Metasploit para Pentesters

/RootedCON 2017

/Rooted®

Objetivos

En este *training*, orientado a la práctica del *hacking*, podrás adentrar en el mundo de Metasploit, el framework de explotación más utilizado en el mundo del pentesting. En el *training* se irá de menos a más hasta lograr sacar un gran rendimiento con técnicas más avanzadas que aportarán en tu pentest.

Disponer de una visión global de Metasploit Framework, conocimiento sobre la utilización de herramientas que ayudan a Metasploit y al pentester en su tarea.

Conocer la arquitectura del framework, distintas etapas de un test de intrusión (gathering, exploiting, post-exploiting) y desarrollo de nuestras primeras pruebas con ruby.

A quién va dirigido

Profesionales del sector de la Seguridad de la Información

Estudiantes

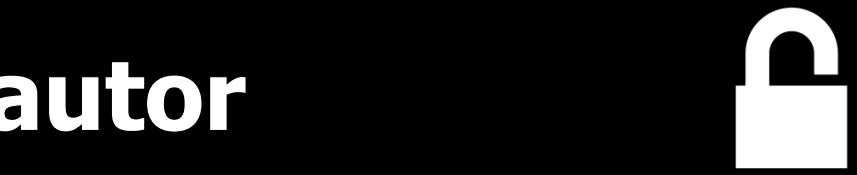
Administradores de sistemas y redes

Desarrolladores que quieran mejorar su perfil

Cuerpos y Fuerzas de Seguridad

Docentes

Sobre el autor



/Rooted®

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 Identity & Privacy como Project 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 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. Fundador de hackersClub Academy (http://hackersclub.academy)

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:
  - 4 GB RAM mínimo
  - Máquinas virtuales:
    - Kali Linux
    - Windows 7/8
    - Otras aplicaciones serán indicadas por el instructor en el propio taller

Contenido

Introducción

Durante el RootedLab, los asistentes tendrán la oportunidad de trabajar con pruebas de concepto, con ejercicios prácticos y entornos reales de pentesting con la herramienta Metasploit. El alumno recorrerá diferentes ambientes con diferentes tipos de dificultad. Comenzará con una visión básica hasta completer acciones más avanzadas con el framework.

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.

Metasploit para Pentesters

- **Introducción al Framework**
  - –Fases del test
  - –Arquitectura
  - –Módulos
  - –Adición de componentes al framework
  - –Comandos básicos
- **Los preliminares**
  - –Las auxiliary: un cajón
  - –Escáneres de puertos
  - –Fingerprinting
    - •SSH
    - •SMB
    - •HTTP
    - •Otros
  - –Servidores
    - •DNS
    - •DHCP
  - –Protocolo ARP
  - –DoS

Metasploit para Pentesters

- **Exploiting & Payloads**
  - –Tipos de payloads
    - •Inline
    - •Stagers
    - •Stage
  - –Tipos de explotación y módulos
    - •Explotación directa
    - •Client-Side
    - •Explotación local
    - •Fileformat
  - –Explotación en distintos sistemas:
    - •Windows (XP, 7, 8, 8.1)
    - •Linux
    - •Servicios multiplataforma

Metasploit para Pentesters

- **Post-Explotación**
  - –Funcionalidades
    - •Recolección de información y ámbito
  - –Módulos de Meterpreter
    - •¿Qué me permite?
    - •¿Qué puedo hacer yo?
  - –Pass the hash
  - –Persistencia de payloads
  - –Pivoting
- **Herramientas del framework**
  - –Msfvenom
  - –Msfd
  - –Pattern_create
  - –Pattern_offset
  - –Metasm

Metasploit para Pentesters

- **Metasploit Avanzado**
  - –Técnicas y usos en un pentest
    - •VPN como MiTM
    - •ProxyChains & Socks4a
  - –Generación de módulos
    - •Creación de módulos
  - –Generación de scripts para Meterpreter
    - •Creación de un módulo básico para Meterpreter

Costes

Coste

- El coste del curso es de 200€
- **IMPORTANTE:** se requiere un mínimo de diez (10) asistentes para que el curso tenga lugar.

Contacto

General information:	info@rootedcon.com
Registration form:	
https://reg.rootedcon.es/training/.../	
Hashtag:	**#RC17**
Pablo's twitter:	@pablogonzalezpe
Facebook, LinkedIn:	*Rooted CON*
Twitter:	*@rootedcon* *Tags:* *#rooted y #RC17*

/Rooted®

Muchas gracias