

# Unidad de trabajo



Alumno: Jonathan Jesus Jacinto Badillo

País: Perú

Telegram: Jesús.J

Correo: [jesusbjonathan@gmail.com](mailto:jesusbjonathan@gmail.com)

SEMANA 1

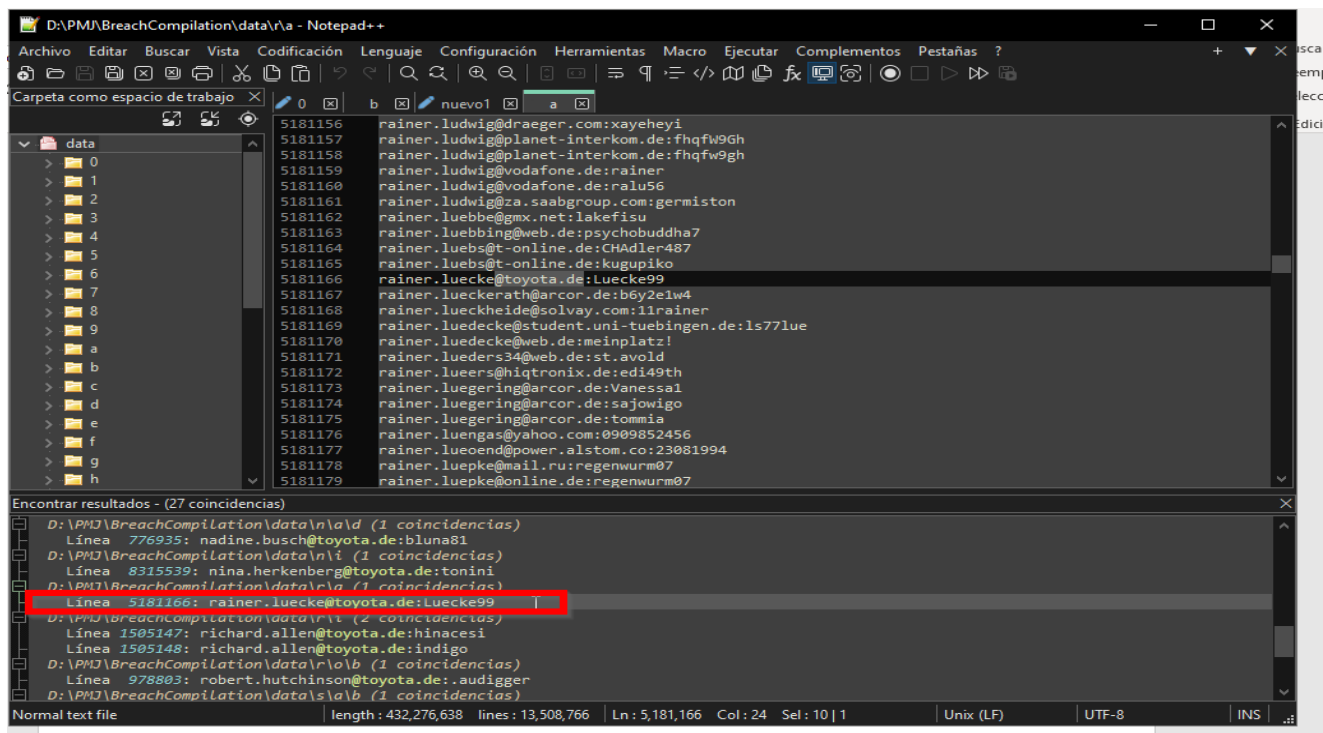
Fecha: 25 de agosto del 2023

# SEMANA 1

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"

