Metasploit & Hacking Ético RootedLAB

/Rooted Valencia 2018

Pablo González

/Rooted®

@pablogonzalezpe

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* irá de menos a más hasta lograr sacar un gran rendimiento con técnicas más avanzadas que aportarás en tu pentest. Todo desde el punto de vista del hacking ético.

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)

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

@pablogonzalezpe

/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. MVP Microsoft 2017-2018 en Security.

Trabaja en 11Paths – Telefónica Digital España 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. Además, es docente en el Máster de Seguridad Informática de la Universidad Internacional de La Rioja. También es docente en la Universidad Oberta de Catalunya, Universidad Rey Juan Carlos, Universidad de Castilla La Mancha y ESIC. 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.
- Autor del libro Pentesting con Powershell. Editorial 0xWord.
- Autor del libro Got Root.

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, 2014 y 2016, No cON Name 2011, Navaja Negra 2014 y 2016 y otros congresos como Hackron, Sh3llCon, Qurtuba Security Congress, Cybercamp o Rooted Valencia, entre otros. Ponente en congresos internacionales como la Black Hat Europe Arsenal 2017, 8dot8 celebrada en Chile en 2014, Bsides Colombia en 2016 o el IEEE SBS Gold en 2012. Fundador de hackersClub Academy

Requisitos

/Rooted®

@pablogonzalezpe

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

/Rooted®

@pablogonzalezpe

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 completar acciones más avanzadas con el framework.

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.

Metasploit & Pentesting

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

Metasploit & Pentesting

- **Exploiting & Payloads**
  - Tipos de payloads
    - Inline
    - Stagers
    - Stage
  - Tipos de explotación y módulos
    - Explotación directa
    - Client-Side
    - Explotación local
      - Escalada privilegio (módulos configuración débil & vulns)
      - Bypass UAC
    - Fileformat
  - Explotación en distintos sistemas:
    - Windows (XP, 7, 8, 8.1)
    - Linux
    - Servicios multiplataforma
    - Credenciales (Volcado de hashes, Hashes DC, Mimikatz...)

Metasploit & Pentesting

- **Post-Explotación**
  - Funcionalidades
    - Recolección de información y ámbito
  - Módulos de Meterpreter
    - ¿Qué me permite?
    - Extensiones / Plugins
  - Pass the hash
  - Persistencia de payloads
  - Pivoting
    - Túneles
    - Portfwd
    - PortProxy
    - Proxychains
- **Herramientas del framework**
  - Msfvenom
  - Msfd
  - Pattern_create
  - Pattern_offset

Costes

/Rooted®

Coste

- El coste del curso es de 100€ (incluye libro del docente)
- **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.com	
Hashtag:	**#rootedvlc**
Pablo's twitter:	@pablogonzalezpe
Facebook, LinkedIn:	*Rooted CON*
Twitter:	*@rootedcon*

/Rooted®

Muchas gracias

@pablogonzalezpe