Análisis digital forense utilizando herramientas de software libre

Lic. Francisco Javier Díaz - Lic. Paula Venosa - Lic. Nicolás Macia - Lic. Einar Lanfranco
Lic. Alejandro Sabolansky - Damian Rubio
[javierd | pvenosa | nmacia | einar | asabolansky | drubio] at linti.unlp.edu.ar

LINTI (Laboratorio de Investigación en Nuevas Tecnologías Informáticas)
Facultad de Informática - UNLP
Calle 50 y 120 – 2do piso – La Plata, Buenos Aires, Argentina

1. Resumen

En la actualidad el mundo es digital. La mayor parte de la población utiliza medios digitales. Hoy en día se conecta a Internet gran cantidad de hardware y software sin considerar, muchas veces, los problemas de seguridad asociados con su uso.

Cuando se aprovecha una vulnerabilidad de un sistema informático y se concreta la amenaza mediante un ataque, nos encontramos con un incidente de seguridad que hay que estudiar.

En cualquier caso se necesita saber qué fue lo que sucedió teniendo como principal objetivo determinar las causas del problema para poder solucionarlo e identificar a los responsables del mismo. Ante esto, el análisis forense digital toma una gran relevancia.

Entre los alcances esperados de esta línea de I/D/I se espera ganar experiencia en lo que se refiere al campo de investigación del estudio digital forense. Para ello, se pretende identificar y probar herramientas de software libre que puedan ser utilizadas cuando se realiza este tipo de actividad. Además, en base al conocimiento adquirido, se espera generar documentos de buenas prácticas, procedimientos y materiales adecuados que puedan ser utilizados en cursos y capacitaciones sobre temáticas relacionadas con el estudio forense digital.

Palabras clave: seguridad de la información, forensia digital, software libre

2. Contexto

En el Laboratorio de Investigación en Nuevas Tecnologías Informáticas (LINTI) [1] de la Facultad de informática de la Universidad Nacional de La Plata [2], un grupo de docentes/investigadores se dedica a estudiar temas relacionados con la seguridad y privacidad de la información, aplicando los conocimientos en los distintos proyectos en el que participan.

En el marco del proyecto de incentivos "Internet del Futuro: Ciudades Digitales Inclusivas, Innovadoras y Sustentables, IoT, Ciberseguridad, Espacios de Aprendizaje del Futuro", este grupo investiga vulnerabilidades de seguridad actuales que afectan a sistemas, redes y servicios. En particular, la línea que se presenta se enfoca en el estudio de la forensia digital en los incidentes de seguridad, utilizando sofware libre, considerando:

- Relevamiento de buenas prácticas en el campo de la investigación forense.
- Definición de documento de procedimientos a aplicar.
- Relevamiento de las herramientas existentes para cada uno de los pasos del procedimiento.
- Relevamiento de los dispositivos de hardware que sean elementales.
- Elección de las herramientas que se consideren adecuadas.
- Generación de guía de análisis forense para capacitar.

Este grupo de investigadores forma parte del Centro de excelencia de la UNLP en el tema "Ciberseguridad" [3], seleccionado por la UIT (Unión internacional de Telecomunicaciones) para el año 2015.

3. Introducción

En la actualidad el mundo es digital, la mayor parte de la población utiliza medios digitales. Si bien esta adopción fue en paulatino y constante crecimiento desde la aparición de las primeras computadoras personales allá por el año 1981 [6], en los últimos años se aceleró de manera notable la penetración de la tecnología en el día a día de las personas. Esto se debió a distintos factores como:

- La disponibilidad de conexión a Internet, sobre todo con la masificación del acceso a través de banda ancha.
- La aparición de dispositivos móviles, en particular los denominados smartphones o teléfonos inteligentes [7].
- La llegada del fenómeno denominado Internet de la Cosas (IoT) [8].

