PERUHACK2016NOT

Forense Digital Ofensivo

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético e Informática Forense

reydes@gmail.com -:- www.reydes.com

Jueves 24 de Noviembre del 2016. Lima, Perú

Presentación

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

Cuenta con más de trece años de experiencia en el área y desde hace nueve años labora como Consultor e Instructor Independiente en las áreas de Hacking Ético & Informática Forense. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú.

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

Sobre el Taller

Objetivos:

El objetivo de este taller es presentar los fundamentos del forense digital, captura y análisis de evidencia.

Exponer un enfoque centrado en un servidor para la recopilación de evidencia, como también establecer patrones de actividad maliciosa. Estos patrones se utilizan para la identificación de eventos similares del pasado en el futuro cuando ocurran.

También se proporciona una introducción a las características del Malware, métodos para identificarlo y herramientas factibles de utilizarse en estos escenarios.

* Este taller se basa en el material para el entrenamiento en línea sobre Forense Digital de ENISA.

Sobre el Taller (Cont.)

Agenda

- Introducción
- Integridad de Datos
- Rastreo para Auditoría
- Soporte Especializado
- Entrenamiento Adecuado
- Tema Legal
- Ejemplos Prácticos

Conocimientos Previos:

- Conocimientos básicos de la shell de comandos en GNU/Linux
- Conocimientos básicos de redes

Introducción

Evidencia es cualquier ítem material o aseveración de 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 proceso de recolección.

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

Introducción (Cont.)

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

- Manejado por especialistas
- Evolución rápida
- Utilización de procedimientos, técnicas y herramientas adecuadas
- Admisibilidad
- Autenticidad
- Completitud
- Confiabilidad
- Credibilidad
- Proporcionabilidad

Introducción (Cont.)

Algunas características de la evidencia digital

- Es invisible a un ojo no entrenado
- Podría necesitar ser interpretado por un especialista
- Es altamente volátil
- Podría ser alterado o destruido a través de un uso normal
- Puede ser copiado 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**.

Introducción (Cont.)

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 para la “incautación 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 de auditoria
- Soporte de un especialista
- Entrenamiento
- Legalidad

Escenario

Un cliente de banco recientemente ha hecho una queja sobre una transferencia de dinero hacia una cuenta desconocida y nunca antes utilizada. De acuerdo a la declaración del cliente, 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, encontró 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 notó ninguna situación sospechosa; declara utilizar únicamente una computadora para la banca electrónica con el mismo navegador de Internet todo el tiempo.

Escenario (Cont.)

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

Se ha recibido una notificación desde el equipo del sistema de detección de 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 investigación futura.

El cliente niega acceso a 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.

Tarea 1

Identificar las características del fraude en la sesión HTTP

El principal objetivo es encontrar la diferencias entre una sesión HTTP normal y una fraudulenta, para luego identificar las características de la sesión fraudulenta de tal manera sea utilizada en las siguientes tareas.

Se trabaja con archivos “log” recolectados y se utilizan herramientas para extraer información desde estos para lograr el objetivo.

Tarea 2

Identificar otros clientes atacados basado en estas características

Después de haber identificado una característica patrón de la sesión fraudulenta, la siguiente tarea es rápidamente identificar otras posibles victimas.

Se debe preparar una lista de clientes registrando transacciones con el mismo patrón. La lista será enviada al equipo de detección de fraude para realizar una verificación telefónica con los clientes listados.

Tarea 3

Análisis manual de un volcado de procesos en memoria

Ahora se trabajará sobre el material recolectado desde la estación de trabajo del cliente victima del fraude. El cliente ha estado de acuerdo en proporcionar la información almacenada en su computadora.

Se verificará si esta información obtenida realmente contiene malware, extraer su tipo, versión y verificar si está configurada para atacar el banco.

Se trabaja con el volcado de memoria obtenido desde la estación de trabajo infectada.

Resumen Final

- Se ha realizado análisis en el lado del servidor de un caso de fraude bancario como también en el lado del cliente.
- Los participantes han aprendido sobre los fundamentos de la recolección de evidencia.
- Los participantes han aprendido sobre como se extrae la evidencia desde los archivos “logs” del sistema.
- Los participantes han realizado un análisis manual de Malware, y aprendido los fundamentos sobre las características del mismo.
- Se debe ser consciente sobre la complejidad de los procedimientos forenses y entender los aspectos legales.

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

https://www.reydes.com

PERUHACK2016NOT

Forense Digital Ofensivo

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético e Informática Forense

reydes@gmail.com -:- www.reydes.com

Jueves 24 de Noviembre del 2016. Lima, Perú

¡Muchas Gracias!