ÍNDICE

ACERCA DEL AUTOR

Mario Guerra Soto es Ingeniero de Telecomunicación por la Universidad de Cantabria (UC). Durante siete años trabajó en el Mando Conjunto de Ciberdefensa como DFIR, *threat hunter*, analista de ciberinteligencia, y analista de *malware*. Es Máster en Seguridad de Tecnologías de Información y Comunicación por la Universitat Oberta de Catalunya (UOC), y Máster en Análisis de Evidencias Digitales y Lucha contra el Cibercrimen por la Universidad Autónoma de Madrid (UAM). Dispone de las certificaciones en ciberseguridad GCFA, GCTI, GREM, CEH, CHFI, CND, CCPA, CASA y KAPE. Además, ha realizado otros cursos relacionados con la ciberseguridad, como el de Cyber Security Professional por la NATO School of Oberammergau, y el Curso de Especialidades Criptológicas por el Centro Criptológico Nacional (CCN). Ha colaborado como ponente en diferentes CON nacionales como RootedCON, Cybercamp, C1b3rwall, IntelCon, Hackron y TACS. Colabora como docente en el programa de postgrado de la UAM y de la Universidad de Salamanca (USAL).

1

INTRODUCCIÓN A FORENSE DIGITAL

1.1 CONCEPTOS BÁSICOS

1.1.1 Definición de forense digital

La Ciencia Forense juega un papel fundamental en las investigaciones criminales. Debe entenderse como una aproximación multidisciplinar que permite juntar todo tipo de evidencias en una investigación. Normalmente, durante el transcurso de una investigación, deberán aplicarse los principios y metodologías de diferentes disciplinas científicas para la presentación de evidencias ante un tribunal.

En 1910, el francés Edmond Locard establece el primer laboratorio forense policial en Lyon. Pasa además a la historia de la ciencia forense por enunciar el denominado **Principio de Locard** "*Todo contacto deja una huella*". Es decir, que la presencia del autor de los hechos en la escena del crimen conlleva una transferencia de evidencias, pues el criminal deja rastros en la escena del crimen, pero también lleva consigo evidencias que demuestran su presencia en dicho lugar. Dicho de otra forma, las acciones físicas dejan evidencias físicas en el mundo físico; las acciones digitales dejan evidencias digitales en el mundo digital.

Actualmente, entre las diferentes ramas de la Ciencia Forense destacan: Toxicología, Psicología, Podología, Patología, Odontología, Lingüística, Geología, Entomología, Ingeniería, Análisis de ADN, Botánica, Arqueología, Antropología, Balística y Digital.

Podría definirse Forense Digital como la disciplina que combina elementos legales, informáticos y de telecomunicaciones para obtener y analizar evidencias

digitales (Ej. Ordenadores, tráfico de red, dispositivos de almacenamiento, teléfonos móviles, *smartphones*, *wearables*) de modo que sean admisibles ante un tribunal. Si bien a primera vista su principal aplicación sería la investigación de cibercrímenes, el nivel de digitalización de la sociedad moderna provoca que, en la mayoría de los casos, sea necesario el análisis de una o más evidencias digitales.

A su vez, Forense Digital puede subdividirse en diferentes ramas: forense de ordenadores, análisis forense de información, forense de bases de datos, forense de red, forense de dispositivos móviles y forense de vídeo/audio.

Uno de los aspectos más complejos de las investigaciones forenses digitales consiste en determinar el papel que desempeña el dispositivo en el incidente objeto de estudio. En general, los dos roles que puede adoptar el dispositivo son:

- La herramienta empleada para realizar la acción objeto de estudio, es decir, el *arma del crimen*.
- El objetivo de la acción objeto de estudio, es decir, el *cadáver*.

Un ejemplo que permite ilustrar la clasificación anterior sería un escenario en el que un agente malicioso consigue tomar el control del equipo de un usuario de una organización. El atacante podría utilizar ese equipo bajo su control para intentar acceder a un servidor de ficheros dentro de dicha organización y exfiltrar información (entiéndase por exfiltrar la extracción ilícita de información sin conocimiento de su legítimo propietario). En este escenario, el equipo controlado por el atacante es la herramienta, mientras que el servidor es el objetivo. No obstante, si el atacante hubiese exfiltrado información del equipo corporativo bajo su control, este equipo sería a la vez la herramienta y el objetivo del ataque.

