UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO

INSTITUTO DE CIENCIAS BÁSICAS E INGENIERÍA

LICENCIATURA EN SISTEMAS COMPUTACIONALES

"METODOLOGÍA PARA LA FORENSIA INFORMÁTICA"

M O N O G R A F I A

QUE PARA OBTENER EL TITULO
DE LICENCIADO EN SISTEMAS COMPUTACIONALES

P R E S E N T A
EDGAR CALDERÓN TOLEDO

ASESOR
M.C.C. LUIS ISLAS HERNÁNDEZ

Pachuca Hgo. 2008

AGRADECIMIENTOS

Mis Padres

Por que gracias a ellos soy quien soy…

A mis Hermanos

Porque siempre han creído en mí.

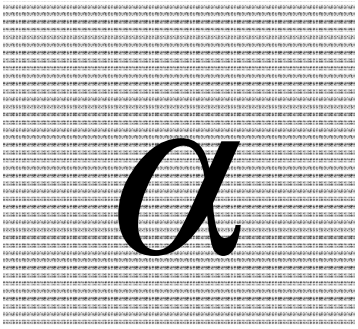
A mis amigos…

Por brindarme su apoyo en cada momento

A Nancy Márquez Lázaro

Gracias por estar en mi vida…

INDICE



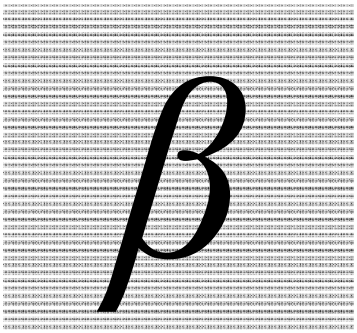
OBJETIVOS

OBJETIVO GENERAL

Presentar la metodología y las herramientas necesarias que sirvan de apoyo para quienes han decidido dedicarse al área de protección de sistemas informáticos o seguridad informática requiriendo la correcta recolección y presentación de evidencias para la toma de decisiones y medidas de respuesta ante incidentes que pueden implicar incluso persecuciones criminales; Además de presentar de una manera mas detallada la nueva área de “Forensia informática”.

OBJETIVOS ESPECÍFICOS

- Presentar los antecedentes de los delitos informáticos.
- Presentar el estatus de las leyes referentes a la informática en México.
- Dar a conocer qué es un delito informático.
- Presentar las herramientas de prevención de incidentes
- Presentar las herramientas de verificación de integridad de archivos y sistemas.
- Determinar qué puede ser considerado como evidencia.
- Explicar en qué consiste la cadena de custodia.
- Presentar una metodología para la recolección de las evidencias.
- Presentar el concepto de Honeypot y Honeynet.
- Se realizará el análisis de un incidente recabando las evidencias apegado a la metodología presentada en este mismo trabajo.



JUSTIFICACIÓN

En la actualidad los medios digitales se han constituido como la manera de almacenar la información, lejos quedaron los días donde los documentos oficiales estaban firmados con tinta y papel, en estos días, las firmas electrónicas no sólo son validas sino obligatorias en muchas transacciones.

De la misma forma las telecomunicaciones o la transmisión de datos de un lado a otro toma cuestión de segundos cuando en otros tiempos podría tardar días, esto ha dado paso a un nuevo campo o rama de la investigación criminal, que consiste en recuperar la información de manera confiable para sustentar un caso legal.

Pero no solo compete a los investigadores legales la recuperación de evidencias, sino también a los encargados de la seguridad en cualquier organización, debe ser de interés saber que fue lo que paso y cómo pasó un incidente determinado.

La investigación forense en los medios digitales crece día a día, al existir cada ves nuevos dispositivos capaces de transportar información de un lugar a otro, desde teléfonos celulares, memorias portátiles, equipos de sonido o cámaras fotográficas que pueden almacenar no solo fotografías sino datos importantes.

También crece la problemática del investigador al desarrollarse mecanismos de encriptación cada vez más complejos, estos mecanismos son usados por los atacantes o por los criminales como ya se ha presentado en muchos casos en los estados unidos.

Sin embargo quizás el mayor problema que enfrenta un investigador de este tipo es el abismo legal que existe en muchos países, en los cuales no es posible llevar acabo una

persecución criminal de tipo informático, como es el caso de México donde aun quedan muchos asuntos que resolver.

También se debe de mencionar que en la actualidad la investigación forense realiza ingeniería inversa y desempaquetado de archivos ejecutables encontrados en los equipos vulnerados, estos pueden ser rootkits o virus polimorficos, también se han presentado casos en los que se crean túneles de datos ya sea VPN's o túneles Ipv6, que constituyen mayor complejidad debido a que existen pocos analizadores capaces de descifrar de manera correcta este tipo de tráfico.

La complejidad que supone el desensamblado o ingeniería inversa de archivos queda fuera de los límites de este trabajo, ya incluye mecanismos de programación en lenguaje ensamblador y de no haberse acotado el trabajo, este seria demasiado extenso, por lo que puede quedar para trabajos futuros en el área.

El presente trabajo pretende ser un iniciador en aquellos que tengan el interés de dedicarse a la investigación criminal informática o que busquen un apoyo completo acerca de cómo realizar su trabajo dentro de su organización.

INTRODUCCION

Este trabajo presenta las bases para poder llevar acabo una investigación no solo competente a los investigadores legales si no a todo jefe de seguridad, y trata de ser el iniciador de la exigencia de seguridad en las organizaciones de pequeño y mediano nivel.

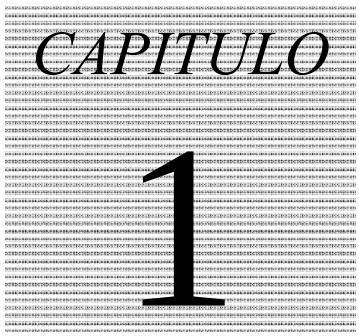
En el primer capítulo se presentan los antecedentes y conocimientos que cualquiera que pretenda iniciarse en este tipo de ambiente debe saber, iniciando por las políticas de seguridad y los planes de recuperación de desastres, además de hacer notar los diferentes tipos de incidentes informáticos y por supuesto aclarar ¿qué es la forensia informática? y ¿cuales son los alcances de un investigador?

En el segundo capítulo se presenta el estatus de las leyes en el aspecto informático, mostrando cuales son las penas por infiltrarse o por alterar información que se encuentre protegida con algún mecanismo de seguridad y por ultimo se presentan algunas de las propuestas de reformas al código penal federal en las leyes informáticas.

Es muy importante prestar atención a este capitulo ya que como experto o futuros expertos en seguridad de sistemas debemos conocer los límites de acción y cuáles son las implicaciones que puede tener el simple hecho de experimentar con una red sin previa autorización de el administrador de la red.

En el tercer capítulo se presentan las herramientas de Forensia informática que aunque no son todas las herramientas que existen para la investigación de incidentes informáticos, si presentan un panorama de este tipo de herramientas, hay que destacar que el uso de estas supone el conocimiento de conceptos básicos de informática como la distribución de los datos en un disco y como funciona la memoria RAM. También es preciso aclarar que la investigación siempre debe de realizarse de manera “solo lectura”, por lo que muchas de las herramientas no permiten hacer modificaciones sobre la información que se esta analizando.

En el capítulo cuatro se presenta una metodología para la investigación forense siguiendo los principios de la cadena de custodia y finalmente en el capitulo cinco se aplica esta metodología en la presentación de un caso práctico creado, refiriéndose a que se simula la penetración de un sistema virtual, también se presentan los nuevos alcances de los equipos virtuales así como su aplicación en la investigación forense.



INTRODUCCIÓN A LA FORENSIA INFORMÁTICA

1.1 ANTECEDENTES

Entre los años 1971 y 1981 con la aparición de los circuitos integrados comenzó la revolución de las computadoras, ya que permitió hacer más accesibles, no solo a las empresas si no a otras personas y centros de investigación el tener acceso a estas tecnologías, lo que por ende propició un gran desarrollo en esta área.

Con el desarrollo que surgió, los algoritmos y programas se fueron haciendo mas complejos y en ocasiones las computadoras no hacían las cosas para las que fueron programadas, así que surgió una nueva necesidad, la de contar con mecanismos de depuración de código para el rastreo de fallas o errores en el mismo.

Así que se comenzaron a usar programas y herramientas que inicialmente fueron pensados para optimizar la relación costo-velocidad en los equipos de cómputo, pero debido a la misma complejidad del software, en ocasiones los programas no funcionaban como se suponía que debían funcionar, así que se crearon programas para identificar cual era el problema que había provocado el error.

Esto fue llevando poco a poco al desarrollo de software tolerante a fallas, más robusto y por ende más complejo. De esta manera fueron surgiendo nuevas herramientas que permitían poner a prueba el software bajo todo tipo de condiciones iniciando así un nuevo concepto conocido como ***pruebas de penetración***[1].

Las pruebas de penetración en el software consistían en poner aprueba el código de los programas para encontrar errores que pudieran provocar inestabilidad en el sistema o que pudieran permitir a algún tipo de intrusión al sistema, ya sea por parte de código malicioso o de un atacante en específico.

Pero con la expansión del Internet y la oportunidad de intercambio y acceso a la información que esto permitió, comenzaron a aparecer nuevos problemas para los ahora encargados de mantener la seguridad de los sistemas de amenazas como lo fueron los virus que se distribuían a través de las redes.

Los incidentes no se pueden evitar, así que el problema entonces siguió siendo el mismo, saber que es lo que había pasado, es decir el encontrar el ¿Cómo? y ¿Cuándo? de un ***incidente informático***.

Fue así como surgieron centros de desarrollo e investigación dedicados al análisis de este tipo de incidentes, comenzando solo por desensamblar el código de algunos virus con la finalidad de entender su funcionamiento y posteriormente continuando por el análisis completo de incidentes que implicaban pérdidas de datos y requerían el rastreo de las causas del incidente; Es aquí cuando surge la ***Forensia Informática.***

[1] **Pruebas de penetración,** consiste en probar si el sistema es vulnerable sometiéndolo a pruebas de ataques conocidos y posibles condiciones de ataques nuevos.

Con la consolidación del uso de las computadoras personales además de la introducción y uso masivo de equipos como computadoras portátiles, ***PDA***'s[2], equipos celulares, etc. El área en la que un forense informático puede encontrar evidencia o pruebas de algún tipo de crimen, se extendió a todos estos equipos.

Sumado a esto en la década de los noventas, el número de usuarios de Internet se incrementó de manera exponencial, al mismo tiempo se incremento el uso del correo electrónico, cuartos de Chat y foros de discusión. Lo que implica que la recolección de información se extiende y se complica más para el Forense informático.

LA FORENSIA INFORMÁTICA

La informática forense como rama relativamente nueva, tiene ciertas diferencias en cuanto a su definición, una de estas es la presentada por Juan Carlos Guel, jefe del departamento de seguridad en cómputo de la UNAM y del UNAM-CERT:

> *"informática o cómputo forense es un conjunto de técnicas especializadas que tiene como finalidad la reconstrucción de hechos pasados basados en los datos recolectados, para lo cual se procesa la información que pueda ser usada como evidencia".*

El forense informático se encarga de recolectar las evidencias en el caso de un incidente, también es su responsabilidad el preservarla de manera intacta, y en base a lo recolectado en la escena del crimen, determinar ¿qué fue lo que pasó? Y ¿Cómo pasó?.

El investigador debe contar con conocimientos en casi todas las áreas de las tecnologías de comunicación e información, ya qué no solo se requieren conocimientos sobre sistemas operativos o redes de comunicación, si no conocimientos en bases de datos, programación e ingeniería inversa, se requieren también conocimientos en protocolos de comunicación y diversas arquitecturas de computadoras.

El ámbito de esta área, se limita en la mayoría de los casos sólo a recopilar información y presentarla a las autoridades, es decir no corresponde al forense informático la persecución de los responsables, solo en los casos en los que se este acreditado como forense informático, en nuestro país, no existe esta acreditación sino solo la acreditación de "perito en informática", lo que limita las acciones que el investigador puede hacer.

1.2 VALOR DE LA INFORMACIÓN

Como consecuencia de los incidentes informáticos, los cuales pueden ser desde ataques deliberados por espionaje o sabotaje, hasta por el mal uso de un usuario de la empresa, la información o los sistemas informáticos de la empresa pueden quedar fuera de línea por un determinado periodo de tiempo.

[2] **PDA,** Asistente personal de datos por sus siglas en ingles, es una computadora personal de bolsillo

Esto implica un problema en el seguimiento del caso y la recolección de las evidencias ya que para la empresa es importante saber que fue lo que ocurrió para poder deslindar responsabilidades, pero también es muy importante el que los sistemas y la información estén disponibles lo mas pronto posible.

Aquí podemos hacer una división de los expertos forenses, los que trabajan para la ley o para el estado y los que trabajan para la empresa.

Los Expertos Forenses que trabajan para la ley y/o para el estado, son los encargados de recolectar y poner bajo custodia la información que pueda estar implicada en el delito, siendo esta la que será usada para el aspecto legal. Estos expertos deben de mantener la información sin ningún tipo de modificación, para que pueda aportar evidencia sustentable en el juicio.

Por el otro lado tenemos a los expertos forenses o expertos en seguridad que trabajan para la empresa, además de ayudar en la recolección de la evidencia en conjunto con los expertos del estado, su misión es además de determinar cuales son los daños potenciales causados, poner el sistema o la información en un estado *"Disponible",* lo mas pronto posible y de manera confiable.

Con esto nos referimos a que el sistema y/o la información solo deberán regresar a un estado disponible, en el momento en el que se haya comprobado que no existen modificaciones a esta y que los posibles errores de seguridad han sido corregidos.

En algunos delitos informáticos, lo importante no es solo el encontrar al responsable del incidente y demostrar su culpabilidad, sino recuperar la información que pudo haberse perdido por la intervención del agresor.

Este trabajo es responsabilidad del personal de la misma empresa o en casos de ***Outsorcing***[3] de empresas especializadas en estos casos.

Como antecedentes podemos mencionar que al igual que se crearon herramientas para buscar las causas de fallos en los programas, también se desarrollaron mecanismos para recuperar datos de equipos dañados parcialmente.

El forense informático hace uso de estos dos tipos de herramientas para realizar la recuperación de información. Con la reserva de que el forense informático busca información que le pueda ser útil para formar y llevar un caso, y descarta a su vez la información que no es relevante para este fin; Pero en la actualidad, la información es uno de los bienes mas importantes para las empresas, por lo que la información debe de ser recuperada, sea esta de utilidad para el caso o no.

Los expertos en Tecnologías de información y comunicación, deben de estar al tanto de los mecanismos usados para la recuperación de datos, así como contar con ***políticas de destrucción de información de tipo digital***. La cuál podría comprometer en determinado momento la seguridad de la empresa.

[3] **Outsourcing, C**uando una compañía delega cierta actividad a otra mediante un contrato de servicio.

1.3 POLÍTICAS DE DESTRUCCIÓN DE INFORMACIÓN

Este punto es en muchas ocasiones olvidado por las empresas y es de vital importancia cuando se trata de la información, el contar con una política de destrucción de información que ayuda no solo a evitar espionaje o sabotaje, sino que también obliga a contar con respaldos fiables de la información.

Un ejemplo sería el hecho de que los archivos de un empleado no se destruirán o borrarán hasta que se encuentren respaldados en una cinta de seguridad, ya que esto permitirá deslindar responsabilidades en casos de investigación.

Debe estar claro que en la política de destrucción y de respaldo de información se debe de establecer ¿qué información deberá ser respaldad? y ¿cuál deberá ser destruida?.

Con la destrucción de la información nos referimos a la limpieza del área en la que los datos se almacenan y en ciertos casos de la destrucción de los medios responsables de contenerla, un método de destrucción usado comúnmente, consiste en que el espacio ocupado por un archivo es sobre escrito con "0" y luego es borrado de la tabla de archivos **MFT**[4] así como de la **FAT**[5].

Procedimientos más estrictos como los gubernamentales establecen que el archivo deberá ser sobre escrito en tres ocasiones, la primera poniendo todos los bytes del archivo a "AA", en la segunda pasada se establecen a "00" y en la tercera pasada se establecen en "FF", además de que se usa el mismo procedimiento en el **MFT** y la **FAT.**

La destrucción de información en medios de almacenamiento extraíble es generalmente la puesta en "0" de todos los bytes del archivo o del disco en su caso, pero en los medios de solo lectura es preferible su destrucción física.

Como ejemplo tenemos que el departamento de defensa de los Estados Unidos destruye su información llevando acabo el procedimiento de borrado en tres pasadas y posteriormente los discos duros son destruidos completamente.

1.4 TIPOS DE INCIDENTES INFORMÁTICOS

De acuerdo con el **FedCIRC**[6], los tipos de incidentes, se dividen en [1]:

- Ataques de código malicioso:

  Este tipo de ataques incluye ataques por virus, caballos de Troya, gusanos, scripts, usados por algún atacante para robar información, passwords, modificar log's o realizar

[4] **MFT,** Master file table, es usado por el sistema operativo para ubicar de manera mas rápida los archivos en las diferentes particiones y áreas del disco.
[5] **FAT,** File Allocation Table, aquí se almacena la dirección exadecimal del área en la que un archivo se encuentra almacenado en el disco duro, generalmente se cuenta con dos tablas por disco duro para poder comprobar la coherencia de la ubicación y como respaldo.
[6] **FedCIRC** The Federal Computer Incident Reporting Center

alguna actividad no autorizada. Los ataques de código malicioso son los más comunes y se pueden convertir en un gran problema debido a que pueden auto replicarse en sistemas conectados a la red.

- Accesos no autorizados:

Este tipo de incidentes engloba muchos otros en si, como cuando un atacante entra al sistema con una cuenta valida robada para acceder a sistemas y/o archivos, o cuando un atacante accede a los archivos al obtener el rango de súper usuario de manera no autorizada, por ejemplo al explotar alguna vulnerabilidad del sistema.

- Utilización no autorizada de servicios:

En este caso no es necesario acceder de manera no autorizada a un sistema para perpetrar el ataque, probablemente el atacante obtuvo información por medio de un programa de tipo caballo de Troya, usando servicios mal configurados, de esta manera puede obtener acceso a ciertos sistemas o archivos a los cuales no esta autorizado.

- Perturbación de servicios:

Los usuarios tienen acceso a muchos servicios proveídos por un ***ISP***, estos pueden ser perturbados de diferentes maneras, como lo el envío de correo electrónico basura también conocido como *Spam*, borrando programas críticos, la saturación de cuentas de correo electrónico de otros usuarios o alterando el funcionamiento de los sistemas con la instalación de programas tales como caballos de Troya.

- **Mal uso**[7]:

El mal uso de los sistemas ocurre cuando un usuario ocupa los recursos computacionales para otro fin diferente al que está destinado.

- Espionaje:

Se refiere a todo tipo de intercepción de información, así como el robo de la misma. Esta es una de las prácticas más comunes en los gobiernos y empresas de investigación.

- Hoaxes:

Este tipo de incidentes ocurre cuando se distribuye información falsa acerca de vulnerabilidades, virus o incidentes. Provocando temor y falsa alarma entre los usuarios. Aunque no causa pérdida de datos o información, si provoca pérdida en la productividad de las empresas y organizaciones.

1.5 DESCRIPCIÓN DE LOS TIPOS INCIDENTES INFORMÁTICOS

Los incidentes o ataques se pueden dividir en descripciones más completas, esto con la finalidad de hacer más fácil el entendimiento y por ende el seguimiento de todos los tipos de incidentes.

[7] **Mal uso,** Traducción literal del termino **Miss use** usado en seguridad informática.

1.5.1 Intrusión Y Ataques

Para que el trabajo de un forense o investigador informático sea llevado de manera correcta, este tiene que tener claro la diferencia entre un ataque y una intrusión, ya que el entendimiento de estos hará que la búsqueda de la evidencia así como la presentación de ella sea la correcta.

Una intrusión difiere en muchos aspectos de un ataque, ya que el ataque puede ser perpetrado sin necesidad de que exista intrusión en algún tipo de sistema o computadora, es el caso de un ataque de negación de servicio, en el cual se satura la red o el acceso a un recurso de manera que los usuarios que normalmente hacen uso de este, no puedan hacerlo, podemos poner como ejemplo los ataques contra paginas Web como la de **Amazon.com** que generan grandes perdidas

En este tipo de incidentes, no se realiza una intrusión a un sistema, sino solo es un ataque, es importante entender esto para que al momento de llevar la investigación no existan huecos que permitan algún tipo de evasión de la justicia.

De lo anterior derivamos dos tipos de ataque que se deben entender, los ataques distribuidos y los ataques directos contra los sistemas o las redes.

Los ataques directos se efectúan cuando una computadora es usada para dirigir un ataque, como inundar una red con peticiones de un cierto tipo hacia un objetivo en particular. Este tipo de ataques en los que una sola computadora realizaba un ataque de negación de servicio, ya no es funcional, salvo en ciertos casos; Esto es debido a que el poder de procesamiento con el que actualmente cuentan las computadoras, les permite atender suficientes peticiones como para soportar las realizadas por un solo equipo, más aun cuando los equipos o redes objetivo son de características especiales, como servidores y redes de banda ancha.

En los ataques distribuidos, un usuario mal intencionado o un grupo de ellos, toman control de un gran número de equipos para dirigir un ataque; en la actualidad este tipo de agresiones a sistemas es el mas común, debido a la efectividad de estos.

Este método funciona de la siguiente manera, supongamos que cientos de máquinas realizan una petición de conexión a un sitio en especial, pero en lugar de completar el saludo de tres vías o ***hand shaking***[8]**,** realizan una nueva petición hacia este mismo sitio, lo que hace que el servidor se quede por un periodo de tiempo esperando la confirmación de la conexión anterior.

Ahora, si multiplicamos esto, es cuestión de tiempo para que el servidor deje de responder las peticiones reales por atender las de estos equipos. Lo mismo ocurre en una red, en la que se envían cientos de paquetes de gran tamaño, de tal manera que los recursos de esta se vuelven inaccesibles para los demás usuarios.

[8] **Hand Shaking,** conocido como el saludo de tres vías en el que se envía una petición de conexión al servidor, este envía una respuesta de aceptación para finalmente enviar la confirmación de la sesión

A todo lo anterior podemos agregar la modalidad de los ataques automatizados, lo que se refiere a que los ataques no son dirigidos en tiempo real por el atacante, sino que son preprogramados para realizarse de manera automática. El ejemplo mas común de estos lo podemos encontrar en los realizados por algunos virus, los cuales luego de infectar un sistema y en base a un disparador programado para una fecha, realizan una agresión distribuida contra algún objetivo en particular.

Los ataques automatizados suelen ser una completa pesadilla tanto para los investigadores, como para las empresas y corporaciones. Ya que por lo general no se dan cuenta del ataque hasta que este se realiza, además de que el rastrear dónde comenzó el ataque o la infección, suele ser mucho más complicado.

1.5.2 Ataques "ACCIDENTALES"

Aunque puede resultar confuso, los ataques accidentales suelen ser mas comunes de lo que parecen, aunque no pueden ser considerados como ataques realmente, pero la ley dicta que el desconocimiento de las leyes no excluye la culpa, por lo que aun tratándose de un incidente se debe de ejecutar la acción penal; muchas compañías toman esto muy enserio, sobre todo al tratarse de empresas muy grandes que pueden perder mucho dinero y reputación por incidentes de este tipo.

Es decir, aunque el incidente o el ataque no haya sido provocado intencionalmente por un usuario, sí es responsabilidad de este lo que haya pasado, es por esto que las compañías de este tipo ponen un gran énfasis en la capacitación de los empleados haciéndolos conscientes de la importancia de la seguridad, para esto hacen uso de las políticas de seguridad mencionadas anteriormente.

1.6 PREPARACIÓN PARA UN INCIDENTE

1.6.1 Políticas de seguridad

Las políticas de seguridad son la primera línea de defensa y respuesta para los incidentes, de hecho, es aquí en donde se encuentran las bases de los sistemas seguros.

Estas deben de ser estudiadas por los expertos en TI, los gerentes de áreas y los encargados de seguridad o los forenses informáticos de la empresa, así también como los responsables de las áreas claves de la organización, estas políticas se deben ajustar a cada empresa, de acuerdo a sus necesidades y área de trabajo.

Para el establecimiento de las políticas de seguridad existe en la actualidad la norma ISO 17799, la cual establece diez puntos en los cuales toda organización podrá basarse para considerar que su política de seguridad es lo suficiente mente confiable para ser implantada.
Los diez puntos que contiene la norma ISO 17799 o conocida también como la norma Británica BS 7799 son:

Planeación de la continuidad del negocio.

Se trata de minimizar el impacto de fallas mayores en los procesos de negocio, de tal manera, que no se vean afectados los procesos críticos de esta.

Con esto nos referimos a que en la implantación de los sistemas de una organización, se deben de contemplar los escenarios más pesimistas en caso de un incidente, a partir de esto se debe analizar ¿cuales serian las áreas afectadas en caso de que esto ocurriera?, ¿cuanto tiempo pueden permanecer sin la información o sin el sistema?, con base en esto se determina cuales son las áreas que no pueden tolerar la falta del sistema o de la información y establecer a la ves mecanismos que le permitan al área continuar operando.

Tenemos por ejemplo, que se podría contar con sistemas de bases de datos en espejo, ubicados en diferentes lugares geográficos, de tal manera que en caso que uno falle, el otro podrá seguir suministrando la información necesaria para seguir operando sin interrumpir las operaciones.

Este tipo de mecanismos son usados principalmente en los bancos, ya que sus grandes bases de datos se encuentran replicadas en diferentes lugares, cada uno con capacidades autónomas de mantenerse funcionando. Ejemplo el ***Prodigy Data Center***, Ubicado en un lugar con sismología casi nula, tres Fuentes de alimentación externa de tres subestaciones de energía distintas y con capacidad para operar sin recursos externos hasta por 7 días de manera ininterrumpida.

Control de acceso al sistema

Los objetivos de este apartado son:

- Controlar el acceso a la información.
- Prevenir el acceso no autorizado a los sistemas de información.
- Asegurar la protección de los servicios de red.
- Prevenir el acceso no autorizado a las computadoras.
- Detectar actividades no autorizadas.
- Aumentar los niveles de seguridad de la información cuando se usan dispositivos móviles y ***tele-trabajo***[9]**.**

En toda organización el acceso debe de estar restringido de acuerdo a niveles, estos niveles de seguridad deben de estar divididos en críticos y no tan críticos, por consiguiente, el acceso a las áreas críticas o donde se maneja información, debe de estar restringido solo al personal autorizado.

Pero esto no solo se aplica a las instalaciones físicas si no al acceso a recursos, sesiones de Terminal remota, redes inalámbricas, redes físicas, a los equipos y servicios que se encuentran en la red.

[9] **Tele-trabajo,** trabajo a distancia, muchas empresas emplean este método para aumentar la productividad sin tener al personal en un solo lugar.

Una manera de hacer esto es en las redes Windows establecer Árboles de dominios y sus respectivas políticas de acceso a recursos, como puede ser que solo sea valido que una secretaria inicie sesión en su equipo y no en ningún otro, o establecer contraseñas de acceso en la capa dos del modelo OSI para las redes inalámbricas.

Aunado a esto se deben de prever mecanismos para detectar si se están realizando actividades no autorizadas, ejemplo, un directivo de un área que accede bases de datos de empleados de otras áreas sin autorización. Esto se deberá hacer con un monitoreo constante o con sistemas mas avanzados como son los IDS.

Desarrollo de sistemas y mantenimiento

Los objetivos de esta sección son:

- Asegurar que los sistemas son diseñados con base a los lineamientos de seguridad establecidos.
- Prevenir la pérdida, modificación o mal uso de la información de los sistemas.
- Proteger la confidencialidad, autenticidad y la integridad de la información.
- Certificar que los proyectos de TI's son conducidos de manera segura.
- Mantener la seguridad de las aplicaciones de los sistemas, el software y los datos.

En el caso de las empresas que desarrollan sus propios sistemas o que desarrollan sistemas para otras empresas, se debe de tener un área o una etapa en la que todo el software que se esta desarrollando se pone a prueba en el aspecto de seguridad, intentando desbordar variables, probando passwords default o errores en el código que puedan abrir un hueco de seguridad en el sistema.

Además de estas pruebas se deben de agregar mecanismos que protejan la información mediante la validación de variables así como con la incorporación de mecanismos de cifrado lo suficientemente robustos para el tipo de información que se va a manejar.

En el caso de empresas desarrolladoras de software, se recomienda que el software sea probado por alguna empresa de seguridad externa, para certificar que la seguridad es la adecuada.

Seguridad física y ambiental

Los objetivos de esta sección son:

- Prevenir el acceso no autorizado, daño e interferencia a las premisas de información de negocio.
- Prevenir pérdida, daño o comprometimiento de los activos y/o interrupción a las actividades de negocio.
- Prevenir el comprometimiento o robo de información en las instalaciones.

En este punto se deben de especificar los lineamientos del área de trabajo, desde, no permitir el acceso a el lugar con líquidos, el control de la humedad, e instruir a los

empleados sobre los elementos a los que los equipos de cómputo son sensibles, como lo es la humedad y el calor excesivo.

También de ser posible o en empresas que están diseñando aun su área de información, determinar cual será el mejor lugar en base a la geografía, para prevenir problemas por inundaciones y cortes del suministro eléctrico.

También encontramos en este punto el aseguramiento del equipo con diversos mecanismos como es el acceso con puertas electrónicas, sensores de movimiento, alarmas en los racks, para evitar el robo de equipo.

Un claro ejemplo es el ***Prodigy Data Center***, en el que se requiere de contraseñas, tarjetas inteligentes, y dispositivos biométricos para acceder solamente al edificio y de la misma manera se cuenta con estos mecanismos para acceder a los equipos.

Conformidad

Los objetivos de esta sección son:

- Prevenir la existencia de brechas o huecos en las leyes de tipo criminal o civil.
- Asegurar la conformidad de los sistemas con las leyes, políticas y estándares de la empresa.
- Maximizar la efectividad y minimizar la interferencia en los procesos de auditoria.

Este punto, debe de ser tratado directamente con los directivos de la organización, así como con los expertos en seguridad y los mismos empleados, definiendo responsabilidades en el uso y manejo de la información.

Es decir, que se le debe notificar al empleado que puede ser monitoreado en sus actividades y que deberá de mantener respaldos de su información, o en otros casos se le informará cuales son los periodos en los que se llevará acabo el respaldo de la información.

Un punto muy importante es el hecho de mantener sobre aviso a los empleados que serán monitoreados, y qué aspectos serán monitoreados, ya que es en este aspecto en el que más evasiones de responsabilidades o de cargos existen. Debido a que se puede considerar invasión a la privacidad del empleado, por tanto la información podría ser descartada en una investigación por considerar que se obtuvo de manera ilegal.

Este tipo de puntos deben de ser discutidos en conjunto con el área de personal, de información, seguridad y los directivos de la empresa antes de ser puesto en marcha.

Seguridad del personal

- Reducir el riesgo del error humano, robo, fraude o mal uso de las instalaciones.
- Asegurar que los usuarios están concientes de la importancia de la información y todos los procesos que la envuelven, para esto deberán estar apoyados en el conocimiento de las políticas de seguridad en el curso normal de su trabajo, para minimizar el impacto de los incidentes de seguridad y aprender de ellos.

De la misma forma en que existen las responsabilidades del empleado, existen las de la empresa para con el empleado, entre ellas se encuentra el mantener capacitado al personal para el uso de los sistemas y equipos de la empresa, previniendo con esto que el desconocimiento del funcionamiento del mismo pueda provocar un incidente.

Uno de los puntos en los que las organizaciones deben invertir es en la capacitación de los empleados para el correcto uso de los sistemas de información y comunicación, esto no solo aumenta la productividad de la organización y agiliza los tiempos de un proceso, si no que previene incidentes de seguridad derivados del desconocimiento en el uso de las TIC's.

Este punto de las políticas de seguridad también incluye el perfil de las personas que deberán ser contratadas, sobre todo para las áreas críticas en las que se maneja información confidencial, se deberá revisar los antecedentes de los postulantes para el puesto, así como pedir referencias de ellos en sus anteriores empleos antes de delegarle un grado de confianza en la organización y por ende en el acceso a la información.

