la convierte en otra petición. En este punto, otros elementos deben ser tomados en cuenta:

a) Reglas de validación de acceso: especifican cómo el monitor de referencia decide el destino de la petición, es decir, cómo realiza la decisión.

b) Reglas de autorización: especifican cómo la matriz de acceso puede ser modificada.[21]

3.5.2.3 MODELO TAKE-GRANT

Los modelos Take-Grant se encuentran estrechamente identificados con los sistemas de capacidad. Estos modelos representan el estado de protección mediante una gráfica dirigida, los elementos utilizados en este modelo son:

a) Vértice sólido: representa un sujeto.

b) Vértice abierto: representa un objeto.

c) Línea dirigida: va de un vértice a otro y representa un derecho que el sujeto tiene sobre el objeto.

d) Vértice mixto: representa a un sujeto o a un objeto

Un modelo Take-Grant especifica un conjunto de reglas para transformar las gráficas de protección. Estas reglas controlan la forma en la que los derechos pueden ser pasados de un sujeto a otro. Al variar las reglas se obtienen diferentes modelos Take-Grant, por ejemplo, cuando se emplean las reglas Create (crear) y Remove (remover), el modelo indica cómo los vértices se añaden y se quitan, pero si se emplean las reglas Grant (conceder) y Take (tomar), entonces se indica cómo un sujeto concede derechos a otro o cómo adquiere los derechos de otros.

El modelo Take-Grant es más restrictivo debido a que tiene reglas particulares para transformar la gráfica de protección, lo cual logra que las decisiones de seguridad sean posibles[21]

3.5.2.4 MODELO BELL-LAPADULA

El modelo BLP[10] formaliza la política de seguridad multinivel - la política multinivel es aquélla que clasifica la información en cuatro niveles: no clasificado, confidencial, secreto y ultra secreto. La información es descrita en términos de compartimentos los cuales representan el asunto del sujeto. El nivel de seguridad o clase de acceso de un documento es la combinación de su nivel y conjunto de compartimentos. Cualquier persona autorizada, recibe un permiso para un cierto nivel, de esta manera tanto las personas como la información, tienen niveles de seguridad o clases de acceso. La política indica que las personas pueden tener acceso a la información que se encuentra hasta su nivel autorizado - y esta política tiene como objetivo controlar el flujo de la información, el modelo también ayuda en la construcción de sistemas cuya seguridad puede ser verificada.

Una de las limitaciones del control de acceso discreto (DAC) es su vulnerabilidad a los ataques de los Caballos de Troya, esto se debe a que el Caballo de Troya se ejecuta con los derechos del usuario que lo invoca sin desearlo ni saberlo, por lo tanto el control de acceso es incapaz de protegerse contra esto. Para intentar resolver dicho problema, se recurre a un modelo mandatario de control de acceso (MAC), el cual restringe lo que pueden hacer los que autorizan. Este modelo recibe el nombre de Bell-LaPadula ya que fue desarrollado por D. E Bell. Y L. J. LaPadula en 1976.

BLP es un modelo de máquina de estado como muchos modelos de seguridad de computadora donde se ve a los sistemas como una tripleta (S, I, F) donde se tiene un conjunto de estados S, un conjunto de posibles entradas I y una función de transición F que transfiere al sistema de un estado a otro.

[10] **BLP:** Modelo Bell Lapadula

El modelo contiene los siguientes elementos:

a) Sujetos: Las entidades del sistema, incluidos usuarios y procesos.
b) Objetos: las estructuras de información, que almacenan la información del sistema.
c) Modos de acceso: como leer y escribir
d) Niveles de seguridad: cada objeto tiene una clasificación y cada sujeto un nivel.

Un estado de seguridad se encuentra definido por tres propiedades que intentan expresar la política de seguridad:

a) Propiedad de seguridad simple (ss-property): expresa la política de autorización-clasificación.
b) Propiedad estrella (star-property): representa la política del flujo de información no autorizado de un nivel alto a uno bajo.
c) Propiedad de seguridad discrecional: refleja el principio de autorización y se expresa en una matriz de acceso.

Se observa que un estado del sistema satisface la propiedad de seguridad simple si para cada elemento del conjunto de acceso actual, el nivel de seguridad del sujeto domina el nivel de seguridad del objeto. La propiedad estrella se satisface si para cada acceso de escritura en el conjunto de acceso actual, el nivel del objeto es igual al nivel actual del sujeto y para cada acceso de lectura, el nivel del sujeto domina al nivel del objeto. Esta propiedad asegura que si el sujeto tiene acceso de lectura a un objeto y acceso de escritura a otro, entonces el nivel del primero se encuentra dominado por el nivel del segundo. La propiedad estrella representa la política de que un sujeto no puede copiar información de un nivel más alto a un objeto de nivel inferior.

El modelo BLP se ha utilizado como base para muchos sistemas concretos ya que estos modelos deben ser una interpretación válida del modelo abstracto BLP.

Algunas consideraciones del modelo son:

1. Limitaciones de los modelos de control de acceso: un modelo de control de acceso sólo puede expresar de un modo general la política multinivel, es decir, un modelo de este tipo no puede ser tan preciso en este aspecto como lo es un modelo de flujo de información.

2. Restricciones de la propiedad estrella: BLP prohibe el flujo de información de un alto nivel a uno inferior. La suposición es que cualquier flujo es equivalente a fusionar diversas secciones.

3. Sujetos confiables: el modelo muestra que no hay presiones sobre cómo los procesos confiables pueden violar la propiedad estrella, cada sistema que es desarrollado realiza sus propias reglas sobre lo que pueden realizar los sujetos confiables.

4. Estado incompleto del modelo: el modelo BLP trabaja con el conjunto de acceso actual, el cual no modela de manera explícita las lecturas y escrituras actuales, para lo cual se necesitan modelos suplementarios que aseguren que las lecturas y escrituras sean consistentes con el conjunto de acceso actual.

5. Canales encubiertos: El modelo no trabaja con información que es transmitida de manera indirecta, mejor conocida como canales encubiertos. Un sujeto puede transmitir información a otro a través de recursos que estén compartiendo.

6. Transición segura de estado: un sistema puede ser seguro según el modelo BLP, pero aún muestra transiciones no seguras, este problema puede corregirse si se añaden al modelo condiciones necesarias para transiciones seguras del estado.[21]

3.5.2.5 Modelos de flujo de información

Una meta de las políticas de seguridad es proteger la información. Los modelos de control de acceso se aproximan a dicha meta indirectamente, sin relacionarse con la información pero sí con objetos (tales como archivos) que contienen información. [22]

3.5.2.5.1 TEORÍA DE LA INFORMACIÓN

La teoría de la información, la cual fue desarrollada por Claude Shannon para tratar con la comunicación, provee una visión sistemática de la información. La teoría de la información ha sido usada en los modelos de flujo de información y está relacionada con otros problemas y métodos de la seguridad de las computadoras.

La teoría de la información define la información en términos de incertidumbre. Al proporcionar información se elimina la incertidumbre. Por ejemplo: Una carrera entre tres competidores, con una categoría mayor, es más incierta que una carrera entre dos competidores. El concepto de la entropía captura esta idea. Los elementos que considera la teoría de la información son:

a) Entropía: una variable aleatoria, tal como el resultado del lanzamiento de un dado, tiene un conjunto de posibles valores, tales como 1,2,3,4, 5 y 6. La entropía de una variable aleatoria depende de las probabilidades de dichos valores.

b) Entropía Condicional: un importante concepto para el modelo de flujo de información es la entropía condicional. La entropía condicional de X dado Y es una medida de la incertidumbre de X dado el conocimiento acerca de Y. Para cada valor yj de Y, existe una entropía condicional de X dado yj.

c) Canales: un canal es una caja negra que acepta cadenas de símbolos desde alguna entrada alfabética y emite cadenas de símbolos desde alguna salida alfabética. La teoría de la información define diferentes tipos de canales.

·Un canal discreto puede transmitir sólo símbolos desde un número finito de entradas alfabéticas.

·En un canal sin memoria la salida es independiente de cualquier entrada o salida anterior.
·Un canal discreto sin memoria emite una cadena de la misma longitud que la cadena de entrada.

La capacidad de un canal es una medida de la habilidad del canal para transmitir información. Ésta es expresada (dependiendo del contexto) como un bit por segundo o bits por símbolo.[22]

3.5.2.5.2 UN MODELO ENREJADO DEL FLUJO DE INFORMACIÓN

Una política del flujo de información define las clases de información que un sistema puede tener y cómo la información puede fluir entre esas clases. Un modelo de flujo de información desarrollado por Dorothy Denning puede expresar la política de multinivel en términos del flujo de información mejor que el control de acceso. Puede también expresar otras políticas más útiles. La política del flujo está definida por un enrejado.

Una definición precisa de una restricción del flujo de información se encuentra en el concepto de no interferencia. Un grupo de usuarios no interfiere con otro grupo si las acciones del primer grupo al utilizar ciertos comandos no tienen efecto sobre lo que el segundo grupo puede ver. La no interferencia fue introducida por Joseph Goguen y José Meseguer entre 1982 y 1984.[22]

3.5.2.5.3 Consideraciones en la seguridad del flujo de información

Debido a que la no interferencia restringe el flujo de información, se observan varios problemas:

1. Los sistemas son modelados como máquinas de estado determinísticas aunque los sistemas frecuentemente son diseñados sin determinismo.

2. Algunos problemas prácticos no pueden ser manejados, como la política de que la información puede fluir a un nivel más bajo al pasar por un degradador confiable.

3. La no interferencia no está permitida para la generación de datos de alto nivel desde entradas de bajo nivel.

4. La no interferencia es un requerimiento muy fuerte y los modelos deben ser capaces de expresar una medida cuantificada de interferencia.[22]

3.5.2.6 MODELOS DE INTEGRIDAD

Recordando que la integridad se refiere a que la información no sufre modificaciones si éstas no se autorizan, aunado a que es consistente internamente y con los objetos del mundo real que representa y que el sistema ejecuta correctamente, la integridad se define como toda la seguridad exceptuando la confidencialidad y la disponibilidad.

Los sistemas de integridad tienen que ver con la conducta del sistema de acuerdo a las expectativas aun cuando tengan que enfrentar ataques. La integridad de los datos incluye dos tipos de consistencia, ya que éstos deben ser internamente consistentes y consistentes con las entidades del mundo real que representan.

Un concepto más amplio de la integridad de los datos es la calidad de los datos, esta calidad incluye atributos como oportuno, genealogía y entereza.

La integridad de los datos tiene las siguientes metas:

·Prevenir las modificaciones no autorizadas

·Mantener la consistencia interna y externa

·Mantener otros atributos de calidad de los datos

·Prevenir las modificaciones autorizadas pero impropias[22]

Los modelos de integridad tienen como objetivo lograr estas metas. Existen dos tipos de modelos:

3.5.2.7 MODELO DE CLARK-WILSON

El modelo de integridad de David Clark y David Wilson desarrollado entre 1987 y 1989 comenzó una revolución en la investigación de la seguridad informática. Aunque no es un modelo altamente formal, es un armazón para describir los requerimientos de la integridad. Clark y Wilson demostraron que para la mayoría del cómputo relacionado con las operaciones de negocios y el control de los recursos, la integridad es más importante que la confidencialidad. Ellos argumentaban que las políticas de integridad demandan modelos diferentes a los modelos de confidencialidad y diferentes mecanismos ya que se enfocan en dos controles que son centrales en el mundo comercial:

a) Las transacciones bien formadas.
b) Separación de la obligación.

El mecanismo de transacciones correctas busca garantizar que un usuario no pueda modificar arbitrariamente. Solamente permite la modificación en determinadas formas, restringiendo los posibles cambios incorrectos. Por ejemplo, un mecanismo de auditoria que recoja todas las transacciones de información, o un sistema en que solamente a un conjunto cerrado de programas se les permita modificar la información siguen este modelo.

El mecanismo de obligación de separación de obligaciones, trata de mantener la consistencia de la información separando todas las operaciones en diferentes partes que deben ser realizadas por diferentes sujetos. De esta manera, un usuario autorizado a iniciar una transacción no estará autorizado a ejecutarla o validarla.

En comparación con el modelo Bell – Lapadula, en este modelo no se definen niveles de seguridad para la información, ni en función de los mismos datos que un usuario puede manejar, sino que se definen los programas que un usuario puede ejecutar, los cuales, a su vez manejarán la información.[23]

3.6 RECOMENDACIONES BÁSICAS DE POLÍTICAS DE SEGURIDAD.

A continuación se presentan algunas políticas de seguridad que se pueden tomar en cuenta:

1. Los administradores de Red, usuarios de estaciones de trabajo y usuarios domésticos deberán actualizar en forma permanente los últimos parches de los sistemas operativos.
2. Es imperativo tener instalado un buen software antivirus, sin importar la marca o procedencia y actualizar su registro de virus diariamente.
3. Usar Claves de Acceso que no estén asociadas a datos comunes del usuario, tales como la fecha de nacimiento, apelativos, nombres de familiares, etc.

