TABLA DE CONTENIDO

CAPITULO I ANTEPROYECTO

1.1. TEMA DE INVESTIGACIÓN

Manual de seguridad contra robo de archivos en sistemas operativos Windows 7 funcionando en entornos de red

1.2. PLANTEAMIENTO DEL PROBLEMA

1.2.1. ANTECEDENTES

Una de las ventajas de trabajar con las computadoras, es la posibilidad de conectarlas entre ellas, debido a esto es posible compartir información con otras personas, sin necesidad de que la información sea trasladada físicamente, pero esta ventaja, se vuelve una desventaja cuando la información es vista u obtenida por personasque son ajenas a su contenido, y que no deben intervenir al compartir los archivos.

El libro "TheCuckoo'sEgg" se considera uno de los primeros casos referentes a seguridad informática, este libro salió a la luz a finales de los años 80 en los EEUU y cuenta la historia de la persecución a un cracker informático que logró entrar en una computadora de forma remota y altera la información.

(LIZARRAGA Mariano, TOLEDO Rommel, 13/marzo/2007) bibliografía anexo 1

A partir de aquí se han escuchado muchos casos parecidos, en la que los crackers han logrado conseguir archivos personales de los usuarios de las computadoras, entre los tipos de archivos más comunes que se sustraen se hallan las fotos, videos y documentos, y en nuestro medio no estamos a salvo de este problema, es claro que se necesita tener conocimiento de cómo poder defenderse.

En nuestro medio, según estudios de GMS, Astaro y KasperskyLab., las empresas ecuatorianas no están exentas de los ataques de los piratas de la web, que en 2009 crearon 110 mil tipos de virus para sustraer información de usuarios corporativos.

(diario HOY, 05/Julio/2010) bibliografía anexo 2

1.2.2. DIAGNÓSTICO

1.2.2.1.CAUSA – EFECTO

Causa:

Las personas con malas intenciones que buscan obtener beneficio, rebajar la reputación de las víctimas o simplemente por demostrar su habilidad.

Las causas mencionadas anteriormente se complementan con los usuarios de las computadoras, que no tienen conocimiento o no dan la debida importancia al tema de la seguridad informática.

Efecto:

Al ignorar la gravedad de este problema, nuestra información puede llegar a personas con intenciones de hacer mal uso de la información, entre ellos está la venta de información confidencial de una empresa, o la publicación o venta de fotos y videos de alta intimidad en internet, que llegan a generar incomodidad con las personas involucradas.

1.2.2.2.PRONÓSTICO Y CONTROL DE PRONÓSTICO

Pronóstico:

De continuar con esta tendencia, debido a que estas prácticas de robo de archivos están en crecimiento, las empresas no invierten en temas de seguridad y los usuarios no se preocupan de estos problemas, serán vulnerables con respecto a pérdida de información, y podrían tener consecuencias graves, se generará una gran desconfianza con los sistemas informáticos.

Control de Pronóstico:

Identificar las malas prácticas de los usuarios y corregirlas, identificar vulnerabilidades o puntos débiles en los sistemas y reforzarlos, tanto a nivel de Sistema Operativo como a nivel de los archivos para alcanzar un elevado nivel de seguridad, educar a los usuarios con conocimientos de seguridad informática, ya que son el punto más vulnerable de toda la cadena, como por ejemplo al establecer contraseñas de seguridad muy débiles.

1.2.3. FORMULACIÓN DE LA PROBLEMÁTICA

1.2.3.1.PROBLEMA PRINCIPAL

Hoy en día se han visto o escuchado muchas noticias en donde el tema es robo de archivos, ya sea a grandes compañías o a personas, entre los más escuchados están el robo de fotos o videos privados que son publicadas y/o distribuidos sin autorización, en el caso de las compañías, se produce una fuga de información valiosa para la empresa, de hecho actualmente la información se considera el recurso más valioso que se posee. Es por esta razón que se debe tomar muy en serio este asunto, La pregunta que se genera es:

¿Cómo protegernos del robo de información?

1.2.3.2.PROBLEMAS SECUNDARIOS

- ¿Se puede compilar información sobre las distintas formas de robo de archivos?
- ¿Se puede sistematizar la información recopilada para elaborar un manual de alta seguridad contra robo de archivos en las redes LAN conectadas mediante WiFi?
- ¿Se puede plantear recomendaciones para el tratamiento de los archivos (ubicaciones, organización)?
- ¿Se puede proponer recomendaciones para establecer contraseñas seguras en el sistema operativo y los archivos?

1.2.4. OBJETIVOS

1.2.4.1. OBJETIVO GENERAL

Diseñar un manual contra robo de archivos basado en el proceso de sistematización en Sistemas Operativos Windows 7 funcionando en un entorno de red LAN empresarial, conectados mediante WiFipara alcanzar un alto nivel de seguridad.

1.2.4.2. OBJETIVOS ESPECÍFICOS

- Conocer los conceptos básicos sobre el presente proyecto (Marco Teórico).
- Compilar las distintas formas de robo de archivos mediante WiFi.
- Plantear recomendaciones para el tratamiento de los archivos (ubicación, organización, etc.)
- Proponer consejos para establecer contraseñas de alta seguridad y que sean fáciles de recordar.
- Elaborar el manual de protección de archivos de alta seguridad.

1.2.5. JUTIFICACIÓN

1.2.5.1. JUTIFICACIÓN TEÓRICA

El tema es altamente preocupante, hoy en día las personas confían en que este tipo de cosas no pasará, o ni siquiera tiene conocimiento de este tipo de actividades, pero la posibilidad de que suceda está presente y cuando ocurra tendrá graves consecuencias.

El robo de información es cada vez más común, ya que es una actividad altamente lucrativa, además gran parte de los usuarios no tienen conocimientos de seguridad,y nuestro medio no es la excepción, los atacantes se aprovechan de ello y mientras esta tendencia siga, estas prácticas solamente aumentaran.

A continuación mencionamos un caso en el cual una pareja ha grabado videos íntimos durante sus vacaciones, sus videos estaban almacenados en el computador, la duda es que si sus videos han sido o no sustraídos y publicados en el internet, incluso su matrimonio está en riesgo si es que realmente el robo y la publicación de estos videos se ha producido.

(blog todoexpertos.com,08/09/2010) Anexo 3

Entonces una vez conscientes de la gravedad del problema en base a las consecuencias que puede tener la pérdida de información, vemos la importancia que tiene el desarrollo de este proyecto.

1.2.5.2.JUTIFICACIÓN METODOLÓGICA

FIREWALL DE SISTEMA OPERATIVO.- Un cortafuegos o firewall es un sistema que previene el uso y el acceso desautorizados a tu ordenador.

Los firewalls pueden ser software, hardware, o una combinación de ambos. Se utilizan con frecuencia para evitar que los usuarios desautorizados de Internet tengan acceso a las redes privadas conectadas con Internet, especialmente intranets.

Todos los mensajes que entran o salen de la Intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea los que no cumplen los criterios de seguridad especificados.

Es importante recordar que un firewall no elimina problemas de virus del ordenador, sino que cuando se utiliza conjuntamente con actualizaciones regulares del sistema operativo y un buen software antivirus, añadirá cierta seguridad y protección adicionales para tu ordenador o red.

(masadelante.com,27/08/2011) bibliografía anexo 7

ANTIVIRUS.- Son programas cuyo objetivo es detectar y/o eliminar virus informáticos. Nacieron durante la década de 1980.

Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e Internet, ha hecho que los antivirus hayan evolucionado hacia programas más avanzados que no sólo buscan detectar virus informáticos, sino bloquearlos, desinfectarlos y prevenir una infección de los mismos, y actualmente ya son capaces de reconocer otros tipos de malware, como spyware, rootkits, etc.

http://es.wikipedia.org/wiki/Antivirus

PROTECTOR DE ARCHIVOS.- proteger los archivos y carpetas mediante contraseñas, de esta manera al no conocer la clave de acceso, será imposible el acceso a los archivos.

1.2.5.3.JUTIFICACIÓN PRÁCTICA

En nuestros computadores almacenamos toda nuestra información (fotos, videos, documentos, etc.), a nadie le gustaría que su información sea obtenida por terceras personas, entonces por esta razón es importante tener en cuenta implementar seguridades en nuestros equipos, al poner en práctica este proyecto, nuestros datos estarán mejor protegidos de los crackers, se preserva la confidencialidad de los datos y la privacidad de los usuarios de la red.

1.2.6. MARCO DE REFERENCIA

1.2.6.1.MARCO ESPACIAL

Este proyecto se puede poner en práctica en cualquier empresa que cumpla con que las computadoras operen con Windows 7 y se encuentre funcionando en un entorno de red empresarial conectada mediante WiFi.

1.2.7.2. MARCO TEMPORAL

Para realizar el presente proyecto se cuenta con aproximadamente dos meses disponibles.

1.2.7. METODOLOGÍA Y CRONOGRAMA

METODOLOGÍA

A medida que pasa el tiempo, los sistemas se van haciendo más complejos, pero a la vez más complicados de controlarlos, ya que por su complejidad pueden existir áreas vulnerables que pueden ser aprovechados por personas con malas intenciones.

Para el desarrollo del proyecto se realiza un estudio de las formas en las que ocurren los robos de archivos y se proponen formas de protección frente a cada caso, esta información será analizada y clasificada para lograr un nivel de seguridad deseado, logrando un proceso de sistematización.

CRONOGRAMA

Actividad	septiembre				octubre				noviembre			
Analisis del proyecto												
Capitulo 1. Anteproyecto												
Capitulo 2. Marco teorico												
Capítulo 3. Casos de robo de archivos.												
Capítulo 4. Recomendaciones para establecer contraseñas seguras.												
prerevision												
correcciones												

1.2.8. PLAN ANALÍTICO

Introducción

Capítulo I

Anteproyecto.

Capítulo II

Marco Teórico (Conceptos básicos).

Capítulo III

Casos de robo de archivos.

Capítulo IV

Sistematización de la información recopilada (manual de seguridad).

Conclusiones y recomendaciones

CAPÍTULO IIMARCO DE REFERENCIA

2.1.MARCO TEORICO

2.1.1. CONCEPTOS GENERALES

ENTORNOS DE RED

En el nivel más elemental, una red consiste en dos equipos conectados entre sí, de forma tal que puedan compartir datos. Todas las redes, no importa lo sofisticadas que sean, parten de este sencillo sistema.

Existen otras formas un poco más sofisticadas de conectar equipos entre sí, utilizando por ejemplo las líneas telefónicas, microondas y hasta los satélites de comunicación para este fin.

Si un equipo es conectado a otros equipos, podría compartir los datos y otros dispositivos. Se llama red al conjunto de equipos y dispositivos conectados entre sí, al concepto de conectar equipos y compartir recursos en una empresa se le llama trabajo en un "entorno de red".

(CECINFO UTEA, 27/08/2011)Anexo 5

SISTEMA OPERATIVO

El sistema operativo es el programa más importante de un ordenador. Para que funcionen los otros programas, cada ordenador de uso general debe tener un sistema operativo. Los sistemas operativos realizan tareas básicas, tales como reconocimiento de la conexión del teclado, enviar la información a la pantalla, no perder de vista archivos y directorios en el disco, y controlar los dispositivos periféricos tales como impresoras, escáner, etc.

En sistemas grandes, el sistema operativo tiene incluso mayor responsabilidad y poder, es como un policía de tráfico, se asegura de que los programas y usuarios que están funcionando al mismo tiempo no interfieran entre ellos. El sistema operativo también es responsable de la seguridad, asegurándose de que los usuarios no autorizados no tengan acceso al sistema.

(masadelante.com, 27/08/2011)Anexo 6

ROBO DE ARCHIVOS

El robo de archivos hace referencia a las fotos, videos, documentos, hojas de cálculo, etc. que son sustraídos de un computador funcionando con sistema operativo Windows 7, sin consentimiento y/o sin conocimiento del usuario del equipo víctima.

ANTIVIRUS

Un antivirus es un programa informático que tiene el propósito de detectar y eliminar virus y otros programas perjudiciales antes o después de que ingresen al sistema.

Los virus, gusanos, troyanos, spywareson tipos de programas informáticos que suelen ejecutarse sin el consentimiento del usuario o propietario de un ordenador y que cumplen diversas funciones dañinas para el sistema. Entre ellas, robo y pérdida de información, alteración del funcionamiento, disrupción del sistema y propagación hacia otras computadoras.

Actualmente en el mercado tenemos varias opciones de antivirus para elegir, y entre algunos antivirus, seleccionaremos uno para el presente manual, según criterios de efectividad y rendimiento.

A continuación se presenta una lista de programas antivirus gratuitos que se destacan:

AVG Anti-Virus Free 2012.

AVG Anti-Virus Free es un eficaz antivirus gratuito. Fue uno de los primeros en aparecer y cuenta con una cifra de usuarios impresionante. Protege en tiempo real contra virus, spyware, rootkits, gusanos e intentos de phishing.

Una característica muy apreciada de AVG Anti-Virus Free es LinkScanner, el módulo que comprueba la seguridad de los resultados de búsqueda y enlaces de las páginas web. En la versión 2012 se ha mejorado para analizar los enlaces de Facebook y MySpace, las redes sociales más conocidas.

Los análisis de AVG Anti-Virus Free se pueden lanzar de inmediato o programar para otro día y hora. La primera vez que analices el equipo, el motor de AVG ejecutará una optimización para adaptarse al rendimiento de tu máquina.

La versión 2012 de AVG Anti-Virus Free ha pegado un salto de calidad con respecto a la anterior. La interfaz es mucho más atractiva y práctica, y se incluye un gadget para lanzar análisis o actualizar AVG desde el Escritorio. Cabe decir que la velocidad de escaneo de AVG Anti-Virus Free no es para lanzar cohetes, aunque ha mejorado bastante.

AVG Anti-Virus Free es ya un clásico de la seguridad a coste cero. Aunque su evolución ha sido menos espectacular que la de otros paquetes de seguridad, mantiene los valores que lo han hecho merecedor de la confianza de más de cien millones de usuarios en todo el mundo.

http://avg.softonic.com/

AVAST Free Antivirus 6.0.1289

Es un antivirus gratuito y sin publicidad. Con sus ocho escudos, mantiene el ordenador constantemente a salvo de una gran variedad de amenazas, la sexta edición de avast! Free Antivirus presenta pocos cambios estéticos en comparación con la anterior, pero amplía aún más el abanico de la protección gratuita.

A los escudos de la versión 5 se añaden los de scripts y comportamiento. Y con el módulo AutoSandbox, avast! Free Antivirus impide que programas potencialmente dañinos puedan afectar el sistema, tres barras coloreadas indican la calidad del sitio y hay recuadros para clasificar el sitio web en distintas categorías. Es un sistema eficaz y abierto a las contribuciones de los usuarios.

Lo cierto es que ningún antivirus gratuito ofrece tanto como avast! Free Antivirus. Traducido y apoyado por una inmensa comunidad de usuarios, se postula como el antivirus gratuito por excelencia.

http://avast-professional.softonic.com/

Panda Cloud Antivirus 1.5.1 Free

Panda Cloud Antivirus emplea una filosofía de protección distinta. Su capacidad para detectar y eliminar virus, troyanos, spyware y otros peligros se basa en una red de servidores que facilita la recolección de muestras y el despliegue de firmas. El resultado es un antivirus ligerísimo y rápido como el rayo.

Tras la instalación, lo primero que notarás de Panda Cloud Antivirus es la sencillez de su interfaz. El panel principal muestra un icono que resume la situación de seguridad. Tres grandes botones dan acceso a los análisis bajo demanda, al informe

de sucesos y a las pocas opciones disponibles. Si pulsas el pequeño icono de la esquina inferior derecha, Panda Cloud Antivirus te mostrará las opciones de configuración.

Una peculiaridad de Panda Cloud Antivirus es que no requiere actualizaciones: cada vez que analiza un fichero, se conecta a la red de servidores de Panda para comprobar sobre la marcha si coincide con las firmas disponibles. La ventaja de este modelo es que Panda Cloud Antivirus puede detectar nuevos peligros y enviar muestras de malware en tiempos muy reducidos.

Desde la versión 1.1, el consumo de memoria de Panda Cloud Antivirus es el mejor de su categoría, inferior a los 30 megabytes durante el análisis. Si algo puede achacarse a Panda Cloud Antivirus es la excesiva simpleza de su aspecto y la poca información que proporciona, algo que, podría gustar a otros usuarios.

http://panda-cloud-antivirus.softonic.com/

ANALISIS DE LOS ANTIVIRUS

En la siguiente tabla están los resultados de una prueba realizada a los diferentes programas antivirus, donde se muestrasus rendimientos con respecto a eliminación de Malware, Rootkits y Scareware,en la cual se destaca el programa AVG Anti-Virus Free 2012, con una calificación de 6.5 en eliminación de Malware, 6.7 en eliminación de Rootkits y 9.5 en eliminación de Scareware.

MALWARE REMOVAL	Suite	Free	All Malware		Rootkits		Scareware	
			%	score	%	score	%	score
NEW MALWARE COLLECTION INTRODUCED								
avast! Rescue Disc			81%	5.7	86%	5.3	80%	7.4
AVG Anti-Virus Free 2012		**Y**	**88%**	**6.5**	**100%**	**6.7**	**100%**	**9.5**
Bitdefender Antivirus Plus 2012			82%	6.0	86%	6.0	100%	9.5
G Data AntiVirus 2012			83%	5.4	86%	5.3	100%	8.4
Kaspersky Anti-Virus 2012			76%	5.7	71%	3.9	75%	6.3
Malwarebytes' Anti-Malware Free 1.51		Y	79%	6.4	57%	3.6	100%	10.0
Norman Malware Cleaner 2.1		Y	85%	5.3	71%	2.4	100%	9.5
Outpost Antivirus Pro 7.5			82%	4.9	86%	2.9	75%	6.3
Panda Antivirus Pro 2012			85%	5.8	100%	4.7	100%	9.5
Panda Cloud Antivirus 1.5 Free Edition		Y	91%	5.9	100%	4.1	100%	9.5
Trend Micro Titanium Antivirus+ 2012			79%	4.7	86%	3.6	100%	7.0
TrustPort Antivirus 2012			88%	5.4	100%	4.4	100%	9.5
ZoneAlarm Antivirus + Firewall 2012			79%	6.0	100%	6.7	75%	7.5

http://www.desarrolloweb.com/de_interes/mejores-antivirus-2011-2012-5796.html#contenido_externo

SELECCIÓN DEL ANTIVIRUS

Debido a las características de rendimiento en cuanto a detección y eliminación de MalWare, brindadas por el programa antivirus AVG, se lo presenta como opción recomendada en el presente manual, en las que destacan también herramientas adicionales a la protección contra MalWare que mejoran la seguridad del usuario.

PROTECTOR DE ARCHIVOS

Programas que sirven para proteger los archivos de consultas de personas ajenas a la lectura del contenido de un archivo mediante el uso de una contraseña, lo que hace es codificar el archivo deseado y no permite su legibilidad.

