Bootcamp de ataques al Directorio Activo

Madrid 3,4 y 5 de Marzo de 2025

DOSSIER DE FORMACIÓN

/Rooted

Del 3 al 5 de Marzo

Tres días de trainings y Workshops

HOTEL Eurostars iHotel
C. de Virgilio, 4, 28223, Madrid
Pozuelo de Alarcón

Del 6 al 8 de Marzo

Ponencias presentadas por speakers internacionales y expertos técnicos.

KINEPOLIS Ciudad de la Imagen
C. Edgar Neville, s/n
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 eventos).

Profesor: Alex Amorín

Alex Amorín es responsable de Pentesting y Red Team en Zerolynx. Ingeniero Informático por la Universidad de Burgos y Máster en Seguridad de las TIC por la Universidad Europea.

Posee certificaciones de seguridad ofensiva como OSCP, OSWP, OSWE, OSEP, OSED, CRTO, CRTL, OSCE3 y más de 25 CVE publicados.

Profesor: Axel Losantos

Axel es Pentester y Operador de Red Team con más de cuatro años de experiencia en ciberseguridad, habiendo trabajado en proyectos internacionales en sectores como bancario, farmacéutico, seguros y administración pública.

Es Técnico Superior en Desarrollo de Aplicaciones Multiplataforma (DAM), Grado en Ingeniería Informática y Máster en Ciberseguridad, ambas por la UNIR y posee certificaciones de seguridad ofensivas como OSCP, OSEP, OSWE, CRTO, CRTL, CRTP, CRTE, CARTP, CARTE, ARTE, eCPPTv2 y CHMRTS.

Objetivos

Este taller proporciona una comprensión integral sobre cómo auditar y explotar un Directorio Activo. Los participantes aprenderán a identificar configuraciones inseguras, explotar vulnerabilidades conocidas, realizar movimientos laterales, y aplicar técnicas avanzadas para comprometer y mantener persistencia en AD. Además, el enfoque práctico permitirá a los asistentes desarrollar sus habilidades probando en entornos simulados realistas.

A quién va dirigido

El taller está diseñado para profesionales de ciberseguridad, administradores de sistemas, analistas y auditores de seguridad interesados en aprender sobre pentesting de AD. Es adecuado tanto para principiantes que quieran iniciarse en la seguridad de AD como para usuarios intermedios que deseen profundizar en técnicas avanzadas de explotación y persistencia.

Requisitos: Conocimientos

- Familiaridad básica con redes, protocolos (TCP/IP, SMB, LDAP).
- Conocimiento introductorio de Windows Server y Directorio Activo.
- Experiencia básica en uso de herramientas como PowerShell y línea de comandos.
- Nociones de scripting o programación (deseable).

Requisitos: Técnicos

Se necesita un equipo capaz de virtualizar dos máquinas virtuales con al menos 1 procesador y 4 GB de RAM cada una.

Guía de Contenidos I

Sesión 0 – Configuración y explicación del entorno

Sesión 1 - Introducción a Active Directory y Reconocimiento
Objetivos: Introducción a los conceptos básicos de Active Directory (AD), la estructura lógica y física de AD, los protocolos clave y la kill chain asociada con la enumeración y reconocimiento de AD.

- Conceptos Básicos de Active Directory
- Fundamentos de GPOs y ACLs
- Kill Chain en Active Directory

Sesión 2 – Enumeración básica de Active Directory
Objetivos: Profundizar en el uso de PowerShell y protocolo LDAP para automatizar la administración y explotación de Active Directory

- Introducción a PowerShell y LDAP
- Enumeración de AD

Sesión 3 - Enumeración avanzada de Active Directory
Objetivos: Profundizar en herramientas avanzadas y técnicas para realizar un reconocimiento exhaustivo en AD, usando herramientas automáticas y técnicas manuales de enumeración.

- Herramientas Internas: RSAT, AD Explorer y ADSI Edit
- Introducción a las herramientas nativas de Windows para interactuar con Active Directory.
- BloodHound y SharpHound
- Explicación de cómo funciona BloodHound y SharpHound para mapear relaciones de confianza en AD.
- Enumeración manual avanzada
- Técnicas avanzadas de enumeración de SMB, GPOs y Sysvol.
- Técnicas de movimiento lateral
- Uso de CrackMapExec/NetExec para interactuar con máquinas en la red y ejecutar comandos en remoto.

Guía de Contenidos II

Sesión 1 - Explotación de vulnerabilidades en AD

Objetivos: Explorar técnicas de explotación y cómo obtener acceso a máquinas dentro de un dominio de AD.

- Exploits comunes en AD
- Ataques conocidos (MS17-010, MS14-025, Kerberoasting, ASREP-Roasting, ZeroLogon, ProxyLogon, ProxyShell)
- Escalada de privilegios local
- PowerUp: Exploits para escalar privilegios
- JuicyPotato: Escalada usando vulnerabilidades de DCOM
- Abuso de servicios y fallos de configuración

Sesión 2 – Abusos de malas configuraciones en AD

Objetivo: Identificar y explotar configuraciones incorrectas o inseguras dentro de un entorno de AD

- ACLs
- LAPS
- gMSA - Group Managed Service Account
- Ataques a MSSQL
- Constrained Delegation
- Unconstrained Delegation
- RBCD
- Extracción de secretos Avanzado

Guía de Contenidos III

Sesión 1 – Técnicas avanzadas de ataque en AD

Objetivo: Obtener los conocimientos necesarios para ejecutar ataques avanzados en AD, especialmente en relación con la manipulación de credenciales, ataques a la infraestructura de certificados (ADCS), etc.

- ADCS
- Shadow credentials y ataques a SPN
- sAMAccountName spoofing

Sesión 2 – Ataques avanzados

Objetivo: Conocer técnicas avanzadas de ataque que permiten a los atacantes obtener acceso a sistemas y servicios utilizando credenciales y tokens de autenticación en situaciones en las que normalmente estarían protegidos.

- Técnicas de Forced Authentication
- Técnicas de Relay (+Forced Authentication)

Sesión 3 – Persistencia en AD

Objetivo: Conocer técnicas de persistencia avanzadas

- Técnicas de persistencia avanzadas: backdoors en GPOs, cuentas shadow admin, modificación de AD

FAQ

1. ¿Dónde se celebra la formación?
   - Las formaciones se celebran en Eurostars I-hotel C/Virgilio,4 28223, Pozuelo de Alarcón (Madrid)
   - Aquí puedes encontrar el mapa de la zona: **https://goo.su/mzpYRaE**
   - ¿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 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.
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