Práctica de laboratorio: Búsquedas avanzadas

Objetivos

Utilice la búsqueda avanzada de Google para realizar un reconocimiento pasivo.

Parte 1: Búsquedas avanzadas de Google (Dorking)

Parte 2: La base de datos de piratería de Google

Parte 3: La máquina Wayback

Aspectos básicos/Situación

El primer paso que realiza un hacker es obtener la mayor cantidad de información posible sobre un objetivo. Cuanto más sepan los atacantes sobre el objetivo, mejor podrán piratearlo con otras técnicas de hackeo. El uso de búsquedas avanzadas de Google y el escaneo de sitios de Internet archivados son dos métodos populares de reconocimiento pasivo. Ayudan a informar a los hackers éticos sobre las vulnerabilidades de un cliente y allanan el camino para las actividades de explotación si son parte del alcance de la prueba.

A través de una búsqueda avanzada en Google, el hacker espera encontrar información que se haya hecho pública por accidente. Por ejemplo, alguien puede haber expuesto contraseñas accidentalmente, haber dejado una cámara web abierta a Internet o haber revelado otra información útil. El hacker buscará con palabras clave específicas y operadores de búsqueda de Google para intentar encontrar lo que está buscando. Esto se llama dorking Google. Implica el uso de consultas de búsqueda específicas de Google para descubrir información que no estaba destinada a estar disponible públicamente.

El archivo web de la máquina Wayback es otra herramienta útil para descubrir posibles vulnerabilidades. En ocasiones, se puede obtener información personal y corporativa valiosa de las páginas web archivadas. Con la máquina Wayback, un hacker puede navegar por el historial de un sitio web y visitar instantáneas del sitio en varios momentos en el pasado. Esto permite que el hacker descubra información que ya no está disponible en Internet en vivo que puede ser útil para futuros ataques.

El acceso no autorizado a datos, computadoras y sistemas de redes es un delito en muchas jurisdicciones y, a menudo, está acompañado por graves consecuencias, independientemente de qué motive al delincuente. En su carácter de usuario de este material, la responsabilidad del alumno es conocer y cumplir las leyes de uso de las computadoras.

Recursos necesarios

- Computadora o dispositivo móvil con acceso a Internet

Instrucciones

Parte 1: Búsquedas avanzadas de Google (Dorking)

Para la mayoría de las personas, Google es una herramienta para buscar texto, imágenes, videos y noticias en Internet mediante consultas de cadenas simples. Sin embargo, para algunos, Google es una herramienta de piratería potente y útil y puede utilizarse para realizar reconocimientos pasivos mediante el uso de operadores de búsqueda avanzados. La práctica de utilizar operadores avanzados de búsqueda de Google para encontrar información y servidores vulnerables se denomina dorking de Google o hackeo de Google. Los hackers utilizan el dorking de Google para intentar encontrar información que nunca tuvo la intención de revelarse públicamente. Es una técnica útil para realizar reconocimientos pasivos en pruebas de penetración.

Nota: Al realizar consultas avanzadas, es posible que Google le solicite que demuestre que no es un robot. Si esto ocurre, como probablemente ocurrirá después de varias búsquedas, simplemente complete el captcha y continúe.

Paso 1: Explore Google dorking.

a. Navegue a www.google.com para abrir el motor de búsqueda de Google.

b. Escriba la cadena de búsqueda **ethical hacker** en la ventana de búsqueda. Desplazarse por los resultados.

Tenga en cuenta la variedad de resultados devueltos. Así es como solemos utilizar Google para realizar búsquedas. Las consultas de cadenas como esta devuelven muchos resultados. Sin embargo, alrededor del 90% de los resultados no son específicos de lo que buscamos. Para restringir los resultados a lo que se desea, como páginas de un único sitio, palabras clave específicas o tipos de archivos específicos, se pueden utilizar los operadores de búsqueda avanzada de Google.

Hay muchos operadores de búsqueda avanzada de Google. Hay listas disponibles en Internet en sitios como SpyFu. Busque en Internet “operadores de búsqueda avanzada” para ver otras fuentes de información, algunas de las cuales tienen ejemplos útiles.

La siguiente tabla muestra los operadores de búsqueda avanzada que se utilizan en esta práctica de laboratorio.

Operadora	Descripción
allintext:	Restringe los resultados a las páginas con todas las palabras de la consulta en el texto de la página.
filetype:	Restringe los resultados a las páginas del tipo de archivo especificado (.pdf, .ppt, .doc, etc.)
intitle:	Restringe los resultados a las páginas con una determinada palabra (o palabras) en el título.
inurl:	Restringe los resultados a las páginas con una determinada palabra (o palabras) en la URL.
site:	Restringe los resultados a las páginas del dominio especificado.

