Análisis de Metodologías de Recolección de Datos Digitales

Mónica D. Tugnarelli (1), Mauro F. Fornaroli (1) , Sonia R. Santana (1), Eduardo Jacobo (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

Una arquitectura de seguridad informática bien 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. Cuando se produce un incidente o amenaza de seguridad, en el cual un recurso del sistema queda comprometido o potencialmente expuesto a accesos no autorizados, esta arquitectura de seguridad se ve vulnerada.

Considerando la fragilidad y volatilidad de un evento digital, las técnicas y metodologías de forensia informática deben asegurar que se pueda determinar adecuadamente el *qué*, *quién, cuándo* y *cómo sucedió* el incidente de seguridad, así como también ocuparse del correcto aseguramiento y preservación de los datos recolectados

Los objetivos establecidos en este proyecto permitirán obtener información sobre la performance de dos metodologías de recolección de datos y analizar comparativamente sus prestaciones en base a determinados criterios y puntos de control establecidos sobre servidores web HTTP y HTTP/2.

Palabras clave: seguridad, incidente, forensia digital, evidencia digital, servidores web, HTTP.

Contexto

El presente PID 7052 se encuadra en una de las líneas de investigación establecidas como prioritarias para su fomento, de la carrera Licenciatura en Sistemas de la Facultad de Ciencias de la Administración correspondiente a la línea "Arquitectura, Sistemas Operativos y Redes". Se adecua además, a las prioridades de la UNER considerando que es un proyecto aplicado a la investigación sobre Tecnologías de la Información y la Comunicación. Asimismo, se continúan y profundizan líneas de trabajo planteadas en cursos de posgrado cursados sobre la temática y en la tesis doctoral presentada por el Dr. Darío Piccirilli [1]

Introducción

Si una arquitectura de seguridad informática está correctamente definida para un sistema, 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. Cuando se produce un incidente o amenaza de seguridad, en el cual un recurso del sistema queda comprometido o potencialmente expuesto a accesos no autorizados, esta arquitectura de seguridad se ve vulnerada.

A modo general, como amenazas del entorno, deben considerarse aspectos que incluyan desde la seguridad administrativa, la seguridad de las comunicaciones, la seguridad informática, la seguridad ambiental hasta la seguridad física. La arquitectura de seguridad debe poder afrontar tanto amenazas intencionales como accidentales, como así también lograr una registración adecuada de los incidentes o eventos de seguridad que ocurran en el sistema.

Diariamente cientos de equipos se encuentran expuestos a potenciales incidentes, consideremos como ejemplo el avance de Internet de las Cosas (IoT) y sus características de trabajo para llegar a dimensionar el grado de posibilidad y el riesgo de ocurrencia de un incidente y su consecuente impacto [2],[3]

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 a ese incidente de seguridad, así como también ocuparse de la correcta preservación y trazabilidad de los datos recolectados.

La definición brindada por la primera *Digital Forensics Research Workshop (DFRWS)* celebrada en Nueva York en 2001, acuerda que el análisis forense digital o forensia informática es "*El uso de métodos científicamente probados y derivados hacia la preservación, recolección, validación, identificación, análisis, interpretación, documentación y presentación de evidencia digital derivada de fuentes digitales con el fin de facilitar o promover la reconstrucción de los hechos, que pueden constituirse en evidencia legal, o ayudando a anticipar acciones no autorizadas que han demostrado ser perjudiciales para operaciones planeadas*." [4]

Las fuentes digitales proveedoras de los datos a analizar son numerosas, abarcan desde computadoras, teléfonos celulares, tarjetas de cámaras digitales, chips embebidos hasta snapshots de memoria, es decir cualquier tipo de dispositivo que produzca datos digitales.

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.

Un aspecto importante es la recolección de esta evidencia y la manera en que se asegura la calidad los datos recolectados.

Actualmente, las metodologías de recolección se concentran mayormente en dos enfoques:

1.- **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. [5],[6], [7]

2.- 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 trabajo se analizarán ambos enfoques metodológicos aplicados a servidores web, específicamente analizando información del protocolo HTTP en sus versiones 1.1 y 2. [8],[9],[10].
Las características funcionales del protocolo HTTP demandan que la recolección de evidencia sea realizada con herramientas o toolkits de análisis forense que proporcionen un entorno adecuado para asegurar la calidad de los datos, su trazabilidad y su eventual admisibilidad como prueba legal.
En este proyecto, para la ejecución de pruebas y adquisición de datos se usarán herramientas de forensia con licenciamiento libre [11],[12],[13] tales como CAINE [14], Xplico [15] y BACKTRACK [16] para las cuales se han configurado entornos de testing. Como guía general para las pruebas se considerará lo establecido en el OSSTMM (Open Source Security Testing Methodology Manual) [17].

Líneas de Investigación, Desarrollo e Innovación

Con este proyecto de investigación se espera conformar una base de conocimiento acerca de la forensia informática en relación a metodologías de recolección de datos digitales. Además del aseguramiento de la evidencia digital, un tema no menor, es poder determinar la calidad de datos obtenidos, la trazabilidad de los mismos y el volumen de información que se recopila con ambas metodologías. Este volumen de datos está directamente relacionado con el análisis de los tiempos de respuesta a incidentes y la capacidad de acciones inmediatas en tal sentido. Se utilizarán herramientas open source de forensia para determinar las más adecuadas para cada metodología y una guía práctica de aplicación de las mismas.

Resultados y Objetivos

Las actividades propuestas en este proyecto se sustentan en la necesidad de arribar a conclusiones generales y comparativas acerca de dos enfoques de recolección de datos digitales. Puntualmente, el objetivo primario es analizar la perfomance de ambas metodologías en entornos de servidores web.

