TEMARIO
FCSE nivel básico

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

PROFESORES

Jesús Díaz Vico

Francisco J. Rodríguez

Taller 10

Introducción a Deep Web

Duración taller: 20 horas

Descripción

Internet es la red global compuesta por cientos de miles de ordenadores a la cual solemos acceder a través de un navegador (Firefox, Chrome, Safari, etc.) y ayudados por un buscador (Google, Bing, DuckDuckGo...). No obstante, la información que podemos obtener a través de estos mecanismos "comunes" no es más que una pequeña porción del total. Términos como Deep Web y Dark Web son cada vez más frecuentes en el mundo tecnológico, especialmente después de escándalos como Silk Road y otros mercados ilegales o del apoyo recibido por activistas de la privacidad como Edward Snowden o Julian Assange.

Temario

1. **Introducción a las redes anónimas**
   - Surface web / Deep Web / Dark web
   - Proxys Tor2Web
   - Las dos caras de la moneda: privacidad y anonimato vs actividades criminales
2. **Tipos de sistemas para comunicaciones anónimas**
   - Redes anónimas más conocidas y cronología
   - Otras redes y herramientas
   - DC-nets, mix-nets y onion networks
   - Redes OutProxy / Inproxy
   - Distribuciones Linux
   - Tor en IOS y Android
3. **Onion networks y Tor**
   - Funcionamiento de redes de tipo cebolla
   - Autoridades de directorio
   - Documento de consenso. Proceso de votación
   - Flags asignados a nodos
   - Tipos de nodos (Guard, Middle y Exit)
   - Mapeado de nodos, estadísticas...
   - Bridges / directorios de caché / establecimiento de circuitos
   - Hidden services y negociación de puntos de encuentro
   - Descriptores
   - Cifrado de información, cifrado cebolla
   - Práctica
   - Ataques a la red Tor
4. **Otras redes anónimas tipo cebolla**
5. **Otras herramientas: Stem, ARM**

PROFESOR

Pedro Sánchez

Taller 11
Introducción a forense en móviles

Duración taller: 10 horas

Descripción

Según diferentes informes de consultoras, se estima que el uso de dispositivos móviles supera en navegación y uso a los ordenadores tradicionales, las comunicaciones, redes sociales, transacciones financieras y los videojuegos hacen de estos dispositivos un objetivo a atacar por parte de los piratas informáticos.

Por otro lado, cada vez salen más casos en los que los espías protegidos por muchos gobiernos utilizan los dispositivos móviles cómo arma y mecanismo de intrusión en empresas y personalidades.

En el curso se pretende dar una visión básica de la seguridad de los distintos dispositivos móviles y de cómo realizar un análisis forense de estos ante un ataque o intrusión.

Temario

1. **Introducción a los dispositivos móviles**
   - Historia y evolución: dispositivos móviles / sistemas operativos / nuevas amenazas en entornos móviles
   - Redes Wifi: GSM / 3G / 4G / Bluetooth / NFC
2. **Arquitectura básica de dispositivos móviles**
   - IOS / Android / Windows phone
3. **Análisis forense**
   - SIM/USIM cards
     - Descripción y arquitectura interna
     - Los datos en las tarjetas SIM / USIM
     - Clonado físico de tarjetas SIM
     - Adquisición de evidencias
   - Dispositivos Windows phone
     - Arquitectura de Windows phone / estructura de: memoria, ficheros / arquitectura interna / sistema de ficheros
     - Recovery
     - Tarjetas SD
     - Adquisición de evidencias / clonado vs ficheros / herramientas de extracción / utilidades comerciales
   - Dispositivos Android
     - Android Internals / sistema de ficheros YAFFS2 / información y configuración del sistema
     - Adquisición de evidencias / análisis de memoria / bloqueo/desbloqueo del dispositivo / logs de Android
     - Análisis forense de aplicaciones
   - Dispositivos IOS
     - Adquisición: desde un backup de iTunes, iCloud; de copia lógica
     - Análisis de la evidencia adquirida
     - Análisis de forense de aplicaciones
     - Análisis con herramientas libres o gratuitas / análisis con herramientas comerciales

PROFESOR

Josep Albors

Taller 12

Introducción al malware

Duración taller: 10 horas

Descripción

El objetivo de este curso es que los alumnos se familiaricen con el análisis de malware a un nivel que les permita analizar malware de forma rápida, centrándonos sobre todo en el análisis dinámico. Se describirán y utilizarán herramientas de forma que los alumnos puedan continuar sus prácticas una vez finalice el curso y puedan así aplicar los conocimientos adquiridos en su día a día.

Temario

1. **Conceptos básicos**
   - Conceptos básicos de seguridad informática
   - Reseña e historia del malware
   - Técnicas de propagación de malware
   - Sistemas operativos y vulnerabilidades
   - Malware en dispositivos móviles
   - Monetización del malware por parte de los cibercriminales
2. **Laboratorio de análisis de malware**
   - ¿Qué es un laboratorio de análisis de malware?
   - Eligiendo entre virtualización y equipos físicos
3. **Análisis de malware**
   - Análisis de malware (1) objetivos (2) tipos: análisis estático y dinámico
   - Herramientas para el análisis de malware
   - Obtención de muestras de malware
   - Técnicas de ofuscación y antidebugging usadas por el malware
   - Códigos maliciosos y sitios Web
4. **Análisis de tráfico de red**
   - Captura y análisis de tráfico de red / Wireshark y T-shark
   - Análisis de direcciones IP y dominios DNS
   - Técnicas de anonimización
5. **Resultados del análisis de malware**
   - Enfoque práctico del análisis de malware y generación de informes
6. **Respuesta a incidentes**
   - Gestión y respuesta a incidentes
   - Continuidad de negocio
7. **Prácticas**