Cuaderno Activa, ISSN 2027-8101. N°5, Enero-Diciembre de 2013, pp. 31-37.
Tecnológico de Antioquia, Colombia.

Cuaderno Activa
Revista científica de la Facultad de Ingeniería

Evaluación y comparación de herramientas para el análisis forense en redes

Ángela Camila Montenegro Granados
Estudiante de Ingeniería de Sistemas y Computación
angela.montenegro@uptc.edu.co
Universidad Pedagógica y Tecnológica de Colombia

Frey Alfonso Santamaría Buitrago
Docente
M. Sc. (c) en Ciencias de la Información y las Comunicaciones
frey.santamaria@uptc.edu.co
Universidad Pedagógica y Tecnológica de Colombia

Recibido: 31 de mayo 2013
Aceptado: 3 de julio 2013

Resumen
El análisis forense en redes se basa en la captura, almacenamiento y análisis de eventos de una red con el fin de descubrir evidencia acerca de la fuente de ataques de seguridad para posteriormente ser llevada a una corte legal. En el momento de recolectar la evidencia digital, existe la dificultad para obtener pruebas contundentes que permitan determinar el origen y la identidad del atacante cuando se produce un ataque. El presente artículo describe las diferentes herramientas y la importancia de su elección en el momento de aplicar un análisis forense en redes, teniendo en cuenta criterios que mejoran la optimización de las metodologías y técnicas en el análisis de la información involucrada.

Palabras clave: Análisis forense en redes, evidencia digital, NFTA, NSMT, tráfico de red, ataque informático.

Assessment and comparison of tools for forensic network analysis

Abstract
Forensic network analysis relies on the capture, storage and analysis of events within a networking order to detect evidence about the source of security attacks, so that it can subsequently be taken to a court of law. At the time of collecting digital evidence, there is the difficulty of obtaining convincing evidence allowing to determine the attacker's location and identity when an attack occurs. This paper describes the different tools and the importance of choosing the right ones when applying a forensic network analysis, considering the optimization of methodologies and techniques in the analysis of the information involved.

Keywords: Forensic network analysis, digital evidence, NFTAs, NSMT, network traffic, computer attack.

1. Introducción

En los últimos años, el avance tecnológico se ha incrementado drásticamente, lo cual ha provocado una migración acelerada de información física a digital en la mayoría de las organizaciones o empresas del mundo. Al aumentar el uso de nuevas tecnologías, el número de actividades ilegales también incrementa exponencialmente. Cuando no se capturan registros de una manera adecuada no es posible realizar análisis posteriores, y esto impide conocer el origen de los ataques y el culpable que interfiere en la seguridad de la red. La computación forense se encarga de colectar y analizar los datos de computadores, redes, comunicaciones y multimedia de una manera autorizada por una corte legal. El análisis forense en redes se encarga estrictamente de la captura, almacenamiento y análisis de eventos ocurridos en un tráfico de red, para descubrir evidencia digital cuando la red ha sido objeto de ataques. Con el rápido crecimiento de actividades ilegales, el análisis forense de redes llega a ser una parte fundamental de la computación forense. Por lo tanto, es importante seleccionar la herramienta correcta y hacer buen uso de ella, con el fin de lograr mejores evidencias para el análisis forense. Este artículo evalúa y compara diferentes herramientas disponibles con el fin de mostrar la eficiencia, la facilidad de uso y la relación costo-efectividad en la conducción de un buen análisis forense en redes.

2. Marco teórico

2.1 Computación forense

Con el rápido avance en la tecnología de computadores y redes, la evidencia digital empieza a tener un rol importante en las cortes en la última década. La computación forense es una disciplina en desarrollo basada en ciencia forense y tecnología de seguridad informática, se enfoca en adquirir evidencia electrónica de los sistemas de cómputo para procesar crímenes de computador (Acurio, 2009).

El concepto general de análisis forense es la aplicación de métodos científicos en investigaciones criminales, pero cuando la evidencia es de naturaleza digital el análisis forense recibe varias definiciones. Las siguientes definiciones de computación forense son una representación del amplio rango existente:

- El proceso de identificar, preservar, analizar y presentar la evidencia digital de forma que sea legalmente aceptada (McKemmish, 1999).