## RESOLUCIÓN:

```
root@DESKTOP-5VQNQJD:/mnt/d/PMJ/BreachCompilation/data# grep "@toyota.de" -r .
.:89165396637@toyota-detail.ru:145236
.:9163963463@toyota-detail.ru:145236
grep: ./b/e: binary file matches
.:BIRGIT.WEBER@toyota.de:toytoa
.:Daniela.Endres@toyota.de:sonnel23
grep: ./d/i: binary file matches
.:ferry.franz@toyota.de:ragna1969
.:Frank.Wielpuetz@toyota.de:Karnevall
.:gerd.hamacher@toyota.de:sabine
.:Hermann.LeRachinel@toyota.de:leonie50
grep: ./i/n: binary file matches
.:irene.kroll@toyota.de:Lennart
.:katrin.schlautmann@toyota.de:london
grep: ./m/a/n: binary file matches
.:marion.adler@toyota.de:titleist
.:moreno@toyota.degmotors.it:GREGORIO
.:moreno@toyota.degmotors.it:gregorio1
.:nadine.busch@toyota.de:bluna81
grep: ./n/i: binary file matches
.:pdejonge@toyota-dejonge.nl:melissa1
.:rainer.luecke@toyota.de:Luecke99
.:richard.allen@toyota.de:hinacesi
.:richard.allen@toyota.de:indigo
grep: ./r/o/b: binary file matches
.:Sabine.Sageb@toyota.de:calypso
grep: ./t/h: binary file matches
.:ulrike.humartus@toyota.de:englein
.:widger.falk@toyota.de:deuce2003
root@DESKTOP-5VQNQJD:/mnt/d/PMJ/BreachCompilation/data#
```



The screenshot shows a Notepad++ window with a list of email addresses and passwords. The entry 'rainer.luecke@toyota.de:Luecke99' is highlighted in red. Below the list, a search results window shows the same entry highlighted in red.

```
5181156 rainer.ludwig@draeger.com:xayehey1
5181157 rainer.ludwig@planet-interkom.de:fhqfw9Gh
5181158 rainer.ludwig@planet-interkom.de:fhqfw9Gh
5181159 rainer.ludwig@vodafone.de:rainer
5181160 rainer.ludwig@vodafone.de:ralu56
5181161 rainer.ludwig@za.saabgroup.com:germiston
5181162 rainer.luebbe@gmx.net:lakefisu
5181163 rainer.luebbing@web.de:psychobuddha7
5181164 rainer.luebs@t-online.de:CHAdler487
5181165 rainer.luebs@t-online.de:kugupiko
5181166 rainer.luecke@toyota.de:Luecke99
5181167 rainer.lueckerath@arcor.de:b6y2e1w4
5181168 rainer.luecke@solway.com:11rainer
5181169 rainer.luedecke@student.uni-tuebingen.de:ls77lue
5181170 rainer.luedecke@web.de:meinplatz!
5181171 rainer.lueders34@web.de:st.avold
5181172 rainer.lueers@hiqtronix.de:edi49th
5181173 rainer.luegering@arcor.de:Vanessa1
5181174 rainer.luegering@arcor.de:sajowigo
5181175 rainer.luegering@arcor.de:tommia
5181176 rainer.luegas@yahoo.com:0909852456
5181177 rainer.luegend@power.alstom.co:23081994
5181178 rainer.luepke@mail.ru:regenwurm07
5181179 rainer.luepke@online.de:regenwurm07
```

Encontrar resultados - (27 coincidencias)

```
D:\PMJ\BreachCompilation\data\n\ad (1 coincidencias)
Línea 776935: nadine.busch@toyota.de:bluna81
D:\PMJ\BreachCompilation\data\n\i (1 coincidencias)
Línea 8315539: nina.herkenberg@toyota.de:tonini
D:\PMJ\BreachCompilation\data\r\l (1 coincidencias)
Línea 5181166: rainer.luecke@toyota.de:Luecke99
D:\PMJ\BreachCompilation\data\r\l (2 coincidencias)
Línea 1505147: richard.allen@toyota.de:hinacesi
Línea 1505148: richard.allen@toyota.de:indigo
D:\PMJ\BreachCompilation\data\r\o\b (1 coincidencias)
Línea 978803: robert.hutchinson@toyota.de:audigger
D:\PMJ\BreachCompilation\data\s\l\b (1 coincidencias)
```

