

Informe Recopilación de Información

CONFIDENCIAL.

Andrés Jesús Ricaurte Valera
KEEPCODING | RECOPILACIÓN DE INFORMACIÓN

Fecha: 09/03/2025

Informe entregado para:
KeepCoding

ÍNDICE.

1. OBJETIVO.....	2
2. ALCANCE.....	2
3. FOOTPRITING.....	3
3.1. WHOIS.....	3
3.2. SHUFLLEDNS.....	3
3.3. GOOGLE ANALYTICS.....	4
3.4. CERO.....	4
3.5. WEB SCRAPING KATANA.....	5
3.6. CTFR.....	5
3.7. GAU.....	6
3.8. PERMUTACIONES.....	6
4. FINGERPRITING.....	7
4.1. HTTPX.....	7
4.2. NMAP/MASSCAN.....	7
4.3. GOWITNESS/WAPPALYZER/WHATWEB.....	9
4.4. IDENTIFICACIÓN WAF/ WAFW00F.....	12
4.5. FUZZING.....	13
5. ANÁLISIS DE VULNERABILIDADES.....	15
5.1. GREENBONE.....	15
5.2. NUCLEI.....	15
5.3. WPSSCAN.....	16
5.4. ANÁLISIS SSL/TLS.....	17
5.5. DMARC/DKIM/SPF.....	18
5.6. SUBZY.....	19
6. OSINT.....	20
6.1. ANALISIS DE REDES SOCIALES.....	23

CONFIDENCIALIDAD.

Este documento es de exclusiva propiedad de mi persona Andres Jesus Ricaurte Valera y de KeepCoding. Este documento contiene información propietaria y confidencial.

DESCARGO DE RESPONSABILIDAD.

Una prueba de penetración se considera una toma instantánea en el tiempo. Los hallazgos y recomendaciones reflejan la información recopilada durante la evaluación y no cualquier cambio o modificación realizada fuera de ese período.

Los compromisos de tiempo limitado no permiten una evaluación completa de todos los controles de seguridad. Yo, Andres Ricaurte prioricé la evaluación para identificar los controles de seguridad más débiles que un atacante podría explotar. Recomiendo realizar evaluaciones similares anualmente, ya sea por evaluadores externos o internos, para garantizar el éxito continuo de los controles.

CONTACTO.

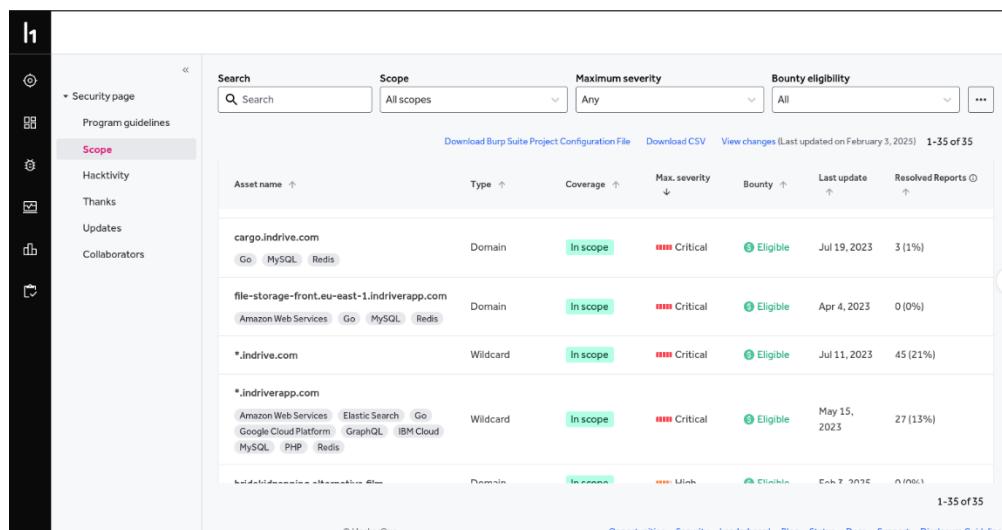
Nombre	Cargo	Contacto
Martín Andres Jesus Ricaurte Valera	Profesor Alumno	Martin@correo.com Andresricv@outlook.es

1. OBJETIVO.

En esta práctica se tiene como objetivo llevar a cabo un trabajo de recopilación de información del dominio de una empresa en específico. Tratar de recopilar el máximo de información que pueda ser vulnerable utilizando las técnicas y herramientas vistas durante el módulo.

2. ALCANCE

El alcance de esta práctica de recopilación se hará en torno al dominio de la empresa InDrive, cuyo dominio a evaluar será *.indrive.com.



The screenshot shows the HackerOne interface for configuring a bug bounty program. The 'Scope' section is selected, displaying a list of assets under evaluation:

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
cargo.indrive.com	Domain	In scope	Critical	Eligible	Jul 19, 2023	3 (1%)
file-storage-front.eu-east-1.indriverapp.com	Domain	In scope	Critical	Eligible	Apr 4, 2023	0 (0%)
*.indrive.com	Wildcard	In scope	Critical	Eligible	Jul 11, 2023	45 (21%)
*.indriverapp.com	Wildcard	In scope	Critical	Eligible	May 15, 2023	27 (13%)

At the bottom of the page, there are links to Opportunities, Security, Leaderboard, Blog, Status, Docs, Support, and Disclosure Guidelines.

3. FOOTPRITING.

3.1. WHOIS.

```
(kali㉿kali)-[~/indrive/recopilacion]
$ whois indrive.com
Domain Name: INDRIVE.COM
Registry Domain ID: 5342839_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: http://cscdbs.com
Updated Date: 2023-12-04T14:54:15Z
Creation Date: 1998-04-08T04:00:00Z
Registry Expiry Date: 2025-04-07T04:00:00Z
Scan Team
Registrar: CSC Corporate Domains, Inc.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: 8887802723
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS-1301.AWSDNS-34.ORG
Name Server: NS-1831.AWSDNS-36.CO.UK
Name Server: NS-389.AWSDNS-48.COM
Name Server: NS-694.AWSDNS-22.NET
Scanning...
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```

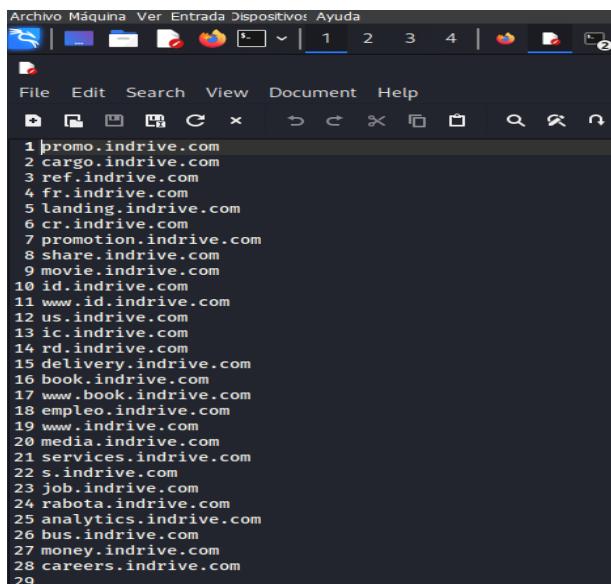
Con el comando “whois” buscamos información que nos pueda interesar respecto a dominios e información técnica relacionada con la organización.

3.2. SHUFLLEDNS.

Utilizaremos esta herramienta de fuerza bruta para obtener subdominios de nuestro objetivo. Antes de ejecutar esta herramienta, es necesario generar un listado de DNS servers. Este archivo llamado “resolvers.txt” está evidenciado en los repositorios de GitHub.

El comando a ejecutar para llevar a cabo la búsqueda de subdominios mediante shuffledns es el siguiente:

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



Como resultado de este comando evidenciamos en la captura de pantalla la obtención de 28 subdominios.

Subdominios como **promo**, **landing**, **analytics**, **delivery**, y **money** son los más interesantes si te interesa la seguridad, ya que suelen estar vinculados a funciones que manejan datos sensibles o tienen un alto tráfico de usuarios. Además, **subdominios de trabajo** como **job**, **careers**, y **empleo** también son clave para proteger datos personales de los usuarios.

3.3. GOOGLE ANALYTICS.

Con esta herramienta buscaremos información en Google analytics respecto a nuestro dominio. El comando para utilizar en este caso es el siguiente:

[analyticsrelationships --url https://indrive.com/](https://indrive.com/)

