

EJERCICIO FINAL DE RED TEAM

INFORME PREPARADO POR: MONICA LICEA CASTRO

OBJETIVO: AIRBNB.COM

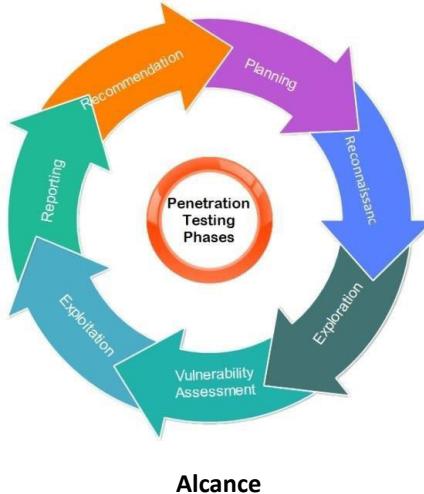


Preparado en: mayo de 2025

Planificación y reconocimiento de la entidad Airbnb.com

Objetivo

El objetivo principal de este análisis es identificar y mapear los activos digitales públicos de esta entidad para comprender mejor su superficie de exposición. Esto incluye la recolección pasiva de información, la enumeración de dominios y subdominios, la identificación de rangos de red y sistemas autónomos relacionados. No se llevarán a cabo acciones agresivas, pruebas de penetración ni escaneos activos que puedan comprometer los sistemas. Todo el análisis será de carácter informativo y enfocado a la simulación de una fase de reconocimiento previa a un test de intrusión ético o una auditoría de ciberseguridad.



Alcance

El alcance de este análisis se limita a los activos públicamente disponibles relacionados con esta entidad. Esto incluye:

- Dominios y subdominios oficiales de la empresa
- Información sobre IPs y rangos de red asociados
- Sistemas autónomos registrados a nombre de la empresa o sus filiales
- Empresas subsidiarias o marcas comerciales operadas por la misma entidad

No se incluirán activos de terceros, proveedores externos ni activos en la nube no identificables como propiedad de la empresa objetivo.

He seleccionado como objetivo a Airbnb Inc., una empresa tecnológica global con una presencia digital significativa y una estructura pública visible, lo que la convierte en un objetivo ideal para un análisis OSINT (Open Source Intelligence).

Airbnb es una plataforma fundada en 2008 que conecta a anfitriones con personas que buscan alojamiento a corto plazo en todo el mundo. Con operaciones en más de 190 países, su presencia online es extensa, y su infraestructura digital incluye múltiples subdominios, servicios en la nube, y aplicaciones móviles, además de haber adquirido otras compañías como HotelTonight.

A diferencia de empresas extremadamente grandes o con infraestructura más distribuida y compleja como Shopify, Airbnb ofrece un equilibrio más manejable entre visibilidad pública de activos digitales y profundidad técnica, permitiendo cumplir con los objetivos del ejercicio dentro del tiempo y recursos disponibles. Su enfoque tecnológico, junto con la transparencia de muchas de sus propiedades digitales, facilita la identificación de dominios, subdominios, rangos IP y sistemas autónomos mediante herramientas pasivas. Este reconocimiento se realizará exclusivamente con técnicas OSINT legales y no intrusivas, centradas en recolección pasiva de información pública accesible en internet.

- **Nombre:** Airbnb Inc.
- **Sector:** Alquileres a corto plazo / Plataforma tecnológica
- **Sitio oficial:** <https://www.airbnb.com>
- **Sede:** San Francisco, California, USA.
- **Fundación:** 2008.
- **Afiladas y marcas asociadas:**
 - HotelTonight (adquirida en 2019).
 - Lux (Airbnb Luxe).
 - Airbnb Experiences.

Objetivo: Identificar activos públicos que puedan ser relevantes para un atacante: dominios, subdominios, rangos de IP, ASNs, etc.

```
osboxes@osboxes:~/análisis_airbnb$ nslookup airbnb.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   airbnb.com
Address: 54.243.237.216
Name:   airbnb.com
Address: 44.223.197.210
Name:   airbnb.com
Address: 34.231.2.231
```

```
osboxes@osboxes:~/análisis_airbnb$ host airbnb.com
airbnb.com has address 34.231.2.231
airbnb.com has address 54.243.237.216
airbnb.com has address 44.223.197.210
airbnb.com mail is handled by 5 alt2.aspmx.l.google.com.
airbnb.com mail is handled by 10 alt3.aspmx.l.google.com.
airbnb.com mail is handled by 5 alt1.aspmx.l.google.com.
airbnb.com mail is handled by 1 aspmx.l.google.com.
airbnb.com mail is handled by 10 alt4.aspmx.l.google.com.
```