Organización de la seguridad

- Manejar la seguridad de la información en conjunto con toda la empresa.
- Mantener la seguridad de la información que es intercambiada con terceras partes.
- Mantener la seguridad de la información cuando el uso de esta ha sido delegada a otra organización mediante Outsourcing

En casi todas las organizaciones existe el intercambio de información, es decir diversas organizaciones comparten información que es útil o que su administración y/o adquisición ha sido delegada a terceros, por lo que se deben de establecer los mecanismos y cuales son los protocolos para el intercambio de información.

Esto lo podemos ver en los bancos y tiendas que ofrecen crédito, que mantienen sus sistemas interconectados con el Buroe Federal de Crédito, para obtener información en tiempo real.

También tenemos la información recolectada por los *contac center* y que es entregada a la empresa en periodos determinados para realizar estudios de mercado. Pero no solo esto, también se da la renta de equipo, por lo que se deberán de seguir ciertos lineamiento en la destrucción de información cada que los equipos son remplazados como parte del arrendamiento.

En el caso del Buroe Federal de crédito, se establecen linimientos de acceso a sus bases de datos, como protocolos de autentificación y cifrado de datos, así como la expedición de certificados digitales para el intercambio de información.

Es importante que se pongan en claro todos estos puntos antes de realizar o contratar los servicios externos, además de establecer los lineamientos del monitoreo de intercambio de información y responsabilidades de cada parte.

Administración de la red y el equipo de cómputo.

- Asegurar la correcta operación de la información en las instalaciones.
- Minimizar el riesgo de fallas en los sistemas.
- Proteger la seguridad del software y la información.
- Mantener la integridad y la disponibilidad de los procesos de comunicación de información.
- Asegurar el resguardo de la información en las redes y la protección de la infraestructura.
- Prevenir el daño a los activos y la interrupción a las actividades de negocio.
- Prevenir perdida modificación o mal uso en el intercambio de la información entre organizaciones.

Estos puntos serán tratados en su mayor parte por los expertos en TIC's y de seguridad, se refiere a el nivel operativo de los sistemas, se deberán de hacer pruebas constantes, mantener actualizados los sistemas, actualizar los sistemas de respaldo y verificar que estos sean correctos.

Se deberán realizar pruebas de penetración y pruebas de errores a los sistemas, con herramientas propias y de uso comercial para anticiparse a cualquier tipo de ataque, además de plantear nuevos escenarios de caídas del sistema o de desastres naturales para actualizar los mecanismos de respuesta de incidentes.

También se incluye en este punto los lineamientos del monitoreo de las actividades y la descripción de ¿que deberá ser monitoreado?; por ejemplo, si se monitoreará el tiempo que el empleado navega en Internet, a que sitios accedió, cuanto tiempo gasta en pláticas en línea o incluso el monitoreo de las conversaciones en línea.

De esta forma, se debe establecer ¿Quiénes? y ¿Cómo? deberán realizar estas actividades, cuales son sus responsabilidades y sus áreas de acción, además de establecer los procedimientos de respuesta de incidentes.

Clasificación de activos y control

Mantener la apropiada protección de los activos de la corporación para asegurar que la información es manejada con el nivel apropiado de seguridad.

También se debe de determinar ¿que equipos deberán ser asegurados?, ¿Cómo? Y ¿contra que?, ¿si se ha de contratar una empresa de seguridad privada? o si es suficiente con la seguridad de la empresa, además se deberá de mantener un control de la salida y entrada de los equipos.

También se deberá contemplar si se han de instalar dispositivos especiales en ciertas áreas, como dispositivos contra incendios o sistemas de enfriamiento y control de humedad.

Política de seguridad

Se refiere a tener una política de seguridad lo suficientemente robusta y que esta sea manejada y soportada por los estándares de seguridad, así como también asegurar su correcta distribución a los miembros de la organización.

Se establece que áreas deberán de contar con certificados que avalen sus niveles de operación y de seguridad, la manera en la que la información se hará llegar a los empleados y los periodos en los que las políticas deberán ser revisadas para que se encuentren actualizadas evitando que se pueda ignorar algún punto.

1.6.2 ESQUEMA DE UN ATAQUE

Uno de los procedimientos de seguridad más importantes en la forensia informática, es la capacidad para reconocer un ataque o el inicio de un ataque potencial. Aunque, actualmente ya existen sistemas que detectan patrones de inicio de un ataque como son los ***IDS's***[10], es necesario que los expertos en TIC's y los forenses informáticos conozcan todos estos patrones para poder dar el seguimiento necesario.

Esencialmente los ataques tienen el siguiente patrón:

- El pre-ataque o reconocimiento.
- Acceso inicial.
- Acceso completo o privilegiado al sistema.
- Preparar el acceso futuro.
- Cubrir el ataque.

1.6.2.1 Pre-ataque o reconocimiento

Este punto se refiere a la obtención de información del objetivo, para comenzar un ataque es necesario tener la mayor cantidad de información posible, con el objetivo de poder acceder al sistema sabiendo que es lo que se va a encontrar en el y la manera precisa de llegar a el.

Los procesos de obtención de información son diversos, aquí se presentará una descripción de algunos de estos métodos.

Escaneo de puertos:

Este es uno de los métodos básicos para la preparación de un incidente, como sabemos todos los servicios de red que se ejecutan en un equipo necesitan de un ***puerto***[11] para poder atender las peticiones realizadas por los otros equipos. De esta misma forma cada servicio que trabaja en la red, es un riesgo potencial de seguridad debido a que estos programas en

[10] **IDS's,** sistema de detección de intrusos por sus siglas en ingles, detectan patrones que pueden suponer que el sistema esta bajo ataque y lo informan al administrador de diferentes maneras.
[11] **Puerto:** Se le conoce como puerto a un lugar no tangible en el que se realiza una conexión de datos.

ocasiones pueden estar mal configurados o presentar algún tipo de vulnerabilidad explotable.

De esta forma cada puerto que esté ofreciendo un servicio se le conoce como un puerto abierto. Los escaners de puertos intentan identificar ¿cuales están abiertos? y ¿qué servicios se están ejecutando en estos?, ¿qué versiones de software? y algunos otros detalles que puedan ser útiles para un atacante.

Existen diferentes formas y por lo tanto programas que realizan el escaneo de puertos; la manera en que estos trabajan es enviando peticiones de conexión a puertos específicos o a todos los puertos del equipo objetivo, si el puerto responde con una señal de aceptación, el puerto está abierto, además de la respuesta algunos programas agregan información adicional que informa sobre el tipo de servicio que se esta ejecutando y la versión del software.

IP spoofing y DNS spoofing

Esta técnica consiste en suplantar la dirección de origen de los paquetes enviados a un equipo, con la finalidad de suplantar a otro que esté dentro del esquema de seguridad; También es usado para ocultar el origen de un ataque, haciendo mas complicada la labor de rastreo de los investigadores.

Esta técnica solía ser algo compleja de utilizar pero en la actualidad, existen programas que no solo pueden falsificar la dirección IP, si no también las direcciones ***MAC***[12] de los equipos; aun así, la correcta utilización de esta técnica requiere de un cierto conocimiento de la pila de protocolos del TCP/IP.

El DNS spoofing consiste igualmente en suplantar direcciones y/o peticiones de un servidor DNS con la finalidad de que la información sea redireccionada a un equipo en especifico, así como para obtener información privilegiada de la red interna.

1.6.2.2 Acceso inicial

Cuando el atacante ha logrado recabar suficiente información, es momento para que intente ingresar al sistema. En este punto pueden ocurrir dos cosas, si el encargado de la administración de sistemas se ha percatado de que existe la posibilidad de un ataque, se encargará de cerrarle las puertas al intruso y tomar las medidas necesarias; de lo contrario, no se hará nada hasta que el daño este echo.

Solo en algunos casos el administrador del sistema tomará las medidas necesarias para hacer parecer que el sistema aun es vulnerable y dejar que el atacante siga con sus actividades, esto con la finalidad de tener evidencia necesaria para detenerlo y darle seguimiento al caso.

Generalmente este tipo de medidas requieren un conocimiento muy amplio de técnicas y mecanismos de seguridad, además que las autoridades correspondientes ya estarán

[12] **MAC**: Médium Access Control.

enteradas para dar fe de la legalidad de la investigación, y asegurar que la misma no será desacreditada posteriormente.
El lograr acceso en un sistema, se puede hacer de dos formas, obteniendo un nombre de usuario y contraseña o, explotando alguna vulnerabilidad que permita saltar el mecanismo de autentificación del sistema.

El obtener un password y un nombre de usuario valido, se puede hacer de las siguientes formas:

Ingeniería Social

Uno de los métodos más usados y más efectivos de obtener acceso a un sistema, es la llamada ingeniería social, que consiste en:

"Hacer que las personas nos digan las cosas que necesitamos saber y que no deberíamos saber sin que ellos estén conscientes de lo que estamos haciendo."

Esta técnica requiere de mucha astucia, y de mucha pericia para convencer a las personas, la manera mas fácil de obtener información sobre una cuenta de usuario en un sistema, es preguntándole al propio usuario.

Es decir, el atacante podría acudir a la empresa u organización y convencer de alguna manera al usuario de que le proporcione la información, su nombre de usuario e incluso hasta su contraseña convenciéndolo que él esta autorizado para saberlo o quizás solo como parte de una plática común como un detalle sin importancia.

La ingeniería social también consiste en vigilar a las personas que tienen acceso al sistema, ya que mientras mas sepa sobre ellos, será más fácil obtener el acceso y cubrir las huellas. Por ejemplo, las contraseñas de los empleados suelen ser combinaciones de nombres, fechas y otros datos personales de personas cercanas, esto suele facilitar mucho el trabajo del atacante y es responsabilidad del experto en seguridad el hacer consciente a los empleados de estos riesgos.

Por esto mismo muchos expertos en seguridad entre ellos el mismo Kevin Mitnick, aseguran que el eslabón más débil de la seguridad de la empresa son los empleados.

Intercepción de passwords

Existen muchas formas de lograr interceptar información que viaja a través de una red, si el atacante logra obtener un nombre de usuario, es muy probable que también obtenga el password, afortunadamente en la actualidad la mayoría de los passwords que viajan en la red, son cifrados con algún mecanismo de seguridad.

Sin embargo, también existen programas que pueden identificar el tipo de cifrado que es usado en el password y, teóricamente, descifrarlo, esto debido a que en la actualidad los mecanismos de cifrado usados, son tan complejos que a un equipo convencional le tomaría

años descifrarlo, amenos claro que exista un error de programación o de diseño del algoritmo que permita lo contrario.

Es por esto que las técnicas de penetración basadas en intercepción de passwords, están dejando de ser efectivas, pero no por esto se debe de dejar de lado la seguridad y complejidad de las contraseñas, ya que un ataque de **fuerza bruta** podría fácilmente encontrar una contraseña que utiliza un mecanismo de seguridad muy complejo, es decir, no sirve de nada que existan mecanismos de cifrado tan complejos si los usuarios del sistema usan contraseñas que son fáciles de deducir para el atacante.

Exploits

Los llamados exploits, suelen ser un método complejo de obtener acceso a los sistemas y generalmente requiere un cierto grado de conocimiento en programación y protocolos de Internet.

Un exploit consiste en un programa o código que explota una vulnerabilidad o problema de programación en los sistemas para tener acceso a un sistema, servicio o incluso provocar una negación de servicio por el bloqueo del equipo.

Existen dos tipos de exploits, los llamados de protocolo y de aplicación. Los exploits de protocolo, se refieren a aquellos que explotan algún tipo de error en la programación y/o diseño de un protocolo en particular como el TCP/IP.

Un ejemplo de este tipo de exploits, es el conocido como Ping de la muerte, que consistía en enviar una petición con un paquete de mas de 65,536 bytes, que es el máximo tamaño permitido por las especificaciones del protocolo, lo que provocaba que el sistema atacado se bloqueara, trabara o en algunos casos reiniciara.

Afortunadamente este error ya ha sido corregido en las implementaciones de sistemas operativos más nuevos. Pero muchos otros problemas siguen sin resolverse, algunos de estos por ser directamente generados por las especificaciones del protocolo, lo que hace muy difícil resolver el problema; Los exploits de protocolo suelen ser usados para provocar negación de servicio en los sistemas y no para obtener acceso a ellos.

Los exploits de aplicación generalmente explotan vulnerabilidades en los sistemas operativos y aplicaciones que ofrecen algún servicio en red e incluso de manera local, ya que existen exploits locales y remotos. Generalmente los exploits usan vulnerabilidades conocidas como **buffer overflow**.

La explotación de un **buffer overflow** o un desbordamiento de buffer, suele ser algo complejo de realizar y de entender en un principio, pero se trata de un concepto básico de seguridad y programación que engloba muchos conceptos que no fue tomado en cuenta sino hasta que en 1988 un gusano llamado “morris” hizo ver el gran riesgo que representa.

Una explicación sencilla de un buffer overflow, sería la siguiente: Como sabemos los programas usan segmentos de memoria para guardar las variables que se van a procesar, estos espacios de memoria tienen que ser reservados con anterioridad para hacer mas eficiente el programa y el aprovechamiento de los recursos del equipo.

Pero si al recibir las variables que se van a procesar estas son de un tamaño mayor al esperado, se produce una excepción u error conocido como desbordamiento de buffer. El problema radica en que la información que sobrepasa la variable tiene que ir a parar en algún lugar, que, normalmente son los registros contiguos de memoria, estos son los registros EBP e EIP.

Ahora supongamos lo siguiente, tenemos una variable que va a aceptar 256 bytes, pero nosotros ponemos en el buffer de entrada 264 bytes en lugar de los 256 esperados, esto provocará un desbordamiento hacia los registros contiguos escribiendo la información restante en EBP y EIP.

En el registro EIP se encuentra la dirección de la siguiente instrucción a ejecutarse en un programa y esta representada en formato hexadecimal, si sobre-escribimos estos registros con letras 'A', es decir, ponemos 264 letras 'A' en el buffer de entrada en lugar de los 256 esperadas, tendríamos algo como se muestra en la figura 1.1

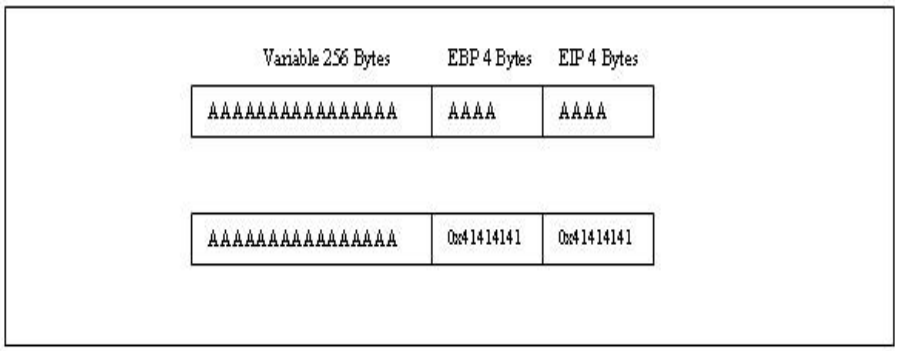


Figura 1.1 Desbordamiento del buffer

En el espacio de memoria reservado para la variable tendríamos solo letras A o su equivalente en hexadecimal, pero de la misma forma el registro EIP y EBP contendrían la dirección '0x41414141', que es el equivalente en hexadecimal de 'AAAA', esto debido a que desbordamos la memoria con mas información de la que le cabía al buffer; Lo que sucederá a es que el procesador intentará ejecutar la siguiente instrucción que se encuentra en la dirección contenida en EIP, provocando un error.

Ahora tenemos control sobre cuál será la siguiente instrucción a ejecutarse en el programa, así que vasta con poner un **shell code**[13] en los primeros 256 bytes y en los restantes poner la dirección de esta variable, esto se ilustra en la figura 1.2

[13] **Shell code,** código de un shell o línea de comandos generalmente en código ensamblador o hexadecimal.

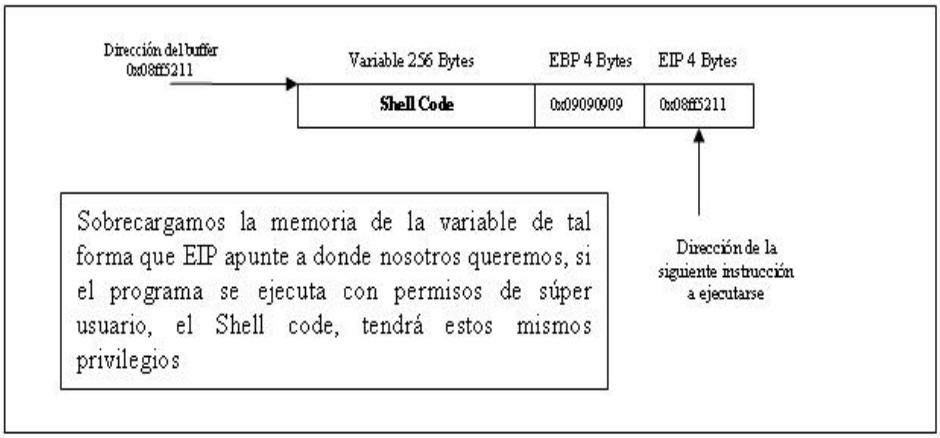


Figura 1.2 Introducción de un Shell code

Si el programa en el que realizamos la sobre carga de la variable se esta ejecutando con privilegios de administrador en el equipo, el shell que nosotros obtendremos como resultado tendrá los mismos privilegios de ejecución.

De esta forma podemos hacer que un pequeño error de programación nos de acceso privilegiado al sistema; existen muchos tipos de exploits de este tipo, pero todos siguen el mismo principio. Por el momento no se entrara en más detalles de este tipo de vulnerabilidad, como podrían ser, obtener la dirección de la variable y los diferentes tipos de arquitectura de procesador.

1.6.2.3 Acceso completo y privilegiado al sistema

Si el atacante a realizado su trabajo de manera correcta podrá tener acceso al sistema con privilegios altos, tales como el de administrador, esto implica que el sistema ha sido comprometido, en este punto el crimen de acceso ilícito a sistemas y/o recursos ha sido consumado y debería haber suficiente evidencia para armar un caso.

Para lograr el acceso privilegiado al sistema se usa una combinación de las técnicas anteriores como son los métodos de fuerza bruta y el uso de exploits.

1.6.2.4 Preparar el acceso futuro

Los atacantes astutos no realizan sus acciones desde la cuenta de administrador o súper usuario, eso implicaría el ser descubiertos rápidamente, lo que prosigue una ves que se tiene acceso privilegiado al sistema, es la generación de cuentas con privilegios de administrador, cuentas fantasma para acceso además de plantar programas de tipo troyano para robar información.

Debemos recordar que el comprometimiento del equipo no solo implica el robo o la alteración de la información del equipo, sino que ese equipo puede ser usado para obtener acceso a otros equipos o para dirigir algún tipo de ataque.

1.6.2.5 Cubrir el ataque

Una ves que se ha dejado preparado todo, es hora de cubrir toda la evidencia, este es un momento crucial, ya que el atacante intentará borrar toda evidencia que pudiera existir no solo ¿de dónde vino el ataque?, sino que existió un ataque.

Existen muchos casos en los que la evidencia es borrada de manera que los administradores del sistema no se dan cuenta que el sistema ha sido comprometido si no hasta cuando ya es muy tarde.

1.6.3 HACKING PARA LOS NO EXPERTOS

En la actualidad se registra un gran numero de ataques o incidentes provocados por los llamados ***Newbies o Script Kiddies,*** estos son personas que no tienen un amplio conocimiento en informática, sino que hacen uso de una gran cantidad de información y programas que existen en Internet para realizar sus ataques.

Generalmente, este tipo de ataques, no suelen ser efectivos contra organizaciones o empresas que tengan bien definidos sus esquemas de seguridad, pero como sabemos, no todas las organizaciones tienen sus esquemas tan bien definidos.

Los llamados Script Kiddies, suelen ser personas que buscan un programa o un pequeño código de explote alguna vulnerabilidad de algún sistema o algún servicio en particular, pero sin saber necesariamente la manera en la que esté trabaja. Es decir el trabajo del Script Kiddie, consiste solo en buscar el *exploit,* compilarlo y ejecutarlo.

Debido a que la mayoría de estos ataques son realizados con los conocimientos mínimos de seguridad, es más fácil para los encargados y para los investigadores el rastrearlos en caso de un incidente, pero esta misma facilidad de ejecución provoca que las empresas reciban alertas de ataques contra los cuales ya están protegidos.

Lo anterior provocaba un exceso de información sobre intentos de ataques y fue provocando que los encargados de la seguridad descartaran mucha información, ya que revisar tales volúmenes de datos tomaría mucho tiempo.

En la actualidad ya existen sistemas mucho más complejos que en conjunto con técnicas de inteligencia artificial, filtran la información generada por los sistemas de seguridad para solo presentar a los encargados la información que, realmente puede presentar un peligro potencial por un ataque.

Pero así como ha existido un gran avance para facilitar las cosas en los sistemas operativos, de esta misma forma, muchos Hackers e incluso empresas de seguridad, han puesto a disposición de el público en general, herramientas en las cuales, basta con hacer un clik, para realizar un ataque a toda una red, como el caso de los llamados ***Floders***[14], que con un solo clik, inundan toda una red con paquetes de gran tamaño, provocando una negación de servicio.

[14] **Floders,** programas que inundan una red con paquetes de datos especialmente formados, saturando los recursos de esta

Es por esto que los expertos en seguridad como David Rhoades, han comenzado a usar el término ***Clik Kiddies*** para este tipo de atacantes, ya que basta solo con presionar un botón, además de que estos programas están basados en sistemas gráficos muy amigables para el usuario.

1.7 Plan de recuperación de desastres

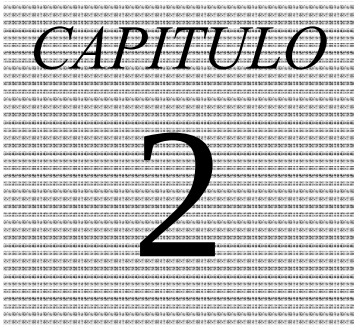
El contar con un plan de recuperación de desastres es vital, ya que de no contarse con este, al presentarse un desastre la continuidad del negocio se vería afectada de manera por demás severa.

Este plan, debe de tomar en cuenta ¿qué información es la crucial para la empresa? y ¿cual es la manera correcta de regresar o recuperar el funcionamiento de los mecanismos de los cuales depende?.

El plan debe de tener como base un análisis de los activos de información de la empresa, de manera que se pueda tener un esquema de importancia de la información y así priorizar los tiempos de recuperación.

Aunque todos los planes de recuperación cubren ciertos aspectos, puede resultar imposible plantear todos los escenarios que pueden ocurrir. Los puntos que se recomienda que cubra un plan de recuperación de desastres, son los siguientes [4].

- Proveer administración con el conocimiento de todos los recursos necesarios para desarrollar y mantener un plan efectivo de recuperación de desastres. En adición a esto, el plan debe de contar con el apoyo de los miembros de la organización como son los expertos en TIC's.
- Contar con un equipo de respuesta de incidentes, en el cual se cuente con por lo menos un miembro de las áreas mas críticas de la organización.
- Definir los requerimientos de recuperación desde la perspectiva de la continuidad del negocio.
- Identificar los riesgos. Todos los riesgos deben ser identificados para determinar la manera en la que estos ocurren, para evitar que ocurran.
- Determinar los riesgos de un incidente prolongado o de la pérdida de una de las funciones claves para el negocio.
- Reunir periódicamente al equipo de recuperación de desastres para asegurar que se mantiene el equilibrio del plan de recuperación de datos.
- Desarrollar un plan de contingencia que sea fácil de entender, fácil de aplicar y fácil de mantener en la empresa.
- Definir como el plan de contingencia de negocio será implantado en el plan actual de negocio.



ESTATUS DE LAS LEYES INFORMÁTICAS

2.1 HISTORIA DE LOS DELITOS INFORMÁTICOS

Los delitos informáticos aparecieron prácticamente en el momento en el que las computadoras aparecieron, pero fue hasta que el acceso a ellas fue más fácil y menos costoso cuando este fenómeno se acentuó. En nuestros días, millones de personas tienen acceso a las computadoras, en escuelas, bibliotecas, centros de consulta y sus trabajos.

Otro aspecto que permitió el crecimiento de los delitos informáticos, es el hecho de que anteriormente además de ser muy complicado el tener acceso a una computadora, se requería de conocimientos específicos para poder lograr que la computadora realizara una tarea; Esto cambió radicalmente con la aparición de sistemas gráficos y amigables para los usuarios, ya que permitió que usuarios sin mucho conocimiento informático, pudiesen realizar tareas supuestamente complejas como el descargar o transferir un archivo, enviar un correo electrónico, etc.

En la actualidad existen muchos llamados ***Hackers***[15] que cuentan con grandes conocimientos en el área como programación, protocolos y sistemas operativos, Conocidos también como la Elite o Gurús, pero también existe un gran numero de usuarios que son personas las cuales cuentan con un conocimiento mínimo de estas áreas.

En el año 1960 apareció la primera computadora de tipo comercial, esta fue la **PDP-1**[16], las empresas, escuelas y otras organizaciones rentaban tiempo en estas computadoras para realizar sus tareas de procesamiento; Debido a esto la información estaba almacenada en un solo equipo y muchas personas tenían acceso a este, lo que abrió la primera puerta de los delitos informáticos, Véase figura 2.1.

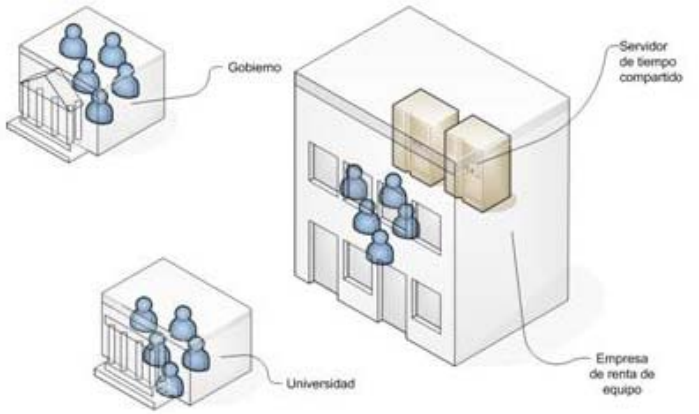


Figura 2.1 Uso de tiempo compartido en servidores

[15] **Hacker** Termino inicialmente usado para nombrar a los técnicos de sistemas telefónicos, usado en la actualidad para nombrar a quienes irrumpen en sistemas informáticos.
[16] **PDP-1** Programed Data Processor, desarrollado por DEC en los 60's.

Entre los años 60's y 70's el ***hacking*** se relaciono de alguna forma con los movimientos radicales de esa época. Igualmente en estos días la policía comenzó a realizar los primeros arrestos relacionados con fraudes a los sistemas telefónicos, conocidos desde entonces como ***Phreaking***[17].

En los años 80's se comenzaron a realizar los primeros arrestos relacionados con los delitos por computadora, incluyendo el de Kevin Mitnik, quien fuera considerado mártir de la causa y apoyado por muchos otros hackers de esa época. Esto dio al término hacker un sentido de héroe que rompía la ley pero con propósitos nobles.

Pero del otro lado del mundo también comenzaron a aparecer este tipo de criminales, en un principio, de igual forma que en América, los llamados Phreackers, quienes se dedicaban a hacer llamadas telefónicas de larga distancia sin pagar, por medio de un pequeño dispositivo llamado "Toll A" el equivalente a la "Blue Box" en América.

Se puede decir que existieron todo tipo de cajas, en esta época, como la "Red box" y "black box", en su mayoría eran usadas para realizar llamadas telefónicas de larga distancia sin pagar por ello, pero no solo eran usadas para estos fines, existió también la llamada "cheese box", usada para conectar dos líneas telefónicas de tal manera que al intentar rastrear una llamada, pareciese que esta venia de otro número y fue usada para concretar otro tipo de actividades criminales.

Un punto muy importante en la informática y por ende en los delitos informáticos fue el desarrollo de las redes. Fue en 1970 cuando investigadores de Xerox, Intel y DEC, desarrollaron Ethernet, el cual se convertiría en el estándar para las redes de computadoras.

En 1983 el instituto de ingenieros eléctricos y electrónicos liberó el estándar 802.3 basado en el cable coaxial conocido también como 10Base5. De esta forma **Ethernet**[18] se convirtió en una alternativa viable para las empresas y con la llegada del cable coaxial delgado o también conocido como 10Base2 en 1985 las redes de computadoras comenzaron a ser una alternativa real a la computación centralizada.

2.2 El BBS

El sistema BBS o "***Bulleting Board Service",*** es el antecesor real del Internet como lo conocemos en la actualidad. Consistía en una computadora con varios módems, a los cuales los usuarios se conectaban para subir o descargar archivos, así como para intercambiar ideas por medio de los sistemas de boletines [1]. Véase figura 2.2

Los primeros hackers encontraron en los BBS una forma de comunicarse e intercambiar información, además de esto, se convirtió en un medio muy común para intercambiar programas como ***warez***[19] así como juegos de computadora.

[17] **Phreacking** Termino dado a aquellos que realizan algún tipo de fraude con o por medio del sistema telefonico
[18] **Ethernet** Conocido en un principio como DIX por las siglas de las tres compañías, DEC, Intel y Xerox
[19] **Warez** Termino usado por comúnmente por los hacker para denominar al software pirata.

Sin embargo a principios de los años 90's el BBS comenzó a declinar debido a que el acceso a Internet se hizo mas comercial y tenia como aliado los sistemas gráficos que hacían ver totalmente obsoleto al BBS con su sistema basado en dibujos **ASCII**[20].

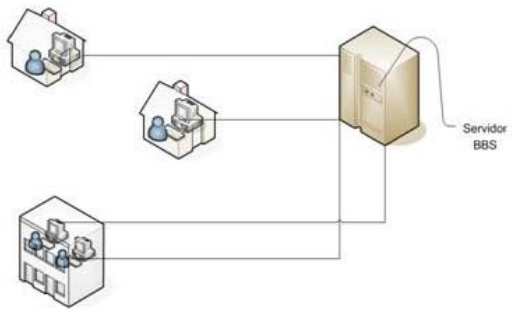


Figura 2.2 El BBS

2.3 LOS PRIMEROS INCIDENTES INFORMÁTICOS

Con la aparición de los primeros proveedores de servicios de Internet, también lo hicieron muchos usuarios expertos e inexpertos en el área, en un principio el simple método de conexión era excluyente, ya que no cualquiera podía conectarse con los ***ISP's***[21] ya que se requería de conocimiento para instalar el protocolo y realizar la conexión necesaria con este.

Pero con la aparición de proveedores como Compuserve, Prodigy y AOL, el trabajo se hizo más fácil, ya que estas compañías incluían formas de configurar fácilmente el acceso a su servicio.

Pero fue hasta 1988 cuando apareció el primer ***gusano***[22], el cual infectó a los sistemas basados en UNIX Berkeley, dejando fuera casi la mitad del Internet. Este fue el primero de muchos incidentes de este tipo y fue la llamada de alerta acerca del problema que venia.

En 1991 los usuarios de Internet comenzaron a preocuparse de que sus mensajes de correo electrónicos pudiesen ser interceptados por alguien. Fue Philip Zimmerman, quien diseñó un programa de encriptación de datos conocido como ***PGP***[23] que también fuera usado por los hackers para esconder evidencia de sus actos criminales.

En 1994 el primer banco virtual abrió un nuevo mundo para los criminales informáticos. En ese mismo año, investigadores comenzaron a trabajar en un nuevo estándar para el protocolo de Internet conocido como IPv6 y que se supone substituirá al protocolo actual

[20] **ASCII** código de caracteres utilizado por las computadoras, en el que cada letra, dígito y símbolo (¨, ?, ",...) es representado por un número de 0 al 255

[21] **ISP** proveedor de servicios de Internet por sus siglas en ingles.

[22] **Gusano,** se denomina gusano a un programa que es capas de propagarse por la red de manera automatizada

[23] **PGP,** pretty good privacy, compañía dedicada actualmente a los sistemas de cifrado de información con llave publica

conocido como IPv4, y cuya principal innovación será el incluir mecanismos de seguridad en si.

En 1996 el congreso de Estados Unidos fue advertido acerca de la cantidad de pornografía que se intercambiaba en Internet y el departamento declaró el intercambio como inconstitucional. En ese mismo año, un programa fue liberado en Internet destruyendo cerca de 25000 mensajes de grupos de noticias y el sistema del departamento de justicia de los Estados Unidos fue hackeado.