- Obtención y análisis de datos de una forma libre de distorsión para reconstruir datos o conocer lo que ha ocurrido en el pasado sobre un sistema.

- El uso de métodos derivados y probados científicamente para la preservación, colección, validación, identificación, análisis, interpretación, documentación y preservación de evidencia digital, entregados desde fuentes digitales con el propósito de facilitar o promocionar la reconstrucción de eventos criminales, o ayudar a anticipar acciones no autorizadas.El trabajo de Broucek y Turner (2013) muestra las implicaciones metodológicas por la falta de coherencia, revisa los modelos y trabajos existentes como una forma de explorar sus diferencias, y examina la ambigüedad de definiciones de la computación forense. El trabajo de la computación forense debe ser el resultado de la cooperación y colaboración entre varias disciplinas, como lo muestra la Figura 1.

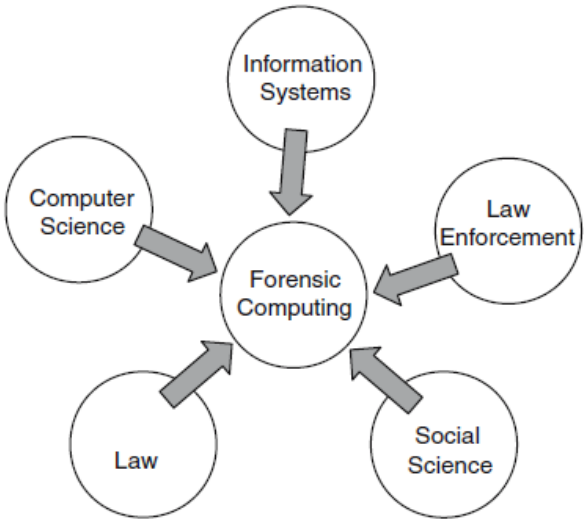

Figura1. Dominio de Computación Forense
Fuente: Tomado de Broucek y Turner (2013)

2.2 Análisis forense en redes

El concepto de análisis forense en redes se enfoca en datos encontrados en una conexión de red, en su mayoría el tráfico de entrada y salida desde un host a otro. El análisis forense en redes intenta analizar el tráfico de datos registrados a través de firewalls y sistemas de detección de intrusos o en los dispositivos de red como routers y switches.

Según Sisniega (2010) El análisis forense en redes se define como el uso de:

> *(...) técnicas científicamente probadas para recolectar, identificar, analizar, relacionar y documentar evidencias digitales a partir del múltiplos procesamientos y la transmisión digital de fuentes activas con el propósito de descubrir hechos relacionados con intención planificada, o el éxito de actividades no autorizadas con la intención de interrumpir, corromper y/o comprometer el sistema o sus componentes, así como proporcionar información para ayudar a respuestas de recuperación de estas actividades.*

El análisis forense de redes implica la supervisión del tráfico de la red, para determinar si existe una anomalía en el tráfico y establecer si se indica un ataque. Si se detecta un ataque, a continuación también se determina su naturaleza. Las técnicas en análisis forense permiten a los investigadores rastrear el atacante. El objetivo final es proporcionar pruebas suficientes para permitir que el agresor sea procesado (Cruz, 2007).

2.3 Ataques informáticos

Un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware e, incluso, en las personas que forman parte de un ambiente informático, a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema que luego repercute directamente en los activos de la organización (Gutiérrez, 2006).

Anatomía de un ataque informático

Conocer las diferentes etapas que conforman un ataque informático brinda la ventaja de aprender a pensar como los atacantes y a jamás subestimar su mentalidad. Desde la perspectiva del profesional de seguridad, se debe aprovechar esas habilidades para comprender y analizar la forma en que los atacantes llevan a cabo un ataque. La Figura 2 muestra las cinco etapas por las cuales suele pasar un ataque informático al momento de ser ejecutado.

