

# **Recopilación Pasiva de Información utilizando Google Hacking y Shodan**

## Contenido

<b>Parte 1: Google Hacking</b> .....	3
Búsqueda de Google: .....	3
Consulta con Google Dorks .....	5
<b>Parte 2: Shodan</b> .....	7
Exploración de Shodan .....	7
<b>Parte 3: Reflexión ética</b> .....	8
¿Cuáles son las responsabilidades éticas y legales de un hacker ético en este contexto? .....	8

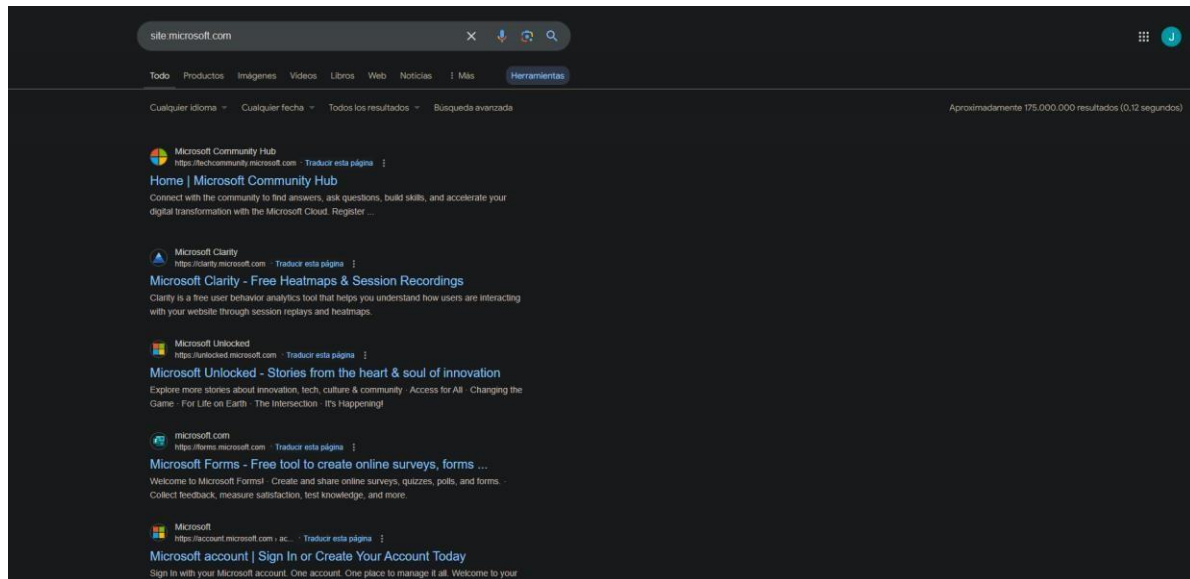
## Parte 1: Google Hacking

Búsqueda de Google:

**Buscar todas las URL indexadas de Microsoft (175.000.000 resultados)**

**“site:microsoft.com”**

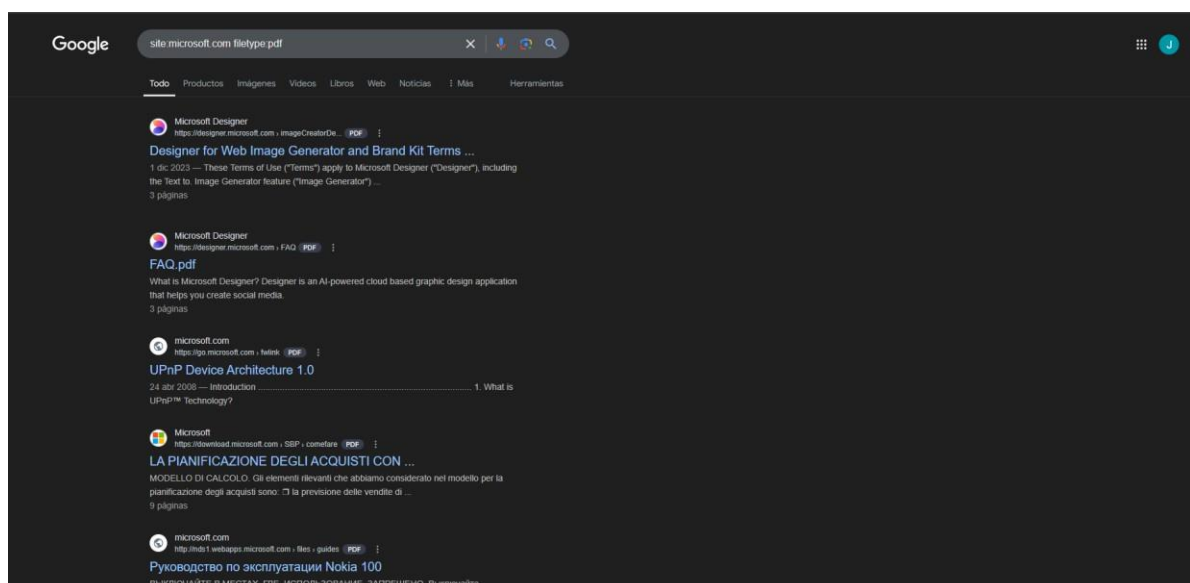
Esto muestra todas las páginas indexadas en el dominio de Microsoft.