En los años siguientes, varias instancias gubernamentales de los estados unidos fueron hackeadas incluyendo el departamento de comercio, UNICEF, el New York Times, eBay, Microsoft y el sitio del senado norteamericano. Fue liberado el virus melisa, el cual causó que los sistemas de correo electrónico de muchas compañías dejaran de funcionar provocando grandes pérdidas.

Ya en el año 2000, los ataques de negación de servicio distribuidos lograron que sitios como Yahoo y Amazon dejaran de funcionar. ***Código rojo*** atacó diversos sitios Web y ***Sircam*** afecto un gran número de cuentas de correo electrónico alrededor del mundo.

En la actualidad, los incidentes informáticos han crecido en número y en tipo, afectando diversas actividades, empresas y organizaciones, además de que con la llegada de tecnologías como el ***Wireless,*** las líneas ***xDSL***[24]**,** el comercio en línea, el correo HTML y los nuevos sistemas operativos han abierto nuevas puertas y brechas de seguridad difíciles de resguardar.

2.4 LEGISLACION INFORMÁTICA

Al hablar de delitos informáticos, es necesario el hablar del estado actual de las leyes que los engloban.

En un principio, los delitos que tenían que ver con el uso de la tecnología, no fueron tomados en cuenta, ya que las posibles perdidas que se generaban de estos, no eran tangibles porque era solo información.

Conforme los servicios que hacían uso de la tecnología se fueron extendiendo los delitos que tenían que ver con ellos, fueron aumentando, provocando perdidas a las empresas, de tal forma que fue la iniciativa privada la primera en exigir la persecución y castigo de estos crímenes.

Pero a principios de los años ochentas, la legislación no cubría los casos de crímenes realizados por medios tecnológicos, así que los primeros crímenes tenían que ver generalmente con el servicio telefónico, fueron tratados y perseguidos con recursos legales demasiado ambiguos, lo que en la mayoría de los casos resultaba en sentencias pobres o en ciertos casos no se podía dictaminar una sentencia.

[24] **xDSL,** Se usa para referirse a todos los tipos de líneas de abonado de datos como ADSL, SDSL ,etc.

Estos "huecos" en la legislación, permitía que muchos de los delitos quedaran sin castigar o que el castigo no fuera el adecuado.

Poco a poco las leyes fueron evolucionando hasta poder incorporar los términos como *"delito informático" y "cibercrimen"*, pero, aún en la actualidad la legislación que regula este tipo de crímenes no contempla muchos otros aspectos, esto provoca que algunos de los delitos cometidos no sean juzgados o no puedan ser perseguidos por las autoridades correspondientes.

2.4.1 DELITO INFORMÁTICO

Un delito informático o ***Cibercrimen*** como tal, no tiene una definición oficial, esto es debido a que en ocasiones lo que es un crimen en un país o región del mundo, muy probablemente no lo sea en otra región del país o en otra región del mundo.

Esto es debido sobre todo a problemas en interior de los países, en los cuales se ha dejado de lado por mucho tiempo una cultura sobre la legislación de los sistemas informáticos.

El delito informático puede ser definido por varios aspectos, esencialmente se le da esta categoría cuando para su ejecución se hace uso de sistemas informáticos o redes de transmisión de datos.

Las computadoras pueden estar inmersas en el delito de diferentes maneras [1]:

- La computadora o la red puede ser la herramienta para cometer el delito, usado para realizar y completar el crimen.
- La computadora y/o la red pueden ser el blanco del crimen o la victima del crimen.
- La computadora puede ser usada para propósitos criminales indirectos, como el almacenamiento de direcciones de ventas de drogas.

El departamento de justicia de los estados unidos considera un crimen informático como:

"Cualquier actividad que viole las leyes y que para esto involucre el conocimiento y uso de tecnologías computacionales para la perpetración persecución o investigación del crimen"

La definición anterior es una clara prueba de lo imprecisas que pueden ser las leyes, ya que virtualmente todos los crímenes pueden ser catalogados como *"Cibercrímenes"*, ya que los investigadores tendrían que buscar en bases de datos información relevante a cualquier caso.

Otro gran problema referente a la legislación informática, es el aspecto de la jurisdicción, debido a que la mayoría de este tipo de delitos ocurren en el Internet o en el llamado ***Ciberespacio***[25], en el cual como sabemos no existe una jurisdicción, es muy complicado determinar que leyes deben o pueden ser aplicadas a cierto delito.

[25] **Ciberespacio,** Termino usado para definir el espacio virtual en el que interactúan las personas en Internet.

En general, el delito informático aun no cuenta con una forma de definirlo sin que tenga ambigüedades en esta, debido quizás a que quienes escriben las leyes, en muchos de los casos tiene poco que ver con el manejo de las tecnologías de información, como lo son las redes y las computadoras.

2.4.2 LEYES INTERNACIONALES RELACIONADAS CON LOS CIBERCRIMENES

Debido a que los crímenes de carácter informático o relacionado con la informática en la mayoría de los casos tienen lugar en un espacio intangible, el problema jurisdiccional es siempre un problema.

En el décimo congreso de las naciones unidas para la prevención del crimen y el trato de los ofendidos, los crímenes cibernéticos fueron divididos en dos y definidos de la manera siguiente [3]:

- **Un crimen computacional es:** un acto ilegal cometido mediante una operación electrónica que afecta una computadora y/o la información procesada por esta.
- **Un crimen cometido por computadora es:** Cualquier acto ilegal cometido por medio de, o en conjunto con una red de computadoras, incluyendo la posesión ilegal de información, oferta y/o distribución de esta por medio de la computadora o las redes de computadoras.

Esta definición se complica ya que lo que puede ser considerado ilegal en un país, puede no serlo en otro. La definición se extiende dando algunos ejemplos más concretos de estos actos ilegales.

- Acceso no autorizado.
- Daño a los datos de la computadora o programa en cuestión.
- Sabotaje computacional.
- Intercepción no autorizada de información.
- Espionaje computacional

A pesar de que estas definiciones no son aplicables en todos los ámbitos, si da un punto de inicio para definir que es un delito informático o cibernético, ya que cuenta con reconocimiento internacional.

Sin embargo, aun falta mucho que hacer para poder tener una definición y categorización aceptable de lo que es un crimen cibernético. Además de que cada país debería contar con una definición propia para la correcta aplicación de la ley.

2.4.3 ESTATUS DE LAS LEYES MEXICANAS RELACIONADAS CON LOS CRÍMENES INFORMÁTICOS

Actualmente la legislación en México no cuenta con una definición de crimen cibernético o crimen informático. Fue si no hasta 1999 cuando se reformo el articulo 211 del código penal federal, para contemplar los crímenes cometidos en contra de las computadoras y por medio de estas; posteriormente se realizaron diversas modificaciones y anexos a otras leyes para dar cabida a los nuevos delitos.

Mas sin embargo las leyes excluyen muchos términos y son en muchos casos ambiguos y faltos de claridad. Entre las reformas que se han realizado recientemente a la legislación mexicana para dar cabida a la revolución informática son:

- Reformas al código de comercio.
- Reformas a los artículos 1803, 1811 del código civil federal.
- Reformas a la ley federal de protección al consumidor.
- Reformas a la ley de derechos de autor.
- Reformas a la ley de propiedad industrial.
- Reformas a la ley del mercado de valores.
- Reformas a la ley de instituciones de crédito.

Pero lo más relevante para este capitulo, son las reformas en el **Código penal federal**, ya que es aquí en donde se hace énfasis en los tipos de delitos y las penas que pueden darse a estos.

En este código y de acuerdo con las reformas presentadas el 19 de Mayo de 1999, se reformó el Titulo noveno que habla de la revelación de secretos y se adicionó el capitulo II al mismo titulo, que habla de el acceso ilícito a sistemas y equipos de informática, para quedar de la siguiente manera. [4]

TITULO NOVENO
Revelación de secretos y acceso ilícito a sistemas y equipos de informática
CAPITULO I
Revelación de secretos

Artículo 210
Se impondrán 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 algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto.

Artículo 211
La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año, cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado público o cuando el secreto revelado o publicado sea de carácter industrial.

Artículo 211 Bis
A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.

Capitulo II
Acceso ilícito a sistemas y equipos de informática

Artículo 211 bis 1
Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2
Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Artículo 211 bis 3
Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

Artículo 211 bis 4
Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 5
Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Artículo 211 bis 6
Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

Artículo 211 bis 7
Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

Si se realiza el análisis de estos artículos, se puede uno dar cuenta que aun falta mucho en materia informática, además de que hay muchos aspectos que aun no se contemplan en la legislación mexicana.

Tal es el caso de los sistemas no protegidos, es decir, se contempla que será un delito cuando alguien perpetre en un sistema protegido por un mecanismo de seguridad, pero los usuarios comunes o aquellos que no protejan su sistema con un mecanismo de seguridad, quedan fuera de estos artículos o, según la interpretación, puede darse el caso en el que cualquier *"mecanismo"* puede ser tomado como un mecanismo de seguridad.

Es decir no existe una definición de que puede ser considerado mecanismo de seguridad, dejando un gran abismo para la persecución de un caso.

Por esto diversas organizaciones y algunos partidos políticos, han presentado propuestas de reformas, para poder incluir estos aspectos no previstos; pero aun no se han realizado modificaciones al código penal.

Con forme a lo expuesto en los artículos anteriores en el *"código de procedimientos penales de México"* los delitos informáticos quedan clasificados de la siguiente manera.

Los delitos contra la confidencialidad, la integridad o la disponibilidad incluyen :

- El acceso no autorizado; es decir, el acceso sin derecho a un sistema o a una red informática violando medidas de seguridad.
- El daño a los datos o a los programas informáticos, como la descomposición, el deterioro, la supresión de datos o de programas informáticos sin derecho a ello.
- El sabotaje informático, que consiste en introducir, alterar, suprimir datos o programas informáticos, con la intención de obstaculizar el funcionamiento de un sistema de computadoras o de telecomunicaciones.
- La intercepción no autorizada, es decir, la interceptación realizada sin autorización y por medios técnicos, de comunicaciones destinadas a un sistema o a una red informáticas, provenientes de ese sistema o esa red o efectuados dentro de dichos sistemas o red.
- El espionaje informático, es decir, la adquisición, la revelación, la transferencia o la utilización de un secreto comercial sin autorización o justificación legítima, con la intención de causar una pérdida económica a la persona que tiene derecho al secreto o de obtener un beneficio ilícito para sí mismo o para una tercera persona.

2.4.4 PROPUESTAS DE REFORMAS

Para tratar de evitar los llamados huecos existentes en la legislación actual, diversas instancias han presentado propuestas de ley en diferentes áreas.

Actualmente solo existe una propuesta de reforma referente a los delitos informáticos, la cual fue presentada por la Senadora Emilia Patricia Gómez Bravo.

En la exposición de motivos[5] la senadora presenta la necesidad de reformar las leyes para poder estar si no a la par de las legislaciones de otros países, por lo menos en un rango aceptable ya que por el carácter internacional de estos delitos, es necesario que sean legislados para lograr una cooperación internacional.

En esta propuesta de reforma se presenta la necesidad de legislar en lo referente a:

- El fraude electrónico y la falsificación informática.
- Obtención ilícita de servicios de telecomunicaciones.
- Uso ilícito de instrumentos de pago.

En las reformas se contemplan los fraudes electrónicos, delito ya común en estos días y para el cual no existe la correcta regulación salvo en los casos en los que se ven envueltas las instituciones financieras, como esta previsto en la "*Ley de servicios financieros"*.

También se contempla el uso ilegal de servicios, algo muy común entre los usuarios de Internet, que en un gran numero de casos, es usado en conjunto con el fraude electrónico y el uso ilícito de instrumentos de pago.

En resumen y según consta en la propuesta, las reformas serían las siguientes [5]:

Se reforma el Título Decimotercero para adicionar un Capítulo Segundo Bis que se denominará "Falsificación Electrónica" con los artículos 240 Ter y 240 Quáter; se adicionan los artículos 211 Bis 6 y 211 Bis 7, recorriéndose los demás en su orden; se adicionan los artículos 168 Ter y 389 Ter; y se reforma la fracción II del artículo 424 BIS, del Código Penal Federal

Sin embargo hay que recordar que estas aun son propuestas, y hace falta mucho trabajo para que la legislación quede en niveles aceptables.

2.4.5 PROPUESTAS LEGALES ACERCA DE LOS SISTEMAS DE INFORMACION

El problema de la legislación informática en México también tiene que ver con las propuestas hechas para la incorporación de TIC's en el gobierno, ya que no solo se trata de implementar las tecnologías, sino de enseñar la manera correcta para su uso.

Diversos organismos han planteado diferentes propuestas para la incorporación de **TIC's** en el uso cotidiano del sector gubernamental como las propuestas echas por las siguientes instancias:

En el sector público:

- Secretaría de Contraloría y Desarrollo Administrativo.
- Secretaría de Agricultura, Ganadería, Desarrollo Rural, Pesca y Alimentación.
- Secretaría de Salud.
- Secretaría del Trabajo y Previsión Social.
- Comité de Informática de la Administración Pública Estatal y Municipal.
- Asociación Nacional de Investigadores en Informática Jurídica.

En el sector educativo se han hecho propuestas por parte de:

- Universidad de las Américas – Puebla.
- UPIICSA – IPN.
- Asociación Mexicana de Estándares para el Comercio Electrónico, A.C.
- Asociación Nacional de Instituciones de Educación en Informática, A.C.
- Instituto Latinoamericano de la Comunicación Educativa.

En el sector social y privado se han hecho propuestas por parte de:

- Comité de Peritos en Informática y Computación (CIME).
- Federación de Asociaciones Mexicanas en Informática, A.C.
- Cámara Nacional de la Industria Electrónica de Telecomunicaciones e Informática, A.C.

- Consejo Mexicano de la Industria de Productos de Consumo.
- Asociación Mexicana de Estándares para el Comercio Electrónico, A.C.
- Banco Bilbao Vizcaya A / Bancomer, S.A.
- Asociación Mexicana de la Industria de Tecnologías de la Información, A.C.

Entre las propuestas anteriores, cabe destacar las echas por el comité de peritos en informática, ya que su opinión tiene una gran importancia por el conocimiento de las áreas de acción como es lo legal y lo informático.

CAPITULO

3

HERRAMIENTAS DE FORENSIA INFORMÁTICA

3.1 PREVENCION DE INCIDENTES

3.1.2 FIREWALL

El Firewall o también conocido como muro de fuego, suele ser la primera línea de defensa en los sistemas conectados a la red, estos se dividen en:

- Firewall implementado por Software
- Firewall implementado por Hardware

Aunque difieren de sus capacidades y otros aspectos como el rendimiento, el funcionamiento del firewall es el mismo, consiste, en bloquear tráfico proveniente de la red, de acuerdo con reglas establecidas por el administrador de la red o equipo. Se debe tener en cuenta que contar con un firewall no garantiza la protección, ya que el contar con un firewall no representa ninguna seguridad si este se encuentra mal configurado.

La mala configuración de un firewall, no solo es un riesgo potencial de un incidente, sino que también puede implicar que se descarte la estructura del caso. Es decir en el artículo *211 bis* del código de procedimientos penales en México, supone una pena para "*los sistemas que se encuentren protegidos por un mecanismo de seguridad*", lo que podría suponer un recoveco legal para le evasión de la justicia al no encontrarse completamente protegido o mal protegido por un mecanismo de seguridad.

El firewall implementado por software es aquel que no requiere de un equipo especialmente diseñado y dedicado para procesar las directivas, tráfico que entra al sistema o red. Generalmente este tipo de firewall consiste en un software que se instala en el equipo y suelen ser fáciles de configurar para el usuario común; son muy usados en computadoras personales.(figura 3.1)

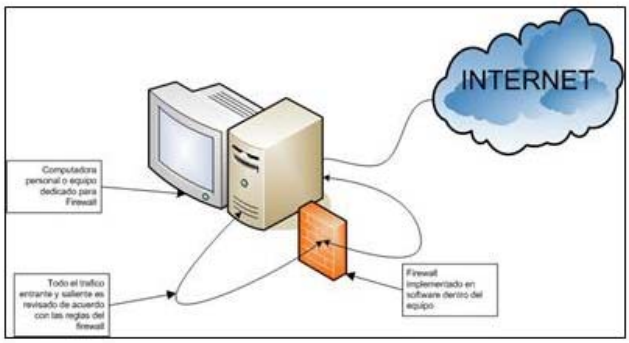


Figura 3.1 Firewall Implementado por software

Este tipo de firewalls generan log's y alertas que son guardadas en el equipo, a salvedad de que el software se encuentre configurado para enviar una copia de los eventos a un servidor central, en cuyo caso será necesario preservar no solo el equipo victima, si no también la integridad del equipo servidor, para evitar alteración a estos registros, además que el contar

con este tipo de logs, permitirá cotejar los datos para dar mayor validez a la información en la estructuración y seguimiento del caso.

Los firewalls implementados por Hardware, consisten en un equipo dedicado únicamente a procesar las directivas de seguridad, además, a diferencia del firewall implementado por software, cuentan con un sistema operativo diseñado para optimizar el rendimiento y la capacidad de procesar las directivas de seguridad. (figura 3.2)

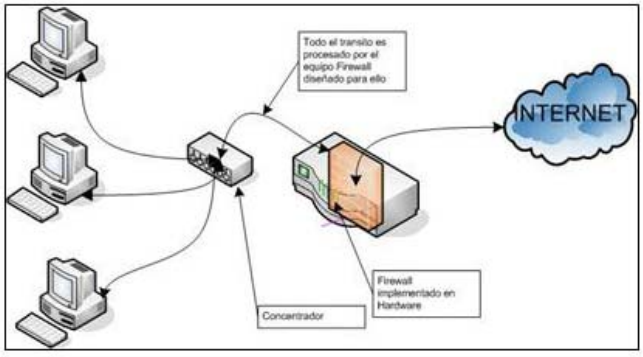


Figura 3.2 Firewall implementado por Hardware

Este tipo de firewalls suele ser mas costoso, pero mas efectivo, sobre todo en redes de gran tamaño, ya que la capacidad de procesamiento que tienen estos dispositivos permite tener un gran numero de equipos conectados a la red, por esta misma razón suelen ser equipos caros y que requieren de instalaciones especiales.

Los firewalls de hardware generan logs o registros de eventos de acuerdo con la configuración de seguridad, estos logs son almacenados en la memoria interna del equipo y, conforme el espacio reservado para esto se satura, los logs son descartados. Pero este tipo de equipos puede ser configurado para enviar los logs directamente a otro equipo dedicado a guardarlos, lo que supone un respaldo y una buena fuente de evidencia en un caso.

3.1.2 SISTEMAS DE DETECCIÓN DE INTRUSOS

En un principio, los firewalls podían ser suficiente, pero con el crecimiento de las redes, la cantidad de información que se generaba, era demasiada para intentar detectar un posible ataque o intento de intrusión a los sistemas, es decir, la cantidad de información sobrepasó la capacidad de los administradores o expertos en seguridad para revisar y detectar patrones que pudieran suponer un ataque.

Por estas razones surgió la necesidad de contar con sistemas que hicieran el trabajo de revisar los logs de la manera más parecida a la que lo haría un experto, estos sistemas fueron los llamados IDS’s, o sistemas de detección de intrusos.

Existe una gran variedad de sistemas de detección de intrusos, aquellos que basados en reglas estáticas, emiten alertas cuando detectan el patrón de un ataque, como lo es el escaneo de puertos mediante peticiones de conexión no completadas, hasta sistemas IDS’s

basados en inteligencia artificial que son capases de aprender y reducir el numero de alertas falsas.

Los sistemas de detección de intrusos suelen ser implementados en Hardware, pero también existen implementaciones en software que suponen un menor costo o quizás, solo, una segunda línea de defensa.(figura 3.3)

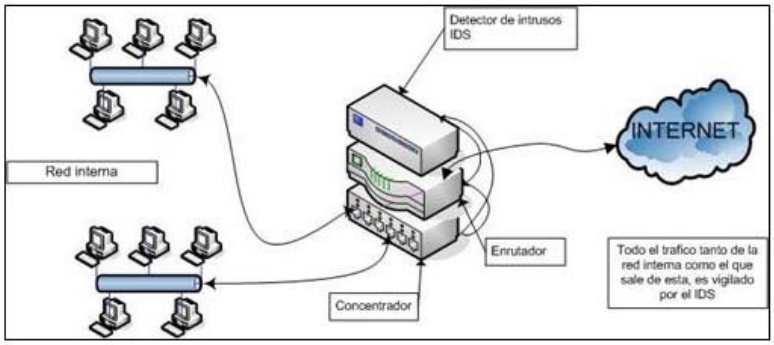


Figura 3.3 Sistema detector de intrusos IDS

Como se mencionó en el capítulo dos, un ataque tiene un patrón, los IDS's son capaces de detectar escaneo de puertos de diferentes tipos, e incluso cuando trabajan como un firewall o en conjunto con uno, generar nuevas reglas para evitar el riesgo de un incidente. Algunos IDS's son capases de detectar mediante sistemas heurísticos, el comportamiento de algunos tipos de virus, bloqueando su acceso a la red.

Compañías como ***Symantec***, proveen actualizaciones para sus sistemas de detección de intrusos para incorporar los nuevos tipos de ataques y formas de propagación que usan los virus.

Los IDS's pueden ser usados como Firewalls o interactuar con estos; la manera en la que los registros de accesos son generados por estos es similar, solo que los IDS's filtran la información para presentar aquella que es de mayor relevancia para los administradores, guardando también un registro de todos los sucesos detectados, esto con la finalidad de no descartar ninguna información que pueda ser útil posteriormente.

Existen sistemas IDS's que son capases de desplegarse en toda la red por lo que también son conocidos como **NIDS,** es decir, existe un ***agente***[26] en cada equipo de la red que reporta al sistema central sobre algún tipo de actividad sospechosa en el equipo, lo que puede no solo detectar un ataque a un solo equipo, si no permite detectar un posible ataque a toda la red, de manera distribuida o solo con la finalidad de cubrir el ataque.

Es decir, algunos sistemas no detectarían como un posible ataque el escaneo de servicios en equipos diferentes, o la transferencia inusual de información entre equipos de la misma red.(figura 3.4)

[26] **agente**: Programa basado en inteligencia artificial con un propósito específico y capas de aprender.

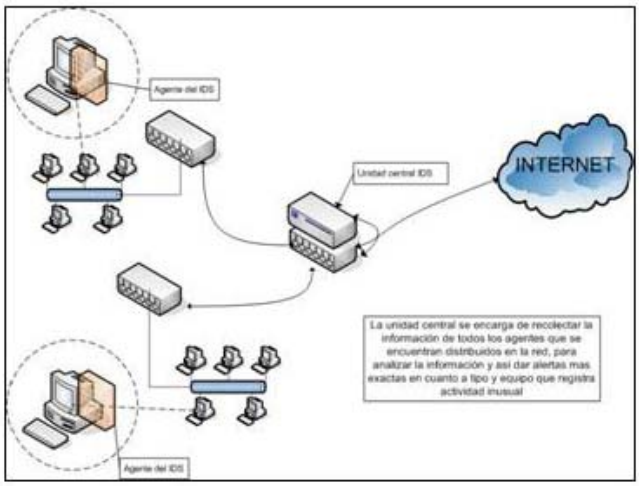


Figura 3.4 Sistema de detección de intrusos distribuido NDIS

Algunos de los sistemas IDS's mas conocidos y de mayor reputación son:

- Sistemas Firewall y IDS's de la compañía Cisco Systems
- GFI LANguard
- La familia de productos de Internet Security Systems (ISS)
- Familia de productos de Network-1 Security Solutions
- Tripwire, uno de los más conocidos que cuenta con una versión libre que se mostrará mas adelante.

Pero los sistemas IDS's no son la panacea de la seguridad informática, ya que al ser sistemas computacionales, se encuentran dentro de ciertos limites de razonamiento automatizado, por lo que los atacantes también han desarrollado técnicas para burlar algunos de estos sistemas de detección de intrusos.

Este tipo de técnicas no solo supone que el atacante es una persona con amplios conocimientos de las TIC's, sino que también exige una gran capacidad de análisis por parte del administrador de la red y los encargados de la seguridad.

3.1.3 SISTEMAS ANTIVIRUS

Los sistemas antivirus son uno más de los elementos necesarios para considerar completo un esquema de seguridad, sobre todo en el aspecto de prevención.

También es una fuente de evidencia, sobre todo en los casos en que exista pérdida por parte de la compañía o el empleado y se quieran deslindar responsabilidades. Por ejemplo, si se cuenta con un sistema antivirus centralizado se generaran log's sobre los virus encontrados en el equipo, como es el caso de aquellos que accedan a la red por medio del correo electrónico.

Esto debido a que en algunas compañías se considera quebrantamiento de las políticas de seguridad el que los empleados abran correos electrónicos infectados por algún tipo de virus, más aun, cuando el virus introducido en la red corporativa provoca perdidas, los log's almacenados por el sistema antivirus en conjunto con los generados en los servidores de correo, servirán para deslindar responsabilidades de estos incidentes.

3.2 VERIFICADORES DE INTEGRIDAD

Los verificadores de integridad suelen ser programas que validan y alertan sobre la modificación de archivos en el sistema. Esto supone que si los archivos son modificados de manera no autorizada, existe un comprometimiento del sistema.

Estos sistemas se basan principalmente en métodos matemáticos que generan un numero o secuencia alfanumérica única para cada archivo, es técnicamente imposible que dos archivos cuenten con la misma marca numérica, lo que hace este método muy confiable, además de que la alteración de un solo bit en el archivo provoca que la marca numérica se modifique.

Los verificadores de integridad también sirven para determinar si la copia generada en la investigación no ha sido alterada del original, además de que las fechas de modificación del archivo también generan cambios en la marca, lo que hace indispensable este tipo de herramientas para dar validez a la información recaba en el caso y para las empresas representa una medida de seguridad sobre su información confidencial, ya que nadie podría acceder a esta información sin modificar la marca.

La mayoría de los programas para la recolección de evidencias y los Kits de herramientas generan automáticamente las cadenas de verificación o MD5 de los archivos recolectados, así como, de las imágenes de los discos. Por lo que solo se hablará de los verificadores de integridad mas conocidos.

3.2.1 md5sum

En realidad md5sum es un programa incluido en Linux, el cual genera cadenas de verificación en base al algoritmo MD5, este algoritmo se encuentra descrito con detalle en el RFC 1321.

A sabiendas de que es teóricamente imposible que dos archivos tengan la misma firma MD5, el programa está diseñado para poder comprobar la integridad de un archivo, es decir, constatar que los archivos no han sido modificados, ya que la más mínima modificación en el archivo producirá una firma diferente.

Aunque este fue un programa diseñado originalmente para sistemas Linux, existen programas para Windows que realizan la misma función.

Para usar en Linux, la sintaxis es la siguiente:

#md5sum [*OPCION*] [ARCHIVO]

Este comando crea la cadena MD5 para el archivo y con base en las opciones dadas.

#**md5sum** [*OPCION*] *--check* [ARCHIVO]

Este comando genera la cadena MD5 y la compara con la cadena en el archive dado, esta es la opción que comprueba la integridad del archivo

Las opciones con las que se puede combinar el comando se muestran en la tabla 3.1

-b, **--binary**	Lee los archivos en formato binario.
-c, **--check**	Checa las sumas MD5 contra una lista dada
-t, **--text**	Lee los archivos en modo texto
--status	No muestra ninguna salida, devuelve un código de estatus
-w, **--warn**	Advierte acerca de líneas MD5 mal formadas
--help	Muestra la ayuda
--version	Muestra la versión del programa y sale

Tabla 3.1 Opciones de ejecución del programa md5sum

Existe un programa diseñado para el sistema operativo Windows que genera las sumas MD5, **md5summer** programado por *Luke Pasco;,* el uso de este programa es muy simple, el programa nos da la opción de crear sumas o de verificarlas, podemos seleccionar un directorio completo o un archivo para generarlas y una vez generadas el programa preguntará por un nombre de archivo y una ubicación para guardar el archivo. Véase figura 3.5

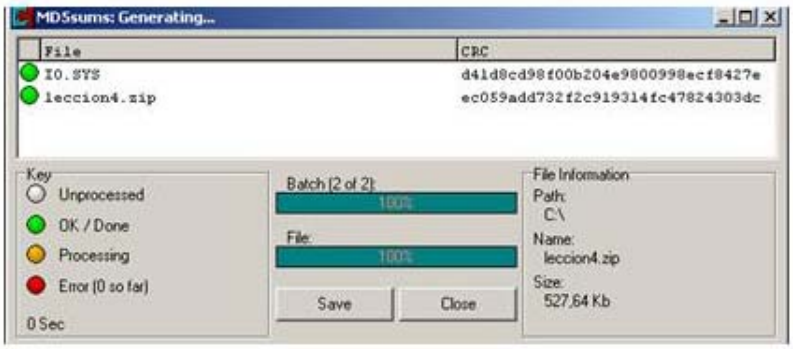


Figura 3.5 MD5summer

Para la verificación de las cadenas, el programa preguntará por la ubicación del archivo *.MD5 que contiene las cadenas a verificar y realizará la comparación correspondiente, la estructura de los archivos MD5 se muestra en la figura 3.6

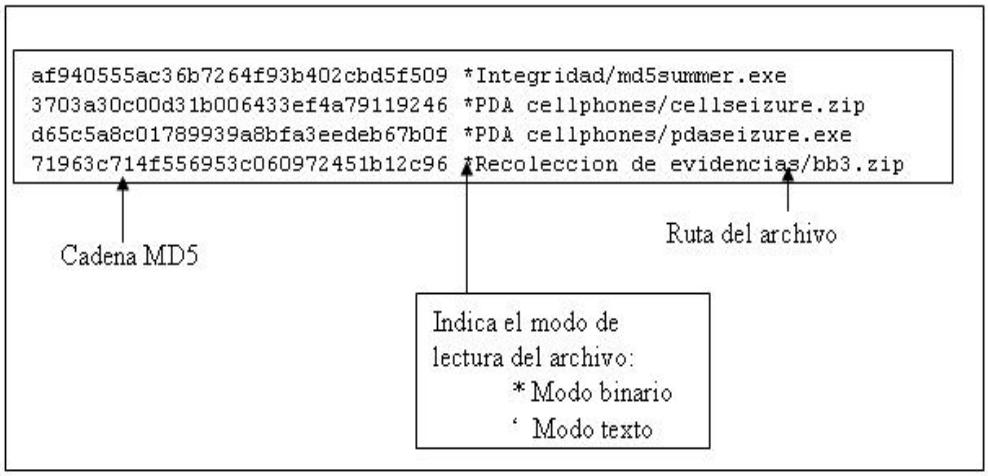


Figura 3.6 Formato del archivo generado por el MD5summer

Nota: El formato usado por el md5sum de Linux y el programa MD5summer para Windows es el mismo.

3.2.2 Sumas de verificación

Además de los programas anteriores, cabe destacar que en los sistemas informáticos existen muchos mecanismos de sumas de verificación, los cuales trabajan en complemento con otros programas y que por lo tanto su funcionamiento no es visible para el usuario.

Tenemos entre los mas usados el Código de Redundancia Cíclica (CRC), incluido en los sistemas de archivos para comprobar el tamaño en sectores de los archivos, además de que muchos programas incluyen una rutina de CRC para comprobar que el archivo no ha sido alterado por algún programa externo tales como virus o por ingeniería inversa.

Es importante tener en cuenta esto, ya que en el transcurso de la recolección de la información, en más de una ocasión puede aparecer un mensaje haciendo alusión a este código, sobre todo en los sistemas Windows, esto es debido generalmente a que existen sectores dañados en el disco duro.

En los programas es poco común que se den problemas de este tipo, pero de darse, es una clara evidencia que el archivo ha sido alterado o se le ha aplicado algún tipo de reingeniería. Más adelante se hablará de la reingeniería como método para obtener evidencias en ciertos casos.

3.3 HERRAMIENTAS PARA LA RECOLECCIÓN DE EVIDENCIAS

En esta sección se presentan algunas de las herramientas usadas para obtener evidencias o información que pueda ser considerada como tal, cabe destacar que la mayoría de las herramientas son usadas en conjunto con otras por lo que muchas son integradas dentro de los tool kits, o como parte de los Live Boot CDs, a continuación solo se mostrarán algunos de los mas destacados.

3.2.3 Fatback

Este es un programa diseñado para correr en sistemas Linux y FreeBSD, es usado para recuperar archivos de sistemas FAT incluyendo FAT12, FAT16 y FAT 32 incluye soporte de nombres largos, puede restaurar directorios completos y recuperar cadenas de clusters perdidos, así mismo puede trabajar con particiones o con discos completos.

