Labor de los agentes forenses en los sistemas de información

Autor: Edgar Julio Hernández García

Tesina presentada para obtener el título de:
Lic. En Sistemas computarizados [sic]

Nombre del asesor:
Gabriel Nava Vazquez

UNIVERSIDAD VASCO DE QUIROGA

ESCUELA DE LICENCIATURA EN SISTEMAS COMPUTARIZADOS

N° DE ACUERDO: 952006 CLAVE: 16PSU0049F

"LABOR DE LOS AGENTES FORENSES EN LOS SISTEMAS DE INFORMACION"

TESINA

QUE PARA OBTENER EL TÍTULO DE

LICENCIADO EN SISTEMAS COMPUTARIZADOS

PRESENTA:

EDGAR JULIO HERNÁNDEZ GARCÍA

DIRECTOR DE TESIS: ING. GABRIEL NAVA VAZQUEZ

MORELIA, MICHOACAN AGOSTO DE 2006

AGRADECIMIENTO:

A MIS PADRES POR LA EDUCACION QUE ME HAN DADO, ASI COMO EL APOYO MORAL Y ECONOMICO QUE ME HAN BRINDADO DURANTE TODO ESTE TRAYECTO DE MI VIDA.

INDICE

PLANTEAMIENTO DEL PROBLEMA

En la actualidad la informática forense es un campo del cual pocos tienen conocimiento, debido a esto se presentan muchos casos tales como ataques, perdida de información, y otros daños a la información contenida en las computadoras víctimas de personas con la intención de perjudicar, o de utilizar la información que hay en los sistemas informáticos de organismos de todo tipo tanto gubernamentales como empresas privadas, que manejan grandes cantidades de información muy valiosa para su correcto funcionamiento.

Una forma de poder evitar ser afectado por estos ataques es estar informado sobre como prevenirlos, lo que se tiene que hacer en el momento, o bien, saber reparar los daños tales como la perdida de información que estos eventos ocasionan. Este problema involucra tanto a las personas que están en busca de información en específico como a los responsables de la seguridad informática de los sistemas.

La información con la que se cuenta en la mayoría de los organismos acerca de informática forense se puede decir que es pobre, por lo tanto no están capacitados para saber enfrentar una situación de esta naturaleza, por esa razón es necesario que las personas encargadas de manejar los sistemas de información tengan unas bases firmes y sólidas en cuanto a conocimientos de seguridad informática e informática forense.

El problema se plantea de la siguiente manera: **¿Qué relación tiene la informática forense con la información que se guarda en los sistemas de información?**

JUSTIFICACION

La elección de este tema es debido al papel importante que juega la informática forense ya que es requerida y aplicada en todo tipo de instituciones puesto que todos están expuestos a ser víctimas de ataques, por lo tanto se hizo esta recopilación de información para darla a conocer donde sea necesario, de esta manera ayudar a tener una idea mas clara acerca de los procesos que se llevan acabo en la labor que realiza la Informática Forense.

Una vez comprendidos los temas se sabrá como aplicar los conocimientos de informática forense, esto se refiere a que dentro de este documento se hablara de metodologías, técnicas y herramientas disponibles para la realización de labores correspondientes a los agentes forenses.

Esto se hace con la intención de que las personas encargadas de los sistemas de información sepan que hacer en caso de ser víctimas de ataques a sus sistemas y realizar las tareas correspondientes que van desde recuperar información hasta saber prevenir un suceso similar.

OBJETIVOS

a) **General**

Dar a conocer los conceptos básicos, objetivos y fundamentos de la informática forense

b) **Particular**

Crear una conciencia de mayor atención a la seguridad en los encargados de administrar sistemas de información.

c) **Específicos**

Analizar la información existente acerca de este tema y reunirla en un solo documento de informática forense de fácil entendimiento, útil y aplicable.

INTRODUCCION

La Informática Forense se puede definir como el área de la informática encargada de llevar acabo todos los pasos necesarios para la recuperación de información e investigación de los sistemas informáticos corrompidos.

La Informática Forense está adquiriendo una gran fuerza esto debido a la importancia que tiene la información que actualmente se maneja en medios electrónicos y al creciente uso de computadoras dentro de las organizaciones.

Cuando se atenta en contra de los sistemas de información muchas veces los registros quedan almacenados. Sin embargo, existe un gran problema debido a que las computadoras guardan la información de forma digital de tal manera no puede ser recolectada o usada como evidencia utilizando medios comunes, se deben utilizar mecanismos diferentes a los tradicionales. Es aquí donde se origina el estudio de la Informática forense como una ciencia relativamente nueva. Es gracias a fenómenos electromagnéticos que la información se puede almacenar, leer e incluso recuperar cuando se creía eliminada. La informática forense, aplicando procedimientos estrictos y rigurosos puede ayudar a resolver grandes crímenes apoyándose en el método científico, aplicado a la recolección, análisis y validación de todo tipo de pruebas digitales.

CAPITULO 1

ASPECTOS IMPORTANTES DE SEGURIDAD INFORMATICA

1.1 Seguridad en los Sistemas Operativos

Los sistemas operativos son el medio de comunicación entre usuario y máquina así como también son los encargados de administrar los recursos del sistema de una manera eficiente. Los sistemas operativos cada vez son mas extensos por lo tanto a medida que evolucionan presentan un grado mayor de complejidad, esto tiene como consecuencia un mayor número de errores incluyendo vulnerabilidades en la seguridad del sistema. Para saber el grado de seguridad con el que cuenta un sistema es necesario realizar una evaluación y tratar de corregir sus vulnerabilidades para obtener un sistema lo mas seguro posible evitando intrusiones y otros daños que se pueden ocasionar debido al bajo nivel de seguridad.

Una buena manera de controlar la seguridad de los equipos de cómputo es centralizarla, sin necesidad de estar configurando cada uno de los equipos. Además, el costo de no tener la seguridad centralizada y automatizada es elevado ya que gran parte de las intrusiones no son responsabilidad de defectos que contenga el sistema operativo, sino a que no son configurados correctamente antes de ponerlos en servicio ya que se instalan con la configuración que viene de fábrica, y no se actualizan de manera constante por eso quedan como un blanco perfecto para los intrusos. **[Ref1]**

1.2 Seguridad de la Información

La seguridad de la información dentro de las organizaciones debe ser garantizada de tal manera que se logre mantener su integridad, disponibilidad para el personal interno de la organización que necesita el uso de esta para el desempeño de su función y al mismo tiempo su confidencialidad con respecto a personas ajenas quienes la pueden robar para posteriormente manipularla haciendo un mal uso de la misma, es por eso que se debe contar con un sistema de protección de información ya que juega un papel importante en el funcionamiento eficiente de la organización.

La información se puede encontrar guardada en diferentes medios

1 **No automatizados:** Documentos, Impresos.
2 **Automatizados:** Medios electrónicos.

En estos últimos, se deben de tomar medidas de seguridad con mayor complejidad. Entre las medidas de seguridad que se pueden recomendar están:

- Tener el equipo de cómputo en un lugar seguro donde se permita el acceso solo a cierto personal.
- Tener el equipo de cómputo en un lugar con protección en contra de accidentes o catástrofes naturales como incendios e inundaciones.
- Tener siempre un respaldo de toda la información para evitar la pérdida de la misma en caso de errores del sistema.
- Tener control de acceso a programas y bases de datos en donde se maneje información valiosa.
- Dar a conocer a todo el personal las medidas de seguridad con el fin de evitar accidentes como el daño o pérdida de información.

Mediante la puesta en práctica de estas medidas de seguridad en las instituciones donde se manejan grandes cantidades de información se ayudará a conservarla sin correr riesgos para lograr mantener unos sistemas confiables evitando un mal funcionamiento y generar costos a las instituciones.

1.3 Políticas

Las políticas de seguridad son indicaciones donde se especifica la forma en que se deben manejar los procesos de información dentro de una organización, estas contienen medidas restrictivas las cuales están basadas en objetivos y metas por alcanzar previamente establecidas. La carencia de políticas de seguridad es un problema al cual hoy en día se enfrentan las organizaciones lo

cual pone en una situación de riesgo su información. Por lo tanto, es importante que las organizaciones cuenten con sus propias políticas de seguridad adecuadas a los procedimientos que se llevan a cabo dentro de las mismas.

Para llevar a cabo la implantación de las políticas de seguridad es recomendable previamente hacer un análisis de riesgo en donde se detecten vulnerabilidades en los sistemas de información y de acuerdo a los resultados obtenidos implementar políticas que ayuden a mejorar la situación, también se pueden tomar en cuenta los problemas de seguridad que se hayan tenido con anterioridad.

Una vez elaborada la lista de los puntos que se necesitan cubrir se comienza la elaboración de las políticas las cuales deberán ser redactadas de una manera clara y concisa, se aconseja hacer documentos diferentes dependiendo a quien irán dirigidos, los empleados podrían recibir un pequeño folleto que contiene las políticas de seguridad más importantes que ellos necesitan tener presente a diferencia del personal que trabaja en el área de informática y telecomunicaciones podrían recibir un documento considerablemente más largo que proporciona mucho más detalles por lo cual es necesario elaborar redacciones diferentes para cada uno de ellos.

Una vez implementadas las políticas de seguridad es necesario darlas a conocer en toda la institución y vigilar que su cumplimiento sea llevado a cabo.

Como recomendaciones básicas de políticas de seguridad útiles para toda institución podemos encontrar:

1 Mantener los sistemas operativos actualizados descargando parches de seguridad constantemente.
2 No usar software ilegal ya que esto esta prohibido por la ley y no hay garantía de la autenticidad de la fuente.
3 Tener instalado en todos los equipos antivirus y actualizarlo periódicamente.
4 Tener los equipos protegidos con contraseñas de longitud mínima asignadas por el administrador.

5 No descargar archivos de sitios de red inseguros.
6 Cambiar las contraseñas cada determinado tiempo según se crea conveniente.
7 No abrir correos sospechosos ya que pueden contener virus.
8 Las carpetas compartidas en la red deberán tener asignada una clave de acceso.
9 No debe haber archivos personales ocultos en los sistemas.
10 Manejar cuentas de usuario restringido de tal manera que los usuarios no puedan instalar software adicional al necesario.
11 No ejecutar archivos que contengan doble extensión.**[Ref2]**

Estas políticas son unos ejemplos que pueden ser útiles para la correcta administración de equipos de cómputo por lo cual se recomienda que se lleven a cabo para mantener una seguridad mas sólida.

1.4 Gestión

Un Sistema de Gestión consta de la implementación de procesos que permitan realizar un servicio o producto con confiabilidad y conformidad dentro de una organización.

La gestión de la seguridad informática es un punto importante dentro de las empresas ya que en base a las decisiones que se tomen sobre como controlar la seguridad de la información serán los resultados que se obtengan en beneficio de la organización. Se debe elegir un esquema de seguridad adecuado para el correcto funcionamiento, esta elección debe ser tomada con el debido cuidado ya que un buen sistema de seguridad informática requiere de una inversión elevada.

Existen diferentes esquemas de seguridad para la correcta elección se deben tomar en cuenta las ventajas y desventajas de cada uno así como también sus costos de implementación y su tiempo de recuperación de la inversión.

A nivel internacional los estándares comúnmente aceptados como válidos son los que proclama la norma internacional ISO/IEC 17799:2000 "Information technology. Code of practice for information security management" (Tecnología de información. Código de prácticas para el control de la seguridad de la información).

Recientemente, el 17 de mayo de 2005, ha visto la luz una ampliación denominada "Security techniques" (Técnicas de Seguridad) dentro del marco que brinda ISO 17799:2000.

Esta norma internacional deriva del marco reglamentario BS 7799, elaborado y definido por el British Standards Institution, en el que se definieron diez puntos de control para gestionar adecuadamente los sistemas de la información. Estos puntos de control han sido contemplados igualmente en el marco ISO 17799 y sus trasposiciones a normas nacionales.

1) Política de Seguridad, donde se establecen las directrices gerenciales en materia de seguridad.

2) Organización de recursos y activos de la información, para sentar las correctas bases de la gestión de la seguridad dentro de la empresa.

3) Clasificación y control de activos de la información, donde se pretende inventariar los activos a proteger así el establecimiento de las correctas medidas de protección.

4) Seguridad ligada al personal, con el fin de tratar aspectos relativos a la seguridad vinculada a los recursos humanos: confidencialidad, accesos no permitidos, fugas de información, etc.

5) Seguridad física y del entorno, donde se establecen las pautas correspondientes a la seguridad de las instalaciones físicas.

6) Gestión de las comunicaciones y las operaciones, con la idea de asegurar el procesado de la información.

7) Control de acceso, en el que se establecen privilegios y autorizaciones para acceder a los recursos.

8) Desarrollo y mantenimiento de sistemas, que serán los destinatarios principales de la gestión de la seguridad.

9) Gestión de la continuidad de los negocios, donde se establecen planes de recuperación y minimización del impacto ante discontinuidades en los procesos críticos de la empresa.

10) Conformidad legal, donde se observa el cumplimiento con la legislación vigente según la localización territorial de la empresa. **[Ref3]**

En México el estándar de seguridad ISO 17799 puede ser implementado con el apoyo del Departamento de Seguridad en Cómputo de la UNAM (DSC) y UNAM-Cert (Equipo de Respuesta a Incidentes de Seguridad en Cómputo) ya que cuentan con personal capacitado par llevar a cabo esta labor dentro de cualquier organización.

