



TAREA 1 – RECONOCIMIENTO PASIVO - RETO 0

PENTESTER HACKER MENTOR

JUC4ZU
PMJ
CERTIFICACION HACKER MENTOR

Contenido

1 – Ejercicio:2

Paso 1:.....2

Paso 2:.....3

Paso 3:.....4

Bandera 1:.....4

2 – Ejercicio:5

Paso 1:.....5

Paso 2:5

Paso 3:.....8

Bandera 2:.....8

3 – Ejercicio:9

Paso 1:.....9

Paso 2:.....10

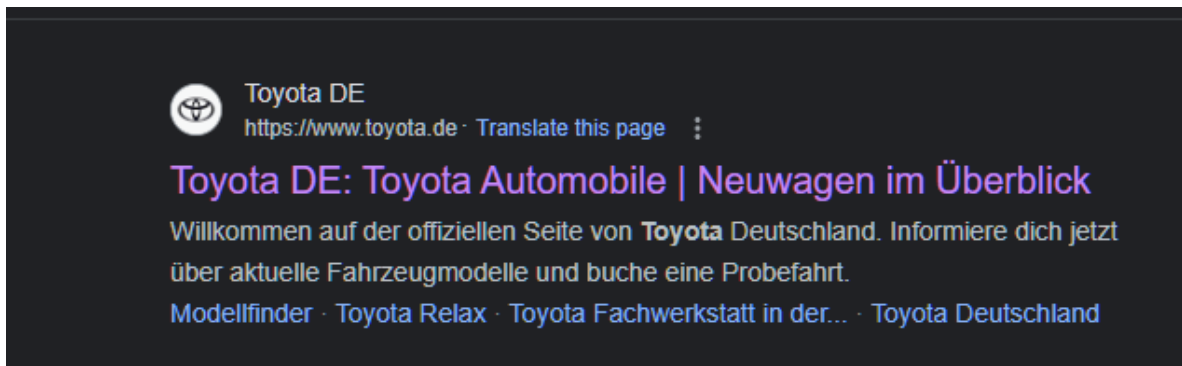
Bandera 3:.....11

1 – Ejercicio:

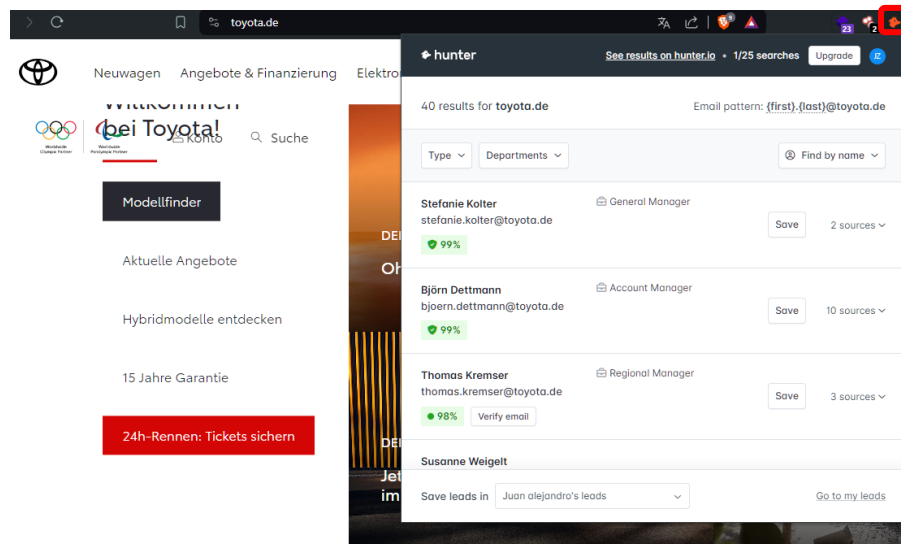
Solicitud: ¿Estás realizando un Ethical Hacking a la empresa Toyota sucursal Alemania, se presume que hubo una filtración de datos indexada en BreachParse, serás capaz de encontrar la contraseña de correo del usuario administrador Rainer Luecke? El dominio es "toyota.de"

Paso 1:

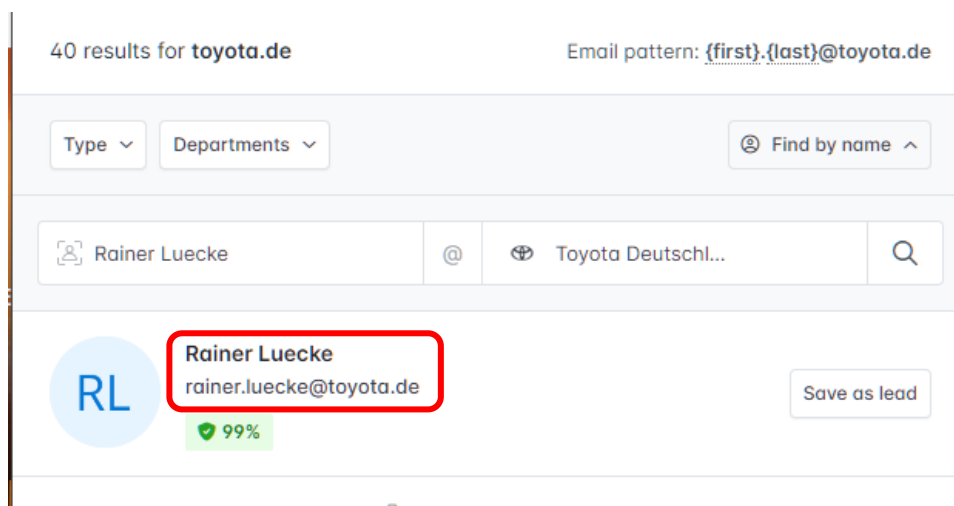
Como paso preliminar podemos ir a investigar con la extensión de "Hunter.io", si existe algún correo relacionado a Rainer Luecke filtrado por la página de Toyota Alemania, así que nos dirigimos a su página principal, en <https://www.toyota.de>



Ya dentro de la página podemos usar la extensión para verificar algunos correos:



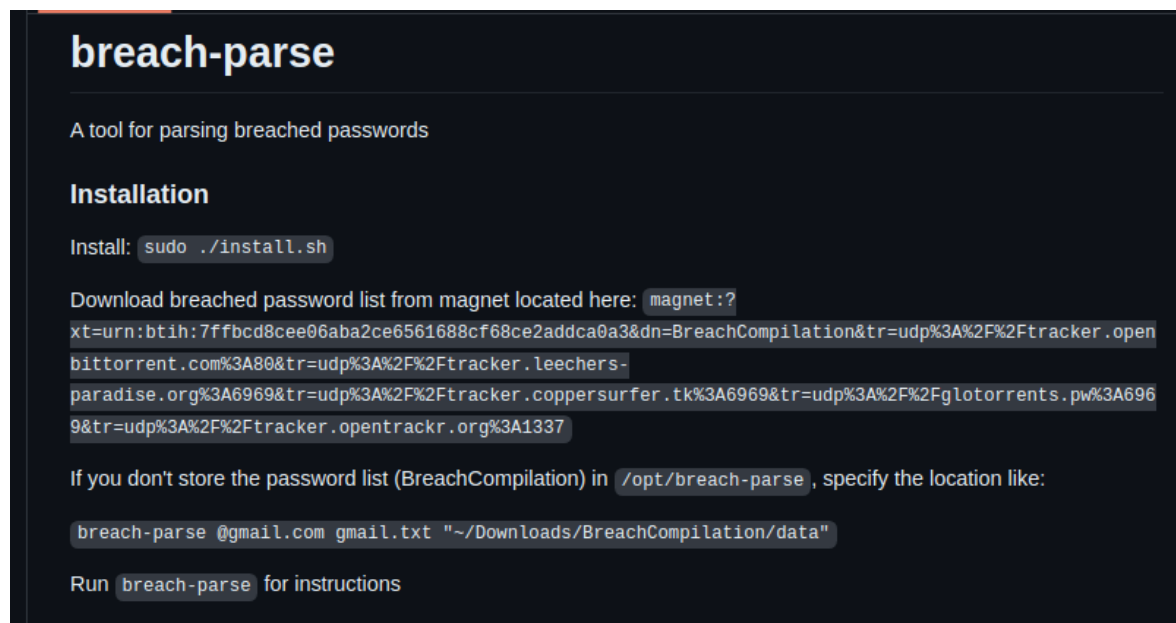
Si escribimos y filtramos el nombre completo de Rainer, esta extensión nos permite ubicar el correo de nuestro objetivo que en este caso es **rainer.luecke@toyota.de**



