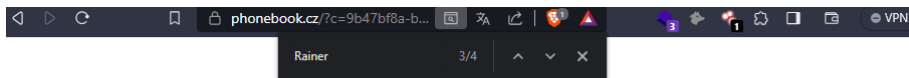


Tarea- Semana 1 Desarrollo

- 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"
2. 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?
3. ELon Musk debido los cambios en las politicas 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?

Desarrollo

- 1.) Teniendo en cuenta la información del dominio y el nombre del administrador, nos damos a la tarea de buscar el correo de la persona llamada (**Rainer Luecke**) en la siguiente pagina (**phonebook.cz**) de la empresa **_Intelligence X.** , Dando como resultado 268 correos con el dominio **Toyota.de**.



Phonebook.cz

[Logout](#)

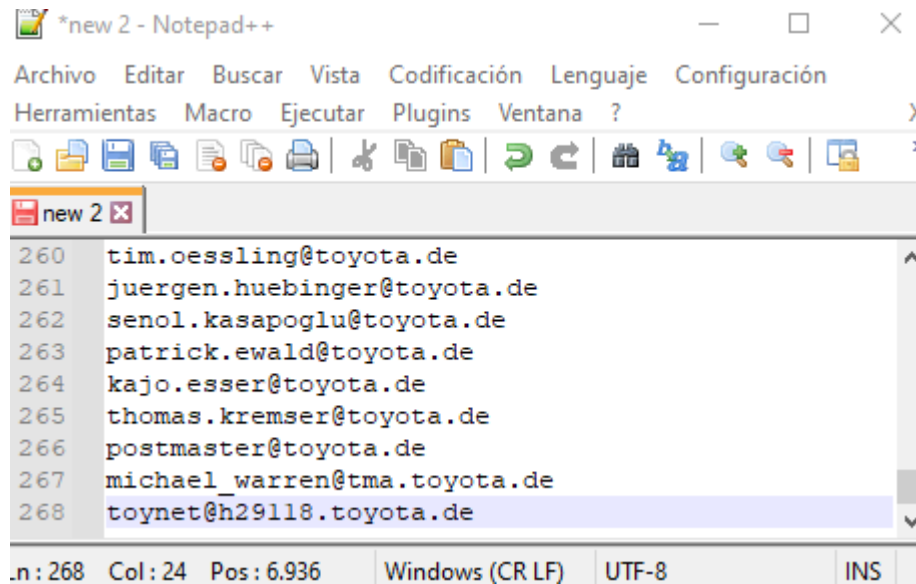
Phonebook lists all domains, email addresses, or URLs for the given input domain. Wildcards such as *.gov.uk are allowed. You are searching 100 billion records.

toyota.de

Try: [cia.gov](#), [cnn.com](#), [netflix.com](#), [*.ru](#), [*.gov.uk](#), [solarwinds.com](#)

- ☐ Domains
- ☒ Email Addresses
- ☐ URLs

[andre.schmidt@toyota.de](#)
[social@toyota.de](#)
[thomas.heidbrink@toyota.de](#)
[florian.kress@toyota.de](#)
[susanne.weigelt@toyota.de](#)
[katrin.schlautmann@toyota.de](#)
[dietrich.hartmann@toyota.de](#)
[ekhardt_sensendorfer@toyota.de](#)
[frank.dudley@toyota.de](#)
[achim.koch@toyota.de](#)



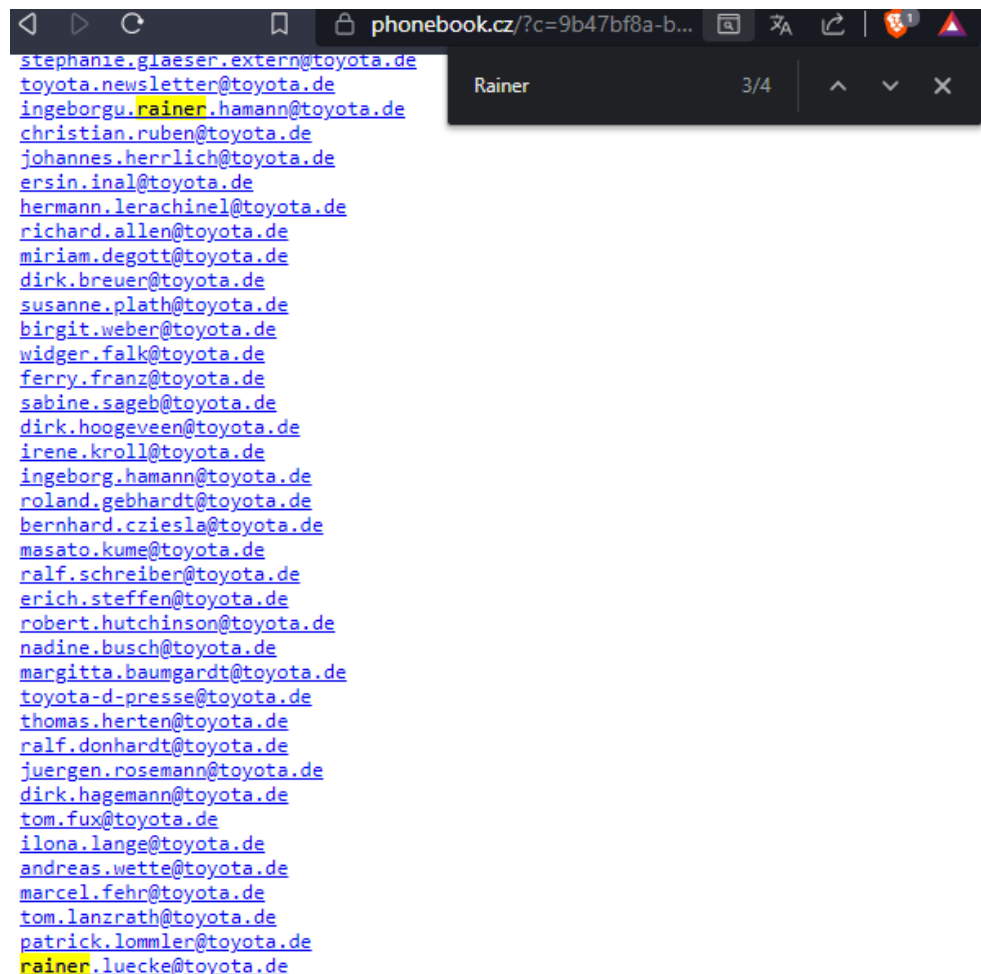
```

260 tim.oessling@toyota.de
261 juergen.huebinger@toyota.de
262 senol.kasapoglu@toyota.de
263 patrick.ewald@toyota.de
264 kajo.esser@toyota.de
265 thomas.kremser@toyota.de
266 postmaster@toyota.de
267 michael_warren@tma.toyota.de
268 toynet@h29118.toyota.de

```

.n: 268 Col: 24 Pos: 6.936 Windows (CR LF) UTF-8 INS

Con la ayuda del buscador damos que hay dos correos posibles con el nombre de **Rainer** pero solo uno con el apellido **Luecke**



phonebook.cz/?c=9b47bf8a-b...