```
(kali㉿kali)-[~/indrive/recopilacion]
$ analyticsrelationships --url https://indrive.com/
[UA-152845245] dates
[UA-152845245] subdomains
[UA-152845245] cargo.indrive.com
[UA-152845245] Go MySQL Redis
[UA-152845245] file-storage-front.eu-east-1.indriverapp.com
[UA-152845245] Amazon Web Services Go MySQL
[UA-152845245] *.indriverapp.com
[UA-152845245] Amazon Web Services Elastic Search
[+] Analyzing url: https://indrive.com/ Amazon Web Services Elastic Search
[+] URL with UA: https://www.googletagmanager.com/gtm.js?id=GTM-WF37D8H IB
[+] Obtaining information from builtwith and hackertarget Redis
> Get related domains / subdomains by looking at Google Analytics IDs
> Python version
> By @JosueEncinar
[*].indriverapp.com
>> UA-152845245
|__ error getting results
[+] Done!
```

Como podemos ver en la captura de pantalla, no obtenemos ninguna información acerca de nuestro objetivo.

3.4. CFRO.

Esta herramienta la utilizaremos para obtener información respecto a los certificados TLS/SSL. El comando para utilizar es el siguiente:

```
cero -d indrive.com | grep 'indrive.com' > cero.txt
```

```
1 |indrive.com  
2
```

Como resultado nos encuentra nuestro dominio de origen, por lo que no podemos rescatar nada importante del uso de esta herramienta.

3.5. WEB SCRAPING|KATANA.

Para intentar recopilar información de la web de nuestro dominio principal utilizaremos Katana y el comando para utilizar es el siguiente:

```
echo indrive.com | katana -jc -o katanaoutput.txt -kf robotstxt,sitemapxml cat katanaoutput.txt | unfurl --unique domains > katana.txt
```

Como podemos ver reflejado, tras filtrar con el comando unfurl, no nos devuelve nada relevante, ya que nos refleja nuestro dominio principal.

3.6. CTFR.

Utilizaremos la herramienta ctfr para consultar los logs de nuestro entorno web. Usaremos el siguiente comando:

ctfr -d indrive.com > ctfr.txt

Obtuvimos los siguientes subdominios:

```
[ -] www.lp-services.indrive.com
[ -] www.sparklab.indrive.com
[ -] www.supernovas.indrive.com
[ -] www.updrive.indrive.com
[ -] www.yourpace.indrive.com
[ -] yourpace.indrive.com

[!] Done. Have a nice day! ;).

└─[(kali㉿kali)-[~/indrive/recopilacion]]
$ cat ctfr.txt | wc
    132      266     3312

└─[(kali㉿kali)-[~/indrive/recopilacion]]
$ █
```

De todos estos subdominios, tenemos algunos que son relevantes en cuanto a la seguridad de la empresa:

Subdominios de desarrollo y pruebas (Frecuentemente mal protegidos)

```
*.dev.delivery.indrive.com  
*.qa.delivery.indrive.com  
*.sandbox.delivery.indrive.com  
*.internal.dev.delivery.indrive.com  
*.internal.qa.delivery.indrive.com  
*.internal.sandbox.delivery.indrive.com  
*.internal.delivery.indrive.com
```

3.7. GAU.

Utilizaremos esta herramienta para determinar el cache de nuestro sitio web. El comando para llevar a cabo esta herramienta es el siguiente:

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

Tras ejecutar esta herramienta, no nos devuelve ninguna información relevante.

```
(kali㉿kali)-[~/indrive/recopilacion]  
└─$ cat gauoutput.txt | unfurl --unique domains > gau.txt  
  
(kali㉿kali)-[~/indrive/recopilacion]  
└─$ cat gau.txt  
www.indrive.com  
indrive.com  
  
(kali㉿kali)-[~/indrive/recopilacion]  
└─$ █
```

3.8. PERMUTACIONES.

Ya que tenemos toda la información obtenida gracias a las herramientas aplicadas anteriormente, vamos a permutar mediante alterx y dnsx, de la siguiente manera:

```
cat cero.txt ctfr.txt gau.txt katana.txt shuffledns.txt > subdominios.txt
```

```
cat subdominios.txt | alterx | dnsx -o > alterx.txt
```

Los resultados de esta permutación estarán reflejados en los repositorios de GitHub.

4. FINGERPRITING.

4.1. HTTPX.

Con esta herramienta vamos a filtrar los subdominios para quedarnos con los que estén activos. Los comandos que usaremos son los siguientes:

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

```
cat subdominios.txt | httpx --silent > subdominios_vivos.txt
```

```
cat subdominios_vivos.txt | unfurl --unique domains > subdominiosfinal.txt
```

Tras ejecutar estos comandos, podemos ver que nos ha quedado una cantidad reducida de subdominios.

```
(kali㉿kali)-[~/indrive/recopilacion]
$ cat subdominiosfinal.txt | wc
    38      38     740
```

4.2. NMAP/MASSCAN.

Para poder ejecutar la herramienta de Masscan, debemos primero transformar nuestros subdominios en IP´s, para ello utilizamos el siguiente comando:

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

```
(kali㉿kali)-[~/indrive/recopilacion]
$ for subdominio in $(cat subdominiosfinal.txt); do dig +short $subdominio | grep -Eo '([0-9]{1,3}.){3}[0-9]{1,3}'; done > subdominiosfinal_ips.txt
(kali㉿kali)-[~/indrive/recopilacion]
$ cat subdominiosfinal_ips.txt
54.192.95.50
54.192.95.101
54.192.95.69
54.192.95.7
54.192.95.7
54.192.95.69
54.192.95.101
54.192.95.50
3.160.231.46
3.160.231.125
3.160.231.77
3.160.231.4
18.154.48.60
18.154.48.9
18.154.48.37
18.154.48.117
172.66.0.157
162.159.140.159
3.160.231.94
3.160.231.5
3.160.231.111
3.160.231.30
34.149.86.174
18.154.48.60
18.154.48.37
```

Name	Target	Started	Finished	Status	Elapsed
	indrive.com	2025-03-07 15:34:10		Not yet	RUNNING

En los repositorios de GitHub se podrá ver el archivo completo de los subdominios finales convertidos a IP´s.

NMAP:

Para identificar los puertos abiertos, ejecutamos el siguiente comando:

```
sudo nmap -Pn -sS -sV -p0- indrive.com > nmap.txt
```

Como resultado obtenemos los puertos: 80 y 443

```
(kali㉿kali)-[~/indrive/recopilacion]
└─$ sudo nmap -Pn -sS -sV -p0- indrive.com > nmap.txt

(kali㉿kali)-[~/indrive/recopilacion]
└─$ cat nmap.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-07 17:29 EST
Nmap scan report for indrive.com (54.192.95.101)
Host is up (0.0031s latency).
Other addresses for indrive.com (not scanned): 54.192.95.50 54.192.95.7 54.192.95.69
rDNS record for 54.192.95.101: server-54-192-95-101.mad51.r.cloudfront.net
Not shown: 65534 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Amazon CloudFront httpd
443/tcp   open  ssl/http Amazon CloudFront httpd

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 116.98 seconds

(kali㉿kali)-[~/indrive/recopilacion]
└─$
```

Did you know?

MASSCAN:

Intentamos recopilar mas información específica respecto a los puertos utilizando esta herramienta. Para ello utilizaremos la lista de subdominios convertidos a direcciones IP. Lanzaremos un comando en el cual se incluyen los puertos más importantes:

```
sudo masscan -p21,22,80,443,8080 -iL subdominiostxt > masscan.txt
```

En este análisis, podemos ver que, al igual que con nmap nos muestra información acerca del puerto 80 y 443. Sin embargo, en este escaneo debemos resaltar que también nos ha mostrado información respecto al puerto 22, cuyo puerto es un objetivo común para ataques de fuerza bruta y exploits de vulnerabilidades en implementaciones de SSH mal configuradas.

El archivo “masscan.txt” se podrá mirar en los repositorios de GitHub, sin embargo en la captura de pantalla se puede ver reflejado el puerto antes mencionado.

