/Rooted

Exploit Development for Pentesters

Pablo San Emeterio

MADRID

2 al 4 de Marzo de 2020

DOSSIER DE FORMACIÓN

/Rooted

Días 2-4 de Marzo

Tres días de trainings y workshops

HOTEL Eurostars iHotel
Pozuelo de Alarcón

Días 5-7 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 amplíen sus conocimientos en el desarrollo efectivo de exploits, de forma que puedan utilizar estos conocimientos en sus actividades diarias. Durante el Bootcamp los asistentes trabajarán de manera teórica y práctica las distintas técnicas utilizadas en la explotación de vulnerabilidades de aplicaciones. Durante la mayor parte del tiempo, los asistentes al Bootcamp estarán trabajando de forma eminentemente práctica, explotando vulnerabilidades sobre aplicaciones reales y afrontando los retos que supone lograr la ejecución de código arbitraria sobre las mismas.

Durante el desarrollo del Bootcamp los asistentes recibirán varias máquinas virtuales sobre las que realizar los distintos ejercicios que se propondrán. Durante los tres días que dura el Bootcamp se programarán exploits y shellcodes sobre aplicaciones en sistemas operativos Windows y Linux, lo que nos permitirá conocer las similitudes y diferencias a la hora de lograr ejecutar código en ambos sistemas operativos.

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

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:

- Programar *exploits* en sistemas operativos Windows y Linux
- Programar *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
- Utilizar eficazmente varios *debuggers* y *plug-ins* 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

Pablo tiene Máster en Auditoria y Seguridad Informática por la Universidad Politécnica de Madrid y es 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 impartir ponencias y publicar artículos en blogs de seguridad como Security By Default o Seguridad Ofensiva y a colaborar activamente con distintos medios de comunicación. 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.

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 .

Requisitos: Conocimientos

Muchas ganas de aprender, de pasar 3 días a tope desarrollando exploits sobre aplicaciones reales y de lograr superar los retos que supone desarrollar un exploit para una aplicación y eludir las medidas de prevención de ejecución de exploits añadidas por los sistemas operativos.

Tener alguna experiencia en programación en C y Python

No es necesario tener unos profundos conocimientos de lenguaje ensamblador

Estar familiarizado con el uso de tecnologías de virtualización como VirtualBox o VMWare

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

Durante este primer módulo se llevará a cabo una introducción a los conocimientos teóricos necesarios para el desarrollo del Bootcamp. También presentarán las herramientas con las que se trabajará durante el desarrollo del mismo. Se tratarán temas como:

- Arquitectura de computadores
- Lenguaje ensamblador X86
- Zonas de memoria de un proceso
- Herramientas y utilidades que se emplearán durante el curso

Agenda (ii) - Linux

En este módulo el asistente comenzará a explotar vulnerabilidades en sistemas Linux. Durante este módulo se irán abordando las vulnerabilidades de forma progresiva, desde las más sencillas hasta llegar a las más complejas. Los puntos destacados a tratar durante este módulo son:

- Stack buffer overflow
- Function pointer overwrite
- Heap buffer overflow
- Explotación de format string
- Medidas de protección contra la ejecución de código
- Sortear con éxito las medidas de protección

Agenda (iii) - Windows

Después de explotar vulnerabilidades en sistemas Linux, este módulo introduce al asistente en la explotación de vulnerabilidades en sistemas Windows. Las primeras vulnerabilidades que el asistente al Bootcamp tendrá que afrontar tienen una base teórica común con las vulnerabilidades en sistemas Linux. Los asistentes pronto podrán ver que existen matices y técnicas que lo hacen diferente. Los puntos destacados a tratar en este modulo son:

- Stack buffer overflow
- Detección de bad caracters
- Explotación del SEH
- Medidas de mitigación contra la ejecución de código
- Sortear con éxito las medidas de mitigación contra la ejecución de código
- Portar exploits a Metasploit

Agenda (iv) - Navegadores

En este último módulo el asistente afrontará el reto de explotar vulnerabilidades en los navegadores. Durante mucho tiempo estos fallos han sido la principal vía de ataque contra empresas y particulares. Use after free (UAF) o Type Confusion son algunos de fallos de corrupción de memoria que se han utilizado para explotar los navegadores. Estas vulnerabilidades se deben principalmente, a la complejidad que supone la gestión de memoria en aplicaciones de gran tamaño desarrolladas en C++. Este módulo supone un cambio frente a las vulnerabilidades tratadas anteriormente. Algunos puntos destacados son:

- Comprender el funcionamiento de las vftable/vtable en C++
- Heap Spray
- Use-After-Free
- Como sobrepasar DEP y ASLR

Costes

- El precio final del Bootcamp + entrada al Congreso RootedCON es 1200 €

- Cuando se abra el registro para las entradas al Congreso, se te enviará un código para canjear tu entrada.

IMPORTANTE: Se requiere un mínimo de DIEZ (10) asistentes para que el curso pueda llevarse a cabo.

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. 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.
- Puedo pagar con transferencia bancaria?
  - Si, desde el propio RootedManager podrás gestionar el pago mediante transferencia bancaria.
- El training incluye comida?
  - Los trainings no incluyen comida. Pero hay varias opciones en la zona, y el profesor os dará más información.

/Rooted

Contacto: info@rootedcon.com