Entorno de disponibilidad forense para la recolección de datos digitales en HTTP

Mónica D. Tugnarelli [(1)], Mauro F. Fornaroli [(1)],
Sonia R. Santana [(1)], Javier Díaz [(2)]

[(1)] Facultad de Ciencias de la Administración – Universidad Nacional de Entre Ríos
[(2)] Facultad de Informática – Universidad Nacional de La Plata
e-mail: montug, maufor [@fcad.uner.edu.ar]

Resumen

En este artículo se presentan los avances del análisis de prestaciones y características de dos metodologías de recolección de datos digitales asociadas a eventos de seguridad, la primera llamada Enfoque preventivo- Recolección de datos a priori o *Forensic Readiness* y, la segunda, Enfoque reactivo - Recolección de datos a posteriori de un incidente. Para el desarrollo del trabajo se establecieron etapas y actividades tendientes a la identificación y descripción de puntos de control en protocolos HTTP, la configuración de un entorno de prueba para la captura de datos, procedimientos para la preservación de la evidencia, aspectos de integridad y trazabilidad de la misma y la descripción de resultados comparativos entre ambos enfoques de recolección.

Palabras clave: seguridad, disponibilidad forense, evidencia digital, servidores web, HTTP.

Contexto

El Proyecto de Investigación y Desarrollo PID-UNER 7052 para Director Novel con Asesor, denominado "Análisis de Metodologías de Recolección de datos digitales" se encuadra en una de las líneas de investigación establecidas como prioritarias para su fomento, "Arquitectura, Sistemas Operativos y Redes", de la carrera Licenciatura en Sistemas de la Facultad de Ciencias de la Administración. Se adecua además, a las prioridades de la Universidad Nacional de Entre Ríos por ser un proyecto aplicado a la investigación sobre Tecnologías de la Información y la Comunicación [1].

Introducción

Si una arquitectura de seguridad informática está correctamente definida debe ofrecer un plan y un conjunto de políticas que describan tanto los servicios de seguridad ofrecidos a los usuarios como los componentes del sistema requeridos para implementar dichos servicios. Estas políticas de seguridad se aplican a los activos de información identificados por su relevancia con los objetivos de la organización, conociendo como se gestionan y cuáles son sus riesgos, con la finalidad de implementar estrategias y mecanismos que aseguren la confidencialidad, la integridad y la disponibilidad de los mismos [2].

En este entorno tecnológico las técnicas y metodologías de forensia informática deben asegurar que se pueda determinar adecuadamente el *qué*, *quién, cuándo* y *cómo sucedió* en relación al incidente de seguridad, así como también ocuparse de la correcta preservación y trazabilidad de los datos recolectados. Entonces, el análisis forense digital requiere aplicar métodos científicos, técnicas y herramientas para cumplimentar etapas relacionadas con la identificación, preservación y análisis de la evidencia digital, la cual llegado el caso puede ser considerada legalmente en un proceso judicial [3]. Una etapa destacada es la recolección de esta evidencia y la manera en que se asegura la calidad e integridad de los datos recolectados.
En el marco del proyecto se analizan dos enfoques de recolección de datos:

a) Recolección de datos a priori de un evento de seguridad: también conocido como *Forensic Readiness*. Este enfoque introduce el concepto de resguardar la posible evidencia antes de que ocurra el incidente para cubrir dos objetivos: maximizar la capacidad del entorno para reunir evidencia digital confiable y minimizar el costo forense durante la respuesta a un incidente. [4], [5], [6]. La planificación del entorno de disponibilidad forense incluye, entre otras acciones:

- Definir activos que pueden requerir de pruebas digitales;
- Identificar las fuentes disponibles y los diferentes tipos de pruebas;
- Establecer una forma segura de obtención de pruebas para cumplir con el requisito de admisibilidad legal;
- Establecer una política para el almacenamiento y el manejo seguro de las evidencias;
- Capacitar al personal de modo que todos entiendan su papel en el proceso de pruebas digitales y la sensibilidad jurídica de las mismas.

b) Recolección de datos a posteriori de un evento de seguridad. Este enfoque recupera la evidencia luego de que se haya detectado el incidente de seguridad con el objetivo de realizar un análisis forense para determinar lo ocurrido.