```
Discovered open port 80/tcp on 52.84.66.83
Discovered open port 80/tcp on 3.160.231.30
Discovered open port 443/tcp on 3.160.231.94
Discovered open port 443/tcp on 18.154.48.37
Discovered open port 443/tcp on 3.160.231.4
Discovered open port 443/tcp on 18.154.22.36
Discovered open port 443/tcp on 34.149.86.174
Discovered open port 443/tcp on 18.154.22.48
Discovered open port 80/tcp on 34.160.19.16
Discovered open port 80/tcp on 172.66.0.157
Discovered open port 80/tcp on 52.223.52.2
Discovered open port 22/tcp on 167.172.86.54
Discovered open port 443/tcp on 54.192.95.112
Discovered open port 443/tcp on 18.154.48.60
Discovered open port 443/tcp on 52.84.66.23
Discovered open port 80/tcp on 18.67.240.117
Discovered open port 443/tcp on 3.248.56.152
Discovered open port 80/tcp on 3.248.56.152
```

4.3. GOWITNESS/WAPPALYZER/WHATWEB

GOWITNESS:

El comando para ejecutar esta herramienta es el siguiente:

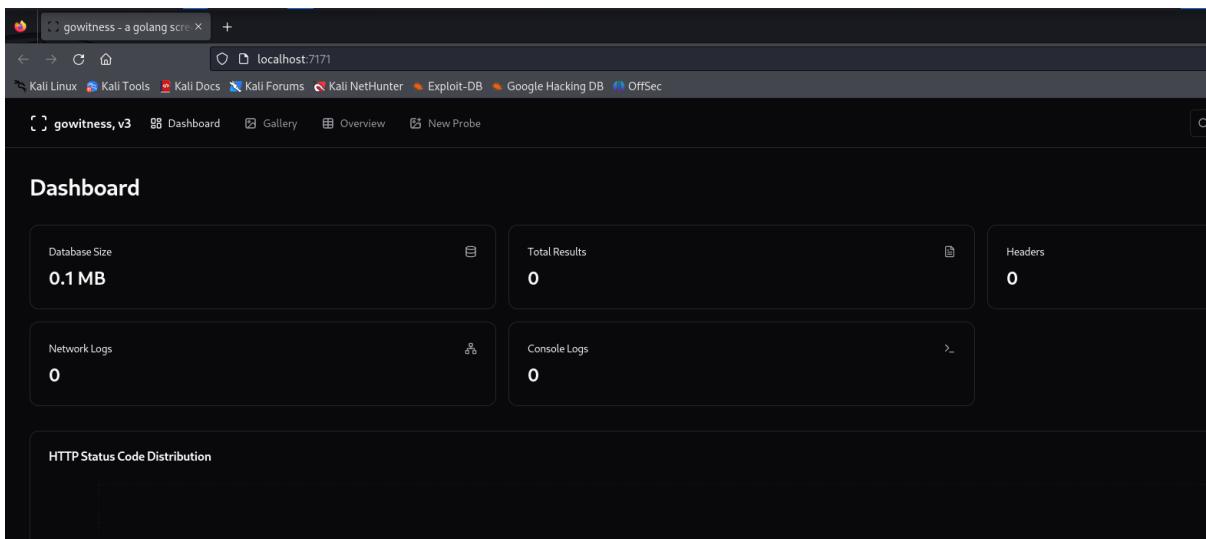
gowitness scan file -f subdominiosfinal.txt

Este comando realiza capturas de pantallas basadas en los subdominios generados en el archivo “subdominiosfinal.txt”.

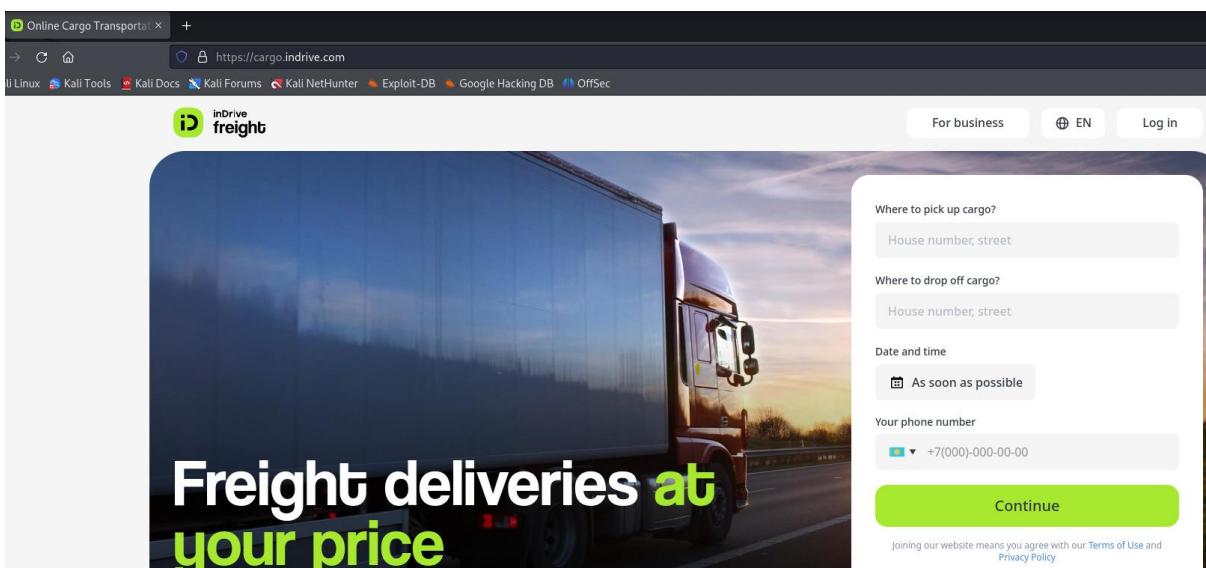
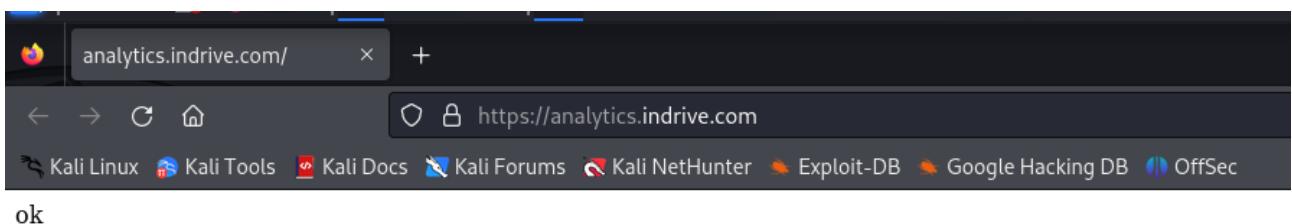
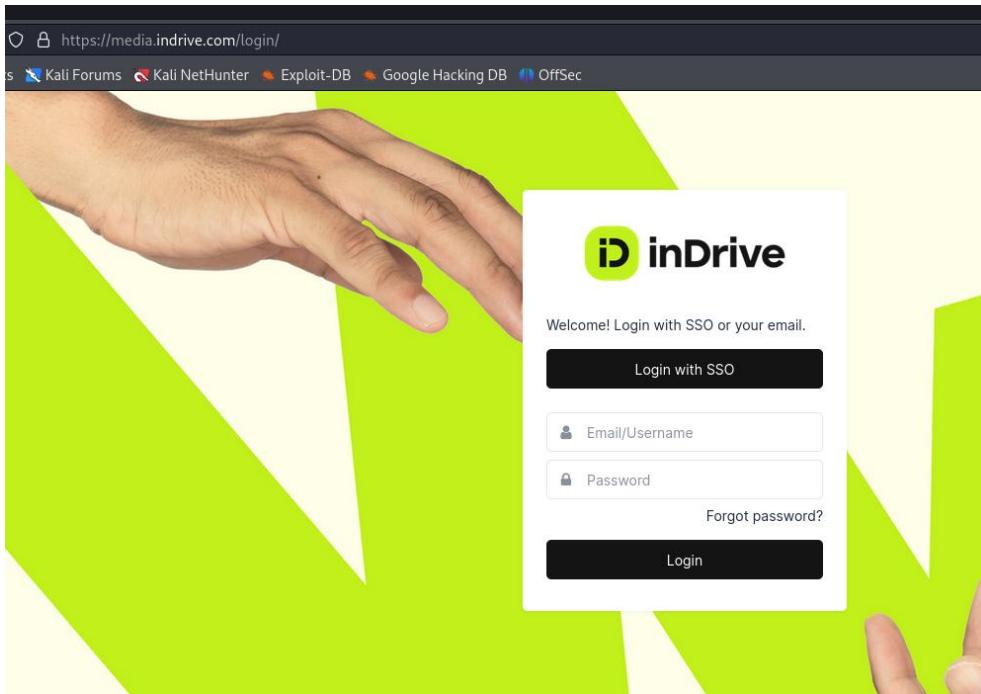
```
[kali㉿kali]:~/indrive/recopilacion]$ gowitness scan file -f subdominiosfinal.txt
2025/03/07 17:52:51 [WARN] no writers have been configured. to persist probe results, add writers using --write-* flags
2025/03/07 17:52:55 [INFO] result [target=http://www.indrive.com:443 status-code=400 title="ERROR: The request could not be satisfied" have-screenshot=true
2025/03/07 17:52:56 [INFO] result [target=http://www.indrive.com:443 status-code=400 title="ERROR: The request could not be satisfied" have-screenshot=true
2025/03/07 17:52:59 [INFO] result [target=https://www.indrive.com:443 status-code=200 title="Earn With inDrive or Offer Your Fare and Get Ride | inDrive" have-screenshot=true
2025/03/07 17:52:59 [INFO] result [target=https://www.indrive.com:80 status-code=200 title="Earn With inDrive or Offer Your Fare and Get Ride | inDrive" have-screenshot=true
2025/03/07 17:53:00 [INFO] result [target=http://s.indrive.com:443 status-code=400 title="ERROR: The request could not be satisfied" have-screenshot=true
2025/03/07 17:53:01 [INFO] result [target=https://s.indrive.com:443 status-code=400 title="ERROR: The request could not be satisfied" have-screenshot=true
2025/03/07 17:53:01 [INFO] result [target=https://s.indrive.com:80 status-code=200 title="Earn With inDrive or Offer Your Fare and Get Ride | inDrive" have-screenshot=true
2025/03/07 17:53:02 [INFO] result [target=https://indrive.com:443 status-code=400 title="Earn With inDrive or Offer Your Fare and Get Ride | inDrive" have-screenshot=true
2025/03/07 17:53:02 [INFO] result [target=https://indrive.com:80 status-code=200 title="Earn With inDrive or Offer Your Fare and Get Ride | inDrive" have-screenshot=true
2025/03/07 17:53:03 [INFO] result [target=https://s.indrive.com:443 status-code=403 title="" have-screenshot=true
2025/03/07 17:53:04 [INFO] result [target=https://job.indrive.com:443 status-code=403 title="" have-screenshot=true
2025/03/07 17:53:06 [INFO] result [target=https://share.indrive.com:80 status-code=403 title="Attention Required! | Cloudflare" have-screenshot=true
2025/03/07 17:53:07 [INFO] result [target=https://job.indrive.com:80 status-code=200 title="Earn With inDrive or Offer Your Fare and Get Ride | inDrive" have-screenshot=true
2025/03/07 17:53:07 [INFO] result [target=https://share.indrive.com:443 status-code=403 title="Access Denied" have-screenshot=true
2025/03/07 17:53:10 [INFO] result [target=https://job.indrive.com:443 status-code=200 title="Earn With inDrive or Offer Your Fare and Get Ride | inDrive" have-screenshot=true
2025/03/07 17:53:10 [INFO] result [target=https://www.intercity.indrive.com:443 status-code=400 title="ERROR: The request could not be satisfied" have-screenshot=true
2025/03/07 17:53:11 [INFO] result [target=https://analytics.indrive.com:80 status-code=200 title="" have-screenshot=true
2025/03/07 17:53:11 [INFO] result [target=https://analytcs.indrive.com:443 status-code=200 title="" have-screenshot=true