A continuación se presentan tres opciones se selección:

AndrosaFileProtector

Su funcionamiento es de lo más sencillo, una vez el programa instalado, puedes proteger tus archivos de dos maneras: desde el entorno del programa o desplegando el menú contextual de Windows.

Para desproteger archivos, basta con hacer doble clic e introducir la contraseña de acceso que hayas definido en el proceso de cifrado.

Como métodos de protección utiliza una contraseña de acceso y tres algoritmos de cifrado diferentes: Rijndael (AES); TripleDES de y DES.

Encrypt Files

Proteger tus archivos y carpetas y evitar que sean vistos por ojos no autorizados. En concreto esteprograma soporta hasta 13 métodos de encriptación diferentes, rápido a la hora de encriptar y desencriptar, y además permite ocultar los archivos tras encriptarlos.

FreeOTFE Explorer

Es una utilidad que te permitirá crear espacios cifrados de memoria en tu disco duro para que guardes tus secretos, Básicamente, se puede crear una unidad virtual o volumen en cualquier medio de almacenamiento disponible en tu PC, copiar o mover archivos y cifrar todo el contenido mediante algoritmos de encriptado como AES. De esta manera, te asegura que todo lo que guardes en tus volúmenes protegidos estará a salvo de miradas extrañas.

SELECCIÓN DEL ENCRIPTOR DE ARCHIVOS

Todas estas herramientas se han probado y se recomienda el uso de “Encryptfiles”, ya que destaca de los demás en: facilidad de uso, la variedad de métodos de encriptación, opciones de seguridad, como la de ocultar archivos encriptados y su amigable interface.

2.1.2. SEGURIDAD INFORMATICA

Para lograr la seguridad de la información, debe tener tres características fundamentales que son:

Confidencialidad.- es la propiedad de la información, por la que se garantiza que ésta sea accesible únicamente para el personal autorizado a acceder a dicha información.
Integridad.- la información debe mantenerse tal y como se la dejo, toda modificación a datos o información es realizada por personas autorizadas de manera autorizada.
Disponibilidad.- La información y datos se encuentran disponibles para personal autorizado siempre y cada vez que se la necesita.
Podemos establecer controles que pueden ayudar a alcanzar estas tres características en la información, estas pueden ser:

- Preventivos
- Detectivos
- Correctivos

Todos los días se tratan de buscar falencias o formas para romper cualquiera de estas tres características, haciendo que el tema de la seguridad un problema complicado, en este trabajo se clasifica los diferentes tipos de amenazas, tanto físicas como lógicas de la mejor manera para poder entender su funcionamiento y objetivos.

2.1.3. SEGURIDAD FÍSICA

Es muy importante ser consciente que por más que nuestra empresa 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.
Así, la Seguridad Física consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

Las principales amenazas que se prevén en la seguridad física son:

- Desastres naturales.
- Huracanes, terremotos, etc.
- Desastres del entorno.
- Electricidad, ruido eléctrico, incendios, humedad, etc.
- Acciones humanas.
- Incendios, negligencia, accesos no autorizados, etc.

2.1.4. SEGURIDAD LOGICA

Es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputos no será sobre los medios físicos sino contra información por él almacenada y procesada.

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.

Es decir que la Seguridad Lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."

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 contraseña 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.

2.1.5. ROBO DE ARCHIVOS

Contempla la adquisición sin permiso de cualquier dato almacenado en un dispositivo que pueda ser legible mediante un programa.

2.1.6. ATAQUES DE MONITORIZACIÓN

Este tipo de ataque se realiza para observar a la víctima y su sistema, con el objetivo de identificar sus vulnerabilidades y posibles formas de acceso futuro.

2.1.6.1.EAVESDROPPING–PACKET SNIFFING

Muchas redes son vulnerables al Eavesdropping, o a la pasiva intercepción del tráfico de red, esto se realiza con PacketSniffers, los cuales son programas que monitorean los paquetes que circulan por la red, cada máquina conectada a la red 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.

2.1.6.2.DECOY (SEÑUELOS)

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

2.1.6.3.SHOULDER SURFING

Consiste en espiar físicamente a los usuarios para obtener el login y su contraseña correspondiente. El Surfing explota el error de los usuarios de dejar su login y contraseña anotadas cerca de la computadora. Cualquier intruso puede pasar por ahí, verlos y memorizarlos para su posterior uso.

2.1.6.4.SNOOPING–DOWNLOADING

Los ataques de esta categoría tienen el mismo objetivo que el Sniffing: obtener la información sin modificarla, 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 de esa información a su propia computadora, para luego hacer un análisis exhaustivo de la misma.

2.1.6.5.KEYLOGGERS

La mayoría de las fuentes consultadas definen keylogger como un programa diseñado para, en secreto, monitorear y registrar cada pulsación del teclado. Esta definición no es correcta del todo, pues un keylogger no necesariamente tiene que ser un programa, sino que también puede ser un dispositivo físico. Los dispositivos keylogger son menos conocidos que el software keylogger, pero es importante tener en cuenta la existencia de ambos cuando se habla de seguridad informática.

2.1.6.6.ESCANEO DE PUERTOS

El escaneo, como método de descubrir canales de comunicación susceptibles de ser explotados, lleva en uso mucho tiempo. La idea es recorrer tantos puertos de escucha como sea posible, y guardar información de aquellos que sean receptivos o de utilidad para cada necesidad en particular.

El permitir o denegar acceso a los puertos es importante porque las aplicaciones servidoras (que aceptan conexiones originadas en otro ordenador) deben 'escuchar' en un puerto conocido de antemano para que un cliente (que inicia la conexión) pueda conectarse. Esto quiere decir que cuando el sistema operativo recibe una petición a ese puerto, la pasa a la aplicación que escucha en él, si hay alguna, y a ninguna otra. Los servicios más habituales tienen asignados los llamados *puertos bien conocidos*, por ejemplo el 80 para web, el 21 para ftp, el 23 para telnet, etc. Así pues, cuando usted pide una página web, su navegador realiza una conexión al puerto 80 del servidor web, y si este número de puerto no se supiera de antemano o estuviera bloqueado no podría recibir la página.

Un puerto puede estar:

Abierto: Acepta conexiones. Hay una aplicación escuchando en este puerto. Esto no quiere decir que se tenga acceso a la aplicación, sólo que hay posibilidad de conectarse.

Cerrado: Se rechaza la conexión. Probablemente no hay aplicación escuchando en este puerto, o no se permite el acceso por alguna razón. Este es el comportamiento normal del sistema operativo.

Bloqueado o Sigiloso: No hay respuesta. Este es el estado ideal para un cliente en Internet, de esta forma ni siquiera se sabe si el ordenador está conectado. Normalmente este comportamiento se debe a un cortafuegos de algún tipo, o a que el ordenador está apagado.

Para el escaneo de puertos se envía una serie de paquetes para varios protocolos y se deduce que servicios están "escuchando" por las respuestas recibidas o no recibidas.

Existen varios tipos de scanning según la técnica, puertos y protocolos explotados:

TCP connect() scanning: Es la forma más popular de escaneo TCP y consiste básicamente en usar la llamada a sistema connect() del sistema operativo, si se logra establecer la conexión con el puerto de la otra computadora entonces este puerto está abierto.

TCP SYN scanning: esta técnica es la llamada escaneo "half-open" (mitad abierto), porque no establecemos una conexión TCP completa. Se enviar un paquete SYN como si fuéramos a entablar una conexión TCP completa y esperamos por una respuesta.

TCP FIN scanning: algunos firewalls y packetsfilters escuchan por los paquetes SYN en algunos puertos, y programas como el synlogger pueden detectar este tipo de escaneo. En cambio los paquetes FIN pueden penetrar sin mayor problema. La idea consiste en que al enviar un paquete FIN si el puerto está cerrado nos va a devolver un RST, y si el puerto está abierto nos va a ignorar.

Fragmentationscanning: Es una modificación de otras técnicas. Consiste en hacer una división de los paquetes que enviamos, para no ser detectados por los packetfilters y los firewalls. Por ejemplo podemos hacer un SYN o un FIN scanning fragmentando los paquetes que enviamos, y al ir quedando en cola en los firewalls y en los packetfilters no somos detectados.

TCP reverse identscanning: el protocolo ident permite averiguar el nombre de usuario y el dueño de cualquier servicio corriendo dentro de una conexión TCP. Por ejemplo podemos conectarnos al puerto http y usar ident para averiguar que está corriendo la víctima como root; esto solo es posible estableciendo una conexión TCP completa.

FTP bounceattack: algo interesante del protocolo ftp, es que permite lo que se llama conexión proxy ftp. O sea, yo podría conectarme a un ftp desde un servidor proxy y al hacer esto establecer una conexión y enviar un archivo a cualquier parte de la Internet. Esto lo podemos aprovechar también para hacer por ejemplo un escaneo TCP, ya que estaríamos haciéndolo desde un servidor ftp pero detrás de un firewall.

UDP ICMP portunreachablescanning: Lo que varía significativamente de esta técnica con respecta a las otras es que estamos usando el protocolo UDP (protocolo de datos de usuario), este protocolo puede ser más simple que el TCP pero al escanear se vuelve sumamente más complejo; esto se debe a que si un puerto está abierto no tiene que enviarnos un paquete de respuesta, y si un puerto está cerrado tampoco tiene que enviarnos un paquete de error. Afortunadamente, la mayoría de los hosts nos envían un paquete de error "ICMP_PORT_UNREACH" cuando un puerto UDP está cerrado. Esta técnica suele volverse muy lenta.

2.1.7. ATAQUES DE AUTENTICACIÓN

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

2.1.7.1.SPOOFING

Este tipo de ataques suele implicar un buen conocimiento del protocolo en el que se va a basar el ataque. Los ataques tipo Spoofing bastante conocidos son:

- IP Spoofing,
- DNSSpoofing
- Web Spoofing

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.

DNS Spoofing

Este ataque se consigue mediante la manipulación de paquetes UDP pudiéndose comprometer el servidor de nombres de dominios (DomainName Server–DNS) de Windows NT©. Si se permite el método de recursión 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.

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 las contraseñas, números de tarjeta de créditos, etc.

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

2.1.7.2.SPOOFING-LOOPING

Spoofing puede traducirse como "hacerse pasar por otro" y el objetivo de esta técnica, justamente, es actuar en nombre de otros usuarios, usualmente para realizar tareas de Snooping o Tampering.

Una forma común de Spoofing es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él.

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, llamado Looping, tiene la finalidad de "evaporar" la identificación y 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 atacado por un Insider, o por un estudiante a miles de Kilómetros de distancia, pero que ha tomado la identidad de otros.

2.1.7.3.EXPLOITS

Es muy frecuente ingresar a un sistema explotando agujeros en los algoritmos de encriptación utilizados, en la administración de las 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.

2.1.7.4.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 producto ya que cualquiera que conozca el agujero o lo encuentre en su código podrá saltarse los mecanismos de control normales.

2.1.7.5.MAN-IN-THE-MIDDLE

El atacante se interpone entre el origen y el destino en una comunicación pudiendo conocer y/o modificar el contenido de los paquetes de información, sin esto ser advertido por las víctimas. Esto puede ocurrir en diversos ambientes, como por ejemplo, en comunicaciones por e-mail, navegación en Internet, dentro de una red LAN, etc.

2.1.7.6.DHCP STARVATION

El atacante busca reemplazar al servidor DHCP (protocolo de configuración dinámico de host) que se encuentra funcionando en la red, de forma de asignar a los clientes direcciones IP y otra información (como ser el servidor Gateway) de acuerdo a su conveniencia. De esta forma podría luego simular ser el Gateway (equipo para interconectar redes) e interceptar la información que los clientes envíen, con el tipo de ataque Man-in-the-middle.

2.1.7.7.FORZADO DE CONTRASEÑAS

Consiste en la prueba metódica de contraseñas para lograr el acceso a un sistema, siempre y cuando la cuenta no presente un control de intentos fallidos de logueo. Este tipo de ataques puede ser efectuado:

Por diccionario: existiendo un diccionario de palabras, una herramienta intentará acceder al sistema probando una a una las palabras incluidas en el diccionario.

Por fuerza bruta: una herramienta generará combinaciones de letras números y símbolos formando posibles contraseñas y probando una a una en el login del sistema.

2.1.8. ATAQUES DE MODIFICACIÓN

2.1.8.1.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 puede incluso terminar en la baja total del sistema.

2.1.8.2.MALEWARE

Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario.

El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto. El término virus informático es utilizado en muchas ocasiones de forma incorrecta para referirse a todos los tipos de malware, incluyendo los verdaderos virus.

El software es considerado malware basándose en los efectos que cause en un computador, El término malware incluye virus, gusanos, troyanos, la mayoría de los rootkits, spyware, adwareintrusivo,crimewarey otros software maliciosos e indeseables.

Virus

Tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este.

Pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

Spyware

Aplicaciones que recogen y envían información sobre las páginas web que más frecuentemente visita un usuario, tiempo de conexión, datos relativos al equipo en el que se encuentran instalados (sistema operativo, tipo de procesador, memoria, etc.) e, incluso, hay algunos diseñados para informar de si el software que utiliza el equipo es original o no.

Bombas lógicas

Se entiendo por bomba lógica (en inglés denominado time bombs), aquel software, rutinas o modificaciones de programas que producen modificaciones, borrados de ficheros o alteraciones del sistema en un momento posterior a aquél en el que se introducen por su creador.

Gusanos

Hace referencia a programas capaces de viajar por sí mismos a través de redes de computadores para realizar cualquier actividad una vez alcanzada una máquina; aunque esta actividad no tiene por qué entrañar peligro, los gusanos pueden instalar en el sistema alcanzado un virus, atacar a este sistema como haría un intruso, o

simplemente consumir excesivas cantidades de ancho de banda en la red afectada. Aunque se trata de *malware* muchísimo menos habitual que por ejemplo los virus o las puertas traseras, ya que escribir un gusano peligroso es una tarea muy difícil, los gusanos son una de las amenazas que potencialmente puede causar mayores daños.

Troyanos

Un troyano o caballo de Troya actual es un programa que aparentemente realiza una función útil para quién lo ejecuta, pero que en realidad - o aparte - realiza una función que el usuario desconoce, generalmente dañina.

Conejos o bacterias

Son programas que de forma directa no dañan al sistema, sino que se limitan a reproducirse, generalmente de forma exponencial, hasta que la cantidad de recursos consumidos se convierte en una negación de servicio para el sistema afectado.

2.1.9. VARIOS

2.1.9.1.INGENIERÍA SOCIAL

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, más seguras para el atacante y una de las más efectivas para atacar, no necesita tener conocimientos avanzados para quebrar seguridades, sino que se aprovecha de la ingenuidad de las personas.

2.1.9.2.INGENIERÍA SOCIAL INVERSA

Se realiza cuando el atacante suplanta a una persona que se encuentra en una posición con autoridad suficiente para que los empleados le pidan información al atacante, en lugar de ser informado el atacante, una vez generada la confianza, el atacante podría obtener información valiosa de parte de los propios empleados; sin embargo, este atraque requiere un grado elevado de preparación e investigación.

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

2.1.9.3.TRASHING

Generalmente, un usuario anota su login y password en un papelito y luego, cuando lo recuerda, lo desecha en la basura. Este procedimiento por más inocente que parezca es el que puede aprovechar un atacante para hacerse de una llave para entrar en el sistema.

El Trashing puede ser físico o lógico, como analizar buffers de impresora y memoria, bloques de discos, etc.

2.1.9.4.CANALES OCULTOS

Un canal oculto es un cauce de comunicación que permite a un proceso receptor y a un emisor intercambiar información de forma que viole la política de seguridad del sistema; esencialmente se trata de un método de comunicación que no es parte del diseño original del sistema pero que puede utilizarse para transferir información a un proceso o usuario que no estaría autorizado a acceder a dicha información. Los canales ocultos existen solamente en sistemas con seguridad multinivel, aquellos que contienen y manejan información con diferentes niveles de sensibilidad, de forma que se permite acceder simultáneamente a varios usuarios a dicha información pero con diferentes puntos de vista de la misma, en función de sus privilegios y sus necesidades de conocimiento.

2.1.9.5.SUPERZAPPING

Pasa por alto todos los controles de seguridad para realizar cierta tarea administrativa, presumiblemente urgente; se trataba de un *`Rompa el cristal en caso de emergencia'*, o de una llave maestra capaz de abrir todas las puertas.

Obviamente, el problema sucede cuando la llave se pierde y un atacante la utiliza en beneficio propio.

2.1.9.6.CONTROL REMOTO DE EQUIPOS

Un atacante puede tomar el control de un equipo en forma remota y no autorizada, mediante la utilización de programas desarrollados para tal fin, e instalados por el atacante mediante, por ejemplo la utilización de troyanos.

2.1.9.7.ROBO DE EQUIPAMIENTO O COMPONENTES

El robo puede involucrar todo un equipo o de parte del mismo, ej.: un disco rígido. Puede ocurrir por un deficiente control de acceso establecido al centro de cómputos (o recinto donde residen los equipos: servidores, routers, switches, etc.), así como a las propias instalaciones del Organismo.

2.1.9.8.PÉRDIDA DE COPIAS DE RESGUARDO

Si no existen adecuadas medidas de seguridad física para las copias de resguardo, las mismas pueden dañarse, por ejemplo, en caso de ser afectadas por desastres como un incendio, inundación, o incluso por robo. Asimismo, una administración inadecuada de los medios físicos de almacenamiento puede provocar la obsolescencia de los mismos (ej.: reutilización excesiva de cintas).

Por otra parte, se debe tener en cuenta la obsolescencia tecnológica de los medios de almacenamiento con el paso del tiempo, de manera de actualizarlos adecuadamente para permitir su restauración en caso de ser necesaria.

2.1.9.9.ACCESO A INFORMACIÓN CONFIDENCIAL IMPRESA

Ocurre cuando información confidencial impresa es obtenida por personal no autorizado debido a que la misma no es resguardada adecuadamente mediante por ejemplo, una política de limpieza de escritorios.

2.2.MARCO TEMPORO/ESPACIAL

Para realizar el presente proyecto se cuenta con aproximadamente dos meses disponibles, dentro de los cuales vamos a tomar dos semanas para el proceso de análisis, tres semanas para la recolección y organización de datos, una semana para agregar información adicional y semanas una semana de revisiones y arreglos menores.

Este proyecto se puede poner en práctica en cualquier empresa que cumpla con que las computadoras operen con Windows 7 conectada mediante WiFi en un entorno de red empresarial.

2.3.MARCO LEGAL

Cada programa planteado para el presente proyecto tiene sus propias normas y condiciones de uso, los mismos que deben ser cumplidos.

