Curso básico de análisis de memoria RAM

/RootedCON Valencia 2019

/Rooted

Objetivos

- El curso mostrará la importancia del análisis de memoria RAM en los procesos de análisis forense y en la gestión de incidentes
- Introducirá los conceptos básicos del sistema operativo (**Windows**) que ayudan al análisis de la memoria RAM
- Los alumnos aprenderán a realizar la adquisición de memoria RAM con la herramienta **winpmem**
- Los alumnos prepararán el entorno para el análisis de memoria con todo el juego de herramientas necesarias
- Los alumnos aprenderán a manejar la herramienta **volatility**
- Los alumnos aprenderán diferentes estrategias de análisis de la memoria ram que ayuden a poder abordar este tipo de análisis en una organización

Sobre el formador

Sobre el formador

- **José Miguel Holguín** es ingeniero informático y lleva más de 10 años dedicado al área de la seguridad informática. En la actualidad trabaja en la empresa S2 Grupo como miembro del equipo **Lab52** centrado en proyectos de tipo DFIR (Digital Forensics and Incident Response) y Threat Intelligence.

- **Marc Salinas Fernández.** Analista de malware en S2 Grupo como miembro del equipo **Lab52**. Muy interesado en Windows Internals y virtualización.

Requisitos

/Rooted®

Requisitos

- Ordenador portátil
- Hipervisor: Virtualbox.
- Máquinas:
  - Máquina virtual windows 7 con: ProcessHacker, la suite de las sysinternals, x64dbg, yara (con las reglas de yararules.com).
  - Máquina Linux basada en la distribución remnux (https://remnux.org/).

Contenido

Introducción

El análisis de memoria RAM es una pieza fundamental en muchos incidentes hoy en día y su análisis requiere definir diferentes estrategias dependiendo de cuál es el objetivo del análisis.

En este curso se mostrarán diferentes estrategias de análisis básicas que ayuden a los asistentes a aplicar el análisis de memoria RAM en los casos más adecuados y obtengan el máximo fruto de dicho análisis.

El curso está centrado principalmente en **sistema Microsoft Windows** dado que es el sistema más extendido y por tanto el más atacado. El curso requiere es eminentemente práctico y los alumnos podrán practicar con la herramienta volatility y enfrentarse a casos reales de análisis.

Agenda

- 09:00 – 09:30 ¿Qué es y Porqué hacer Memory Forensics?
- 09:30 – 10:30 Introducción a arquitecturas Windows
- 10:30 – 11:00 Introducción a Volatility y preparación del entorno
- 11:00 – 12:00 Análisis de memoria con inteligencia de terceros
- 12:00 – 14:00 Análisis de evidencias de usuario en memoria (procesos, servicios, ficheros, red, etc.)
- 14:00 – 15:00 COMIDA
- 15:00 – 16:00 Detección de código inyectado en procesos
- 16:00 – 19:00 Ejercicio final y resolución

Costes

Coste

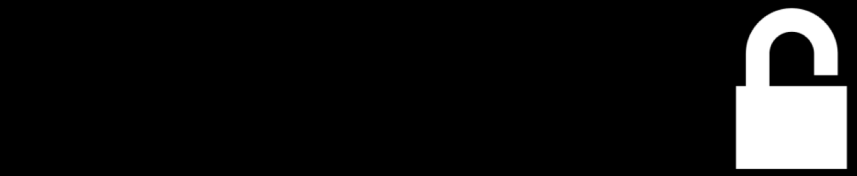
- El coste del curso es de 100€

- **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.es/training/.../	
Hashtag:	**#rootedvlc2019 #rootedcon**
Twitter:	
Facebook, LinkedIn:	*Rooted CON*
Twitter:	*@rootedcon* *Tags:* *#rootedvlc2019 #rootedcon*

/Rooted®



Muchas gracias