



# **Confidential Security**

Recopilación de información

---

Confidencial

---

Nombre del auditor: Kacper Mariusz Koper Mielczarek

Fecha: 27/02/2025

## Índice

<b>Recopilación de información.....</b>	<b>1</b>
<b>Introducción.....</b>	<b>4</b>
<b>Footprinting Vertical.....</b>	<b>4</b>
DNS Brute-force.....	4
Google Analytics.....	6
TLS Probing.....	7
Web scraping.....	7
Certificate transparency log.....	7
Archivos web/cache .....	9
Permutaciones.....	11
Agrupación de todos los subdominios encontrados .....	11
<b>Fingerprinting.....</b>	<b>11</b>
Identificar subdominios online.....	12
Escanear puertos y detectar servicios.....	12
Masscan .....	12
Nmap.....	14
Shodan.....	15
Identificar tecnología web .....	15
Gowitness .....	15
Wappalyzer.....	15
Whatweb.....	16
Identificar posibles WAF .....	16
Wafw00f.....	16
Unwaf.....	16
Descubrimiento de contenido / fuzzing.....	17
<b>Análisis de Vulnerabilidades.....</b>	<b>17</b>
Análisis estandar .....	17
Greenbone.....	17
Nuclei.....	18
Análisis web.....	19
Wpscan.....	19
Análisis SSL/TLS .....	19
Testssl.sh.....	19
Análisis de servidores de correo: DMARC/DKIM/SPF.....	20

Pagina web .....	20
Spoofcheck .....	20
<b>Detección de subdominios takeover .....</b>	<b>21</b>
Subzy .....	21
<b><i>OSINT</i>.....</b>	<b>21</b>
<b>Encontrar correos electrónicos y/o usuarios / información sensible .....</b>	<b>21</b>
Maltego .....	21
Spiderfoot .....	24
Exiftool + Buscadores web .....	24
<b>Búsqueda de personas en redes sociales .....</b>	<b>25</b>
LinkedIn .....	25

## Introducción

El dominio que se ha elegido para realizar la práctica sobre la **búsqueda de información** corresponde a la empresa Kiwi, que es una agencia de viajes en línea fundada en 2012 en la República Checa por Oliver Dlouhý y Jozef Képesi. Esta empresa se especializa en ofrecer a los usuarios la posibilidad de combinar vuelos y otros medios de transporte de diferentes compañías que normalmente no colaboran entre sí, mediante una tecnología conocida como “Virtual Interlining”. Todo esto se encuentra en su página web oficial: <https://www.kiwi.com>.

El análisis se realizará al dominio **\*.kiwi.com** encontrado en la página web: [https://hackerone.com/kiwicom/policy\\_scopes](https://hackerone.com/kiwicom/policy_scopes)

Por lo tanto, este análisis sobre la búsqueda de información se realiza en un entorno seguro y legal, donde la empresa Kiwicom Newco S.L. da su consentimiento a través de la plataforma web mencionada con anterioridad, para ser analizada según las normas que se relatan en la misma web.

## Footprinting Vertical

El primer paso de la investigación es realizar un footprinting vertical, que consiste en recopilar todos los posibles subdominios posibles.

Esto lo realizamos utilizando diversas herramientas:

### DNS Brute-force

Shuffledns es una herramienta para la enumeración de subdominios que combina resolución masiva con wordlists personalizadas y servidores DNS externos para mejorar la precisión y velocidad.

Pudimos conseguir un total de 65 subdominios al realizar dos variantes del comando:

La primera variante nos sonsaco 32 subdominios:

```
shuffledns -mode bruteforce -d kiwi.com -w $HOME/recopilacion/lists/domains.txt -r $HOME/recopilacion/lists/resolvers.txt -silent > subdomains1.txt
```

Al añadir “-t 1000” al comando anterior hemos podido sonsacar 33 dominios:

```
shuffledns -mode bruteforce -d kiwi.com -t 1000 -w $HOME/recopilacion/lists/domains.txt -r $HOME/recopilacion/lists/resolvers.txt -silent > subdomains2.txt
```

Al final hemos juntado las dos listas eliminando los dominios repetidos, quedándonos solamente con 35 subdominios.

Juntar lista:

```
cat subdominios1.txt subdominios2.txt > subdominios_juntos.txt
```

Obtener dominios únicos y limpiamos la lista de cualquier otro texto basura:

```
cat subdominios_juntos.txt | unfurl --unique domains > subdominios_unicos.txt
```

Y, por último, nos quedamos solamente con los subdominios vivos, que son los restantes 35.

```
cat subdominios_unicos.txt | httpx > 1_subdominios_unicos_vivos.txt
```

En resumen, los subdominios más interesantes que hemos encontrado con esta herramienta fueron:

## 1. Infraestructura y Seguridad

**https://pki.kiwi.com:** Posible infraestructura de claves públicas (PKI), puede contener certificados o información sobre autenticación.

**https://status.kiwi.com:** Monitoreo del estado del sistema, útil para detectar posibles vulnerabilidades o caídas.

**http://mail.kiwi.com** y **https://email.kiwi.com:** Servidores de correo, posibles puntos de entrada para ataques de phishing o enumeración de correos.

**https://static.kiwi.com** y **https://assets.kiwi.com:** Podrían alojar recursos estáticos que, si están mal configurados, exponen datos sensibles.

## 2. Desarrollo y Documentación

**https://code.kiwi.com:** Repositorio de código, podría contener credenciales o lógica interna de aplicaciones.

**https://docs.kiwi.com:** Documentación de APIs, puede revelar endpoints interesantes para pruebas de seguridad.

**https://design.kiwi.com:** Posible entorno de diseño, podría filtrar información sobre la interfaz o componentes reutilizables.

### 3. Plataformas Internas

**<https://jira.kiwi.com> y <https://confluence.kiwi.com>:** Herramientas de gestión interna, pueden exponer información sobre proyectos y errores de seguridad.