2.4.METODOLOGÍA

2.4.1. MÉTODOS Y TECNICAS

A medida que pasa el tiempo, los sistemas se van haciendo más complejos, pero a la vez más complicados de controlarlos, ya que por su complejidad pueden existir áreas vulnerables que pueden ser aprovechados por personas con malas intenciones.

Para el desarrollo del proyecto se realiza un estudio de las formas en las que ocurren los robos de archivos y se proponen formas de protección frente a cada caso, esta información será analizada y clasificada para lograr un nivel de seguridad deseado, logrando un proceso de sistematización.

CAPÍTULO IIIFORMAS DE ROBO DE ARCHIVOS

3.1. ATAQUES DE MONITORIZACIÓN

Realizados para observar a la víctima y su sistema

3.1.1. DECOY

Son programas que imitan la interface de otro programa original, puede ser por ejemplo se puede presentar el programa Decoy en el momento de iniciar sesión Windows, el usuario desprevenido lo hace y envía la información de acceso al atacante para su posterior acceso, el Decoy desaparece dejando salir la verdadera pantalla de inicio y luego continúa con las actividades normales del sistema.

3.1.2. EAVESDROPPING – PACKET SNIFFING

Consiste en la intercepción del tráfico de una red mediante el uso de dispositivos o software, dependiendo del tipo de la red, este método es muy utilizado para capturar usuarios y contraseñas, que generalmente viajan claros y sin encriptación, al ingresar a sistemas de acceso remoto. También son utilizados para capturar números de tarjetas de crédito y direcciones mail entrantes y salientes.

3.1.3. SNOOPING–DOWNLOADING

Los ataques de esta categoría tienen el mismo objetivo que el Sniffing, obtener la información sin modificarla, además de interceptar el tráfico de red, el atacante captura los documentos, mensajes e-mail y otra información guardada, descargando en la mayoría de los caso esa información a su propia computadora.

El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software. Los casos más resonantes de este tipo de ataques fueron: el robo de un archivo con más de 1700 números de tarjetas de crédito desde una compañía de música mundialmente famosa, y la difusión ilegal de reportes oficiales reservados de las Naciones Unidas, acerca de la violación de derechos humanos en algunos países europeos en estado de guerra.

3.1.4. SHOULDER SORFING

Consiste en el espionaje físico a los usuarios de las PCs para obtener el usuario y su contraseña correspondiente, mediante la explotación de las malas prácticas de seguridad de los usuarios como por ejemplo el hecho de tener las contraseñas anotas en papelitos pegados en el monitor.

3.1.5. ESCANEO DE PUERTOS

La idea es enviar una serie de paquetes para varios protocolos y se deduce que servicios están escuchando mediante las respuestas recibidas o no recibidas, hay diversos tipos de scanning según técnicas, puertos y protocolos explotados.

¿Por qué es peligroso tener un puerto abierto?

Al fin y al cabo los puertos son puntos de acceso a aplicaciones corriendo en un ordenador. Aunque en teoría no fuese un problema, estas aplicaciones pueden tener vulnerabilidades que pueden ser aprovechadas por otros usuarios. Desde el punto de vista de seguridad, es recomendable permitir el acceso sólo a los servicios que sean imprescindibles, dado que cualquier servicio expuesto a Internet es un punto de acceso potencial para intrusos.

También es recomendable el funcionamiento sigiloso para no dar facilidades a los *hackers*. Algunos *hackers* hacen exploraciones aleatorias de IPs y puertos por Internet, intentando identificar las características de los sistemas conectados, y creando bases de datos con estas. Cuando se descubre una vulnerabilidad, están en disposición de atacar rápidamente a las máquinas que se sabe que son del tipo vulnerable.

Comprobar el estado de un determinado puerto es una tarea muy sencilla; incluso es posible llevarla a cabo desde la línea de órdenes, usando una herramienta tan genérica como telnet. Por ejemplo, imaginemos que queremos conocer el estado del puerto 5000 en la máquina cuya dirección IP es 192.168.0.10; si el telnet a dicho puerto ofrece una respuesta, entonces está abierto y escuchando peticiones:

```
anita:~$ telnet 192.168.0.10 5000
Trying 192.168.0.10...
Connected to 192.168.0.10.
Escape character is '^]'.
^D
Connection closed by foreign host.
anita:~$
```

Si por el contrario el puerto está abierto pero en él no hay ningún demonio atendiendo peticiones, la respuesta será similar a la siguiente:

```
anita:~$ telnet 192.168.0.10 5000
Trying 192.168.0.10...
telnet: Unable to connect to remote host: Connection refused
anita:~$
```

Por último, si el puerto está protegido por un cortafuegos, lo más probable es que no obtengamos respuesta alguna; el telnet lanzado se quedará intentando la conexión hasta que se produzca un *timeout* o hasta que lo paremos manualmente:

```
anita:~$ telnet 192.168.0.10 5000
Trying 192.168.0.10...
^D
anita:~$
```

3.2.ATAQUES DE AUTENTICACIÓN

Tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y contraseña.

3.2.1. SPOOFING

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.

DNS Spoofing

Este ataque hace referencia al falseamiento de una dirección IP ante una consulta de resolución de nombre (esto es, resolver con una dirección falsa un cierto nombre DNS), o viceversa (resolver con un nombre falso una cierta dirección IP). Esto se puede conseguir de diferentes formas, desde modificando las entradas del servidor encargado de resolver una cierta petición para falsear las relaciones dirección-nombre, hasta comprometiendo un servidor que infecte la caché de otro (lo que se conoce como DNS Poisoning); incluso sin acceso a un servidor DNS real, un atacante puede enviar datos falseados como respuesta a una petición de su víctima sin más que averiguar los números de secuencia correctos.

Web Spoofing

Este ataque permite a un pirata visualizar y modificar cualquier página web que su víctima solicite a través de un navegador, incluyendo las conexiones seguras vía SSL.

Para ello, mediante código malicioso un atacante crea una ventana del navegador correspondiente, de apariencia inofensiva, en la máquina de su víctima; a partir de ahí, enruta todas las páginas dirigidas al equipo atacado - incluyendo las cargadas en nuevas ventanas del navegador - a través de su propia máquina, donde son modificadas para que cualquier evento generado por el cliente sea registrado.

3.2.2. SPOOFING LOOPING

El envío de falsos e-mails es otra forma de Spoofing que las redes permiten. Aquí el atacante envía e-mails a nombre de otra persona con cualquier motivo y objetivo. Tal fue el caso de una universidad en EE.UU. que en 1998, que debió reprogramar una fecha completa de exámenes ya que alguien en nombre de la secretaría había cancelado la fecha verdadera y enviado el mensaje a toda la nómina de estudiantes.

Muchos ataques de este tipo comienzan con Ingeniería Social, y los usuarios, por falta de cultura, facilitan a extraños sus identificaciones dentro del sistema usualmente través de una simple llamada telefónica.

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.

3.2.3. BACKDOORS

Son trozos de código en un programa que permite a quien las conoce saltarse los métodos usuales de autenticación para realizar ciertas tareas que requieren privilegios de usuarios.

Por lo general los programadores las crean a propósito para poder probar los sistemas mientras están en fases de desarrollo, saltándose así los procesos de autenticación, permitiéndole así realizar cualquier actividad posible en el programa.

3.2.4. EXPLOITS

Son programas que aprovechan los errores de diseño en los sistemas hardware o software, con el fin de poder acceder a los mismos.

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.

3.2.5. MAN IN THE MIDDLE

El atacante se interpone entre el origen y el destino, logrando de esta manera interceptar el tráfico de red que fluye entre los dos puntos sin el conocimiento de las víctimas.

3.2.6. FORZADO DE CONTRASEÑA

Consiste en probar una a una las posibles contraseñas hasta que se logre atinar a la contraseña del usuario, existen dos posibles formas para la prueba de contraseñas, las cuales son:

Mediante el uso de un diccionario.- el cual cuenta con una gran lista de posibles contraseñas, entre las cuales se hallan *palabras,secuencias y nombres*; las mismas que gran porcentaje de los usuarios utilizan normalmente como contraseñas, razón por la cual es el método más utilizado, pero en caso de que la contraseña no se encuentre en el diccionario referencia, no se encontrará la contraseña.

Mediante el uso de todas las posibles combinaciones de caracteres.- esta característica busca secuencialmente la contraseña, por ejemplo desde "aaaa" hasta "zzzz" esta es la forma más segura de encontrar contraseñas, pero no es la más rápida, dependiendo del tamaño de la contraseña, podría demorar incluso miles de años la búsqueda de la contraseña.

Este método resulta ventajoso cuando la contraseña a buscar sea numérica o de un solo tipo de carácter, por ejemplo mayúsculas.

En la tabla podemos observar el tiempo de búsqueda de una clave de acuerdo a su longitud y tipo de caracteres utilizados. La velocidad de búsqueda se supone en 100.000 passwords por segundo, aunque este número suele ser mucho mayor dependiendo del programa utilizado.

El uso de varios tipos de caracteres así como la cantidad de dígitos utilizados en una contraseña aumenta de manera exponencial la seguridad de los mismos.

Cantidad de Caracteres	26-Letras minúsculas	36-Letras y dígitos	52-Mayúsculas y minúsculas	96-Todos los caracteres
6	51 minutos	6 horas	2,3 días	3 meses
7	22,3 horas	9 días	4 meses	24 años
8	24 días	10,5 meses	17 años	2.288 años
9	21 meses	32,6 años	890 años	219.601 años
10	45 años	1.160 años	45.840 años	21.081.705 años

3.3. ATAQUES DE MODIFICACIÓN

3.3.1. TAMPERING O DATA DIDDLING

Hace referencia a la modificación no autorizada de datos o el software instalado en el sistema víctima, Son innumerables los casos de este tipo como empleados bancarios que crean falsas cuentas para derivar fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes, o contribuyentes que pagan para que se les anule la deuda por impuestos en el sistema municipal.

Múltiples Web Sites han sido víctimas del cambio en sus páginas por imágenes (o manifiestos) terroristas o humorísticos, como el ataque de The Mentor, ya visto, a la NASA.

3.3.2. MALEWARE

Término utilizado para todo tipo de código que resulta molesto o dañino para un computador, entre las categorías que abarca el término malware están:

Los virus, Gusanos, Caballos de Troya, Spyware, etc.

Bombas lógicas

> Un ex-empleado descontento de UBS PaineWebber activó una bomba lógica que provocó en la red informática de la corporación daños valorados en 3 millones de dólares, según informó Oxygen.
>
> 19 diciembre 2002
>
> La bomba lógica, que actuó como un virus, afectó a cerca de 1.000 ordenadores -de los 1.500 que integran la red de sucursales de UBS PaineWebber en Estados Unidos-, eliminando y dañando archivos.
> El empleado, llamado Roger Duronio, intentó aprovechar una previsible caída en la Bolsa de las acciones de la empresa para beneficiarse económicamente. Sin embargo, sus planes fracasaron, ya que el precio de las acciones no bajó tras el ataque.
> Roger Duronio, que abandonó la compañía 10 días antes del incidente, se había quejado en varias ocasiones por su sueldo y por las primas. Fue acusado federalmente por fraude de la seguridad y en la conexión con los ordenadores. Cada acusación puede acarrearle hasta 10 años en prisión. Por su parte, el fraude en la seguridad contempla multas de hasta 1 millón de dólares, mientras que en el fraude informático la multa máxima asciende a 250.000 dólares.

3.4. VARIOS

3.4.1. INGENIERÍA SOCIAL

Imaginemos que un usuario de una máquina recibe el siguiente correo electrónico:

> From: Super-User <root@sistema.com>
> To: Usuario <user@sistema.com>
> Subject: Cambio de clave
>
> Hola,
> Para realizar una serie de pruebas orientadas a conseguir un óptimo funcionamiento de nuestro sistema, es necesario que cambie su clave mediante la orden 'password'. Hasta que reciba un nuevo aviso (aproximadamente en una semana), por favor, asigne a su contraseña el valor 'PEPITO' (en mayúsculas).
> Rogamos disculpe las molestias. Saludos,
>
> Administrador

Si el usuario no sabe nada sobre seguridad, es muy probable que siga al pie de la letra las indicaciones de este *e-mail*; pero nadie le asegura que el correo no haya sido enviado por un atacante - es muy fácil camuflar el origen real de un mensaje -, que consigue así un acceso al sistema: no tiene más que enviar un simple correo, sin complicarse buscando fallos en los sistemas operativos o la red, para poner en juego toda la seguridad. Sin saberlo, y encima pensando que lo hace por el bien común, el usuario está ayudando a romper todo el esquema de seguridad de nuestra máquina.

También es posible que intente engañar al propio administrador del sistema. Por ejemplo, imaginemos que la máquina tiene el puerto *finger* abierto, y el atacante detecta un nombre de usuario que nunca ha conectado al sistema; en este caso, una simple llamada telefónica puede bastarle para conseguir el acceso:

> **Administrador:**
> Buenos dias, aquí área de sistemas, en qué podemos ayudarle?
> **Atacante:**
> Hola, soy José Luis Pérez, llamaba porque no consigorecordar mi*contraseña* en la máquina *sistema.upv.es*.
> **Administrador:**
> Un momento, me puede decir su nombre de usuario?
> **Atacante:**
> Sí, claro, es jlperez.
> **Administrador:**
> Muy bien, la nueva contraseña que acabo de asignarle es *pepito*. Por favor, nada más conectar, no olvide cambiarla.
> **Atacante:**
> Por supuesto. Muchas gracias, ha sido muy amable.
> **Administrador:**
> De nada, un saludo.

Ahora es el *root* quien facilita la entrada del atacante en la máquina; lo único que este ha necesitado es un nombre de usuario válido.

5.2.2. INGENIERÍA SOCIAL INVERSA

Esta es una conversación entre dos usuarios de los juegos online de STEAM,

Greg_ValveOLS dice:	buenas tardes
br0kenrabbit dice:	qué pasa?
Greg_ValveOLS dice:	mi nombre es greg y soy miembro del equipo de Soporte online de Valve
br0kenrabbit dice:	por messenger?
Greg_ValveOLS dice:	si
br0kenrabbit dice:	y bien?
Greg_ValveOLS dice:	Hemos 'loggeado' múltiples ips desde su cuenta y necesitamos verificar su información
br0kenrabbit dice:	Mi información?
Greg_ValveOLS dice:	creemos que alguien puede haber robado su cuenta mmmm no ha compartido la información de su cuenta con nadie, verdad?
br0kenrabbit dice:	No. Ni siquiera la tengo escrita.
Greg_ValveOLS dice:	hmmm quizá tiene algún 'keylogger' en tu PC y necesita formatear
br0kenrabbit dice:	Pues bueno….
Greg_ValveOLS dice:	si me verificase los datos de su cuenta puedo asegurarme de que sólo su ip tenga acceso. Es un nuevo sistema de seguridad que estamos probando porque esto pasa mucho. los nombres de usuario y contraseña ya no son seguros, sabe?
br0kenrabbit dice:	Bueno
Greg_ValveOLS dice:	no se preocupe, es una conexión segura
br0kenrabbit dice:	Puedo ser sincero contigo, Greg?
Greg_ValveOLS dice:	si
br0kenrabbit dice:	Mira, no se cómo has conseguido esta cuenta de Messenger, ni me importa. Al contrario que tú, yo SI trabajo para Valve. Traza mi ip y lo verás.
Greg_ValveOLS dice:	huh?
br0kenrabbit dice:	Trázala.
Greg_ValveOLS dice:	cómo
br0kenrabbit dice:	Inicio/Ejecutar/cmd escribes Tracert y luego mi dirección IP y luego le das a Enter.
Greg_ValveOLS dice:	ah si
br0kenrabbit dice:	Como empleado, se que los empleados de Valve NUNCA contactan con los usuarios por el Messenger. También se que un empleado de Valve NUNCA pediría a un usuario su contraseña. Voy a cerrar temporalmente tu cuenta en Steam.
Greg_ValveOLS dice:	por qué?
br0kenrabbit dice:	Has leído el 'ToS'?
Greg_ValveOLS dice:	Tod? tos?
br0kenrabbit dice:	'Términos del Servicio'
Greg_ValveOLS dice:	dónde?
br0kenrabbit dice:	Greg, es una infracción muy seria del 'ToS'. Corres el riesgo de perder tu cuenta.
Greg_ValveOLS dice:	por qué?
br0kenrabbit dice:	Te acabo de decir por qué
Greg_ValveOLS dice:	:S
br0kenrabbit dice:	Necesito tus datos si quieres que desbloquee tu cuenta. Te voy a amonestar pero sólo te suspenderé la cuenta durante tres días, ya que es tu primera infracción, de acuerdo?
Greg_ValveOLS dice:	si
br0kenrabbit dice:	Primero, cuál es el nombre al que está registrada. No el usuario, sino el nombre de la persona real que creó la cuenta. Es para verificarlo.
Greg_ValveOLS dice:	xxxxxxxxxxx
br0kenrabbit dice:	¿Eres tú?
Greg_ValveOLS dice:	si

br0kenrabbit dice:	Muy bien, y cuál es el usuario
Greg_ValveOLS dice:	xxxxxxxx
br0kenrabbit dice:	Muy bien.
br0kenrabbit dice:	Veo que has comprado unos cuántos de nuestros juegos, gracias
Greg_ValveOLS dice:	algunos
br0kenrabbit dice:	Siempre conectas desde la misma IP?
Greg_ValveOLS dice:	si
br0kenrabbit dice:	Y cuál es tu proveedor de internet, tu ISP?
Greg_ValveOLS dice:	xxxxxxx
br0kenrabbit dice:	Gracias. Un momento, por favor, déjame verificar esta información.
Greg_ValveOLS dice:	podré jugar esta noche?
br0kenrabbit dice:	Cuál es tu ciudad de residencia? Depende de si cooperas. De momento vas bien.
Greg_ValveOLS dice:	xxxxxx
br0kenrabbit dice:	xxxxxx?
Greg_ValveOLS dice:	si
br0kenrabbit dice:	Muy bien. Y cuál es el password asociado a esta cuenta?
Greg_ValveOLS dice:	xxxxxxx
br0kenrabbit dice:	Muy bien. No intentes conectarte ahora al Steam. Si estás conectado, tienes que desconectar.
Greg_ValveOLS dice:	por?
br0kenrabbit dice:	Para que pueda actualizar tu cuenta.
Greg_ValveOLS dice:	voy a poder jugar esta noche? hay pelea del 'clan' no ganarán sin mi, jeje
br0kenrabbit dice:	Jeje. Tendrás que esperar unos minutos. Estás desconectado?
Greg_ValveOLS dice:	si
br0kenrabbit dice:	Muy bien. Dame sólo un momento.
br0kenrabbit dice:	Intenta conectarte ahora.
Greg_ValveOLS dice:	No puedo conectarme. Dice 'loginfailed'! qué pasa??qué #&%$%&# pasa?!?!
br0kenrabbit dice:	Greg
Greg_ValveOLS dice:	me has engañado!?POR QUE??
br0kenrabbit dice:	Greg
Greg_ValveOLS dice:	qué
br0kenrabbit dice:	Valve nunca pide el usuario y contraseña.
Greg_ValveOLS dice:	quéeee?
br0kenrabbit dice:	Yo no trabajo para Valve, pero a ti te acabo de #&%$%&# (OWNED!)
Greg_ValveOLS dice:	no puede ser, qué #&%$%&# por qué??
br0kenrabbit dice:	¿Por qué querías tú robarme la cuenta?
Greg_ValveOLS dice:	no quería
br0kenrabbit dice:	¿Entonces para qué me pedías los datos?
Greg_ValveOLS dice:	Por favor!!solo quería gastar una broma pero tio, te lo juro que no quería devuélveme mi cuenta porfavooooooorrrrr!!! sólo tengo 13 años y ahorré todo un año para comprarla
br0kenrabbit dice:	Greg
Greg_ValveOLS dice:	qué
br0kenrabbit dice:	Que te sirva de lección, #&%$%&#

En este ejemplo se ve claramente como el atacante trata de engañar a la víctima, pero la victima sabia claramente que se trataba de un ataque y espero el momento oportuno para invertir el ataque, de esta forma el atacante se convierte en víctima y la victima en atacante, logrando obtener datos de inicio de sesión del atacante y cambiando la clave de acceso para que no pueda volver a ingresar al sistema.

