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

Módulo 8: Casos Prácticos y Desafíos Finales

1. Análisis de casos reales de Google Hacking y sus implicaciones.
2. Desafíos de Google Hacking: Encuentra información oculta con dorks.
3. Proyecto final: Realización de una auditoría OSINT con Google Dorks.

En este módulo se aplicará todo lo aprendido en Google Hacking mediante el análisis de casos reales, desafíos prácticos y la realización de una auditoría OSINT basada en Google Dorks. Se explorarán incidentes donde Google Hacking fue clave en la exposición de información sensible y se pondrán en práctica técnicas avanzadas de recolección de datos.

1. Análisis de Casos Reales de Google Hacking y sus Implicaciones.

- El uso de Google Dorks ha permitido descubrir información confidencial en diversas ocasiones. A continuación, se presentan algunos casos destacados:

Caso 1: Fuga de Bases de Datos Sensibles.

En 2021, investigadores de seguridad descubrieron múltiples bases de datos expuestas mediante Google Dorks. Usando la consulta:

- site:example.com filetype:sql | filetype:db | filetype:mdb

Se encontraron archivos de bases de datos MySQL, PostgreSQL y Access accesibles desde servidores mal configurados. Entre los datos expuestos se incluían credenciales, direcciones de correo electrónico y registros financieros.

Caso 2: Paneles de Administración Expuestos.

Un pentester descubrió accesos no protegidos a paneles de administración mediante la siguiente búsqueda:

- inurl:admin login | inurl:cpanel | inurl:dashboard site:example.com

El resultado reveló múltiples interfaces de administración sin autenticación adecuada, lo que permitió acceder a configuraciones sensibles y potencialmente comprometer el sistema.

Caso 3: Indexación de Documentos Confidenciales.

Un gobierno filtró accidentalmente documentos internos debido a una mala configuración de permisos en su servidor web. La búsqueda:

- site:gov filetype:pdf confidential

Permitió a investigadores encontrar documentos clasificados que contenían información sobre proyectos de infraestructura crítica.

2. Desafíos de Google Hacking: Encuentra Información Oculta con Dorks.

Desafío 1: Identificación de Archivos Expuestos.

Utiliza Google Dorks para encontrar archivos de configuración o copias de seguridad accesibles en un dominio objetivo. Algunos ejemplos de consultas:

- site:target.com filetype:bak | filetype:old | filetype:zip

Desafío 2: Descubrimiento de Cámaras de Seguridad en Línea.

Encuentra cámaras de vigilancia indexadas en Google utilizando búsquedas como:

- inurl:view/view.shtml
- intitle:"Live View / - AXIS"

Desafío 3: Extracción de Metadatos en Documentos.

Utiliza Google para localizar documentos de un dominio y luego extraer sus metadatos con herramientas como ExifTool.

Ejemplo de búsqueda:

- site:example.com filetype:docx | filetype:xlsx | filetype:pptx

Extracción de metadatos en Linux:

- exiftool archivo.docx

3. Proyecto Final: Realización de una Auditoría OSINT con Google Dorks.

Como actividad final del curso, se deberá realizar una **auditoría OSINT completa** sobre un dominio objetivo aplicando Google Hacking.

Objetivos del Proyecto:

- Identificar archivos sensibles expuestos en un dominio.
- Localizar directorios y paneles administrativos sin protección.
- Determinar posibles filtraciones de información en documentos públicos.
- Documentar los hallazgos y proponer medidas de mitigación.

Pasos para la Auditoría:

- **Definir el alcance**: Seleccionar un dominio o entidad específica para la investigación.
- **Ejecutar Google Dorks**: Aplicar consultas avanzadas para extraer información relevante.
- **Analizar los datos obtenidos**: Clasificar los hallazgos según su criticidad.
- **Generar un informe final**: Incluir capturas de pantalla, consultas utilizadas y recomendaciones de seguridad.

Conclusión.

Este módulo demuestra el **impacto real de Google Hacking**, destacando cómo una mala configuración de servidores o permisos puede llevar a la exposición de datos críticos. A través de casos prácticos y desafíos, se han puesto en práctica habilidades fundamentales para realizar auditorías OSINT eficaces.

Google Hacking es una herramienta poderosa, pero su uso debe ser **ético y legal**. Con este conocimiento, los profesionales de ciberseguridad pueden detectar y mitigar riesgos antes de que sean explotados por actores maliciosos.

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