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

Módulo 4: Google Hacking en la Ciberseguridad

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

El Google Hacking es una técnica avanzada utilizada en auditorías de seguridad y pruebas de penetración para encontrar información sensible expuesta en motores de búsqueda. Muchas organizaciones no protegen adecuadamente sus servidores, permitiendo la indexación de archivos, credenciales, bases de datos y sistemas críticos.

Este módulo cubre el uso de **Google Dorks** para la identificación de bases de datos, configuraciones inseguras, cámaras de seguridad accesibles y la integración de estas técnicas en auditorías de seguridad.

Identificación de Bases de Datos Expuestas mediante Dorks.

Las bases de datos pueden quedar expuestas cuando servidores mal configurados permiten que motores de búsqueda indexen archivos .sql, .db o .json con información sensible. Mediante Google Dorks, es posible identificar estas fugas de datos:

- **Archivos de volcado SQL expuestos:**
  - filetype:sql intext:"MySQL dump"
  - filetype:sql "phpMyAdmin SQL Dump"

- **Bases de datos NoSQL accesibles:**
  - filetype:json intext:"_id" intext:"password" → Archivos JSON con credenciales.
  - inurl:mongodb → Instancias de MongoDB indexadas.

- **Copias de seguridad y archivos de configuración sensibles:**
  - filetype:bak OR filetype:old OR filetype:backup → Identifica archivos de respaldo sin proteger.
  - filetype:ini intext:"password" → Localiza archivos de configuración con credenciales.

Encontrar Credenciales y Configuraciones Sensibles con Google.

Los administradores de sistemas y desarrolladores a menudo dejan archivos de configuración en ubicaciones accesibles, exponiendo claves API, credenciales de bases de datos y configuraciones críticas. Algunos Dorks efectivos incluyen:

- **Archivos de configuración con credenciales:**
  - filetype:env "DB_PASSWORD=" → Encuentra archivos .env con credenciales de bases de datos.
  - filetype:cfg intext:"admin" intext:"password" → Localiza archivos de configuración con credenciales de administrador.

- **Claves API y tokens de autenticación:**
  - inurl:github.com "api_key" → Identifica posibles claves API en GitHub.
  - filetype:json intext:"access_token" → Filtra tokens de autenticación en archivos JSON.

- **Correos y contraseñas filtradas en texto plano:**
  - filetype:txt intext:"email" intext:"password" → Busca listas de credenciales en archivos de texto.
  - site:pastebin.com "username" "password" → Examina credenciales expuestas en Pastebin.

Indexación de Cámaras de Seguridad Accesibles desde Google.

Muchas cámaras IP y sistemas de videovigilancia quedan accesibles en internet debido a configuraciones incorrectas, permitiendo que sean localizadas mediante motores de búsqueda:

- **Búsqueda de cámaras abiertas:**
  - intitle:"Live View / - AXIS" → Cámaras de seguridad AXIS con acceso público.
  - intitle:"webcamXP 5" inurl:"8080" → Cámaras de seguridad con software WebcamXP.

- **Sistemas de vigilancia industrial:**
  - intitle:"MOBOTIX MxControlCenter" → Sistemas de vigilancia MOBOTIX accesibles.
  - inurl:"ViewerFrame?Mode=" → Cámaras expuestas sin autenticación.

- **Transmisiones en vivo sin seguridad:**
  - inurl:"/view.shtml" → Encuentra cámaras conectadas sin autenticación.
  - inurl:"/live.html" → Localiza cámaras con streaming en vivo abierto.

Uso de Google Hacking en Auditorías de Seguridad y Pentesting.

El Google Hacking se ha convertido en una herramienta clave en **auditorías de seguridad**, **reconocimiento en pentesting** y **OSINT**, ya que permite identificar configuraciones erróneas antes de que sean explotadas por atacantes. Su aplicación en **pruebas de penetración** incluye:

- **Reconocimiento pasivo en pentesting:**
  - Obtener información sobre la infraestructura de una empresa sin generar tráfico sospechoso.
  - Identificar servidores web con configuraciones inseguras.

- **Detección de información expuesta en sitios corporativos:**
  - Localizar documentos internos confidenciales en intranets mal protegidas.
  - Descubrir portales de administración accesibles sin autenticación.

- **Análisis de superficie de ataque:**
  - Encontrar subdominios y paneles de control ocultos.
  - Identificar dispositivos IoT conectados sin protección.

Conclusión.

El uso de **Google Hacking** en ciberseguridad es una técnica poderosa, pero también un riesgo cuando no se aplican las configuraciones adecuadas en servidores y aplicaciones. Este módulo ha mostrado cómo encontrar bases de datos expuestas, credenciales filtradas y cámaras de seguridad accesibles, demostrando la importancia de **revisar periódicamente la huella digital de una organización**.

Para los pentesters, dominar Google Dorks es esencial para el reconocimiento pasivo y la identificación de vulnerabilidades sin necesidad de realizar escaneos intrusivos.
