/Rooted

Respuesta ante incidentes en Windows y O365

MADRID

4 al 6 de Marzo de 2024

DOSIER DE FORMACIÓN


/Rooted

/Rooted

Días 4-6 de Marzo

Tres días de trainings y workshops

HOTEL Eurostars iHotel
Pozuelo de Alarcón

Días 7-9 de Marzo

Ponencias presentadas por speakers internacionales y expertos técnicos.

KINEPOLIS
Pozuelo de Alarcón

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).

Profesor: Antonio Sanz

- Ingeniero Superior de Telecomunicaciones por la Universidad de Zaragoza, con más de 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

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 dos CTF (uno de Windows y otro de O365)

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…

Requisitos: Conocimientos

Conocimientos básicos de:

- ✔ Conocimientos básicos de Windows
- ✔ Conocimientos básicos de O365
- ✔ Conocimientos básicos de virtualización (Vmware / VirtualBox)
- ✔ Conocimientos básicos de redes

Requisitos: Técnicos

Para el correcto funcionamiento del training será necesario que los alumnos dispongan de equipos con acceso de administrador para poder añadir, eliminar software o cambiar cualquier configuración del mismo.

Las máquinas deben contar con las siguientes características mínimas:

- ✔ Equipo portátil con al menos 8Gb de RAM
- ✔ Capacidad para ejecutar al menos 1 máquina virtual (Vmware/VirtualBox), ya que se facilitará una máquina virtual de Windows con herramientas y evidencias ya preconfiguradas
- ✔ Al menos 80Gb de disco duro (recomendable SSD pero no imprescindible)

Agenda (i)

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 (Artefactos forenses I)

14.00-15.00h Comida

15.00-17.00h Análisis de incidentes (Artefactos forenses II)

17.00-17.15h Micropausa café

17.15 – 20.00h Resto de fases de la respuesta ante incidentes

Agenda (ii)

09.00 - 11.00h Comienzo del CTF (Bases y nivel 1)

11.00 - 11.30h Pausa café

11.30 - 14.00h CTF (nivel 1-2)

14.00 - 15.00h Comida

15.00 - 17.00h CTF (nivel 2)

17.00 - 17.15h Micropausa café

17.15 – 20.00h CTF (nivel 3, lecciones aprendidas y cervezas post-incidente)

Agenda (iii)

09.00 - 11.00h Teoría de DFIR en O365

11.00 - 11.30h Pausa café

11.30 - 14.00h Adquisición de evidencias en O365. Incidentes típicos

14.00 - 15.00h Comida

15.00 - 17.00h CTF (nivel 1-2)

17.00 - 17.15h Micropausa café

17.15 – 19.00h CTF (nivel 2-3, lecciones aprendidas)

Costes

- El precio final de este **Bootcamp + entrada** al Congreso RootedCON es **1250 €**

- **Puedes registrarte y formalizar el pago en: https://reg.rootedcon.com**

IMPORTANTE:

Se requiere un mínimo de **SEIS (6)** asistentes para que el curso pueda celebrarse.

FAQ

- Dónde se celebra la formación?
  - A diferencia del Congreso RootedCON, las formaciones se celebran en el Hotel Eurostarts i-Hotel
  - Aquí puedes encontrar el mapa de la zona: Google Maps
- Qué diferencia hay entre BootCamp y RootedLab?
  - Diferenciamos los training por horas de formación. Un RootedLab tiene 8 horas de formación, mientras que un BootCamp tiene unas 24h.
- Qué horario tiene la formación?
  - La formación comienza a las 9 de la mañana, pero procura estar un poco antes para poder acreditarte y tener tu portátil preparado. El primer día recomendamos estar a las 8 :)
  - Las formaciones suelen acabar entre las 19h y 20h.
- Como puedo registrarme?
  - Para el registro, ve directamente al RootedManager: https://reg.rootedcon.com. 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.
- Puedo pagar con transferencia bancaria?
  - Si, desde el propio RootedManager podrás gestionar el pago mediante transferencia bancaria.
- 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