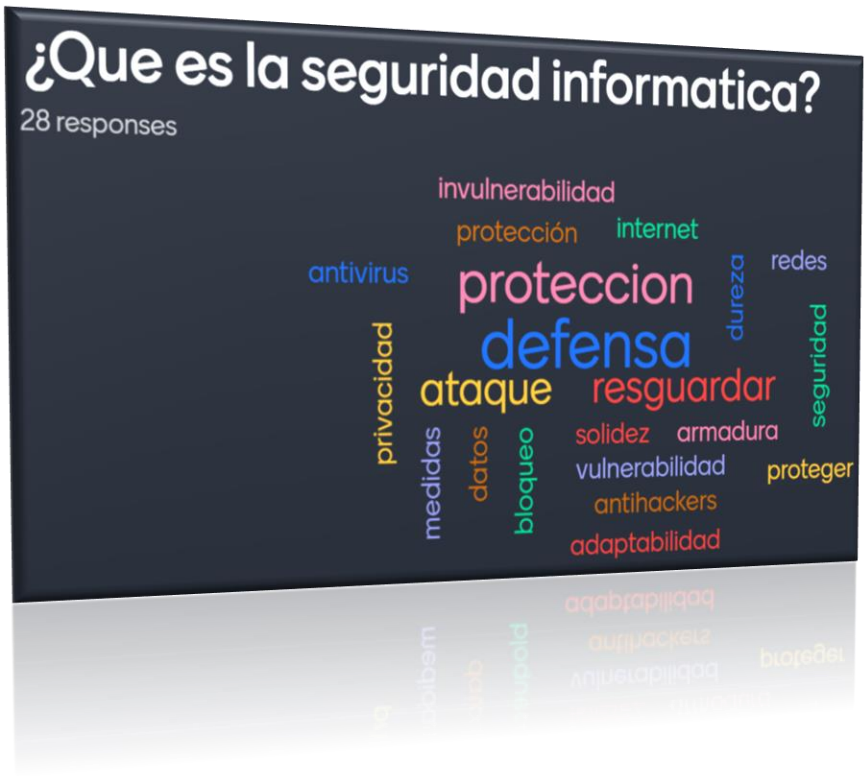
Universidad Paraguayo Alemana

UNIVERSIDAD PARAGUAYO ALEMANA
HEIDELBERG - ASUNCIÓN



Seguridad TICs

Prof.: Chrystian Ruiz Diaz

Contenido

Nota de Uso Académico

Este documento ha sido preparado exclusivamente para el uso académico del docente. Este documento no puede ser distribuido a ninguna otra parte ni utilizado para ningún otro propósito, diferente al establecido como alcance en el proyecto académico de la **UNIVERSIDAD PARAGUAYO ALEMANA**. El uso indebido del material fuera del ámbito académico no representa ninguna responsabilidad del docente.

Google Dorking: ¿Qué es y Cómo Utilizarlo?

Introducción a Google Dorking

Google Dorking, también conocido como Google Hacking, es una técnica que consiste en aplicar la búsqueda avanzada de Google para conseguir encontrar en internet aquella información concreta a base de ir filtrando los resultados con operadores (Los conocidos como dorks).

Aplicaciones de Google Dorking

Google Dorking es una técnica de OSINT (Open Source Intelligence) que permite:

- **Seguridad Informática**: Enumerar activos, buscar versiones vulnerables, y detectar fugas de información.
- **Investigación y Periodismo**: Facilita la búsqueda de información pública relevante.
- **Egosurfing**: Permite ver qué información está disponible sobre individuos y organizaciones.