Paso 2:

Iremos a la siguiente dirección: <https://github.com/hmaverickadams/breach-parse>

Instalaremos el “**BreachParse**” en nuestro equipo (recomendable que sea en Kali), siguiendo los pasos explicados en la página:



Teniendo en cuenta del espacio en disco (son 40 gigas de descarga aproximadamente), además de considerar como se instala en nuestro sistema, y el comando para realizar las búsquedas mediante la terminal

Ya que tenemos el correo oficial de Rainer, podemos utilizar el “BreachParse” para realizar la búsqueda de brechas en Toyota.

```
File Actions Edit View Help
(hmstudent@kali)-[~/Desktop/arsenal/breach-parse]
$ sudo ./breach-parse.sh rainer.luecke@toyota.de toyota.txt "/home/hmstudent/Desktop/arsenal/"
[sudo] password for hmstudent:
Progress : [-----] 1%
```

Haremos uso del comando `sudo ./breach-parse.sh` “correo objetivo” “archivo en el equipo” “ubicación de nuestra carpeta de BreachParse” – Confirmaremos con la contraseña para ejecutar como administrador.

Cuando el proceso de búsquedas termine, se nos va a mostrar un mensaje similar al siguiente:

```
[sudo] password for hmstudent:
Progress : [#####] 99%grep: /home/hmstudent/Desktop/arsenal/breach-parse/toy
ota-master.txt: input file is also the output
Progress : [#####] 100%
Extracting usernames...
Extracting passwords...
```

Paso 3:

El proceso nos genera 3 archivos con información, uno de ellos cuenta con el usuario y contraseña (-master.txt), el otro solo con usuario (-users.txt), y el otro solo con contraseña (-passwords.txt), abriremos el archivo de texto deseado que se creó en nuestra carpeta mediante el comando del paso anterior, a través de la terminal usando “`cat toyota-master.txt`”

```
(hmstudent@kali)-[~/Desktop/arsenal/breach-parse]
$ cat toyota-master.txt
rainer.luecke@toyota.de:Luecke99
```

Con el documento ya abierto en la consola, se nos muestra el usuario y contraseña correspondiente a Rainer Luecke

Bandera 1:

rainer.luecke@toyota.de – Contraseña: Luecke99

2 – Ejercicio:

Solicitud: Analizando los logs del sistema se ha detectado una intrusión, pero están incompletos conocemos parte de su email hacker-root_@live.cn, ¿podrías encontrar la contraseña del hacker?

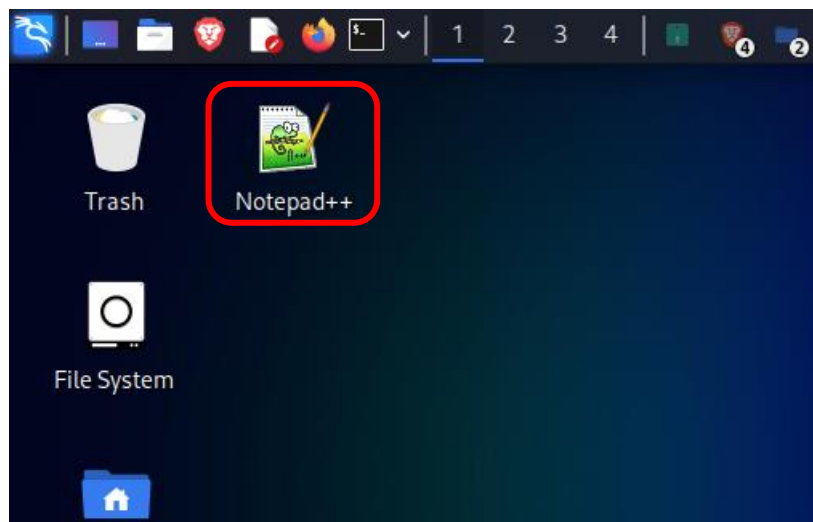
Paso 1:

Para este ejercicio se hace suposición que los datos de la intrusión fueron encontrados en algún log de una página web o talvez algún rastro dejado en un servidor, así que podemos utilizar el dominio de la dirección para intentar recabar la contraseña y el usuario sospechoso.

