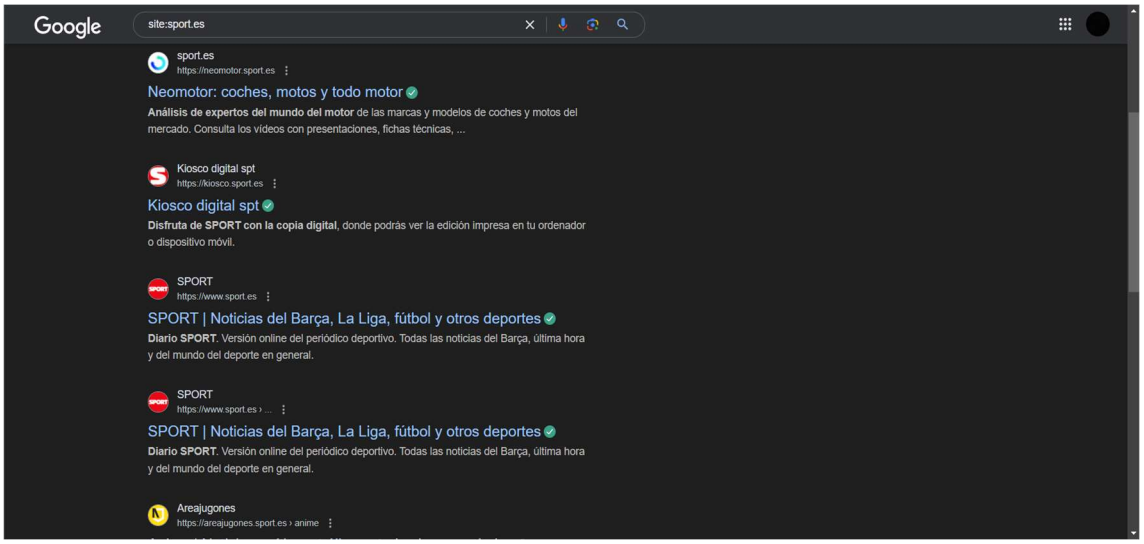
Recopilación Pasiva de Información utilizando Google Hacking y Shodan

