Practical Wireless & Radio Hacking (PWRH)
- Bootcamp -

/RootedCON 2017

Hacking Práctico de Tecnologías Inalámbricas y Comunicaciones vía Radio
- Bootcamp -

/RootedCON 2017

Introducción (1/2)

- El curso **Practical Wireless & Radio Hacking (PWRH)** se impartirá por segundo año en RootedCON 2017 como resultado de la experiencia en formación adquirida durante años previos sobre la seguridad de tecnologías inalámbricas más tradicionales como Wi-Fi y Bluetooth, ampliada a nuevas tecnologías, como Bluetooth Low Energy (BLE), comunicaciones de radio en frecuencias inferiores a 1 GHz (433 MHz, 868 MHz, etc.) y otras comunicaciones de radio tanto estándar como propietarias.

Introducción (2/2)

- 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).
- 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 ☺).

Objetivos

- Evaluar la seguridad del Internet de las Cosas (IoT - Internet of Things), y de otros dispositivos, desde el aire a través de la investigación y hacking de sus mecanismos de comunicación, tecnologías inalámbricas multifrecuencia y comunicaciones de radio empleando capacidades de Software Defined Radio (SDR), Bluetooth, Bluetooth Low Energy (BLE), Wi-Fi, comunicaciones de radio con frecuencias inferiores a 1 GHz, Z-Wave, etc.

A quién va dirigido

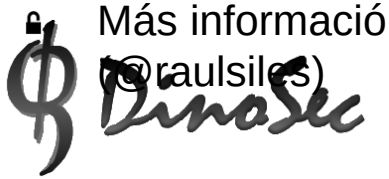
- Profesionales de seguridad de tecnologías de la información y las comunicaciones, pen-testers, auditores, administradores de redes, analistas, entusiastas de la seguridad y de las tecnologías inalámbricas, apasionados de las nuevas tecnologías, o cualquiera con conocimientos técnicos sólidos y con 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!**

Sobre el instructor

/Rooted®

Raúl Siles

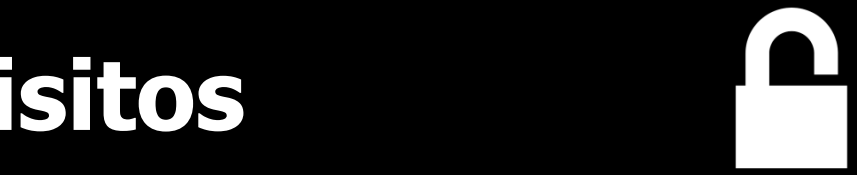
- Raúl Siles es fundador y analista de seguridad de DinoSec. Durante más de 15 años ha aplicado su experiencia en la realización de servicios técnicos avanzados de seguridad e innovado soluciones ofensivas y defensivas para organizaciones internacionales de diferentes industrias.
- A lo largo de su carrera, ha trabajado como experto de seguridad, ingeniero, investigador y pen-tester en Hewlett Packard, como consultor independiente, o en sus propias compañías, Taddong y DinoSec.
- Una de sus pasiones y áreas de especialización, entre otras, son las tecnologías inalámbricas, de las que lleva disfrutando durante la última década.
- Raúl es instructor certificado del SANS Institute y ponente habitual en conferencias y eventos de seguridad internacionales como RootedCON, 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.
- Más información en https://www.dinosec.com (@dinosec) y http://www.raulsiles.com (@raulsiles)



Sobre la formación de DinoSec

- 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.

Pre-requisitos



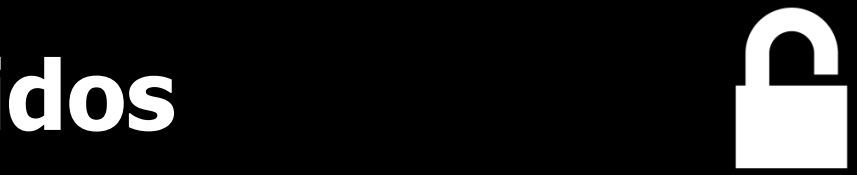
Conocimientos y aptitudes

- 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.

Pre-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).
  - Al menos 4 GB de RAM.
  - 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 con capacidades inalámbricas para su posible análisis y estudio.
- Se proporcionarán más detalles sobre los pre-requisitos técnicos tras completar el registro, aproximadamente una semana antes del curso.

Contenidos



Contenidos (1/2)

- Se trata de 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 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.

Contenidos (2/2)

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

Planificación

- El curso se impartirá durante tres días intensos, previos a la conferencia RootedCON 2017.
- Fechas:
  - De lunes a miércoles.
  - 27 y 28 de febrero y 1 de marzo de 2017.
- Horario:
  - Desde las 9:00h hasta 19:00h (aproximadamente).

