Exploiting Bootcamp:

/RootedCON Madrid 2018

/Rooted

Objetivos

En este *BootCamp*, orientado a que los asistentes se introduzcan en el fascinante mundo del *exploiting* o amplíen sus conocimientos. Durante *Bootcamp* se presentaran distintas técnicas y trucos utilizadas en la explotación de vulnerabilidades de aplicaciones. Se trabajará de forma eminentemente práctica ya que bajo mi punto de vista y mi propia experiencia es la mejor forma de sentar bases teóricas sobre las que se sostiene el desarrollo de exploits.

Durante los tres días que dura el BootCamp se programarán exploits tanto en Windows como en Linux de 32 bits lo que nos permitirá conocer las similitudes y diferencias en la explotación de vulnerabilidades de ambos sistemas operativos.

A lo largo del curso también se explicaran 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 o profundizar el desarrollo y comprensión de exploits

Sobre el autor

Pablo San Emeterio

/Rooted

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 14 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 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.

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

Conocimientos básicos de:

- Experiencia en programación y lectura de códigos sencillos en Python y C
- Conocer herramientas de ingeniería inversa.
- No es necesario conocer ensamblador o ser un gran *reverser*, pero tener algún conocimiento básico de ensamblador será de gran ayuda

Estar familiarizado con:

- Metasploit
- Manejo de herramientas de virtualización VirtualBox o VMWare y sistemas operativos Windows y Linux

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

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
  - Capacidad de CPU como para tener ejecutando simultáneamente dos maquinas virtuales
  - 4 GB de memoria RAM
  - Espacio en disco suficiente como para crear hasta 4 máquinas virtuales.
  - Tener instalado VirtualBox o VMWare

/Rootəd

Contenido

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 **3 días.**
- 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
- SEH
- Medidas de mitigación 2 (DEP, ASLR)

Agenda

Linux 32 bits:

- Stack Buffer Overflow
- Format String Bugs
- Heap Buffer Overflow

Agenda

Win 32 bits:

- Bypass DEP
- Bypass ASLR

Escribir o portar exploits a Metasploit

Explotación de navegadores

/Rooted

Costes

Coste

- El coste del curso es de 1100€
- Si te has registrado en RootedCON, el precio es de 990€
- **IMPORTANTE**: se requiere un mínimo de seis (6) asistentes para que el curso tenga lugar.

Contact

General information:	info@rootedcon.com
Registration form:	
https://reg.rootedcon.es/training/.../	
Hashtag:	**#rooted2018**
Pablo's twitter:	@psaneme
Facebook, LinkedIn:	*Rooted CON*
Twitter:	*@rootedcon* *Tags:* *#rooted2018 #rootedcon*

/Rooted®

Muchas gracias