ADRIÁN CONESA GUIRAO

Contenido

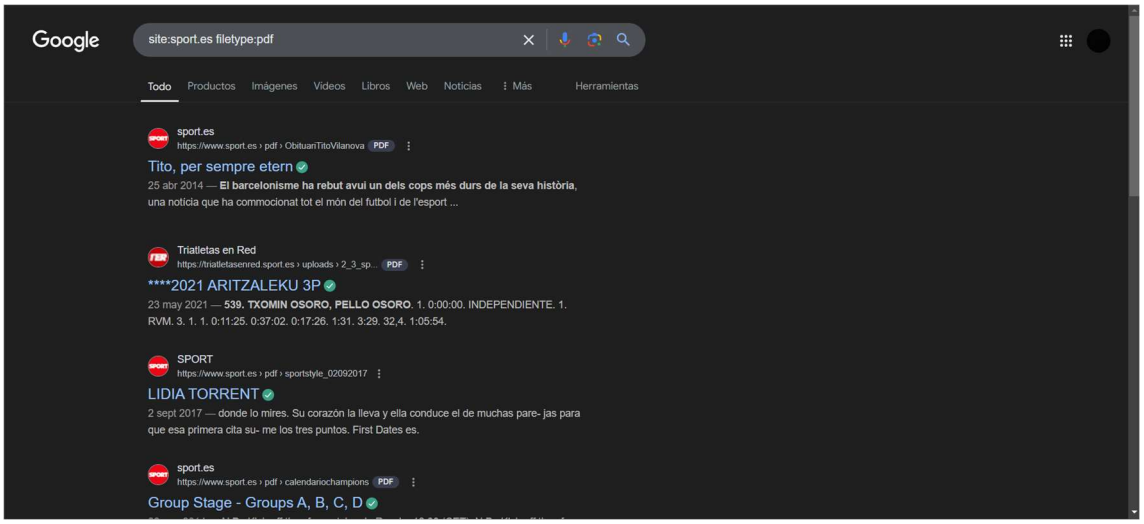
Parte 1: Google Hacking

Búsqueda en Google



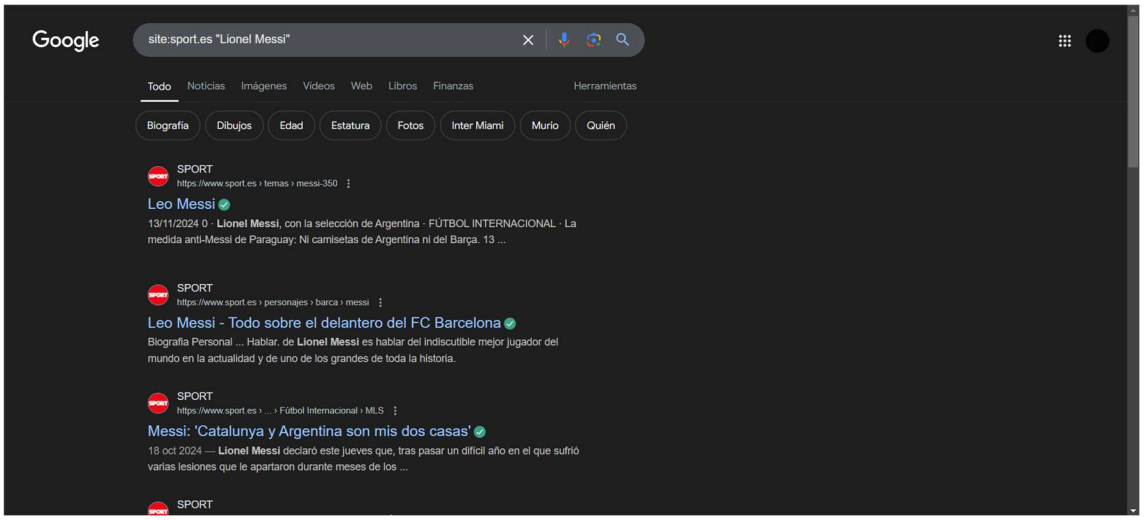
Mi primera búsqueda es “site:sport.es” me sale algunas páginas antes de la que yo busco pero en la que me centraré será el Diario Sport.

Comando site: Esto devolverá todos los resultados de Google relacionados con el dominio sport.es.



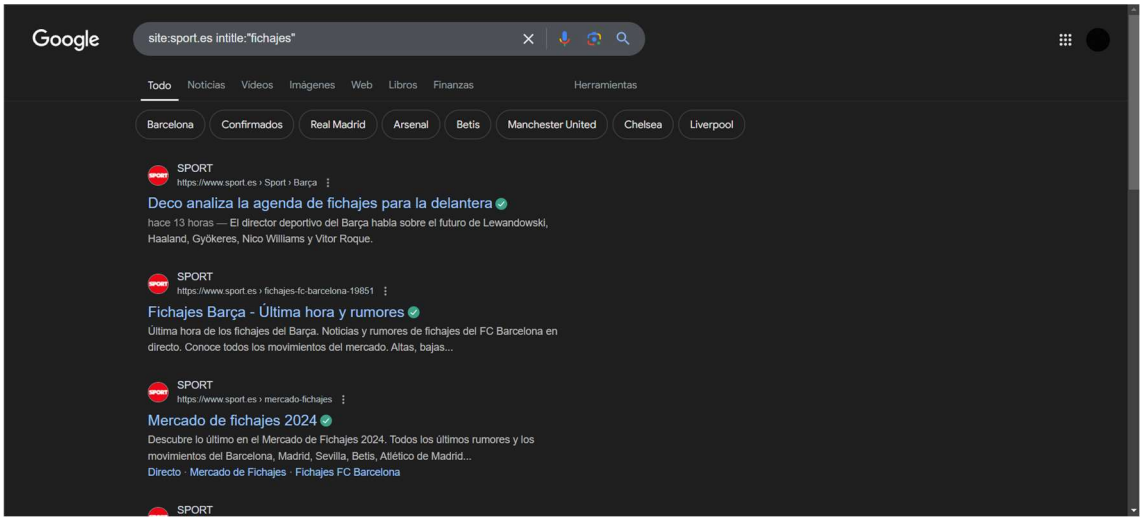
La segunda búsqueda que he hecho ha sido “site:sport.es filetype:pdf”