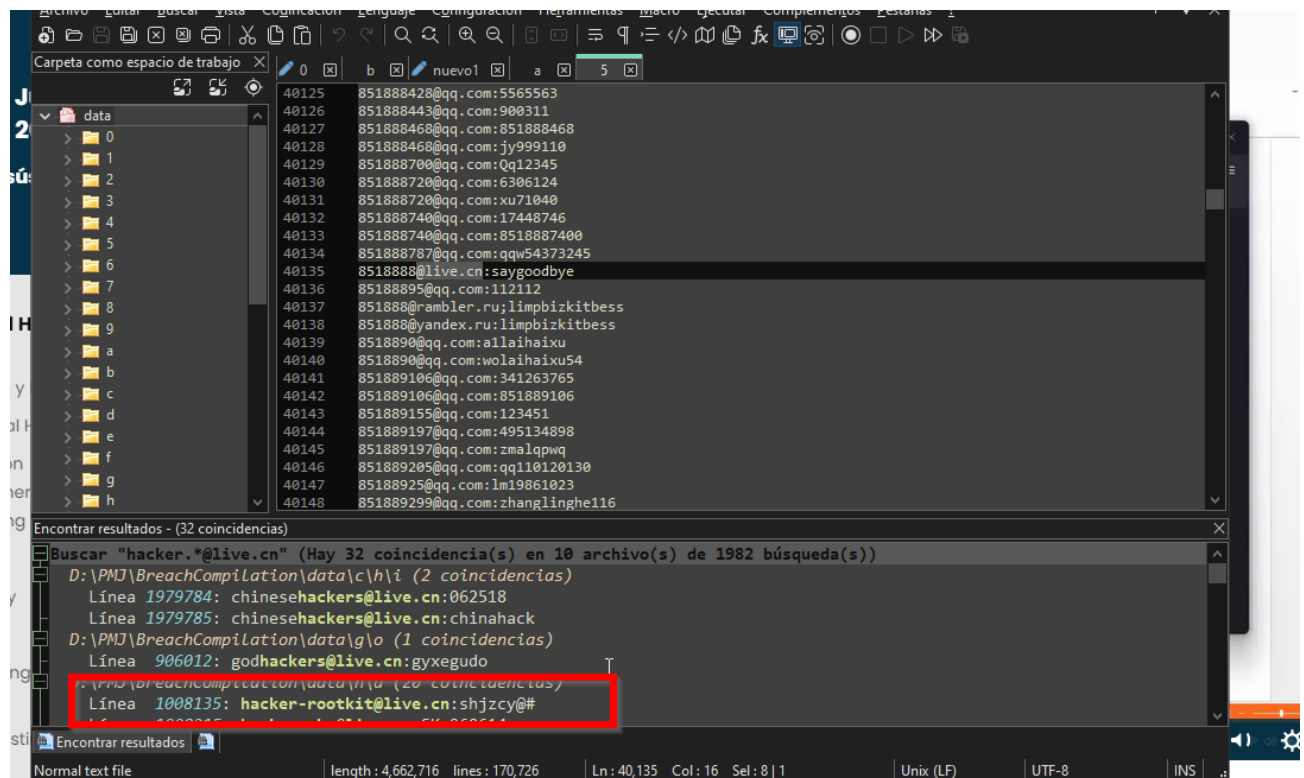
ADMIN USER: [rainer.luecke@toyota.de](mailto:rainer.luecke@toyota.de)

PASSWORD: Luecke99

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?

#### RESOLUCIÓN:

```
root@DESKTOP-5VQNQJD: /mnt/d/PMJ/BreachCompilation/data
root@DESKTOP-5VQNQJD: /mnt/d/PMJ/BreachCompilation/data# grep "hacker-root.*@live.cn" -r .
root@DESKTOP-5VQNQJD: /mnt/d/PMJ/BreachCompilation/data# grep -E "hacker-root.*@live.cn" -r .
:hacker-rootkit@live.cn:shjzcy@#
```