Rainer 3/4

```

stephanie.glaeser.extern@toyota.de
toyota.newsletter@toyota.de
ingeborgu.rainer.hamann@toyota.de
christian.ruben@toyota.de
johannes.herrlich@toyota.de
ersin.inal@toyota.de
hermann.lerachinel@toyota.de
richard.allen@toyota.de
miriam.degott@toyota.de
dirk.breuer@toyota.de
susanne.plath@toyota.de
birgit.weber@toyota.de
widgef.falk@toyota.de
ferry.franz@toyota.de
sabine.sageb@toyota.de
dirk.hoogeveen@toyota.de
irene.kroll@toyota.de
ingeborg.hamann@toyota.de
roland.gebhardt@toyota.de
bernhard.cziesla@toyota.de
masato.kume@toyota.de
ralf.schreiber@toyota.de
erich.steffen@toyota.de
robert.hutchinson@toyota.de
nadine.busch@toyota.de
margitta.baumgardt@toyota.de
toyota-d-presse@toyota.de
thomas.herten@toyota.de
ralf.donhardt@toyota.de
juergen.rosemann@toyota.de
dirk.hagemann@toyota.de
tom.fux@toyota.de
ilona.lange@toyota.de
andreas.wette@toyota.de
marcel.fehr@toyota.de
tom.lanzrath@toyota.de
patrick.lommler@toyota.de
rainer.luecke@toyota.de

```

Los dos posibles correos son :

rainer.luecke@toyota.de

ingeborgu.rainer.hamann@toyota.de

Dando como resultado que el primer correo seria el mas acertado ya que cuenta con nombre y apellido brindado por la **Tarea – Semana 1** .

rainer.luecke@toyota.de

Para dar con la contraseña, e descargado una compilación de una fuente GitHub, donde tenemos que descargar un Utorrent que pesa alrededor de 41GB con documentos de contraseñas filtradas en internet.

The screenshot shows the GitHub repository page for 'breach-parse'. The repository is public and has 67 watches, 478 forks, and 1.5k stars. The main content area displays the repository's README, which describes it as a tool for parsing breached passwords. The README includes an installation section with a command to run 'install.sh' and a list of magnet links for downloading breached password lists. The right sidebar shows the repository's activity, including recent commits and a list of contributors.

breach-parse (Public)

Watch 67 Fork 478 Star 1.5k

master 1 branch 0 tags

Go to file Add file Code

About

A tool for parsing breached passwords

Readme Activity 1.5k stars 67 watching 478 forks Report repository

Releases

No releases published

Packages

No packages published

Contributors 4

- hmaverickadams
- seanbreckenridge
- evanottinger Evan Ottinger
- ChillerDragon Chiller Dragon

Languages

- Shell 100.0%

hmaverickadams Update breach-p... 84c59a4 on Mar 23, 2021 20 commits

File	Description	Time
.gitignore	add a gitignore to ignore any output files	4 years ago
README.md	Add auto-install. Usage: 'sudo ./install.sh'	2 years ago
breach-parse.sh	Update breach-parse.sh	2 years ago
install.sh	Change mode of install.sh to allow execution.	2 years ago

README.md

breach-parse

A tool for parsing breached passwords

Installation

Install: `sudo ./install.sh`

Download breached password list from magnet located here:

`magnet:?xt=urn:btih:7FbCd8cee06aba2ce6561688cf68ce2addca0a3&dn=BreachCompilation&tr=udp%3A%2F%2Ftracker.openbittorrent.com%3A80&tr=udp%3A%2F%2Ftracker.leechers-paradise.org%3A6969&tr=udp%3A%2F%2Ftracker.coppersurfer.tk%3A6969&tr=udp%3A%2F%2Fglotorrents.pw%3A6969&tr=udp%3A%2F%2Ftracker.opentrackr.org%3A1337`

If you don't store the password list (BreachCompilation) in `/opt/breach-parse`, specify the location like:

```
breach-parse @gmail.com gmail.txt "~/Downloads/BreachCompilation/data"
```

Run `breach-parse` for instructions

Una vez descargado todo el archivo, procedemos a nombrar todos los archivos con la extensión .txt, para eso se utiliza el comando en (Windows) Powershell

Get-ChildItem -File -Recurse | ForEach-Object { Rename-Item \$_.FullName -NewName "\$(\$_.BaseName).txt" }

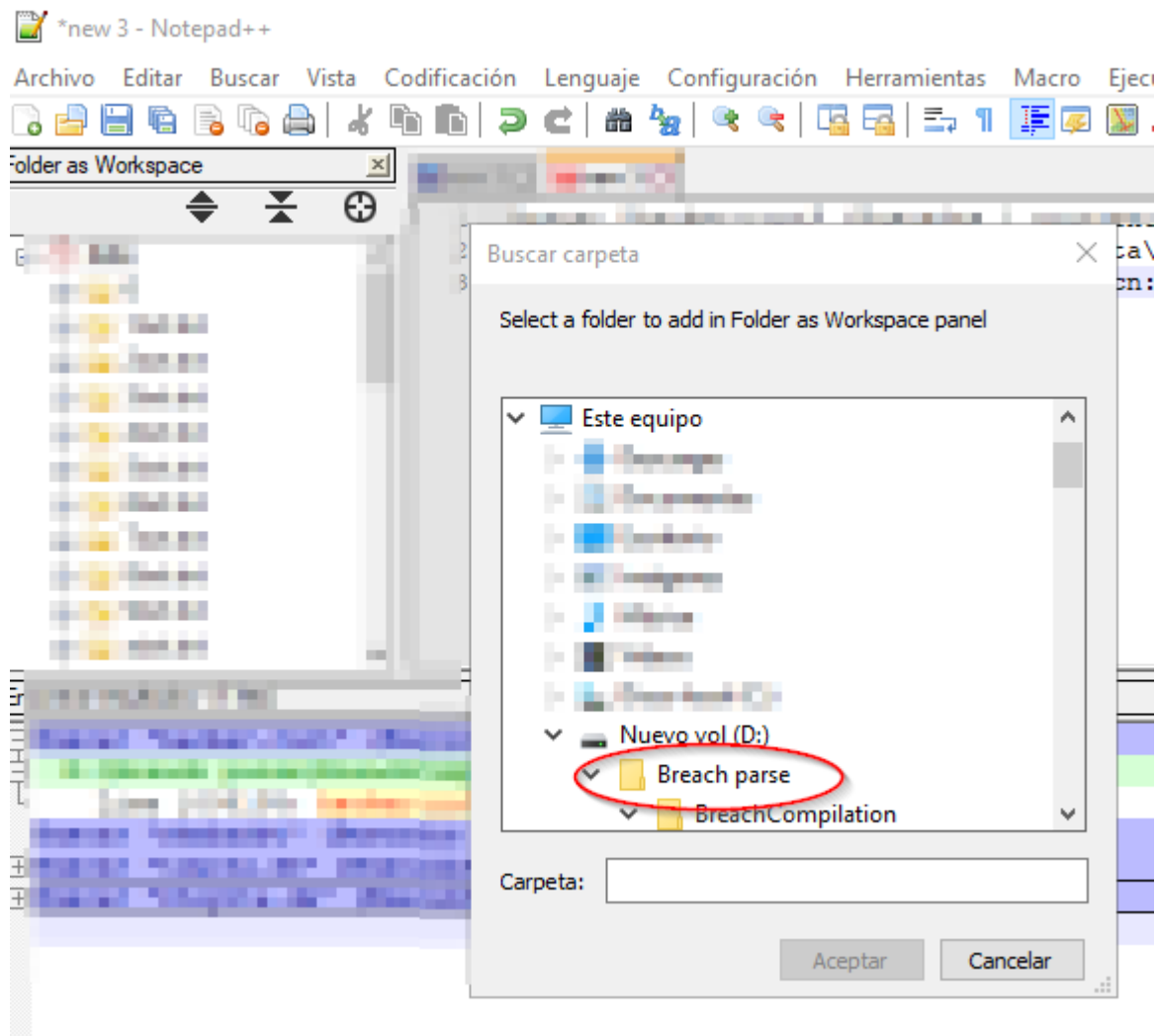
Este comando realizará lo siguiente:

1. **Get-ChildItem -File -Recurse:** Obtiene una lista de todos los archivos (-File) en todas las carpetas y subcarpetas (-Recurse).
2. **ForEach-Object { ... }:** Ejecuta el siguiente bloque de comandos para cada archivo encontrado.
3. **Rename-Item \$_.FullName -NewName "\$(\$_.BaseName).txt":** Cambia el nombre del archivo completo (\$_.FullName) agregando la extensión ".txt" al final del nombre base (\$_.BaseName).

Nombre	Fecha de modificación	Tipo	Tamaño
l.txt	28/08/2023 2:01 p. m.	Carpeta de archivos	
n.txt	28/08/2023 2:01 p. m.	Carpeta de archivos	
0	26/08/2023 3:24 p. m.	Archivo TXT	2.806 KB
1	26/08/2023 3:25 p. m.	Archivo TXT	6.723 KB
2	26/08/2023 3:24 p. m.	Archivo TXT	4.129 KB
3	26/08/2023 3:16 p. m.	Archivo TXT	2.518 KB
4	26/08/2023 3:16 p. m.	Archivo TXT	1.945 KB
5	26/08/2023 3:24 p. m.	Archivo TXT	1.890 KB
6	26/08/2023 3:24 p. m.	Archivo TXT	1.563 KB
7	26/08/2023 3:24 p. m.	Archivo TXT	3.157 KB
8	26/08/2023 3:24 p. m.	Archivo TXT	1.733 KB
9	26/08/2023 3:24 p. m.	Archivo TXT	1.455 KB
a	26/08/2023 3:24 p. m.	Archivo TXT	57.559 KB
b	26/08/2023 3:25 p. m.	Archivo TXT	131.713 KB
c	26/08/2023 3:24 p. m.	Archivo TXT	60.972 KB
d	26/08/2023 3:26 p. m.	Archivo TXT	188.182 KB
e	26/08/2023 3:25 p. m.	Archivo TXT	19.354 KB
f	26/08/2023 3:25 p. m.	Archivo TXT	34.069 KB
g	26/08/2023 3:26 p. m.	Archivo TXT	65.507 KB
h	26/08/2023 3:26 p. m.	Archivo TXT	51.864 KB
i	26/08/2023 3:27 p. m.	Archivo TXT	69.323 KB
j	26/08/2023 3:27 p. m.	Archivo TXT	37.064 KB
k	26/08/2023 3:27 p. m.	Archivo TXT	71.000 KB
m	26/08/2023 3:33 p. m.	Archivo TXT	213.007 KB
o	26/08/2023 3:35 p. m.	Archivo TXT	11.150 KB
p	26/08/2023 3:35 p. m.	Archivo TXT	61.330 KB
q	26/08/2023 3:35 p. m.	Archivo TXT	11.685 KB
r	26/08/2023 3:37 p. m.	Archivo TXT	279.333 KB
s	26/08/2023 3:39 p. m.	Archivo TXT	207.045 KB

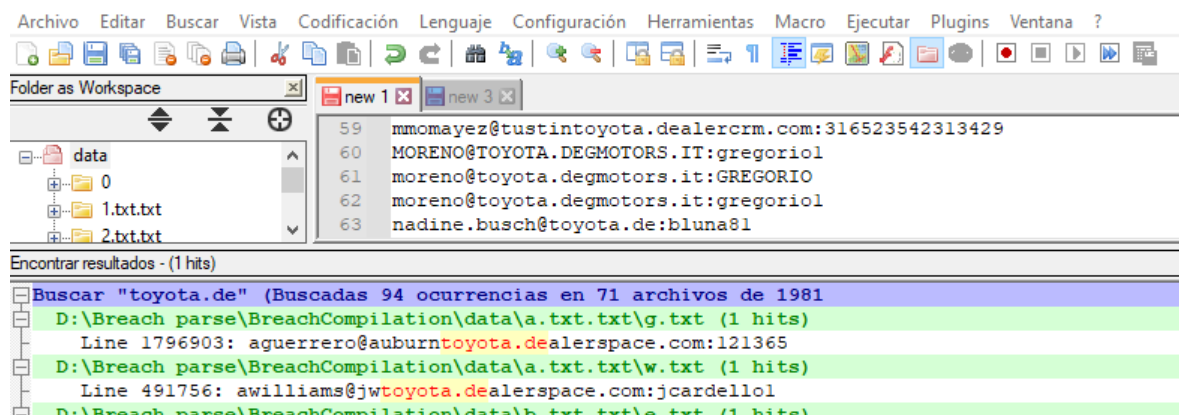
NOTA: No interesa que las carpetas también tengan el .txt, solo es la manera más fácil y rápida de poder colocar todos los archivos con extensión (.TXT)

Una vez tengamos todos los archivos en formato .txt procedemos a utilizar el Notepad++, el cual es un editor de notas pero con muchas mas funciones! En la parte de archivo y abrir carpeta de trabajo, vamos a buscar el **Breach parse** Para que la aplicación busque especialmente en esta carpeta los datos que necesitamos



Una vez dentro de la app y con la carpeta seleccionada procedemos a colocar el dominio que al cual tenemos conocimiento por la **Tarea – Semana1**

@toyota.de



Da como resultado “toyota.de” 94 ocurrencias en 71 archivos de 1981, copiamos los resultados y los pegamos en una nueva hoja, para luego proceder a colocar el correo anteriormente encontrado rainer.luecke@toyota.de

*new 1 - Notepad++

Archivo Editor **Buscar** Vista Codificación Lenguaje Configuración Herramientas Macro Ejecutar Plugins Ventana ?

