Recopilación Pasiva de Información utilizando Google Hacking y Shodan

Contenido

Parte 1: Google Hacking 3

Búsqueda de Google: 3

Consulta con Google Dorks 5

Parte 2: Shodan 7

Exploración de Shodan 7

Parte 3: Reflexión ética 8

¿Cuáles son las responsabilidades éticas y legales de un hacker ético en este contexto? 8

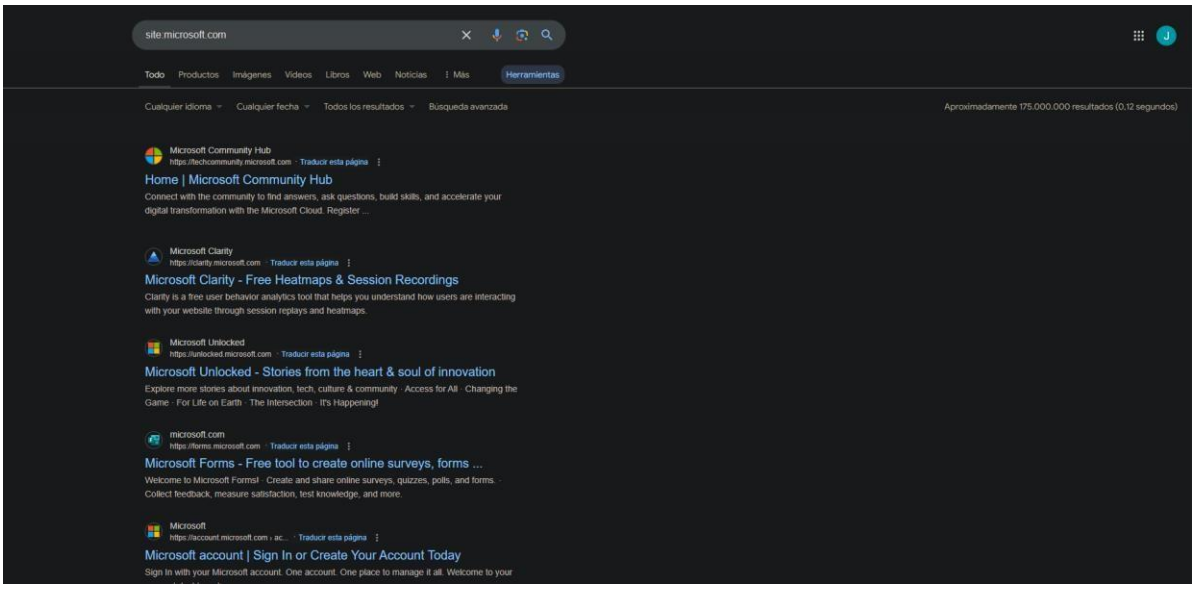
Parte 1: Google Hacking

Búsqueda de Google:

Buscar todas las URL indexadas de Microsoft (175.000.000 resultados)

“site:microsoft.com”

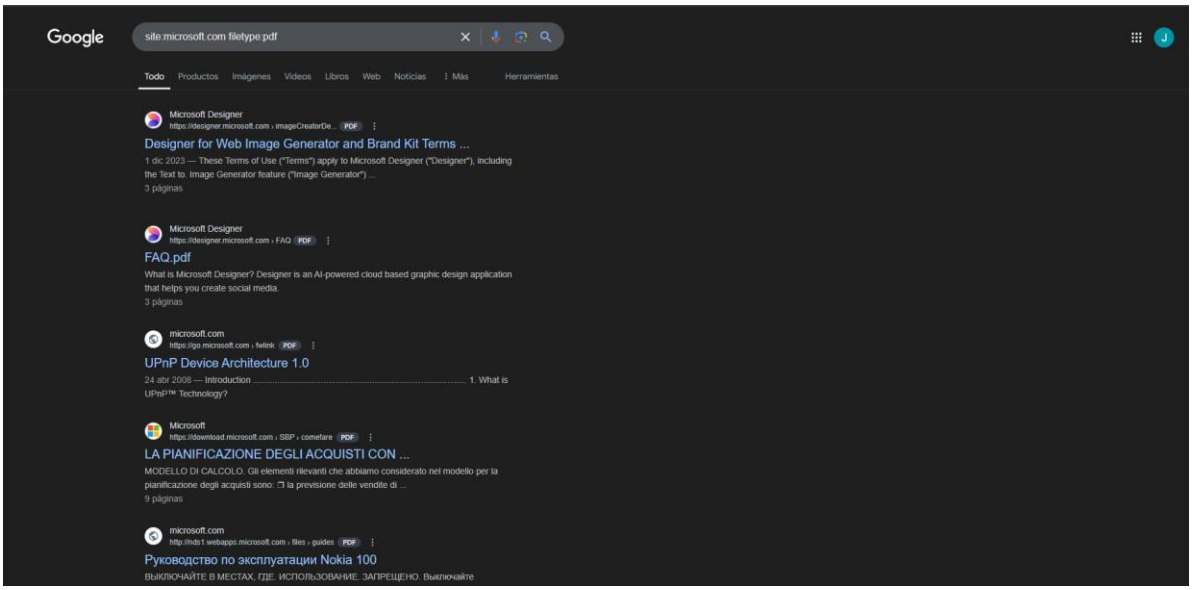
Esto muestra todas las páginas indexadas en el dominio de Microsoft.