La aparición de IoT ha generado un crecimiento exponencial de la cantidad de dispositivos conectados por persona. Por ejemplo, la persona que antes tenia una PC, hoy suele tener en el mejor de los casos la PC, un router inalámbrico, el celular, la tablet y el TV. Esta evolución de dispositivos interconectados va de la mano de la funcionalidad que brindan generando que se desarrolle y conecte muchísimo hardware y software sin considerar, muchas veces, los problemas de seguridad que su uso trae asociado. Esto se debe a que se desarrollan dispositivos pensando en la funcionalidad y usabilidad de los productos y no en la seguridad de la información que los mismos manipulan [9].

Cuando a través de un ataque informático se concreta una amenaza aprovechando una vulnerabilidad existente, se está frente a un incidente de seguridad. Los incidentes de seguridad deben ser analizados, ya sea tanto para solucionar el problema como para poder determinar el origen del mismo. Esta investigación se la conoce como análisis forense. El análisis forense digital, según Miguel López Delgado [10], en un sentido formal, es definido como un conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que llegado el caso puedan ser aceptadas legalmente en un proceso judicial.

El análisis forense se puede realizar simplemente a nivel institucional o llegar al ámbito de la justicia civil o penal. A nivel mundial la legislación se está adecuando a los nuevos tiempos que vive el mundo [11] [12], donde la mayoría de los delitos que existían en el mundo no digital se transladan al mundo virtual. Es importante destacar que en muchos países el fraude electrónico se encuentra en el podio de los delitos más efectivos [13], considerándose muchas veces tan rentable como el narcotráfico.

Aún en instituciones donde las pérdidas no son económicas, ante un ataque exitoso aparecen problemas de diversos tipos, como ser en el caso de la UNLP donde el defacement de la página institucional implica una pérdida de prestigio [14] o la pérdida de disponibilidad de los recursos de la organización, por ejemplo.

Cualquiera sea el perjuicio producido se necesita saber qué fue lo que pasó, para paliar la situación, para solucionarla y para perseguir a los responsables. Para lograrlo es necesario el análisis forense y de allí su importancia.

A esta disciplina, se la puede definir como un área perteneciente al ámbito de la seguridad informática surgida a raíz del incremento de los diferentes incidentes de seguridad. Éste es un tipo de análisis que se realiza con posterioridad a la ocurrencia de los incidentes, intentando reconstruir cómo se ha penetrado o vulnerado un sistema y en lo posible identificando a los responsables.

A modo de resumen, podemos decir que se intenta responder al menos a las siguientes preguntas:

- ¿Quién ha realizado el ataque?
- ¿Cúando y cómo se hizo?
- ¿Qué vulnerabilidades aprovechó?
- ¿Qué hizo el atacante una vez que tuvo exito y accedió al sistema?

Para llevar adelante estos estudios existen una serie de herramientas de hardware y de software que posibilitan tanto llevarlos a cabo técnicamente como que sus resultados tengan validez, ya que hay que tener en cuenta una serie de cuestiones que tienen que ver con la preservación de la evidencia. Un ejemplo de este tipo de herramientas es un dispositivo, denominado duplicador [15], el cuál permite realizar una copia exacta de la información de un

disco rígido a nivel físico sin alterar la información original existente en el dispositivo a analizar.

4. Líneas de Investigación, Desarrollo e Innovación

Sobre los ejes de investigación, inicialmente planteados: forensia digital utilizando software libre hasta el momento podemos mencionar que:

- Realizamos una recopilación de bibliografía para conocer el estado del arte actual.
- Participamos de una serie de charlas en distintas conferencias de seguridad que trataban la temática.
- Asistimos al cyberdrill para CSIRTS realizado por la ITU .
- Participamos de seminarios web dictados por la OEA.
- En el marco del trabajo diario de CERTUNLP hemos realizado varias forensias digitales ante eventos.

5. Resultados y Objetivos

5.1. Objetivo General

Se espera ganar experiencia en lo que se refiere al campo de investigación del estudio digital forense, lo que permitirá hacer una selección de un conjunto de herramientas de software libre que puedan ser recomendadas para realizar este tipo de actividad.