Filetype: Buscará archivos en formato PDF dentro del sitio web del dominio puesto.



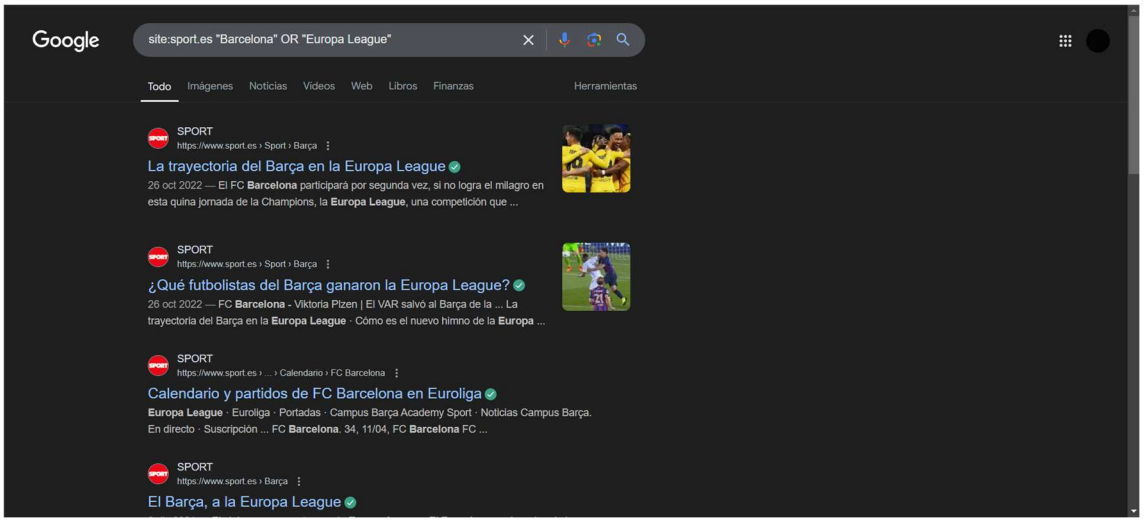
La búsqueda que he hecho ha sido “site:sport.es "Lionel Messi"

Uso de comillas: De esta manera le estamos pidiendo que busque dentro del dominio las páginas que mencionen lo puesto entre las comillas en mi caso que nombren a Lionel Messi



