/Rooted

Offensive Hardware Hacking for noobs

MADRID

7 al 9 de Marzo de 2022

DOSIER 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 objetivo de este bootcamp es que personas sin conocimientos profundos de electrónica, radio o matemáticas puedan adquirir destrezas necesarias para la realización de auditorías de hardware hacking en su variante ofensiva.

Aunque el bootcamp tiene una orientación eminentemente práctica —con ejercicios guiados por los profesores— otro de sus objetivos será la transmisión de las intuiciones teóricas detrás de cada nuevo concepto, dotando al alumno de la autonomía necesaria para aplicar estas destrezas a escenarios alternativos.

A quién va dirigido

- Profesionales de la informática
- Profesionales de la ciberseguridad
- Autodidactas y hackers sin afiliación

Profesor: David Reguera Garcia

- Profesional seguridad informática +15 años
- Senior malware researcher, AV & EDR dev, reversing, OS Internals, C/C++, x86 x64 ASM, forensics, AVR, ARM CORTEX
- Contributing to:
  - x64dbg
  - Rootkit Unhooker
  - DbgChild
  - More info: https://github.com/therealdreg

Profesor: Gonzalo José Carracedo Carballal

Gonzalo José Carracedo Carballal es un profesional de la informática con 7 años de experiencia y actualmente cursa el doctorado en Astrofísica por la Universidad Complutense de Madrid. Anteriormente fue consultor de ciberseguridad (y más tarde, responsable de Innovación) en la firma española Tarlogic Security. Su experiencia abarca desde el desarrollo de software hasta la ingeniería inversa y hardware hacking (con especial interés en las comunicaciones por radiofrecuencia). Ha impartido charlas y talleres en congresos de ciberseguridad como RootedCON, EkoParty o GSICKMinds. Ocupa su tiempo libre desarrollando SigDigger, una herramienta gráfica de análisis de señales digitales que intenta acercar tanto a aficionados como a profesionales al mundo del SDR.

GitHub: https://github.com/BatchDrake

Sitio web: https://actinid.org

Requisitos: Conocimientos

Conocimientos básicos de:

- ✓ Python 3 (nivel principiante)

Requisitos: Técnicos

Para el correcto funcionamiento del training 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:

- ✓ Ordenador portátil con puertos USB libres y Windows nativo instalado.
- ✓ Máquina virtual con Ubuntu 18.04 o superior

Es deseable que la máquina virtual con Ubuntu disponga de:

- ✓ AppImage de SigDigger (https://github.com/BatchDrake/SigDigger/releases/tag/latest)
- ✓ Gnuradio (https://wiki.gnuradio.org/index.php/UbuntuInstall)
- ✓ Python 3 con los paquetes de pip3: numpy, matplotlib y jupyterlab

Temario

1. **Offensive Hardware & hardware hacking**: USB Attacks, hackrf, proxmark, car hacking, bus pirate, jtagulator, rpk2 evil mass storage...
2. **Electronica básica y práctica** (ICSP, JTAG...)
3. Práctica soldar SMD con cautin, desoldar con pistola, tips and tricks, PCB hacks, captura de datos UART...
4. Analizador lógico vs osciloscopio y práctica
5. **SPI y práctica:** captura y modificación FLASH
6. **I2C y práctica:** captura y modificación EEPROM
7. Prácticas, demos, CTF...
8. **Señales, ondas de radio y SDR**
   - Herramientas hardware y software
   - Introducción a SDR: las señales (sin matemáticas)
   - Introducción a SDR: propagación de ondas de radio (sin matemáticas)
   - Introducción a SDR: otros conceptos importantes (sin matemáticas)
   - El espectro radioeléctrico: qué puedes y no puedes hacer.
9. **Ingeniería inversa de señales de radio**
   - Modulando señales. Señales en ráfagas.
   - Codificando la información.
   - Workflow y ejercicios prácticos.
10. **Interactuando con dispositivos de RF**
    - Antes de transmitir: cosas a tener en cuenta.
    - Haciendo un ataque de replay y ejercicios prácticos
    - Sintetizando una señal y ejercicios prácticos

Costes

- El precio final de este **Bootcamp + entrada** al Congreso RootedCON es 1500 **€**

- **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