PRÁCTICA 3 UD 1: NAVEGADORES

Búsqueda avanzada en buscadores como Google, Bing , Robtex, Shodan o Spyse

Introducción

En el siguiente enlace existen múltiples opciones para definir con mayor precisión la consulta en Google https://www.google.com/advanced_search

En la parte derecha de los campos tienes ejemplos de los parámetros que puedes usar.

Pero además **Google** permite que indiques una serie de comandos para hacer búsquedas avanzadas. Algunos de los principales son:

- **” ”** : buscar frase exacta.
- **OR** puede ser reemplazado por el símbolo **|** .
- **NOT** puede ser reemplazado por el símbolo menos **-** . Ej: jaguar -coches: busca la palabra “jaguar”, pero omite las webs con la palabra “coches”
- **AND** puede ser reemplazado por un solo espacio (pulsando el espacio), pero los resultados pueden diferir si tecleamos AND específicamente entre las palabras.
  Nota: La búsqueda en Google distingue entre mayúsculas y minúsculas cuando usamos operadores lógicos. Por lo tanto, no puedes escribir oR, o anD, sino que debes usar mayúsculas o símbolos.
- ***** (asterisco): comodín, cualquier palabra.
- **intitle:** la palabra buscada está en el título.
  P.ej: intitle:mazinger
- **allintitle:** todas las palabras siguientes están contenidas en el título.
  P. ej: allintitle:coche historia apodado → muestra una página con las tres palabras en el título
- **inurl** o **allinurl**: la expresión buscada está en la URL. La diferencia entre ambas es como se indica en la anterior (una palabra o todas las palabras)
- **site**: sólo busca resultados dentro de la web que va detrás de “site:”.

P.ej: MACARRONES SITE:MERCADONA.ES

- **filetype** o **ext**: sólo busca archivos de una extensión (doc, xls, txt…) P.ej: filetype: sql
- **link**: sólo busca en páginas que tienen un link a una determinada web
- **inanchor**: sólo busca en páginas que tienen en el texto de enlace la expresión buscada
- **cache**: muestra el resultado en la caché de Google de una página web
- **related**: busca webs relacionadas con una determinada

Como información para ampliar, tienes la referencia de todos los operadores de búsqueda en los siguientes enlaces, aunque hay que indicar que Google elimina algunos de ellos y con el tiempo es muy posible que no funcionen (como es el caso del operador link):
https://ahrefs.com/blog/es/operadores-de-busqueda-avanzada-de-google/
https://www.xataka.com/basics/operadores-busqueda-para-google

BING

El buscador Bing tiene muchas similitudes con Google, pero también diferencias. Entre sus operadores podemos encontrar:

- **” ” :** buscar frase exacta. P.ej: "EL BARCELONA FICHA A MESSI"
- **OR** puede ser reemplazado por el símbolo | .
- **site**: sólo busca resultados dentro de la web que va detrás de “site:”. Además, permite indicar hasta dos niveles de directorios.
  P.ej: site: portal.edu.gva.es/iesserraperenxisa/
- **domain:** permite buscar en dominio y subdominios.
  P.ej: domain: gva.es
- **url:** indica si esa URL ha sido indexada o no por BING.
- **filetype**: sólo busca archivos de un tipo. Nota: en Bing el tipo no tiene porqué coincidir con la extensión. Un fichero .sql para bing es de tipo txt por tanto no mostraría ninguno.
  P.ej: filetype: txt
- **ext**: busca archivos con esa extensión.
- **ip**: indica todos los dominios o servidores virtuales que tiene la misma ip. Es una función muy interesante para averiguar los hostings compartidos en una misma ip. Actualmente parece que esa función está deshabilitada en Bing, aunque se puede suplir con la web https://ipinfo.io/<ip> sustituyendo <ip> por la que quieras consultar.
  P.ej: ip:87.98.231.18
- **feeds**: busca en los RSS la expresión indicada.
  P.ej: feeds:pedro martinez
- **contains**: busca páginas que contengan enlaces a ficheros con la extensión dada.
  P.ej: contains:sql
- **intitle, inbody, inanchor**: permite buscar términos en zonas específicas de la web.
- **instreamset(url)**: busca por palabras en la url. El comando inurl fue desactivado en Bing hace tiempo.
- **instreamset:(title url)**:busca por palabras en el título. Similar a intitle
- **loc**: Para buscar páginas localizadas en IPs relativas a un país. Hay que usar los códigos internacionales de cada país. P.ej: loc:es

Microsoft puede eliminar algunos de estos operadores porque no se utilicen y con el tiempo es muy posible que no funcionen.

SHODAN

Shodan no es el típico buscador de documentos, sino que se centra en recopilar información sobre servidores, redes o dispositivos como IoT, cámaras IP, etc. Es una excelente herramienta para realizar fingerprinting pasivo porque sin conectarnos a los dispositivos, podemos saber qué puertos abiertos tienen, qué servicios tienen en marcha y qué versiones: Shodan realiza esa tarea por nosotros.

Pero Shodan es un servicio de pago aunque tiene una versión gratuita limitada que se utiliza mediante registro. Por tanto para realizar la práctica, debes registrarte o iniciar sesión mediante Google, Twitter o Windows Live.

En https://help.shodan.io/the-basics/search-query-fundamentals tienes información sobre los comandos y operadores de búsqueda.