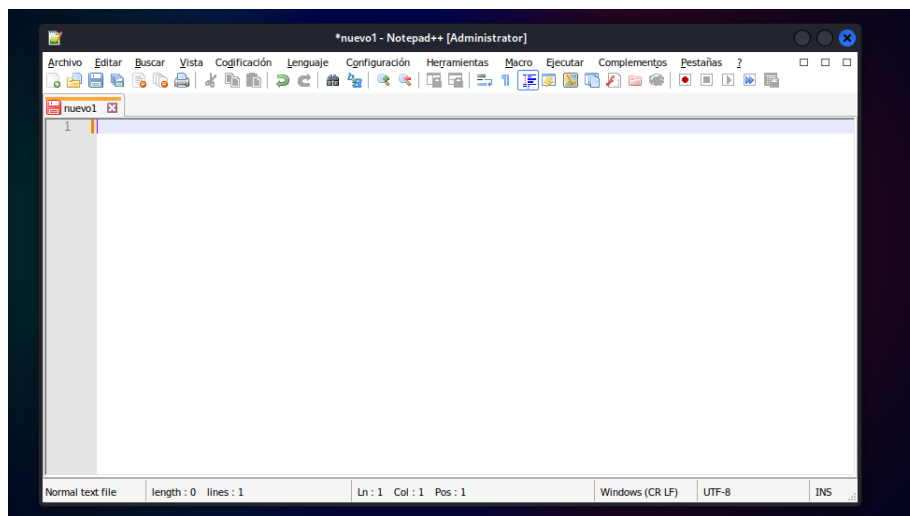
hacker-root_@live.cn – El “**BreachParse**”, nos permite utilizar solamente el dominio del correo “@live.cn” como parámetro, mediante los comandos que provee para hallar correos filtrados, nos puede llevar mucho tiempo, así que como ya sabemos parte del correo, aplicaremos la búsqueda mediante un gestor de texto.

Paso 2:

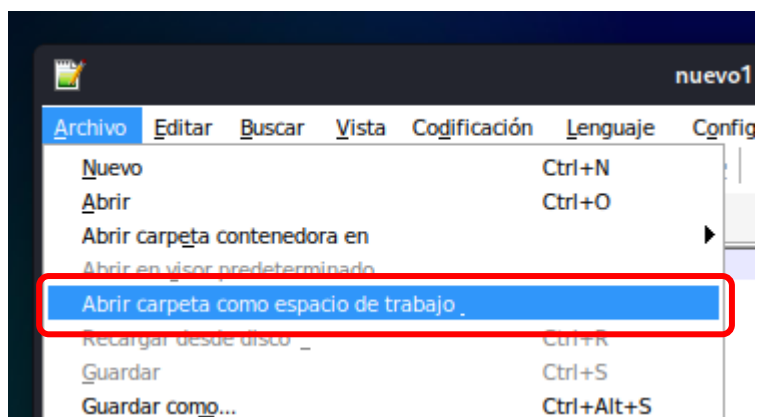
Utilizaremos Notepad ++ en Kali Linux (Se instala con **WineHQ** – permite el uso de programas nativos de Windows, su instalación es un poco prolongada, así que por ahora estará fuera de este paso a paso)



Al Abrir el Notepad ++, se nos mostrara un espacio como el siguiente



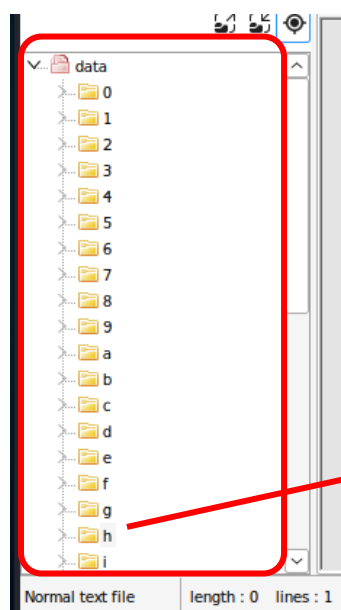
Iremos al botón “archivo>abrir carpeta como espacio de trabajo”