El programa FatBack fue desarrollado inicialmente por los laboratorios de forensia informática en el departamento de defensa de los estados unidos y fue utilizado en un principio solo para investigaciones del gobierno. Posteriormente fue hecho público y se facilitó el uso para todo tipo de investigaciones referentes a los delitos informáticos.

Este programa supone un conocimiento de la manera en la que el sistema de archivos FAT funciona, así como cuales son los parámetros que este tiene.

El uso de este programa seria el siguiente:

/fatback [FILE] -l [LOG] [OPTION]

Las opciones modificadoras que podría tener este programa se muestran en la tabla 3.2

-o, --output=DIR	Especifica un directorio para los archivos de salida.
-a, --auto	Auto-recuperación de archivos, de manera no interactiva.
-l, --log=LOGFILE	Especifica un archive para guardar el log generado por el programa.
-v, --verbose	Muestra información extra en la pantalla mientras realiza la recuperación.
-p, --partition=PNUM	Va directamente a la partición especificada por PNUM
-d, --delprefix=PREFIX	Usa PREFIX como marca para los archivos borrados .
-s, --single	Fuerza el modo de solo una partición.
-z, --sectsize=SIZE	Ajusta el tamaño del sector el default es 512
-m, --mmap	Usa la función mmap() para mejorar el performance I/O para los archivos.
-h, --help	Muestra la ayuda

Tabla 3.2 Opciones del programa FatBack

3.2.4 Memdump

Este es un programa para sistemas basados en Unix y Linux, este programa tiene el propósito de hacer una descarga de la memoria o *dump*, consiste en mandar a un archivo toda la información residente en memoria.

Esto puede ser usado para tratar de conservar evidencia que se encuentre en ese momento en la memoria RAM y que en no se almacena en ningún otro lugar.

Cabe destacar que en la memoria que se descarga al archivo se encontrara información del sistema operativo, librerías que se estén ejecutando, programas, etc. Por lo que la información deberá ser revisada exhaustivamente para descartar lo que no sea de utilidad para la investigación.

El uso de esta herramienta puede ser desde un dispositivo de almacenamiento externo como un floppy, una vez descomprimido construido el ejecutable la sintaxis puede ser la siguiente y las opciones se muestran en la tabla 3.3

#memdump [opciones]

-b [tamaño]	Se usa para modificar el tamaño del buffer de memoria
-k	Se usa para realizar un dump de la memoria del Kernel además de la memoria física
-m [archivo]	Se usa para imprimir el mapa de memoria
-p [tamaño]	Se usa para modificar el tamaño de la pagina de memoria
-s [tamaño]	Se usa para determinar el tamaño del dump de memoria, por default todo.
-v	Se usa para mostrar en pantalla lo que el programa esta realizando

Tabla 3.3 opciones del programa memdump

Aparte de lo anterior la salida a un archivo puede ser dirigida a una conexión de red, por ejemplo con netcat:

#memdump | nc host port

O con un cliente ssl :

#memdump | openssl s_client -connect host:port

En el uso de este programa y de muchos otros de este tipo existe un problema, que es referente a la integridad de la información, ya que para poder realizar el *dumping* de la memoria, se deberá de mantener funcionando el sistema y se deberá tener un medio distinto a los medios primarios del sistema para almacenar la información generada, esto puede suponer la conexión de discos portátiles o de transferencia de la información por medio de una red.

Debido a lo anterior, el uso de esta herramienta debe de ser estudiado dependiendo si las condiciones lo ameritan, es decir si se espera encontrar información relevante, para la investigación.

3.2.5 dump drive

Esta es una de las herramientas mas poderosas y es usada tanto por el gobierno americano, como por investigadores de todo el mundo. Originalmente diseñada para ejecutarse en sistemas Linux y UNIX, pero, es capas de realizar copias exactas de discos duros y particiones de todo tipo de sistemas operativos.

Este programa puede ser usado desde sistemas Live boot, debemos tomar en cuenta que realiza una copia exacta del disco duro, por lo que el espacio necesario para almacenar los archivos de salida es considerable, se recomienda un disco duro extra de por lo menos 20 GB para realizar una investigación, en investigaciones que lo requieran se deberá optar por la opción de ***storage servers***[1].

El uso **dd** seria:

#dd [opciones]

Las opciones con las que cuenta este programa son muchas y pueden ser usadas de manera combinada, véase tabla 3.4

--help	Muestra la ayuda del programa.
--version	Muestra la versión del dd.
if=fichero	Lee de un archivo en vez de leer de la entrada estándar.
of=fichero	Escribe en un fichero en vez de la salida estándar a menos que se de la opcion **conv=notrunc**, que truncara el fichero al tamaño especificado por **seek** que seran 0 bytes si **seek** no se da.
ibs=bytes	Lee bytes por vez.
obs=bytes	Escribe bytes por vez.
bs=bytes	Lee y escribe bytes por vez y tiene prioridad sobre **ibs** y **obs.**
cbs=bytes	Convierte bytes por vez.
skip=bloques	Se salta bloques de tamaño determinado por **obs** al comienzo de la salida.
seek=bloques	Se salta bloques de tamaño determinado por **obs** al comienzo de la salida.
count=bloques	Solo copia bloques de entrada del tamaño determinado por **ibs.**
conv={opcion}	Convierte el fichero según los argumentos dados. Las opciones de este argumento se muestran en la tabla 3.5

Tabla 3.4 Opciones de *dump drive*

Los argumentos para la opción **conv** son:

ascci	Convierte EBCDIC a ASCII.
ebcdic	Convierte ASCCI a EBCDIC.
ibm	Convierte ASCII a un EBCDIC alternativo.
block	Para cada línea de entrada saca el numero de bytes especificados por **cbs**, remplazando el salto de línea de la entrada con un espacio.
unblock	Remplaza espacios del fin de bloques del tamaño determinado por **cbs** en la entrada por un salto de línea.
lcase	Cambia las letras en mayúsculas a minúsculas.
ucase	Cambia las letras minúsculas a mayúsculas.
swab	Intercambia cada par de bytes de la entrada.
noerror	Continua aun después de que se produzcan errores de lectura.
notrunc	No trunca el fichero de salida.
Sync	Rellena cada bloque de entrada de tamaño determinado por **ibs** con valores nulos al final.

Tabla 3.5 modificadores de la opcion **conv** de *dump drive*

Además de las opciones anteriores se puede combinar para que el archivo de salida se transfiera a través de la red con conexiones ssl o con netcat.

3.2.6 dcfldd

Este programa es en realidad una modificación del **dd** hecha por los laboratorios del departamento de defensa de los estados unidos. Su desarrollo sirvió para apoyar y sustentar las investigaciones del departamento de defensa, en la actualidad ha sido puesto a disposición de todos los investigadores de delitos informáticos.

Ya que es una variante del *dump drive*, los comandos son los mismos así como las opciones, uno de los cambios mas visibles el la generación automática de cadenas MD5, además de esto tiene mejoras en las librerías y otras funciones usadas en la ejecución del programa.

3.2.7 Forensic Replicator

Esta herramienta complementa la recolección de evidencias, ya que es capaz de generar imágenes de discos duros y de otros dispositivos como los CD y los floppy, además de poder clonar los discos a partir de un archivo imagen.

Esta herramienta está diseñada para ejecutarse en sistemas Windows y es parte de una serie de programas diseñados por la compañía **Paraben,** para las investigaciones de tipo criminal. Su uso es intuitivo, a través de sus menús es fácil realizar las funciones de clonación y creación de archivos imagen. Véase figura 3.7

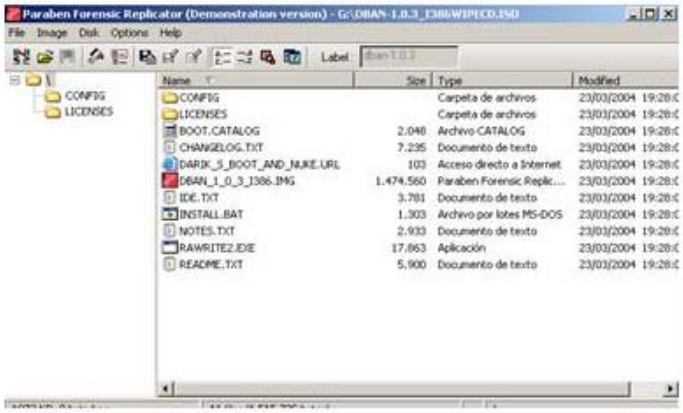


Figura 3.7 Paraben Forensic Replicator

3.2.8 TCPDUMP

Como su nombre lo dice, este programa está diseñado para realizar un *dump* de los paquetes que atraviesan una red, un muy potente *sniffer*, puede capturar trafico en base a filtros, por ejemplo, capturar solamente el tráfico *ARP.*

Originalmente fué creado para ejecutarse en sistemas basados en Unix y se distribuye bajo la licencia GNU, lo que indica que puede ser copiado y usado libremente, esto también implica la existencia de mucha información sobre esta aplicación, módulos nuevos y actualizaciones.

Para poder ejecutar este programa se requieren permisos de administrador o superusuario, o que el programa este elevado a nivel de root (*seguid*), para ejecutarlo es necesario contar con la librería lib-cap, una ves compilado e instalado, bastará con mandarlo a llamar desde la consola.

```
#tcpdump [ -adeflnNOpqRStuvxX ] [ -c count ] [ -F file ] [ -i interface ]
 [ -m module ] [ -r file ] [ -s snaplen ] [ -T type ] [ -U user ] [ -w file ]
 [ -E algo:secret ] [ expression ]
```

El uso de esta herramienta suele volverse mas complejo a medida que se usa y las opciones con las que puede ser usado son muchas, así que solo se presentan las opciones y uso básico de este programa.

-a	Intenta convertir las direcciones de red y de broatcast a nombre.
-c	Sale después de recibir paquetes *count.*.
-d	Hace un *dump* en formato legible de los paquetes coincidentes compilados.
-dd	Hace un *dump* de los paquetes coincidentes como fragmento de código de un programa en **C**.
-ddd	Hace un *dump* de los paquetes coincidentes en formato decimal
-e	Imprime la cabecera del nivel de enlace en cada línea.
-E	Usa *algo:secret* para desencriptar los paquetes IPsec ESP. Los algoritmos pueden ser **des-cbc**, **3des-cbc**, **blowfish-cbc**, **rc3-cbc**, **cast128-cbc**, o **ninguno**. El algoritmo default es **des-cbc**. Para que esta opción este presente *tcpdump* debe ser compilado con la opción de criptografía activada. Esta opción es

	experimental aun y es solo con propósitos de prueba ya que implica riesgos de seguridad en el uso del comando.
-f	Imprime direcciones de Internet externas en forma numerica o simbólica.
-F	Usa a *file* como la entrada para los filtros normalmente definidos en expresiones en el comando, cualquier otra opción dada será ignora.
-i	Escucha en la interfase especificada por *interfase*. Si no se especifica se toma la primera interfase activa en la numeración del sistema ignorando el loopback. En algunas versiones Linux con kernel 2.2 se puede usar la opción *any* para escuchar en todas las interfaces.
-l	Imprime una salida con un buffer, es útil si se quiere ver la información mientras se captura.
-n	No convertir las direcciones a nombres. Se puede usar par evitar las búsquedas de DNS.
-nn	No convertir el protocolo o los números de protocolo a nombres.
-N	No imprimir los nombres de dominio si no solo los nombres de host.
-m	Cargar el modulo de definiciones SMI MIB del archivo *modulo*. Se puede usar varias veces para cargar diversos módulos MIB.
-O	No ejecuta el optimizador de paquetes coincidentes.
-p	No poner la interfase en modo promiscuo.
-q	Imprime información corta, por lo que la información presentada por línea es menor.
-r	Lee los paquetes de un archivo creado con la opción –w, la entrada estándar es usada si el archivo dado es "-".
-R	Asume que los paquetes son del protocolo ESP/AH (RFC1825 a RFC1829).
-s	Captura un numero dado de bytes por cada paquete, el dafault son 68 bytes y es adecuado para la captura de paquetes IP, ICMP, TCP y UDP.
-S	Imprime los números absolutos de la secuencia TCP en lugar de los relativos.
-t	No imprime el sello de tiempo en cada línea.
-tt	Imprime un sello de tiempo sin formato en cada línea.
-ttt	Imprime un delta (en microsegundos) entre cada línea.
-tttt	Imprime un sello de tiempo con formato estándar precedido por la fecha en cada línea.
-U	Descarta los privilegios de root y cambia el identificador de usuario a usuario y grupo del grupo primario del usuario.
-T	Fuerza que los paquetes seleccionados por la expresión sean interpretados como de un tipo específico. Los formatos conocidos son **cnfp** (Cisco NetFlow protocol), **rpc** (Remote Procedure Call), **rtp** (Real-Time Applications protocol), **rtcp** (Real-Time Applications control protocol), **snmp** (Simple Network Management Protocol), **vat** (Visual Audio Tool), and **wb** (distributed White Board).
-u	Imprime los manejadores NFS sin codificar.
-v	Salida de información simple.
-vv	Salida de información mas completa.
-vvv	Salida de aun más información, como las opciones de Telnet.
-w	Escribe los paquetes capturados a un archivo después pueden ser mostrados usando la opción –r
-x	Imprime cada paquete en formato hexadecimal.
-X	Cuando imprime hexadecimal imprime ASCII también.

Tabla 3.6 Opciones de TCPdump

En resumen, este es una de las herramientas de análisis y de captura de información en los ambientes u incidentes que involucran redes, ya que permite la captura de información a un archivo para su posterior análisis, también es compatible con los archivos generados por algunos IDS's como *Snort*.

3.2.9 Ethereal

Este es un analizador de protocolos, también puede ser considerado como un sniffer, una de las mayores ventajas de este analizador es que cuenta con una interfase gráfica para su uso lo que facilita el análisis de la información en el instante.

Ethereal puede abrir y analizar archivos generados por diversos programas entre ellos *TCPdump* y *snoort*, también puede reconstruir una *conversación* de paquetes TCP y mostrar todo el contenido ASCII, EBCDIC o hexadecimal. También se pueden crear filtros o usar los ya preestablecidos para el análisis de los paquetes. (Figura 3.8)

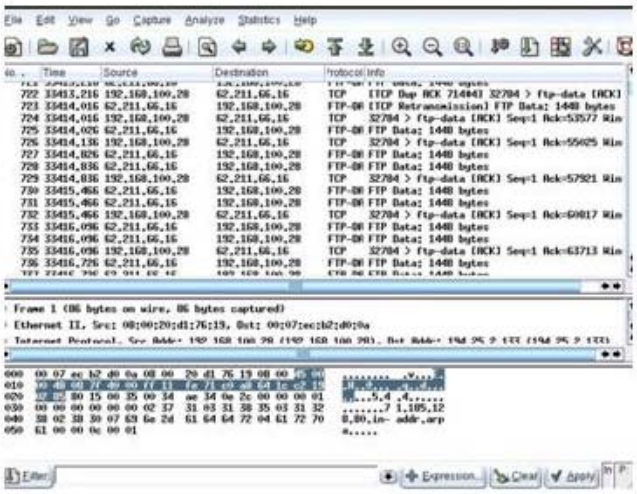


Figura 3.8 Etheral

Ethereal cuenta con la opción de generar filtros y analizar los paquetes de un archivo de tal forma que puede mostrar el tipo de paquete en base a su protocolo y el tipo de puerto al que estaba dirigido el paquete.

Esta es una herramienta indispensable para el análisis de incidentes en los que se cuenta con información generada por *sniffers* o programas de detección de intrusos.

-B	Establece la altura inicial para la vista de los bytes.
-c	Establece el número de paquetes a capturar.
-f	Establece la expresión del filtro de captura.
-h	Imprime la versión, las opciones y sale del programa.
-i	Estable el nombre la interfase de red que se usara para la captura de paquetes, este nombre debe de coincidir con uno de los mostrados con el comando **netstat –i** o **ifconfig** –a.

-k	Inicia la inmediatamente la captura de paquetes, se usa la interfase especificada si no se da una interfase para la captura ethereal busca y toma la primera interfase activa, descartando el loopback.
-m	Establece el nombre de la fuente usada por ethereal.
-n	Desactiva la resolución de nombres de equipos y de puertos.
-p	No pone la interfase en modo promiscuo.
-P	Estable el tamaño de la lista de paquetes a mostrarse.
-Q	Sale inmediatamente después de terminar la captura, es util cuando se programan capturas de datos, esta opción requiere del uso de **–i** y **–w.**
-r	Lee los paquetes de un archivo.
-R	Cuando lee de un archivo con la opción **–r** aplica las opciones establecidas por esta opción, los paquetes que no cumplan con la regla no son mostrados.
-S	Estable que se realizara una captura “en vivo” y que los paquetes serán mostrador inmediatamente después de ser capturados.
-s	Establece el tamaño de los paquetes a ser mostrados en una captura “en vivo” ningún paquete que exceda este tamaño será mostrado o guardado.
-T	Establece el tamaño inicial de la vista de árbol.
-t	Establece el formato del sello de tiempo mostrado en la venta de paquetes. El formato puede ser `r' (relativo), `a' (absoluto), `ad' (absoluto con fecha), o `d' (delta). El tiempo relativo es el tiempo transcurrido entre el primer paquete y el paquete actual. El tiempo absoluto es el tiempo en el que el paquete fue capturado sin mostrar la fecha; el tiempo absoluto y la fecha son el tiempo actual y la fecha en la que el paquete fue capturado. El tiempo delta es el tiempo en el que el paquete anterior fue capturado. La opción default es el tiempo relativo.
-v	Imprime la versión y sale.
-w	Establece el nombre del archivo para guardar la captura.

Tabla 3.7 Opciones de Ethereal

3.4 KIT’S DE HERRAMIETAS Y LIVE BOOT

Cuando se comenzó a dar importancia a la investigación de los delitos informáticos también surgió la necesidad de contar con herramientas mas robustas que permitieran ahorro de tiempo en la investigación y recolección de evidencias, por lo que surgieron los Kits de herramientas y los llamados sistemas Live boot, que incorporan herramientas como *dump drive, ethereal, TCPdump, netcat, etc.* Aquí se muestran algunas de estas herramientas.

3.4.1 The Coroner's Toolkit (TCT)

Este kit de herramientas es uno de los más completos y esta diseñado para el análisis de incidentes en sistemas Linux, a pesar de no contar con una herramienta que cree imágenes de discos duros es una de las mejores opciones para los investigadores de las empresas y si se usa de manera adecuada es muy útil en investigaciones criminales.

Las herramientas incluidas en este kit están escritas en C y perl, lo que les da mayor portabilidad, cabe destacar que las herramientas que se incluyen no son convencionales ya que realizan análisis de aspectos que otras herramientas no toman en cuenta, como son los tiempos de acceso a los archivos y modificaciones por medio de las librerías

Grave-robber

Este programa es el soporte para otras herramientas y durante su ejecución llama diversas rutinas en Perl la mayoría residentes en el directorio Lib. Una de las razones por las que ejecuta rutinas en Perl es para no realizar ejecuciones sobre el Shell y en caso de ser necesaria la ejecución de comandos en el shell estas son logueadas así como la hora y fecha en el que fueron ejecutados.

Por default grave-robber captura o intenta capturar la mayor cantidad de información posible, como el estado de los dispositivos, conexiones de red, además de buscar los archivos de logs críticos como son los de configuración. Cabe destacar en este punto que grave-robber puede ser usado en sistemas que se encuentran ejecutando ("Live") o en archivos de imágenes de discos duros es decir, se puede ejecutar sobre sistemas pasivos o activos.

Un punto que se debe de tener en cuenta es el que grave-robber realizará diversas búsquedas sobre el sistema de archivos, búsquedas que pueden tardar mucho tiempo y en ciertos casos retrasar la investigación por lo que se hace hincapié en la importancia de trabajar con copias de la evidencia y por su puesto nunca sobre la evidencia original.

La ejecución de grave-robber seria la siguiente

#grave-robber [DIRECTORIO] [OPCION]

Por default si no se da el parámetro DIRECTORIO, grave-robber se ejecutará sobre la raíz del sistema "/" y las opciones con las que se puede usar se muestran en la tabla 3.6

Grave-robber genera diversos archivos, los cuales contienen información como los MACtimes, logs de los comandos ejecutados por todos los subprogramas llamados por el mismo programa, cadenas MD5 para los programas ejecutados y para algunos de los archivos analizados.

Los archivos generados por este programa se presentan en la tabla 3.8

command_out	Es un directorio y contiene la salida generada por todos los programas ejecutados por grave-robber, cada archivo es nombrado en base a el comando ejecutado además se genera una cadena MD5 para la salida del archivo, una firma de tiempo (timestamp) del momento en el que el programa fue ejecutado y es guardado con la extensión ".MD5".
strings_log	Es la salida del comando strings en cada directorio. Esto puede revelar nombres de archivos eliminados.
body	Es la base de datos de MACtime.
body.S	Contiene los atributos para todos los archivos SUID en el mismo formato de los mactimes.
coroner.log	Contiene el día y la fecha de todos los programas ejecutados por grave-robber y se encuentra en el directorio principal.

error.log	Contiene los errores generados por grave-robber y se encuentra en el directorio principal.
deleted_files	Este directorio contiene todos los archivos que fueron borrados pero aun continúan ejecutándose en el momento de la ejecución de grave-robber.
pcat	Este directorio contiene una imagen de todos los procesos que se estaban ejecutando en el momento de la ejecución de grave-robber. También se puede encontrar historiales de los comandos ejecutados en el shell, además de que algunos programas almacenan en la memoria as direcciones IP de los últimos accesos recibidos.
conf_vault	En este directorio se recopila un conjunto de archivos que grave-robber considera de interés como son archivos de configuración, archivos críticos como logs,etc.

Tabla 3.8 Archivos generados por *grave-robber*

MACtime

Cada acción que se realiza sobre un archivo en sistemas Linux o Unix modifica los valores conocidos como mtimes, atimes, y ctimes de aquí en adelante MACtimes. Estos valores se refieren a la fecha de la ultima modificación de un archivo y son una de las herramientas mas poderosas en la reconstrucción de la escena del incidente, para los investigadores del crimen proporciona una idea de la manera en la que los hechos ocurrieron y para los expertos en seguridad es la guía para reparar los errores.

MACtime depende de la base de datos creada por *grave-robber*, por lo que primero se deberá ejecutar este programa, posteriormente es muy sencillo usar MACtimes.

```
#mactimes dd/mm/yy
```

La información devuelta por mactime consiste en los archivos que han sufrido algún tipo de modificación desde la fecha dada y tiene el formato mostrado en la figura 3.7

```
(date      time     size   MAC   perms    owner    group   file)

  [....]
  Apr 05 99 04:05:00 5506499 m.. -rw-rw-rw- root     mailman /var/log/syslog.7
  Apr 10 99 04:05:00 6389017 m.. -rw-rw-rw- root     mailman /var/log/syslog.6
  Apr 12 99 01:04:39    3978 .a. -rw------- root     mailman /var/log/arclog
  Apr 12 99 14:10:15    3978 m.c -rw------- root     mailman /var/log/arclog
  [....]
```

Figura 3.7 Formato de *mactime*

Al usarse de manera correcta *mactimes* puede ayudar a virtualmente reconstruir los eventos que tuvieron lugar durante el incidente.

unrm

Este pequeño programa es complemento para la herramienta *Lazarus*, su función es separar el espacio "libre" del disco duro en un solo archivo, con la finalidad de que pueda ser analizado más fácilmente en búsqueda de archivos borrados o cadenas de texto.

Lazarus

Es un programa que intenta "resucitar" los archivos, es decir, busca archivos que hayan sido borrados y trata de restaurarlos en una ubicación alternativa, Lazarus puede buscar archivos en el espacio no particionado así como en la memoria y la partición de intercambio.

Esta compuesto principalmente de dos partes, una la que lee los datos del área especificada y otra la que se encarga de diseccionar y analizar la información mostrando los resultados de la búsqueda.

Para ejecutar esta herramienta no es necesario tener privilegios de administrador, pero si se desea acceder a la memoria, partición swap o arreglos de disco, es necesario tener estos privilegios ya que la mayoría de estas áreas solo son accesibles por el súper usuario.

Los archivos generados por *dump drive* pueden ser usados como entrada para esta herramienta y si se combina con *unrm* los resultados son mejores. A pesar de que este programa fue diseñado y probado para sistemas de archivos FAT, UFS, EXT2, NTFS, puede ser usado en todo tipo de sistemas de archivos con buenos resultados.

Antes de ejecutar *Lazarus* debemos tomar en cuenta que realizará una búsqueda sobre el espacio libre del disco duro, por lo que puede generar una salida de datos mayor a ese espacio libre, es decir, si se va a ejecutar *Lazarus* en un disco duro el cual tiene 8 GB de espacio libre, se recomienda contar con un disco que tenga mas de 8GB libre para los datos recolectados por el programa.

La manera común de ejecutar este programa es primero ejecutar *unrm* y posteriormente *Lazarus*, esto podria hacerse de la siguiente forma:

```
#./unrm /dev/sda1 | dd count=10000 bs=1024 > archivo_de_salida
```

Con el comando anterior aremos que *unrm* cree un archivo de 10 MB usando *dump drive* para posteriormente ser analizado con *Lazarus*:

```
#./lazarus –h archivo_de_salida
```

Esto creará dos directorios "www" en donde en formato HTML, se guardaran los resultados generados por *Lazarus*. Las opciones con las que lazarus puede ser usado se muestran en la tabla 3.9

-1	Lee y procesa un byte por vez, no es muy común pero es útil cuando se examina la memoria.
-b	No escribir los bloques binarios, por defecto los escribe.
-B	No escribir ningún bloque binario, por default escribe todos.
-d	Activa el modo de depuración
-h	Emite la salida en código HTML en ligar de texto ASCII, tiene como salida tres archivos, el archivo de datos, el archivo de menú y el framework.
-H directorio	Guarda el código HTML en el directorio actual
-D directorio	Escribe los bloques de datos en el directorio del mismo nombre
-t	No escribir bloques de texto no reconocidos, por default los escribe
-T	No escribir ningún bloque de texto.
-w directorio	Usa este directorio para escribir todo el código HTML

Tabla 3.9 Opciones de Lazarus

Lazarus es una herramienta muy potente en la recolección de evidencias si se le ocupa adecuadamente, además por incluir firmas MD5, es fácil validar la información.

3.4.2 Byte Back

Es un programa diseñado para realizar copias de discos duros o algún otro tipo de medio, es usado para recolectar evidencias y fue desarrollado por la empresa *Tech Assist* y es de tipo comercial, lo que supone la adquisición de una licencia para su uso.

Algunas de las opciones con las que cuenta esta herramienta son:

- Clonar o copiar
- Analizar
- Editar medio
- Borrar medio
- Pruebas de superficie

Clonar o copiar

Esta opción nos permite clonar el disco o medio en el que se esta trabajando, por razones de seguridad es preferible para la investigación primero realizar una copia exacta del disco duro y posteriormente una copia a archivo usando compresión, esto nos permitirá contar con un respaldo, a la ves tener la evidencia en un espacio mas reducido y de mas fácil transportación, tomado en cuenta de que cada archivo que se genere contará con su firma MD5 para su validación posterior.

Analizar

La opción de analizar con la que cuenta este programa, puede mostrar la estructura de los directorios del sistema de archivos sean estos FAT o NTFS (este programa solo incluye soporte para sistemas MS-Windows).

Puede restaurar sectores de arranque dañados y recuperar archivos de manera individual, también puede analizar estructuras de directorios marcando aquellos que tengan problemas o contengan referencias no validadas y en conjunto con el editor puede modificar cualquier sección del disco duro en cuestión, esta opción es usada cuando se trata de recuperar el sistema o los archivos que hay en el, ya que para casos de investigación el programa puede bloquear el acceso al medio como de solo lectura.

También es capaz de buscar en el disco duro por nombres de archivos y tipos de extensión y recuperarlos a unidades externas u otros medios.

Editar medio

Como se mencionó anteriormente la opción de editar medio, se usa con propósitos que tiene que ver con la recuperación de archivos o de sistemas completos, ya que en los casos de investigaciones criminales es imperativo el conservar intacta la evidencia.

Consiste en un editor hexadecimal que muestra la información en ASCII y por sectores, facilitando la edición y búsqueda de algún dato en particular, el editor hexadecimal suele ser una de las herramientas mas poderosas en cuanto a la recolección de evidencias se refiere.

El editor puede buscar cadenas de texto dentro de los archivos o nombres de archivo y extensiones, también puede editar secciones del propio sistema como son las entradas FAT, directorios, sector de arranque y tabla de particiones.

Borrar medio

Esta opción consiste en borrar archivos de manera segura, cuenta con la opción del borrado estándar del departamento de defensa (tres pasadas) y es posible configurar el inicio y final del borrado en sectores.

Pruebas de superficie

Como su nombre lo dice, esta opción nos permite probar la lectura y la escritura del disco duro, con la finalidad de encontrar sectores dañandos y mover la información contenida en estos de ser posible. Una vez más se hace notar que esta opción es útil solo si se trata de recuperar la información o el sistema y no en una investigación de tipo criminal.

3.4.3 F. I. R. E

Forensics Incident Response Environment, consiste en un CD que contiene diversas herramientas para la recolección y análisis de evidencias en un sistema comprometido. Se le llama live boot, porque permite iniciar el equipo comprometido con el CD y cargar el sistema operativo y las herramientas sobre la memoria física disponible, creando un disco virtual y sin modificar la evidencia, ya que todos los dispositivos del sistema son montados como de solo lectura.

Esta herramienta es muy útil cuando se trata de recuperar la información de un sistema que ha sufrido algún tipo de ataque o que no le es posible arrancar por que la tabla de partición este dañada o algún otro tipo de incidente y no es viable el quitar el disco duro del equipo por diversas razones.

En sistemas como Windows XP o Windows 2000 que usan el sistema de archivos NTFS y reglas de acceso sobre los archivos, es muy útil, ya que es capaz de acceder a los archivos de todo el sistema sin la necesidad de contar con privilegios de acceso. Pero también puede representar un peligro si este tipo de herramientas cae en manos equivocadas ya que puede permitir el acceso a información confidencial.

Entre otras herramientas F. I. R. E. contiene:

- Dump drive
- Ethereal
- Editores de texto
- Editores hexadecimales
- Md5sum
- Tripwire
- TCPdump
- Netcat
- Ssh

Está preparado para ejecutarse en sistemas Windows y Linux para establecer un servidor VNC y FTP para transferir archivos entre equipos, también cuenta con una gran cantidad de herramientas para sistemas Windows como son:

- Sniffers para redes Gíreles
- Sniffers para ethernet
- Editores de registro
- John the ripper
- Pwdump (extraer los passwords de sistemas Windows)
- Recuperadores de contraseñas de BIOS
- Clientes IRC
- Servidor VNC

Con la capacidad de copiar archivos a través de la red de manera segura o algún otro tipo de medio, y un conjunto de herramientas por demás amplio, F. I. R. E. es uno de los Kits mas completos además de poder personalizarse, ya que con programas como *Paraben forensic Replicator* se puede editar el contenido de todo el CD para ajustarlo a las necesidades de cada investigador o encargado de seguridad.

También incluye una herramienta para la generación de reportes de la investigación, los cuales pueden ser fácilmente transferidos por la red de manera segura y recibidos en otro equipo que ejecute la herramienta o también transferir los reportes por medio de floppys.

El modo de uso de esta herramienta es simple, ya que incluye soporte para diversos tipos de hardware, basta con configurar el equipo en cuestión para iniciar desde la unidad de CD y establecer si desea iniciar con un modo gráfico o solo con el shell. Una vez cargado el sistema, se pueden ejecutar las herramientas según se requiera.

F. I. R. E. es un software libre que se rige bajo la licencia GNU, que permite su libre distribución, por lo que su uso en investigaciones criminales esta sujeta a una revisión y validación exhaustiva de todo lo contenido en el CD para evitar cualquier tipo de alteración a la evidencia.

Figura 3.9 Forensics Incident Response Environment

3.4.4 HELIX

Un sistema Live Boot, contiene una gran cantidad de herramientas y esta basado en la distribución Knopix de Linux, permite el acceso a los archivos en modo de solo lectura y incluye diversas interfases gráficas para las herramientas como *dump drive, dcfldd, etheral*.

