

INFORME REDTEAM



Informe de Reconocimiento RedTeam
Scope (*.indrive.com)

RedTeam / Seguridad de la Información

Estudiante: Jordan Andres Diaz
Profesor: Pablo Ambite

TABLA DE CONTENIDO

1. INTRODUCCIÓN

- 1.1. Objetivo de la revisión
- 1.2. Alcance y consideraciones éticas
- 1.3. Metodología empleada

2. RECONOCIMIENTO Y RECOPIACIÓN DE INFORMACIÓN

- 2.1. Información general de la organización
- 2.2. Empresas asociadas y estructura corporativa
- 2.3. Sistemas Autónomos (ASN)
- 2.4. Dominios y subdominios
- 2.5. Tecnologías y servicios detectados
- 2.6. DNS, WHOIS, robots.txt y certificaciones SSL

3. PLANIFICACION DEL EJERCICIO

- 3.1. Priorización de activos y superficie de ataque
- 3.2. Vectores de acceso potenciales
- 3.3. Herramientas y técnicas propuestas

4. LABORATORIO DE SIMULACIÓN

- 4.1. Diseño del entorno
- 4.2. Configuración y creación payloads (Command and Control)

5. CONCLUSIÓN Y RECOMENDACIONES

- 5.1. Valoración del proceso
- 5.2. Recomendaciones de seguridad
- 5.3. Lecciones aprendidas

6. REFERENCIAS Y BIBLIOGRAFÍA

1. INTRODUCCIÓN

1.1. Objetivo de la revisión

El presente informe tiene como finalidad documentar el proceso de planificación, reconocimiento y análisis técnico inicial sobre la organización InDrive (*.indrive.com), en el contexto del módulo de Red Team. Esta práctica forma parte del ejercicio, cuyo objetivo es poner en práctica técnicas de reconocimiento pasivo y activo sobre un objetivo real, permitiéndome adquirir experiencia en la fase de recolección de información dentro de un ejercicio ofensivo controlado.

Durante esta revisión se identifican activos expuestos públicamente tales como dominios, subdominios, rangos de IP, sistemas autónomos y tecnologías utilizadas. Se priorizan dichos activos en función de su criticidad y superficie de exposición, sentando las bases para el diseño de un plan de ataque ético en un entorno simulado.

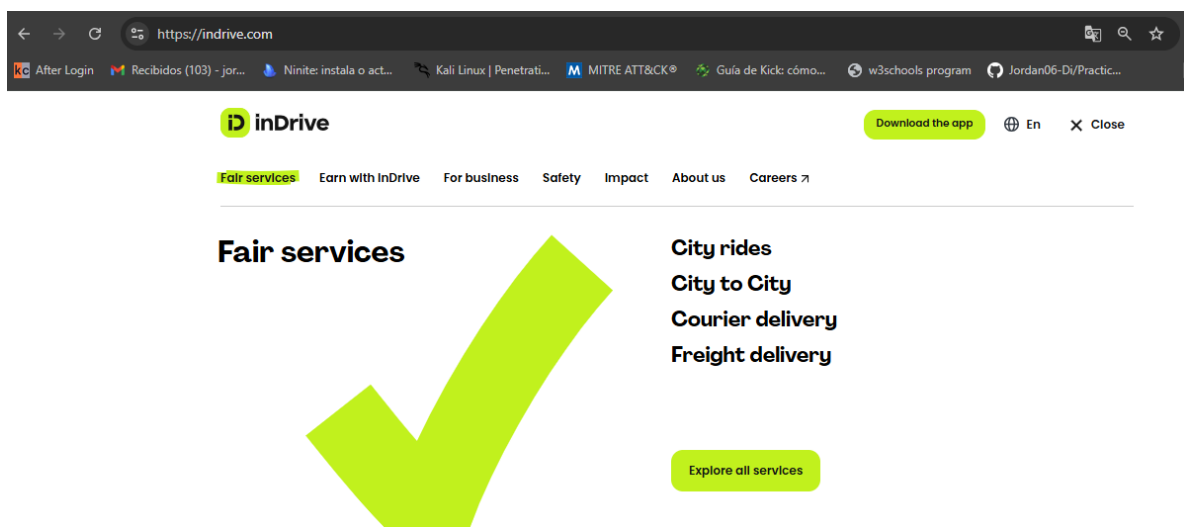


Ilustración 1

1.2. Alcance y consideraciones éticas

El alcance de este ejercicio se limita estrictamente a técnicas de reconocimiento pasivo y activo no intrusivo, aplicadas sobre el dominio público (*.indrive.com) y sus activos asociados. En ningún momento se ejecutarán acciones ofensivas reales como explotación de vulnerabilidades, denegación de servicio, acceso no autorizado o modificación de sistemas de la organización objetivo.

Las acciones realizadas están dirigidas exclusivamente a fines académicos, dentro de un entorno de aprendizaje, y bajo principios éticos que respetan la legalidad y la privacidad de terceros. En caso de hallazgos críticos o accesos abiertos inadvertidos, estos no serán utilizados ni divulgados, siguiendo la conducta profesional esperada en entornos de ciberseguridad.

1.3. Metodología empleada

La metodología seguida se basa en las primeras fases del ciclo de vida de una operación Red Team: planificación, reconocimiento, enumeración y simulación de escenarios de ataque. Se utilizaron herramientas OSINT y técnicas de análisis pasivo para obtener una visión detallada de la infraestructura tecnológica de la organización.

Los pasos clave fueron los siguientes:

- ❖ Investigación general de la organización y sus afiliados.
- ❖ Recolección de información desde fuentes abiertas (WHOIS, DNS, Shodan, Censys, Crunchbase, etc.).
- ❖ Enumeración de dominios, subdominios y rangos IP.
- ❖ Identificación de tecnologías y servicios expuestos.
- ❖ Priorización de activos para su análisis más profundo.
- ❖ Planificación teórica de posibles vectores de entrada.
- ❖ Implementación de un laboratorio propio para la simulación del ejercicio ofensivo con herramientas como Havoc.

Este enfoque permite no solo evaluar la superficie de exposición de una organización real, sino también construir una base sólida para ejercicios ofensivos en entornos simulados, cumpliendo los objetivos pedagógicos del módulo.

2. RECONOCIMIENTO Y RECOPIACIÓN DE INFORMACIÓN

2.1. Información general de la organización (indriver.com)

InDrive (anteriormente conocida como inDriver) es una plataforma global de transporte fundada en 2012, que ofrece servicios de movilidad urbana bajo un modelo de negociación directa entre pasajeros y conductores. A diferencia de las plataformas tradicionales de ridesharing, InDrive permite que el usuario proponga una tarifa y el conductor acepte, rechace o contra oferte dicha cantidad.

La compañía ha experimentado un crecimiento significativo en América Latina, Asia, Europa del Este y África, posicionándose como una alternativa innovadora en el mercado de transporte bajo demanda. Además del transporte de pasajeros, InDrive ha ampliado su catálogo de servicios para incluir envíos de paquetería, transporte de carga y servicios personales como ayuda doméstica y mensajería.

Su sede central se encuentra en Mountain View, California (EE. UU.), aunque mantiene operaciones activas en decenas de países. Según diversas fuentes abiertas, InDrive ha adoptado una infraestructura tecnológica basada en servicios web modernos, soluciones cloud y aplicaciones móviles para Android e iOS, lo cual la convierte en un objetivo relevante para el estudio del reconocimiento técnico en contextos de Red Team.

A lo largo de este ejercicio, se trabajará exclusivamente sobre recursos accesibles públicamente bajo el dominio (*.indrive.com), sin realizar ninguna interacción directa que afecte a la operación real de sus sistemas. Esta fase introductoria permite contextualizar a la organización como objetivo de análisis, entendiendo su presencia digital, estructura y posible superficie de exposición.

2.2. Empresas asociadas y estructura Corporativa

InDrive opera bajo la razón social SUOL INNOVATIONS LTD., registrada inicialmente en Rusia y posteriormente trasladada a jurisdicciones más favorables para su expansión internacional, como Chipre y Estados Unidos. La estructura corporativa de la organización refleja una estrategia de crecimiento agresiva, con múltiples entidades subsidiarias o representantes legales en países clave donde ofrece servicios de movilidad.

Según fuentes abiertas como Crunchbase, LinkedIn corporativo, registros mercantiles y prensa tecnológica, la empresa ha establecido filiales o representantes en países como:

1. México (para operaciones en América Latina)
2. India y Pakistán (como parte de su expansión en Asia)
3. Rusia (como base original de operaciones)
4. Estados Unidos (actual centro estratégico de negocios y desarrollo tecnológico)

Aunque no se identifican adquisiciones importantes como ocurre con conglomerados tipo Booking Holdings, la estructura de InDrive sí muestra una diversificación geográfica significativa. Esta presencia distribuida conlleva la gestión de dominios y subdominios independientes por región, así como configuraciones particulares de infraestructura digital adaptadas a requerimientos legales y técnicos locales.

Esta descentralización puede generar una superficie de ataque más amplia y heterogénea, ya que cada entidad operativa puede emplear proveedores de servicios distintos, implementar configuraciones específicas o mantener niveles de madurez en ciberseguridad variables.

Durante la fase de enumeración, se tendrá en cuenta esta posible ramificación organizacional al identificar dominios y subdominios que podrían estar asociados a diferentes regiones operativas o funciones internas, como soporte, reclutamiento, pagos o integración de aplicaciones móviles.

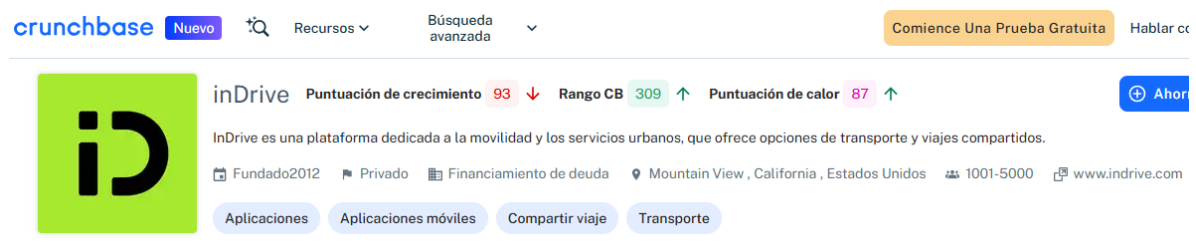


Ilustración 2

Ilustración 3

2.3. Sistemas Autónomos (ASN)

Durante la fase de reconocimiento, se identificaron los sistemas autónomos asociados al dominio (indrive.com), revelando la infraestructura de red utilizada por la organización para prestar sus servicios globales.

