
NetHunter Academy
Telegram: @nethunteracademy | TikTok: @nethunter.academy | YouTube: @NetHunter_Academy

Índice del Curso Google Hacking Mastery: Dorks, OSINT, Python y Herramientas Automatizadas para la Dark Web.

✅ Introducción al Curso de Google Hacking:

En este curso, exploraremos el fascinante mundo del **Google Hacking**, una técnica avanzada utilizada para descubrir información oculta en la web mediante motores de búsqueda. Aprenderás cómo utilizar **Google Dorks** y otros motores de búsqueda avanzados para realizar investigaciones en **OSINT**, auditorías de seguridad y pruebas de penetración. A través de módulos prácticos y teóricos, descubrirás cómo localizar archivos sensibles, dispositivos expuestos y vulnerabilidades web, utilizando técnicas legales y éticas.

Al final del curso, tendrás las habilidades necesarias para identificar información oculta, automatizar consultas con herramientas avanzadas y aplicar **Google Hacking** en escenarios de ciberseguridad, todo mientras implementas buenas prácticas para proteger tu propia información y la de las organizaciones.

¡Prepárate para sumergirte en el mundo del hacking ético y mejorar tus habilidades en seguridad informática!.💻🏁☢️

Índice del Curso.

Módulo 3: Dominando los Google Dorks.

- Operadores básicos de búsqueda avanzada en Google.
- Filtrado de información con operadores booleanos.
- Google Dorks para encontrar archivos sensibles (**PDF, XLS, DOC**, etc.).
- Extracción de información de sitios web con estructuras de URL específicas.
- Uso de Dorks para descubrir directorios y paneles de administración expuestos.

Módulo 4: Google Hacking en la Ciberseguridad:

- Identificación de bases de datos expuestas mediante Dorks.
- Encontrar credenciales y configuraciones sensibles con Google.
- Indexación de cámaras de seguridad accesibles desde Google.
- Uso de Google Hacking en auditorías de seguridad y **pentesting.**

Módulo 5: Automatización y Herramientas para Google Hacking

- **Bingoo** – Automatización de consultas con Google Dorks.
- **Dorks-Eye** – Extracción y uso de dorks desde GitHub.
- **ExifTool** – Extracción de metadatos en imágenes y documentos.
- **SpiderFoot** – Reconocimiento y análisis automatizado de información.
- **Dorksearch** – Búsqueda de dorks en una plataforma en línea.
- **Exploit-DB** – Base de datos de exploits y vulnerabilidades mediante dorks.
- **Cxsecurity** – Recolección de dorks y análisis de vulnerabilidades.
- **Script en Python** – Automatización de scraping con dorks en motores de búsqueda.
- **Script en Python** – Exploración de la Dark Web y obtención de información.

Módulo 6: Técnicas Avanzadas y Búsqueda en Sistemas Conectados y la Deep Web.

1. Motores de búsqueda enfocados a sistemas conectados:

- **Censys** - Herramienta para descubrir dispositivos y servicios expuestos a Internet.
- **Shodan** - Motor de búsqueda especializado en localizar dispositivos conectados.
- **Zoomeye** - Motor similar a Shodan para explorar dispositivos y servicios en Internet.
- **Herramienta shodan** - Busca sistemas conectados desde tu terminal usando la API de shodan.

2. Motores de búsqueda Deep Web:

- **Robots.txt** - Archivo de indexacion web.

- **Startpage** - Motor que respeta la privacidad y permite búsquedas sin censura.
- **Yandex** - Motor de búsqueda ruso con acceso a la Deep Web.
- **Boardreader** - Búsquedas especializadas en foros y contenido de la Deep Web.
- **Ahmia** - Motor de búsqueda dedicado a indexar sitios .onion de la red Tor.

3. Motores de búsqueda y servicios web enfocadas al **OSINT:**

- **Have I Been Pwned:** Plataforma para verificar si un correo electrónico ha sido comprometido en filtraciones de datos.
- **IntelTechniques:** Proporciona herramientas para realizar investigaciones OSINT, desde búsquedas de correos hasta rastreo de direcciones IP.
- **NixIntels OSINT:** Herramienta web que organiza y categoriza recursos y herramientas de código abierto para realizar investigaciones OSINT.
- **Pastebin:** Plataforma para compartir texto donde se busca información filtrada o datos expuestos, útil en investigaciones OSINT.

4. Detección y Prevención de Google Hacking en Entornos Empresariales:

- Métodos para detectar Google Hacking en una organización.
- Restricción de indexación en motores de búsqueda.
- Protección contra Google Dorks maliciosos, **(Teoría).**

Módulo 7: Buenas Prácticas y Defensa contra Google Hacking:

- Cómo evitar la exposición de información sensible en motores de búsqueda.
- Métodos para proteger servidores y sitios web contra indexación no deseada.
- Uso de robots.txt y encabezados **HTTP** para limitar la recolección de datos.

Módulo 8: Casos Prácticos y Desafíos Finales:

- Análisis de casos reales de Google Hacking y sus implicaciones.
- Desafíos de Google Hacking: Encuentra información oculta con dorks.
- Proyecto final: Realización de una auditoría OSINT con Google Dorks.

Módulo 9: Conclusión del Curso de Google Hacking:

- Resumen de las técnicas y herramientas aprendidas
- Importancia del Google Hacking en **ciberseguridad** y OSINT
- Buenas prácticas y consideraciones éticas en su uso
- Recursos adicionales para seguir aprendiendo

- Preguntas y respuestas para afianzar conocimientos

Índice del Curso Google Hacking Mastery: Dorks, OSINT, Python y Herramientas Automatizadas para la Dark Web.

Versión 1.0 – Febrero 2025

Para más información, visita: NetHunter Academy | Contacto: info@nethunteracademy.com

---