1.5 Herramientas

Debido al alto nivel de riesgo que se tiene al estar conectado a una red como Internet se está expuesto a ser víctima de cualquier ataque ya sea interno, externo, infección de virus por lo tanto no se deben dejar los equipos únicamente bajo la seguridad del sistema operativo sino que es conveniente integrar mas mecanismos de seguridad que protejan los equipos.

1.5.1 Protección por Contraseña

El esquema más común de autenticación es la protección por contraseña para acceder a su equipo. La protección por contraseñas tiene ciertas desventajas si no se utilizan criterios adecuados para elegirlas, modificarlas periódicamente y comunicarlas.

No se debe dejar a decisión de los usuarios la elección de contraseñas ya que ellos tienden a elegir contraseñas fáciles como:

- Nombre de un amigo, pariente, mascota etc.
- Número de documento, domicilio, patente del auto, etc.

Estos datos podrían ser conocidos por quien intente una violación a la seguridad mediante intentos repetidos, por lo tanto debe limitarse la cantidad de intentos fallidos de acierto para el ingreso de la contraseña, así como también implementar requisitos que deben cumplir las contraseñas tales como:

1. La contraseña no debe ser corta, se debe poner un número mínimo de caracteres.
2. Tampoco debe ser muy larga para que no se dificulte su memorización
3. Combinación de letras minúsculas y mayúsculas
4. Cadena de caracteres incluyendo números **[Ref1]**

1.5.2 Antivirus

Un virus es un pequeño programa hecho con la intención de instalarse en las computadoras sin el conocimiento o el permiso de los usuarios ya que el programa ataca a los recursos y se replica a sí mismo para continuar su esparcimiento.

Los antivirus como su nombre lo dice son aplicaciones para combatir este creciente problema de los virus, la función de un programa antivirus es detectar la presencia de un virus informático en una computadora es importante contar

con uno aunque es únicamente una herramienta que ayuda a minimizar los riesgos ya que nunca será una solución definitiva, lo principal es mantenerlo actualizado.

Las organizaciones deben saber elegir un antivirus apropiado tomando en cuenta las características administrativas que el antivirus ofrece ya que algunos pueden carecer de herramientas o servicios que la organización pueda necesitar para su seguridad.

Es importante tener en claro la diferencia entre "detectar" e "identificar" un virus en una computadora, la detección es la determinación de la presencia de un virus, la identificación es la determinación de qué virus se trata, aunque parezca contradictorio lo mejor que debe tener un antivirus es su capacidad de detección, pues las capacidades de identificación están expuestas a muchos errores y sólo funcionan con virus conocidos. La actualización debe ser fácil de obtener, pero también debe influir en la adquisición de un antivirus el tipo de tecnología aplicada en su desarrollo.

Es de suma importancia el saber como manejar este tipo de software y mantener a los equipos fuera del peligro que representan los virus, al igual que el software es importante que también los administradores de equipos estén actualizados en cuanto a los virus que se propaguen por la red para tomar las medidas de seguridad necesarias y evitar una infección.

1.5.3 Copias de Seguridad

La información que se encuentra almacenada en los sistemas puede resultar afectada por diferentes causas o circunstancias tales como virus, usuarios, deterioro, fallas de hardware, o simplemente por accidente o descuido, es por esa razón se deben tomar medidas de precaución tales como realizar copias de seguridad para evitar la perdida de la información valiosa que se maneja en las computadoras.

Las copias de seguridad consisten en respaldar todos los archivos que se crean convenientes y almacenarlos de preferencia en un medio distinto al disco duro, ya sea en discos compactos, cintas, otros equipos, servidores, ya que en casos de pérdidas o daños de los archivos se recurre al respaldo que se hizo para recuperarlos. También es bueno realizar copias de seguridad y guardarlas en un lugar externo a las instalaciones ya que en caso de incendio las copias de seguridad pueden perderse.

Existen 3 tipos fundamentales de copias de seguridad:

Completa: La cual consiste en copiar todas las carpetas y archivos seleccionados.

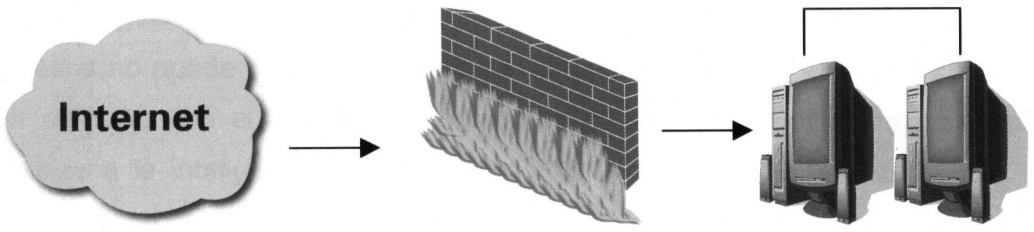
Incremental: Es la que se realiza cuando únicamente se incrementan los archivos nuevos o modificados.

Diferencial: Consiste en una manera similar a la Incremental a diferencia que se realiza una comparación del contenido de los archivos para determinar los que realmente se han modificado.

Cada organización debe tomar la decisión de que tipo de copia de seguridad adoptar y con que frecuencia realizarla esto dependiendo de la importancia de su información y los sistemas de seguridad con los que cuente. **[Ref4]**

1.5.4 Cortafuegos (*firewall*)

La palabra *firewall* en ingles significa pared de fuego, en términos de informática se refiere a un sistema de seguridad que consiste proteger los equipos de computo de posibles ataques provenientes del exterior ya que su trabajo es decir quien puede hacer uso de los servicios de red de una organización, esto se logra pasando toda la información que venga del exterior de la red a través del *firewall* el cual se hará cargo de inspeccionarla y no autorizar el acceso a nada que no sea seguro.



El *firewall* mediante la definición de un "choke point", el cual funciona de una manera similar a un embudo, mantiene al margen a usuarios no autorizados de acceder a la red, de esta manera proporciona una protección de los sistemas ante posibles ataques. También tiene como ventaja el ayudar a administrar la red, ofrece un punto de seguridad monitoreada y si aparece alguna actividad sospechosa genera una alarma ante la posibilidad de que ocurra un ataque.

Una zona des-militarizada (DMZ), es parte de una red que no está dentro de la red interna (LAN) pero tampoco está directamente conectada hacia Internet. Podría resumirse como una red que se localiza entre dos redes. En términos más técnicos se refiere a un área dentro del cortafuegos donde los sistemas que la componen tienen acceso hacia las redes interna y externa, sin embargo no tienen acceso completo hacia la red interna y tampoco acceso completamente abierto hacia la red externa. Los cortafuegos y ruteadores protegen esta zona con funcionalidades de filtrado de tráfico de red.**[Ref5]**

1.5.5 Sistema de Detección de Intrusos

Un IDS (Intruder Detection System) es un programa que realiza en un análisis del tráfico de la red que sirve para detectar accesos no autorizados a una red o a una computadora el cual consiste en comparar el tráfico actual con comportamientos sospechosos tales como el escaneo de puertos y otras acciones que pueden llevar a cabo los intrusos.

Por lo regular un IDS se integra con un *firewall* debido a que el detector de intrusos no puede detener ataques por cuenta propia, pero al estar trabajando en conjunto con el *firewall* se convierten en una herramienta muy poderosa gracias a la inteligencia que posee el IDS el cual no solo analiza el tipo de trafico, si no que también revisa el contenido y su comportamiento, y junto con el poder de bloqueo del *firewall* que es el punto por donde deben pasar los paquetes para poder ser bloqueados sin problema alguno.**[Ref6]**

CAPITULO 2
ATAQUES REMOTOS

2.1 Introducción

Se puede definir como ataque a un conjunto de acciones realizadas por un individuo a través de una computadora llevadas a cabo en contra de otra, esto con intenciones maliciosas tales como la obtención de información o causar daños al sistema.

Un ataque remoto es todo aquel proveniente de una computadora dirigido a otra sin importar su ubicación geográfica, ya que puede ser originado desde la misma oficina donde se encuentra la víctima, así como también puede ser que el agresor se encuentre en otro país a miles de kilómetros de distancia.

Según una encuesta de seguridad en el 2003 los costos relacionados con los sitios Web paralizados, el acceso no autorizado a las redes, junto con la pérdida de información costaron mas de 200 millones de dólares, también reveló que los costos por robo de información se dieron un total de 70 millones de dólares.**[Ref7]**

Este tipo de ataques se dan con frecuencia en organizaciones que contienen información valiosa almacenada en sus sistemas y pueden llegar a ser costosos los daños ocasionados, por lo que es necesario contar con tecnología de seguridad eficiente.

Existen diferentes tipos de ataques remotos como Escaneo de puertos, Spoofing, Negaciones de Servicio, Interceptación y Ataques a aplicaciones, de los cuales se hablara con mayor detalle más adelante.

2.2 Escaneo de puertos

El escaneo de puertos es un ataque mediante el cual se pretende obtener información del sistema víctima tales como sistema operativo instalado en una máquina o en varias si se trata de una red, agujeros mediante los cuales se puede lograr introducirse, así como otros problemas y vulnerabilidades en la seguridad, de esta manera saber por donde se puede atacar a la víctima.

Los escaneos de puertos se pueden clasificar en:

1 ***Horizontal:*** Es el que se da cuando el atacante se dedica a buscar solamente un determinado servicio en varias maquinas pertenecientes a una red.

2 ***Vertical:*** Se denomina escaneo vertical cuando el atacante se enfoca únicamente en un solo *host*, si se escanean todos los puertos pertenecientes a esa maquina se le llama *vanilla*, en cambio si solo se escanean determinados puertos o rangos se le conoce como *strobe*.

Existen diferentes técnicas utilizadas para realizar escaneos, las cuales se dividen en: *open*, *half-open* y *stealth* las cuales se van a explicar a continuación:

1 ***OPEN:*** Consiste en establecer una conexión TCP completa mediante este protocolo, el escaneador intenta establecer una conexión con un puerto concreto del *host* atacado, y dependiendo de la respuesta obtenida conoce su estado. Debido a su conexión de 3 vías (*threeway handshake*) son muy fáciles de detectar y detener.

2 ***HALF-OPEN:*** A diferencia de los escaneos OPEN estos consisten en finalizar la conexión antes de que se complete el protocolo a 3 vías, esto dificulta un poco su detección, pero se puede decir que casi todos los detectores de intrusos actuales son capaces de detectarlos. Como ejemplo de esta técnica se puede mencionar el SYN (Synchronize sequence Number) *Scanning* que consiste en que cuando el atacante recibe de la víctima los bits SYN+ACK, envía un bit RST en lugar del ACK (Acknowledge) lo que correspondería a una conexión de 3 vías completa. Este tipo de escaneo también son fáciles de detectar, pueden ser bloqueados por cualquier *firewall*. Pero existe una variante de esta técnica llamada *dumb scanning* en la que se utiliza otra maquina que ayuda a disfrazar el origen real del atacante, esta técnica debido a su complejidad es menos usada en la vida real.

3 ***STEALTH:*** Se conoce por este nombre a un grupo de técnicas que

cumplen una de las siguientes condiciones: *Eludir cortafuegos o listas de control de acceso, no ser registradas por sistemas de detección de intrusos, ni orientados a red ni en el propio host escaneado o simular tráfico normal y real para no levantar sospechas ante un analizador de red.* Una de las técnicas pertenecientes a esta familia es la llamada SYN+ACK la cual consiste en una violación a la conexión de 3 vías en donde el atacante en vez de enviar una trama SYN envía SYN+ACK si el puerto se encuentra abierto simplemente se ignora, y si se encuentra cerrado se da cuenta que no ha recibido un paquete SYN, por lo tanto se toma como un error y envía una trama RST para poner fin a la conexión.**[Ref8]**

Así es como funcionan las técnicas de escaneo existentes de las cuales se debe tener conocimiento y noción de su mecanismo de funcionamiento.

2.3 Spoofing

Se denomina IP Spoofing a la técnica que consiste en realizar un ataque simulando la identidad de otra máquina sin importar su ubicación, esto se hace con la intención de lograr obtener permisos y beneficios con los que cuenta la máquina por la cual se hace pasar el intruso, de esta manera poder acceder sin problemas a los recursos del sistema.

Como ya se mencionó, en este tipo de ataques entran en juego 3 máquinas cada una juega su propio papel. El principal objetivo del atacante es lograr establecer una comunicación falseada con su objetivo víctima y evitar que el equipo falseado interfiera en el ataque, esto se realiza simplemente lanzando una negación de servicio.

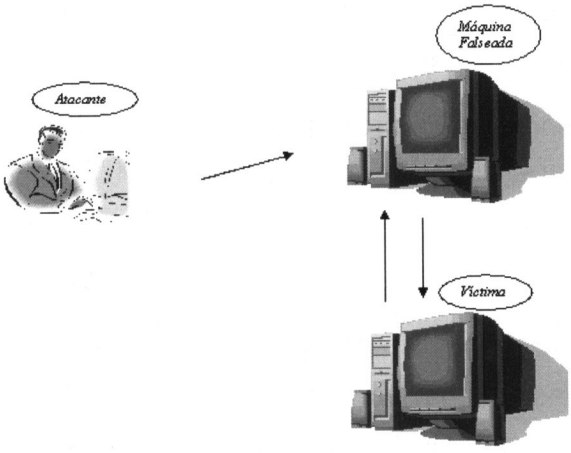


Figura 2.3 Elementos que intervienen en un ataque spoofing: **Atacante, Máquina Falseada y Víctima.**

Normalmente el ataque empieza cuando el intruso manda una trama SYN a su víctima dando una dirección correspondiente a otra maquina. La maquina objetivo lo que hace es responder mandando un SYN+ACK a esa dirección, el intruso ahora procederá a mandar una trama ACK a la víctima con la dirección de esa tercera máquina. Un punto importante a mencionar es que para lograr establecer la conexión, la trama ACK debe mandarse con un número de secuencia correcto, y es labor del intruso saber este número correctamente para lograr establecer la comunicación entre él y su víctima, una vez establecida la comunicación deberá a empezar a mandar datos a la víctima, lo cual se hace generalmente con el objetivo de tratar de abrir una puerta que permita una conexión normal entre las 2 máquinas.

