

/Rooted®



RootedLAB: Ethical Hacking & Pentesting

Pablo González

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

En este training, orientado a la práctica del hacking, podrás introducirte y sentar bases en los tipos de auditorías, en la forma de trabajo, en cómo llevar a cabo auditorías y como se debe presentar los resultados de éstas. Además, se introducirá y mostrarán ejemplos de Red Team y las diferencias de éste respecto al Hacking Ético y al Pentesting.

El alumno obtendrá una visión global del hacking ético, profundizando en ciertas partes prácticas de pentesting.

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

RootedCON 2020 - Dossier de Formación

Profesor: Pablo González

Máster Universitario en Seguridad Informática por la Universidad Internacional de La Rioja. Ingeniero en Informática por la Universidad Rey Juan Carlos. Ingeniero Técnico en Informática de Sistemas en la Universidad Rey Juan Carlos. Premio al mejor expediente de su promoción en la Universidad Rey Juan Carlos y Premio Extraordinario Fin de Carrera en Ingeniería Técnica en Informática de Sistemas. MVP Microsoft Security desde 2017.

Trabaja en Telefónica como Responsable del Departamento de Ideas Locas del área CDCO. Es docente y Director en el Máster de Seguridad de Tecnologías de la Información y de las Comunicaciones en la Universidad Europea de Madrid. Además, es docente en otros másteres de seguridad de la información. Trabajó en Informática64 durante 4 años en Formación, Consultoría y Auditoría.

Tiene diversas publicaciones en el ámbito de la Seguridad de la Información en la editorial Oxword

Pablo ha impartido formación en Rooted CON 2013-2019. También ha sido docente en los Labs de No cON Name 2013 y 2014 con Metasploit para Pentesters. Ha sido ponente en Rooted CON 2013, 2014, 2016, 2018 y 2019, No cON Name, Navaja Negra y otros congresos como Hackron, Sh3llCon, Cybercamp o Rooted Valencia, entre otros. Ponente en congresos internacionales como la Black Hat Europe Arsenal 2017, 2018 y 2019, 8dot8 en 2014, 2018 y 2019, EkoParty 2018, LeHack 2019, Bsides Colombia en 2016 o el IEEE SBS Gold en 2012. Fundador de hackersClub Academy

Requisitos: Conocimientos

Conocimientos básicos de:

Sistemas operativos

Conocimientos básicos de redes (TCP/IP)

Requisitos: Técnicos

Para el correcto funcionamiento de los labs será necesario que los alumnos dispongan de equipos con las siguientes características o similares:

El equipo portátil de los asistentes necesita:

Mínimo 4 GB RAM de memoria. Recomendable 6-8 GB RAM.

Software de virtualización Virtual Box (VMWare también es viable)

Máquinas virtualizadas:

Windows XP, Windows 7, Kali Linux virtualizados.

Opcional Windows 8 / 8.1 / 10 virtualizado

Contenido

En este lab con enfoque totalmente práctico se estudiarán las diferentes auditorías de un proyecto de hacking ético, así como las diferencias actuales entre un Red Team, un hacking ético y un Pentest. Dentro del ámbito del hacking ético se estudiarán técnicas que pueden ser utilizadas en un ejercicio de Red Team, en su vector digital.

El alumno contextualizará el hacking ético en un organización y realizará diferentes ejercicios basados en ataques físicos, enumeración de servicios, recopilación de información, técnicas de explotación, post-explotación, técnicas de escalada de privilegios, técnicas de bypass y evasión de protecciones en sistemas, técnicas de movimiento lateral en la organización y de pivoting. Además, se finalizará estudiando ataques de red modernos.

Un día entero de práctica y diversión para aprender o reciclarse en el ámbito del hacking ético.

Agenda (i)

Tipos de auditorías

Hacking ético: la ética

- Ley de Hacking

Estándares y modelos

- Metodologías
- Vulnerabilidades
- Evaluación

Red Team Vs Ethical Hacking

Metodología y vectores en el Red Team

Ataques físicos

Agenda (ii)

Autenticación & Autorización

- Windows Logon
- Autenticación
- Access Token
- Control Cuentas Usuario - UAC

Credenciales

- Hashes
- Extracción de credenciales
- MovimienPass the hash
- Ataque NTLM Relay

Agenda (iii)

Explotación de sistemas

- Explotación remota
- Explotación local (escalada privilegio, bypass UAC)

Técnicas de movimiento lateral (Lateral Movement - PtH & Pivoting)

Obtención de los primeros datos de interés

- Ataques redes (ARP Spoof, DNS Spoof, MiTM)
- Ataques redes modernos (SSL Strip+, Delorean...)

Costes

- El precio final del Rooted Lab es **200€**

IMPORTANTE: Se requiere un mínimo de **DIEZ (10)** 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®

