Forense Digital a un Fraude Electrónico Bancario

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Forense Digital & GNU/Linux

Sitio Web: http://www.ReYDeS.com | e-mail: ReYDeS@gmail.com

Viernes 20 de Octubre del 2017 - Lima Perú

8.8 Presentación

Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator Certified, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics y Cybersecurity Management.

Ha sido Instructor y expositor en OWASP Perú y en PERUHACK. Cuenta con más de catorce años de experiencia y desde hace diez años labora como Consultor e Instructor Independiente en las áreas de Hacking Ético e Forense Digital. Perteneció por muchos años al grupo internacional de Seguridad RareGaZz y al Grupo Peruano PeruSEC. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Forense Digital y GNU/Linux.

@Alonso_ReYDeS
www.facebook.com/alonsoreydes
pe.linkedin.com/in/alonsocaballeroquezada/

Evidencia Electrónica

Evidencia es cualquier ítem material o aseveración sobre un hecho, el cual puede ser enviado hacia un tribunal competente, como un medio de comprobar la verdad de cualquier asunto alegado sobre un hecho en investigación.

En la práctica judicial moderna, la evidencia electrónica no difiere de la evidencia tradicional, de tal manera es obligatorio para las partes presentándolas en un proceso legal, ser capaces de demostrar la evidencia está intacta desde el momento de su recolección, incluyendo el mismo proceso de recolección.

La captura, custodia, transferencia, análisis y disposición de la evidencia debe ser cronológicamente documentada de manera adecuada, constituyendo una cadena de custodia.

8.8 Directrices Generales

El manejo apropiado de cualquier evidencia, incluyendo evidencia electrónica, requiere seguir las algunas directrices generales.

- Debe ser manejado por especialistas.
- Es de rápida evolución.
- Utilización de procedimientos, técnicas y herramientas adecuadas.
- Debe ser admisible.
- Debe ser autentica.
- Debe ser completa.
- Debe ser confiable.
- Debe tener credibilidad.
- Debe ser proporcional.

Características

Algunas características de la evidencia digital

- Es invisible a un ojo no entrenado.
- Podría necesitar ser interpretada por un especialista.
- Es altamente volátil.
- Podría ser alterada o destruida a través de un uso normal.
- Puede ser copiada sin limites.

La rama de la ciencia forense enfocada en identificar, adquirir, procesar, analizar y reportar evidencia almacenada en sistemas de cómputo, dispositivos digitales y otros medios de almacenamiento, con el objetivo de ser admisible en una corte es denominada **Forense Digital**.

8.8 Principios base

Existen cinco principios base para tratar con evidencia electrónica. Estos principios fueron adoptados como parte de la Unión Europea y el Proyecto del Consejo de Europa para desarrollar una guía sobre la “captura de evidencia electrónica”.

Mientras las leyes respecto a la admisibilidad de evidencia difieren entre países, el utilizar estos principios se considera adecuado, pues son comunes a nivel internacional.

- Integridad de datos.
- Rastreo para auditoria.
- Soporte de un especialista.
- Entrenamiento.
- Legalidad.

8.8 Escenario

Un cliente de banco recientemente ha realizado una queja sobre una transferencia de dinero hacia una cuenta desconocida y nunca antes utilizada. De acuerdo a la declaración del cliente del banco, la transferencia fue hecha cuando no estaba utilizando el sistema de banca electrónica.

Sin embargo, el cliente admitió durante su llamada a la línea del banco, encontrar un mensaje de texto con un código de autorización para la transferencia en cuestión. Recuerda también interactuar con un juego de preguntas del banco para móviles. El cliente no percibió ninguna situación sospechosa; declara utilizar únicamente una computadora para la banca electrónica, con el mismo navegador de Internet todo el tiempo.

8.8 Escanerio (Cont.)

Como un mecanismo de prevención, el cliente cambio su contraseña durante la llamada.

Se ha recibido una notificación desde el equipo del sistema para la detección del fraude, sobre un fraude con un conjunto de característica previamente desconocidas para los sistemas.

La tarea es establecer un patrón para permitir encontrar otras transacciones requiriendo una investigación futura.

El cliente niega acceso hacia su computadora o móvil, por lo tanto se debe utilizar cualquier medio técnico disponible sobre el lado del banco, para encontrar pistas sobre las transacciones fraudulentas. Y encontrar datos relacionados con transacciones no autorizadas.

Resumen

- Se ha realizado un análisis en el lado del servidor sobre un caso de fraude bancario, como también en el lado del cliente.
- Se ha expuesto sobre los fundamentos relacionados a la captura de evidencia digital.
- Se ha expuesto sobre la extracción de evidencia desde los archivos “logs” (registro de eventos o sucesos) del sistema.
- Se ha realizado un análisis manual de Malware, además de conocer los fundamentos sobre las características del mismo.
- Resaltar lo siguiente: “Se debe ser consciente sobre la complejidad de los procedimientos forenses y entender los aspectos legales”.