Mediante herramientas como Hurricane Electric BGP Toolkit y SecurityTrails, se obtuvo la siguiente información:

- ASN principal: AS209671 – Qrator Labs CZ s.r.o.
- Rango de IP asignado: 185.104.208.0/22
- Dirección IP asociada al dominio: 185.104.210.6

La presencia del ASN AS209671, operado por Qrator Labs CZ s.r.o., sugiere que InDrive utiliza servicios de mitigación de ataques DDoS y protección de infraestructura proporcionados por este proveedor. Qrator Labs es conocido por ofrecer soluciones de seguridad y rendimiento para redes, lo que indica un enfoque proactivo de InDrive hacia la protección de sus activos digitales.

La identificación de este ASN permite acotar la infraestructura visible en Internet, así como delimitar posibles activos externos expuestos, lo cual es fundamental para la priorización de objetivos y el análisis de superficie de ataque.

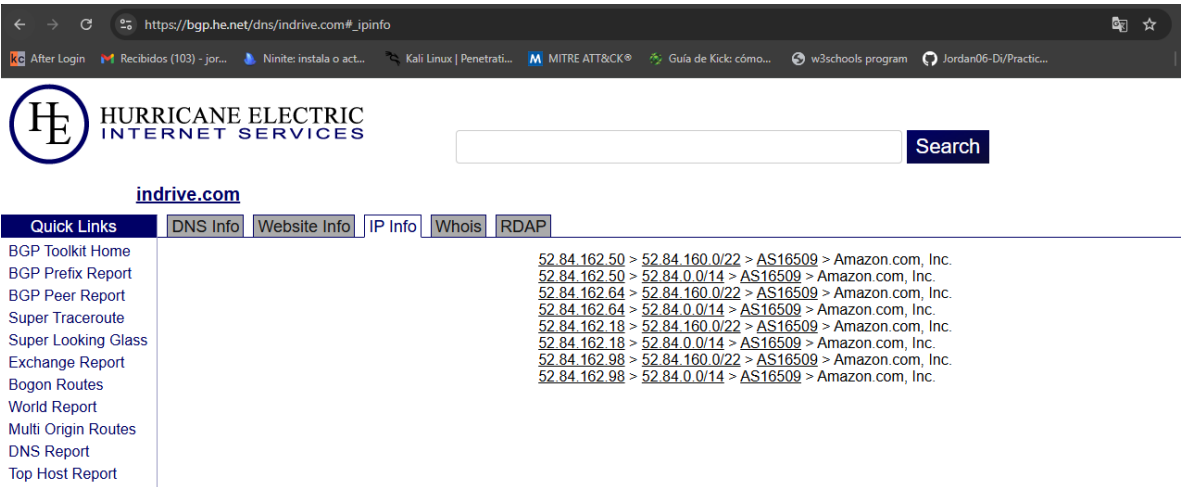


Ilustración 4

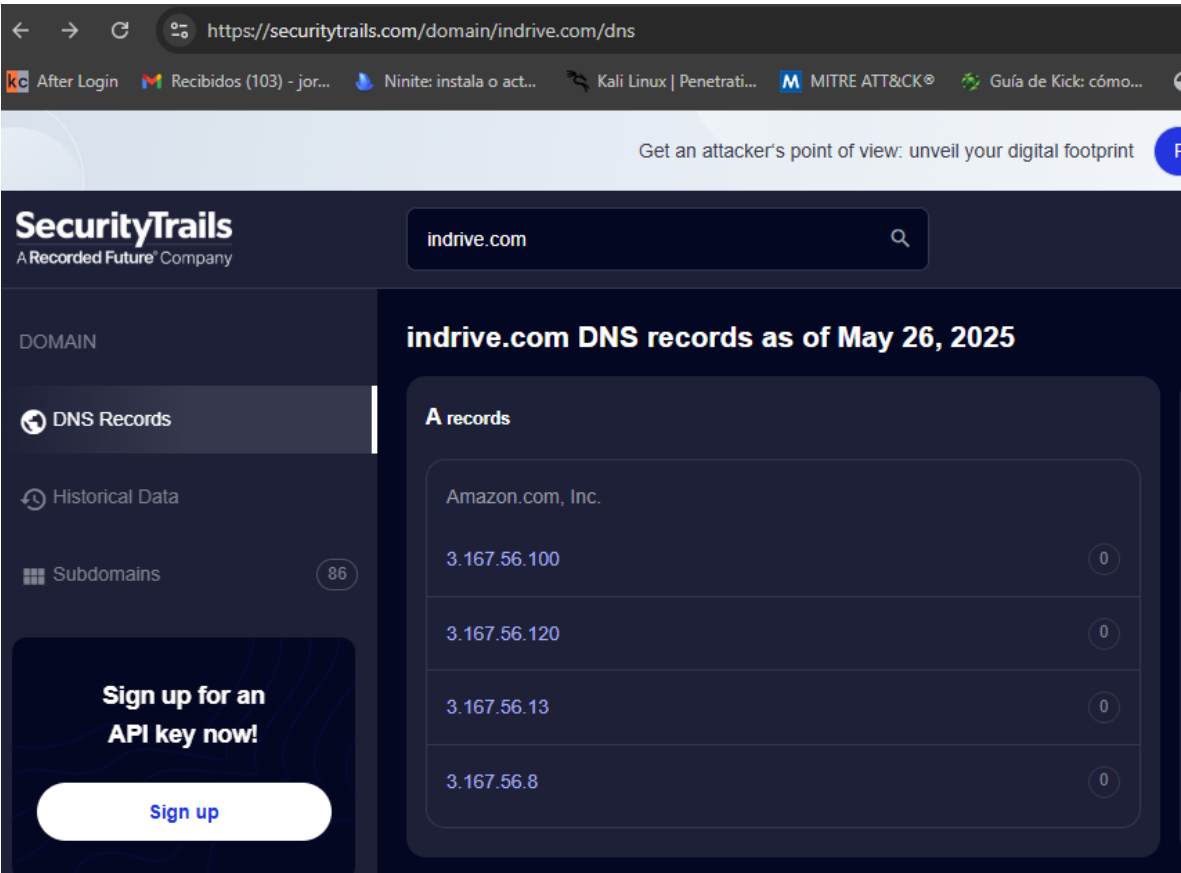


Ilustración 5

2.4. Dominios y subdominios

Durante esta fase del ejercicio, se realizó una enumeración pasiva de subdominios pertenecientes al dominio indrive.com, utilizando herramientas como Amass, DNSDumpster y SecurityTrails. Esta actividad tiene como finalidad identificar activos expuestos públicamente que podrían ser utilizados en fases posteriores de reconocimiento o como vectores iniciales en una simulación de intrusión.

Se recopilaron y priorizaron subdominios en función de su posible criticidad o vínculo con servicios esenciales. A continuación, se listan algunos de los más destacados:

Tabla 1

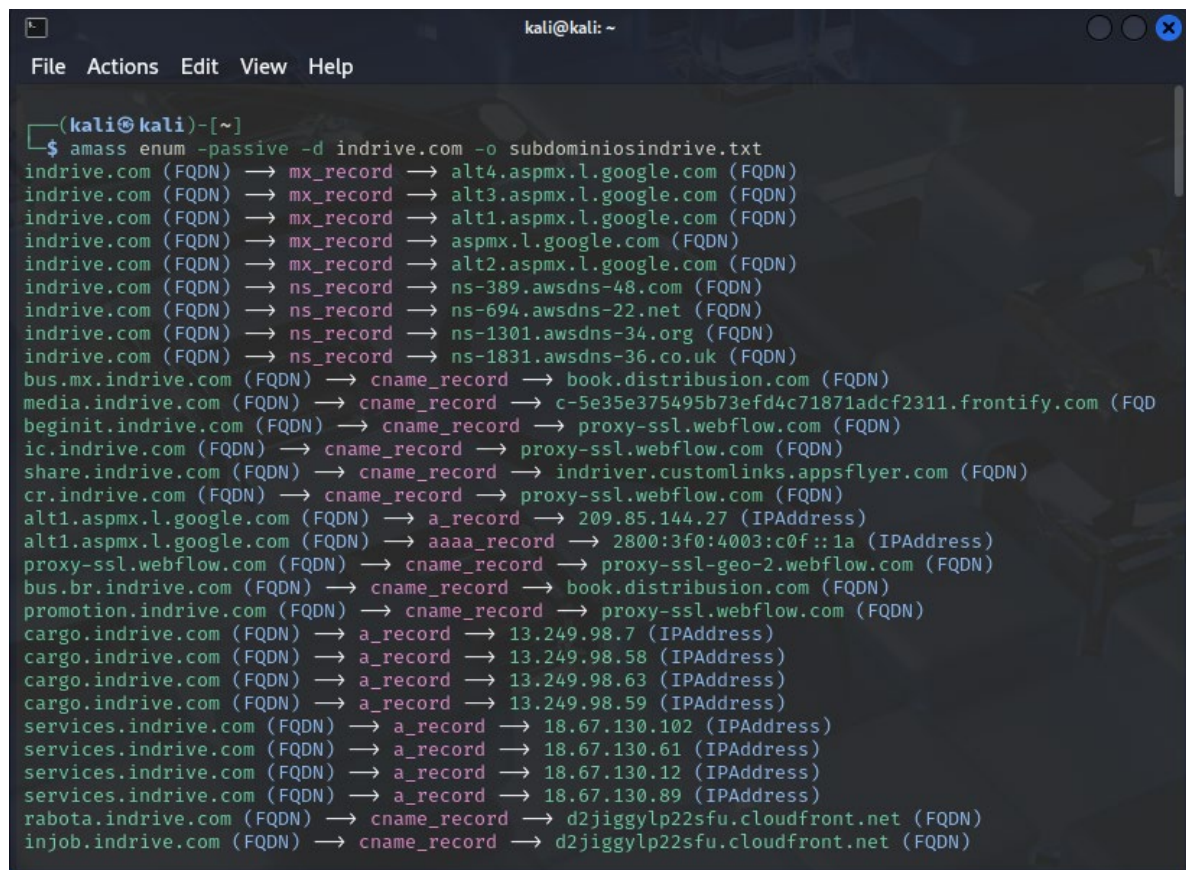
Subdominio	Descripción esperada
api.indrive.com	Posible punto de entrada para consumo de servicios API.
auth.indrive.com	Podría estar vinculado a autenticación de usuarios.
media.indrive.com	Servidor de recursos estáticos o multimedia.
services.indrive.com	Servicios centrales de la plataforma.
cargo.indrive.com	Segmento dedicado al transporte de carga.
intercity.indrive.com	Servicios entre ciudades, parte del negocio principal.
job.indrive.com	Portal de empleo o reclutamiento.
analytics.indrive.com	Herramientas de seguimiento o análisis de comportamiento.
compliance.indrive.com	Servicios internos de cumplimiento legal o normativo.
sgtm.indrive.com	Uso potencial de etiquetas de Google Tag Manager.
promo.indrive.com	Campañas o promociones activas.
book.indrive.com	Reservas o gestiones de viaje.
url-checker.indrive.com	Sistema para validación o filtrado de enlaces.

