/Rooted

Practical Pentesting: Entrenamiento a través de escenarios

Pablo González

MADRID

7 al 9 de Marzo de 2022

DOSIER DE FORMACIÓN

/Rooted

Días 7-9 de Marzo

Tres días de trainings y workshops

HOTEL Eurostars iHotel
Pozuelo de Alarcón

Días 10-12 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

Hoy en día es necesario de un entrenamiento constante de los equipos de Red Team, Hacking Ético y/o Pentesting. Este entrenamiento se lleva a cabo a través del uso de escenarios preparados que permiten al pentester reciclarse en sus conocimientos. ¿Qué son los escenarios? Son un conjunto de máquinas virtuales y contenedores que muestran casos reales a los que un pentester se enfrenta. Este lab proporciona un aprendizaje de técnicas del día a día del pentester a través del uso de diferentes escenarios reales y clasificados por las diferentes técnicas y por nivel.

- Aprender metodología para hacer un pentesting práctico y resolver problemas
- Enfrentarse a entornos reales
- Resolver escenarios a través de un entrenamiento práctico

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

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 0xword

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, BlackHat USA 2020, 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 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 8 GB RAM de memoria. Recomendable 8-12 GB RAM.

Software de virtualización Virtual Box o Hyper-V (VMWare también es viable)

Docker instalado y funcionando

Máquinas virtualizadas:

Windows 7/10 & Kali Linux virtualizados.

Contenido

Hoy en día es necesario de un entrenamiento constante de los equipos de Red Team, Hacking Ético y/o Pentesting. Este entrenamiento se lleva a cabo a través del uso de escenarios preparados que permiten al pentester reciclarse en sus conocimientos. ¿Qué son los escenarios? Son un conjunto de máquinas virtuales y contenedores que muestran casos reales a los que un pentester se enfrenta. Este lab proporciona un aprendizaje de técnicas del día a día del pentester a través del uso de diferentes escenarios reales y clasificados por las diferentes técnicas y por nivel.

¿Qué herramientas se verán en este lab? Todas valen. Lo importante son las técnicas y el conocimiento, así como poder aplicarlo sobre un escenario real construido para el lab. La visión que obtiene el alumno es la siguiente:

Contenido

Parte I. Se enseñan diferentes técnicas de enumeración de máquinas y redes. En esta primera parte del lab, se resuelven escenarios de enumeración y se muestra el uso de técnicas y herramientas sobre ellos.

Parte II. Identificación de vulnerabilidades y explotación de éstas. El alumno recorrerá diferentes escenarios viendo cómo se detectan vulnerabilidades y cómo éstas se pueden explotar (con diferentes herramientas y con técnicas manuales). Esta parte cubre un amplio abanico que puede ir desde la generación de un exploit propio hasta el uso de herramientas automáticas. Todo ello sobre un escenario.

Parte III. Post-explotación. En esta parte se tratarán técnicas de escalada de privilegios, pivoting, técnicas de movimiento lateral, extracción de credenciales, etcétera. Todo a través del uso de escenarios reales (a los que un pentester se puede enfrentar en su día a día).

Los escenarios pueden contener diferentes máquinas (GNU/Linux), por lo que el enfoque es más global y real. Se estudiarán escenarios con vulnerabilidades en diferentes entornos, se utilizarán técnicas de post-explotación para poder elevar privilegio o pasar a otra máquina. El objetivo es claro: ¡Conseguir la flag!

Contenido

Cuando las máquinas y los escenarios se van comprometiendo se deberá ir recopilando flags (como si de un CTF se tratase) y escalando privilegios para conseguir otro tipo de flags. Este tipo de entorno competitivo enriquece la formación y el entrenamiento del alumno.

Por último, el docente enseñará todo sobre escenarios preparados para que el alumno pueda aprender. El alumno posteriormente, dispone de escenarios (entornos GNU/Linux) para llevar a cabo las mismas pruebas (tanto los que el profesor enseña como otros nuevos).

En este tipo de formación no todo sale a la primera, pero entenderás cómo funciona la metodología, tendrás tiempo para 'pegarte' con entornos reales, preguntar y aprender (o reciclarte) en las técnicas del pentesting.