Folder as Workspace

new 1 x new 3 x

59 mmomayez@tustintoyota.dealercrm.com:316523542313429
60 MORENO@TOYOTA.DEGMOTORS.IT:gregoriol
61 moreno@toyota.degmotors.it:GREGORIO
62 moreno@toyota.degmotors.it:gregoriol
63 nadine.busch@toyota.de:bluna81
64 nina.herkenberg@toyota.de:tonini
65 pbrown@raybrandttoyota.dealercrm.com:pl23456
66 ppittman@charlesbarkertoyota.dealercrm.com:carsales1
67 **rainer.luecke@toyota.de:Luecke99**
68 richard.allen@toyota.de:rhinacsi
69 richard.allen@toyota.de:indigo
70 robert.hutchinson@toyota.de:audigger
71 roger_lejeune@northshorettoyota.dealercrm.com:123451
72 roycesatterlund@kalispelltoyota.dealercrm.com:879666673099540
73 Sabine.Sageh@toyota.de:caluma

Encontrar resultados - (1 hits)

Buscar "toyota.de" (Buscadas 94 ocurrencias en 71 archivos de 1981)

D:\Breach parse\BreachCompilation\data\1.txt.txt\g.txt (1 hits)
Line 1796903: aguerrero@auburntoyota.dealerspace.com:121365
D:\Breach parse\BreachCompilation\data\1.txt.txt\w.txt (1 hits)
Line 491756: awilliams@jwtoyota.dealerspace.com:jcardellol
D:\Breach parse\BreachCompilation\data\2.txt.txt\w.txt (1 hits)
Line 9248144: bernhard.cziesla@toyota.de:311102481526736
D:\Breach parse\BreachCompilation\data\2.txt.txt\i.txt (2 hits)
Line 106476: BIRGIT.WEBER@TOYOTA.DE:toytoa
Line 106477: BIRGIT.WEBER@toyota.de:toytoa
D:\Breach parse\BreachCompilation\data\2.txt.txt\w.txt (1 hits)
Line 43892: bwalden@valentitoyota.dealercrm.com:dealer8960
D:\Breach parse\BreachCompilation\data\3.txt.txt\d.txt (1 hits)
Line 659339: cdubord@raybrandttoyota.dealercrm.com:cl23456
D:\Breach parse\BreachCompilation\data\3.txt.txt\r.txt (1 hits)
Line 2290782: create@putnamtoyota.dealerspace.com:gosia999
D:\Breach parse\BreachCompilation\data\4.txt.txt\1.txt (1 hits)
Line 232535: Daniela.Endres@toyota.de:sonnel23

Nos da como resultado a la búsqueda

rainer.luecke@toyota.de:Luecke99

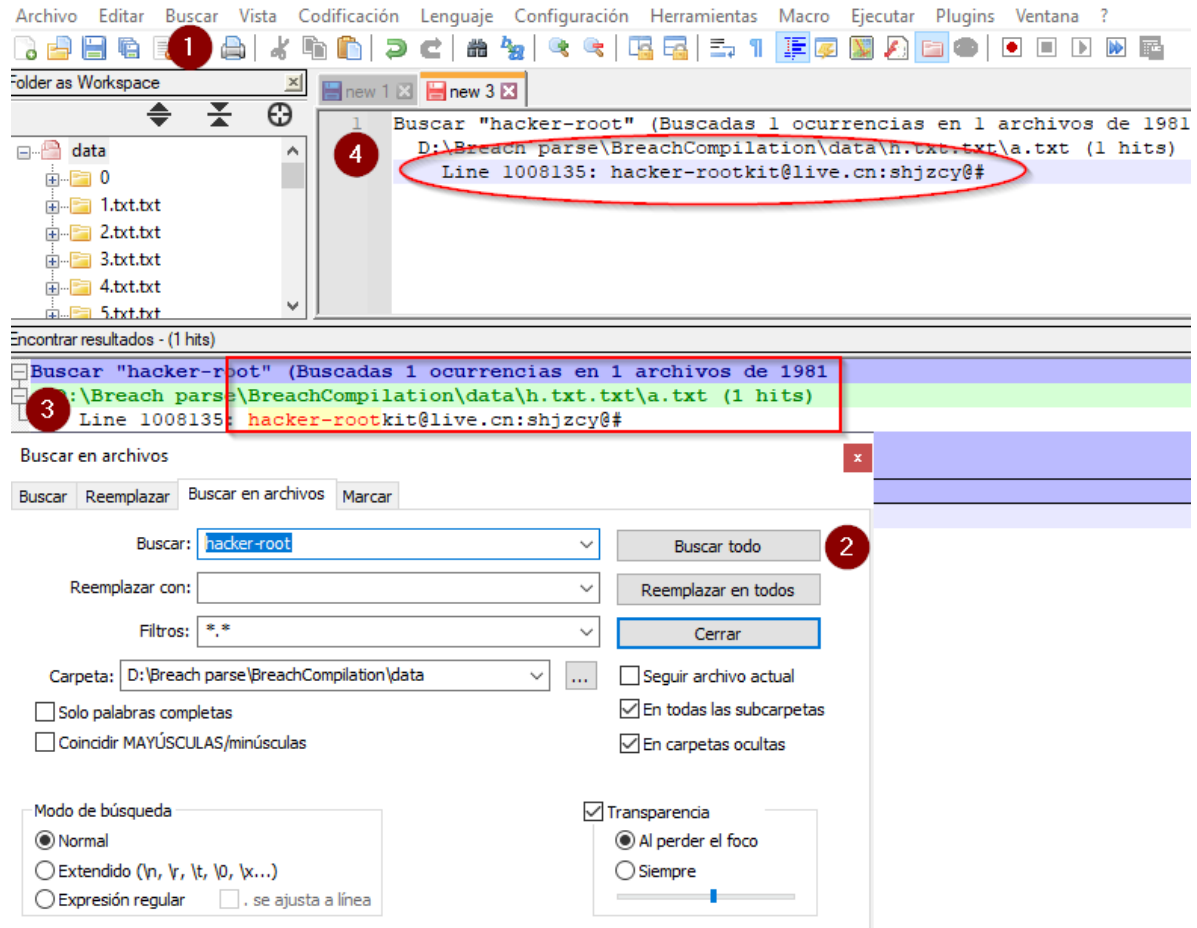
En este momento tenemos la solución del primer problema dándonos como resultado el correo y su posible contraseña

rainer.luecke@toyota.de



rainer.luecke@toyota.de: - Pass: Luecke99

- 2.) Nuevamente vamos a buscar un usuario con contraseña con la compilación de GitHub llamado "breach parse" en el mismo programa de Notepad++, la única información es que era un correo con dominio @live.cn y con una parte de nombre hacker-root__ después de filtrar nos da este resultado

