/Rooted

Respuesta a **incidentes de seguridad**, **análisis de malware** y **reversing** con herramientas **Open Source**

Abraham Pasamar

MADRID

2 al 4 de Marzo de 2020

DOSSIER DE FORMACIÓN

/Rooted

Días 2-4 de Marzo

Tres días de trainings y workshops

HOTEL Eurostars iHotel
Pozuelo de Alarcón

Días 5-7 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).

Objetivos

El Botcamp *Respuesta a incidentes de seguridad, análisis de malware y reversing con herramientas Open Source* está formado por tres partes individuales que, en su conjunto, aportan al alumno una visión profunda de los escenarios de respuesta a incidentes de seguridad, partiendo de la gestión y obtención de evidencias, pasando por el análisis de malware implicado en el incidente y finalizando con una introducción al *reversing* de malware (desde cero).

El creciente aumento de los incidentes de seguridad hace que sea cada vez más importante prepararse parar poder afrontar con garantías dichos episodios. Para ello, es necesario conocer y practicar metodologías y herramientas que nos podrán facilitar mucho la correcta gestión, diagnóstico e investigación de los incidentes de seguridad.

Este es un curso práctico pensado para técnicos que quieran conocer y profundizar en el área de respuesta a incidentes y en el análisis y *reversing* de malware.

Todas las herramientas que se utilizan son herramientas Open Source.

A quién va dirigido

- Profesionales del sector de la Seguridad de la Información
- Administradores de sistemas y/o redes
- Cuerpos y Fuerzas de Seguridad
- Docentes
- Estudiantes
- Cualquiera que este interesado en aprender y profundizar en el mundo de los Incidentes de Seguridad, en el análisis y el *reversing* de malware

Profesor: Abraham Pasamar

Abraham Pasamar es Ingeniero Superior y Master en Seguridad de la Información. Es CEO y fundador de la empresa INCIDE, especializada en DFIR y *Offensive Security*. Cuenta con más de 15 años de experiencia como *Incident Responder* y Analista Forense. Ha participado en cientos de investigaciones forenses e incidentes de seguridad.

Es profesor en postgrados, masters y otros cursos especialistas en diversas Universidades, entre otras, Universidad Politécnica de Catalunya (UPC), Instituto Empresa (IE), Universidad Internacional de Valencia (VIU), Universidad de Barcelona, Universidad Internacional de Catalunya.

Es habitual colaborador en la difusión y concienciación de ciberseguridad en diversos medios de comunicación.

Ha sido ponente en diversas conferencias de seguridad, entre otras, RootedCON, r2CON, ShellCON, Navaja Negra, No cON Name, ConectaCON, SnowCON.

Requisitos: Conocimientos

- Soltura en la shell de Linux
- Conocimientos de bash & python scripting
- Conocimiento de js, vbs y PS
- Conocimiento básico de C

Requisitos: Técnicos

El alumno deberá disponer de un equipo informático portátil con acceso administrativo. La maquina de ser capaz de ejecutar dos maquinas virtuales de forma simultánea, para ello se estiman las siguientes características mínimas:

- ✓ CPU DualCore
- ✓ 4 GB de memoria RAM
- ✓ Espacio en disco suficiente como para crear hasta 4 máquinas virtuales (60-80GB).
- ✓ Tener instalado VirtualBox o VMWare

Contenido

El *bootcamp* se llevará a cabo utilizando material didácticos que proporcionará el profesor, así como máquinas virtuales y otro software o ficheros que serán descargados de internet con la conexión proporcionada por *Rooted*.

Se impartirán ciertas explicaciones teóricas que se irán intercalando con ejercicios prácticos que los alumnos deberán ir resolviendo. Se adaptará el tiempo de resolución a un ritmo aceptable para la mayoría de los alumnos.

El curso se impartirá en castellano, aunque los materiales que se entregarán serán en Inglés.

Agenda (i)

- Incident Response [day 1]
  - IR Management
  - IR Preparation
  - IR Detection and Characterisation
  - Data Collection
  - Data Analysis
  - Intelligence Analysis
  - Attacker Methodology
  - Tools development
  - Practice: GRR, sleuthkit, log analysis, bash, PS and python scripting

Agenda (ii)

- Malware Analysis [day 2]
  - Malware Triage
  - Setting Up a Virtual Environment
  - Static Analysis (AntiVirus, Hashing, Strings, Packed Files,Yara rules)
  - Dynamic Analysis (Manual-> Runtime Monitoring, Automatic-> Sandbox)
  - Memory Analysis
  - Practice: Executing and extracting IOCs from malware samples and analysing Word Macro Documents (i.e. Emotet, etc.)

/Rooted

Agenda (iii)

- Malware Reversing (win32) [day3]
  - PE File
  - Introducing radare2 (r2)
  - Recognising C Code Constructs in Assembly (Pointers, Variables, Statements)
  - Calling Conventions
  - Malware Analysis Concepts (Malware Behavior, Persistence Mechanism)
  - API Functions
  - Data Encoding
  - Scripting with r2 (r2pipe)
  - Practice: Malware Analysis Examples (with r2)

Costes

- El precio final del Bootcamp + entrada al Congreso RootedCON es **1.100 €**

- **Cuando se abra el registro para las entradas al Congreso, se te enviará un código para canjear tu entrada.**

IMPORTANTE: Se requiere un mínimo de **DIEZ (10)** asistentes para que el curso pueda llevarse a cabo.

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. 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.
- Puedo pagar con transferencia bancaria?
  - Si, desde el propio RootedManager podrás gestionar el pago mediante transferencia bancaria.
- El training incluye comida?
  - Los trainings no incluyen comida. Pero hay varias opciones en la zona, y el profesor os dará más información.

/Rooted

Contacto: info@rootedcon.com