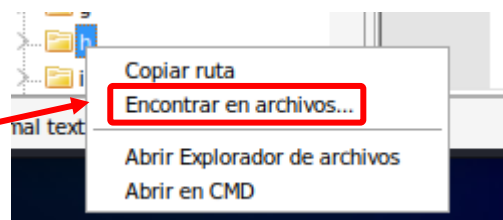
Nos aparecerá una ventana emergente desde la cual podemos elegir la carpeta “data” dentro de la carpeta raíz donde esta nuestro “BreachCompilation” (los datos filtrados)



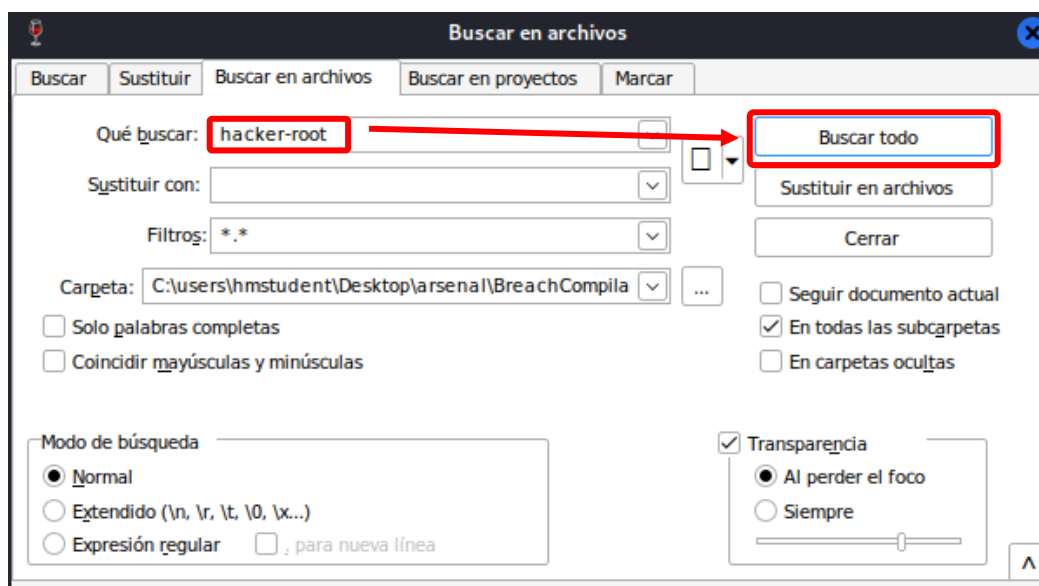
Al lado izquierdo del programa de texto se nos abrirán las carpetas contenidas en “data”



Como ya sabemos que la dirección objetivo comienza con “H” daremos clic derecho en la letra del lado izquierdo y a continuación en “Encontrar en archivos...”

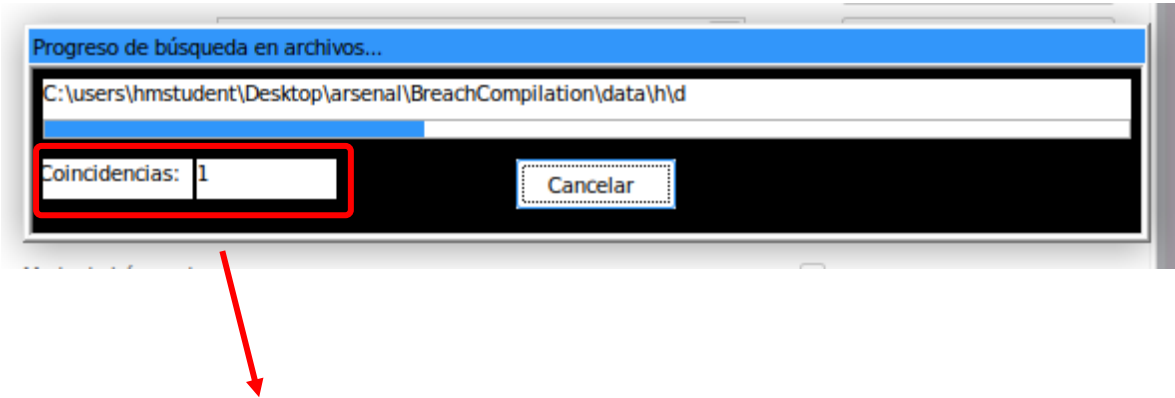


Nuevamente se nos mostrará una ventana emergente, desde la cual podemos poner nuestros términos de búsqueda, que para este proceso en particular serán el prefijo del correo “**hacker-root**”, con esto podremos buscar en todos los registros que empiecen por “h”, modificándolo a nuestro gusto según la búsqueda.