En este proyecto el activo identificado es un servidor web, específicamente analizando información del protocolo HTTP en sus versiones 1.1 y 2 [7], [8], empleando para la ejecución de pruebas y adquisición de datos herramientas de forensia con licenciamiento libre [9], principalmente Kali Linux [10]. Como guía y marco general para las pruebas se consideran las especificaciones de la RFC 3227 - Guidelines for Evidence Collection and Archiving [11], la ISO/IEC 27037- Guidelines for identification, collection, acquisition and preservation of digital evidence [12] y el Open Source Security Testing Methodology Manual (OSSTMM) [13].

Líneas de Investigación, Desarrollo e Innovación

Con este proyecto de investigación se espera conformar una base de conocimiento que aporte al análisis de la forensia informática en relación a metodologías de

recolección de datos digitales y, específicamente a entornos de Forensic Readiness y las buenas prácticas asociadas a su implementación. Se prevé profundizar la línea de investigación con nuevos proyectos y con la firma de convenios de colaboración con otras instituciones de investigación en la temática.

Resultados y Objetivos

El PID 7052 tiene como objetivo principal analizar comparativamente la perfomance y características de las dos metodologías de recolección de datos en entornos de servidores web.
Como puntos de control HTTP para la recolección de datos, sobre los cuales se realizó un monitoreo activo, la captura de tráfico y recolección de datos, se identificaron los siguientes:

- puertos 80 y 443
- logs del sistema operativo *(/var/log/)*: *messages.log*, *auth.log, secure, utmp/wtmp,*
- logs *httpd*: error.log y access.log.

Según el enfoque varía el resguardo de información, considerando que para la metodología *Forensic Readiness* cada dato recolectado debe ser asegurado como posible evidencia digital.
En la Figura 1 se muestra la secuencia del procedimiento aplicado para la recolección y aseguramiento de los datos en el Enfoque preventivo [14]:

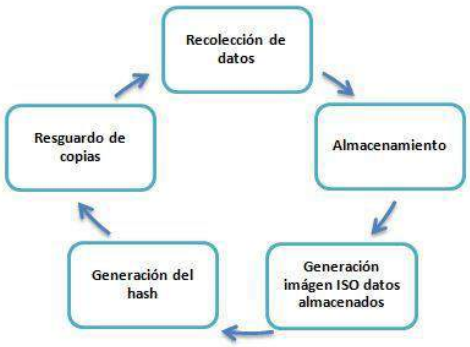

Figura 1. Secuencia procedimiento enfoque preventivo

En la Figura 2 se presenta la secuencia del procedimiento para el Enfoque reactivo:

Figura 2. Secuencia procedimiento enfoque reactivo

Como parte de las actividades se realizó la simulación de un ataque de Denegación de Servicios Distribuido (DDoS) a los fines de observar el comportamiento del servidor, el volumen de datos resguardados en logs y para analizar la perfomance de las metodologías en instancias de recuperación del servicio y resguardo de la evidencia.

Los primeros resultados obtenidos en este proyecto permiten establecer que:

1. La metodología preventiva proporciona un mecanismo activo de anticipación a los incidentes en contraste con las metodologías de respuesta a un incidente de seguridad.

2. En un enfoque preventivo, la integridad de los datos tratados como evidencia digital se puede asegurar con el hash que actúa como una faja digital cumpliendo la misma función que el sellado físico utilizado para resguardar dispositivos comprometidos [15]

3. La trazabilidad de los datos considerados evidencia puede mantenerse implementando un control de versiones, que registra los cambios realizados sobre un archivo o conjunto de archivos a lo largo del tiempo.

4. En relación a la infraestructura mínima necesaria, hay que considerar también el valor temporal que la organización le otorgue a la información recolectada, que puede estar sujeto a políticas de la organización como así también a leyes nacionales e internacionales y/o a restricciones dadas por el propio carácter de los datos. El enfoque preventivo, y a medida que se avanza en la recolección de datos de los activos identificados requiere una infraestructura de alta prestación, cuestión que se abordará en un próximo proyecto de investigación

5. En el enfoque preventivo se maximiza la explotación de potencial evidencia, ya que la misma puede ser preservada y mantenerse no contaminada o dañada por el incidente de seguridad, aspecto que es muy difícil de asegurar en un enfoque reactivo cuando ya un ataque de seguridad se ha producido.

