

Informe Tarea 1 PMJ

1.- 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"

Tenemos de información lo siguiente:

- Un dominio: toyota.de
- Nombre de la persona a analizar: Rainer Luecke

¿Qué se debe de encontrar?

Correo electrónico de Rainer Luecke

Saber si hubo una filtración

Contraseña del correo electrónico del administrador llamado Rainer Luecke

PASOS A SEGUIR

- a) Analizar a través del dominio para saber si podemos detectar el correo de Rainer Luecke

Entrar al dominio y usar la herramienta hunter.io

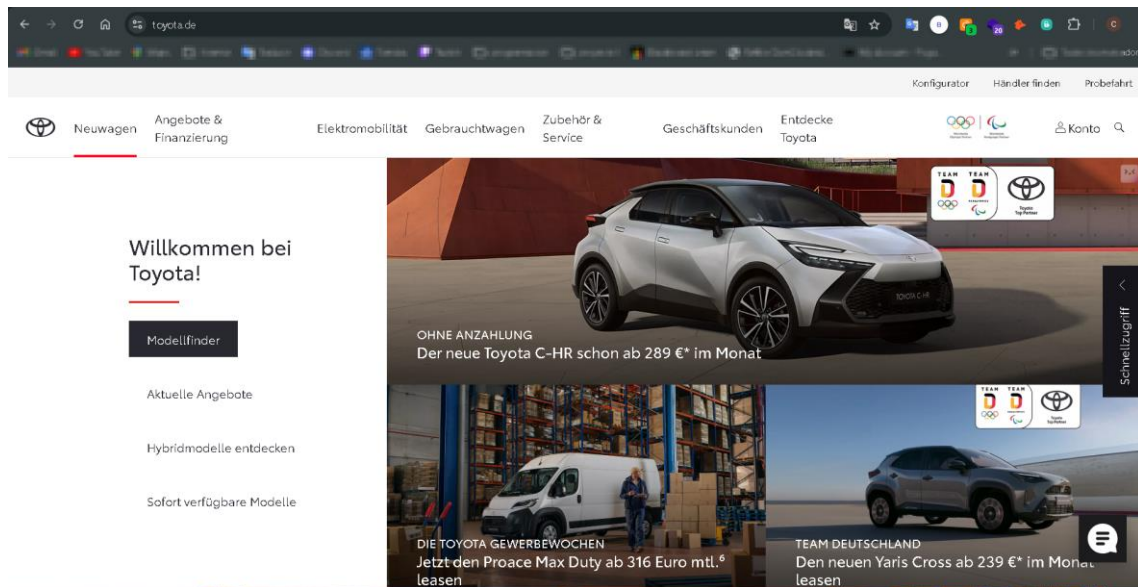






Ilustración 1. Imagen del dominio

 See results on hunter.io • 2/25 searches Upgrade 


34 results for **toyota.de** Email pattern: **{first}-{last}@toyota.de**


Type ▾ Departments ▾


 Find by name ▴


 Rainer Luecke


@

 Toyota Deutschl...








Rainer Luecke
rainer.luecke@toyota.de







Save as lead

Heiko Taubert
heiko-peter.taubert@toyota.de


 Regional Manager Business
Clients East


Save 4 sources ▾

Christian Selbach
christian.selbach@toyota.de


 International Key Account
Manager


Save 7 sources ▾

Save leads in Carlos' leads ▾

[Go to my leads](#)

Ilustración 2. Buscando a la persona en la herramienta hunter.io

Tenemos el correo de Rainer Luecke: **rainer.luecke@toyota.de**

- b) Una vez obtenido el correo podemos usar herramientas para saber si este correo esta filtrada

Probando con el dominio <https://haveibeenpwned.com/> para saber si ha sido filtrado