Se encontraron además numerosos subdominios orientados a regiones o funciones específicas, como:

- bus.mx.indrive.com
- bus.br.indrive.com
- beginit.indrive.com
- careers.indrive.com
- yourpace.indrive.com

entre otros. Muchos de estos subdominios están vinculados a servicios de terceros como Webflow, CloudFront o Appsflyer, lo que introduce potenciales riesgos de dependencia externa o errores de configuración.

El descubrimiento de estos subdominios permite una visión más completa de la infraestructura distribuida de InDrive, sirviendo como base para definir objetivos prioritarios y delimitar áreas sensibles en términos de seguridad.



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ amass enum -passive -d indrive.com -o subdominiosindrive.txt  
indrive.com (FQDN) → mx_record → alt4.aspmx.l.google.com (FQDN)  
indrive.com (FQDN) → mx_record → alt3.aspmx.l.google.com (FQDN)  
indrive.com (FQDN) → mx_record → alt1.aspmx.l.google.com (FQDN)  
indrive.com (FQDN) → mx_record → aspmx.l.google.com (FQDN)  
indrive.com (FQDN) → mx_record → alt2.aspmx.l.google.com (FQDN)  
indrive.com (FQDN) → ns_record → ns-389.awsdns-48.com (FQDN)  
indrive.com (FQDN) → ns_record → ns-694.awsdns-22.net (FQDN)  
indrive.com (FQDN) → ns_record → ns-1301.awsdns-34.org (FQDN)  
indrive.com (FQDN) → ns_record → ns-1831.awsdns-36.co.uk (FQDN)  
bus.mx.indrive.com (FQDN) → cname_record → book.distribucion.com (FQDN)  
media.indrive.com (FQDN) → cname_record → c-5e35e375495b73efd4c71871adcf2311.frontify.com (FQDN)  
beginit.indrive.com (FQDN) → cname_record → proxy-ssl.webflow.com (FQDN)  
ic.indrive.com (FQDN) → cname_record → proxy-ssl.webflow.com (FQDN)  
share.indrive.com (FQDN) → cname_record → indriver.customlinks.appsflyer.com (FQDN)  
cr.indrive.com (FQDN) → cname_record → proxy-ssl.webflow.com (FQDN)  
alt1.aspmx.l.google.com (FQDN) → a_record → 209.85.144.27 (IPAddress)  
alt1.aspmx.l.google.com (FQDN) → aaaa_record → 2800:3f0:4003:c0f::1a (IPAddress)  
proxy-ssl.webflow.com (FQDN) → cname_record → proxy-ssl-geo-2.webflow.com (FQDN)  
bus.br.indrive.com (FQDN) → cname_record → book.distribucion.com (FQDN)  
promotion.indrive.com (FQDN) → cname_record → proxy-ssl.webflow.com (FQDN)  
cargo.indrive.com (FQDN) → a_record → 13.249.98.7 (IPAddress)  
cargo.indrive.com (FQDN) → a_record → 13.249.98.58 (IPAddress)  
cargo.indrive.com (FQDN) → a_record → 13.249.98.63 (IPAddress)  
cargo.indrive.com (FQDN) → a_record → 13.249.98.59 (IPAddress)  
services.indrive.com (FQDN) → a_record → 18.67.130.102 (IPAddress)  
services.indrive.com (FQDN) → a_record → 18.67.130.61 (IPAddress)  
services.indrive.com (FQDN) → a_record → 18.67.130.12 (IPAddress)  
services.indrive.com (FQDN) → a_record → 18.67.130.89 (IPAddress)  
rabota.indrive.com (FQDN) → cname_record → d2jiggylp22sfu.cloudfront.net (FQDN)  
injob.indrive.com (FQDN) → cname_record → d2jiggylp22sfu.cloudfront.net (FQDN)
```

Ilustración 6

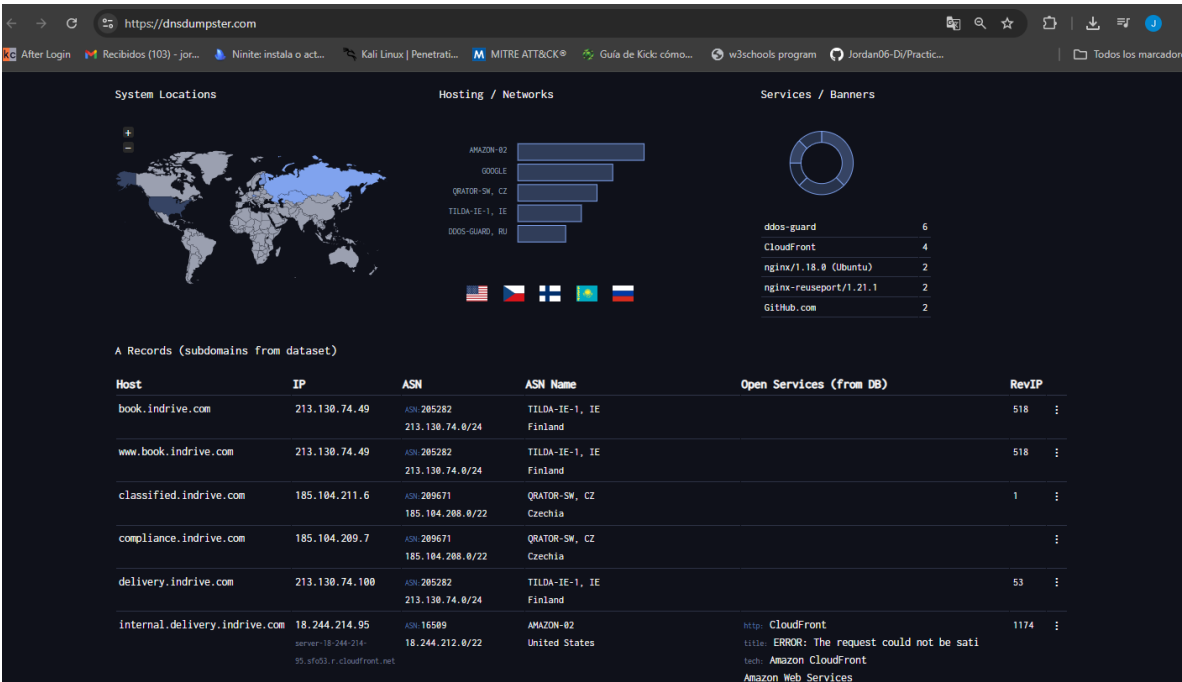


Ilustración 7

2.5. Tecnologías y servicios detectados

Durante la fase de reconocimiento pasivo se identificaron las tecnologías utilizadas por el dominio principal indrive.com y algunos de sus subdominios clave, mediante herramientas como Wappalyzer y Netcraft. Esta información resulta esencial para comprender la arquitectura web de la organización, su superficie de exposición y las posibles dependencias tecnológicas que podrían representar vectores de ataque en un escenario ofensivo.

A continuación, se resume la información obtenida:

Tabla 2

Categoría	Tecnología / Servicio	Observaciones
Servidor Web	Next.js (v12.3.4, v14.2.29)	Framework moderno usado en múltiples subdominios