2025/03/07 17:53:16 [INFO] result [target=http://rabota.indrive.com:443 status-code=400 title="ERROR: The request could not be satisfied" have-screenshot=true
2025/03/07 17:53:30 [INFO] result [target=http://empleo.indrive.com:443 status-code=400 title="ERROR: The request could not be satisfied" have-screenshot=true
2025/03/07 17:53:49 [INFO] result [target=https://www.intercity.indrive.com:80 status-code=200 title="Comfortable Rides Between Cities At Your Price - inDrive City to city" have-screenshot=true
2025/03/07 17:53:50 [INFO] result [target=https://www.intercity.indrive.com:443 status-code=200 title="Comfortable Rides Between Cities At Your Price - inDrive City to city" have-screenshot=true
2025/03/07 17:53:50 [INFO] result [target=https://www.indrive.com:443 status-code=200 title="Earn With inDrive or Offer Your Fare and Get Ride | inDrive" have-screenshot=true
2025/03/07 17:53:51 [INFO] result [target=https://rabota.indrive.com:443 status-code=200 title="Earn With inDrive or Offer Your Fare and Get Ride | inDrive" have-screenshot=true
2025/03/07 17:53:52 [INFO] result [target=http://empleo.indrive.com:80 status-code=200 title="Earn With inDrive or Offer Your Fare and Get Ride | inDrive" have-screenshot=true
2025/03/07 17:53:53 [INFO] result [target=https://empleo.indrive.com:443 status-code=200 title="Earn With inDrive or Offer Your Fare and Get Ride | inDrive" have-screenshot=true
2025/03/07 17:53:56 [INFO] result [target=http://delivery.indrive.com:80 status-code=404 title="Domain has been assigned" have-screenshot=true
2025/03/07 17:53:55 [INFO] result [target=https://delivery.indrive.com:443 status-code=404 title="Domain has been assigned" have-screenshot=true
2025/03/07 17:53:56 [INFO] result [target=http://www.book.indrive.com:80 status-code=404 title="Domain has been assigned" have-screenshot=true
2025/03/07 17:53:56 [INFO] result [target=https://www.book.indrive.com:443 status-code=404 title="Domain has been assigned" have-screenshot=true
2025/03/07 17:53:58 [INFO] result [target=http://cr.indrive.com:80 status-code=200 title="Feel the freedom" have-screenshot=true
2025/03/07 17:53:58 [INFO] result [target=https://cr.indrive.com:443 status-code=200 title="Feel the freedom" have-screenshot=true
```

También a través de gowitness, intentamos recopilar la información desde la web, utilizando el siguiente comando:

gowitnness report server <http://localhost:7171>



Con esta herramienta no pudimos recopilar ningún tipo de información. Por lo que haremos la investigación manualmente de las capturas de pantallas obtenidas mediante el comando “**gowitnness scan file -f subdominiosfinal.txt**”.



WAPPALYZER:

The screenshot shows the Wappalyzer interface. At the top, there's a navigation bar with a logo, settings, and export options. Below it, the main content area is divided into several sections: CMS (Contentful), Analytics (Google Analytics, Microsoft Clarity 0.8.0, TikTok Pixel), JavaScript frameworks (Next.js 15.1.3, React), and Issue trackers. On the right, there are sections for Web frameworks (Next.js 15.1.3), Reverse proxies (Envoy), UI frameworks (Tailwind CSS), and Cookie compliance (Usercentrics). A sidebar on the right contains a 'Generate sales leads' section with a link to 'Create a lead list'.

El análisis de Wappalyzer muestra las tecnologías utilizadas en un sitio web. Algunos puntos relevantes:

CMS: Usa Contentful, un CMS basado en la nube.

Web Server y Framework: Next.js (versión 15.1.3) es usado tanto como framework de JavaScript como servidor web.

CDN: Amazon CloudFront, lo que indica optimización en la entrega de contenido.

Analítica: Google Analytics, Microsoft Clarity y TikTok Pixel, lo que sugiere un enfoque en el análisis del comportamiento del usuario.

Publicidad: Microsoft Advertising está implementado.

Gestor de etiquetas: Google Tag Manager, lo que permite una gestión más flexible de scripts.

UI y desarrollo: Tailwind CSS para diseño y Webpack como herramienta de empaquetado.

Seguridad y Cumplimiento: Usercentrics para la gestión del consentimiento de cookies.

WHATWEB:

Comando para realizar el análisis web mediante esta herramienta:

```
Whatweb -i subdominiosfinal.txt > whatweb.txt
```

Algunos puntos clave de relevancia:

Uso de CloudFront: La mayoría de los sitios de indrive.com están utilizando Amazon CloudFront como su servidor de origen, lo que podría sugerir una optimización en la entrega de contenido y la seguridad.

Redirecciones 301: La mayoría de los dominios redirigen a versiones "seguras" de sus URLs, probablemente utilizando HTTPS (por ejemplo, <https://empleo.indrive.com/>). Esto es positivo desde el punto de vista de la seguridad web.

IP de Origen en los EE. UU: Todos los dominios analizados tienen servidores en los Estados Unidos, lo que puede indicar que las operaciones están centralizadas en ese país, aunque algunas direcciones tienen una capa adicional de servidores (como CloudFront).

Accesibilidad en algunos dominios: Algunos dominios presentan errores, como 404 Not Found (por ejemplo, delivery.indrive.com y book.indrive.com), lo que sugiere que esos enlaces están rotos o no tienen contenido disponible. Otros muestran 403 Forbidden, indicando que el acceso está restringido, posiblemente por políticas de seguridad.

Diferentes ubicaciones geográficas: Algunos dominios están registrados en otros países, como Bulgaria y el Reino Unido, lo que podría implicar una infraestructura distribuida globalmente, aunque las solicitudes van a servidores en los EE. UU.

Tecnologías involucradas: Además de CloudFront, se observa que algunos sitios están usando servidores como nginx y Ubuntu Linux.

4.4. IDENTIFICACIÓN WAF/ WAFW00F.

Comando para la aplicación de esta herramienta:

Wafw00f.indrive.com

El resultado indica que el sitio web <https://indrive.com> está protegido por un WAF de Cloudfront (Amazon). Esto es relevante porque:

Seguridad del sitio: Indica que el sitio usa un servicio de protección contra ataques web, como SQL Injection o XSS.

Enumeración de seguridad: Si estás haciendo pruebas de seguridad (pentesting), saber qué WAF está presente puede ayudarte a elegir técnicas para evadirlo.

Uso de infraestructura en la nube: Amazon Cloudfront es un CDN con capacidades de protección, lo que sugiere que el sitio usa infraestructura en la nube.

4.5. FUZZING.

`ffuf -w ~/indrive/recopilacion/common.txt -t 10 -mc 200,401,403 -u https://indrive.com/FUZZ`