Incluye soporte para una gran cantidad de hardware incluyendo dispositivos USB, siendo capaz de montarlos durante el inicio, tiene soporte para grabadoras de CD y unidades ZIP.

Cabe destacar que este sistema también se rige bajo las normas del software libre pero cuenta con soporte de diversas universidades y se actualiza constantemente con nuevos drivers y herramientas, incluso su ultima version ya es avalada por la compañía e-fense.

Incluye herramientas tanto para Linux, Solaris y Windows además de poder establecer servidores FTP y VNC temporalmente para la transferencia de archivos entre el equipo comprometido y el de investigación.

Su uso es muy censillo y al igual que *F. I. R. E.* es posible personalizarlo en cuanto a los paquetes y herramientas además de configuraciones de inicio, mediante herramientas como *Paraben Forensic Replicator.*

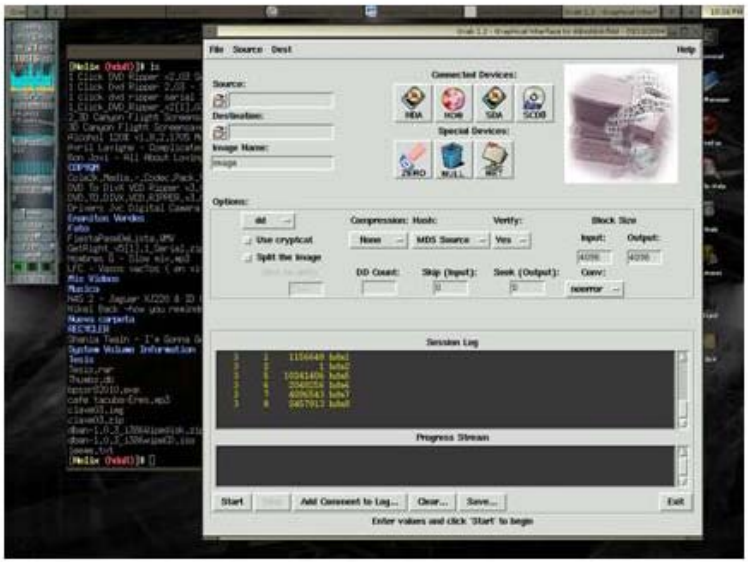


Figura 3.10 Helix

3.4.5 EndCase

Es un tool kit desarrollado por *Guidance Software,* es uno de los mas completos y reconocidos en el ambiente legal, diseñado para correr en sistemas Windows, entre otras cosas es capaz de crear réplicas de todo tipo de medios generando cadenas MD5 para cada nuevo archivo creado durante la investigación, en adición a esto el programa genera un *código de redundancia ciclica* (CRC) por cada 64 sectores de evidencia creados.

Una de las ventajas de este software es que incluye herramientas para la documentación y generación de reportes automáticos para agilizar el proceso de recolección de evidencias.

Incluye su propio lenguaje de scripts llamado **EndScript,** el cual permite al investigador automatizar tareas que requieran repetir procesos o incluso tareas más complejas de la investigación.

Puede realizar búsquedas de cadenas de texto en las evidencias así mismo como cadenas CRC o MD5 para facilitar la búsqueda y organización de la información, tiene soporte para los sistemas de archivos FAT12 , FAT16, FAT32, NTFS, HFS, HFS+, Sun Solaris UFS, EXT2/3, Reiser, BSD FFS, Palm, CDFS, Joliet, UDF and ISO 9660.

Es capaz de buscar imágenes dentro de la evidencia y cuenta con su propio visor para reconstruir estas para facilitar la recolección y organización, también tiene soporte para archivos comprimidos y correos archivos de electrónico.

Tiene incorporado un manejador de discos virtuales para poder montar imágenes de discos duros y de equipos virtuales generados con otras herramientas para facilitar el análisis de evidencias.

EndCase es una de las herramientas mas usadas por los investigadores, por tratarse de un software de tipo comercial se vende bajo un esquema de licencias.

3.4.6 X-Ways forensics

Un tool kit bastante completo y muy competitivo, desarrollado para ejecutarse sobre sistemas Windows, requiere de muy poco espacio para instalarse, es desarrollado por la compañía *X-ways software technology AG* Y su uso se rige bajo un esquema de licencias por lo que es necesario adquirirlo para poder usarlo en una investigación. (Figura 3.11)

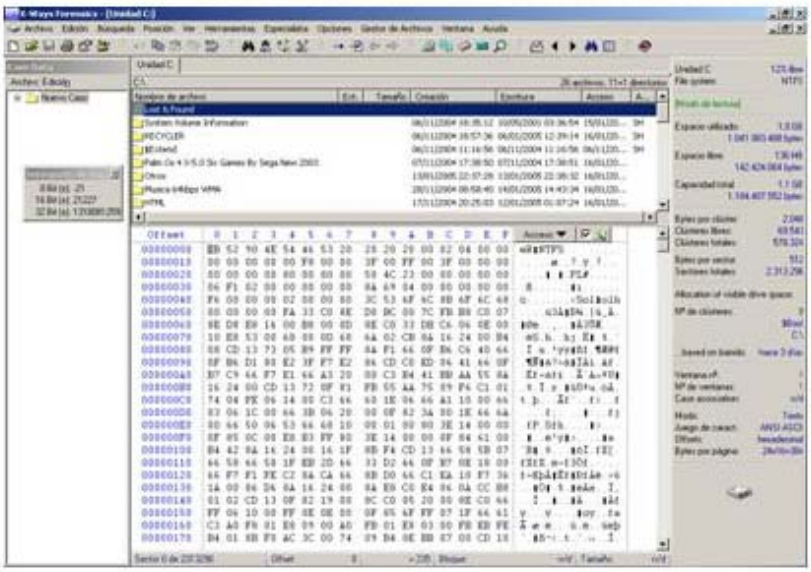


Figura 3.11 X-ways forensics

Entre otras cosas incluye:

- Copia de sectores específicos.
- Clonación creación de archivos imagen de discos.
- Búsquedas de cadenas de texto y de cadenas hexadecimal.
- Búsqueda de archivos borrados por nombre y por tipo.
- Borrado seguro de archivos de diversos dispositivos.
- Documentación automática de las acciones realizadas
- Generación de cadenas MD5 para todos los discos y archivos usados además de tener soporte para otros algoritmos de verificación.
- Análisis de la superficie del disco.
- Puede concatenar, diseccionar, unir o comparar archivos.
- Puede realizar un *dump* de la memoria RAM.
- Puede generar archivos con la información del espacio libre en el disco (similar a *unrm* y *lazarus* en *The coroners Tool Kit*)

También cuenta con un editor hexadecimal y un visor de imágenes integrado para agilizar la búsqueda de evidencias, cuenta con plantillas predeterminadas de las cabeceras de archivos por el tipo de extensión.

X-Ways Forensics es una muy buena opción para llevar una investigación de tipo criminal y para realizar recuperación de datos en equipos que hayan sufrido alguna contingencia.

3.5 HERRAMIENTAS PARA SISTEMAS MOVILES

En la escena del crimen no solo pueden estar implicados equipos de computo como discos duros, CDs o Floppys, recientemente se ha agregado a los medios en los que se pueden encontrar evidencias los dispositivos móviles como son PDAs y teléfonos celulares, en este tipo de dispositivos se puede encontrar mucha información importante para el caso.

Debido a su amplio uso para contener información importante como direcciones, número telefónicos, registros de llamadas en el caso de los celulares, incluso pueden ofrecer acceso a información en Internet, video y fotografía. Es mucha la información que puede ser encontrada en estos dispositivos, pero antes de presentar las herramientas usadas para esto, se tiene que entender la manera en la que estos dispositivos trabajan.

Asistentes personales de datos o PDA

El concepto de PDA fue introducido por la empresa PALM, misma que diseñó el sistema operativo para estos dispositivos, poco a poco se extendió su uso, siendo en la actualidad la mano derecha de muchos ejecutivos y personas de negocio.

A diferencia de las computadoras, los dispositivos PDA pocas veces cuentan con un disco duro, ya que esto elevaría mucho su costo, además que, al estar diseñados para ser portátiles, supone que el dispositivo estará sometido a vibraciones lo que supone un costo mayor para proporcionar seguridad a la integridad del disco duro. Es por estas razones que muchos dispositivos no cuentan con discos duros, en lugar de esto cuentan con unidades de memoria ROM y RAM, que se usan para contener la información mediante una batería de respaldo.

Al contar con unidades de memoria en lugar de discos duros, el preservar la información de estos dispositivos intacta se puede dificultar para el investigador, ya que la información puede ser borrada permanentemente de manera mas rápida que en los discos duros.

Incluso la falta de batería en el dispositivo puede hacer que pierdan la información que se encuentra almacenada en el dispositivo, ya que este consiste solo en cargas eléctricas almacenadas en celdas de energía a la cual se accede por medio de un vector de direcciones, por lo que la ausencia de la energía supone la volatilización de la información.

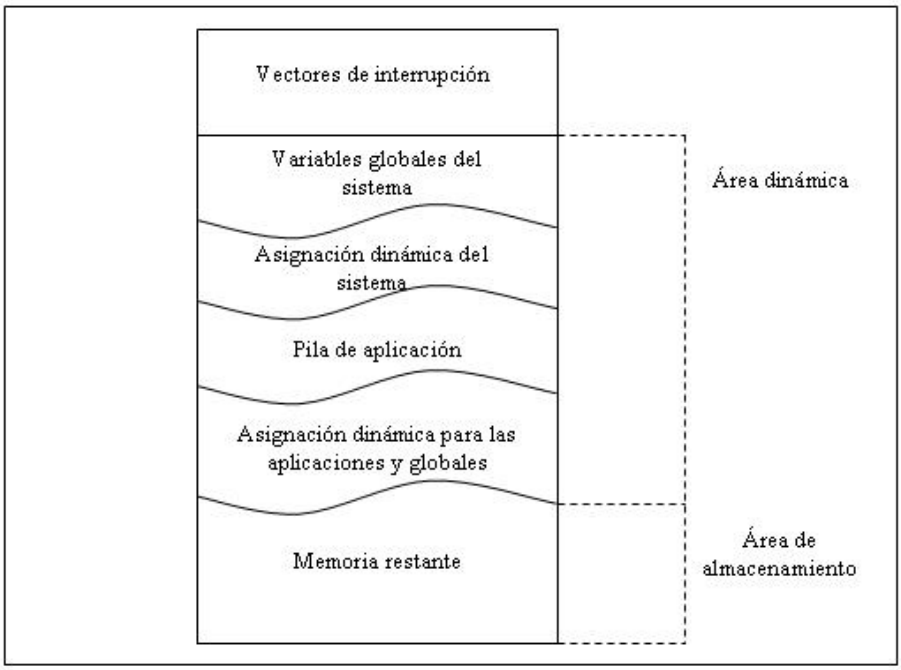


Figura 3.12 vista conceptual de la memoria de un PDA

La memoria de un PDA se divide en RAM y ROM (véase figura 3.12), en la memoria ROM, solo se almacena el sistema operativo del dispositivo así, como las aplicaciones que la empresa instala por default, la memoria RAM es usada para almacenar la información como son direcciones, fotos, incluso video, así también se almacenan los programas que pueden ser cargados en el dispositivo y es esta misma memoria la que el programa usa para ejecutarse.

La memoria que estos dispositivos incluyen, suele ser pequeña en comparación con lo que un usuario esta acostumbrado, 8 MB, 16 MB, 32 MB e incluso los dispositivos mas nuevos tienen 512 MB de memoria interna, pero si consideramos que un archivo de audio mide en promedio 3 MB o que un archivo de video de 30 minutos puede medir 64 MB, la memoria resulta insuficiente, por lo que estos dispositivos incluyen ranuras para memorias externas como son tarjetas SD, Smart Media, Compac Flash, etc.

Estas memorias también son una gran fuente de información y deben de ser tratadas con el mismo cuidado que son tratados los discos duros. Su sistema de archivos generalmente es FAT y dependiendo de su tamaño sería FAT12, FAT16 o FAT32.

El procedimiento para extraer la información de estos dispositivos es dejar el medio intacto, es decir no removerlo del dispositivo hasta que la información haya sido extraída, una ves realizada esta operación de congelamiento de la escena, es posible retirar el dispositivo y realizar un análisis con los mismos procedimientos con los que son tratados los discos duros, es por esto que el equipo del investigador debe contar con dispositivos de lectura de todo tipo de medios.

Otro aspecto importante es la manera en la que los dispositivos PDA manejan los archivos, el sistema operativo PALM OS maneja solo tres tipos de archivos que son los siguientes:

- **Base de datos PALM (*.PDB).** Registro de base de datos usado para almacenar información de una aplicación o información del usuario.
- **Recurso PALM (*.PRC).** Base de datos de recursos, los programas que se ejecutan en los dispositivos PALM son solamente un conjunto de estas bases de datos que contiene el código del programa así como información de interfase con el usuario.
- **Aplicación de preguntas PALM (*.PQA).** Es un nuevo tipo de archivo que contiene información de Internet para ser procesado por los dispositivos PALM con soporte Wirelees.

El sistema de archivos de los dispositivos PALM funciona en cierta forma como los dispositivos de almacenamiento externo, ya que no borra el archivo de la memoria, si no que lo marca como espacio disponible y borra la entrada de la tabla de asignación, adicionalmente, los registros de programas propios del sistemas como son el block de notas o la lista de pendientes, no son borrados de la memoria, son marcados como no disponibles pero su espacio en la memoria no es liberado si no hasta que se realiza una sincronización del sistema.

Teléfonos Celulares

Los teléfonos celulares, los cuales en estos días han sido considerados incluso como una extensión del cuerpo, debido a la necesidad de comunicación que se requiere, son una fuente de información, en los últimos días hemos podido ver como estos dispositivos han pasado de ser solo un instrumento de comunicación para convertirse en un dispositivo multimedios.

Los dispositivos celulares actuales, no solo pueden realizar llamadas con calidad de audio digital, si no que también pueden tomar fotografías, reproducir MP3, grabar video, almacenar memos de voz, y usan sistemas operativos mucho más complejos que hace 4 años.

La adquisición de la información de estos dispositivos puede llegar a convertirse en un problema debido a la poca apertura que existe en lo referente a las especificaciones técnicas de algunos de estos dispositivos y a la gran variedad de ellos.

Hasta el momento no existen dispositivos celulares que cuenten con discos duros integrados, aunque no pasará mucho antes de que eso cambie, debido al tamaño que tienen, por lo que todos usan memorias internas Flash o ROM usada para almacenar la información propia del dispositivo como es su sistema operativo números telefónicos, fotos video, etc. Algunos dispositivos como el **NGrage** de **Nokia** tienen soporte para tarjetas de memoria *SD*.

La memoria de estos dispositivos suele ser menor que la de los dispositivos PALM, siendo estos desde los 4MB hasta los 128MB en los dispositivos mas modernos, cabe destacar que las compañías celulares están realizando poco a poco una integración entre los dispositivos

PDA y los teléfonos celulares, por lo que compañías como **Motorola** han comenzado a usar el sistema operativo Palm OS en sus teléfonos celulares.

La adquisición de información en estos dispositivos suele ser complicada, ya que supone el contar con los medios necesarios como los cables Link que no siempre son proporcionados por las compañías, además de que algunos de estos celulares necesitan de un código de acceso que solo posee la compañía que lo fabricó.

No obstante, poco a poco se esta viendo una apertura por parte de los fabricantes de estos equipos para poder extraer la información de estos dispositivos, además de que algunas compañías están optando por el software libre tal es el caso de **Nokia** con el sistema operativo **Simbian**.

3.5.1 PDASeizure

Esta es una herramienta diseñada para adquirir la información contenida en los dispositivos PDA, diseñada por la compañía **Paraben**, tiene soporte para equipos con Palm OS y Windows CE, incluye un emulador de Palm OS lo que permite "traer a la vida" nuevamente el dispositivo sin alterar el equipo original.

Incluye un editor Hexadecimal que permite hacer búsquedas de cadenas de texto, no solo en un archivo en específico, sino en todos los archivos descargados del equipo.

Para realizar la descarga de la información del equipo, es necesario poner en modo de depuración el equipo, ya que para descargar toda la información es usado el protocolo de este modo de sistema, para hacer esto se necesita escribir una "l" minúscula, un punto y un dos en el área de graffiti del equipo. (Figura 3.13)

Figura 3.13 Dibujo requerido en el área de graffiti para el modo de depuración

Ya que el equipo se encuentra en el modo de depuración, se realiza la descarga de los datos, esto tarda mas tiempo del requerido por una sincronización normal, ya que se descargan todos los archivos contenidos en el equipo y si se encuentra un medio como una tarjeta de expansión SD, también se realiza una copia de los archivos contenidos en esta.

Todos los archivos descargados son clasificados de acuerdo al área de memoria en la que se encontraban y es creada la cadena MD5 para su posterior autentificación, se leen todos los datos del archivo como el creador y la firma digital que pueda contener. (Figura 3.14)

Si el equipo requiere de una contraseña, en sistemas operativos iguales o menores a Palm OS 4 el programa puede tratar de romperla o de "saltarla", los sistemas operativos posteriores requerirán otros medios y el uso de otros programas para la adquisición de la contraseña.

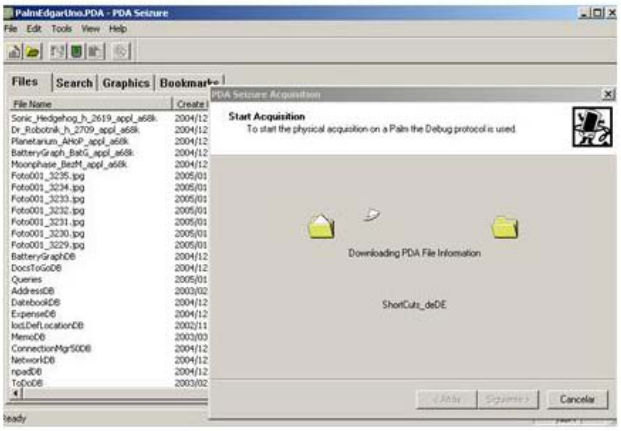


Figura 3.14 Adquisición de evidencia con PDASeizure

3.5.2 CellSeizure

De la misma compañía que creo el *PDASeizure* tenemos el CellSeizure, diseñado para adquirir datos de los dispositivos celulares y tarjetas de memoria SIM, la versión completa incluye el *CellSeizure Toolkit*, que incluye los cables para descargar información de celulares Motorota, SonyEricson y otros.

Para usar este software basta con conectar el celular con el cable correspondiente al equipo de investigación y seleccionar el Plugin a utilizar, después de esto solo se tiene que seleccionar la información que se desea descargar del equipo y realizar la adquisición. (Figura 3.15)

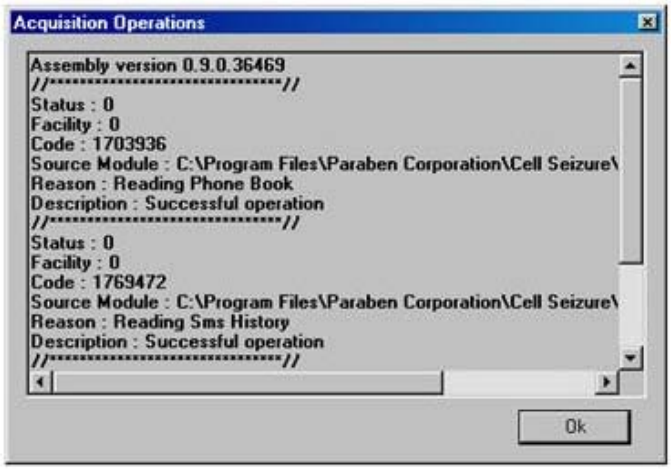


Figura 3.15 Adquisición de datos con CellSeizure

Este programa también puede generar reportes en formato HTML para su revisión, en la que se pueden apreciar registros de llamadas y la libreta de direcciones. También maneja la autentificación MD5 para todos los datos descargados del equipo.

3.6 EQUIPOS ESPECIALIZADOS

Además de las herramientas presentadas anteriormente y por la creciente necesidad de contar con herramientas más robustas y especializadas en la investigación de tipo criminal, se han desarrollado equipos especializados para la recolección de evidencias, así como para el análisis de estas. A continuación se presentan algunos de estos equipos.

3.6.1 Mobile Forensics Workstation

Este equipo fue diseñado por la compañía **VOGON INTERNATIONAL** para los casos en los que se requiere asistencia inmediata y cada segundo cuenta, es fácil de transportar he incluye todo lo necesario para adquisición de evidencias.

Incluye unidades de cinta y un pod para evadir las contraseñas de equipos portátiles, soporte para dispositivos ATA, SCSI, S-ATA, cuenta con un sistema operativo basado en Windows, lo que permite el uso de herramientas de otras compañías como parte de la investigación.

Las características de este equipo se presentan en la tabla 3.10

Estación de trabajo de alto desempeño	PC compatible con pantalla de panel plano dos adaptadores Ultra SCSI 160 incluidos
Pod de duplicación de discos.	Bus de expansión de medios con protección contra escritura de medios, pod externo para dispositivos IDE, Pod de duplicación de discos SCSI, Pod de duplicación de discos S-ATA, Tarjeta de expansión PCMCIA para proveer acceso a tarjetas de memoria externa SD, Multimedia Card, USB drives, etc.
Fuente de alimentación regulada	Fuente de alimentación para los dispositivos externos y otros equipos lo que evita la necesidad de encender el equipo bajo investigación.
Formato de grabación en cinta LTO Ultrium-1 y 2	cerca de 200GB de capacidad en formato nativo y 400GB en formato comprimido, algoritmo ALDC la velocidad de transferencia es de 15MB/s, 30MB/s, 60MB/s
Formato de grabación en cinta DDS-4 DAT	20 GB de capacidad nativa, hasta 40GB con compresión algoritmo DCLZ, hasta 6MB/s en velocidad de transmisión de datos.
Velocidad de captura de la información	Hasta 2GB/minuto, dependiendo del equipo a analizar
Técnicas anti-repudio	Comprobación de los archivos creados con cadenas CRC32 y MD5, y generación automática para cada archivo creado.

Tabla 3.10 Características del mobile forensics Workstation

3.6.2 Enterprice Imagin System

Este equipo fue diseñado por la compañía **VOGON INTERNATIONAL** para los casos en los que se requiere recopilar evidencias de una gran cantidad de equipos, es capaz de conectarse a la red para realizar la adquisición de datos e imágenes de discos duros, al estar diseñado para la investigación criminal, el rendimiento que este tiene para la recolección de evidencia es muy bueno.

Entre otras características incluye un modulo para romper los passwords de equipos portátiles como Laptops y discos duros, tiene soporte para cintas de datos y toda la transmisión e intercambio de información con esta estación es cifrada, además de incluir mecanismos antirepudio como es la generación de Códigos CRC y MD5 en la creación de cada archivo.

Las características detalladas de este equipo se muestran en la tabla 3.11

Estación de trabajo de alto rendimiento	HP o Dell Workstation, procesador 2.0GHz, 40GB, 512MBRDRAM y un monitor de 18" de panel plano.
Software incluido	Sistema operativo basado en Unix, Vogon's Enterprise Imaging Software, Vagon's Tape autoloader control software.
Unidad para romper password	Unidad para evadir passwords de discos duros en Laptops
Formato de grabado de datos LTO Ultrium-1 en cinta	100 GB de capacidad nativa, 200GB con compresión típica (algoritmo mejorado ALDC) 15MB/s 30MB/s velocidad sostenida.
Formato de grabado de datos Super DLT en cinta	110GB de capacidad en formato nativo, 220GB con compresión (algoritmo DLZ) 12MB/s velocidad máxima de transferencia.
Formato de grabado de datos DLT 8000 en cinta	40GB de capacidad nativa 80GB con compresión (algoritmo DLZ) 12 MB por segundo velocidad máxima de transferencia.
Formato de grabado de datos DDS-4 DAT en cinta	20GB de capacidad en formato nativo, 40GB con compresión (algoritmo DCLZ) 6MB/s velocidad máxima de transferencia.
Técnicas de antirepudio	Compara la imagen creada con el original en el momento de la creación y en cualquier otro momento con sumas MD5128 o CRC32

Tabla 3.11 Carateristicas de Enterprise Imaging System

CAPITULO

4

METODOLOGÍA PARA REALIZAR LA FORENSIA INFORMÁTICA

4.1 IMPORTANCIA DE LA METODOLOGÍA

Toda investigación debe tener una metodología que permita dar credibilidad a la misma, y en el caso de la forensia informática, es de suma importancia, ya que el no acatar alguno de los pasos provocaría una falta de credibilidad en las evidencias encontradas y por tanto en todo el caso.

La metodología para este tipo de investigaciones debe estar compuesta por lo menos por los siguientes pasos:

- Congelación de la escena del crimen.
- Recolección y etiquetado de la evidencia.
- Investigación y reconstrucción del crimen con base a las evidencias.
- Generación de reportes de la investigación.

La metodología que se presenta a continuación presenta otros puntos, como son el resguardo de la evidencia original y la cadena de custodia, pero, está basada en los puntos presentados anteriormente.

4.2 EVIDENCIA ELECTRÓNICA

Antes de comenzar con la recolección de evidencias para el caso se debe de tener muy claro que es una evidencia electrónica.

- **Evidencia digital.** Información de valor para la investigación de un caso que se encuentra en formato digital o que es transmitida en este formato.

Además de esto tenemos otras definiciones que son útiles.

- **Objeto de datos**. Información de valor para la investigación que se encuentra asociado con un objeto físico.
- **Componente físico.** Objeto físico en el que se encuentra almacenada la información que es de valor para la investigación.

Para que la evidencia pueda ser admitida como tal, tiene que cumplir con ciertos requerimientos, a continuación se presentan los puntos mínimos con los que se debe de cumplir para esto.

- La evidencia original deberá ser conservada lo mas parecido posible a el estado original en el que fue encontrada.
- Si es posible realizar una copia exacta (imagen) de la evidencia original con la finalidad de realizar el trabajo de investigación sobre la copia y evitar daños o modificaciones al material original.
- Las copias realizadas para examinar deberán ser en medios considerados estériles, es decir que no debieron existir ningún tipo de datos en el medio a usar para las copias, deberán estar completamente “limpios”.

- Toda la evidencia será propiamente etiquetada y documentada en la cadena de custodia, además que cada paso que implique acción sobre el original o la copia de la evidencia deberá ser documentada de manera detallada.
- Toda la evidencia digital deberá ser documentada con en mecanismo antirepudio como son las firmas digitales del investigador y las sumas MD5 o CRC de el medio.

4.3 ASEGURAMIENTO Y CONGELACIÓN DE LA ESCENA DEL CRIMEN

El aseguramiento de la escena, se llevara acabo de manera inmediata a la detección de un incidente, si se pretende seguir un caso de tipo criminal, esta acción deberá ser realizada por un perito calificado y autorizado para ello, en compañía de los responsables del área.

El primer paso una vez que los expertos se encuentran en el lugar de la escena del crimen, que puede estar ocurriendo en ese momento o haber sucedido unas horas o incluso días antes, es apagar los equipos.

El apagado de los equipos es crucial y literalmente deben de ser apagados, desconectados de la corriente eléctrica, de preferencia sin ejecutar o terminar algún tipo de tarea en el equipo, de ser necesario terminar una aplicación para asegurar la consistencia de la información, esta será documentada paso por paso.

La necesidad de apagar el equipo con una desconexión de la corriente eléctrica, es debido a que el atacante pudo haber preprogramado secuencias de comandos que eliminarían evidencias de su presencia al iniciar el apagado del sistema.

Estos scripts pueden destruir toda la información sensible, como logs de conexiones de red, accesos a archivos y modificaciones, algunos realizan una limpieza exhaustiva del espacio vacío y de la memoria swap antes de apagar el sistema, es por esto que el equipo debe ser apagado evitando en la medida posible cualquier modificación a la información y ejecución de programas después de la detección de el incidente.

4.4 LA CADENA DE CUSTODIA

La cadena de custodia se refiere a las personas que desde el principio de la investigación estarán involucrados, y serán los responsables de obtener y preservar las evidencias. Esta cadena de custodia deberá estar formada por personal de la empresa u organización afectada, en su caso por personal de seguridad externo en caso de OutSourcing, y por el personal de la división que investiga el caso criminal, el gobierno.

Cada parte deberá contar con especialistas en leyes y especialistas técnicos que den fe de la adquisición de la evidencia y su análisis correspondiente. No siendo necesario que estén presentes todos en un mismo lugar para realizar la investigación, ya que cada uno puede contar con copias de la evidencia original certificada, cada copia que se entregue así como cada movimiento de la evidencia original, deberá ser agregado a la documentación de la cadena de custodia.

4.5 RECOLECCIÓN DE EVIDENCIA

Una vez que el equipo ha sido apagado, se deben de tomar fotografías del equipo y del lugar en el que se encuentra, como en toda investigación criminal, este tipo de evidencia sirve para evitar inconsistencia en la presentación del caso. (Figura 4.1)

En determinadas situaciones que se pudiera presentar acceso al equipo de manera física, se deberán tomar fotografías de todo el lugar en el que se encuentra el equipo y las medidas de seguridad que se tienen para acceder al lugar.

Figura 4.1 Fotografías del lugar y el equipo.

4.6 DOCUMENTACIÓN DE LA EVIDENCIA FÍSICA

En este paso se debe de realizar un inventario minucioso del equipo incluyendo números de serie y características del equipo, en otro apartado se realizara una descripción completa de la configuración del equipo y para lo que estaba destinado.

También se debe de documentar si el equipo se encontraba conectado a la red, el puerto del switch o equipo al que se encontraba conectado y de ser posible la dirección de hardware del puerto.

También deberá recibirse por porte de los encargados de el área, una descripción y documentación de direcciones IP, MAC y topología de la red en la que le equipo se encuentra hasta su punto frontera de existir como se muestra en la figura 4.2.

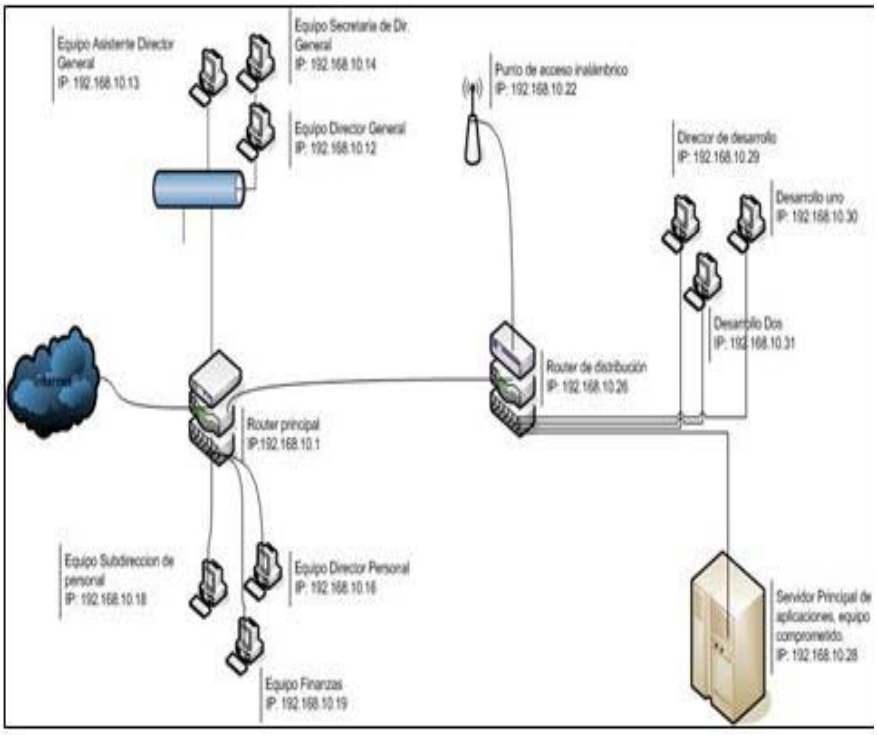


Figura 4.2 Topología de la red atacada hasta su punto frontera.

Es de utilidad que se entregue documentación referente a la actividad de la empresa, reportes de tráfico en la red y descripción de quienes acceden a la red; esto es útil para ubicar al equipo en un contexto con el fin de facilitar la búsqueda de la evidencia.

4.7 REUBICACIÓN DEL EQUIPO A UN AMBIENTE SEGURO

Aun suponiendo que el equipo de cómputo se encuentra en un lugar seguro, es necesario asegurarse de que la evidencia no sea modificada ya sea de manera intencional o no, es por esto que se debe de mantener el equipo bajo vigilancia y de ser posible será trasladado a otra ubicación para su investigación.

