/Rooted

Técnicas para el desarrollo de ejercicios Red Team

Eduardo Arriols
Roberto López

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

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 todos los aspectos de una intrusión, desde la creación de vectores de acceso (involucrando cualquier ámbito de actuación y la combinación de estos ya sea intrusión digital, física o mediante el uso de ingeniería social), hasta acciones internas como el desarrollo de movimiento lateral, persistencia o compromiso de infraestructuras Microsoft.

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

A quién va dirigido

La formación 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.

La formación también está abierta a todos aquellos que ya cuenten con conocimientos de hacking medio que serán expuestos posteriormente, tales como estudiantes, desarrolladores, administradores de sistemas y/o redes, Cuerpos y Fuerzas de Seguridad, o cualquiera que esté interesado en aprender y profundizar en el desarrollo de ejercicios Red Team.

Profesor: Eduardo Arriols

Es Ingeniero Informático por la Universidad Autónoma de Madrid y co-fundador de RootPointer, una empresa de Ciberseguridad especializada en la identificación y gestión de activos en Internet. Anteriormente ha trabajado durante 6 años como responsable de equipos Red Team en diferentes organizaciones.

Es profesor de grado y postgrado en diversas universidades como U-Tad, UCLM o URJC, además de escritor del libro "CISO: El Red Team de la empresa", de la editorial 0xWord. Ha sido ponente en congresos nacionales e internacionales tales como RootedCON, Navaja Negra, Jornadas STIC (CCN-Cert) o 8.8 Security Conference (Chile y Bolivia).

Profesor: Roberto López

Ingeniero Informático por la Universidad Autónoma de Madrid. Trabaja como Red Team Technical Manager en Entelgy Innotec en donde coordina ejercicios de intrusión avanzada (Red Team). Es profesor universitario en el grado de Ingeniería del software en U-Tad.

Ha impartido formaciones en Cybersecurity Summer BootCamp (INCIBE), EUSchool y UAM entre otros. Co-Fundador de RootPointer (startup de ciberseguridad).

Requisitos: Conocimientos

Para el correcto aprovechamiento del curso es recomendable que el alumno cuente con, al menos, los siguientes conocimientos básicos:

- Manejo de sistemas operativos Windows y Linux.
- Manejo de herramientas de hacking ético tales como Metasploit, Nmap, Sqlmap, …
- Explotación de vulnerabilidades en sistemas y metodologías de auditoría.
- Explotación de vulnerabilidades web tales como SQL Injection o File Upload.

Y sin duda, muchas ganas de ponerse en la piel de un atacante y crear ataques reales.

Requisitos: Técnicos mínimos

Para el correcto desarrollo de las prácticas que serán realizadas en el Bootcamp será necesario que los alumnos dispongan de equipos con acceso de administrador. Las máquinas deben contar con las siguientes características mínimas:

- 8 GB de memoria RAM.
- Espacio en disco suficiente como para crear una maquina virtual de Kali Linux.
- Tener instalado VMWare (independientemente de ser la versión gratuita o de pago).

A todos los alumnos se les proporcionará una infraestructura completa virtualizada, aunque en aquellos casos en los que por motivos de recursos no sea posible que el alumno despliegue dicha infraestructura, podrá realizar las pruebas contra una infraestructura desplegada adicional.

Requisitos: Técnicos recomendados

Con el objetivo de poder desplegar la infraestructura completa desplegada para el correcto desarrollo de las pruebas, se recomienda que el equipo anfitrión pueda ser capaz de ejecutar al menos cuatro máquinas virtuales de forma simultánea.

Para ello se estima que las características mínimas son las siguientes:

- 16 GB de memoria RAM.
- 150GB de espacio en disco.

Se proporcionará a cada alumno un dispositivo de almacenamiento externo con todas las máquinas virtuales, por lo que el espacio en disco no sería requisito imprescindible.

Contenido

- Despliegue de infraestructura
- Reconocimiento del objetivo
- Identificación de vectores de acceso
- Descubrimiento interno
- Elevación de privilegios
- Acceso a credenciales
- Movimiento lateral
- Despliegue de persistencia
- Evasión de medidas de seguridad

Agenda (i)

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

2. **Despliegue de infraestructura**: 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. **Reconocimiento**: Identificación de todos los activos existentes en los ámbitos de actuación, tales como sistemas expuestos en Internet, infraestructura Wi-Fi, entorno físico, empleados, etcétera.

Agenda (ii)

4. **Identificación de vectores de acceso**: 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. También se profundizará en las acciones posteriores para utilizar el activo comprometido para acceder a la red interna de la organización.

5. **Descubrimiento interno**: 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 y el compromiso de la entidad.

Agenda (iii)

6. **Elevación de privilegios local**: 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.

7. **Acceso a credenciales y elevación en dominio**: Acciones y herramientas para lograr la obtención de credenciales internas sobre el dominio, técnicas para elevar privilegios en el dominio y pivotar entre diferentes dominios, así como otras útiles tales como Kerberoast, revisión de shares, etcétera.

8. **Movimiento lateral**: Técnicas para moverse entre sistemas, redes y dominios internos mediante el acceso a sistemas con el uso de diferentes protocolos (SSH, SMB, WMI, WinRM o DCOM), o técnicas como NTLMrelay, impersonificación de usuarios, etcétera.

Agenda (iv)

9. **Persistencia**: Conjunto de acciones y pautas para desplegar persistencia en puestos de usuario, equipos en DMZ y servidores internos, además de en el propio dominio. Esto implica el uso y despliegue de múltiples tipo de tunelización y uso de protocolos, servidores C&C, vectores alternativos para el acceso a la red mediante Wi-Fi, etcétera.

10. **Evasión de medidas de seguridad**: 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.

Material proporcionado

Al inicio los alumnos el temario completo, así como el laboratorio y herramientas. Concretamente se proporcionarán los siguientes materiales

- Disco duro con todo el entorno de pruebas virtualizado
- Dispositivo USB con un distribución Kon-boot
- Libro “CISO: El Red Team de la empresa”, de 0xWord

Adicionalmente durante el curso se proporcionará acceso personalizado a diferentes sistemas VPS y dominios públicos para el desarrollo de las pruebas planteadas.

Costes

- El precio final del Bootcamp + entrada al Congreso RootedCON es **1300 €**

- **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 **SEIS (6)** 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