**Buscar archivos PDF en el dominio de Microsoft:**

**“site:microsoft.com filetype:pdf”**

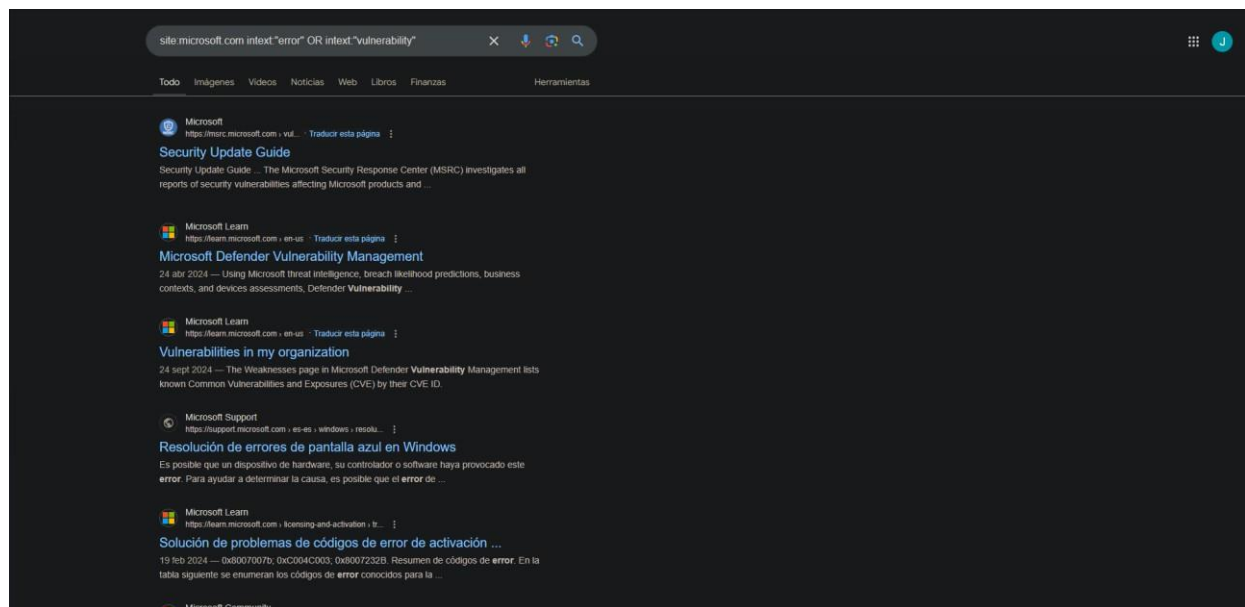
Muestra archivos en formato PDF que están en el dominio microsoft.com.



**Buscar información sobre errores o vulnerabilidades:**

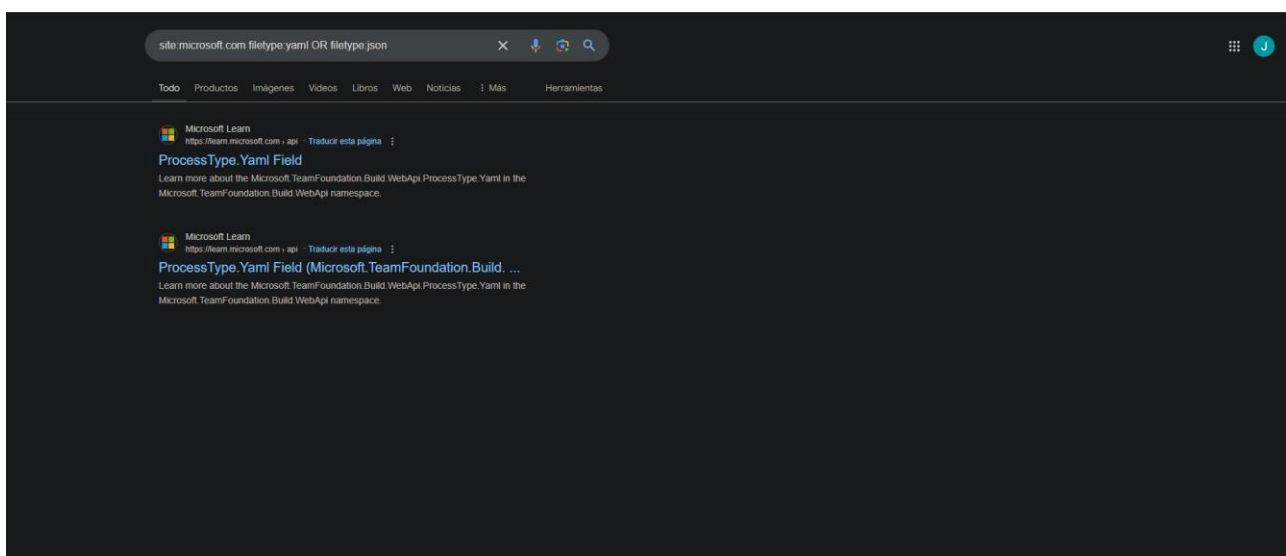
“site:microsoft.com intext:"error" OR intext:"vulnerability"”