**https://preprod.kiwi.com:** Entorno de preproducción, usualmente menos seguro y más vulnerable a pruebas de intrusión.

#### 4. Servicios Relacionados con Usuarios

**https://kyc.kiwi.com:** Know Your Customer (KYC), puede manejar datos sensibles de clientes.

**https://partners.kiwi.com:** Portal de socios, podría ofrecer información sobre integraciones con terceros.

**<https://surveys.kiwi.com>:** Encuestas, podría ser un punto de recopilación de información personal.

## Google Analytics

Con esta técnica hemos intentado sonsacar subdominios, pero no hemos obtenido ningún tipo de resultado salvo el dominio principal que se está analizando.

```
analyticsrelationships --url https://www.kiwi.com/ > subdominios.txt
```

Al principio el directorio de los subdominios tuvo caracteres innecesarios, por lo que decidimos limpiarla con el siguiente comando:

```
grep -oP '(?<=\\|_).*' subdominios.txt > 2_subdominios_unicos_vivos.txt
```

```

████████████████████████████████████████████████████████████████████████████████
> Get related domains / subdomains by looking at Google Analytics IDs
> Python version
> By @JosueEncinar

[+] Analyzing url: https://www.kiwi.com/
[+] URL with UA: https://www.googletagmanager.com/gtm.js?id=GTM-KPB9P5
[+] Obtaining information from builtwith and hackertarget

>> UA-22858434
|_ amp.travelpirates.com
|_ amp.wakacyjnipiraci.pl

[+] Done!

(kk@kk)-[~/recopilacion]
$ █

```

## TLS Probing

Esta herramienta TLS lo que realiza es una comprobación si otros subdominios utilizan el mismo certificado TLS. Ahora vamos a utilizar la herramienta “cero” utilizando el siguiente comando para comprobarlo:

```
cero -d in.search.kiwi.com
```

```
cero -d kiwi.com | grep 'kiwi.com' > 3_subdominios_unicos_vivos.txt
```

En este caso solo pudimos encontrar un dominio, kiwi.com que es el dominio principal.

## Web scraping

En este caso utilizaremos la herramienta “katana”, lo que realiza es buscar todos los directorios que se encuentran en “kiwi.com”.

Al realizar el siguiente comando nos ha devuelto primero 1.327 subdominios, pero al intentar ejecutar el comando por segunda vez, solo nos devolvió 2 resultados. En este preciso momento nos dimos cuenta de que el Firewall de kiwi.com nos había bloqueado temporalmente. Después de unos 15 minutos pudimos volver a acceder a la página web oficial de kiwi.com.

```
echo kiwi.com | katana -silent -jc -o subdominios.txt -kf robotstxt,sitemapxml
```

Después filtramos todo el fichero para que solo nos devuelva los subdominios, donde en este caso solo nos devuelve solamente dos resultados, que son los dominios principales:

```
cat subdominios.txt | unfurl --unique domains > 4_subdominios_unicos_vivos.txt
```



## Certificate transparency log

En este método utilizaremos la herramienta “ctfr”, que se encarga de buscar los dominios expuestos en los logs de transparencia de certificados. Para ello utilizaremos el siguiente comando:

```
ctfr -d kiwi.com > subdominios.txt
```

Con esta técnica hemos conseguido 437 subdominios, los cuales tuvimos que limpiar con el comando:

```
sed 's/^\[-\] //' subdominios.txt > subdominios_limpios.txt
```

Despues eliminaremos los subdominios duplicados.

```
cat subdominios_limpios.txt | unfurl --unique domains > subdominios_limpios_unicos.txt
```

Y, por último, filtraremos los dominios vivos.

```
cat subdominios_limpios_unicos.txt | httpx > 5_subdominios_unicos_vivos.txt
```

El resultado final fueron 185 subdominios.

En conclusión, este es el resumen de los subdominios más interesantes encontrados con esta herramienta:

### 1. Infraestructura y Seguridad

**pki.kiwi.com:** Gestión de claves públicas (PKI), posible acceso a certificados.

**status.kiwi.com:** Estado del servicio, útil para conocer infraestructura y downtime.

**ssl-for-saas-proxy.kiwi.com:** Relacionado con proxies y seguridad SSL.

### 2. Desarrollo, APIs y Código

**code.kiwi.com:** Posible repositorio de código fuente.

**docs.kiwi.com:** Documentación de APIs, puede contener endpoints interesantes.

**api.tequila.kiwi.com / tequila-api.kiwi.com:** API de servicios de Kiwi.com, posible fuga de datos.

**graphql-cr.kiwi.com:** API GraphQL, potencialmente expone información estructurada.

**geoip-api-cr.kiwi.com:** API de geolocalización, puede revelar cómo manejan datos de usuarios.

### 3. Entornos de Prueba y Staging

**preprod.kiwi.com:** Entorno de preproducción, generalmente menos seguro.

**staging-tequila-fe.kiwi.com:** Servidor de pruebas, potencialmente mal protegido.



**static-sandbox.kiwi.com:** Puede contener datos de prueba o configuraciones expuestas.

#### 4. Correo y Comunicación

**email.kiwi.com / mail.kiwi.com:** Servidores de correo, interesantes para phishing o enumeración.

**email.txn-mg.kiwi.com:** Sistema de correos transaccionales, podría exponer datos de clientes.

**check-phone.kiwi.com:** Relacionado con validación de teléfonos, posible fuga de datos.

#### 5. Portales Internos y Gestión

**kyc.kiwi.com:** Maneja verificación de identidad, puede contener datos personales sensibles.

**partners.kiwi.com:** Portal de socios, posible acceso a integraciones y credenciales API.

**confluence.kiwi.com:** Documentación interna, puede filtrar información sensible.

**jira.kiwi.com:** Gestión de proyectos, podría exponer vulnerabilidades y errores de software.

### Archivos web/cache

Lo que realiza esta herramienta es escanear las webs y hacer capturas a lo largo del tiempo de dicha web. El objetivo es analizar todas las URLs y extraer sus dominios. Por lo tanto, el objetivo es recorrerse todas las capturas con la siguiente herramienta:

```
gau --threads 5 kiwi.com --o gauoutput.txt
```

Esta herramienta nos ha devuelto 388.565 resultado, de los cuales solamente 64 son subdominios:

```
cat gauoutput.txt | unfurl --unique domains > subdominios_unicos.txt
```

Por último, hemos revisado todos los subdominios que estaban vivos, y nos hemos encontrado de los 64 subdominios 42 subdominios:

```
cat subdominios_unicos.txt | httpx > 6_subdominios_unicos_vivos.txt
```

En conclusión, los subdominios más interesantes encontrados con esta herramienta son:

##### 1. Infraestructura y Seguridad

**logg.kiwi.com / loglady.kiwi.com:** Almacenamiento de logs, posible exposición de datos sensibles.

**static.kiwi.com / static-data.kiwi.com:** Archivos estáticos, podrían contener configuraciones expuestas.

**public-documents.kiwi.com:** Documentos accesibles públicamente, riesgo de filtración de información interna.

## 2. APIs, Código y Desarrollo

**code.kiwi.com:** Repositorio de código, útil para analizar seguridad.

**api.tequila.kiwi.com / tequila-api.kiwi.com:** API de servicios, posible filtración de datos.

**help-graphql.kiwi.com:** API GraphQL, puede ser explotada para extracción de datos.

**tag-manager.kiwi.com:** Scripts de tracking, interesante para fingerprinting.

## 3. Correo y Comunicaciones

**email.txn-mg.kiwi.com / email.txn-ov.kiwi.com:** Servidores de correo, potencial riesgo de phishing o filtraciones.

**email.surveys-mg.kiwi.com:** Correos de encuestas, posible recolección de datos de clientes.

## 4. Portales Internos y Gestión

**partners.kiwi.com:** Portal de socios, podría contener credenciales API.

**jira.kiwi.com:** Gestión de proyectos, posible filtración de vulnerabilidades internas.

**frontend-old-legal-page.fe-cloudrun.kiwi.com:** Página de términos legales antiguos, posible exposición de datos desactualizados.