Buscar archivos PDF en el dominio de Microsoft:

“site:microsoft.com filetype:pdf”

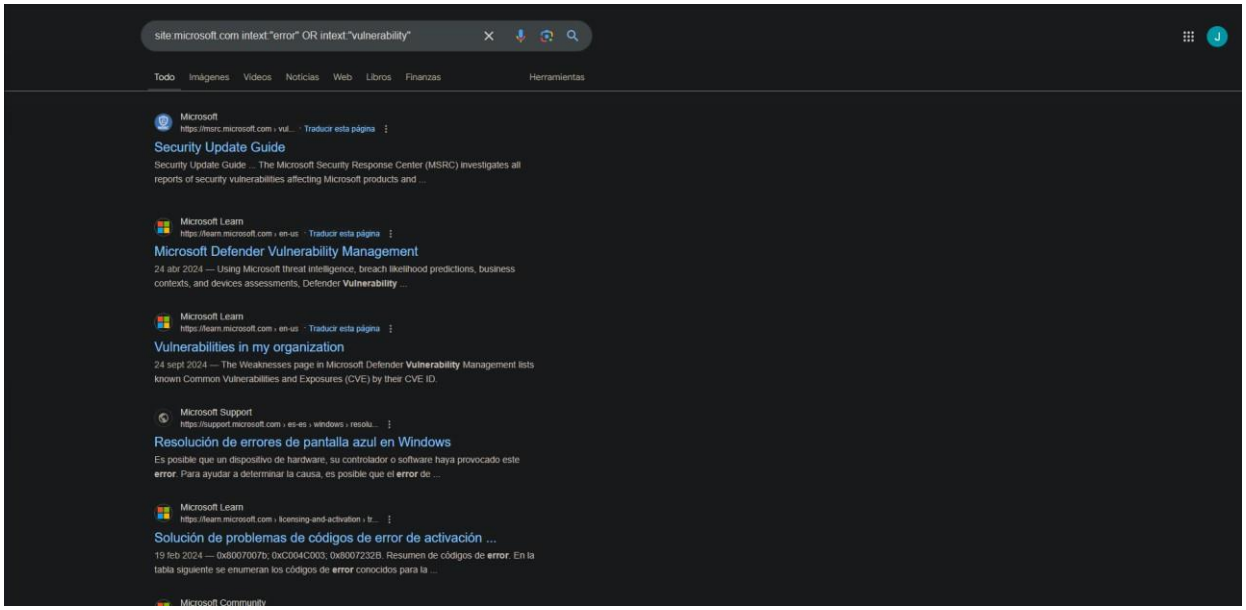
Muestra archivos en formato PDF que están en el dominio microsoft.com.



Buscar información sobre errores o vulnerabilidades:

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

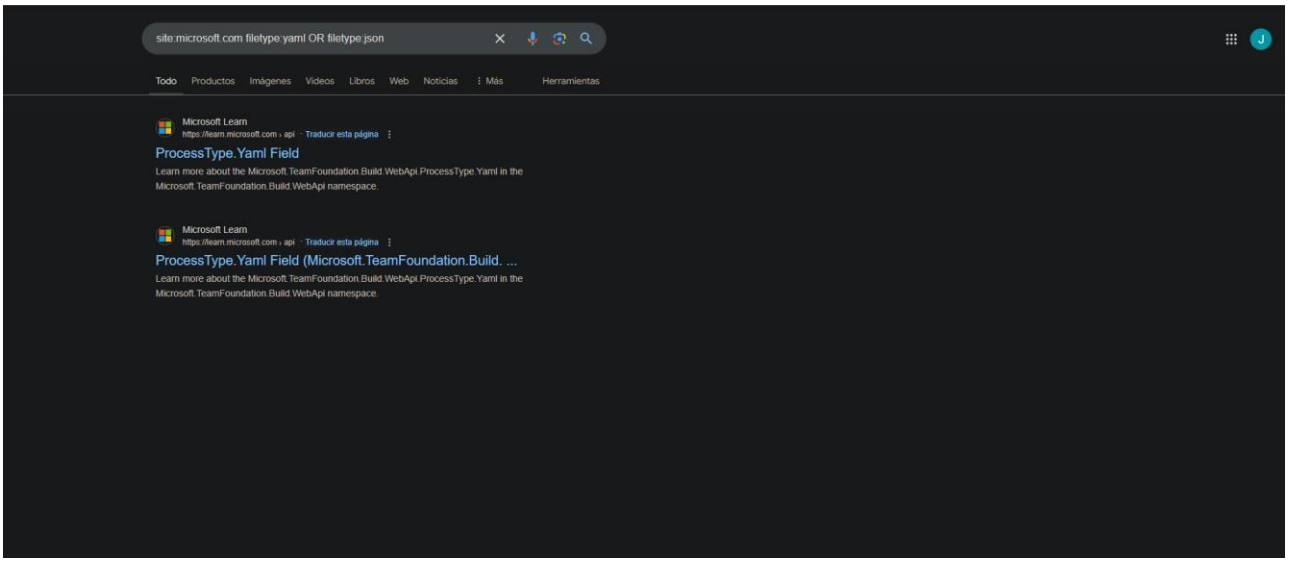
Busca páginas dentro de Microsoft que muestren"error" o "vulnerability", lo que puede ser útil para encontrar errores conocidos o información sobre vulnerabilidades.