Busca páginas dentro de Microsoft que muestren "error" o "vulnerability", lo que puede ser útil para encontrar errores conocidos o información sobre vulnerabilidades.

**Buscar archivos de configuración YAML o JSON:**

“site:microsoft.com filetype:yaml OR filetype:json”

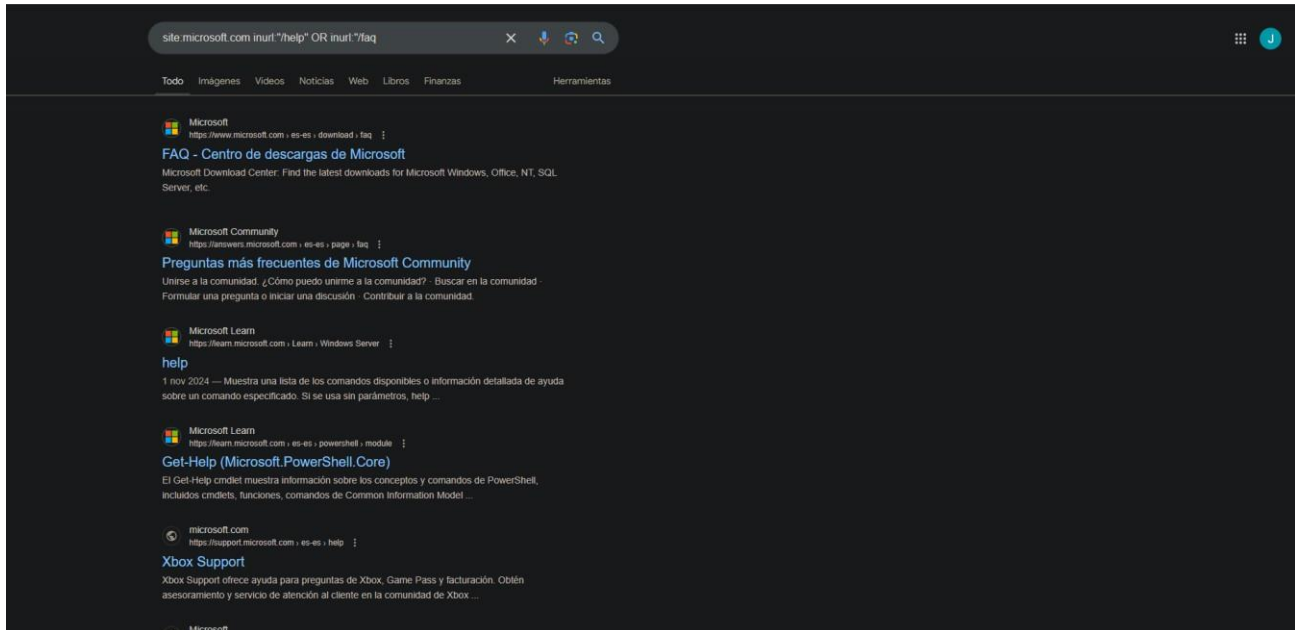
Esto identifica archivos YAML o JSON, que pueden incluir configuraciones o parámetros públicos.