## 5. Servicios de Viaje y Turismo

**hotels.kiwi.com / rooms.kiwi.com:** Reservas de hoteles, posible exposición de datos de clientes.

**cars.kiwi.com:** Alquiler de autos, podría tener integraciones de pago vulnerables.

**volagratis.kiwi.com / rumbo.kiwi.com:** Relacionado con viajes, potencial fuga de información de reservas.

## Permutaciones

Con esta herramienta lo que vamos a realizar es combinar todas las listas con los subdominios en una sola. Además, va a realizar un ataque de fuerza bruta para asegurarse de que existen esas permutaciones.

Primero juntamos todas las listas:

```
cat 1_subdominios_unicos_vivos.txt 2_subdominios_unicos_vivos.txt  
3_subdominios_unicos_vivos.txt 4_subdominios_unicos_vivos.txt  
5_subdominios_unicos_vivos.txt 6_subdominios_unicos_vivos.txt  
> 7_permutaciones
```

A continuación, ejecutamos el comando para empezar el análisis de las permutaciones con “alterx” y verifica la existencia de los subdominios gracias a la validación de “dnsx”:

```
cat 7_permutaciones.txt | alterx | dnsx -o alterx.txt
```

Nos dio un resultado de 691 subdominios, de los cuales los mas interesantes son:

## Agrupación de todos los subdominios encontrados

Por último, vamos a recopilar todos los subdominios de todas las listas y vamos a ordenarles alfabéticamente y a proceder a eliminar los duplicados; todo esto con el siguiente comando;

```
cat 1_subdominios_unicos_vivos.txt 2_subdominios_unicos_vivos.txt  
3_subdominios_unicos_vivos.txt 4_subdominios_unicos_vivos.txt  
5_subdominios_unicos_vivos.txt 6_subdominios_unicos_vivos.txt alterx.txt | sort -u >  
8_final_subdominios.txt
```

Con este comando hemos acotado la lista a 887 subdominios.

## Fingerprinting

El fingerprinting es el proceso de recopilación de información sobre un sistema objetivo para identificar sus características y posibles vulnerabilidades. Se obtiene datos como el sistema operativo, puertos abiertos y tecnologías utilizadas. La técnica más común es el escaneo de puertos, que permite identificar servicios en ejecución. Otras técnicas incluyen el banner grabbing, el descubrimiento de contenido y la identificación del sistema operativo.

### Identificar subdominios online

Aunque ya hayamos utilizado esta herramienta en algunas listas de subdominios, lo volveremos a realizar a la lista final.

Esta herramienta “httpx” lo que hace es verificar que subdominios de la lista están accesible en la web:

```
cat 8_final_subdominios.txt | httpx -silent > subdominios_vivos.txt
```

Y nos ha devuelto 866 subdominios vivos en la web.

Ahora eliminamos los duplicados y nos ha devuelto solamente 50 subdominios.

```
cat subdominios_vivos.txt | unfurl --unique domains > 9_subdominios_unicos_limpios.txt
```

### Escanear puertos y detectar servicios

#### Masscan

Con la herramienta “masscan” vamos a detectar servicios abiertos en el rango de ip que vayamos a especificar. Esta herramienta al ser tan agresiva es fácil de detectar.

Primero tenemos que convertir toda la lista de subdominios en IPs, ya que masscan solo funciona con direcciones IP.

```
for subdominio in $(cat 9_subdominios_vivos.txt); do dig +short $subdominio | grep -Eo '([0-9]{1,3}\.){3}[0-9]{1,3}'; done > subdominios_ips.txt
```

Al ya tener convertidos todos los dominios a sus correspondientes IPs, debemos ahora limpiar la lista para que solo se queden las IPs, quitando todo tipo de datos que no correspondan.

```
grep -Eo '([0-9]{1,3}\.){3}[0-9]{1,3}' subdominios_ips.txt | awk -F'.' '{ $1<=255 && $2<=255 && $3<=255 && $4<=255 }' > ips_limpias.txt
```

Ahora podremos ejecutar la herramienta de masscan.

```
sudo masscan -iL ips_limpias.txt \ -p1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-  
85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,163,179,199,211-  
212,222,254-256,259,264,280,301,306,311,340,366,389,406-407,416-417,425,427,443-  
445,458,464-465,481,497,500,512-515,524,541,543-545,548,554-555,563,587,593,616-  
617,625,631,636,646,648,666-  
668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-  
801,808,843,873,880,888,898,900-903,911-912,981,987,990,992-993,995,999-  
1002,1007,1009-1011,1021-1100,1102,1104-1108,1110-1114,1117,1119,1121-  
1124,1126,1130-1132,1137-1138,1141,1145,1147-1149,1151-1152,1154,1163-  
1166,1169,1174-1175,1183,1185-1187,1192,1198-1199,1201,1213,1216-1218,1233-  
1234,1236,1244,1247-1248,1259,1271-1272,1277,1287,1296,1300-1301,1309-  
1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,1461,1494,1500-  
1501,1503,1521,1524,1533,1556,1580,1583,1594,1600,1641,1658,1666,1687-  
1688,1700,1717-1721,1723,1755,1761,1782-1783,1801,1805,1812,1839-1840,1862-  
1864,1875,1900,1914,1935,1947,1971-1972,1974,1984,1998-2010,2013,2020-  
2022,2030,2033-2035,2038,2040-2043,2045-2049,2065,2068,2099-2100,2103,2105-  
2107,2111,2119,2121,2126,2135,2144,2160-2161,2170,2179,2190-  
2191,2196,2200,2222,2251,2260,2288,2301,2323,2366,2381-2383,2393-  
2394,2399,2401,2492,2500,2522,2525,2557,2601-2602,2604-2605,2607-2608,2638,2701-  
2702,2710,2717-2718,2725,2800,2809,2811,2869,2875,2909-2910,2920,2967-  
2968,2998,3000-3001,3003,3005-3007,3011,3013,3017,3030-  
3031,3052,3071,3077,3128,3168,3211,3221,3260-3261,3268-3269,3283,3300-  
3301,3306,3322-3325,3333,3351,3367,3369-3372,3389-  
3390,3404,3476,3493,3517,3527,3546,3551,3580,3659,3689-  
3690,3703,3737,3766,3784,3800-3801,3809,3814,3826-  
3828,3851,3869,3871,3878,3880,3889,3905,3914,3918,3920,3945,3971,3986,3995,3998,4  
000-4006,4045,4111,4125-4126,4129,4224,4242,4279,4321,4343,4443-  
4446,4449,4550,4567,4662,4848,4899-4900,4998,5000-5004,5009,5030,5033,5050-  
5051,5054,5060-5061,5080,5087,5100-5102,5120,5190,5200,5214,5221-5222,5225-  
5226,5269,5280,5298,5357,5405,5414,5431-  
5432,5440,5500,5510,5544,5550,5555,5560,5566,5631,5633,5666,5678-  
5679,5718,5730,5800-5802,5810-5811,5815,5822,5825,5850,5859,5862,5877,5900-  
5904,5906-5907,5910-5911,5915,5922,5925,5950,5952,5959-5963,5987-5989,5998-  
6007,6009,6025,6059,6100-  
6101,6106,6112,6123,6129,6156,6346,6389,6502,6510,6543,6547,6565-  
6567,6580,6646,6666-6669,6689,6692,6699,6779,6788-  
6789,6792,6839,6881,6901,6969,7000-  
7002,7004,7007,7019,7025,7070,7100,7103,7106,7200-  
7201,7402,7435,7443,7496,7512,7625,7627,7676,7741,7777-7778,7800,7911,7920-  
7921,7937-7938,7999-8002,8007-8011,8021-8022,8031,8042,8045,8080-  
8090,8093,8099-8100,8180-8181,8192-8194,8200,8222,8254,8290-  
8292,8300,8333,8383,8400,8402,8443,8500,8600,8649,8651-  
8652,8654,8701,8800,8873,8888,8899,8994,9000-9003,9009-9011,9040,9050,9071,9080-
```

```
9081,9090-9091,9099-9103,9110-9111,9200,9207,9220,9290,9415,9418,9485,9500,9502-  
9503,9535,9575,9593-9595,9618,9666,9876-9878,9898,9900,9917,9929,9943-  
9944,9968,9998-10004 \ --banner -oG  
/home/kk/recopilacion/10_subdominios_servicios_masscan.txt > /dev/null 2>&1
```