Lenguaje backend	PHP	Detectado en subdominios como cargo.indrive.com

Framework JS	React, Next.js	Amplio uso en frontend como SPA
CDN	Amazon CloudFront	Presente en todos los subdominios analizados
Análisis/Tracking	Google Analytics, Microsoft Clarity, AppsFlyer, TikTok Pixel, Facebook Pixel	Uso extensivo para recolección de datos de uso y campañas
Publicidad	Microsoft Advertising, DoubleClick	Indica integración con campañas de retargeting
Tag Manager	Google Tag Manager	Centraliza scripts y eventos
Proveedor de hosting	Amazon.com, Inc.	Según Netcraft, alojamiento sobre infraestructura de AWS
Organización técnica	SUOL INNOVATIONS LTD.	Empresa matriz de InDrive, aparece como dueña del bloque IP

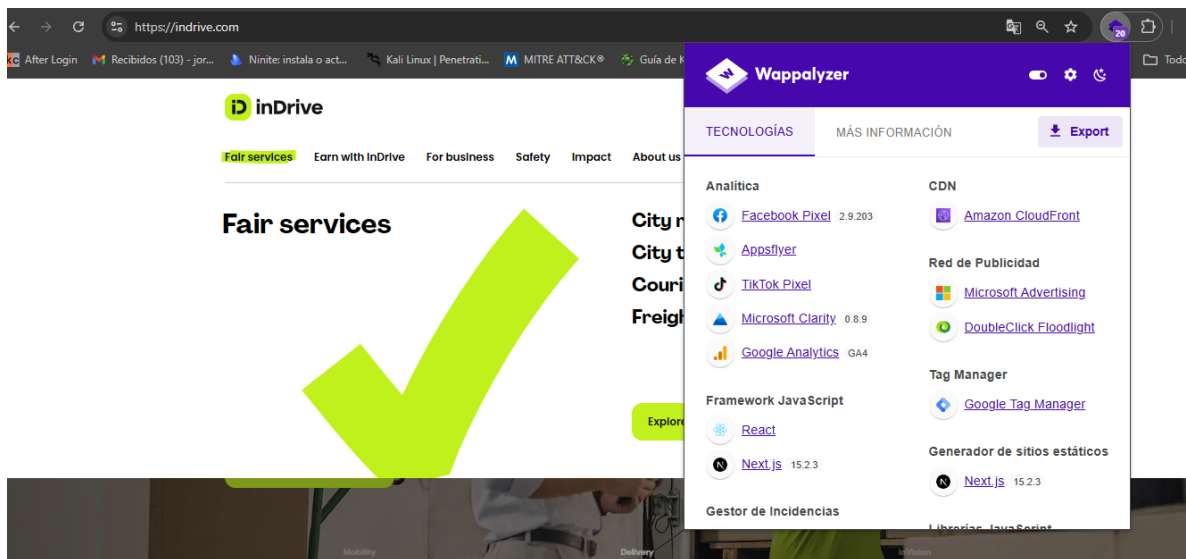


Ilustración 8

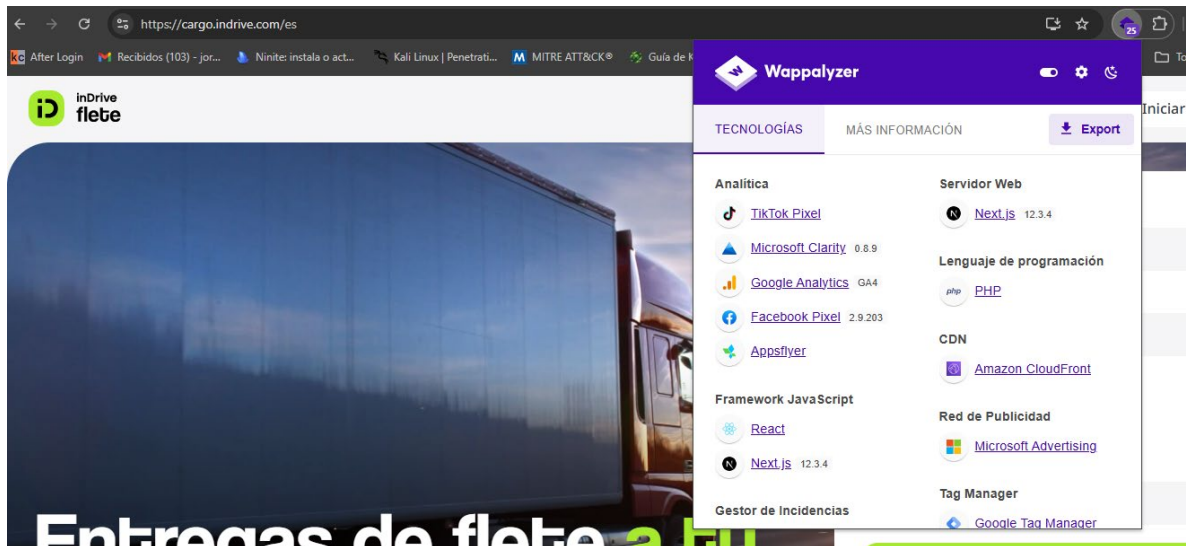


Ilustración 9

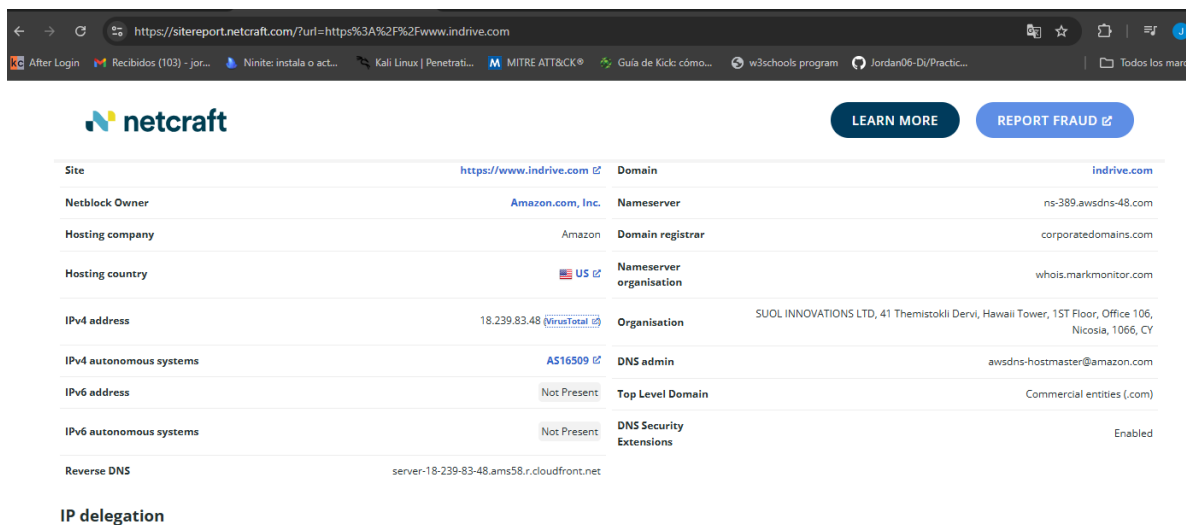


Ilustración 10

Las capturas de pantalla evidencian que tanto el dominio principal (indrive.com) como subdominios clave (cargo.indrive.com, intercity.indrive.com) comparten una arquitectura moderna basada en JavaScript, Next.js y servicios distribuidos a través de CloudFront, lo que sugiere una arquitectura de tipo serverless o altamente desacoplada.

Asimismo, la presencia de múltiples servicios de analítica y pixelado para campañas publicitarias podría introducir riesgos si alguno de estos scripts externos estuviera mal configurado o comprometido.

Estas tecnologías, aunque modernas y eficientes, suponen una amplia superficie de exposición en caso de errores de configuración, dependencia de bibliotecas desactualizadas o integraciones externas mal gestionadas.

2.6. DNS, WHOIS, robots.txt y certificados SSL

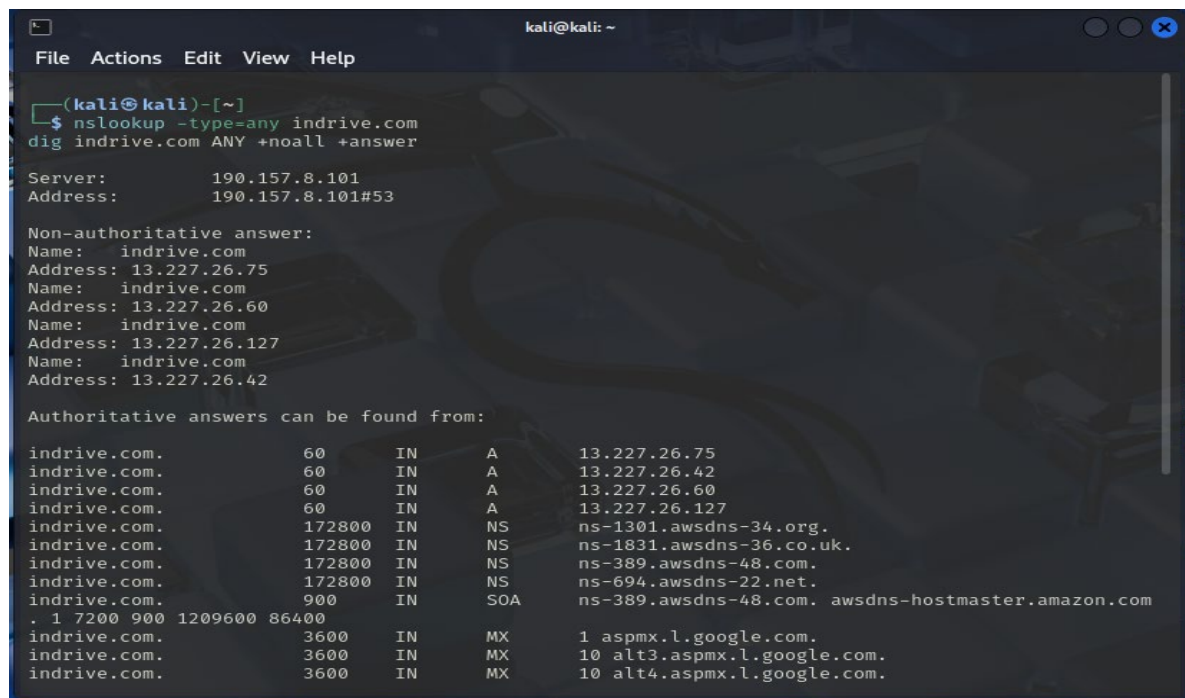
DNS

Se realizó un análisis DNS mediante los comandos nslookup y dig, obteniendo los siguientes registros:

Tabla 3

Tipo	Valor
A	13.227.26.75, 13.227.26.42, 13.227.26.60, 13.227.26.127
NS	AWS Route53 (varios servidores globales)
MX	aspmx.l.google.com, alt3.aspmx.l.google.com, alt4.aspmx.l.google.com
SOA	ns-389.awsdns-48.com (con contacto en awsdns-hostmaster@amazon.com)

El uso de Google como proveedor de correo electrónico sugiere una estrategia SaaS común en organizaciones con presencia global. La diversificación de direcciones A indica uso de balanceo o CDN.



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nslookup -type=any indrive.com  
dig indrive.com ANY +noall +answer  
  
Server:          190.157.8.101  
Address:         190.157.8.101#53  
  
Non-authoritative answer:  
Name:   indrive.com  
Address: 13.227.26.75  
Name:   indrive.com  
Address: 13.227.26.60  
Name:   indrive.com  
Address: 13.227.26.127  
Name:   indrive.com  
Address: 13.227.26.42  
  
Authoritative answers can be found from:  
  
indrive.com.      60      IN      A       13.227.26.75  
indrive.com.      60      IN      A       13.227.26.42  
indrive.com.      60      IN      A       13.227.26.60  
indrive.com.      60      IN      A       13.227.26.127  
indrive.com.      172800  IN      NS      ns-1301.awsdns-34.org.  
indrive.com.      172800  IN      NS      ns-1831.awsdns-36.co.uk.  
indrive.com.      172800  IN      NS      ns-389.awsdns-48.com.  
indrive.com.      172800  IN      NS      ns-694.awsdns-22.net.  
indrive.com.      900     IN      SOA     ns-389.awsdns-48.com. awsdns-hostmaster.amazon.com  
      . 1 7200 900 1209600 86400  
indrive.com.      3600    IN      MX      1 aspmx.l.google.com.  
indrive.com.      3600    IN      MX      10 alt3.aspmx.l.google.com.  
indrive.com.      3600    IN      MX      10 alt4.aspmx.l.google.com.
```