A continuación, mostramos algunos de ellos:

- **os**: busca por sistema operativo. P.ej: os:linux
  os:windows
- **port**: busca por puerto abierto
  P.ej: port:22
- **product** y **version**: permiten indicar un software y la versión, usando uno a ambos.
  P.ej: product: “iis” version: “6.0”
- **country**: busca por país con los códigos internacionales de dos caracteres
  P.ej: country:es

- **city**: busca por ciudad
  P.ej: country:es
- **net**: busca información sobre una red o un rango de direcciones IP
  P.ej: net:203.0.113.0/24
- **hostname**: permite buscar por un nombre de host
  P.ej: hostname:www.example.com
- **after** y **before**: permite filtrar los resultados que han sido recogidos antes o después de las fechas indicadas.
  P.ej: after:31-12-2015 before:10-11-2020
- **title**: busca en el título de la página

Además, Shodan incluye un buscador de exploits y vulnerabilidades en la siguiente url: https://exploits.shodan.io/

En la parte izquierda de la ventana permite aplicar filtro por base de datos de

ROBTEX

Robtex es, según sus creadores, la navaja suiza de Internet. Es capaz de encontrar información relacionada con el dominio de una organización, como por ejemplo otros servidores virtuales alojados en la misma IP, información de subdominios (similar a como hace fierce y otras herramientas de enumeración dns), otras direcciones IP que apuntan al dominio indicado, los routers a los que están conectados los servidores del dominio, el AS (sistema autónomo) o si el dominio se encuentra en alguna lista negra de SPAM (DNSBL).
Obtiene la información de fuentes OSINT como DNS, Whois, información de rutas BGP, Alexa (servicio web de estadísticas de sitios web), Sedo (mercado de compra/venta y subasta de dominios), etc.

SPYSE

Spyse es una excelente herramienta OSINT online que nos ofrece la posibilidad de realizar búsquedas relacionadas con los datos de un dominio, dirección IP, certificados, etc. Combina diferentes herramientas y servicios en un único lugar, incluso un escaner de puertos. Es una gran alternativa a Shodan o Robtex, ofreciendo incluso más servicios.

ACTIVIDADES

Ejercicio 1. Búsqueda de información con GOOGLE

Con ayuda de la información y los enlaces anteriores, realiza las siguientes búsquedas y tras observar los resultados, explica qué es lo que buscan analizando su sintaxis:

- intitle:"index of" inurl:/backup
- filetype:sql “MySQL dump” (pass|password|passwd|pwd)
- intitle:(confidential|restricted) filetype:pdf site:gov
- allintitle:index of queen mp3
- intitle:”index of” id_rsa -id_rsa.pub

- intitle:"index of" inurl:ftp
- inurl:robots.txt filetype:txt “disallow:”

APORTA CAPTURAS DE PANTALLA EN LAS QUE SE VEA LA FECHA.

En https://www.exploit-db.com/google-hacking-database tienes muchos más ejemplos de Google Dorks con la explicación de cada uno de ellos.

Ejercicio 2 Búsqueda de información con BING

Con ayuda de la información y los enlaces anteriores, realiza las siguientes búsquedas y tras observar los resultados, explica qué es lo que buscan analizando su sintaxis:

- filetype:xls name phone position ó filetype:xls nombre puesto telefono
- ext:log ws_ftp.log (“c:\users” OR “documents and settings”)
- intitle:"index of " queen contains:mp3
- filetype:txt ext:sql insert into password

APORTA CAPTURAS DE PANTALLA EN LAS QUE SE VEA LA FECHA.

Ejercicio 3 Búsqueda de información con Shodan

La versión gratuita tiene un límite de búsquedas por tiempo (además Conselleria corta el tráfico), así que es posible que te muestre un mensaje de error durante la práctica. En ese caso, indica cómo sería el comando de búsqueda aunque no adjuntes la captura.

- Busca máquinas con Windows en Madrid, España
- Busca máquinas en España con Terminal Server abierto (posible ataque con malware BlueKeep)
- Busca routers Asus RT-AC68U en Portugal (pt)
- Busca servidores Apache versión 2.4.6 en Centos en Francia (fr)

APORTA CAPTURAS DE PANTALLA EN LAS QUE SE VEA LA FECHA.

Ejercicio 4. Búsqueda de información del dominio de una organización con Robtex

Accede a Robtex y realiza alguna consulta sobre algún nombre de dominio o alguna dirección IP y adjunta una captura del resultado. Comenta brevemente el tipo de información que te muestra. *Para determinado tipo de información, es necesario hacer login. Puedes hacerlo de manera gratuita (aunque limitado como en Shodan) con una cuenta de Google.*

APORTA CAPTURAS DE PANTALLA EN LAS QUE SE VEA LA FECHA.

Ejercicio 5. Búsqueda de información de una organización con Spyse

Accede a Spyse y utiliza algunas de las herramientas que incluye explicando lo que hacen. Utiliza como host o dominio para las consultas (según lo que te pidan), el servidor web https://portal.edu.gva.es/iesserraperenxisa/ o el dominio gva.es respectivamente.
En algunos casos debes introducir la IP y no el nombre de dominio (fqdn). Se propone realizar como ejemplo las siguientes herramientas (menú Tools superior):
- Información sobre un host IPv4
- IP Lookup
- Port Scanner
- Reverse IP Lookup

- Website Technology Checker- SSL Lookup Service

APORTA CAPTURAS DE PANTALLA EN LAS QUE SE VEA LA FECHA.

Comenta brevemente el tipo de información que te muestra en cada herramienta

NOTA: habrás observado que prácticamente todas las herramientas web que hemos propuesto tienen la opción de usar una API. De esta forma se pueden automatizar las búsquedas usando lenguajes como bash, python, perl, powershell, etc de tal manera que la fase de recopilación de información se acelere.