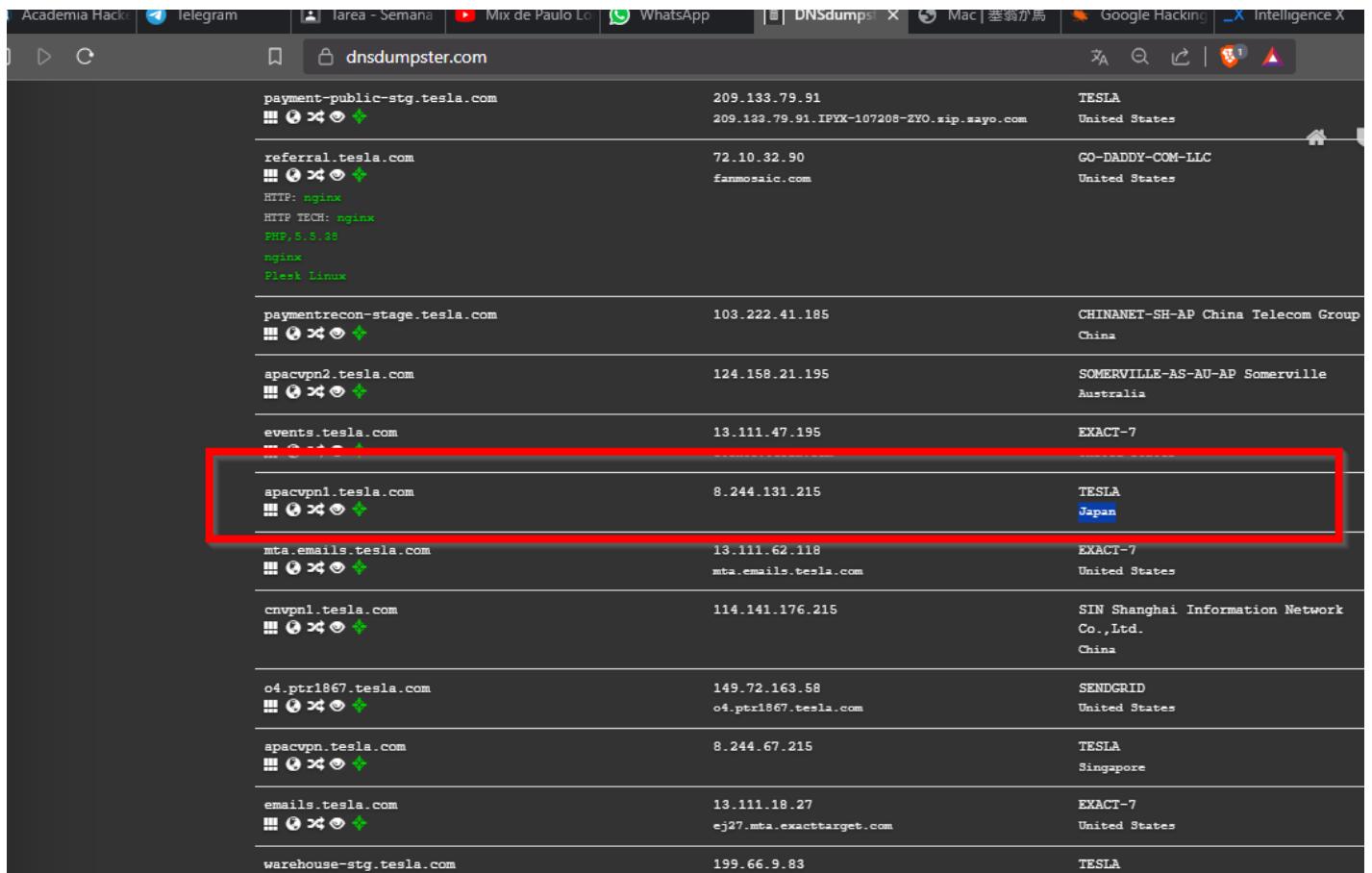


ADMIN USER: hacker-rootkit@live.cn

PASSWORD: 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?

**RESOLUCIÓN:**



payment-public-stg.tesla.com	209.133.79.91	TESLA
	209.133.79.91.IFYX-107208-ZYO.sip.sayo.com	United States
referral.tesla.com	72.10.32.90	GO-DADDY-COM-LLC
	fanmosaic.com	United States
HTTP: nginx		
HTTP TECH: nginx		
PHP: 5.3.28		
nginx		
Fresh Linux		
paymentrecon-stage.tesla.com	103.222.41.185	CHINANET-SH-AP China Telecom Group
		China
apacvpn2.tesla.com	124.158.21.195	SOMERVILLE-AS-AU-AP Somerville
		Australia
events.tesla.com	13.111.47.195	EXACT-7
		United States
apacvpn1.tesla.com	8.244.131.215	TESLA
		Japan
mta.emails.tesla.com	13.111.62.118	EXACT-7
	mta.emails.tesla.com	United States
cnvpn1.tesla.com	114.141.176.215	SIN Shanghai Information Network
		Co.,Ltd.
		China
o4.ptr1867.tesla.com	149.72.163.58	SENDGRID
	o4.ptr1867.tesla.com	United States
apacvpn.tesla.com	8.244.67.215	TESLA
		Singapore
emails.tesla.com	13.111.18.27	EXACT-7
	cj27.mta.exacttarget.com	United States
warehouse-stg.tesla.com	199.66.9.83	TESLA

Nombre del servidor:

Dirección IP:

- apacvpn1.tesla.com → - 8.244.131.215