5.2.3. TRASHING

Por lo general una persona, tiene anotada su su usuario y contraseña en un pequeño papel, cuando lo memoriza lo desecha, esta acción es aprovechada por un atacante, el cual revisa las papeleras en búsqueda de información, contraseñas o directorios, para poder obtener información importante.

El trashing también puede ser lógico, en el caso de revisar archivos eliminados en la papelera de reciclaje o revisando el buffer de la impresora y memorias.

5.2.4. CANALES OCULTOS

Permite a un proceso receptor y a un emisor intercambiar información de forma que viole la política de seguridad del sistema, esencialmente se trata de un método de comunicación que no es parte del diseño original. Los canales ocultos existen solamente en sistemas con seguridad multinivel, aquellos que contienen y manejan información con diferentes niveles de sensibilidad, de forma que se permite acceder simultáneamente a varios usuarios a dicha información, pero con diferentes puntos de vista de la misma.

5.2.5. CONTROL REMOTO DE EQUIPOS

Un atacante puede tomar el control total del equipo de forma remota y sin autorización mediante la utilización de programas desarrollados para tal fin, e instalados por el atacante mediante la utilización de un troyano, de esta forma podrá tener acceso a toda la información del usuario.

5.2.6. ROBO DE EQUIPAMIENTO O COMPONENTES

El robo puede involucrar todo un equipo o de parte del mismo, ej.: un disco rígido. Puede ocurrir por un deficiente control de acceso establecido al centro de cómputos (o recinto donde residen los equipos: servidores, routers, switches, etc.), así como a las propias instalaciones del Organismo.

Se debe tener un control de accesos hacia las diferentes áreas de la empresa, mediante el uso de tarjetas de identificación.

5.3. ANÁLISIS DE LAS AMENAZAS

5.3.1. TABLA ANALÍTICA DE AMENAZAS.

ATAQUES DE MONITORIZACIÓN				
AMENAZA	**CARACTERISTICAS**	**OBJETIVOS**	**VICTIMAS**	**MEDIOS**
DECOY	Programas que simulan la solicitud de inicio de sesión.	Obtener datos de inicio de usuario y contraseñas para el acceso a un sistema.	Usuarios y administradores	Redes y equipos locales.
KEY LOGGERS	Programas o software cuyo función es registrar las pulsaciones del usuario	Obtener usuarios, claves de acceso o cuentas bancarias	Usuarios y administradores	PCs y Servidores
EAVES DROPPING	Intercepta información que no le iba dirigida.	Capturar información privilegiada y claves para obtener acceso a más información sin que nadie se dé cuenta	Usuarios	Redes empresariales Cableadas y inalámbricas
SNOOPING	Intercepción y copia de información (correo, fotos, etc.)	Analizar los archivos en busca de información útil para el atacante.	Usuarios y administrados	Redes
SHOULDER SURFING	Espionaje físico a los usuarios. Revisa oficinas en busca de documentos útiles.	Buscar información útil como usuarios, contraseñas o cuentas bancarias	Usuarios y administradores	Oficinas o habitaciones
ESCANEO DE PUERTOS	Aprovecha los puertos abiertos de los ordenadores	Analizar los archivos en busca de información útil para el atacante.	Usuarios y administradores	Redes empresariales e internet
ATAQUES DE AUTENTICACIÓN				
AMENAZA	**CARACTERISTICAS**	**OBJETIVOS**	**VICTIMAS**	**MEDIOS**
SPOOFING	Modificación de ip, macaddress o web, de esta forma asume otra identidad.	Actuar en nombre de otros usuarios.	Usuarios y administradores	Redes empresariales
EXPLOITS	Explota agujeros de seguridad de los programas o del hardware.	Obtener accesos o privilegios de usuarios.	Usuarios o administradores	Equipos o redes

SPOOFING – LOOPING	Realiza las actividades desde diferentes equipos.	Actuar en nombre de otros usuarios.	Usuarios y administradores	Redes empresariales e internet
FORZADO DE CONTRASEÑAS	Consiste en la búsqueda de la posible clave de acceso al sistema	Acceder al sistema de la víctima.	Usuarios o administradores	Redes empresariales y equipo
BACKDOORS	Trozos de código de los programas que permiten saltarse los métodos de autenticación.	Obtener privilegios de usuario.	Usuarios o administradores	Equipos o redes
MAN IN THE MIDDLE	Se interpone entre el origen y el atacante.	Conocer o modificar el contenido de la información.	Usuarios y servidores	Red empresarial e internet.
DHCP STARVATION	Busca reemplazar el servidor DHCP	Asigna a los usuarios ips y otras informaciones a su conveniencia	Usuarios y administradores	Red empresarial e internet
ATAQUES DE MODIFICACIÓN				
AMENAZA	**CARACTERISTICAS**	**OBJETIVOS**	**VICTIMAS**	**MEDIOS**
DESBORDAMIENTO DE CAM	Inunda la tabla de direcciones de un swich	Bloquear la capacidad de que los paquetes lleguen a su destino	Usuarios y administradores	Internet y redes empresariales.
DHCP STARVATION	Reemplaza el servidor DHCP	Asignar informaciones a los usuarios según conveniencia, logrando interceptar información que los clientes envían	Usuarios y administradores	Internet y redes empresariales
TAMPERING O DATA DIDDLING	Modificación o eliminación desautorizada de los datos o el software instalado.	Perjudicar al usuario victima con actividades laborales	PCs y servidores	Internet y redes empresariales
CODIGO MALICIOSO O MALEWARE	Código instalado en una maquina (virus, troyanos, conejos, gusanos, bombas lógicas)	Dañar o alterar el funcionamiento de normal de un sistema, o enviar información privada sin autorización.	Usuarios y servidores	Internet

VARIOS				
AMENAZA	**CARACTERISTICAS**	**OBJETIVOS**	**VICTIMAS**	**MEDIOS**
INGENIERIA SOCIAL	Aprovecha la ingenuidad de las personas. No necesita nivel elevado de conocimientos tecnológicos.	Lograr acceder a las cuentas de los usuarios, de esta forma tiene acceso a todo el sistema.	Usuarios y administradores	Redes empresariales e internet
INGENIERIA SOCIAL INVERSA	Mismas características de la ingeniería social.	Obtener información de los usuarios con usuarios y contraseñas o cuentas bancarias.	Usuarios y administradores	Redes empresariales e internet
TRASHING	Busca en los basureros de las oficinas. Revisa buffers de impresora. Aprovecha las malas costumbres de los usuarios.	Obtener claves de usuario y contraseñas para obtener acceso a los computadores.	Usuarios y administradores	Redes empresariales e internet.
CANALES OCULTOS	Intercambio de información violando políticas de seguridad	Realizar actividades que normalmente no son posibles para ciertos usuarios	Usuarios y administradores	Redes empresariales
CONTROL REMOTO DE EQUIPOS	El atacante toma el control total del equipo de forma remota	Tomar el control total del equipo	Usuarios y administradores	Redes e internet
ROBO DE EQUIPOS O COMPONENTES	Robo o hurto de equipos o dispositivos con información	Conseguir información confidencial de la victima	Usuarios y administradores	Oficinas y casas

5.3.2. AMENAZAS A CONSIDERACIÓN EN EL MANUAL

A continuación se realiza un análisis de las técnicas que intervienen de forma directa con el robo de archivos en redes empresariales mediante conexión WIFI.

INGENIERIA SOCIAL E INGENIERIA SOCIAL INVERSA

Es una de las amenazas que tiene más éxito a la hora de los ataques a los usuarios, consiguiendo información de la forma más segura.

Esta amenaza interviene directamente en el manual, ya que uno de los medios utilizados para esta práctica es la red empresarial.

Para cuidarse de esta amenaza, es necesario tener mayores conocimientos acerca de procedimientos de seguridad de la empresa, que por lo general son dictador por el administrador del sistema, pero tenga en cuenta que por ninguna causa los administradores de los sistemas requieren contraseñas de acceso para realizar mantenimientos de cuenta de ningún tipo.

TRASHING

Por lo general las personas tienen esta práctica de anotar contraseñas en papelitos y una vez memorizados lo desechan sin preocupación alguna.

Esta amenaza, requiere la presencia física del atacante en la oficina y se pueden obtener claves de acceso, pero debe ser considerada en el manual.

Se le recomienda al usuario memorizar la contraseña asignada lo más pronto posible, (inmediatamente) y una vez memorizada destruir el papel (quemándolo o rompiéndolo en varias partes), de esta forma se evitará este tipo de inconvenientes.

DECOY

Esta técnica imita las pantallas de acceso a los sistemas, son difíciles de detectar, y también muy efectivos a la hora del ataque, pero para lograr este ataque, el atacante tiene que instalar en el PC de la víctima el programa decoy.

Este es otra amenaza de la cual se debe tener en cuenta, ya que se pueden conseguir claves de acceso al PC o a un sistema, pueden suceder a través de la red o en la PC.

Para evitar este ataque, el usuario debe evitar el acceso físico de terceras personas a su equipo, también requiere de un cuidado lógico, el cual consiste en configurar el sistema operativo para funcionamiento en redes empresariales, que ya se lo explicara en la fase de desarrollo del manual

EAVESDROPPING Y SNOOPING

Esta técnica consiste en la intercepción del tráfico de red, y el método de intercepción varía según la tecnología de la red, de la misma forma también varía el tipo de protección para evitar el ataque, por lo generar se tiene que invertir en hardware cuya función es codificar los paquetes que viajan a través de la red.

Esta amenaza tendrá gran consideración debido a la facilidad con la que se puede obtener datos, se recomienda no ingresar datos de inicios de sesión si la red no está codificada recomendable en WPA2, y en caso de enviar programas útiles, codificarlo previamente antes del envio.

SHOULDER SURFING

Consiste en el espionaje físico de un usuario, desde observar por encima del hombro del usuario mientras este teclea la contraseña de acceso, hasta revisar físicamente el entorno laboral físico del usuario, en búsqueda de alguna información útil para el atacante.

Esta es otra de las técnicas peligrosas a tener en cuenta, aparentemente sin importancia pero con gran peligro, la recomendación para que no sucedan estos ataques es:

Que en lo posible no digitar claves de acceso frente a otra persona, aunque se trate de un compañero de igual forma, se recomienda tener cuidado con los documentos que requieren de un cuidado especial, debido a la alta confidencialidad de su contenido.

ESCANEO DE PUERTOS

La idea es pasar por todos y cada uno de los puertos, con el fin de revisar cuales son los que están avientos y vulnerables para atacar, esto se lo realiza enviando cierto tipo de paquetes a cada puerto dependiendo de la funcionalidad, esperando una respuesta del mismo, lo cual indicaría que el puerto está abierto.

Las razones por las que un puerto se puede abrir un puerto, es de forma intencional, para poder brindar servicios, por ejemplo de correo o servicios web, otra forma es la no intencional, que podría suceder mediante un maleware, el mismo que cuando es ejecutado envía una orden para abrir un puerto en el sistema.

Esta forma de ataque se la previene mediante el uso de un firewall, este tipo de programa monitorea e informa sobre los cambios de estado de los puertos e impide los accesos a equipos desconocidos.

SPOFFING

Ipspoofing, dnsspoofing y webspoofing, básicamente cualquiera de estos tipos de ataque realiza una suplantación de identidad, con el fin de realizar acciones maléficas a nombre de otro usuario, estos ataques son complicados de detectar, y debido a que realiza ataques a nivel de los servidores, este método no será tomado en cuenta al momento de la elaboración del presente manual.

ACCESS POINT SPOOFING

El atacante se hace pasar por un Access Point y el cliente piensa estar conectado a una red LAN verdadera, para defenderse de este ataque se recomienda asegurarse de la legitimidad de la red en la primera conexión, y configurarla para conexión automática.

BACKDOORS

Son trozos de código en un programa que permite saltarse los métodos de autenticación y realizar tareas que normalmente requieren autenticación de usuario, este tipo de ataque necesita realizar un estudio de las vulnerabilidades de los programas.

Para protegerse de esta amenaza, lo más recomendable, es mantener actualizado los programas, ya que mediante las actualizaciones se realizan correcciones de seguridad.

Este método de ataque se tendrá en cuenta, ya que es una de las formas que más éxito tienen a la hora de atacar un sistema, y se puede evitar actualizando los programas.

EXPLOITS

Son programas que aprovechan errores de diseño de equipos o de software, constantemente se publican nuevos errores de sistema, por lo tanto mantenerse informado acerca de herramientas para combatirlos es vital.

Este método de ataque también será tomado en cuenta, el sistema operativo es complejo y debido a esto pueden existir falencias que los atacantes pueden aprovechar para realizar sus ataques.

Para mantenerse protegido se recomienda mantener activado las actualizaciones automáticas del sistema operativo, ya que mediante estas actualizaciones se incluyen parches de seguridad que corrigen fallas de seguridad del sistema.

CANALES OCULTOS

Los usuarios realizar tareas que normalmente no podrían realizar mediante cierto proceso, esto se debe a una falla de diseño en los sistemas, y la forma de protegerse de este problema es corregir la falla de diseño.

KEYLOGGERS

Amenaza que no interviene directamente en el manual de seguridad, esta amenaza puede ser física o lógica, requiere que el atacante tenga contacto directo con el equipo.

La forma de protegerse frente a estas amenazas, con respecto al keylogger es evitar el acceso a terceras personas hacia el computador, tanto físicamente (como mantener la oficina con llave) como lógicamente (mediante el uso de contraseñas de acceso).

MALEWARE

Programas que tienen como objetivo alterar el funcionamiento del sistema, existen dentro de esta categoría, los spyware, que son programas que monitorean las actividades del usuario víctima, obteniendo así usuarios y contraseñas de acceso, también existen los troyanos, que se disfrazan de programas útiles, pero realizan actividades malignas como abrir un backdoor, para protegerse de estas amenazas es necesario la instalación de un antivirus.

CONTROL REMOTO DE EQUIPOS

El atacante toma el control total del equipo, mediante diferentes métodos de ataque, la primera línea de defensa contra este ataque son las contraseñas seguras, ya sea para acceder al sistema operativo como para proteger los archivos de alta prioridad.

CAPITULO IVMANUAL DE SEGURIDAD CONTRAROBO DE ARCHIVOS

4.1.INTRODUCCIÓN AL MANUAL

Mediante el uso de este manual se logrará un alto nivel de seguridad en los archivos de nuestro ordenador, de igual forma se alcanzará un elevado nivel de confianza por parte de los usuarios de los equipos al tener conocimiento de que su información está altamente protegida.

El presente manual de seguridad se desarrolló para equipos con sistema operativo Windows 7 funcionando en entornos de redes LAN empresarial, que se encuentran conectados mediante WIFI.

Se recomienda seguir al pie de la letra los pasos a seguir en el presente manual para asegurar la seguridad de los datos de los usuarios, empezando desde los productos recomendados en el presente manual así como sus respectivas configuraciones.

En caso de que el sistema operativo no sea Windows 7, se pueden implementar programas alternativos, compatibles con la versión o marca de sistema operativo en el que se va a implementar, de la misma forma, se puede implementar otros programas con funcionalidad similar en los sistemas operativos Windows 7, pero no se garantiza la efectividad del manual.

En caso de que los equipos en los que se desee implementar el manualya se encuentrenen uso, es decir que el equipo ya cuente con tiempo de trabajo o no se encuentre recién instalado, se recomienda una reinstalación del sistema operativo, con la finalidad de eliminar cualquier amenaza que ya se hallaubicado en el equipo e implementar las configuraciones planteadas en el presente manual.

Antes de iniciar debemos cuidarnos de los ataques de Ingeniería social, para lo cual con el simple hecho de no proporcionar información que sea solicitado por terceras personas, por ningún motivo, los administradores no necesitan estos datos para realizar actividades de mantenimiento.

4.2.RECOMENDACIONES PARA TRABAJAR EN REDES WIFI

Mediante las redes WiFi, la información viaja a través del aire, es decir que está libre a ser interceptada, se debe tener cuidado con la información que se envíe a través de este medio, mucho más si es que es de carácter de alta prioridad.

- En primer lugar debemos asegurarnos de que la red hacia donde nos vamos a conectar sea la correcta, existen la posibilidad de que un atacante simule ser un Access Point legítimo, el atacante configura la red con el nombre de la red original esperando una equivocación por parte de la víctima, la solución a este problema es asegurar que la primera conexión a la red WLAN sea correcta, de esta forma se puede configurar una conexión automática hacia la red correcta.

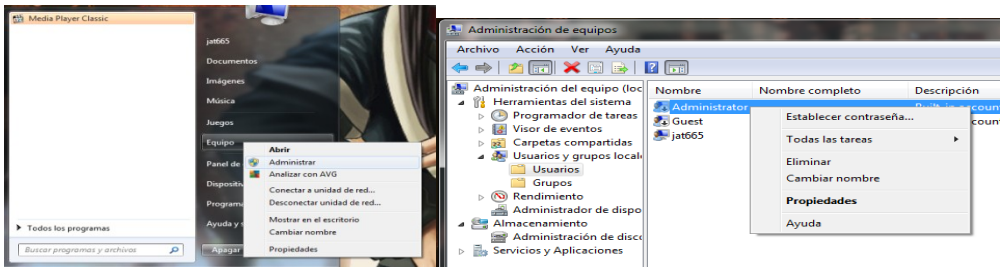
- Una vez conectada a la red, el firewall de Windows preguntara a qué tipo de red acaba de conectarse, se puede elegir entre una red pública, red doméstica o red de trabajo, si la red es publica, al seleccionar esta opción el firewall de Windows no permitirá compartir archivos en la red, y si la red es de trabajo o domestica permita compartir archivos mediante el uso de una clave de conexión.