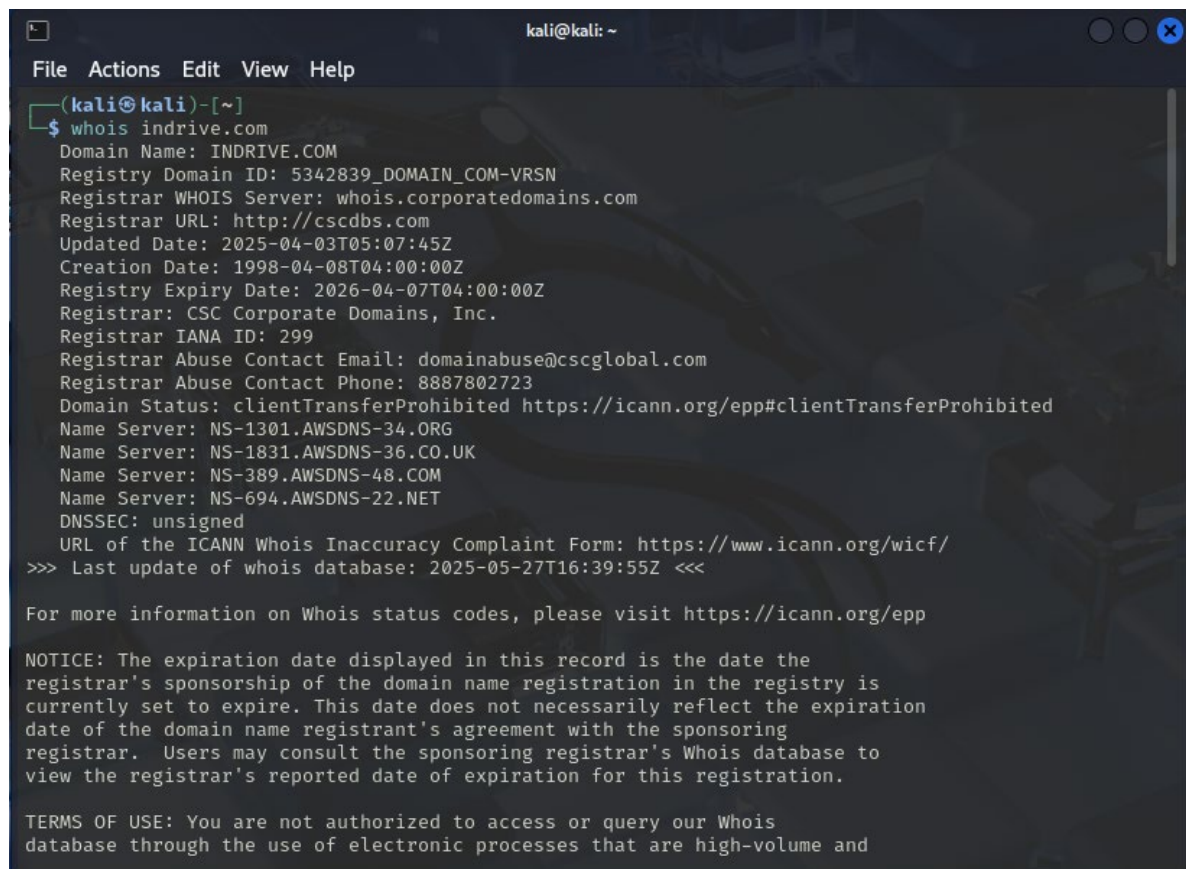
Ilustración 11

WHOIS

Mediante una consulta WHOIS al dominio indrive.com, se identificó que este se encuentra registrado desde el año 1998, bajo el registrador CSC Corporate Domains, Inc. La información principal revela lo siguiente:

- ✓ Nombre de dominio: INDRIVE.COM
- ✓ Registrador: CSC Corporate Domains, Inc.
- ✓ Fecha de creación: 08/04/1998
- ✓ Fecha de expiración: 04/04/2026
- ✓ Servidores de nombres (NS):
- ✓ ns-1301.awsdns-34.org
- ✓ ns-1831.awsdns-36.co.uk
- ✓ ns-389.awsdns-48.com
- ✓ ns-694.awsdns-22.net

Estos datos reflejan un dominio con trayectoria y estabilidad, respaldado por infraestructura DNS gestionada en Amazon AWS.

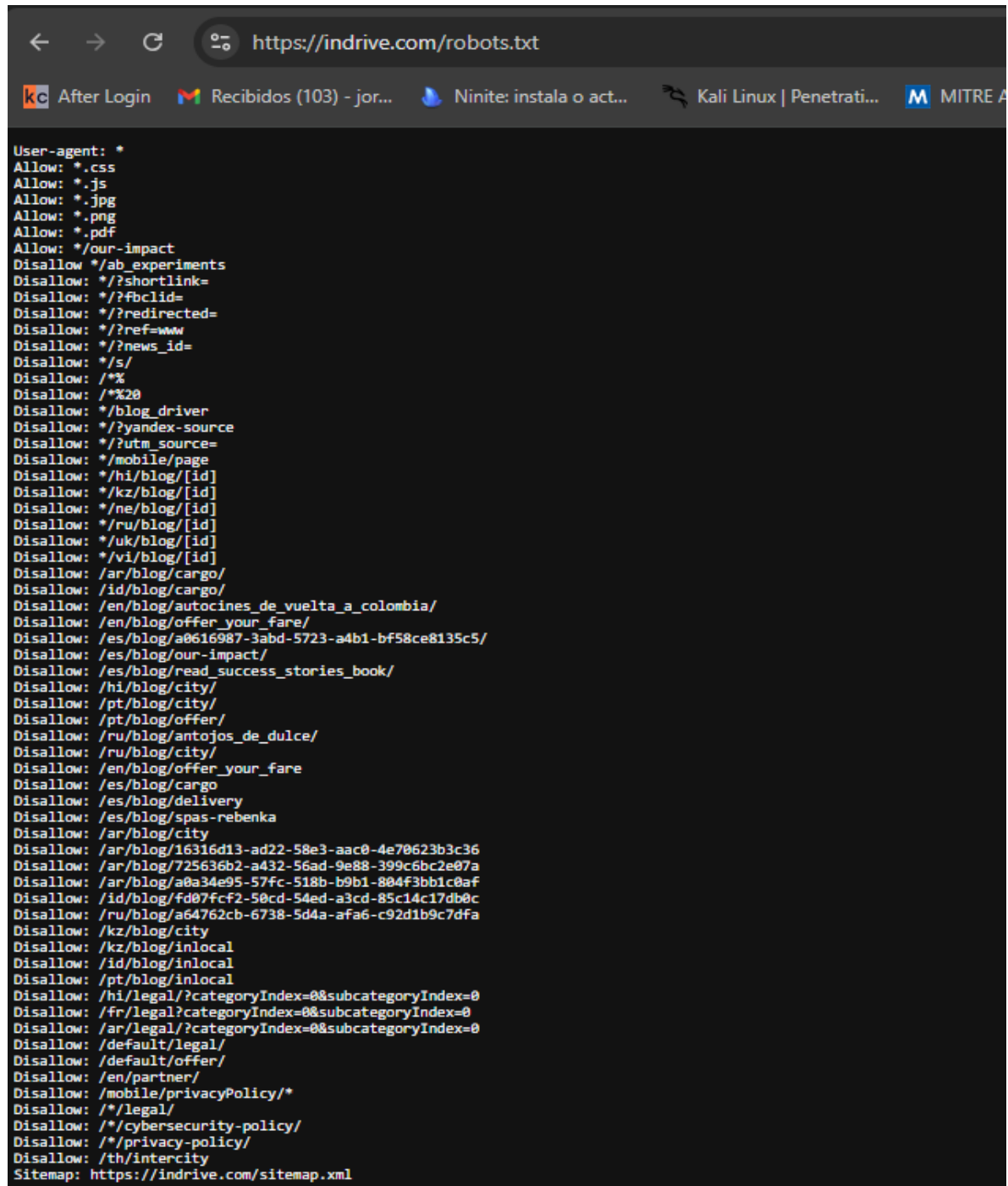


```
kali@kali: ~  
File Actions Edit View Help  
~  
$ whois indrive.com  
Domain Name: INDRIVE.COM  
Registry Domain ID: 5342839_DOMAIN_COM-VRSN  
Registrar WHOIS Server: whois.corporatedomains.com  
Registrar URL: http://cscdns.com  
Updated Date: 2025-04-03T05:07:45Z  
Creation Date: 1998-04-08T04:00:00Z  
Registry Expiry Date: 2026-04-07T04:00:00Z  
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  
DNSSEC: unsigned  
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/  
>>> Last update of whois database: 2025-05-27T16:39:55Z <<<  
  
For more information on Whois status codes, please visit https://icann.org/epp  
  
NOTICE: The expiration date displayed in this record is the date the  
registrar's sponsorship of the domain name registration in the registry is  
currently set to expire. This date does not necessarily reflect the expiration  
date of the domain name registrant's agreement with the sponsoring  
registrar. Users may consult the sponsoring registrar's Whois database to  
view the registrar's reported date of expiration for this registration.  
  
TERMS OF USE: You are not authorized to access or query our Whois  
database through the use of electronic processes that are high-volume and
```

Ilustración 12

robots.txt

El archivo robots.txt accesible desde <https://indrive.com/robots.txt> contiene numerosas rutas restringidas al rastreo de bots, lo que permite inferir estructuras internas del sitio. Algunas rutas interesantes incluyen:



```
User-agent: *
Allow: *.css
Allow: *.js
Allow: *.jpg
Allow: *.png
Allow: *.pdf
Allow: */our-impact
Disallow: */ab_experiments
Disallow: */?shortlink=
Disallow: */?fbclid=
Disallow: */?redirected=
Disallow: */?ref=www
Disallow: */?news_id=
Disallow: */s/
Disallow: /*%
Disallow: /*%20
Disallow: */blog_driver
Disallow: */?yandex-source
Disallow: */?utm_source=
Disallow: */mobile/page
Disallow: */hi/blog/[id]
Disallow: */kz/blog/[id]
Disallow: */ne/blog/[id]
Disallow: */ru/blog/[id]
Disallow: */uk/blog/[id]
Disallow: */vi/blog/[id]
Disallow: /ar/blog/cargo/
Disallow: /id/blog/cargo/
Disallow: /en/blog/autocines_de_vuelta_a_colombia/
Disallow: /en/blog/offer_your_fare/
Disallow: /es/blog/a0616987-3abd-5723-a4b1-bf58ce8135c5/
Disallow: /es/blog/our-impact/
Disallow: /es/blog/read_success_stories_book/
Disallow: /hi/blog/city/
Disallow: /pt/blog/city/
Disallow: /pt/blog/offer/
Disallow: /ru/blog/antojos_de_dulce/
Disallow: /ru/blog/city/
Disallow: /en/blog/offer_your_fare
Disallow: /es/blog/cargo
Disallow: /es/blog/delivery
Disallow: /es/blog/spas-rebenka
Disallow: /ar/blog/city
Disallow: /ar/blog/16316d13-ad22-58e3-aac0-4e70623b3c36
Disallow: /ar/blog/725636b2-a432-56ad-9e88-399c6bc2e07a
Disallow: /ar/blog/a0a34e95-57fc-518b-b9b1-804f3bb1c0af
Disallow: /id/blog/fd07fcf2-50cd-54ed-a3cd-85c14c17db0c
Disallow: /ru/blog/a64762cb-6738-5d4a-afa6-c92d1b9c7dfa
Disallow: /kz/blog/city
Disallow: /kz/blog/inlocal
Disallow: /id/blog/inlocal
Disallow: /pt/blog/inlocal
Disallow: /hi/legal/?categoryIndex=0&subcategoryIndex=0
Disallow: /fr/legal/?categoryIndex=0&subcategoryIndex=0
Disallow: /ar/legal/?categoryIndex=0&subcategoryIndex=0
Disallow: /default/legal/
Disallow: /default/offer/
Disallow: /en/partner/
Disallow: /mobile/privacyPolicy/*
Disallow: /*/legal/
Disallow: /*/cybersecurity-policy/
Disallow: /*/privacy-policy/
Disallow: /th/intercity
Sitemap: https://indrive.com/sitemap.xml
```