4. Cambiar de Clave de Acceso por lo menos cada 3 meses. Aunque lo ideal es hacerlo mensualmente.
5. Las carpetas compartidas, dentro de una Red, deben tener una Clave de Acceso, la misma que deberá ser cambiada periódicamente.
6. No ejecutar ningún archivo contenido en un mensaje de correo no solicitado o enviado por un remitente desconocido, asi ofrezca atractivos premios o temas provocativos. Mucho menos si estos archivos tienen doble extensión.
7. Verificar cualquier software que haya sido instalado, asegurándose que provenga de fuentes conocidas y seguras.
8. No instalar copias de software pirata. Además de transgredir la Ley, pueden contener virus, spyware o archivos de sistema incompatibles con el del usuario, lo cual provocará su inestabilidad.
9. Tomar precauciones con los contenidos de applets de Java, JavaScripts y Controles ActiveX, durante la navegación, así como los Certificados de Seguridad. Es recomendable configurar el navegador desactivando la ejecución automática de estos contenidos.
10. Instalar un Firewall de software o cualquier sistema seguro para controlar los puertos de su sistema.
11. No emplear los máximos privilegios en tareas para las que no sean extrictamente necesarios.
12. No almacenar información importante en su sistema. Si un intruso la captura, puede borrar esos archivos y eliminar toda prueba, para posteriormente usar los datos obtenidos. Es recomendable mantener esta información en diskettes o en un Zip drive.
13. No se debe confiar en los archivos gratuitos que se descargan de sitios web desconocidos, ya que son una potencial vía de propagación de virus.
14. Configurar el sistema para que muestre las extensiones de todos los archivos.

15. De ninguna manera se debe ejecutar ningún archivo con doble extensión.
16. No contestar los mensajes SPAM, ya que al hacerlo se re-confirmará su dirección IP, ni prestar atención a los mensajes con falsos contenidos, tales como ofertas de premios, dinero, solicitudes de ayuda caritativa, advertencia de virus de fuentes desconocidas, etc.
17. Si el servidor no reconoce su nombre y clave de acceso o servicio de correo, podría ser que ya esté siendo utilizado por un intruso. A menos que haya un error en la configuración, la cual deberá ser verificada.
18. Tampoco se deben descargar archivos con títulos atractivos pero sospechosos, desde canales de Chat, Newsgroups, redes compartidas como KaZaa, Morpheus, BearShare, etc. o vía FTP.
19. La aparición y desaparición de archivos, incluso temporales injustificadamente, lentitud del sistema, bloqueos o re-inicios continuos, desconexiones del modem, inicialización o finalización de programas o procesos sin justificación, la bandeja del CD/DVD se abre y cierra sin motivo alguno, el teclado, mouse u otro periférico dejan de funcionar, son evidencias de que nuestro equipo está siendo controlado por un hacker que ha ingresado a nuestro sistema con un troyano/backdoor.
20. Borre constantemente los cookies, archivos temporales e historial, en la opción Herramientas, Opciones de Internet, de su navegador.
21. Si se posee un buen Router se deben enmascarar las direcciones IP (consulte a un especialista).
22. Es preferible navegar a través de un Proxy anónimo que no revele nuestra identidad o adquirir un software de navegación segura como Anonymizer, Freedom WebSecure, etc. que emplean sistemas de túneles con IPs de intercambio aleatorio.[24]

CAPITULO

4

HERRAMIENTAS DE SEGURIDAD.

RESUMEN.

En este capítulo comprende lo que son las herramientas de seguridad, que así, como las políticas de seguridad, ambas son un complemento para tener una mayor protección en la seguridad. Existen muchas herramientas de seguridad, pero solo se escogieron las más utilizadas, comentando sus características, como son los firewalls, su la evolución de ellas hasta la actualidad y también se conocerá de otros sistemas de protección como lo son la criptografía y kerberos.

Se describe también las herramientas de monitoreo, algunos tipos de ellos, las ventajas de unos y desventajas de otros.

4.1 CONCEPTO DE HERRAMIENTA DE SEGURIDAD

Es un programa que corre en espacio de usuario diseñado para ayudar al administrador ya sea alertándolo o realizando por sí mismo las acciones necesarias a mantener su sistema seguro.

- Orientadas a host[11]: Trabajan exclusivamente con la información disponible dentro del host (configuración, bitácoras, etc.)
- Orientadas a red: Trabajan exclusivamente con la información proveniente de la red (barridos de puertos, conexiones no autorizadas, etc.) [25]

4.2 HERRAMIENTAS DE SEGURIDAD

Así como existen herramientas para el análisis de la seguridad en redes también hay herramientas para modificar parámetros en nuestro sistema y con esto asegurarlo contra dicersos ataques.
El firewall o muro de fuego, constituye una de las herramientas más importantes de la seguridad de redes, pero también existen otros sistemas de protección como son la criptografía y kerberos, sin embargo, éstas no son las únicas ya que en el mercado existen un sin fin de ellas.[26]

A continuación hablaremos un poco de estas herramientas y algunas de sus características.

[11] HOST: Término utilizado para denominar cada uno de los pasos que es preciso dar para llegar de un punto de origen a otro de destino a lo largo de una red a través de direccionadores (*routers*).

4.2.1 MUROS DE FUEGO (FIREWALLS)

Básicamente un firewall es una computadora que se encarga de filtrar el tráfico de información entre dos redes. El problema no es el controlar a los usuarios de un sistema sino el prevenir accesos no autorizados de hackers que pudieran atacar la seguridad.

La ventaja de construir un firewall entre una red confiable y una insegura, es la de reducir el campo de riesgo ante un posible ataque. Un sistema que no cuente con este tipo de protección es propenso a sufrir un acceso no autorizado en cualquier nodo que compone la red confiable. En el momento de proteger el sistema con un firewall, el peligro se reduce a un solo equipo.

La mejor manera de proteger una red interna es vigilando y con un firewall bien diseñado obtenemos esta ventaja. Este medio nos puede proveer información de los paquetes de datos que entran a la red, los que son rechazados, el número de veces que tratan de entrar, cuantas veces un usuario no autorizado ha querido penetrar en la red, etc. Con esta información se puede actualizar el sistema de seguridad y prevenir una posible violación al mismo.

Un firewall debe proveer los fundamentos de seguridad para un sistema, pero no es lo único que necesitamos para proteger la red ya que no esta exento de ser pasado por un hacker. Esencialmente se instala entre la red interna y la Internet. El firewall previene el acceso del resto del mundo al sistema y sobre todo a la información que circula por la Intranet[12]. Un firewall combina hardware y software para proteger la red de accesos no autorizados.[27] La figura 4.1 muestra un Firewall de cisco.

[12] INTRANET: **Red propia de una organización, diseñada y desarrollada siguiendo los protocolos propios de Internet, en particular el protocolo TCP/IP. Puede tratarse de una red aislada, es decir no conectada a Internet.**

Fig.4.1 Firewall Cisco 515.

4.2.1.1 TIPOS DE FIREWALL

Existen varios tipos de técnicas para implementar un firewall:

- ♠ Filtros a nivel paquete (Packet Filters)
- ♠ Firewall a nivel circuito (Circuit Level Firewalls)
- ♠ Firewall a nivel aplicación (Application Layer Firewalls)
- ♠ Filtros dinámico a nivel paquete (Dynamic Packet Filters

4.3.1.1.1 FILTROS A NIVEL PAQUETE (PACKET FILTERS):

Esta tecnología pertenece a la primera generación de firewalls la cual analiza el tráfico de la red. Cada paquete que entra o sale de la red es inspeccionado y lo acepta o rechaza basándose en las reglas definidas por el usuario. El filtrado de paquetes es efectivo y transparente para los usuarios de la red, pero es difícil de configurar. Además de que es susceptible a IP Spoofing[13].

Las reglas para rechazar o aceptar un paquete son las siguientes:

- √ Si no se encuentra una regla que aplicar al paquete, el paquete es rechazado.
- √ Si se encuentra una regla que aplicar al paquete, y la regla permite el paso, se establece la comunicación.
- √ Si se encuentra una regla que aplicar al paquete, y la regla rechaza el paso, el paquete es rechazado.[27]

[13] **IP SPOOFING: Es una técnica usada para obtener acceso no autorizado a las computadoras, en donde el "intruso" envía mensajes a una computadora con una dirección IP indicando que el mensaje viene de una computadora confiable.**

4.2.1.1.2 FIREWALL A NIVEL CIRCUITO (CIRCUIT LEVEL FIREWALLS):

Esta tecnología pertenece a la segunda generación de firewalls y valida que los paquetes pertenezcan ya sea a una solicitud de conexión o bien a una conexión entre dos computadoras. Aplica mecanismos de seguridad cuando una conexión TCP o UDP[14] es establecida. Una vez que la conexión se establece, los paquetes pueden ir y venir entre las computadoras sin tener que ser revisados cada vez.
El firewall mantiene una tabla de conexiones válidas y permite que los paquetes de la red pasen a través de ella si corresponden a algún registro de la tabla. Una vez terminada la conexión, la tabla se borra y la transmisión de información entre las dos computadoras se cierra.[27]

4.2.1.1.3 FIREWALL A NIVEL APLICACIÓN (APPLICATION LAYER FIREWALLS):

Pertenece a la tercera generación de firewalls. Examina la información de todos los paquetes de la red y mantiene el estado de la conexión y la secuencia de la información. En este tipo de tecnología también se puede validar claves de acceso y algunos tipos de solicitudes de servicios.

La mayoría de estos tipos de firewalls requieren software especializado y servicios Proxy. Un Servicio Proxy es un programa que aplica mecanismos de seguridad a ciertas aplicaciones, tales como FTP[15] o HTTP. Un servicio proxy puede incrementar el control al acceso, realizar chequeos detallados a los datos y generar auditorias sobre la información que se transmite.[27]

[14] UDP: Abreviatura para 'User Datagram Protocol', es un protocolo sin conexión, ofrece a cambio una manera directa de enviar y recibir datagramas sobre una red IP. Este protocolo es usado principalmente para transmitir mensajes sobre una red.

[15] FTP: Abreviatura para 'File Transfer Protocol', es el protocolo usado en Internet para enviar archivos.

4.2.1.1.4 FILTROS DINÁMICOS A NIVEL PAQUETE (DYNAMIC PACKET FILTERS):

Pertenece a la cuarta generación de firewall y permite modificaciones a las reglas de seguridad sobre la marcha. En la práctica, se utilizan dos o mas técnicas para configurar el firewall.

Un firewall es considerado la primera línea de defensa para proteger la información privada.[27]

4.2.2 CRIPTOGRAFÍA

Este es un medio para proveer seguridad a las transmisiones de datos. En Internet, la información viaja por la red en forma de paquetes bajo el protocolo TCP/IP y algunos hackers pudieran interceptarlos, esto es un peligro potencial de manera individual y organizacional. Cuando se obtiene acceso a estos paquetes, la comunicación entre dos nodos es insegura por que existe una persona que puede recibir al mismo tiempo información confidencial.

Una manera de protección es la criptografía ya que el mensaje es codificado por medio de un algoritmo y sólo puede ser leído o decodificado con el mismo algoritmo en el nodo receptor. En otras palabras, el mensaje es oculto dentro de otro mensaje haciéndolo imposible de leer para todos excepto para el receptor. Al algoritmo de encriptación se le conoce como llave secreta o pública según sea el caso.[28]

4.2.3 KERBEROS

Kerberos es un sistema de autentificación en red desarrollado por el MIT[16]. Permite a los usuarios comunicarse sobre las redes computacionales enviando su identificación a los otros, previniendo la escucha indiscreta. Tiene como principio el mantener un servidor de la red seguro o confiable ya que sería imposible asegurar todos.

Provee confidencialidad de la información usando la encriptación y también una autentificación en tiempo real dentro de un ambiente distribuido inseguro.

El modelo de kerberos esta basado en un protocolo de autentificación a través de un servidor confiable ya que este sistema considera que toda la red es una región de riesgo grande excepto por éste servidor. Trabaja proporcionando a los usuarios y a los servicios boletos que pueden usar para identificarse a sí mismos, además de llaves encriptadas secretas proporcionando cierta seguridad en la comunicación con los recursos de la red.[29]

4.2.4 S/KEY

S/Key es un esquema de degeneración de contraseña de uso temporal desarrollado por Bellcore y que no requiere hardware adicional. Este programa se puede obtener vía internet en la siguiente dirección: http://thumper.bellcore.com/pub/nmh/skey

[16] MIT: Instituto Tecnológico de Masschussets

4.2.5 MUY BUENA PRIVACIDAD (PGP)

(Pretty Good Privacy)

PGP es un sistema de protección de E-mail y de archivos de datos, que proporciona una comunicación segura a través de canales inseguros. Fue desarrollado a principios de los 90's, por Phill Zimmermann, con el fin de otorgar confidencialidad y autentificación. Es decir, sólo aquellos que deben recibir un mensaje pueden leerlo y el origen de un mensaje es comprobable.

Permite una administración de llaves además de la compresión de datos. Es usado en las firmas digitales. [30]

Este sistema se justifica debido a las siguientes razones:

- No se necesita ser un criminal para querer disfrutar del derecho a la privacidad.
- El fisgoneo en internet es cada día más sencillo.

Para su desarrollo el autor realizó lo siguiente:

- Seleccionó los mejores algoritmos de criptografía disponibles como bloques de construcción.

- Integró éstos algoritmos dentro de una aplicación de propósito general independiente de sistema operativo o el procesador, basándose en un pequeño conjunto de comandos fáciles de usar.
- Realizando el paquete y su documentación, incluyendo el código fuente, propuso disponible ampliamente vía internet y redes comerciales como Compuserve.