Pruebe cada uno de los operadores en una búsqueda en Google. Cuando utilice la búsqueda avanzada, no ponga espacios entre el operador y el dominio o las palabras clave.

c. Escriba **ethical hacker site:pearson.com** en la ventana de búsqueda. La sintaxis es **search term operator:domain**. Desplazarse por los resultados.

¿Qué tienen en común todos los resultados?

Todos los resultados proceden del dominio especificado por el operador site: (en este caso pearson.com) y están relacionados con la búsqueda “ethical hacker”, ya que la consulta fue limitada a ese sitio en particular.

Todos contienen información sobre la piratería ética de un solo sitio, pearson.com

d. Escriba **ethical hacker site: pearson.com filetype:pdf** en la ventana de búsqueda. Desplazarse por los resultados.

¿Qué tipo de archivo abre cada uno de los resultados?

Todos los resultados son archivos PDF, porque se aplicó el operador filetype:pdf en la búsqueda, que restringe los resultados a documentos en formato PDF.

Todos los resultados deben estar en archivos PDF.

e. Escriba **ethical hacker intitle:certificate** en la ventana de búsqueda. Desplazarse por los resultados.

Todos los resultados deben estar relacionados con la piratería ética e incluir la palabras clave **certification** en el título de la página.

f. Escriba **ethical hacker inurl:free** en la ventana de búsqueda. Desplazarse por los resultados.

Los resultados incluyen páginas cuyo título contiene la palabra “certificate” y que están relacionadas con certificaciones o acreditaciones sobre hacking ético; por lo tanto, el operador intitle: limita los resultados a páginas con esa palabra en el título.

Todos los resultados deben estar relacionados con la piratería ética y deben tener la palabra clave **free** en la URL.

g. Escriba **allintext:free ethical hacker practice test questions** en la ventana de búsqueda. Esto realiza prácticamente la misma función que una búsqueda normal de Google, pero solo devuelve resultados con cada palabra clave en el texto de la página. No devolverá resultados con las palabras clave solo en el título. Pruebe colocar el texto de búsqueda entre comillas.

Los resultados deben incluir todas las palabras clave del texto de la página.

Devuelve páginas cuyo **texto** contiene todas las palabras indicadas (free, ethical, hacker, practice, test, questions), lo que permite encontrar páginas cuyos cuerpos de texto incluyen exactamente esas palabras.

Paso 2: Realice un reconocimiento pasivo con operadores de búsqueda avanzados.

Los operadores de búsqueda avanzada son útiles para delimitar los resultados de la búsqueda. Esto los hace útiles también para realizar reconocimientos pasivos. Los hackers utilizarán operadores de búsqueda avanzada para encontrar vulnerabilidades e información sobre objetivos potenciales. Si bien los resultados de las búsquedas pueden parecer inofensivos por sí solos, pueden proporcionar inteligencia valiosa a un hacker. El hacker espera encontrar sitios o archivos que la empresa objetivo no tenía la intención de hacer públicos, o encontrar información que pueda utilizarse para futuros ataques, como ataques de ingeniería social.

Al realizar estas búsquedas, utilice una empresa objetivo de su elección. El reconocimiento pasivo es legal, pero se detiene allí porque el uso de cualquier información que descubra para el reconocimiento activo no lo es. Si encuentra vulnerabilidades, considere informar a la empresa para que puedan corregir el problema.

a. Busque en el sitio de la empresa de destino con el operador **inurl:**.

En la ventana de búsqueda, escriba el comando **site:*examplecompany.com* inurl:admin** reemplazando *examplecompany.com* con una empresa de su elección.

Esto devolverá páginas que tengan la palabra clave **admin** en algún lugar de la URL.

Revise las páginas devueltas y haga clic en algunas para ver si hay información interesante.

b. Realice otra búsqueda, esta vez con el operador **intitle:**.

En la ventana de búsqueda, escriba el comando **site:*examplecompany.com* intitle:login**.

Esto devolverá las páginas que tienen la palabra clave **login** en el título. Nuevamente, revise los resultados y haga clic en algunos para ver si hay información interesante.

c. A continuación, intente utilizar el operador **filetype:**.

En la ventana de búsqueda, escriba el comando **site:*examplecompany.com filetype*:pdf**.