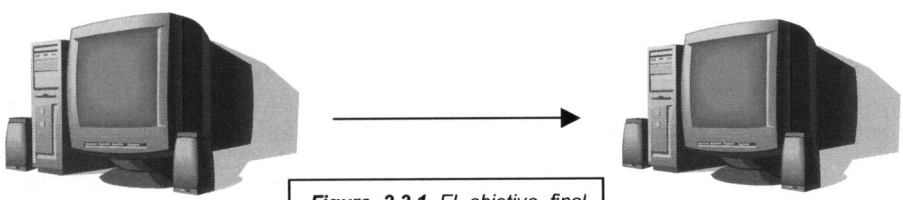


***Figura 2.3.1** El objetivo final es establecer una conexión directa entre las 2 maquinas (atacante y víctima), sin necesidad de una tercera.*

El IP spoofing se puede considerar un ataque ciego ya que el atacante no sabe nada de las respuestas o reacciones que tiene su víctima debido a que estas van hacia la maquina que fue deshabilitada anteriormente, por lo tanto el

atacante debe suponerse o imaginarse lo que esta sucediendo cada momento y tratar de responder adecuadamente a las respuestas que emite la víctima.

Aparte del IP Spoofing existen otras técnicas de falseamiento como: DNS Spoofing, ARP Spoofing y Web Spoofing de las cuales se hablará a continuación:

1 ***DNS Spoofing:*** Se refiere a falsear una dirección IP ante una consulta de resolución de nombre (resolver con una dirección falsa un nombre DNS) o viceversa (resolver un nombre falso una dirección IP. Este falseamiento de direcciones puede conseguirse de diferentes maneras, como 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 denomina DNS POISONING. Sin necesidad de tener acceso a un servidor DNS real, un atacante puede mandar como respuesta a una petición de una víctima datos falseados.

2 ***ARP Spoofing:*** Consiste en construir tramas de petición y respuesta ARP falseadas de tal modo que se puede obligar a una máquina víctima dentro de una red local enviar paquetes a la máquina atacante en vez de hacerlo a su correcto destino.

3 ***WEB Spoofing:*** Consiste en la creación de un sitio Web (falso) con contenido de interés de la víctima. El acceso a este sitio esta controlado por el atacante, de esta manera se pueden monitorizar todas las acciones de la víctima, su información, passwords, números de tarjetas de crédito. Así mismo el atacante puede modificar cualquier información que se transmita entre el servidor original y la víctima, a esta actividad también se le conoce con el nombre de *Phishing.*

Así es como funcionan las diferentes técnicas existentes de Spoofing de las cuales se debe tener conocimiento, tomar precauciones y saber que hacer en caso de ser víctimas de este tipo de ataques. **[Ref8]**

2.4 Negaciones de servicio (dos, denial of service)

Una negación de servicio es un ataque que consiste en deshabilitar los servicios que presta alguna red, computador o algún otro dispositivo. Este tipo de ataques se dividen en 3 grupos:

1 **Consumo de recursos escasos:** Su objetivo es agotar los recursos por ejemplo la conectividad de la red con el fin de evitar la comunicación con las demás máquinas. Así como se puede evitar la conectividad también se pueden evitar otros recursos del sistema, como espacio en disco duro, memoria, etc.

2 **Destrucción o alteración de la configuración:** Lo cual puede provocar problemas en cualquier área del sistema.

3 **Destrucción o alteración física de los componentes de la red:** Puede ocasionar problemas como no poder ingresar a la red, no tener comunicación con las demás máquinas y otros problemas que pueden hacer que el sistema trabaje de una manera ineficiente.

Existen diferentes técnicas para la realización de estos ataques a continuación se mencionarán las básicas:

1 **Negación de Servicio mediante UDP Flood (Inundación UDP):** Consiste en enviar muchos paquetes UDP (Protocolo de Datagramas de Usuario, User Datagram Protocol) a la víctima, por lo regular este tipo de ataques son acompañados por IP spoofing.

2 **Negación de Servicio con TCP SYN Flood:** Las víctimas de este tipo de ataques son los sistemas con servicios TCP. Una vez que el atacante ha enviado un mensaje SYN y ha recibido respuesta por parte del servidor con un mensaje SYN-ACK, el atacante no responde con el mensaje ACK, de esta manera se crea una conexión “medio abierta”. El servidor almacena en memoria la información mediante estructuras de datos indispensables para describir todas las conexiones pendientes, esta estructura de datos tiene un tamaño finito, por lo que puede ser desbordada intencionadamente creando múltiples conexiones "medio abiertas" y una vez que esta desbordada el sistema no es capaz de aceptar nuevas conexiones. La creación de conexiones “medio abiertas”

se realiza de manera fácil con IP spoofing, de tal manera que el paquete SYN llega al servidor y es imposible saber el origen del paquete.

3 **Negación de Servicio mediante paquetes ICMP:** Es una técnica cuyo objetivo principal es agotar el ancho de banda de la víctima, consiste en mandar a la víctima de forma constante una gran cantidad de paquetes de un tamaño considerable *ICMP echo request (ping)*, de tal manera que la víctima debe de responder con paquetes *ICMP echo reply (pong)* lo que provocaría una sobrecarga de información tanto en la red como en el sistema de la víctima. El nivel de sobrecarga varía dependiendo las capacidades de procesamiento con las que cuenten el atacante y la víctima, si el atacante cuenta con un nivel mucho mayor de procesamiento la víctima no puede controlar el tráfico generado.

Existe una variante denominada *smurf* que amplia de manera considerable los efectos de un ataque ICMP. En el *smurf* el atacante dirige paquetes *ICMP echo request* a una dirección IP de broadcast.

Cuando el atacante genera el paquete *ICMP echo request*, este es dirigido a una dirección IP de broadcast, pero la dirección origen del paquete IP la cambia por la dirección de la víctima (IP spoofing), de manera que todas las máquinas intermediarias (máquinas pertenecientes a la red donde se envió el paquete) responden con *ICMP echo reply* a la víctima.

Estas son las diferentes técnicas que existen para lanzar este tipo de ataques llamados Negaciones de Servicio, de las cuales es conveniente tener conocimiento de su existencia, así como de su mecanismo de funcionamiento con la finalidad de poder identificar las características pertenecientes a este tipo de ataques utilizando estos conocimientos en casos necesarios.

2.5 Sniffing

El concepto *sniffing* consiste en husmear todo el tráfico que pasa por una red filtrando la información que circula a través de la misma, aceptando únicamente la información que va dirigida a direcciones pertenecientes a esa red. Un sniffer puede ser software o hardware y funciona de manera similar a la intervención de líneas telefónicas que permite escuchar las conversaciones, de igual manera un *sniffer* permite ver todo la información que circula entre las computadoras pertenecientes a una red, su uso no es necesariamente mal intencionado.

Las principales tareas que se pueden llevar acabo gracias a los sniffers son:

1. Capturar nombres de usuarios de la red y contraseñas
2. Interpretar la situación del tráfico de red y mostrarla en una manera entendible para el usuario.
3. Analizar errores con el objetivo de descubrir problemas en la red
4. Medir el tráfico de red mediante el cual se pueden detectar cuellos de botella en algún punto de la red.
5. Detección de intrusos en algún *host* de la red
6. Crear registros de red con la intención de que los intrusos no se percaten que están siendo investigados

Los sniffers de paquetes están compuestos por diferentes componentes:

1. **Hardware:** Aunque la mayoría funcionan con adaptadores de red estándar hay algunos que necesitan algún hardware especial.
2. **Driver de captura:** Es la parte encargada de capturar el trafico de red, filtrar su contenido especifico previamente definido por el usuario y los resultados son almacenados en un búfer.
3. **Buffer:** Existen 2 diferentes mecanismos de funcionamiento del buffer, parar hasta que el búfer este lleno, o bien, ir sobrescribiendo los nuevos datos en los mas antiguos.
4. **Análisis en tiempo real:** Consiste en realizar un análisis de los bytes

que forman los paquetes que viajan a través de la red.

5 **Decodificación:** Es la parte donde se convierten los datos binarios en una forma legible e interpretable.

6 **Edición de Paquetes:** Consiste en editar paquetes en la propia red y reenviarlos a ésta misma, generando así paquetes personalizados con fines específicos.

2.6 Ataques a aplicaciones web

Cada vez son más las empresas que ponen en servicio una página Web, que tienen como objetivo el comercio electrónico o simplemente dar a conocer sus productos y/o servicios. Por esta razón se da el creciente número de sitios que para los atacantes es favorable ya que aumenta el número de sus posibles víctimas. La mayoría de los ataques exitosos se deben a una incorrecta configuración en el servidor, hablando en el caso de los sitios pertenecientes a grandes empresas los servidores con los que cuentan son de una gran complejidad ya que son varios aspectos los que se deben de tomar en cuenta como: Alta disponibilidad, balanceo de carga, lo cual se hace con la finalidad de lograr un buen servicio a los clientes esto debido a su gran número de visitantes.

Utilizando cualquier analizador de vulnerabilidades en los sistemas nos dará información útil para hacer mejoras en la seguridad de los servidores Web, además existen analizadores especializados en servicio Web. Estos analizadores proporcionan bastante información sobre la configuración así como de archivos y carpetas en los servidores que pueden resultar ser bastante útiles para los atacantes.

Cuando se habla de CGI (Common Gateway Interface, Pasarela de Interfaz Común), se esta haciendo referencia a una importante tecnología de la World Wide Web que permite a un cliente solicitar datos a través de un programa ejecutado en un servidor web. CGI especifica un estándar para transferir datos

entre el cliente y el programa, es utilizado para contadores de visitas, bases de datos, motores de búsqueda, formularios, generadores de mail automáticos, chats juegos en línea y otros.**[Ref8]**

Para mejorar la seguridad en el caso del uso de archivos CGI populares, lo que se tiene que hacer es consultar una base de datos de vulnerabilidades como *securityfocus* **[Ref9]**, y buscar el nombre de ese archivo CGI, y así obtener información sobre los posibles problemas de seguridad que el servidor pueda presentar.

Para evitar este tipo de problemas se puede tomar algunas medidas de seguridad como:

1 **Eliminar del servidor directorios o archivos CGI** que se instalen por defecto.

2 **No Instalar en el servidor programas innecesarios** para el correcto funcionamiento del *software*, ya que en ciertos casos abren grandes agujeros de seguridad que permiten el acceso al código fuente de archivos, lectura de archivos o hasta la ejecución de comandos bajo la identidad del usuario con que se ejecuta el demonio servidor obteniendo privilegios para manipular información.

3 **Deshabilitar el *Directory Indexing*** que por defecto muchos servidores incorporan la capacidad de obtener el listado de un directorio cuando no existe un fichero `index.html` o similar en el mismo.

4 **Nunca ejecutar el demonio servidor con el usuario Administrador** pero tampoco un usuario genérico; siempre debe ser un usuario dedicado y sin acceso real al sistema, sin otorgarle los privilegios de escritura.

Con la puesta en práctica de estas recomendaciones se podrá obtener una seguridad con mayor fiabilidad en los servidores, evitando así ser víctimas de ataques que pueden llegar a ocasionar grandes daños en el funcionamiento adecuado de los servidores en las corporaciones.

CAPITULO 3
SISTEMAS DE DETECCION DE INTRUSOS

3.1 Definición de IDS

Un IDS es un sistema de seguridad que funciona mediante un monitoreo constante, buscando determinados patrones de actividad sospechosa que pretenda comprometer la seguridad de una red o *host*. Con la implementación de un IDS se aumenta la seguridad de manera considerable ya que previenen y alertan al usuario ante la posibilidad de un ataque.**[Ref10]**

3.2 Clasificación de los IDS

Los IDS pueden ser clasificados según el sistema que tienen a cargo ya que pueden ser IDS basados en:

1. **Red:** Se encarga de monitorear toda la información que circula por la red, buscando elementos sospechosos que puedan comprometer la seguridad de algún *host* que se encuentre dentro de la red. Este tipo de IDS puede ser colocado en cualquier punto de la red ya sea un *host* o un elemento que supervise el trafico (enrutador o *firewall*).
2. **Máquina:** Los IDS basados en máquina tienen la labor de proteger únicamente una máquina buscando patrones de actividad dentro de la misma que atente en contra de su seguridad. Estos a su vez se dividen en 3 categorías:
    - **Verificadores de Integridad del Sistema (SIV, System. Integrity Verifiers):** Se encargan de monitorear archivos de la máquina buscando posibles modificaciones realizadas sin autorización. Debido a la importancia de estos mecanismos ya están siendo incluidos en sistemas operativos.
    - **Monitores de Registros (LFM):** Monitorean los archivos de bitácora *(*.log)* que son originados por programas, y es en estos en donde se buscan patrones de actividad que puedan indicar algún ataque o intrusión.
    - **Sistemas de Decepción:** Estos funcionan mediante la simulación de problemas de seguridad, de tal manera que el intruso crea que es un buen momento para acceder al sistema pero en verdad se están registrando todas sus actividades.

