/Rooted

# Red Team Operations

**MADRID**

6 al 8 de Marzo de 2023

**DOSIER DE FORMACIÓN**

/Rooted

**Días 6-8 de Marzo**

*Tres días de trainings y workshops*

*HOTEL Eurostars iHotel*
*Pozuelo de Alarcón*

**Días 9-11 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).

# Profesor: Eduardo Arriols

- CEO y Offensive Director en SilentForce, una start-up especializada en Adversarial Simulation y desarrollo de productos para la protección y gestión de la superficie de ataque en Internet.
- Más de 12 años de experiencia en seguridad ofensiva, y más de 8 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.

# 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. Se proporcionará a los alumnos un laboratorio tanto en local como en Cloud sobre el que simular todas las técnicas aprendidas.

# 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, así como cualquiera que esté interesado en aprender y profundizar en el desarrollo de ejercicios Red Team.

# Requisitos: Conocimientos

Conocimientos básicos de:

- ✔ Administración y manejo de sistemas Windows o Linux.
- ✔ Programación básica 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, …
- ✔ Proceso de intrusión y explotación de vulnerabilidades en sistemas y redes.
- ✔ Explotación de vulnerabilidades web tales como SQL Injection, XSS, RCE o File Upload.

Para el máximo aprovechamiento de la formación, se proporcionará antes del inicio material teórico sobre el desarrollo de los ejercicios y aspectos básicos que el alumno deberá leer.

# 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 y metodología
2. Despliegue y configuración de infraestructura
3. Reconocimiento de activos
4. Compromiso inicial
5. Reconocimiento del equipo comprometido
6. Elevación de privilegios local
7. Obtención de credenciales
8. Password Cracking
9. Movimiento lateral
10. Reconocimiento del AD y Azure AD
11. Compromiso de la infraestructura interna
12. Despliegue de persistencia

Los puntos 1 y 3 se verán de forma más rápida al haber proporcionado al alumno el material, centrando así la formación en los aspectos más técnicos. Si se contara con tiempo se podrá incluir material adicional sobre el análisis de las capacidades de detección y respuesta o evasión de medidas de seguridad.

# Agenda (i)

**1. Introducción**: Todo el conocimiento necesario sobre los detalles de la metodología y fases de la intrusión, Threat y Breach model, vectores potenciales según la organización, técnicas para la medición y análisis de las capacidades de detección y respuesta del Blue Team, así como aspectos a tener en cuenta respecto del OPSEC en ejercicios Red Team.

**2. Despliegue y configuración de la infraestructura**: Detalles, pautas y metodología para la construcción de infraestructura de enumeración, intrusión, persistencia y anonimato en Cloud. Se profundizará en el desarrollo de una plataforma de anonimato para la ocultación de acciones, despliegue de sistemas C&C para la recepción de comunicaciones tunelizadas y persistencias, así técnicas como Domain Fronting o IP Laundry.

**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.

# Agenda (ii)

**4. Compromiso inicial**: Principales vectores de acceso en perímetro y tunelización mediante herramientas como reGeorg / NeoRegeorg, ataques de password Spraying, evasión de 2FA, spoofing de servicios en Internet, ataques mediante malware y creación de escenarios de phishing dirigidos.

**5. Reconocimiento del equipo comprometido**: Conjunto de técnicas y pautas para lograr acceso a la red interna desde el equipo comprometido evitando la identificación de posibles medidas de seguridad establecidas tales como AV, EDR, IDS o Honeypots entre otros.

**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 la intrusión en la entidad.

# Agenda (iii)

**7. Obtención de credenciales**: Conjunto de técnicas para lograr la obtención de credenciales durante el proceso de intrusión, tales como obtención de claves mediante archivos locales, DPAPI, claves, hashes y tickets en memoria o spoofing de servicios tanto a nivel local como en red.

**8. Password cracking**: Análisis de diferentes técnicas (diccionarios, uso de reglas, mascaras, combinaciones y ataque híbridos) para la recuperación en claro de contraseñas. Se profundizará en la construcción de entornos en Cloud optimizados y escenarios reales de cracking mediante la combinación de técnicas.

**9. Movimiento lateral:** Conjunto de técnicas de acceso 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. Se analizarán las diferentes técnicas posibles según el nivel de credenciales obtenidos (pass-the-hash, overpass-the-hash, pass-the-ticket, …). Adicionalmente se analizarán las técnicas de compromiso y movimiento lateral en MSSQL.

# Agenda (iv)

**10. Reconocimiento del Directorio Activo y AAD**: Reconocimiento de los dominios internos y Azure AD para profundizar en la intrusión sobre la organización mediante herramientas como PowerView, SharpView, ADSearch o BloodHound entre otras.

**11. Compromiso de la infraestructura interna**: Principales técnicas para lograr el control sobre la infraestructura Microsoft mediante el uso de ataques como Kerberoast, ASREPRoast, Unconstrained/Contraned Delegations, Alternate Service Name, Linux Cache Credentials, DACLs o relaciones de confianza entre otros.

**12. Despliegue de persistencia**: Técnicas para el despliegue de persistencia sobre la organización en todos los niveles (sistemas internos, Directorio Activo, DMZ, Cloud y técnicas alternativas). Se profundizará tanto en las técnicas para mantener persistencia, como las vías de comunicación o uso de dichas persistencias. Así mismo, se trabajará en el desarrollo de una infraestructura propia de persistencias que permita el desarrollo de ejercicios a largo plazo.

# Costes

- El precio final de este **Bootcamp + entrada** al Congreso RootedCON es **1250 €**

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

**IMPORTANTE:**

Se requiere un mínimo de **SEIS (6)** asistentes para que el curso pueda celebrarse.

# 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