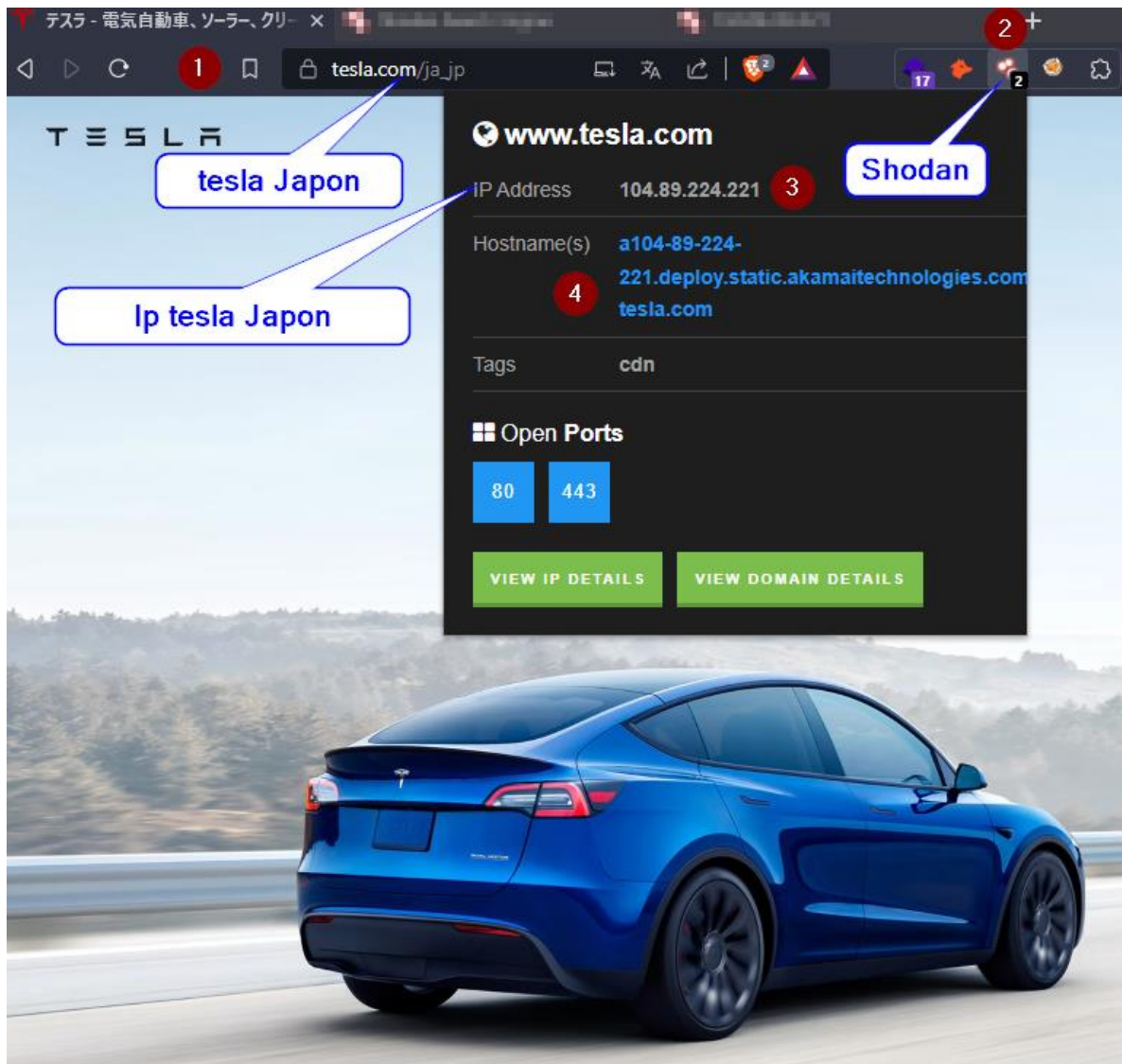


El único usuario que cumple con sus características es

[hacker-rootkit@live.cn – Pass: shjzcy@#](#)