La búsqueda que he hecho ha sido “site:sport.es intitle:"fichajes" “

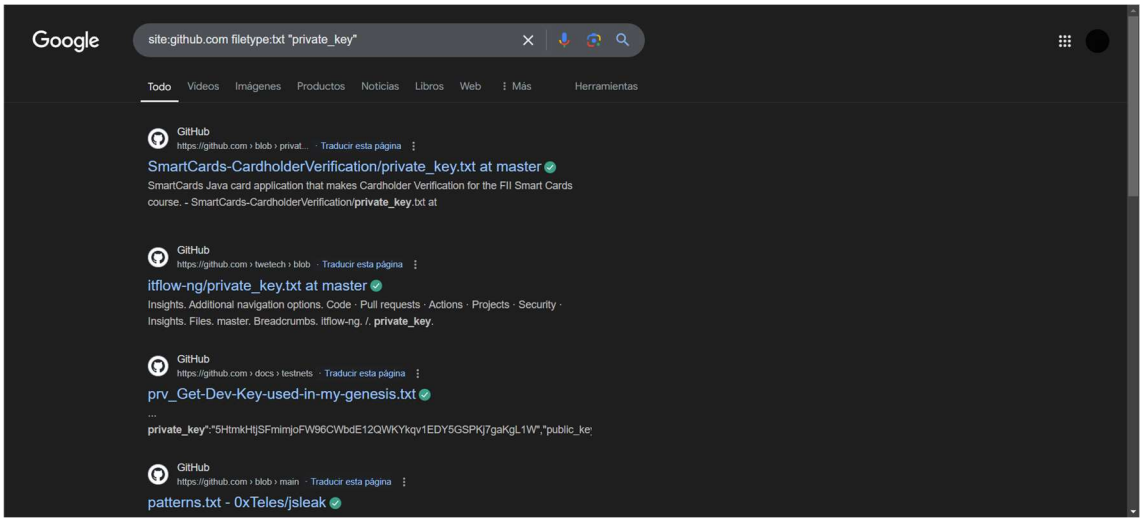
Intitle: De esta manera le pedimos que nos enseñe en el dominio un titulo en específico que contenga en mi caso la palabra “fichajes”



La búsqueda que he hecho ha sido “site:sport.es "Barcelona" OR "Europa League" “

OR: Le pedimos de esta manera que busque las páginas que contiene las palabras Barcelona o Europa League

