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

Módulo 3: Dominando los Google Dorks

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

Módulo 3: Dominando los Google Dorks

Los **Google Dorks** son consultas avanzadas que utilizan operadores específicos para filtrar y extraer información de los motores de búsqueda, especialmente en Google. Esta técnica, ampliamente usada en **OSINT (Open Source Intelligence)** y auditorías de seguridad, permite identificar archivos sensibles, directorios abiertos, credenciales expuestas y configuraciones erróneas en servidores web.

Operadores Básicos de Búsqueda Avanzada en Google

Google permite realizar búsquedas refinadas mediante operadores avanzados. Los más utilizados incluyen:

- **site:**→ Filtra los resultados dentro de un dominio específico.
  - site:example.com → Muestra solo resultados del dominio "example.com".

- **filetype:**→ Permite buscar archivos de un formato específico (PDF, DOCX, XLSX, etc.).
  - filetype:pdf site:gov → Encuentra documentos PDF en sitios gubernamentales.

- **intitle:**→ Busca páginas web con una palabra clave en el título.
  - intitle:"index of" → Localiza directorios abiertos en servidores web.

- **inurl:**→ Filtra resultados que contengan un texto específico en la URL.
  - inurl:admin → Identifica URLs con la palabra "admin", útiles para encontrar paneles de administración.

- **intext:**→ Busca palabras clave dentro del contenido de la página.
  - intext:"password" → Intenta localizar páginas con contraseñas expuestas.

- **cache:**→ Muestra la última versión en caché de un sitio indexado por Google.
  - cache:example.com → Permite ver una versión anterior de una página eliminada o modificada.

Filtrado de Información con Operadores Booleanos

Los operadores booleanos permiten combinar múltiples filtros en una misma consulta para refinar aún más los resultados:

- **AND:**→ Obliga a que ambos términos aparezcan en la búsqueda.
  - site:example.com AND filetype:pdf

- **OR:**→ Muestra resultados que contengan al menos uno de los términos.
  - filetype:doc OR filetype:xls

- **- (guion):**→ Excluye términos de la búsqueda.
  - site:example.com -inurl:login → Muestra páginas de example.com excluyendo aquellas que contengan "login" en la URL.

- **" (comillas):**→ Busca frases exactas.
  - "Confidential Report" → Encuentra documentos con esa frase exacta.

Google Dorks para Encontrar Archivos Sensibles (PDF, XLS, DOC, etc.)

Los motores de búsqueda indexan archivos que, en muchos casos, no deberían ser públicos. Mediante dorks específicos, es posible localizar documentos con información sensible, como contraseñas, configuraciones de servidores y bases de datos expuestas:

- **Archivos PDF con credenciales:**
  - filetype:pdf intext:"username" intext:"password"

- **Hojas de cálculo con datos sensibles:**
  - filetype:xls intext:"email" intext:"password"

- **Archivos de configuración con credenciales:**
  - filetype:env "APP_KEY=" → Encuentra archivos .env con claves de aplicaciones web.
  - filetype:xml intext:password → Localiza archivos XML con posibles credenciales embebidas.

- **Bases de datos expuestas en servidores web:**
  - filetype:sql intext:"-- phpMyAdmin SQL Dump"
  - filetype:json intext:"api_key"

Extracción de Información de Sitios Web con Estructuras de URL Específicas

Los motores de búsqueda indexan estructuras de URL comunes en múltiples plataformas, permitiendo identificar recursos mal configurados:

- **Páginas de login expuestas:**
  - inurl:login → Encuentra páginas de inicio de sesión.
  - inurl:wp-admin → Ubica paneles de administración de WordPress.

- **Repositorios de código fuente accesibles:**
  - inurl:gitlab → Filtra instancias de GitLab expuestas.
  - site:github.com "token" → Busca claves API en GitHub.

- **Sistemas de monitoreo expuestos:**
  - intitle:"Nagios" inurl:nagios → Encuentra paneles de monitoreo Nagios.
  - intitle:"Zabbix Monitoring" → Localiza servidores de Zabbix accesibles.

Uso de Dorks para Descubrir Directorios y Paneles de Administración Expuestos

Es común que los administradores de sistemas dejen directorios abiertos sin restricciones de acceso, lo que puede revelar archivos y configuraciones sensibles:

- **Directorios abiertos en servidores web:**
  - intitle:"index of /" → Muestra listas de archivos en servidores sin restricciones.
  - intitle:"index of /backup" → Encuentra carpetas de respaldo accesibles.

- **Paneles de administración mal protegidos:**
  - inurl:admin → Ubica accesos administrativos.
  - inurl:phpmyadmin → Encuentra paneles phpMyAdmin expuestos.

- **Interfaces de dispositivos IoT y cámaras de seguridad:**
  - intitle:"webcamXP" → Filtra cámaras de vigilancia expuestas.
  - inurl:"ViewerFrame?Mode=" → Muestra transmisiones en vivo sin autenticación.

Conclusión.

El dominio de los **Google Dorks** no solo es esencial para **OSINT** y auditorías de seguridad, sino también para la protección de infraestructura, permitiendo detectar configuraciones erróneas antes de que sean explotadas por actores malintencionados.

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