NETWORK SECURITY MONITORING COMO MÉTODO DE PENETRATION TESTING

Marin Rojas Diana Carolina
Universidad Piloto de Colombia
Bogotá D.C, Colombia
dicamaro@gmail.com

Resumen **- En este artículo se plasma la posibilidad de uso de una metodología forense llamada networking security monitoring para descubrir y determinar las distintas vulnerabilidades presentes en la red de una organización, y con ello determinar políticas o medidas para garantizar la seguridad de la información. Para que esta metodología sea exacta se acompañara con la técnica de recolección de evidencia digital para tener aún más garantías de que las muestras recolectadas cumplan con lo establecido por la comunidad científica y enfocada a la seguridad de la información. Esta metodología puede suplir en algunos casos las técnicas conocidas para el descubrimiento de las vulnerabilidades y en dado caso, ser una forma de penetration testing, pero esta no quiere suplir o desplazar otras metodologías conocidas sino fortalecerlas.**

Palabras Clave **- Network Security Monitoring, administración de la evidencia digital, forense, vulnerabilidades, incidentes y metodología.**

Abstract **- This article discusses the possibility of using forensic methodology called networking security monitoring to detect and identify various vulnerabilities in the network of an organization, thereby determining policies or measures to guarantee the information security. For this methodology should be accurate, go with the technique of digital evidence collection for even more assurance that the samples collected to comply with the provisions of scientific community and focused on information security. This methodology can supplement in some cases the known for the discovery of vulnerabilities and techniques in such case be a form of penetration testing, but this does not replace or displace other known methodologies but rather strengthen them.**

Index Terms **- Network Security Monitoring Administration of digital evidence, forensic, vulnerabilities, incidents and methodology.**

I. INTRODUCCIÓN

En la actualidad, las organizaciones encuentran distintas metodologías para buscar e identificar las distintas vulnerabilidades presentes en la red o dado en caso ya existen software especializado para encontrar las diferentes vulnerabilidades tecnológicas; con ello y con el objetivo de mejorar los sistemas de seguridad de información, las organizaciones encuentran varias metodologías, que se ajusten a sus políticas, entre ellas están la 27001, ISACA, cobit, entre otros. En la mayoría de estas organizaciones se empieza a definir la metodología cuando no se ha producido un evento que haya afectado seriamente la información de la organización, pero ¿qué pasaría si en la organización ocurre un incidente de seguridad de la información y posterior pérdida, fuga, duplicación de la misma?, ¿es posible a través de métodos forenses identificar las vulnerabilidades que dieron como consecuencia del incidente informático?, ¿ésta detección puede servir, tanto a los ingenieros de seguridad de la información como a los peritos e investigadores para determinar la vulnerabilidad que causo el incidente?. Esta búsqueda no implica la detección de vulnerabilidades en el sistema afectado, sino también en todos los sistemas que involucra la organización de acuerdo a los resultados.

Las técnicas forenses son adecuadas para recolectar, identificar, determinar y realizar un análisis y detectar así las distintas vulnerabilidades que afectaron a las organizaciones, estas técnicas no solo sirven para recolectar evidencia y analizarla dentro de un caso de un incidente informático, que involucra un daño, robo, destrucción, perdida entre otros de datos sensibles. Las técnicas forenses son los que en algún momento nos ayudan a determinar cómo, que, quien, cuando y porque del incidente.

A caso ¿son vulnerabilidades del sistema y/o política de seguridad?, es por ¿algún sistema que no estaba correctamente monitoreado que causo esto? y si es así podrá determinarse si fueron consecuencia de la creación errada de políticas de seguridad, error de monitoreo, de ser así, nacen inquietudes como ¿porque no lo pude determinar antes?, ¿se pudo prevenir estos hechos si se hubiera controlado la vulnerabilidad?, dudas que salen después de un incidente de seguridad son las que con las mismas técnicas forenses podemos resolver.

Los sistemas y técnicas forenses no deben ser de uso exclusivo cuando sucede un incidente informático en las organizaciones sino también una medida de simulacro para prevenir estos incidentes. Estas técnicas no deben ser de uso exclusivo para determinar quién y cómo se realizó la acción. Por lo tanto podemos usarlos como un elemento de fortalecimiento, para mejorar la capacidad de análisis de los profesionales de administración de sistemas de seguridad de la información, mejorando la infraestructura y administración de la seguridad informática.