Existe otra manera de clasificar los IDS que es conforme a su manera de actuar y son las siguientes:

1 **Detección de Anomalías:** Una intrusión ocasiona comportamientos anormales en el sistema, por lo tanto, estableciendo ciertos lineamientos de comportamiento del sistema cualquier actividad que sobrepase estos lineamientos puede considerarse como una anomalía es decir un ataque o intrusión.

2 **Detección de Usos Indebidos:** En este tipo de mecanismos se establecen los patrones de comportamiento de diferentes tipos de ataques y sus variantes.

La diferencia del funcionamiento de estos dos tipos de mecanismos de detección de ataques es que en la *Detección de Anomalías* su objetivo es detectar los comportamientos desconocidos mientras que la *Detección de usos Indebidos* detecta los patrones de comportamiento de ataques conocidos.

Así es como se pueden clasificar los IDS existentes, esto con la finalidad obtener un mejor entendimiento de su funcionamiento, conociendo así las diferentes maneras que existen para detectar intrusos en una red o máquina, buscando siempre la seguridad e integridad de los sistemas.**[Ref8]**

3.3 Requisitos de un IDS

Independientemente del mecanismo de funcionamiento y de los sistemas que estén bajo su vigilancia, un IDS debe cumplir con ciertos requisitos para desempeñar su función de la manera correcta los cuales a continuación se van a mencionar y explicar:

1 **Continuidad:** Un IDS debe ejecutarse de manera continua sin la necesidad de supervisión del hombre.

2 **Aceptabilidad:** Lograr un nivel de aceptabilidad por parte del usuario ya que no debe generar sobrecarga en el sistema, así como tampoco debe generar demasiadas falsas alarmas de intrusión (falsos positivos) o

registros de bitácoras ya que llegará un momento en que se perderá la credibilidad y no se tomaran en cuenta las alertas emitidas.

3 **Adaptabilidad:** Debe tener la capacidad de adaptarse al entorno de trabajo, ya que en los sistemas informáticos se da una gran variedad de eventos como instalaciones de aplicaciones que cambian el entorno.

4 **Tolerancia:** Debe tener un nivel de tolerancia a errores o bien, una capacidad saber responder a situaciones inesperadas, ya que los entornos informáticos son cambiantes, muchos de estos cambios se pueden considerar bruscos y es por eso que un IDS debe saber como responder a estos cambios.

Un IDS que cumpla con los puntos ya mencionados se puede decir que cuenta con un buen desempeño de su funcionamiento, realizando así su labor de una manera eficiente y efectiva.**[Ref8]**

3.4 IDS Basados en Máquina

Un IDS basado en máquina es un sistema de seguridad encargada de detectar intrusiones en la máquina en donde se esta ejecutando.

Por lo general los IDS basados en máquina han funcionado mediante el ***análisis de logs*** los cuales son generados por aplicaciones o por el mismo sistema operativo, otros en la ***verificación de la integridad*** de archivos importantes para el sistema como el referente a las contraseñas. Sin embargo hace algunos años se ha empezado a usar otro método de detección de intrusos el cual consiste en el uso de ***honeypots*** (tarros de miel).

El ***análisis de logs*** generados por el sistema varía entre cada sistema operativo ya que cada uno guarda la información en diferentes formatos y en diferentes ubicaciones, aunque la mayoría de los sistemas operativos puedan guardar los datos suficientes para poder identificar un ataque ya que todas las actividades que se llevan acabo en el sistema son registradas, el problema se

encuentra en los administradores del sistema ya que muy pocos de ellos se preocupan por revisar esas bitácoras y es por eso que los ataques exitosos o no, pasan desapercibidos, es por eso que es conveniente con una herramienta automática de análisis que se encargue de analizar los archivos de bitácora.

La ***verificación de integridad*** de los archivos puede ser realizada a diferentes niveles variando el grado de seguridad entre uno y otro, independientemente del modelo de verificación que se este usando se debe generar una base de datos la cual posteriormente será comparada con la información de los archivos, de esta manera si se encuentra diferencia entre la información guardada en la base de datos y la información actual de los archivos puede ser una señal de ataque.

Los ***Sistemas de Decepción o Honeypots*** se basan en lo que se le conoce como "conocimiento negativo" que consiste en dar al intruso información falsa simulando vulnerabilidades en el sistema de interés para él, esto con la finalidad de monitorear las actividades que realiza o simplemente despistarlo. Para que este tipo de engaños tenga resultado se debe contar con una simulación bastante real ya que existen atacantes muy experimentados y no son tan fáciles de engañar.

Existen otros sistemas de decepción que su labor no es precisamente engañar simulando vulnerabilidades durante un largo lapso de tiempo mostrando un apariencia muy realista, sino que únicamente muestran un entorno simple, su labor consiste en recopilar la información del atacante y su comportamiento.**[Ref8]**

3.5 IDS Basados en Red

Los IDS basados en red son sistemas encargados de detectar ataques dirigidos en contra de diferentes *hosts* pertenecientes a una misma red, por lo general los IDS son ejecutados solamente en uno de los *host* que forman parte de la misma. Para cumplir con su trabajo todas las tramas que pasan por ahí

son capturadas y analizadas buscando comportamientos que puedan indicar ataques.

Muchos de los campos que forman parte de una trama de red TCP/IP pueden tener valores que puedan representar un ataque, entre los casos mas comunes se encuentran:

1 **Campos de fragmentación:** Una cabecera IP contiene 16 bits asignados para información acerca del nivel de fragmentación del datagrama, de los cuales 1 no se utiliza y 13 indican la ruta del la información que llevan. Los otros 2 bits restantes indican si el paquete ha sido fragmentado por un router o es único, esto sirve para indicar si a continuación vendrán mas paquetes (MF, More fragments) o no (DF, Dont fragment). Mediante el uso de alteraciones de información de fragmentación de los datagramas se han estado causando negaciones de servicio a los sistemas, además también han servido para obtener información del sistema operativo que se utiliza en determinada máquina.

2 **Dirección Origen y Destino:** Estas direcciones referidas a una máquina que envía un paquete y a otra que lo recibe, son información importante para detectar intrusiones dentro de alguna máquina o red. Tan sólo pensando en el tráfico que viene de la DMZ que tenga como objetivo nuestra red, existe gran probabilidad que esos paquetes sean enviados con la finalidad de una violación de la seguridad de nuestros sistemas.

3 **Puerto Origen y Destino:** Mediante estos valores se pueden detectar comportamientos anormales que puedan atentar en contra de la seguridad de nuestros sistemas, como troyanos, escaneo de puertos, o bien la presencia de sistemas no autorizados dentro de nuestra red.

4 **Flags TCP:** Dentro de una cabecera TCP un campo contiene 6 bits (URG, ACK, PSH, RST, SYN Y FIN) cada uno de estos tienen una finalidad diferente (por ejemplo, SYN su función es crear una conexión nueva, por el contrario FIN sirve para liberarla). El valor de cada uno de estos *bits* será 0 o 1, lo cual de forma aislada no suele decir mucho de su emisor, ciertas combinaciones de valores suelen ser bastante

sospechosas: por ejemplo, una trama con los dos *bits* que se mencionaron anteriormente SYN y FIN activados simultáneamente sería indicativa de una conexión que trata de abrirse y cerrarse al mismo tiempo.

5 **Campos de Datos:** El campo de datos de un paquete que circula por la red es con el que se tiene una alta probabilidad de localizar ataques en contra de nuestros sistemas, esto debido a que el *firewall* detendrá tramas que contengan cabecera sospechosa pero en rara ocasión un *firewall* analizará los datos contenidos en la trama.

Estos campos pertenecientes a una trama TCP/IP al presentar comportamiento anormal en sus valores, puede ser indicativo de un ataque ya que son características propias del mismo.

Otro punto importante del cual se hablará en este tema de los sistemas de detección de intrusos basados en red son las *Honeynets* que son una herramienta con cierto parecido a las *honeypots* pero a diferencia de éstas, las *honeynets* son aplicadas a redes las cuales son diseñadas para ser comprometidas, una vez penetradas capturan y analizan las acciones que realiza el intruso de esta manera tener información sobre sus técnicas y objetivos

Básicamente las diferencias existentes entre una *Honeypot* y una *Honeynet* son:

1 *Honeynet* es una red que consta de **varias máquinas** a diferencia de una *honeypot* que es únicamente para una máquina.

2 *Honeynet* **no simula vulnerabilidad** puesto que los sistemas dentro de la red son sistemas reales, ya que ejecutan aplicaciones reales como bases de datos, sistemas de desarrollo y todo lo que se pueda encontrar en un entorno de trabajo normal.

3 *Honeynet* **no tiene como objetivo la decepción** sino conocer las acciones que realiza un intruso.

El correcto funcionamiento de una *honeynet* tiene 2 principios que son sus principales tareas a realizar para el correcto funcionamiento y se mencionan a continuación:

1 **Control de flujo de datos:** Esto se refiere a que una vez penetrado algún sistema que esté bajo la *honeynet* evitar que sea utilizado como arma de ataque a otras máquinas dentro o fuera de la red, manteniendo la *honeynet* bajo un perfecto control.

2 **Captura de datos:** Monitorización de las acciones que un atacante realiza dentro de la *honeynet* ya que el objetivo es conocer las acciones que realizan los piratas para poder aplicarlos a sistemas reales, debido a esto es necesario llevar acabo una correcta recopilación de los datos aportados por el intruso de ser posible realizar captura de datos de cada una de las acciones que realice sin que el intruso se percate de ello. Además se deberán mantener los datos fuera de la *honeynet* ya que de lo contrario seria posible su destrucción por parte de cualquier intruso.

Este concepto de *honeynet* es relativamente nuevo, se puede considerar una idea bastante interesante es por eso que se espera que empiece a ser implantada en mas lugares de esta manera extendiéndose su uso para la obtención de resultados de beneficio para la seguridad en las organizaciones.

Un claro ejemplo de honeynet es el proyecto llamado *"Conoce a tu enemigo" (Honeynet Project Know your enemy)* el cual esta hecho con la intención obtener y aportar información con el fin de ayudar a tener unos sistemas con mayor seguridad por lo tanto mas difíciles de violar. **[Ref11].**

3.6 Detección de anomalías

Un IDS basado en detección de anomalías funciona conociendo lo que es normal en el comportamiento de la red o máquina donde sea empleado, de esta manera los eventos que se producen son comparados con patrones de comportamiento considerados normales, por lo tanto en caso de que se

produzca un evento que este fuera de los limites de lo normal, es catalogado como sospechoso.

Existen 2 maneras para que un sistema de detección de anomalías sepa lo que es normal:

1 **Especificando:** Consiste en especificar mediante reglas los perfiles de comportamiento normal, basándose en determinados parámetros de los sistemas.
2 **Aprenderlo por cuenta propia:** Para lograr esto se utilizan métodos estadísticos, también existe la aplicación de algoritmos para un aprendizaje automático.

Los sistemas de detección de anomalías basados en especificaciones funcionan mediante la descripción del comportamiento deseable o normal de aquellos programas cuya seguridad sea crítica, esa descripción se elabora basándose en una especificación de seguridad y es realizada mediante gramáticas, es considerada una violación de seguridad la ejecución de programas que violen esta especificación.

Los problemas en este tipo de sistemas se presentan a la hora que se tienen que especificar los parámetros que deben ser considerados normales y conforme van aumentando el tamaño de los sistemas en caso de las redes se hacen mas imprescindibles por lo tanto mayor dificultad para establecer los parámetros normales.

En el caso de los métodos estadísticos, el detector monitorea las actividades de los elementos del sistema y genera un perfil que define el comportamiento de cada uno de ellos, este perfil se almacena en el sistema y es actualizado con cierta frecuencia dándole preferencia a la información mas reciente. El comportamiento del usuario es almacenado de manera temporal en otro perfil llamado “perfil actual” (current profile), y de esta manera se compara constantemente el perfil almacenado con el perfil actual buscando comportamientos anormales.

Para la elaboración de estos perfiles que se mencionaron anteriormente se toman en cuenta diferentes datos tales como:

1 **Intensidad de la actividad:** Son los que dicen el progreso de la actividad del sistema para lo cual los datos son recogidos a intervalos muy pequeños (entre un minuto y una hora). De esta manera mediante estas descargas de datos se detectan comportamientos que en lapsos de tiempo mas largos no podrían ser detectadas

2 **Numéricas:** Son medidas de la actividad del sistema que pueden ser representadas mediante valores numéricos, como la cantidad de archivos usados por cierto usuario, el numero de intentos fallidos de ingreso al sistema, etc.

3 **Categóricas:** Consiste en categorizar las actividades de acuerdo a la frecuencia con la que se realizan con respecto a otras actividades.

4 **Distribución de registros de auditoria:** Consiste en analizar las actividades realizadas con anterioridad basándose en las bitácoras que son generadas por las mismas, este análisis es realizado con una ponderación de las actividades, dándole mayor valor a las realizadas recientemente, y es comparado con un perfil de actividades "habituales" almacenado previamente, de esta manera se detecta si en un pasado reciente se han generado eventos anormales.