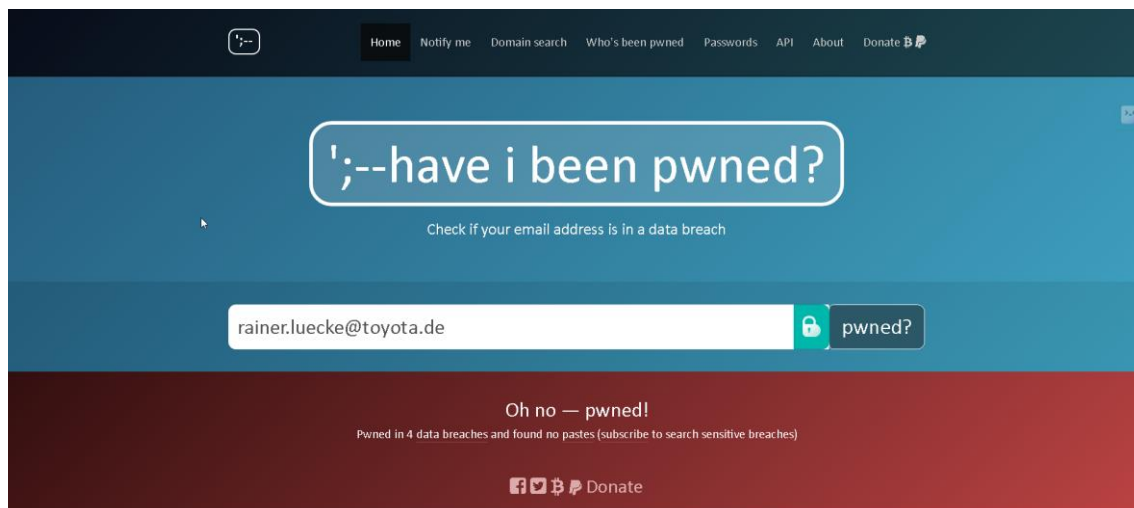


Ilustración 3. Probando el correo en la plataforma

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the [1Password password manager](#) helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.





- 
LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.
Compromised data: Email addresses, Passwords
- 
Nitro: In September 2020, the Nitro PDF service suffered a massive data breach which exposed over 70 million unique email addresses. The breach also exposed names, bcrypt password hashes and the titles of converted documents. The data was provided to HIBP by [dehashed.com](#).
Compromised data: Email addresses, Names, Passwords
- 
Operation Endgame: In May 2024, a coalition of international law enforcement agencies took down a series of botnets in a campaign they coined "Operation Endgame". Data seized in the operation included impacted email addresses and passwords which were provided to HIBP to help victims learn of their exposure.
Compromised data: Email addresses, Passwords
- 
Data Enrichment Exposure From PDL Customer: In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.
Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles

Ilustración 4. Donde se han filtrado y que datos fueron vulnerados

En la plataforma nos indica que el correo del usuario administrador ha sido vulnerado. **Esto quiere decir que si hubo una filtración**

c) Buscando la contraseña del correo usando breach parse.

Se tomo en cuenta la base de datos que nos da el repositorio de Github
Breach-parse (base de datos de 40GB)

Dentro de la base de datos iremos a la carpeta de data>r y buscamos el
archivo a

El motivo de este archivo es porque ahí se encuentra toda la data de correos que
comiencen con las iniciales “ra”. Este archivo nos será de utilidad debido a que el
correo que debemos analizar es **rainer.luecke@toyota.de**