II. QUÉ ES NETWORK SECURITY MONITORING (NMS)

En concepto de varios analistas, NSM no es una herramienta, sino una metodología de captura de información para que sea

analizada y usada para determinar diferentes vulnerabilidades, por medio de un análisis y luego responder a diferentes intrusiones que aparecen en la red. Los cuatro niveles son:

- Datos estadísticos.
- Datos de sesión.
- Trazas completas del tráfico de red.
- Alertas.

Para ello, usa un ciclo sencillo donde primero realiza una captura de tráfico a esto se le llama recolección, luego de realizar una observación y análisis a esta recolección, a continuación se desarrolla la identificación en donde evalúan diferentes eventos puntuales (sistemas, usuarios, conexiones, entre otros) para así llegar a una validación de estos datos en donde si la organización sufrió un ataque de pérdida o alteración de datos nos mostrarán diferentes alertas y notificaciones, donde después de determinar las conclusiones podemos dar un escalamiento que permite la identificación de las vulnerabilidades presentes en la red, que en definitiva son las posibles causantes de los incidentes de seguridad de la información. Este proceso se puede observar en la figura 1.

Fig. 1: Forma de recolección de datos por el NSM [2]

Según el mismo desarrollador de la idea Richard Bejtlich sostiene que para NSM "necesitamos un alto tráfico de red de calidad, a partir de el, se llevará a cabo las investigaciones de seguridad" [1] por lo tanto, él explica que la creación de esta metodología puede ser una recolección de diferentes tráficos de red, desde diferentes sitios del mismo, no perdiendo lo importante de NSM, que es plasmar la historia real contada por el mismo autor es decir la misma organización.

NMS no es considerado como una herramienta sino como una metodología que utiliza varias herramientas para llegar a un fin, descubrir inconsistencias o eventos extraños que hacen que una red sea insegura. Esta metodología relativamente nueva en el área forense se basa en la necesidad de complementar el uso de un sistema de detección de intrusos o en sus siglas en ingles IDS (Instruction Detection System) con otras herramientas que permitan a los especialistas descubrir, monitorear cambios o reglas estructurales para la protección de la información. No es necesario que se use herramientas precisas sino que se utilicen de forma adecuada para detectar anormalidades o evidencia de eventos que pueden afectar o vulnerar la red de una organización.

NSM a partir de cuatro formas de recolectar datos evalúa todo el tráfico que se presenta en una red, una definición más precisa es: "NSM es la recolección, análisis y escalamiento de indicadores y advertencias para detectar y responder a intrusiones" [1].

III. HISTORIA DE NMS

El siguiente texto, sobre la historia de NMS, es una recopilación realizada por el creador durante varios seminarios, tomado de la misma experiencia que comparte con los demás "pioneros", como él lo describe; desde su blog.

NSM se inició como una disciplina informal usando el desarrollo de Todd Heberlein del monitor de seguridad de la red. El NSM fue el primer sistema de detección de intrusos en utilizar el tráfico de red como su principal fuente de datos para generar alertas. Heberlein y otros trabajaron en la universidad de California en Davis desde 1988 hasta 1995, sobre NSM, aunque en 1991 la investigación inicial de NSM y el desarrollo se había completado.

La air force computer emergency response team (AFCERT) fue la primera organización en seguir los principios de NSM de manera informal. El AFCERT fue creado el 1 de octubre de 1992, en parte como resultado del gusano morris 1988.

El equipo comenzó a trabajar como parte del centro criptológico con apoyo de la fuerza aérea en la base aérea kelly en San Antonio Texas. Cuando la air force warfare center (AFIWC) se activó el 10 de septiembre de 1993, la AFCERT se unió a esa unidad.

La misión de la AFCERT durante la década de 1990 era llevar a cabo redes informáticas de defensa (CND), las operaciones para asegurar y proteger la comunicación global de la Fuerza Aérea y la computadora (C2).

La fuerza aérea ha reconocido siempre la necesidad de sistemas de detección de intrusos, en un principio la financiación de la haystack basado en host, y la auditoría de intrusión en el sistema de detección. En 1993, el AFCERT trabajó con Heberlein para desplegar una versión del NMS como una medición automatizada de incidentes de seguridad (ASIM) del sistema. La intención de la fuerza aérea fue medir el nivel de actividad maliciosa en sus redes como una forma de realizar la evaluación de amenazas. Al obtener una idea exacta de las capacidades e intenciones de sus adversarios, el AFCERT podría posicionarse para adquirir la financiación, el personal y las responsabilidades necesarias para vigilar adecuadamente las redes de la fuerza aérea.