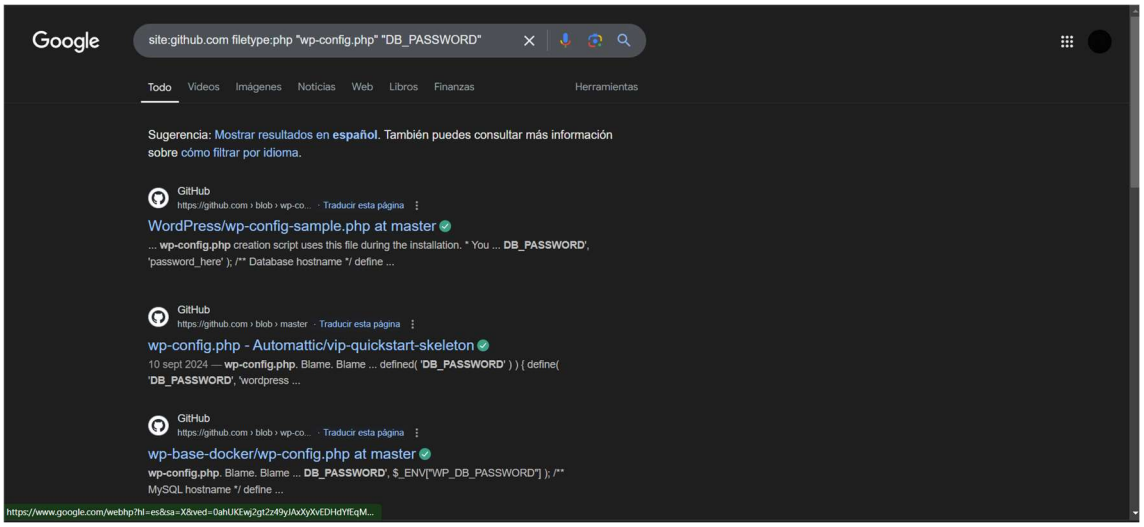
Consultas con Google Dorks



La búsqueda ha sido “site:github.com filetype:txt "private_key" “

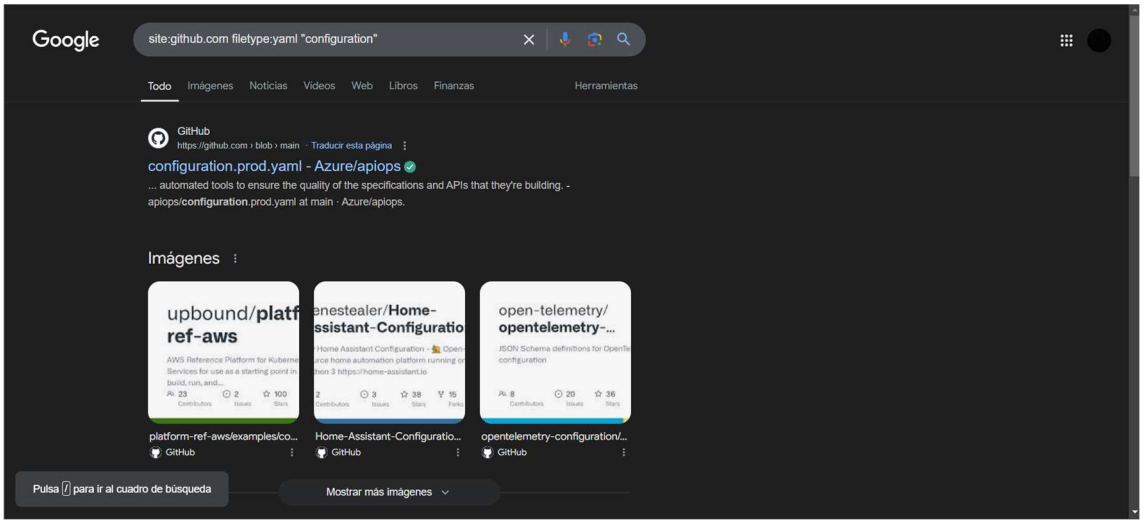
Búsqueda: Este dork busca archivos de texto (filetype:txt) en GitHub que contengan la frase "private_key".

Las claves privadas son fundamentales para la seguridad de los repositorios y si se exponen públicamente, pueden comprometer su seguridad



La búsqueda que he hecho ha sido “site:github.com filetype:php "wp-config.php" "DB_PASSWORD" “

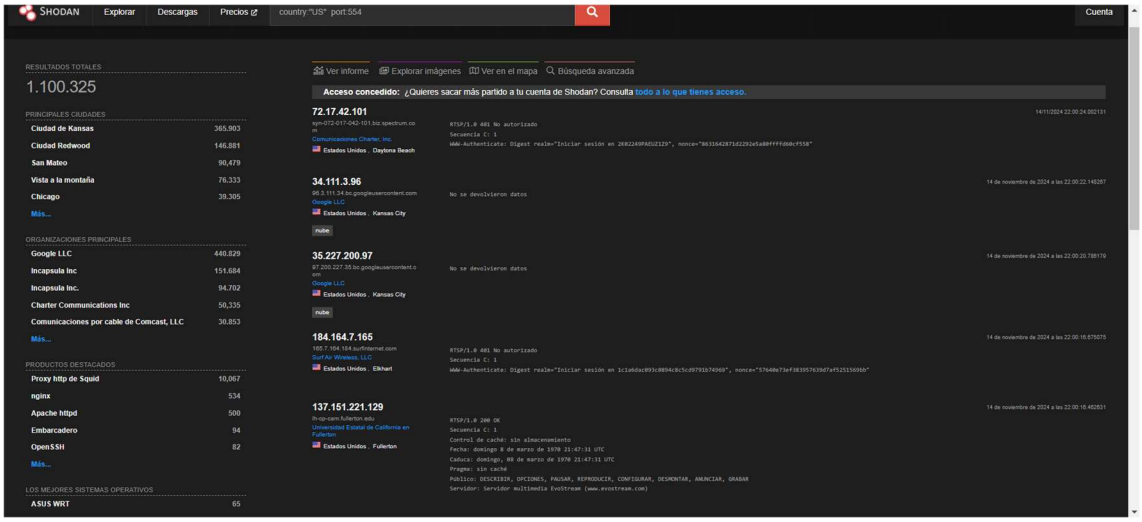
Búsqueda: Esta consulta buscará archivos PHP con el nombre "wp-config.php" y la palabra clave "DB_PASSWORD" en GitHub.