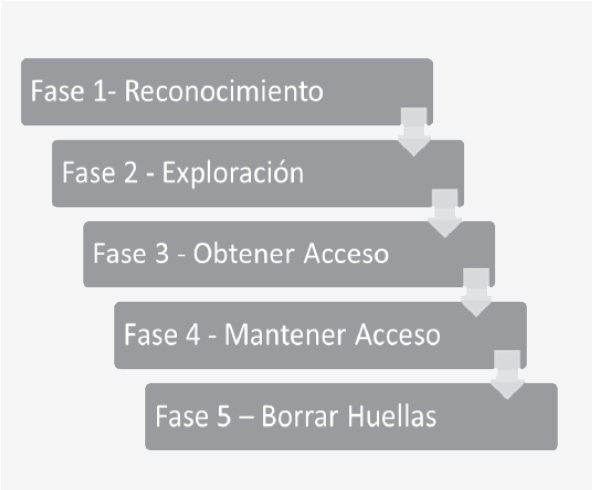

Figura 2. Fases comunes de un ataque informático
Fuente: Elaboración propia (2013)

Fase 1: Reconocimiento. Esta etapa involucra la obtención de información sobre una potencial víctima, que puede ser una persona u organización. Por lo general, durante esta fase se recurre a diferentes recursos de internet como Google, entre tantos otros, para recolectar datos del objetivo. Algunas de las técnicas utilizadas en este primer paso son la ingeniería social, el dumpster diving, el sniffing (Vinueza, 2011).

Fase 2: Exploración. En esta segunda etapa se utiliza la información obtenida en la fase 1 para sondear el blanco y tratar de obtener información sobre el sistema víctima, como direcciones IP, nombres de hosts, datos de autenticación, entre otros. Entre las herramientas que un atacante puede emplear durante la exploración se encuentran: network mappers, port mappers, network scanners, port scanners, y vulnerability scanners (Lerones, 2006).

Fase 3: Obtener acceso. En esta instancia comienza a materializarse el ataque a través de la explotación de los defectos y vulnerabilidades del sistema (Flaw exploitation) descubiertos durante las fases de reconocimiento

y exploración. Algunas de las técnicas que el atacante puede utilizar son ataques de Buffer Overflow, de Denial of Service (DoS), Distributed Denial of Service (DDos), Password filtering y Session hijacking.

Fase 4: Mantener el acceso. Una vez que el atacante ha conseguido acceder al sistema, buscará implantar herramientas que le permitan volver a acceder en el futuro desde cualquier lugar donde tenga acceso a internet. Para ello, suelen recurrir a utilidades backdoors, rootkits y troyanos.

Fase 5: Borrar huellas. Cuando el atacante logra obtener y mantener el acceso al sistema, intentará borrar todas las huellas que haya dejado durante la intrusión para evitar ser detectado por el profesional de seguridad o los administradores de la red. En consecuencia, buscará eliminar los archivos de registro (log) o alarmas del sistema de detección de intrusos (IDS).

2.4 Herramientas

Las herramientas de análisis forense en redes (NFAT) permiten a los administradores monitorizar redes, recopilar toda la información sobre el tráfico anómalo, ayudar en la investigación de delitos de red y mostrarlo a través de la generación de una respuesta a incidentes adecuada. También ayudan en el análisis del robo de información privilegiada y el abuso de recursos, predicen los ataques a objetivos en un futuro próximo, plasman riesgos de evaluación, evalúan el rendimiento de la red y ayudan a proteger la propiedad intelectual (Calderón, 2008).