En estos casos la empresa no puede detener sus operaciones a causa de la investigación, por lo que deberá tener un plan de contingencia que le permita seguir operando, ejemplo, con un servidor de respaldo o con una copia de respaldo del equipo afectado.

Existen casos en los que la evidencia no se encuentra en un solo equipo si no en varios de estos, incluso cientos de estos, por lo que no siempre es posible reubicar el equipo, en estos casos, se utilizarán medios masivos de almacenamiento como, **storage servers** con capacidades de dos a cuatro terabytes para almacenar las copias de los discos en cuestión, pero aun así, el equipo deberá mantenerse bajo custodia durante un periodo de tiempo para la recolección de la evidencia, lo cual en estos casos puede tardar varios días.

La empresa debe tener definidas todas estas cuestiones en sus políticas de seguridad, para asegurar el funcionamiento de la empresa aun cuando se este realizando una investigación.

4.8 CLONACIÓN, AUTENTICACIÓN, ETIQUETADO Y VERIFICACIÓN DE LOS DATOS

Una vez que el equipo está seguro, y se ha realizado un inventario, se debe proceder a la extracción de la evidencia, en el caso de equipos de cómputo como PC's y servidores, se deberá realizar una copia de los discos duros bit a bit, esta copia de información depende en gran medida del equipo con el que se cuente para esto, pero el montaje de la unidad deberá ser siempre en modo de solo lectura, y bajo la supervisión de personal que certifique la operación.

Antes de realizar la clonación de los discos, se deberán crear las cadenas MD5 o CRC que certifiquen de manera matemática el estado del la información, y una vez realizada la copia de la información, se generará la firma correspondiente a la o las copias de la información, debiendo coincidir completamente con la de la original.

En el caso de equipo como PDA's y equipos celulares la extracción de la información no siempre es de manera limpia, por lo que todos los pasos deberán ser documentados y en presencia de personal que certifique la operación, además que por la naturaleza volátil de la información de estos dispositivos, la extracción de la información se deberá hacer de la manera mas rápida posible, esto implica el traslado de equipo para la extracción de la información al lugar del incidente.

Una ves extraída la información o en el momento de estarla extrayendo, se deberán generar las firmas digitales de cada archivo encontrado en los dispositivos así como de la imagen completa de la información.

4.9 RESGUARDO DE LA EVIDENCIA ORIGINAL

La investigación deberá ser llevada sobre las copias certificadas de la evidencia, se deberá evitar siempre el trabajar directamente con la evidencia original, lo que implica que los originales deberán ser etiquetados con un número de investigación y en el caso de los discos duros o medios de almacenamiento con una etiqueta que indique su firma CRC o MD5.

Toda la evidencia deberá ser resguardad en un lugar certificado para esto, con las medidas de seguridad pertinentes, tomando en cuenta niveles de humedad y temperatura que pueden afectar a los equipos electrónicos aun estando apagados, así también como el polvo que pueden destruir la información contenida en los medios originales.

4.10 DETERMINACIÓN DEL CONTEXTO DEL CASO

Cuando ya se ha recolectado la evidencia o los medios en los que se encuentra esta, y una ves que se han creado las copias de la información y según la cadena de custodia se ha repartido copias certificadas a todos los investigadores del caso, se procede a la búsqueda de la información que servirá para la presentación del caso y en su caso la persecución y aseguramiento del responsable.

Para la determinación del contexto del caso, se deberá contar con toda la información recolectada hasta el momento, incluyendo las declaraciones de los administradores o encargados del área afectada, con la finalidad de determinar una línea de tiempo entre el momento en el que se detectó el incidente y el momento en el que iniciaron los acontecimientos.

Es preciso hacer una diferencia entre el tipo de investigación, ya que si el objetivo del ataque fue un equipo informático, la manera en la que se lleva la investigación es diferente cuando la evidencia digital o contenida en un equipo es de utilidad para un caso, ejemplo, un caso de venta de pornografía infantil.

4.10.1 EL EQUIPO ES EL OBJETIVO

En este caso, la estructuración de la línea del tiempo es indispensable para saber ¿que paso? y como fue que ocurrió, para esto la investigación se apoyará de logs generados por los accesos al sistema, y la información generada por sistemas de detección de intrusos, así como sniffers y otras herramientas.

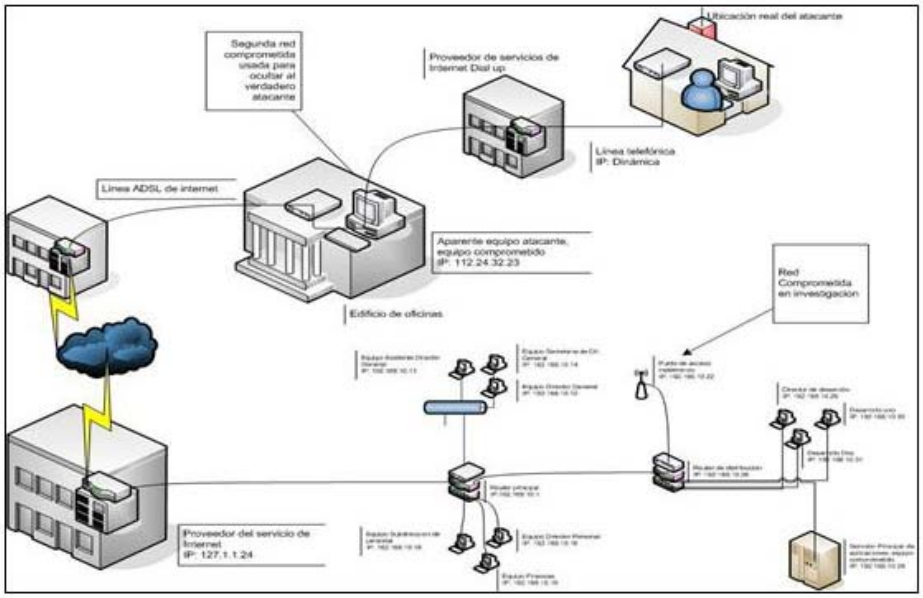


Figura 4.3 Seguimiento a otras redes usadas en el ataque

Los logs y sniffers pueden arrojar información como direcciones IP, o direcciones MAC, así como el protocolo y puerto usado, en una revisión mas minuciosa es posible encontrar información de los sistemas operativos involucrados, y gracias a los mecanismos de direccionamiento, se puede encontrar información de logs en otros servidores que estén involucrados de manera indirecta. (Véase figura 4.3)

En el caso de vulneración de un equipo específico se pueden ocupar las firmas de tiempo de los sistemas de archivos para reconstruir la línea de tiempo.

De existir, los archivos modificados y creados en el equipo comprometido, son una gran fuente de información, ya que muchos atacantes suelen firmar sus archivos con algún pseudónimo y esto puede ayudar a ligar un patrón de casos realizados por el mismo atacante.

En los casos de ataques, en los que no se vulnera un equipo en específico si no una red, la información generada por los sniffers e IDS, suele arrojar información de otros servidores comprometidos, siendo esta la mayor fuente de evidencia, hasta llegar al último punto que pueda suponer por ejemplo una conexión **dialup,** con una cuenta específica, apoyándose para esto de una orden de tipo federal para la adquisición de los logs de conexión de este tipo.

4.10.2 EL EQUIPO ES EL MEDIO

En los casos en los que el equipo es usado para la realización de un delito o contiene evidencia de un caso criminal, como la venta de pornografía infantil o de drogas, la línea de tiempo puede no ser tan indispensable, pero sí se requiere contar con las firmas de tiempo de toda la información para evitar la introducción de información falsa al caso.

En estos casos, la información contenida en el equipo es la indispensable, y es aquí donde se debe de plantear con mas cautela, ¿qué es lo que se esta buscando? y en donde podría estar.

En casos de pornografía infantil, suele ser fácil determinar qué se busca, imágenes o video, pero no se pueden pasar por alto archivos que contengan direcciones o nombres.

En casos de fraudes o venta de droga, la búsqueda de la evidencia suele ser más compleja, ya que supone mucha astucia por parte del investigador y conocimiento del caso, ya que el más mínimo detalle puede contener información importante, por esto se deberán realizar análisis exhaustivos como son:

- Búsqueda y recuperación de archivos borrados.
- Búsqueda de modificaciones en los tamaños de archivos.
- Archivos cifrados o enmascarados con mecanismos avanzados como PGP o esteganográficos.
- Búsqueda y análisis de logs o conversaciones grabadas.
- Evaluación de programas y su funcionalidad
- Búsqueda de anomalías en el sistema de archivos y los archivos mismos.

4.11 BUSQUEDA Y DESCARTE DE EVIDENCIA

Cuando se tiene definido que tipo de caso es el que se esta estructurando, se debe de determinar qué es lo que se va a buscar y qué podría considerarse evidencia para el caso, por ejemplo, ¿es importante buscar todos los archivos “dll” del equipo y realizar un análisis sobre ellos?

En esta parte de la investigación se continúa con base en el contexto del caso si el caso trata de pornografía infantil, se buscarán archivos de imágenes, ya sea en el sistema de archivos en la FAT o el MFT, o con búsquedas secuenciales directas de las cabeceras de imagen en el disco duro.

Si se trata de un caso de fraude, se buscarán y analizarán archivos que puedan contener esta información, como hojas de cálculo, o bases de datos.

Pero esto no quiere decir que toda la demás información será descartada, sino que se debe de tener una prioridad sobre lo que se busca, no tiene caso el realizar búsquedas secuénciales de cabeceras de archivos “*.dll” si no es prioridad.

Es decir primero se buscará la información obvia del caso y posteriormente lo que pueda implicar un conocimiento mas profundo de la tecnología implicada, ejemplo, si se encuentra que el equipo contaba con programas de cifrado esteganográfico, es posible que la información se encuentre disfrazada en archivos de imágenes.

Otro punto que se debe tener en cuenta es en donde buscar, ya qué la información puede estar contenida de diversas maneras en diversos medios, es decir, puede estar en lugares en los que comúnmente no estaría, se deben realizar búsquedas secuenciales sobre la información de manera directa, ya que por ejemplo podría esconderse una cadena de texto de manera directa en el sistema de archivo con un editor hexadecimal, sin que exista una entrada para un archivo en el sistema FAT.

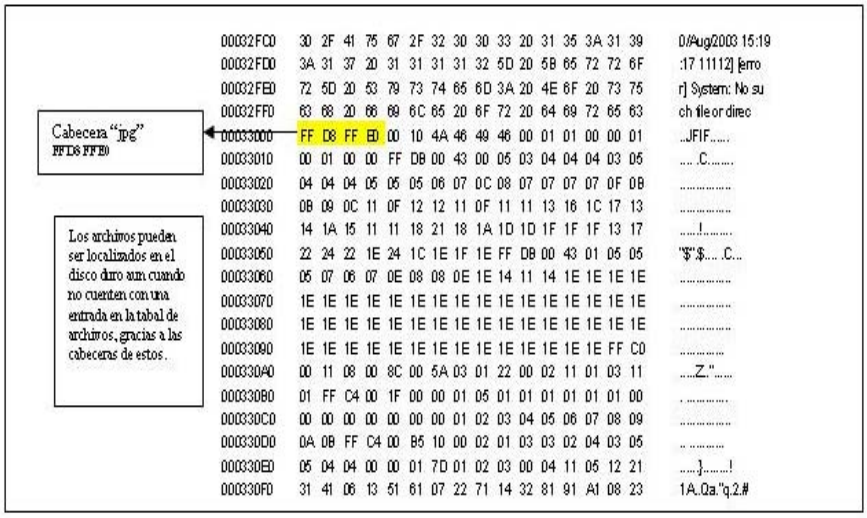


Figura 4.4 Búsqueda secuencial de una cabecera jpg

Por último se debe mencionar que la información o la evidencia no siempre esta completa, pero puede ser considerada como evidencia, es decir, una cadena de un archivo “jpg”, puede reconstruir parte de una imagen, sin importar si el archivo está completo o no, esto puede ser una evidencia en un caso de pornografía infantil.(figura 4.4)

Un archivo de texto incompleto puede contener información que pueda ser de utilidad en la formación de las circunstancias del caso, esta búsqueda de archivos incompletos se puede

realizar con programas como **EndCase, X-way forensics, Pro-Discover** que permiten la búsqueda y localización de archivos mediante las cabeceras de los formatos específicos.

Este tipo de búsquedas supone muchos falsos positivos, pero es una manera de realizar una búsqueda exhaustiva sin pasar por alto nada.

4.12 GENERACIÓN DE REPORTES

Para poder dar estructura al caso y dar seguimiento, es necesario contar con documentación que dé formalidad a la información, estos son, los reportes que deben de incluir información referente al contexto y al equipo.

Inicialmente la organización debe tener un mecanismo para reportar qué ha ocurrido un incidente, por lo que se recomienda llenar un reporte de incidente, esto con la finalidad de cumplir con las políticas de seguridad que implican la división de responsabilidades en un incidente.

La información que puede estar contenida en un reporte de un incidente puede ser la siguiente:

- El día y la hora actual, de ser posible el día y la hora en la que ocurrió el incidente.
- Nombre y dirección de quien reporta el incidente, así como su puesto en la organización.
- Dirección IP del equipo afectado.
- Nivel de riesgo del incidente.
- Servicios que ejecuta el equipo y los medios por los que es accesible.
- Una descripción de la detección del incidente y los posibles mecanismos usados.

No solo se deben tener reportes de este tipo, también se deben de tener reportes de la cadena de custodia, es decir, cada copia de la evidencia o cada original que se mueva deberá ser documentado, con la siguiente información:

- Tipo de evidencia
- Numero de caso al que pertenece
- Numero de serie
- Firma digital CRC o MD5
- Fecha
- Nombre, teléfono y firma de quien recibe la información así como la organización a la que pertenece.

Durante el análisis de los medios, se deberá de llenar uno o varios reportes de los medios que se están analizando, esta información deberá ser llenada por quien realiza el análisis de la evidencia, la información que debe contener el reporte es la siguiente:

- Numero del caso.
- Nombre de quien realiza el análisis.
- Fecha de recepción de la evidencia y fecha de adquisición de esta.
- Tipo del caso y observaciones.

En un apartado aparte se presentará un resumen del tipo de medios que se están analizando, como el número de Discos duros, marca modelo, número de serie y Firma MD5 o CRC. Se pondrá una descripción para cada tipo de medio.

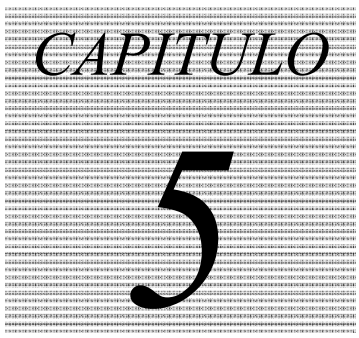
Aparte de lo anterior se deberá presentarse un reporte técnico que incluya la información encontrada y una descripción del contexto del caso, qué se busco y qué se encontró, esto como reporte final de la investigación, este reporte deberá contener por lo menos lo siguiente:

- Descripción del caso y su contexto.
- Descripción de la evidencia y la manera en la que se obtuvo.
- Descripción de las herramientas usadas para la obtención y análisis de la evidencia.
- Una descripción de la línea del tiempo del incidente y de la investigación.
- Parámetros usados para la búsqueda de la evidencia así como líneas y supuestos.
- Listado de archivos encontrados, reconstruidos y originales con firmas de tiempo y MD5 o CRC.

En un medio aparte se mantendrán y entregarán copias de la evidencia recolectada, cada una con sus respectivas etiquetas que indicarán el número del caso, número de evidencia y firmas digitales. También se debe suponer que se contará con una cadena de custodia para la entrega de la evidencia y su preservación.

Para la presentación de la información el investigador se puede apoyar en los programas para forensia informática que generan un reporte de manera ordenada y con los aspectos necesarios, algunos programas pueden generar los reportes en html o en documentos de texto enriquecido.

En el último capítulo se presenta un caso práctico en el cual se pretende ampliar la descripción de la información contenida en los reportes; en los apéndices se anexan algunos de los reportes usados por algunas organizaciones.



CASO PRÁCTICO DE FORENSIA INFORMÁTICA

5.1 HONEYPOT Y HONEYNET

Los llamados Honeypot y Honeynet, fueron creados pensando en resolver una gran problemática, la seguridad de sistemas que se encuentran conectados a la red de Internet o a redes privadas de gran tamaño.

En un principio los desarrolladores de sistemas operativos y sistemas que ejecutan servicios en red, y así mismo las compañías que ejecutan este software, solo podían confiar en que los desarrolladores y personal de seguridad de sistemas conocieran todos los "trucos" para acceder de manera ilícita a un sistema o que estarían al día con las nuevas vulnerabilidades encontradas.

Pero desafortunadamente esto no era así, los atacantes siempre estaban un paso al frente de los encargados de la seguridad, así que porqué no hacer que los atacantes nos muestren sus técnicas sin necesidad de poner en riesgo los sistemas de la empresa.

De esta forma surgió la idea de crear sistemas que emularan cualquier tipo de equipo que ejecute un sistema operativo específico y de esta forma simular un sistema vulnerable o un posible sistema vulnerable, dejándolo en parte fuera de las políticas de seguridad de la organización.

El objetivo de estos sistemas es el recolectar información acerca de la manera en la que un atacante accede o vulnera un sistema. Esta recolección se hace mediante diferentes tipos de herramientas como son Sniffers, analizadores de protocolos, verificadores de integridad, sistemas de detección de intrusos y herramientas de forensia informática en general.

Las herramientas de forensia informática son usadas en campo en casos reales, pero se recomienda probarlas antes en escenarios controlados para poder asegurar que ante un incidente se tendrá todo lo necesario. Esta es otra ventaja de los honeypot, permiten probar y mejorar las herramientas en un habiente lo mas real posible.

Pero de la misma manera en la que las técnicas de ataques se modernizaron, los honeypot evolucionaron hacia sistemas mas complejos, de esta forma surgieron los honeynets, los cuales son mas complejos y requieren de una administración mas minuciosa y dedicada, ya que no se simulara un equipo, si no que se montaran sistemas reales pero controlados.

5.2 PREPARACION DEL HONEYPOT

Para poder instalar un sistema honeypot básico se necesita un equipo que cumpla los requerimientos necesarios para ejecutar el sistema operativo y los servicios necesarios, en el caso que se presenta, se instalo Windows 2000 Server con IIS. Las características del equipo se muestran en la tabla 5.1

Procesador	Intel Pentium IV 1.6 GHZ
Memoria	512 MB RAM, 2.5GB Virtual
Disco Duro	40GB, 20GB
Unidades de medios removibles	CD-RW, DVD-ROM
Placa base	D845HV

Tabla 5.1 Características del equipo

Se instaló primeramente el equipo con el sistema Windows XP profesional como el sistema huésped y se uso VMware Workstation 4.5.2 (8848), de esta manera el host será el sistema operativo Windows XP profesional SP2 y el sistema huésped o el sistema trampa será Windows 2000 Server, así, podremos instalar las herramientas como sniffers e IDS en el equipo host, evitando así que al ser vulnerado el sistema huésped el intruso pueda borrar las bases de datos de este.

Este esquema de instalación de un Honeypot es bastante sencillo ya que solo requiere de un equipo con suficiente potencia para ejecutar de manera correcta los dos sistemas operativos y las herramientas que se usaron, gracias a VMware, será posible emular el Switch en el que se encontraban conectados los dos equipos como se muestra en la figura 5.1.

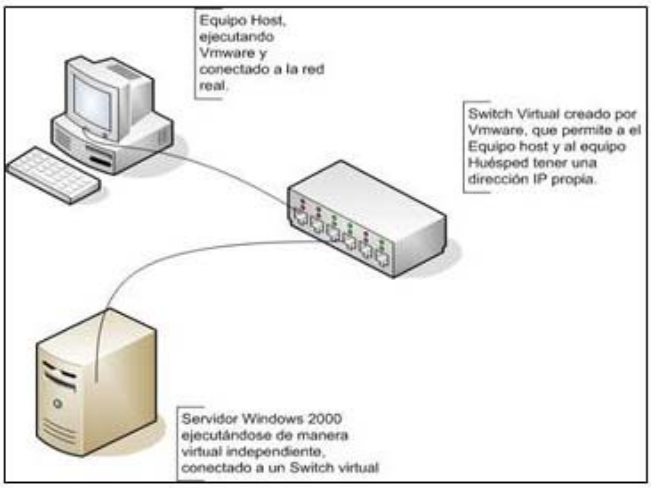


Figura 5.1 Diagrama de conexión a la red de manera virtual.

De esta manera para el atacante existirán dos equipos conectados a la red, pero para evitar cualquier incidente, el equipo host no será accesible en la red, solo tendrá acceso a esta, pero no será visible desde el exterior, esto lo haremos instalando un firewall, para bloquear cualquier tipo de ataque sobre nuestro sistema, véase figura 5.2.

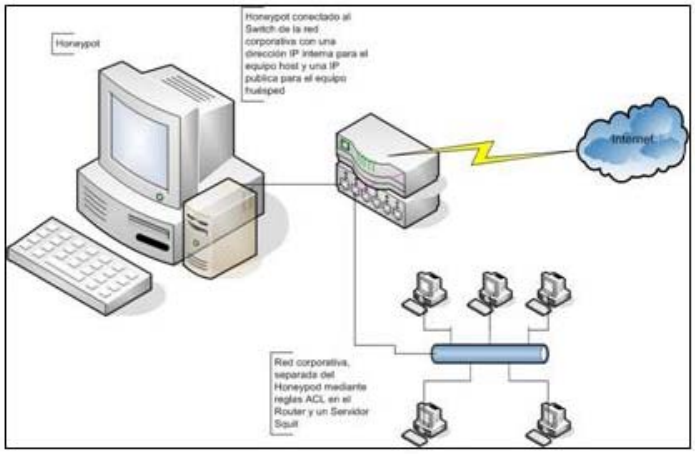


Figura 5.2 conexión de el Honeypot a la red corporativa

5.3 INSTALACION DEL SISTEMA OPERATIVO

Para este caso práctico fué necesario preparar dos sistemas operativos, primeramente la puesta a punto del sistema host con Windows XP y posteriormente la instalación del sistema huésped con Windows 2000 Server.

La instalación del sistema operativo Windows XP profesional se hizo de manera normal, pero se crearon dos particiones, una para contener el sistema operativo del host y la otra para contener el disco duro virtual de nuestro honeypot, esto con la finalidad de aumentar el performance del equipo host.

De esta misma forma, se desactivaron opciones como efectos visuales y temas en el sistema host, también se llevo acabo la de fragmentación del disco duro del equipo host una vez realizado esto, se estableció el tamaño fijo del archivo de paginación, con la finalidad de evitar insuficiencia de memoria en el equipo y la fragmentación del archivo de paginación.

En el sistema host solo se instaló un sniffer, un analizador de protocolos y un IDS, se utilizó Snort para esto ya que es uno de los mas completos además de ser freeware, el sniffer y analizador de protocolos fué Ethereal, se consideró que estas herramientas serían suficientes para recolectar las evidencias necesarias.

Cabe destacar que las herramientas se instalaron en el sistema operativo host ya que de instalarse en el sistema huésped, el atacante podría tomar control de este y borrar la evidencia que necesitamos; aunque también se instaló en el sistema operativo huésped una versión del Snort para hacer parecer que el sistema esta vigilado.

Una vez que se terminó la instalación del sistema Windows XP, se instaló VMware Workstation 4.5.2, este software nos permitió crear un equipo virtual con las características necesarias para la instalación del equipo huésped, además de crear un switch virtual que dará acceso a los dos equipos a la red de manera independiente.

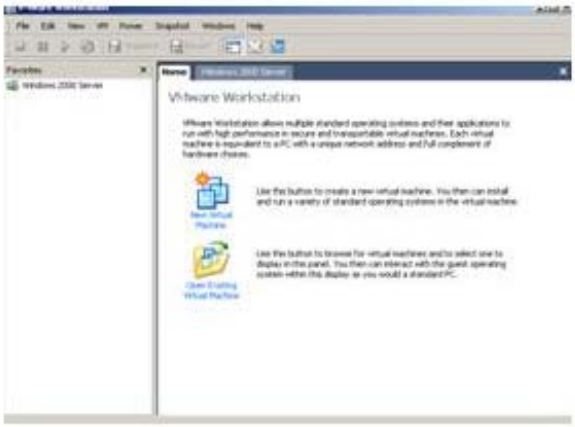


Figura 5.3 VMware

5.4 CONFIGURACION DE SNORT

Este fué instalado en el equipo huésped, como dispositivo de monitoreo, aunque también fue instalado en otro equipo para monitorear la información, por lo tanto snort estará instalado en dos equipos Windows XP (host) y Windows 2000 Professional (huésped).

Antes de instalar Snort, debimos instalar WinPcap (http://winpcap.polito.it), esta es la versión de las librerías LibCap originalmente para sistemas Linux, que recopila muchas funciones necesarias para el sniffer y análisis de paquetes.

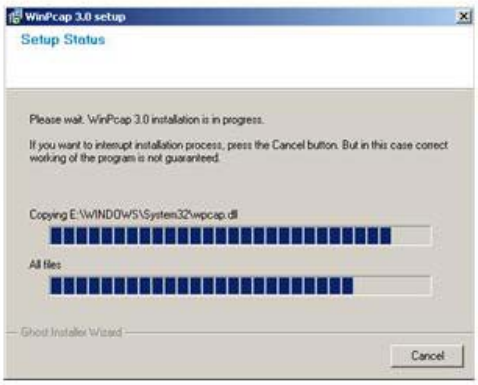


Figura 5.4 Instalación de WinPCap

Una vez instalado WinPcap, podemos proseguir a instalar Snort, el cual existe en varias versiones, por comodidad usaremos la versión que viene en un instalador al cual basta con indicarle si deseamos que se instalen componentes para usar con SQL o Oracle y la ruta de la instalación que para tratar de evitar que el atacante borre los logs en este equipo, lo colocaremos no en la raíz de sistema si no en una carpeta falsa en Archivos de programa: C:\Archivos de programa\WinZipp\Snort

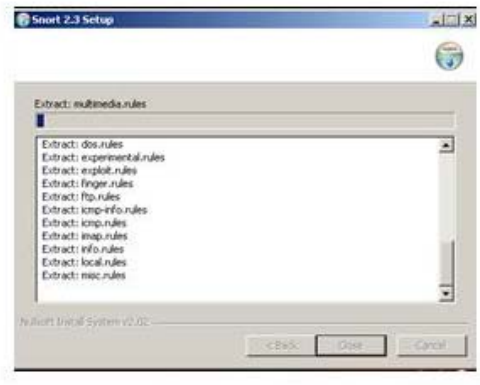


Figura 5.5 Instalación de Snort

El instalador extraerá todos los archivos necesarios para ejecutar Snort así como las reglas de monitoreo preconfiguradas, si queremos agregar mas reglas, es necesario agregarlas en

el archivo de configuración aunque esto resulta un poco complicado además de que las reglas con las que cuenta son suficientes por el momento, así que solo se hicieron algunas modificaciones en el archivo de configuración de snort.

El archivo de configuración de Snort se ubicó en la siguiente ruta:

C:\Archivos de programa\WinZipp\Snort\etc

En archivo de configuración Snort.conf encontraremos texto plano que podemos editar con el Wordpad, lo que deberemos configurar de ser necesario en este archivo es:

1) Establecer las variables de red para nuestra red
2) Configurar los preprocesadores
3) Configurara los plugins de salida
4) Establecer nuestras modificaciones al conjunto de reglas (si es necesario)

1) Establecer las variables de red para nuestra red

Las variables a configurar son las siguientes.

Aquí se especifica la red local, pueden ser especificadas varias redes en esta variable separando cada dirección con una coma.	var HOME_NET 10.10.100.0/24
Aquí se puede especificar la dirección IP con la que se inicializara la interfaz de red cuando inicie Snort. Esta variable puede quedar comentada, pero también puede ser especificada de la siguiente manera.	var HOME_NET $(Initializing Network Interface \Device\NPF_{918B1AE7-212D-4A50-A241-05F1524776C2)
En esta variable se establecen las redes externas, para este caso, usaremos el valor any para todas las redes.	var HOME_NET any
En esta variable estableceremos si tenemos algún servidor DNS en la red, para esta opción usaremos el valor de nuestra misma red así mismo para las demás variables, esto nos sirve para vigilar actividad en servidores de este tipo.	var DNS_SERVERS $HOME_NET var SMTP_SERVERS $HOME_NET var HTTP_SERVERS $HOME_NET var SQL_SERVERS $HOME_NET var TELNET_SERVERS $HOME_NET var SNMP_SERVERS $HOME_NET
Esta variable indica donde deberá buscar Snort las reglas usadas para el IDS, esta se establecerá como una ruta relativa para evitar cualquier problema.	`var RULE_PATH ../rules`

Tabla 5.2 Variables de Snort.conf

2) Configurar los preprocesadores

Los preprocesadotes son como motores que nos ayudarán a detectar actividad relacionada con el flujo de datos en la red, además de que algunos como el Telnet, pueden ser decodificados para poder tener un log de toda la sesión de manera entendible.

Los preprocesadores ya se encuentran activos por defaul, y en este caso se usó la configuración preestablecida de Snort.

3) Configurara los plugins de salida

Esto se refiere a la manera en la que los logs son presentados, la información puede ser mandada a una base de datos para generar estadísticas y un monitoreo mas activo del sistema. En esta ocasión los parámetros son los ya establecidos por Snort, pero agregaremos la línea:

```
output log_tcpdump: tcpdump.log
```

Que nos permitió que los logs también sean generados en el formato de TCPDump, para ser analizados después con ethereal.

4) Establecer nuestras modificaciones al conjunto de reglas (si es necesario)

En este caso tampoco se crearon reglas personalizadas para Snort, se usaron el conjunto de reglas incluido en /Snort/rules asegurándose que esta ruta es la correcta en el archivo de configuración estableciendo la variable `RULE_PATH` en la ruta correcta.

5.5 CONFIGURACION DE ETHERAL

Ethereal cuenta también con una versión para Windows que es la que usaremos en esta ocasión, cuenta con un instalador así que bastara con ejecutarlo en la ruta defaul.

Etheral nos sirve para monitorear el tráfico de la red de manera transparente, lo usamos primero como un Sniffer, para lo cual basto con ejecutar Ethereal y hacer clic en la opción capturar>interfaces, con esto ethereal nos muestra cuales son las interfaces que están activas y por ende en las que podemos escuchar, en la configuración de la interfaz, dejaremos desmarcada la opción de “actualizar los paquetes en tiempo real” ya que esto le resta rendimiento al Sniffer y podría provocar problemas en la captura.

La captura se realizó en modo promiscuo, esto lo configuramos en las opciones de captura de ethereal, y en esta ocasión no se estableció un límite para el tamaño del archivo, sabemos que los archivos generados por ethereal suelen ser pequeños y con una gran cantidad de información.

Una vez instalado Snort en el equipo huésped y en el equipo de monitoreo, y con Ethereal corriendo en el equipo de monitoreo, nuestro escenario esta listo para comenzar con el caso.

5.6 ANALISIS DEL INCIDENTE

El equipo se dejó trabajando durante la noche, mas sin embargo se detectó actividad inusual en el equipo incluyendo el paro del servicio snort, por lo que se procedió de acuerdo a la metodología planteada en el capitulo cuatro.

5.6.1- CONGELACIÓN DE LA ESCENA

Para congelar la escena y de acuerdo con el procedimiento el equipo fue apagado desconectándolo de la corriente, en este caso por ser un equipo virtual en **VMWare**, basta con hacer un stop del sistema operativo, pero antes creando un snapshot del sistema con fines de documentación.

También cabe aclarar, que dependiendo de los servicios que ofrezca el equipo y el tipo de actividad que se detecte en el, será como el **CSIO** deberá tomar la dedición de desconectar el equipo, sacarlo de línea, desconectarlo de la red, o en su caso usar un espejo (Un servidor replicado o redundante) para mantener ciertos servicios en línea.

También se detiene snort en el equipo host con la finalidad de evitar logs innecesarios, pero antes asegurándonos de que toda actividad al equipo host ha cesado; de esta misma forma detenemos el sniffer Ethereal.

