TAREA - Semana 1:
RECONOCIMIENTO PASIVO

PROF. ISRAEL AGUIRRE

Alumno:

Nahuel Matías Fortuna

Correo:

nahu_888@hotmail.com

-2024-

INDICE

***CONTENIDO**

1) Introducción.

En el presente informe se abordan tres actividades relacionadas con la seguridad informática, específicamente en el contexto del Ethical Hacking. Este trabajo tiene como objetivo poner en práctica habilidades de análisis y resolución de problemas ante situaciones de ciberseguridad.

Las actividades propuestas involucran el análisis de posibles filtraciones de datos en empresas reconocidas, como Toyota y Tesla, así como la identificación de contraseñas y la localización de servidores a través de técnicas de investigación digital. A través de este ejercicio, se busca fomentar una comprensión más profunda de los métodos de defensa y ataque en el mundo cibernético.

2) Objetivo.

- Identificar y analizar vulnerabilidades en sistemas informáticos a través de técnicas de Ethical Hacking.
- Recopilar y evaluar información para descifrar contraseñas relacionadas con filtraciones de datos.
- Localizar servidores y su configuración para asegurar la protección de la infraestructura digital de empresas reconocidas.

3) Consigna.

Subir en un documento PDF las 3 respuestas de las siguientes actividades:

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 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?

Nota:

- Para este trabajo pueden utilizar cualquier formato.
- Ejemplo de cómo nombrar el archivo PDF: Tarea 1 - Juan López. pdf
- Deben colocar los siguientes datos dentro del documento PDF para poderles identificar y asignarles su calificación:
  - nombre y apellido
  - correo

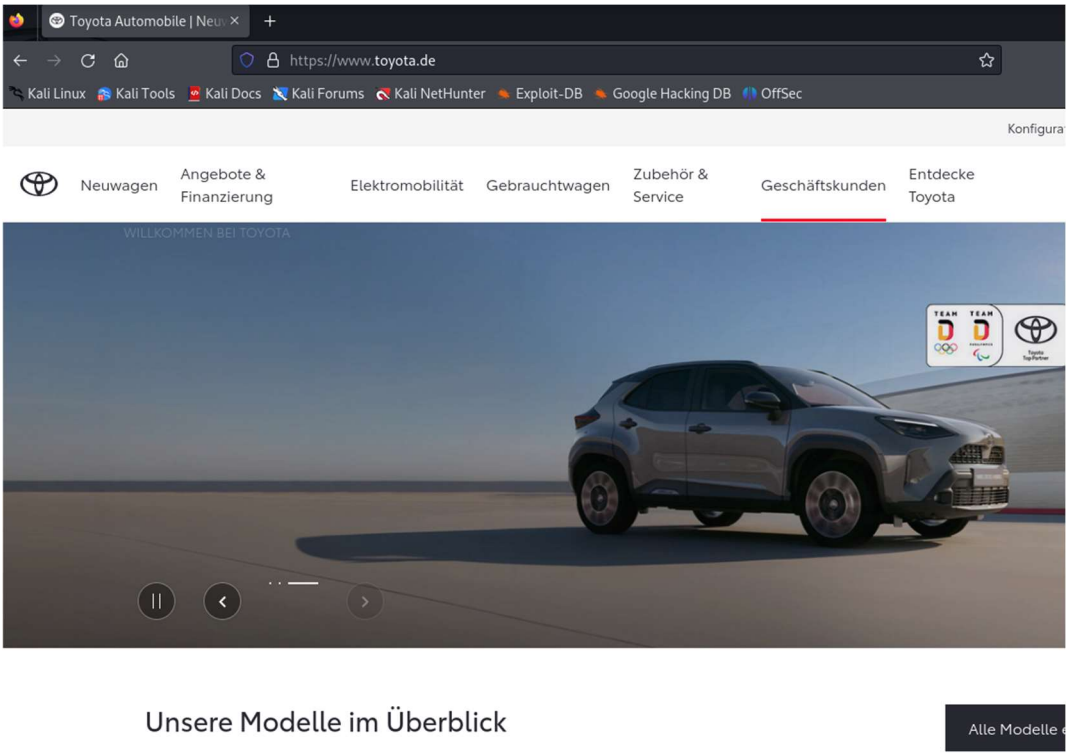
IMPORTANTE

Revisar que cuenten con espacio en su drive para poder subir la tarea y recibir su calificación.