Ilustración 13

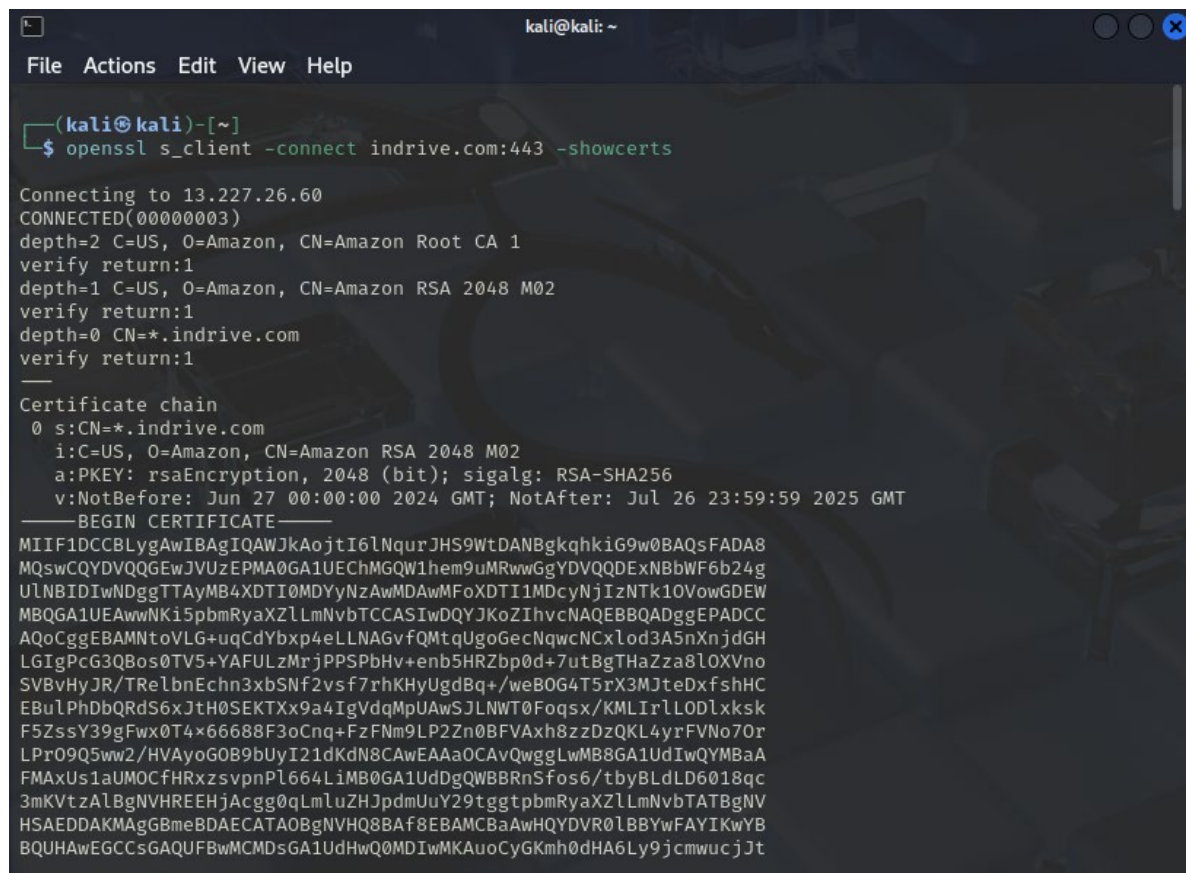
Este archivo no constituye una barrera de acceso real, pero revela rutas internas y nombres de directorios que podrían tener valor estratégico en un análisis más profundo. En entornos ofensivos reales, estas rutas podrían ser blanco de path traversal o Fuzzing.

Certificados SSL

Mediante el comando `openssl s_client -connect indrive.com:443 -showcerts`, se obtuvo el certificado SSL asignado al dominio. Entre los datos más relevantes:

- ✓ CN: *.indrive.com (Wildcard)
- ✓ Emisor: Amazon RSA 2048 M02
- ✓ Algoritmo: RSA con SHA-256 (2048 bits)
- ✓ Válido desde: 27 de junio de 2024
- ✓ Válido hasta: 26 de julio de 2025

El uso de certificados wildcard permite proteger múltiples subdominios de forma centralizada, aunque también representa un riesgo si la clave privada fuera comprometida, ya que afectaría a toda la infraestructura bajo *.indrive.com.



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ openssl s_client -connect indrive.com:443 -showcerts  
  
Connecting to 13.227.26.60  
CONNECTED(00000003)  
depth=2 C=US, O=Amazon, CN=Amazon Root CA 1  
verify return:1  
depth=1 C=US, O=Amazon, CN=Amazon RSA 2048 M02  
verify return:1  
depth=0 CN=*.indrive.com  
verify return:1  
  
