Mi primera revisión de Directorio Activo desde un punto de vista ofensivo

MADRID

6 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: Jorge Escabias

Graduado en Ciencias Matemáticas por la Universidad Complutense de Madrid y Máster en Ciberseguridad por la UNIR. Es Team Leader en Zerolynx y cuenta con un dilatado conocimiento en Red Team, exploiting y pentesting sobre entornos de Directorio Activo. Posee las principales certificaciones del mercado como el OSCP y el OSCE de Offensive Security, el CRTO de ZeroPointSecurity y el CRTE de Pentester Academy. Actualmente es el responsable del equipo de seguridad ofensiva de Zerolynx y encargado de ejecutar proyectos de Red Team, pentest y auditorías de seguridad. Anteriormente se ha encargado de realizar las labores de auditoría anuales y pentesting en un cliente de seguros multinacional, labores de hacking para otros clientes y de Threat Hunting, junto al despliegue e integración de los diferentes elementos de seguridad defensiva pertenecientes a un centro de operaciones (SOC).

Ha participado como ponente en las XV Jornadas del CCN-CERT,en la RootedCON y en la NoCon. También, impartirá el taller “Creando tu propio bypass de AMSI” en la HackplayersCon del 2023.

Objetivos

En esta formación, orientada a un primer contacto sobre entornos de Directorio Activo desde una perspectiva de un atacante, los asistentes podrán conocer todos los puntos necesarios para realizar una revisión de seguridad sobre este tipo de entornos. A lo largo del taller, los asistentes conocerán qué es y por qué elementos está formado un Directorio Activo, cómo enumerar estos entornos; conocerá las vulnerabilidades y fallos de configuración más comunes y sencillos que se pueden encontrar y entenderán los riesgos que pueden implicar en sus respectivas organizaciones. Además, dispondrán del conocimiento necesario para corregir (o mitigar) estas vulnerabilidades en entornos reales.

Además, los asistentes también tendrán oportunidad de emplear herramientas legítimas ampliamente utilizadas por los auditores de seguridad para realizar reconocimiento, detectar y explotar las vulnerabilidades durante sus ejercicios de pentest.

Por último, todos los asistentes podrán poner a prueba el conocimiento adquirido en un entorno controlado mediante la realización de determinados ejercicios siguiendo la modalidad CTF, ampliamente extendida en el sector de la ciberseguridad. Este entorno es propio y se divide en dos partes: una primera parte guiada con una serie de objetivos sencillos predefinidos y una segunda parte más libre orientada a la competición entre los participantes.

A quién va dirigido

- Profesionales del sector de la Ciberseguridad sin conocimiento en auditoría de Directorio Activo: pentesters, auditores, analistas de ciberseguridad, threat hunters…
- Administradores de sistemas y/o redes especializados en Directorio Activo.
- Estudiantes.
- Docentes.
- Cuerpos y Fuerzas de Seguridad.
- Cualquiera que esté interesado en aprender sobre Directorio Activo desde un punto de vista ofensivo y defensivo partiendo desde cero.

Requisitos: Conocimientos

Conocimientos básicos de:

- ✔ Funcionamiento TCP/IP
- ✔ Conocimiento básico de PowerShell
- ✔ Entornos Microsoft
- ✔ Uso básico de Windows/Linux

Importante: no es necesario disponer de conocimientos previos (más allá de los indicados arriba), el taller cubre lo básico y no es indispensable disponer de base técnica. Todo lo necesario se abarcará en el taller.

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:

- ✔ Capacidad para ejecutar dos máquinas virtuales de manera simultánea.
- ✔ Muy recomendable disponer de SSD para la ubicación de las máquinas virtuales.
- ✔ Mínimo de 8 GB de RAM.
- ✔ Tener instalado VirtualBox o VMWare.
- ✔ Máquina Linux o Parrot Security virtualizada.

Contenido

En este laboratorio, organizado en dos secciones, se estudiarán los vectores de ataques más comunes que se pueden identificar en un entorno de Directorio Activo. En el primer apartado teórico-práctico, se darán a conocer estos fallos de configuración, se explicará cómo identificarlos, cómo explotarlos y cómo corregirlos o mitigarlos. En la segunda sección, se facilitará un entorno simulando una empresa en la que los alumnos pondrán en práctica todo el conocimiento adquirido en la primera sección con el objetivo de alcanzar los mayores privilegios siguiendo la modalidad de CTF.

Un día entero orientado a la ejecución de una auditoría interna centrada exclusivamente en entornos de Directorio Activo para desarrollar tus capacidades de pentesting/Red Team.

Agenda (i)

Módulo I - Breve introducción a Windows Active Directory

- ✔ Qué es un Directorio Activo
- ✔ Agrupación de un Directorio Activo
- ✔ Protocolos de un Directorio Activo
- ✔ Estructura y elementos de un Directorio Activo
- ✔ Objetos principales, GPOs y ACLs

Módulo II - PowerShell: Uso y manejo desde un punto de vista ofensivo

- ✔ Qué es PowerShell
- ✔ Conceptos básicos

Agenda (ii)

Módulo III - Reconocimiento y enumeración en un Directorio Activo

- ✔ Estructura de un Controlador de Dominio
- ✔ Enumeración básica con comandos nativos de Windows

Módulo IV - Abusos básicos y vulnerabilidades clásicas de un Directorio Activo

- ✔ Secretos en parámetros de objetos
- ✔ Enumeración de carpetas compartidas
- ✔ Password Spraying
- ✔ Replicación de cuentas

Agenda (iii)

Módulo V - Cómo desplazarse por un Directorio Activo: técnicas comunes de movimiento lateral

- ✔ Protocolos nativos de Windows de administración remota
- ✔ Repaso de las principales herramientas: usos y condiciones

Módulo VI - Laboratorio práctico donde poner a prueba lo comentado.

- ✔ Laboratorio emulando un Dominio de Windows con varias máquinas para realizar una serie de ejercicios prácticos con el objetivo de afianzar los conocimientos explicados durante el taller. Se trata de un entorno controlado donde poder ejecutar comandos y herramientas, así como, familiarizarse con entornos de Directorio Activo.

Costes

- El precio final de este **RootedLAB** es **250 €**

- **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