5.6.2- RECOLECCIÓN DE EVIDENCIAS

Antes de comenzar con la recolección de logs y clonado del disco se debe de fotografiar la escena del crimen (el site) y se debe de levantar un inventario del equipo (o equipos involucrados). En caso de que se vaya a realizar una investigación de tipo legal a partir de este punto deberán estar presentes los peritos que darán fe en la recolección de la información.

En este caso por tratarse de un honeypot se omitirán las fotografías, se generará la cadena MD5 del disco duro antes de realizar la copia o el dump del disco duro, esto con la finalidad de asegurar la integridad de la información del disco duro.

Para generar las cadenas MD5 se puede ocupar una diversidad de herramientas mencionadas en el capítulo tres, en este caso se usó un disco de emergencia HELIX para iniciar el equipo en modo de solo lectura y generar las cadenas MD5.

Para realizar esto, se tuvo un segundo equipo en el cual ejecutamos una versión de netcat para Windows, esto con la finalidad de transferir el archivo imagen que se encuentra en el equipo virtual en el disco *hda1*.

El equipo comprometido se inició con el disco de emergencia HELIX, una vez que inicio en modo de solo lectura, se usó G*rab,* para crear y transferir la imagen del disco duro, *Grab* tiene en si un conjunto de herramientas como son **md5sum, netcat** y **dd**.

Usamos el siguiente comando para que netcat reciba los datos que le son enviados por *Grab* netcat:

C:\Evidencia>nc –l –p 2006 > DDEvidencia.img

Una vez que *netcat* está listo para recibir los datos que le son enviados, ejecutamos *Grab* y le especificamos que el origen de datos es **/dev/hda**. (Véase video en los anexos) también tendremos que especificar la dirección IP del equipo que va a recibir los datos y el puerto, por supuesto que se genero la respectiva cadena MD5.

Destino: 192.168.44.1:2006
Origen: /Dev/hda

Adicionalmente para evitar cualquier cambio al disco duro virtual también se generaron las cadenas MD5 para el disco duro ya que esta será la que compararemos con la cadena del archivo recibido las cuales deben de ser iguales como se ve en la figura 5.6.

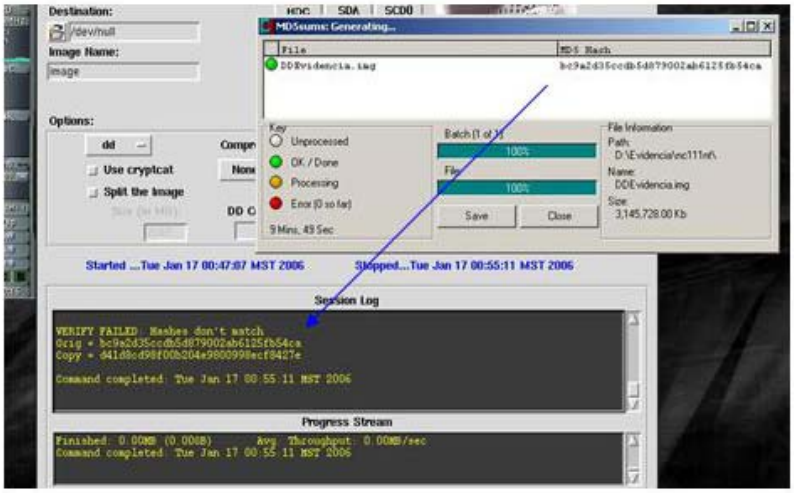


Figura 5.6 Cadenas MD5 en ambos discos

De esta manera tendremos la cadena MD5 para el archivo imagen del disco duro, el cual deberá ser verificado cada que sea necesario para asegurar la autenticidad de la información.

```
# MD5 checksums generated by MD5summer
# Generated 16/01/2006 11:23:40 p.m.

bc9a2d35ccdb5d879002ab6125fb54ca *DDEvidencia.img
```

MD5 para la imagen del disco duro

En este punto también se generaran las cadenas MD5 para todos los archivos de logs:

```
# MD5 checksums generated by MD5summer
(http://www.md5summer.org)
# Generated 17/01/2006 01:13:06 a.m.

610016f0a14084ea556939617c1a7bb0 *alert.ids
716679303154feebfdb608d5317e5827 *snort.log.1137438633
3c218154e192db578beb893e74af048c *snort.log.1137439041
```

MD5 para archivos log de *Snort*

```
# MD5 checksums generated by MD5summer
(http://www.md5summer.org)
# Generated 17/01/2006 01:18:37 a.m.

e58d1775837834dc65cf936ca891cf36 *capturadetrafico
```

MD5 para archivo de Ethereal.

Antes de comenzar con el análisis, se crearán copias de el archivo imagen, y se trabajará con copias del original, también se generarán cadenas MD5 para cada copia con la finalidad de asegurar que son idénticas al original. Son estas copias las que son repartidas a los investigadores de las diferentes áreas y dependencias que cooperan en la investigación.

5.6.3- ANÁLISIS DE LA EVIDENCIA Y DETERMINACIÓN ATAQUE

Para el análisis de la evidencia, comenzaremos con los logs de ethereal y snort, en los cuales podremos encontrar información que nos sirva para determinar como fue realizado el ataque.

Un primer vistazo al archivos generado por Snort, alert.ids, nos muestra que se realizó un ataque de RPC DCOM, como el usado por el gusano Blaster.

```
[**] [1:2251:14] NETBIOS DCERPC Remote Activation bind attempt [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
01/16-13:42:02.281375 192.168.44.1:3206 -> 192.168.44.128:135
```

Tabla 5.6 Alert.ids

En este momento sabemos que el ataque que se realizó fue explotando una vulnerabilidad ya descrita por Microsoft en el boletín MS03-039[12], también aquí podemos ver la dirección IP desde la que se dirigió el ataque, **192.168.44.1** y el ataque se origino desde el puerto **3206.**

Mas adelante, una vez que se ha completado la explotación de la vulnerabilidad, se ejecutó un shell inverso, por lo que existe la posibilidad de que este ataque no haya sido realizado por algún tipo de virus si no haya sido un ataque realizado directamente por un hacker.

En este punto, la persona que esté detrás del ataque o de la creación del virus podría ser juzgado en México bajo los cargos señalados en el artículo 211 y 211bis del código penal federal.

También encontramos un log que nos muestra que el atacante se conectó a los recursos del equipo por medio de NetBios, pero hasta este momento no sabemos exactamente que fue lo que hizo, ya que en ese momento la actividad no se considera fuera de lo usual y el IDS no genera logs de todos los comandos ejecutados, pero el Sniffer ethereal nos muestra cual fue la actividad realizada por el atacante o el virus en cuestión.

```
[**] [1:2466:6] NETBIOS SMB-DS IPC$ unicode share access [**]
[Classification: Generic Protocol Command Decode] [Priority: 3]
01/16-13:48:19.714165 192.168.44.1:3213 -> 192.168.44.128:445
```

5.7 Acceso a los recursos compartidos

Además de todo lo anterior, snort creó registros que indican que el atacante realizó un escaneo de puertos desde el equipo comprometido a la dirección IP 200.36.96.74, por lo que podemos suponer en este momento que se trata de un atacante tratando de triangular una conexión para atacar otro sitio.

```
[**] [1:469:3] ICMP PING NMAP [**]
[Classification: Attempted Information Leak] [Priority: 2]
01/16-14:12:15.669442 192.168.44.128 -> 200.36.96.74
ICMP TTL:54 TOS:0x0 ID:3128 IpLen:20 DgmLen:28
Type:8  Code:0  ID:15422   Seq:6711  ECHO
[Xref => http://www.whitehats.com/info/IDS162]

[**] [122:1:0] (portscan) TCP Portscan [**]
01/16-14:12:34.975971 192.168.44.128 -> 200.36.96.74
PROTO255 TTL:0 TOS:0x0 ID:65269 IpLen:20 DgmLen:167

[**] [122:1:0] (portscan) TCP Portscan [**]
01/16-14:13:19.327124 192.168.44.128 -> 200.36.96.74
PROTO255 TTL:0 TOS:0x0 ID:65485 IpLen:20 DgmLen:167

[**] [122:1:0] (portscan) TCP Portscan [**]
01/16-14:14:19.478303 192.168.44.128 -> 200.36.96.74
PROTO255 TTL:0 TOS:0x0 ID:195 IpLen:20 DgmLen:166
```

5.8 Escaneo de puertos

Hasta aquí el análisis de los logs de snort, en este momento podemos determinar lo siguiente:

- El ataque fue realizado desde la dirección IP 192.168.44.1, amenos que el sniffer muestre algo más.
- Se explotó una vulnerabilidad conocida y común que afecta a los sistemas operativos Windows XP, 2000 y Server ya que estos implementan **RPC.**
- El atacante obtuvo una shell inversa que le permitió realizar diversas actividades de manera aparentemente lícita para el sistema.
- El atacante accedió a los recursos ofrecidos por NetBios.
- El atacante realizó un escaneo de puertos hacia la dirección IP 200.36.96.74

Analizando los logs generados por Ethereal, encontramos el momento en el que es devuelta la shell al atacante.

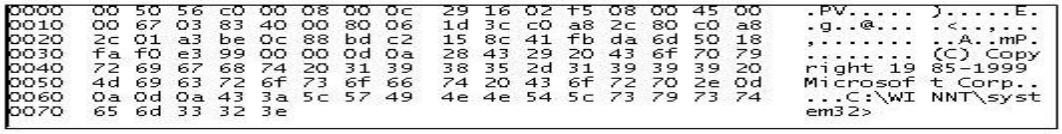


Figura 5.7 Shell devuelto

A partir de aquí analizaremos cual fué la actividad que realizó el atacante y porqué realizó una conexión por NetBios.

Encontramos en el frame 71 que capturó ethereal, que una vez que se explotó la vulnerabilidad, se agregó un usuario llamado “soporte técnico” con la contraseña “s0porte” (figura 5.8), y podemos ver como en el frame 73 el comando es aceptado por el sistema (figura 5.9).

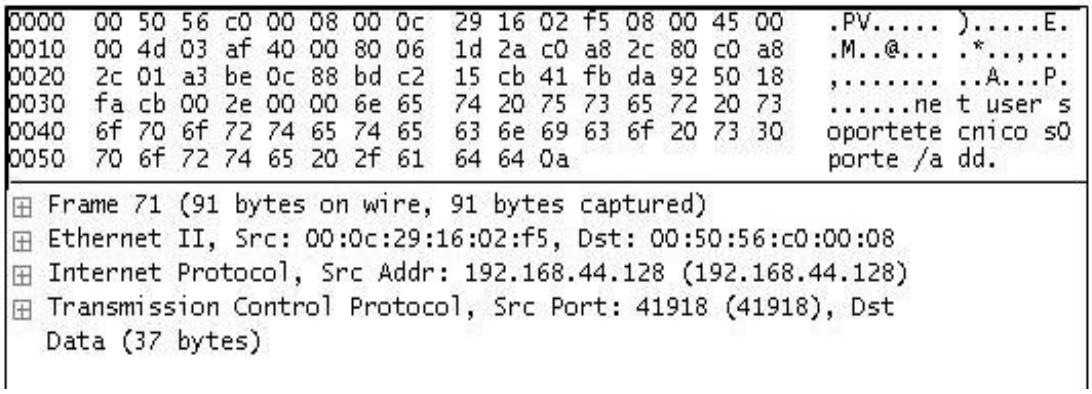


Figura 5.8 Se agrega un nuevo usuario

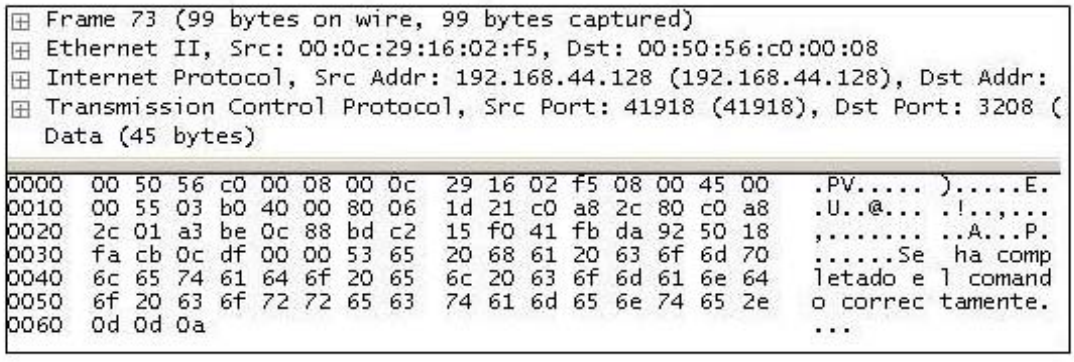


Figura 5.9 Se completa el comando

Ahora sabemos que la intención es la de acceder a los archivos del sistema o quizá subir alguna aplicación ya que como se vio en los logs generados por Snort, posteriormente se ataca a otro sitio.

Una vez qué se agregó un usuario, se comparte la raíz del disco duro, esto permitiría al atacante acceder a todos los directorios del equipo.

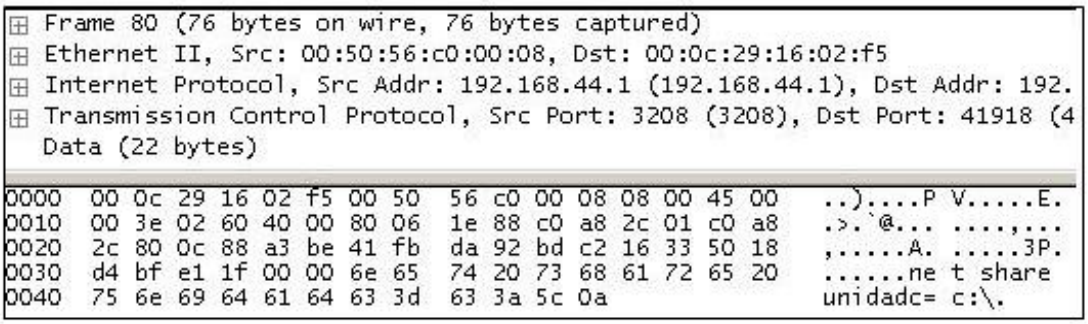


Figura 5.10 Se comparte unidad la C

Inmediatamente que es compartida la unidad se crean en el servidor los archivos de un Keylogger y del escáner de puertos Nmap. (Figura 5.11 y 5.12)

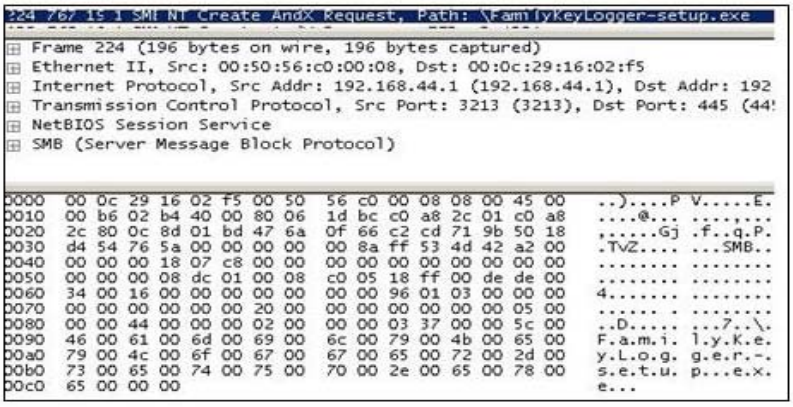
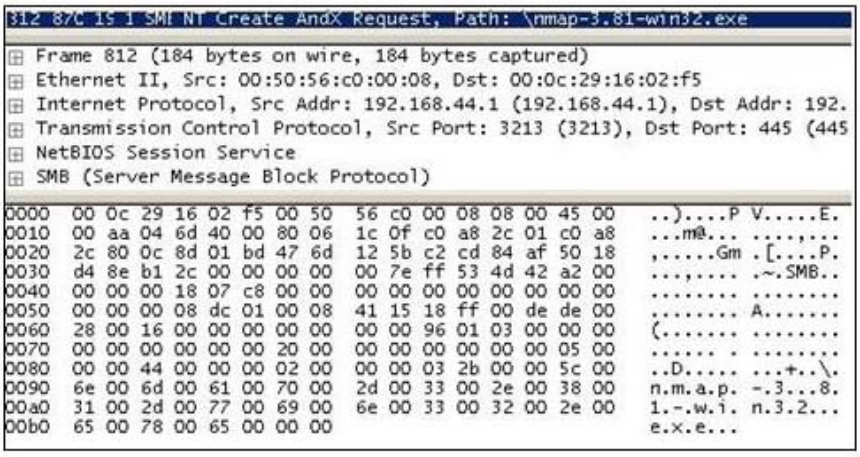


Figura 5.11 KeyLogger



5.12 Nmap

Gracias a los datos generados por Ethereal, podemos saber que el equipo usado por el atacante es un equipo Windows XP versión 2600, esto gracias a que el protocolo netBios requiere de intercambiar esta información.

```
d4   A2..... .5.....
00   ...}.NTL MSSP....
08   ........ .(......
55   . ...MIE QUIPOGRU
00   PO_TRABA JOW.i.n.
00   d.o.w.s.  .2.0.0.
00   2. .2.6. 0.0...W.
00   i.n.d.o. w.s. .2.
00   0.0.2. . 5...1...
     ..
```

Figura 5.13 sistema operativo del atacante

En este momento tenemos ya suficiente información para ser presentada como evidencia, pero aun falta el revisar el disco duro para obtener el software que el atacante puso en nuestro servidor, así como una lista de los archivos modificados del disco duro.

Para hacer esto ocuparemos el software ProDiscover, el cual nos permitirá montar la imagen del disco duro en modo de solo lectura y trataremos de reconstruir la estructura del directorio ya que ethereal también nos muestra que la mayor parte de la actividad se realizó en el directorio Inetpub.

Al abrir el ProDiscover creamos un nuevo caso para iniciar la búsqueda de la información y generar un informe del caso al final. (Véase anexos).
Montamos la imagen del disco duro y notamos que ProDiscover (Figura 5.14) no tiene problema en leer toda la estructura de directorios, por lo que será sencillo encontrar la evidencia que se busca.

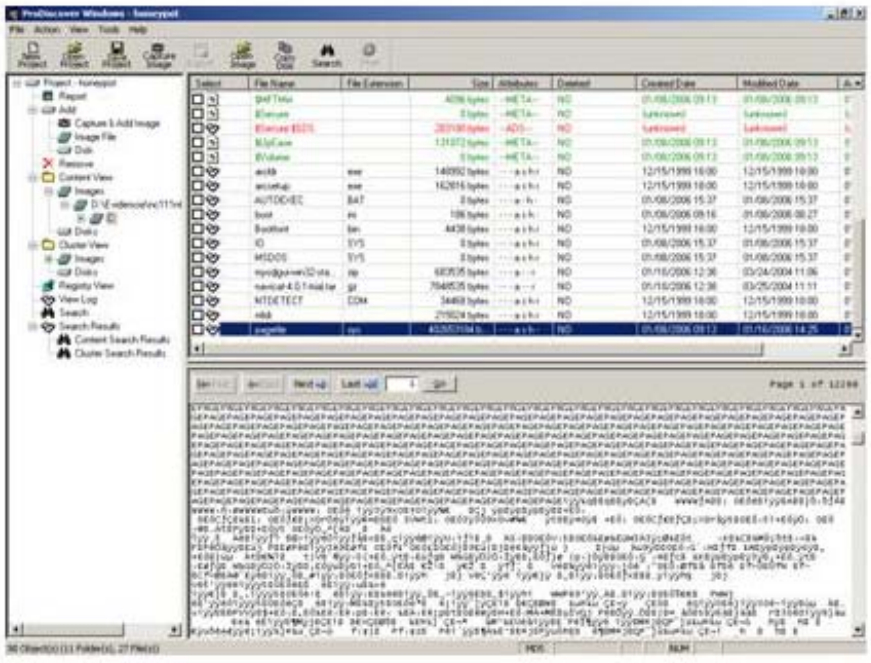


Figura 5.14 análisis del disco duro

Una vez que hemos buscado y seleccionado la información que nos interesa, podemos ver el reporte que ProDiscover genera.

5.7 CONCLUSIONES DEL INCIDENTE

El día 16 de enero aproximadamente a las 14:30 horas se detectó actividad inusual en el sistema TEZCAT, el cual fue instalado como un honeypot para el caso de estudio, con suficiente tráfico en el sistema, se procedió según la metodología al apagado y aseguramiento del equipo y la evidencia.

Después de analizar y recolectar las evidencias se puede concluir lo siguiente:

El ataque fué realizado a las trece horas con cuarenta y ocho minutos del día 16 de enero, el ataque se realizó explotando una vulnerabilidad que provoca un **buffer overflow**, y permite escribir cualquier segmento de memoria en el sistema usando la llamada a procedimiento remoto.

Usando este desbordamiento el atacante envió y colocó en la memoria un shell del sistema operativo, al ejecutarse el servicio de RPC en el grado más alto, la shell obtenida tenía los mismos privilegios que las cuentas de administración de Windows.

Una vez que el shell fué devuelto, se agregó un nuevo usuario llamado “soportetecnico” con el password “s0porte”, además de compartir toda la raíz del sistema, la cuenta fué usada para colocar algunos archivos en el directorio \Inetpub; una lista de los archivos se encuentra en la tabla 5.3.

Archivo	MD5
C:\Inetpub\FamilyKeyLogger-setup.exe	2B8931296D158493F00036894B151D6E
C:\Inetpub\HomeKeyLogger-setup.exe	301B76BCCA77855CA1D44136FB2FD435
C:\Inetpub\KeyLogger.Dll	432A012D496DF3B33D55B3D54172BA35
C:\Inetpub\KeyLogger.exe	4F2D146582D432E9557D3C48315E87A3
C:\Inetpub\README.TXT	8B7884126AB54CE7945CFC42956BCADC
C:\Inetpub\nmap_performance.reg	75D89ECF430FE2291FEC68769C43DD43
C:\Inetpub\nmap.xsl	8E7A7D8B1E91E6694766DD5575455DE1
C:\Inetpub\nmap.exe	69927C556A0DBE3B51D7FFD6F63E4E27
C:\Inetpub\nmap-services	58A456C7630EF7C16FB82553CC14A0BD
C:\Inetpub\nmap-service-probes	05EE8D80E4A6DC03A12D5CADF6B74278
C:\Inetpub\nmap-rpc	A365EDEEBBAFAECA057397C19CF94C2D
C:\Inetpub\nmap-protocols	51CE065D1A40AADE914E7FE3658EE852
C:\Inetpub\nmap-os-fingerprints	8CE620F3B78AF130BDC5BD15B87D6556
C:\Inetpub\nmap-mac-prefixes	7768B1E21B494F062334BB5E78EBA5F0
C:\Inetpub\nmap-3.81-win32.exe	03157B895E773EE62A3080DF321D5DA1

Tabla 5.3 Archivos que el atacante coloco en el servidor

Después de subir los archivos a TEZCAT, se realizó un escaneo de puertos a la dirección IP 200.36.96.74, después de esto el recurso de red fue desconectado al igual que el shell, dos archivos ejecutables que fueron colocados en el directorio \Inetpub pero no fueron ejecutados y no hay rastro de que se haya intentado eliminar o copiar algún archivo de TEZCAT por lo que se concluye que solo se quería usar para realizar un ataque a otro sitio,

esta es una práctica común para evitar ser rastreado y es posible que el ataque haya venido de otro equipo comprometido y no del equipo del atacante.

Resumen del análisis:

Detalles del acceso no Autorizado, formato Efence

<table>
<tr><td colspan="2">Dirección origen aparente:
• Dirección IP : 192.168.44.1
• Ubicación del host:
❑ Domestico
❑ Externo
❑ Interno</td></tr>
<tr><td colspan="2">Sistema Primario (s) involucrado:
• Dirección IP o dirección de subred. 192.168.44.128
• Versión del sistema operativo(s) Windows 2000 Server</td></tr>
<tr><td colspan="2">Otros sistemas afectados o redes involucradas (IPs y SOs): 200.36.96.74</td></tr>
<tr><td>Método del ataque:
❑ Sniffed/guessed/cracked password
❑ Accesos de equipos de confianza
❑ Explotación de vulnerabilidad
❑ Herramienta de Hacking
❑ Utilidad o puerto atacado
❑ Ingeniería social</td><td>Detalles: se exploto la vulnerabilidad conocida Como RPC DCOM buffer overflow, detallada En el boletín de seguridad de Microsoft MS03-039, ataque realizado directamente sobre El puerto 445.</td></tr>
<tr><td colspan="2">Otros sistemas afectados o redes (IPs y SOs):</td></tr>
<tr><td colspan="2">Metodo del ataque:
❑ Sniffed/guessed/cracked password
❑ Accesos de equipos de confianza
❑ Explotación de vulnerabilidad
❑ Herramienta de Hacking
❑ Utilidad o puerto atacado
❑ Ingeniería social</td></tr>
<tr><td colspan="2">❑ Nivel de acceso obtenido— Administrador</td></tr>
<tr><td colspan="2">Método de operación del ataque (Descripción mas detallada de lo que fue hecho):
Se ataco específicamente el puerto 445 del servidor, aparentemente pudo a ver sido realizado con alguna herramienta por la velocidad con la que se realize el ataque.
Se cargaron al equipo un scanner de equipos y un key logger, aunque el key logger no fue usado, el scanner Conocido como Nmap fue usado para escanear otro equipo con dirección IP 200.36.96.74.

Las herramientas usadas fueron copias desde un recurso compartido por windows, lo que denota poca Experiencia por parte del atacante.

Las herramientas fueron localizadas en el directorio c:\Inetpub\ por lo que se puede suponer que el Atacante tenia intenciones de publicar un sitio web para acceder a estas herramientas.

Se creo la cuenta soportetecnico con el password s0porte

Aparentemente se pretendía inciar un ataque a la dirección IP 200.36.96.74, porque se realizo un scaneo de puertos a esta IP, pero no se realizo ningun otro ataque.</td></tr>
</table>

Detalles del acceso no autorizado (Continuación)

Como fue detectado: ❑ Otro sitio ❑ Equipo de respuesta a incidentes ❑ Archivo de logs ❑ Sniffer /Sistema de detección de intrusos ❑ Sistema de detección de intrusos ❑ Comportamiento anómalo ❑ Usuario ❑ Disparo de alarmas ❑ TCP Wrappers ❑ TRIPWIRE® ❑ Otros	Detalles: La detección fue hecha al analizar los archivos De log de el sistema de detccion de intrusos Snort, para el análisis completo se ocuparon los logs generados por el analizador de trafico ethereal.

Extractos de los Logs:

[**] [1:2251:14] NETBIOS DCERPC Remote Activation bind attempt [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
01/16-13:42:02.281375 192.168.44.1:3206 -> 192.168.44.128:135
TCP TTL:128 TOS:0x0 ID:583 IpLen:20 DgmLen:244 DF
AP Seq: 0x41F99310 Ack: 0xBDBFEA62 Win: 0xD590 TcpLen: 20

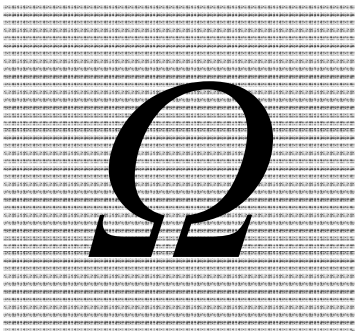
Remedio *(que fue hecho para regresar el sistema a un funcionamiento confiable):* ❑ Parches aplicados ❑ Scaners de seguridad ❑ Software de seguridad instalado ❑ Servicios y aplicaciones innecesarias removidas ❑ Reinstalación del SO ❑ Restauración de una copia de respaldo ❑ Se movió alguna aplicación a otro equipo ❑ Se incremento el espacio en disco ❑ Se reubico atrás de un firewall o router ❑ Archivos detectados removidos ❑ Troyano detectado y removido ❑ Se dejo sin cambios para monitoreo ❑ Otro	Details: Ya que el sistema estaba diseñado para Ser un Honeynet simple, para su reparación solo Se reinstalo el sistema operativo y se aplicaron Los parches recomendados en el boletín de Seguridad.

Comentarios adicionales:
El tiempo estimado del ataque fue de 52 minutos entre las 13:42 y las 14:24 horas.

Este reporte es solo para fines ilustrativos dentro de este trabajo, se incluyen los detalles del incidente pero Debido a que este fue un incidente simulado los detalles pueden ser pocos aparentemente.

En los extractos de los logs solo se agrego el log donde se detalla la explotación de la vulnerabilidad, en un anexo se incluye el archivo de logs completo.

Aparte de la información anterior, no se encontró evidencia de otra actividad o ataque, incluyendo la base de datos MySQL que se encontraba instalada.



CONCLUSIONES

Este trabajo, ha presentado una nueva área de las tecnologías de información, como lo es la forensia informática, se han presentado las bases que todo investigador debe tener, desde cómo surgió y cuales son los pasos para realizar una investigación, apoyando todo en el uso de herramientas especializadas que se presentaron en el capítulo tres.

El último capítulo de este trabajo presenta el caso práctico en el que se culmina con los objetivos de trabajo de presentar una metodología de investigación forense.

Se considera que, se ha cumplido con el objetivo de mostrar al lector que todo aquel que vulnera un sistema, de alguna manera, está cometiendo un delito y debe ser castigado, este castigo variará dependiendo de muchos factores entre estos el grado de conocimiento del que lo comete, pero aun falta mucho por hacer en el aspecto legal, ya que como se mencionó en el capítulo dos, la ley es demasiado inexacta, siendo ejemplo de esto la falta de definición de “sistema informático” y “mecanismo de seguridad”, permitiendo la evasión de la justicia en algunos casos y la mala aplicación de esta en otros.

Aunado a los “agujeros” que existen en las leyes, tenemos el problema de la falta de personal especializado en estas áreas, por lo que es muy complicado encontrar un abogado que sepa lo suficiente de informática para llevar uno de estos casos, por lo que es mas fácil encontrar informáticos aprendiendo leyes para convertirse en investigadores y que decir de los peritos en esta área; este es otro de los problemas al no contar, con una jurisprudencia informática en el país.

Es importante el incluir este tipo de procedimientos dentro de la definición de las políticas de seguridad de una organización, Por último se debe agregar que se ha presentado en este

trabajo una “Metodología” y para ser aplicada en una organización con un cierto grado de éxito, se deberá convertir en un procedimiento de la organización y todo lo que implica, como la definición de las políticas de seguridad, definición de los procedimientos legales y sanciones.

Aunque actualmente instituciones como la UNAM o la PFP están haciendo su parte en la investigación de los delitos informáticos, la UNAM con su HoneyNET y la PFP con la policía cibernética, donde realmente hace falta trabajo es en las organizaciones, en las instituciones y escuelas, ya que al no contarse con reglamentos bien definidos sobre cómo se deben tratar estos casos, en pocas ocasiones se da el seguimiento y no llegan a reportarse los incidentes o ataques de las que son objeto.

Como trabajo posterior a este, se puede agregar la investigación forense usando ingeniería inversa, ya que en muchas ocasiones el o los atacantes usan programas que se encuentran “disfrazados” o empaquetados de tal forma que pueden pasar desapercibidos, estos mecanismos de análisis sugieren un gran conocimiento de lenguajes ensambladores para múltiples procesadores Intel, sparc, RISC, etc. Y por el gran tamaño del tema quedo fuera de esta investigación.

REFERENCIAS BIBLIOGRÁFICAS

[1] Shinder Littlejohn, Debra. Scene of the Cybercrime, *"Computer forensics handbook"* Ed. SYNGRESS.

[4] Código penal federal de los estados unidos mexicanos.
Cámara de Diputados del H. Congreso de la Unión

[5] Gaceta parlamentaria No. 48 año 2004, jueves 22 de Abril.
Cámara de Diputados del H. Congreso de la Unión

[6] George Mohay, Alison Anderson, Byron Collie, Olivier De Vel, Rod Mckemmish. *"Computer and intrusion Forensics",* Ed. Artech House.

[7] K. Shim, Jae, Qureshi A. Anique, Siegel G. Joel, *"The Internacional Handbook of Computer Security"*, Ed. Glenlake Publishing Company.

[8] Marcella J. Albert, Greenfield S. Robert, *"Cyber Forensics",* Ed. Auerbach publications a CRC press company.

[9] Schweitzer, Douglas, *"Incident Response, computer forensics toolkit"*, Ed.WILEY.