Información Que Se Puede Encontrar

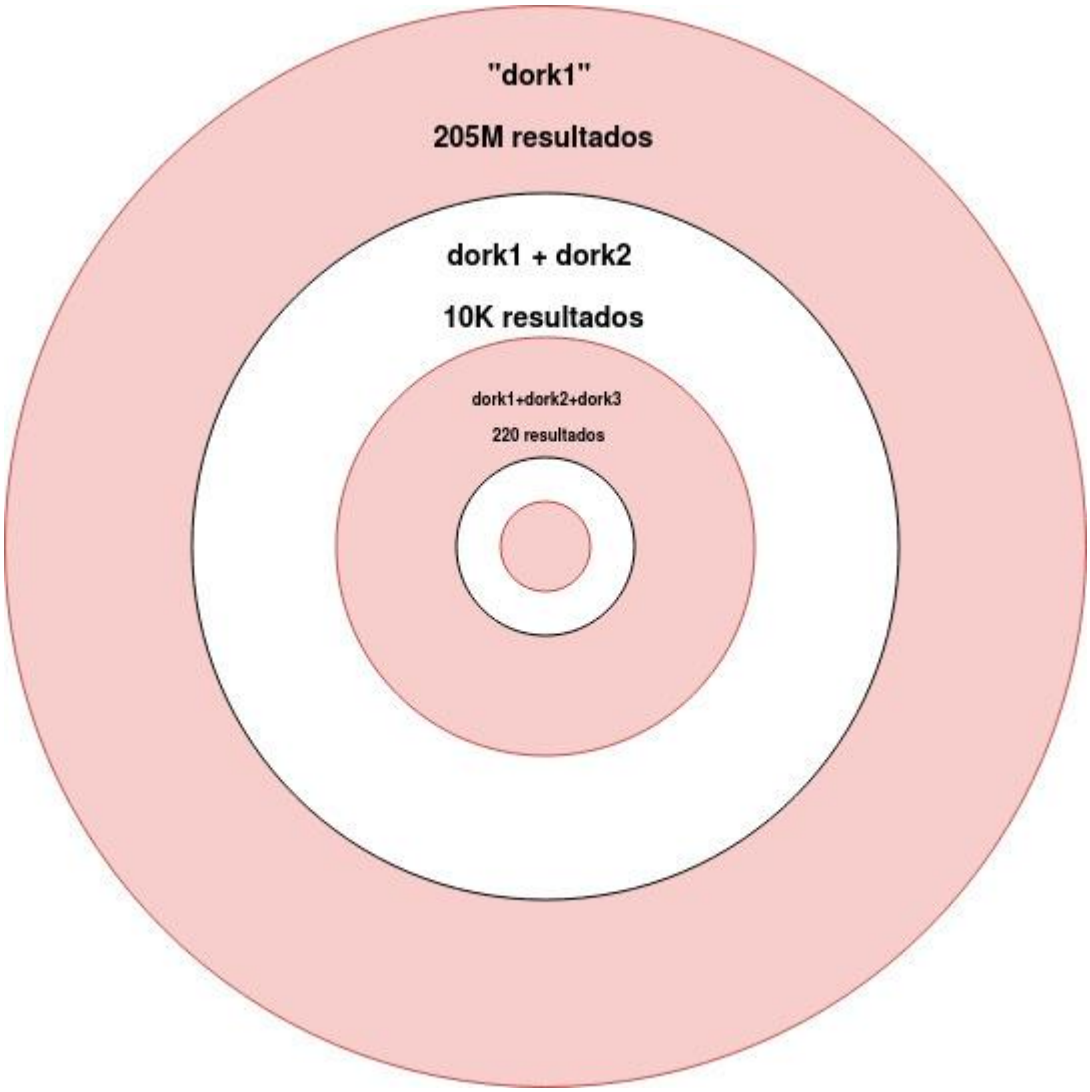
Gracias a Google Dorking, es posible encontrar:

- Datos sobre personas y organizaciones.
- Contraseñas y documentos confidenciales.
- Versiones vulnerables de servicios.
- Directorios expuestos.
- Y más.

Los robots de Google indexan todo lo que encuentran en internet, a menos que los archivos `robots.txt` lo impidan.

Cómo Utilizar Google Dorking

Para utilizar Google Dorking, se debe usar la barra de búsqueda de Google junto con dorks y palabras clave para filtrar los resultados. Cuantos más dorks se utilicen y más específicos sean, más refinados serán los resultados. Este proceso se puede comparar con una diana, donde una búsqueda simple dará muchas coincidencias y estaremos lejos del objetivo, mientras que a medida que se añaden más dorks, nos acercamos más a este.



Como en muchos ámbitos de la vida y la ciberseguridad, el Thinking Out the Box marcará las diferencias a la hora de sacar más rendimiento a esta técnica. El ingenio dará grandes resultados.

Operadores

Para poder aplicar con éxito Google Hacking, será necesario comprender perfectamente el funcionamiento de los operadores. Los operadores son comandos que se utilizan para filtrar de diferente modo la información que se encuentra indexada, permitiendo lo que se conoce como búsqueda avanzada.

A continuación se verán algunos de los operadores más utilizados y su propósito. Además es interesante tener en cuenta que el uso de los operadores puede ser combinado para que la búsqueda sea más refinada.

