Digital Forensics & Incident Response RootedLAB

/RootedCON 2018

/Rooted®

Objetivos

Durante este taller aprenderemos las diversas técnicas que emplean los Red Team para vulnerar y atacar un sistema, de la misma manera veremos como los Blue Team establecen todas las medidas necesarias para una defensa. En el taller aprenderemos las capas normativas como NIST o Cyber Kill Chains hasta la adquisición de evidencias necesarias para una investigación forense digital como artefactos de Windows, arquitectura del sistema, Powershell, análisis de memoria ram, análisis de red, sistemas de ficheros y ataques laterales y también mecanismos de defensa cómo sysmon y herramientas orientadas a la respuesta ante incidentes. Si quieres estar cerca de los atacantes y que no te sorprendan entonces este es tu taller. ¿Te lo vas a perder?

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

El nivel que se impartirá es básico-medio

Sobre el autor

PEDRO SANCHEZ - CONEXIONINVERSA

He trabajado en importantes empresas como consultor especializado en Incident Response y pen-testing. He implantado normas ISO 27001, CMMI, PCI-DSS y diversas metodologías de seguridad en el sector bancario durante mas de diez años.

También colaboro sobre Respuesta ante incidentes, seguridad y análisis forense informático con diversas organizaciones comerciales y con las fuerzas y empresas de seguridad del estado.

He trabajado en el área de BlueTeam de Bitdefender para OTAN durante cuatro años. Participando en las jornadas LookShields organizadas por el ministerio de defensa y también obtuve la habilitación Nato Secret trabajando en proyectos de Defensa

Profesor del Summer BootCamp de INCIBE, formando a CERTS y Fuerzas de seguridad

He trabajado como responsable del equipo de respuesta ante incidentes (IR) de Deloitte.

Fundador del blog de Conexión Inversa

Actualmente soy el CSO & Incident Response de ITS Security y UNIT71 empresa y división cuya especialización es la protección de sistemas aeroespaciales, defensa militar e infraestructura criticas.

Requisitos

/Rooted®

Conocimientos y aptitudes

*No se requieren conocimientos avanzados los puntos enumerados anteriormente.

Requisitos técnicos

- Puedes traer tu equipo preferiblemente con Windows 10 o Windows 8 o una máquina virtual. Sería recomendable disponer de un mínimo de 6 u 8 Gb de ram
- Se te entregarán los materiales necesarios para la elaboración del taller

/Rooted®

Contenido

Introducción

Durante el lab se trabajará sobre una misma metodología pero con diferentes entornos de trabajo.

- Los siguientes puntos pueden variar en función de la dinámica del grupo de trabajo.
- Todos los asistentes irán al mismo ritmo y no se avanzará en los temas hasta que el grupo haya cumplido en sus totalidad los objetivos de cada uno de los puntos.

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.

/Rooted

- INTRODUCCIÓN
- METODOLOGIA
- ARQUITECTURA EN WINDOWS
- ATAQUES LATERALES
- ADQUISICIÓN – CLONADO
- ARTEFACTOS
- ANALISIS DE MEMORIA RAM

/Rooted

- DETECCIÓN BÁSICA DE MALWARE
- POWERSHELL EN DFIR
- INDICADORES DE COMPROMISO
- MEMORIA RAM
- SISTEMA DE FICHEROS
- ANALISIS DE RED

- DETECCIÓN DE ANOMALIAS
- HERRAMIENTAS DFIR
- TALLER DFIR
  - INSTALACIÓN DE UN SISTEMA DE DETECCIÓN AVANZADA (RECOLECTOR DE EVENTOS)
  - FILTRADO DE TRÁFICO

/Rooted

Costes

Coste

- El coste del curso es de 200€
- **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:	*#rooted 2018 #rootedcon*
Pedro's twitter:	@ConexionInversa
Facebook, LinkedIn:	
Twitter:	*@rootedcon #rooted2018 #rootedcon*

/Rooted®

Muchas gracias