Al final del lab, el alumno se enfrentará a una prueba global con un escenario al que habrá que aplicarle la metodología detallada en el lab y obtener todas las flags.

NOTA: Si tienes dudas sobre la dinámica del lab. Contacta con nosotros para preguntar

Dinámica

- Se despliega el primer escenario. El profesor enseña todo lo referente con el apartado estudiado sobre dicho escenario. El alumno puede resolver dicho escenario y, posteriormente, resolver (y 'pegarse') el escenario propuesto para ellos.
- Segunda parte del lab. Se despliega el escenario. El docente enseña sobre escenario las diferentes técnicas y situaciones que se pueden dar. El alumno dispone después de otro escenario sobre el que trabajar.
- Tercera parte del lab. Se despliega el escenario. El docente enseña sobre escenario las diferentes técnicas y situaciones que se pueden dar. El alumno dispone después de otro escenario sobre el que trabajar.
- Otros escenarios alternativos pueden verse.

• Escenario final. Prueba para determinar el aprovechamiento del lab.

Agenda (i)

- MakeLab: Escenarios de entrenamiento preparados
- Metodología de Pentesting
- Mochila del pentester
  - ¿Qué debo tener a mano en un Red Team?
  - ¿Qué debo tener a mano en un pentest?
  - Distros & Tools
- Fase 1: Enumeración y reconocimiento
- Escenario: Enumeración
  - Técnicas de enumeración
  - Herramientas
  - Información relevante
  - Existencia de vectores de ataque
  - Escenario propuesto

Agenda (ii)

- Fase 2: Identificación de vulnerabilidades y explotación
- Escenario: Identificación y explotación
  - Técnicas para identificar vulnerabilidades
  - Técnicas de explotación vulnerabilidades
  - Overflow
  - Bind. Reverse
  - Herramientas
  - Escenario propuesto

Agenda (iii)

- Fase 3: Post-Explotación
- Escenario: Post-Explotación
  - Recopilación de información
  - Escalada de privilegios
  - Pivoting
  - Movimiento lateral
  - Herramientas
  - Escenario propuesto
- Resolución escenario final

Costes

- El precio final de este **RootedLAB** es **250 €**

- **Puedes registrarte y formalizar el pago en: https://reg.rootedcon.com**

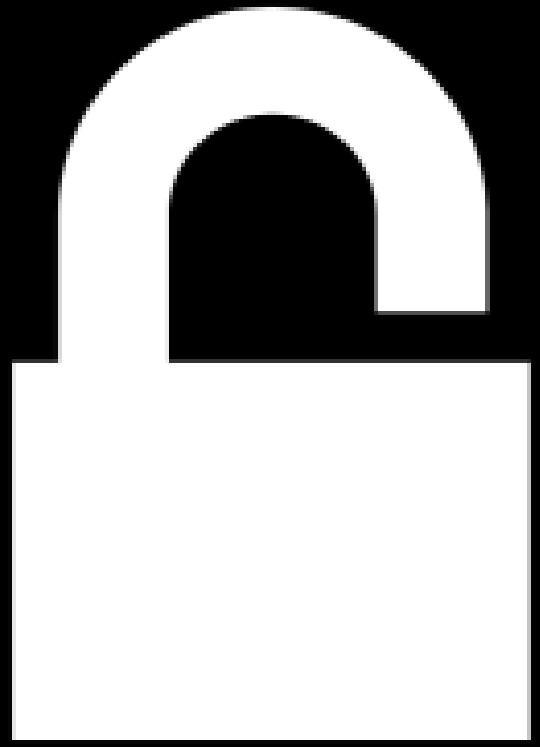
IMPORTANTE:

Se requiere un mínimo de **CINCO (5)** asistentes para que el curso pueda celebrarse.

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: https://reg.rootedcon.com. 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.
- Puedo pagar con transferencia bancaria?
  - Si, desde el propio RootedManager podrás gestionar el pago mediante transferencia bancaria.
- El training incluye comida?
  - Los training no incluyen comida. Pero hay varias opciones en la zona, y el profesor os dará más información.

/Rooted



Contacto:

info@rootedcon.com