/Rooted

RootedLAB: Offensive Powershell

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 utilizando powershell, podrás introducirte y sentar bases en el uso de Powershell como herramientas de pentesting.

Este novedoso taller presenta el poder que Powershell ofrece al pentester en entornos como Windows (7/8/8.1/10). El taller ofrece diferentes entornos en los que iremos viendo cómo funciona Powershell, por qué es tan importante en el pentesting de hoy en día y cómo poder crear algunas funciones que necesitemos en nuestro día a día. El taller se divide en 4 partes.

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, 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 la primera parte trabajaremos los conceptos básicos en los que se fundamenta Powershell. Con esta parte podremos crear pequeñas funcionalidades orientadas al pentest. En la segunda parte trabajaremos con los conjuntos de scripts más clásicos que han ido saliendo en los últimos años orientados a Pentesting (nishang, Powershell Mafia, Power up, etcétera). En la tercera parte trabajaremos con Empire. Empire es, posiblemente, el proyecto más potente en lo que a uso de Powershell en Pentesting se refiere. Entraremos a fondo en el uso de esta magnífica herramienta. La última parte se la dedicaremos a ibombshell y las posibilidades que trae la herramienta. Además, el alumno tendrá nociones para realizar una pequeña herramienta de pentesting con todo lo visto en el lab y de poder manejar estas potentes herramientas en su día a día.

Cabe destacar que Powershell puede ser utilizado en sistemas GNU/Linux y macOS por lo que escenarios y conceptos que trabajemos para Windows nos funcionarán en las otras plataformas.

Agenda (i)

Introducción Powershell

Conceptos básicos & Comandos

Scripting

- Variables
- Estructuras
- Bucles
- Funciones

Agenda (ii)

Pentesting I. Scripts aplicados a:

- Enumeración
- Recopilación
- Explotación
- Post-Explotación
- Escenarios prácticos aplicados

Agenda (iii)

Pentesting II. Empire

Arquitectura

- Agents
- Listeners
- Stagers

Tipos listeners

Escenarios prácticos aplicados

- Inclusión agente Empire en máquina
- Recopilación información
- Elevación privilegios Empire
- Movimiento lateral Empire

Agenda (iv)

Pentesting III. Ibombshell

- –Introducción a la herramienta
- –Aprovechamiento carga dinámica
- –Modos: Everywhere Vs Silently
- –Escenarios prácticos aplicados

Pentesting IV. Creando tu propia tool

- –Creación de una pequeña tool orientada al pentest con Powershell

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

Contacto: info@rootedcon.com