/Rooted

Exploit Development for Pentesters

Pablo San Emeterio

MADRID

7 al 9 de Marzo de 2022

DOSSIER DE FORMACIÓN

/Rooted

Días 7-9 de Marzo

Tres días de trainings y workshops

HOTEL Eurostars iHotel
Pozuelo de Alarcón

Días 10-12 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).

Objetivos

El Bootcamp Exploit Development for Pentesters, esta orientado a que los asistentes se introduzcan y profundicen sus conocimientos en el desarrollo de exploits, de forma que puedan utilizar estos conocimientos en sus actividades diarias. Durante el Bootcamp los asistentes trabajarán de manera teórica y práctica distintas técnicas utilizadas en la explotación de vulnerabilidades de aplicaciones. Durante la mayor parte del tiempo, los asistentes al Bootcamp estarán trabajando de forma práctica, explotando vulnerabilidades sobre aplicaciones reales y afrontando los retos que supone lograr la ejecución de código arbitraria sobre las mismas.

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 Bootcamp también se abordan las distintas medidas de protección que han sido añadidas por los sistemas operativos para mitigar la explotación de vulnerabilidades a lo largo del tiempo y se trabajarán las técnicas que permiten evadir dichas protecciones para lograr la explotación en sistemas modernos

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

Objetivos

Al finalizar este Bootcamp los asistentes adquirirán una serie de conocimientos que le resultarán muy útiles a la hora de realizar las tareas habituales en auditorias de seguridad, tests de intrusión o Red Team. Dispondrá de los conocimientos necesarios para:

- Desarrollar *exploits* en sistemas operativos Windows y Linux
- Crear *exploits* para aplicaciones que no disponen de un *exploit* público.
- Modificar los *exploits* conocidos para evitar ser detectados o añadirles funcionalidad para eludir las medidas de mitigación contra la ejecución de código
- Crear o adaptar *exploits* en Metasploit
- Utilizar eficazmente varios *debuggers* y herramientas para mejorar la investigación y el desarrollo de exploits

A quién va dirigido

El Bootcamp *Exploit Development for Pentesters* esta dirigido a todas aquellas personas que deseen ampliar sus conocimientos en la explotación de vulnerabilidades y el desarrollo de explotis

- Pentesters
- Analistas de malware
- Arquitectos y Analistas de seguridad
- Adminstradores de sistemas
- Cuerpos y Fuerzas de Seguridad el Estado
- Estudiantes y Docentes
- Cualquier persona con ganas de aprender a desarrollar exploits, shellcodes e integrarlos con Meterpreter

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 3 días a tope** explotando vulnerabilidades.

Conocimientos **básicos** de:

- Programación en Python
- Sistemas operativos
- Haber utilizado maquinas virtuales (VMWare o VBox)
- No es necesario tener unos profundos conocimientos de lenguaje ensamblador

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

Durante el Bootcamp se trabajará sobre una misma metodología pero con diferentes entornos de trabajo.

- Los puntos de la agenda 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 (i) - Introducción

[Teoría] Durante este primer módulo se llevará a cabo una introducción a los conocimientos teóricos necesarios para el desarrollo del Bootcamp. Se tratarán temas como:

- Arquitectura de computadores
- X86 y X86-64
- La memoria de un proceso
- Herramientas y utilidades que se emplearán durante el curso
- Desensambladores, Debuggers y Decompiladores

Agenda (ii) – Smashing the stack

En este módulo vamos a trabajar distintas formas de explotar un Stack buffer Overflow en varios sistemas operativos:

- [Prac] SBO Windows X86
- [Prac] SBO Linux X86
- [Prac] Detección de Bad Caracters
- [Prac] Explotación en buffers restringidos
- [Prac] Portar y adaptar exploits a Metasploit
- [Prac] Windows SEH
- [Prac] SBO Windows X86-64
- [Prac] SBO Linux X86-64

Agenda (iii) – Análisis de bugs

Bugs:

- [Teoria] Banned funcions / Funciones prohibidas
- [Practica] Análisis estático
- [Practica] Análisis dinámico
- [Practica] Fuzzing
- [Practica] Execution trace

/Rooted

Agenda (iv) – Advanced Exploiting

Bypass exploit mitagations:

- [Teoria] DEP y NX
- [Teoría] Return Oriented Programing
- [Practica] Bypass Windows DEP
- [Practica] Bypass Linux NX usando Return to libc
- [Practica] Bypass Linux NX usando ROP
- [Teoría] ASLR
- [Practica] Bypass Windows ASLR

Agenda (v) - Browsers

Durante mucho tiempo estos fallos han sido la principal vía de ataque contra empresas y particulares. Estas vulnerabilidades se deben principalmente, a la complejidad que supone la gestión de memoria en aplicaciones de gran tamaño. En este módulo vamos a trabajar la explotación de navegadores:

- [Teoría] vftable/vtable en C++
- [Prac] Heap Spray
- [Prac] Use-After-Free
- [Prac] UAF + ASLR bypass + DEP bypass

Costes

- El precio final de este **Bootcamp + entrada** al Congreso RootedCON es **1250€**

- **Puedes registrarte y formalizar el pago en: https://reg.rootedcon.com**

IMPORTANTE:

Se requiere un mínimo de **CINCO (5)** 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. 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

Contacto: info@rootedcon.com