Iniciación al análisis de malware RootedLAB

/RootedCON Valencia 2018

/Rooted

A quién va dirigido

Profesionales del sector de la Seguridad de la Información

Estudiantes

Administradores de sistemas y redes

Desarrolladores que quieran mejorar su perfil

Cuerpos y Fuerzas de Seguridad

Docentes

Sobre el autor

Abraham Pasamar

- Abraham Pasamar es Ingeniero Superior por la Universidad de Zaragoza y Máster en Seguridad de Tecnologías de la Información por la Universidad de La Salle, Barcelona. Cuenta con más de 10 años de experiencia en el campo de la Ciberseguridad. Trabaja como experto en ciberseguridad especializado en análisis forense informático y respuesta a incidentes de seguridad. Es socio fundador y director de la empresa INCIDE.
- Más de 10 años de experiencia práctica como experto DFIR (forense digital e *incident responder)*, Consultor en ciberseguridad y Perito Informático
- Más de 10 años liderando un laboratorio forense
- Headhunter y formador de equipos DFIR
- Experiencia en la gestión de APT, fraude interno, pérdida de datos y otros incidentes en entornos complejos y casos de alto perfil. Tanto desde una perspectiva técnica y de gestión del caso y del cliente
- Conocimiento de artefactos forenses y automatización masiva de tareas
- Desarrollador de herramientas DFIR: shell scripting / python / Perl, Autoit, C, C ++
- Experto en Análisis de Malware
- Experto en ejercicios Red Team/ Blue Team
- Pentest Análisis de vulnerabilidades
- Experto Evasion Antivirus / Crypter s y técnicas fileless

Requisitos

Conocimientos y aptitudes

Requisitos previos:

- Conocimiento general de linux y windows
- Conocimeinto general del uso de máquinas virtuales (y snapshots)

Requisitos técnicos

- Los alumnos deberán traer configuradas 2 máquinas virtuales (un Windows 10 y un linux (distribución remnux)
- Deberán poder realizar snapshots (en la máquina windows) VBOX o VMWARE Workstation/Fusion (no player)

Contenido

Agenda

- El training transcurría durante **1 día.**
- Se realizará una pausa a media mañana y otra pausa para comer.
- La comida corre a cargo de cada uno de los asistentes.

Introducción

Curso práctico de iniciación al análisis de Malware

- Introducción / Contexto
- ¿Qué es malware?
- Tipos de malware
- Evolución del malware
- Objetivos del análisis del malware
- Inteligencia: Amenza vs Herramientasc

- Análisis estático – teoría
  - Formato PE
  - Strings
  - grep / Regular Expresion
  - Reglas Yara
  - Packers/Crypters
  - Ofuscación/cifrado de datos

- PRACTICA ANÁLISIS ESTÁTICO
  - Análisis estático de 2 muestras de malware

- Análisis dinámico - teoría
  - Tipos de análsis dinámico
  - Entorno de análisis
  - Herramientas

- PRACTICA ANÁLISIS DINÁMICO
  - Análisis dinámico de 2 muestras de malware

- Analisis en memoria - teoría
  - Procesos y uso de memoria
  - PRACTICA ANALISIS EN MEMORIA

- Desensamblado y debuging - teoría
  - x86 / x64 crash course
- PRACTICA DEBUGGING
  - Análisis debuging de 1 muestra de malware

- Tendencia actual: ataques fileless y uso de scrips - teoría
- PRACTICA ANALISIS SCRIPS
  - Análisis de 1 muestra (script) de malware

Costes

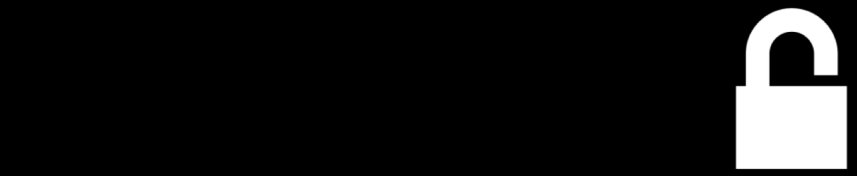
Coste

- El coste del curso es de 80€
- **IMPORTANTE**: se requiere un mínimo de DIEZ (10) asistentes para que el curso tenga lugar.

Contact

General information:	info@rootedcon.com
Registration form:	
https://reg.rootedcon.com	
Hashtag:	**#rootedvlc**
Abraham's twitter:	@apasamar
Twitter:	*@rootedcon*

/Rooted®



Muchas gracias