En el caso de los sistemas de aprendizaje automático rápido el problema se encuentra en que un intruso antes de que el responsable de los sistemas se percate puede realizar acciones para conseguir un modelo distorsionado de lo "normal", de tal forma que el IDS no llegue a detectar un ataque porque lo considera algo normal. En cambio si el aprendizaje es lento, a cualquier evento que se aleje lo mas mínimo de sus patrones el IDS lo considerará como algo anormal, generando así un gran número de falsos positivos, que a un largo plazo harán que los responsables de los sistemas ignoren cualquier información proveniente del IDS, de esta manera tomando riesgos. **[Ref8]**

3.7 Detección de usos indebidos

Así como están los IDS basados en Detección de anomalías también existen los IDS basados en Detección de usos Indebidos y su funcionamiento consiste en especificar las diferentes tipos de intrusiones que amenazan a los sistemas y para esto existen 4 diferentes mecanismos: los sistemas expertos, los análisis de transición entre estados, las reglas de comparación y emparejamiento de patrones (*pattern matching*) y la detección basada en modelos.

1 **Sistemas Expertos:** En estos sistemas las intrusiones se detectan a través de condiciones que son codificadas con la estructura básica *Si Condición entonces Acción (If-then),* es decir contienen una condición para cada evento que se pueda presentar que denote una intrusión.

2 **Análisis de Transición entre Estados:** Este método consiste en dividir en estados del sistema el lapso que transcurre entre el inicio de una intrusión y la culminación de la misma, cada estado es una configuración diferente de los parámetros del sistema, por lo tanto si se logra identificar los estados que se encuentran entre el inicio y el final de la intrusión será posible detener la intrusión antes de que esta finalice con éxito.

3 **Reglas de Comparación y Emparejamiento de Patrones (*Pattern Matching*):** Este sistema funciona utilizando una base de datos que contiene información referente a los patrones que denotan ataques, de esta manera el programa monitorea el trafico examinando y comparando determinadas propiedades de cada trama con la información almacenada en la base de datos, en caso de que alguna de las tramas empareja con un patrón sospechoso automáticamente se genera una alarma en el registro del sistema.

4 **Detección Basada en Modelos:** Se trata de un mecanismo que contiene cierta similitud con la técnica de *Análisis de Transición* entre *Estados* ya que considera los ataques como un conjunto de estados y objetivos, pero en vez de tomarlos como *transiciones* de estado los

representa como *escenarios*, y su mecanismo de detección consiste en realizar una deducción sobre la existencia o no de una intrusión, para esto se utiliza una base de datos de escenarios los cuales están formados por eventos que constituyen un ataque. En cada momento existe un conjunto de escenarios, a los que se les llama escenarios activos que son los ataques que se pueden presentar en el ámbito. El sistema genera unos registros de auditoria los cuales son analizados por un proceso llamado *anticipador*, de esta manera obtiene los eventos que hay que verificar en tales registros y de esta manera determinar si la intrusión se esta o no produciendo.

El anticipador también se encarga de actualizar de manera constante el conjunto de escenarios activos, de manera que este estará siempre formado por los escenarios que representan posibles ataques en un momento determinado y no por toda la base de datos.

Así es como funcionan los diferentes tipos de IDS existentes para la protección de los sistemas, ya sea que se trate de una sola máquina o bien de toda una red a la que se tenga que brindar protección, los Sistemas de Detección de Intrusos son una buena herramienta para la prevención de ataques que pueden llegar a ocasionar grandes daños a la información manejada a través de los sistemas. **[Ref8]**

CAPITULO 4
INFORMATICA FORENSE

4.1 ¿Qué es la Informática Forense?

Se puede definir a la informática forense como el área de la informática encargada de llevar acabo todos los pasos necesarios para la investigación de sistemas informáticos corrompidos que va desde investigar las causas como ataques, fallas de dispositivos o errores humanos hasta la recuperación y presentación de información perdida. La búsqueda y extracción de información valiosa de los sistemas dañados se realiza mediante la ayuda de técnicas y herramientas tales como hardware y software especializados, posteriormente la reconstrucción de los hechos con la finalidad de obtener la información que le ayudara a saber determinar la causa del mal funcionamiento de los sistemas y finalmente la implementación de normas de seguridad que ayudaran a prevenir un suceso similar.

Sin duda alguna la informática forense es de gran importancia, principalmente para las empresas e instituciones gubernamentales que manejan grandes cantidades de información a través de medios electrónicos, por lo que están expuestos a sufrir perdidas si no se tienen las debidas precauciones, es por eso que se recomienda estar preparados tomando medidas tales como establecer políticas de seguridad informática, en donde se especifique la prohibición de acciones con las que se considere se ponga en riesgo la información, así como también tener respaldos de la misma para evitar una perdida mayor en caso de presentarse una situación que atente en contra de la seguridad de los sistemas de información.

4.2 Su Labor

La informática forense esta encargada de varias tareas entre las más importantes se puede destacar la recuperación de información donde a veces se presentan dificultades y es necesario el uso de herramientas especiales para la extracción de la información. En informática forense hablamos ya no sólo de recuperación de información sino de descubrimiento de la misma debido a que no necesariamente se haya presentado una falla del dispositivo ni

un error humano sino alguna actividad oculta para borrar, alterar o esconder información.

Como ya se menciono la informática forense no solamente se encarga de recuperar información, sino que su campo de acción es más amplio ya que también juega un papel importante utilizando sus herramientas y conocimientos para el cumplimiento de la ley mediante la investigación de otros delitos tales como:

Pornografía Infantil: producción, distribución y posesión de pornografía

Infantil.

Fraude en las comunicaciones: Locutorios telefónicos clandestinos.

Dialers: Modificación oculta del número de teléfono de destino.

Producción y distribución de decodificadoras de televisión privada.

Fraudes en Internet: Estafas, subastas ficticias y ventas fraudulentas.

Carding: Uso de tarjetas de crédito ajenas o fraudulentas.

Phishing: Redirección mediante correo electrónico a falsas páginas simuladas trucadas.

Cartas nigerianas: Correos electrónicos que ofrecían participar en una operación de exportación de capitales depositados en un país africano o en Irak a cambio de una comisión, cuando la víctima acepta se le exige dinero justificándolo en el pago de tasas aduaneras.

Seguridad lógica: Virus, Ataques de denegación de servicio, Sustracción de datos, Hacking, Descubrimiento y revelación de secretos, Suplantación de personalidad, Sustracción de cuentas de correo electrónico, Delitos de injurias, Calumnias y amenazas a través del e-mail, noticias, foros, chats o SMS.

Propiedad intelectual: Piratería de software, música y de producciones cinematográficas.

Robos de código: Obtención ilícita de código fuente original de aplicaciones, videojuegos, etc.**[Ref12]**

También algunos otros delitos relacionados con nuestra vida cotidiana pueden ser investigados con la ayuda de la informática forense:

1. **Prosecución Criminal:** Ayudando a proseguir con la investigación de delitos como homicidios, fraudes financieros, evasión de impuestos.
2. **Litigación Civil:** Puede ayudar a resolver casos relacionados de tipo civil como fraudes, discriminación, acoso, divorcios.
3. **Investigación de Seguros:** Ya que la información encontrada en computadoras puede ayudar a las compañías de seguros a disminuir sus costos de reclamos por accidentes.
4. **Temas Corporativos:** Se puede obtener información relacionada con acosos sexuales, robos, mal uso o apropiación de información confidencial de las corporaciones.
5. **Mantenimiento de la ley:** Aplicada en la búsqueda inicial de ordenes judiciales, así como la búsqueda de información útil una vez que se tiene la orden judicial y realizar una búsqueda exhaustiva. **[Ref13]**

Estos son tan solo unos ejemplos de las labores que realiza la informática forense. Como se puede apreciar es bastante amplio su campo de aplicación ya que puede ayudar a muchas áreas del conocimiento puesto que en la actualidad dentro de las computadoras se maneja cualquier tipo de información.

4.3 Elementos que Intervienen en ella

Los elementos de la informática forense son aquellos necesarios para que se lleve acabo un proceso de investigación a cargo de personas especializadas en el campo de la Informática forense, para que una investigación se inicie se requiere que un autor atente en contra de una víctima y es aquí donde se necesita la labor de las personas especializadas en la materia para realizar una investigación completa y efectiva ya que ellos cuentan con mayor conocimiento

y con herramientas para lograr una investigación a fondo y recuperación de información exitosa.

4.4 El Futuro de la Informática forense

Se dice que es un área que continuará creciendo debido a que se están requiriendo cada vez más los servicios de la informática forense. El experto en la materia Doctor Jeimy J.Cano, Ingeniero de Sistemas y Computación Universidad de los Andes (Colombia) comentó respecto al auge que estará tomando en un futuro no muy lejano esta área del conocimiento, y lo expreso de esta manera:

> *"el desafortunado 11-S fue uno de los detonantes que nos alertó sobre las fallas reiterantes que las organizaciones venían teniendo con relación a la seguridad. Sin embargo, pese a esta realidad, con anterioridad diversos medios de información y estudios indicaban la necesidad de contar con personal entrenado en actividades forenses, como soporte y ayuda en investigaciones on-line. A la fecha, las autoridades de policía, los fiscales o autoridades judiciales, continúan en la búsqueda de profesionales en computación forense, con relativo éxito. En este sentido, revisando estudios sobre programas de formación y especialidades en esta rama, el resultado es pobre; lo que sugiere la necesidad de establecer programas de formación técnica y forense para desarrollar un perfil adecuado a las necesidades y evolución de la delincuencia informática"* **[Ref14].**

Por lo tanto, podemos decir que la ciencia forense experimentará un crecimiento apreciable hasta llegar a un punto donde tendrá un alto nivel de demanda, es por eso que cada vez mayor numero de profesionales de esta área deberán estar preparados manteniéndose en constante actualización en cuanto a las tendencias y soluciones de los casos que se les pueden presentar ya que serán requeridos para prestar sus servicios de manera eficiente.

4.5 Análisis Forense

Se conoce como Análisis Forense al proceso de investigación que se lleva a cabo con el objetivo de reconstruir los hechos que fueron realizados para finalmente saber lo que sucedió y encontrar al individuo responsable de las actividades que fueron llevadas a cabo. Cuando se habla de un Análisis Forense en materia de Informática se hace con la intención de saber de donde se originó el ataque, cuales fueron los daños ocasionados en los sistemas de información, que herramientas fueron utilizadas para realizar el ataque, y todo lo que pueda ayudar a saber con claridad lo que aconteció. El análisis forense consiste en llevar a cabo los siguientes pasos:

1 Aseguramiento del Lugar de los Hechos.
2 Identificación de Indicios.
3 Preservación de Indicios.
4 Análisis de Indicios.
5 Presentación y Reporte.

Es necesario tener una idea bien definida sobre los conceptos mencionados anteriormente, ya que solo de esta manera se obtendrán buenos resultados obteniendo una completa y exitosa investigación.

Antes de realizar un análisis se debe tener en cuenta la siguiente información:

a) Sistema operativo afectado.
b) Inventario de software instalado en el equipo
c) Tipo de hardware del equipo
d) Accesorios y/o periféricos conectados al equipo
e) Si posee *firewall*
f) Si esta en el ámbito del DMZ
g) Conexión a Internet
h) Configuración
i) Parches y/o actualizaciones de software
j) Políticas de seguridad implementadas
k) Forma de almacenamiento de la información (cifrada o no)
l) Personas con permisos de acceso al equipo

m) La Pc esta dentro del DMZ

n) Existe IDS

o) Cuantos equipos en red **[Ref15]**

Es así como la informática forense cumple su labor de esclarecer los hechos relacionados con los sistemas de información corrompidos.

4.5.1 Aseguramiento del Lugar de los Hechos

El lugar de los hechos es el lugar en donde se llevan a cabo las actividades efectuadas por un individuo que atentan en contra de una víctima alterando su integridad. En términos de Informática Forense cuando se habla del Lugar de los Hechos (Escena del crimen) se esta haciendo referencia a la máquina o red que ha sido víctima de un ataque.

El lugar de los hechos juega un papel importante para la investigación del origen del ataque, es por eso que una vez después de haber comprobado haber sido víctima de un ataque se debe tener un cuidado extremo, esto con el objetivo de evitar realizar cambios en la información manteniendo intacto el lugar de los hechos, por lo tanto el primer paso para realizar una investigación de informática forense será asegurar esta zona restringiendo el acceso al lugar evitando que se produzca alguna modificación, ya que ésta será el área de trabajo que los agentes forenses deberán inspeccionar en busca de evidencias hasta que todas las pruebas posibles sean recolectadas.

Para llevar a cabo esta tarea es necesario asignar a una persona con suficiente autoridad para la toma de decisiones que aseguren el lugar de los hechos, dirigir la búsqueda de indicios y llevar a cabo el proceso de preservación de los mismos, el cual se realiza mediante el seguimiento de los siguientes pasos:

1. Identificar el Lugar de los hechos, para lo cual se debe establecer un área determinada en donde el sospechoso habría estado realizando su ataque.

2. Elaborar un listado de los sistemas relacionados con el ataque.

3. Restringir el acceso al Lugar de los hechos tanto a personas como a otros equipos.

4. Preservar todas las huellas digitales, usar guantes de látex.

5. Tomar fotografías, video grabar y realizar un esquema del Lugar de los hechos, en caso de que la información de alguna fotografía o video grabación no sea identificable, copiar manualmente la información entendible.