```
(kali㉿kali)-[~/indrive/recopilacion]
$ ffuf -w ~/indrive/recopilacion/common.txt -t 10 -mc 200,401,403 -u https://indrive.com/FUZZ
v2.1.0-dev

:: Method      : GET
:: URL         : https://indrive.com/FUZZ
:: Wordlist    : FUZZ: /home/kali/indrive/recopilacion/common.txt
:: Follow redirects : false
:: Calibration   : false
:: Timeout       : 10
:: Threads       : 10
:: Matcher       : Response status: 200,401,403

.git          [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 63ms]
.git-rewrite   [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 70ms]
.git/config    [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 66ms]
.git/HEAD      [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 112ms]
.git/index     [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 64ms]
.git/logs/     [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 61ms]
.gitattributes [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 49ms]
.git_release   [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 122ms]
.gitconfig     [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 113ms]
.gitk          [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 103ms]
.gitignore     [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 124ms]
.gitkeep       [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 49ms]
.gitmodules   [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 69ms]
.gitreview    [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 113ms]
.svnignore    [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 48ms]
.svn/entries   [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 68ms]
.svn          [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 108ms]
.well-known/assetlinks.json [Status: 200, Size: 837, Words: 191, Lines: 29, Duration: 122ms]
.well-known/apple-app-site-association [Status: 200, Size: 78, Words: 17, Lines: 6, Duration: 304ms]
```

```
(kali㉿kali)-[~/indrive/recopilacion]
$ cat fuzzing.txt
.git          [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 79ms]
.git-rewrite   [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 87ms]
.git/config    [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 65ms]
.git/HEAD      [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 81ms]
.git/index     [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 68ms]
.gitconfig     [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 33ms]
.gitignore     [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 34ms]
.gitk          [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 35ms]
.git/logs/     [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 56ms]
.git_release   [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 63ms]
.gitmodules   [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 36ms]
.gitattributes [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 66ms]
.gitreview    [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 56ms]
.gitkeep       [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 69ms]
.svn          [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 34ms]
.svn/entries   [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 37ms]
.svnignore    [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 34ms]
.well-known/assetlinks.json [Status: 200, Size: 837, Words: 191, Lines: 29, Duration: 4ms]
.well-known/apple-app-site-association [Status: 200, Size: 78, Words: 17, Lines: 6, Duration: 30ms]
blog          [Status: 200, Size: 16224, Words: 9849, Lines: 1, Duration: 84ms]
book          [Status: 200, Size: 177871, Words: 10741, Lines: 2, Duration: 31ms]
business      [Status: 200, Size: 181621, Words: 10668, Lines: 4, Duration: 29ms]
company       [Status: 200, Size: 227308, Words: 12835, Lines: 19, Duration: 40ms]
contacts      [Status: 200, Size: 168301, Words: 10108, Lines: 1, Duration: 33ms]
driver         [Status: 200, Size: 198345, Words: 12198, Lines: 5, Duration: 34ms]
en            [Status: 200, Size: 218312, Words: 12201, Lines: 14, Duration: 29ms]
favicon.ico   [Status: 200, Size: 15086, Words: 11, Lines: 1, Duration: 81ms]
legal          [Status: 200, Size: 162697, Words: 9850, Lines: 1, Duration: 90ms]
newsroom       [Status: 200, Size: 166343, Words: 10016, Lines: 1, Duration: 80ms]
offer          [Status: 200, Size: 159111, Words: 9694, Lines: 1, Duration: 81ms]
robots.txt    [Status: 200, Size: 1896, Words: 65, Lines: 64, Duration: 31ms]
safety         [Status: 200, Size: 195568, Words: 11760, Lines: 9, Duration: 32ms]
security.txt  [Status: 200, Size: 220, Words: 15, Lines: 9, Duration: 36ms]
sitemap.xml   [Status: 200, Size: 14588, Words: 4780, Lines: 344, Duration: 94ms]
```

Este escaneo con fuzzing revela información relevante sobre la estructura del sitio web indrive.com. Aquí están los puntos clave que destacan:

Archivos y Directorios Sensibles Bloqueados (403 - Forbidden)

Se detectaron múltiples archivos y directorios relacionados con Git y SVN, aunque están protegidos:

git, .git/config, .gitignore, .gitmodules, .gitreview, etc.

.svn, .svn/entries, .svnidignore.

Relevancia: Aunque están restringidos, su existencia indica que el código fuente del sitio puede haber estado en algún momento expuesto o mal gestionado. Si estos directorios fueran accesibles, podrían revelar información como credenciales, claves API o historial de cambios del repositorio.

Archivos y Directorios Públicos (200 - OK)

.well-known/assetlinks.json y .well-known/apple-app-site-association

Estos archivos confirman que el sitio tiene soporte para Android App Links y iOS Universal Links, usados para vincular aplicaciones móviles con el sitio web.

Páginas de interés detectadas:

/blog, /book, /business, /company, /contacts, /driver, /legal, /newsroom, /offer, /safety

Estas rutas pueden contener información corporativa, datos de contacto, términos legales, noticias, etc.

Archivos de configuración y seguridad:

/robots.txt → Puede contener rutas ocultas que los administradores no quieren que sean indexadas por buscadores.

/sitemap.xml → Proporciona una lista estructurada de páginas públicas del sitio.

/security.txt → Contiene detalles sobre cómo reportar vulnerabilidades a la empresa.

5. ANÁLISIS DE VULNERABILIDADES.

5.1 GREENBONE.

Report: Thu, Mar 6, 2025 7:25 PM UTC

Vulnerability	Severity	QoD	Host
	IP	Name	
TCP Timestamps Information Disclosure	2.6 (Low)	80 %	54.192.95.50 server-54-1
TCP Timestamps Information Disclosure	2.6 (Low)	80 %	54.192.95.101 server-54-1
TCP Timestamps Information Disclosure	2.6 (Low)	80 %	54.192.95.69 server-54-1
TCP Timestamps Information Disclosure	2.6 (Low)	80 %	54.192.95.7 server-54-1

Vulnerabilidades Detectadas:

Se han encontrado 4 vulnerabilidades, todas relacionadas con "TCP Timestamps Information Disclosure".

Cada una de ellas tiene una severidad baja (2.6) en la escala CVSS.

Equipos Afectados:

Los hosts afectados tienen direcciones IP en el rango 54.192.95.X.

Nombres de servidor: server-54-192-95-XX.

Calidad de Detección (QoD):

El nivel de confianza en la detección de estas vulnerabilidades es del 80%.

Errores Detectados:

Se han registrado 100 de 100 mensajes de error, lo que puede indicar problemas adicionales.

5.2. NUCLEI.

Utilizamos el siguiente comando para ejecutar la herramienta:

nuclei -u indrive.com > nuclei.txt

Como se puede apreciar en la imagen, esta herramienta no proporciona ninguna información relevante, únicamente INFO. El archivo txt se puede mirar en los repositorios de GitHub.

5.3. WPSSCAN.

Se ha ejecutado esta herramienta con el siguiente comando:

```
wpscan --random-user-agent --url https://indrive.com/
```

Como podemos apreciar en la imagen, nuestro dominio no usa Wordpress.

5.4. ANÁLISIS SSL/TLS.

 Qualys. SSL Labs

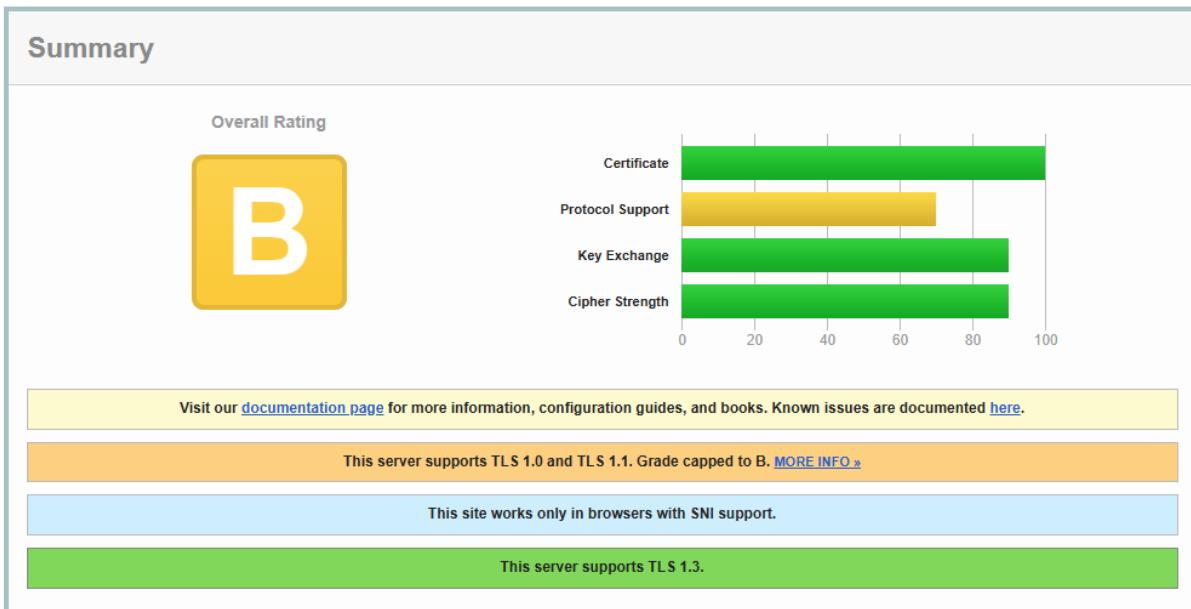
Home Projects Qualys Free Trial Contact

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [indrive.com](#) > 18.173.121.124

SSL Report: [indrive.com](#) (18.173.121.124)

Assessed on: Sat, 08 Mar 2025 16:41:25 UTC | [Hide](#) | [Clear cache](#)

[Scan Another](#)



Cipher Suites

TLS 1.3 (suites in server-preferred order)

TLS_AES_128_GCM_SHA256 (0x1301) ECDH x25519 (eq. 3072 bits RSA) FS 128

TLS_AES_256_GCM_SHA384 (0x1302) ECDH x25519 (eq. 3072 bits RSA) FS 256

TLS_CHACHA20_POLY1305_SHA256 (0x1303) ECDH x25519 (eq. 3072 bits RSA) FS 256

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH x25519 (eq. 3072 bits RSA) FS 128

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH x25519 (eq. 3072 bits RSA) FS WEAK 128

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH x25519 (eq. 3072 bits RSA) FS WEAK 128

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH x25519 (eq. 3072 bits RSA) FS 256

TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa) ECDH x25519 (eq. 3072 bits RSA) FS 256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH x25519 (eq. 3072 bits RSA) FS WEAK 256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH x25519 (eq. 3072 bits RSA) FS WEAK 256

TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK 128

TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) WEAK 256

TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK 128

TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK 256

TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK 128

TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK 112

TLS 1.1 (suites in server-preferred order)

TLS 1.0 (suites in server-preferred order)

Cipher Suites Débiles o Obsoletas (WEAK)

TLS 1.2 con AES en CBC (Cipher Block Chaining) - Vulnerable a ataques BEAST y Lucky13

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

TLS 1.2 sin Forward Secrecy (RSA estático)

TLS_RSA_WITH_AES_128_GCM_SHA256

TLS_RSA_WITH_AES_256_GCM_SHA384

TLS_RSA_WITH_AES_128_CBC_SHA256

TLS_RSA_WITH_AES_256_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_3DES_EDE_CBC_SHA (Triple DES es altamente inseguro)

5.5. DMARC/DKIM/SPF

Tras el uso de distintas herramientas podemos ver que nuestro dominio principal tiene una buena configuración de DMARC/DKIM/SPF. Adjunto pantallazos que lo demuestran.

The screenshot displays the results of a DMARC domain check for the domain `indrive.com`. The interface includes a search bar with the domain name and a green "CHECK DOMAIN" button. Below the search area, there's a message about the tool's purpose: "Use our DMARC Domain Checker to quickly find out if a domain is properly protected against phishing, spoofing and domain abuse. This tool inspects DMARC, SPF and DKIM records to see if any issues are present." The main results section is framed in green and contains three items:

- DMARC:** Shows a green icon with a checkmark and the text "Well done! You have a valid DMARC record that provides visibility into the entirety of your email program(s) and helps ensure you meet email sending best practices. Your domain takes full advantage of the domain protections afforded by DMARC." A "GET STARTED" button is visible to the right.
- SPF:** Shows a green icon with a checkmark and the text "Great job! You have a valid SPF record, which specifies a soft fail (~all)." A "+ Details" link is provided.
- DKIM:** Shows a green icon with a checkmark and the text "We found at least one DKIM valid record. It's likely that you have others as each email sending source should have its own DKIM keys. DMARC visibility can help you discover each of your DKIM keys and much more." A "+ Details" link is provided.

indrive.com

CHECK DMARC

Protected by reCAPTCHA. Google [Privacy Policy](#) and [Terms of Service](#) apply.

Your results

Full DMARC record

v=DMARC1; p=reject; rua=mailto:indrivepostmaster@gmail.com; sp=reject; pct=100; adkim=s; aspf=s;

Declared tags

Tag	Value	Description
v	DMARC1	DMARC protocol version.
p	reject	Apply this policy to email that fails the DMARC check. This policy can be set to 'none', 'quarantine', or 'reject'. 'none' is used to collect the DMARC report and gain insight into the current email flows and their status.
sp	reject	This policy should be applied to email from a sub-domain of this domain that fail the DMARC check. Using this tag domain owners can publish a 'wildcard' policy for all subdomains.
rua	mailto:indrivepostmaster@gmail.com	A list of URIs for ISPs to send XML feedback to. NOTE: this is not a list of email addresses. DMARC requires a list of URIs of the form 'mailto:test@example.com'.

SPF Results for domain:

indrive.com

indrive.com

DNS Record Total look ups: 15 Look ups: 6

No problems were detected with this record

v=spf1 include:_spf.google.com include:spf.mandrillapp.com include:_spf.salesforce.com include:amazoneses.com +a +mx ~all

A/AAAA Records

MX Records

No MX record found for this domain

_spf.google.com

DNS Record Look ups: 3

No problems were detected with this record

v=spf1 include:_netblocks.google.com include:_netblocks2.google.com include:_netblocks3.google.com ~all

_netblocks.google.com

DNS Record Look ups: 0

No problems were detected with this record

v=spf1 ip4:35.190.247.0/24 ip4:64.233.160.0/19 ip4:66.102.0/20 ip4:66.249.80.0/20 ip4:72.14.192.0/18 ip4:74.125.0/16 ip4:108.177.8.0/21 ip4:173.194.0/16 ip4:209.85.128.0/17 ip4:216.58.192.0/19 ip4:216.239.32.0/19 ~all

IP Records

5.6. SUBZY.

Subzy es una herramienta de seguridad utilizada para detectar subdominios vulnerables a secuestro (subdomain takeover). El comando que utilizaremos para ejecutar esta herramienta es el siguiente:

subzy run --targets subdominios_vivos.txt > subzy.txt