4) Resolución.

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".

Para esta tarea debemos primero reconocer nuestro objetivo con una búsqueda simple en el navegador.



Toyota es una de las principales fabricantes de automóviles en el mundo, originaria de Japón. Fundada en 1937 por Kiichiro Toyoda, la empresa es conocida por su innovación en la industria automotriz, incluyendo el desarrollo de métodos de producción eficientes, como el sistema de producción Toyota (TPS). Además, Toyota ha sido pionera en la producción de vehículos híbridos, destacándose con el modelo Prius. La compañía también se enfoca en la sostenibilidad y la movilidad futura, explorando tecnologías como vehículos eléctricos y autónomos.

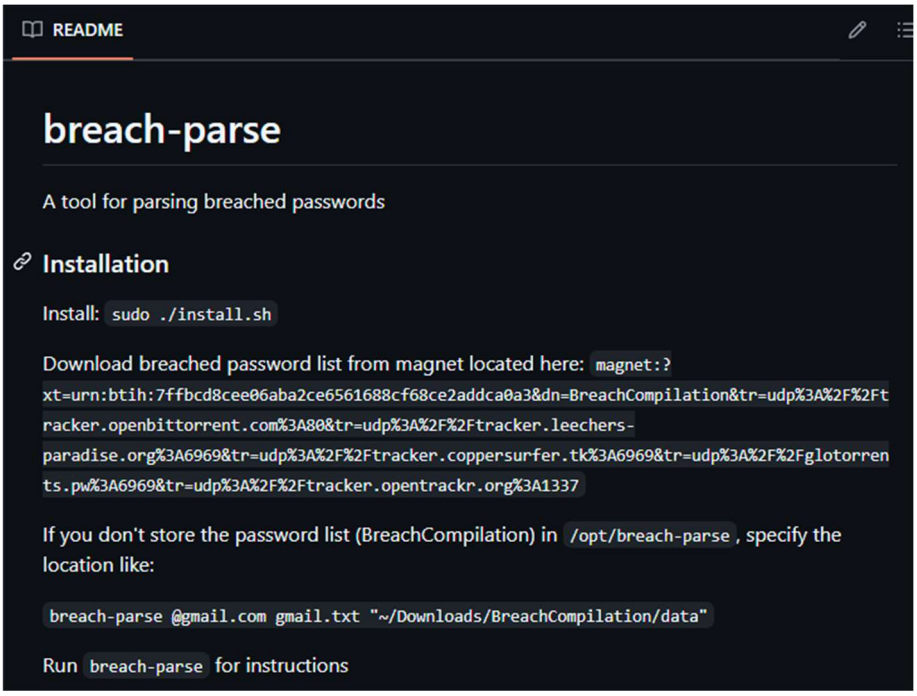
Entendiendo entonces cual es nuestro objetivo, pasamos a la descarga del Breach-Parce donde dice nuesto enunciado que encontramos el usuario/contraseña de Rainer Luecke.

Para esto en Kali descargamos una herramienta para poder obtenerlo, Transmision es un cliente de BitTorrent que se utiliza en sistemas operativos basados en Linux, como Kali Linux. Permite a los usuarios descargar y compartir archivos a través de la red BitTorrent de manera eficiente. Para instalarlo:

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install transmission
```

Se descargaran una serie de paquetes, si te pide alguna apbacion debes apretar “y” luego finalizara correctamente.

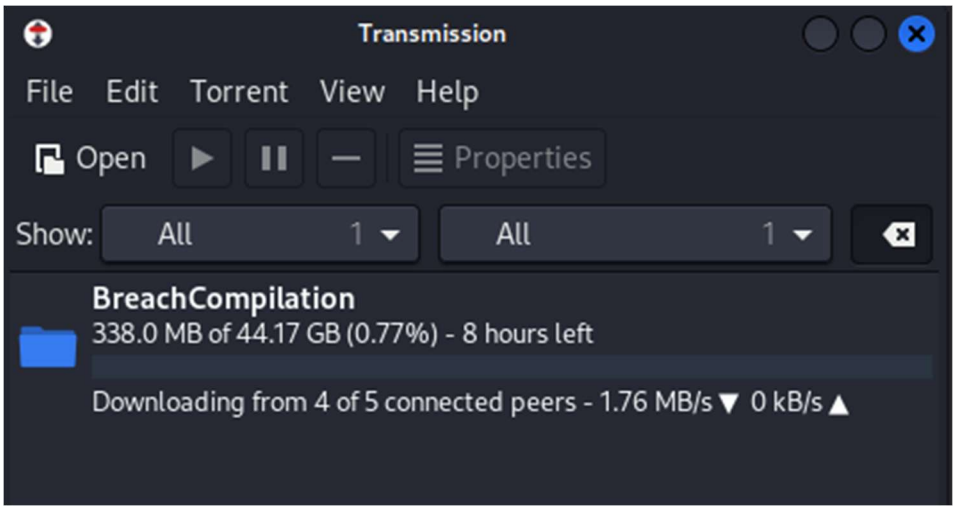
Pasamos a buscar el Breah Parce, si buscamos en Google apaecera el repositorio siguiente: https://github.com/hmaverickadams/breach-parse/tree/master, allí tenemos los pasos de instalación.



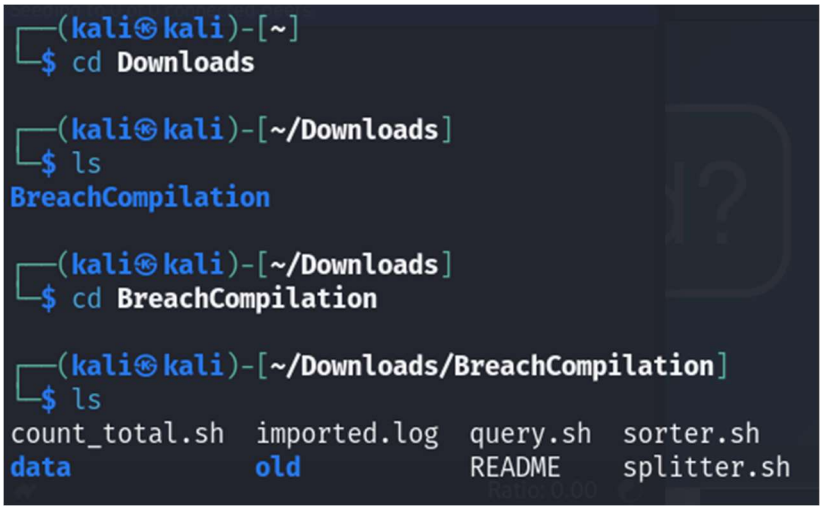
Copiamos entonces lo siguiente y lo pegamos en el navegador.

```
Download breached password list from magnet located here: magnet:?
xt=urn:btih:7ffbcd8cee06aba2ce6561688cf68ce2addca0a3&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
```

Ahora pegamos en el navegador y ENTER.



Comenzara la descarga, luego terminada la misma se vera de la siguiente manera.



Lo movemos de la carpeta de descargas a la de opt como dice allí y luego le damos los permisos necesarios para ejecutarlo.

Creamos un .txt con los posibles nombres que podría tomar el usuario administrador. En nuestro caso será RainerLuecke.txt.

```
┌──(kali㉿kali)-[/opt/BreachCompilation]
└─$ nano RainerLuecke.txt
```

```
┌──(kali㉿kali)-[/opt/BreachCompilation]
└─$ cat RainerLuecke.txt
RainerLuecke
rainerluecke
LueckeRainer
lueckerainer
Rainer.Luecke
Rainer_Luecke
rainer.luecke
rainer_luecke
```

Listo entonces nuestro diccionario pasamos a ejecutar el Breach con el dominio @toyota.de y nuestro diccionario, buscando en “data” donde posee la información la herramienta si encuentra nuestro objetivo.