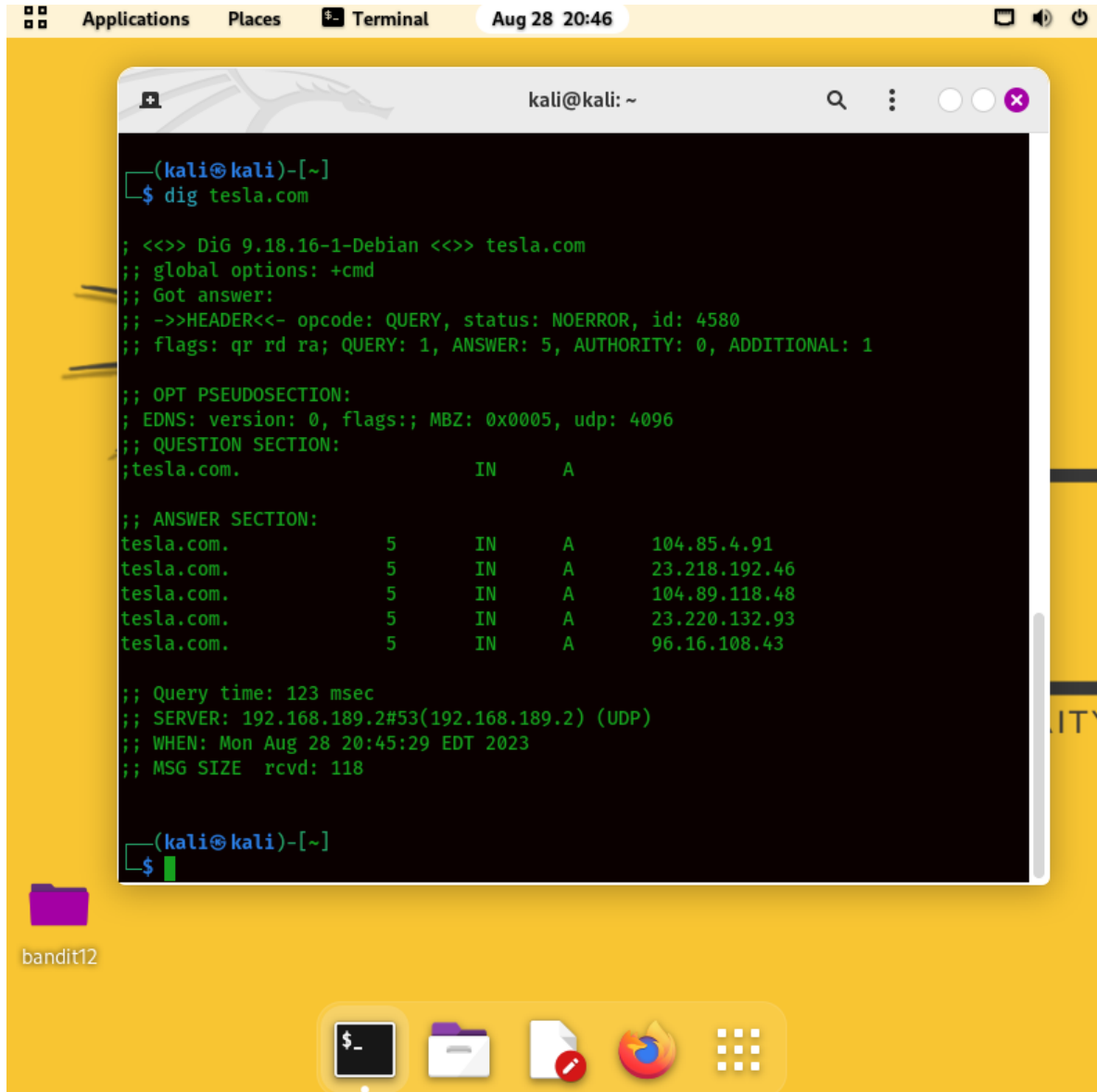


- 3.) Primero vamos a ingresar a la pagina oficial de tesla japon, que en este caso es tesla.com/ja_jp, una vez dentro vamos a la pestaña del plugin de [Shodan](#) para poder verificar la dirección IP y el nombre del host.



Una vez tengamos esa información podemos proceder al Kali, y verificarlo con el comando `dig` para ver los servidores DNS mas las direcciones IP asociadas al nombre host TESLA.COM el comando seria

`dig tesla.com`



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the output of the command `dig tesla.com`. The output includes DNS header information, a question section for tesla.com, and an answer section listing five IP addresses for tesla.com. The desktop background is yellow, and the terminal window has a dark background with green text. The terminal window title is 'kali@kali: ~'. The desktop has a top bar with 'Applications', 'Places', and 'Terminal' buttons, and a bottom bar with icons for a terminal, file manager, and other applications. A folder icon labeled 'bandit12' is visible on the desktop.

```
(kali@kali)-[~]
$ dig tesla.com

;; <<>> DiG 9.18.16-1-Debian <<>> tesla.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4580
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4096
;; QUESTION SECTION:
;tesla.com.                IN      A

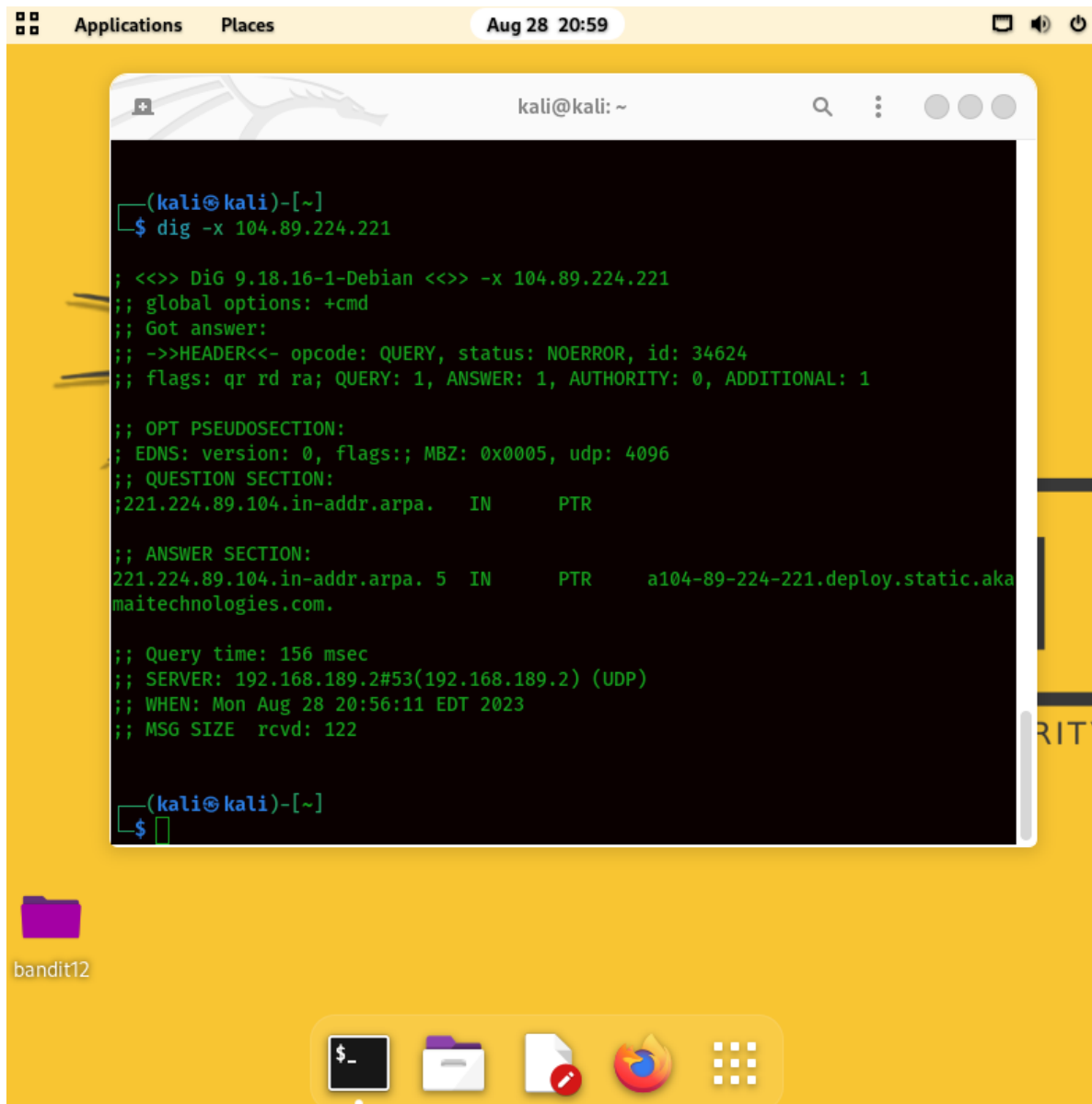
;; ANSWER SECTION:
tesla.com.                5       IN      A      104.85.4.91
tesla.com.                5       IN      A      23.218.192.46
tesla.com.                5       IN      A      104.89.118.48
tesla.com.                5       IN      A      23.220.132.93
tesla.com.                5       IN      A      96.16.108.43

;; Query time: 123 msec
;; SERVER: 192.168.189.2#53(192.168.189.2) (UDP)
;; WHEN: Mon Aug 28 20:45:29 EDT 2023
;; MSG SIZE rcvd: 118

(kali@kali)-[~]
$
```