6. Dejar intacto el estado de los dispositivos ya sea que se encuentren prendidos, apagados, hibernando, etc.

7. Si hay equipos portátiles apagados, retirar la batería.

8. Si hay equipos prendidos fotografiar y grabar la pantalla.

9. Retirar las conexiones de red.

10. Verificar si existen conexiones inalámbricas que puedan permitir conexiones remotas, en caso que si existan desconectarlas.

11. Si se encuentran impresoras funcionando, permitir que terminen su trabajo.

12. Antes de apagar el sistema tomar nota de la fecha y hora del mismo, registrándolo con fotografías y si es posible con video grabación.

13. Los dispositivos encendidos apagarlos retirándoles el cable de alimentación de la parte de atrás, no de la toma de corriente. Ya que esto previene que se graben datos en el disco duro o en el medio de almacenamiento del dispositivo.

14. Colocar etiquetas a cables y componentes.

15. Una vez colocadas las etiquetas fotografiar y video grabar de nuevo.**[Ref16]**

4.5.2 Identificación de Indicios

Un indicio se puede decir que es una prueba que confirma la veracidad o falsedad de cierta situación, en el caso de la Informática Forense se puede catalogar como indicio la información que contribuye a la investigación realizada con el objetivo de conocer el origen o causa de un ataque realizado en contra de los sistemas de información.

Los indicios digitales se pueden presentar en diferentes formas, para llevar a cabo el proceso de identificación de indicios, es necesario saber que técnicas o procedimientos serán utilizados para el análisis forense así mismo los agentes forenses deben saber identificar el formato en el que se encuentra la información, saber determinar los mecanismos para extraerla, almacenarla y preservarla. Para realizar una identificación de los indicios primeramente se deberá clasificar entre la información en volátil (aquella información que se pierde a falta de energía eléctrica) y no volátil (aquella información que perdura aun sin energía eléctrica).

La información volátil se deberá obtener con la mayor rapidez posible, este tipo de información se puede localizar en las siguientes ubicaciones:

1 En los registros y el cache del procesador
2 En la memoria Ram

3 Estado de la red
4 Tablas de ruteo
5 Caché ARP
6 Estadísticas del Kernel y Módulos
7 Archivos Temporales del Sistema
8 Tabla de procesos
9 Archivos abiertos
10 Tiempos de los archivos (tiempos MAC: creación, acceso y modificación)
11 Sistemas de Archivos Montados
12 Sistemas de Archivos virtuales.
13 Mensajes de Correo Electrónico
14 Archivos de Impresión
15 Historiales de los navegadores
16 Favoritos de los navegadores
17 Cookies
18 Bitácora del Sistema Operativo
19 Bitácora de aplicaciones
20 Bitácora de clientes de Chat
21 Documentos de texto
22 Hojas de cálculo

Estos elementos forman parte de la información volátil por lo que puede ser fácilmente perdida sin necesidad de reiniciar el equipo. Por lo tanto, toda aquella información que forme parte de este grupo al ser conseguida deberá ser guardada como archivo en otro dispositivo de almacenamiento logrando que su integridad sea preservada.

También se deberá realizar una clasificación de las pruebas según el lugar donde se pueda encontrar.

En las Computadoras:

1 En sus dispositivos como Teclado, Ratón, Monitor.
2 Cámaras de video digitales y Cámaras de fotografía digitales
3 Cintas usadas para respaldo

4 Tarjetas PCMCIA
5 Unidades de almacenamiento como: Discos duros, Disquetes, Discos Compactos, DVD's, "Memory Stick", "Memory Cards".
6 Impresoras y Escáneres

En las Redes:

1 Switches
2 Ruteadores
3 Concentradores
4 Tarjetas de red
5 Modems
6 Tarjetas de Red inalámbricas
7 Puntos de Acceso

Otros lugares:

1 Teléfonos
2 Organizadores de mano (PDA, PocketPC, etc)
3 Contestadoras
4 Fax
5 Fotocopiadoras
6 Manuales
7 Papel de la(s) impresora(s)

Por lo general las pruebas se encontrarán en el sistema de archivo del equipo o dispositivo comprometido, por lo cual a veces es innecesario emplear tiempo en la recolección de información que no será útil para resolver el caso. **[Ref16]**

4.5.3 Preservación de Indicios

El proceso de preservación debe ser realizado lo más pronto posible evitando generar cualquier cambio durante la realización del mismo, la preservación de la evidencia es necesaria debido a que puede ser requerida posteriormente su

análisis ante una entidad judicial, aun así existen situaciones en que el realizar algún cambio es inevitable, por lo tanto todo cambio o alteración realizada debe ser registrada, documentada y justificada.

Para lograr una correcta preservación de la información es necesario llevar a cabo un proceso siguiendo paso a paso las siguientes indicaciones:

1. Si el sistema se encuentra encendido de ser posible retirar el dispositivo de almacenamiento del sistema y colocarlo en otra computadora con la finalidad de extraer su información.

2. La información deberá ser copiada por medio de software especial con la finalidad de no alterar la información manteniéndola integra.

3. Utilizar métodos para crear duplicados de los dispositivos de almacenamiento de la información a nivel de bit, guardando el duplicado de la información en cualquier otro medio de almacenamiento.

4. Asegurar que la fecha y hora del sistema sean correctas ya que pueden ser importantes en la resolución del caso.

5. Conservar datos que se encuentren en dispositivos de mano como PDA´s y PocketPC`s utilizando programas que realizan el trabajo de duplicar los datos que se encuentran almacenados en este tipo de dispositivos.

6. Checar la integridad de los archivos originales y copia mediante el método de checksum criptográfico el cual verifica los archivos bit por bit, esto con la finalidad de asegurar que no hayan sido alterados.

7. Documentar quien, donde, como, cuando y porqué preservó la evidencia.

8. Realizar el embalaje empaquetando todos aquellos dispositivos que

contengan evidencias registrándolos con un identificador, nombre de la persona y organización responsables de la recolección y empaquetado del material.

9. Introducir en bolsas antiestáticas todos los dispositivos ópticos, magnéticos y otros dispositivos que contengan circuitos eléctricos, una vez introducidos en las bolsas antiestáticas colocarlos en una caja y rellenarla con algún material protector ya sea plástico con burbujas o algún otro.

10. Toda la documentación en papel colocarla en bolsas protegiéndola así del exterior.

11. Tomar precauciones para proteger las evidencias de factores externos como exceso de calor, exceso de humedad, electricidad estática, etc.

12. Una vez extraídas y protegidas las evidencias deberán ser llevadas a un lugar cerrado y seguro.

13. En caso de que sea necesario enviar las evidencias mediante correo, paquetería o algún otro método de envío habrá que asegurarse que haya forma de darle seguimiento hasta llegar a su destino.

4.5.4 Análisis de Indicios

Mediante el análisis de los indicios como de discos duros, discos extraíbles, discos compactos y otros medios de almacenamiento se pretende encontrar información valiosa como nombres de usuario, contraseñas, archivos y demás que sirvan como indicios para encontrar los orígenes de los ataques y rastros de actividad en Internet, también con la ayuda de herramientas especiales se buscan archivos que fueron borrados por el intruso, pero que en realidad siguen en el medio de almacenamiento pudiendo así ser utilizados como indicio. El análisis debe ser llevado a cabo por profesionales especialistas en

materia del manejo de datos y tecnologías.

Gracias a la aplicación de herramientas de recuperación de datos, la complejidad de estas tareas ha sido reducida en gran medida. Esto se ha logrado gracias a que el software utilizado tiene integrado el conocimiento necesario para realizar las labores de extracción de datos obteniendo así resultados eficientes.

Para iniciar un análisis el investigador debe comenzar por tratar de dar respuesta a las siguientes preguntas:

1. ¿Qué? Esta pregunta se hace con la intención de buscar la causa de lo ocurrido.
2. ¿Quién? Tratando de buscar un individuo responsable que haya realizado las acciones y provocado el evento.
3. ¿Cuándo? Tratar de determinar la secuencia de tiempo en que sucedieron los hechos.
4. ¿Cómo? Investigar las herramientas que se utilizaron para llevar a cabo las acciones realizadas por el individuo.

Para realizar un análisis de los medios de almacenamiento, se requiere tener una comprensión completa y clara acerca de la estructura física y el mecanismo de funcionamiento de los medios de almacenamiento, así como también sobre la forma y estructura lógica en que se almacenan los datos.

Existen diferentes maneras de encontrar indicios en un dispositivo de almacenamiento, la información almacenada deberá ser extraída y analizada para así lograr obtener los indicios, los datos que se pueden encontrar en un medio de almacenamiento se clasifican en 4 categorías:

1. **Datos lógicamente accesibles:** Son los datos mas comunes con los cuales no existe ninguna complicación al momento de su extracción, una vez ya extraídos las complicaciones que se pueden presentar son:

- Que exista un gran volumen de información para analizar
- Que se encuentren datos cifrados
- Encontrar información con virus por lo cual se debe utilizar un buscador de virus antes de que cause problemas hasta poder echar a perder la investigación.

2. **Datos que hayan sido borrados:** Estos se pueden recuperar por medio de software especial.

3. **Datos en "Ambient Data":** En esta categoría entran los siguientes elementos: Espacio no asignado, archivos de *swap*, espacio entre sectores, espacio entre particiones, etc. Su recuperación se realiza con software especializado.

4. **Datos en Estenografía (datos que estén ocultos):** La búsqueda se realiza con técnicas y software para buscar este tipo de datos. **[Ref16]**

Tomando en cuenta esta clasificación de los datos es posible realizar una extracción de los mismos para realizar su análisis y lograr obtener un resultado favorable y en base al mismo elaborar el reporte o presentación.

4.5.5 Presentación y Reporte

Una vez realizadas los pasos anteriores llega el momento de la presentación y reporte que consiste en dar a conocer los resultados obtenidos del análisis realizado, este proceso involucra la especialización o calificaciones por parte de un perito así como la credibilidad de los procesos que fueron empleados para producir el indicio que se está presentando ante la autoridad.

La fase de presentación y reporte se hace con la finalidad de proporcionar toda la información importante encontrada y explicar de una manera lógica, clara y concisa el resultado obtenido de la investigación realizada de una forma

entendible para el público en general evitando usar tecnicismos. Esto implica que los pasos llevados a cabo por parte del analista forense sean reconstruidos con el mayor detalle posible incluyendo fechas, horas, tablas y demás gráficos útiles para un mayor entendimiento, de tal manera que el resultado obtenido sea irrevocable por parte de las autoridades y demás elementos involucrados en un juicio, ya que si uno de ellos es capaz de despertar una duda todo el resultado puede ser rechazado, por lo tanto además de saber realizar un buen reporte es importante contar con elementos que puedan sustentar los resultados de la investigación.

El reporte debe tener una estructura lógica, debe incluir un resumen ejecutivo y las recomendaciones priorizadas, el alcance de la investigación, la información más detallada, seguida por las conclusiones finales y recomendaciones detalladas.

El cuerpo del reporte principal debe ser completo y educar al lector. Explicar, defender todas las recomendaciones y reclamos con las pruebas recogidas durante la investigación. Se necesita dividir los problemas en partes más pequeñas, proveyendo los detalles de los pasos llevados a cabo.

Cuando se dividan los problemas en partes más pequeñas, buscar elementos clave como máquina-nivel de seguridad y arquitectura de la seguridad. Hablar del alcance de la investigación, la importancia de esta investigación para los sistemas investigados, que herramientas y métodos fueron usados, y lo que fue descubierto como resultado.

Las conclusiones finales junto con las recomendaciones detalladas unen el resumen ejecutivo y cuerpo en un mensaje coherente como resultado del proceso de investigación, se debe priorizar y resumir todas las recomendaciones. Evaluar el nivel del sistema total de seguridad. También detallar el estado de los datos de investigación recolectados, donde son almacenados, cómo se guardan de manera segura, cómo pueden ser recuperados, quien debe tener el acceso permitido y cómo adquirir el acceso.

Los apéndices deben incluir los detalles de las herramientas usadas durante la investigación, y cualquier detalle de los sistemas o las redes revisadas que no pudieron quedar en el cuerpo de informe principal. Incluir listas de las correcciones de seguridad y las actualizaciones de OS que son requeridas para los sistemas investigados **[Ref17]**.

CONCLUSIONES

Los sistemas de seguridad existentes implementados para la protección de equipos informáticos son cada vez más complejos, pero a pesar de esto las intrusiones en los sistemas de información se presentan con mayor frecuencia causando grandes daños a las víctimas, esto debido a que las herramientas utilizadas para este tipo de actividades requieren menos conocimientos por parte del usuario, por lo tanto el número de personas que se involucran en estas actividades se va incrementando de forma rápida, así ocasionando un mayor número de problemas que provocan perdidas de información por lo tanto pérdidas monetarias de gran magnitud que se ve reflejada cada año en los estados financieros de las pequeñas, medianas y grandes instituciones.

Por lo tanto es evidente que tanto la Seguridad Informática como la Informática Forense ocupan un lugar importante en ésta era de la información, ya que estas 2 áreas de la informática en conjunto realizan un trabajo de suma importancia para las instituciones.

