textOsFtextTOsFliningLFliningTLFtextosflininglftabulartabproportionalpropsuperiorSup superiorSup

fontspechyperref

TITLE

Author1

University

HERRAMIENTA DE ENTRENAMIENTO EN SEGURIDAD INFORMÁTICA BASADA EN CÓMPUTO FORENSE.

Jesús Antonio Álvarez Cedillo, Félix Saucedo Garnica

Centro de Innovación y Desarrollo Tecnológico en Cómputo
"UP Adolfo López
Mateos", Av. Juan de Dios
Bátiz s/n casi esq. Miguel Othon de Mendizabal
Edificio del CIDETEC. Colonia Nueva Industrial Vallejo. México DF.
Email: jaalvarez@ipn.mx, fsaucedog0200@ipn.mx

RESUMEN

EL constante reporte de vulnerabilidades en sistemas de información, el aprovechamiento de fallas, bien sea humanas, procedimentales o tecnológicas, sobre infraestructuras de computación en el mundo, ofrecen un escenario perfecto para que se cultiven tendencias relacionadas con intrusos informáticos. Estos intrusos poseen diferentes motivaciones, alcances y estrategias que desconciertan a analistas, consultores y cuerpos especiales de investigaciones, pues sus modalidades de ataque y penetración de sistemas varían de un caso a otro. A pesar de esto, el cómputo forense nos ofrece un espacio de análisis y estudio que nos permite procurar una reflexión profunda sobre los hechos y las evidencias que se identifican en el lugar donde se llevaron a cabo las acciones catalogadas como criminales. En este momento es preciso establecer un nuevo conjunto de herramientas, estrategias y acciones que permitan descubrir en los medios informáticos la evidencia digital que sustente y verifique las afirmaciones que sobre los hechos delictivos se han materializado en el caso bajo estudio. Este trabajo pretende mostrar una panorámica general de la informática forense, resaltando en primer lugar su importancia, sus objetivos y usos. Acto seguido se explica la necesidad de las herramientas informáticas de entrenamiento y de análisis de las evidencias digitales en los medios informáticos.

1.

INTRODUCCION

La computación forense es una disciplina naciente que desde sus inicios ha establecido un reto tanto para los profesionales de ciencias de la computación y tecnología de información, como para los criminalistas tradicionales y la administración de la justicia en general. La necesidad de contar con un profesional que reconozca y actúe conforme a los requisitos de ley y siga los procedimientos básicos en criminalística, ahora en fenómenos o casos donde la informática y la tecnología se hacen presentes, es una ventana para repensar la práctica de las ciencias forenses en un entorno digital [7,1].

La seguridad de la información es muy reciente. Sus implicaciones van desde el análisis forense de un incidente común de pérdida o de ocultamiento de información en una computadora personal, hasta aspectos de defensa nacional. Esta disciplina está adquiriendo una gran importancia dentro del área de la información electrónica, esto debido al aumento del valor de la información y al uso que se le da a ésta, al desarrollo de nuevos espacios donde es usada, por ejemplo el internet, y al extenso uso de computadoras por parte de las compañías de negocios tradicionales como los bancos. Es por esto que cuando se realiza un crimen, muchas veces la información queda almacenada en forma digital. Sin embargo, existe un gran problema, debido a que los computadores guardan la información de información forma tal que no puede ser recolectada o usada como prueba utilizando medios comunes, se deben utilizar mecanismos diferentes a los tradicionales. Es de aquí que surge el estudio de la computación forense como una ciencia relativamente nueva [3,1].

2.
EVIDENCIA DIGITAL

La evidencia digital es cualquier información que, sujeta a una intervención humana u otra semejante ha sido extraída de un medio informático [8]. En este sentido, la evidencia digital es un término utilizado de manera amplia para describir cualquier registro generado por o almacenado en un sistema computacional que puede ser utilizado como evidencia en un proceso legal.

En este sentido, el documento mencionado establece que la evidencia digital puede ser dividida en tres categorías, a saber:

1.

Registros almacenado el en equipo de tecnología informática. Como ejemplos tenemos: correos electrónicos, archivos de aplicaciones, imágenes, etc.