Posteriormente ejecutamos nuevamente el comando `dig` pero esta vez con la función `-x` para realizar una consulta DNS inversa y poder encontrar el nombre del dominio registrado a esta IP, en este caso el comando seria

`dig -x 104.89.224.221`



The screenshot shows a Kali Linux desktop with a yellow background. A terminal window is open, displaying the output of the command `dig -x 104.89.224.221`. The output shows a successful reverse DNS lookup for the IP address 104.89.224.221, identifying it as `a104-89-224-221.deploy.static.akamaitechnologies.com`. The desktop includes a top bar with 'Applications' and 'Places' menus, a clock showing 'Aug 28 20:59', and system icons. The bottom dock contains icons for a terminal, file manager, a document, Firefox, and the application menu. A folder icon labeled 'bandit12' is visible on the left side of the desktop.

```
(kali㉿kali)~  
$ dig -x 104.89.224.221  
  
; <<>> DiG 9.18.16-1-Debian <<>> -x 104.89.224.221  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34624  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4096  
;; QUESTION SECTION:  
;221.224.89.104.in-addr.arpa. IN PTR  
  
;; ANSWER SECTION:  
221.224.89.104.in-addr.arpa. 5 IN PTR a104-89-224-221.deploy.static.akamaitechnologies.com.  
  
;; Query time: 156 msec  
;; SERVER: 192.168.189.2#53(192.168.189.2) (UDP)  
;; WHEN: Mon Aug 28 20:56:11 EDT 2023  
;; MSG SIZE rcvd: 122  
  
(kali㉿kali)~  
$
```

En la sección **ANSWER SECTION** veremos la dirección IP proporcionada mas el nombre del servidor asociado en este caso

ANSWER SECTION

221.224.89.104.in-addr.arpa. 5 IN PTR a104-89-224-221.deploy.static.akamaitechnologies.com.

```
;; ANSWER SECTION:  
221.224.89.104.in-addr.arpa. 5 IN PTR a104-89-224-221.deploy.static.akamaitechnologies.com.
```

221.224.89.104.in-addr.arpa. Esto nos traduce a que la dirección IP esta en formato reversa el cual se forma al tomar los octetos de la dirección ip original y se escriben en orden inverso, seguido de “in-addr.arpa” la cual es una convención utilizada en las consultas de resolcion inversa DNS

5 en este contexto se refiere al tiempo de vida (TTL) de la entrada en segundos, indicando cuanto tiempo la respuesta se mantendrá en el cache antes que deba ser refrescada

IN el tipo de registro en este caso IN de (Internet) el cual se utiliza para direcciones IPv4

PTR este tipo de registro significa “Pointer o puntero”. Los registros PTR se utilizan en consultas de resolución inversa para asociar una dirección IP con un Dominio

a104-89-224-221.deploy.static.akamaitechnologies.com. este es el nombre del dominio asociado a la dirección IP proporcionada, en este caso parece ser a nombre de Akamai Technologies, una empresa que ofrece servicios de entrega de contenido y aeleracion WEB

Con lo anterior podemos deducir que el VPN instalado en Tesla Japon, es prestado por la empresa Akamai Technologies, dando como resultado la dirección IP **104.89.224.221** a nombre de Akamai Technologies de la VPN

Ya que las direcciones IP de tesla.com serian

```
└─(kali㉿kali)-[~] └─$ dig +short tesla.com
```