**Buscar recursos de ayuda o preguntas frecuentes:**

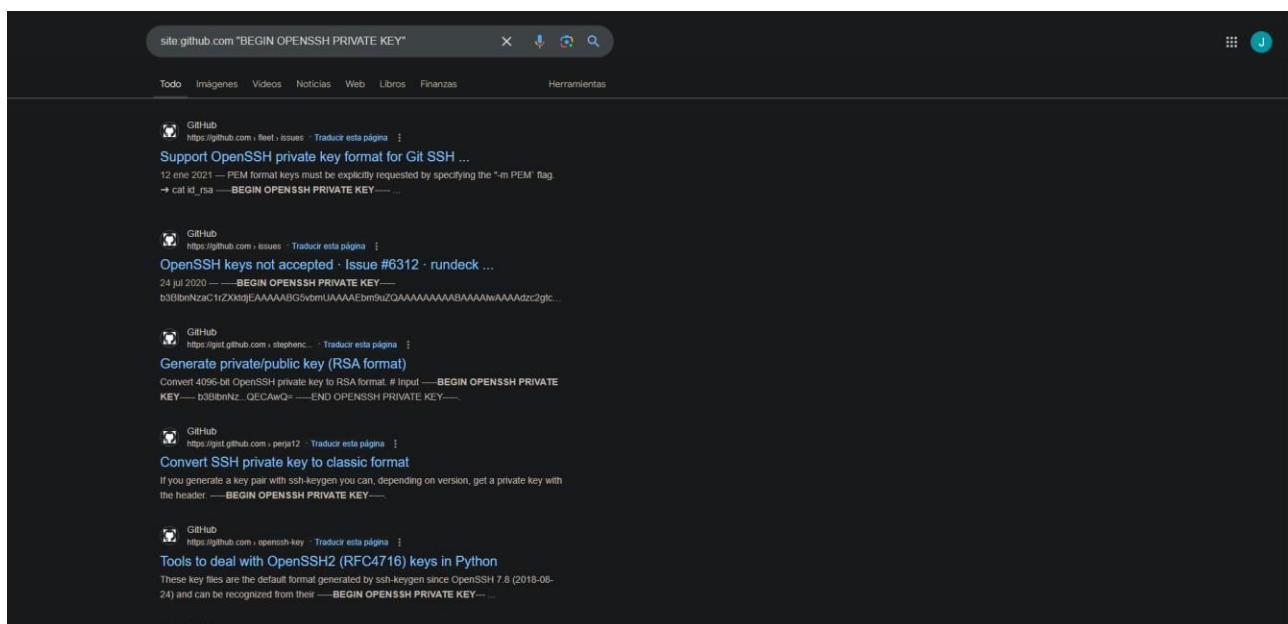
"site:microsoft.com inurl:"/help" OR inurl:"/faq"

Encuentra páginas de ayuda y preguntas frecuentes.

**Consulta con Google Dorks:**

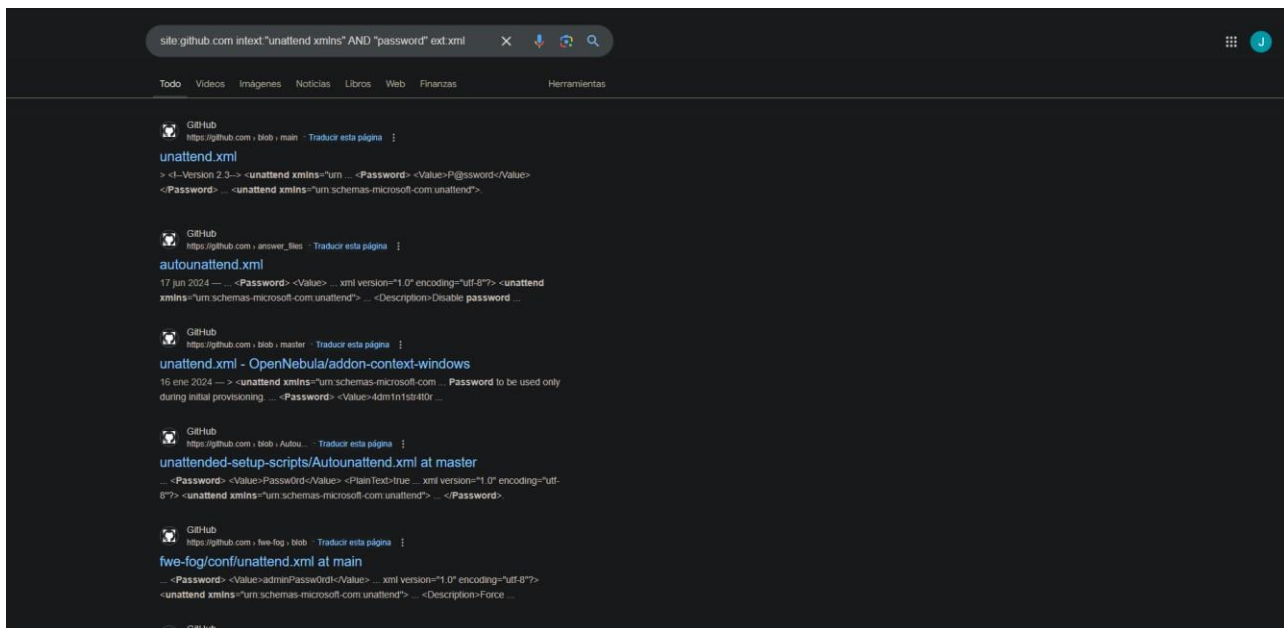
"site:github.com \"BEGIN OPENSSSH PRIVATE KEY\""

Muestra las claves privadas SSH, lo cual llama mucho la atención porque esta clave permite autenticación en servidores remotos, y si está expuesta en un repositorio público, cualquiera que la encuentre podría obtener acceso a los servidores o sistemas asociados con esa clave.