4.2.6 SHELL SEGURO (SSH)

(Secure Shell)

Una alternativa para tratar con vulnerabilidades de la fase por no es mediante el programa recientemente introducido secure shell o ssh. Tiene reemplazos para rlogin, remsh y rcp pero no requiere el overhead de kerberos, y ofrece más altos niveles de seguridad criptográfica. Además, puede ser usado para mejorar la seguridad en X Windows. El programa ssh protege contra el engaño de IP (IP spoofing), el ruteo de origen IP (IP source routing), el engaño de DNS[17] (DNS spoofing), la corrupción de datos en una conexión y los ataques de autentificación X.

4.2.7 LIBRERÍA DE SOCKETS SEGUROS (SSL)

(Secure Sockets Library)

Otra forma de tratar con las vulnerabilidades de la fase de 1, localizados por SATAN es SSL. La Librería de Socket Seguros (Secure Sockets Library) fue introducida originalmente para Roberto seguridad a los visualizados de Web mediante la encriptación de conexiones http, sin embargo con el paso del tiempo ha sido considerada como un medio para dar seguridad a los servicios en general de internet.

SSL usa la tecnología de llave pública para negociar una llave de sesión y un algoritmo de encriptación entre el cliente y el servidor. La llave pública es almacenada en un certificado X.509[18] que soporta una firma digital de una tercera parte confiable.

[17] DNS **(Sistema de denominación de dominio)** : **Sistema utilizado en Internet para convertir los nombres de los nodos de red en direcciones.**

[18] Un certificado X-509 es un documento digital que identifica de forma unívoca al remitente del mensaje transmitido y garantiza la integridad y privacidad de su contenido

SSL lleva los detalles de la encriptación y autentificación dentro de los llamados a la librería de sockets, permitiendo la implantación de programas internet mucho más fácil. Comparativamente la implantación de un servidor SSL es completamente más fácil que la de un servidor Kerberos.

Desde el punto de vista del usuario, SSL no requiere la participación activa de un KDC[19] servidor de llaves, dado que las firmas digitales se hacen fuera de línea. Así la conexión de red es una transacción de dos partes, más que una transacción entre tres partes. Tanto el cliente como servidor pueden ser autentificados, aunque los clientes visualizadores Netscape actuales usan sólo la autentificación del servidor. [30]

4.3 HERRAMIENTAS DE MONITOREO

Las herramientas de monitoreo están diseñadas específicamente para analizar la confiabilidad de un sistema y para ofrecer cierto grado de seguridad a una red. En la actualidad existen muchas herramientas de seguridad donde analizaremos algunos de ellos para saber sus defectos y ventajas para diseñar la estrategia de protección en un ambiente de red distribuida.[31]

[19] KDC: Centro de distribución de las claves Kerberos.

4.3.1 SATAN

SATAN es una herramienta de búsqueda y generación automática de reportes acerca de las vulnerabilidades de una red, la cual provee un excelente marco de trabajo para continuar creciendo. Es conocido con dos diferentes nombres: SATAN (Security Analysis Tool for Auditig Networks) lo cual significa herramienta de análisis de seguridad para la auditoría de redes y santa (Security Analysis Network Tool For Administrators) herramienta de análisis de la seguridad en red para los administradores.

SATAN es un programa bajo UNIX que verifica rápidamente la presencia de vulnerabilidades en sistemas remotos, ofrece una forma fácil de que el usuario normal examine en corto tiempo la seguridad en red de los sistemas computacionales.

Las características y requerimientos de SATAN son:

- ♠ Diseñado para sistemas UNIX
- ♠ Debe ejecutarse a nivel sistema o con privilegios de roọt
- ♠ Requiere de programas clientes de WWW
- ♠ Requiere de PERL[20].

Aunque existe una forma del programa SATAN para ejecutarse desde la línea de comandos de UNIX, SATAN está diseñado para correrse principalmente desde un visualizado ("browser") de web. Los usuarios le indican el host o red objetivo, el nivel de profundidad de la búsqueda y punto de inicio de esta.

[20] **PERL: (Lenguaje Práctico de Extracción e Informes) Lenguaje de programación muy utilizado para la elaboración de aplicaciones CGI.**

SATAN contiene tanta información como le es posible acerca del objetivo y puede buscar incluso en hosts cercanos, guiado por las reglas de proximidad. La información se agrega a la base de datos estandarizada para ser utilizada en una variedad de reportes.

SATAN consiste de un pequeño Kernel de PERL, junto con un conjunto de programas en C para la verificación de la vulnerabilidad, así como un gran número de programas de soporte en PERL para controlar las búsquedas, almacenar los resultados en los archivos de la base de datos, generación de reportes y emisión de formas HTML. Con estos ejecutar les se incluye un amplio número de documentos en HTML y tutoriales. Tiene una interfaz fácil de usarse, consiste de páginas de HTML usadas a través de un visualizador Web tal como Netscape o Microsoft internet explorer, donde un usuario puede aprender rápida y fácilmente a operarlo.
Aunque SATAN esta disponible con unas pruebas de seguridad interconstruidas, la arquitectura de SATAN le permite aún usuario agregar fácilmente pruebas adicionales.

La contribución principal de SATAN en su novedosa visión de la seguridad, la cual considera que la mejor forma de que un administrador puede asegurarla en su sistema es mediante la consideración de como un hacker trataría de introducirse. Mediante el uso de SATAN un hacker de cualquier parte del mundo puede verificar cada sistema en red de internet. Estos potenciales intrusos no tienen que ser brillantes, dado que SATAN es fácil de usarse, ni tampoco deben tener una cuenta del sistema objetivo, o ser del mismo país, ya que intermedio ofrece la conectividad de todo mundo. Incluso los hackers no requieren conocer la existencia de los sistemas porque pueden usar como objetivo los rangos de red. Para administradores conscientes, SATAN permite establecer el grado de seguridad de los hosts en una red. Sin embargo, dado que cada intruso en el mundo puede identificar rápidamente los hosts vulnerables es necesario elevar los niveles de seguridad.

Las metas pensadas al diseñar SATAN son las siguientes:

- Usar el planteamiento tradicional del conjunto de herramientas UNIX para diseño de programas.
- Generar un producto disponible libremente.
- Investigar la seguridad de grandes redes.
- Crear la mejor herramienta de investigación de la seguridad en red .
- Descubrir tanta información de la red como sea posible sin ser destructivo .
- Investigar los servicios de internet disponibles.
- Descubrir los servicios mal configurados.
- Verificar los servicios que representan una vulnerabilidad para el sistema[32]

4.3.2 COPS (Computer Oracle and Password System)

El paquete COPS (sistema de contraseña y oráculo de computadora) fue desarrollado por Dan Farmer de la Universidad de Purdue. Es una herramienta de seguridad para administradores de sistema que permite examinar sistemas UNIX, con el fin de localizar un número conocido de debilidades y problemas de seguridad, alertando al administrador sobre ellas, en algunos casos puede corregir automáticamente estos problemas. Es un sistema modular, por cable, de auditoría de sistemas basado en una colección de scripts y programas en C, que puede utilizarse para evaluar el estado de seguridad de casi cualquier sistema UNIX. [32]

Entre las funcionalidades que tiene Cops podemos destacar.

- Chequeo de modos y permisos de los ficheros, directorios y dispositivos
- Palabras de paso pobres (en el caso que tengamos una herramienta como crack, la línea de chequeo de palabras de paso)
- Chequeo de contenido, formato y seguridad de los ficheros de "password" y "group"
- Chequeo de programas con root-SUID.
- Permisos de escritura sobre algunos ficheros de usuario como ".profile" y ".cshrc"
- Configuración de ftp "anonymous".
- Chequeo de algunos ficheros del sistema como "hosts.equiv", montajes de NFS[21] sin restricciones, "ftpusers", etc.

Incluye características para verificar contraseñas, archivos SUID[22] y SGID, programas protegidos y otros más.

4.3.3 CPM (Verificando el modo promiscuo)

(Check Promiscuos Mode)
El programa cpm de la Universidad de Carnegie Mellon verificar cualquier interfaz de red de un sistema para localizar alguna que trabajé en modo promiscuo, esto puede indicar que un hacker ha violado el sistema y ha iniciado un programa para entrometerse en los paquetes de red.[32]

4.3.4 IFSTATUS

El programa ifstatus de Dave Curry puede verificar también cualquier interface de red de un sistema para localizar alguna que trabajé en modo promiscuo, con la diferencia de estar diseñada para ser ejecutada por fuera del sistema.[32]

[21] NFS: Network File System. Capacidad del sistema operativo unix de compartir su estructura de directorios a través de una red.
[22] SUID: set user id.

4.3.5 ISS (Internet Security Scanner)

El programa del autor Christopher Klaus es un explorador de seguridad de multinivel del mismo tipo que SATAN, que verifica un sistema UNIX en búsqueda de un número conocido de huecos de seguridad, tales como los problemas en el sendmail, o una de compartición de archivos NFS configurada impropiamente. [32]

4.3.6 MERLÍN

Merlín fue desarrollado por CIAC[23] y es una herramienta para la administración y realce de las herramientas de seguridad existentes. Provee un front-end gráfico a muchas de las populares herramientas, tales como SPI, Tiger, COPS, Crack y Tripwire. Merlín permite que estas herramientas sean más fáciles de usar, mientras que el mismo tiempo extiende sus capacidades.[32]

4.3.7 INSPECTOR DEL PERFIL DE SEGURIDAD (SPI)

(Security Profile Inspector)

En inspector del perfil de seguridad fue desarrollado en el Centro de Tecnología de la Seguridad Computacionales CSTC, para proveer una suite de inspecciones de seguridad para la mayoría de los sistemas UNIX con sólo tocar un botón. El producto de software SPI está disponible libre de costo para toda organización, la cual puede definir las políticas de redistribución a sus propias comunidades de usuarios.[32]

4.3.8 TIPWIRE

Este paquete de la Universidad de Purdue verifica los sistemas de archivos, y así poder usar las verificaciones de aquellos registros para descubrir cualquier cambio.[32]

[23] CIAC: Computer Incident Advisory Capability (capacidad de asesoría en incidentes de computadoras).

4.3.9 EL TIGRE (TIGER)

Es un paquete de scripts para monitorear de sistemas y de su seguridad. Es similar al COPS pero significativamente más actualizado, fácil de configurar y usar. Con él es posible construir una barrera de protección o detectar señales de ataque.[32]

Entre la información que chequea el programa tenemos.

- Configuración del sistema.
- Sistemas de ficheros.
- Ficheros de configuración de usuario.
- Chequeo de caminos de búsqueda.
- Chequeos de cuentas.
- Chequeos de alias.
- Comprueba la configuración de ftp "anonymous".
- Chequeo scripts de cron.
- NFS.
- Chequeo de servicios en el fichero /etc/inetd.conf
- Chequeo de algunos ficheros de usuario (.netrc, .rhosts, .profile, etc)
- Comprobación ficheros binarios (firmas). Para poder chequear éstos es necesario disponer de fichero de firmas.

4.3.10 OBSERVADOR (WATCHER)

Este paquete de Kenneth Ingham es una herramienta de monitoreo de sistemas expandible que verifica un número de comandos especificados por el usuario, analizando la salida, localizando elementos significativos y reportando estos al administrador del sistema.[32]

CAPITULO

5

CASO DE ESTUDIO: SEGURIDAD EN WINDOWS XP PROFESIONAL

RESUMEN:

En este último capítulo se presenta que es un sistema operativo en red, y el caso de estudio enfocado a windows XP, en cuestión a la seguridad que ofrece este sistema operativo en red, como la descripción de sus funciones para la seguridad, los servicios, las restricciones de usuarios no autorizados, el funcionamiento del firewall de conexión a internet que se incluye en esta versión de windows, el uso de políticas de restricciones de software y los diferentes tipos de dichas políticas, el soportes de tarjetas inteligentes (usando NIP's), el uso de Kerberos y para finalizar se hace un comparativo de Windows XP Profesional, con otras versiones anteriores a ella, en cuanto en confiabilidad, seguridad, su rendimiento y ha su facilidad de uso

5.1 DEFINICIÓN DE SISTEMA OPERATIVO EN RED.

Son aquellos sistemas que mantienen a dos o más computadoras unidas a través de algún medio de comunicación (físico o no), con el objetivo primordial de poder compartir los diferentes recursos y la información del sistema.[33]

5.2 SEGURIDAD CORPORATIVA

Windows XP Professional ofrece funciones robustas de seguridad para ayudar a los negocios a proteger los datos sensibles y ofrecer soporte para los usuarios de administración en la red. Una de las excelentes funciones disponibles en Windows XP Professional es el uso de objetos de Políticas de grupo (GPO). GPOs permite a los administradores del sistema aplicar un perfil único de seguridad para múltiples computadoras y utilizar de manera opcional tecnología de tarjeta inteligente para autenticar a los usuarios al utilizar información almacenada en una tarjeta inteligente. [34]

5.2.1 MEJORAS EN LA SEGURIDAD

Windows XP Professional incluye un número de funciones que las organizaciones pueden utilizar para proteger archivos, aplicaciones y otros recursos. Estas funciones incluyen Listas de control de acceso (ACLs), grupos de seguridad y Políticas de grupo, además de las herramientas que permiten a las organizaciones configurar y administrar estas funciones.

