/Rooted

# EndPoint Threat Hunting

Roberto Amado

**MADRID**

7 al 9 de Marzo de 2022

**DOSSIER DE FORMACIÓN**

/Rooted

**Días 7-9 de Marzo**

*Tres días de trainings y workshops*

*HOTEL Eurostars iHotel*
*Pozuelo de Alarcón*

**Días 10-12 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

Este Bootcamp pretende enseñar a los asistentes como "cazar" tanto malware genérico, como especímenes pertenecientes a grupos APT mediante una correcta instrumentación de diversas herramientas y la generación de una serie de “Hunts” capaces de identificar los más sofisticados ataques. La orientación totalmente práctica permitirá aprender no solo técnicas de intrusión sino los “Hunts” que permiten identificarlas. Estos se agruparán según la matriz de Mitre ATT&CK™ en : movimiento lateral, reconocimiento, persistencia , explotación, entre otros.

El proceso de caza de malware se abordará desde dos perspectivas: por una parte el análisis del comportamiento de los procesos del sistema desde una perspectiva temporal (apoyándonos en la herramienta Sysmon) y por otra desde el punto de vista de la memoria RAM de los equipos, es decir se realizará un *hunting* de artefactos maliciosos basándonos en anomalías residentes en memoria.

Complementando lo anterior se abordarán tanto nociones de análisis de malware básicas como de *Threat Modeling*, que permitirán a los asistentes afrontar de forma completa un proceso de *Threat Hunting* orientado al *endpoint* y a entornos servidor de tecnologías Microsoft Windows.

Por último los alumnos afrontarán el reto de poder detectar actividades maliciosas de actores avanzados que hagan uso de ciberarmas como **Cobalt Strike** inmersos en un juego de RED vs BLUE team.

# A quién va dirigido

Este bootcamp va dirigido a profesionales del sector de la ciberseguridad que quieran o estén orientando su carrera hacia la búsqueda de amenazas activa. A *Threat Hunters* que quieran ampliar conocimientos en el campo de identificación de malware por comportamiento en entornos Microsoft Windows.

Tanto si eres un estudiante como un ingeniero senior y te quieres dedicar a la caza de software malicioso, este bootcamp cubrirá todo el proceso de hunting necesario para ello. Desde la configuración de la herramienta, al análisis de sus logs y la identificación de amenazas avanzadas, tanto en disco como en memoria.

¿Qué mayor satisfacción existe que destapar las actividades de grupos APT o de cibercriminales antes que nadie, incluso antes que las grandes firmas de antivirus?

Si quieres saber que se siente, este es tu bootcamp.

/Rooted

# Profesor: Roberto Amado @ramado78

Ingeniero en Informática y Telecomunicaciones trabaja en S2 grupo y en el mundo de la seguridad desde hace más de 13 años como: Pentester, Incident Handler, ICS security analyst y APT hunter siendo actualmente el director técnico de seguridad de la compañía. Autor de varias guías STIC (Pentesting, DNS y revisión WIFI) , con publicaciones como "Seguridad en Redes 802.11" y editor de securityartwork.com y lab52.io. Esta certificado como: CISA, CISSP, GIAC-GPEN, GIAC-GICSP, GIAC-GCIH.

LinkedIn - https://www.linkedin.com/in/robertoamado/

Twitter - https://twitter.com/ramado78

/Rooted

# Profesor: Jose Miguel Holguin

## @j0sm1

---

Ingeniero en Informática trabaja en S2 grupo y en el mundo de la seguridad desde hace más de 13 años como, Incident Handler, APT hunter, malware analysis y Threat intelligence  analyst siendo actualmente el coordinador técnico de Lab52 en S2 Grupo. Formador en varios cursos STIC y con varias publicaciones en el mundo de la seguridad relacionadas con investigaciones de grupos APT. Está certificado como: CISSP y GREM.

LinkedIn - https://www.linkedin.com/in/jholguin/

Twitter - https://twitter.com/j0sm1

# Requisitos: Conocimientos

Conocimientos básicos de:

- Análisis Forense.
- Análisis de malware.
- Desarrollo a nivel de lenguajes de scripting (Ej.Python).
- Threat Intelligence

Conocimientos medios de:

- Administración de sistemas operativos Microsoft Windows
- Redes conocimientos de protocolos de comunicación

Preferiblemente para estudiantes y profesionales de Ing. Informatica o Ing. Telecomunicación y apasionados de la ciberseguriad que dispongan del *skill* anteriormente descrito.

# Requisitos: Técnicos

Portátil con sistema operativo Windows y sistema de virtualización VMWARE.

Se proveerán las maquinas virtuales en el curso.

# Contenido

Un buen proceso de "caza" de artefactos malware hoy en día no está completo sin la revisión de la actividad de los equipos de usuario y servidores. Esta actividad puede ser trazada y monitorizada de diversas maneras y con diferentes herramientas, pero es Sysmon de Sysinternals, la que hoy en día ha ganado más popularidad por su potencia y versatilidad. Durante esta formación se mostrará como identificar malware perteneciente a actores clasificados como Amenazas Avanzadas Persistentes (APT), así como diversas actividades maliciosas en entornos Microsoft Windows de software malicioso de cibercriminales.

Para el proceso de caza en memoria se definirán una serie de “Hunts” a utilizar principalmente con la herramientas *Volatility*.

El contenido está estructurado en 3 días descritos a continuación.