Operador	Utilidad	Ejemplo
""	Búsqueda con coincidencia exacta	"Derechodelared"
site:	Busca en el sitio web especificado en concreto	site:derechodelared.com
filetype:	Busca resultados que tienen la extensión de archivo especificada (pdf,txt,xls, etc.)	filetype:pdf
ext:	Misma utilidad que filetype	ext:pdf
inurl:	Busca la palabra especificada en una URL	inurl:dorking
intext:	Resultados con páginas en cuyo contenido aparece la palabra especificada	intext:dorking
intitle:	Resultados con páginas en cuyo título aparece la palabra especificada	intitle:dorking
allinurl:	Busca todas las palabras especificadas en una URL	allinurl:Google Dorks
allintext:	Resultados con páginas en cuyo contenido aparecen todas las palabras especificadas	allintext:Google Dorks
allintitle:	Resultados con páginas en cuyo título aparecen todas las palabras especificadas	allintitle:Google Dorks
-	Símbolo de exclusión, se excluirá de los resultados lo que vaya a continuación de él	dorking -Google
*	Se usa como comodín, el asterisco representa que puede ser sustituido por cualquier palabra	site:*.ejemplo.com

Operador	Utilidad	Ejemplo
`cache:`	Mostrará la versión en caché de la web en cuestión	`cache:derechodelared.com`
`OR`	Operador lógico, también se puede representar por |	`ext:pdf OR ext:txt`
`AND`	Operador lógico, normalmente se deja el espacio en blanco	`Google AND Bing`

En SANS se puede encontrar un cheatsheet muy práctico que muestra más operadores.
En Search Engine Journal se documentan los operadores al detalle.

Ejemplos

A continuación, para ver y entender cómo los operadores entran en juego, se verán unos cuantos ejemplos de diferentes búsquedas que se pueden realizar. La combinación de dorks puede traer unos resultados muy potentes. Ser ingenioso es un plus importante a la hora de lograr buenos hallazgos, y la imaginación pondrá el límite.

DISCLAIMER: *Con Google Dorking se puede encontrar mucha información de carácter confidencial. Aunque se encuentre pública, utilizar esa información, difundirla o cualquier tipo de explotación es ilegal.*

- **Buscar PDFs sobre Google Dorking**:

```
"Google Dorking" filetype:pdf
```

- **Buscar personas que trabajan en una localidad**:

```
site:es.linkedin.com intext:localidad
```

- **Buscar parámetros que puedan ser vulnerables**:

```
inurl:php?id=
```

- **Buscar subdominios excluyendo el principal**:


```
site:*.ejemplo.com -site:www.ejemplo.com
```

- **Buscar referencias a un sitio web excluyendo el propio sitio web**:

```
intext:derechodelared.com -site:derechodelared.com
```

- **Buscar listados de personas en varios formatos de fichero**:

```
intext:nombre intext:email intext:DNI (ext:pdf OR ext:txt OR
ext:xls OR ext:docx) intitle:lista
```

- **Buscar programas de Bug Bounty de empresas**:

```
inurl:/responsible-disclosure/ bounty
```

- **Buscar versiones vulnerables**:

```
allintext:powered by .... (especificar servicio con versión
vulnerable)
```

- **Buscar servidores FTP expuestos**:

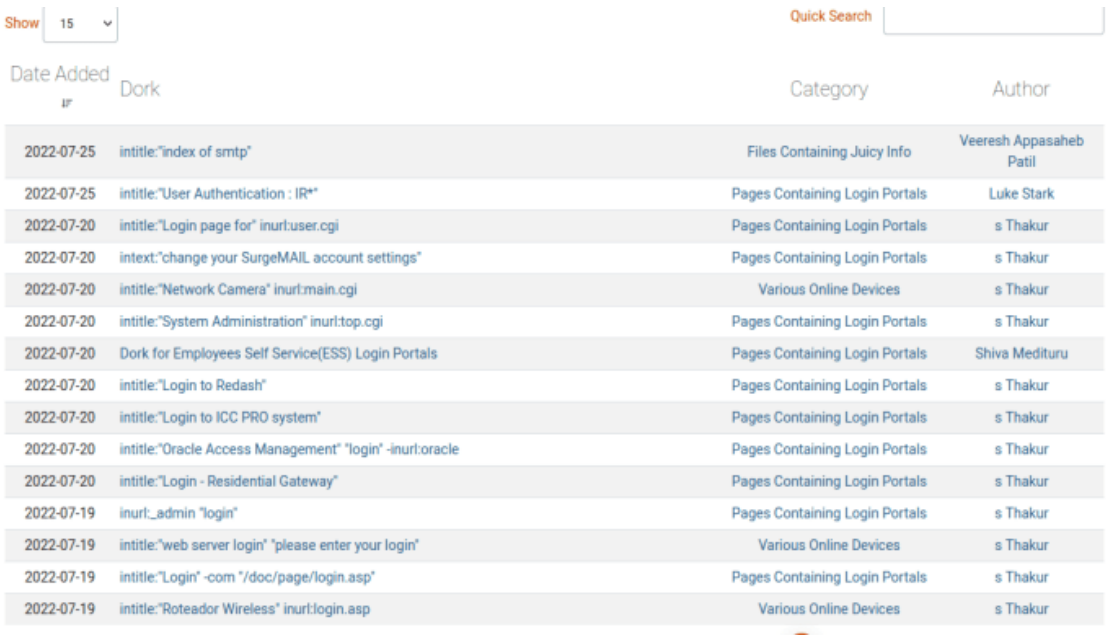
```
intitle:"index of" inurl:ftp
```

- **Buscar servicios que corren en el puerto 8080**:

```
inurl:8080 -intext:8080
```

