Red Team Operations (One day edition)

VALENCIA

15 de Octubre de 2024

DOSSIER DE FORMACIÓN

/Rooted

Valencia 2024

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).

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 13 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, los alumnos trabajarán 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 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 (las máquinas serán proporcionadas en .ova).
- ✔ 120 GB de espacio libre en disco.
- ✔ Al menos 8GB de memoria RAM.

Agenda

1. Introducción y conceptos base
2. Reconocimiento de activos en perímetro
3. Vectores de acceso y compromiso inicial
4. Obtención de credenciales y password cracking
5. Técnicas de movimiento lateral y pivoting
6. Reconocimiento interno del Directorio Activo
7. Ataques y control de la infraestructura interna
8. Bypass de medidas de seguridad con IA

La formación se centrará y profundizará en aquellas técnicas novedosas o que realente cuenten con un amplio uso dentro del desarrollo de escenarios de intrusión actualmente. Se proporcionará acceso a los asistentes a herramientas privadas de SilentForce para la automatización de acciones durante el proceso de intrusión.

Detalles (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. 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 envío de malware dirigido. Se proporcionará acceso al servicio ATLAS de SilentForce para el desarrollo del reconocimiento.

Detalles (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), VBA macros, Remote Template Injection o HTML Smuggling entre otros.

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, máscaras, combinaciones y ataque híbridos) para la recuperación en claro de contraseñas tanto de forma local como en Cloud. Se proporcionará acceso a la herramienta Cerberus de SilentForce.

Detalles (iii)

5. Técnicas de movimiento lateral y pivoting: 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.

6. Reconocimiento interno del Directorio Activo: 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. Se analizarán múltiples técnicas nativas para desarrollar el proceso sin la identificación de medidas de seguridad.

Detalles (iv)

7. Control de la infraestructura: 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.

8. Bypass de medidas de seguridad con IA: Uso de servicios como ChatGPT para la generación de scripts que permitan la evasión de sistemas de seguridad como Antivirus o EDR, automatización de acciones ofensivas, etcétera. Se mostrarán diferentes casos de uso llevados a cabo por el equipo de SilentForce en intrusiones recientes.

Costes

- El precio final de este **RootedLAB** es de 175**€**

- **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.

FAQ

1. ¿Dónde se celebra la formación?
   - Las formaciones se celebran en el edificio del ADEIT Fundación Universidad – Empresa de la Universidad de Valencia.
   - Plaza Virgen de la Paz, 3 46001 Valencia
   - ¿Qué diferencia hay entre BootCamp y RootedLab?
   - Diferenciamos los trainings por horas de formación. Un **RootedLab tiene 8 horas** de formación, mientras que un **BootCamp tiene unas 24h**.
2. ¿Qué horario tiene la formación?
   - La formación comienza a las 9:00h de la mañana, pero procura estar un poco antes para poder acreditarte y tener tu portátil preparado. El primer día recomendamos estar a las 8:30h.
   - Las formaciones suelen acabar entre las 18:00h y 19:00h.
3. ¿Cómo puedo registrarme?
   - Para el registro, ve directamente al Rooted Manager: 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.
4. ¿Puedo pagar con transferencia bancaria?
   - Si, desde el propio Rooted Manager podrás gestionar el pago mediante transferencia bancaria.
5. ¿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