Sysmon Threat Hunting

/RootedCON Valencia 2019

/Rooted

Objetivos

¿Quieres ser Threat Hunter?

Este taller pretende como objetivo 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 mas sofisticados ataques.

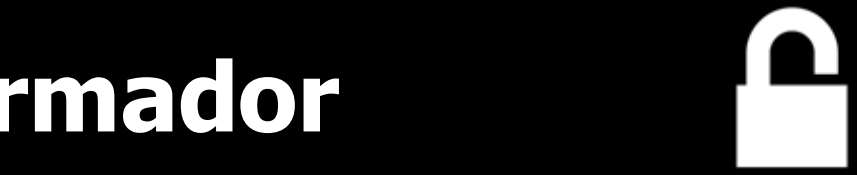
La orientación totalmente práctica tendrá una doble vertiente:

- Por un lado, el auditorio será capaz de ejecutar ataques sobre una maqueta previamente configurada, aprendiendo cuales son las principales técnicas utilizadas por el malware actualmente.
- Y por otro ver como Sysmon es capaz de registrar estos ataques, siendo estos analizados por el Threat Hunter.

Por lo tanto el alumnado obtendrá conocimiento no solo de las técnicas de intrusión sino los "*Hunts*" que permiten identificarlas. Estos se agruparán en como conocer en los logs de Sysmon las principales técnicas de:

- Movimiento lateral
- Reconocimiento
- Persistencia
- Explotación

Sobre el formador



/Rooted®

Sobre el formador

@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.

Requisitos

Requisitos

- Portátil con sistema operativo Windows y sistema de virtualización VMWARE.
- Se proveerán las maquinas virtuales en el curso.

Contenido

Introducción

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, así como diversas actividades maliciosas en un entorno Microsoft Windows.

Agenda

- **0x1.- [Teoria] Intro TH**
  - Se detalla el proceso de TH las diferentes aproximaciones y porque es importante establecer un proceso de defensa proactiva.

- **0x2.- [Teoria] Conociendo lo normal par encontrar lo malicioso**
  - Se detallaran 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.- [Practica] 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*.

    - 0x3.1- Instalando sysmon. Se procederá a instalar la configuración de Sysmon en la maquina victima
    - 0x3.2- Desplegando entorno de ataque y detección. Se desplegara un maqueta reconfigurada de 2 maquinas virtuales donde una será la atacante y otra la victima con el sysmon instalado.

Agenda

- **0x4.- [Practica] Identificando anomalías y lanzando hunts!**
  - Se proveerá de una maquina 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.

    - 0x4.1 [practica] hunting reconocimiento. Basándose principalmente en el process ID 1 se identificaran las principales acciones que los atacantes realizan para llevar a cabo el reconocimiento en una organización
    - 0x4.2 [Practica] hunting persistencia. Cazar la persistencia es la mejor manera de detectar malware desconocido, se presentara como detectar los principales metodos de persistencia a través de sysmon, tanto en el momento que se crean como una vez ejecutados.
    - 0x4.3 [Practica] 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 técnicas de movimiento lateral: DCOM, psexec, WMI, tarea programada, etc.

Agenda

- **0x5.-[Teoría - Practica] 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 atribuir la legitimidad del artefacto.

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