Alonso Eduardo Caballero Quezada
Consultor en Hacking Ético & Informática Forense

Único Curso del Año 2015

Este curso ha sido grabado y está disponible en video
Para adquirir los videos escribir a: caballero.alonso@gmail.com

1. Presentación:

El Sistema Operativo Windows XP aún es utilizado en diversos escenarios dentro de las empresas u organizaciones. Es el sistema operativo predominante en cajeros automáticos (ATMs). También es utilizado en algunos dispositivos médicos particulares. Así mismo se ejecuta en computadoras caseras y servidores proporcionando servicios internos. El soporte para Windows XP finalizó en Mayo del año 2014, esto deja una puerta abierta a temas de seguridad como exploits y malware.

Este Curso completamente práctico expone los aspectos técnicos para realizar un análisis forense a sistemas Windows XP. Abarcando las principales fuentes de evidencia digital, como también la utilización de herramientas forenses. Siendo una excelente fuente de conocimiento para profesionales forenses.

2. Temario:

- Análisis a la Memoria de Windows
- Análisis de un Volcado de Memoria Física
- Recolección de Procesos en Memoria
- Estructura del Registro de Windows
- Recolección y Análisis de datos desde el Registro de Windows
- Análisis de diversos Tipos de Archivos
- Registros de Eventos

- Metadatos de Archivos
- Métodos de Análisis Alternativos
- Análisis de Archivos Ejecutables

3. Material:

Se sugiere al participante descargar como mínimo los siguientes archivos en su sistema para desarrollar el Curso.

- **SANS Investigate Forensic Toolkit (SIFT)**
  Link de Descarga: https://digital-forensics21.sans.org/community/download-sift-kit/3.0
  Nombre del Archivo: SIFT Workstation 3.0.7z

- **DOMEXUSERS (NTFS)**
  Link de Descarga: http://digitalcorpora.org/corp/nps/drives/nps-2009-domexusers/
  Nombre del Archivo: nps-2009-domexusers.E01

[*] Si el participante lo requiere se le puede enviar un DVD con las máquinas virtuales e imágenes forenses, añadiendo S/. 40 Soles por el concepto de gastos de envío a cualquier lugar del Perú.

4. Día y Horario:

La duración total del Curso es de 6 (seis) horas. El Curso se dictará en los siguientes días y horarios.

Este curso ha sido grabado y está disponible en video
Para adquirir los videos escribir a: caballero.alonso@gmail.com

[*] No habrá reprogramaciones. El Curso se dictará **sin** ningún requisito mínimo de participantes.

5. Inversión y Forma de Pago:

El Curso tiene un costo de:

S/. 135 Soles o $ 45 Dólares

El pago del Curso se realiza mediante un depósito bancario en la siguiente cuenta:

ScotiaBank
Cuenta de Ahorros en Soles: 324-0003164
A nombre de: Alonso Eduardo Caballero Quezada

Una vez realizado el depósito, enviar por favor el voucher escaneado o sencillamente detallar los datos al siguiente correo: **caballero.alonso@gmail.com**.

Para residentes en otros países por favor escribir un mensaje de correo electrónico para consultar el mecanismo de pago. Confirmado el depósito se enviará al correo electrónico del participante, los datos necesarios para conectarse al Sistema y poder participar en el Curso.

6. Más Información:

Si desea mayor información sobre el Curso Forense de Windows XP, tiene a su disposición los siguientes mecanismos de contacto:

Correo electrónico: caballero.alonso@gmail.com

Vía Web: http://www.reydes.com

Celular: (+51) 949304030

7. Sobre el Instructor:

Alonso Eduardo Caballero Quezada es Brainbench Certified Network Security (Master), Computer Forensics (U.S.) & Linux Administration (General), IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling y Miembro de Open Web Application Security Project (OWASP). Ha sido Instructor en el OWASP LATAM Tour Lima, Perú del año 2014, y Conferencista en PERUHACK 2014. Cuenta con más de once años de experiencia en el área y desde hace siete años labora como Consultor e Instructor Independiente en las áreas de Hacking Ético & Informática Forense. Perteneció por muchos años al grupo internacional de Seguridad RareGaZz e integra actualmente el Grupo Peruano de Seguridad PeruSEC. Ha dictado cursos en Perú y Ecuador, presentándose también constantemente en exposiciones enfocadas a, Hacking Ético, Informática Forense, GNU/Linux y Software Libre. Su correo electrónico es ReYDeS@gmail.com y su página personal está en: http://www.ReYDeS.com