```
┌──(kali㉿kali)-[/opt/BreachCompilation]
└─$ ./breach-parse.sh @toyota.de RainerLuecke.txt "/opt/BreachCompilation/
data"

Progress : [########################################] 100%
Extracting usernames...
Extracting passwords...
```

Terminado el proceso (100%), pasamos a revisar nuestros archivos creados de usuarios, contraseñas y masters.

```
┌──(kali㉿kali)-[/opt/BreachCompilation]
└─$ ls
breach-parse.sh  old                        RainerLuecke-users.txt
count_total.sh   query.sh                   README
data             RainerLuecke-master.txt    sorter.sh
imported.log     RainerLuecke-passwords.txt splitter.sh
install.sh       RainerLuecke.txt
```

```
┌──(kali㉿kali)-[/opt/BreachCompilation]
└─$ cat RainerLuecke-master.txt
marion.adler@toyota.de:titleist
manfred.draschner@toyota.de:md041958
moreno@toyota.degmotors.it:GREGORIO
moreno@toyota.degmotors.it:gregorio1
rainer.luecke@toyota.de:Luecke99
robert.hutchinson@toyota.de:audigger
richard.allen@toyota.de:hinacesi
richard.allen@toyota.de:indigo
nadine.busch@toyota.de:bluna81
nina.herkenberg@toyota.de:tonini
Frank.Wielpuetz@toyota.de:Karneval1
ferry.franz@toyota.de:ragna1969
89165396637@toyota-detail.ru:145236
katrin.schlautmann@toyota.de:london
bernhard.cziesla@toyota.de:311102481526736
```

rainer.luecke@toyota.de:Luecke99

Obtenemos entonces rainer.luecke@toyota.de y su contraseña 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 este ejercicio, ya descargada la herramienta, utilizamos el mismo método pero ahora usando @live.cn y creando un nuevo mail.txt que tenga dentro la opción hacker-root*.

Nos quedaría asi:

```
┌──(kali㉿kali)-[/opt/BreachCompilation]
└─$ ./breach-parse.sh @live.cn mail.txt "/opt/BreachCompilati
on/data"
```

Termina de cargar veremos nuestras archivos.

```
Progress : [########################################] 100%
Extracting usernames...
Extracting passwords...
```

```
┌──(kali㉿kali)-[/opt/BreachCompilation]
└─$ ls
breach-parse.sh     old
count_total.sh      query.sh
data                RainerLuecke-master.txt
imported.log        RainerLuecke-passwords.txt
install.sh          RainerLuecke.txt
mail-master.txt     RainerLuecke-users.txt
mail-passwords.txt  README
mail.txt            sorter.sh
mail-users.txt      splitter.sh
```

Pasamos a leer el master, y que nos busque directamente la opción que empiece como dice nuestra consigna con grep hacker-root*.