- Otro punto a tener en cuenta son los ataques de vigilancia ”Sniffing” y “Snooping”, considerados los ataques más peligrosos, ya que un atacante tiene la posibilidad de ver las actividades que la víctima realiza, desde introducción de claves o contraseñas, datos introducidos hasta revisión de archivos y correo electrónico.
    - La solución a este problema sería evitar navegar en sitios que requieran autenticación como sitios web financieros o correos electrónicos cuando se navegue a través de redes WIFI, mucho menos si la red es pública (aeropuertos, parques, centros comerciales, etc.).
    - En casos de que se necesite enviar información cuyo contenido es importante a través de la red, se recomienda cifrar o codificar dicho archivo antes de enviarlo, de esta forma, si el archivo es interceptado, la información no será legible.

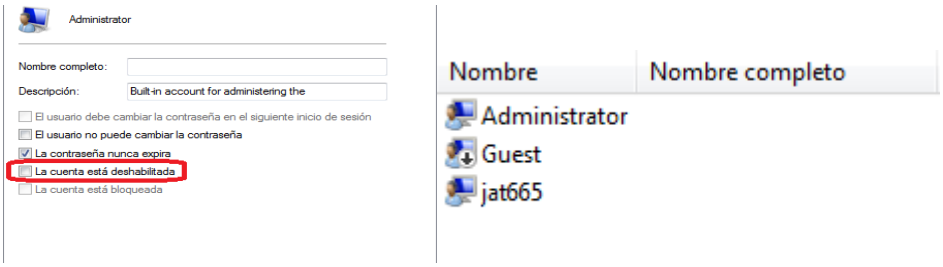
4.3.CONFIGURACIONES PREVIAS DEL SISTEMA OPERATIVO

4.3.1. CONFIGURACIÓN DE LA CUENTA ADMINISTRADOR W7

Antes de empezar con el uso del PC se recomienda colocar una contraseña en la cuenta administrador, para lo cual abrimos el administrador de tareas, para abrir el administrador de tareas nos dirigimos a Equipo y a continuación seleccionamos Administrar.



Una vez ubicados en la ventana de administración nos dirigimos a Usuarios y grupos locales, y finalmente seleccionamos la carpeta usuarios, en la parte central de la ventana se nos abre la lista de usuarios del equipo, La cuenta de Administrador e invitado aparece deshabilitada (una flecha visible al lado derecho del icono), damos clic derecho en la cuenta administrador y seleccionamos propiedades.

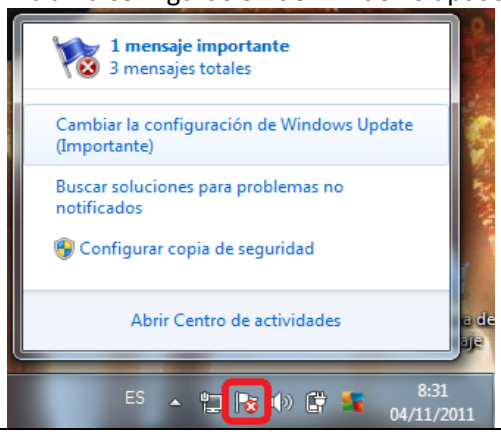
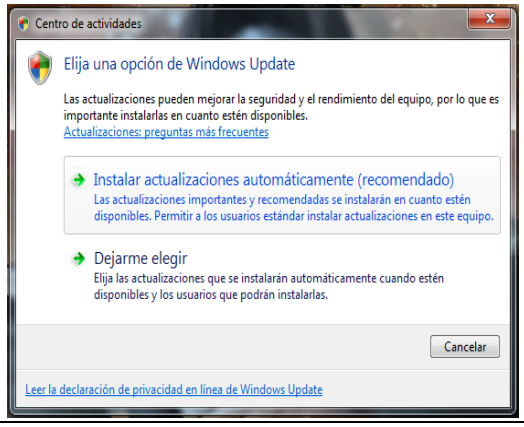


Desmarcamos la opción "la cuenta esta deshabilitada" y damos en aceptar, en la ventana de administración desaparece la flecha y ahora la cuenta administrador ya está habilitada. A continuación establecemos la contraseña mediante el panel de control, Cuentas de Usuarios y a continuación en la pantalla que sale seleccionamos administrar otra cuenta, buscamos Administrador y finalmente establecemos la contraseña, le damos en aceptar y listo.

Establecemos la contraseña (ver apartado para crear contraseñas seguras mas adelante) y seleccionamos aceptar, esta contraseña no debe olvidarse, se recomienda colocar un indicio de contraseña si es necesario, y regresamos a la desactivar la cuenta.

4.3.2. CONFIGURACIÓN DE ACTUALIZACIONES AUTOMÁTICAS

Antes que nada es de vital importancia configurar el sistema operativo para realizar actualizaciones automáticas de seguridad, debido a que el sistema operativo es muy complejo, es posible que durante el proceso de desarrollo del mismo existan varios agujeros de seguridad que pueden ser aprovechados por los atacantes, pero al configurar el sistema para actualizaciones automáticas de seguridad, se minimiza al máximo estos posibles ataques.

En la parte inferior izquierda buscamos una bandera, le damos clic y seleccionamos cambiar la configuración de Windows update 	Nos aparecerá la siguiente ventana, en la que seleccionamos instalar actualizaciones automáticas. 

4.3.3. PARTICIÓN DEL DISCO DURO

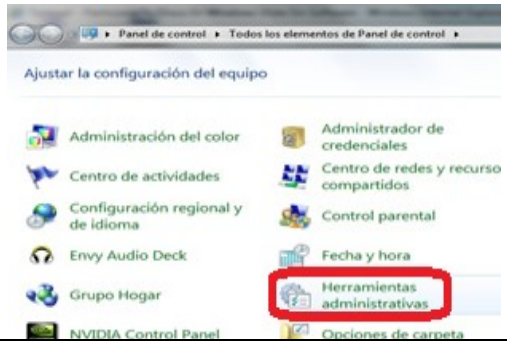
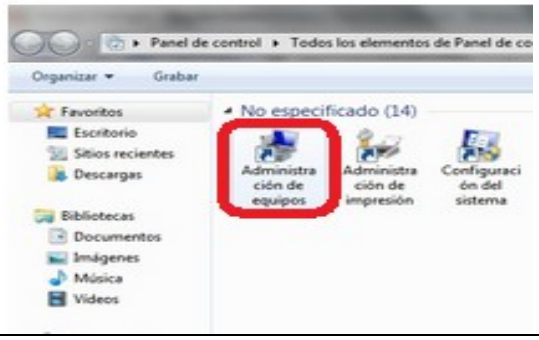
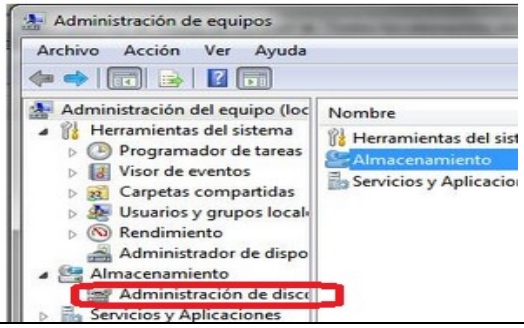
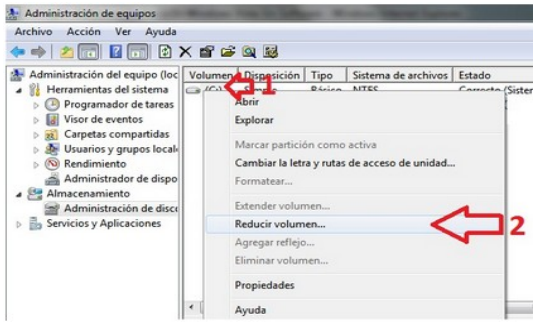
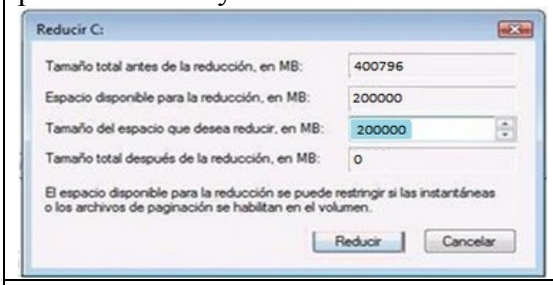
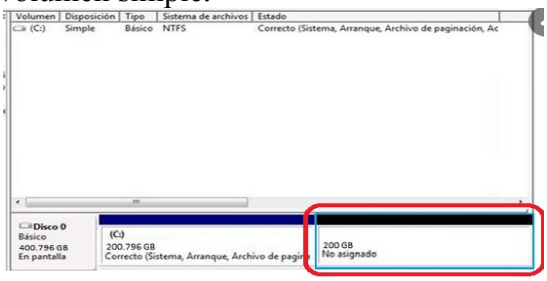
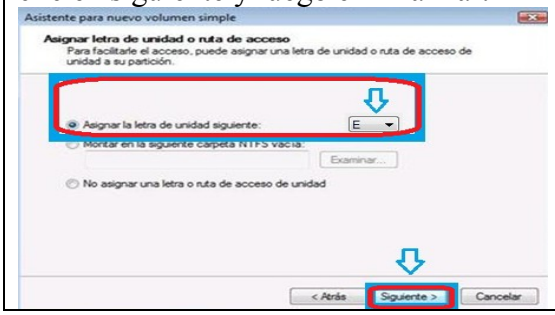
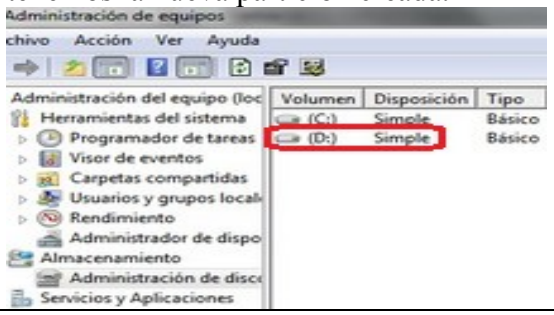
A continuación es necesario tener la información en otra partición lógica, a continuación vamos a ver las ventajas que logramos cuando tenemos la información en otra parte diferente a la del sistema operativo.

En primer lugar no disminuye el rendimiento del Sistema Operativo, ya que la partición del sistema operativo siempre queda libre de información adicional aparte de los programas instalados.

Otra ventaja es que si la PC se infecta de virus o es necesario formatearlo por para mejorar la versión del sistema operativo, se puede formatearlo sin ninguna preocupación, los datos del usuario quedaran intactos y en la otra partición del Disco.

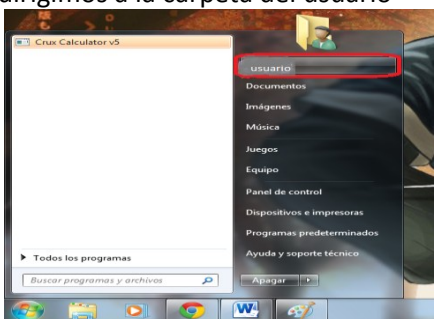
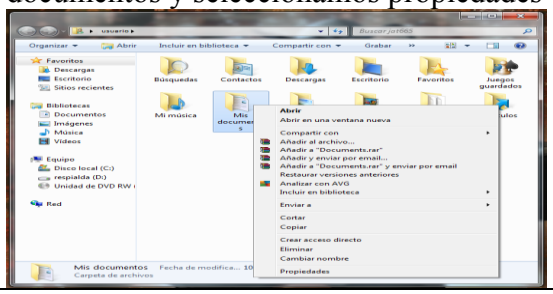
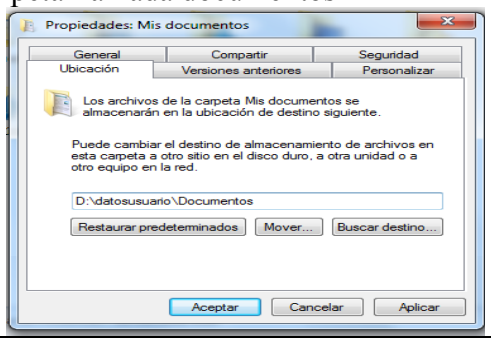
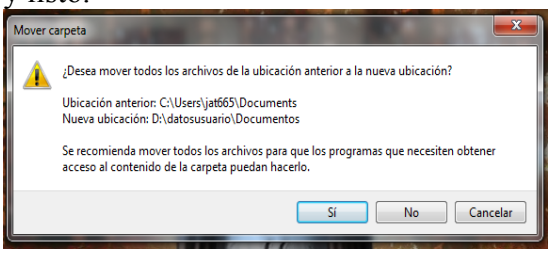
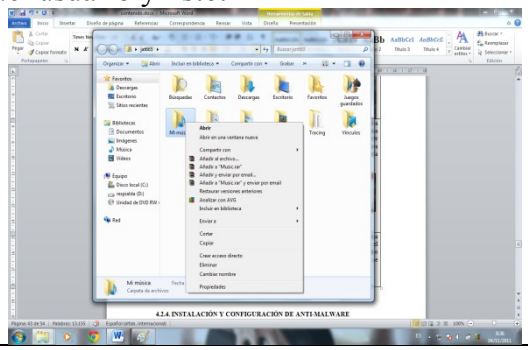
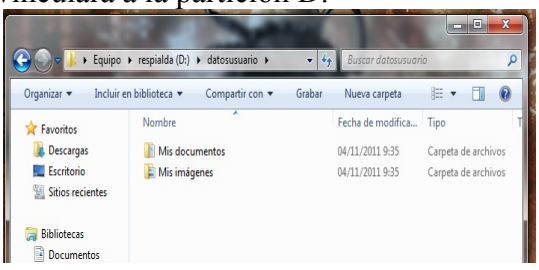
Ahora nos adentraremos en la configuración de la partición del disco.

El tamaño de la partición asignada para los datos del usuario depende directamente del tamaño total del disco duro, ya que la partición donde se encuentra el Sistema Operativo requiere de un espacio aproximado de 60 a 70 gigas, dependiendo del espacio que ocupen los programas que se utilicen en el equipo, el resto del Disco Duro que por lo generar debe ser de mayor tamaño, se los asigna para la nueva partición.

Primero nos dirigimos a panel de control y buscamos herramientas administrativas. 	Seleccionamos administración de dispositivos. 
Nos dirigimos a almacenamiento y luego a administración de discos. 	En la unidad c: damos clic derecho y seleccionamos reducir volumen. 
Colocamos el tamaño de la partición deseada, se recomienda que sea la partición de mayor tamaño. 	Damos clic derecho sobre la nueva partición creada y seleccionamos nuevo volumen simple. 
Elegimos el nombre de la unidad y damos clic en siguiente y luego en finalizar. 	Esperamos un tiempo y finalmente tenemos la nueva partición creada. 

4.3.4. CONFIGURACIÓN DE LA BIBLIOTECA DE DATOS DE WINDOWS

A continuación se presenta la forma de configurar el equipo para mayor comodidad en el tratamiento de archivos, mediante la vinculación directa de la biblioteca de datos de Windows a la partición D que es la partición asignada para los datos o archivos del usuario, con lo cual para almacenar los archivos, seguimos trabajando en la biblioteca organizada que nos ofrece el Sistema Operativo, pero nuestros datos se almacenan de forma segura y organizada en la partición D.

<table>
<tr>
<td>Nos dirigimos a la carpeta del usuario
 
</td>
<td>Damos clic derecho sobre mis documentos y seleccionamos propiedades
  </td>
</tr>
<tr>
<td>Luego seleccionamos la pestaña ubicación y a continuación la cambiamos a una ubicación en el disco D, dentro de una carpeta llamada documentos
 
</td>
<td>Si es que ya tenemos datos en la carpeta de mis documentos, nos visualiza una pantalla para preguntar si deseamos mover los datos a la nueva ubicación, le damos en aceptar que es la opción recomendada y listo.
 
</td>
</tr>
<tr>
<td>Realizamos los mismos pasos para el resto de carpetas ubicadas en la carpeta de datos del usuario y listo.
  </td>
<td>En el disco D se vendrá a armar una estructura similar a la que teníamos en el disco C, y a partir de ahora, cualquier dato que guardes, automáticamente se vinculará a la partición D.
 
</td>
</tr>
</table>

4.3.5. CONFIGURACIÓN DE FIREWALL DE WINDOWS

El firewall de Windows 7 tiene 3 configuraciones distintas para los 3 tipos de red:

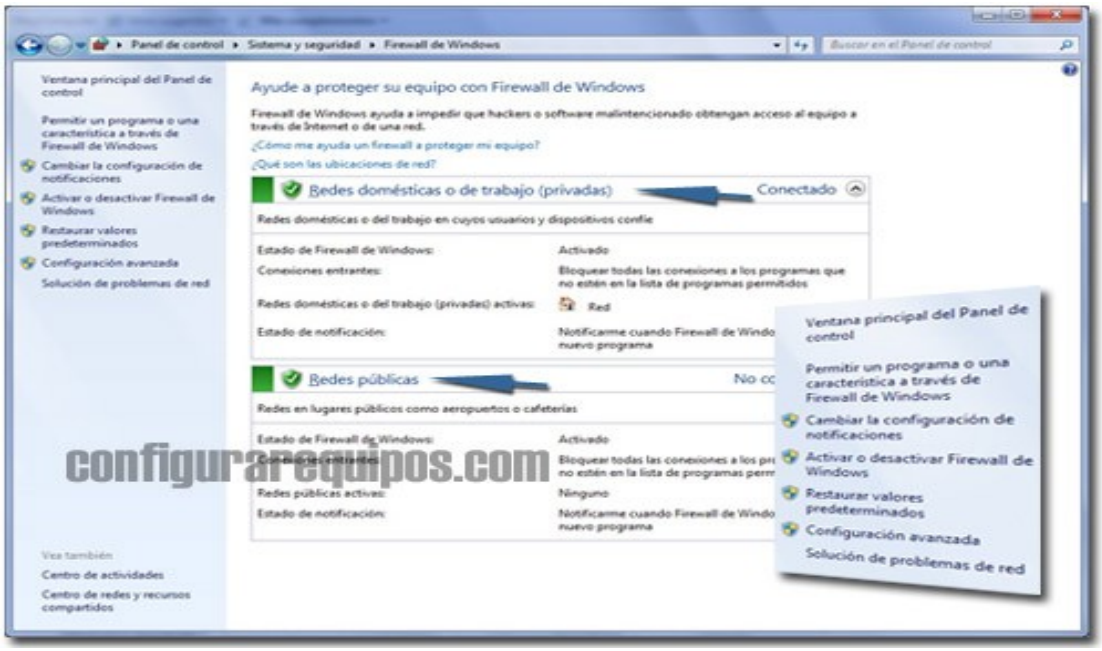
- Red Dominio
- Red Pública
- Red doméstica o de trabajo (red privada)

Para acceder al firewall de Windows 7, podremos hacerlo desde:

- Inicio> Panel de Control > Sistema de Seguridad > Firewall de Windows

  Una vez dentro, veremos las opciones básicas para activar el firewall de Windows 7 o desactivarlo. El sistema nos permite modificar las opciones por defecto para cada tipo de conexión por separado, pudiendo bloquear todas las conexiones entrantes, desactivar el firewall de Windows 7, que nos notifique cuando bloquee una conexión, etc.