La búsqueda que he hecho ha sido “site:github.com filetype:yaml "configuration" “

Búsqueda: Esta consulta buscará archivos de tipo Yaml con el nombre "configuration " en GitHub.

Búsqueda en Shodan



La búsqueda que he hecho ha sido “country”US” port:554”

Búsqueda: He pedido que me aparezca lo que haya en Estados Unidos en el puerto 554 que según en visto en Google es el puerto en el que suelen estar las cámaras Ip

Resultados totales

1.100.325

Algunas de las IP´S encontradas

72.17.42.101

34.111.3.96

35.227.200.97

184.164.7.165

137.151.221.129

Principales ciudades

Ciudad de Kansas 365.903

Ciudad Redwood 146.881

San Mateo 90,479

Vista a la montaña 76.333

Chicago 39.305

Organizaciones principales

Google LLC 440.829

Incapsula Inc 151.684

Incapsula Inc. 94.702

Charter Communications Inc 50,335

Comunicaciones por cable de Comcast, LLC 30.853

Productos destacados

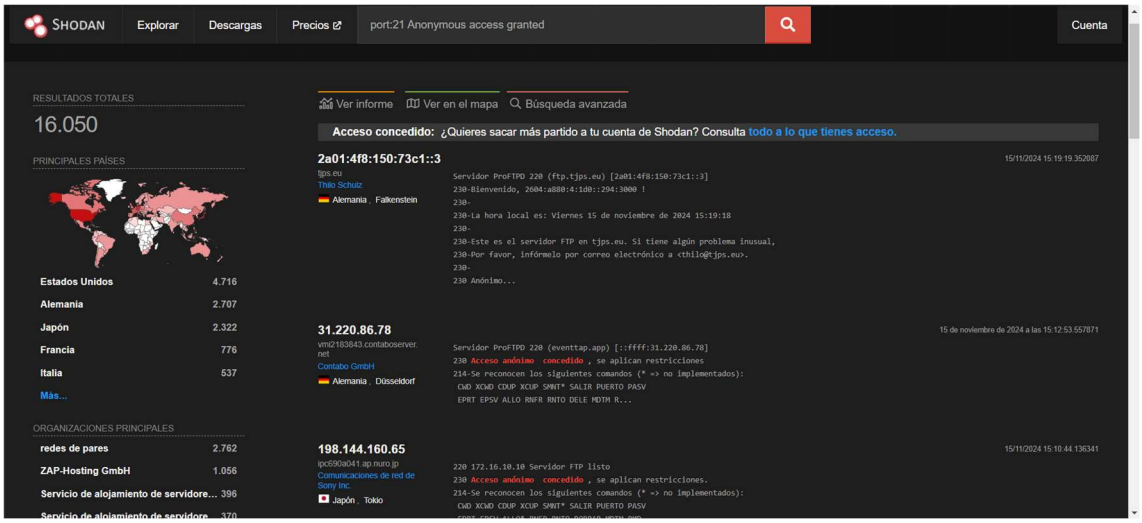
Proxy http de Squid 10,067

nginx 534

Apache httpd 500

Embarcadero 94

OpenSSH 82



He buscado todos los puertos 21 (Servidores FTP) los cuales tengan el acceso anónimo aceptado. “port:21 Anonymous Access granted”

