Introducción **al Exploiting: RootedLAB**

/RootedCON Valencia 2017

/Rooted®

Objetivos

En este *training*, 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 tanto en Windows como en Linux de 32 bits para poder ver las diferencias y las similitudes en la explotación de vulnerabilidades de ambos sistemas operativos.

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

Estudiantes

Administradores de sistemas y redes

Desarrolladores que quieran mejorar su perfil

Cuerpos y Fuerzas de Seguridad

Docentes

Sobre el autor

Pablo San Emeterio

/Rooted

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

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 docente en la iniciativa HackMeets con presentaciones y talleres sobre distintas temáticas de seguridad, destacando exploiting o seguridad en redes WiFi. También es profesor del *Título Propio de Especialista en Seguridad Informática y de la Información* de la Universidad de Castilla La Mancha y del Master en Ciberseguridad de la UCAM. Ha trabajado durante más de 10 años en diversas compañías del sector de las Tecnologías de la Información. Ha publicado artículos en blogs de seguridad como Security By Default o Seguridad Ofensiva.

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

Conocimientos y aptitudes

Conocimientos básicos de:

- Sistemas operativos
- Conocer herramientas de ingeniería inversa.
- Experiencia en programación en Python

*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 mínimas.

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

  - La maquina de ser capaz de ejecutar dos maquinas virtuales de forma simultánea

/Rooted®

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.

Exploiting techniques lab

Introducción:

- Repaso de arquitectura de computadores
- Introducción a sistemas operativos
- Repaso X86

Introducción al exploiting lab

Win 32 bits:

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

Introducción al exploiting lab

Linux 32 bits:

- Stack Buffer Overflow
- Format String Bugs

/Rooted®

Costes

Coste

- El coste del curso es de 80€
- **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:	**#RVLC**
Pablo's twitter:	@psaneme
Facebook, LinkedIn:	*Rooted CON*
Twitter:	*@rootedcon* *Tags:* *#rooted y #RootedVLC*

/Rooted®

Muchas gracias