/Rooted

10 YEAR ANNIVERSARY

Tácticas para el desarrollo de ejercicios Red Team

MADRID

25 al 27 de Marzo de 2019

DOSIER DE FORMACIÓN

/Rooted

Días 25-27 de Marzo

Tres días de trainings y workshops

HOTEL Eurostars iHotel
Pozuelo de Alarcón

Días 28-30 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

El objetivo del Bootcamp es profundizar en el desarrollo de simulaciones reales de ataques dirigidos o ejercicios Red Team, mostrando las diferentes fases, acciones, herramientas y principales pautas a tener en cuenta para la realización de escenarios reales a través de los cuales desarrollar una intrusión en una organización.

Durante el transcurso de la formación, de 3 días de duración, los alumnos trabajaran desde la creación de vectores de acceso realistas, involucrando cualquier ámbito de actuación y la combinación de estos, ya sea intrusión digital, física o mediante el uso de ingeniería social, hasta las acciones internas como el desarrollo de movimiento lateral, persistencia o compromiso de infraestructuras Microsoft. Todas estas acciones se expondrá la forma de actuar en diferentes escenarios, tanto con permisos de administrador como sin ellos, desde un sistema Windows o Linux, etcétera.

Los asistentes contaran con todo el material necesario para desarrollar las pruebas sobre un entorno real, que simule una organización.

Profesores

Eduardo Arriols Núñez: Es Ingeniero Informático por la Universidad Autónoma de Madrid. Trabaja actualmente como responsable del servicio Red Team en Innotec System (Entelgy) y profesor de grado y postgrado en diversas universidades como U-Tad, UCLM o URJC. Es escritor del libro "CISO: El Red Team de la empresa", de la editorial 0xWord. Ha sido ponente tanto en congresos nacionales como internacionales tales como RootedCON, Navaja Negra, Jornadas STIC (CCN-Cert) o 8.8 Security Conference (Chile y Bolivia) entre otros.

Roberto López Santoyo: Es Ingeniero Informático por la Universidad Autónoma de Madrid. Actualmente trabajando en el Red Team de Innotec System. Fundador de la comunidad de seguridad Highsec (blog, congresos, etcétera). Instructor de Ciberseguridad en U-Tad.

A quién va dirigido

El curso no pretende servir de introducción al hacking ético, sino profundizar en el desarrollo de técnicas de Red Team. Por este motivo, está enfocado especialmente a profesionales del sector de la Seguridad de la Información y especialmente a aquellos relacionados con la auditoria de seguridad y pentesting.

Así mismo, también está abierto a todos aquellos que ya cuenten con algunos conocimientos de auditoría que serán expuestos posteriormente, tales como:

- Estudiantes
- Desarrolladores
- Administradores de sistemas y/o redes
- Cuerpos y Fuerzas de Seguridad
- Y cualquiera que esté interesado en aprender y profundizar en el desarrollo de ejercicios Red Team

Requisitos: Conocimientos

Para el correcto aprovechamiento del curso el alumno deberá contar con los siguientes conocimientos básicos:

- Manejo de sistemas operativos Windows y Linux.
- Herramientas de hacking ético tales como Metasploit, Nmap, Sqlmap, …
- Conocimiento de vulnerabilidades tales como SQL Injection o File Upload.
- Y sin duda, muchas ganas de ponerse en la piel de un atacante y crear ataques reales.

Esto permitirá encadenar múltiples acciones a través de las cuales crear vectores de ataque reales.

Requisitos: Técnicos

Para el correcto funcionamiento del Bootcamp será necesario que los alumnos dispongan de equipos con acceso de administrador. Las máquinas deben contar con las siguientes características mínimas:

- 4 GB de memoria RAM.
- Espacio en disco suficiente como para crear una maquina virtual de Kali Linux.
- Tener instalado VirtualBox o VMWare.

Durante el curso se proporcionará al alumno el entorno completo de máquinas virtuales, las cuales podrá desplegar en su equipo o hacer uso de la infraestructura que se pondrá in situ para el desarrollo del curso. En este caso el equipo deberá contar con al menos:

- La máquina de ser capaz de ejecutar cuatro máquinas virtuales de forma simultánea, para ello se estima que las siguientes características son las mínimas.
- 16 GB de memoria RAM.
- Espacio en disco suficiente como para copiar hasta 4 máquinas virtuales.