Buscar archivos de configuración YAML o JSON:

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

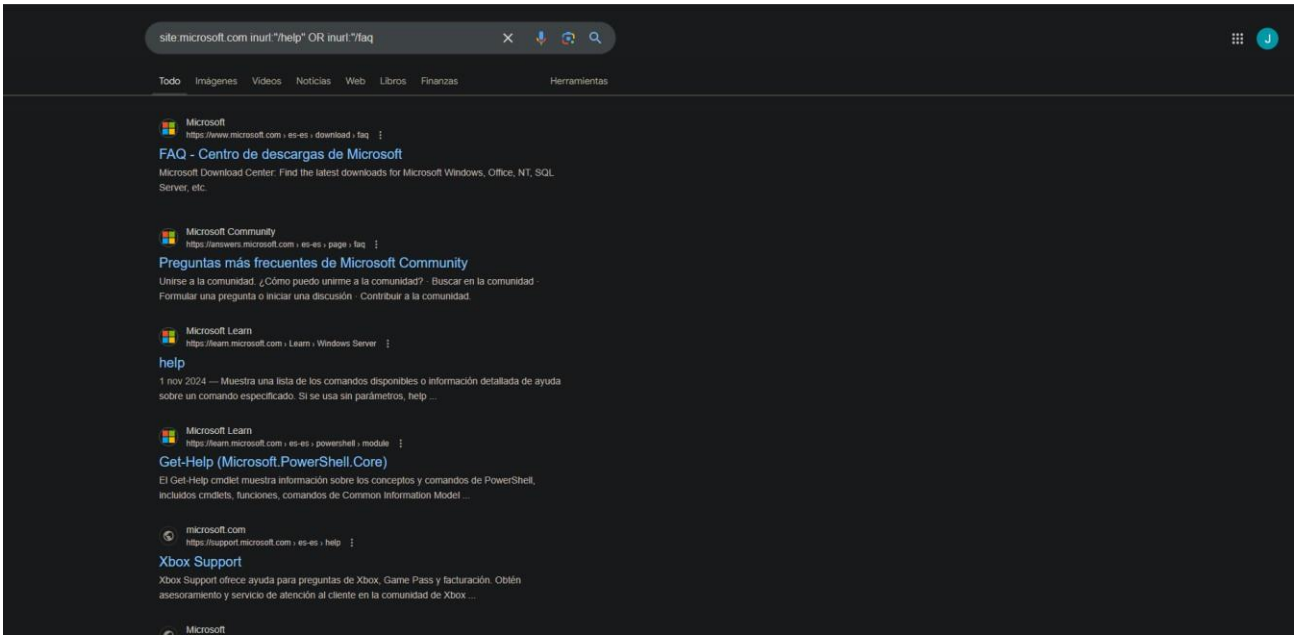
Esto identifica archivos YAML o JSON, que pueden incluir configuraciones o parámetros públicos.



Buscar recursos de ayuda o preguntas frecuentes:

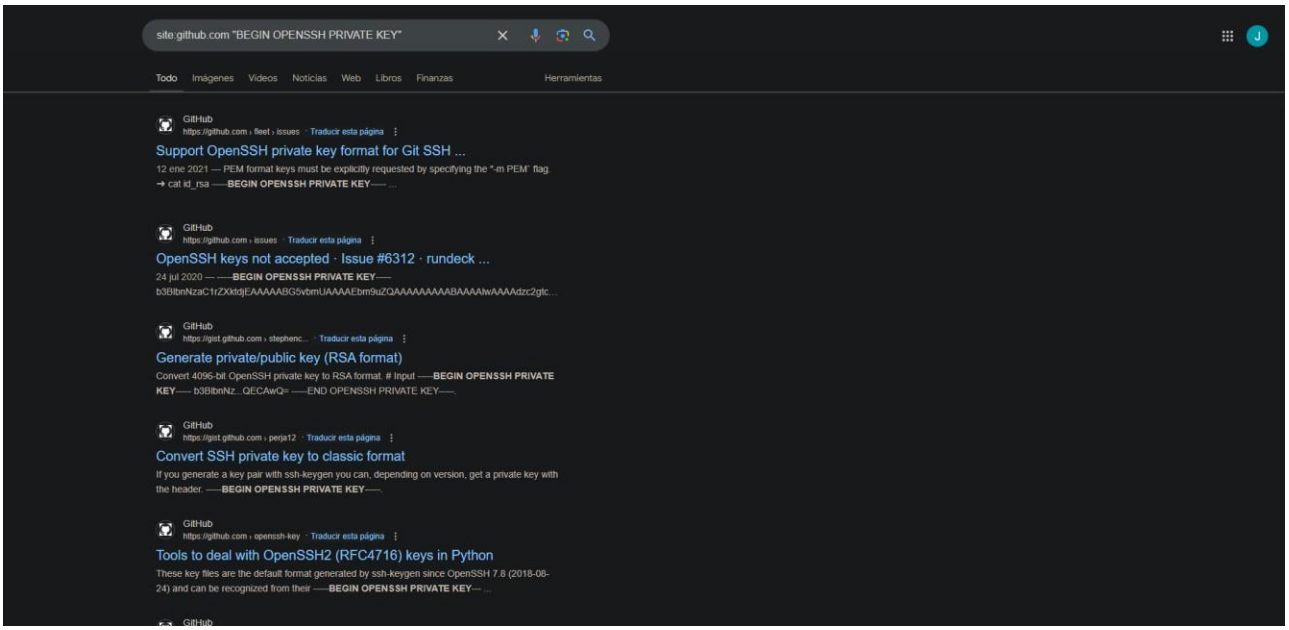
“site:microsoft.com inurl:"/help" OR inurl:"/faq"”

