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

Módulo 1: Introducción al Google Hacking.

¿Qué es Google Hacking? Conceptos y Fundamentos:

- Google Hacking es una técnica de búsqueda avanzada que utiliza operadores específicos en los motores de búsqueda para localizar información expuesta involuntariamente en la web. También conocido como "Google Dorking", permite encontrar archivos sensibles, configuraciones erróneas, credenciales filtradas y otras vulnerabilidades sin necesidad de acceder directamente a los sistemas.
- Los motores de búsqueda indexan automáticamente el contenido disponible en servidores web, y muchas organizaciones, por desconocimiento o descuido, dejan información accesible sin restricciones adecuadas. Google Hacking explota esta exposición mediante consultas avanzadas (Google Dorks) para extraer datos relevantes.

Historia y Evolución del Uso de Dorks en la Ciberseguridad:

- El concepto de Google Hacking surgió en la década de los 2000 cuando Johnny Long, un experto en seguridad, publicó el **Google Hacking Database (GHDB)**, una recopilación de consultas que permitían encontrar información crítica en la web.
- A lo largo de los años, estas técnicas han evolucionado y se han integrado en la ciberseguridad ofensiva, OSINT (Open Source Intelligence) y auditorías de seguridad. Además, herramientas automatizadas como Dork Eye**, Bingoo, etc.** Han implementado Dorks para agilizar la recopilación de información.

Las principales etapas de su evolución incluyen:

- **2002-2005:** Popularización de Google Hacking con la publicación del GHDB.
- **2010-2015:** Uso de Dorks en OSINT y auditorías de seguridad web.
- **2015-actualidad:** Automatización con inteligencia artificial y la incorporación de motores alternativos como **Shodan y Censys** para búsqueda de dispositivos conectados.

Usos Legales y Éticos del Google Hacking:

El **Google Hacking**, aunque poderoso, debe utilizarse con responsabilidad. En entornos legales, se emplea para:

- **Auditorías de seguridad:** Identificación de información expuesta en servidores de empresas.
- **Investigación OSINT:** Recopilación de datos en investigaciones forenses digitales.

- **Protección de infraestructuras:** Evaluación de la superficie de ataque de organizaciones.

Sin embargo, el uso indebido de Google Hacking para obtener información privada sin autorización puede violar leyes como el **CFAA (Computer Fraud and Abuse Act)** en EE.UU. o normativas de protección de datos en Europa **(GDPR)**. Es fundamental contar con permisos antes de realizar búsquedas de seguridad en infraestructuras ajenas.

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