TEMARIO
FCSE nivel avanzado

Cybersecurity Summer BootCamp 2017

Cybersecurity Summer BootCamp 2017
18-29 julio - León (España)
www.incibe.es/summer-bootcamp

Organizado por:

Gobierno de España – Ministerio de Energía, Turismo y Agenda Digital
incibe_ Instituto Nacional de Ciberseguridad
OEA OAS

Con la colaboración de:

universidad de León
Ayuntamiento de León
León Cuna del Parlamentarismo
Gobierno de España – Ministerio de Asuntos Exteriores y de Cooperación
Santander
BID Banco Interamericano de Desarrollo
EUROPOL EC3 European Cybercrime Centre
INTERPOL

PROFESOR

Daniel Echeverri

Taller 13

Deep Web

Duración: 20 horas

Descripción

El principal objetivo del curso es el de enseñar las técnicas, herramientas y herramientas más importantes a la hora de configurar y aprovechar las características avanzadas de las principales redes de anonimato disponibles actualmente.
Se enseñarán los detalles más interesantes de soluciones tales como Tor, I2P y Freenet para comprender sus diferencias y características particulares. Finalmente, los alumnos adquirirán los conocimientos necesarios para realizar procesos de análisis y recolección de información estructurados y metódicos con el fin de obtener información sobre servicios ocultos en las principales darknets y en algunos casos, sobre los usuarios que navegan por dichos espacios.

Temario

1. **TOR**
   - Instalación y configuración de una instancia de TOR
   - Elementos básicos y configuración avanzada de TOR
   - Configuración en TOR de repetidores y servicios ocultos
   - Configuración y uso de TOR Bridges y Pluggable Transports / OnionCAT
   - Protocolo de control de TOR
   - Evitando fugas de información: Torifying con TorSocks
   - Personalización de direcciones onion con Shallot
2. **I2P**
   - Instalación y configuración inicial de I2P
   - Elementos de un router I2P
   - Servicios y aplicaciones preconfiguradas
   - Sistema de resolución de dominios I2P
   - Funcionamiento de la NetDB
   - Deep web y Servicios ocultos en I2P
   - Acceso programático a instancias de I2P
3. **Freenet**
   - Arquitectura de Freenet y funcionamiento de Fproxy
   - Funcionamiento de las claves en Freenet
   - Complementos y servicios en Freenet
   - Acceso programático a instancias de Freenet
4. **Darknets**
   - Creación de scripts para automatización de tareas contra redes anónimas
   - Búsqueda de contenidos en darknets y principales buscadores
   - Desarrollo de scripts para la automatización de tareas de análisis
   - Procesos de crawling, stemming y recolección de información contra darknets
   - Creación de hooks para ejecutar procesos de tracking contra usuarios

PROFESOR

Lorenzo Martínez

Taller 14

Forense en móviles

Duración: 10 horas

Descripción

Los smpartphones y tablets se han convertido en una herramienta indispensable en el día a día de los usuarios. Estos dispositivos no solo son capaces de almacenar información referente a la agenda de contactos, fotografías, mensajes, música o vídeos, sino que también pueden almacenar una gran cantidad de información que puede resultar de especial relevancia en casos de investigaciones y/o análisis forense.

Precisamente el uso extendido de los dispositivos móviles, y en muchas ocasiones sin grandes medidas de seguridad en el acceso a los mismos por parte de todos, incluidos los ciberdelincuentes, habilita una vía de obtención de información que puede resultar decisiva en el desenlace de una investigación policial.

Por ello, esta sesión pretende profundizar en el conocimiento necesario para la realización de un análisis forense a dispositivos móviles y mostrar el correcto uso de herramientas que faciliten la realización de este análisis, con el fin de extraer la información sensible al ser utilizada en un caso real.

Temario

1. **Gestión y respuesta ante incidentes relacionados con dispositivos móviles**
   - ¿Qué hacer?, ¿cómo?, ¿cuándo?
   - ¿Robo?, ¿malware?
   - Despliegue de un laboratorio necesario para el análisis de actividad en los dispositivos móviles
2. **IOS**
   - El backup en IOS
   - Juicy Files
   - Timeline
   - Análisis de actividad con herramientas comerciales: Oxigen
3. **Android**
   - Las aplicaciones en Android
   - Análisis estático
   - Análisis dinámico
   - Análisis de actividad con herramientas comerciales: Oxigen

PROFESOR

Ricardo Rodríguez

Taller 15
Análisis de malware

Duración: 10 horas

Descripción

El software con código malicioso, o malware, es una constante habitual en el día a día de la informática. Como reportan numerosas industrias del sector de ciberseguridad, el número de amenazas y su complejidad han ido en aumento en los últimos años. Es fácil de entender este aumento, dado la cantidad de dinero que es capaz de generar de una manera rápida y "sencilla".

El objetivo de este taller es realizar una aproximación al malware para la gente de las FCSE, de modo que conozcan los diferentes tipos de malware a los que se van a enfrentar, así como los conocimientos básicos y avanzados en el análisis de malware, junto con buenas prácticas recomendadas en caso de que tengan que gestionar incidentes de ciberseguridad relacionados con código malicioso.

Así, se enseñarán herramientas para el análisis de muestras maliciosas, tanto de manera estática como dinámica, junto con pautas para la creación de entornos de análisis, informes de resultados, y estrategias de mitigación.

Temario

1. **Introducción al malware**
   - Características, tipos, evolución
   - Vectores de ataques y canales de distribución
2. **Creación de laboratorio de análisis**
   - Necesidades y herramientas mínimas
   - Metodología de análisis de malware
3. **Conocimientos previos**
   - Arquitectura de x86 y ensamblador (conceptos mínimos necesarios)
   - Windows Internals: estructura PE, carga de binarios, binarios en memoria, APIs
4. **Análisis básico**
   - Análisis estático
   - Análisis dinámico
5. **Fases de ataque del malware**
6. **Análisis avanzado**
   - Análisis estático
   - Análisis dinámico
7. **Informes de amenazas: alcance y mitigación**
   - Desinfección
   - Reglas de detección (YARA, SNORT, IOC)