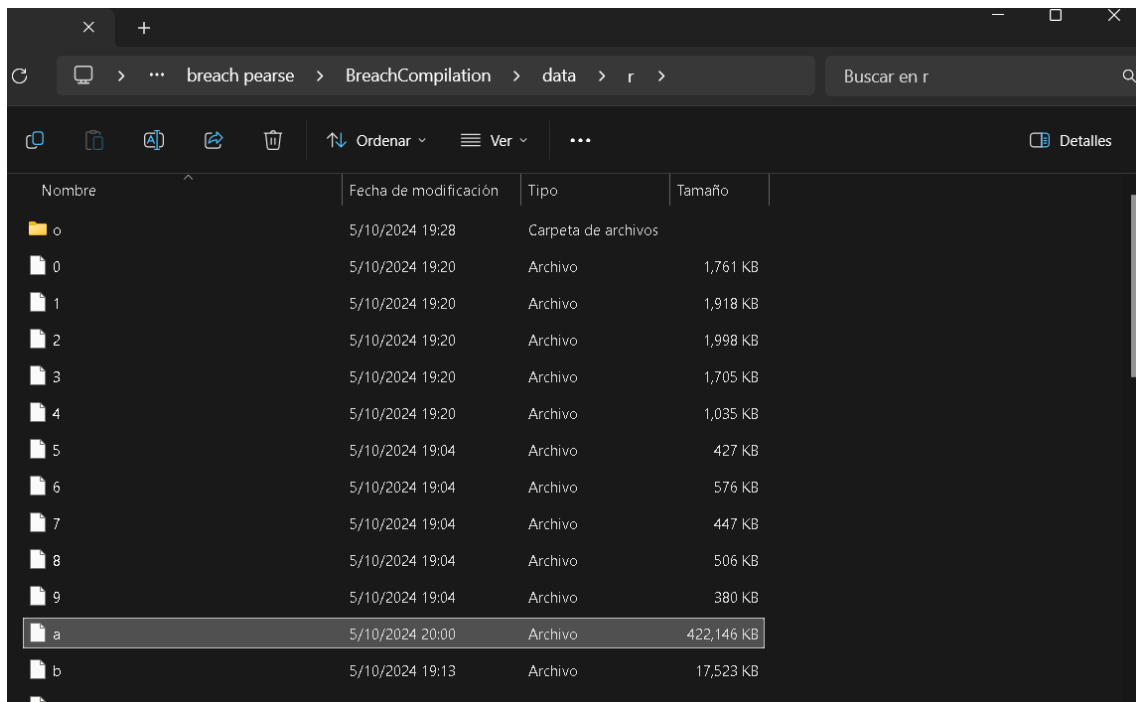
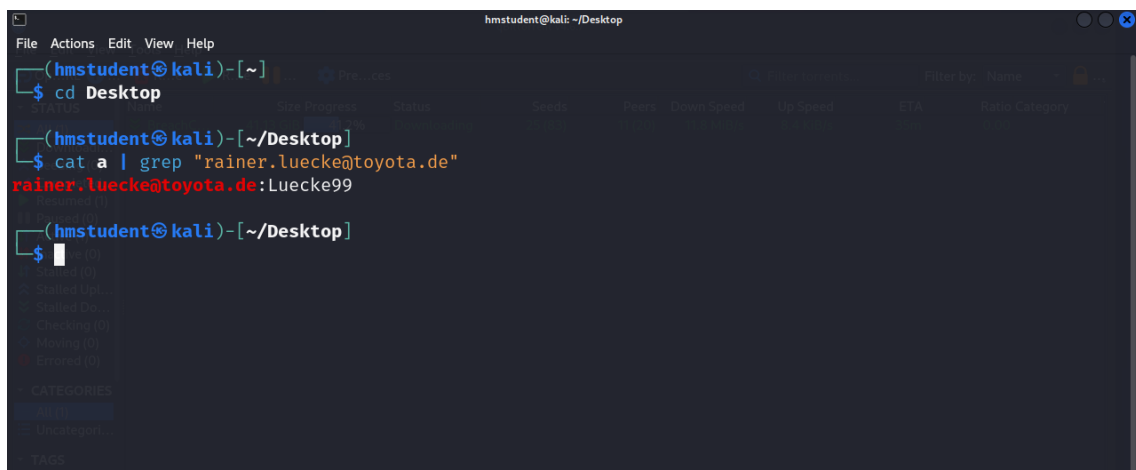


Ilustración 5. Sacando la base de datos de correos con iniciales ra.



Usando el comando grep hacemos búsqueda la línea donde se encuentre el correo electrónico.

Tenemos como respuesta -> rainer.luecke@toyota.de:Luecke99 siendo **Luecke99** la contraseña buscada.

2. Analizando los logs del sistema se ha detectado una intrusión, pero están incompletos conocemos parte de su email hacker-root_ _ [@live.cn](mailto:___@live.cn), podrías encontrar la contraseña del hacker?

¿Qué nos pide?