Igualmente aparece información relevante para subdominios como los que aparecen a continuación:

```
osboxes@osboxes:~/análisis_airbnb$ nslookup api.airbnb.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
api.airbnb.com canonical name = san.airbnb.com.edgekey.net.
san.airbnb.com.edgekey.net canonical name = e118243.a.akamaiedge.net.
Name:   e118243.a.akamaiedge.net
Address: 2.20.187.67
Name:   e118243.a.akamaiedge.net
Address: 2.20.187.82
Name:   e118243.a.akamaiedge.net
Address: 2.20.187.83
Name:   e118243.a.akamaiedge.net
Address: 2.20.187.64
Name:   e118243.a.akamaiedge.net
Address: 2.20.187.80
Name:   e118243.a.akamaiedge.net
Address: 2.20.187.66
Name:   e118243.a.akamaiedge.net
Address: 2.20.187.72
Name:   e118243.a.akamaiedge.net
Address: 2.20.187.59
Name:   e118243.a.akamaiedge.net
Address: 2.20.187.65
```

```
osboxes@osboxes:~/análisis_airbnb$ nslookup press.airbnb.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
press.airbnb.com canonical name = w.airbnb.com.edgekey.net.
w.airbnb.com.edgekey.net canonical name = e74147.a.akamaiedge.net.
Name:   e74147.a.akamaiedge.net
Address: 23.33.143.115
Name:   e74147.a.akamaiedge.net
Address: 23.33.143.80
```

Durante el análisis de direcciones IP asociadas a Airbnb.com, se identificó que estas pertenecen a bloques IP dentro de los sistemas autónomos **AS14618** y **AS16509**, ambos registrados a nombre de **Amazon.com, Inc.**. Esto indica que Airbnb aloja parte importante de su infraestructura web en **Amazon Web Services (AWS)**, una práctica común entre empresas tecnológicas por la escalabilidad, seguridad y distribución global que ofrece esta plataforma. En particular, el ASN **AS16509** está vinculado con la infraestructura moderna y global de AWS, lo que sugiere el uso de servicios en la nube como EC2, CloudFront o S3. Esta información es clave para comprender la superficie expuesta y los servicios potenciales involucrados.

The screenshot shows the Hurricane Electric BGP Toolkit interface for the domain `airbnb.com`. The top navigation bar includes the HE logo, the URL `airbnb.com`, and a search bar. Below the search bar is a menu with tabs: `Quick Links`, `DNS Info`, `Website Info`, `IP Info`, `Whois`, and `RDAP`. The `IP Info` tab is currently active, displaying a detailed route map. The map shows the path from the external IP address `44.223.197.210` through various routers and ASes to the final destination at `54.240.0.0/12`. The ASes involved are `AS14618` and `AS16509`, both of which are associated with `Amazon.com, Inc.`.

airbnb.com

Quick Links | DNS Info | Website Info | IP Info | Whois | RDAP

BGP Toolkit Home
BGP Prefix Report
BGP Peer Report
Super Traceroute
Super Looking Glass
Exchange Report
Bogon Routes
World Report
Multi Origin Routes
DNS Report
Top Host Report
Internet Statistics
Looking Glass
Network Tools App
Free IPv6 Tunnel
IPv6 Certification
IPv6 Progress
Going Native
Contribute Data
Credits
About Us

Domain Name: AIRBNB.COM
Registry Domain ID: 1512196199_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: https://www.markmonitor.com
Updated Date: 2024-10-11T18:52:35Z
Creation Date: 2008-08-05T07:29:00Z
Registry Expiry Date: 2026-08-05T07:29:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: DNS1.P08.NSONE.NET
Name Server: DNS2.P08.NSONE.NET
Name Server: DNS3.P08.NSONE.NET
Name Server: DNS4.P08.NSONE.NET
Name Server: NS-1453.AWSDNS-53.ORG
Name Server: NS-1932.AWSDNS-49.CO.UK
Name Server: NS-474.AWSDNS-59.COM
Name Server: NS-558.AWSDNS-05.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-03-25T16:48:11Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

Al consultar los registros RDAP del dominio airbnb.com a través del servicio de Hurricane Electric, se observa que el dominio está registrado bajo el identificador único 1512196199_DOMAIN_COM-VRSN.

airbnb.com

DNS Info | Website Info | IP Info | Whois | RDAP

1512196199_DOMAIN_COM-VRSN [primary]

Del análisis y acceso a la siguiente información a través de Viewdns.info:

Viewdns.info

Tools API Research Data Login Sign Up

DNS Record Lookup
View all configured DNS records (A, MX, CNAME etc.) for a specified domain name.