Formación de Recursos Humanos

En este proyecto se forman e inician en actividades de investigación tres docentes de la carrera Licenciatura en Sistemas y un docente en la dirección de proyectos. Asimismo da el marco para la realización de una tesis de maestría correspondiente a la Maestría en Redes de Datos de la Facultad de Informática de la Universidad Nacional de La Plata.

Referencias

[1] Tugnarelli, M., Fornaroli, M., Santana, S., Jacobo, E., Díaz, J.: Análisis de Metodologías de Recolección de Datos Digitales. In: Libro de Actas Workshop de Investigadores en Ciencias de la Computación 2017, pp. 1000-1004. ISBN 978-987-42-5143-5.

[2] Incident Management and Response ISACA http://www.isaca.org/

[3] Digital Forensic Research Workshop (DFRWS). http://www.dfrws.org/

[4] TAN, John. (2001). Forensic Readiness. http://isis.poly.edu/kulesh/forensics/forensic_readiness.pdf

[5] Rowlingson, Robert. A Ten Step for Forensicc Readiness. (2004) International Journal of Digital Evidence. Volume 2, Issue 3.

[6] Pooe, A. , Labuschagne, L. A conceptual model for digital forensic readiness (2012) http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6320452

[7] RFC 2616 Hypertext Transfer Protocol - HTTP/1.1 http://tools.ietf.org/html/rfc2616

[8] RFC 7540 Hypertext Transfer Protocol Version 2 (HTTP/2). https://tools.ietf.org/html/rfc7540

[9] Tugnarelli, M.; Fornaroli, M.; Pacifico, C. Análisis de prestaciones de herramientas de software libre para la recolección a priori de evidencia digital en servidores web. Workshop de Investigadores en Ciencias de la Computación (WICC 2015). ISBN 978-987-633-134-0

[10] KALI Linux. www.kali.org

[11] RFC 3227 Guidelines for Evidence Collection and Archiving. https://www.ietf.org/rfc/rfc3227.txt

[12] Guidelines for identification, collection, acquisition and preservation of digital evidence" ISO/IEC 27037:2012

[13] Open Source Security Testing Methodology Manual (OSSTMM) http://www.isecom.org/mirror/OSSTMM.3.pdf

[14] Mónica D. Tugnarelli, Mauro F. Fornaroli, Sonia R. Santana, Eduardo Jacobo, Javier Díaz: Análisis de metodologías de recolección de datos digitales en servidores web. Libro de Actas. XXIII Congreso Argentino de Ciencias de la Computación CACIC 2017. VI Workshop de Seguridad Informática, pp. 1230-1238. ISBN 978-950-34-1539-9.

[15] Piccirilli, Darío. (2016). Protocolos a aplicar en la forensia informática en el marco de las nuevas tecnologías (pericia – forensia y cibercrimen). Tesis de doctorado. Facultad de Informática. Universidad Nacional de La Plata. http://hdl.handle.net/10915/52212

[16] U.S. Department of Justice. Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition. https://www.ncjrs.gov/pdffiles1/nij/219941.pdf, last accessed 2017/08/30.

[17] Forte, D: Principles of digital evidence Collection. ElSevier, Network Security, Volume 2003, Issue 12, 6-7 (2003).

[18] Caracciolo Claudio, Rodriguez Marcelo, Sallis Ezequiel. (2010). *Ethical Hacking - un enfoque metodológico para profesionales*

[19] Computer Forensics. (2008) Volume 56, Number 1. U.S. Department of Justice

[20] FBI Cyber Crime. http://www.fbi.gov/about-us/investigate/cyber

[21] Jarrett, Marshall. Bailie, Michael W. Electronic Evidence in Criminal Investigations. Computer Crime and Intellectual Property Section

[22] del Peso Navarro, Emilio y colaboradores. (2001) *Peritajes Informáticos*. Editorial Díaz de Santos

[23] Noblett, M., Pollitt, M., Presley, L. (2000). *Recovering and Examining Computer Forensic Evidence*. Forensic Science Communications. Volume 2, Number 4. U.S. Department of Justice. Federal Bureau of Investigation (FBI)

[24] Digital Evidence and Computer Crime. Forensic Science, Computers and Internet. Third Edition (2011). Eoghan Casey. Elsevier Inc.