Windows XP ofrece cientos de configuraciones relacionadas con la seguridad que se pueden implementar individualmente. El sistema operativo Windows XP también incluye plantillas predefinidas de seguridad, las que pueden implementar las organizaciones sin necesidad de hacer modificaciones o utilizarlas como la base de una configuración de seguridad más personalizada. Las organizaciones pueden aplicar estas plantillas de seguridad cuando:

- Creen un recurso, tal como una carpeta o archivo compartido, y ya sea que acepten las configuraciones de lista de control de acceso por predeterminación o implementen configuraciones de listas de control de acceso personalizado.

- Coloquen usuarios en los grupos de seguridad estándar, tales como Usuarios, Usuarios avanzados y Administradores, y acepten las configuraciones ACL predeterminadas que aplican a dichos grupos de seguridad.
- Utilicen las plantillas de Políticas de grupo Básica, Compatible, Segura y Altamente segura que se han incluido con el sistema operativo.[34]

5.3 ACCESO CONTROLADO A LA RED

Windows XP ofrece seguridad integrada para mantener alejados a los intrusos. Esto se realiza al limitar a cualquiera que trate de tener acceso a su computadora de una red hacia los privilegios del nivel "huésped". Si los intrusos tratan de pasar a su computadora y obtener privilegios no autorizados tratando de adivinar las contraseñas, no tendrán éxito u obtendrán únicamente acceso de nivel huésped limitado.[34]

5.3.1 ADMINISTRACIÓN DE LA AUTENTICACIÓN DE LA RED

Un número cada vez mayor de sistemas basados en Windows XP Professional están conectados directamente a la Internet más que a los dominios. Esto hace que la administración adecuada del control de acceso (incluyendo contraseñas duras y permisos asociados con diferentes cuentas), sea más importante que nunca antes. Para asegurar la seguridad, necesita personalizar las configuraciones de control de acceso relativamente anónimas comúnmente asociadas con ambientes abiertos de Internet.

Como resultado, las funciones predeterminadas en Windows XP Professional requieren que todos los usuarios se conecten en la red para utilizar la cuenta Huésped. Este cambio está designado para evitar que los piratas traten de tener acceso a un sistema a través del Internet al conectarse utilizando una cuenta local de Administrador que no tiene contraseña.[34]

5.4 Uso compartido simple

Por predeterminación, en los sistemas Windows XP Professional que no están conectados a un dominio, todos los intentos para conectarse a través de la red estarán forzados a utilizar la cuenta Huésped. Además, en las computadoras que utilizan un modelo de seguridad de uso compartido simple, el cuadro de diálogo Propiedades de seguridad se reemplaza por un cuadro de diálogo simplificado Propiedades de documentos compartidos.[34]

5.4.1 HUÉSPED FORZADO

El modelo de uso compartido y seguridad para cuentas locales, le permite elegir entre el modelo de seguridad únicamente para Huésped o el modelo de seguridad Clásico. En el modelo únicamente para Huésped, todos los intentos para conectarse a la computadora local desde la red se verán obligados a utilizar la cuenta Huésped. En el modelo de seguridad Clásico, los usuarios que traten de conectarse a la computadora local desde la red se autenticarán con sus propios nombres. Esta política no aplica para computadoras que están unidas a un dominio. De otra manera, la función únicamente para Huésped se habilita por predeterminación.[34]

Si una cuenta Huésped está habilitada y tiene una contraseña en blanco, se permitirá conectarse y tener acceso solo a los recursos autorizados.

5.5 SISTEMA DE ENCRIPTACIÓN DE ARCHIVOS

La funcionalidad aumentada del Sistema de encriptación de archivos (EFS) ha mejorado de manera importante el poder de Windows XP Professional al ofrecer flexibilidad adicional para usuarios corporativos cuando implementan soluciones de seguridad basadas en archivos de datos encriptados.[34]

5.5.1 ARQUITECTURA EFS

EFS está basado en la encriptación de clave pública. La configuración predeterminada de EFS no requiere un esfuerzo administrativo, puede encriptar archivos inmediatamente. EFS genera automáticamente un par de claves de encriptación y un certificado para un usuario en caso de que éste no exista.

Si encripta una carpeta, todos los archivos y subcarpetas creados en ella, o agregados a la misma, se encriptan automáticamente. Se le recomienda encriptar al nivel de carpeta para evitar que se creen archivos temporales de texto completo en el disco duro durante la conversión de archivos.[34]

5.5.2 EFS Y NTFS

El Sistema de archivo de encriptación (EFS) protege datos sensibles en archivos que se almacenan en el disco utilizando el sistema de archivo NTFS. EFS es la tecnología central para encriptar y desencriptar archivos almacenados en volúmenes NTFS. Únicamente el usuario que encripta un archivo protegido puede abrirlo y trabajar en él. Esto es especialmente útil para usuarios de computadoras móviles debido a que aun si alguien más logra tener acceso a una laptop que se ha perdido o que ha sido robada, no podrá tener acceso a ninguno de los archivos en el disco. Para Windows XP, EFS ahora funciona con Archivos y carpetas fuera de línea.[34]

5.5.3 MANTENER LA CONFIDENCIALIDAD DEL ARCHIVO

Las funciones de seguridad tales como la autenticación de registro o los permisos de archivo protegen los recursos de la red de acceso no autorizado. Sin embargo, cualquiera con acceso físico a una computadora, puede instalar un nuevo sistema operativo en esa computadora y sobrepasar la seguridad existente del sistema operativo. De esta manera, datos sensibles pueden quedar expuestos. Al encriptar archivos sensibles a través de EFS, agrega otro nivel de seguridad. Cuando los archivos están encriptados, sus datos están protegidos aun cuando un atacante tenga acceso total al almacén de datos de la computadora. [34]

Únicamente los usuarios autorizados y los agentes de recuperación de datos designados, pueden desencriptar y encriptar archivos. La Figura 5.1 muestra en dónde podría crear configuraciones para EFS.

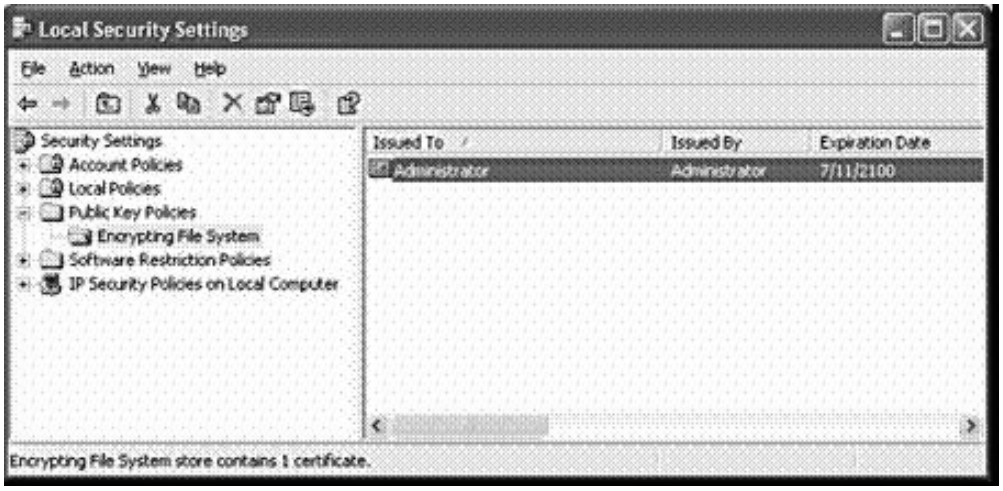

Fig. 5.1 Configuraciones de seguridad local EFS

5.5.4 FUNCIONAMIENTO DE EFS

EFS le permite almacenar información confidencial acerca de una computadora cuando las personas que tienen acceso a ella, de otra manera podrían comprometer dicha información, de manera intencional o no intencional. EFS es especialmente útil para asegurar datos sensibles en computadoras portátiles o en computadoras compartidas por varios usuarios. Ambos tipos de sistemas son susceptibles de ataque por técnicas que evaden las restricciones de ACLs.

En un sistema compartido, un atacante puede tener acceso al iniciar un sistema operativo diferente. Un atacante también puede robar una computadora, quitar el disco duro, colocar el disco duro en otro sistema y obtener acceso a los archivos almacenados. Los archivos encriptados a través de EFS, sin embargo, aparecen como caracteres ilegibles cuando el atacante no tiene la clave de desencriptación. Debido a que EFS está estrechamente integrado con NTFS, la encriptación y desencriptación se realizan de manera transparente. Cuando abre un archivo, EFS lo desencripta mientras se lee la información del disco. Cuando guarda el archivo, EFS encripta los datos mientras se escriben al disco. Como usuario no autorizado

incluso puede no darse cuenta que los archivos están encriptados debido a que puede trabajar con ellos en la manera en que siempre lo hace. [34]

5.5.5 ARCHIVOS ENCRIPTABLES

Los archivos individuales y las carpetas de archivo (o subcarpetas) en volúmenes NTFS se pueden establecer con el atributo de encriptación. Aunque es común referirse a las carpetas de archivo con el conjunto de atributos de encriptación como “encriptado”, la carpeta por sí misma no está encriptada, y no se requiere ningún par de claves públicas-privadas para establecer el atributo de encriptación para una carpeta de archivo. Cuando la encriptación se establece para una carpeta, EFS automáticamente encripta lo siguiente:[34]

- Todos los archivos nuevos creados en la carpeta.
- Todos los archivos de texto completo que se copien o se muevan a la carpeta.
- De manera opcional, todos los archivos y subcarpetas existentes.

5.5.6 ENCRIPTACIÓN DE ARCHIVOS FUERA DE LÍNEA

Esta es una tecnología de administración que permite a los usuarios de la red acceder a los archivos en uso compartido de la red aun cuando la computadora del cliente esté desconectada de la red. Cuando se desconectan de la red, los usuarios móviles pueden seguir explorando, leyendo y editando archivos debido a que han realizado el caché en la computadora del cliente. Cuando el usuario posteriormente se conecta al servidor, el sistema reconcilia los cambios con el servidor. [34]

5.5.7 ENCRIPTACIÓN DE LA BASE DE DATOS DE ARCHIVOS FUERA DE LÍNEA

Windows XP ofrece la opción de encriptar la base de datos de los Archivos fuera de línea para salvaguardar contra robo todos los documentos con caché local, mientras que al mismo tiempo ofrece seguridad adicional a sus datos con caché local. Por ejemplo, el usuario puede utilizar archivos fuera de línea mientras mantiene sus datos sensibles seguros. Si es un administrador en informática

puede utilizar esta función para salvaguardar todos los documentos con caché local. Los Archivos fuera de línea son una salvaguarda excelente si su computadora móvil con datos confidenciales guardados en el caché de Archivos fuera de línea se llega a perder o se la roban.

Esta función soporta la encriptación y desencriptación de la base de datos completa fuera de línea. Se requieren privilegios administrativos para configurar la manera en que se encriptarán los archivos fuera de línea. Para encriptar archivos fuera de línea, vaya a Opciones de carpeta en Herramientas en Mi computadora y verifique Encriptar Archivos fuera de línea para asegurar los datos en la pestaña Vea la Figura 5.2 para ver las opciones para encriptar la base de datos de Archivos fuera de línea.[34]

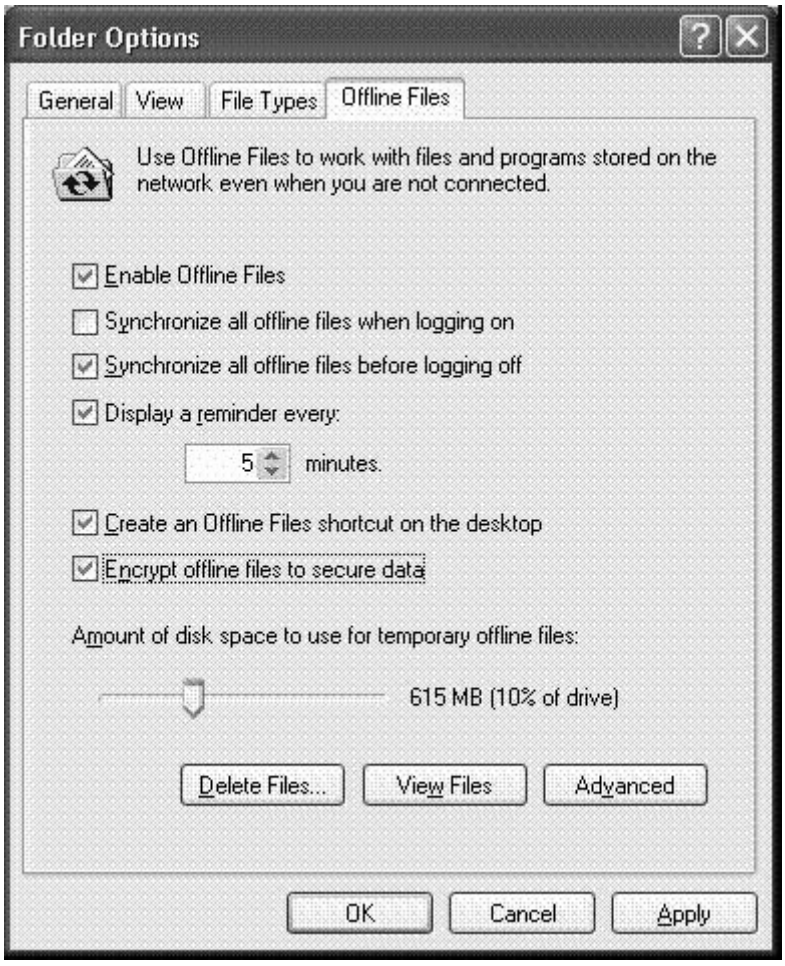

Fig. 5.2 Encriptación de base de datos de Archivos fuera de línea

5.6 SERVICIOS DE CERTIFICADO

Servicios de certificado forman parte central del sistema operativo que permite a los negocios actuar como su propia autoridad de certificación (CA), y emitir y administrar certificados digitales. Windows XP Professional soporta diferentes niveles de una jerarquía CA y una red de confianza de certificado cruzado: Esto incluye autoridades de certificado en línea y fuera de línea.[34]

5.6.1 ALMACENAMIENTO DE CERTIFICADO Y CLAVE PÚBLICA

Windows XP Professional almacena sus certificados de clave pública en un almacén personal de certificados. Los certificados se almacenan como texto completo debido a que son información pública, y están firmados digitalmente por autoridades de certificación para protegerlos contra el uso no autorizado.