Encuentra páginas de ayuda y preguntas frecuentes.



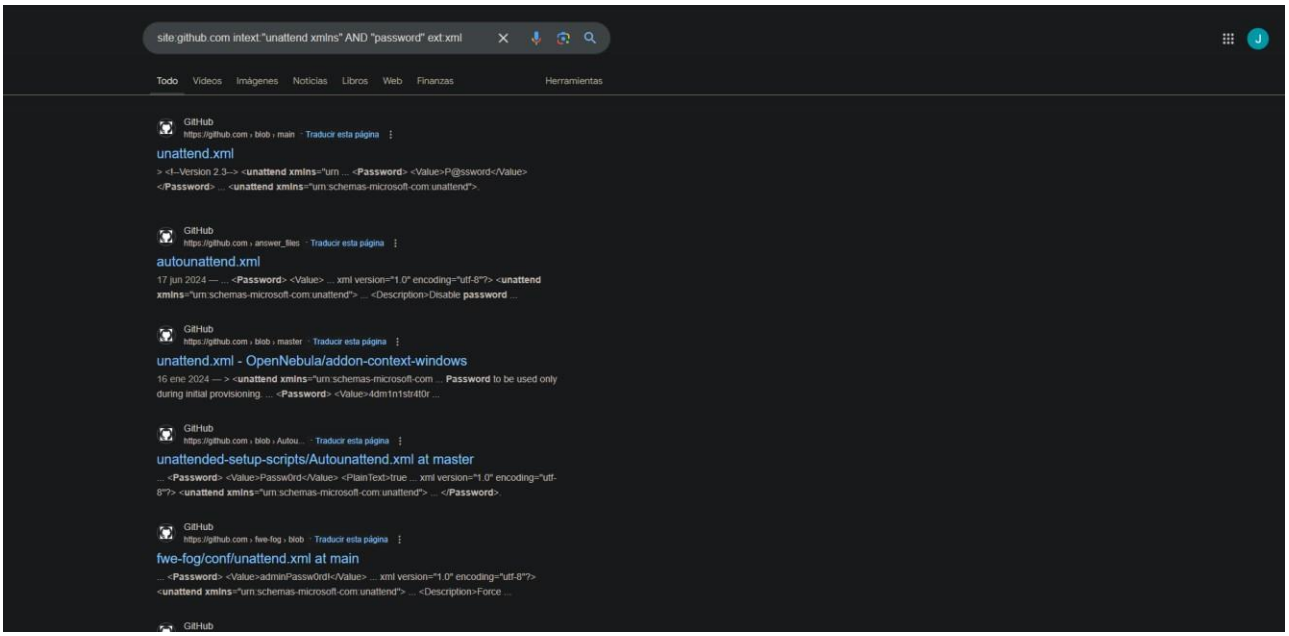
Consulta con Google Dorks:
“site:github.com "BEGIN OPENSSH PRIVATE KEY"”

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.



