DFIR

Digital Forensics Incident Response

RootedLAB

/RootedCON 2017

/Rooted

Objetivos

En este *training* el asistente aprenderá las diferentes técnicas para la detección y análisis de un incidente de seguridad. También conocerá y dispondrá de las herramientas que se emplean en un equipo de respuesta ante incidentes.

A quién va dirigido

Profesionales del sector de la Seguridad de la Información

Estudiantes

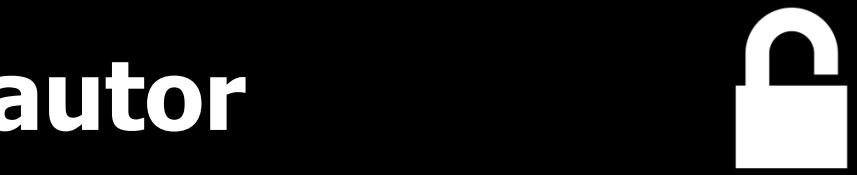
Administradores de sistemas y redes

Desarrolladores que quieran mejorar su perfil

Cuerpos y Fuerzas de Seguridad

Docentes

Sobre el autor



/Rooted®

Pedro Sánchez Cordero

Ingeniero informático. Ha trabajado en importantes empresas como consultor especializado en Computer Forensics, Honeynets, detección de intrusiones, redes trampa y pen-testing. Ha implantado normas ISO 27001, CMMI (nivel 5), PCI-DSS y diversas metodologías de seguridad especialmente en el sector bancario durante mas de diez años. Colabora sobre Respuesta ante incidentes, seguridad, peritaje y análisis forense informático con diversas organizaciones comerciales y con las fuerzas y empresas de seguridad del estado y agencias gubernamentales.

Ha trabajado en el área de Digital Forensics Incident Response de Bitdefender donde colaboro en proyectos con OTAN y donde obtuvo la certificación NATO Secret.

Es profesor del Summer BootCamp de INCIBE y es miembro de la Spanish Honeynet Project, fundador de Conexión Inversa y Perito Judicial Informático en la Asociación Nacional de Ciberseguridad y Peritaje Tecnológico (ANCITE).

Pedro ha sido ponente en Rooted CON 2010 y 2012 y ha impartido el training de RootedLabs de 2016. También ha sido ponente en NoConName, Navaja Negra y otros congresos como Hackron, Sh3llCon, Cybercamp entre otros. Ponente en congresos internacionales como BugCOM en México y DFRWS en Canadá.

Actualmente Pedro es el responsable del equipo de respuesta ante incidentes (DFIR) de Deloitte

Requisitos

/Rooted®

Conocimientos y aptitudes

Conocimientos básicos de:

- Sistemas operativos
- Conocimientos básicos de redes (TCP/IP)

*No se requieren conocimientos avanzados los puntos enumerados anteriormente.

Requisitos técnicos

- Para el correcto funcionamiento de los labs será necesario que los alumnos dispongan de equipos con las siguientes características o similares:
  - Equipo con al menos 4 GB de memoria RAM (recomendable más de 4)
  - Windows 8 o Windows 10
  - Ultima versión de VirtualBox
  - Tarjeta de red wifi y ethernet

Contenido

/Rooted®

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.

DFIR – DIGITAL FORENSICS INCIDENT RESPONSE

- INTRODUCCIÓN A DFIR
- METODOLOGIA
  - –Normativa
  - –Gestión de incidentes
  - –Procedimientos operativos
- ADQUISICIÓN – CLONADO
  - –Triage local
  - –Triage remoto
  - –Scripting

DFIR – DIGITAL FORENSICS INCIDENT RESPONSE

- ANÁLISIS DE ARTEFACTOS
  - –Introducción a artifacts
  - –Registro de windows
  - –Memoria virtual
  - –Sistema de cache

- ANALISIS DE MEMORIA RAM
  - –Adquisición
  - –Rekall
  - –Volatility
    - •Analisis de procesos
    - •Artefactos de memoria
    - •Analisis de malware

DFIR – DIGITAL FORENSICS INCIDENT RESPONSE

IOC's indicadores de compromiso
- –Crear un indicador
- –Aplicar un indicador ante un incidente

Reglas yara

HERRAMIENTAS DFIR
- –IRTOOLS POWERSHELL
  - •Remoting powershell
  - •Obtención de datos forenses
- –MONITORIZACIÓN Y DETECCIÓN
  - •IRTOOLS detección de procesos con sysmon

DFIR – DIGITAL FORENSICS INCIDENT RESPONSE

- Detección de incidencias con CROWDRESPONSE
- Detección de Malware con LOKI
- Detección de anomalías con BRO
- Detección con ANTIRANSOM
- Análisis con GRR
- Detección con MALICE

Costes

/Rooted®

Coste

- El coste del curso es de 200€
- **IMPORTANTE**: se requiere un mínimo de diez (10) asistentes para que el curso tenga lugar.

Contacto

General information:	info@rootedcon.com
Registration form:	
https://reg.rootedcon.es/training/.../	
Hashtag:	**#RC17**
Pedro's twitter:	@conexioninversa
Facebook, LinkedIn:	*Rooted CON*
Twitter:	*@rootedcon* *Tags:* *#rooted y #RC17*

/Rooted®

Muchas gracias