**ALUMNO: David Tafolla Recinos**

## 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"

1. Con el BerachParse descargado hice la búsqueda del domino “toyota.de”

```
┌──(root㉿kali)-[/home/hmstudent/Clase1/breach-parse]
└─# breach-parse @toyota.de  Toyota.txt "/home/hmstudent/Clase1/breach-parse/BreachCompilation/data"
Progress : [########################################] 100%
Extracting usernames...
Extracting passwords...
```

2. Abrí el archivo “Toyota-master.txt” para verificar la información completa de los usuarios; y como eran pocos usuarios solamente busqué el nombre de la persona o algo aparecido a su nombre habiendo una coincidencia:

```
┌──(root㉿kali)-[/home/hmstudent/Clase1/breach-parse]
└─# cat Toyota-master.txt
Sabine.Sageb@toyota.de:calypso
89165396637@toyota-detail.ru:145236
Hermann.LeRachinel@toyota.de:leonie50
BIRGIT.WEBER@toyota.de:toytoa
bernhard.cziesla@toyota.de:311102481526736
thomas.herten@toyota.de:th987654
moreno@toyota.degmotors.it:GREGORIO
moreno@toyota.degmotors.it:gregorio1
manfred.draschner@toyota.de:md041958
marion.adler@toyota.de:titleist
katrin.schlautmann@toyota.de:london
Daniela.Endres@toyota.de:sonne123
dirk.hoogeveen@toyota.de:denise
gerd.hamacher@toyota.de:sabine
9163963463@toyota-detail.ru:145236
pdejonge@toyota-dejonge.nl:melissa1
nadine.busch@toyota.de:bluna81
nina.herkenberg@toyota.de:tonini
widger.falk@toyota.de:deuce2003
ingeborg.hamann@toyota.de:familie5
irene.kroll@toyota.de:Lennart
robert.hutchinson@toyota.de:.audigger
rainer.luecke@toyota.de:Luecke99
richard.allen@toyota.de:hinacesi
richard.allen@toyota.de:indigo
ulrike.humartus@toyota.de:englein
Frank.Wielpuetz@toyota.de:Karneval1
ferry.franz@toyota.de:ragna1969
```

3. Dando como resultado final el usuario: **rainer.luecke@toyota.de: 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?**

Para ello hay 2 opciones ya que se sabe parte del correo:

1. **Utilizando el query.sh de BreachCompilation que es un filtro :**

```
┌──(root㉿kali)-[/home/hmstudent/Clase1/breach-parse/BreachCompilation]
└─# bash query.sh hacker-root
hacker-rootkit@live.cn:shjzcy@#
```

   Dando como resultado final el correo y pasword de la filtración:
   **hacker-rootkit@live.cn**

2. **Utilizando la extracción del dominio "live.cn" mediante Breach-parse:**

```
┌──(root㉿kali)-[/home/hmstudent/Clase1/breach-parse]
└─# breach-parse @live.cn  Livecn.txt "/home/hmstudent/Clase1/breach-parse/BreachCompilation/data"
Progress : [########################################] 100%
Extracting usernames...
Extracting passwords...
```

   Posteriormente se utiliza grep para filtrar el resultado de "Livecn-master-txt" que es donde se guardaron todos los resultados de la búsqueda anterior con la información brinda del correo, dando como resultado final la búsqueda del correo:

```
┌──(root㉿kali)-[/home/hmstudent/Clase1/breach-parse]
└─# grep "hacker-root" Livecn-master.txt
hacker-rootkit@live.cn:shjzcy@#
```

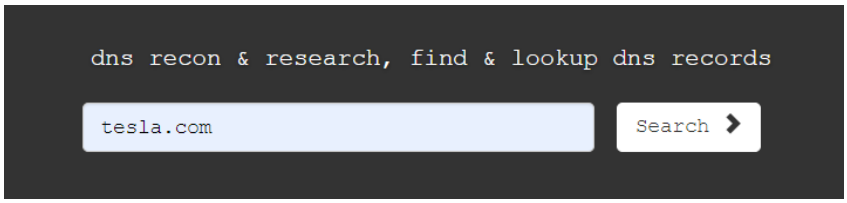
3. **ELon Musk debido los cambios en las políticas de EEUU ha decidido instalar un servicio VPN para su empresa TESLA (tesla.com), en Japón, serás capaz de encontrar el nombre y dirección ip del servidor?**

   Para buscar información de TESLA utilice https://dnsdumpster.com/ de esta forma indicándome todos los subdominios de TESLA y solamente busque uno que me indicará que estuviera en Japón dando como resultado final:

   **Nombre: apacvpn1.tesla.com**

   **IP del servidor: 8.244.131.215**

   Búsqueda:




   Resultado: