Detección y recuperación de procesos en el puesto de usuario

Tapia Pocoata Jhep Omar
Universidad Mayor De San Andrés
Carrera De Informática
Simulación de Sistemas
pedro_mc@hotmail.com

RESUMEN

En El siguiente articulo esta orientado a la utilización de la informática forense en el campo de la tecnología computacional y su transmisión de datos entre estas últimos tiempos esta se convirtió en una necesidad de cualquier índole de la población, por las características que ofrece de comunicación y otros tipos de servicio que ofrece se ha vuelto de mucha importancia sin duda ya que esta tecnología se ha vuelto una herramienta poderosa tanto de comunicación de gestión etc. Es importante remarcar los peligros que acechan a su alrededor tanto de los famosos virus (software malicioso) y otros como los hacker y personas inescrupulosas que hacen daño al usuario independientemente de quien lo use por esta razón la informática forense se convirtió en un policía de esta tecnología el cual puede regular e finalizar el tipo de uso que le dan a esta por ser una herramienta fácil de fracturar en muchos aspectos.

Palabras clave

Network, evidencia, Wifi, Network forense.

1. INTRODUCCIÓN

La información es el activo más valioso que poseemos en la sociedad actual. Ésta es cada vez más importante para el desarrollo de las empresas y de negocios exitosos a través de la implementación de sistemas de información. Para proteger la información surge una nueva ciencia, la Informática Forense; ésta persigue objetivos preventivos así como reactivos, una vez se ha dado una infiltración en el sistema.

La Informática forense es una ciencia relativamente nueva y no existen estándares aceptados. Existen proyectos que están en desarrollo como el C4PDF (Código de Prácticas para Digital Forensics)

Actualmente la tecnología esta avanzando a pasos agigantados, y con ella la forma en que todos operamos. Ahora toda la información es almacenada en los ordenadores de manera automática, a diferencia de épocas anteriores en donde la información se almacenaba de manera manual y en papel. Esto conlleva cierto tipo de ventajas y desventajas.

Las ventajas son evidentes, mayor facilidad en el manejo de la información, rapidez en la recolección y análisis de la misma, alta disponibilidad tanto en tiempo como en localidad. Sin embargo, las desventajas y riesgos en los que se incurre no son tan obvios. Entre estos, la vulnerabilidad de la información a ser borrada, la fácil replicación de la información, la explotación de la información por vulnerabilidades en el sistema.

Con todo el riesgo que se corre al manejar información debemos de tener una manera de protegernos y de proteger a las personas de las que mantenemos información. Para poder garantizar las políticas de seguridad y la protección de la información y las tecnologías que facilitan la gestión de la información surge la Informática forense.

Hace ya unos 6 años que la conectividad inalámbrica tomo bríos acelerados en cuanto a su desarrollo masivo y no se diga en cuanto a su adopción. Hoy es evidente que las redes inalámbricas han llegado a las casas y a lugares que antes no se hubiera pensado como hoteles, carreteras, aeropuertos e incluso en el interior de algunos aviones.

Es claro que la tecnología inalámbrica es muy útil y el mayor beneficio es la movilidad de los usuarios de tal manera que puedan estar consultando Internet o el correo electrónico desde una computadora con la cual se utilizan otras herramientas de trabajo (software) que en una pda o dispositivo móvil con funcionalidades de teléfono celular no se tienen.

Sin embargo, el avance de la tecnología inalámbrica hoy atiende la conectividad a Internet pero a una escala mayor, es decir, con la tecnología actual inalámbrica o WiFi por sus siglas en ingles el beneficio es para aquellos que tienen acceso a este recurso ya sea con una computadora portátil o con una pda equipada con wifi, pero cuando se trata de conectar instituciones o personas que no tienen acceso a un medio de conectividad en su entorno por estar en lugares muy apartados o bien porque simplemente los servicios de conectividad a Internet como celular, adsl o cable son escasos, las cosas se complican y la brecha digital se hace mas grande.

Para ello, la tecnología wimax llego para precisamente permitir la conectividad inalámbrica de banda ancha (alta velocidad) a esos sitios que carecen de medios que permitan a la gente y a las organizaciones a conectarse a Internet y en consecuencia a los servicios que con ello se ofrecen.

Es evidente que la tecnología wimax no llega de la nada. Para ello se requiere que “alguien” ponga la infraestructura para poder conectar a todos.

Ese alguien tiene que ser una empresa privada, el gobierno

o bien una combinación. Sin embargo, es importante mencionar que la tecnología es de vanguardia y que las empresas privadas apenas están pensando como hacer las cosas.

2. OBJETIVOS

2.1. La compensación de los daños causados por los criminales o intrusos

Las diferentes acciones corruptas deben de ser sancionadas pero debe de realizarse una compensación por los daños causados por la infiltración en las transmisiones de datos, robo de datos etc. Cualquier delito informático que afecte al usuario por otro usuario de la tecnología el fin es de precautelar la integridad de uso de la información para uno mismo, sin que se vea afectado por la intromisión de otro y que este lo utilice tanto en contra de los intereses de un o para su favor.

2.2. La persecución y procesamiento judicial de los criminales

Existen varios delitos y uno de estos y mas frecuentes es la de meter las narices en computadores de empresas, usuarios donde se tiene información de alto peligro si cae en manos maliciosas se le hace a través de uno de los procesos de muchos que hay para acceder a esta es menéame.

Este servicio de Geolocalización de IP, que es muy curioso. En nuestro sector de la seguridad ya se sabe desde hace algún tiempo que, gracias al sistema de asignación de direcciones IP de la IANA, es relativamente sencillo asignar una ubicación física a una dirección IP concreta, y conocer detalles como el ISP y el sistema de asignación. Pero este te lo da todo hecho, la precisión, digamos, que el punto buscado está dentro de un círculo de unos 10 kilómetros de radio del indicado.

Este es uno de los pasos a seguir un IP de donde se hubiese cometido el delito por el cual también sabremos cual es su situación en el momento que intervino en el PC del usuario.

En este ejemplo hemos hablado de evidencias físicas, en la ciencia forense tradicional hay varios tipos de evidencias físicas.

Evidencia transitoria. como su nombre indica es temporal por naturaleza, por ejemplo un registro, tiempo, o unas letras sobre la direccionamiento (un objeto blando o cambiante).

Evidencia curso o patrón: producidas por contacto, por ejemplo la trayectoria de un dato, un patrón de rotura o brake de enlace, patrones de posicionamiento ordenador, etc.

Evidencia condicional causadas por una acción o un evento en la escena del crimen, por ejemplo la localización de una evidencia en relación con el cuerpo (ordenador), una ventana abierta o cerrada, una frecuencia encendida o apagada, dirección del IP, etc.

El proceso judicial será determinado por leyes creadas sobre estas tecnologías las cuales determinaran los castigos a los criminales encontrados por la informática forense.

2.3. La creación y aplicación de medidas para prevenir casos similares

En el mundo no es posible calcular los daños que se realizan por día de un ordenador a otro claro esta conducidos por personas inescrupulosas, pero una de las formas si bien vale el termino es poniéndole cerrojos a los ordenadores, no si bien el firewall (cortafuegos) seria una de las muchas aplicaciones de seguridad y otros que responden a otros tipos de manipulación cibernética.

No podemos tener el control total de lo que pasa en nuestro ordenador pero teniendo antecedentes de infiltración y sus pasos a seguir se puede contrarrestar con una previa implementación computacional para que estos no se puedan pasear libremente en nuestras narices el recopilar, suprimir o vaya saber que daño nos puedan causar los inescrupulosos.

3. NETWORK FORENSE

Forensia en redes, es un escenario aún más complejo, pues es necesario comprender la manera como los protocolos, configuraciones e infraestructuras de comunicaciones se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento particular. Esta conjunción de palabras establece un profesional que entendiendo las operaciones de las redes de computadores, es capaz, siguiendo los protocolos y formación criminalística, de establecer los rastros, los movimientos y acciones que un intruso ha desarrollado para concluir su acción. A diferencia de la definición de computación forense, este contexto exige capacidad de correlación de evento, muchas veces disyuntos y aleatorios, que en equipos particulares, es poco frecuente.

Es la captura, almacenamiento y análisis de los eventos de una red, para descubrir el origen de un ataque o un posible incidente.

3.1. Criterios de admisibilidad

En legislaciones modernas existen cuatro criterios que se deben tener en cuenta para analizar al momento de decidir sobre la admisibilidad de la evidencia: la autenticidad, la confiabilidad, la completitud o suficiencia, y el apego y respeto por las leyes y reglas del poder judicial .

Autenticidad. Una evidencia digital será autentica siempre y cuando se cumplan dos elementos:

Primero, demostrar que dicha evidencia ha sido generada y registrada en el lugar de los hechos

Segundo, la evidencia digital debe mostrar que los medios originales no han sido modificados, es decir, que la los registros corresponden efectivamente a la realidad y que son un fiel

reflejo de la misma.

