/Rooted

RED TEAM Operations

Eduardo Arriols

Valencia 2022

DOSSIER DE FORMACIÓN

/Rooted

Valencia 2022

Ponencias presentadas por speakers internacionales y expertos técnicos.

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 RootedLAB 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, los alumnos trabajaran los principales aspectos para desarrollar una intrusión, desde el reconocimiento de activos en perímetro, hasta acciones internas como el movimiento lateral entre sistemas, reconocimiento y análisis del Directorio Activo, y compromiso de la infraestructura.

El RootedLAB 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. Otros perfiles que objetivo de la formación son:

- Estudiantes
- Desarrolladores y Administradores de sistemas y/o redes
- Cuerpos y Fuerzas de Seguridad
- Cualquiera que esté interesado en aprender técnicas de 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.

/Rooted

Contenido

Agenda (i)

1. Introducción y conceptos base: 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. Reconocimiento de activos en perímetro: 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)

3. Vectores de acceso y 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.

4. Obtención de credenciales y password cracking: 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. Posteriormente se analizarán 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.

Agenda (iii)

5. Técnicas de movimiento lateral y pivoting: 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. Así mismo, serán analizadas técnicas útiles como NTLMrelay o robo de sesiones.

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

7. 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.

Costes

- El precio final del Lab será de 125 euros

IMPORTANTE: Se requiere un mínimo de **SEIS (6)** asistentes para que el Lab pueda llevarse a cabo.

FAQ

- Dónde se celebra la formación?
  - A diferencia del Congreso RootedCON, las formaciones se celebran en la ADEIT - Fundación Universidad-Empresa. Dirección: Plaza Virgen de la Paz, 3. Valencia.
- Qué horario tiene la formación?
  - La formación comienza a las 9:00 de la mañana, pero procura estar un poco antes para poder acreditarte y tener tu portátil preparado.
  - 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.
- 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