Cuando nos queramos conectar a una red con Windows 7, será cuando seleccionemos el tipo de red y la protección del Firewall.



Las limitaciones de conectividad para los 3 tipos de redes en Windows 7, contemplan distintas condiciones de seguridad:

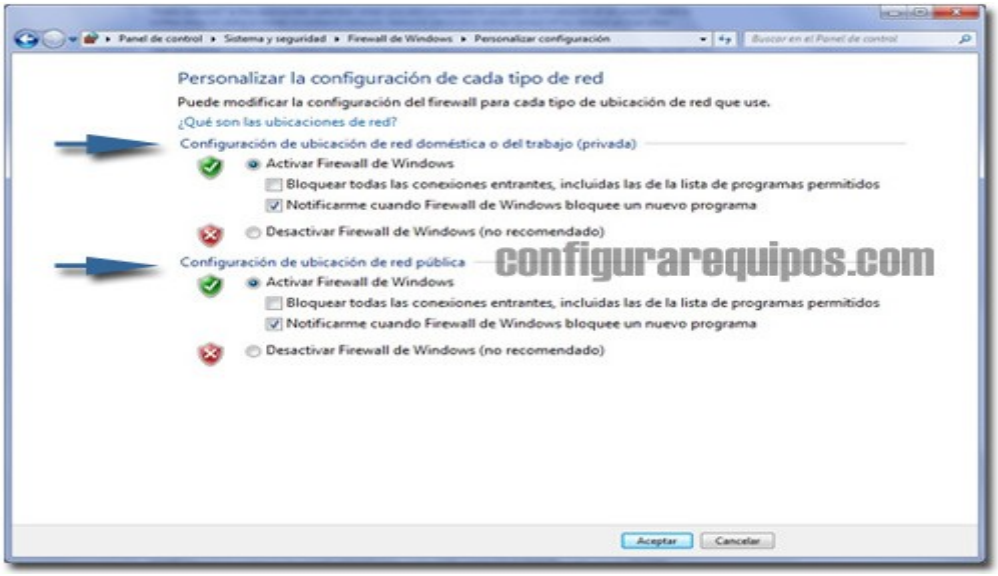
- Red pública en Windows 7: Para este tipo de red, Windows 7 no permite que otros ordenadores puedan localizarnos para compartir recursos.
- Red doméstica en Windows 7: Para este tipo de red, Windows 7 permite que nos podamos conectar a redes del tipo "grupo en el hogar", pudiendo compartir recursos en Windows 7 y que serán públicos para el resto de la red.

- Red de trabajo en Windows 7: En esta última situación, el firewall de Windows 7 no permite conectar a un grupo hogar, aunque si se puede compartir recursos con otros componentes de la red.

En las redes de trabajo, el firewall de Windows 7 permite acceder a la red mediante un dominio que podremos establecer en:

- Inicio > Panel de Control > Sistema de seguridad > Sistema > Configuración avanzada del sistema > Nombre del Equipo

Una vez estemos aquí, pulsaremos cambiar, y el controlador de dominio del Firewall reconocerá el modo de conexión de red dentro de un dominio.

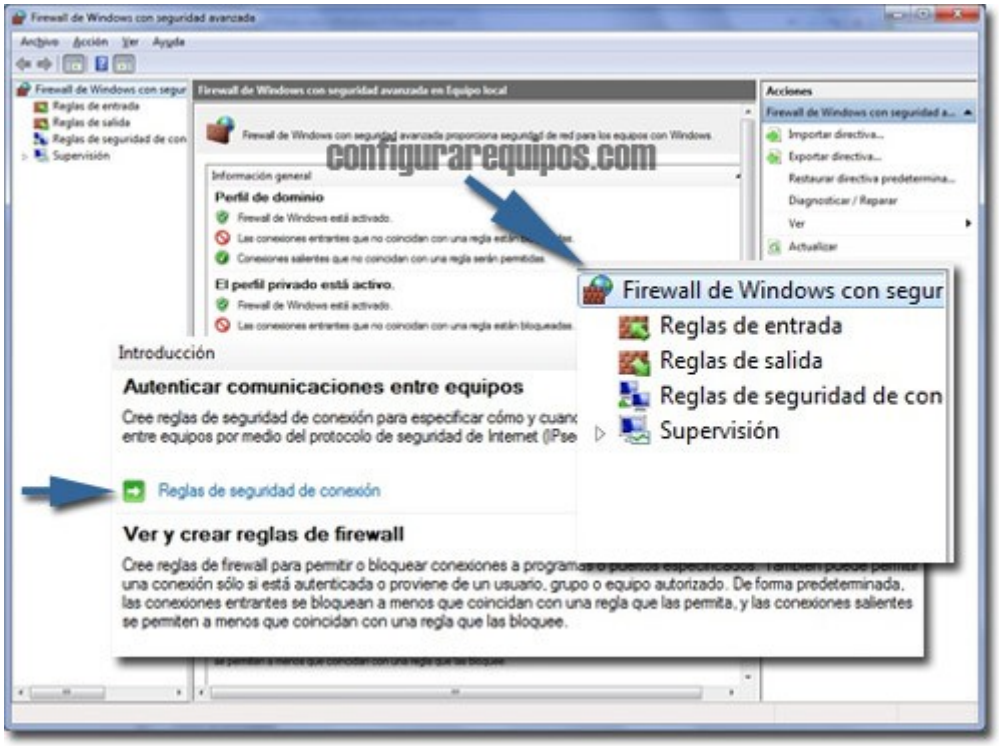


Una de las cosas que el firewall de Windows 7 ofrece, es la posibilidad de proteger 2 tipos de red al mismo tiempo, es decir, podemos crear dos redes distintas en Windows 7 y que la protección del firewall actúe por separado con respecto a cada red.

- Ejemplo: Si tenemos un ordenador portátil que usamos tanto en el trabajo como en casa, el firewall de Windows 7 nos permite crear 2 perfiles de protección distintos. De esta forma, podremos compartir ciertos recursos con los demás equipos de la oficina y bloquear el acceso a otros recursos que sólo estén autorizados para ordenadores que pertenezcan a la red doméstica.

CREAR REGLAS DE CONEXIÓN EN EL FIREWALL DE W7

Otra de las funciones que encontraremos al configurar el firewall de Windows 7, es que podemos crear y acceder a las reglas de conexión para cada tipo de red.



Podemos acceder a esta función desde la sección de Firewall de Panel de Control, y pulsando sobre Configuración Avanzada. Una vez dentro, podremos crear una regla de conexión.

En el centro de la ventana, pulsaremos sobre Ver y Crear reglas de firewall. Seguidamente sólo tendremos que seleccionar en Reglas de Entrada o Reglas de salida y especificar las características y parámetros para cada una de ellas.

El firewall de Windows 7 también ofrece una nueva función, y es que podemos definir un rango de puertos para las conexiones entrantes desde la misma consola con el que las conexiones entrantes deben de cumplir.

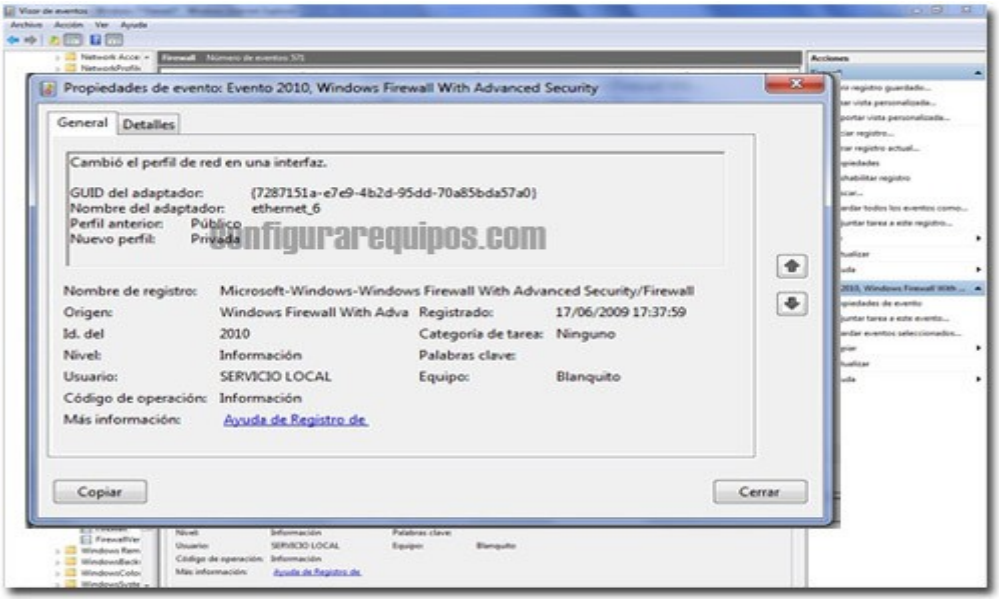
Registro de Eventos del firewall en Windows 7

Cuando se produce una incidencia en el firewall de Windows 7, se crea un log o registro donde se almacena la actividad y bloqueos de conexiones entrantes por parte del firewall.

En otras ediciones de Windows, para analizar el registro de incidencias sólo podíamos verlo desde un archivo de texto y buscar a mano alzada la incidencia relevante. El firewall de Windows 7 ahora permite configurar el Visor de eventos sin tener que

abrir un archivo de texto. Para acceder al archivo de incidencias abriendo el Visor de eventos, sólo tenemos que ir a:

- Menú Inicio > Registro de aplicaciones y servicios > Microsoft > Windows > Windows Firewall Advanced Security



Una vez que hayamos accedido a la entrada, podremos ver los eventos del firewall, filtrarlos, exportar el archivo, consultar los datos de cada evento, etc.

4.4.INSTALACIÓN Y CONFIGURACIÓN DE ANTI-MALWARE

DESCARGA E INSTALACION DE AVG ANTIVIRUS

Vaya a la página de descargas para obtener el archivo de instalación más reciente (una vez ahí, haga clic con el botón secundario en el archivo que necesite y guárdelo en el escritorio).

Si no sabe exactamente qué archivo elegir, seleccione el archivo del Administrador de descargas de AVG.

Si necesita descargar todo el archivo de instalación de AVG, utilice el archivo instalación de 32 o 64 bits (si no está seguro, elija la versión de 32 bits).

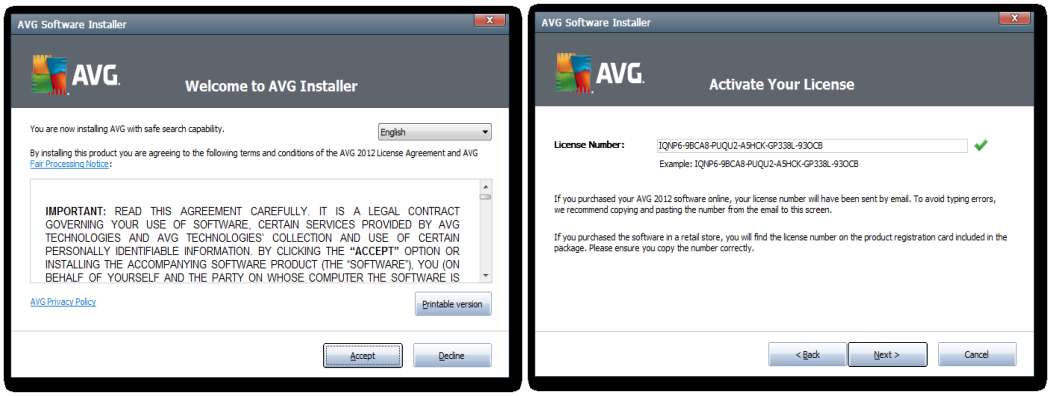
Haga doble clic en el archivo de instalación de AVG descargado en el escritorio.

El asistente de instalación de AVG le guiará por el proceso de instalación o desinstalación de AVG en su equipo. Le recomendamos que utilice siempre el archivo de instalación más reciente. De este modo tendrá la seguridad de que dispone del nivel de protección más alto posible y tendrá que descargar menos archivos de actualización después de la instalación.

Puede descargar un archivo de instalación completo o bien el instalador en línea de AVG. Mientras que el archivo de instalación completo para descargar es un archivo de gran tamaño y contiene todos los archivos necesarios para la instalación de AVG, el instalador en línea de AVG es pequeño y descarga sólo los archivos necesarios para instalar la edición adquirida de AVG.

Tenga en cuenta que los pasos indicados a continuación son similares para los dos tipos de archivo de instalación. Las diferencias en el proceso de instalación entre estos dos tipos de archivos se describirán en los pasos correspondientes.

El primer paso consiste en seleccionar el idioma que desea utilizar durante el proceso de instalación de AVG. El primer cuadro de diálogo proporciona un menú desplegable con todas las opciones de idioma disponibles para la instalación. Más adelante se podrá seleccionar qué idiomas se instalarán con el producto. Posteriormente podrá cambiar entre los idiomas seleccionados una vez que se haya instalado AVG.



La pantalla de bienvenida también contiene el contrato de licencia. El contrato de licencia de AVG es un documento legal donde se especifican las condiciones para el uso del software AVG. Para proseguir con la instalación, deberá leer el contrato de licencia y hacer clic en Aceptar.

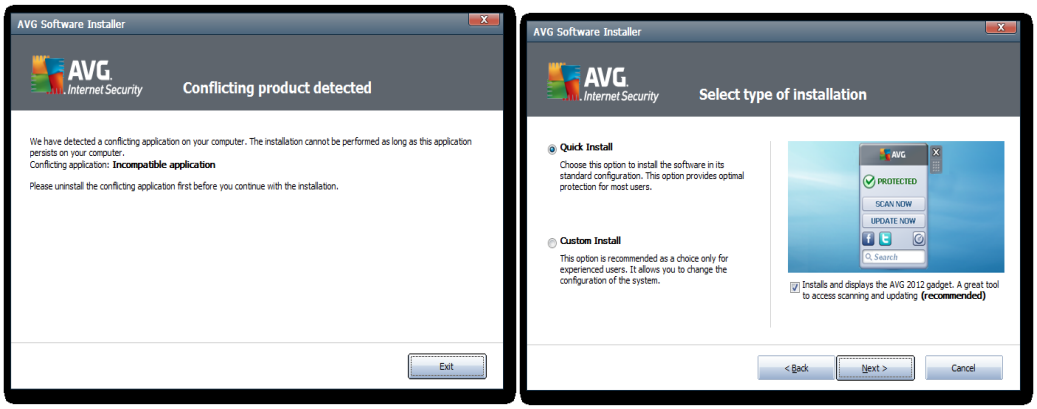
ACTIVACIÓN DE LICENCIA

Ahora debe introducir su número de licencia AVG. Le recomendamos copiar y pegar el número de licencia a partir del mensaje de correo electrónico que le enviamos después de su compra.

Una vez especificado el número de licencia, haga clic en Siguiente para continuar con el paso posterior.

COMPROBACIÓN DEL ESTADO DEL SISTEMA

El asistente de instalación ahora comprobará si hay aplicaciones no compatibles en el equipo. Si se detecta alguna, el asistente de instalación le informará de ello. Le recomendamos desinstalar el software no compatible que se detecte con el fin de evitar futuros problemas de estabilidad o rendimiento del equipo. Una vez realizado esto, vuelva a iniciar la instalación de AVG.



Si no se encuentra ninguna aplicación incompatible, la instalación procederá automáticamente al siguiente paso.

Selección del tipo de instalación

Si AVG ya está instalado en el equipo, se le mostrarán diferentes opciones en este paso.

Si no hay ninguna versión anterior de AVG instalada en su equipo, podrá elegir entre la instalación rápida y la instalación personalizada:

Instalación rápida es la opción recomendada para la mayoría de los usuarios, y no le solicitará una configuración detallada.

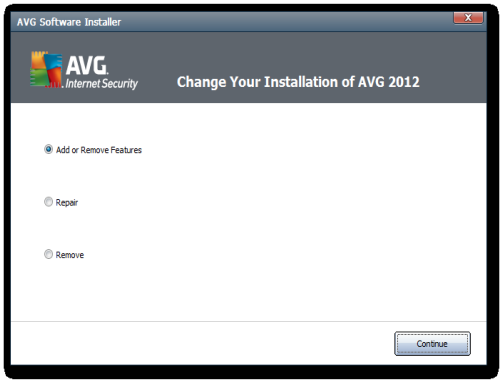
Con Instalación personalizada, puede cambiar la configuración de la instalación, seleccionar manualmente los componentes de AVG que desea instalar, etc.

Si ya hay software AVG instalado en el equipo, se le ofrecerán tres opciones:

La opción Agregar o quitar componentes le permite instalar componentes adicionales para AVG (por ejemplo, cuando actualiza a una edición superior de AVG) o quitar componentes si no desea utilizarlos.

La opción Reparar instalación puede utilizarse para reparar AVG reemplazando los archivos que están dañados o que faltan en el software AVG instalado.

La opción Desinstalar eliminará el producto AVG instalado.



Tras seleccionar una de las opciones disponibles, haga clic en Siguiente para continuar con el paso posterior.

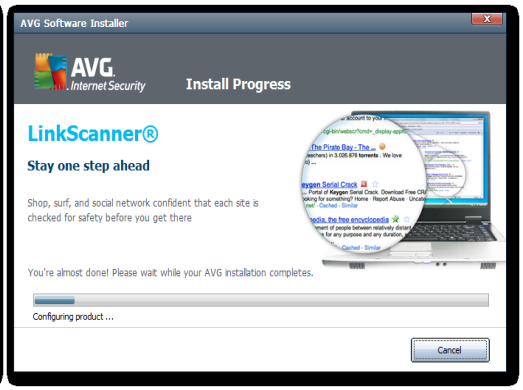
Selección de componentes

Este paso sólo aparece si en los pasos anteriores seleccionó las opciones Instalación personalizada o Agregar o quitar componentes. Puede omitir este cuadro de diálogo haciendo clic en el botón Siguiente) si no le concierne.

Este cuadro de diálogo le permite elegir qué partes de AVG se instalarán. Puede seleccionar o quitar la selección de cualquiera de las opciones. Si la casilla de verificación que aparece junto al elemento no está seleccionada, la parte correspondiente no estará disponible cuando haya finalizado la instalación. Si la casilla de verificación está seleccionada, la opción se instalará. Además de los componentes diseñados para proteger su equipo frente a las amenazas de seguridad, la opción Otros idiomas instalados le permite seleccionar qué idiomas estarán disponibles en AVG después de la instalación. El idioma utilizado en el asistente de instalación se utilizará siempre como opción predeterminada.