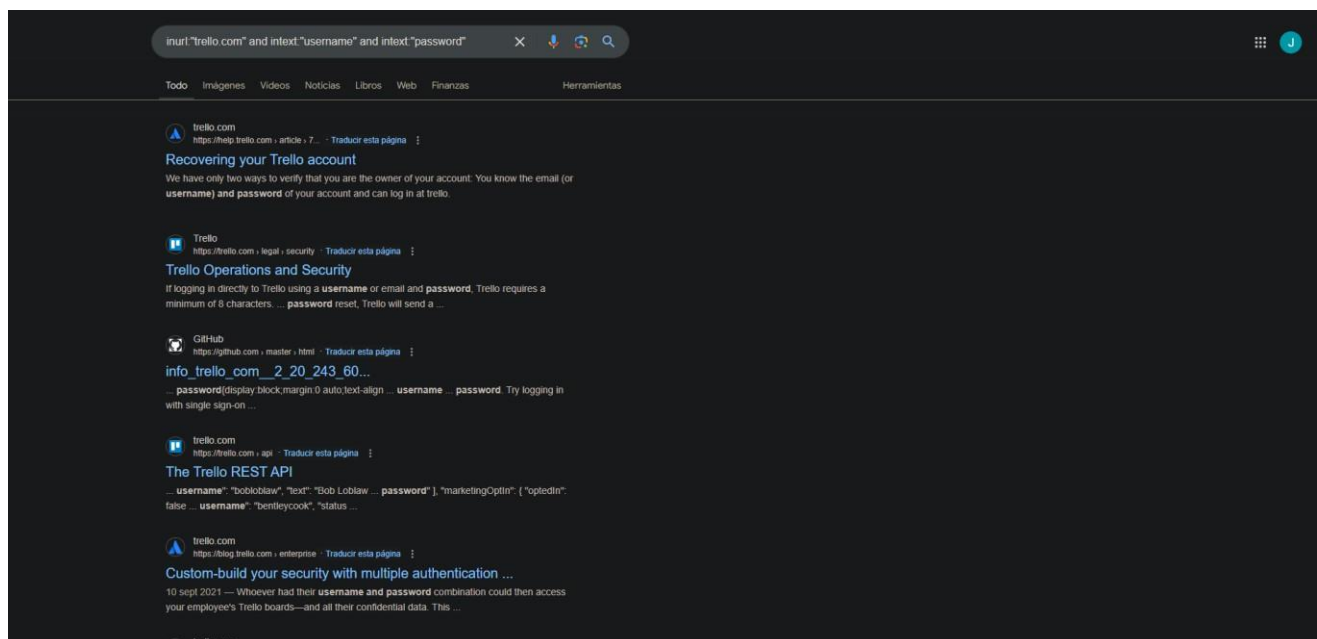
“site:github.com intext:"unattend xmlns" AND "password" ext:.xml”

Esta consulta busca archivos conocidos como "unattended" o "desatendidos" en repositorios de GitHub, que contienen contraseñas y están en formato XML.



“inurl:"trello.com" and intext:"username" and intext:"password"”

Busca tableros de Trello que tengan las palabras "username" y "password" en su contenido. Esto puede identificar posibles credenciales u otra información de inicio de sesión que haya sido publicada accidentalmente en tableros públicos de Trello.



## Exploración de Shodan:

Busca dispositivos en España (country:"ES") que tengan el puerto 8080 abierto.

SHODAN

[Explore](#)
[Downloads](#)
[Pricing](#)

port:8080 country:"ES"

Q

Account

TOTAL RESULTS

77,132

TOP CITIES

Madrid	25,660
Sevilla	2,936
Barcelona	2,346
Vigo	1,596
Águlas	1,530

More...

TOP ORGANIZATIONS

TELEFONICA DE ESPAÑA S.A.U.	12,232
Invermar Solutions SL	5,530
Telefonica de Espana SAU	5,371
Orange Espagne SA	2,462
GLOBAL MOBILE OPERATOR	2,290

More...

TOP PRODUCTS

Apache httpd	4,826
lighttpd	3,994
Hikvision IP Camera	3,514
nginx	2,511
QNAP	1,531

More...

