TÉCNICAS DE DORKING DE GOOGLE POR EQUIPOS ROJOS

Por ejemplo, en soluciones de seguridad ofensivas, es fundamental utilizar Google Dorking antes de la evaluación. Estas técnicas no se suelen dar en el pentesting profesional ya sea por falta de habilidad o porque se ofrecen opciones más económicas que no se ofrecen. Si desea saber qué podría revelar esto a un atacante, muchas veces puede encontrar información confidencial disponible públicamente para cualquier empresa o palabras clave específicamente en su país u otros factores que puede utilizar para limitar los resultados a lo que está buscando. , en una sola línea y que sirve como un atajo rápido para, a veces, obtener credenciales, archivos pdf confidenciales o información del cliente.

Supongamos que desea buscar todos los archivos PDF disponibles públicamente en un país específico utilizando Google. Puede proporcionar fácilmente lo siguiente:

```
'nda tipo de archivo:pdf ubicación:malta'
```

SIMPLES DE DORKING

A continuación se muestran algunos ejemplos del uso de dorking. Esto se considera OSINT, lo que significa que está utilizando datos disponibles de código abierto mediante un motor de búsqueda que ya los ha indexado.

1) Busque sitios web que contengan la palabra "cripto" y un número entre 1 y 1337:

```
"cripto" 1..1337
```

2) Busque el término "VideoName" pero excluya los resultados de YouTube:

```
Nombre del vídeo -sitio:youtube.*
```

3) Busque sitios web publicados después del 1 de enero de 2023 que traten sobre cómo utilizar '/reparar/apagar/... una computadora':

```
Cómo * una computadora después:2023-01-01
```

4) Busque sitios web publicados antes de 2023 que tengan el TLD .gov, sean documentos html o php y contengan las palabras "tarea". , "maestro" y "escuela":

```
allintext:tarea maestro escuela sitio:gov antes:2023 ext:(html | php)
```

Ahora bien, hay una frase muy poderosa que puede brindarle información confidencial.

COMPLEJOS DE DORKING CON INFORMACIÓN VALIOSA

- Encuentre cámaras web abiertas/públicas disponibles con enlaces directos:

```
intitle:"webcamXP 5" | inurl:"lvappl.htm"
```

- Busque documentos de registro que contengan la cadena "contraseña":

```
intext:contraseña ext:log
```

- Encuentre servidores web vulnerables. Siéntase libre de cambiar el POC:

```
inurl:/proc/self/cwd
```

- Encuentre documentos de Excel que contengan direcciones de correo electrónico:

```
inurl:correo electrónico.xlsx ext:xlsx
```

PRINCIPALES OPERADORES DE BÚSQUEDA PARA DORKING

Operador	Explicación	Sintaxis	Ejemplo
()	Agrupar varios términos o operadores. Permite avanzados expresiones	(<término> o <operador>) inurl:(html | php)	
*	Comodín. Coincide con cualquier palabra	<texto> * <texto>	Cómo * a computadora
“”	La palabra clave dada tiene que coincidir exactamente. No distingue entre mayúsculas y minúsculas	" <palabras clave> "	"Google"
m…n / m…n	Busque una variedad de números. n debería ser mayor que m	<número>.. <número>	1..1337
-	Documentos que coincidan con el operador están excluidos. NO-Operador	- <operador>	-sitio:youtube.com
+	Incluir documentos que coincidan el operador	+ <operador>	+sitio:youtube.com
|	Operador O lógico. Sólo uno el operador necesita coincidir en orden para que la expresión general sea fósforo	<operador> | <operador>	"googlear" | "yahoo"
~	Buscar sinónimos de lo dado palabra. No soportado por Google	~ <palabra>	~ libro
@	Realice una búsqueda sólo en el plataforma de redes sociales dada. Prefiero usar el sitio	@ <redes sociales>	@instagram
después	Buscar documentos publicados / indexado después de la fecha dada	después: <aa(-mm-dd)> después:2023-01-01	

PRINCIPALES OPERADORES DE BÚSQUEDA PARA DORKING

todo en título	Igual que intitle pero permite múltiples palabras clave separadas por un espacio	allintitle: <palabras clave>	allintitle:hola mundo
allinurl	Igual que inurl pero permite múltiples palabras clave separadas por un espacio	allinurl: <palabras clave>	allinurl: buscar com
todo en texto	Igual que intext pero permite múltiples palabras clave separadas por un espacio	allintext: <palabras clave>	allintext: universidad de ciencias matemáticas
ALREDEDOR	Busque documentos en los que la primera palabra tenga hasta 'n' palabras de distancia de la segunda palabra y viceversa	<palabra1> ALREDEDOR(<n>) <palabra2>	google ALREDEDOR(10) bien
autor	Busque artículos escritos por el autor determinado, si corresponde.	autor: <nombre>	autor:max
antes	Buscar documentos publicados / indexados antes de la fecha indicada	antes: <aa(-mm-dd)>	antes:2023-01-01
cache	Busque en la versión en caché del sitio web indicado. Utiliza el caché de Google para hacerlo	caché: <dominio>	caché: google.com
contiene	Busque documentos que enlacen al tipo de archivo dado. No soportado por Google	contiene: <tipo de archivo>	contiene:pdf
fecha	Busque documentos publicados en los últimos 'n' meses. No soportado por Google	fecha: <número>	fecha:3
definir	Busque la definición de la palabra dada.	definir: <palabra>	definir: divertido

PRINCIPALES OPERADORES DE BÚSQUEDA PARA DORKING

extensión	Buscar un tipo de archivo específico	text: <tipo de documento>	extensión:pdf
Tipo de archivo	Consulte la extensión	Tipo de archivo: <tipo de documento>	tipo de archivo:pdf
anclar	Busque la palabra clave dada en anclajes de un sitio web	ancla: <palabra clave>	anclaje: seguridad
índice de	buscar documentos que contiene descargas directas	índice de: <término>	índice de: vídeos mp4
información	Buscar información sobre un sitio web	información: <dominio>	información: google.com
en el texto	La palabra clave debe estar en el texto. del documento	texto: <palabra clave>	intexto:noticias
título	La palabra clave debe estar en el título. del documento	título: <palabra clave>	título: dinero
URL	La palabra clave debe estar en la URL. del documento	inurl: <palabra clave>	inurl:hoja
enlace/enlaces	Búsqueda de documentos cuyos Los enlaces contienen la palabra clave dada. Útil para encontrar documentos. ese enlace a un sitio web específico	enlace: <palabra clave>	enlace: google
ubicación	Mostrar documentos basados en el ubicación dada	ubicación: <ubicación>	Ubicación:Reino Unido

PRINCIPALES OPERADORES DE BÚSQUEDA PARA DORKING

rango numérico	Consulte 'm...n'	rango numérico: <número>- <número>	rango numérico: 1-1337
O	Consulte '|'	<operador> O <operador>	"google" O "yahoo"
directorio telefónico	Busque números de teléfono relacionados asociados con el nombre de pila	directorio telefónico: <nombre>	directorio telefónico: "elon musk"
relacionar / relacionado	Buscar documentos relacionados con el sitio web determinado.	relacionar: <dominio>	relacionar: google.com
fuente	Busque en un sitio de noticias específico. Prefiero usar el sitio	fuente: <noticias>	fuente:theguardian
sitio	Busque en el sitio indicado. El argumento dado también podría ser solo un TLD como com, net, etc.	sitio: <dominio>	sitio:google.com
existencias	Buscar información sobre una acción del mercado	valores: <valores>	valores: Microsoft
clima	Buscar información sobre el clima de la ubicación determinada.	clima: <ubicación>	clima:París