
OSINT OFENSIVO
PARA RED TEAMERS

¿Sos un apasionado del pen testing y te gustaría aventurarte en el mundo del Red Team?

Entonces este curso es para vos.

El nuevo curso **“OSINT Ofensivo para Red Teamers”**, forma parte del track de cursos y certificaciones relacionadas con Red Team que te ayudaran a convertirte en Red Team Operator.

Verás en profundidad todos los conceptos del mundo de OSINT e inteligencia de fuentes abiertas que se pueden aplicar, con una orientación netamente ofensiva (relacionada a los Pentest y al Red Team), para generar inteligencia accionable, sobre la infraestructura objetivo, como para la construcción de pretextos creíbles en campañas relacionadas a escenarios de Red Team.

El curso está orientado a Pentesters, Operadores de Red Team, estudiantes de Sistemas, Analistas de Seguridad Informática, Jefes y/o CISOs que quieran profundizar sus conocimientos y cualquier persona con curiosidad y pasión por la tecnología y la seguridad.

Es un curso orientado a la práctica por lo que está diseñado para ser 30% Teórico y 70 % de Práctico, generando un enfoque en dónde el asistente, al finalizar el mismo, conozca y pueda aplicar los conocimientos adquiridos a su labor.

Al finalizar este curso el asistente será capaz de:

• Entender los principales conceptos de Inteligencia, fuentes abiertas y flujo de OSINT, como ciclo de recolección de datos e inteligencia.

• Entender como mapear las actividades de OSINT, con las correspondientes fases del Ciber kill chain, así como los TTPs de la matriz de Mitre Att&ck.

• Navegar TTPs de la matriz de Mitre y como identificar los TTPs asociados a las actividades de OSINT.

• Comprender los principales conceptos del buscador google, y el uso en profundidad de muchos de sus operadores avanzados (google dorks) para la búsqueda de datos sensibles de una organización.

• Crear tableros y alertas de google personalizadas con Google CSE.

• Llevar adelante actividades de SOCMINT, aplicándolo a people information gathering y persona development.

• Mapear la infraestructura del objetivo, utilizando diferentes técnicas y herramientas open source, tanto para infraestructura on-premise, como cloud y los TTPs de target selection, spoofing y technical information gathering asociados a esta actividad.

MÓDULOS

01

CONCEPTOS DE OSINT E INTELIGENCIA

En este módulo se hará una breve introducción a los conceptos de OSINT e inteligencia y su flujo de trabajo, como así también, un entendimiento conceptual de los tipos de fuentes.

02

OSINT AL SERVICIO DEL ENGAGEMENT

En el módulo 2 se relacionarán los conceptos de OSINT con las tácticas, técnicas y procedimientos (TTP's) de la matriz Mitre Attack (y la ex Pre-Attack), considerando también su relación con las primeras fases del Cyberkill Chain, para la planificación del engagement de Red Team.

Estos TTPs guiaran las actividades de OSINT posteriores, focalizando los esfuerzos en los objetivos buscados.

Se trabajará en relación a la explotación de OSINT, para la construcción de pretextos que formen parte de los ataques a realizar (ej.: ataques de spearpishing personalizados).

03

GOOGLE HACKING PARA RED TEAMERS

En este módulo abordaremos el funcionamiento del buscador google, para luego usarlo en nuestro favor para encontrar información sensitiva tanto a nivel de personas, cómo de infraestructura e información.

También se trabajará con algunas herramientas cómo la Google Hacking Database y Google CSE para el armado de nuestros dashboards de búsqueda y alarmas.

04

LAS PERSONAS COMO ACTIVO DE LA INFORMACIÓN A ENUMERAR Y EXPLOTAR

Las personas como parte de los activos de la empresa u organización.
SOCMINT como sub ciclo de inteligencia para el OSINT.
Personas target o de interés en la organización objetivo.
Búsqueda de información de la organización target, personal de interés de la misma, posibles adquisiciones, etc.

El flujo de OSINT y sus diferentes fases de inteligencia para enumeración y perfilación de personal clave.
Búsqueda de correos corporativos y leaks públicos de contraseñas.
Perfilación y scraping de redes sociales.
Operadores avanzados en redes sociales clave y armado de dashboards de monitoreo.

05

OSINT PARA RECON Y MAPEO DE INFRAESTRUCTURA DE ORGANIZACIONES

En este módulo final utilizaremos OSINT como fuente de information gathering pasivo, manual y automatizado, en relación a la búsqueda y recolección de datos de la infraestructura de una compañía u organización objetivo, como ser:

- Búsqueda de bases de datos públicas de registros whois.
- Técnicas de búsqueda a través de la línea de comando de la Bash Shell.
- Búsqueda de ASN y bloques IP asociados.
- Flujos de búsqueda de dominios y sub dominios tanto a través de scraping, cómo de brute force.
- Búsquedas de Reverse Whois.
- Búsqueda y enumeración de Tenant de Azure y los tipos de autenticación que utilizan.
- Búsqueda de Buckets públicos en cloud.
- Búsqueda de Github leaks.

CONOCIMIENTOS NECESARIOS

No se requiere tener experiencia o conocimiento de conceptos de OSINT ya que los mismos serán explicados rápidamente en el inicio del curso. Será necesario que los asistentes tengan un manejo básico tanto de Linux y el uso de la consola por línea de comando (Bash Shell), cómo de Windows y su respectiva línea de comando (CMD), ya que en muchos de los ejercicios en los que el alumno tendrá que trabajar a lo largo del curso serán, de acuerdo al escenario y herramienta a utilizar, en un entorno de sistema operativo u otro.

Es recomendable tener una experiencia mínima en el uso y creación de máquinas virtuales (VM) a través de Virtual Box o VMWare ya que se requerirá a lo largo del curso que el alumno utilice una VM con la distribución de Kali Linux para ciertos ejercicios.

EQUIPAMIENTO NECESARIO

El alumno necesita contar con un equipo PC o Notebook con al menos 4GB de Memoria RAM (Recomendamos 8GB para una mejor experiencia con la máquina virtual y ciertas herramientas) y unos 40GB de espacio en disco libres para poder levantar la máquina virtual, como así también, la instalación de algunas herramientas adicionales.

cursos@blackmantisecurity.com
+54 911 58101244 @Blackmantisec