TOP OPERATING SYSTEMS

154.26.76.107	HTTP/1.1 400 Bad Request
---------------	--------------------------

View Report

Browse Images

View on Map

Advanced Search

Partner Spotlight: Looking for a Splunk alternative to store all the Shodan data? Check out [Gravwell](#)

83.48.18.168

162-nd-83-45-10-static.rima-tde.net

Telefonica de Espana SAU

Spain, Madrid

HTTP/1.1 200 OK

Date: Thu, 14 Nov 2024 21:51:51 GMT

Server: httpd/2.4.18

Content-Type: text/html; charset=utf-8

Last-Modified: Wed, 19 Jun 2024 06:21:11 GMT

Accept-Ranges: bytes

Content-Length: 500

Vary: Accept-Encoding

Qnap TS-430P II:

Hostname: HERCULES2

Model:

Model Name:...

403 Forbidden

90.84.162.16

GBS OGB MONEY AS2285

Spain, Madrid

HTTP/1.1 403 Forbidden

Server: openresty

Date: Thu, 14 Nov 2024 21:46:47 GMT

Content-Type: text/html

Connection: keep-alive

Content-Length: 314

Via: 0.0.0.0:8080 (B-R0002-C000051)

X-CDN-Forwarded-For: 90.84.162.16

45.134.213.182

45-134-213-182-datapacket.co.in

Dataramp Limited

Spain, Madrid

No data returned

ERROR: The requested URL could not be retrieved

154.26.76.107

HTTP/1.1 400 Bad Request

2024-11-14T21:51:53.291673

2024-11-14T21:46:47.080207

2024-11-14T21:46:01.003614

2024-11-14T21:43:05.797205

SHODAN | 
 Explore | 
 Downloads | 
 Pricing ↗ | 
  Search | 
 Account

91.193.154.192

Regular View | 
 > Raw Data

General Information	
Hostnames	91.193.154.192 radiokable.net
Domains	<span style="border: 1px solid green; padding: 2px;">RADIOKABLE.NET</span>
Country	Spain
City	Madrid
Organization	RADIOCABLE INGENIEROS S.L.
ISP	RADIOCABLE INGENIEROS S.L.
ASN	AS199478

### Open Ports

8080

// **8080** / TOP 🔍

58662458 | 2024-11-26T18:14:12.89767Z

### 403 Forbidden

```
HTTP/1.1 403 Forbidden
Content-Type: text/html; charset=utf-8
Content-Length: 106
Set-Cookie: JSESSIONID=deleted; Expires=Thu, 01 Jan 1970 00:00:00 GMT; Path=/; HttpOnly
Connection: close
```

## Información relevante:

- Dirección IP: 91.193.154.192
- Hostnames: 91.193.154.192, radiokable.net
- Dominios: RADIOKABLE.NET
- País: España
- Ciudad: Motril
- Organización: RADIOCABLE INGENIEROS S.L.
- ISP: RADIOCABLE INGENIEROS S.L.
- ASN: AS199478
- Puertos abiertos:
- 8080/TCP: Devuelve un código de error 403 Forbidden. Esto significa que el acceso al servicio en ese puerto está prohibido.

## ¿Qué significa esto?

La información proporcionada por Shodan es un servidor web propiedad de RADIOCABLE INGENIEROS S.L. y ubicado en España.

El hecho de que el puerto 8080 esté abierto, pero devuelva un error 403 indica que el servicio web está activo pero no es accesible públicamente.

## ""Cisco" country:"CA""

Busca dispositivos relacionados con Cisco en Canadá (country:"CA"). Esto es útil para ver qué dispositivos de esa marca están expuestos en la región.

Aparecen 2.801 resultados, las ciudades donde más se encontraron resultados, otros puertos de escucha y otras organizaciones

SHODAN Explore Downloads Pricing [org:"Cisco" country:"CA"](#) Account

TOTAL RESULTS  
**2,801**

View Report View on Map Advanced Search

Access Granted: Want to get more out of your existing Shodan account? Check out [everything you have access to.](#)

**23.89.242.123**  
info2mcs222.gcp.pub.webex.com  
Cisco Webex LLC  
Canada, Toronto  
RTSP/1.0 200 OK  
CSeq: 1  
Public: DESCRIBE, SETUP, TEARDOWN, PLAY

**23.90.96.68**  
esa2.hc545-88.ca.iphmx.com  
esa1.hc545-88.ca.iphmx.com  
mx1.hc545-88.ca.iphmx.com  
mx2.hc545-88.ca.iphmx.com  
Cisco Systems Ironport Division  
Canada, Toronto  
starttls

**SSL Certificate**  
Issued By: HybridMD Server CA 01  
Issued To: mx1.hc545-88.ca.iphmx.com  
Organization: Cisco Systems Inc.  
Supported SSL Versions: TLSv1.2

220 esa.hc545-88.ca.iphmx.com ESMTP  
250 esa.hc545-88.ca.iphmx.com  
250-8BITMIME  
250-SIZE 41943940  
250 STARTTLS