A pesar de la importancia del área de Informática Forense se puede considerar que es poca la atención que se le ha brindado, ya que no han sido suficientes los conocimientos que se han logrado obtener acerca de esta materia, así como también pocas las personas que tienen conocimiento de esta área, por lo tanto es necesario promover su estudio para la creación de nuevas herramientas capaces de ayudar a realizar las tareas necesarias para llevar a cabo un análisis forense desde su inicio hasta su etapa final, ayudando así al crecimiento de la Informática Forense.

ANEXOS

HERRAMIENTAS UTILES PARA LA INFORMATICA FORENSE

A) Easy Recovery Professional
Fabricante: ONTRACK Data International, Inc.
Origen: España
Uso: Diagnóstico de disco,
Recuperación de Datos
Recuperación de Archivos
Reparación de Correo Electrónico
Compatibilidad con: Windows 98 SE, Windows Me, Windows 2000 y Windows XP.
Costo: Desde $7000.00 pesos (IVA no incluido)
o US$540.00 (IVA no incluido)
Sitio Web: http://www.ontrack.es/

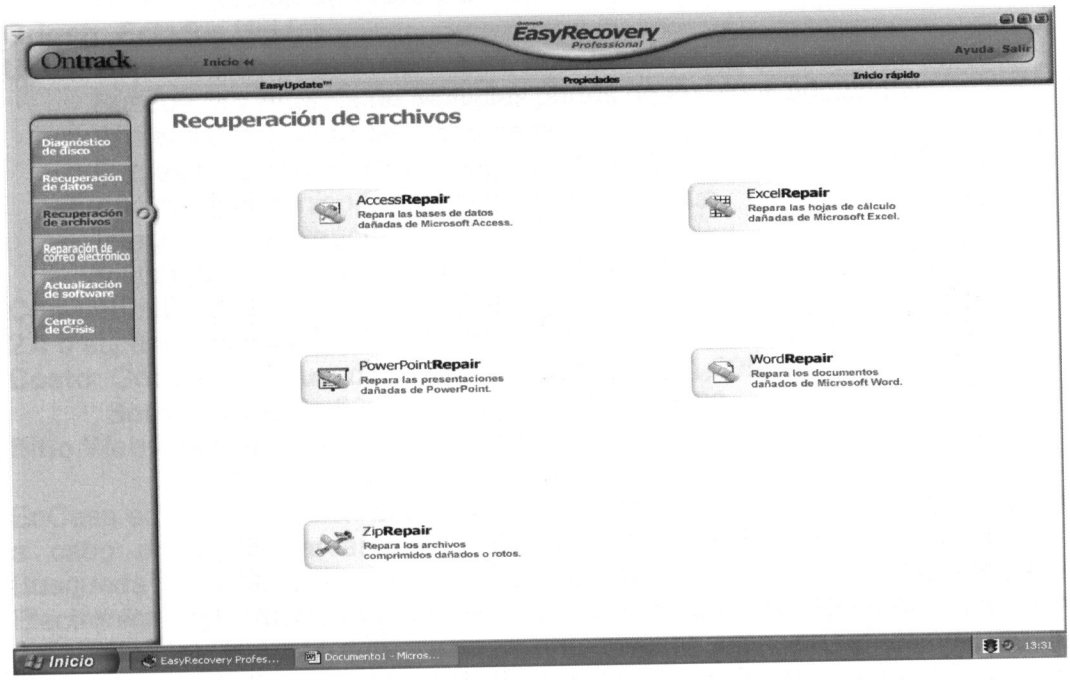
Easy recovery es una aplicación útil para realizar un análisis forense ya que lleva a cabo diferentes tareas como Diagnostico de disco, Recuperación de datos, Recuperación de Archivos que son necesarias al momento de realizar una investigación en el campo de la informática forense, por lo que a continuación se muestra para que tareas sirve y como se llevan a cabo.

MENU DE EASY RECOVERY PROFESSIONAL

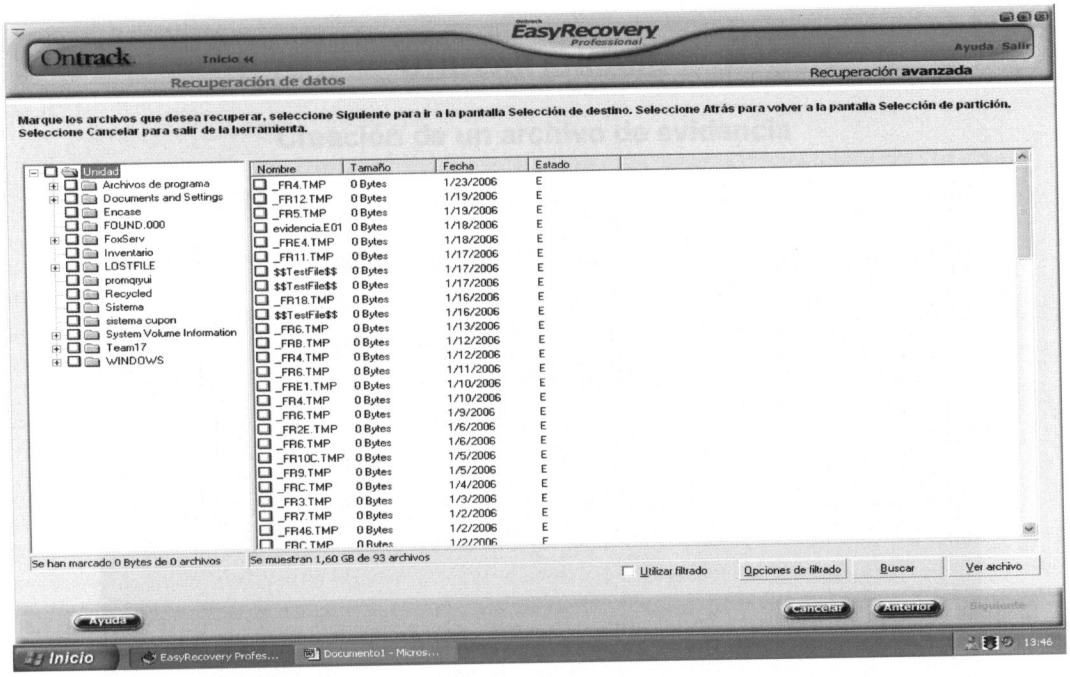
Diagnóstico de Disco

Recuperación de Datos

Recuperación de Archivos



Obtención de Resultados

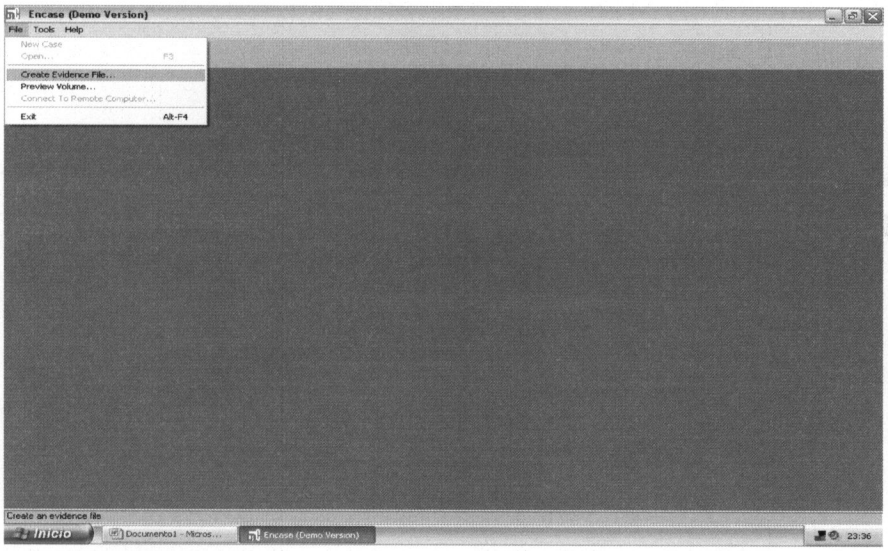


B) EnCase
Fabricante: Guidance Software Inc
Origen: Estados Unidos
Usos: Copiado Comprimido de Discos Fuente
Búsqueda y Análisis de Múltiples partes de archivos adquiridos
Análisis Compuesto del Documento
Firmas de archivos, Identificación y Análisis
Análisis Electrónico Del Rastro De Intervención.
Integración de Reportes
Visualizador Integrado de imágenes con Galería
Compatibilidad con: Windows 95/98/NT/2000/XP/2003 Server, Linux Kernel 2.4 o superior, Solaris 8/9 de 32 & 64 bit, AIX, OSX.
Costo: Gobierno y Educación $25935 pesos o US$1,995.00
Sector Privado o $32435 pesos o US$2,495.00
Sitio Web: http://www.guidancesoftware.com

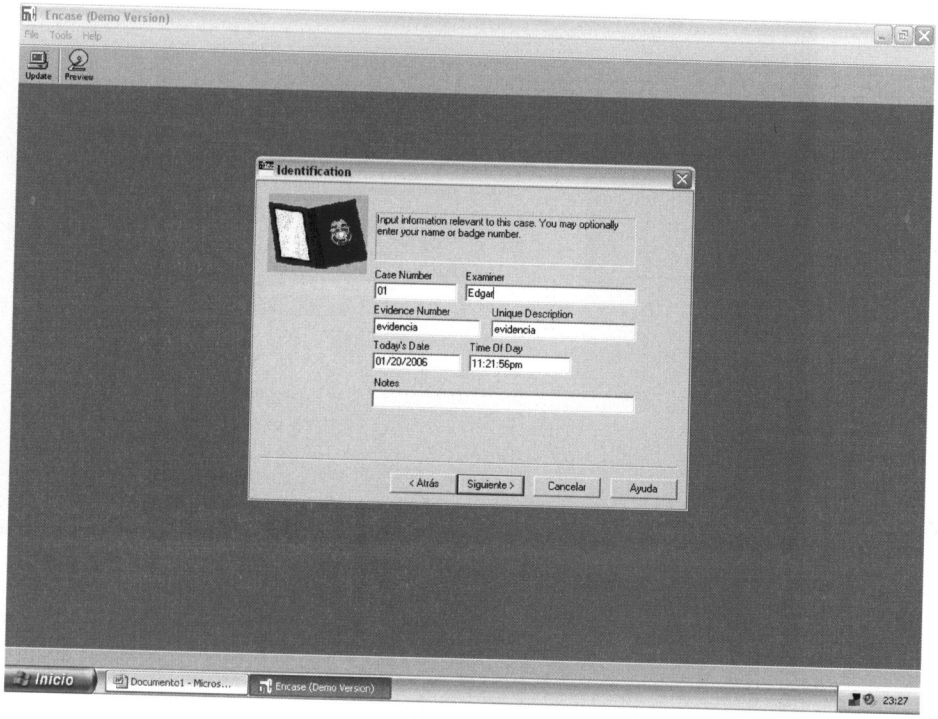
EnCase es una aplicación que ayuda a realizar un análisis forense ya que lleva a cabo diferentes tareas como Copiado Comprimido de Discos Fuente, Búsqueda y Análisis de Múltiples partes de Archivos adquiridos, Análisis Electrónico del Rastro de Intervención, Integración de Reportes que son necesarias al momento de realizar una investigación en el campo de la informática forense, a continuación se muestra como se llevan a cabo las tareas ya mencionadas.

UTILIZAR ENCASE

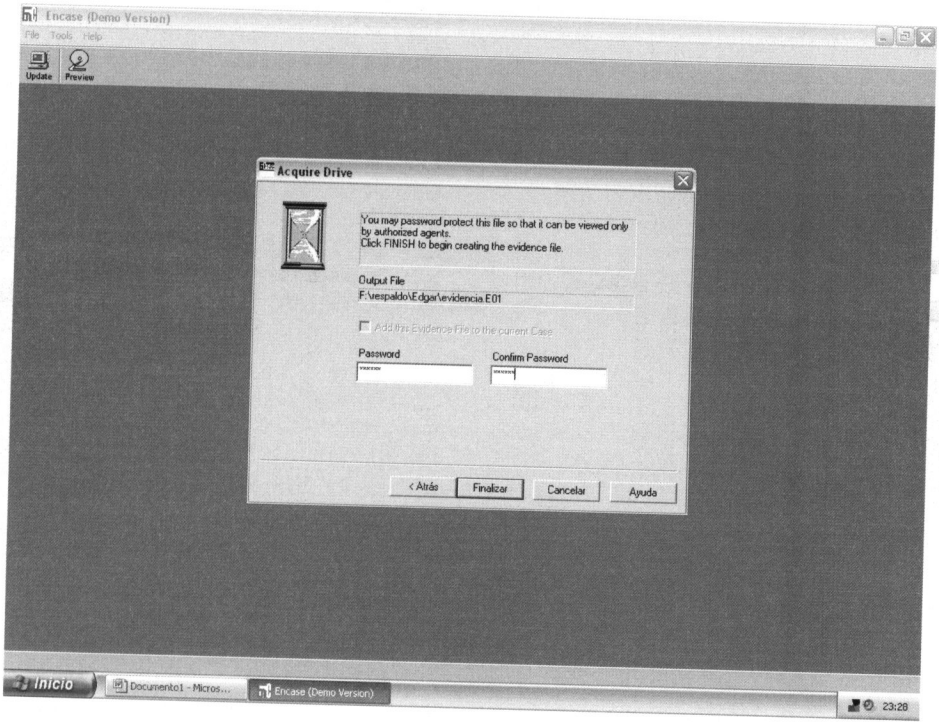
Creación de un archivo de evidencia



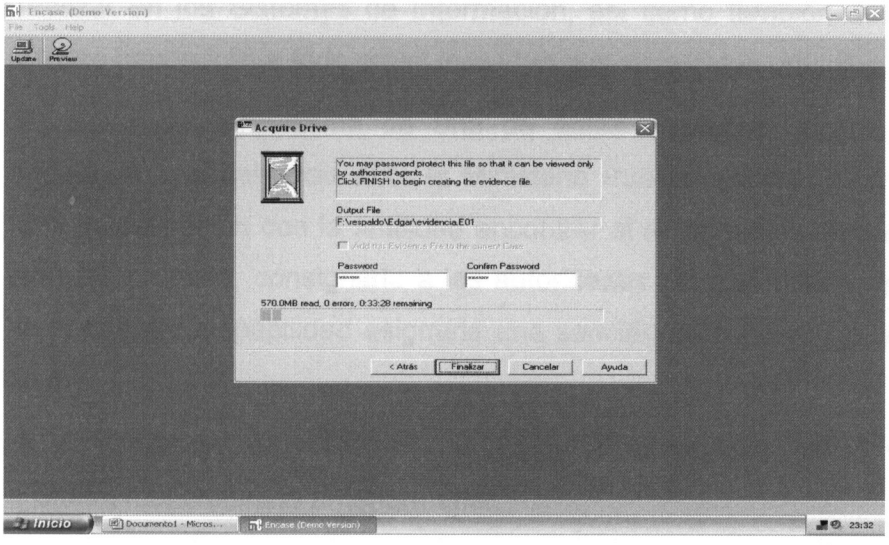
Introducción del nombre y número de caso



Asignación de contraseña al archivo



Comenzar a crear el archivo de evidencia



FUNDAMENTO LEGAL

Hablando de cuestiones legales referentes a los Sistemas de Información se puede mencionar que existen 10 artículos que van del 210 al 211 bis 7 dentro del Código Penal Federal los cuales hablan de las actividades que se prohíben realizar en los Sistemas de Información, así como también de las sanciones que se impondrán a todo aquel individuo que viole estos artículos.

