Ethical hacking: Pentesting RootedLAB

/Rooted Valencia 2016

/Rooted®

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

A quién va dirigido

Profesionales del sector de la Seguridad de la Información

Estudiantes

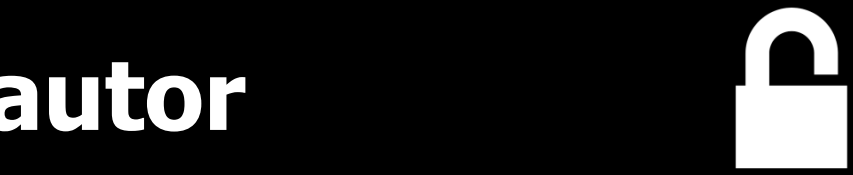
Administradores de sistemas y redes

Desarrolladores que quieran mejorar su perfil

Cuerpos y Fuerzas de Seguridad

Docentes

Sobre el autor



Pablo González

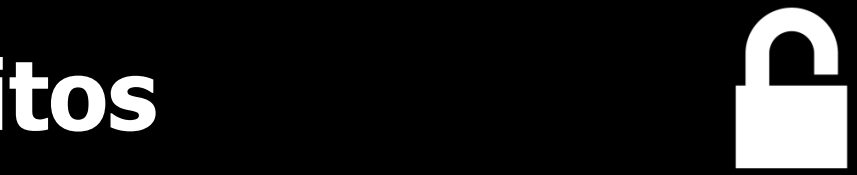
Máster Universitario en Seguridad Informática por la Universidad Internacional de La Rioja. Ingeniero en Informática por la Universidad Rey Juan Carlos. Ingeniero Técnico en Informática de Sistemas en la Universidad Rey Juan Carlos. Premio al mejor expediente de su promoción en la Universidad Rey Juan Carlos y Premio Extraordinario Fin de Carrera en Ingeniería Técnica en Informática de Sistemas. Trabaja en 11Paths – Telefónica Digital España como Technical Business Manager. Es docente en el Máster de Seguridad de Tecnologías de la Información y de las Comunicaciones en la Universidad Europea de Madrid. Trabajó en Informática64 durante 4 años en Formación, Consultoría y Auditoría.

Tiene diversas publicaciones en el ámbito de la Seguridad de la Información:

- Autor del libro Metasploit para Pentesters. Editorial 0xWord. 1ª ed. 2012, 2ª ed. 2013 y 3ª ed. 2014.
- Autor del libro Ethical Hacking: Teoría y práctica para la realización de un pentesting. Editorial 0xWord.
- Autor del libro Got Root: El poder de la mente. Editorial 0xWord. 2016.
- Autor del libro Pentesting con Kali. Editorial 0xWord.

Pablo ha impartido formación en Rooted CON 2013, 2014 y 2015 con Metasploit Labs y Hacking de dispositivos iOS. 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 y 2014, No cON Name 2011, Navaja Negra 2014 y otros congresos como Hackron, Sh3llCon, Qurtuba Security Congress, Cybercamp o Rooted Valencia, entre otros. Ponente en congresos internacionales como la 8dot8 celebrada en Chile en 2014 o el IEEE SBS Gold en 2012.

Requisitos



Conocimientos y aptitudes

Conocimientos básicos de:

- Sistemas operativos
- Conocimientos básicos de redes (TCP/IP)

*No se requieren conocimientos avanzados los puntos enumerados anteriormente.

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 virtualizado

Contenido

Introducción

Durante el lab 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.
- La formación es eminentemente práctica.

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.

Ethical Hacking: Pentesting

Introducción:

- Tipos de auditorías
- Hacking ético: la ética
  - Ley de Hacking
- Estándares y modelos
  - Metodologías
  - Vulnerabilidades
  - Evaluación

Ethical Hacking: Pentesting

- Metodología de trabajo
  - RFP
  - Equipo
  - Proyecto
  - Fases
  - Comunicación
  - Documentación

Ethical Hacking: Pentesting

- ¿Cómo publicar una vulnerabilidad?
  - CVE
  - Detalles
  - Ejemplo

Ethical Hacking: Pentesting

- Auditorías (I)
  - Auditoría interna
    - Pruebas
    - Escenario inicial
    - Identificación de servicio, entorno y límites
    - Obtención de los primeros datos de interés
      - Ataques redes (ARP Spoof, DNS Spoof, MiTM)
      - Ataques redes modernos (SSL Strip+, Delorean…)
    - Explotación de sistemas
      - Exploits (Local, Remote)
    - Técnicas de movimiento lateral (Lateral Movement - PtH & Pivoting)

Ethical Hacking: Pentesting

- Auditorías (II)
  - Ethical Hacking: Otras auditorías y pruebas de un RFP
    - APT: Simulación
      - ¿Qué es el APT?
      - Pruebas
      - ¿Cómo llevarlo a cabo con un porcentaje alto de éxito?

Ethical Hacking: Pentesting

- Informe y medidas correctoras
  - Tipos de informe
  - Generación y partes de un informe
  - Plantillas
  - Recomendaciones genéricas y específicas del auditor

Costes

Coste

- El coste del curso es de 70€
- Si te has registrado en Rooted Satellite Valencia, el precio es de 50€
- **IMPORTANTE**: se requiere un mínimo de diez (10) asistentes para que el curso tenga lugar.

Contact

General information:	info@rootedcon.com
Registration form:	
https://reg.rootedcon.es/training/.../	
Hashtag:	**#RVLC**
Pablo's twitter:	@pablogonzalezpe
Facebook, LinkedIn:	*Rooted CON*
Twitter:	*@rootedcon* *Tags:* *#rooted y #RVLC*

/Rooted®

Muchas gracias