Nos ha encontrado 124 puertos abiertos dentro del rango de todas las IPs; en resumen los puertos abiertos son:

**80 (HTTP)** - Página web no cifrada, permite obtener banners, tecnología del servidor, etc.

**443 (HTTPS)** - Página web cifrada, pero sigue siendo posible obtener certificados SSL, nombres de dominio, etc.

**8080 (HTTP-ALT)** - Puede ser un proxy, panel de administración o aplicación web en otro puerto.

**8443 (Alternativo HTTPS o VPNs)** - A veces usado para interfaces de administración.

## Nmap

Ahora vamos a utilizar la herramienta de nmap para ver si podemos conseguir más información sobre nuestro objetivo. Debemos atacar los certificados TLS 1 y 2 con fuerza bruta.

```
sudo nmap -sUV -Pn -p161 -open -iL 9_subdominios_unicos_limpios.txt >  
10_nmap_pv123.txt
```

Hemos conseguido bastantes resultados de IPs con SNMP pero no se ha especificado ninguna versión en concreto, ya que ese rango venía vacío. Por lo tanto, extraeremos todas las IPs de la lista.

```
grep -oP 'Nmap scan report for \K[\d.]+' 10_nmap_pv123.txt | sort -u > ips_sub_nmap.txt
```

Nos tendremos que descargar una lista de posibles contraseñas de SNMP:

```
wget  
https://raw.githubusercontent.com/danielmiessler/SecLists/master/Discovery/SNMP/co  
mmon-snmp-community-strings.txt
```

Ahora podemos realizar un ataque de fuerza bruta a la lista de IPs que hemos identificado anteriormente. Con este comando nos mostrará las posibles credenciales para acceder a la enumeración.

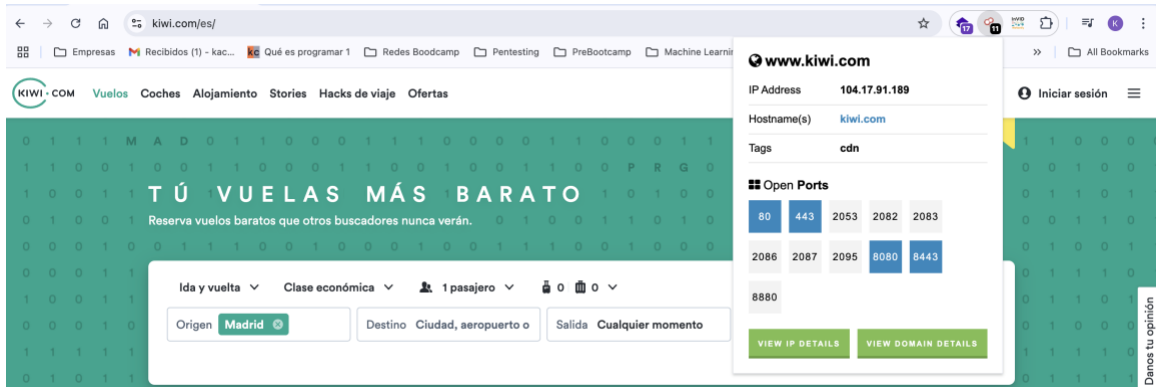
```
sudo nmap -sU -p 161 -vv --script=snmp-brute --script-args snmp-  
brute.communitiesdb=common-snmp-community-strings.txt -iL ips_sub_nmap.txt >  
credenciales.txt
```

No se ha detectado ninguna credencial, por lo que no podremos acceder e utilizar el siguiente comando:

```
snmpwalk -v <version> -c <string> <TARGET>
```

### Shodan

Con esta extensión de Google podremos averiguar los puertos abiertos que tiene la página web del cliente. En este caso tiene abiertos los puertos 80, 443, 8080 y 8443.



### Identificar tecnología web

#### Gowitness

Lo que hace esta herramienta es visitar todas las páginas web a lo largo del tiempo y hacerlas captura de pantalla:

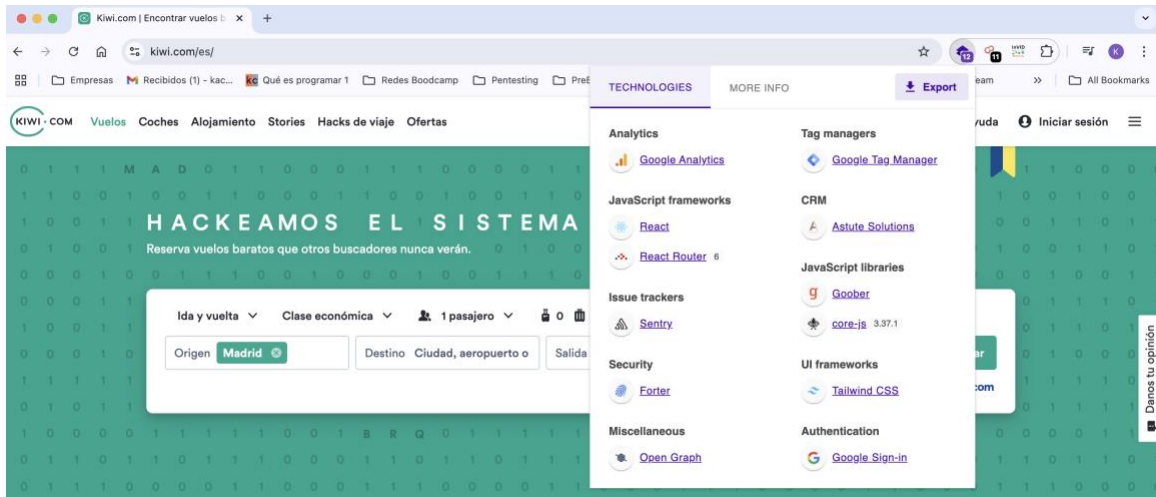
```
gowitness scan file -f 9_subdominios_unicos_limpios.txt > 11_gowitness_capturas.txt
```

Ahora accedemos a la página web <http://localhost:7171> para poder ver el resumen de toda la recopilación.