A mediados de la década de los 90, la red de la fuerza aérea consistió en más de 100 puntos de internet, pero a finales de 1995, el AFCERT sólo dio seguimiento a 26 instalaciones. A finales de 1996 la cobertura se ha duplicado a 52 bases aéreas, "conjuntos" o multi-servicio. (Al igual que cualquier gran organización, el AFCERT ha luchado para hacer frente a los comandantes locales de base, o "de gestión", que han pasado por alto las conexiones de Internet autorizados por la instalación de sus enlaces de internet propios.) En 1998, el AFCERT añadido sensores del grupo rueda de netranger a su caja de herramientas, y su uso a petición del comando central para controlar sus lugares de avance en el medio oriente.

El AFCERT implementó supervisión de la seguridad de la red a través de productos, personas y procesos. ASIM es la herramienta utilizada para generar las indicaciones y advertencias. Los analistas AFCERT trabajan en las células en tiempo real o por lotes, ya sea revisando casi en tiempo real alertas, o los registros diarios de la sesión. Ambos equipos tuvieron acceso al contenido completo o transcripción de datos recogidos por ASIM para determinados servicios de alto valor, tales como telnet, rlogin, ftp, http y otros protocolos, los analistas intensificaron la evidencia de las intrusiones sospechosas al equipo de respuesta a incidentes (IRT), que validó e investigó intrusiones. Después de que el virus melissa golpeo en marzo de 1999, el AFCERT formo un equipo dedicado específicamente para manejar los brotes de malware.

A finales de 2000, ball aerospace & technologies corporation (BATC) solicitaron a Robert "Bamm" Visscher ayuda en la transición de técnicas de detección de intrusión para el sector comercial. Bamm había trabajado con Larry Shrader en el AFCERT, se dedicaron a la creación de una operación NSM a partir de cero. Trabajó en un presupuesto apretado y a la realización de los productos comerciales disponibles IDS, pero al no satisfacer las necesidades, Bamm desarrolló el snort visor personal en tiempo real de eventos basados en GUI (spreng).

Spreng comenzó su vida como un programa tcl / tk para ver los ataques sobre la conexión de bamm de cable módem. Analistas capacitados tomaron las funciones de supervisión 24 x 7, spreng se refino para satisfacer las necesidades de NSM. John Curry, actuando como un consultor, escribió el código para recoger datos de la sesión. Los tres elementos se integraron, y en la primavera de 2001 BATC ofreció la primera verdadera operación NSM comercial a los clientes no gubernamentales. Doce analistas interpretaron alertas, la sesión y los datos completos de contenido para descubrir a los intrusos.

En junio de 2001 fue "hackeada" una copia de la página web de la congresista Lamar Smith, mientras que bamm demostró la capacidad de control. El 13 de julio de 2001, un analista, Crooks Leroy, detecta el gusano code red seis días antes de que golpeara la población de internet. Envió sus conclusiones a la lista de incidentes del securityfocus el 15 de julio de 2001.

En abril de 2002, sale de BATC para convertirse en un consultor de foundstone. Durante la realización de tareas de respuesta a incidentes que emplea NSM de emergencia para investigar intrusiones en contra de la lista fortune 100. Se inició a utilizar argus para recoger datos de la sesión porque ya no tenía acceso al código propietario BATC adquirido para recoger datos de la sesión. Empezó a enseñar los principios de NSM a los estudiantes en las clases de "respuesta a incidentes" en foundstone y "ultimate hacking".

El 4 de diciembre de 2002, bamm presentan un webcast para searchsecurity.com titulado "supervisión de la seguridad de red" (www.taosecurity.com/news.html). Esta presentación ofrece la primera definición formal de NSM como "la recopilación, análisis, y la escalada de las indicaciones y advertencias (I & W) para detectar y responder a las intrusiones." En ese momento sólo se estaba teorizando sobre el uso de información estadística, la sesión y los datos completos de contenido y de NSM. (Que comenzó a usar el término "alerta" en lugar de datos de "evento" al escribir este libro en el otoño de 2003.)

En finales de 2002 bamm comenzó a trabajar en un producto de código abierto llamado NSM de la interfaz gráfica de usuario de snort para Lamerz (sguil). (El nombre sguil, nació en una sesión de IRC y no fue diseñado para la comercialización) sguil.sourceforge.net anuncio la disponibilidad inicial de sguil en enero de 2003. En el momento fue la interfaz gráfica de usuario de código abierto más popular para snort. A lo largo de 2003 sguil cobró impulso, y apareció en un webcast NSM 2.0 el 21 de agosto de 2003. Durante el año 2003 la cuarta edición de “hacking exposed” fue publicada. Se presentó un caso de estudio, que incluyó la definición de NSM se asentó esto como el "padre de la NSM".

