

/Rooted®



Sysmon Threat Hunting

Roberto Amado

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

Este Bootcamp pretende enseñar a los asistentes como "cazar" tanto malware genérico, como especímenes pertenecientes a grupos APT mediante una correcta instrumentación de la herramienta Sysmon 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.

Complementando lo anterior se abordarán tanto nociones de análisis de malware, como Threat modeling y forense *First cut*, que permitirá a los asistentes afrontar de forma completa un proceso de *Threat Hunting* orientado al *endpoint* y 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**.

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.

¿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.

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: Penetester, 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>

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. Informática o Ing. Telecomunicación y apasionados de la ciberseguridad 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.

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 reconocimiento

Basándose principalmente en el process ID 1 se identificarán las principales acciones que los atacantes realizan para llevar a cabo el reconocimiento en una organización

0x4.2 [Práctica] Hunting acceso inicial

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

Agenda Día 1 (iV)

0x4.3 [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.

0x4.4 [Práctica] Hunting elevación de privilegios

Se identificarán las principales acciones que los atacantes realizan para llevar a cabo ataques de elevación de privilegios.

Agenda Día 2 (i)

0x4.5 [Práctica] Hunting evasión de medidas de seguridad

Mediante el análisis de los registros de Sysmon se identificarán algunas de las técnicas en este ámbito.

0x4.6 [Práctica] Hunting de acceso a credenciales

Se identificarán las principales acciones que los atacantes realizan para llevar a cabo acciones que les permiten obtener credenciales de acceso a los sistemas.

0x4.7 [Teoría] Evasión de sysmon

0x4.8 [Práctica] Hunting de obtención de información [1h] [JOAN]

Uno de los posibles objetivos finales de los atacantes es la posibilidad de extraer información de la red de la víctima. Veremos por tanto como es posible detectar con Sysmon alguna de las técnicas en este ámbito.

Agenda Día 2 (ii)

0x4.9 [Teoría] Threat modeling

0x4.10 [Práctica] Threat modeling

Se propone que el alumno es un cliente/organización concreta, se les insta a que lo modelen con lab52 Después han de buscar las TTPS de esos grupos en el mitre.

Deben huntar en un evtx para responder a la pregunta que grupo APT tienes dentro de la organización.

0x4.11 [Práctica] Hunting movimiento lateral [1h] [JOAN]

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

Agenda Día 3 (i)

0x5.-[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 atribuirle legitimidad del artefacto.

0x6.-[Teoría - Práctica] Forense first cut

Tras la conclusión e identificación de una pieza de malware es necesario saber como ha llegado hasta el equipo comprometido. Este estadio es muy importante dado que nos permitirá trazar posibles movimientos laterales, así como otros posibles equipos comprometido dentro de la red bajo análisis. Para ello se deben de disponer de conceptos básicos de análisis forense que nos ayuden, tanto a obtener evidencias como a posibles "huellas" que el atacante haya podido dejar en los equipos.

Agenda Día 3 (ii)

0x7.-[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 **1200€**
- 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®

