Hooking RootedLAB

/RootedCON 2017

/Rooted

Objetivos

En este *training*, orientado a la práctica del *hooking*, podrás introducirte y sentar bases en las distintas técnicas que se utilizan para modificar el comportamiento de aplicaciones y sistemas operativos mediante la interceptación de mensajes, llamadas a función y eventos.

El alumno obtendrá una visión global, mediante una aproximación eminentemente práctica, de las distintas técnicas que permiten manipular el comportamiento de aplicaciones y del sistema operativo de un equipo sin tener acceso al código fuente de los mismos.

Las técnicas de *hooking* son utilizadas ampliamente tanto por herramientas de seguridad, para monitorizar determinadas partes del sistema operativo y aplicar protecciones sobre el mismo, como por el malware para poder ocultarse en el sistema operativo o modificar el comportamiento de aplicaciones en su beneficio.

A quién va dirigido

Profesionales del sector de la Seguridad de la Información

Estudiantes

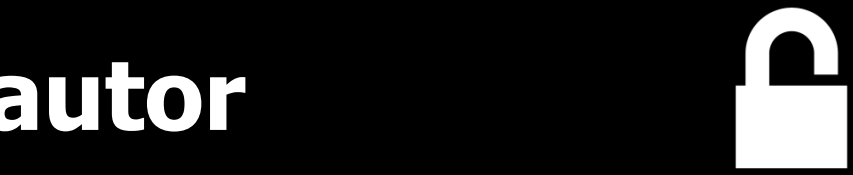
Administradores de sistemas y redes

Desarrolladores que quieran mejorar su perfil

Cuerpos y Fuerzas de Seguridad

Docentes

Sobre el autor



Pablo San Emeterio

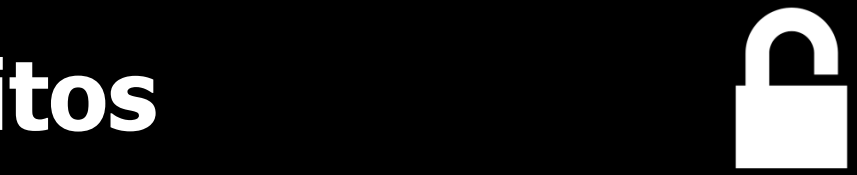
Máster en Auditoria y Seguridad Informática por la Universidad Politécnica de Madrid. Ingeniero en Informática por la Universidad Politécnica de Madrid.

Trabaja en Telefónica España donde ha desarrollado diferentes funciones como Product Manager del Servicio AntiFraude o CSA. Es docente en la iniciativa HackMeets con presentaciones y talleres sobre distintas temáticas de seguridad, destacando exploiting o seguridad en redes WiFi. Ha trabajado durante más de 12 años en diversas compañías del sector de las Tecnologías de la Información de los cuales los últimos 9 ha trabajado en el sector de la seguridad informática. Durante estos 9 años trabajó en el departamento de I+D de Optenet, empresa española centrada en la seguridad en redes de comunicaciones.

Ha publicado artículos en blogs de seguridad como Security By Default o Seguridad Ofensiva, y colabora activamente con distintos medios de comunicación.

Pablo ha sido ponente en Rooted CON 2012, 2014 y 2016 además de en otros congresos nacionales como No cON Name, ConectaCON, Cybercamp, STIC e internacionales como BlackHat o ShmooCon.

Requisitos



Conocimientos y aptitudes

Conocimientos básicos de:

- Sistemas operativos
- Experiencia en programación

*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:
  - 4 GB de memoria RAM
  - 30 GB de espacio en disco
  - Tener instalado VirtualBox

Contenido

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.

Hooking techniques lab

Introducción:

- ¿Que es el hooking?
- Mensajes, APIs, eventos
- Windows vs Linux
- Herramientas y frameworks disponibles

Hooking techniques lab

Userland:

- Hook de mensajes
  - Key and mouse logger
- Técnicas de inyección de código
- Formato PE
- IAT, EAT, Delay Load Hooking
- Inline Hooking
- Parcheo de binarios

Hooking techniques lab

Kernelland:

- Pros & Cons
- Event callbacks
- API hooks
- Filter drivers
- Interrupciones

Costes

Coste

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

Contact

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

/Rooted®

Muchas gracias