/Rooted

Practical Wireless & Radio Hacking (PWRH)

Raúl Siles

DinoSec

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 curso Practical Wireless & Radio Hacking (PWRH) se impartirá por quinto año consecutivo en RootedCON 2020, actualizado, como resultado de la experiencia profesional, en investigación y en formación adquirida durante años sobre la seguridad de tecnologías inalámbricas más tradicionales como Wi-Fi y Bluetooth, ampliada a nuevas tecnologías, como Bluetooth Low Energy (BLE), y comunicaciones de radio en frecuencias inferiores a 1 GHz (433 MHz, 868 MHz, etc.) y otras frecuencias, tanto estándar como propietarias.

Se trata de un curso eminentemente práctico donde los asistentes podrán conocer, profundizar, analizar la seguridad y aplicar técnicas de investigación y hacking sobre diferentes tecnologías inalámbricas y comunicaciones vía radio, empleando tanto herramientas hardware y software específicas, como soluciones más genéricas basadas en SDR (Software Defined Radio).

El objetivo principal del curso es proporcionar los conocimientos y las capacidades necesarias para evaluar la seguridad “desde el aire” de múltiples dispositivos (portátiles, móviles, Internet de las Cosas – IoT, Internet of Things –, y otros), a través del análisis y la investigación de sus mecanismos de comunicación y protección, centrándose en tecnologías inalámbricas multifrecuencia y comunicaciones de radio: Bluetooth, Bluetooth Low Energy (BLE), Wi-Fi, y frecuencias inferiores a 1 GHz.

A quién va dirigido

Profesionales de seguridad de tecnologías de la información y las comunicaciones, investigadores, pen-testers, auditores, administradores de redes, desarrolladores, analistas, entusiastas de la seguridad y de las tecnologías inalámbricas, apasionados de las nuevas tecnologías, o cualquiera con conocimientos técnicos sólidos y con muchas ganas de aprender.

Si tienes muchas ganas de descubrir que contiene el aire que respiras, absorber conocimientos sobre nuevas tecnologías, cacharrear con múltiples componentes hardware y software, y "sufrir" mientras disfrutas durante interminables horas… **¡este curso es para ti!**

NOTA: La modalidad Bootcamp implica una formación muy intensiva, extendiéndose desde el principio de la mañana hasta la tarde-noche durante bastantes horas al día (se recomienda disponer de bebida y alimentos :-).

Profesor: Raúl Siles

Raúl Siles es fundador y analista de seguridad de DinoSec. Durante casi 20 años ha aplicado su experiencia en la realización de servicios técnicos avanzados de seguridad e innovado soluciones ofensivas y defensivas para organizaciones internacionales de diferentes industrias. A lo largo de su carrera, ha trabajado como experto de seguridad, ingeniero, investigador y pen-tester en Hewlett Packard, como consultor independiente, o en sus propias compañías, Taddong, CriptoCert y DinoSec.

Una de sus pasiones y áreas de especialización, entre otras, son las tecnologías inalámbricas, de las que lleva disfrutando durante más de 15 años.

Raúl es instructor certificado del SANS Institute y ponente habitual en conferencias y eventos de seguridad nacionales e internacionales como RootedCON, Navaja Negra, Black Hat, OWASP, BruCON, etc. Raúl es uno de los pocos profesionales a nivel mundial que ha obtenido la certificación GIAC Security Expert (GSE), es Ingeniero Superior Informático por la UPM (España) y tiene un master en seguridad y comercio electrónico.

DinoSec fue co-fundada en 2008 por Raúl Siles. DinoSec pretende transmitir, a través de sus cursos de formación, el conocimiento y la experiencia adquiridas a lo largo de los años durante la realización de tareas de investigación de seguridad en nuevas tecnologías y de los servicios profesionales que ofrece a sus clientes.

Más información en https://www.dinosec.com (@dinosec) y http://www.raulsiles.com (@raulsiles).

Requisitos: Conocimientos

Conocimientos básicos de tecnologías y protocolos de comunicaciones.

Conocimientos básicos de comunicaciones inalámbricas y radio frecuencia.

Conocimientos básicos de seguridad de la información y comunicaciones, técnicas de ataque y de defensa, sistemas operativos (especialmente Linux), redes, programación, etc.

Requisitos: Técnicos

Para la realización de los ejercicios prácticos cada asistente deberá disponer de un ordenador portátil con las siguientes características:

- Kali Linux instalado nativamente (no pudiéndose hacer uso de una máquina virtual, por los requerimientos de acceso a los puertos USB por parte de los componentes hardware que serán utilizados en el curso).
- Al menos 4 GB de RAM (preferiblemente 8 GB o más).
- Múltiples puertos USB libres (recomendándose disponer alternativamente de un hub USB).
- Acceso completo (sin restricciones) como root en el equipo.

Se recomienda disponer de diferentes dispositivos víctima (móviles, IoT, etc.) con capacidades inalámbricas para su posible análisis y estudio.

NOTA: Se proporcionarán más detalles sobre los prerrequisitos técnicos tras completar el registro, aproximadamente entre una y dos semanas antes de comenzar el curso.

Contenido (i)

PWRH es un curso de nivel intermedio, en el que se comenzará introduciendo el funcionamiento de diferentes tecnologías inalámbricas y de comunicación vía radio, para posteriormente analizar sus mecanismos de seguridad y potenciales debilidades.

Progresivamente, se profundizará en aspectos más avanzados y técnicas de ataque y hacking, basadas en el descubrimiento pasivo y activo de dispositivos, suplantación de dispositivos, la captura e interceptación de tráfico, y la manipulación e inyección de tráfico.