5.2. Objetivos Específicos

- Indagar sobre las prácticas recomendadas en forensia digital.
- Identificar los posibles escenarios de un estudio forense y las mejores técnicas a seguir en cada uno de ellos.
- Relevar las múltiples herramientas de software existentes, poniendo especial énfasis en aquellas que sean de software libre.
- Relevar las múltiples herramientas de hardware existentes.
- Generar una lista de todas las herramientas que se consideren recomendables para este tipo de investigaciones.
- Generación de material que pueda ser utilizado en cursos de capacitación o cátedras de la Facultad relacionadas con la temática.
- Formar RRHH que retroalimenten al grupo de investigadores convirtiéndolo en un referente en el tema.

6. Formación de Recursos Humanos

La línea de investigación en forensia digital está siendo abordada por integrantes del LINTI que forman parte del grupo de seguridad: Nicolás Macia, Paula Venosa, Einar Lanfranco y Alejandro Sabolansky, quienes desarrollan su actividad también desde el año 2008 en CERTUNLP, el centro de respuesta a incidentes académico de la Universidad Nacional de La Plata.

En CERTUNLP trabajan tres becarios, entre ellos Damián Rubio, que se encuentra actualmente participando en las tareas relacionadas a forensia digital, formándose y capacitándose en esta temática.

El plan de trabajo del docente Lic. Einar Lanfranco se encuentra en sintonía con la presente línea de investigación, dirigido por el Lic. Javier Díaz y la Lic. Paula Venosa.

El grupo de seguridad del LINTI de la Facultad de Informática de la UNLP trabaja desde el año 2000 con distintas experiencias relacionadas con la Seguridad de la Información: auditorias de seguridad, implementación de infraestructuras de seguridad, consultoría, desarrollo e implementación de Software Libre y concientización.

Cabe destacar que este grupo de investigadores representa a la UNLP en el Centro de excelencia en el tema “Ciberseguridad” de la UIT, durante el transcurso del año 2015 [5].

Dentro de este marco, durante año 2016 se dictará el curso “Tratamiento y resultados desde la Evidencia digital usando software libre”, coordinado por el Lic. Einar Lanfranco.

Además el grupo comenzó a participar en el año 2014 de la comisión de estudio ITU-T SG17:Security

de la UIT [4], donde se abordan temas actuales de seguridad de la información.

La Facultad de Informática aprobó a fines de 2015 el proyecto de transferencia "La Forensia Digital en el mundo del software libre" coordinado por los docentes: Lic. Einar Lanfranco, Lic. Nicolas Macia y Lic. Paula Venosa, el cuál debe llevarse a cabo durante el año 2016.

Referencias

[1] Laboratorio de Investigación de Nuevas Tecnologías Informáticas - LINTI.Facultad de Informática: `https://www.linti.unlp.edu.ar`

[2] Facultad de Informática: `https://info.unlp.edu.ar`

[3] Centro de excelencia en Ciberseguridad. http://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2015/0225-BR-COE/Agenda-EN.pdf

[4] Grupo de Estudio 17 en la ITU http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/default.aspx.

[5] ITU. http://www.itu.int

[6] http://www-03.ibm.com/ibm/history/exhibits/pc25/pc25_birth.html

[7] https://www.itu.int/net/itunews/issues/2011/03/12-es.aspx

[8] http://www.cisco.com/web/solutions/trends/iot/overview.html

[9] http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[10] Análisis Forense Digital. Miguel López Delgado. http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

[11] http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Default_en.asp

[12] http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Legal-Measures.aspx

[13] http://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf

[14] http://www.zone-h.org/archive/filter=1/fulltext=1/domain=unlp.edu.ar

[15] https://www2.guidancesoftware.com/products/Pages/tableau/products/forensic-duplicators/td3.aspx