GHDB (Google Hacking Database)

Para encontrar más ejemplos de Dorks, GHDB es un fantástico recurso. GHDB (Google Hacking Database) es un proyecto open-source que recopila una serie de dorks conocidos que pueden revelar información interesante y probablemente confidencial disponible públicamente en internet. Este proyecto es mantenido por Offensive Security, una organización muy reconocida en el mundo de la ciberseguridad.



Show 15 Quick Search

Date Added	Dork	Category	Author
2022-07-25	intitle:"index of smtp"	Files Containing Juicy Info	Veeresh Appasaheb Patil
2022-07-25	intitle:"User Authentication : IR*"	Pages Containing Login Portals	Luke Stark
2022-07-20	intitle:"Login page for" inurl:user.cgi	Pages Containing Login Portals	s Thakur
2022-07-20	intext:"change your SurgeMAIL account settings"	Pages Containing Login Portals	s Thakur
2022-07-20	intitle:"Network Camera" inurl:main.cgi	Various Online Devices	s Thakur
2022-07-20	intitle:"System Administration" inurl:top.cgi	Pages Containing Login Portals	s Thakur
2022-07-20	Dork for Employees Self Service(ESS) Login Portals	Pages Containing Login Portals	Shiva Medituru
2022-07-20	intitle:"Login to Redash"	Pages Containing Login Portals	s Thakur
2022-07-20	intitle:"Login to ICC PRO system"	Pages Containing Login Portals	s Thakur
2022-07-20	intitle:"Oracle Access Management" "login" -inurl:oracle	Pages Containing Login Portals	s Thakur
2022-07-20	intitle:"Login - Residential Gateway"	Pages Containing Login Portals	s Thakur
2022-07-19	inurl:_admin "login"	Pages Containing Login Portals	s Thakur
2022-07-19	intitle:"web server login" "please enter your login"	Various Online Devices	s Thakur
2022-07-19	intitle:"Login" -com "/doc/page/login.asp"	Pages Containing Login Portals	s Thakur
2022-07-19	intitle:"Roteador Wireless" inurl:login.asp	Various Online Devices	s Thakur

Conclusión

El poderoso sistema de Crawling de Google, que indexa todo tipo de contenido que hay en Internet, hace que saber buscar eficiente y precisamente sea de gran valor. Google dorks permite ayudar a encontrar rápidamente cualquier cosa en Internet y, como en muchas otras ocasiones, serán la pericia y el ingenio del hacker los que determinarán una investigación exitosa. Además, hay que tener muy en cuenta que todo lo visto en este artículo se puede aplicar también a otros buscadores. La metodología será idéntica y tan solo se encontrarán diferencias en la sintaxis de sus dorks. Por tanto, en una investigación, no hay que subestimar las ganancias que puede traer consultar Bing, Yahoo y DuckDuckGo para continuar avanzando.

Desde un punto de vista defensivo, será interesante practicar el egosurfing, es decir, buscarnos a nosotros mismos (a nivel personal o como organización) y ver qué información se está haciendo pública sin desearlo. A partir de ahí, habría que revisar los ajustes de privacidad (por ejemplo, si estamos haciendo público algo a través de Google Drive) o, si se trata de nuestro propio sitio web, editar el archivo `robots.txt`.

Como se puede ver, las técnicas de dorking son un imprescindible en la “mochila de conocimientos de un hacker”. Tanto para seguridad ofensiva como defensiva, dominar los dorks hará que no se escape nada de lo que haya en Internet.

Referencias y Recursos Adicionales:

- Google Dorking ¿Qué es? - Alberto Fonte - agosto 13, 2022
- Qué es Google Dorking, Dorks y Búsquedas Avanzadas – Tutorial de Google Hacking en Español (Contando Bits)
- HakByte: How to find anything on the internet with Google Dorks
- Bug Bounty con Google Dorks – Pablo García y Luis Madero
- Top 20 Google Hacking Techniques (Security Trails)
- Smart Searching with Google Dorking (exposingtheinvisible)

Para más información, consulta el artículo completo en Derecho de la Red.