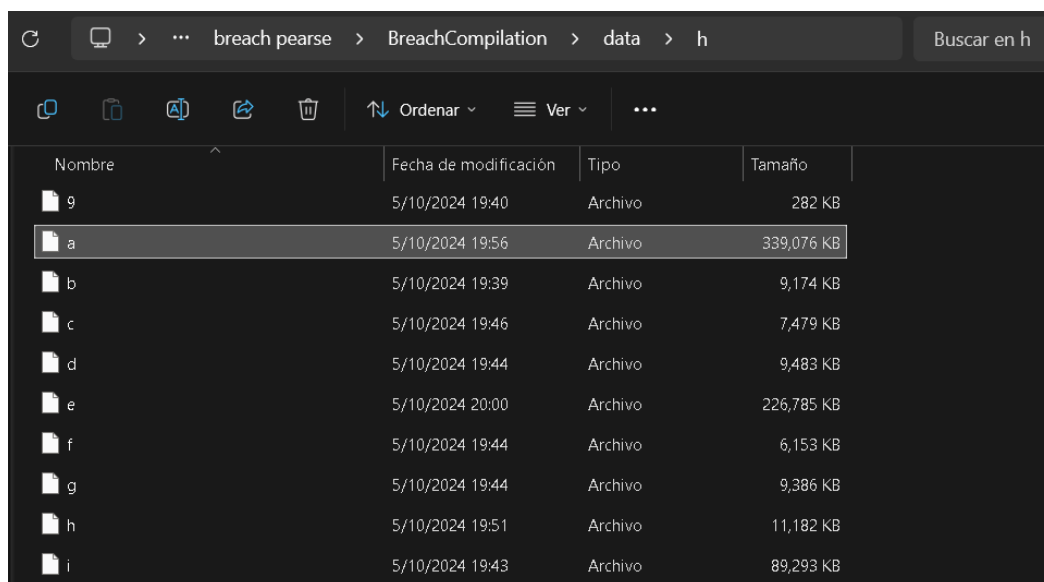
La contraseña de un correo electrónico que se encuentra dentro de la base de datos del repositorio Breach-parse

¿Qué información tenemos para investigar?

Tenemos un correo electrónico incompleto: hacker-root_ _ [@live.cn](mailto:___@live.cn)

Pasos a seguir

a) Buscar dentro de la base de datos los correos con las iniciales “Ha”



breach parse > BreachCompilation > data > h				Buscar en h
Nombre	Fecha de modificación	Tipo	Tamaño	
9	5/10/2024 19:40	Archivo	282 KB	
a	5/10/2024 19:56	Archivo	339,076 KB	
b	5/10/2024 19:39	Archivo	9,174 KB	
c	5/10/2024 19:46	Archivo	7,479 KB	
d	5/10/2024 19:44	Archivo	9,483 KB	
e	5/10/2024 20:00	Archivo	226,785 KB	
f	5/10/2024 19:44	Archivo	6,153 KB	
g	5/10/2024 19:44	Archivo	9,386 KB	
h	5/10/2024 19:51	Archivo	11,182 KB	
i	5/10/2024 19:43	Archivo	89,293 KB	

Ilustración 6. Base de datos de correos con las iniciales Ha

- b) Se hace uso del comando grep para buscar una línea dentro de la base de datos que contenga la parte inicial del correo.



```
(hmstudent@kali)-[~/Desktop]
$ cat a | grep "hacker-root"
hacker-rootkit@live.cn:shjzcy@#
```

Ilustración 7. Usando el comando grep para filtrar correo

Tenemos como respuesta un único correo con esa inicial por lo cual se asume que es el correo buscado debido a que también acaba en “live.cn”

Por lo tanto el correo buscado es hacker-rootkit@live.cn y la contraseña es shjzcy@#

3. 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?

Información obtenida del caso:

Dominio de la empresa TESLA: Tesla.com

¿Qué cosas se necesita hallar?

El nombre del servidor que se encuentre en Japón de la empresa tesla.com

La dirección IP del servidor del domino

Pasos a seguir:

- Usando la herramienta **dnsdumper** ponemos los dominios de la empresa a analizar