Inspirado en el nombre de Todd Heberlein de “network security monitoring”, NSM es un modelo operativo basado en la recolección de señales de la fuerza aérea de inteligencia. NSM integra productos IDS, que generan las alertas, las personas, los que interpretan las indicaciones y avisos; y procesos que guían la escalada de los eventos validados a quienes toman las decisiones. [1]

IV. CICLOS DEL NSM

NSM usa evidencia recolectada, esta es analizada y verificada para que así puedan determinar un análisis al respecto y realizar los diversos correctivos sea a aplicaciones de seguridad o en políticas y ejecución de acciones dentro de una organización, por lo tanto NSM usa 4 niveles de datos:

1) Datos estadísticos:

Es analizar todo lo concerniente a la red, como su uso de ancho de banda, cantidad de usuarios, paquetes de trasmisión realizados satisfactoriamente, errados, sospechosos entre otros y determinar la “salud” de la red.

2) Datos de sesión:

Permite analizar las comunicaciones entre los host de una empresa con aplicaciones, protocolos y otros host, como las ip de origen y de destino.

3) Alertas:

Son alarmas que suscitan en el tráfico interno de una red y verifican con esto anomalías e intrusiones, determinando los falsos positivos, falsos negativos, verdaderos negativos o verdaderos positivos.

4) Trazas completas de tráfico:

En ellas es registrar de forma detallada, segundo a segundo que está pasando en una red por lo tanto la extracción de esta

información debe ser veraz y objetiva ya que es considerado el corazón de la acción de NSM.

Este último punto es muy importante ya que en el se basa según el autor de NSM el sentido de esta metodología "necesitamos un alto tráfico de red de calidad para llevar a cabo las investigaciones de seguridad" [5] por lo tanto este análisis debe llevarse a cabo con profundidad y detenimiento para saber cuál es el verdadero alcance y determinar elementos probatorios, donde exista un posible riesgo que afecte la vulnerabilidad en una organización.

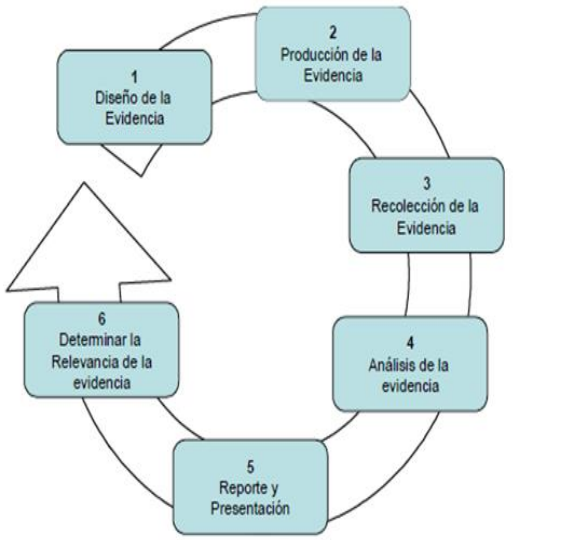
V. RELACIÓN FORENSE

Sabiendo los ciclos de NSM que es importante, hay que relacionarlo con la informática forense o el forense digital, ya que se hace un análisis forense sobre las trazas recolectadas en la red y así se determinar con mayor profundidad la relación entre los clientes, el servidor, sistemas de información, entre otros y luego identificar patrones comunes de la red, ver la información que viaja (peticiones, entradas, salidas, bloqueos, solicitudes no respondidas) por la red y el estado de esta (interrumpida, con conflicto, con tipos de ataques de intrusión, entre otros). Si en caso de que suceda una interceptación, modificación o perdía de datos, o algún elemento que indique anormalidad, es importante determinar los orígenes del ataque el cómo se realizó, origen, destino, afectación a los sistemas de información y demás factores que contribuyeron a que la organización sufra este tipo de incidentes. Por lo cual con este análisis se detecta que vulnerabilidades son encontradas y cómo afectarían en caso de un posible ataque. En este caso sería una simulación o realización de lo que se conoce como penetration testing o pen test pero usando la metodología NSM.

