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

Módulo 5: Automatización y Herramientas para Google Hacking

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

La automatización en Google Hacking permite optimizar la búsqueda de información mediante herramientas especializadas y scripts personalizados. Este módulo cubre diversas herramientas OSINT diseñadas para facilitar la extracción y análisis de datos a través de Google Dorks, bases de datos de exploits y metadatos en documentos e imágenes.

1. Bingoo – Automatización de consultas con Google Dorks.

- **Bingoo** es una herramienta que automatiza la ejecución de Dorks en múltiples motores de búsqueda, permitiendo la recolección de información de manera eficiente. Es utilizada en auditorías de seguridad y **OSINT** para identificar información sensible de forma rápida.

2. Dorks-Eye – Extracción y uso de Dorks desde GitHub.

- **Dorks-Eye** facilita la recolección de Google Dorks desde repositorios públicos, permitiendo automatizar búsquedas avanzadas. Su uso es clave en investigaciones OSINT y en la identificación de datos expuestos en la web.

3. ExifTool – Extracción de metadatos en imágenes y documentos.

- **ExifTool** permite extraer y analizar **metadatos** de archivos como imágenes y documentos. Estos metadatos pueden incluir información sobre ubicación, fecha de creación y software utilizado, siendo de gran utilidad en investigaciones **OSINT** y análisis forenses.

4. SpiderFoot – Reconocimiento y análisis automatizado de información.

- **SpiderFoot** es una plataforma de recopilación automatizada de información que analiza dominios, direcciones IP y otros datos relevantes. Se integra con múltiples fuentes para realizar un análisis detallado de infraestructuras y posibles vulnerabilidades.

5. Dorksearch – Búsqueda de Dorks en una plataforma en línea.

- **Dorksearch** es un motor de búsqueda especializado que permite encontrar Google Dorks relevantes para auditorías de seguridad. Su uso facilita la identificación de información expuesta en sitios web y bases de datos en línea.

6. Exploit-DB – Base de datos de exploits y vulnerabilidades mediante Dorks.

- **Exploit-DB** es una de las principales bases de datos de vulnerabilidades y exploits. Su integración con Google Dorks permite localizar sistemas y aplicaciones potencialmente vulnerables mediante búsquedas avanzadas.

7. Cxsecurity – Recolección de Dorks y análisis de vulnerabilidades.

- **Cxsecurity** proporciona una base de datos de vulnerabilidades explotables mediante Google Dorks. Es una fuente clave para investigadores de seguridad, permitiendo analizar posibles fallos en aplicaciones web y sistemas en línea.

8. Script en Python – Automatización de scraping con Dorks en motores de búsqueda.

- El **scraping** con Google Dorks mediante scripts en Python permite automatizar la extracción de información de motores de búsqueda. Utilizando bibliotecas específicas, se pueden obtener datos estructurados y relevantes para auditorías de seguridad.

9. Script en Python – Exploración de la Dark Web y obtención de información.

- Los scripts en Python pueden ser utilizados para acceder y extraer información de la **Dark Web**, explorando sitios ocultos y bases de datos no indexadas en la web superficial. Su uso es relevante en investigaciones OSINT avanzadas.

Conclusión.

El **Google Hacking** se vuelve mucho más eficiente con la automatización mediante herramientas OSINT y scripts personalizados. En este módulo hemos visto cómo herramientas como **Bingoo, Dorks-Eye y Exiftool** pueden facilitar la recolección masiva de datos, así como el uso de **IA y chatbots** para optimizar los procesos de búsqueda.

Dominar la automatización en **Google Hacking** no solo mejora la rapidez y precisión en auditorías de seguridad, sino que también reduce las limitaciones impuestas por los motores de búsqueda.

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