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

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

**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.
- **Hearramienta 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).

**1. Motores de búsqueda enfocados a sistemas conectados.**

En esta parte del curso aprenderás a utilizar herramientas que permiten descubrir **dispositivos conectados a internet** que, muchas veces sin saberlo, están expuestos al público. Esto incluye cámaras de seguridad, servidores web, impresoras, paneles de control y muchos otros sistemas que no deberían estar accesibles.

- **Censys** te ayuda a buscar estos dispositivos mediante información técnica que recopila constantemente de todo internet. Es ideal para detectar servicios mal configurados.
- **Shodan** es uno de los más conocidos. Su buscador te muestra desde cámaras de vigilancia hasta señales de tráfico conectadas a la red. Con solo escribir una palabra clave, puedes ver qué dispositivos están disponibles en tiempo real.
- **Zoomeye** es una alternativa muy usada en Asia. También analiza la red y te muestra qué hay conectado, con qué software y desde qué país.
- También exploraremos cómo usar **Shodan desde la terminal**, una forma más directa y automatizada de realizar búsquedas usando comandos. Esto es útil para quienes trabajan en auditorías o análisis de ciberseguridad.

**2. Motores de búsqueda en la Deep Web.**

La Deep Web incluye toda aquella información que no aparece en buscadores comunes como Google. Aquí vamos a explorar **herramientas que te permiten acceder a ese contenido oculto**, útil para investigaciones, análisis o búsquedas avanzadas.

- Empezaremos con **robots.txt**, un archivo que los sitios web usan para decirle a los buscadores qué partes del sitio deben ocultarse. Aprenderás a interpretarlo y a ver qué están intentando esconder.
- **Startpage** es un buscador alternativo que prioriza la privacidad. A diferencia de Google, no guarda tus datos ni personaliza resultados según tu historial.
- **Yandex**, el buscador más popular de Rusia, permite llegar a contenidos y resultados distintos a los occidentales. También tiene acceso a parte de la Deep Web.
- **Boardreader** está enfocado en foros de discusión. Muchas veces, los foros contienen información útil o sensible, y este buscador te ayuda a encontrarla.
- Por último, conocerás **Ahmia**, un motor que permite buscar sitios con direcciones .onion (de la red Tor), abriendo una puerta al contenido más oculto de internet de forma segura.

**3. Motores de búsqueda y servicios web enfocados al OSINT.**

OSINT (Open Source Intelligence) significa **investigación basada en fuentes públicas**. En este apartado aprenderás a utilizar plataformas y buscadores que te ayudan a recolectar información útil que está disponible en internet, pero que muchas veces pasa desapercibida.

- **Have I Been Pwned** te permite saber si un correo electrónico ha sido filtrado en alguna brecha de datos. Es muy útil para comprobar si alguien ha sido víctima de un robo de datos.
- **IntelTechniques** es un sitio que reúne herramientas para buscar personas, direcciones IP, imágenes, redes sociales y más. Todo desde un enfoque práctico y organizado.
- **OSINT Framework** funciona como un mapa de herramientas. Está organizado por temas (correos, personas, dominios, etc.) y te permite descubrir muchas plataformas para realizar investigaciones abiertas.
- **Pastebin** es una web donde la gente publica notas de texto, pero también se han filtrado allí contraseñas, bases de datos y documentos confidenciales. Aprenderás a usarla como fuente de inteligencia.

**4. Detección y prevención de Google Hacking en entornos empresariales.**

Una parte muy importante del curso es aprender **cómo las empresas pueden protegerse del Google Hacking**. Aunque esta técnica no es maliciosa por sí sola, puede ser aprovechada para obtener información sensible que nunca debió ser pública.

- Aprenderás a **detectar si alguien está usando motores de búsqueda para encontrar vulnerabilidades** en tus sitios web o servidores. Esto es útil para prevenir filtraciones de datos o accesos no autorizados.
- Verás cómo **limitar la indexación en buscadores**, de modo que archivos internos, paneles de administración o bases de datos no aparezcan en Google.
- También hablaremos sobre cómo **prevenir búsquedas maliciosas usando Google Dorks**, y qué tipo de errores comunes suelen cometer las empresas que dejan su información expuesta sin saberlo.