Pero al intentar acceder a la web nos da error y no siquiera nos deja ver nada. Encambio, hemos creado una carpeta "screenshots" y hemos almacenado todas las capturas que realizo gowitness.

#### Wappalyzer

Con esta extensión de Chrome podemos averiguar las direfentes herramientas que utiliza la página web del cliente. Por ejemplo, podemos ver que utiliza Google Sign-in para almacenar contraseñas.



### Whatweb

Esta herramienta complementa a wappalyzer.

```
whatweb kiwi.com > 11_whatweb.txt
```

Con esta herramienta hemos podido averiguar que detrás del servidor HTTPServer esta cloudflare.

### Identificar posibles WAF

#### Wafw00f

Esta herramienta identifica todos los WAFs.

```
wafw00f -i 9_subdominios_unicos_limpios.txt > 12_wafw00f.txt
```

Ha detectado CloudFlare en diferentes subdominios.

#### Unwaf

Esta herramienta en cambio intenta saltarse los WAFs.

Primero instalamos la aplicación:

```
go install github.com/mmarting/unwaf@latest
```

Le otorgamos acceso directo:

```
sudo ln -s $HOME/go/bin/unwaf /usr/bin/unwaf
```



Y, por último, la ejecutamos:

```
unwaf -d kiwi.com > 12_unwaf.txt
```

No ha encontrado ninguna manera de saltarse el WAF.

## Descubrimiento de contenido / fuzzing

Esta herramienta realiza ataques de fuerza bruta para descubrir rutas, archivos y parámetros en un servidor web.

Primero descargamos la lista para el ataque de fuerza bruta.

```
wget  
https://raw.githubusercontent.com/danielmiessler/SecLists/refs/heads/master/Discovery/Web-Content/common.txt
```

Y ahora ejecutamos el comando:

El 200 es si nos responde con un positivo; 401 y 403 el fichero existe, pero el servidor nos está bloqueando.

```
ffuf -w ~/recopilacion/lists/common.txt -t 10 -mc 200,401,403 -u https://kiwi.com/FUZZ >  
13_ffuf.txt
```

Nos ha devuelto 4.744 resultados.

## Análisis de Vulnerabilidades

### Análisis estándar

Permite identificar vulnerabilidades en sistemas mediante escáneres de seguridad de infraestructura y aplicaciones.

### Greenbone

Es una plataforma similar a Nexus que realiza un análisis de vulnerabilidades que utiliza OpenVAS para escanear sistemas en busca de fallos de seguridad. Permite detectar configuraciones débiles, servicios desactualizados y posibles vectores de ataque en una red.

Se ha realizado un escaneo de vulnerabilidades a la ip principal de kiwi.com que es 104.17.91.189

## Confidential Security

Hemos detectado una vulnerabilidad leve:

The screenshot shows the Greenbone Enterprise Appliance interface. The top navigation bar includes links for Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. The main content area displays a report titled "Report: TCP Timestamps Information Disclosure" with a severity of 2.6 (Low). The report details include the host IP 104.17.91.189, the location general/tcp, and the creation date Wed, Feb 26, 2025 11:35 AM UTC. The interface also shows various tabs for Information, Results, Hosts, Ports, Applications, Operating Systems, CVEs, Closed CVEs, TLS Certificates, Error Messages, and User Tags.

Y, además se ha detectado un fallo TLS 1.2

The screenshot shows the Greenbone Enterprise Appliance interface displaying details for a vulnerability titled "Internet Engineering Task Force (IETF) Transport Layer Security (TLS) 1.2". The vulnerability is identified by NVD ID 90debbcc-2389-4663-9b15-12218781d623 and has a severity of 0.1 (High). The interface also shows a section for "Reported Vulnerabilities" with a table listing the vulnerability name and severity.

Name	Severity
CVE-2015-8960	0.1 (High)

### Nuclei

Realiza todo tipo de escaneo, aunque esta más orientado a escaneo web. Vamos a utilizar esta herramienta para realizar un escaneo de vulnerabilidades.

```
Nuclei -u kiwi.com > 14_nuclei.txt
```

No nos ha detectado ningún tipo de vulnerabilidad excepto distintos "info".

## Análisis web

### Wpscan

Esta herramienta lo que realiza es escanear sitios web basados en WordPress para identificar vulnerabilidades, temas y plugins instalados.

```
wpscan -random-user-agent -url https://kiwi.com/ > 15_wpscan.txt
```

Lo que ha devuelto que no tiene WordPress. Lo hemos comprobado entrando al navegador y filtrando si kiwi.com tiene WordPress, y lo que nos ha salido son solo los documentos PDF. Al realizar un filtro sin PDF no nos devolvía ningún resultado.

```
site:kiwi.com inurl:wp-content -filetype:pdf
```

## Análisis SSL/TLS

### Testssl.sh

Este script permite evaluar configuraciones de SSL/TLS mediante herramientas o servicios web, buscando de este modo versiones obsoletas.

Instalamos el script:

```
git clone --depth 1 https://github.com/testssl/testssl.sh.git
```

Ejecutamos la herramienta:

```
./testssl.sh kiwi.com > 16_testssl_sh.txt
```

Hemos detectado una posible vulnerabilidad, donde LUCKY13 sigue utilizando cifrado CBC debe por ejemplo AES.