Las NFAT pueden capturar todo el tráfico de red, lo que permite a los usuarios analizar el tráfico de red de acuerdo con sus necesidades y descubrir características importantes sobre él. Las NFAT pueden trabajar de la mano con sistemas de detección de intrusos y firewalls para hacer, a largo plazo, preservación de los registros de tráfico de red para el análisis rápido. El tráfico de ataque se puede reproducir, y si hay movimiento de atacantes se puede analizar para detectar su intención maliciosa (Gómez y Monserrat, 2011). El uso de NFAT facilita la organización de los paquetes de tráfico de red capturados para ser vistos como conexiones de capa de transporte individuales entre máquinas, que permiten al usuario analizar capas de protocolo, contenido del paquete, datos retransmitidos y tráfico de extracto de patrones entre diferentes máquinas. Hay algunas NFAT disponibles que proporcionan datos fiables, adquisición y capacidad de análisis de gran alcance. En la Figura 3 se muestran algunas herramientas y su clasificación:

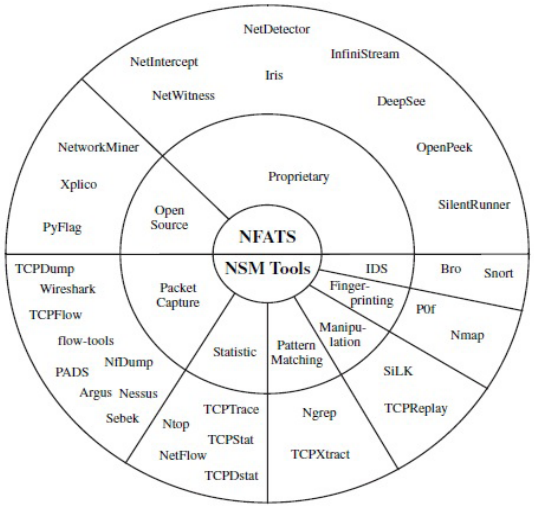

Figura 3. Clasificación de Herramientas
Fuente: A. Campos (2008)

3. Metodología

La metodología aplicada en esta investigación se dividió en cinco fases:

Fase 1. Revisión de herramientas: En esta etapa se identifican todas las herramientas existentes sobre análisis forense en redes. Las herramientas se clasifican en dos grandes grupos: Herramientas para el análisis forense en redes (NFTA) y herramientas de seguridad y monitoreo (NSMT). Las NFTA son más completas que las NSMT, en su mayoría las NSMT se utilizan para un campo en específico. Por ejemplo, si el usuario desea hacer captura de paquetes en el tráfico de red, él no podría seleccionar una herramienta utilizada para IDS cuando trabaja con NSMT, situación que no sucede con las NFTA.

Fase 2. Selección de herramienta: Como existe un número grande de herramientas y aún siguen surgiendo nuevas, se hizo una limitación a dos herramientas. Se evaluó y comparó una herramienta de cada tipo. Para las NFTA se tomó como caso de estudio NetworkMiner y para las NSMT, Wireshark. En ambos casos, las herramientas se caracterizan por ser completas y usadas en los últimos años.

NetworkMiner es una herramienta que permite cap-

turar tráfico de red de forma pasiva/activa a partir de un fichero .pcap o directamente desde la interfaz de red deseada. El objetivo es hacer un seguimiento de sistemas operativos, sesiones, nombres de host, etc. desde una interfaz amigable y sencilla. NetworkMiner también te permite extraer certificados y ficheros de protocolos como FTP, TFTP, HTTP y SMB.

Wireshark es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándares de un analizador de protocolos. Permite ver todo el tráfico que pasa a través de una red (usualmente una red Ethernet, aunque es compatible con algunas otras) estableciendo la configuración en modo promiscuo.

Permite examinar datos de una red viva o de un archivo de captura salvado en disco. Se puede analizar la información capturada a través de los detalles y sumarios por cada paquete. Wireshark incluye un completo lenguaje para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP.

Fase 3. Creación de la red: Para hacer las pruebas se creó una red LAN con dos terminales y un servidor. Una de las terminales se puso como atacante y las otras dos como víctimas.

Fase 4. Elección de ataque: Según la información leída, se procedió a seleccionar tres tipos de ataques.

> *Denegación de servicio: Envío de paquetes al servidor hasta que este quede saturado.*
> *Hombre en el medio: Conexión intermedia del atacante, donde el servidor como el terminal no detectan la presencia de este ni el cambio de información durante el ataque.*
> *Rastreador: Se dedica a espiar las actividades de sus víctimas sin modificar información.*

Los tres ataques fueron ejecutados con una herramienta libre conocida como BackTrack (Rivas et al., 2009; Zapata, 2012).