```
[ NOT VULNERABLE ] - https://money.indrive.com
[ NOT VULNERABLE ] - https://promotion.indrive.com
[ NOT VULNERABLE ] - https://www.indrive.com
[ NOT VULNERABLE ] - https://us.indrive.com
[ NOT VULNERABLE ] - https://services.indrive.com.co

[ VULNERABLE ] - http://promo.indrive.com [ Tilda ]
[ DISCUSSION ] - [Issue #155](https://github.com/EdOverflow/can-i-take-a-look)
[ DOCUMENTATION ] - 

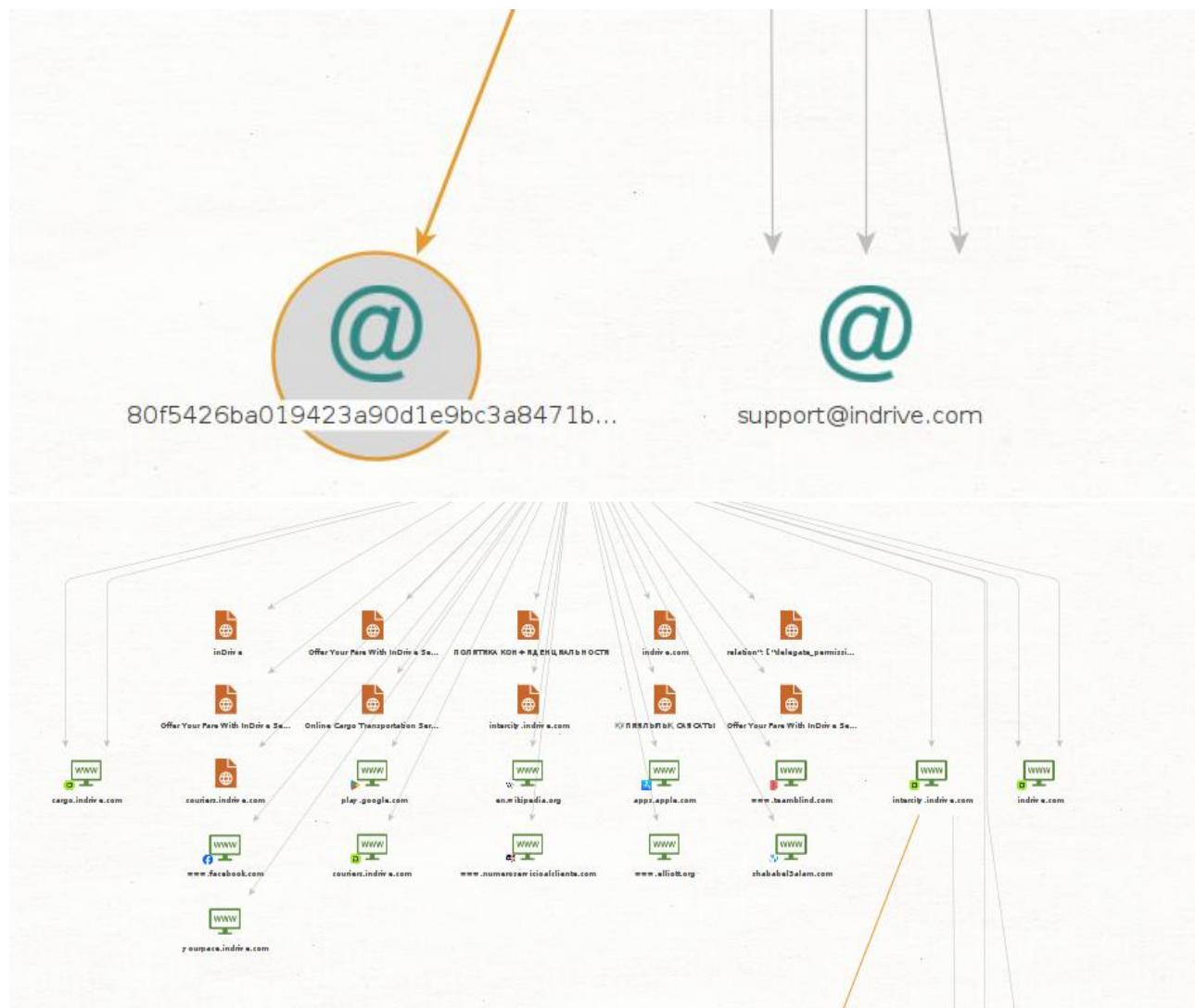
[ NOT VULNERABLE ] - https://careers.indrive.com
[ NOT VULNERABLE ] - https://www.id.indrive.com
[ NOT VULNERABLE ] - https://id.indrive.com
[ NOT VULNERABLE ] - https://movie.indrive.com
```

Parece que el único subdominio vulnerable es <http://promo.indrive.com>, el cual está marcado como [VULNERABLE] y asociado a un posible takeover mediante Tilda.

El escaneo completo esta en los repositorios de GitHub como “subzy.txt”.

6. OSINT.

Maltego: Con maltego no se ha encontrado información relevante tras una cantidad numerosa de intentos, adjunto pantallazos de lo que he podido obtener con maltego.



Spiderfoot: Con spiderfoot si pudimos obtener una lista de emails, los cuales serán evaluados con la herramienta de havebeenowned para verificar si algún correo ha aparecido en algún breach/leak.

	Data Element	Source Data Element	Source Module	Identified
■	aleksandr.blanar@indrive.com	indrive.com	sfp_skymem	2025-03-07 15:38:47
■	beginit@indrive.com	indrive.com	sfp_skymem	2025-03-07 15:38:47
■	cybersecurity@indrive.com	indrive.com	sfp_skymem	2025-03-07 15:38:47
■	elizaveta.surganova@indrive.com	indrive.com	sfp_skymem	2025-03-07 15:38:47
■	gr@indrive.com	indrive.com	sfp_skymem	2025-03-07 15:38:47
■	hr@indrive.com	indrive.com	sfp_skymem	2025-03-07 15:38:47
■	indriveeduardo@indrive.com	indrive.com	sfp_skymem	2025-03-07 15:38:47
■	indrivenatalia.espejo@indrive.com	indrive.com	sfp_skymem	2025-03-07 15:38:47
■	info@indrive.com	indrive.com	sfp_skymem	2025-03-07 15:38:47
■	pr@indrive.com	indrive.com	sfp_skymem	2025-03-07 15:38:47
■	shoroukibrahim@indrive.com	indrive.com	sfp_skymem	2025-03-07 15:38:47
■	supernovas@indrive.com	indrive.com	sfp_skymem	2025-03-07 15:38:47
■	u003support@indrive.com	indrive.com	sfp_skymem	2025-03-07 15:38:47
■	upport@indrive.com	indrive.com	sfp_skymem	2025-03-07 15:38:47

Tras introducir manualmente cada correo mostrado en la tabla en havelbennspawned ningn correo ha aparecido en ningn breach/leak.

Los mas relevantes, ya que son correos asociados a personas:

[shoroukibrahim@indrive.com](#)

[elizaveta.surganova@indrive.com](#)

[aleksandr.blanar@indrive.com](#)

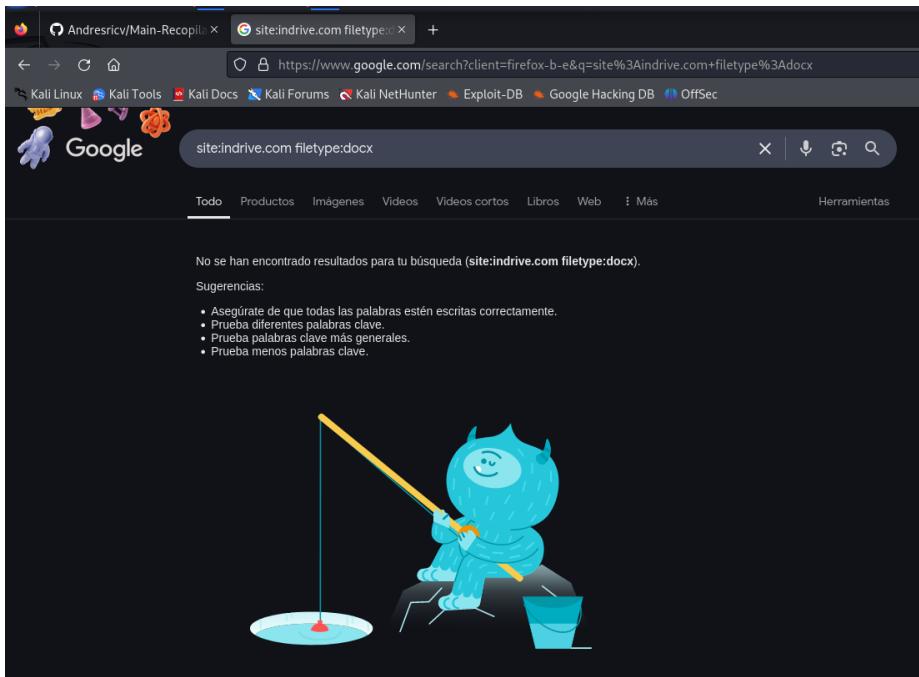
Tambin mediante otra herramienta llamada “anymailfinder” hemos podido obtener otros correos electrnicos:

The screenshot shows the Anymailfinder search interface. At the top, there's a green bar with the text "Start your 3 days trial today." Below it, the search form has "Start your Search" and "Search history". Under "Search history", the domain "indrive.com" is listed with "18 results found". A "Hide Emails" button is visible. Below this, a grid of 18 email addresses is shown, each with a green checkmark icon and a small "copy" icon. The emails include: solomatina.v@indrive.com, kate.mikolenko@indrive.com, jorge.rossiter@indrive.com, alina.baibulatova@indrive.com, rodrigo.garcia@indrive.com, andries.smit@indrive.com, mohamed.galala@indrive.com, oksana.levkovich@indrive.com, anna.pyasetskaya@indrive.com, stefano.mazzaferro@indrive.com, ilia.kliuchnikov@indrive.com, mikhaill.avdeev@indrive.com, nikita.simonov@indrive.com, teena.dambiraja@indrive.com, marcella.cruz@indrive.com, abhishek.uniyal@indrive.com, vladislav.teterin@indrive.com, and nadeen.hossam@indrive.com. At the bottom of the list, there's a "Copy 18 emails" button.

Tambin se ha realizado la exploracin manual en havlbeenspawned de cada correo electrnico y ninguno de ellos tiene ningn breach/leak.

Para avanzar en la bsqueda, buscaremos en internet si hay ficheros compartidos en distintos formatos:

DOCX:



PDF:

6.1. ANALISIS DE REDES SOCIALES.

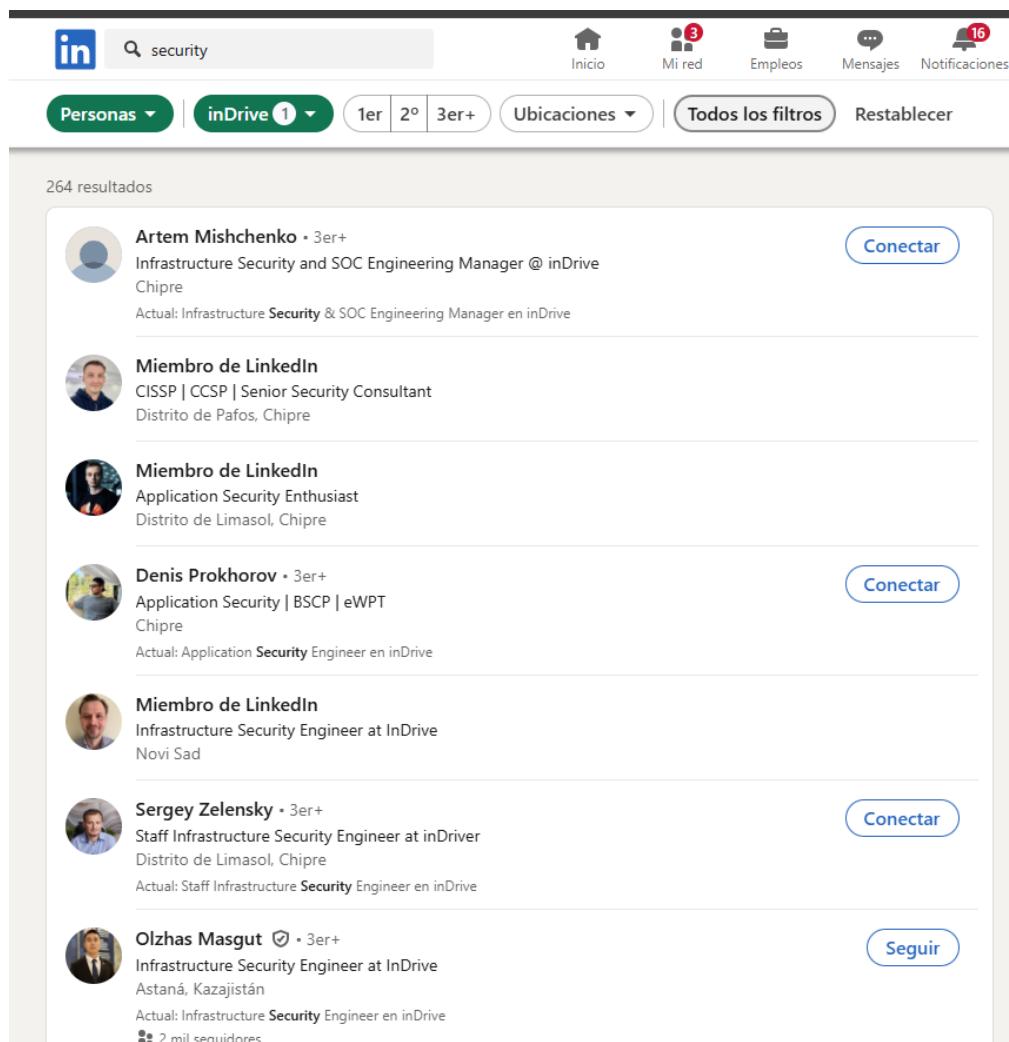
Para este análisis nos enfocaremos en la red social LinkedIn. A través del buscador intentaremos encontrar información de empleados, cuyos puestos puedan ser de interés.

Se ha encontrado al CEO de la empresa.



LinkedIn search results for "ceo": 108 resultados

Miembro de LinkedIn
CEO & Founder w INDRIVE Sp. z o.o.
Bielsko-Biala y alrededores



LinkedIn search results for "security": 264 resultados

- Artem Mishchenko** • 3er+
Infrastructure Security and SOC Engineering Manager @ inDrive
Chipre
Actual: Infrastructure **Security** & SOC Engineering Manager en inDrive
- Miembro de LinkedIn**
CISSP | CCSP | Senior Security Consultant
Distrito de Pafos, Chipre
- Miembro de LinkedIn**
Application Security Enthusiast
Distrito de Limasol, Chipre
- Denis Prokhorov** • 3er+
Application Security | BSCP | eWPT
Chipre
Actual: Application **Security** Engineer en inDrive
- Miembro de LinkedIn**
Infrastructure Security Engineer at InDrive
Novi Sad
- Sergey Zelensky** • 3er+
Staff Infrastructure Security Engineer at inDriver
Distrito de Limasol, Chipre
Actual: Staff Infrastructure **Security** Engineer en inDrive
- Olzhass Masgut** ✅ • 3er+
Infrastructure Security Engineer at InDrive
Astaná, Kazajistán
Actual: Infrastructure **Security** Engineer en inDrive
2 mil seguidores