104.85.4.91

23.220.132.93

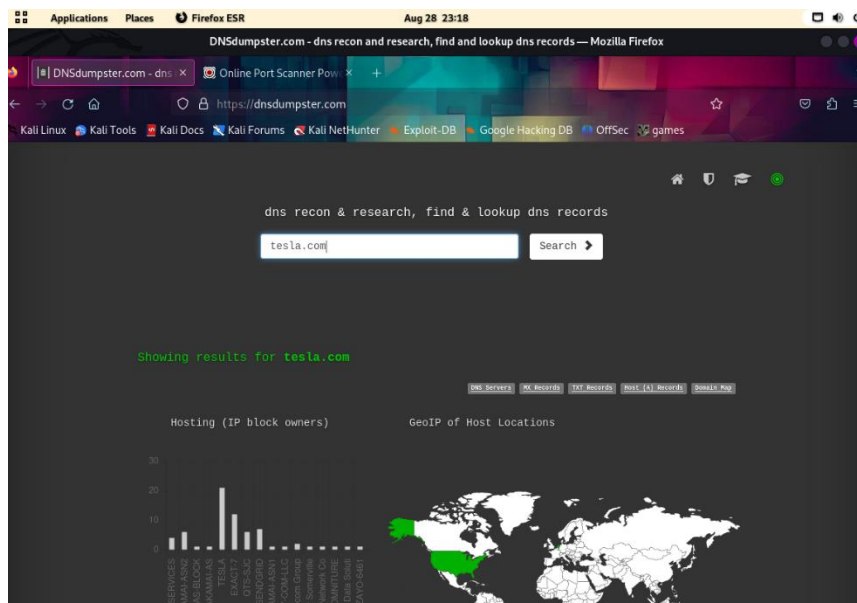
96.16.108.43

23.218.192.46

104.89.118.48

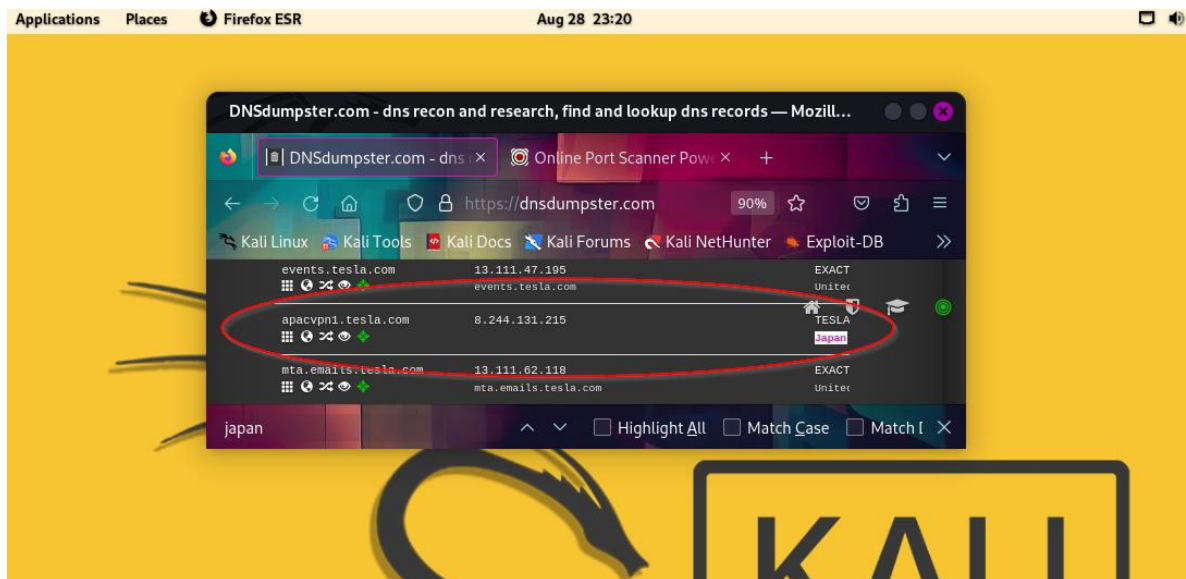
En conclusión, la VPN esta a nombre de 
Akamai Technologies con la IP 104.89.224.221

Por otro lado investigando, podemos entrar a la pagina DNSdumpster.com para verificar el cual es un sitio web y una herramienta en línea que se utiliza para recopilar y mostrar información relacionada con nombres de dominio y registros DNS. Una vez dentro colocamos el nombre de dominio en este caso esla.com)



Podemos obtener informacion variada de Tesla.com, en este caso utilice

CTRL + F para buscar en la pagina el nombre de japon y ver que resultados me arrojaba, una vez el buscador subraya la palabra japon me encuentro con esta información



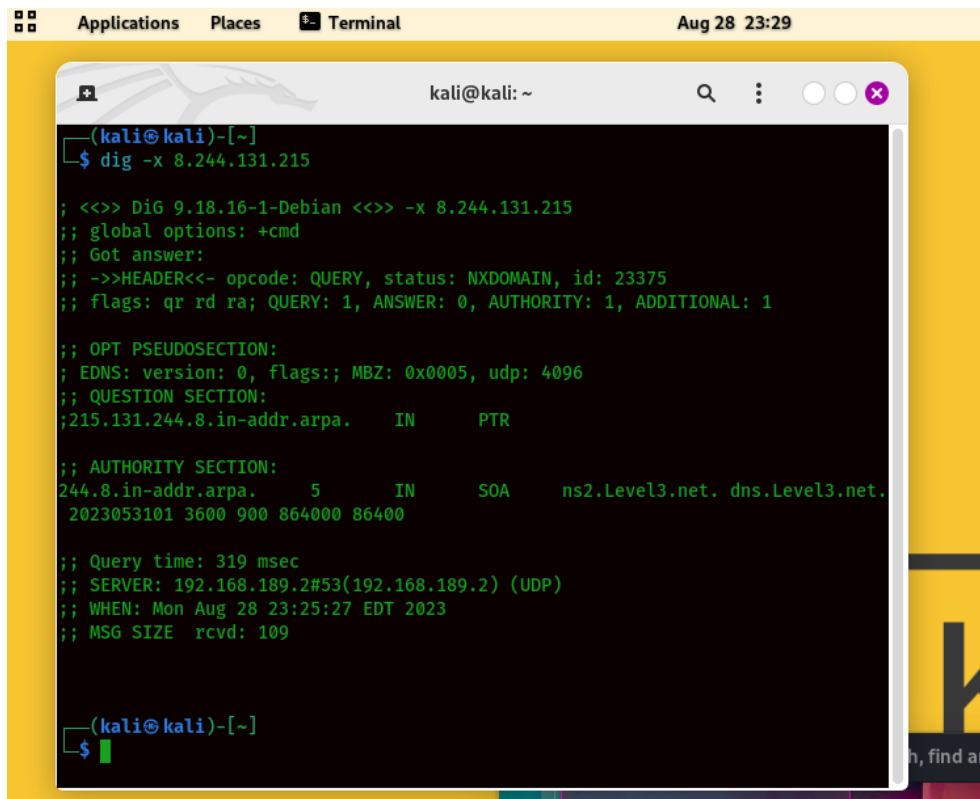
apacvpn1.tesla.com

8.244.131.215

TESLA

Japan

Una vez dada una IP diferente a la anteriormente encontrada, vamos a la terminal de Kali a verificar la dirección IP con una búsqueda inversa para eso colocaremos el comando **dig -x 8.244.131.215** y nos encontramos con el siguiente resultado



```
(kali@kali)-[~]
$ dig -x 8.244.131.215

;<<>> DiG 9.18.16-1-Debian <<>> -x 8.244.131.215
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 23375
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:;; MBZ: 0x0005, udp: 4096
;; QUESTION SECTION:
;215.131.244.8.in-addr.arpa.    IN      PTR

;; AUTHORITY SECTION:
244.8.in-addr.arpa.    5      IN      SOA     ns2.Level3.net. dns.Level3.net.
2023053101 3600 900 864000 86400

;; Query time: 319 msec
;; SERVER: 192.168.189.2#53(192.168.189.2) (UDP)
;; WHEN: Mon Aug 28 23:25:27 EDT 2023
;; MSG SIZE rcvd: 109

(kali@kali)-[~]
$
```

El comando **dig -x 8.244.131.215** ejecutado realiza una búsqueda inversa (también conocida como resolución inversa) de la dirección IP 8.244.131.215. La resolución inversa implica buscar el nombre de dominio asociado con una dirección IP dada. Sin embargo, el resultado obtenido indica que no se encontró un registro PTR (Pointer) asociado con esa dirección IP.

El status "**NXDOMAIN**" significa que no se encontró un registro PTR asociado con la dirección IP 8.244.131.215. Esto sugiere que el nombre de dominio reverso para esa dirección IP no está configurado.

En la sección de "**AUTHORITY**", se proporciona información sobre la autoridad responsable de la zona de dirección IP inversa 244.8.in-addr.arpa. El servidor de nombres autorizado es ns2.Level3.net.

Con esto deducimos que otra posible respuesta sería que la dirección IP y el nombre sería

En conclusión, la VPN está a nombre de
ns2.Level3.net con la IP 8.244.131.215



¡Este último Ejercicio se me dificultó un poco, por eso coloqué las dos posibles respuestas! Espero pronto aclarar dudas