Para entender el tema final de NSM es importante recalcar que esta metodología usa distintas herramientas para verificar, recolectar y analizar el tráfico de una red, por lo tanto no se considera como una herramienta sino de estructurar de forma adecuada como se analizan los datos recolectados y que tengan alguna integridad. Y por ello el siguiente tema que trataremos es cómo recolectamos esta evidencia para analizarla y así preservar las temáticas de la seguridad de la información.

A. Administración de la evidencia digital AED

Este es un ciclo donde la recolección de información es importante para preservar los pilares de la seguridad de información que son la Integridad, disponibilidad y confidencialidad y demás para que toda la evidencia pueda considerarse fidedigna y que no se basa en juicios subjetivos. El ciclo de la AED [3] (ver figura 2), consta en 6 pasos que a continuación explicaremos:



Ciclo de vida de la administración de la evidencia digital.
[Tomado de: HB171:2003 Handbook Guidelines for the management of IT Evidence.]

Fig. 2 Ciclo de la administración de evidencia digital [6]

- Diseño de la evidencia
- Producción de la evidencia
- Recolección de la evidencia
- Análisis de la evidencia
- Reporte y presentación
- Determinar la relevancia de la evidencia

- *Diseño de la evidencia:*

Determina si la evidencia electrónica recolectada tiene relevancia para el proceso y que estas sean identificables y puedan ser usadas. Estos deben tener un autor claramente identificado y por lo tanto sus registros de recolección deben ser claros (bitácora de información de la evidencia) y por lo tanto deben tener los criterios del CIA.

- *Producción de la evidencia:*

Se debe identificar los autores de tales registros tomados, al igual fecha y hora de la recolección o creación, determinar el objetivo específico por el cual se toma este registro informático y por ultimo determinar la completitud de los registros generados.

- *Recolección de la evidencia:*

Su objetivo general es recolectar y preservar que esta evidencia no sea alterada o modificada, es decir que sean los "los registros electrónicos originales" por lo cual se puede establecer buenas practicas.

- *Análisis de la evidencia:*

En esta se empezaría formalmente a realizar un análisis y la concatenación de registros entregados de toda la evidencia recolectada y establecer si con estos datos es posible realizar un reporte o es necesario realizar un nuevo proceso de recolección de nuevas evidencias que completen el análisis respectivo.

- *Reporte y presentación:*

Se debe expresar de forma clara cómo se va presentar un informe de resultados, estos basados en los hallazgos y resultados de la evidencia electrónica recolectada, para que esta información sea entendida, comprensible y auditada por los interesados.

- *Determinar relevancia de la evidencia:*

Se encarga de categorizar la evidencia o resultados específicos que llevan a identificar una acción o un acontecimiento realizado que aportaría una decisión clave o a probar hechos relevantes a una investigación.

Es importante sea o no, que la metodología del NSM sea aplicada en la detección de vulnerabilidades, toda muestra que se recopile debe seguir los lineamientos de la AED y así garantizar la seguridad de que la información y evidencia recolectada sea legitima y que no de juicios a priori que puede afectar los resultados del análisis de las trazas de tráfico. En forma general se puede definir la unión de los dos elementos como una jerarquía en donde lo primero que se debe realizar es la toma de muestras para analizarlas es por eso que primero se realizará AED siguiendo los pasos anteriormente dados.

Seguidamente se puede usar diferentes herramientas para evaluar la red sea de monitoreo o de verificación y así determinar que la información que se recolecto en un principio, esto se hace con NSM ya que evalúa todo el contenido, control y monitoreo que se presenta para llegar a unos análisis y resultados finales que pueden ayudar a los analistas de seguridad a crear políticas y soluciones específicas a herramientas como antivirus, firewall, detectores de intrusos (IDS), routers, detectores de intrusos en la red (NIDS), detectores de intrusos a nivel de maquina o host (HIDS), Aplicaciones entre otras herramientas de administración de seguridad.

VI. POSIBILIDADES DE USO DEL NSM COMO METODOLOGÍA FORENSE

En este se busca la viabilidad de que el uso de NSM usando como apoyo el AED para la búsqueda de vulnerabilidades en la red de una organización o la realización de un pen test, ya que este tema no ha sido debatido claramente por expertos tanto en gestión como en los expertos de análisis forense; y la definimos como:

El uso de NSM con la ayuda de AED permitiría generar una nueva metodología para realizar la búsqueda, detección y verificación de vulnerabilidades que se presentan en las organizaciones y mejorar los procesos de penetration testing.