## Análisis de servidores de correo: DMARC/DKIM/SPF

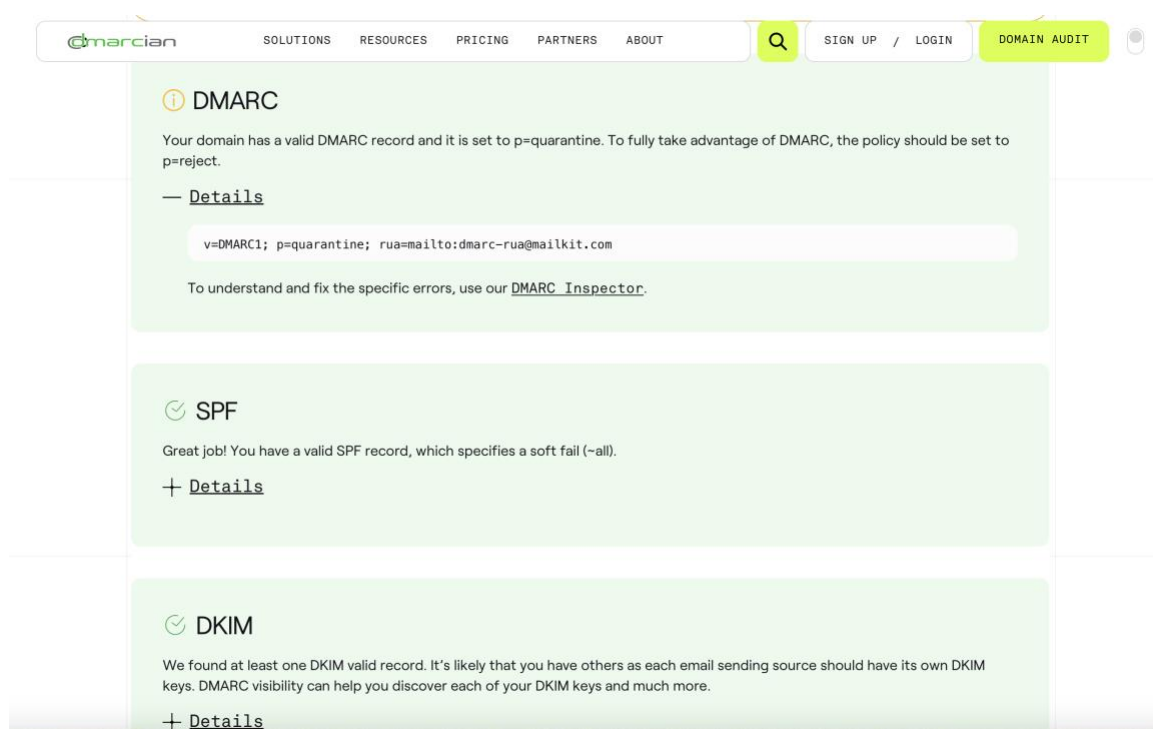
Lo que realizan estas herramientas es comprobar que protocolos sigue una empresa al recibir un correo electrónico, por si se les puede hacer phishing.

En este caso kiwi.com cuando recibe un correo que no pasa los controles los manda a cuarentena (DMARC). Pero sí que tiene unos correos definidos desde los que puede recibir correos (SPF) y también tiene aplicado una firma de verificación de mensajes de que no hayan sido modificados por el camino (DKIM).

### Página web

Todo esto se analizó a través de:

<https://dmarcian.com>



### Spoofcheck

Realiza lo mismo que la página web pero desde la terminal de Kali.

Primero debemos instalar la herramienta:

```
git clone https://github.com/a6avind/spoofcheck.git
```

Instalamos dependencias:

```
pip install -r requirements.txt --break-system-packages
```

Ejecutamos la herramienta:

```
python spoofcheck.py kiwi.com > 17_spoofcheck.txt
```

Solo ha detectado el DMARK y SPF dejándose de lado DKIM. Por lo demás, el resultado es el mismo que el de la página web. Además, concluye que no es posible hacer spoofing en el.

## Detección de subdominios takeover

### Subzy

Esta herramienta detecta dominios huérfanos susceptibles a un subdomain takeover. Lo que significa que si a un dominio se le acaba la licencia y la empresa no se da cuenta, y un atacante paga la licencia de ese dominio tendrá acceso en vista a derechos a todos los subdominios asociados a ese dominio.

Primero la instalamos:

```
go install -v github.com/PentestPad/subzy@latest
```

Acceso directo:

```
sudo ln -s $HOME/go/bin/subzy /usr/bin/subzy
```

Ejecución de la herramienta:

```
subzy run --targets 9_subdominios_unicos_limpios.txt > 18_subzy.txt
```

Al parecer ha encontrado 2.470 líneas de resultados, de los cuales 590 subdominios con posibles vulnerabilidades a subdomain takeover.

## OSINT

### Encontrar correos electrónicos y/o usuarios / información sensible

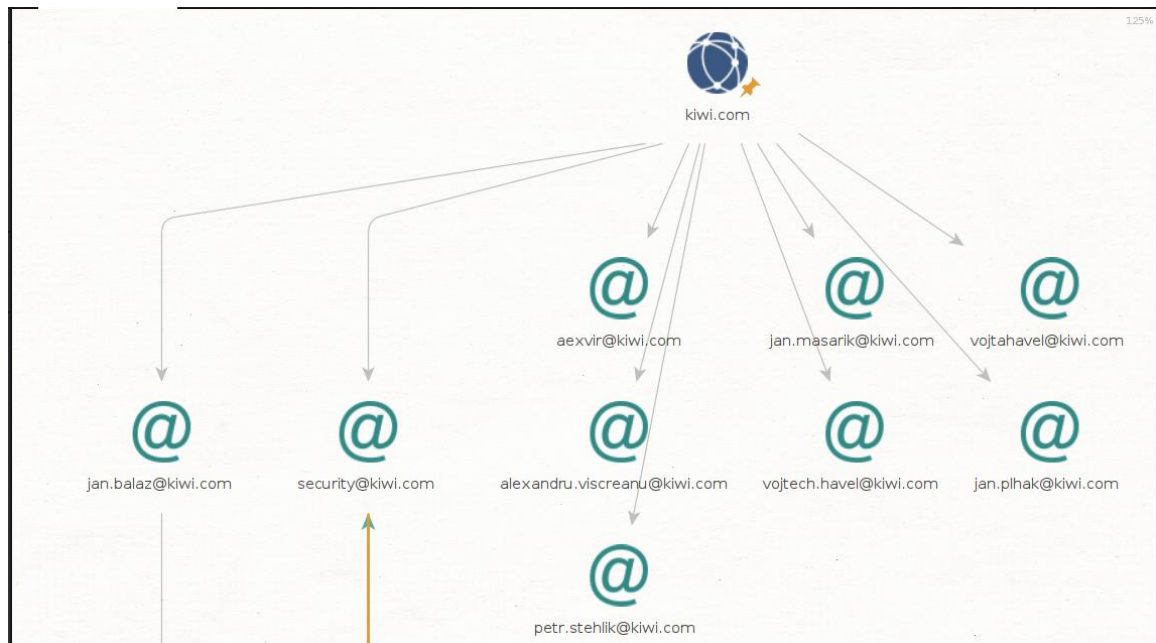
#### Maltego

El objetivo de esta herramienta es recopilar información de diferentes usuarios, empleados, empresas. Lo realiza mediante diferentes técnicas de búsqueda, ya sea por dominio, correo, etc.

