/Rooted

DFIR
Respuesta ante incidentes

Antonio Sanz

Valencia 2022

DOSSIER DE FORMACIÓN

/Rooted

Valencia 2022

Ponencias presentadas por speakers internacionales y expertos técnicos.

Presentación

- **Misión**: queremos compartir conocimientos, atraer diferentes culturas, exponer el talento local y marcar la diferencia.
- **Visión**: ser responsables haciendo algo diferente, compartiendo cultura y construyendo una red de conocimiento. Ser un evento honesto, confiable, beneficioso y establecer alianzas y colaboraciones con socios, clientes y competidores.
- **Nuestra cultura ganadora y nuestros valores en vivo:** colaboración, diversidad, talento por todas partes, pasión, calidad y enfoque en los clientes (cada persona que asiste a nuestros congresos).

Objetivos

Ransomware. Estafas al CEO. Robo de datos por empleados descontentos. Ciberespionaje (industrial o de otros estados nación). El mundo actual depende totalmente de la tecnología, y los cibercriminales lo saben muy bien. Ante el aumento de los incidentes, la necesidad de tener personal técnico preparado para responder de manera rápida y eficiente es cada vez más importante.

El objetivo de la formación es dotar a los asistentes de procedimientos, estrategias y herramientas para que sean capaces de responder ante un incidente de seguridad de forma solvente.

Con un carácter eminentemente práctico, se plantearán las fases de la respuesta ante incidentes, indicando en cada caso las mejores herramientas disponibles y la mejor forma de sacarles el máximo partido, así como los quick wins que permiten encontrar la actividad maliciosa lo antes posible.

El curso tendrá una componente forense fuerte, pero con la orientación propia de la respuesta ante incidentes, ofreciendo una simulación de incidente, 15 ejercicios prácticos y un CTF

A quién va dirigido

- Profesionales del sector de la ciberseguridad: analistas de SOC, peritos forenses, threat hunters, pentesters
- Administradores de sistemas
- Estudiantes
- Docentes
- Fuerzas y Cuerpos de Seguridad
- Cualquiera que quiera aprender las bases de la respuesta ante incidentes

Profesor: Antonio Sanz

- Ingeniero Superior de Telecomunicaciones por la Universidad de Zaragoza, con más 20 años de experiencia en el sector de la seguridad de la información.

- Actualmente es el responsable de análisis forense y respuesta ante incidentes de S2 Grupo, estando a cargo de los GIR (Grupos de Intervención Rápida) para la respuesta ante ransomware, ciberespionaje y otros incidentes a gran escala.

- Antonio es ponente habitual de conferencias nacionales de reconocido prestigio (RootedCON, STIC CCN-CERT, C1b3rwall), habiendo ofrecido de forma frecuente formación y talleres de respuesta ante incidentes y contando con una plataforma de CTF de forense y respuesta ante incidentes de acceso libre: https://ctf.unizar.es

Requisitos: Conocimientos

- Conocimientos básicos de Windows
- Conocimientos básicos de Linux
- Conocimientos básicos de virtualización (Vmware / VirtualBox)
- Conocimientos básicos de redes

Requisitos: Técnicos

- Equipo portátil con al menos 8Gb de RAM
- Capacidad para ejecutar al menos 1 máquina virtual (Vmware/VirtualBox), ya que se facilitarán máquinas virtuales de Windows y Linux con herramientas ya preconfiguradas
- Al menos 100Gb de disco duro (recomendable SSD pero no imprescindible)

Contenido

- Respuesta ante incidentes: conceptos básicos
- Preparación: Forensic readiness. Hablaremos de cómo podemos preparar nuestra organización para que, en caso de sufrir un incidente, tengamos toda la información necesaria para poder llevar a cabo la investigación de forma correcta.
- Detección de incidentes y activación de la respuesta: En esta fase se detecta el incidente, se descarta que se trata de un falso positivo, y se clasifica, activando la respuesta ante el mismo.
- Adquisición de evidencias: esta fase es vital, ya que toda evidencia no adquirida correctamente no podrá ser analizada. Se hablará de herramientas de adquisición, así como de procedimientos para minimizar los errores en la toma de datos.
- Análisis de incidentes: en esta parte (que llevará la mayor parte de la parte práctica) se comentarán los artefactos forenses más productivos a la hora de investigar un incidente de seguridad:
    - Logs del antivirus
    - Logs del firewall
    - MFT
    - Logs de eventos
    - Registro de Windows
    - Navegación de usuarios
    - Correo electrónico
    - USB
    - Análisis de RAM
    - Prefetch / UserAssist / BAM
    - SRUM

Contenido

- Contención: Una vez detectado el incidente y obtenido el alcance, discutiremos las opciones que tenemos para poder atajar el incidente y las medidas que podemos tomar para ello
- Erradicación: la erradicación es quizás una de las fases más complejas, ya que tiene que ejecutarse con unas condiciones específicas y siguiendo un procedimiento estricto. Hablaremos de cómo hacerlo bien, y sobre todo de cómo hacerlo bien a la primera.
- Recuperación: Una vez pasada la tormenta, hay que volver a la normalidad. Comentaremos las mejores estrategias de cómo recuperarnos del incidente (y sí, hablaremos de las copias de seguridad también, y algo de continuidad de negocio)
- Diseminación: todo lo hecho durante el incidente tiene que estar debidamente documentado, tanto para demostrar la debida diligencia como para tener un archivo de los incidentes gestionados. Hablaremos de cómo tomar notas, redactar informes de incidentes y presentarlos debidamente.
- Lecciones aprendidas: todo incidente es una oportunidad… si aprendes del mismo. Aquí tocará discutir lo que se ha hecho bien, lo que se ha hecho mal, y cómo podemos mejorar nuestra ciberseguridad para evitar que nos vuelva a pasar lo mismo.

Agenda

- 08.30-09.00h Bienvenida, café y puesta a punto de los equipos
- 09.00-11.00h Comienzo de la parte de respuesta ante incidentes
- 11.00-11.30h Pausa café
- 11.30-14.00h Análisis de incidentes
- 14.00-15.00h Comida
- 15.00-17.00h Análisis de incidentes
- 17.00-17.15h Micropausa café
- 17.15 – 20.00h Resto de fases de la respuesta ante incidentes, comienzo del CTF

Nota: El CTF lo comenzaremos en el bootcamp pero lo iremos resolviendo vía Telegram a lo largo del fin de semana

Costes

- El precio final del Lab será de 125 euros

IMPORTANTE: Se requiere un mínimo de **SEIS (6)** asistentes para que el Lab pueda llevarse a cabo.

FAQ

- Dónde se celebra la formación?
  - A diferencia del Congreso RootedCON, las formaciones se celebran en la ADEIT - Fundación Universidad-Empresa. Dirección: Plaza Virgen de la Paz, 3. Valencia.
- Qué horario tiene la formación?
  - La formación comienza a las 9:00 de la mañana, pero procura estar un poco antes para poder acreditarte y tener tu portátil preparado.
  - Las formaciones suelen acabar entre las 19h y 20h.
- Como puedo registrarme?
  - Para el registro, ve directamente al RootedManager. Ahí, una vez registrado podrás seleccionar la formación y pagar directamente. Una vez se imparta la formación podrás solicitar la factura siguiendo los pasos indicados en el Portal.
- El training incluye comida?
  - Los training no incluyen comida. Pero hay varias opciones en la zona, y el profesor os dará más información.

/Rooted

Contacto: info@rootedcon.com