/Rooted

Red Team Operations

MADRID

7 al 9 de Marzo de 2022

DOSIER DE FORMACIÓN

/Rooted

Días 7-9 de Marzo

Tres días de trainings y workshops

HOTEL Eurostars iHotel
Pozuelo de Alarcón

Días 10-12 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 dotar a los asistentes de capacidades para desarrollar ejercicios de intrusión y simulaciones reales de ataque, entendiendo el proceso, fases y acciones, así como las técnicas, herramientas y pautas para tener éxito en cualquier ejercicio independientemente de la organización objetivo.

Durante el transcurso de la formación, de 3 días de duración, los alumnos trabajaran todos los aspectos de una intrusión, desde el despliegue de la infraestructura necesaria y el reconocimiento de activos hasta acciones internas como el movimiento lateral entre sistemas, compromiso de la infraestructura y el despliegue de una completa red de persistencias internas.

El bootcamp tiene un claro objetivo de mostrar de forma práctica una metodología y técnicas útiles para desarrollar ataques dirigidos, motivo por el cual no se profundizará en técnicas que se salgan de ello.

A quién va dirigido

La formación no pretende servir de introducción al hacking ético, ya que el objetivo es profundizar en el desarrollo de técnicas avanzadas que permiten el desarrollo de intrusiones reales. Por ello, el bootcamp está enfocado especialmente a profesionales del sector de la Ciberseguridad, y especialmente a aquellos relacionados con la auditoria de seguridad y pentesting.

La formación también está abierta en cualquier caso, a todos aquellos que ya cuenten con 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

Profesor: Eduardo Arriols

- Fundador de SilentForce, una start-up especializada en servicios ofensivos de Ciberseguridad, y desarrollo de productos para la protección y gestión de la superficie de ataque en Internet.
- Más de 10 años de experiencia en seguridad ofensiva, y más de 6 años desarrollando y coordinando ejercicios Red Team sobre grandes organizaciones nacionales e Internacionales.
- Profesor de grado y postgrado en materia de Ciberseguridad para diversas universidades.
- Autor del libro "CISO: El Red Team de la empresa", de la editorial 0xWord.
- Ponente en congresos nacionales e internacionales tales como RootedCON, Navaja Negra, Jornadas STIC (CCN-Cert) o 8.8 Security Conference (Chile y Bolivia).
- Ingeniero Informático por la UAM y master en Ciberseguridad por la UOC.

Requisitos: Conocimientos

Conocimientos básicos de:

- ✓ Administración de sistemas con Windows o Linux.
- ✓ Programación en lenguajes tales como Bash scripting y Python.
- ✓ Funcionamiento y operativa de entornos Microsoft con Directorio Activo.
- ✓ Manejo de herramientas de hacking ético tales como Metasploit, Nmap, Sqlmap, …
- ✓ Explotación de vulnerabilidades en sistemas y redes.
- ✓ Explotación de vulnerabilidades web tales como SQL Injection, RCE o File Upload.

Requisitos: Técnicos

Para el correcto funcionamiento del training será necesario que los alumnos dispongan de equipos con acceso de administrador para poder añadir, eliminar software o cambiar cualquier configuración del mismo.

Las máquinas deben contar con las siguientes características mínimas:

- ✓ Acceso de administrador al equipo personal que será usado en el laboratorio.
- ✓ Capacidad de conexión por cable e inalámbrica.
- ✓ Capaz de ejecutar tres máquinas virtuales simultáneamente utilizando VMware Workstation / Player o VirtualBox.
- ✓ 120 GB de espacio libre en disco.
- ✓ Al menos 8GB de memoria RAM.

Agenda

1. Introducción
2. Despliegue y configuración de la infraestructura
3. Reconocimiento de activos
4. Compromiso inicial
5. Elevación de privilegios local
6. Persistencia en el sistema
7. Reconocimiento interno
8. Técnicas de movimiento lateral
9. Obtención de credenciales e impersonificación
10. Password cracking
11. Técnicas de pivoting interno
12. Control de la infraestructura
13. Persistencia completa en la organización
14. Bypass de medidas de seguridad

Se muestra a continuación una breve descripción sobre los conocimientos que serán adquiridos en cada módulo.