El dispositivo debe ser considerado la escena del crimen digital, pues contiene las evidencias digitales que permitirán al investigador forense digital determinar cuándo (*When*) y cómo (*How*) el ataque tuvo lugar. Adicionalmente, podrían obtenerse evidencias que demostraran quién (*Who*), qué (*What*), dónde (*Where*) y por qué (*Why*) realizó el ataque. Las famosas 5WH a obtener en toda investigación forense.

En forense digital, separar la parte legal de la parte técnica puede ser en ocasiones complicado. Los avances técnicos alteran los tipos de evidencia que pueden ser obtenidos; las modificaciones en las leyes afectan el modo en el que las evidencias pueden ser obtenidas y si esas evidencias serán admisibles ante un tribunal.

El reconocimiento de la importancia de las investigaciones forenses digitales tiene su primer hito con la creación en 1984 por el FBI del CART (*Computer Analysis and Response Team*).

La capacidad de determinar con prontitud el impacto de un ataque, la identidad del atacante y sus posibles objetivos son una muestra de los beneficios aportados a una organización por la disciplina de forense digital. Otros beneficios adicionales serían el mantenimiento del estado operacional de sistemas informáticos y redes, además de poder facilitar a las FCSE (Fuerzas y Cuerpos de Seguridad del Estado) la información necesaria de las actividades maliciosas llevadas a cabo por empleados maliciosos haciendo uso de los equipos y redes corporativas.

Existe cierta controversia a la hora de determinar qué es un cibercrimen. En general, suele considerarse que una actividad delictiva es un cibercrimen cuando solo pueda cometerse empleando ordenadores o comunicaciones digitales. Es decir, acceso ilegal a sistemas informáticos, distribución de *malware*, manipulación de aplicaciones informáticas, fraude en apuestas ilegales, ataques DoS (*Denial of Service*), *webjacking*, contrabando de identidades digitales y uso ilegal de equipos de telecomunicaciones contra dispositivos en red (Ej. *Eavesdropping*, creación de identidades digitales fraudulentas).

Por un lado, el atacante podría haber utilizado el dispositivo como herramienta para la comisión del delito (Ej. Acceder a un sistema remoto, envío de mensajería digital, videoconferencia). Por otro, el dispositivo pudiera ser el objetivo del ataque (exfiltración, modificación o borrado de información). Por tanto, el dispositivo será la escena del crimen en la cual hay que preservar las evidencias (Ej. Archivos de *log*, aplicaciones instaladas, línea temporal de actividades). Algunas de estas evidencias (Ej. Memoria RAM, tablas ARP, conexiones de red) tendrán un elevado grado de volatilidad (es decir, que su grado de permanencia con respecto del tiempo es limitada), debiendo ser por tanto obtenidas con la mayor presteza posible o desaparecerían. En cambio, otras evidencias (Ej. Archivos en disco duro, soporte óptico) tendrán un grado de volatilidad menor o, dicho de otro modo, su grado de persistencia será mayor.

Resulta por tanto necesario dentro de una organización que exista un equipo con las capacidades técnicas y recursos necesarios para poder hacer frente a un incidente concreto. La seguridad informática puede ser vista como un triángulo donde uno de sus lados lo constituye la detección y respuesta a intrusiones, siendo sus otros dos lados el análisis de vulnerabilidades y las investigaciones informáticas.

La detección de intrusiones, el análisis de vulnerabilidades y las investigaciones informáticas están directamente relacionadas con diferentes controles de seguridad que pueden ser implementados en una organización. El análisis de vulnerabilidades identifica los fallos a corregir o mitigar; la detección y respuesta a intrusiones representan controles de investigación y compensación; y las investigaciones intentan analizar el origen y establecer los pertinentes controles preventivos.