Enter domain **Lookup**

HTML JSON

DNS Records for 'airbnb.com'

RECORD NAME	TTL	CLASS	TYPE	PRIORITY	DATA
airbnb.com.	3600	IN	SOA		dns1.p02.nsone.net, hostmaster.nsone.ne
airbnb.com.	147	IN	NS		dns1.p08.nsone.net.
airbnb.com.	147	IN	NS		ns-558.awsdns-05.net.

Del análisis detallado de cada renglón que aquí aparece pude concluir lo siguiente de utilidad para Ciberseguridad / Pentesting.

Se podría detectar si hay **subdominios mal configurados** (no revelado en este dump, pero usando herramientas tipo Sublist3r, Amass, crt.sh, etc.); CAA y DMARC muestran **buenas higiene de seguridad**, pero si encontráramos **subdominios sin CAA**, podrían estar expuestos; TXT con muchos SaaS → se podría investigar si alguno tiene **configuración débil** (ej: Atlassian, Webex, etc.). La información muestra que **Airbnb tiene una configuración DNS madura y segura**, pero también evidencia el uso de muchos proveedores externos que podrían formar parte de la **superficie de ataque** si no están bien protegidos. Airbnb ofrece el servicio global de ping test y además especifica cada IP ADDRESS para cada ciudad en específico.

Global Ping Test

Test the response time to your domain name or IP address from multiple locations around the world. Useful for detecting latency issues on network connections.

Enter hostname **Check**

HTML JSON

PING Results for 'airbnb.com'

Intenté utilizar herramientas de Linux tales como el comando **whois** para mi investigación de IP's addresses vinculadas a mi objetivo pero el hecho de que Airbnb utiliza rutas IP anunciadas por Amazon, no solo las que usa Airbnb hace que Airbnb no tenga un AS propio ni bloques IP dedicados públicos por lo tanto esa lista gigantesca no sirve para un análisis fiable por si sola. El comando que sigue a continuación fue una variante de las dos que utilice, pero siempre con un resultado ambiguo sino específico.

adudife_sjofnaw > pfunu | fufsos | ,e,5-[e-0][e-0][e-0][e-0][e-0]-:exoxdozso

En su lugar continue utilizando herramientas como la siguiente:

```
osboxes@osboxes:~/analysis_airbnb$ dig +short airbnb.com
54.243.237.216
44.223.197.210
34.231.2.231
```

```
osboxes@osboxes:~/analysis_airbnb$ dig +short www.airbnb.com  
san.airbnb.com.edgekey.net.  
e118243.a.akamaiedge.net.  
23.211.15.162  
23.211.15.156  
23.211.15.160
```

Resultado:

Resolución a san.airbnb.com.edgekey.net → e118243.a.akamaiedge.net

IPs devueltas: 23.211.15.162, 23.211.15.156, 23.211.15.160

Estas IPs pertenecen a la red de distribución de contenido (CDN) de Akamai (AS20940). Esto indica que Airbnb utiliza Akamai para distribuir contenido estático y posiblemente también para proteger su infraestructura a través de mecanismos como WAF, caching geodistribuido y balanceo global. Airbnb mezcla infraestructura: el dominio raíz (airbnb.com) apunta directamente a AWS, mientras que subdominios críticos como www y api están protegidos por Akamai.