Como resultados principales se espera lograr una matriz comparativa que permita:

1. Identificar y describir puntos de control en protocolos HTTP y HTTP/2
2. Identificar puntos de comparación entre enfoques de recolección de evidencia digital
3. Definir y configurar entornos de testing.
4. Describir procedimientos para la recolección de pruebas.
5. Determinar la correcta aplicación de herramientas/toolkits de análisis forenses considerando el entorno y el enfoque de recolección.

Formación de Recursos Humanos

Este proyecto prevé la formación e iniciación en actividades de investigación de cuatro docentes de la carrera Licenciatura en Sistemas, también la incorporación de un becario estudiante, el desarrollo de, al menos, dos proyectos de Trabajo Final de la carrera Licenciatura en Sistemas y la realización de una tesis de maestría correspondiente a la Maestría en Redes de Datos de la Facultad de Informática de la UNLP.

Referencias

1. Piccirilli, Dario. (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
2. Internet Crime Complaint Center (IC3). *Annual Report 2015* http://www.ic3.gov/media/annualreports.aspx
3. Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires. *CyberCrime Informe Final 2013 - Delitos Informáticos*. http://delitosinformaticos.fiscalias.gob.ar/wp-content/uploads/2014/02/CyberCrime-Informe-Final-2013-flip.pdf
4. Digital Forensic Research Workshop (DFRWS). http://www.dfrws.org/
5. TAN, John. (2001). *Forensic Readiness*. http://isis.poly.edu/kulesh/forensics/forensic_readiness.pdf
6. Rowlingson, Robert. *A Ten Step for Forensicc Readiness*. (2004) International Journal of Digital Evidence. Volume 2, Issue 3.
7. Pooe, A. , Labuschagne, L. *A conceptual model for digital forensic readiness* (2012) http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6320452
8. RFC 1945 Hypertext Transfer Protocol - HTTP/1.0 http://tools.ietf.org/html/rfc1945
9. RFC 2616 Hypertext Transfer Protocol - HTTP/1.1 http://tools.ietf.org/html/rfc2616
10. Draft Hypertext Transfer Protocol version 2.0 draft-ietf-httpbis-http2-04 https://tools.ietf.org/html/draft-ietf-httpbis-http2-04
11. *Digital Forensic with Open Tools*. (2011). DOI: 10.1016/B978-1-59749-586-8.00001-7. Elsevier.Inc
12. Díaz, Francisco Javier.Venosa, Paula.| Macía, Nicolás. Lanfranco, Einar Felipe. Sabolansky, Alejandro Javier. Rubio, Damián. *Análisis digital forense utilizando herramientas de software libre* . Aticulo presentado en Workshop de Investigadores en Ciencias de la Computación (2016) http://sedici.unlp.edu.ar/handle/10915/52766
13. 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*. Articulo presentado en Workshop de Investigadores en Ciencias de la Computación (WICC 2015). ISBN 978-987-633-134-0
14. Computer Aided Investigative Environment http://www.caine-live.net/
15. Open Source Network Forensic Analysis Tool (NFAT). http://www.xplico.org/
16. Penetration Testing and Security Auditing Linux Distribution. www.backtrack-linux.org/
17. Open Source Security Testing Methodology Manual (OSSTMM) http://www.isecom.org/mirror/OSSTMM.3.pdf
18. . U.S. Department of Justice. *Electronic Crime Scene Investigation: A Guide for*

First Responders, Second Edition. https://www.ncjrs.gov/pdffiles1/nij/219941.pdf
19. Forte, D. *Principles of digital evidence Collection* (2003) http://www.sciencedirect.com/science/article/pii/S1353485803000060
20. World Wide Web Consortium (W3C). http://www.w3.org/
21. Stallman, Richard: "*Free Software, Free Society: Selected Enssays"*. (2002). GNU Press, Boston Massachusetts,
22. RFC 3227 Guidelines for Evidence Collection and Archiving. https://www.ietf.org/rfc/rfc3227.txt
23. The *Open Web Application Security Project* (*OWASP*). https//www.owasp.org
24. Ley 26.388 "Ley de Delitos Informáticos". http://www.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm
25. Caracciolo Claudio, Rodriguez Marcelo, Sallis Ezequiel. (2010). *Ethical Hacking - un enfoque metodológico para profesionales*
26. López Rivera, Rafael. (2012). *Peritaje Informático y Tecnológico.*
27. Piattini, Mario. del Peso, Emilio. *Auditoria Informática*, 2da.edicion (2001) Editorial Alfaomega
28. Computer Forensics. (2008) Volume 56, Number 1. U.S. Department of Justice
29. FBI Cyber Crime. http://www.fbi.gov/about-us/investigate/cyber
30. Jarrett, Marshall. Bailie, Michael W. Electronic Evidence in Criminal Investigations. Computer Crime and Intellectual Property Section
31. del Peso Navarro, Emilio y colaboradores. (2001) *Peritajes Informáticos*. Editorial Díaz de Santos
32. Northcutt, Stephen. Novak, Judy. *Detección de Intrusos* 2da. Edición. (2001). Editorial Prentice Hall
33. Código Procesal Penal de la Nación Argentina. http://www.infojus.gov.ar
34. Código Procesal Civil de la Nación Argentina. http://www.infojus.gov.ar
35. Ley 25236, Habeas Data. http:// www.infojus.gov.ar
36. 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)
37. Digital Evidence and Computer Crime. Forensic Science, Computers and Internet. Third Edition (2011). Eoghan Casey. Elsevier Inc.