Es importante para definir las ventajas y desventajas que existen en el uso de NSM, en lo que lleva a la investigación no se ha encontrado a profundidad que está sea aplicada en la actualidad, se plantea la posibilidad pero no se ha realizado un estudio formal sobre el tema.

No hay que dejar a un lado lo que son los métodos usados actualmente para un análisis de riesgos o detección de vulnerabilidades en las organizaciones ni que sean dejadas a un lado, sino que sea un refuerzo a las organizaciones para saber con veracidad y precisión las distintas vulnerabilidades y así llevar a cabo la ejecución de planes de acción para preservar la seguridad de la información; esta metodología NSM debe ser un complemento más a estas técnicas ya usadas.

La utilización de las metodologías forenses al momento de que sucede un evento que produjo una perdida sustancial de información o vulnero el sistema de una organización puede servir no solo para encontrar las causas y los culpables de este incidente, sino también ayuda a determinar las debilidades presentes sin tener un incidente de seguridad, empezando así una mejora de la "inseguridad" de la información en las organizaciones, fortaleciendo la seguridad presente en una organización.

También es valioso determinar si esta metodología realmente puede servirnos para la detección de vulnerabilidades, el objeto del presente artículo es despertar el interés por esta metodología, en dado caso aplicarla como prueba y verificar si es viable o no al momento de un incidente o verificación de vulnerabilidades presentes en la organización. Podemos indicar buscar sus beneficios y sus contras y en definitiva dejar en claro la orientación del uso del NSM.

CONCLUSIONES

La comunidad científica identifica, evalúa y avala los procesos, estos deben estar cumpliendo con la investigación, la recolección y conclusiones de la información recolectada, la información que necesita la metodología NSM es el tráfico de red. Cumpliendo con los mecanismos de la comunicad científica, del NSM y la AED se tendría resultados favorables e identificar las vulnerabilidades de una red.

Para llegar a una conclusión, y tener bases sólidas es necesario tener una buena calidad y manejo de muestras recolectadas, sin estas podemos llegar a otras conclusiones y por lo tanto a realizar correcciones en la organización de manera errada.

Las organizaciones buscan estar más protegidas en todos los aspectos incluyendo un activo importante como es la información digital, es por ello, buscan mecanismos, modelos, estructuras que identifiquen inconvenientes, falencias, fallos en los sistemas; la idea de proponer el uso de NSM, como su mismo autor comenta, no debe ser forzosamente el mismo lineamiento pero debe llegar a la misma conclusión, determinar que está afectando el tráfico de red y de ahí corregir, políticas, procedimientos y elementos de la seguridad de información. A una primera instancia el procedimiento en conjunto del NSM y AED es la de generar un método de penetration testing.

RECONOCIMIENTOS

Debo a este esfuerzo a mis jefes en Frontech Ltda y ESET

latinoamérica, que creen en la labor desempeñada, profesionalismo y en apoyar las ideas y mejoras que hay que hacer en mi campo profesional y personal.

BIBLIOGRAFIA

[1] BEJTLICH, R. (11 de Abril de 2007). TaoSecurity: Richard Bejtlich's blog on digital security, concentrating on global challenges posed by China and other targeted adversaries. [En línea] Recuperado diciembre de 2013, de Network Security Monitoring History: http://taosecurity.blogspot.com/search?q=network+security+monitoring.

[2] VALENZUELA, Ismael. (11 de Mayo de 2010). Passionate about Information Security. [En línea]. Recuperado Diciembre de 2013. Obtenido de http://blog.ismaelvalenzuela.com/wp-content/uploads/2010/06/Forman_NSM_May_10.pdf

[3] CANO, Jeimy J. Computación Forense: Descubriendo los rastros informáticos. Colombia: Alfaomega Editores, Primera Edición, 2009.

[4] BIANCO, David J. (2005). Open Sourse Network Security Monitoring. [En línea] Recuperado Diciembre de 2013, Obtenido de http://www.vorant.com/files/nsm_with_sguil.pdf

[5] BEJTLICH, Richard. The Tao of Network Security Monitoring: Beyond Intrusion Detection: Addison-Wesley, Décima Edición, 2010.

[6] CANO, Jeimy J. Administración de la evidencia digital, 2006. [En línea] Recuperado Diciembre de 2013. Disponible en http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VI_JornadaSeguridad/JeimyCano_VIJNSI.pdf

[7] SHELL, Michael. How to Use the IEEEtran. [En línea] Recuperado Febrero de 2014. http://www.laqee.unal.edu.co/tex-archive/macros/latex/contrib/IEEEtran/IEEEtran_HOWTO.pdf