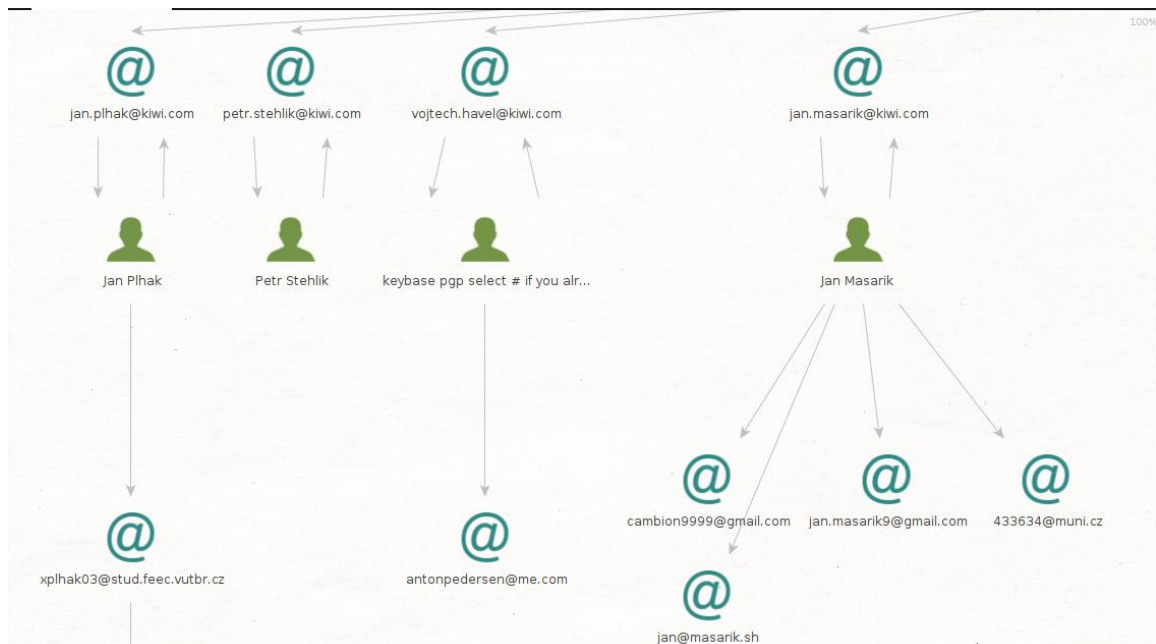
Nosotros hemos utilizado esta herramienta principalmente para recopilar el nombre de los trabajadores de kiwi y sus correos electrónicos, para poder realizarles un ataque de phishing. Además de ver si sus contraseñas de sus correos han sido filtradas.