Fase 5. Ejecución de las herramientas: Las herramientas se ejecutaron de dos formas: La primera corresponde al mismo tiempo que se ejecuta el ataque, la segunda, después de que el ataque ha sido ejecutado. Ambas herramientas ofrecen una detección inmediata de tráfico de red.

4. Resultados

Una vez se obtuvo la información analizada por las herramientas, se procedió a realizar la comparación con respecto a los siguientes criterios:

Preparación: Ambas herramientas consideran algunas fases como: detección de intrusos en el sistema, analizadores de paquetes, servidores de seguridad y medición de flujo de tráfico. Los software están desplegados en varios puntos estratégicos de la red, con las autorizaciones necesarias y las garantías legales obtenidas, de manera que la privacidad no sea violada.

Detección: Las alertas generadas por ambas herramientas de seguridad fueron parcialmente analizadas. Indican la observación de una violación de políticas de seguridad no autorizadas. Wireshark detectó los ataques en la primera prueba, a diferencia de NetworkMiner, que detectó el ataque producido en la tercera prueba. La presencia y naturaleza del ataque se determinan a partir de diversos parámetros y se reportan los protocolos mediante los cuales ingresaron los ataques. Ambas herramientas hacen una validación rápida para evaluar y confirmar la sospecha de ataque. Esto facilita la importante decisión de continuar la investigación o ignorar la alerta como una falsa alarma.

Colección: Los datos que se obtienen a partir de los sensores que se utilizan para recoger el tráfico de datos de ambas herramientas, definen bien el uso de hardware fiable para reunir pruebas máximas causando el mínimo impacto a la víctima. Es muy importante el cambio de datos de tráfico a un ritmo rápido, el cual las herramientas evaluaron de forma satisfactoria, siendo posible generar la misma traza en un momento posterior. La cantidad de datos registrados fue enorme, lo cual requirió gran espacio de memoria, y el sistema fue capaz de manejar diferentes formatos de datos de registro de manera apropiada.

Preservación: Los datos originales obtenidos y los registros que son almacenados en las herramientas generan una copia de seguridad como el único medio de lectura. Las herramientas conservan los datos de seguimiento, analizan una copia de los datos y los datos de tráfico de red originales están intactos. Esto es algo muy impor-

tante, ya que facilita los requisitos legales que pueden arrojar los resultados obtenidos por la investigación y demostrar que es igual cuando el proceso se repite en los datos originales.

Examinación: Las trazas obtenidas de ambas herramientas se integran y se fusionan para formar un conjunto de datos grande en el que se puede realizar el análisis. Hay algunos temas, como información redundante y la superposición de zonas de tiempo, que necesitan apropiación, tanto en Wireshark como en NetworkMiner. En algunos casos las alertas fueron contradictorias, es decir, arrojaban supuestos ataques cuando no se había iniciado ninguno. Sin embargo, se destacó que la información crucial de fuentes importantes no se perdió, y fue posible almacenarla para nuevamente ser analizada. Los datos recogidos se extraen para tener indicadores específicos de la delincuencia. Wireshark identifica el ataque con un mínimo de atributos, de manera que la menor información registrada contiene la mayor evidencia probable. Mientras NetworkMiner solo se limita a tomar atributos generales, de los cuales no se puede obtener la mayor información. Ambas herramientas permiten una regeneración del tráfico de red.

Análisis: Los indicadores se clasifican y correlacionan para deducir importantes observaciones utilizando los patrones de ataque existentes. A diferencia de NetworkMiner, Wireshark utiliza estadística y enfoques de minería de datos informáticos y suaves para buscar los datos y combinar patrones de ataque. Algunos de los parámetros importantes están relacionados con la conexión de red del establecimiento, las consultas DNS, la fragmentación de paquetes, el protocolo y la operación del sistema de toma de huellas dactilares. Los patrones de ataque son reconstruidos y reproducidos de manera conjunta para entender la intención y la metodología del atacante.