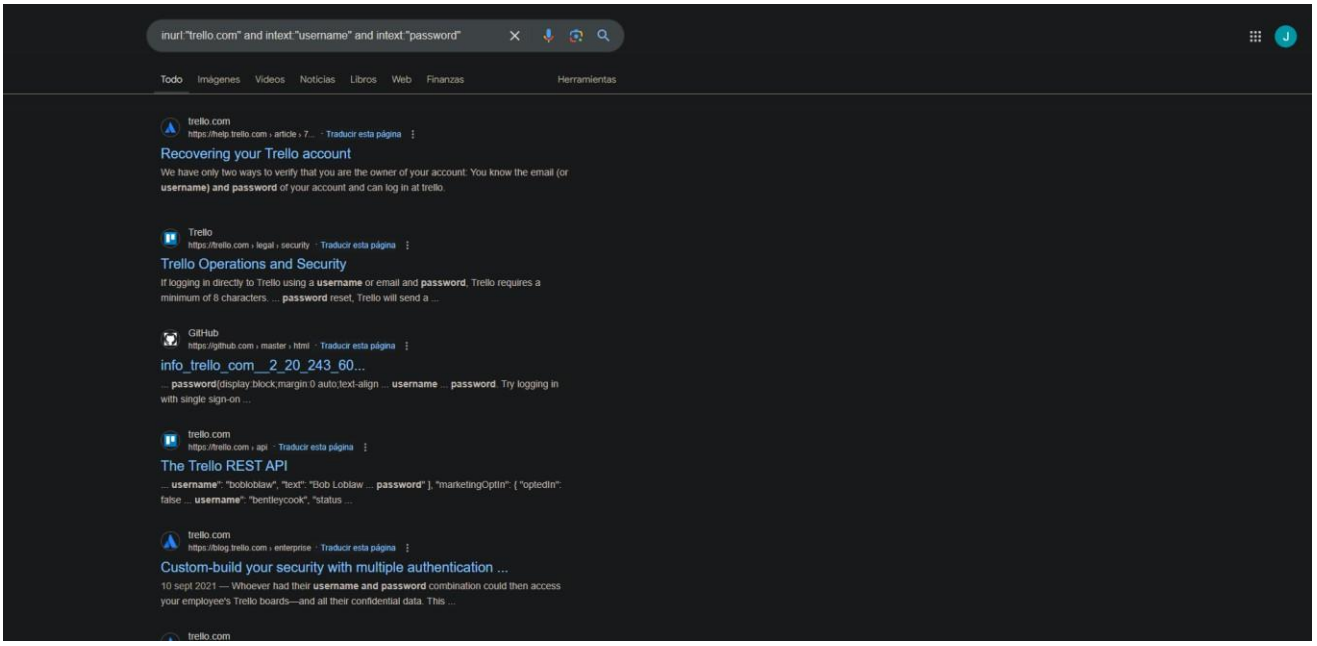
“site:github.com intext:"unattend xmlns" AND "password" ext:xml”

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.



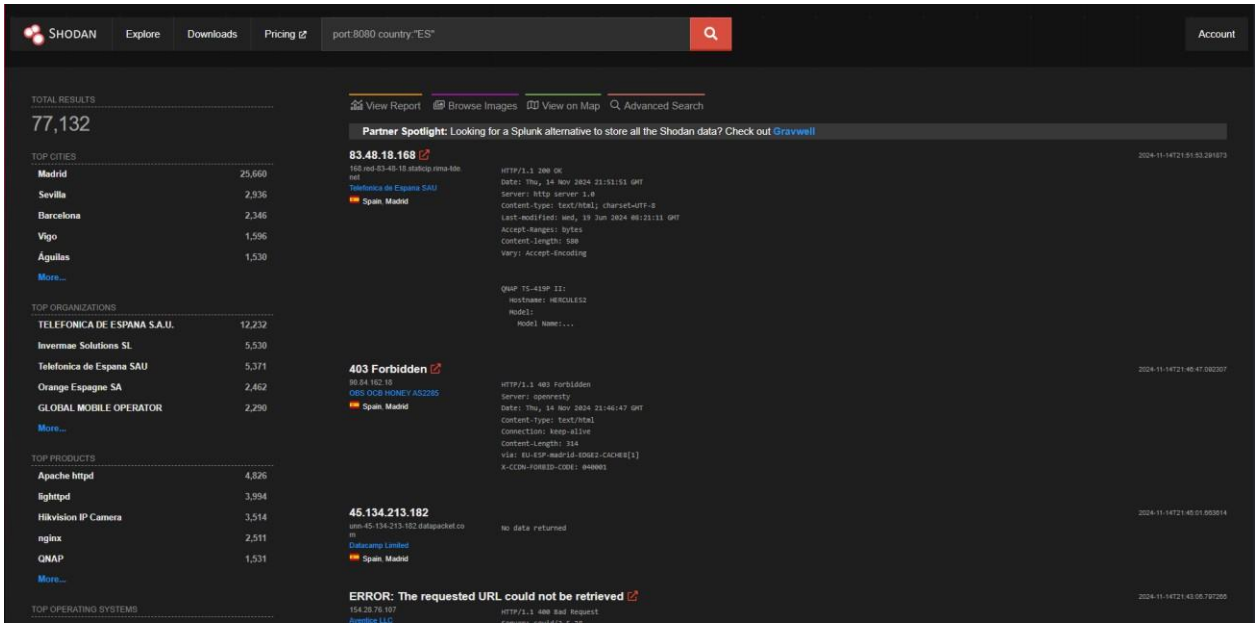
Parte 2: Shodan

Exploración de Shodan:

