/Rooted

FRIDA.

Pablo San Emeterio

Valencia 2022

DOSSIER DE FORMACIÓN

/Rooted

Valencia 2022

Ponencias presentadas por speakers internacionales y expertos técnicos.

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 iniciar a los asistentes en FRIDA, un framework de instrumentación dinámica prodigioso que todo desarrollador, amante de la ingeniería inversa o analista de seguridad debería conocer y tener entre sus herramientas.

A lo largo de este training se presentaran las capacidades de FRIDA y se explorará mediante casos prácticos los múltiples usos que se le puede dar a este framework, tanto desde el punto de vista defensivo como desde el punto de vista ofensivo.

A quién va dirigido

- Profesionales del sector de la Seguridad de la Información como pueden ser:
  - Pentesters
  - Auditores
  - Analistas de malware & inteligencia
  - Analisistas de seguridad
- Estudiantes
- Administradores de sistemas y/o redes
- Desarrolladores
- Cuerpos y Fuerzas de Seguridad
- Docentes

Profesor: Pablo San Emeterio

Es Máster en Auditoria y Seguridad Informática por la Universidad Politécnica de Madrid e Ingeniero en Informática por la misma Universidad, 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 programar herramientas. Esto le ha llevado a publicar artículos en distintos blogs de seguridad como Security By Default, Seguridad Ofensiva o en su propio blog psaneme.com y a colaborar activamente con distintos medios de comunicación, entre los que destaca Capital Radio donde todos los lunes desde hace 4 años desarrolla junto a Monica Valle y Eduardo Castillo CiberAfterWork.

Ha trabajado durante más de 20 años en diversas compañías del sector de las Tecnologías de la Información y más de 13 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 o del Master en Ciberseguridad de IEBS.

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

Sobre todo, **tener muchas ganas de aprender** y pasar un buen rato utilizando FRIDA.

Conocimientos básicos de:

- Algo de experiencia en programación en Python y Javascript
- Sistemas operativos

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
- Tener instalado VirtualBox o VMWare

Contenido

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

Introducción:

- Que es FRIDA
- Entornos de trabajo
- Instrumentación dinámica y sus usos
- Instalación
- Herramientas & FRIDA Friends
- Spawn vs Attach

Agenda

Comenzando con FRIDA:

- Analizar funciones invocadas por un ejecutable
- Obtener argumentos utilizados por una función
- Analizar resultados de una función
- Modificar argumentos utilizados
- Modificar resultados obtenidos
- Resolución de crackmes

Agenda

Análisis de ejecuciones:

- Stalker
- Extracción de IOCs
- Unpacking

Modificar aplicaciones:

- Objection
- Cifrado de ficheros
- Detección de maquinas virtuales

Costes

- El precio final del Lab será de 125 euros

IMPORTANTE: Se requiere un mínimo de **SEIS (6)** asistentes para que el Lab pueda llevarse a cabo.

FAQ

- Dónde se celebra la formación?
  - A diferencia del Congreso RootedCON, las formaciones se celebran en la ADEIT - Fundación Universidad-Empresa. Dirección: Plaza Virgen de la Paz, 3. Valencia.
- Qué horario tiene la formación?
  - La formación comienza a las 9:00 de la mañana, pero procura estar un poco antes para poder acreditarte y tener tu portátil preparado.
  - 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.
- 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