Nota: es posible que vea un número distinto de componentes al instalar AVG. Los componentes disponibles se muestran en función de la edición de AVG que ha adquirido.

Haga clic en el botón Siguiente para continuar con la instalación.



Después de hacer clic en el botón Siguiente, se iniciará el proceso de instalación.

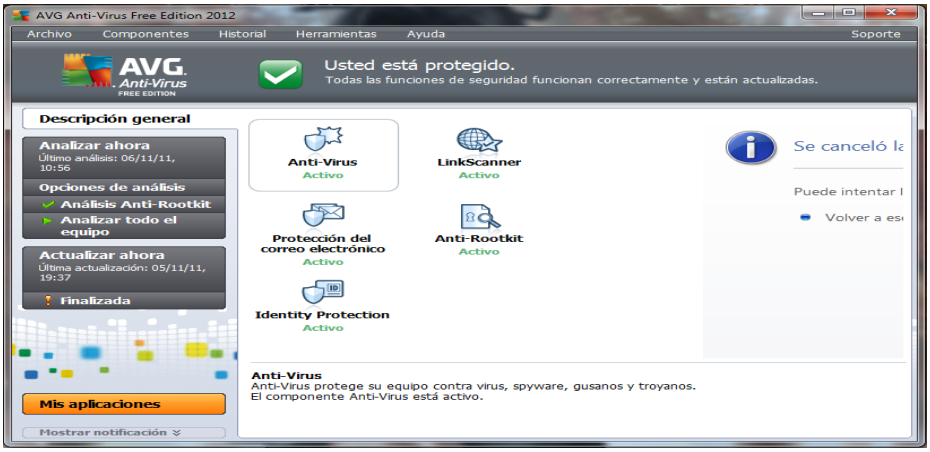
Espere mientras se copian los archivos en el equipo (es posible que la ventana no responda durante un breve periodo durante la instalación). Si utiliza el instalador en línea de AVG, ahora se descargarán todos los archivos necesarios.

Después de finalizar la instalación, aparecerá el resultado de la instalación. La pantalla de resultados también le permite registrar el programa para obtener noticias e información actualizada del producto.

En este punto se le solicitará que reinicie el equipo. Reinícielo, ya que algunas partes de AVG sólo funcionarán correctamente después del reinicio.

Ahora AVG 2012 está instalado.

Una vez instalado el antivirus, accedemos a la interfaz de AVG Free, como podemos verificar, tiene otras opciones de seguridad adicionales al antimalware, razón por la cual fue elegido, entre sus componentes tenemos la función misma de antimalware, analizador de e-mail, IdentityProtection y Link-Scanner, a continuación se detalla funcionalidad y configuración de cada uno de ellos:

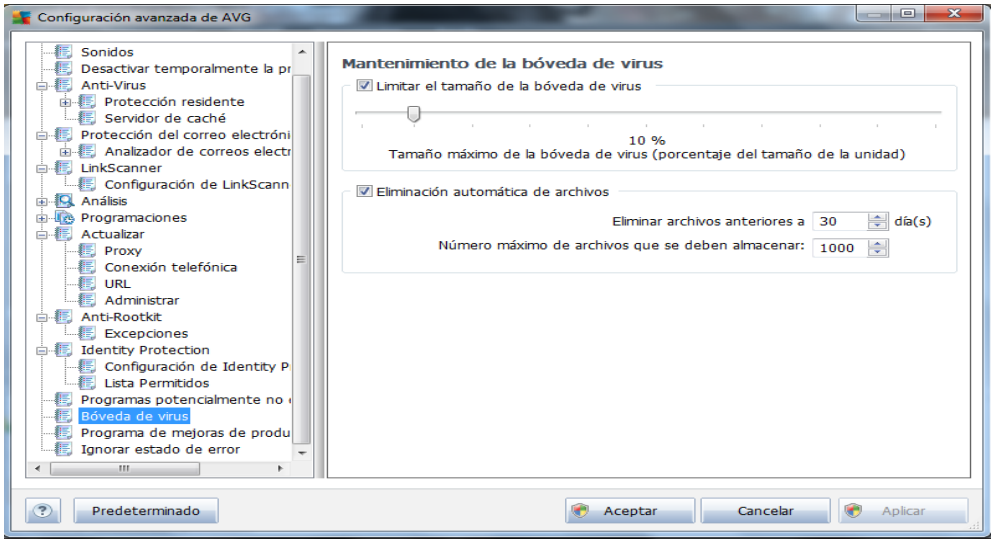


CONFIGURACIONES GENERALES DEL ANTIVIRUS

Como se mencionó anteriormente el termino correcto es antispyware, pero por costumbre se lo llama antivirus, detecta virus, spyware, gusanos, troyanos, archivos ejecutables, adware malicioso y bibliotecas (dll) no deseados.

CONFIGURACIÓN DE LA BÓVEDA DE VIRUS

Para entrar a la configuración de la Bóveda de virus: en la interfaz de AVG haz clic en el menú que se encuentra en la parte superior, selecciona "Herramientas > Configuración avanzada > Bóveda de virus"



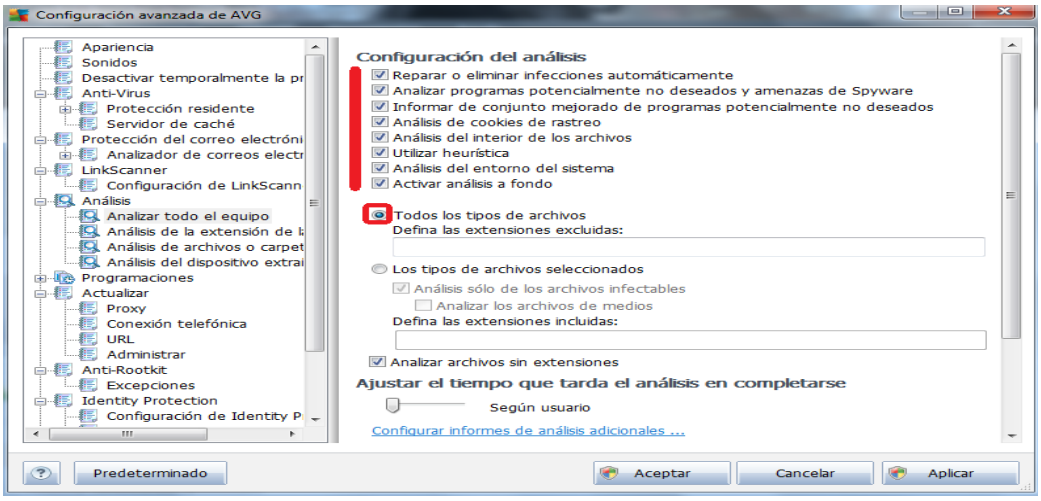
El tamaño de la Bóveda de virus, lo dejamos en 10% del disco duro, por lo general será suficiente ya que la mayoría de objetos en cuarentena son peligrosos y deben ser eliminados.

En cuanto a la "Eliminación automática de archivos", lo configuramos para que sean eliminados rápidamente (2a 5 días como máximo, para darnos un plazo si deseamos conservar un fichero importante):

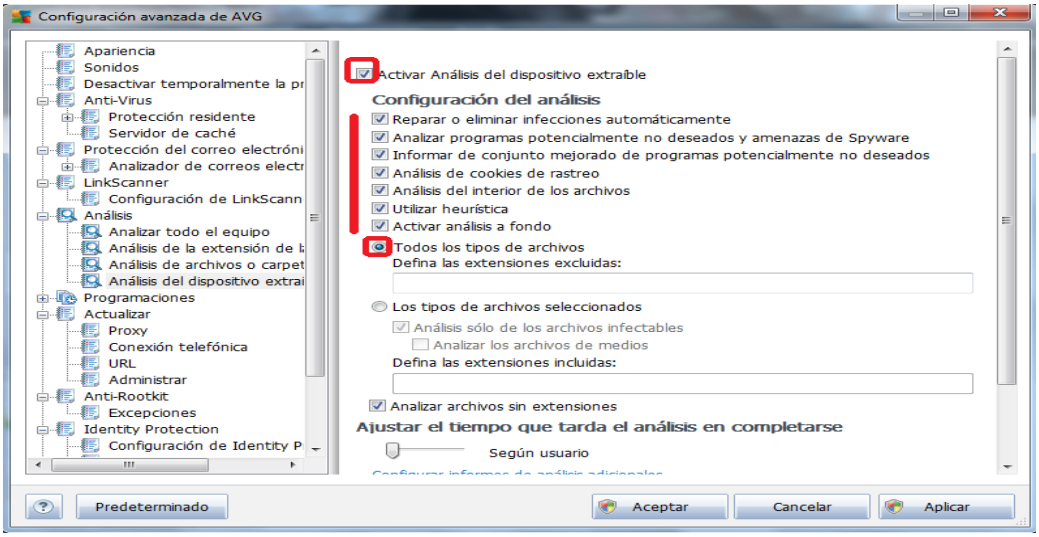
CONFIGURACIÓN DE ANÁLISIS

Para acceder a la configuración del análisis del antivirus, hacemos clic en el signo + al lado de "Análisis" en la ventana "Configuración avanzada de AVG".

En "Analizar todo el equipo", marcamos todas las casillas y seleccionamos la opción "Todos los tipos de archivos". Repetimos esta operación para "Análisis de la extensión de la Shell" y "Analizar carpetas/archivos específicos".



ANÁLISIS DEL DISPOSITIVO EXTRAÍBLE



Esta opción permite analizar automáticamente un disco extraíble (memoria USB, DD externo, etc.) en cuanto es conectado al PC (a menudo los discos extraíbles son fuentes de virus).

Aquí también, marcamos todas las casillas y seleccionamos la opción "Todos los tipos de archivos".

EL ANÁLISIS PROGRAMADO:

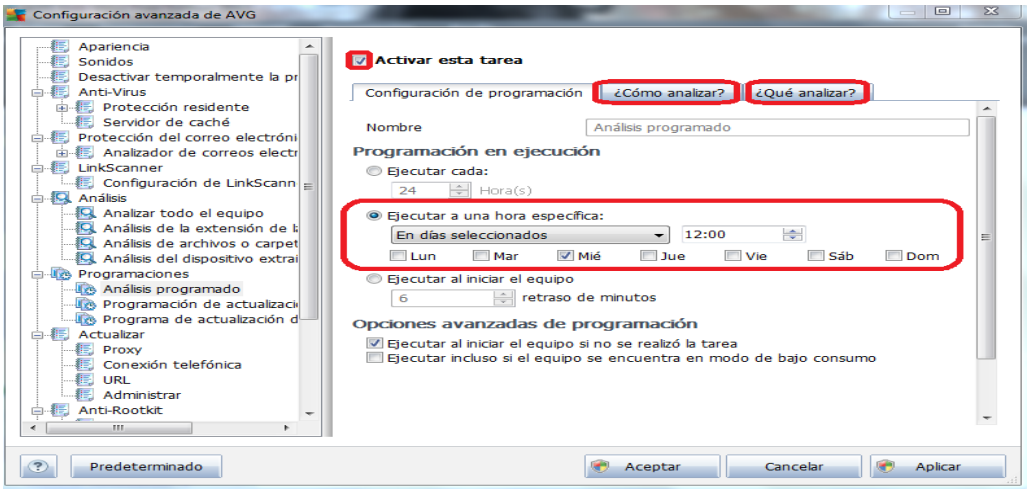
Para acceder a las opciones del análisis programado, hacemos clic en el signo + al lado de "Programaciones".

Esta opción permite hacer un análisis automáticamente a una hora y fecha precisa.

En la pestaña "Configuración de programación", se recomienda configurar el análisis para que se haga al menos una vez por semana.

En la pestaña "Cómo analizar", al igual que en los casos anteriores, marcamos todas las casillas y seleccionamos "Todos los tipos de archivos".

En la pestaña ¿Qué analizar?, comprobamos que "Analizar todo el equipo" esté seleccionado".



CONFIGURACIÓN DEL ANALIZADOR DE CORREOS ELECTRÓNICOS

AVG free posee un escáner de correos electrónicos que analiza los emails entrantes y salientes.

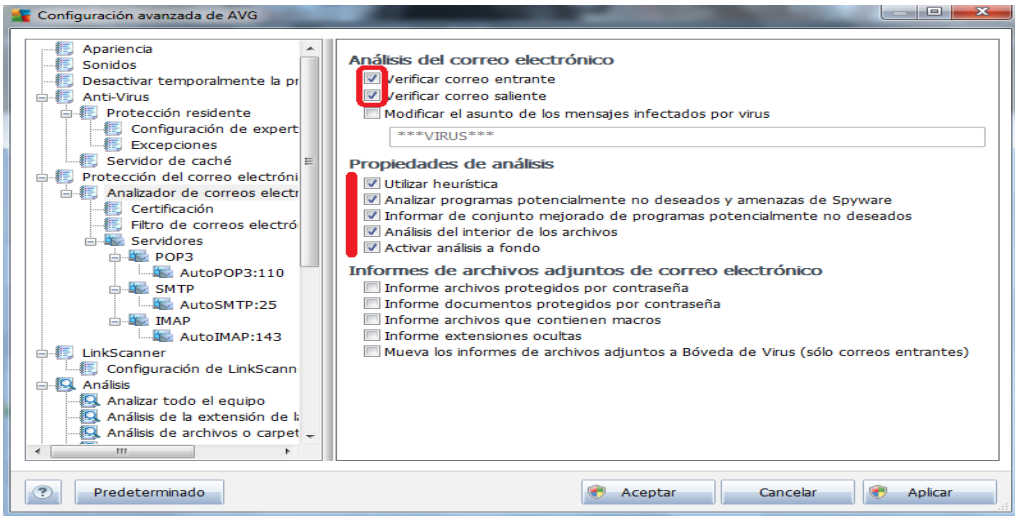
Para acceder a las opciones del análisis del antivirus, hacemos clic en el signo + al lado de "Analizador de correos electrónicos".

En la sección "Análisis del correo electrónico":

Marcamos las casillas "Verificar correo entrante", "Verificar correo saliente", "Certificar correo".

En la sección "Propiedades de análisis" marcamos todas las casillas

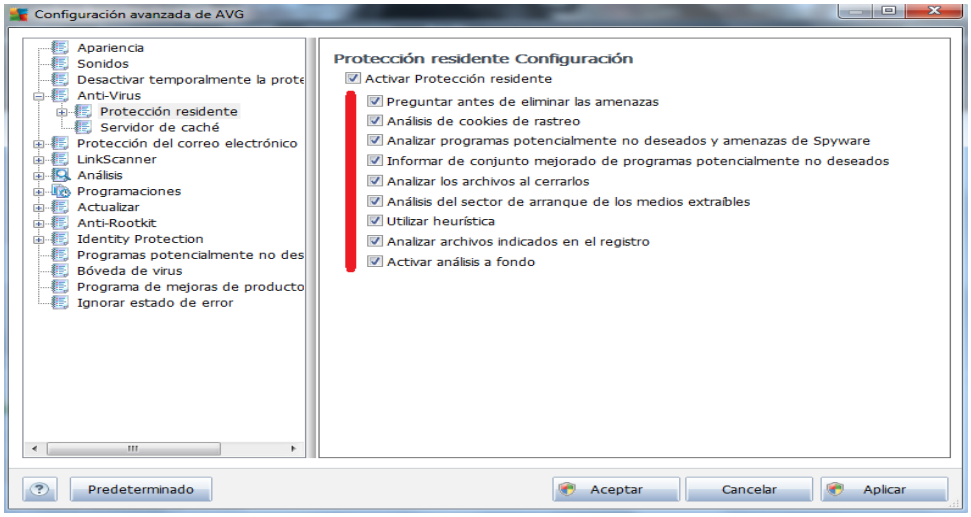
En "Informe de archivos adjuntos de correo electrónico", no marcamos nada en especial.



CONFIGURACIÓN DE LA PROTECCIÓN RESIDENTE

AVG free posee una protección residente, lo que quiere decir que analiza en tiempo real el PC en búsqueda de virus.

Para acceder a las opciones del análisis del antivirus, hacemos clic en el signo + al lado de "Protección residente", marcamos las casillas: "Activar protección residente", "Análisis de cookies de rastreo", "Analizar programas potencialmente no deseados y amenazas de Spyware", "Análisis del sector de arranque de los medios extraíbles", "Utilizar heurística"



En la pestaña "Configuración avanzada":

En "Archivos analizados por la Protección residente", marcamos la casilla "Analizar todos los archivos"

LINK SCANNER

Es una herramienta integrada a AVG free que informa de páginas web infectadas. En la lista de resultados, cuando hagas una búsqueda en Google, aparecerá un icono al lado derecho de cada página. Si el icono es de color verde quiere decir que la página no presenta ninguna amenaza. En cambio, si es de otro color, mejor evita entrar a esa página. Si la página es realmente peligrosa, AVG bloqueará la página y te advertirá.

Página que no presenta ningún riesgo. Página con riesgo.

ANTI ROOTKIT

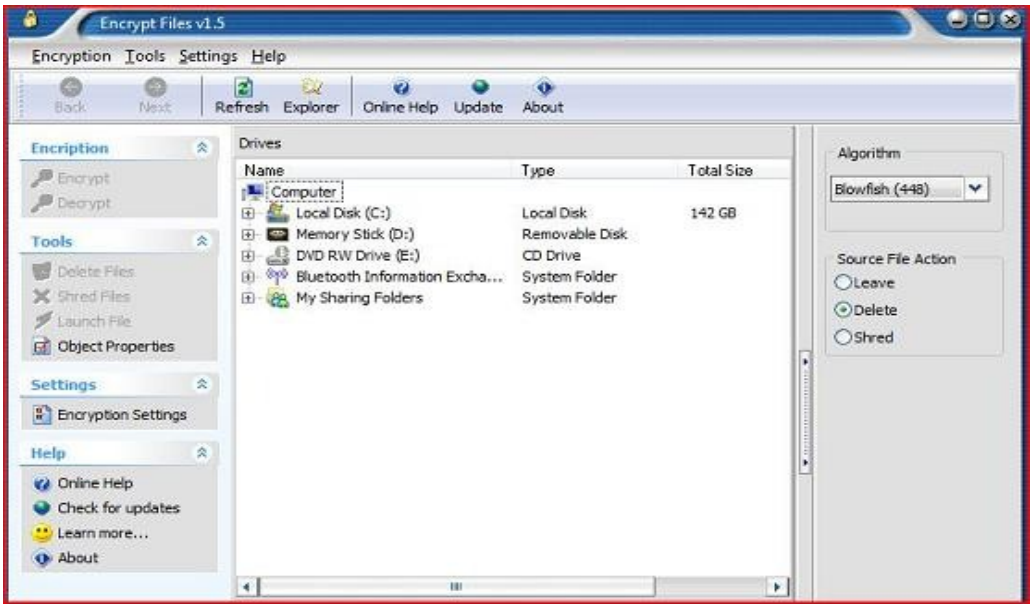
Los rootkitsson una colección de software malicioso que permite que un atacante obtenga privilegios de administrador a un equipo y posiblemente a una red completa, el componente anti.rootkit analiza programas en búsqueda de rootkit ocultos dentro de aplicaciones, controladores o bibliotecas dll.