En caso de ser víctima de una de estas conductas ilícitas es necesario presentar una denuncia ante el Ministerio Publico Federal para llevar a cabo una investigación con la finalidad encontrar al responsable de los hechos junto con las pruebas, consignarlo a las autoridades competentes y una vez que se le encuentre culpabilidad asignarle una sanción de a cuerdo a como lo señala la ley.

A continuación se muestran los artículos contenidos en el Código Penal Federal mencionados anteriormente.

CODIGO PENAL FEDERAL

TÍTULO NOVENO. REVELACIÓN DE SECRETOS Y ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

CAPÍTULO I. REVELACIÓN DE SECRETOS

ARTICULO 210.- SE IMPONDRAN DE TREINTA A DOSCIENTAS JORNADAS DE TRABAJO EN FAVOR DE LA COMUNIDAD, AL QUE SIN JUSTA CAUSA, CON PERJUICIO DE ALGUIEN Y SIN CONSENTIMIENTO DEL QUE PUEDA RESULTAR PERJUDICADO, REVELE ALGUN SECRETO O COMUNICACION RESERVADA QUE CONOCE O HA RECIBIDO CON MOTIVO DE SU EMPLEO, CARGO O PUESTO.

ARTICULO 211.- LA SANCION SERA DE UNO A CINCO AÑOS, MULTA DE CINCUENTA A QUINIENTOS PESOS Y SUSPENSION DE PROFESION EN SU CASO, DE DOS MESES A UN AÑO, CUANDO LA REVELACION PUNIBLE SEA HECHA POR PERSONA QUE PRESTA SERVICIOS PROFESIONALES O TECNICOS O POR FUNCIONARIO O EMPLEADO PUBLICO O CUANDO EL SECRETO REVELADO O PUBLICADO SEA DE CARACTER INDUSTRIAL.

ARTICULO 211 BIS.- A QUIEN REVELE, DIVULGUE O UTILICE INDEBIDAMENTE O EN PERJUICIO DE OTRO, INFORMACION O IMAGENES OBTENIDAS EN UNA INTERVENCION DE COMUNICACION PRIVADA, SE LE APLICARAN SANCIONES DE SEIS A DOCE AÑOS DE PRISION Y DE TRESCIENTOS A SEISCIENTOS DIAS MULTA.

TÍTULO NOVENO. REVELACIÓN DE SECRETOS Y ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

CAPÍTULO II. ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

ARTICULO 211 BIS 1.- AL QUE SIN AUTORIZACION MODIFIQUE, DESTRUYA O PROVOQUE PERDIDA DE INFORMACION CONTENIDA EN SISTEMAS O EQUIPOS DE INFORMATICA PROTEGIDOS POR ALGUN MECANISMO DE SEGURIDAD, SE LE IMPONDRAN DE SEIS MESES A DOS AÑOS DE PRISION Y DE CIEN A TRESCIENTOS DIAS MULTA.

AL QUE SIN AUTORIZACION CONOZCA O COPIE INFORMACION CONTENIDA EN SISTEMAS O EQUIPOS DE INFORMATICA PROTEGIDOS POR ALGUN MECANISMO DE SEGURIDAD, SE LE IMPONDRAN DE TRES MESES A UN AÑO DE PRISION Y DE CINCUENTA A CIENTO CINCUENTA DIAS MULTA.

ARTICULO 211 BIS 2.- AL QUE SIN AUTORIZACION MODIFIQUE, DESTRUYA O PROVOQUE PERDIDA DE INFORMACION CONTENIDA EN SISTEMAS O EQUIPOS DE INFORMATICA DEL ESTADO, PROTEGIDOS POR ALGUN MECANISMO DE SEGURIDAD, SE LE IMPONDRAN DE UNO A CUATRO AÑOS DE PRISION Y DE DOSCIENTOS A SEISCIENTOS DIAS MULTA.

AL QUE SIN AUTORIZACION CONOZCA O COPIE INFORMACION CONTENIDA EN SISTEMAS O EQUIPOS DE INFORMATICA DEL ESTADO, PROTEGIDOS POR ALGUN MECANISMO DE SEGURIDAD, SE LE IMPONDRAN DE SEIS MESES A DOS AÑOS DE PRISION Y DE CIEN A TRESCIENTOS DIAS MULTA.

ARTICULO 211 BIS 3.- AL QUE ESTANDO AUTORIZADO PARA ACCEDER A SISTEMAS Y EQUIPOS DE INFORMATICA DEL ESTADO, INDEBIDAMENTE MODIFIQUE, DESTRUYA O PROVOQUE PERDIDA DE INFORMACION QUE CONTENGAN, SE LE IMPONDRAN DE DOS A OCHO AÑOS DE PRISION Y DE TRESCIENTOS A NOVECIENTOS DIAS MULTA.

AL QUE ESTANDO AUTORIZADO PARA ACCEDER A SISTEMAS Y EQUIPOS DE INFORMATICA DEL ESTADO, INDEBIDAMENTE COPIE INFORMACION QUE CONTENGAN, SE LE IMPONDRAN DE UNO A CUATRO AÑOS DE PRISION Y DE CIENTO CINCUENTA A CUATROCIENTOS CINCUENTA DIAS MULTA.

ARTICULO 211 BIS 4.- AL QUE SIN AUTORIZACION MODIFIQUE, DESTRUYA O PROVOQUE PERDIDA DE INFORMACION CONTENIDA EN SISTEMAS O EQUIPOS DE INFORMATICA DE LAS INSTITUCIONES QUE INTEGRAN EL SISTEMA FINANCIERO, PROTEGIDOS POR ALGUN MECANISMO DE SEGURIDAD, SE LE IMPONDRAN DE SEIS MESES A CUATRO AÑOS DE PRISION Y DE CIEN A SEISCIENTOS DIAS MULTA.

AL QUE SIN AUTORIZACION CONOZCA O COPIE INFORMACION CONTENIDA EN SISTEMAS O EQUIPOS DE INFORMATICA DE LAS INSTITUCIONES QUE INTEGRAN EL SISTEMA FINANCIERO, PROTEGIDOS POR ALGUN MECANISMO DE SEGURIDAD, SE LE IMPONDRAN DE TRES MESES A DOS AÑOS DE PRISION Y DE CINCUENTA A TRESCIENTOS DIAS MULTA.

ARTICULO 211 BIS 5.- AL QUE ESTANDO AUTORIZADO PARA ACCEDER A SISTEMAS Y EQUIPOS DE INFORMATICA DE LAS INSTITUCIONES QUE INTEGRAN EL SISTEMA FINANCIERO, INDEBIDAMENTE MODIFIQUE, DESTRUYA O PROVOQUE PERDIDA DE INFORMACION QUE CONTENGAN, SE LE IMPONDRAN DE SEIS MESES A CUATRO AÑOS DE PRISION Y DE CIEN A SEISCIENTOS DIAS MULTA.

AL QUE ESTANDO AUTORIZADO PARA ACCEDER A SISTEMAS Y EQUIPOS DE INFORMATICA DE LAS INSTITUCIONES QUE INTEGRAN EL SISTEMA FINANCIERO, INDEBIDAMENTE COPIE INFORMACION QUE CONTENGAN, SE LE IMPONDRAN DE TRES MESES A DOS AÑOS DE PRISION Y DE CINCUENTA A TRESCIENTOS DIAS MULTA.

LAS PENAS PREVISTAS EN ESTE ARTICULO SE INCREMENTARAN EN UNA MITAD CUANDO LAS CONDUCTAS SEAN COMETIDAS POR FUNCIONARIOS O EMPLEADOS DE LAS INSTITUCIONES QUE INTEGRAN EL SISTEMA FINANCIERO.

ARTICULO 211 BIS 6.- PARA LOS EFECTOS DE LOS ARTICULOS 211 BIS 4 Y 211 BIS 5 ANTERIORES, SE ENTIENDE POR INSTITUCIONES QUE INTEGRAN EL SISTEMA FINANCIERO, LAS SEÑALADAS EN EL ARTICULO 400 BIS DE ESTE CODIGO.

ARTICULO 211 BIS 7.- LAS PENAS PREVISTAS EN ESTE CAPITULO SE AUMENTARAN HASTA EN UNA MITAD CUANDO LA INFORMACION OBTENIDA SE UTILICE EN PROVECHO PROPIO O AJENO.

REFERENCIAS

[Ref1] Seguridad de los Sistemas Operativos
Profesor David Luis la Red Martínez
http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/SO14
.htm (Agosto 2005).

[Ref2]Políticas de Seguridad 2003 contra Virus, Gusanos, Troyanos/Backdoors
Jorge Machado, 2003
http://www.perantivirus.com/sosvirus/pregunta/segu2003.htm
(Agosto 2005).

[Ref3] La gestión del riesgo
Sergio Hernando, 2005
URL: *http://laflecha.net/canales/seguridad/200506083/* (Agosto 2005).

[Ref4] Copia de Seguridad
Wikipedia®, 2006
URL: *http://es.wikipedia.org/wiki/Copia_de_seguridad* (Abril 2006).

[Ref5] Cómo configurar un muro cortafuegos con Shorewall y tres interfaces de red
Joel Barrios Dueñas, 2006
URL:*http://www.linuxparatodos.net/geeklog/staticpages/index.php?page=como-shorewall-3-interfaces-red* (Abril 2006).

[Ref6] Sistema de detección de intrusos
Wikipedia®, 2006
URL:*http://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_*intrusos
(Septiembre 2005).

[Ref7] Protección para todas las estaciones de trabajo y para los usuarios remotos, móviles e interconectados
Stephen G. Cullen Vicepresidente, Productos y Soluciones de Seguridad
Symantec Corporation (Mayo 2005)
URL:http*://206.204.52.54/region/mx/enterprisesecurity/content/expert/LAM_3594.html#2* (Septiembre 2005).

[Ref8] Seguridad en Unix y en Redes
Antonio Villalón Huerta (Julio, 2002)
http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html/unixsec.html (Septiembre 2005).

[Ref9] The Largest Community of Security Professionals Available Anywhere
Robert Lemos, 2005
URL: *http://www.securityfocus.com* (Septiembre 2005).

[Ref10] Red Hat Enterprise Linux 4 Manual de seguridad
Red Hat, Inc. 2005
URL: *http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4* (Octubre 2005)

[Ref11] The Honeynet Project
Honeynet Team,2005
URL: *http://www.honeynet.org* (Octubre 2005)

[Ref12] Análisis Forense
Ausejo.net,2005
URL:*http://www.ausejo.net/seguridad/forense.htm* (Septiembre 2005)

[Ref13]Informática Forense : Generalidades, Aspectos Técnicos y Herramientas
Óscar López, Haver Amaya, Ricardo León; Beatriz Acosta, Febrero 2002
URL:http://www.criptored.upm.es/guiateoria/gt_m180b.htm (Agosto 2005)

[Ref14] Informático Forense, una profesión con futuro
VIRUSPROT.COM, 2002
URL:*http://www.virusprot.com/Col12.html* (Septiembre, 2005)

[Ref15] El mundo de la Informática Forense
Xombra Team www.xombra.com, 2005
URL: *http://www.xombra.com/go_news.php?articulo=1942* (Septiembre 2005)

[Ref16]Herramientas para Análisis Forense
Cynthia Patricia Castelan Vázquez
Instituto Tecnológico de Morelia, 2005

[Ref17] How to Conduct a Security audit.
Justin Kapp, 2000
URL: *http://www.itp-journals.com* (Febrero 2006)