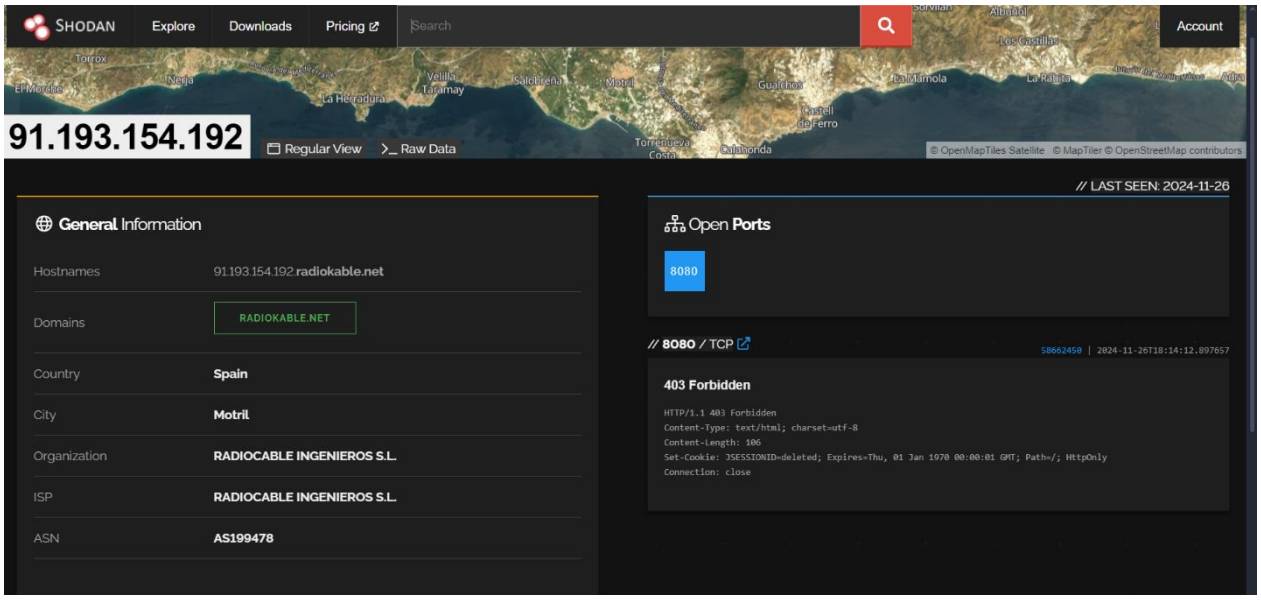
“port:8080 country:"ES"”

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

Hay 77,132 resultados, las ciudades donde mas resultados hay, las organizaciones con mas resultados y los productos top.



En este caso he entrado en 402 Forbidden.



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?

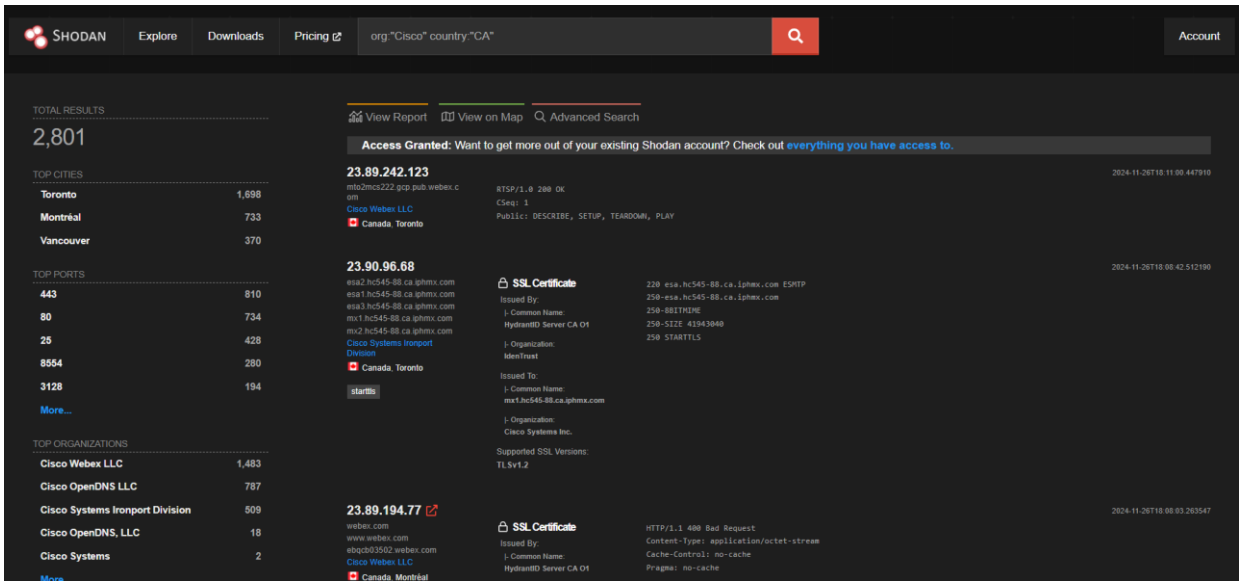
La información proporcionada por Shodan es un servidor web propiedad de RADIOCABLE INGENIEROS S.L. y ubicado en España.