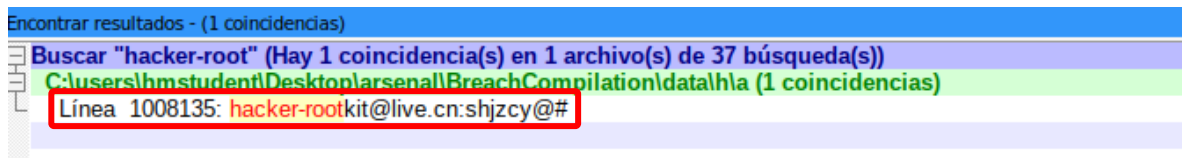
Paso 3:

Ahora nos queda esperar, hasta que el proceso termine, tener en cuenta que haciéndolo así nos ahorramos bastante tiempo, ya que de la manera vista en el ejercicio 1, podrá tardar alrededor de 10 minutos y nos mostrará muchos resultados que no requerimos, mismos que están presentes en la base de datos del “**BreachParse**”, esto más bien pueden entorpecer encontrar a nuestro objetivo.



Si alguno de los términos
corresponde a nuestra búsqueda se
nos mostrará mediante las
coincidencias.

Cuando el proceso llegue a su final, nos mostrará los resultados que encontró dentro de la carpeta “h”, y justo aquí la concordancia con el correo sospechoso que nos indicaron ubicar, claro, sin olvidar, su contraseña.



Bandera 2:

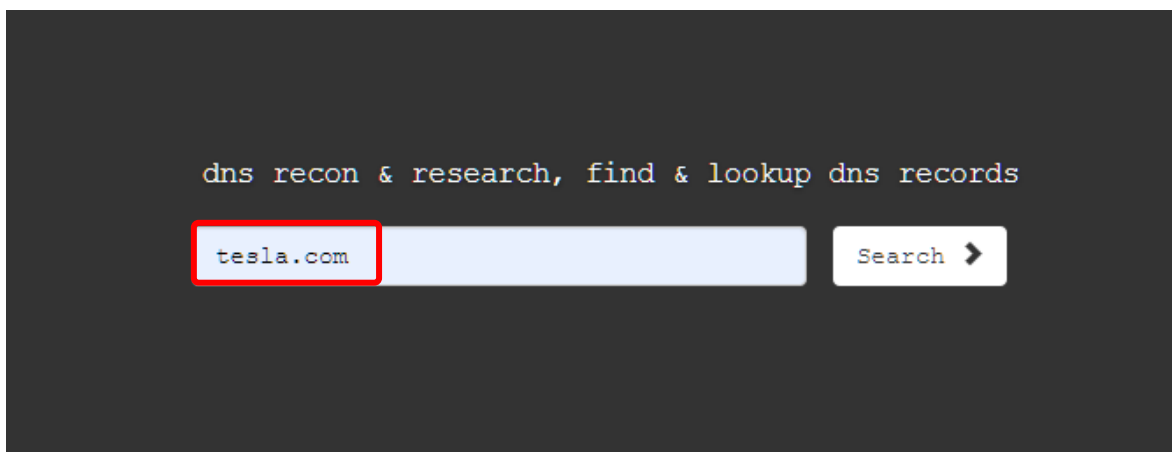
hacker-rootkit@live.cn – Contraseña: shjzcy@#

3 – Ejercicio:

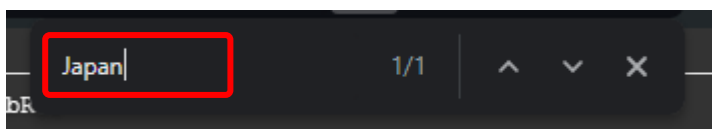
Solicitud: Elon Musk debido los cambios en las políticas de EEUU ha decidido instalar un servicio VPN para su empresa TESLA (**tesla.com**), en Japón, ¿serás capaz de encontrar el nombre y dirección IP del servidor?