Los certificados de usuario se localizan en Documentos y Configuraciones\nombre del usuario\Datos de aplicación\ Microsoft\SystemCertificates\My\Certificates para cada perfil de usuario. Estos certificados se escriben en el almacén personal en el registro de sistema cada vez que se conecta a su computadora. Para perfiles roaming, sus certificados se pueden almacenar en cualquier parte y lo seguirán cuando se conecte en las diferentes computadoras en el dominio.[34]

5.6.2 ALMACÉN DE CLAVE PRIVADA

Las claves privadas para los proveedores de servicio criptográfico basadas en Microsoft (CSPs), incluyen el CSP básico y el CSP mejorado, se ubican en el perfil del usuario como Directorio raíz\Documentos y Configuraciones\nombre de usuario\Datos de aplicación\Microsoft\Crypto\RSA.

En el caso de un perfil de usuario roaming, la clave privada reside en la carpeta RSA en el controlador de dominio y se descarga a su computadora, en donde permanece hasta que usted se desconecta o la computadora se vuelve a iniciar.

Debido a que las claves privadas deben estar protegidas, todos los archivos en la carpeta RSA automáticamente se encriptan con una clave simétrica y aleatoria llamada la clave maestra del usuario. La clave maestra del usuario tiene 64 bytes de longitud y se genera por medio de un generador robusto de números aleatorios

Las claves 3DES se derivan de la clave maestra y se utiliza para proteger las claves privadas. La clave maestra se genera automáticamente y se renueva con frecuencia.[34]

5.6.3 REQUISITOS Y RENOVACIÓN DEL CERTIFICADO PENDIENTE

La autosuscripción del usuario en Windows XP Professional soporta las funciones de solicitud y renovación de certificado pendiente. Puede solicitar manual o automáticamente un certificado de un Windows .NET Server CA. Esta solicitud permanece vigente hasta que se recibe una aprobación administrativa o hasta que se completa el proceso de verificación. Una vez que el certificado se ha emitido o aprobado, el proceso de autosuscripción completará e instalará sus certificados automáticamente.

La Figura 5.3 muestra algunas de las opciones disponibles para configuración de su autosuscripción de certificados.

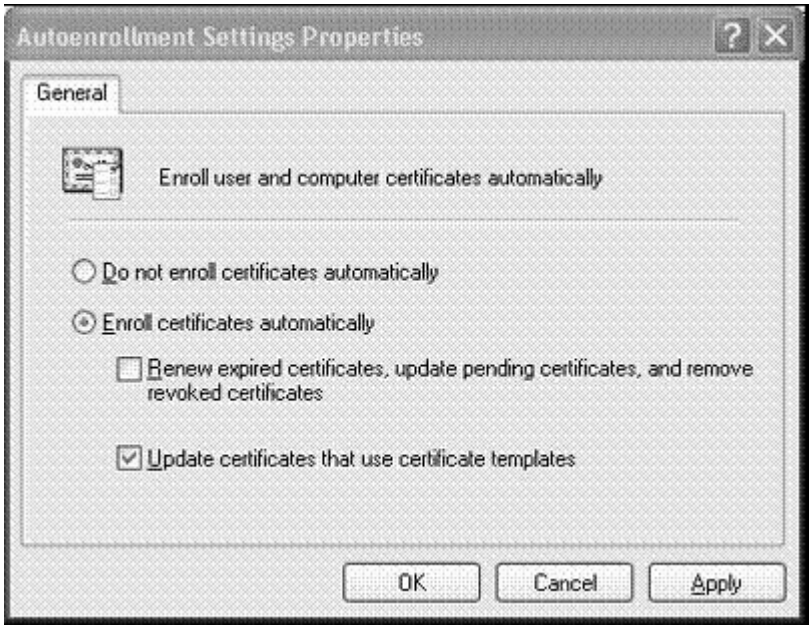

Fig. 5.3 Propiedades de configuraciones de autosuscripción

5.7 ADMINISTRADOR DE CREDENCIALES

La Administración de credenciales en Windows XP tiene tres componentes: interfaz de aparición súbita de la credencial, nombres de usuarios y contraseñas almacenados, y el keyring (anillo de clave). Juntos, estos tres componentes crean una solución única de registro.[34]

5.7.1 APARICIÓN SÚBITA DE LA CREDENCIAL

La interfaz de aparición súbita de credenciales la muestra una aplicación cuando el paquete de autenticación devuelve un error de autenticación. (Esto aplica únicamente para aplicaciones que tienen implementada la interfaz). Desde el cuadro de diálogo puede escribir un nombre de usuario y contraseña, o seleccionar un certificado X.509 del objeto Mi almacén. La aplicación también tiene la opción de mostrar el cuadro Recordar mi contraseña, el cual le permite guardar su credencial para un uso posterior.

Únicamente los paquetes de autenticación integrada (por ejemplo, protocolo Kerberos, NTLM, SSL y así sucesivamente) permiten que se guarden las credenciales. Para la autenticación básica seguirá apareciendo la interfaz de aparición súbita de las credenciales, pero no tendrá la opción de guardar su credencial. Vea la Figura 5.4 para un ejemplo de la interfaz de aparición súbita de credenciales.

Fig. 5.4 Indicador de la interfaz de aparición súbita de credenciales

5.7.2 NOMBRES DE USUARIOS Y CONTRASEÑAS ALMACENADOS

Nombres de usuarios y contraseñas almacenadas es el almacén de roaming seguro en donde se mantienen sus credenciales guardadas. El acceso a las credenciales está controlado por las Configuraciones de seguridad local (LSA). Las credenciales se almacenan basándose en la Información objetivo que devolvió la fuente. Cuando la credencial se guarda al marcar Recordar mi contraseña en la interfaz de aparición súbita de credenciales, la credencial se guardará en la forma más general posible. Por ejemplo, si estaba teniendo acceso a un servidor específico en un dominio, la credencial podría guardarse como “domain.com”. Al guardar una credencial diferente para un servidor diferente en este dominio, evita que se sobrescriba esta credencial.

Cuando un recurso se accede a través de un paquete de autenticación integrado, el paquete de autenticación buscará en los nombres de usuarios y contraseñas almacenados para una credencial más específica que se ajuste a la Información objetivo que devolvió la fuente. Si se encuentra alguna, el paquete de autenticación utilizará la credencial sin ninguna interacción de su parte. Si no se encuentra una credencial, se regresará un error de autenticación a la aplicación que trató de acceder a ese recurso.

Vea las Figuras 5.5, 5.6, y 5.7 para ejemplos de interfaces de administración de contraseña.[34]

Fig. 5.5 Interfaz clásica de administración de contraseña (Windows XP Professional en un dominio)

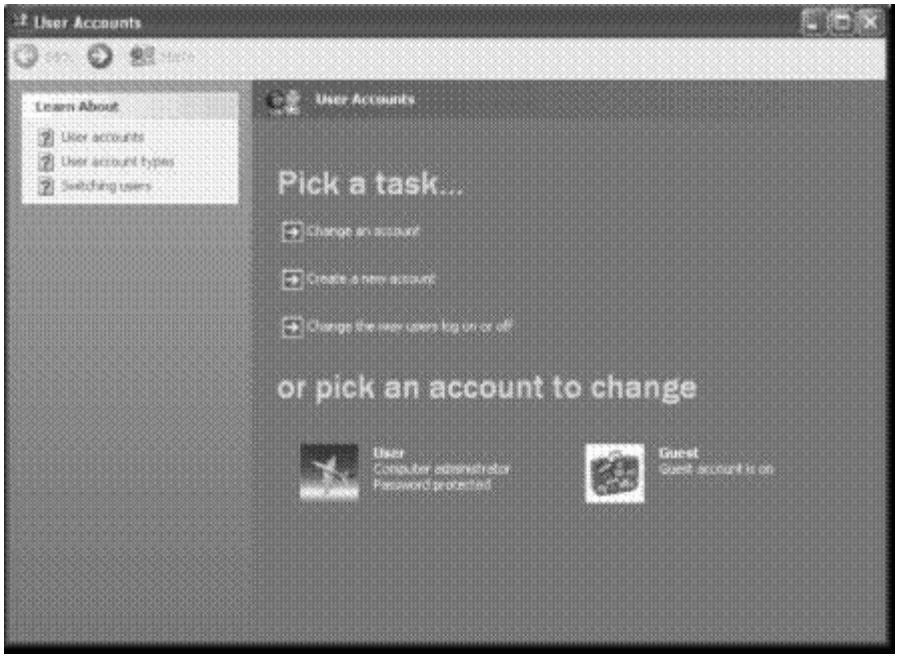

Fig. 5.6 Interfaz amigable de administración de contraseña (Windows XP Home Edition y Windows XP Professional en un grupo de trabajo).

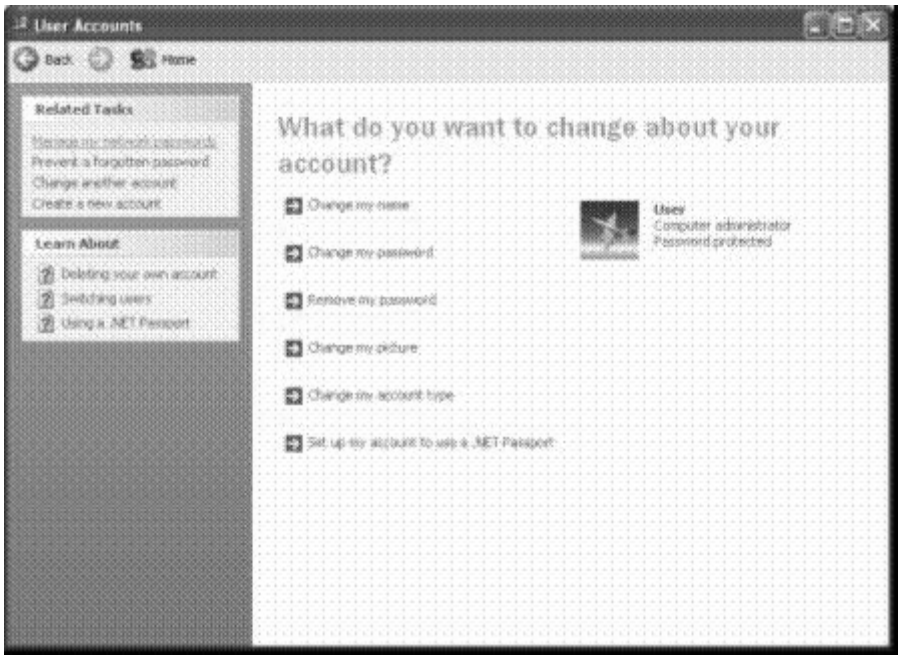

Fig. 5.7 Interfaz amigable de administración de contraseña (Windows XP Home Edition y Windows XP Professional en un grupo de trabajo)

5.7.3 KEYRING

El keyring (anillo para clave) le permite administrar manualmente las credenciales que están almacenadas que están en nombres de usuarios y contraseñas almacenadas. Se tiene acceso al keyring a través de la aplicación elemental del Panel de control de las cuentas del usuario.

En el keyring verá una lista de todas las credenciales que están actualmente en los nombres de usuarios y contraseñas almacenados. Cuando se selecciona cada credencial, un campo de descripción en la parte inferior presentará una breve descripción de la credencial. Desde ahí, puede agregar una nueva credencial, editar una credencial existente o eliminar una credencial existente.

- Agregar una credencial. Para agregar una credencial, aparecerá una interfaz similar a la interfaz de aparición súbita de la credencial, y necesitará llenar la Información objetivo. Recuerde que la información objetivo puede aceptar comodines en la forma de “*”.

- Editar una credencial. Editar una credencial le permite cambiar la información objetivo de las credenciales en sí mismas. Si es una credencial de nombre de usuario y/o contraseña, puede cambiar la contraseña en el servidor desde aquí. No podrá utilizar la interfaz de aparición súbita de las credenciales para editar credenciales que se hayan creado específicamente por una aplicación. Por ejemplo, no puede editar credenciales de pasaporte.
- Eliminar una credencial. Puede eliminar cualquier credencial.