Resultados obtenidos

Total

16.050

Principales países

Estados Unidos 4.716

Alemania 2.707

Japón 2.322

Francia 776

Italia 537

Organizaciones principales

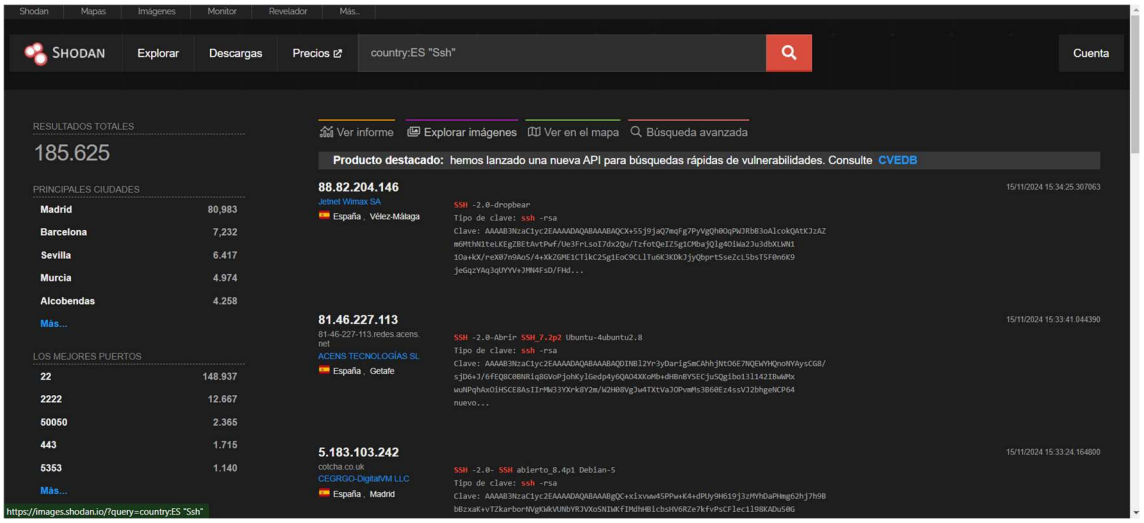
redes de pares 2.762

ZAP-Hosting GmbH 1.056

Servicio de alojamiento de servidores (NTTPCCommunications,Inc.) 396

Servicio de alojamiento de servidores (NTTPC Communications, Inc.) 370

Deutsche Telekom AG 366



Le he pedido que me busque en España las direcciones que tenga de tipo de clave Ssh

Resultados obtenidos

Resultados totales

185.625

Principales ciudades

Madrid 80,983

Barcelona 7,232

Sevilla 6.417

Murcia 4.974

Alcobendas 4.258

Los mejores puertos

22 148.937

2222 12.667

50050 2.365

443 1.715

5353 1.140

Organizaciones principales

TELEFÓNICA DE ESPAÑA SAU 21.136

IONOS SE 12.671

arsys.es 10,581

Telefónica de España SAU 9,384

Google LLC 9,216

Reflexión ética

Google Hacking y Shodan son herramientas poderosas que pueden ser utilizadas para mejorar la seguridad de los sistemas informáticos. Sin embargo, su uso debe ser responsable y ético. Es importante recordar que un mal uso de estas herramientas puede hacer que cometas un delito.

Riesgos y Consecuencias

- **Acceso no autorizado:** El uso de estas herramientas para acceder a sistemas o información sin autorización previa constituye un delito informático.
- **Daños a terceros:** La explotación de vulnerabilidades encontradas puede causar pérdidas económicas, interrupción de servicios esenciales o incluso poner en riesgo la seguridad de personas.
- **Reputación dañada:** Tanto la persona que realiza el ataque como la organización afectada pueden sufrir un grave daño a su reputación.

- **Persecución legal:** Las actividades ilícitas en el ciberespacio están penadas por la ley en la mayoría de los países dependiendo de la gravedad del delito variaran las penas.

Hacker Ético

Un hacker ético es aquel que utiliza sus conocimientos y habilidades para identificar vulnerabilidades en sistemas informáticos con el objetivo de mejorar la seguridad. Sin embargo, incluso los hackers éticos deben actuar de manera responsable y ética.

- Es fundamental obtener el permiso explícito de los propietarios de los sistemas antes de realizar cualquier tipo de prueba de penetración.
- Una vez identificadas las vulnerabilidades, deben ser reportadas de manera responsable a los responsables de la seguridad del sistema.
- Un hacker ético no debe aprovechar las vulnerabilidades encontradas para obtener beneficios personales o causar daños.
- Es esencial conocer y respetar las leyes y regulaciones aplicables en materia de ciberseguridad.