/Rooted

Hacking Ético de Aplicaciones Móviles (Android / iOS)

MADRID

7 al 9 de Marzo de 2022

DOSIER DE FORMACIÓN

/Rooted

Días 7-9 de Marzo

Tres días de trainings y workshops

HOTEL Eurostars iHotel
Pozuelo de Alarcón

Días 10-12 de Marzo

Ponencias presentadas por speakers internacionales y expertos técnicos.

KINEPOLIS
Pozuelo de Alarcón

Presentación

- **Misión**: queremos compartir conocimientos, atraer diferentes culturas, exponer el talento local y marcar la diferencia.
- **Visión**: ser responsables haciendo algo diferente, compartiendo cultura y construyendo una red de conocimiento. Ser un evento honesto, confiable, beneficioso y establecer alianzas y colaboraciones con socios, clientes y competidores.
- **Nuestra cultura ganadora y nuestros valores en vivo:** colaboración, diversidad, talento por todas partes, pasión, calidad y enfoque en los clientes (cada persona que asiste a nuestros congresos).

Objetivos

Este Bootcamp está orientado a la práctica de pentesting y hacking ético de aplicaciones móviles, con él se podrán sentar las bases de los diferentes técnicas de auditoría de aplicaciones móviles que existen, tanto para Android como iOS, así como llevar a cabo estas auditorías haciendo uso de la metodología OWASP Mobile Security Testing Guide y cómo presentar los resultados obtenidos en un informe.

Se ofrecerá un taller práctico en el que los asistentes podrán practicar con aplicaciones preparadas para tal finalidad en un entorno virtual al que se facilitará el acceso (Android / iOS).

A quién va dirigido

El Bootcamp está dirigido a todas aquellas personas que deseen ampliar sus conocimientos en el hacking ético de aplicaciones móviles (Android/iOS):

- Profesionales del sector de la Seguridad de la Información (pentesters, auditores y analistas de seguridad…)
- Estudiantes y docentes
- Desarrolladores
- Fuerzas y Cuerpos de Seguridad
- Cualquier persona interesada en aprender y ampliar conocimientos en las auditorías de seguridad de aplicaciones móviles

Profesores:
Carlos Alberca y Daniel González

Carlos Alberca:

@f00bar_

Graduado en Ingeniería Informática y máster en Ciberseguridad por la Universidad Carlos III de Madrid e investigador en seguridad informática con más de 7 años de experiencia en el sector. Actualmente es el responsable del grupo de auditorías de ciberseguridad de 'Seccion 7' y CISO de 'Ravenloop'. Además, forma parte del programa de recompensas de vulnerabilidades de Google (VRP - Vulnerability Reward Program - Google Bug Hunter Hall of Fame), participando también en otros como, por ejemplo, 'Microsoft Bug Bounty Program'. Previamente trabajó en proyectos de ciberseguridad y ciberdefensa para el Ministerio de Defensa de España, además de haber sido ponente en las jornadas del CCN-CERT.

Daniel González:

@dgc441

Ingeniero en Informática y Máster en Tecnologías de la Seguridad, trabaja en Ravenloop como auditor y consultor de seguridad. Es un apasionado de las TIC en general, más sobre todo en la seguridad que las aplica, temática sobre la cual le encanta investigar y lo que le ha llevado a participar en el programa 'Microsoft Bug Bounty Program' Lleva más de 6 años con experiencia en este sector, trabajando en múltiples proyectos para Ministerio de Defensa. Además ha tenido la posibilidad de ser ponente en otras conferencias, como PyConES y CCN-CERT.

Requisitos: Conocimientos

Los alumnos deben tener un **requisito básico**, que es venir con **ganas de aprender y profundizar en conocimientos de auditoría de seguridad de aplicaciones móviles** (Android / iOS).

Además, se recomienda tener **conocimientos básicos en metodologías de auditoría de seguridad**, sistemas operativos, redes y saber manejarse con fluidez en sistemas Linux/Windows y entornos móviles (Android/iOS).

Los docentes en todo momento darán soporte con explicaciones claras y concisas.