Paso 1:

Ya que la información preliminar que tenemos es “**tesla.com**” podemos dirigirnos a “**dnsdumpster**” (<https://dnsdumpster.com/>) ya que desde esta página es más sencillo ubicar algunos servidores o páginas web enlazadas a servicios relacionados a dominios de empresas que están en la web.

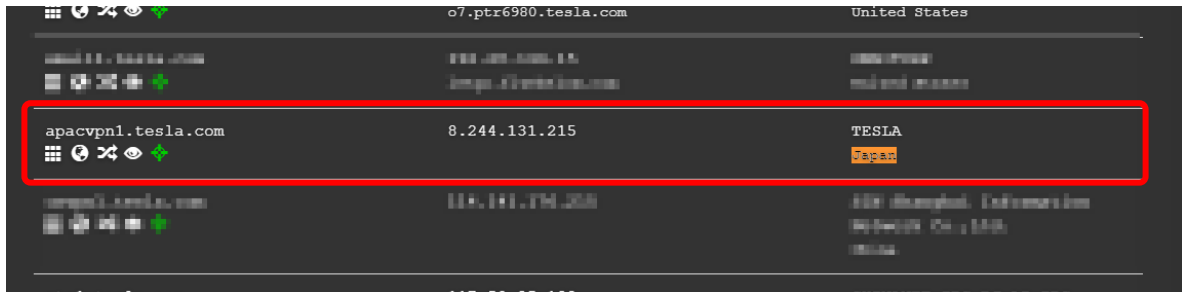


Realizaremos la búsqueda con este término (**tesla.com**) para ubicar todos los datos relacionados. Podemos filtrar estos datos en la página con la tecla “**F3**” (varía según el navegador)



Como esta web está en inglés, el filtro de país lo canalizaremos por medio de ese idioma con la palabra “**Japan**”

Entre los términos de búsqueda, se nos van a mostrar los datos que podremos estar necesitando:

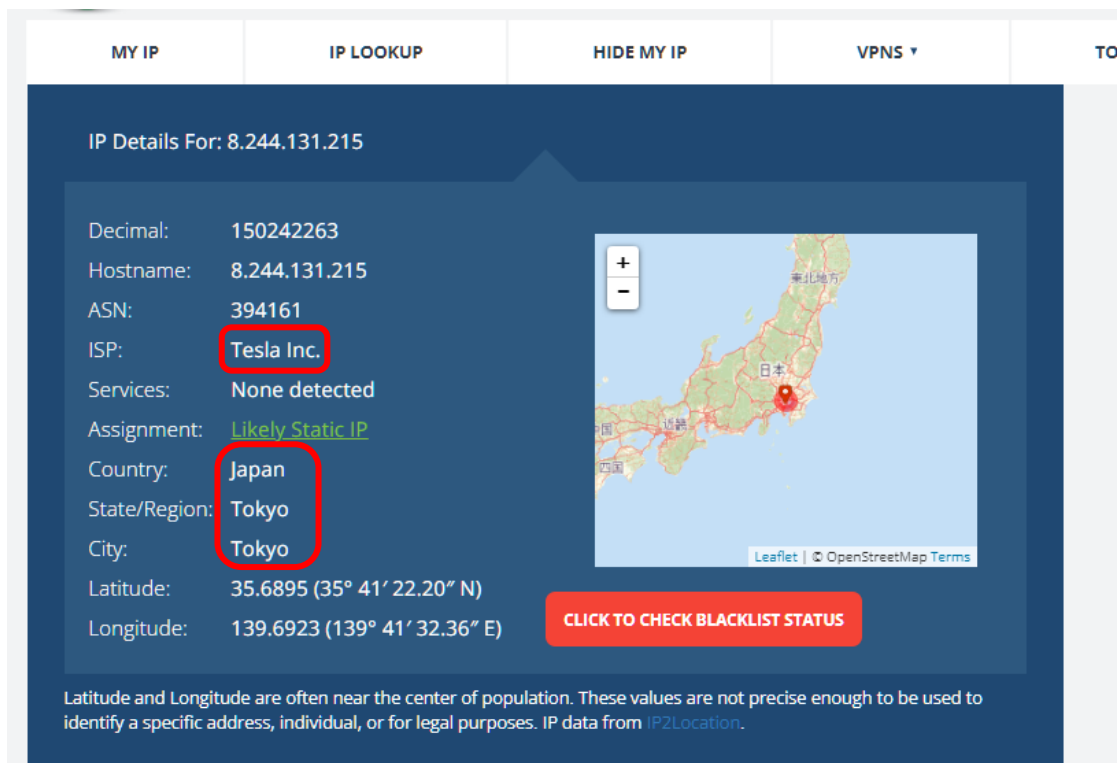


o7.ptr6980.tesla.com		United States
apacvpn1.tesla.com	8.244.131.215	TESLA Japan
114.111.111.111		
112.58.25.100		

Ubicamos los siguientes datos “**apacvpn1.tesla.com**” y su ip: “**8.244.131.215**”, puede que estos sean los necesarios, pero podemos asegurarnos que sea el objetivo de esta manera.

Paso 2:

Nos dirigimos a servicios como (<https://whatismyipaddress.com/ip/>) o (<https://www.cual-es-mi-ip.net/geolocalizar-ip-mapa>) desde los cuales podemos asegurarnos que el servicio de VPN se encuentra físicamente en Japón, y además que pertenece a Tesla.



MY IP IP LOOKUP HIDE MY IP VPNS ▼ TO

IP Details For: 8.244.131.215

Decimal:	150242263
Hostname:	8.244.131.215
ASN:	394161
ISP:	Tesla Inc.
Services:	None detected
Assignment:	Likely Static IP
Country:	Japan
State/Region:	Tokyo
City:	Tokyo
Latitude:	35.6895 (35° 41' 22.20" N)
Longitude:	139.6923 (139° 41' 32.36" E)

CLICK TO CHECK BLACKLIST STATUS

Latitude and Longitude are often near the center of population. These values are not precise enough to be used to identify a specific address, individual, or for legal purposes. IP data from IP2Location.

O también podemos hacer una búsqueda en la web de <https://talosintelligence.com/> y ubicar la ip o nombre del servidor para obtener algunos datos más exactos.

This screenshot shows a Talos Intelligence report for the domain **teslamotors.com**. The report is divided into several sections: **OWNER DETAILS** (Domain: teslamotors.com, Hostname: apacvpn1.tesla.com, Network Owner: level 3 parent llc), **CONTENT DETAILS** (Content Category: Transportation), **ADDITIONAL INFORMATION** (IP Addresses, Whois, Email Volume History, Top Network Owners), **REPUTATION DETAILS** (Web Reputation: Favorable), **EMAIL VOLUME DATA** (Email Volume: 0, Volume Change: 0%), and **BLOCK LISTS** (Talos Security Intelligence Block List: No). A note at the bottom states: "Top IP Addresses used to send emails in apacvpn1.tesla.com".

Nos puede mostrar a que dominio pertenece, su reputación y hasta a que otros sitios se encuentran indexados o son relativos a este.

This screenshot shows a Talos Intelligence report for the IP address **8.244.131.215**. The report is divided into several sections: **LOCATION DATA** (Koto, Japan), **OWNER DETAILS** (IP Address: 8.244.131.215, Fwd/Rev DNS Match: No data, Hostname: -, Domain: -, Network Owner: level 3 parent llc), **CONTENT DETAILS** (Content Category: No established content categories), **REPUTATION DETAILS** (Sender IP Reputation: Neutral, Web Reputation: Unknown), **EMAIL VOLUME DATA** (Email Volume: 0.0, Volume Change: 0%, Spam Level: Medium), and **BLOCK LISTS** (BL.SPAMCOP.NET, CBL.ABUSEAT.ORG, PBL.SPAMHAUS.ORG, SBL.SPAMHAUS.ORG: Not Listed). A red box highlights the location data "Koto, Japan".

Si volvemos a hacer la búsqueda, pero desde su IP, nos muestra la ubicación geográfica que en este caso es Koto, Japón. De esta manera ya nos podemos asegurar que esta es la bandera que estábamos investigando.

Bandera 3:

Servidor VPN: **apacvpn1.tesla.com** – IP: **8.244.131.215**