/Rooted

# Introducción al pentesting sobre entornos de Directorio Activo

Jorge Escabias, Helena Jalain y Luis Vázquez

**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

En esta formación, orientada a las auditorías sobre entornos de Directorio Activo, 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 las vulnerabilidades y fallos de configuración más comunes que se pueden encontrar en un Directorio Activo y entenderán los abusos que se pueden realizar. Además, dispondrán del conocimiento necesario para corregir (o mitigar) estas vulnerabilidades en entornos reales.

Durante el curso, los asistentes también tendrán oportunidad de emplear herramientas ampliamente utilizadas por los auditores de seguridad para detectar y explotar las vulnerabilidades durante sus ejercicios de pentest, como PowerView, BloodHound, Mimikatz, Rubeus o SharpDPAPI, para entender y poner en práctica toda la teoría tratada. Además, se realizará un pequeño apartado para realizar mecanismos de evasión de AMSI.

Por último, todos los asistentes podrán poner a prueba el conocimiento adquirido en un entorno controlado siguiendo el formato CTF.

# A quién va dirigido

- Profesionales del sector de la Ciberseguridad: 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.

# Profesores: 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 se encarga de realizar las labores de auditoría anuales y pentesting en un cliente de seguros multinacional. Anteriormente ha realizado 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 sido ponente en las XV Jornadas del CCN-CERT con su taller “Creando y automatizando tu propio laboratorio de Directorio Activo”.

# Profesores: Helena Jalain

Ingeniera de Telecomunicación por la Universidad Politécnica de Madrid. Es auditora de ciberseguridad senior en Zerolynx. Posee más de seis años de experiencia en investigación, consultoría de ciberseguridad y servicios técnicos de seguridad ofensiva, entre los que se incluyen auditorías internas de redes e infraestructura y pentesting web. Posee las certificaciones CEH y OSCP.

Ha participado también en diversos proyectos de operaciones de seguridad y desarrollo seguro para clientes a nivel nacional e internacional. Comenzó como investigadora en el grupo de Redes y Servicios de Telecomunicación e Internet (RSTI) en la Universidad Politécnica de Madrid, y estuvo trabajando en el Cyberlab de KPMG España.

Ha participado como ponente en varias conferencias de seguridad, entre las que destacan RootedCON 2019 y Mundo Hacker Day 2019.

# Profesores: Luis Vázquez

Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid. Es auditor de ciberseguridad senior en Zerolynx, contando con más de seis años de experiencia en roles ofensivos en todo tipo de proyectos, tanto de pentesting de aplicaciones como de redes y sistemas IT, habiendo realizado una gran cantidad de auditorías de redes Windows en clientes del IBEX 35 y NASDAQ. Anteriormente ha trabajado en el Cyberlab de KPMG España, como consultor de ciberseguridad, y en el grupo de Redes y Servicios de Telecomunicación e Internet (RSTI) de la Universidad Politécnica de Madrid, como investigador de ciberseguridad.

Posee las certificaciones CEH y OSCP, ha participado como ponente en varios congresos de seguridad y ha descubierto y publicado múltiples vulnerabilidades, como CVE-2020-28210, CVE-2020-8967, CVE-2021-40850 y CVE-2021-40851.

# Requisitos: Conocimientos

Conocimientos básicos de:

- ✓ Entornos Windows
- ✓ Funcionamiento TCP/IP
- ✓ Protocolos de red comunes
- ✓ Sistemas Operativos

# Requisitos: Técnicos

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

Dicho equipo deberá contar con las siguientes características:

- ✓ Capacidad para ejecutar dos máquinas virtuales (en VirtualBox o VMWare) de manera simultánea:
  - ✓ W10 (evaluación).
  - ✓ Kali Linux/Parrot Security con CrackMapExec e Impacket instalado.
  - ✓ BloodHound instalado en cualquiera de ambas máquinas.
- ✓ Mínimo de 8 GB de RAM.
- ✓ Tener unos 100 GB de espacio en disco duro suficiente para disponer de 2 máquinas virtuales. Muy recomendable disponer de SSD para no tener problemas de rendimiento.

# Contenido

En este laboratorio, organizado en dos secciones, se estudiarán los vectores de ataque 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 el acceso a un entorno de pruebas simulando una red empresarial en la que los alumnos pondrán en práctica todo el conocimiento adquirido en la primera sección con el objetivo de alcanzar los máximos privilegios siguiendo la modalidad de CTF.

# Agenda (i)

1. Breve introducción AD
2. Breve introducción PowerShell
   a) Funcionamiento PowerShell
   b) Políticas de ejecución de PowerShell
   c) Importar Módulos
   d) Pequeños consejos de uso
3. Evasión de AMSI
4. Técnicas de enumeración de dominios
   a) BloodHound
   b) ADRecon
   c) PowerView

# Agenda (ii)

5. Vulnerabilidades clásicas de AD: Explicación y explotación
   a) Kerberoast
   b) Asreproast
   c) ACLs
   d) Fallos de configuración comunes

6. Movimiento lateral
   a) Impacket
   b) PowerShell Remoting
   c) Evil-WinRM

# Agenda (iii)

7. Extracción de secretos
   a) DPAPI
   b) Secretsdump
   c) Mimikatz
8. Persistencia
   a) Golden Ticket
   b) Silver Ticket
9. Defensas/Remediaciones
10. Laboratorio
    a) CTF: Tu primera revisión de AD

# 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 **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