Y muy importante, **muchas ganas de aprender, aportar y pasar un buen rato.**

Requisitos: Técnicos

Para el correcto funcionamiento del training será necesario que los alumnos dispongan de equipos portátiles con acceso de administrador para poder añadir, eliminar software o cambiar cualquier configuración del mismo si fuera necesario.

Las máquinas deben contar con las siguientes características:

- Capacidad de conexión por cable e inalámbrica
- Capacidad de ejecutar máquinas virtuales utilizando Vmware Workstation/Player o VirtualBox.
  - Se recomienda asistir con una máquina virtual instalada Kali Linux o Parrot.
- Las máquinas virtuales deben poder contar con las siguientes características mínimas
  - 4GB de RAM
  - 20GB de disco
  - 2 procesadores

Los asistentes **NO** necesitaran ningún terminal físico Android y/o iOS para este taller ya que se facilitará acceso individual a cada alumno a un entorno virtual y online.

Contenido

A lo largo del desarrollo del Bootcamp se trabajará sobre la metodología OWASP MSTG (Mobile Security Testing Guide) sobre diferentes entornos (Android / iOS).

El contenido de la agenda podría sufrir modificaciones en función de la dinámica del grupo de trabajo, pues se hará hincapié en que todos los asistentes entiendan correctamente el contenido.

El contenido puede estar sujeto a cambios, los cuales se podrán realizar en cualquier momento entre el registro y el comienzo del Bootcamp.

Agenda (i)

- Introducción
- Conceptos generales de auditoría de seguridad en entornos móviles
- Taxonomía de las aplicaciones móviles
- Metodología de auditoría (OWASP Mobile Security Testing Guide)
- Preparación y configuración del entorno de auditoría (Android / iOS)

Agenda (ii)

Auditoría de seguridad sobre entorno Android:

- Android - Arquitectura
- Android - Análisis estático (SAST)
- Android - Análisis dinámico (DAST)
- Android - Análisis y pruebas de:
  - Almacenamiento y tratamiento de datos (en reposo y en tránsito)
  - Criptografía
  - Red
  - Tipos de autenticación
  - Ingeniería inversa

*Los conocimientos serán puestos en práctica mediante aplicaciones (Apps) demo.

Agenda (iii)

Auditoría de seguridad sobre entorno iOS:

- iOS - Arquitectura
- iOS - Análisis estático (SAST)
- iOS - Análisis dinámico (DAST)
- iOS - Análisis y pruebas de:
  - Almacenamiento y tratamiento de datos (en reposo y en tránsito)
  - Criptografía
  - Red
  - Tipos de autenticación
  - Ingeniería inversa

*Los conocimientos serán puestos en práctica mediante aplicaciones (Apps) demo.

Costes

- El precio final de este **Bootcamp + entrada** al Congreso RootedCON es **1250 €**

- **Puedes registrarte y formalizar el pago en: https://reg.rootedcon.com**

IMPORTANTE:

Se requiere un mínimo de **CINCO (5)** asistentes para que el curso pueda celebrarse.

/Rooted

FAQ

- Dónde se celebra la formación?
  - A diferencia del Congreso RootedCON, las formaciones se celebran en el Hotel Eurostarts i-Hotel
  - Aquí puedes encontrar el mapa de la zona: Google Maps
- Qué diferencia hay entre BootCamp y RootedLab?
  - Diferenciamos los training por horas de formación. Un RootedLab tiene 8 horas de formación, mientras que un BootCamp tiene unas 24h.
- Qué horario tiene la formación?
  - La formación comienza a las 9 de la mañana, pero procura estar un poco antes para poder acreditarte y tener tu portátil preparado. El primer día recomendamos estar a las 8 :)
  - Las formaciones suelen acabar entre las 19h y 20h.
- Como puedo registrarme?
  - Para el registro, ve directamente al RootedManager: https://reg.rootedcon.com. Ahí, una vez registrado podrás seleccionar la formación y pagar directamente. Una vez se imparta la formación podrás solicitar la factura siguiendo los pasos indicados.
- Puedo pagar con transferencia bancaria?
  - Si, desde el propio RootedManager podrás gestionar el pago mediante transferencia bancaria.
- El training incluye comida?
  - Los training no incluyen comida. Pero hay varias opciones en la zona, y el profesor os dará más información.

/Rooted

Contacto:

info@rootedcon.com