

/Rooted®



Frida & Mobile Pentesting

MADRID

4 de Marzo 2024

DOSIER DE FORMACIÓN

/Rooted[®]

Días 4-6 de Marzo

Tres días de trainings y workshops

*HOTEL Eurostars iHotel
Pozuelo de Alarcón*

Días 7-9 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).

Profesor: Pablo San Emeterio

Pablo es un reconocido profesional del sector de la ciberseguridad, posee un Máster en Auditoria y Seguridad Informática por la Universidad Politécnica de Madrid y es Ingeniero en Informática por la Universidad Politécnica de Madrid. Es profesor en el Master de Ciberseguridad de la UCAM donde imparte las asignaturas de Vulnerabilidades y Análisis de Malware.

Lleva trabajando más de 20 años en el sector y es fundador de la compañía de ciberseguridad VAPASEC. Anteriormente trabajo para empresas del sector de la ciberseguridad como son Telefónica y Optenet.

Pablo es ponente habitual en congresos y conferencias de ciberseguridad como son RootedCON, No cON Name, ConectaCON, Cybercamp, Jornadas STIC, Navaja Negra, ViCON e internacionales como BlackHat o ShmooCon.

Objetivos

El principal objetivo de este training es conocer las enormes posibilidades que ofrece Frida en el mundo de la ciberseguridad. La instrumentación dinámica de aplicaciones se utiliza tradicionalmente para analizar el rendimiento de aplicaciones o depurar programas, pero grandes aplicaciones, desde el punto de vista defensivo como desde el punto de vista ofensivo.

Frida se puede emplear como herramienta para llevar a cabo auditorias de aplicaciones móviles, como herramienta de análisis de código o como herramienta para corregir aplicaciones de las que no disponemos de su código.

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

Requisitos: Conocimientos

Conocimientos básicos de:

- ✓ Sistemas operativos
- ✓ Comunicaciones
- ✓ Auditoría

Requisitos: Técnicos

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

Las máquinas deben contar con las siguientes características mínimas:

- 8 GB de memoria RAM
- 40 GB de espacio en disco
- Tener instalado Android Studio
- Tener instalado VirtualBox o VMWare

Agenda (i)

Introducción a Frida.

- Que es Frida
- Donde se puede utilizar Frida
- Como instalar Frida
- Primeros ejemplos con Frida

Agenda (ii)

Frida en Android

- Creando un entorno de trabajo
- Root & Google Services en AVD
- Analizando las comunicaciones de un APK
- Eludiendo detección de root
- Analizando aplicaciones en Flutter

Agenda (iii)

Linux o Windows.

- Tracear binarios
- Hookeando funciones en Linux o Windows
- Modificando el log de un programa
- Resolución automática de crackme's
- Otros usos

Costes

- El precio final de este RootedLAB es **250 €**
- Puedes registrarte y formalizar el pago en: <https://reg.rootedcon.com>

IMPORTANTE:

Se requiere un mínimo de **SEIS (6)** asistentes para que el curso pueda celebrarse.

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): <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®