8.8 Más Contenidos

Cursos Virtuales en Video

http://www.reydes.com/d/?q=cursos

Videos de Webinars Gratuitos

http://www.reydes.com/d/?q=videos

Mi Blog

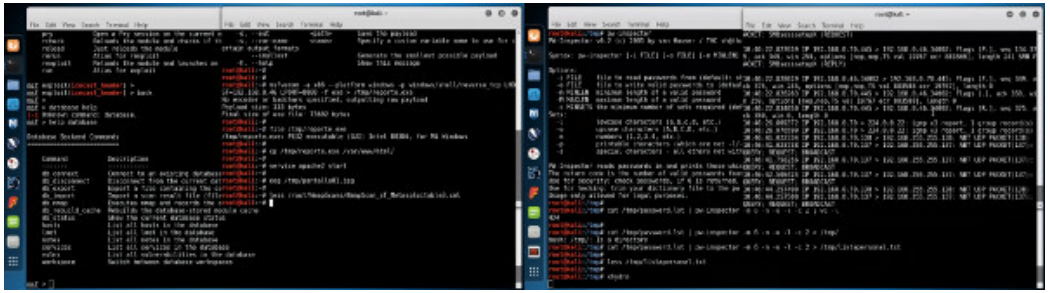
http://www.reydes.com/d/?q=blog/1

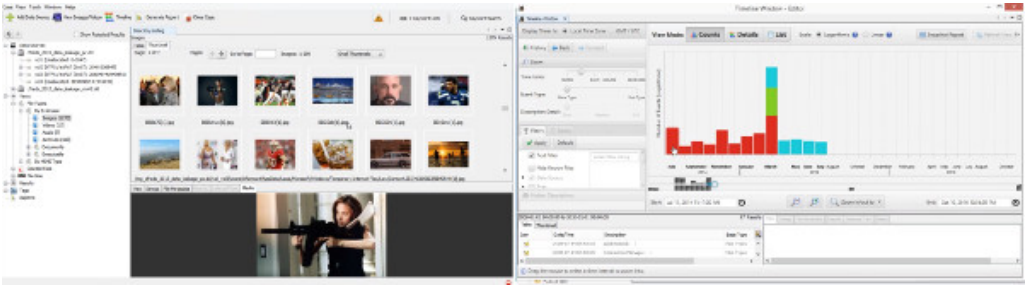
Mi Sitio Web

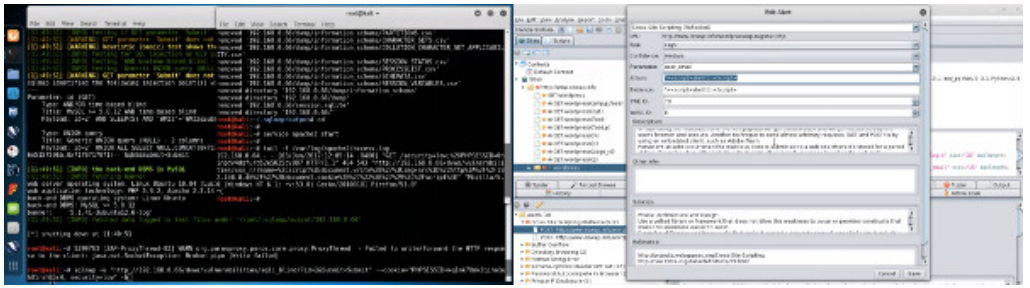
http://www.reydes.com/

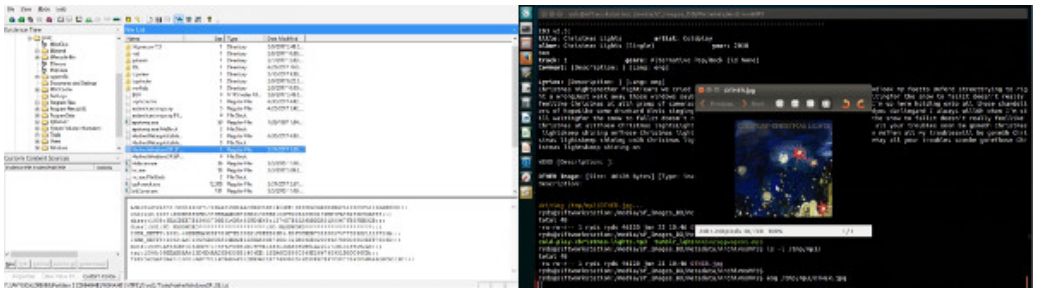
Correo Electrónico

reydes@gmail.com









¡Muchas Gracias!

Forense Digital a un Fraude Electrónico Bancario

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Forense Digital & GNU/Linux

Sitio Web: http://www.ReYDeS.com | e-mail: ReYDeS@gmail.com

Viernes 20 de Octubre del 2017 - Lima Perú