## Confidential Security

### 1. Muestra todos los correos encontrados asociados a kiwi.com

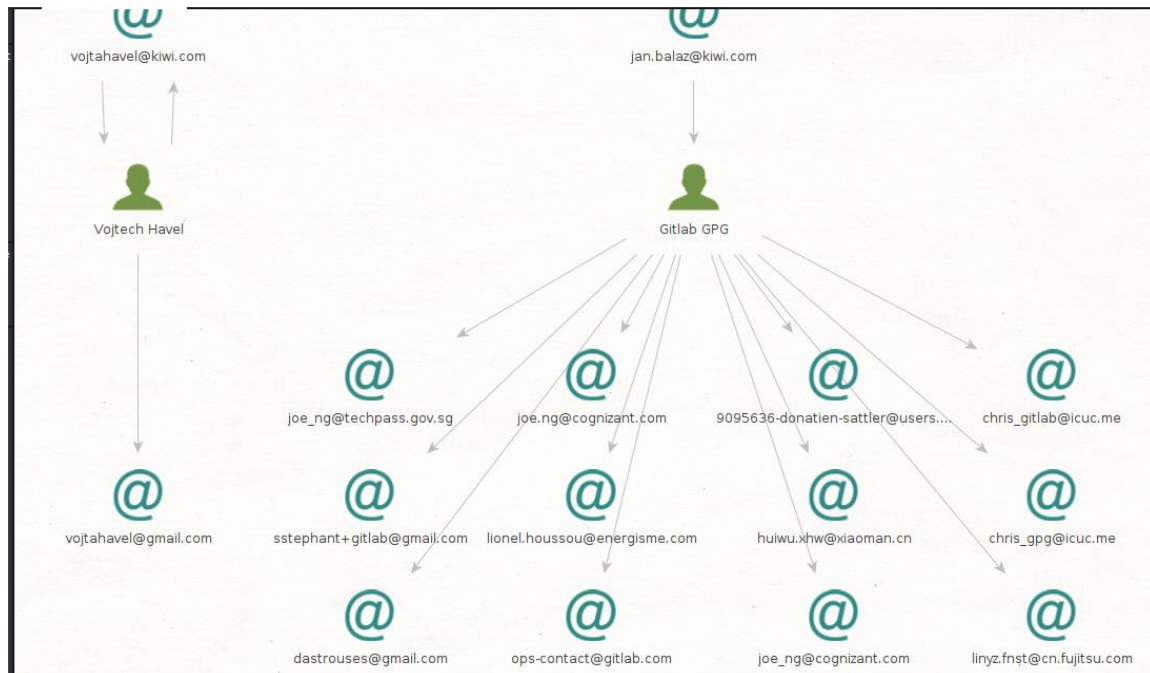


### 2. Muestra los trabajadores y sus correos personales asociados a dichas cuentas de correo del punto 1.

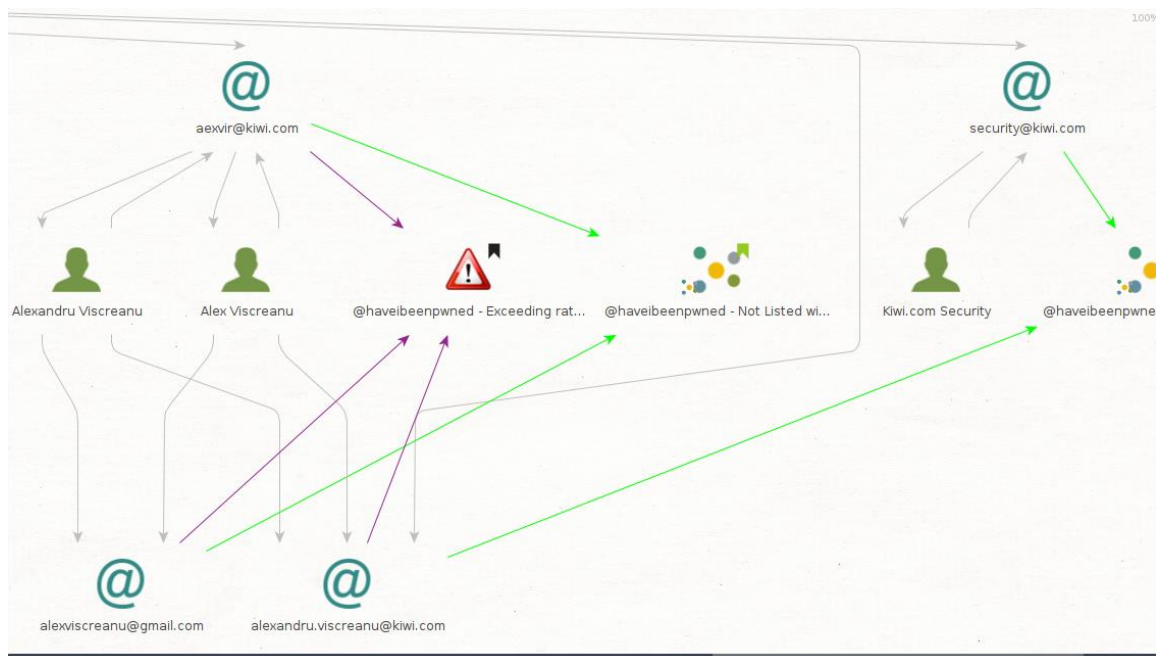


## Confidential Security

3. Muestra los trabajadores y sus correos personales asociados a dichas cuentas de correo del punto 1.



4. Muestra los trabajadores y sus correos personales asociados a dichas cuentas de correo del punto 1. Además, muestra en que plataformas posiblemente se filtraron las contraseñas de dichos correos.

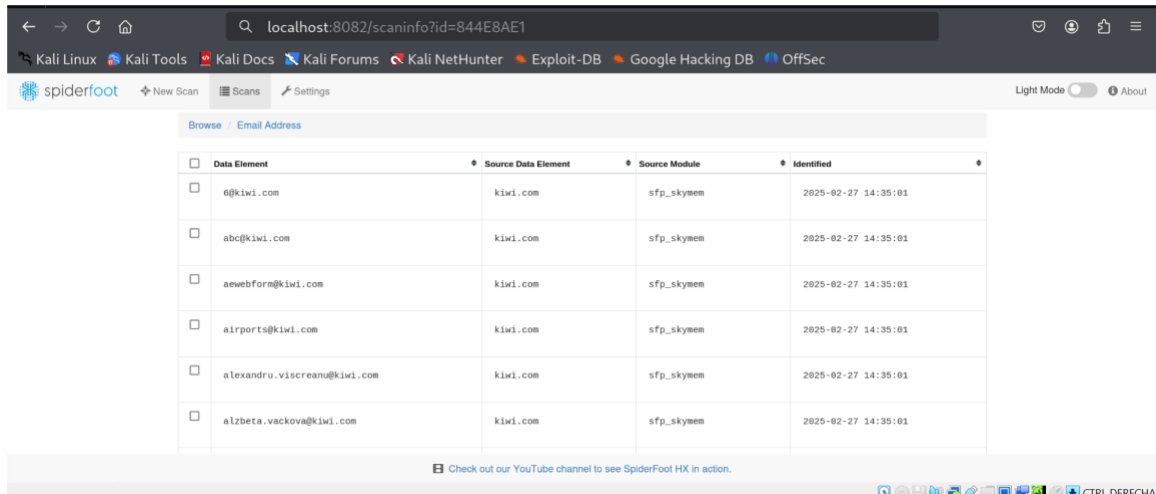




### Spiderfoot

Esta herramienta es parecida a la de Greenbone, pero lo que nos va a interesar buscar son los correos electrónicos asociados a kiwi.com.

Hemos encontrado 40 posibles correos electrónicos, que se almacenaron en el archivo spiderfoot.



The screenshot shows the Spiderfoot web interface in a browser. The address bar displays 'localhost:8082/scaninfo?id=844E8AE1'. The interface includes a navigation bar with links to 'Kali Linux', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', and 'OffSec'. Below this is a 'spiderfoot' logo and buttons for 'New Scan', 'Scans', and 'Settings'. A 'Light Mode' toggle and an 'About' link are also present. The main content area is titled 'Browse Email Address' and contains a table with the following data:

<input type="checkbox"/>	Data Element	Source Data Element	Source Module	Identified
<input type="checkbox"/>	@kiwi.com	kiwi.com	sfp_skymem	2025-02-27 14:35:01
<input type="checkbox"/>	abc@kiwi.com	kiwi.com	sfp_skymem	2025-02-27 14:35:01
<input type="checkbox"/>	aewebform@kiwi.com	kiwi.com	sfp_skymem	2025-02-27 14:35:01
<input type="checkbox"/>	airports@kiwi.com	kiwi.com	sfp_skymem	2025-02-27 14:35:01
<input type="checkbox"/>	alexandru.viscreanu@kiwi.com	kiwi.com	sfp_skymem	2025-02-27 14:35:01
<input type="checkbox"/>	alzbeta.vackova@kiwi.com	kiwi.com	sfp_skymem	2025-02-27 14:35:01

At the bottom of the table, there is a link: 'Check out our YouTube channel to see SpiderFoot HX in action.'

### Exiftool + Buscadores web

La herramienta exiftool lo que realiza es la búsqueda de metadatos de imágenes u otros archivos como PDF, Word, etc.

Hemos intentado averiguar la dirección de su residencia a través de alguna foto que se localizaba en Google y usando exiftool, pero los metadatos no contenían su localización.

*Foto CEO Oliver Dlouhy en su posible residencia (Nombre CEO averiguado por LinkedIn)*





También lo hemos intentado sonsacar mediante la página web “chrome-extension://mhccpoafgdgbhnjfhkcmgknnndkeenfhe/popup.html#/app/tools/metadata\_image” que tiene una herramienta para sonsacar los metadatos de las fotografías entre otros.

#### *Metadatos exiftool:*

```
(kk) [~/Desktop]
$ exiftool 3.webp
ExifTool Version Number      : 13.00
File Name                    : 3.webp
Directory                   : .
File Size                    : 31 kB
File Modification Date/Time   : 2025:02:27 15:52:11+01:00
File Access Date/Time        : 2025:02:27 15:52:11+01:00
File Inode Change Date/Time   : 2025:02:27 15:52:11+01:00
File Permissions              : -rw-rw-r--
File Type                    : WEBP
File Type Extension          : webp
MIME Type                    : image/webp
VP8 Version                  : 0 (bicubic reconstruction, normal loop)
Image Width                  : 700
Horizontal Scale              : 0
Image Height                 : 525
Vertical Scale               : 0
Image Size                   : 700x525
Megapixels                   : 0.367
```

## Búsqueda de personas en redes sociales

### LinkedIn

Hemos averiguado quien es el CEO de kiwi.com (<https://www.linkedin.com/in/oliverdlouhy/>). Lo hemos conseguido mediante la página principal de LinkedIn, con la búsqueda kiwi.com, en el apartado de personas (<https://www.linkedin.com/company/kiwi.com/people/>).

Además, en la página principal de LinkedIn de kiwi aparecen todo tipo de trabajadores que podríamos investigar para realizarles un ataque de phishing.



## **Confidential Security**

Última Página