

Hardware Hacking: Introduction for beginners.

RootedLAB

/RootedCON 2018

/Rooted[®]



Objetivos

Durante este taller descubriremos qué hay dentro de muchos de los aparatos que nos rodean en nuestro día a día como pueden ser routers, camaras, bombillas inteligentes, dispositivos médicos, alarmas, consolas, etc.

Aprenderemos a identificar los componentes físicos que contienen, con qué protocolos de comunicación interactúan entre ellos y cómo podemos manipularlos en nuestro beneficio con ejemplos prácticos.

Se realizaran distintas conexiones con las herramientas hardware proporcionadas para investigar los puertos de comunicaciones de los dispositivos así como el dumpeo de firmware.

Una vez dominada la parte física pasaremos a jugar con el firmware mediante el análisis, modificación y búsqueda de vulnerabilidades entre otras tareas.

Para todo ello solo se requiere un manejo básico de Linux y un portátil. ¿Aceptáis el reto?.



A quién va dirigido

Profesionales del sector de la Seguridad de la Información

Estudiantes

Administradores de sistemas y redes

Desarrolladores que quieran mejorar su perfil

Cuerpos y Fuerzas de Seguridad

Docentes

Cualquier persona con ganas de aprender



/Rooted[®]

Sobre el autor



Martina Matarí

Martina Matarí forma parte del equipo de CSIRT Global en Telefónica S.A.. Además, es fundadora de The Hackers Garage, una empresa que pretende acercar el hardware aplicado a la seguridad desde cero a través de proyectos DIY y talleres. Martina cuenta con más de 8 años de experiencia en el sector y con certificaciones tales como CEH y OSCP.

Oscar Tébar

Oscar Tébar es Auditor de Seguridad. Oscar cuenta con más de 8 años de experiencia en el sector y con certificaciones tales como OSCP.



/Rooted[®]

Requisitos



Conocimientos y aptitudes

- Recomendado un conocimiento básico de Linux a nivel de usuario.
- No es necesario contar con conocimientos en electrónica.
- Al finalizar el taller el usuario habrá obtenido un conocimiento básico a nivel de hardware y las herramientas esenciales para seguir profundizando en el aprendizaje de esta materia.

*No se requieren conocimientos avanzados los puntos enumerados anteriormente.



Requisitos técnicos

- Portátil con al menos dos puertos USB, 2GB de ram para usar y 20GB de espacio libre.
- Virtualbox y la maquina virtual del taller instalada y funcionando.
- Se entregará una caja de 'The Hackers Garage' con los componentes necesarios para la realización del laboratorio en el transcurso de las 8 horas



/Rooted[®]

Contenido



Introducción

Durante el laboratorio 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 haya cumplido en sus totalidad los objetivos de cada uno de los puntos.



Agenda

- El training transcurría durante **1 día**.
- Se realizará una pausa a media mañana y otra pausa para comer.
- La comida corre a cargo de cada uno de los asistentes.



Agenda

- Se realizará un libro/cuestionario a la vez que se realizan las practicas para afianzar los conocimientos adquiridos durante los objetivos.
- Se realizaran distintos ataques físicos realizando conexiones a varios buses(UART, SPI, etc) sobre varios dispositivos hardware preparados para el taller.
- Se aprenderá el uso de distintas herramientas de hardware hacking.
- Se realizará la extracción, análisis y modificación del firmware de un dispositivo hardware preparado para el taller.



Hardware Hacking: Introduction for beginners.

- The Hackers Garage
- Contenido de la Box
- Hardware for beginners
 - Buses
 1. UART
 2. I2C
 3. SPI
 4. JTAG



Hardware Hacking: Introduction for beginners.

- Herramientas de Hardware Hacking
 1. Analizador lógico (Sniffer de protocolos)
 2. FT232H (Herramienta multiusos)
 3. Hydrabus (Herramienta multiusos)
 4. BlackMagicProbe (Debugger de ARM)
 5. JTAG-Enum (JTAG pinout finder)



Hardware Hacking: Introduction for beginners

- Firmware for beginners
 - Extracción del firmware
 - Análisis del firmware
 - Modificación del firmware
 - Emulación del firmware
 - Explotación del firmware
 - Troyanización del firmware



/Rooted[®]

Costes



Coste

- El coste del curso es de 300€ (Caja con componentes incluida valorada en 100€)
- **IMPORTANTE:** se requiere un mínimo de diez asistentes para que el curso tenga lugar.



Contact

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



/Rooted[®]

Muchas gracias