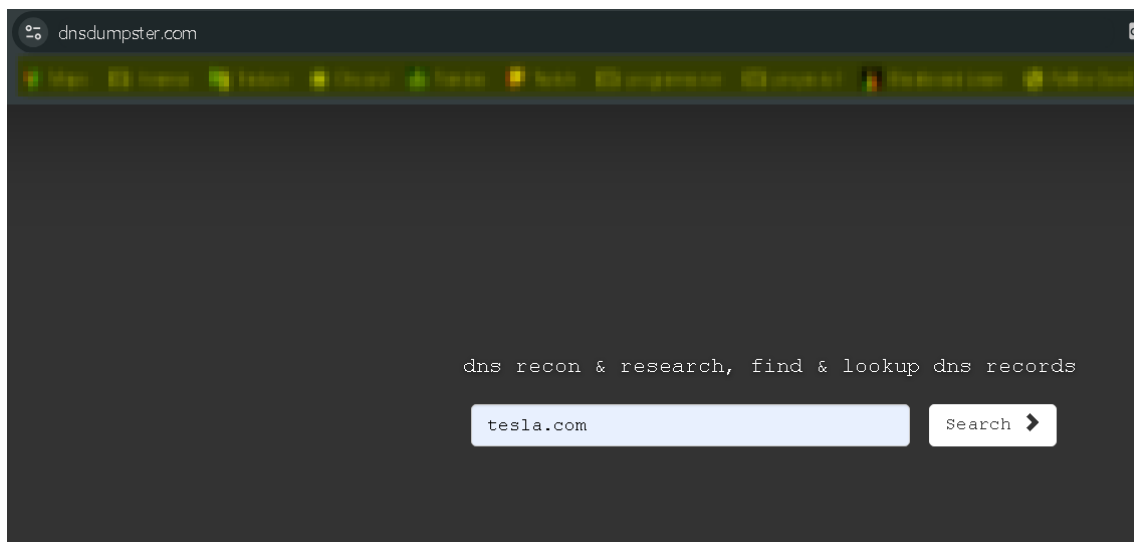


Ilustración 8. Usando el buscador de subdominios

- Nos mostrara una lista de dominios con su lugar de origen y la dirección IP

DNS Servers		
a10-67.akam.net. 🔍 🔄 🚫 🌐 🟢	96.7.50.67	AKAMAI-ASN2 United States
a12-64.akam.net. 🔍 🔄 🚫 🌐 🟢	184.26.160.64	AKAMAI-ASN2 United States
a28-65.akam.net. 🔍 🔄 🚫 🌐 🟢	95.100.173.65	AKAMAI-ASN2 The Netherlands
a1-12.akam.net. 🔍 🔄 🚫 🌐 🟢	193.108.91.12	AKAMAI-ASN2 The Netherlands
a9-67.akam.net. 🔍 🔄 🚫 🌐 🟢	184.85.248.67	AKAMAI-ASN2 United States
a7-66.akam.net. 🔍 🔄 🚫 🌐 🟢	23.61.199.66	AKAMAI-ASN2 United States
edns69.ultradns.com. 🔍 🔄 🚫 🌐 🟢	204.74.66.69	SECURITYSERVICES United States
MX Records ** This is where email for the domain goes...		
10 tesla-com.mail.protection.outlook.com. 🔍 🔄 🚫 🌐 🟢	52.101.41.21	MICROSOFT-CORP-MSN-AS-BLOCK United States

Ilustración 9. Resultados de las DNS de la empresa buscada

- Al analizar los dominios solo provenientes de Japón podemos ver que solo hay una dirección y a su vez podemos ver que proviene de una dirección de VPN

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

tesla.com [DNS] [OK] [X] [OK] [OK] [OK] HTTP: Akamai3Host	96.16.108.43 a96-16-108-43.deploy.static.akamaitechnologies.com	AKAMAI-AS United Kingdom
o7.ptr6980.tesla.com [DNS] [OK] [X] [OK] [OK] [OK]	149.72.144.42 o7.ptr6980.tesla.com	SENDGRID United States
email1.tesla.com [DNS] [OK] [X] [OK] [OK] [OK]	192.28.144.15 letgo.fivebelow.com	OMNITURE United States
apacvpn1.tesla.com [DNS] [OK] [X] [OK] [OK] [OK]	8.244.131.215	TESLA Japan
cnvpn1.tesla.com [DNS] [OK] [X] [OK] [OK] [OK]	114.141.176.215	SIN Shanghai Information Network Co.,Ltd. China
ptr1.tesla.com [DNS] [OK] [X] [OK] [OK] [OK]	117.50.35.199 ptr1.tesla.com	CHINANET-IDC-BJ-AP IDC, China Telecommunications Corporation China
vpn2.tesla.com [DNS] [OK] [X] [OK] [OK] [OK]	8.47.24.215	TESLA United States
ptr2.tesla.com [DNS] [OK] [X] [OK] [OK] [OK]	117.50.14.178 ptr2.tesla.com	CHINANET-IDC-BJ-AP IDC, China Telecommunications Corporation China
model3.tesla.com [DNS] [OK] [X] [OK] [OK] [OK]	205.234.27.221 origintest.teslamotors.com	QTS-SJC United States

Ilustración 10. Dominio con los requisitos pedidos

Debido a que es la única dirección que hace referencia una dirección VPN se asume que es la dirección buscada siendo el nombre de la dirección **apacvpn1.tesla.com** y la dirección IP **8.244.131.215**.