# Agenda Día 1 (i)

**0x1.- [Teoría] Intro TH**

Se detalla el proceso de TH las diferentes aproximaciones y porque es importante establecer un proceso de defensa proactiva.

**0x2.- [Teoría] Conociendo lo normal par encontrar lo malicioso**

Se detallarán todos los procesos estándar que un sistema windows tiene en ejecución por defecto. Identificando: Funcionalidad, jerarquía (árbol del proceso), Numero de instancias, Propietario, momento de ejecución y descripción

**0x3.- [Práctica] Estableciendo una buena config de Sysmon**

El taller comienza la parte practica a través de la realización por parte de la audiencia de una configuración de sysmon que permite identificar las amenazas que posteriormente se detallan en los *hunts*.

# Agenda Día 1 (ii)

**0x3.1- Instalando Sysmon**

Se procederá a instalar la configuración de sysmon en la maquina víctima

**0x3.2- Desplegando entorno de ataque y detección**

Se desplegara un maqueta preconfigurada de 2 maquinas virtuales donde una será la atacante y otra la victima con el sysmon instalado.

**0x4.- [Práctica] Identificando anomalías y lanzando hunts**

Se proveerá de una máquina atacante con los vectores de intrusión maliciosos preparados (scripts de powershell, WMI, etc.) para ejecutar. El enfoque de esta sección permite tener una visión doble, la del atacante mostrando sus armas y la del defensor identificando la amenaza a través de Sysmon.

# Agenda Día 1 (iii)

**0x4.1 [Práctica] Hunting acceso inicial**

Se identificaran las principales acciones que los atacantes realizan para llevar a cabo el acceso inicial

**0x4.2 [Práctica] Hunting persistencia**

Cazar la persistencia es la mejor manera de detectar malware desconocido, se presentara como detectar los principales métodos de persistencia a través de sysmon, tanto en el momento que se

crean como una vez ejecutados.

**0x4.3 [Práctica] Hunting movimiento lateral**

El atacante necesita moverse dentro de la red por lo que se cubrirán los hunts que proporcionan la detección de las principales tecnicas de movimiento lateral: DCOM, psexec, WMI, tarea programada, etc.

**0x5 [Teoría] Evasión de sysmon**

# Agenda Día 2 (i)

0x6 [Teoría] Threat modeling

0x6.1 [Práctica] Threat modeling

Se propone que el alumno es un cliente/organización concreta, se les insta a que modelen sus posibles amenazas. Después han de buscar las TTPS de esos grupos en el mitre. Deben huntear en un evtx para responder a la pregunta que grupo APT tienes dentro de la organización.

0x7.- [Teoría] Hunting en memoria

El proceso de TH no está completo sin la revisión de la memoria de los equipos. En esta sección se abordarán un conjunto de anomalías o hunts que pueden darse en la memoría y que pueden ser indicativos de la presencia de malware.

0x7.1.- [Teoría] Qué es y porqué hacer Hunting en memoria

Cada vez es mas común observar malware fileless, es decir sin presencia de un artefacto en disco, es por eso que el análisis de memoria es fundamental para completar el proceso de TH.

# Agenda Día 2 (ii)

0x7.2.- [Práctica] Estrategias de hunting en memoria

0x7.2.1.- Hunting remoto con Yara

0x7.2.2.- Adquisición de memoria y hunting local con Volatility

0x7.3.- [Teoría - Práctica] Hunting activo en memoria

0x7.3.1 Hunting automatizado

Mediante herramientas de terceros se procede a lanzar un conjunto de hunts sobre la memoria adquirida.

- Hollowhunter
- Bulkextractor

0x7.3.2 Hunting manual

- Anomalías de procesos
- Anomalías en Virtual Address Descriptors
- Anomalías en Handles
- Anomalías en Conexiones de red
- Anomalias en Registro

# Agenda Día 3 (i)

0x7.4.- [Teoría - Práctica] Hunting Ring 0 Rootkits

Si el adversario ha conseguido implantar a nivel de kernel un rootkit es posible que nuestras herramientas de monitorización y caza no detecten su actividad maliciosa, es por eso que el último rincón del sistema donde este tipo de malware no puede esconderse es la memoria. En esta sección veremos como cazar rootkits de ring 0 mediante un conjunto de hunts para Volatility.

0x7.4.1.- Anomalias en Devices Trees
0x7.4.2.- Anomalias en Kernel callbacks
0x7.4.3.- Anomalias en Kernel Timers
0x7.4.4.- Anomalias en SSDT e IDT

# Agenda Día 3 (ii)

**0x8.-[Teoría - Práctica] Factores de decisión de legitimidad**

Una vez identificada una posible anomalía a través de un hunt se ha de saber decidir si el proceso que la causa es malicioso o no. En esta sección se cubrirán los factores principales de decisión que permiten atribuirla legitimidad del artefacto.

**0x9.-[Práctica] Reto detección de intrusión con Cobalt Strike y Metasploit**

Por ultimo y para cerrar el curso, el instructor desplegará una maqueta de equipos a la cual los alumnos tendrán acceso, protegiéndola y monitorizándola con la configuración de Sysmon elaborada por ellos. A continuación el instructor procederá a atacarla en modalidad CTF, mediante las suites Cobalt Strike y Metasploit, siendo los alumnos los encargados de detectar, analizar y responder con los conocimientos adquiridos en el curso.

# Costes

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

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

**IMPORTANTE**: Se requiere un mínimo de **CINCO (5)** 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: 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