La capacidad para guardar credenciales en nombres de usuarios y contraseñas almacenados se puede alternar entre activada y desactivada a través de las Políticas de grupo.[34]

5.8 FIREWALL DE CONEXIÓN A INTERNET

El Firewall de conexión a Internet (ICF) en Windows XP Professional ofrece a los escritorios y computadoras móviles protección de las amenazas de seguridad cuando utilizan DSL, módem de cable, o conexiones por módem de marcación a un Proveedor de servicio de Internet (ISP).[34]

5.8.1 FUNCIONAMIENTO DE ICF

El ICF funciona como un filtro de paquete estable que utiliza tecnología compartida con ICS. Aunque la función ICF es independiente, también puede ejecutarla en un adaptador compartido para proteger su red en el hogar.

Cuando está habilitado, este filtro estable bloquea todas las conexiones no solicitadas que se originan en la interfaz de red pública. Para lograr esto, el ICF utiliza la tabla de flujo Traducción de dirección de red (NAT) y valida cualquier flujo de entrada contra las entradas en la tabla de flujo NAT. Los flujos de datos de entrada sólo se permiten si hay una tabla de flujo NAT existente correlacionando aquellos datos que se originan en el sistema firewall o dentro de la red protegida interna. En otras palabras, si la comunicación en red no se origina dentro de la red protegida, los datos de entrada serán rechazados.[34]

Cuando utiliza el ICF en Windows XP Professional puede estar seguro de que los atacantes no podrán escanear sus sistemas o conectarse a sus recursos. El firewall dificultará la configuración de su sistema para que funcione como un servidor para otros a través de Internet.[34]

5.8.2 CONFIGURACIONES DE POLÍTICAS DE GRUPO RELACIONADAS CON LA SEGURIDAD

Windows XP incluye plantillas de seguridad, colecciones preconfiguradas de políticas relacionadas con seguridad que se pueden utilizar para asegurar el nivel adecuado de seguridad en las estaciones de trabajo. Estas plantillas representan configuraciones de seguridad estándar bajas, medias y altas, y se pueden personalizar para cumplir las necesidades de seguridad específicas.

También puede establecer políticas de seguridad para artículos de administración de contraseña, tales como:[34]

- ♠ Determinar longitudes mínimas de contraseña.
- ♠ Establecer el intervalo entre los cambios de contraseña requeridos.
- ♠ Controlar el acceso a recursos y datos.

5.9 POLÍTICAS DE RESTRICCIÓN DE SOFTWARE

Las políticas de restricción de software ofrecen a los administradores un mecanismo controlado por políticas que identifica el software que se ejecuta en su dominio y controla la capacidad para ejecutar de ese software. Al utilizar una política de restricción de software, un administrador puede evitar aplicaciones no deseadas de la ejecución; esto incluye virus y caballos de Troya, u otro software que es conocido por causar problemas cuando se instala.[34]

5.9.1 USO DE POLÍTICAS PARA RESTRICCIÓN DE SOFTWARE

Si es un administrador, puede utilizar una política de restricción de software para limitar la ejecución a un conjunto de aplicaciones confiables. Las aplicaciones se presentan a la política por medio de la ruta de acceso de archivo. Una vez que se ha identificado, el sistema hace cumplir las políticas establecidas por el administrador.

Las políticas de restricción de software también ayudan a proteger en contra de virus basados en script y caballos de Troya. Un administrador puede configurar una política de restricción de software para permitir que se ejecuten únicamente los scripts autorizados por un miembro de la organización de informática. Esto evita todos los virus basados en script, tales como ILOVEYOU.VBS. Las políticas de restricción de software también se pueden utilizar para regular qué aplicaciones se pueden instalar los usuarios en sus computadoras.[34]

5.9.2 CREACIÓN DE UNA POLÍTICA DE RESTRICCIÓN DE SOFTWARE

Una política está formada por una regla predeterminada acerca de qué programas están permitidos para ejecución y las excepciones a dicha regla. La regla predeterminada se puede establecer como no restringida o no permitida — esencialmente “ejecutar” o “no ejecutar”. Al establecer la regla predeterminada como “no restringida” el administrador puede definir las excepciones que son justamente el conjunto de programas que está prohibido ejecutar. Un enfoque más seguro tiene que ver con la configuración de reglas predeterminadas como no permitidas, y especifica únicamente los programas que son conocidos y confiables para ejecutarse.[34]

5.9.3 DOS TIPOS DE POLÍTICAS DE RESTRICCIÓN DE SOFTWARE

Hay dos maneras para utilizar las políticas de restricción de software. Si los administradores han identificado todo el software que debería permitirse para ejecutar, pueden utilizar una política de restricción de software para limitar la ejecución únicamente a aquella lista de aplicaciones confiables. Si los administradores no saben acerca de todas las aplicaciones que sus usuarios ejecutarán, tendrán que ser reactivos y restringir las aplicaciones no adecuadas en la medida en que se identifiquen.

Las políticas de restricción de software se pueden aplicar en los siguientes escenarios:

- ♠ Permitir únicamente la ejecución de código confiable. Si se pueden identificar todos los códigos confiables, el administrador puede bloquear el sistema de manera eficiente.

Un ejemplo de esta política sería una computadora en donde únicamente cierto software de aplicación se ejecutará, y los usuarios no pueden instalar otro software en la computadora. Un administrador puede crear una política en donde únicamente se permita ejecutar Microsoft Word y Microsoft Excel en la computadora. Si el usuario descarga un programa o ejecuta un programa desde un disco flexible, no podrá ejecutarlo, debido a que no se encuentra en la lista de programas confiables definida por la política.

- Evitar la ejecución de código no deseado. En algunos casos un administrador no puede predecir la lista completa del software que los usuarios necesitarán ejecutar. En estos casos, el administrador únicamente puede reaccionar e identificar los códigos no deseados en la medida en que se enfrenta con ellos. Las compañías con clientes administrados relajadamente entrarían en este modelo.

Por ejemplo, si el administrador se da cuenta de que muchos usuarios están ejecutando aplicaciones de archivo compartido y creando una fuga en el ancho de banda de la red, el administrador puede crear una regla que identifique el programa de uso compartido de archivos y evitar que se ejecute. Si los usuarios instalan un programa que se sabe causa problemas con el software existente, el administrador puede crear una regla que identifique el programa instalado de ese software y evitar que se instale.[34]

Vea la Figura 5.8 para una presentación de configuraciones de política de restricción de software.

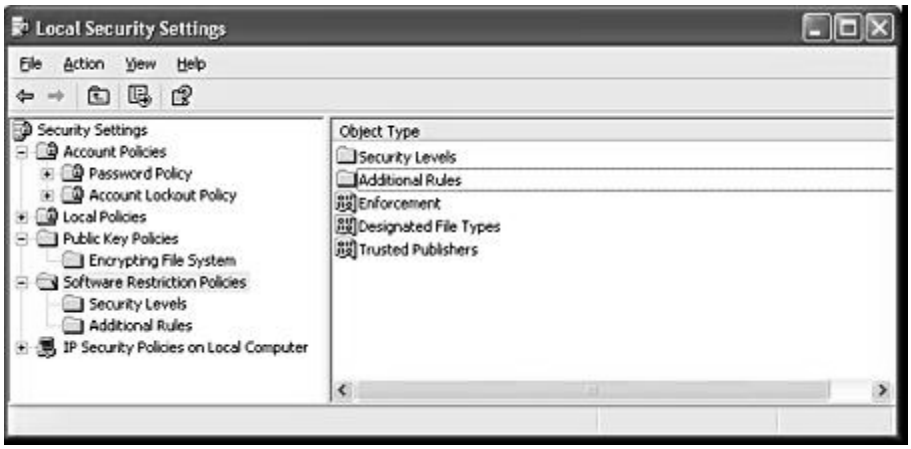

Fig. 5.8 políticas de restricción de software—Configuraciones de seguridad local

5.9.4 CONTROL DE SOFTWARE FIRMADO DIGITALMENTE

Las políticas de restricción de software mejoran la capacidad de administrador para controlar el software firmado digitalmente de las siguiente maneras:

- Limitar controles Microsoft ActiveX. Un administrador puede especificar los controles ActiveX que se ejecutarán en Internet Explorer para un dominio en particular al utilizar una política de restricción de software que se encuentre en la lista confiable de certificados del editor de software. Si el editor de un control ActiveX está en la lista de editor confiable, su software automáticamente se ejecuta al momento de descargarlo. Una política de restricción de software también puede hacer una lista de editores no permitidos. Esto evita automáticamente que los controles ActiveX firmados por dichos editores se ejecuten.

Al utilizar una política de restricción de software, también es posible controlar quién puede tomar una decisión confiable acerca de un editor no conocido—un editor que no está explícitamente en la lista de confiable o no confiable. Las políticas de restricción de software se pueden establecer para permitir únicamente que administradores locales, o administradores de dominio, decidan qué editores son confiables, y evitar que los usuarios tomen dichas decisiones. [34]

- Uso del Windows Installer. Los programas instalados con el uso de Windows Installer se pueden firmar digitalmente. Al utilizar una política de restricción de software, un administrador puede solicitar que únicamente se instale el software firmado digitalmente por ciertos editores de software. Windows Installer verificará que una firma aprobada esté presente antes de instalar el software en la computadora.
- Uso de Microsoft Visual Basic® Script. Los archivos de Visual Basic Script se pueden firmar digitalmente. Un administrador puede configurar una política de restricción de software para que los archivos de Visual Basic Script (.vbs) tengan que ser firmados digitalmente por editores de software autorizados antes de que se ejecuten.

5.10 SEGURIDAD DE PROTOCOLO EN INTERNET (IPSEC)

La necesidad de seguridad en red basada en IP es casi universal en el mundo empresarial interconectado actual de Internet, intranets, sucursales y acceso remoto. Debido a que la información sensible constantemente cruza las redes, el reto para los administradores de red y otros profesionales de servicio de información es asegurar que este tráfico esté:

- Seguro de la modificación de datos mientras está en tránsito.
- Seguro contra intercepción, consulta o copiado.
- Seguro de ser usurpado por partes no autorizadas.
- Seguro de ser capturado y reproducido posteriormente para obtener acceso a recursos sensibles. Por lo general, una contraseña encriptada se puede utilizar de esta manera.

Estos servicios de seguridad se conocen como integridad de datos, confidencialidad de datos, autenticación de datos y protección de reproducción.

Algunos ataques son pasivos, lo que significa, que la información simplemente es monitoreada. Otros son activos, lo que significa que la información se altera con la intención de dañar o destruir la información o la red misma.

La Tabla 5.1 muestra algunos riesgos de seguridad comunes encontrados en las redes actuales, y como utilizar IPSec para evitarlos.

Tipo de ataque	Descripción	Cómo IPSec evita el ataque
Husmear (también llamado sniffing, snooping)	Monitoreo de texto completo o paquetes no encriptados.	Los datos se encriptan antes de la transmisión, evitando el acceso a los datos originales aun si el paquete es monitoreado o interceptado. Únicamente los iguales conocen la clave de encriptación.
Modificación de datos	Alteración y transmisión de paquetes modificados.	El código de control de los datos se anexa a una suma de verificación criptográfica para cada paquete, el cual es revisado por la computadora receptora para detectar cualquier modificación.
Spoofing de identidad	Uso de paquetes construidos o capturados para asumir falsamente la identidad de una dirección válida.	El protocolo Kerberos versión 5, certificados de clave pública, o las claves precompartidas autentican a iguales antes de que inicie la comunicación segura.
Negación de servicio	Evitar el acceso a la red por usuarios válidos. Un ejemplo es inundar la red con tráfico de paquetes.	Los puertos o protocolos se pueden bloquear.
Hombre en medio	Desviación de paquetes IP a un tercero no intencionado, para que se monitoree y posiblemente se altere.	Autenticación de iguales.
Clave conocida	Se utiliza para desencriptar o monitorear o modificar datos.	En Windows XP Professional, las claves criptográficas se refrescan continuamente, reduciendo la posibilidad de que una clave capturada se pueda utilizar para obtener acceso a información segura.
Ataque en nivel de aplicación	Principalmente dirigido a servidores de aplicación, este ataque se utiliza para causar una falla en un sistema operativo de una red o aplicaciones, o para introducir miembros en la red.	Debido a que IPSec se implementa en una capa en la red, los paquetes que no cumplen con los filtros de seguridad en este nivel nunca pasan a las aplicaciones, protegiendo a las aplicaciones y los sistemas operativos.

Tabla 5.1 Tipos de ataques en la red y cómo evitarlos utilizando IPSec

5.11 SOPORTE A TARJETAS INTELIGENTES

Una tarjeta inteligente es una tarjeta de circuito integrada (ICC) aproximadamente del tamaño de una tarjeta de crédito. Puede utilizarla para almacenar certificados y claves privadas y para llevar a cabo operaciones de criptografía de clave pública tales como la autenticación, la firma digital y el intercambio de claves.

Una tarjeta inteligente mejora la seguridad de las siguientes maneras:

- Ofrece almacenamiento resistente al saboteo para claves privadas y otras formas de identificación personal.
- Aísla cálculos de seguridad críticos que tienen que ver con la autenticación, firmas digitales e intercambio de claves de las partes del sistema que no necesitan estos datos.
- Permite mover credenciales y otra información privada de una computadora a otra (por ejemplo, de una computadora de lugar de trabajo a una computadora remota o del hogar). [34]

5.11.1 UN NIP EN LUGAR DE UNA CONTRASEÑA

Una tarjeta inteligente utiliza un número de identificación personal (NIP) en lugar de una contraseña. La tarjeta inteligente está protegida del más mal uso por el NIP, el cual es seleccionado por el propietario de la tarjeta inteligente. Para utilizar la tarjeta inteligente, puede insertar la tarjeta en un lector de tarjeta inteligente anexo a una computadora, y después escribir el NIP.