```
┌──(kali㉿kali)-[/opt/BreachCompilation]
└─$ cat mail-master.txt | grep hacker-root*
hacker-rootkit@live.cn:shjzcy@#
```

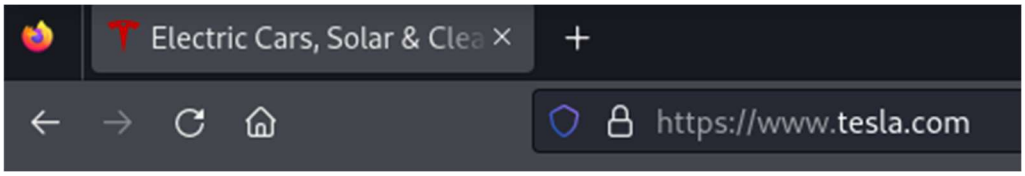
El mail se encontraba incmpleto en nuestra consigna, por lo tanto las letras faltantes eran las que siguen del texto en rojo.

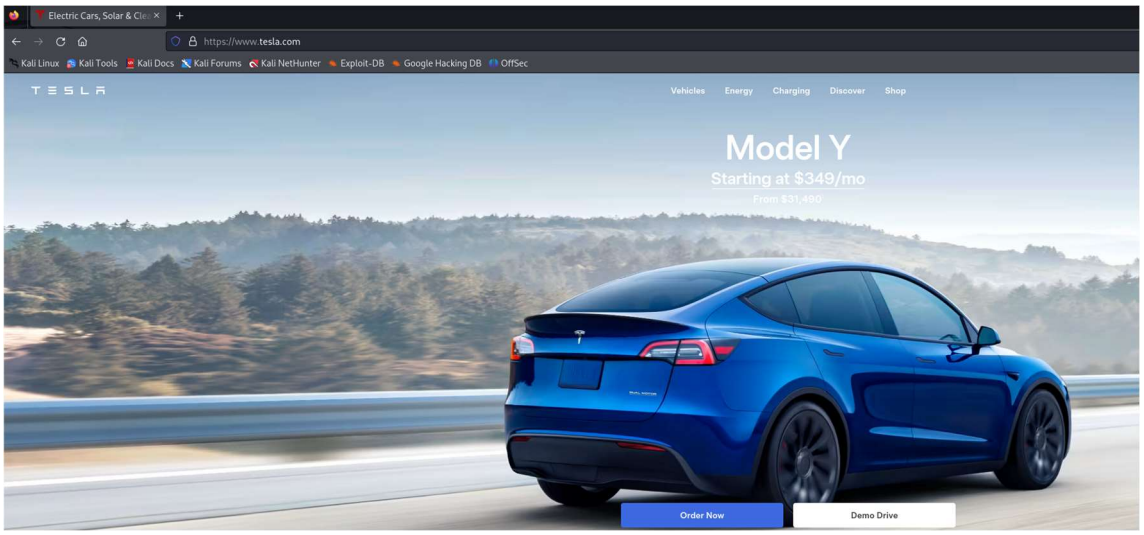
```
hacker-rootkit
```

Obtenemos así hacker-rootkit@live.cn y la contraseña 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 esta actividad ingresamos a su pagina principal para conocer el objetivo.



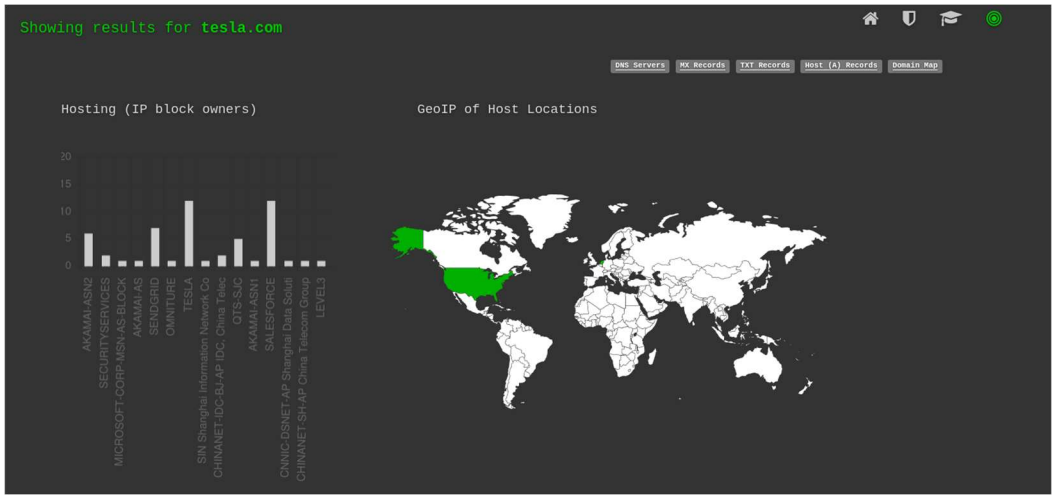


Tesla, Inc. es una empresa estadounidense de automóviles y energía renovable fundada en 2003 por Elon Musk, JB Straubel, Martin Eberhard, Marc Tarpenning y Ian Wright. Es conocida principalmente por sus vehículos eléctricos, que incluyen modelos populares como el Model S, Model 3, Model X y Model Y.

Conocido esto, procedemos a buscar su DNS mediante la página:

Allí colocamos entonces nuestro objetivo:

Los resultados son los siguientes:



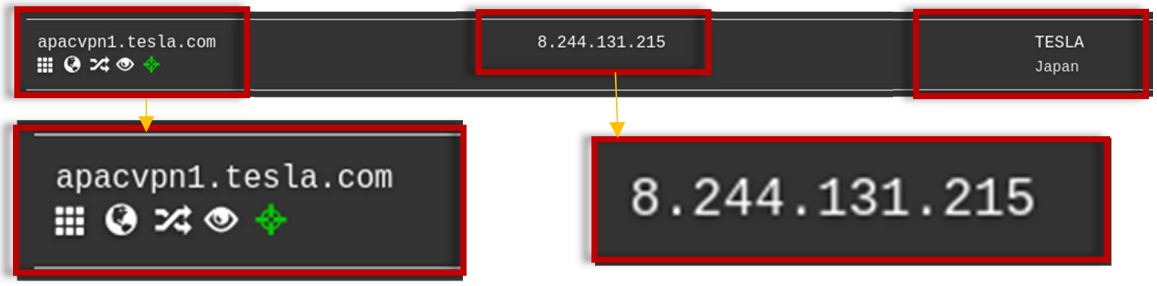
Podemos observar que posee una gran concentración en lo que es el norte de America, esta herramienta. DNSDumpster es una herramienta en línea que permite a los usuarios realizar investigaciones sobre dominios y obtener información relacionada con su configuración de DNS (Sistema de Nombres de Dominio), geolocalización de IPs, mapeo de subdominios, entre otras cosas.

Pasamos a revisar los hosts:

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

tesla.com HTTP: AkamaiGHost	96.16.108.43 a96-16-108-43.deploy.static.akamaitechnologies.com	AKAMAI-AS United Kingdom
o7.ptr6980.tesla.com	149.72.144.42 o7.ptr6980.tesla.com	SENDGRID United States
email1.tesla.com	192.28.144.15 letgo.fivebelow.com	OMNITURE United States
apacvpn1.tesla.com	8.244.131.215	TESLA Japan