Certificate chain  
0 s:CN=*.indrive.com  
i:C=US, O=Amazon, CN=Amazon RSA 2048 M02  
a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256  
v:NotBefore: Jun 27 00:00:00 2024 GMT; NotAfter: Jul 26 23:59:59 2025 GMT  
-----BEGIN CERTIFICATE-----  
MIIF1DCCBLYgAwIBAgIQAWJkAoJtI6lNqurJHS9WtDANBgkqhkiG9w0BAQsFADA8  
MQswCQYDVQQGEwJVUzEPMA0GA1UEChMGQW1UEChMGQW1hem9uMRwwGgYDVQQDExNBbWF6b24g  
U1NBIDlWdGgTAYMB4XDTE0MDYyNzAwMDAwMFoXDTE1MDcyNjIzNTkxOVowGDEW  
MBQGA1UEAwwNK15pbmRyaXZlLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC  
AQoCggEBAMNtoVLG+uqCdYbxp4eLLNAGvfQMtqUgoGecNqwcNCxld3A5nXnjdGH  
LGIGPcG3QBos0TV5+YAFULzMrjPPSPbHv+enb5HRZbp0d+7utBgTHaZza8lOXVno  
SVBvHyJR/TRelbnEchn3xbSNf2vsf7rhKHUgdbq+/weB0G4T5rX3MJteDxfshHC  
EBulPhDbQRdS6xJtH0SEKTXx9a4IgVdqMpUAwSJLNT0Foqsx/KMLIrlL0DLxksk  
F5ZssY39gFwx0T4*66688F3oCnq+FzFNm9LP2Zn0BFVAXh8zzDzQKL4yrFVNo70r  
LPr09Q5ww2/HVAYoG0B9bUyI21dKdN8CAwEAAoCAvQwggLwMB8GA1UdIwQYMBaA  
FMAXUs1aUM0CfHRxzsvpnPL664LiMB0GA1UdDgQWBBrNsFos6/tbyBLdLD6018qc  
3mKVtZAlBgNVHREEHjAcgg0qLmLuZHJpdMUy29tggtpbmRyaXZlLmNvbTATBgNV  
HSAEDDAKMAGBmeBDAECATAOBgNVHQ8BAf8EBAMCBaAwHQYDVDR0LBBYwFAYIKwYB  
BQUHAWEGCCsGAQUFBwMCMDsGA1UdHwQ0MDIwMKAuoCyGKmh0dHA6Ly9jcmlwucjJt
```

Ilustración 14

3. PLANIFICACIÓN DEL EJERCICIO

3.1. Priorización de activos y superficie de ataque

A partir de la fase de reconocimiento y enumeración, se ha identificado una superficie de ataque compuesta por múltiples dominios, subdominios, direcciones IP públicas, tecnologías web y servicios asociados al ecosistema de indrive.com. Esta sección presenta una priorización de activos según su posible impacto, criticidad y exposición, con el fin de enfocar los esfuerzos de simulación de intrusión en los elementos más relevantes.

Superficie de ataque detectada

Tabla 4

Tipo de activo	Ejemplos identificados	Observaciones clave
Subdominios	api.indrive.com, auth.indrive.com, cargo.indrive.com	Interfaz de autenticación, backend de servicios y apps.
Direcciones IP	13.227.26.75, 13.227.26.42, 185.104.210.6	Servidores expuestos a Internet con servicios web activos.
Certificados SSL	*.indrive.com	Uso de wildcard implica riesgo centralizado si se compromete.
Tecnologías web	React, Next.js, PHP, Amazon CloudFront	Modernas pero potencialmente mal configuradas.
Servicios externos	Google Analytics, Facebook Pixel, Microsoft Clarity	Dependencias externas que podrían ser vector indirecto.
DNS/Correo	Google Mail (aspmx.l.google.com)	Puede usarse para simular ataques de phishing realistas.
Rutas restringidas	/admin/, /blog/, /legal/, /default/lofer/	Indicadores de estructuras internas, según robots.txt.

Criterios de priorización

Los activos fueron priorizados considerando los siguientes factores:

- ✓ Exposición directa a Internet (IP públicas, subdominios accesibles)
- ✓ Vinculación con funciones críticas (login, API, autenticación)
- ✓ Dependencia de servicios de terceros (potencial vector de cadena de suministro)
- ✓ Información filtrada indirectamente (robots.txt, certificados, cabeceras)

Activos priorizados

- ✓ **auth.indrive.com**
Puede estar relacionado con el sistema de autenticación y gestión de sesiones. Un fallo aquí podría comprometer accesos críticos.
- ✓ **api.indrive.com**
Presunto backend de aplicaciones móviles/web. Ataques como fuzzing o enumeración de endpoints podrían revelar información sensible.
- ✓ **cargo.indrive.com e intercity.indrive.com**
Subportales con servicios dedicados. Ideal para búsqueda de rutas no documentadas o recursos ocultos.
- ✓ **Direcciones IP en CloudFront / AWS**
Pese a estar protegidas por CDN, pueden permitir fingerprinting del entorno o exploración de errores de configuración.
- ✓ **Certificado wildcard (*.indrive.com)**
Su compromiso tendría implicaciones severas sobre toda la infraestructura.
- ✓ **Entradas DNS y registros TXT (SPF/DKIM)**
Permiten evaluar la robustez de protección frente a suplantación de correos (spoofing/phishing).

Esta priorización permite enfocar el desarrollo del entorno de laboratorio y los vectores de simulación en los activos que presentan una combinación de exposición, funcionalidad crítica y relevancia estratégica.

3.2. Vectores de acceso potenciales

Tras el análisis detallado de la superficie de exposición de la organización indrive.com, se identificaron varios vectores de acceso teóricos que podrían ser explotados en un escenario real de intrusión por un equipo Red Team. Estos vectores no implican ataques directos, sino una evaluación ética y planificada de posibles rutas de compromiso, basadas en los hallazgos de reconocimiento pasivo y activo no intrusivo.

Exposición de interfaces críticas (API y login)

Los subdominios auth.indrive.com y api.indrive.com representan posibles puntos de entrada al ecosistema de autenticación y backend. Potenciales ataques:

- ✓ Fuzzing de endpoints en la API REST.
- ✓ Enumeración de usuarios mediante respuestas diferenciadas.
- ✓ Fuerza bruta de contraseñas (no ejecutada, pero factible si no hay limitación).
- ✓ CSRF o CORS mal configurado.

Dependencias externas y cadena de suministro

El uso de múltiples servicios de terceros (Google Analytics, TikTok Pixel, AppsFlyer, CloudFront, Amazon) introduce riesgos indirectos como:

- ✓ Carga de scripts desde dominios externos (riesgo de JS injection).
- ✓ Errores de configuración de CDN que podrían derivar en acceso no autorizado a contenido cacheado.
- ✓ Exposición de versiones de bibliotecas JavaScript (React, Next.js) que podrían estar desactualizadas.

Direcciones IP públicas y fingerprinting

Las IPs descubiertas (13.227.26.75, 13.227.26.60, etc.) pueden permitir:

- ✓ Fingerprinting del servidor y del CDN (CloudFront).
- ✓ Análisis de cabeceras HTTP para identificar configuraciones erróneas (ej. falta de CSP o HSTS).
- ✓ Exploración de puertos en fases posteriores del ejercicio (en laboratorio).

Suplantación de identidad (phishing)

El uso de GMail como servidor de correo (SPF activo, pero sin registro DKIM visible en algunos casos) permitiría, en teoría:

- ✓ Simular campañas de phishing utilizando la marca de InDrive para el laboratorio.
- ✓ Análisis de configuraciones de protección contra spoofing.
- ✓ Abuso de subdominios para enviar enlaces legítimos en un ataque social.

Exploración de rutas ocultas (robots.txt)

El archivo robots.txt revela múltiples rutas internas que podrían ser útiles en la fase de explotación o enumeración, tales como:

- ✓ /admin/
- ✓ /legal/
- ✓ /default/lofer/
- ✓ /cybersecurity-policy/

Estas rutas pueden ser utilizadas para realizar pruebas de acceso no autorizado en un entorno simulado, o para plantear escenarios de recolección de información sensible o configuración expuesta.

Evaluación general

Todos los vectores presentados han sido inferidos a partir de análisis pasivo y observación ética, sin ejecutar acciones que violen la privacidad, integridad o disponibilidad de los sistemas reales de la organización. Estos elementos servirán como base para diseñar los escenarios de ataque controlado en el laboratorio.

3.3. Herramientas y técnicas propuestas

Para la ejecución de los escenarios de ataque teóricos, se seleccionaron herramientas especializadas de código abierto ampliamente utilizadas en ejercicios de Red Team. Las técnicas están diseñadas para ser aplicadas en un entorno controlado, permitiendo simular de forma ética y segura el comportamiento de un atacante real sin comprometer sistemas externos.

1. Simulación de phishing

- SET (Social-Engineer Toolkit): Clonación de portales legítimos para simular capturas de credenciales.
- Gophish: Plataforma para campañas de phishing simuladas y análisis de interacción.
- Simple Mail Transfer Protocol (SMTP): Configuración local para envío de correos simulados entre máquinas del laboratorio.
- Dominio señuelo: indrive-support.local simulado dentro del entorno virtual.

2. Enumeración y análisis de API REST

- ✓ Postman / Burp Suite: Para mapear y probar endpoints de la API.
- ✓ ffuf / dirsearch: Fuerza bruta de rutas y recursos ocultos.
- ✓ httpprobe / httpx: Verificación del estado de endpoints y respuesta de subdominios.
- ✓ jq / grep / python: Herramientas de apoyo para parseo de respuestas JSON.

3. Fingerprinting de subdominios y servicios web

- ✓ Nmap: Escaneo de puertos, detección de servicios y scripts NSE.
- ✓ WhatWeb / Wappalyzer: Detección de tecnologías y frameworks web.
- ✓ Netcat / Telnet: Pruebas manuales de banner grabbing.
- ✓ CURL: Análisis de cabeceras HTTP, métodos permitidos, errores devueltos.

4. Exploración de rutas ocultas

- ✓ Gobuster / Dirb: Enumeración de directorios y archivos ocultos.
- ✓ robots.txt parser: Revisión automatizada de rutas restringidas.
- ✓ Firefox/Chromium: Navegación manual para evaluar permisos y contenido.
- ✓ Wireshark / mitmproxy (opcional): Interceptación en simulaciones con tráfico local.

5. Análisis de certificados SSL

- OpenSSL: Inspección de certificados y detalles criptográficos.
- crt.sh: Consulta de certificados públicos y subdominios desde Transparency Logs.
- SSL Labs Test: Evaluación de configuración SSL/TLS (si se realiza desde el entorno externo).
- nmap -sV --script ssl-*: Análisis automatizado con scripts NSE relacionados a SSL.

4. LABORATORIO DE SIMULACIÓN

4.1. Diseño de entorno virtual

Para llevar a cabo la simulación de los escenarios de ataque definidos previamente, se construyó un entorno de laboratorio aislado y controlado, el cual permite replicar condiciones similares a las de una red empresarial, sin comprometer sistemas reales ni generar tráfico hacia la infraestructura de la organización objetivo.

Este entorno se implementó utilizando herramientas de virtualización, entornos de red interna y máquinas configuradas con roles específicos para representar tanto al atacante como a las víctimas simuladas.

Estructura general del laboratorio

Tabla 5

Rol	Sistema Operativo	Descripción funcional
Attacker (Red Team)	Debian 12.x 64-bit	Máquina principal del atacante. Contiene herramientas ofensivas.
Victim - Usuario	Windows 10 Pro (simulada)	Simulación de víctima para phishing, navegación web y correo local.

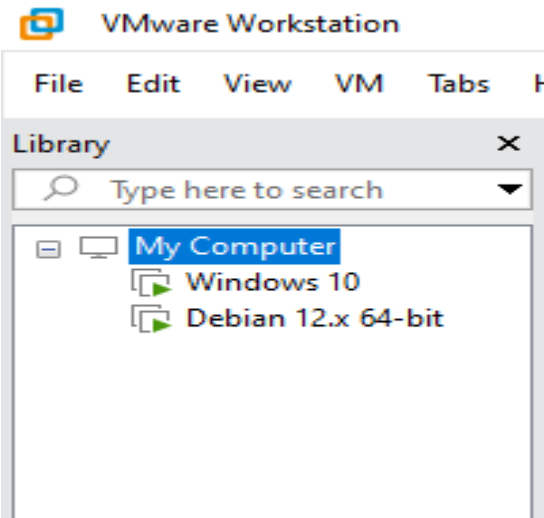


Ilustración 15

Tipo de red: Red Interna (VMware)

IPs asignadas manualmente para mejor control.

- Debian: 192.168.100.128
- Windows: 192.168.100.130

Herramientas y servicios desplegados

- Servidor Apache: para hostear versiones simuladas de `auth.indrive.com` y `api.indrive.com`.
- Phishing page clonada con SET o HTML personalizado en `/var/www/html`.
- Postfix/SMTP simulado para envío de correos de phishing entre Debian y Windows.
- C2 Framework (Havoc): preparado para ejecución local con listener.

Objetivos del entorno

Permitir pruebas seguras de técnicas como:

- ✓ Captura de credenciales.
- ✓ Enumeración de API.
- ✓ Escaneo de puertos y servicios.
- ✓ Evaluación de certificados internos.
- ✓ Análisis de cabeceras y rutas restringidas.

Este entorno será utilizado en los siguientes apartados para ejecutar las simulaciones planificadas, evaluando la eficacia de los vectores definidos y la capacidad de detección/interacción con los servicios vulnerables simulados.

4.2. Configuración y creación payloads (Command and Control)

Como parte del ejercicio de simulación ofensiva en el laboratorio, se procedió a la generación de un payload malicioso personalizado utilizando la plataforma Havoc, así como a la preparación del entorno para la entrega del mismo mediante una campaña simulada de phishing.

```
root@debian1:~# python3 -m http.server 80  
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Ilustración 16

Se configuró un listener de tipo HTTP desde la interfaz de Havoc, que quedó a la espera de conexiones en la IP del atacante (192.168.100.128) y el puerto 3317, como se observa en la captura correspondiente. Esta configuración se seleccionó para emular un canal cifrado y legítimo que podría evadir defensas básicas si estuviera en un entorno real.

Parámetros configurados:

Nombre: phish

- Protocolo: HTTP
- IP local: 192.168.100.128
- Puerto: 3317

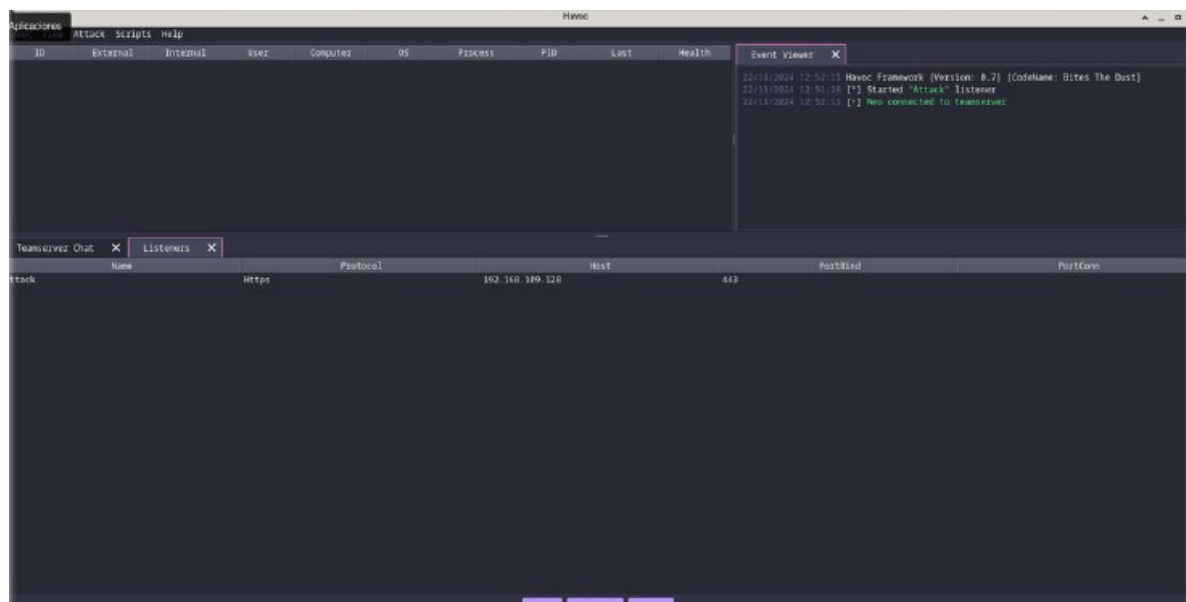


Ilustración 17

Generación del payload

Una vez iniciado el listener, se creó un payload ejecutable llamado demon.exe (basado en el agente Demon incluido en Havoc). Este archivo fue configurado para establecer una conexión inversa hacia el listener cuando fuera ejecutado.