Esto devolverá archivos PDF. Revise algunos archivos para ver si hay información interesante que no esté destinada al acceso público o sea útil para ataques de ingeniería social.

d. Pruebe una búsqueda con varios operadores. Utilice los operadores **intext:** y **filetype:**. En la ventana de búsqueda, escriba el comando **site:*ejemploempresa.com* intext:employee filetype:pdf**

Esto devolverá páginas en PDF que contienen el texto del **employee**.

e. Experimente con **site:*ejemplocompany.com* intext:<palabra clave> filetype:<tipo de archivo>** mediante diferentes palabras clave y diferentes tipos de archivo.

f. LinkedIn puede ofrecer información valiosa sobre una empresa y sus empleados. En la ventana de búsqueda, escriba el comando **site:linkedIn.com intitle:*ejemplo de empresa***. Experimente buscando el nombre de la empresa con y sin .com al final.

g. Experimente con el **site:<*sitio de medios sociales*> intitle:*ejemplo de empresa*** y busque otros sitios de medios sociales.

Parte 2: La base de datos de piratería de Google

La base de datos de piratería de Google (GHDB) es un índice de dorks creados por usuarios que están diseñados para descubrir información interesante y potencialmente confidencial que involuntariamente se puso a disposición del público en Internet.

Paso 1: Explore la página principal de la base de datos de piratería de Google.

a. Realice una búsqueda en Google de **GHDB**. La primera página devuelta debe ser la base de datos de piratería informática de Google.

b. En la página principal de GHDB, haga clic en el botón **Filters** en la parte superior derecha de la ventana.

Esto le permite filtrar los resultados de la base de datos por categoría o autor. También hay una **Quick Search**.

Paso 2: Utilice la búsqueda rápida para encontrar dorks específicos.

a. Seleccione cada una de las categorías de filtros y observe algunos de los dorks disponibles en esa categoría. Seleccione algunos dorks interesantes en los resultados y observe las descripciones de cada uno.

¿Qué información se proporciona sobre los Dork?

Cada entrada de GHDB incluye: un ID del dork, el autor, la fecha de publicación, la categoría a la que pertenece (por ejemplo Files Containing Passwords), una breve descripción de lo que busca el dork, y la consulta (o enlace) que puede ejecutarse para obtener resultados. La entrada explica qué tipo de información puede revelar ese dork y por qué es relevante.

El número de ID de GHDB, el autor, la fecha de publicación, una breve descripción de la función del dork y un enlace en el que se puede hacer clic para iniciarlo en una nueva ventana.

b. Inicie algunos de los dorks que le parezcan interesantes y vea qué resultados se devuelven y el tipo de información que estos resultados pueden proporcionar a un hacker.

Paso 3: Seleccione Categorías para encontrar Dorks interesantes.

a. Realice una búsqueda de **tsweb**.

b. Haga clic en **allinurl:tsweb/default.htm** Dork.

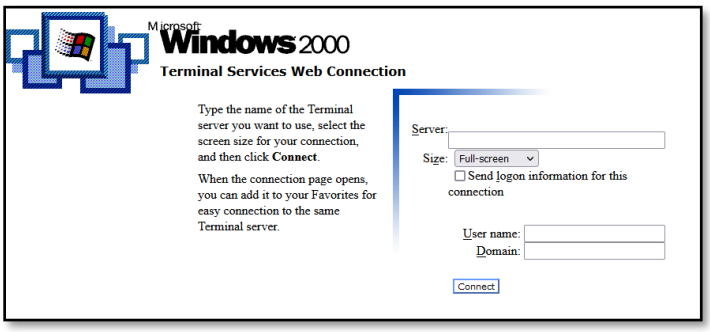
¿Qué devuelve este dork?

Al ejecutar varios dorks de prueba (solo contra dominios de práctica o públicos), se observan diferentes tipos de resultados: archivos con información expuesta, páginas con formularios de administración, índices de directorio y páginas que contienen palabras clave específicas (como password o backup). Estos resultados muestran cómo consultas específicas pueden filtrar y encontrar información que tal vez no debería ser pública.

Páginas para conexiones de servicios de terminal y escritorio remoto

c. Haga clic en algunas de las páginas devueltas. Además de los campos para las credenciales de inicio de sesión, es posible que vea información interesante que un hacker podría aprovechar. Por ejemplo, mire

la figura. El servidor de servicios de Terminal Server ejecuta Windows 2000. Sabiendo esto, un hacker puede centrarse en las vulnerabilidades de Windows 2000. Dado que Windows 2000 finalizó su vida útil en 2010, puede ser vulnerable.



Paso 4: Combine filtros de categorías con términos de búsqueda.

Puede combinar filtros de categorías con términos de búsqueda para refinar y filtrar los resultados según información específica.

a. Seleccione los **Files Containing Passwords** en el menú desplegable **Categories**.

b. En la ventana de **Quick Search**, escriba **db_pass**. Esto devolverá búsquedas de dorks de contraseñas de la base de datos.

Explore algunos de los resultados de búsqueda y vea la información interesante que revelan.

Revise los materiales del curso y pruebe algunas de las búsquedas que se muestran allí.