**23.89.194.77**  
webex.com  
www.webex.com  
info2mcs222.webex.com  
Cisco Webex LLC  
Canada, Montreal

**SSL Certificate**  
Issued By: HybridMD Server CA 01  
Content-Type: application/octet-stream  
Cache-Control: no-cache  
Pragma: no-cache

HTTP/1.1 400 Bad Request

TOP CITIES  
Toronto 1,898  
Montreal 733  
Vancouver 370

TOP PORTS  
443 810  
80 734  
25 428  
8554 280  
3128 194  
[More...](#)

TOP ORGANIZATIONS  
Cisco Webex LLC 1,483  
Cisco OpenDNS LLC 787  
Cisco Systems Ironport Division 509  
Cisco OpenDNS, LLC 18  
Cisco Systems 2



En el caso de “23.89.242.124”

**SHODAN** Explore Downloads Pricing  Type / to search

23.89.242.123 ☐ Regular View ☒ Raw Data

**General Information**

Hostnames	mlo2mcs222.gcp.pri.webex.com mlo2mcs222.gcp.pub.webex.com
Domains	<a href="#">WEBEX.COM</a>
Country	Canada
City	Toronto
Organization	Cisco Webex LLC
ISP	Google LLC
ASN	AS396982

**Open Ports**

80 443 8554

// 80 / TCP

HTTP/1.1 406 Not Acceptable  
Content-Length: 0

// 443 / TCP

HTTP/1.1 406 Not Acceptable  
Content-Length: 0

**SSL Certificate**

Certificate:  
data:  
version: 3 (X.509)  
Serial Number:  
04:30:6d:78:ae:2c:85:d7:c6:eb:ff:fb:53:89:c4:f2:50:e4  
Signature Algorithm: sha256withRSAEncryption  
Issuer: CAUS, O=Let's Encrypt, CN=All  
Validity  
Not Before: Sep 22 15:45:31 2024 GMT  
Not After: Dec 21 15:45:30 2024 GMT

Información relevante:

- Dirección IP: 23.89.242.123
- Hostnames: [se quitó una URL no válida], mlo2mcs222.gcp.pub.webex.com
- Dominios: WEREK.CON
- País: Canadá
- Ciudad: Toronto
- Organización: Cisco Webex LLC, Google LLC
- ISP: Google LLC
- ASN: AS396982
- Puertos abiertos:
- 80/TCP: HTTPS, con un certificado SSL válido.
- 443/TCP: HTTPS, con un certificado SSL válido.

¿Qué significa esto?

La información proporcionada por Shodan es un servidor web utilizado por Cisco Webex LLC y alojado en la infraestructura de Google Cloud Platform.

Los servicios web ofrecidos en este servidor están protegidos con HTTPS, lo que garantiza la seguridad de la comunicación.

El dominio WEREK.CON podría estar asociado a alguna aplicación o servicio específico de Cisco Webex.

**"port:80 org:"Amazon" country:"DE"**

Busca dispositivos en el puerto 80 (HTTP) de Amazon en Alemania (country:"DE"), lo cual podría incluir servidores web de Amazon Web Services

Ha habido 2.987 resultados, la ciudad donde más resultados hay es Frankfurt, varias organizaciones de Amazon y los productos mas top.

**SHODAN** Explore Downloads Pricing **port:80 org:"Amazon" country:"DE"** Account

**TOTAL RESULTS**  
2,987

**TOP CITIES**

City	Count
Frankfurt am Main	2,984
Hannover	2
Berlin	1

**TOP ORGANIZATIONS**

Organization	Count
Amazon Technologies Inc.	2,296
Amazon Data Services NoVa	608
Amazon Data Services Ireland Ltd	80
AMAZON.ACE	2
Amazon Web Services, Inc.	1

**TOP PRODUCTS**

Product	Count
Amazon S3 httpd	554
AWS ELB	26
nginx	19
Apache httpd	8
CloudFront httpd	3

**Access Granted:** Want to get more out of your existing Shodan account? Check out [everything you have access to.](#)

**52.219.75.185**  
s3-eu-central-1.amazonaws.com  
Amazon Technologies Inc.  
Germany, Frankfurt am Main  
cloud

HTTP/1.1 387 Temporary Redirect  
x-amz-id-2: QESZu8yM/eges5AZBACklyMa3C6STGhsl/codJq3jkbac3qubvtZu0K1x1773av9e=  
x-amz-request-id: STDH9E76CQ733  
Date: Thu, 14 Nov 2024 21:37:56 GMT  
Location: https://aws.amazon.com/s3/  
Content-Length: 0  
Server: AmazonS3

**301 Moved Permanently**  
52.219.46.38  
s3-eu-central-1.amazonaws.com  
Amazon Technologies Inc.  
Germany, Frankfurt am Main  
cloud