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.

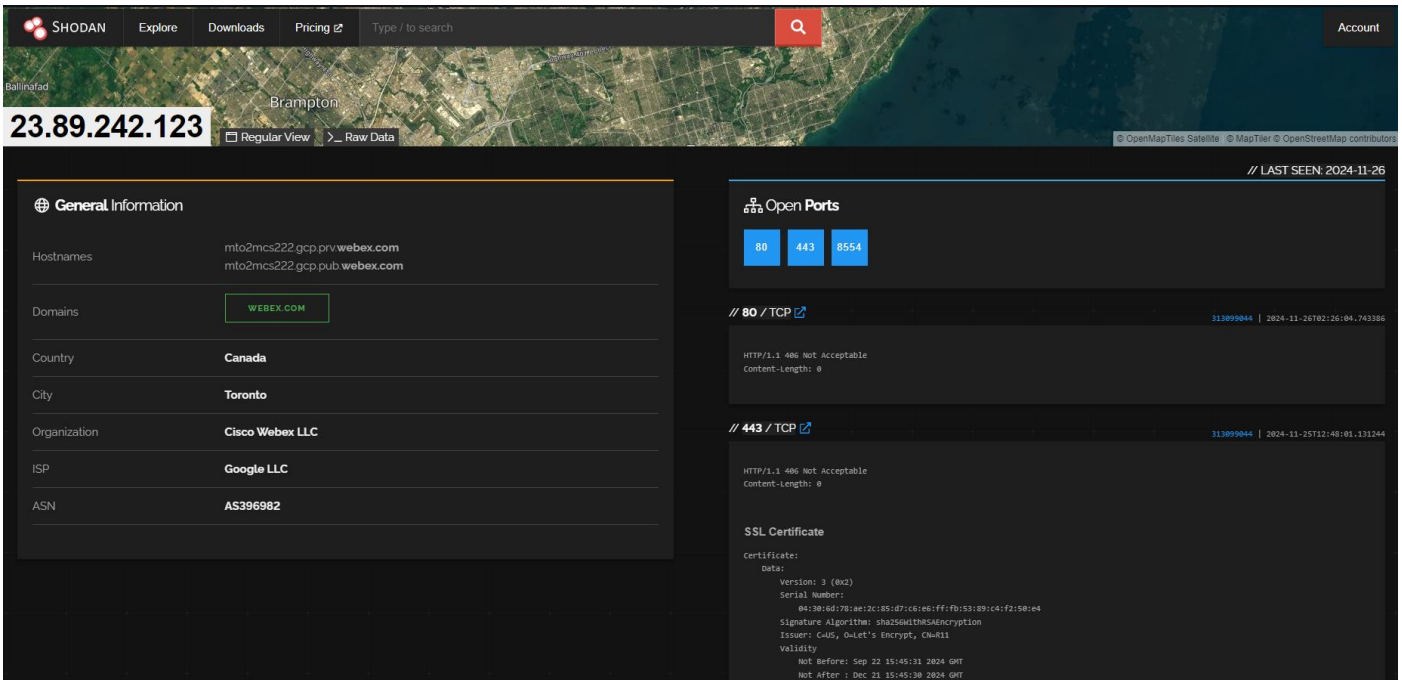
“"Cisco" country:"CA"”

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



En el caso de “23.89.242.124”



Información relevante:

- Dirección IP: 23.89.242.123
- Hostnames: [se quitó una URL no válida], mlo2mcs222.gop.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.