Un NIP ofrece más protección que una contraseña de red estándar. Las contraseñas (o derivaciones, tales como los códigos de control) viajan a través de la red y son vulnerables ser interceptados. La fuerza de la contraseña depende de su tamaño, de que también esté protegida y de cuán difícil sea para un atacante adivinarla. Por el contrario, un NIP nunca viaja en la red. Además, las tarjetas inteligentes permiten un número limitado (por lo general de tres a cinco) de intentos fallidos para escribir la clave en el NIP correcto antes de que la tarjeta se bloquee por si misma. Después de que se logra este limite, aún si se escribe el NIP correcto esto no funcionará. El usuario puede ponerse en contacto con el administrador del sistema para desbloquear la tarjeta.[34]

5.12 PROTOCOLO DE AUTENTICACIÓN KERBEROS VERSIÓN 5

En Windows XP Professional, sus credenciales se pueden suministrar por medio de una contraseña, un ticket Kerberos, o una tarjeta inteligente si la computadora está equipada para manejar una tarjeta inteligente.

El protocolo Kerberos V5 ofrece los medios para autenticación mutua entre un cliente, tal como un usuario, computadora, u otro servicio y un servidor. Esta es una forma más eficiente para que los servidores autentiquen clientes, incluso en los ambientes de red más complejos y grandes.[34]

5.12.1 SUPUESTO DE KERBEROS

El protocolo Kerberos está basado en el supuesto de que las transacciones iniciales entre clientes y servidores se llevan a cabo en una red abierta. Este es un ambiente en el cual un usuario no autorizado puede actuar ya sea como un cliente o un servidor e interceptar o interferir con la comunicación entre clientes y servidores autorizados. La autenticación Kerberos V5 también ofrece una autenticación segura y eficiente para redes complejas de clientes y recursos.

El protocolo Kerberos versión 5 utiliza una encriptación de clave secreta para proteger las credenciales de registro que viajan a través de la red. La misma clave se puede utilizar para desencriptar esas credenciales en el extremo receptor. Esta desencriptación y los pasos subsiguientes se llevan a cabo por medio del Centro de distribución de clave Kerberos, el cual se ejecuta en todos los controladores de dominio como parte de Active Directory. [34]

5.12.2 AUTENTICADOR

Un autenticador es una pieza de información, tal como una estampa de tiempo, que es diferente cada vez que se genera, se incluye con las credenciales de registro encriptadas para verificar que las credenciales de autenticación previa no se reutilizaron. Un nuevo autenticador se genera y se incorpora con la respuesta encriptada de KDC al cliente para confirmar que el mensaje original se recibió y se aceptó. Si las credenciales de registro iniciales y el autenticador se aceptan, el KDC emite un ticket-granting ticket (TGT) que se utiliza por el LAS para obtener tickets de servicio. Estos tickets contienen datos encriptados que confirman su

identidad al servicio que solicitó. A excepción de la captura inicial de la contraseña o de las credenciales de tarjeta inteligente, el proceso de autenticación es transparente. [34]

Vea la Figura 5.9 para una demostración de las propiedades de regla de autenticación.

Fig. 5.9 Propiedades de regla de autenticación

5.13 COMPARACIÓN DE FUNCIONES CON OTROS SISTEMAS OPERATIVOS.

A continuación se presentan tablas comparativas de windows XP con versiones antecesoras en cuanto seguridad, rendimiento y factibilidad de uso.[35]

La simbología a utilizar es la siguiente:

○ indica una función parcial que no está disponible

□ indica una paridad parcial de la función con Windows XP.

● indica una función que tiene una paridad completa con Windows XP Profesional

La tabla 5.2 muestra una comparación con otros sistemas operativos en cuestión a confiabilidad.

Confiable					
Función	**Descripción**	**Windows 9x/Me**	**Windows NT 4.0**	**Windows 2000 Professional**	**Windows XP Professional**
	Windows XP Professional tiene como base el código comprobado de Windows NT® y Windows 2000, que presenta una arquitectura de cómputo de 32 bits, así como un modelo de memoria totalmente protegido.	○	□ Subcon-junto de funciones	□ Subconjunto de funciones	●
Verificador optimizado de drivers de dispositivos	Desarrollado con base en el verificador de drivers de dispositivos de Windows 2000, la versión de Windows XP Professional proporcionará pruebas más fuertes para drivers de dispositivos.	○	○	○	●
Escenarios de reinicio sustancialmente reducidos	Elimina la mayoría de los escenarios que obligaban a los usuarios finales a reiniciar en Windows NT 4.0 y Windows 9x. Así mismo, muchas de las instalaciones de software no requerirán de reinicio.	○	○	●	●
Protección de archivos de Windows	Windows XP Professional protege los archivos del sistema para que no los sobrescriban las instalaciones de las aplicaciones. En el caso de que se sobrescriba un archivo, la Protección de archivos de Windows lo reemplazará con la versión correcta.	○	○	●	●
Windows Installer	Servicios de un sistema que ayuda a los usuarios a instalar, configurar, dar seguimiento, actualizar y remover programas de software correctamente.	○	○	●	●
Políticas mejoradas de restricción de software	Windows XP Professional cuenta con políticas mejoradas para la restricción de software, que le proporcionan a los administradores un mecanismo basado en políticas para identificar software que se ejecute en su ambiente. Este recurso se puede usar para evitar virus y caballos de Troya, así como las interrupciones de software.	○	○	○	●

TABLA 5.2 COMPARACIÓN EN CONFIABILIDAD DE WINDOWS XP Y OTRAS VERSIONES.

La tabla 5.3 y 5.4 muestra las diferencias en rendimiento y seguridad de windows XP profesional con versiones anteriores.

Rendimiento					
Función	**Descripción**	**Windows 9x/Me**	**Windows NT 4.0**	**Windows 2000 Professional**	**Windows XP Professional**
Arquitectura de multitareas preventivas	Windows XP Professional está diseñado para permitir que varias aplicaciones se ejecuten simultáneamente, al tiempo que asegura un excelente tiempo de respuesta y estabilidad del sistema.	○	●	●	●
Memoria escalable y soporte de procesadores	Soporta hasta 4 GB de memoria y hasta dos multiprocesadores simétricos.	○	●	●	●

TABLA 5.3 DIFERENCIAS DE RENDIMIENTO DE WINDOWS XP CON OTRAS VERSIONES.

Seguridad					
Función	**Descripción**	**Windows 9x/Me**	**Windows NT 4.0**	**Windows 2000 Professional**	**Windows XP Professional**
Sistema encriptador de archivos (EFS) con soporte para multiusuarios	Encripta cada archivo con una clave generada aleatoriamente. Los procesos de encriptación y desencriptación son transparentes para el usuario. Con Windows XP Professional, EFS ahora soporta la capacidad de que varios usuarios tengan acceso a un documento encriptado.	○	○	□ No ofrece soporte para uso con múltiples usuarios	●
Seguridad IP (IPSec)	Ayuda a proteger los datos que se transmiten a través de una red. IPSec es parte importante, debido a que proporcionar seguridad para redes privadas virtuales (VPNs), que permiten a las organizaciones transmitir datos de manera segura por Internet.	○	○	●	●
Soporte de Kerberos	Proporciona autenticación de acuerdo con los estándares de la industria y con gran solidez para un registro rápido y único a los recursos corporativos basados en Windows 2000. Kerberos es un estándar de Internet, especialmente efectivo para redes que tienen distintos sistemas operativos, como UNIX.	○	○	●	●
Soporte para tarjetas inteligentes	Windows XP integra capacidades de tarjetas inteligentes en el s.o incluyendo soporte para el registro de Tarjetas inteligentes a sesiones de servidores de terminal alojadas en los servidores de terminal.	□ Subcon-junto de funciones	○	□ Subconjunto de funciones	●

TABLA 5.4 DIFERENCIAS DE WINDOWS XP CON OTRAS VERSIONES

La tabla 5.5 muestra el fácil uso de los sistemas operativo y sus diferencias.

Fácil de usar					
Función	Descripción	Windows 9x/Me	Windows NT 4.0	Windows 2000 Professional	Windows XP Professional
Diseño visual innovador y atractivo	Aunque mantiene los aspectos básicos de Windows 2000, Windows XP Professional cuenta ahora con un diseño visual innovador y atractivo. Se han consolidado y simplificado las tareas comunes y se han agregado nuevas entradas visuales para ayudar a los usuarios a navegar más fácilmente en sus computadoras. Los administradores de informática o los usuarios finales pueden escoger entre esta interfaz actualizada y la apariencia clásica de Windows 2000, mediante un solo clic.	○	○	○	●
Menúes de tareas sensibles al contexto	Cuando se selecciona un archivo en Explorer, aparece un menú dinámico. Este menú enumera las tareas que son apropiadas para el tipo de archivo seleccionado.	○	○	○	●
Grabador de CDs integrado	Windows XP Professional cuenta con soporte integrado para grabar CD-Rs y CD-RWs en Windows Explorer.	○	○	○	●
Publique información fácilmente en la Web	Los archivos y carpetas pueden publicarse fácilmente en cualquier servicio Web que utilice el protocolo WebDAV.	○	○	○	●
Localizadores de fallas	Ayuda a los usuarios finales y a los profesionales de informática a configurar, optimizar y resolver problemas de numerosas funcionalidades en Windows XP Professional.	□ Subconjunto de funciones	□ Subconjunto de funciones	□ Subconjunto de funciones	●

TABLA.5.5 COMPARATIVO EN CUANTO FACTIBILIDAD DE USO DE WINDOWS XP Y SUS VERSIONES ANTECESORAS.

CONCLUSIONES

El gran crecimiento que se tiene de las redes de computadoras ha sido mucho y por ello es que la seguridad también ha crecido a la par, día a día se trata buscar la mejor forma para estar protegidos, pero al mismo tiempo, en cuanto sale algún software o hardware, algunas personas, mejor conocidas como piratas informáticos, encuentran esos puntos débiles, que usando su ingenio, crean programas para destapar esas debilidades que existen en ellas. A pesar de todo esto, también hay herramientas de seguridad como los firewalls, los sistemas de protección como el kerberos, y la criptografía, que se van actualizando y tapan esos huecos que podían tener en sus versiones o generaciones anteriores, pero en si hay muchísimas herramientas de las cuales se pueden conseguir y usar.

Otro punto interesante y muy primordial, son las políticas de seguridad, de las cuales son realmente necesarias para algún tipo de organización, e inclusive para todos aquellos que estamos involucrados desde casa con nuestra pc, por medio de la red de redes, es decir, el internet, ya que los atacantes emplean métodos iguales o casi iguales, para cometer esos actos ilícitos. Y es bueno tener estas precauciones que nos ofrecen las políticas de seguridad, para que se tenga cuidado al realizar actividades que a veces se piensa que no puede causar ningún daño, pero, tal vez, es todo lo contrario.

En si, la seguridad no debería ser un problema, ni en las redes, ni en la vida cotidiana, pero como no se tiene una conciencia social, algunos humanos, ya sea por avaricia, por una curiosidad mala, por ambición, etc, pierden aquellos valores como generosidad, amabilidad, sencillez, etc, por el cual se debería vivir en armonía. Sin embargo, como eso no existe, solo queda buscar los medios para proteger lo que se quiere y necesita.

GLOSARIO

A

ACL: Lista mantenida por un router de Cisco para controlar el acceso desde o hacia un router para varios servicios (por ejemplo, para evitar que los paquetes con una dirección IP determinada salgan de una interfaz en particular del router). Ver también ACL extendida y ACL estándar.

ACL estándar: ACL que filtra basándose en la máscara y dirección origen. Las listas de acceso estándares autorizan o deniegan todo el conjunto de protocolos TCP/IP. Ver también ACL, ACL extendida.

ACL extendida: ACL que verifica las direcciones origen y destino. Comparar con ACL estándar.

ADMINISTRADOR DE RED: Persona a cargo de la operación, mantenimiento y administración de una red.

AUTENTICACIÓN : Con respecto a la seguridad, la verificación de la identidad de una persona o proceso.

APLICACIÓN CLIENTE/SERVIDOR: Aplicación que se almacena en una posición central en un servidor y a la que tienen acceso las estaciones de trabajo, lo que hace que sean fáciles de mantener y proteger.

B

BACKBONE: Núcleo estructural de la red, que conecta todos los componentes de la red de manera que se pueda producir la comunicación.

BROADCAST: Paquete de datos enviado a todos los nodos de una red. Los broadcasts se identifican por una dirección broadcast.

BUFFER (COLCHÓN): Memoria intermedia que se utiliza como memoria de datos temporal durante una sesión de trabajo.

BUG (BICHO, ERROR): Error en el hardware o en el software que, si bien no impide la ejecución de un programa, perjudica el rendimiento del mismo al no permitir la realización de determinadas tareas o al complicar su normal funcionamiento. Esta palabra también se utiliza para referirse a un intruso.

BÚFER DE MEMORIA: área de la memoria donde el switch almacena los datos destino y de transmisión.