HTTP/1.1 301 Moved Permanently  
x-amz-error-code: websiteRedirect  
x-amz-error-message: Request does not contain a bucket name.  
x-amz-request-id: 6TKH2230M2784Y5  
x-amz-id-2: 4G28T6M210M032KUPC4FV54B6g0p9v3J0R0dUSAfPYCQEIhRQ7Iyqer34C60Vh6z0ek=  
Location: https://aws.amazon.com/s3/  
Content-Length: 0  
Server: AmazonS3

**52.219.171.5**  
s3-eu-central-1.amazonaws.com  
Amazon Technologies Inc.  
Germany, Frankfurt am Main  
cloud

HTTP/1.1 387 Temporary Redirect  
x-amz-id-2: UH6Gp3ukhp3KVRIP23Fzw07118GHT0M0Ibvka9qZ1KQ0g0hcQ4r3d/648/EbawecFLAQ0=  
x-amz-request-id: XHAGQ0E1E32FTNAN  
Date: Thu, 14 Nov 2024 21:31:87 GMT  
Location: https://aws.amazon.com/s3/  
Content-Length: 0  
Server: AmazonS3

**52.219.170.97**  
s3-eu-central-1.amazonaws.com  
Amazon Technologies Inc.  
Germany, Frankfurt am Main  
cloud

HTTP/1.1 387 Temporary Redirect  
x-amz-id-2: f4s1v135fFV5161Q0yM54VBE15nukLWJ26K3egF9K0Q0yKT5T6wq30Z79eatv1lM0q39k=  
x-amz-request-id: FHB28KTTT6HPDYC  
Date: Thu, 14 Nov 2024 21:38:30 GMT  
Location: https://aws.amazon.com/s3/

En el caso de "301 Moved Permanently"

**SHODAN** Explore Downloads Pricing **Search** Account

**52.219.140.164** Regular View Raw Data

**General Information**

Field	Value
Hostnames	s3-website-eu-central-1.amazonaws.com
Domains	AMAZONAWS.COM
Cloud Provider	Amazon
Cloud Region	eu-central-1
Cloud Service	S3
Country	Germany
City	Frankfurt am Main
Organization	Amazon Technologies Inc.
ISP	Amazon.com, Inc.
ASN	AS16509

**Open Ports**  
80

**Amazon S3 httpd**  
301 Moved Permanently

HTTP/1.1 301 Moved Permanently  
x-amz-error-code: websiteRedirect  
x-amz-error-message: Request does not contain a bucket name.  
x-amz-request-id: ZCWE19MHZ0Q09  
x-amz-id-2: m4nh-a1b5uhtaw0c1C0qj3F0V13JC2n7b1mW7g1f1YVpMR6/GyCpKcXpG093TC00FETH4=  
Location: https://aws.amazon.com/s3/  
Content-Type: text/html; charset=utf-8  
Content-Length: 348  
Date: Tue, 26 Nov 2024 18:22:37 GMT  
Server: AmazonS3

### Información relevante:

- Proveedor de nube: Amazon Web Services (AWS). Esto significa que el servidor está alojado en la infraestructura de Amazon.
- Servicio: Amazon S3. S3 es un servicio de almacenamiento en la nube de objetos.
- Puerto abierto: El puerto 80 está abierto, lo que indica que el servidor está escuchando solicitudes HTTP. Cuando se realiza una solicitud a este puerto se recibe una respuesta de redirección (301 Moved Permanently), lo que significa que el contenido ha sido movido a otra ubicación.

### ¿Qué significa esto?

Imagina que esta dirección IP es la dirección de una casa. En el pasado, en esa casa había una tienda, pero la tienda se mudó a otro lugar. Ahora, si vas a la dirección original, te van a indicar que la tienda se ha trasladado a una nueva dirección.

## Parte 3: Reflexión ética

Google Hacking es una técnica que usa comandos avanzados en Google para encontrar información sensible en sitios web como contraseñas expuestas o bases de datos mal configuradas. Si se usan estas herramientas de manera irresponsable pueden surgir muchos riesgos. Técnicamente, alguien podría descubrir fallos en la seguridad de un sistema y aprovecharlos para robar datos, interrumpir servicios o poner en peligro la privacidad de los usuarios. Por eso herramientas como Google Hacking y Shodan solo deben usarse con el permiso de los propietarios de los sistemas y siempre en un contexto de pruebas de seguridad o auditorías donde se tiene autorización para hacerlo.

### ¿Cuáles son las responsabilidades éticas y legales de un hacker ético en este contexto?

Un hacker ético debe obtener permiso antes de realizar pruebas de seguridad, proteger la privacidad de los datos, actuar con transparencia y evitar causar daños.

Debe cumplir con las leyes, respetar normativas locales e internacionales y no explotar vulnerabilidades para fines maliciosos, sino para ayudar a mejorar la seguridad.