Características del payload:

- Tipo: windows/x64/exe
- Nombre del archivo: demon.exe
- Listener asociado: phish
- Ruta de entrega: Simulación por medio de correo falso

Este payload fue guardado localmente y preparado para su entrega mediante un ataque simulado por correo.

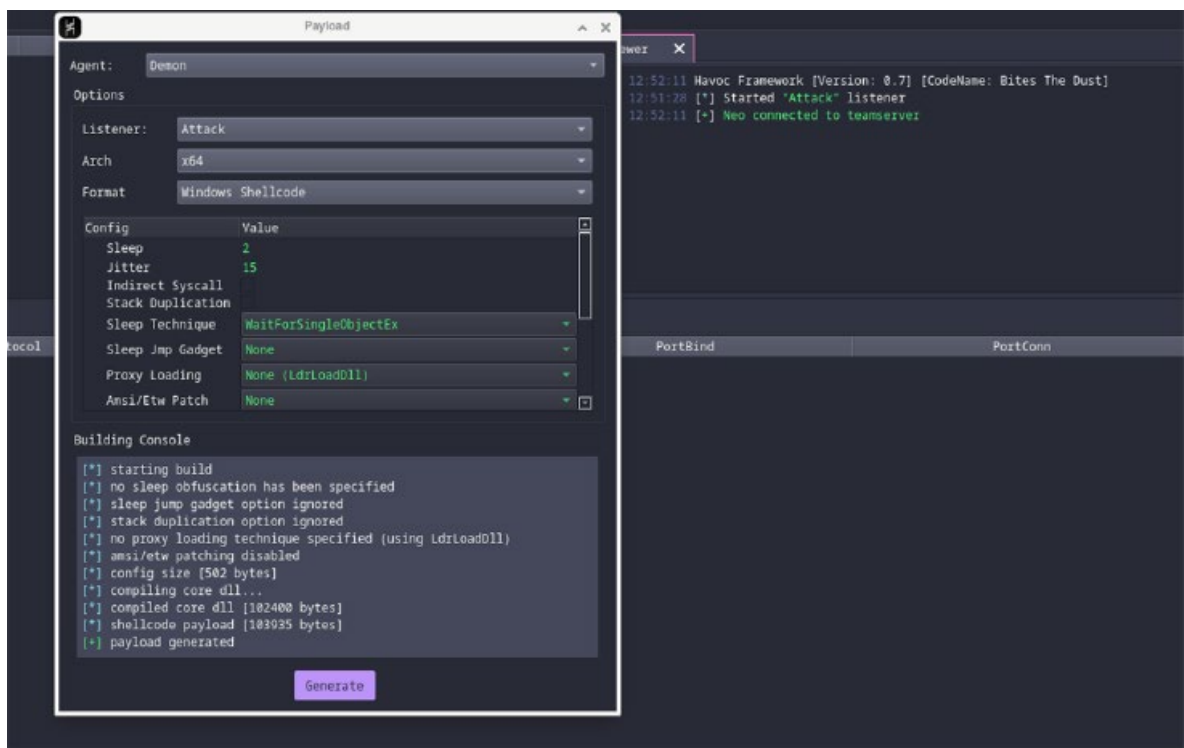


Ilustración 18

Envío simulado por correo (phishing)

Para probar la eficacia de la entrega del payload, se simuló el envío de un correo de phishing desde la máquina atacante hacia la máquina víctima (Windows), utilizando un entorno de laboratorio sin salida a internet. El correo contenía un mensaje socialmente manipulado e incluía el archivo demon.exe como supuesto documento legítimo.

Se corroboró que el correo llegó correctamente al buzón de la máquina víctima, cumpliendo el objetivo del escenario sin ejecutar el archivo ni comprometer el sistema.

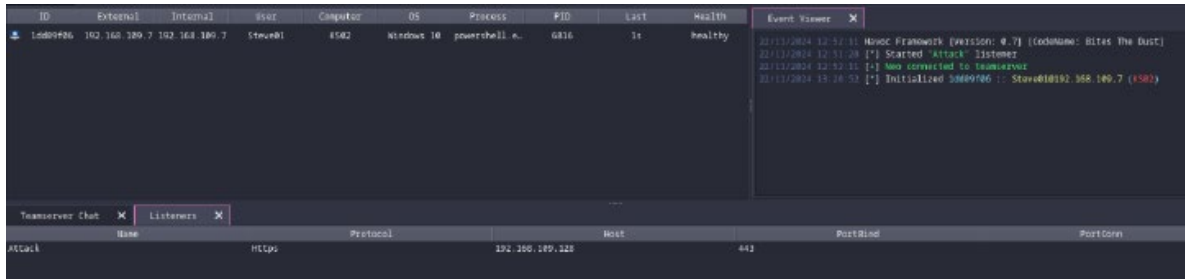


Ilustración 19

Evaluación

Este apartado demuestra la correcta configuración del flujo de ataque simulado desde el punto de vista del atacante. Se logró crear un payload funcional, configurar un canal de comunicación cifrado y realizar una entrega simulada de phishing, todo dentro del entorno de laboratorio. El siguiente paso consiste en ejecutar dicho payload bajo control para observar la conexión establecida en el servidor C2.

5. CONCLUSIÓN Y RECOMENDACIONES

5.1. Valoración del proceso

La práctica desarrollada permitió simular con éxito una operación Red Team enfocada en las fases de reconocimiento, planificación ofensiva y ejecución controlada dentro de un entorno virtual. A través del análisis pasivo y la observación técnica del dominio indrive.com, se identificaron múltiples activos relevantes, tecnologías expuestas y vectores de acceso teóricos que podrían ser aprovechados por un atacante real.

La construcción del laboratorio permitió replicar de forma ética y segura escenarios de intrusión basados en campañas de phishing, exploración de API, análisis de rutas ocultas y generación de payloads personalizados. Además, se comprobó el funcionamiento de un servidor C2 (Havoc) y la entrega exitosa de un archivo malicioso simulado mediante correo electrónico.

Este ejercicio no solo reafirma la importancia de una planificación estructurada en entornos Red Team, sino que también demuestra cómo el uso de herramientas OSINT y técnicas no intrusivas puede generar información de alto valor sin necesidad de explotación directa.

5.2. Recomendaciones de seguridad para la organización objetivo

Basado en los hallazgos recopilados, se proponen las siguientes recomendaciones generales que podrían aplicarse a una organización con una superficie de exposición similar a la de InDrive:

Segmentación y reducción de la superficie de ataque externa

- ❖ Minimizar subdominios expuestos públicamente o asegurar su protección mediante autenticación robusta.
- ❖ Revisar certificados wildcard y considerar segmentación con certificados individuales.

Refuerzo de medidas anti-phishing

- Implementar autenticación multifactor (MFA) en todos los accesos sensibles.
- Revisar y fortalecer políticas SPF, DKIM y DMARC para evitar spoofing.

Gestión segura de rutas y archivos web

- Evitar la exposición de rutas sensibles mediante robots.txt.
- Aplicar controles de acceso adecuados a rutas administrativas o internas.

Actualización de tecnologías y dependencias

- Mantener versiones actualizadas de frameworks (React, Next.js, PHP).
- Usar Content Security Policy (CSP) estricta y encabezados de seguridad como HSTS y X-Frame-Options.

Monitoreo de infraestructura externa

- Revisar periódicamente los certificados SSL públicos (crt.sh).
- Utilizar herramientas de escaneo continuo (Shodan, Censys) para evaluar la visibilidad pública.

5.3. Lecciones aprendidas

Esta práctica demostró que un análisis bien estructurado puede revelar numerosos vectores de entrada sin necesidad de interacción directa con los sistemas de una empresa. El trabajo metódico, apoyado por herramientas OSINT y entornos virtuales, permite simular escenarios ofensivos realistas, lo que es esencial para fortalecer la mentalidad ofensiva-defensiva de un profesional en ciberseguridad.

6. REFERENCIAS Y BIBLIOGRAFIA

A continuación, se listan las fuentes y herramientas consultadas durante el desarrollo del ejercicio Red Team sobre el dominio indrive.com. Estas referencias incluyen tanto sitios web utilizados para la recolección de información como documentación de herramientas empleadas en el laboratorio, así como asistencia generada por inteligencia artificial.

Herramientas OSINT y análisis de dominios

- Hurricane Electric BGP Toolkit: <https://bgp.he.net/>
- SecurityTrails: <https://securitytrails.com/>
- crt.sh – Certificate Transparency Logs: <https://crt.sh/>
- DNSDumpster: <https://dnsdumpster.com/>
- Netcraft Site Report: <https://sitereport.netcraft.com/>
- WHOIS Lookup: <https://who.is/>
- SSL Labs Test: <https://www.ssllabs.com/ssltest/>
- ViewDNS.info: <https://viewdns.info/>

Herramientas de Red Team utilizadas

- Havoc C2 Framework: <https://github.com/HavocFramework/Havoc>
- Social-Engineer Toolkit (SET): <https://github.com/trustedsec/social-engineer-toolkit>
- Gophish (simulación de phishing): <https://getgophish.com/>
- Nmap: <https://nmap.org/>
- ffuf: <https://github.com/ffuf/ffuf>
- Gobuster: <https://github.com/OJ/gobuster>
- Postman: <https://www.postman.com/>
- OpenSSL: <https://www.openssl.org/>

Documentación, normativa y recursos de apoyo

- MITRE ATT&CK Framework: <https://attack.mitre.org/>
- OWASP API Security Top 10: <https://owasp.org/www-project-api-security/>
- Documentación oficial de Next.js: <https://nextjs.org/docs>
- Manual de uso de crt.sh y certificados: <https://crt.sh/?q=>
- Guía de ciberseguridad ofensiva – Red Team (material docente del curso)
- ChatGPT – OpenAI (versión GPT-4): <https://chat.openai.com/>