cnvpn1.tesla.com	114.141.176.215	SIN Shanghai Information Network Co.,Ltd. China
ptr1.tesla.com	117.50.35.199 ptr1.tesla.com	CHINANET-IDC-BJ-AP IDC, China Telecommunications Corporation China
vpn2.tesla.com	8.47.24.215	TESLA United States

Allí encontramos por ubicación y vemos que encontramos nuestro objetivo en Japón.



Por lo tanto la VPN es apacvpn1.tesla.com y su IP: 8.244.131.215.

1) Conclusión.

El reconocimiento pasivo es una técnica clave en la ciberseguridad que permite recopilar información sobre un objetivo sin interactuar directamente con él. Herramientas como Breachparse son fundamentales en este proceso, ya que ayudan a verificar si las credenciales de un usuario han sido comprometidas en brechas de datos, permitiendo así tomar medidas preventivas para proteger las cuentas.

La importancia de utilizar contraseñas seguras no puede ser subestimada. Estas contraseñas son esenciales para salvaguardar la información personal y prevenir accesos no autorizados. Para crear una contraseña segura, se recomienda seguir ciertos pasos: utilizar al menos 12-16 caracteres, combinar mayúsculas, minúsculas, números y símbolos, evitar información personal fácilmente accesible, considerar frases largas o combinaciones aleatorias, y cambiar las contraseñas periódicamente.

Además, al utilizar herramientas como DNSDumpster, podemos realizar un reconocimiento pasivo eficaz sobre dominios, obteniendo información sobre su configuración DNS, registros de subdominios y otros detalles relevantes de la infraestructura

En conclusión, el reconocimiento pasivo, junto con herramientas como Breachparse y DNSDumpster, es esencial para fortalecer la seguridad cibernética. Implementar contraseñas seguras es una de las mejores prácticas para proteger nuestras cuentas y datos personales en un entorno digital cada vez más amenazante.