2.

Registros generados por los equipos se tecnología informática. Como ejemplos tenemos: registros de auditoría, registros de transacciones, registros de eventos, etc.

3.

Registros que parcialmente han sido generados y almacenados en los quipos de tecnología informática. Como ejemplos tenemos: hojas de cálculo financieras, consultas especializadas en bases de datos, vistas parciales de datos, etc.

La evidencia digital es la materia prima para los investigadores donde la tecnología informática es parte fundamental del proceso. Sin embargo y considerando el ambiente tan cambiante y dinámico de las infraestructuras de computación y comunicaciones, es preciso detallas las características propias

de dicha evidencia en este entorno. La evidencia digital, para aquellos que la identifican y analizan en la búsqueda de la verdad, posee, entre otros elementos que la hacen un constante desafío, las características siguientes:

1.

Es volátil

2.

Es anónima

3.

Es duplicable

4.

Es alterable y modificable

5.

Es eliminable

Estas características nos advierten sobre al exigente labor que se requiere por parte de los especialistas en temas de informática forense, tanto en procedimientos como en técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentas la evidencia presente en una escena del delito. Por tanto es necesario mantener un conocimiento detallado de las normas y regulaciones legales asociadas con las pruebas y el derecho procesal, así como de las técnicas y los procesos que permitan mantener la confiabilidad de los datos recogidos, la integridad de los medios, el análisis detallado de los datos y la presentación idónea de los resultados.

3.
HERRAMIENTAS DE INFORMÁTICA FORENSE

Las herramientas informáticas son la base esencial de los análisis de las evidencias digitales en los medios informáticos. Sin embargo, es preciso comentar que éstas requieren una formalidad adicional que permita validar tanto la confiabilidad de los resultados de la aplicación de las mismas, como la formación y el conocimiento del investigador que las utiliza. Estos dos elementos hacen del uso de las herramientas una constante reflexión y un cuestionamiento por parte de la comunidad científica y práctica de la informática forense en el mundo.

Dentro de las herramientas frecuentes utilizadas en procedimientos

forenses en informática, detallamos algunas, las cuales son aplicaciones que tratan de cubrir todo el proceso en la investigación forense en informática. Como se observa en la Tabla 1.

[]@ ¿p() * 0.20 ¿p() * 0.20 ¿p() * 0.20 ¿p() * 0.20 ¿p() * 0.20@

	Licencia	Control de integridad	Análisis	Administración del caso
Encase	Sí	Sí	Sí	Sí
Forensic Toolkit	Sí	Sí	Sí	Sí
Winhex	Sí	Sí	Sí	Sí
Sleuth	No	Sí	Sí	Sí

Tabla 1. Herramientas utilizadas en procedimientos forenses en informática.

La informática forense es un desafío interdisciplinario que requiere un estudio detallado de la tecnología, los procesos y los individuos que permitan la conformación de un cuerpo de conocimiento formal, científico y legal para el ejercicio de una disciplina que apoye el esclarecimiento de los hechos alrededor de los incidentes o los fraudes en las organizaciones. La informática forense es la manifestación natural del entorno digital y de la sociedad de la información para responder a la creciente ola de incidentes, fraudes y ofensas, todo esto en medios informáticos y a través de medios informáticos, con el fin de enviar un mensaje claro a los intrusos indicando que se esta preparado para responder a sus ataques y se continúa aprendiendo para dar con la verdad de sus acciones.

Estas herramientas siguen el proceso operativo de la computación forense, que se representa en la Figura 1.

[]@ll@

Figura 1. Modelo operacional de la computación forense [2].

4.

EL INTRUSO

Es importante conocer la mente del intruso y como éstos piensan, actúan y operan para desarrollar la pericia para predecir y analizar los posibles rastros y acciones que se desarrollen en medios tecnológicos. Esto ofrece al administrador o al informático forense una ventaja estratégica y conceptual sobre el caso que revise, pues se pondrá en el lugar del infractor y tratará de ver como actuaría en un caso semejante. Así mismo, el estudio de otros ataques le dará mayores elementos de juicio para establecer patrones de análisis que ayuden a detallar lo ocurrido y así apoyar las investigaciones relacionadas con el caso. En la tabla 2 es posible apreciar algunas de las características de los intrusos informáticos.