Las técnicas ofensivas se complementarán con recomendaciones defensivas para proteger y aumentar la seguridad de las tecnologías inalámbricas y comunicaciones de radio bajo estudio.

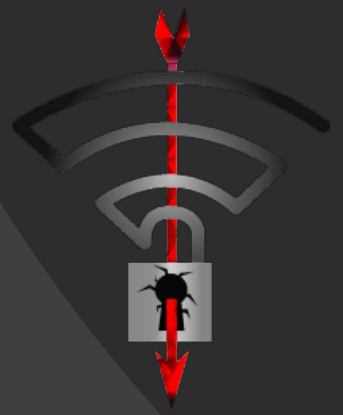
Se intentará ajustar el curso lo más posible a los contenidos descritos, aunque la cantidad de contenidos a cubrir y la profundidad de los mismos se verán influenciados por los intereses de los asistentes y por la dinámica y fluidez de la clase y de los ejercicios prácticos.

NOTA: El contenido del curso es actualizado constantemente, por lo que puede variar ligeramente sin notificación previa entre el momento del registro y la impartición del mismo.

Contenido (ii)

En este 5º aniversario se incluyen nuevos contenidos actualizados sobre Wi-Fi WPA 3, Bluetooth, BLE y radio, ataques relevantes publicados en los últimos años y ataques recientes sobre estas tecnologías, nuevas herramientas y nuevos retos en la parte de ejercicios prácticos.

- Bluetooth (BlueBorne)
- Wi-Fi (KRACK Attacks y PMKID)
- HackRF (Sweep mode)
- OperaCake
- WPA3 (Dragonblood)
- Bluetooth (KNOB)…
- etc.



Agenda: Planificación

El curso se impartirá durante tres días intensos, previos a la conferencia RootedCON 2020.

Fechas:

De lunes a miércoles: 2-4 de marzo de 2020.

Horario:

Desde las 9:00h hasta 19:00h (aproximadamente).

Agenda (i)

Tecnologías inalámbricas:

- Bluetooth.
- Bluetooth Low Energy (BLE).
- Wi-Fi: WPA2 y WPA3.
- Comunicaciones de radio en frecuencias inferiores a 1 GHz.
  - 433 MHz, 868 MHz, etc.
  - Múltiples tecnologías propietarias.
- SDR (Software Defined Radio).

Agenda (ii)

Para cada tecnología inalámbrica se analizarán:

- Introducción a la tecnología
  - Capa física, frecuencias y canales, ratios de transmisión, tramas, establecimiento de comunicaciones o sesiones, arquitectura, etc.
- Mecanismos de seguridad
  - Autentificación, autorización, cifrado e integridad
- Kit de herramientas de hacking y researching
  - Hardware y software (tradicional y móvil)
- Técnicas ofensivas de ataque
  - <Dependientes de cada tecnología inalámbrica>
- Recomendaciones defensivas de seguridad

Agenda (iii)

Software Defined Radio (SDR):

- Conceptos generales de radio frecuencia
- Procesamiento digital de señales (DSP, Digital Signal Processing)
- Descubrimiento e identificación de señales
- (De)modulación y (de)codificación de señales
- Recepción y transmisión de señales
  - Captura/Interceptación, modificación y repetición de señales
- GNU Radio
- Hardware SDR y no SDR

Agenda (iv)

Al finalizar el curso, los asistentes dispondrán de un extenso arsenal de herramientas hardware y software, técnicas y conocimientos que les permitirán analizar y evaluar en detalle la seguridad de las capacidades de comunicación inalámbricas de múltiples dispositivos (tradicionales y móviles) y objetos del Internet de las cosas (IoT, Internet of Things), en auditorías y/o pruebas de intrusión, así como realizar investigaciones (o *research*) de dichas capacidades sobre dispositivos nuevos o desconocidos.

Kit Hardware (i)

El curso incluye para cada asistente un kit hardware minuciosamente seleccionado y compuesto por múltiples componentes hardware necesarios para el análisis de la seguridad de tecnologías inalámbricas y comunicaciones vía radio.

El kit hardware está incluido en el precio del curso, con objeto de que cada asistente pueda disponer de él al finalizar el curso, de cara a poder aplicar de forma práctica los conocimientos adquiridos en múltiples escenarios y entornos reales.

NOTA: Los contenidos del kit hardware podrían variar ligeramente en función de los componentes que se identifiquen finalmente como más adecuados para el curso, en caso de identificarse productos con mejores capacidades.

NOTA: Los kits hardware son paquetes completos indivisibles y no hay posibilidad de solicitar o excluir ninguno de sus diferentes componentes individualmente.

Kit Hardware (ii)

Componentes del kit hardware:

- Ubertooth One + antena
- Yard Stick One + ANT 700
- Dispositivo Bluetooth & BLE:
  - SENA Parani UD-100
- Tarjeta Wi-Fi: Alfa AWUS036NHA
  - 802.11n (WPA3)
- Tarjeta Wi-Fi: Alfa AWUS1900 (AC)
  - 802.11ac

Kit Hardware (iii)

Componentes del kit hardware (continuación):

- Kit RTL-SDR premium + kit de antena(s)
- HackRF One
- ANT 500

Coste estimado del kit hardware ≈750 €

(España)

Costes

- El precio final del Bootcamp + entrada al Congreso RootedCON es de **1.999 € (kit hardware incluido)**

- **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 **DOCE (12)** 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