C

CLAVE PRIVADA: Es la clave que tan sólo nosotros conocemos y que utilizamos para desencriptar el mensaje que nos envían encriptado con nuestra clave pública. Este sistema de clave pública y clave privada se conoce como sistema asimétrico.

CLAVE PÚBLICA: Es la clave que hacemos que esté al alcance de todo el mundo para que nos puedan enviar un mensaje encriptado. También con ella pueden desencriptar lo que les enviemos encriptado con nuestra clave privada.

CERTIFICADO X-509: es un documento digital que identifica de forma unívoca al remitente del mensaje transmitido y garantiza la integridad y privacidad de su contenido

D

DATAGRAMA : Agrupamiento lógico de información enviada como unidad de capa de red a través de un medio de transmisión sin establecer previamente un circuito virtual. Los datagramas IP son las unidades de información primaria de la Internet. Los términos celda, trama, mensaje, paquete y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

DHCP : Protocolo de configuración dinámica del Host. Protocolo que proporciona un mecanismo para asignar direcciones IP de forma dinámica, de modo que las direcciones se pueden reutilizar automáticamente cuando los hosts ya no las necesitan.

DIRECCIÓN MAC: Dirección de capa de enlace de datos estandarizada que se necesita para cada puerto o dispositivo que se conecta a una LAN. Otros dispositivos de la red usan estas direcciones para ubicar dispositivos específicos en la red y para crear y actualizar las tablas de enrutamiento y las estructuras de los datos. Las direcciones MAC tienen 6 bytes de largo, y son controladas por el IEEE. También se denominan direcciones de hardware, dirección de capa MAC o dirección física. Comparar con dirección de red.

E

ENCAPSULAMIENTO: Colocación en los datos de un encabezado de protocolo en particular. Por ejemplo, a los datos de capa superior se les coloca un encabezado específico de Ethernet antes de iniciar el tránsito de red. Además, al puentear redes que no son similares, toda la trama de una red se puede ubicar simplemente en el encabezado usado por el protocolo de capa de enlace de datos de la otra red.

ETHERNET: El método de conexión más común en las redes de área local, LANs. En el caso de Ethernet, todas las estaciones del segmento comparten el ancho de banda total, que es 10 megabits por segundo (Mbps), 100 Mbps para Fast Ethernet, o 1000 Mbps para Gigabit Ethernet.

F

FILTRO: En general, se refiere a un proceso o dispositivo que rastrea el tráfico de red en busca de determinadas características, por ejemplo, una dirección origen, dirección destino o protocolo y determina si debe enviar o descartar ese tráfico basándose en los criterios establecidos.

FIREWALL: Router o servidor de acceso, o varios routers o servidores de acceso, designados para funcionar como búfer entre redes de conexión pública y una red privada. Un router de firewall utiliza listas de acceso y otros métodos para garantizar la seguridad de la red privada.

FTP: Protocolo de aplicación, parte de la pila de protocolo TCP/IP, utilizado para transferir archivos entre nodos de red.

G

GATEWAY: En la comunidad IP, término antiguo que se refiere a un dispositivo de enrutamiento. Actualmente, el término router se utiliza para describir nodos que desempeñan esta función, y gateway se refiere a un dispositivo especial que realiza conversión de capa de aplicación de la información de una pila de protocolo a otro.

GUI: Entorno del usuario que utiliza representaciones gráficas y textuales de las aplicaciones de entrada y salida y de la estructura jerárquica (o de otro tipo) en la que se almacena la información. Las convenciones como botones, iconos y ventanas son típicas, y varias acciones se realizan mediante un apuntador (como un ratón). Microsoft Windows y Apple Macintosh son ejemplos importantes de plataformas que usan GUI.

H

HOST: Computador en una red. Similar a nodo, salvo que el host normalmente implica un computador, mientras que nodo generalmente se aplica a cualquier sistema de red, incluyendo servidores y routers.

HUB: Dispositivo de hardware o software que contiene múltiples módulos de red y equipos de red independientes pero conectados. Los hubs pueden ser activos (cuando repiten señales que se envían a través de ellos) o pasivos (cuando no repiten, sino que simplemente dividen las señales enviadas a través de ellos).

INTERNET: La internetwork de redes más grande del mundo, que conecta decenas de miles de redes de todo el mundo y con una cultura que se concentra en la investigación y estandarización basada en el uso real. Muchas tecnologías de avanzada provienen de la comunidad de la Internet. La Internet evolucionó en parte de ARPANET. En un determinado momento se la llamó Internet DARPA, y no debe confundirse con el término general internet.

INTRANET: Red propia de una organización, diseñada y desarrollada siguiendo los protocolos propios de Internet, en particular el protocolo TCP/IP. Puede tratarse de una red aislada, es decir no conectada a Internet.

ISO: Organización internacional que tiene a su cargo una amplia gama de estándares, incluyendo aquellos referidos al networking. ISO desarrolló el modelo de referencia OSI, un modelo popular de referencia de networking.

M

MAC: Parte de la capa de enlace de datos que incluye la dirección de 6 bytes (48 bits) del origen y del destino, y el método para obtener permiso para transmitir.

MODELO CLIENTE/SERVIDOR: Descripción común de los servicios de red y los procesos del usuario modelos (programas) de estos servicios. Los ejemplos incluyen el paradigma servidor de nombres/resolución de nombres del DNS y las relaciones entre servidor de archivos/archivo-cliente como NFS y hosts sin disco.

N

NETWARE: Popular sistema operativo de red distribuido desarrollado por Novell. Proporciona acceso remoto transparente a archivos y varios otros servicios de red distribuidos

NFS: Se utiliza comúnmente para designar un conjunto de protocolos de sistema de archivos distribuido, desarrollado por Sun Microsystems, que permite el acceso

remoto a archivos a través de una red. En realidad, NFS es simplemente un protocolo del conjunto.

P

PAQUETE: Agrupación lógica de información que incluye un encabezado que contiene la información de control y (generalmente) los datos del usuario. Los paquetes se usan a menudo para referirse a las unidades de datos de capa de red.

PUERTO : Interfaz en un dispositivo de internetwork (por ejemplo, un router). 2. Enchufe hembra en un panel de conmutación que acepta un enchufe macho del mismo tamaño, como un jack RJ-45. En estos puertos se usan los cables de conmutación para interconectar computadores conectados al panel de conmutación. Esta interconexión permite que la LAN funcione. 3. En la terminología IP, un proceso de capa superior que recibe información de las capas inferiores. Los puertos tienen un número, y muchos de ellos están asociados a un proceso específico. Por ejemplo, SMTP está asociado con el puerto 25. Un número de puerto de este tipo se denomina dirección conocida.

R

ROUTER: Dispositivo de capa de red que usa una o más métricas para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes de una red a otra basándose en la información de capa. Denominado a veces gateway (aunque esta definición de gateway se está volviendo obsoleta).

S

SERVIDOR: Nodo o programa de software que suministra servicios a los clientes.

SNMP: Protocolo de administración de redes utilizado casi con exclusividad en redes TCP/IP. El SNMP brinda una forma de monitorear y controlar los dispositivos de red y de administrar configuraciones, recolección de estadísticas, desempeño y seguridad.

SPOOFING :

1. Esquema que usan los routers para hacer que un host trate a una interfaz como si estuviera funcionando y soportando una sesión. El router hace spoofing de respuestas a mensajes de actividad del host para convencer a ese host de que la sesión continúa. El spoofing resulta útil en entornos de enrutamiento como DDR, en el cual un enlace de conmutación de circuito se desconecta cuando no existe tráfico que se deba enviar a través del enlace, a fin de ahorrar gastos por llamadas pagas.
2. La acción de un paquete que ilegalmente dice provenir de una dirección desde la cual en realidad no se lo ha enviado. El spoofing está diseñado para contrarrestar los mecanismos de seguridad de la red, tales como los filtros y las listas de acceso.

SWITCH : Dispositivo que conecta computadoras. El switch actúa de manera inteligente. Puede agregar ancho de banda, acelerar el tráfico de paquetes y reducir el tiempo de espera.

T

TCP: Protocolo de capa de transporte orientado a conexión que provee una transmisión confiable de datos de dúplex completo. TCP es parte de la pila de protocolo TCP/IP.

TCP/IP: Nombre común para el conjunto de protocolos desarrollados por el DoD de EE.UU. en los años ’70 para promover el desarrollo de internetwork de redes a nivel mundial. TCP e IP son los dos protocolos más conocidos del conjunto.

UDP: Protocolo no orientado a conexión de la capa de transporte de la pila de protocolo TCP/IP. UDP es un protocolo simple que intercambia datagramas sin confirmación o garantía de entrega y que requiere que el procesamiento de errores y las retransmisiones sean manejados por otros protocolos.

SIGLARIO.

ACL: lista de control de acceso.

BLP: Modelo Bell Lapadula

CIAC: Capacidad de Asesoría en Incidentes de Computadoras).

DAC: control de acceso discreto

DHCP: Protocolo de Configuración Dinámica de Servidores

DNS: Sistema de denominación de dominio.

FTP: Protocolo de Transferencia de Archivos.

GUI: interfaz gráfica del usuario.

HTML: Lenguaje de Etiquetas por Hipertexto.

HTTP: Protocolo de Transferencia de Hipertexto.

IP: Protocolo Internet.

ISO: Organización Internacional para la Normalización.

ITSEC: Criterios de Evaluación de la Seguridad en las Tecnologías de la Información.

IEC: Comisión Electrotécnica Internacional.

KDC: Centro de distribución de las claves Kerberos**.**

MAC: Control de Acceso al Medio.

MIT: Instituto Tecnológico de Masschussets

MVJ: Máquinas Virtuales Java

NFS: Sistema de Archivos de Red.

NIST: National Institute for Standars and Technology.

PERL: Lenguaje Práctico de Extracción e Informes.

PPP: Protocolo Punto a Punto.

SNMP: Protocolo simple de administración de redes.

SUID: set user id.

TCP: Protocolo de Control de Transmisión.

TCP/IP: Protocolo de Control de Transmisión /Protocolo Internet.

UDP: Protocolo de Datagrama de Usuario.

VI: virus informáctico.

BIBLIOGRAFÍA

[1] http://www.seguridadcorporativa.org

[2] HUERTA, Antonio Villalón. Seguridad en Unix y redes. (Versión 2.1)

[3] http://www.internet-solutions.com.co/ser_fisica_logica.php

[4] ALDEGANI, Gustavo. Miguel. Seguridad Informática. MP Ediciones. 1° Edición. ISBN 987–
9131–26–6. Uruguay. 1997.

[5] http://www.salvador.edu.ar/molina.htm#Niveles de Seguridad

[6]McCLURE, Stuart. “Hackers Secretos y Soluciones Para la Seguridad en Redes. Editorial McGRAW – HILL.

[7] Trabajo sobre DELITOS INFORMÁTICOS desde la Universidad de El Salvador, Octubre 2000 (PDF)
http://www.e-libro.net/E-libro-viejo/gratis/delitoinf.pdf

[8] http://delitosinformaticos.com/trabajos/hackcrack.pdf

[9] www.angelfire.com/ga/metalsystem/ terminologia_tecnica_del_hacker.html

[10] HERNADEZ, Claudio. Hackers “los piratas del chip y de internet.

[11] http://cfbsoft.iespana.es/cfbsoft_es/seguridad/

[12] http://www.el-hacker.com/foro/index.php/topic,24010.0.html

[13]www.caece.edu.ar/Cursos/Docs/
ISEC%20CAECE%20Conferencia%20de%20Seguridad%20Informatica-2.pdf

[14] http://www.indaya.com

[15] Revista red “la seguridad en manos de otros”, julio 2004 , pag 6

[16] Dr. Iván Seperiza Pasquali LOS VIRUS INFORMÁTICOS, ELECTRÓNICOS O COMPUTACIONALES. http://www.isp2002.co.cl/virus.htm

[17] MARTINEZ, Oscar. “VIRUS INFORMATICOS”.
http://www.geocities.com/ogmg.rm/

[18] http://www.zonavirus.com/datos/articulos/167/Tipos_Virus.asp

[19] http://www.mundopc.net/cursos/virus/virus13.php

[20] Seguridad en Centros de Computo. Políticas y Procedimientos. Editorial Trillas.

[21] http://mx.geocities.com/fundamentosdeseguridad/SEMINARIO/SITIOS.htm

[22] www.sc.ehu.es/jiwibmaj/apuntesCatellano/TEMA_12-políticas-.pdf

[23] www.ifi.unizh.ch/~knorr/documents/p_novatica.pdf

[24]http://seguridad.lci.ulsa.mx/POLITICAS_DE_SEGURIDAD_Alberto_Basalo.doc

[25] www.gwolf.org/seguridad/impl/impl.html

[26] www.hackemate.com.ar/tools/

[27] www.tress.com.mx/boletin/julio2003/firewall.htm

[28] www.kriptopolis.com/index.php

[29] kerberos http://www.cs.hmc.edu/~jallen/papers/kerb.html

[30] http://www.delitosinformaticos.com/especial/seguridad/pgp.shtml

[31] www.vialidad.cl/estandares/7Estandaresseguridad.pdf

[32] www.ceedcv.com/paginas/pacodebian/seguridad.pdf

[33] http://files.quadrantcommunications.be/Quadrant.nsf/Pages/CISP

[34] http://www.multingles.net/tutoriales.htm

[35]http://www.microsoft.com/spain/windowsxp