4.5.ENCRIPTACIÓN DE ARCHIVOS

A continuación les presentamos como usar un programa llamado Encrypt Files el cual es Gratis y fácil de usar. Con Encrypt Files usted podrá proteger sus archivos y hasta folders (directorios) completos para que no puedan ser vistos por personas no autorizadas. Encrypt Files soporta hasta 13 métodos de encriptación.

PASOS DE INSTALACIÓN

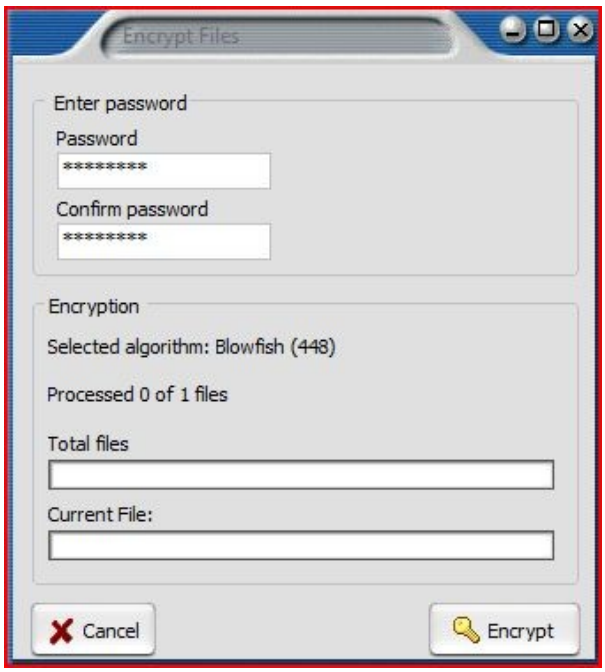
1. Ejecute el programa e instálelo siguiendo sus pasos y al final de la instalación ábralo.
2. Le debe de aparecer la ventana inicial del Programa como la siguiente:



Agrande la ventana para hacer más fácil la búsqueda del archivo a encriptar.
3. Seleccione el simbolo de + sobre el dispositivo donde tiene guardado el archivo que desea encriptar. Ejemplo Local Disk (C:) >Documents

4. Una vez localizado el archivo que desea encriptar, selecciónelo con un solo clic y el nombre del archivo se resalta en azul.

5. Ahora presione el enlace Encrypt que tiene una llave amarilla (Menú Izquierdo) y se abre una ventanita como la siguiente:



6. Entre y confirme el Password que desea ponerle al archivo y presione el botón Encrypt con la llave amarilla.

7. Presione OK y listo, notara que el archivo encriptado ahora se resalta en Rojo.

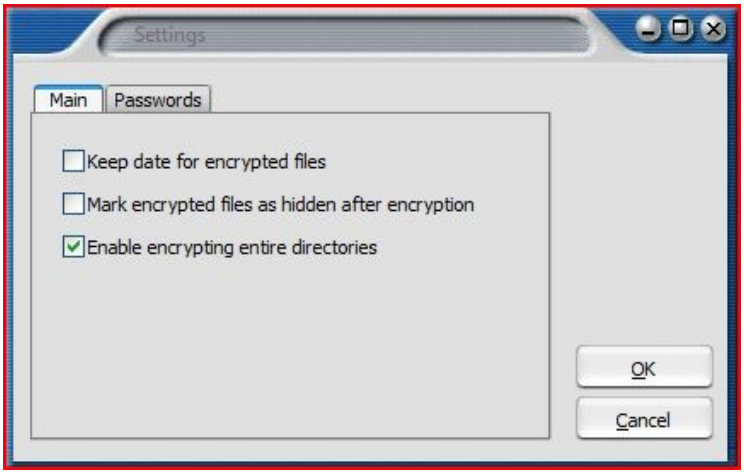
Ahora para estar seguro que el archivo se encriptó correctamente vaya a donde tiene guardado el archivo encriptado y ábralo, notara que no se puede leer nada solo hay un montón de símbolos, si esto es así su archivo esta encriptado.

Para poder desencriptar o descifrar el archivo y poder leerlo abra el programa Encrypt Files, busque donde tiene guardado el archivo encriptado (resaltado en color rojo),selecciónelo y presione el enlace Decrypt que tiene una llave color gris (Menú Izquierdo), se abre la ventanita pidiéndole la contraseña, usted ingresa la contraseña, presiona el botónDecrypt, presiona el botón OK y listo, ahora podrá ver y leer su archivo.

Estos pasos parecen un poco largos pero en realidad no lo son, solo es cuestión de costumbre, a medida que use el programa al cabo de unos días usted encriptará y desencriptará archivos en solo segundos.

OTRAS FUNCIONES ÚTILES DEL PROGRAMA

1. También puede encriptar un folder o directorio con todo su contenido. Para esto seleccione el enlace EncryptionSettings (Menu Izquierdo) se abre la ventanita y habilite la opción Enableencryptingentiredirectories (imagen siguiente) y presione OK y listo! ahora siga los mismos pasos (3 al 7) de encriptar archivos para encriptar todo un folder.



2. También puede ponerle una contraseña al programa Encrypt Files para que el programa sea usado solo por usted.

Para esto seleccione el enlace EncryptionSettings (Menu Izquierdo) se abre la ventanita y seleccione el TabPasswords y habilite la opción Ask forprogrampassword (imagen siguiente), entre y confirme el password para el programa y presione OK y listo! ahora solo usted podrá usar el programa Encrypt Files.

4.6.RECOMENDACIONES PARA CONTRASEÑAS SEGURAS

Una contraseña segura es tu primera línea de defensa contra los intrusos e impostores, existen varias teorías para crear contraseñas seguras pero a la vez que sean fáciles de recordar, a continuación se menciona una de ellascon un ejemplo que podrían ayudar a formar tu contraseña segura y que sea fácil de recordar.

Tomar en cuenta estos consejos:

- Es recomendable que la contraseña tenga por lo menos 8 caracteres.
- Una contraseña ideal tiene letras, signos de puntuación, símbolos y números.
- Verifique su contraseña con un comprobador de contraseñas (analizan la seguridad de su contraseña automáticamente), existen varios de ellos en línea.
- No utilizar la misma contraseña para diferentes inicios de sesión (acceder al PC, acceder al Messenger, Facebook, etc.).
- Evite usar los indicios de contraseña.- si su configuración de contraseña lo solicita, coloque uno que sea falso.

Los delincuentes cibernéticos usan herramientas sofisticadas que pueden descifrar contraseñas rápidamente, al crear contraseñas evite el uso de:

- Palabras del diccionario en ningún idioma.
- Palabras escritas al revés, errores de ortografía comunes y abreviaturas.
- Secuencias de caracteres o caracteres repetidos. Ejemplos: 12345678, 222222, abcdefg.
- letras que se encuentran cerca en su teclado (qwerty).
- Información personal. Su nombre, fecha de nacimiento, número de licencia de conducir, número de pasaporte o información similar.

- Incluye números, mayúsculas y símbolos. usa $ en vez de S o 1 en vez de L, pero ten en cuenta que $o1tero NO es una contraseña segura, pues los ladrones de contraseñas ya se saben este truco.
- Proteja sus contraseñas de los curiosos, no las digite en frente de otras personas, aunque exista confianza.
- Trate de no escribir las contraseñas, si lo hace, no lo ponga a la vista y cuando planee deshacerse de ella destrúyala de forma que no sea legible.

A continuación se muestra una forma que puede simplificarle la memorización de la contraseña:

Qué hacer	Sugerencia	Ejemplo
Comience con una oración o dos (alrededor de 10 palabras en total).	Piense en algo que sea significativo para usted.	Las contraseñas largas y complejas son las más seguras.
Convierta sus oraciones en una fila de letras.	Utilice la primera letra de cada palabra.	lacpasikms (10 caracteres)
Agréguele complejidad.	Escriba en mayúscula sólo las letras de la primera mitad del abecedario.	laCpAsIKMs(10 caracteres)
Agregue números para que la contraseña sea más larga.	Coloque dos números que signifiquen algo para usted entre las dos oraciones.	lACpAs56IKMs (12 caracteres)
Agregue signos de puntuación para que la contraseña sea más larga.	Coloque un signo de puntuación al comienzo de la oración.	?lACpAs56IKMs (13 caracteres)
Agregue símbolos para que la contraseña sea más larga.	Coloque un símbolo al final de la oración.	?lACpAs56IKMs" (14 caracteres)
Reemplaza letras por símbolos parecidos	S -> $ i -> ¡ L -> 1 c -> (a -> @ t -> +	?1A(p@$56IKMs" (14 caracteres)

Puedes saltarte algunos pasos por ejemplo el ultimo, lo importante es no perder la idea de la contraseña y no volverla complicada para recordar.

CAPITULO V CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

El robo de información, es una actividad altamente lucrativa, que factura millones de dólares al año, día a día los atacantes buscan más formas de robar información, debido a esto, el tema la seguridad informática es cada vez más complejo de mantener, sumado a esto, por lo general, una gran cantidad de las personas no tienen conocimiento de estas actividades,es por eso su gran éxito, pero teniendo cuidado y precaución, es posible crear un ambiente de confianza y seguridad en nuestros equipos y de esta forma aprovechar todas las ventajasy facilidades que nos brinda los computadores.

Si bien es cierto que existen varias técnicas para el robo de archivos, cabe recalcar que el elemento más vulnerable respecto a la seguridad informática, es el mismo usuario debido a la falta de conocimiento, ingenuidad o a las malas prácticas de seguridad.

5.2. RECOMENDACIONES

Recuerda que todas estas seguridades planteadas en el presente manual no garantizan la total seguridad en la protección de los datos, pero logra un alto nivel de seguridad, como lo he dicho anteriormente el usuario mismo es el factor más vulnerable, por lo tanto, mientras más preparado este el usuario con respecto a temas de protección y seguridad, será mucho más seguro el entorno del computador.

BIBLIOGRAFIA

- LIZARRAGA Mariano y TOLEDO Rommel, seguridad en Internet (párrafo 5), (13 marzo 2007) recopilado en (agosto 2011)
  http://users.soe.ucsc.edu/~malife/assets/Seguridad%20Informatica.pdf

- (diario HOY, 05/Julio/2010)
  http://www.hoy.com.ec/noticias-ecuador/el-50-de-empresas-ha-sufrido-hacking-417078.html

- (blog todoexpertos.com, 08/09/2010)
  http://www.todoexpertos.com/categorias/tecnologia-e-internet/seguridad-informatica/respuestas/2487684/robo-de-archivos-en-ordenador

- (Wikipedia, 08/09/2010)
  http://es.wikipedia.org/wiki/Windows_7

- (jsequeiros.com, 08/09/2010)
  http://jsequeiros.com/archivos/computacion/winxp/manualwinxp/capitulo11.pdf

- Masadelante.com, 08/09/2010)
  http://www.masadelante.com/faqs/sistema-operativo

- Masadelante.com, 07/09/2010)
  http://www.masadelante.com/faqs/cortafuegos

- Noticias delitos informáticos Ecuador
  http://www.eltelegrafo.com.ec/index.php?option=com_zoo&task=item&item_id=11608&Itemid=17

- Comparativa de mejores antivirus
  http://www.desarrolloweb.com/de_interes/mejores-antivirus-2011-2012-5796.html#contenido_externo

- Configuración del firewall de Windows 7
  http://es.kioskea.net/faq/3555-configuracion-del-firewall-con-seguridad-avanzada-de-windows-7

- Encriptador de archivos y carpetas
  http://www.wisedatasecurity.com/como-encriptar-archivos.html

ANEXOS

ANEXO 1: Noticias acerca de delitos informáticos

Redacción Judicial

De enero a julio de este año se ha reportado alrededor de 600 denuncias por delito informático. Así lo reveló Paúl Pérez, fiscal de Delito contra el Patrimonio Ciudadano, quien explicó que esa cifra corresponde a Pichincha.

Mientras que en 2010 se registró 300 denuncias a nivel nacional.

Aclaró que en la mayoría de los casos los montos de perjuicio por cada víctima superan los $ 1.000.

Los denominados "hackers" o "piratas informáticos" también tienen la capacidad de obtener información interna de las cuentas bancarias de empleados del sector estatal. Esto se evidenció tras la denuncia presentada por Marcela Miranda, presidenta del Consejo de Participación Ciudadana, que alertó sobre el "atraco informático" que afectó a alrededor de 30 funcionarios de esa entidad pública.

A más de $ 20.000 asciende el monto sustraído de las cuentas de los perjudicados mediante desvíos de dinero hacia diferentes entidades financieras del extranjero, como en Houston (Estados Unidos), Bogotá y Cali (Colombia).

Galo Chiriboga, fiscal general del Estado, fue quien acogió la denuncia que fue delegada a Marco Freire, fiscal provincial de Pichincha para realizar las investigaciones correspondientes.

Los peritos informáticos forenses son los encargados de realizar las investigaciones pertinentes en cada caso, identificar el software utilizado, los datos sustraídos y las transacciones realizadas.

En el código penal, artículo 553.1, se establece que el uso fraudulento del sistema de información es utilizado para facilitar estafas financieras y se impondrá una pena de 6 meses a cinco años. Y si una persona interfiere en el funcionamiento de una alarma, utiliza controles de interferencia, manipula sistemas de información, realiza transacciones financieras o manipulación ilícita de redes, la pena será de uno a 5 años.

Explicó que la devolución del dinero a las personas perjudicadas es una diligencia directa con el banco del que ha sido sustraído el dinero.

Pablo Sosa, experto en seguridad electrónica, detalló que existe un mercado negro de tarjetas de crédito, a las cuales se les graba las bandas magnéticas sustraídas de las tarjetas originales.

Sosa señala que son grupos organizados, mafias de "hackers" quienes utilizan técnicas como "phishing", utilizada para obtener información a través de correos electrónicos; otra táctica es grabar todo lo que el usuario escribe en su computadora; también se puede captar fotos instantáneas de todas las páginas que la persona utiliza.

Las seguridades biométricas que los bancos han implementado en el país ayudan a incrementar la seguridad de cada usuario, ya que se incluyen preguntas de tipo personal que solamente el dueño de la cuenta puede conocer.

ANEXO 2: Lista de Antivirus

TABLA DE RENDIMIENTO DE ANTIVIRUS

MALWARE REMOVAL	Suite	Free	All Malware		Rootkits		Scareware	
			%	score	%	score	%	score
Ad-Aware FREE Internet Security 9.0		Y	91%	7.3	100%	6.4	88%	8.0
Ad-Aware Pro Internet Security 9.0			91%	7.4	100%	7.3	88%	8.4
Ad-AwareTotal Security 1.0	Y		86%	7.1	100%	6.6	78%	7.2
avast! Free version 6.0		Y	82%	6.4	100%	6.4	63%	5.3
BullGuard Antivirus 10			76%	6.3	100%	5.8	50%	4.3
Comodo Antivirus 5.0		Y	76%	5.1	78%	2.8	75%	5.5
Double Anti-Spy Professional v2			94%	7.6	100%	8.3	88%	7.8
eScan Anti-Virus 11			82%	6.1	89%	3.6	75%	5.6
F-Secure Anti-Virus 2011			83%	7.0	100%	5.9	78%	6.8
K7 Antivirus Plus 11.0			97%	7.5	100%	7.6	88%	6.9
McAfee AntiVirus Plus 2011			82%	6.6	89%	5.7	63%	5.6
Microsoft Security Essentials 2.0		Y	79%	6.6	89%	5.6	63%	5.9
Norman Antivirus & Antispyware 8	Y		71%	5.5	44%	2.4	67%	5.8
Norton 360 Version 5.0	Y		89%	7.9	100%	8.4	78%	7.8
Norton AntiVirus 2011			89%	7.9	89%	7.7	78%	7.8
Norton Power Eraser		Y	82%	6.1	100%	6.0	88%	6.5
Spyware Doctor with AntiVirus 2011			89%	7.8	100%	9.1	78%	7.7
Webroot AntiVirus with Spy Sweeper 2011			83%	7.0	100%	8.0	89%	7.3
NEW MALWARE COLLECTION INTRODUCED								
avast! Rescue Disc			81%	5.7	86%	5.3	80%	7.4
AVG Anti-Virus Free 2012		Y	88%	6.5	100%	6.7	100%	9.5
Bitdefender Antivirus Plus 2012			82%	6.0	86%	6.0	100%	9.5
G Data AntiVirus 2012			83%	5.4	86%	5.3	100%	8.4
Kaspersky Anti-Virus 2012			76%	5.7	71%	3.9	75%	6.3
Malwarebytes' Anti-Malware Free 1.51		Y	79%	6.4	57%	3.6	100%	10.0
Norman Malware Cleaner 2.1		Y	85%	5.3	71%	2.4	100%	9.5
Outpost Antivirus Pro 7.5			82%	4.9	86%	2.9	75%	6.3
Panda Antivirus Pro 2012			85%	5.8	100%	4.7	100%	9.5
Panda Cloud Antivirus 1.5 Free Edition		Y	91%	5.9	100%	4.1	100%	9.5
Trend Micro Titanium Antivirus+ 2012			79%	4.7	86%	3.6	100%	7.0
TrustPort Antivirus 2012			88%	5.4	100%	4.4	100%	9.5
ZoneAlarm Antivirus + Firewall 2012			79%	6.0	100%	6.7	75%	7.5

MEJORES ANTIVIRUS DEL 2011

13/09/2011

El mero hecho de conectarse a Internet expone nuestro equipo al potencial ataque de todo tipo de software malicioso.

Como consecuencia de lo anterior es interesante conocer que antivirus es el mejor frente al malware en general como de forma específica frente a rootkits y scareware.

Con motivo de la llegada del nuevo AVG Anti-Virus Free 2012 ha sido dado a conocer una tabla con datos acerca de las principales soluciones de seguridad y en donde se mezclan tanto antivirus de pago como gratuitos, o versiones actuales (2011) y nuevas versiones (2012).

Posición destacada ocupa Norton 360 versión 5 un completo software antivirus que detecta el 89% de las amenazas con especial eficacia frente a rootkits, software malicioso cuyo principal objetivo es ocultar procesos y programas con los que de forma remota se lleven a cabo determinadas acciones y/o robo de información.

Entre las soluciones de seguridad gratuita obtiene la mejor puntuación Ad-Aware Free Internet Security 9.0 un reconocido software frente a amenazas como spyware, adware y troyanos que ahora además añade protección antivirus.

Entre los últimos antivirus lanzados destaca AVG Anti-Virus Free 2012 con inmejorables resultados en la detección de rootkits y scareware.