Detalles (i)

1. Introducción: Todo el conocimiento necesario sobre los detalles de la metodología y fases de la intrusión, planteamiento del modelo de amenazas y vectores potenciales según la organización, técnicas para la medición y análisis de las capacidades de detección y respuesta del Blue Team e importancia del OPSEC en ejercicios Red Team.

2. Despliegue y configuración de la infraestructura: Construcción de plataforma de anonimato para la ocultación de acciones, despliegue de sistemas C&C para la recepción de comunicaciones tunelizadas y persistencias, así como la compra y configuración de dominios categorizados para ataques dirigidos de Phishing.

3. Reconocimiento de activos: Conjunto de técnicas para mapear todos los activos sobre los que se desarrollarán las pruebas de intrusión para lograr un vector de acceso, poniendo especial énfasis en la detección de activos no controlados (Shadow IT) y priorización de activos, entornos en Cloud vulnerables y obtención de personal de la organización para el envio de malware dirigido.

Detalles (ii)

4. Compromiso inicial: Principales vectores de acceso en perímetro y tunelización mediante herramientas como reGeorg, ataques de password Spraying, evasión de 2FA, creación de phishing dirigidos, así como escenarios de malware con HTML Application (HTA) y VBA macros.

5. 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 la intrusión en la entidad.

6. Persistencia en el sistema: Conjunto de acciones para mantener el acceso a un sistema accedido. Se verán tanto técnicas de persistencia (Task Scheduler, Startup, AutoRUN, COM Hijacking y otras) como vías de comunicación con el C&C (TCP, HTTP, DNS, …).

7. Reconocimiento interno: Reconocimiento de los dominios internos para profundizar en la intrusión sobre la organización mediante herramientas como PowerView, SharpView, ADSearch o BloodHound entre otras.

Detalles (iii)

8. Técnicas de movimiento lateral: Técnicas para moverse entre equipos, redes y dominios internos mediante el acceso a sistemas, con el uso de los protocolos permitidos tales como SSH, SMB, WMI, WinRM o DCOM.

9. Obtención de credenciales e impersonificación: Obtención y uso de credenciales mediante técnicas como la extracción de credenciales locales y en memoria RAM, Domain Cached Credentials, Process Injection, Pass-the-hash y Overpass-the-hash, impersonificación, Extracción de tickets Kerberos, etcétera.

10. Password cracking: Análisis de diferentes técnicas (diccionarios, uso de reglas, mascaras, combinaciones y ataque híbridos) para la recuperación en claro de contraseñas tanto de forma local como en Cloud.

11. Técnicas de pivoting interno: Conjunto de acciones para el compromiso y acceso a otros sistemas internos mediante el uso de proxies socks, ataques en red mediante NTLM relay o redireccionamiento inverso de puertos.

Detalles (iv)

12. Control del la infraestructura: Principales técnicas para lograr el control sobre la infraestructura Microsoft mediante el uso de ataques como Kerberoast, ASREPRoast, DCSync, Silver y Golden tickets o uso de relaciones de confianza.

13. Persistencia en la organización: Conjunto de acciones para garantizar el acceso de forma persistente y a largo plazo en la organización, desplegando para ello una completa red de persistencias internas.

14. Bypass de medidas de seguridad: Conjunto de técnicas para evadir las medidas de seguridad existentes en la entidad, desde bypassing de antivirus y AppLocker hasta técnicas de inyección de código en memoria.

Costes

- El precio final de este **Bootcamp + entrada** al Congreso RootedCON es **1200 €**

- **Puedes registrarte y formalizar el pago en: https://reg.rootedcon.com**

IMPORTANTE:

Se requiere un mínimo de **CINCO (5)** asistentes para que el curso pueda celebrarse.

/Rooted

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: https://reg.rootedcon.com. 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.
- 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