A diferencia de los medios no digitales, en los digitales se presenta gran volatilidad y alta capacidad de manipulación. Por esta razón es importante aclarar que es indispensable verificar la autenticidad de las pruebas presentadas en medios digitales contrario a los no digitales, en las que aplica que la autenticidad de las pruebas aportadas no será refutada, de acuerdo por lo dispuesto por el artículo 11 de la ley 446 de 1998: "Autenticidad de documentos. En todos los procesos, los documentos privados presentados por las partes para ser incorporados a un expediente judicial con fines probatorios, se reputarán auténticos, sin necesidad de presentación personal ni autenticación. Todo ello sin perjuicio de lo dispuesto en relación con los documentos emanados de terceros" .

Para asegurar el cumplimiento de la autenticidad se requiere que una arquitectura exhiba mecanismos que certifiquen la integridad de los archivos y el control de cambios de los mismos.

Confiabilidad: Se dice que los registros de eventos de seguridad son confiables si provienen de fuentes que son "creíbles y verificable". Para probar esto, se debe contar con una arquitectura de computación en correcto funcionamiento, la cual demuestre que los logs que genera tiene una forma confiable de ser identificados, recolectados, almacenados y verificados.

Una prueba digital es confiable si el "sistema que lo produjo no ha sido violado y estaba en correcto funcionamiento al momento de recibir, almacenar o generar la prueba" . La arquitectura de computación del sistema logrará tener un funcionamiento correcto siempre que tenga algún mecanismo de sincronización del registro de las acciones de los usurarios del sistema y que a posea con un registro centralizado e íntegro de los mismos registros.

Suficiencia o completitud de las pruebas: Para que una prueba esté considerada dentro del criterio de la suficiencia debe estar completa. Para asegurar esto es necesario "contar con mecanismos que proporcionen integridad, sincronización y centralización" para lograr tener una vista completa de la situación. Para lograr lo anterior es necesario hacer una verdadera correlación de eventos, la cual puede ser manual o sistematizada.

Apogeo y respeto por las leyes y reglas del poder judicial: Este criterio se refiere a que la evidencia digital debe cumplir con los códigos de procedimientos y disposiciones legales del ordenamiento del país. Es decir, debe respetar y cumplir las normas legales vigentes en el sistema jurídico.

3.4 Manipulación de la evidencia digital

Es importante tener presente los siguientes requisitos que se deben cumplir en cuanto a la manipulación de la evidencia digital.

Hacer uso de medios forenses estériles (para copias de información)

Mantener y controlar la integridad del medio original. Esto significa, que a la hora de recolectar la evidencia digital, las acciones realizadas no deben cambiar nunca esta evidencia.

Cuando sea necesario que una persona tenga acceso a evidencia digital forense, esa persona debe ser un profesional forense.

Las copias de los datos obtenidas, deben estar correctamente marcadas, controladas y preservadas. Y al igual que los resultados de la investigación, deben estar disponibles para su revisión.

Siempre que la evidencia digital este en poder de algún individuo, éste será responsable de todas la acciones tomadas con respecto a ella, mientras esté en su poder.

Las agencias responsables de llevar el proceso de recolección y análisis de la evidencia digital, serán quienes deben garantizar el cumplimiento de los principios anteriores.

4. CONCLUSIONES

En conclusión los datos generados ya sea un byte deben de estar en buen resguardo ya que estos corren el peligro de ser capturados por otros que no tienen que tener interés en el dato, no es posible que en una tecnología creciente como el de internet y su uso correspondiente de los ordenadores no nos preocupemos al 100% de los riesgos que corremos dentro de la red causado por otras personas o incluso por el sistema puede ser fallos lógicos, pero el mayor temor que se tiene es que seamos monitoreados por otros quienes buscan arruinar o utilizar la información para si mismos, lo cual es preocupante no se puede dejar a la ligera hasta un simple hola, una fotografía etc. Tantos son las acciones que se realizan por una persona o institución y pero si se trata de dinero en medio de toda las acciones es imprescindible tomar acciones de prevención, el cual nos puede ser de mucha ayuda la informantica forense ya que esta como técnica de investigación nos puede dar pautas para reducir la proliferación de los malos usuarios que ponen en peligro nuestro accionar dentro de las TIC's.

8. REFERENCIAS

[1]Informática Forense - Fouz Blog.htm

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

[3]http://www.topremium.info/