Investigación: Ambas herramientas determinan la ruta de acceso de una red o víctima a través de cualquiera de los sistemas intermedios y de los caminos de comunicación, de vuelta al punto de ataque de origen. Las capturas de paquetes y las estadísticas obtenidas se utilizan para atribuir el ataque. La atribución de la identidad del atacante fue la parte más difícil del proceso forense en la red. Las dos herramientas demoraron en identificar la máquina desde donde se generaban las alteraciones a la red. Como era de esperar, Wireshark fue la primera en demostrar que había ingreso no permitido a las terminales que hacen papel de víctima.

Presentación: Ambas herramientas presentan observaciones de manera comprensible para el personal mientras que proporcionan explicación de los diversos procedimientos utilizados para llegar a la conclusión. La documentación sistemática también se incluye para cumplir con el marco jurídico de requisitos. En este proceso, las herramientas concluyen el análisis forense de la información en una red como la que presentó los resultados en la persecución del atacante.

5. Conclusiones y trabajos futuros

Cuando se evalúan herramientas para análisis forense en redes debe tenerse en cuenta el ambiente para el cual se realiza dicho proceso, ya que esto es clave al momento de elegir la herramienta adecuada sin descuidar la veracidad de la información recolectada.

Aunque el resultado final de ambas herramientas es similar, la herramienta Wireshark es más adecuada para el análisis forense en redes, ya que su tiempo de respuesta es menor.

El uso de NFAT permite detectar diferentes tipos de ataques que sirven como base para diseñar estrategias de prevención y seguridad en una red.

Este artículo influye en futuras investigaciones para proporcionar información en la guía de la implementación y mejora de ejecución de herramientas para el análisis forense en redes. La comparación propuesta es genérica, ya que se encarga de mostrar aspectos y criterios básicos en un análisis forense en redes tanto en escenarios de ataque en tiempo real como posterior.

Referencias

Acurio, S. (2009). Informática forense en el Ecuador: una mirada introductoria. Quito: Pontificia Universidad Católica del Ecuador.

Broucek, V. y Turner, P. (2013). Técnicos, legales y éticos: dilemas. Riesgos distintivos que surgen de herramientas de malware y ciber-ataque en la "nube". Una perspectiva informática forense. J. Virología de informática y técnicas de hacking. Vol. 9, Nº 1, pp. 27-33.

Calderón, E. (2008). Metodología para la forensia informática. Monografía. Universidad Autónoma del Estado de Hidalgo, Pachuca, México.

Campos, A. (2008). Analizador Gráfico de Red (sniffer) en entorno GNU. Trabajo final de carrera. Universitat Oberta de Catalunya, Barcelona, España.

Cruz M., J. (2007). Herramienta de apoyo para el análisis forense de computadoras. Proyecto fin de carrera. Universidad de Jaén, Jaén, España.

Gómez, A. F. y Monserrat F. J. (2011). Seguridad en la red y análisis forense. Proyecto fin de carrera, Universidad de Murcia, Murcia, España.

Gutiérrez, R. (2006). Seguridad en VoIP: Ataques, amenazas y riesgos. Valencia, España: Universitat de Valencia.

Lerones L. (2006). Desarrollo de un analizador de red (SNIFFER). Trabajo de investigación. Universitat Oberta de Catalunya, Barcelona, España.

McKemmish, R. (1999). What is Forensic Computing? Canberra, Australia: Australian Institute of Criminology.

Rivas J. L., Rifà H. y Serra J. (2009). Análisis forense de sistemas informáticos. Barcelona, España: Universitat Oberta de Catalunya.

Sisniega J. L. (2010). Sistema de reconstrucción y detección de eventos de seguridad en redes de datos. Tesis de maestría. Instituto Politécnico Nacional, México D.F.

Vinueza P. J. (2011). Análisis para la seguridad de paquetes de datos y evitar ataques mediante sniffing. Tesis de grado. Universidad Tecnológica Israel, Cuenca, Ecuador.

Zapata L. (2012). Evaluación y mitigación de ataques reales a redes IP utilizando tecnologías de virtualización de libre distribución. Ingenius, Nº 8, pp. 11-19.