Esquema de direccionamiento IP RFC1918

REFERENCIAS ELECTRÓNICAS

[3] http://www.informatica-juridica.com/legislacion/mexico.asp

[2] http://www.efense.com

[10] http://www.insecure.org

[11] http://www.honeynet.org

[12] http://www.microsoft.com/technet

http://www.ethereal.com

http://www.snort.org

http://www.honeynet.org

http://www.sysinternals.com

http://www.dibsusa.com

http://www.paraben-forensics.com

http://www.opensourseforensics.org

http://www.encase.com

http://www.e-evidence.info

http://www.fish.com

ANEXOS

A continuación se presenta el archivo **alert.ids** generado por Snort durante el monitoreo del Honeypod, se presenta el archivo completo para análisis del lector.

Alert.ids

[**] [1:538:14] NETBIOS SMB IPC$ unicode share access [**]
[Classification: Generic Protocol Command Decode] [Priority: 3]
01/16-13:35:55.844001 192.168.44.1:3204 -> 192.168.44.128:139
TCP TTL:128 TOS:0x0 ID:524 IpLen:20 DgmLen:124 DF
AP Seq: 0x3C97210D Ack: 0xB8C04A1A Win: 0xD3B7 TcpLen: 20

[**] [1:2251:14] NETBIOS DCERPC Remote Activation bind attempt [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
01/16-13:42:02.281375 192.168.44.1:3206 -> 192.168.44.128:135
TCP TTL:128 TOS:0x0 ID:583 IpLen:20 DgmLen:244 DF
AP Seq: 0x41F99310 Ack: 0xBDBFEA62 Win: 0xD590 TcpLen: 20
[Xref => http://www.microsoft.com/technet/security/bulletin/MS03-039.mspx][Xref =>
http://cgi.nessus.org/plugins/dump.php3?id=11835][Xref => http://cgi.nessus.org/plugins/dump.php3?id=11798][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2003-0715][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2003-
0605][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2003-0528][Xref =>
http://www.securityfocus.com/bid/8458][Xref => http://www.securityfocus.com/bid/8234]

[**] [1:3276:1] NETBIOS DCERPC IActivation little endian bind attempt [**]
[Classification: Generic Protocol Command Decode] [Priority: 3]
01/16-13:42:02.281375 192.168.44.1:3206 -> 192.168.44.128:135
TCP TTL:128 TOS:0x0 ID:583 IpLen:20 DgmLen:244 DF
AP Seq: 0x41F99310 Ack: 0xBDBFEA62 Win: 0xD590 TcpLen: 20

[**] [1:2351:10] NETBIOS DCERPC ISystemActivator path overflow attempt little endian unicode [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
01/16-13:42:02.466160 192.168.44.1:3207 -> 192.168.44.128:135
TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:1720
AP Seq: 0xBDC18536 Ack: 0x41FB3266 Win: 0xFAF0 TcpLen: 20
[Xref => http://www.microsoft.com/technet/security/bulletin/MS03-026.mspx][Xref =>
http://cgi.nessus.org/plugins/dump.php3?id=11808][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2003-0352][Xref
=> http://www.securityfocus.com/bid/8205]

[**] [1:2466:6] NETBIOS SMB-DS IPC$ unicode share access [**]
[Classification: Generic Protocol Command Decode] [Priority: 3]
01/16-13:47:27.122675 192.168.44.1:3209 -> 192.168.44.128:445
TCP TTL:128 TOS:0x0 ID:623 IpLen:20 DgmLen:138 DF
AP Seq: 0x46BF527B Ack: 0xC22EE55E Win: 0xD3BB TcpLen: 20

[**] [1:2466:6] NETBIOS SMB-DS IPC$ unicode share access [**]
[Classification: Generic Protocol Command Decode] [Priority: 3]
01/16-13:48:11.619399 192.168.44.1:3212 -> 192.168.44.128:445
TCP TTL:128 TOS:0x0 ID:641 IpLen:20 DgmLen:138 DF
AP Seq: 0x47692181 Ack: 0xC2CC40F8 Win: 0xD3BB TcpLen: 20

[**] [1:2466:6] NETBIOS SMB-DS IPC$ unicode share access [**]
[Classification: Generic Protocol Command Decode] [Priority: 3]
01/16-13:48:19.714165 192.168.44.1:3213 -> 192.168.44.128:445
TCP TTL:128 TOS:0x0 ID:669 IpLen:20 DgmLen:138 DF
AP Seq: 0x476A0A99 Ack: 0xC2CD6D77 Win: 0xD413 TcpLen: 20

[**] [1:2466:6] NETBIOS SMB-DS IPC$ unicode share access [**]
[Classification: Generic Protocol Command Decode] [Priority: 3]
01/16-13:50:42.028716 192.168.44.1:3213 -> 192.168.44.128:445
TCP TTL:128 TOS:0x0 ID:1089 IpLen:20 DgmLen:138 DF
AP Seq: 0x476D099B Ack: 0xC2CD7D6F Win: 0xD517 TcpLen: 20

[**] [1:1042:8] WEB-IIS view source via translate header [**]
[Classification: access to a potentially vulnerable web application] [Priority: 2]
01/16-13:50:42.445126 192.168.44.1:3215 -> 192.168.44.128:80
TCP TTL:128 TOS:0x0 ID:1094 IpLen:20 DgmLen:190 DF
AP Seq: 0x49A1710D Ack: 0xC4DC3914 Win: 0xD590 TcpLen: 20
[Xref => http://www.securityfocus.com/bid/1578][Xref => http://www.whitehats.com/info/IDS305]

[**] [1:1042:8] WEB-IIS view source via translate header [**]
[Classification: access to a potentially vulnerable web application] [Priority: 2]
01/16-13:50:49.930062 192.168.44.1:3215 -> 192.168.44.128:80
TCP TTL:128 TOS:0x0 ID:1095 IpLen:20 DgmLen:208 DF
AP Seq: 0x49A171A3 Ack: 0xC4DC3A9D Win: 0xD407 TcpLen: 20
[Xref => http://www.securityfocus.com/bid/1578][Xref => http://www.whitehats.com/info/IDS305]

[**] [1:538:14] NETBIOS SMB IPC$ unicode share access [**]
[Classification: Generic Protocol Command Decode] [Priority: 3]
01/16-14:08:00.388092 192.168.44.1:3218 -> 192.168.44.128:139
TCP TTL:128 TOS:0x0 ID:6201 IpLen:20 DgmLen:124 DF
AP Seq: 0x58DCD5DB Ack: 0xD3008E74 Win: 0xD3B7 TcpLen: 20

[**] [1:1917:6] SCAN UPnP service discover attempt [**]
[Classification: Detection of a Network Scan] [Priority: 3]
01/16-14:09:45.616430 192.168.44.1:3220 -> 239.255.255.250:1900
UDP TTL:4 TOS:0x0 ID:6292 IpLen:20 DgmLen:161
Len: 133

[**] [1:1917:6] SCAN UPnP service discover attempt [**]
[Classification: Detection of a Network Scan] [Priority: 3]
01/16-14:09:48.619760 192.168.44.1:3220 -> 239.255.255.250:1900
UDP TTL:4 TOS:0x0 ID:6311 IpLen:20 DgmLen:161
Len: 133

[**] [1:1917:6] SCAN UPnP service discover attempt [**]
[Classification: Detection of a Network Scan] [Priority: 3]
01/16-14:09:51.633863 192.168.44.1:3220 -> 239.255.255.250:1900
UDP TTL:4 TOS:0x0 ID:6333 IpLen:20 DgmLen:161
Len: 133

[**] [1:469:3] ICMP PING NMAP [**]
[Classification: Attempted Information Leak] [Priority: 2]
01/16-14:12:15.669442 192.168.44.128 -> 200.36.96.74
ICMP TTL:54 TOS:0x0 ID:3128 IpLen:20 DgmLen:28
Type:8 Code:0 ID:15422   Seq:6711 ECHO
[Xref => http://www.whitehats.com/info/IDS162]

[**] [122:1:0] (portscan) TCP Portscan [**]
01/16-14:12:34.975971 192.168.44.128 -> 200.36.96.74
PROTO255 TTL:0 TOS:0x0 ID:65269 IpLen:20 DgmLen:167

[**] [122:1:0] (portscan) TCP Portscan [**]
01/16-14:13:19.327124 192.168.44.128 -> 200.36.96.74
PROTO255 TTL:0 TOS:0x0 ID:65485 IpLen:20 DgmLen:167

[**] [122:1:0] (portscan) TCP Portscan [**]
01/16-14:14:19.478303 192.168.44.128 -> 200.36.96.74
PROTO255 TTL:0 TOS:0x0 ID:195 IpLen:20 DgmLen:166

[**] [122:1:0] (portscan) TCP Portscan [**]
01/16-14:15:20.832905 192.168.44.128 -> 200.36.96.74
PROTO255 TTL:0 TOS:0x0 ID:397 IpLen:20 DgmLen:164

[**] [122:1:0] (portscan) TCP Portscan [**]
01/16-14:16:26.421344 192.168.44.128 -> 200.36.96.74
PROTO255 TTL:0 TOS:0x0 ID:559 IpLen:20 DgmLen:165

[**] [122:1:0] (portscan) TCP Portscan [**]
01/16-14:17:28.479271 192.168.44.128 -> 200.36.96.74
PROTO255 TTL:0 TOS:0x0 ID:602 IpLen:20 DgmLen:164

[**] [122:1:0] (portscan) TCP Portscan [**]
01/16-14:18:28.820927 192.168.44.128 -> 200.36.96.74
PROTO255 TTL:0 TOS:0x0 ID:644 IpLen:20 DgmLen:166

[**] [122:1:0] (portscan) TCP Portscan [**]
01/16-14:19:30.677615 192.168.44.128 -> 200.36.96.74
PROTO255 TTL:0 TOS:0x0 ID:687 IpLen:20 DgmLen:164

[**] [122:1:0] (portscan) TCP Portscan [**]
01/16-14:20:32.644613 192.168.44.128 -> 200.36.96.74

PROTO255 TTL:0 TOS:0x0 ID:732 IpLen:20 DgmLen:165

[**] [122:1:0] (portscan) TCP Portscan [**]
01/16-14:21:34.408043 192.168.44.128 -> 200.36.96.74
PROTO255 TTL:0 TOS:0x0 ID:780 IpLen:20 DgmLen:165

[**] [122:1:0] (portscan) TCP Portscan [**]
01/16-14:22:36.061464 192.168.44.128 -> 200.36.96.74
PROTO255 TTL:0 TOS:0x0 ID:822 IpLen:20 DgmLen:165

[**] [122:1:0] (portscan) TCP Portscan [**]
01/16-14:23:35.606015 192.168.44.128 -> 200.36.96.74
PROTO255 TTL:0 TOS:0x0 ID:864 IpLen:20 DgmLen:165

[**] [122:1:0] (portscan) TCP Portscan [**]
01/16-14:24:40.056930 192.168.44.128 -> 200.36.96.74
PROTO255 TTL:0 TOS:0x0 ID:4660 IpLen:20 DgmLen:165

[**] [1:895:7] WEB-CGI redirect access [**]
[Classification: Attempted Information Leak] [Priority: 2]
01/16-14:35:45.373791 192.168.44.128:1394 -> 207.46.18.94:80
TCP TTL:128 TOS:0x0 ID:5994 IpLen:20 DgmLen:308 DF
AP Seq: 0xF26FB5F9 Ack: 0x72782E50 Win: 0xFAF0 TcpLen: 20
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2000-0382][Xref => http://www.securityfocus.com/bid/1179]

[**] [1:895:7] WEB-CGI redirect access [**]
[Classification: Attempted Information Leak] [Priority: 2]
01/16-14:35:47.096876 192.168.44.128:1394 -> 207.46.18.94:80
TCP TTL:128 TOS:0x0 ID:6003 IpLen:20 DgmLen:282 DF
AP Seq: 0xF26FB705 Ack: 0x72786860 Win: 0xF9E8 TcpLen: 20
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2000-0382][Xref => http://www.securityfocus.com/bid/1179]

[**] [1:895:7] WEB-CGI redirect access [**]
[Classification: Attempted Information Leak] [Priority: 2]
01/16-14:35:47.801924 192.168.44.128:1394 -> 207.46.18.94:80
TCP TTL:128 TOS:0x0 ID:6008 IpLen:20 DgmLen:328 DF
AP Seq: 0xF26FB7F7 Ack: 0x727869BE Win: 0xF88A TcpLen: 20
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2000-0382][Xref => http://www.securityfocus.com/bid/1179]

[**] [1:895:7] WEB-CGI redirect access [**]
[Classification: Attempted Information Leak] [Priority: 2]
01/16-14:35:52.941176 192.168.44.128:1399 -> 64.4.21.125:80
TCP TTL:128 TOS:0x0 ID:6059 IpLen:20 DgmLen:375 DF
AP Seq: 0xF2993094 Ack: 0x6034CF5 Win: 0xFAF0 TcpLen: 20
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2000-0382][Xref => http://www.securityfocus.com/bid/1179]

[**] [1:895:7] WEB-CGI redirect access [**]
[Classification: Attempted Information Leak] [Priority: 2]
01/16-14:35:54.535153 192.168.44.128:1398 -> 64.4.21.125:80
TCP TTL:128 TOS:0x0 ID:6074 IpLen:20 DgmLen:320 DF
AP Seq: 0xF2928F31 Ack: 0x4DE68FF8 Win: 0xFAF0 TcpLen: 20
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2000-0382][Xref => http://www.securityfocus.com/bid/1179]

[**] [1:895:7] WEB-CGI redirect access [**]
[Classification: Attempted Information Leak] [Priority: 2]
01/16-14:35:54.940632 192.168.44.128:1399 -> 64.4.21.125:80
TCP TTL:128 TOS:0x0 ID:6076 IpLen:20 DgmLen:370 DF
AP Seq: 0xF29931E3 Ack: 0x60386C1 Win: 0xFAF0 TcpLen: 20
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2000-0382][Xref => http://www.securityfocus.com/bid/1179]

[**] [1:538:14] NETBIOS SMB IPC$ unicode share access [**]
[Classification: Generic Protocol Command Decode] [Priority: 3]
01/16-14:40:04.940842 192.168.44.1:3055 -> 192.168.44.128:139
TCP TTL:128 TOS:0x0 ID:13194 IpLen:20 DgmLen:124 DF
AP Seq: 0x79ACE88F Ack: 0xF61D3681 Win: 0xD50E TcpLen: 20

[**] [1:1917:6] SCAN UPnP service discover attempt [**]
[Classification: Detection of a Network Scan] [Priority: 3]
01/16-14:44:20.724196 192.168.44.1:3212 -> 239.255.255.250:1900
UDP TTL:4 TOS:0x0 ID:14356 IpLen:20 DgmLen:161
Len: 133

[**] [1:1917:6] SCAN UPnP service discover attempt [**]

[Classification: Detection of a Network Scan] [Priority: 3]
01/16-14:44:23.757664 192.168.44.1:3212 -> 239.255.255.250:1900
UDP TTL:4 TOS:0x0 ID:14362 IpLen:20 DgmLen:161
Len: 133

[**] [1:1917:6] SCAN UPnP service discover attempt [**]
[Classification: Detection of a Network Scan] [Priority: 3]
01/16-14:44:26.758652 192.168.44.1:3212 -> 239.255.255.250:1900
UDP TTL:4 TOS:0x0 ID:14365 IpLen:20 DgmLen:161
Len: 133

Anexo 2

A continuación se presenta el formato usado por E-fense, para recolectar la evidencia en sitio; puede ser usado como apoyo en la elaboración de un formato propio para el seguimiento de casos dentro de cualquier organización como investigador interno:

Cyber Incident Reporting Form

Requested for All Incident Types.

❑ Site under attack ☐ Incident investigation in progress ☐ Incident closed

What assistance do you require:
- ❑ Immediate call
- ❑ None needed at this time
- ❑ CERT to follow-up on all affected sites
- ❑ CERT to contact the "hacking" site(s)

Site involved (*Name & Acronym*): _____

POC for Incident: Name _____
- E-mail address _____STU-III number_____
- 7 x 24 contact information _____

Alternative POC for Incident: Name _____
- E-mail address _____STU-III number_____
- 7 x 24 contact information _____

Type of Incident (*provide additional details on the appropriate form):*
- ❑ Malicious code: virus, Trojan horse, worm.
- ❑ Probes/scans (non-malicious data gathering--recurring, massive, unusual).
- ❑ Attack (successful/unsuccessful intrusions including scanning with attack packetsDenial-of-service event.
- ❑ High embarrassment factor
- ❑ Deemed significant by site

Date and time incident occurred (s*pecify time zone):*_____

A summary of what happened:

Type of service, information, or project compromised *(please provide specifics):*
- ❑ Sensitive unclassified such as privacy, proprietary, or source selection _____
- ❑ Other unclassified _____

Damage done:
- Numbers of systems affected _____
- Nature of loss, if any_____ System downtime_____
- Cost incident (unknown, none, <$10K, $10K - $50K, >$50K)

Name other sites contacted (Department of _____ entities, other agencies, law enforcement):

Details for Malicious Code

Apparent source: ❑ Diskette, CD, etc. ❑ E-mail attachment ❑ Software download	
Primary system or network involved: • IP addresses or sub-net addresses _____ • OS version(s) _____ • NOS version(s) _____	
Other affected systems or networks (IPs and OSs):	
Type of malicious code (*include name if known*): ❑ Virus _____ ❑ Trojan horse _____ ❑ Worm _____ ❑ Joke program _____ ❑ Other _____	
❑ Copy sent to CERT	
Method of Operation (*for new malicious code*): ❑ Type—macro, boot, memory resident, polymorphic, self encrypting, stealth ❑ Payload ❑ Software infected ❑ Files erased, modified, deleted, encrypted-- *any special significance to these files* ❑ Self propagating via E-mail ❑ Detectable changes ❑ Other features	Details:
How detected:	
Remediation *(what was done to return the system(s) to trusted operation):* ❑ Anti-virus product gotten, updated, or installed for automatic operation ❑ New policy institute on attachments ❑ Firewall or routers or E-mail servers updated to detect and scan attachments	Details:
Additional comments:	

Details for Probes and Scans

Apparent source:
- IP address _____
- Host name _____
- Location of attacking host:
  - ❑ Domestic
  - ❑ Foreign
  - ❑ Insider

Primary system(s)/network(s) involved:
- IP addresses or sub-net addresses _____
- OS version(s) _____
- NOS version(s) _____

Other affected systems or networks (IPs and OSs):

Method of Operation:	Details:
❑ Ports probed/scanned ❑ Order of ports or IP addresses scanned ❑ Probing tool ❑ Anything that makes this probe unique	
How detected: ❑ Another site ❑ Incident response team ❑ Log files ❑ Packet sniffer ❑ Intrusion detection system ❑ Anomalous behavior ❑ User	Details:

Log file excerpts:

Additional comments:

Details for Unauthorized Access

Apparent source:
- IP address
- Location of host:
  - ❑ Domestic
  - ❑ Foreign
  - ❑ Insider

Primary system(s) involved:
- IP addresses or sub-net addresses
- OS version(s)
- NOS version(s)

Other affected systems or networks (IPs and OSs):

Avenue of attack:	Details:
❑ Sniffed/guessed/cracked password ❑ Trusted host access ❑ Vulnerability exploited ❑ Hacker tool used ❑ Utility or port targeted ❑ Social engineering	

Other affected systems or networks (IPs and OSs):

Avenue of attack:
- ❑ Sniffed/guessed/cracked password
- ❑ Trusted host access
- ❑ Vulnerability exploited
- ❑ Hacker tool used
- ❑ Utility or port targeted
- ❑ Social engineering

❑ Level of access gained—root/administrator, user

Method of Operation of the attack *(more detailed description of what was done):*
- ❑ Port(s) or protocol(s) attacked
- ❑ Attack tool(s) used, if known
- ❑ Installed hacker tools such as rootkit, sniffers, l0phtcrack, zap
- ❑ Site(s) hacker used to download tools
- ❑ Where hacker tools were installed
- ❑ Established a service such as IRC
- ❑ Looked around at who is logged on
- ❑ Trojanned, listed, examined, deleted, modified, created, or copied files
- ❑ Left a backdoor
- ❑ Names of accounts created and passwords used
- ❑ Left unusual or unauthorized processes running
- ❑ Launched attacks on other systems or sites
- ❑ Other

Details for Unauthorized Access (Continued)

How detected: ❑ Another site ❑ Incident response team ❑ Log files ❑ Packet sniffer/intrusion detection software ❑ Intrusion detection software ❑ Anomalous behavior ❑ User ❑ Alarm tripped ❑ TCP Wrappers ❑ TRIPWIRE® ❑ Other	Details:
Log file excerpts:	
Remediation *(what was done to return the system(s) to trusted operation):* ❑ Patches applied ❑ Scanners run ❑ Security software installed: ❑ Unneeded services and applications removed ❑ OS reloaded ❑ Restored from backup ❑ Application moved to another system ❑ Memory or disk space increased ❑ Moved behind a filtering router or firewall ❑ Hidden files detected and removed ❑ Trojan software detected and removed ❑ Left unchanged to monitor hacker ❑ Other	Details:
Additional comments:	

Details For Denial-Of-Service Incident

Apparent source:
- IP address _____
- Location of host:
  - ❑ Domestic
  - ❑ Foreign
  - ❑ Insider

Primary system(s) involved:
- IP addresses or sub-net address _____
- OS version(s) _____
- NOS version(s) _____

Other affected systems or networks (IPs and OSs):

Method of Operation:	Details:
❑ Tool used ❑ Packet flood ❑ Malicious packet ❑ IP Spoofing ❑ Ports attacked ❑ Anything that makes this event unique	
Remediation *(what was done to protect the system(s)):* ❑ Application moved to another system ❑ Memory or disk space increased ❑ Shadow server installed ❑ Moved behind a filtering router or firewall ❑ Other	Details:

Log file excerpts:

Additional comments:

GLOSARIO

***.dll**
Librería de enlace dinámica, contiene los procedimientos usados por programas en Windows

ARP spoofing
Se refiere a la suplantación de una dirección MAC, falsificando peticiones y respuestas ARP

ASCII
American Standard Code for Information Interchange. Es de facto el estándar del World Wide Web para el código utilizado por computadoras para representar todas las letras (mayúsculas, minúsculas, letras latinas, números, signos de puntuación, etc.). El código estándar ASCII es de 128 letras representadas por un digito binario de 7 posiciones (7 bits), de 0000000 a 1111111.

BBS
Servicio que consiste en el intercambio de información con otros usuarios, descarga archivos etc., sin estar conectados a Internet, generalmente por MODEM, por lo que actualmente están cayendo en desuso.

Bit
Unidad mínima de almacenamiento de la información cuyo valor puede ser 0 ó 1; o bien verdadero o falso.

Buffer overflow
Es un desbordamiento de la memoria, un error de programación usado comúnmente por hackers o virus para obtener acceso a sistemas.

Byte
Conjunto de 8 bits el cual suele representar un valor asignado a un carácter.

Cibercrimen
Crimen en el que se ven envueltos mecanismos o medios informáticos, ya sea como medio para el crimen o como el objetivo de este.

ciberespacio
Término concebido por el escritor William Gibson en su novela de ciencia ficción "Neuromancer" (1984) con el propósito de describir un mundo de redes de información. Actualmente es utilizado para referirse al conjunto de información digital y a la comunicación que se realiza a través de las redes, un espacio en el cual casi todo lo que contiene información; o puede transmitirla, debe ser incluido.

ClickKidie
Nuevo termino usado para referirse a aquellos que descargan programas creados por hackers mas experimentados que permiten ejecutar algún tipo de ataque con un solo click del Mouse.

CRC
Código de Redundancia Ciclica, usado para verificar la integridad de los datos, usado en diversos medios de almacenamiento y transmisión digital.

CSIO
Chief Security Information Officer, es el jefe de seguridad informática en la organización, responsable de la toma de decisiones criticas.

dialup
Conexión temporal que se establece usando un emulador de Terminal y un módem; en oposición a conexión dedicada o permanente, la cual es establecida entre ordenadores por línea telefónica normal y realiza una conexión de datos a través de una línea telefónica

DNS
Domain Name Server, Servidor de nombres de dominio, es el encargado de resolver los nombres de dominio a direcciones de red o viceversa.

DNS spoofing
Se refiere a la suplantación o falsificación de las respuestas de un servidor DNS real, usado para realizar ataques de robo de sesión.

Dump
Se refiere a descargar lo contenido en algún medio, ya sea la memoria RAM o los discos rígidos

DoS
Incidente en el cual un usuario o una organización se ven privados de un recurso que normalmente podrían usar. Habitualmente, la pérdida del servicio supone la indisponibilidad de un determinado servicio de red, como el correo electrónico, o la pérdida temporal de toda la conectividad y todos los servicios de red. En los peores casos, por ejemplo, un sitio Web accedido por millones de personas puede verse forzado temporalmente a cesar de operar. Un ataque de denegación de servicio puede también destruir programas y archivos de un sistema informático. Aunque normalmente es realizado de forma intencionada y maliciosa, este tipo de ataques puede también ocurrir de forma accidental algunas veces. Si bien no suele producirse robo de información estos ataques pueden costar mucho tiempo y dinero a la persona u organización afectada.

EIP
Apuntador de programa en el lenguaje ensamblador, este registro le indica al procesador la dirección de memoria en la que se encuentra la siguiente dirección a ejecutarse.

Exploit
Se refiere a un programa o el código fuente de un programa que explota una vulnerabilidad o error de programación en un sistema.

FAT
File Allocation Table. Tabla de asignación de archivos, usado en los sistemas de almacenamiento para organizar la manera en la que son guardados los archivos en el medio, actualmente se esta descontinuando su uso en los discos duros pero se ha extendido su uso a los sistemas de memorias portátiles.

FedCIRC
The Federal Computer Incident Reporting Center, Organización dedicada a dar seguimiento a los incidentes de tipo informático.

Gusano
Programa informático que se auto duplica y auto propaga. En contraste con los virus, los gusanos suelen estar especialmente escritos para redes. Los gusanos de redes fueron definidos por primera vez por Shoch & Hupp, de Xerox, en la revista ACM Communications (Marzo 1982). El primer gusano famoso de Internet apareció en Noviembre de 1988 y se propagó por sí solo a más de 6.000 sistemas a lo largo de Internet.

IDS
Intrusion detection system, sistema de detección de intrusos, un sistema que ocupa diversos mecanismo para detectar el patrón de un ataque a una red o un sistema en particular.

IP address
Internet Protocol, Protocolo de Internet. Conjunto de reglas que regulan la transmisión de paquetes de datos a través de Internet. El más ampliamente utilizado es el Internet Protocol Suite, comúnmente conocido como TCP / IP. Es un protocolo DARPA que proporciona transmisión fiable de paquetes de datos sobre redes. El nombre TCP / IP proviene de dos protocolos importantes de

la familia, el Transmission Control Protocol (TCP) y el Internet Protocol (IP). Todos juntos llegan a ser más de 100 protocolos diferentes. El IP es la dirección numérica de una computadora en Internet de forma que cada dirección electrónica se asigna a una computadora conectada a Internet y por lo tanto es única. La dirección IP esta compuesta de cuatro octetos como por ejemplo, 132.248.53.10

IP spoofing
Suplantación de una dirección IP

ISP
Organización que provee la conexión de computadoras a Internet, ya sea por líneas dedicadas o por líneas conmutadas.

Kbps
Unidad de medida de la velocidad de transmisión por una línea de telecomunicación. Cada kilobit esta formado por mil bits.

KBps
Unidad de medida de la capacidad de transmisión de una línea de telecomunicación equivalente a mil bytes aunque actualmente es usado como 1024 (dos elevado a la 10) bytes.

Keylogger
Programa diseñado para guardar la información tecleada por el usuario, actualmente existen de modo físico y de modo lógico.

Live Boot CD
Sistema capas de iniciar directamente desde un CD, usado en la forensia para iniciar el sistema sin modificar los datos existentes en el disco duro.

MAC address
Direccion "fisica" de una tarjeta de red, esta definida por seis pares de números exadecimales de los cuales los primeros tres indican el fabricante.

MACtimes

MD5
Cadena alfanumérica generada a partir de un algoritmo matemático que garantiza que la información no ha sido modificada en uno solo de sus bits.

MFT
Master File Table, tabla maestra de archivos, usado en sistemas Windows para organizar la manera en la que se almacenan los datos en un disco duro.

NewBie
Termino usado para nombrar a los inexpertos en técnicas de Hacking o seguridad informática.

NIDS
Network Intrusion Detection System, sistema de detección de intrusos en red, generalmente consta de nodos dispersos que monitorean el comportamiento del trafico en la red para intentar identificar posibles ataques.

NTFS
New Technologi File System, sistema de archivos de nueva tecnología, implementado en sistemas NT y posteriores, cuenta con diversos mecanismos de seguridad y mejoras con respecto a su antecesor FAT, como es autentificación, compresión de datos de manera transparente y encriptación de datos.

Outsorcing
Termino que se refiere a contratar a una empresa o persona especializada para realizar algún tipo de trabajo para otra, se delega la responsabilidad de ese servicio o trabajo.

Password
Conjunto de caracteres alfanuméricos que le permite a un usuario el acceso a un determinado recurso o la utilización de un servicio dado. Se destaca que la contraseña no es visible en la pantalla al momento de ser tecleada con el propósito de que sólo pueda ser conocida por el usuario.

PDA
Personal Digital Assitant (Asistente Digital Personal) - Ordenador de pequeño tamaño cuya principal función era, en principio, mantener una agenda electrónica. No obstante, cada vez más se va confundiendo con los ordenadores de mano y de palma

PGP
Pretty Good Privacy - Privacidad Bastante Buena. Conocido programa de libre distribución, escrito por Phil Zimmermann, el cual impide, mediante técnicas de criptografía, que archivos y mensajes de correo electrónico puedan ser leídos por otros. Su finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.

phreaking
Se refiere al acto de usar técnicas que permitan usar el sistema telefónico sin restricciones, ya sea con fines de hacking o solo para evadir el pago del servicio.

portscan
Escaneo de puertos, se refiere a la identificación de los servicios que se están ejecutando en un equipo determinado, es el paso previo a un ataque.

Pruebas de penetracion (Penetration Testing)
Se refiere a realizar diversas pruebas de ataque sobre los sistemas de una organización con la finalidad de encontrar los puntos débiles y corregirlos antes que la red sea atacada de manera real, generalmente realizada por empresas ajenas a la organización.

Puerto
Número que aparece tras un nombre de dominio en una URL. Dicho número va precedido del signo (dos puntos). Canal de entrada/salida de una computadora.

RPC
Remote Procedure Call, llamada a procedimientos remotos, inicialmente implementado en sistemas Unix, y posteriormente usado en sistemas Windows, ofrece gran flexibilidad a la administración de sistemas de manera remota, pero en los sistemas Windows es uno de los servicios que mas vulnerabilidades publicadas tiene de nivel critico.

ScriptKiddie
Se le llama así al que sin tener pleno conocimiento de técnicas de seguridad o programación, es capas de ejecutar un script para atacar una red o un servicio.

script
Secuencia de comandos que se le dan a un módem con el propósito de configurarlo (velocidad, compresión de datos, etc) o para realizar tareas específicas (llamar al proveedor, colgar, etc). A veces es necesario modificar un script o cadena de inicio la cual establece las condiciones iniciales del módem (por ejemplo cambiar ATDT que establece una línea telefónica por tonos a ATDP que indica una línea telefónico por pulsos, etc.)

Shell code
Línea de comandos, programado en lenguaje ensamblador, cuando un atacante logra acceso a un

sistema generalmente necesitara enviar un shellcode para poder ejecutar sus comandos.

Symbian
Sistema operativo de código abierto usado en sistemas móviles como celulares y PDA's.

Sniffer
Programa que literalmente husmea en la red, escuchando todo el transito en ella.

spoofing
Procedimiento que cambia la fuente de origen de un conjunto de datos en una red, por ejemplo, adoptando otra identidad de remitente con el fin de engañar a un servidor firewall.

TCP/IP
Pila de protocolos en los que se sustenta la comunicación por Internet.

TIC's
Tecnologías de Información y Comunicación.

Wireless
Sin cables, se refiere a la disponibilidad de equipos y servicios para poder comunicarse usando como medio el aire.

xDSL
Tecnología de transmisión que permite que los hilos telefónicos de cobre convencionales transporten hasta 16 Mbps mediante técnicas de compresión. Hay diversas modalidades de esta tecnología, tales como ADSL, HDSL y RADSL, siendo la Línea de Suscripción Asimétrica Digital (ADSL) la más utilizada actualmente.