# Introducción explotación de vulnerabilidades

/RootedCON Valencia 2019

/Rooted®

# Objetivos

Este training está orientado a iniciar a los asistentes en el fascinante mundo del exploiting. A lo largo de este training se introducirá a los alumnos en algunas de las técnicas utilizadas en la explotación de vulnerabilidades de aplicaciones. Además se trabajará en sentar bases teóricas sobre las que se sostiene el desarrollo de exploits.

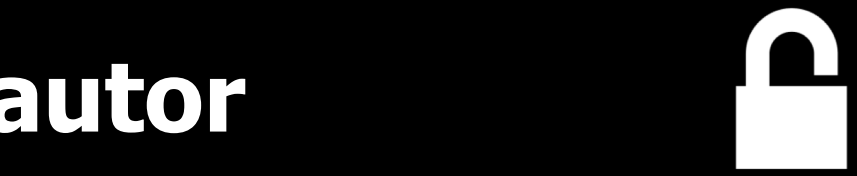
En el curso se programarán varios exploits en Windows de 32 bits.

A lo largo del curso también se explicaran algunas de las medidas de protección que se han sido añadidas por los sistemas operativos para mitigar la explotación de vulnerabilidades y como pueden ser evadidas.

# A quién va dirigido

- Profesionales del sector de la Seguridad de la Información como son pentesters, auditores, analistas de malware
- Estudiantes
- Administradores de sistemas y/o redes
- Desarrolladores
- Cuerpos y Fuerzas de Seguridad
- Docentes
- Cualquiera que este interesado en aprender y profundizar en el desarrollo de exploits

# Sobre el autor



/Rooted®

# Pablo San Emeterio

Es Máster en Auditoria y Seguridad Informática por la Universidad Politécnica de Madrid e Ingeniero en Informática por la Universidad Politécnica de Madrid, es un apasionado de las Tecnologías de la Información en general y de la Seguridad Informática en particular, temática sobre la cual le encanta investigar sus distintas áreas y probar o programar herramientas. Esto le ha llevado a publicar artículos en blogs de seguridad como Security By Default o Seguridad Ofensiva y a colaborar activamente con distintos medios de comunicación.

Ha trabajado durante más de 18 años en diversas compañías del sector de las Tecnologías de la Información y más de 10 años en empresas del sector de la seguridad de la información, en puestos relacionados con el desarrollo de software, administración de bases de datos, relaciones con clientes o investigación. Actualmente trabaja en ElevenPaths con un doble rol, en el primero es CSA (Chief Security Ambasador) de España, participando en diversos congresos y conferencias a nivel nacional. En el segundo rol es miembro del Lab de innovación de ElevenPaths con la función de Analista de Innovación, trabajando en la investigación y desarrollo de soluciones de seguridad.

Además es una persona a la que le gusta afrontar nuevos retos lo cual le ha llevado a ser profesor del Master en Ciberseguridad de la UCAM, del Máster en Ciberseguridad y Seguridad de la Información de la Universidad de Castilla La Mancha, del Programa Superior en Ciberseguridad y Compliance de ICEMD .

Pablo ha sido ponente en Rooted CON 2012, 2014, 2016 y 2017 además de en otros congresos nacionales como No cON Name, ConectaCON, Cybercamp, STIC e internacionales como BlackHat o ShmooCon.

# Requisitos

/Rooted®

# Conocimientos y aptitudes

Sobre todo, **tener muchas ganas de aprender** y pasar un buen rato explotando vulnerabilidades.

Conocimientos básicos de:

- Algo de experiencia en programación en Python
- Sistemas operativos
- Conocer herramientas de ingeniería inversa. No es necesario conocer ensamblador o ser un gran *reverser.*

# Requisitos técnicos

- Para el correcto funcionamiento del Bootcamp 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.
  - La maquina de ser capaz de ejecutar **dos maquinas virtuales de forma simultánea**, para ello se estima que las siguientes características son las **mínimas**
  - CPU DualCore
  - 4 GB de memoria RAM
  - Espacio en disco suficiente como para crear hasta 4 máquinas virtuales.
  - Tener instalado VirtualBox o VMWare

# Contenido

/Rooted®

# Introducción

Durante el Bootcamp 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 en su totalidad haya cumplido con los objetivos de cada uno de los puntos. Se procurará cubrir todo el contenido del curso, pero al depender del tiempo que necesite el grupo para resolver cada ejercicio no se puede garantizar que se cubran todos los puntos del temario
- El contenido del curso puede estar sujeto a cambios sin previo aviso y se podrán hacer estos cambios en cualquier momento entre el registro y el comienzo del mismo.

# 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.

## Agenda

Introducción:

- Repaso de arquitectura de computadores
- X86
- Introducción al ensamblador
- Memoria en un proceso

## Agenda

Win 32 bits:

- Stack Buffer Overflow
- Detección de bad characters
- Medidas de mitigación 1 (stack cookies)
- Bypass stack coockies
- Medidas de mitigación 2 (DEP, ASLR)

# Costes

/Rooted®

# Coste

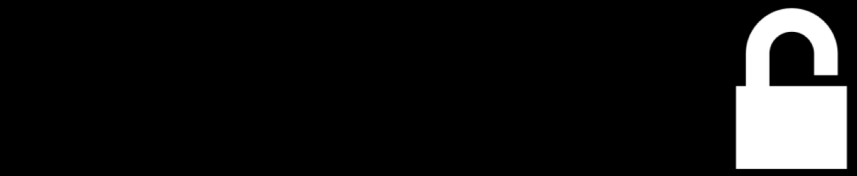
- El coste del curso es de 100€

- **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:** | **#rootedvlc #rootedvlc2019** |
| ***Pablo's twitter:*** | @psaneme |
| ***Facebook, LinkedIn:*** | *Rooted CON* |
| ***Twitter:*** | *@rootedcon*<br>*Tags:*<br>*#rooted2019 #rootedcon #rootedvlc* |
| | |

/Rooted®



Muchas gracias