/Rooted

Exploiting

Pablo San Emeterio

MÁLAGA

10 de Diciembre de 2021

DOSSIER DE FORMACIÓN

/Rooted

Día 10 de Diciembre de 2021

Ponencias presentadas por speakers internacionales y expertos técnicos.

E.T.S. de Ingeniería Informática de Málaga
Bulevar Louis Pasteur, 35.
Campus de Teatinos. 29071 Málaga

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 training está orientado a dar a los asistentes una visión práctica del fascinante mundo del **exploiting**. Los asistentes a este training podrán disfrutar la experiencia única que se siente cuando se desarrolla y ejecuta su propio exploit contra un programa vulnerable. A lo largo de este training los alumnos practicarán distintas técnicas empleadas en la explotación de vulnerabilidades junto con la comprensión de las bases teóricas sobre las que se asienta el desarrollo de exploits.

Durante el curso los asistentes podrán migrar los exploits desarrollados a uno de los frameworks más utilizados en exploiting como es metasploit. También se abordará como adaptar y modificar los exploits de metasploit para ser utilizados contra nuevos objetivos.

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 o b*ypasseadas*.

Además los asistentes entrarán a practicar cómo se pueden emplear Frida y otras herramientas para trabajar en la búsqueda de fallos en un programa.

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.

Profesor: 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.

Ha trabajado durante más de 20 años en diversas compañías del sector de las Tecnologías de la Información y más de 14 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.

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 y en el Master en Ciberseguridad de IEBS. También ha sido formador en Labs y Bootcamps de impartidos en distintos congresos de seguridad informática y compañías.

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.

También colabora todos los lunes en el espacio de Ciberseguridad del programa Afterwork de Capital Radio, donde se tratan temas de actualidad del mundo de la ciberseguridad y se difunde la cultura de ciberseguridad en la sociedad.

Requisitos: Conocimientos

El principal requisito que deben tener los alumnos es venir con **muchas ganas de aprender y pasar un buen rato** explotando vulnerabilidades.

Conocimientos **básicos** de:

- Programación en Python.
- Sistemas operativos.

Requisitos: Técnicos

Para el correcto funcionamiento del Lab 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 Dual Core.
- 4 GB de memoria RAM.
- Espacio en disco suficiente como para crear hasta 4 máquinas virtuales.
- Tener instalado VirtualBox o VMWare.

Contenido

El training transcurría durante 1 día.

- Se realizará una pausa corta a media mañana y otra pausa para comer.
- La comida corre a cargo de cada uno de los asistentes.

Agenda (i)

Introducción

- Tipos de fallos.
- Arquitectura de computadores.
- X86.
- Gestión de memoria de un proceso.

Agenda (ii)

Binary exploiting

- Stack Buffer Overflow.
- Explotación en buffers restringidos.
- Migración y adaptación de exploits en Metasploit.
- Medidas de mitigación y *bypasses.*

Agenda (iii)

Busqueda de Bugs

- Banned functions.
- Análisis estático.
- Análisis dinámico.
- Fuzzing con Frida y otras herramientas.

Costes

- El precio final del Lab será de 149,90€.

IMPORTANTE: Se requiere un mínimo de **DOCE (12)** asistentes para que el Lab pueda llevarse a cabo.

FAQ

- Dónde se celebra la formación?
  - Las formaciones se celebran en la E.T.S. de Ingeniería Informática de Málaga Bulevar Louis Pasteur, 35. Campus de Teatinos. 29071 Málaga.
- Qué horario tiene la formación?
  - La formación comienza a las 9:00de la mañana, pero procura estar un poco antes para poder acreditarte y tener tu portátil preparado.
  - Las formaciones acaban a las 18:00h
- Como puedo registrarme?
  - Para el registro, ve directamente al RootedManager. 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 en el Portal.
- 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