[]@ ¿p() * 0.33 ¿p() * 0.33 ¿p() * 0.33@

Características	Intruso interno	Intruso externo
Psicológicas ·		
Motivado por situación personal o laboral.		
.		
Inestabilidad emocional		
.		
Socialmente hábil para recabar información y conocer a sus victimas. ·		
Generalmente motivado por reto tecnológico y compensación económica		
.		
Sensación de control y poder sobre un tercero		
.		
Relaciones basadas en		
.		
.		
conocimiento y logros		
técnicas ·		
Conocimiento detallado de fallas en procedimientos y regulaciones internas.		
.		
Conocedor y estudioso de la operación de la organización y su modelo de procesos y controles		
.		
Conocedor de los mecanismos de seguridad y control ·		
Conocedor y estudioso de las fallas tecnológicas de los sistemas objetivo		
.		
Conocedor y usuario de técnicas de evasión de investigaciones		
.		
Cuenta con un laboratorio de pruebas para verificar previamente sus acciones		

Tabla 2. Características básicas de los intrusos informáticos [7].

Si bien el rol del intruso es importante y atractivo, no es posible conocer los detalles de los rastros, si el administrador, el profesional de tecnologías de información a cargo de la administración y control de las computadoras que posiblemente están involucradas, no se encuentra capacitado o no cuenta con las herramientas necesarias para analizar las evidencias digitales. En este rol, el administrador de la seguridad debe comprender los conceptos de protección y control de tecnologías de información, no solo para detallar las medidas tecnológicas de seguridad y control configuradas, sino para identificar y analizar las diferentes formas de alerta, detección, registro y monitoreo que la infraestructura tiene definidas para prevenir algún tipo de incursión de autorizada. En este sentido el administrador se enfrentará al reto de la inseguridad de la información y sus diferentes fuerzas, reconocerá las relaciones entre las tecnologías de protección y las fallas de seguridad informática, para afianzar su visión de intruso.

Existen diferentes consideraciones para concebir o para clasificar a los atacantes, así como las motivaciones que los mueven a actuar en una situación particular. Ver Tabla 3

[]@ ¿p() * 0.14 ¿p() * 0.14 ¿p() * 0.14 ¿p() * 0.14 ¿p() * 0.14 ¿p() * 0.14 ¿p() * 0.14@

Motivaciones	**Ciberterroristas**	**Phreakers**	**Script kiddies**	**Crackers**	**Desarrollo de virus**	**Atacante interno**
Reto		X		X	X	
Ego		X	X	X		
Espionaje					X	X
Ideología	X					X
Dinero		X		X	X	X
Venganza	X			X		X

Tabla 3. Algunos tipos de atacantes y sus motivaciones. Obetnido de Furnell, S. 2002, p55.

Furnell habla de atacantes con perfil de, entre otros términos, ciberterrorista, phreakers, script kiddies, crackers, desarrollador de virus. Cada uno de ellos se mueve por motivos diferentes que llevan una carga emocional que es importante analizar y no solamente, las consideraciones técnicas de sus acciones, que dicen del nivel de conocimiento del individuo

5.

EL

INFORMÁTICO FORENSE O ADMINISTRADOR DEL SISTEMA

Este profesional será quien se encargue de la búsqueda de va verdad, en el análisis de la información residente en los dispositivos tecnológicos, en la construcción del caso con las evidencias digitales requeridas para esclarecer los móviles de los hechos, que se han podido presentar, bien sea en medios informáticos o electrónicos, o en combinación de hechos físicos y tecnológicos. Las características que deben tener el informático forense o el administrador del sistema se presentan en la Figura 2.

[]@ll@

Figura 2. Características del administrador de sistema [7].

5.1

Dificultades que se le podrían presentar al Informático forense

El profesional de la computación forense enfrentara en sus labores algunas dificultades, las cuales podrán relacionarse con el personal, los procesos, escasa o ninguna documentación de los sistemas, etc.

A continuación se enumeran algunas de las dificultades a las cuales podrá enfrentarse [1]:

.

No contar con los registros de auditoría. Esto puede suceder, porque el aplicativo no los tiene implementados o si los tiene, están desactivados (la entidad podría justificar que los registros están degradando la computadora).

.

Registros incompletos o no claros de las pistas de auditoría. Esto ocurre porque solo se graban algunos campos para no cargar el sistema o no existen descripciones detalladas de los registros.

.

No se realiza un buen levantamiento de información de la arquitectura del sistema y se dificulta determinar la forma y quién realizó la transacción fraudulenta.

.

Poca habilidad en el manejo de las herramientas.

.

Resistencia por parte de los funcionarios para suministrar información porque no les agrada ser investigados o porque podrían estar relacionados con el ilícito.

.

Restricción de acceso a la información de la entidad. Si se cuenta con el conocimiento y las herramientas necesarias, los funcionarios de seguridad informática y/o auditoría de sistemas de la entidad podrían adelantar la investigación forense y no habría mayor dificultad en el acceso a la información; pero si se requiere que por la especialización del tema lo realice un tercero, éste investigador deberá trabajar de manera estrecha con las áreas de seguridad bancaria, jurídica y la auditoría de sistemas

6. CONCLUSIÓN

Utilizando herramientas de cómputo forense podemos obtener información relativa a cómo, cuándo y dónde se produjo un ataque informático, esto con la finalidad de reparar los daños o de averiguar la procedencia y los objetivos de dicho ataque. Sin embargo, la continua evolución de los sistemas de información permite que los intrusos redefinan sus métodos y técnicas de ataque, por lo que en necesario contar con herramientas y técnicas de análisis de evidencias digitales y así definir una metodología e implementar un plan de prevención,

minimización de daños o de recuperación en caso de un ataque. Es necesario conocer las fortalezas y debilidades de las herramientas de computación forense a nivel comercial y de software libre para adaptar una aplicación que forme el perfil de administrador y entrene al informático forense y así mismo dé confiabilidad de los resultados.

7. REFERENCIAS

[1] Computación forense: una forma de obtener evidencias para combatir y prevenir delitos informáticos.

Yuri Vladimir López Manrique. Guatemala, marzo de 2007.

[2] Desarrollo de una interfaz gráfica multiplataforma para una herramienta de computación forense. Edward Andrés Corredor Rondón. Bogotá D.C. 2007

[3] Informática forense: generalidades, aspectos técnicos y herramientas. Óscar López, Haver Amaya, Ricardo León, Beatriz Acosta. Universidad de Los Andes Bogotá, Colombia

[4] Computational Forensic Techniques for Intellectual Property Protection. Jennifer L. Wong, Darko

Kirovski and Miodrag Potkonjak. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 23, no. 6, june 2004

[5]

Non-parametric statistical techniques for computational forensic engineering. Jennifer lee Wong.

[6]

Relative generic computational forensic techniques Jennifer l. Wong and miodrag potkonjak. University of California, Los Ángeles.

[7]

Computación forense, Descubriendo los rastros informáticos. Jeimy Cano. Alfaomega 2009.

[8]

Guidelines for the Management of IT Evidence. APEC Telecommunications and Information Working Group 29th Meeting | 21-26 March 2004 | Hong Kong, China

Referencias

[1] http://www.robotis.com/xe/darwin˙en

[2] Brushless DC (BLDC) Motor Fundamentals, Padmaraja Yedamale Microchip Technology Inc.

[3] Técnicas de control para motores Brushless Comparativa entre conmutación Trapezoidal, conmutación Sinusoidal y Control Vectorial, Roger Juanpere Tolrà.

Referencias

[1] Albert Einstein, Isaac Newton, Marie Curie, Galileo Galilei, Charles Darwin ***(mayo - junio, 2025)*** *La teoría de la evolución biológica. Boletín UPIITA. año 19, (108) 2025* liga del artículo