Practical Wireless & Radio Hacking (1/4)

- Tecnologías inalámbricas
  - Bluetooth
  - Bluetooth Low Energy (BLE)
  - Wi-Fi
  - Comunicaciones de radio en frecuencias inferiores a 1 GHz
    - 433 MHz, 868 MHz, etc.
  - SDR (Software Defined Radio)
  - Otras tecnologías (*): Z-Wave, LoRa, ZigBee/XBee, etc.

(*) En función del tiempo disponible.

Practical Wireless & Radio Hacking (2/4)

- 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

Practical Wireless & Radio Hacking (3/4)

- 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

Practical Wireless & Radio Hacking (4/4)

- 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 y objetos del Internet of Things (IoT), en auditorías y/o pruebas de intrusión, así como realizar investigaciones o *research* de dichas capacidades sobre dispositivos nuevos o desconocidos.

Hardware incluido en el curso

/Rooted®

Hardware

- El curso incluye para cada asistente un kit minuciosamente seleccionado y compuesto por múltiples componentes hardware necesarios para el análisis de seguridad de tecnologías inalámbricas y comunicaciones vía radio.
- El kit de hardware básico está incluido en el precio estándar del curso para cada asistente, pudiendo estos disponer del mismo al finalizar el curso, y aplicar así los conocimientos adquiridos en múltiples escenarios y entornos reales.
- El kit de hardware avanzado conlleva un coste adicional al precio estándar del curso y se ofrece opcionalmente para todos los asistentes interesados (se recomienda su adquisición).

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

Hardware: Kit Básico

- Componentes del kit básico:
  - Ubertooth One + antena
  - Yard Stick One + ANT 700
  - Kit RTL-SDR + antena(s)
  - Dispositivo Bluetooth & BLE: SENA Parani UD-100
  - Tarjeta Wi-Fi: Alfa AWUS051NH version 2

- Coste estimado del kit básico: 400 € (España)

(*) Los contenidos del kit pueden variar ligeramente en función de los componentes que se identifiquen finalmente como más adecuados para el curso.
(Los kits son indivisibles y no hay posibilidad de fragmentar sus componentes)

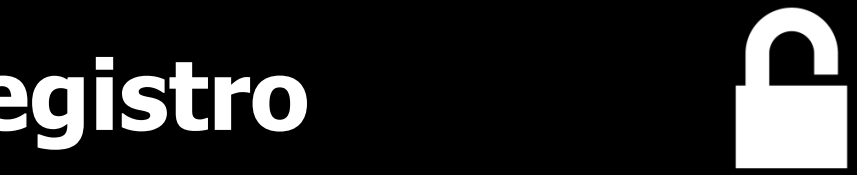
Hardware: Kit Avanzado

- Componentes del kit avanzado (adicionalmente a los componentes del kit básico):
  - HackRF One
  - ANT 500

- Coste estimado del kit avanzado: 375 € (España)
- Precio para los asistentes interesados: **275 €**

DinoSec

Costes y registro



Costes

- El precio final del Bootcamp es 1.400 € (kit básico)
- El precio final del Bootcamp es 1.600 € (kit avanzado)
- Si dispones de entrada confirmada para el congreso RootedCON 2017, **obtendrás un descuento del 10%.**
- Parte del hardware incluido en el curso está patrocinado.
- **IMPORTANTE**: Se requiere un mínimo de **DOCE (12)** asistentes para que el curso pueda realizarse.

Costes (Kit Básico)

Aquí puedes encontrar una referencia de los costes (con el kit básico):
(*Para la opción del kit avanzado deben sumarse 250 € - ver siguiente página*)

Practical Wireless & Radio Hacking	Coste (€)
Practical Wireless & Radio Hacking	1400 €
Sponsored discounts: Hardware Kit Básico	TBD
Final cost (€):	1400 €
RootedCON confirmed ticket discount	-140 €
Final cost *if you have RootedCON ticket* (€)	1260 €

Costes (Kit Avanzado)

Aquí puedes encontrar una referencia de los costes (con el kit avanzado):

Practical Wireless & Radio Hacking	Coste (€)
Practical Wireless & Radio Hacking	1775 €
Sponsored discounts: Hardware Kit Avanzado	TBD
Final cost (€):	1775€
RootedCON confirmed ticket discount	- 175€
Final cost *if you have RootedCON ticket* (€)	1600€

Contacto

General information:	info@rootedcon.com
Registration form:	
https://reg.rootedcon.com/training/bootcamp/Rootedcon2017/	
PWRH&ROOTED hashtag:	**#rooted2017pwrh**
Raul's twitter:	@raulsiles @dinosec
Facebook, LinkedIn:	*Rooted CON*
Twitter:	*@rootedcon* *Tags:* *#rooted and #rooted2017* *Previous editions:* *#rooted2010, #rooted2011, #rooted2012, #rooted2013, #rooted2014, #rooted2015, #rooted2016*

/Rooted®

Muchas gracias