Agenda

- Introduction
- Infrastructure Deployment
- Recon
- Initial Access Vectors
- Internal Discovery
- Defense Evasion
- Local Privilege Escalation
- Credential Access
- Lateral Movement
- Persistence

Descripción (i)

1. **Introduction**: Introducción al desarrollo de los ejercicios, metodología, fases y acciones, así como pautas para su desarrollo y aspectos importantes a tener en cuenta.

2. **Infrastructure Deployment**: Despliegue y configuración de la infraestructura necesaria para el desarrollo del ejercicio, tales como la configuración de servidores VPS para actuar de C&C (HTTP, TCP, DNS, …), USBs para el despliegue de malware, Raspberry para la actuación como implante hardware en la red, etcétera.

3. **Recon**: Identificación de todos los activos existentes en los ámbitos de actuación permitidos (activos en perímetro, infraestructura Wi-Fi, entorno físico, empleados, etcétera).

Descripción (ii)

4. **Initial Access Vectors**: Principales técnicas y acciones que pueden ser realizadas para lograr el compromiso de un primer activo de la organización, con el que continuar posteriormente la intrusión. Así como las acciones posteriores para utilizar el activo comprometido para acceder a la red interna de la organización.

5. **Internal Discovery**: Acciones que pueden ser llevadas a cabo una vez se logra acceso a la red interna, estableciendo las pautas para enumerar el activo comprometido, la red y el entorno de directorio activo en el que se encuentra. Con el objetivo de encontrar potenciales vías para continuar el proceso de intrusión.

Descripción (iii)

6. **Defense Evasion**: Técnicas para evitar las medidas de seguridad que pueden encontrarse tanto en el equipo como en la red tales como antivirus o configuraciones de seguridad restrictivas, así como la forma de actuar en infraestructuras con mayores medidas de monitorización.

7. **Local Privilege Escalation**: Principales técnicas para permitir acceso con privilegios sobre entornos tanto Windows como Linux, que pueden ser utilizadas sobre el activo inicial comprometido, o maquinas internas para continuar con el desarrollo de ataques internos.

8. **Credential Access**: Acciones y herramientas que podrán ser utilizadas para obtener credenciales, elevar privilegios en el dominio y pivotar entre diferentes dominios.

Descripción (iv)

9. **Lateral Movement**: Técnicas para moverse entre equipos, redes y dominios internos mediante el acceso a sistemas con el uso de protocolos como SSH, SMB, WMI, WinRM o DCOM, la explotación de vulnerabilidades, etcétera.

10. **Persistence**: Conjunto de acciones y pautas para desplegar persistencia en puestos de usuario, equipos en DMZ y servidores internos, además de en el propio dominio.

Laboratorio

Las pruebas serán desarrolladas sobre un entorno Windows, con sistemas en dominio y su correspondiente directorio activo. Las maquinas existentes en el laboratorio serán:

- Controlado de Dominio (DC)
- Servidor Windows
- Servidor Linux
- Puesto de usuario
- Puesto de usuario con Antivirus

El alumno recibirá al inicio del curso un pendrive con la infraestructura.

Material proporcionado

Al inicio los alumnos recibirán un USB con el laboratorio, temario y herramientas.

Adicionalmente se proporcionarán los recursos necesarios para que los alumnos desplieguen y configuren durante el curso una infraestructura individual y anónima. Estos son los recursos, que se proporcionaran a cada alumno para su uso durante un mes:

- Servidor dedicado (VPS)
- Alta de un dominio
- Acceso VPN

Costes

- El precio final del Bootcamp + entrada al Congreso RootedCON es **1.200 €**

- **Cuando se abra el registro para las entradas al Congreso, se te enviará un código para canjear tu entrada.**

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 training no incluyen comida. Pero hay varias opciones en la zona, y el profesor os dará más información.

/Rooted

Contacto:

info@rootedcon.com