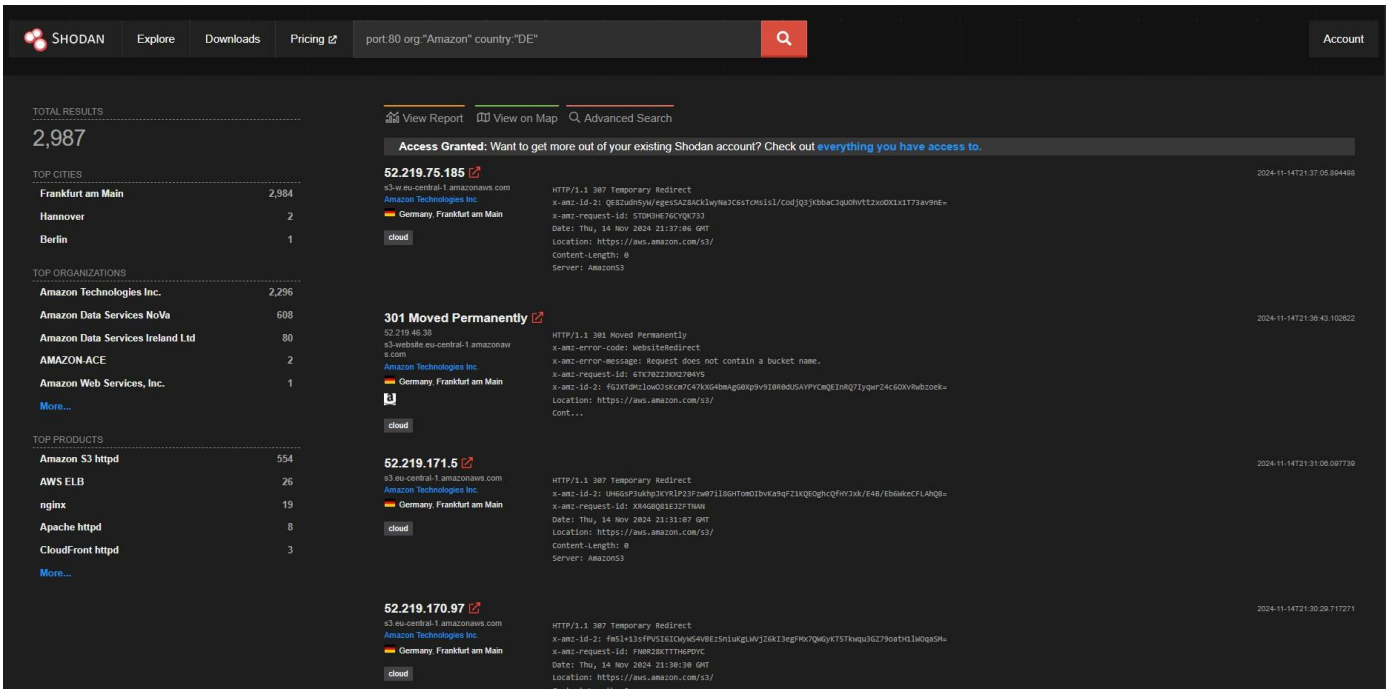
Los servicios web ofrecidos en este servidor están protegidos con HTTPS, lo que garantiza la seguridad de la comunicación.

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

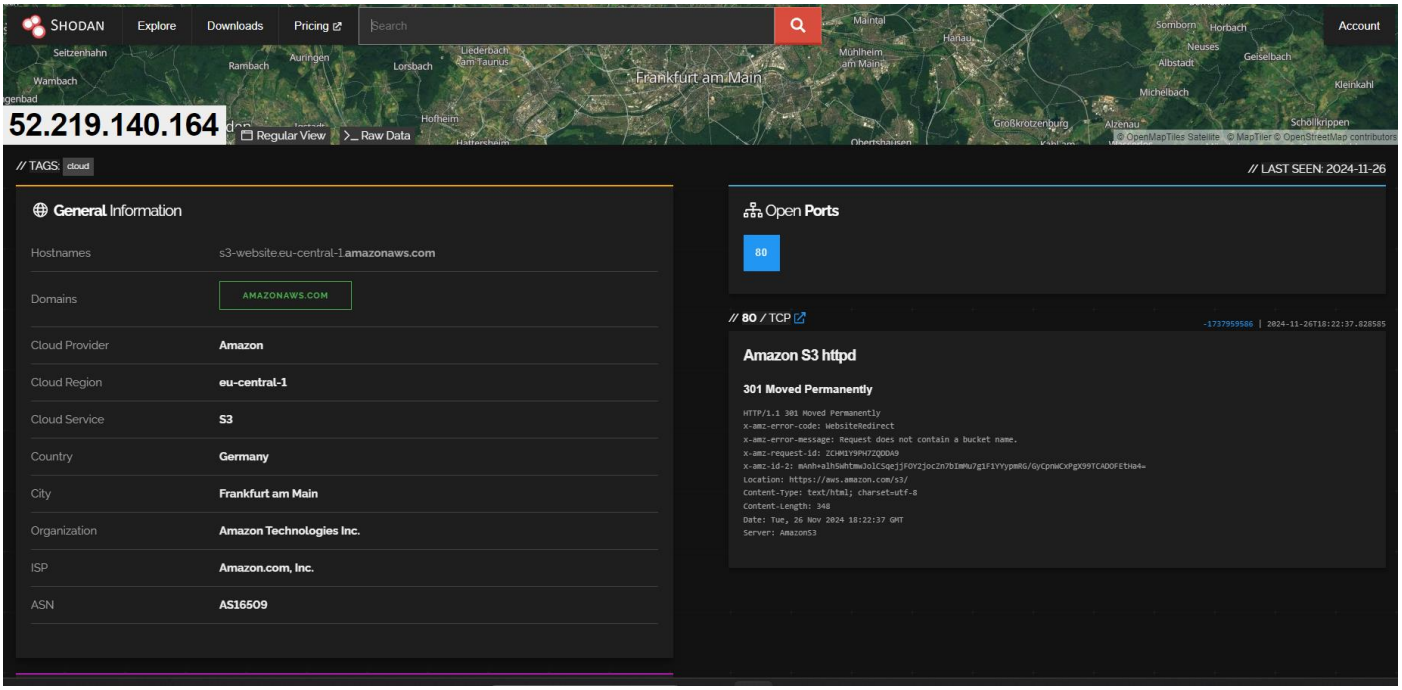
“port:80 org:"Amazon" country:"DE""”

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.



En el caso de “301 Moved Permanently”



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.