***Lo primero es describir con tus palabras en qué consiste el dorking o google hacking.***

Es el hecho de hacer búsqueda avanzada de Google para conseguir encontrar en internet aquella información concreta a base de ir filtrando los resultados con operadores; “los dorks”.



***Lo segundo y antes de pasar a investigar con operadores y filtros de búsquedas en internet, dame 3 razones para usar estas búsquedas.***

1. Busca contraseñas almacenadas en ficheros txt, lógicamente, sin cifrar

**Site:\*.\*es (password | passwd | contraseña | login) ext:txt**

1. Busca registros de conversaciones guardadas en diferentes servidores.

**intext:"Index of /chatlogs"**

1. Busca volcados (DUMP) de bases de datos MySQL donde se encuentren registros del tipo pass|password|passwd|pwd.

**inurl:backup filetype:sql ( pass | password | passwd | pwd )**

1. Busca datos que se guarden entre los ficheros de las web gubernamentales.

**site:\*.gob.es (ext:pdf | ext:xls | ext:doc)**

1. Busca ficheros de carácter sensible, pero se centra más en las webs que compartan información con intranets.

**site:intranet.\*.\*/login/**

**inurl:/intranet/login.ph**p

1. Busca lo que el dominio de la web de amazon NO quiere que veamos… XD

**site:www.amazon.es robots.txt**

1. Busca cámaras ip online disponibles para ser visionadas, ¿crees que alguna de ellas podríamos controlarla?

**intitle:"yawcam" "It's a webcam!" "user" "pass"**

**intitle:"webcamXP 5" inurl:8080 'Live'**

**intitle:"active webcam page"**

1. Localiza curriculums de gente en alguna web, ya sea algún departamento de recursos humanos como cualquier otro portal donde haya datos de candidatos.

**site:linkedin.com/in OR site:linkedin.com/pub -intitle:profiles -inurl:dir "curriculum vitae" OR cv**

1. Busca datos como correos electrónicos, teléfonos de contacto de responsables de Telefónica de España.

**site:telefonica.es intext:"contacto" ejecutivo**

1. Buscar cuentas bancarias con su saldo.

**(intext:iban | intext:swift) & (intext:saldo | intext:balance) & (ext:xls | ext:doc)**

1. Extraer lista de productos y precios de algún sitio comercial.

**intitle:"index of" "/products" prices**

1. Obtener listado de jugadores de algún equipo del deporte que sea con algún dato más personal, indagando en la web del equipo.
2. **site:\*.cdmostoles.com (ext:pdf | ext:xls | ext:doc)**
3. Intentar sacar todo tipo de archivos con datos sensibles de la web del CRN.

**site:cftic.centrosdeformacion.empleo.madrid.org (ext:pdf | ext:xls | ext:doc)**