Las IPs de Akamai no son exclusivas de Airbnb. Son compartidas por múltiples clientes, lo que dificulta atribuirlas directamente sin considerar el dominio que resuelven. Para identificar tráfico legítimo o anómalo relacionado con Airbnb, es más confiable filtrar por dominio (SNI, HTTP Host, TLS cert) que por IP. Utilicé la herramienta [dnsvalidator](#) para generar una lista de servidores DNS públicos confiables y asegurarme que los resolvers utilizados en la etapa de enumeración de subdominios fuesen rápidos, estuviesen activos y no me entregasen resultados falsos.

```
(venv) osboxes@osboxes:~/analisis_airbnb/dnsvalidator$ ./venv/bin/dnsvalidator -tl https://raw.githubusercontent.com/blechschmidt/massdns/master/lists/resolvers.txt -threads 100 -o ~/analisis_airbnb/resolvers.txt
```

[17:25:20] [INFO] Finished. Discovered 884 servers

```
[INF] Found 293 subdomains for airbnb.com in 30 seconds 2 milliseconds
(venv) osboxes@osboxes:~/analisis_airbnb$ ~/go/bin/subfinder -d airbnb.com -r -/analisis_airbnb/resolvers.txt -o
~/analisis_airbnb/subs airbnb.txt > subfinder airbnb
```

```
[INF] Found 293 subdomains for airbnb.com in 30 seconds 2 milliseconds  
(venv) osboxes@osboxes:~/analisis_airbnb$ ~/go/bin/subfinder -d airbnb.com -r ~/analisis_airbnb/resolvers.txt -o  
~/analisis_airbnb/subs_airbnb.txt > subfinder_airbnb
```

Subdominios potencialmente relevantes:

1. [staging.airbnb.com](#) Indica un entorno de pruebas; suelen tener menos medidas de seguridad.
 2. [prototype-staging.airbnb.com](#) Otro entorno de desarrollo/test con alto potencial de fuga de datos o configuración laxa.
 3. [prototype.admin-lite-next.airbnb.com](#) Menciona "admin", "lite", "next" y "prototype" → muy interesante para intentar fingerprinting y auth bypass.
 4. [api.next.airbnb.com](#) Subdominio de API que podría usarse para interacción entre sistemas; potencial vector de ataque si no está bien protegido.
 5. [fastly.airbnb.com](#) y [fastly-dev.airbnb.com](#) Pueden estar relacionados con el CDN; fastly-dev puede ofrecer configuración sensible o endpoints de prueba.
 6. [next.airbnb.com](#) Suele usarse para la nueva versión de una plataforma o frontend. Interesante para detectar endpoints expuestos o funcionalidades no terminadas.

7. careers.airbnb.com Útil para OSINT, encontrar roles técnicos y entender el stack tecnológico de la empresa.
 8. nerds.airbnb.com Muchas veces usado como blog técnico del equipo de ingeniería. Muy útil para fingerprinting tecnológico y extracción de información sensible indirecta.
 9. blog.airbnb.com Otro canal de OSINT para obtener información de herramientas internas, incidentes de seguridad o arquitectura.
- staging subdominios .iac-dev o .iac** como: rtpe-uswest2-01.iac-dev.airbnb.com, rtpe-prod-uswest2-03.iac.airbnb.com, www.akamai-dev.airbnb.com Muestran entornos internos o de infraestructura como código (IAC); valioso para mapear la infraestructura o buscar paneles mal protegidos.

Inicié un footprinting con un reconocimiento vertical pero parcialmente porque si no sería un informe mucho más extenso. Hice un ataque con fuerza bruta utilizando el siguiente comando:

```
osboxes@osboxes:~/analisis_airbnb$ shuffledns -mode bruteforce \
-d airbnb.com \
-w /home/osboxes/massdns/SecLists/Discovery/DNS/subdomains-top1million-110000.txt \
-r ~/analisis_airbnb/resolvers.txt \
-silent > ~/analisis_airbnb/shuffledns.txt
osboxes@osboxes:~/analisis_airbnb$ ls
dnsvalidator resolvers.txt shuffledns.txt shuffledns_verbose.txt subfinder_airbnb subs_airbnb.txt
osboxes@osboxes:~/analisis_airbnb$ cat shuffledns.txt | wc
   98      98    1562
```

Me enfoqué en aquellos que pudiesen:

- Revelar funcionalidades críticas (API, acceso interno, staging).
- Tener potenciales vulnerabilidades (entornos de staging, subdominios internos).
- Estar relacionados con empleados, usuarios, ingeniería o infraestructura.

Subdominios seleccionados (8):

1. api.airbnb.com Subdominio destinado a la interfaz de programación de aplicaciones (API) pública o privada. Es crítico porque podría revelar endpoints sensibles si no está correctamente protegido.
2. staging.airbnb.com Un entorno de preproducción usado para pruebas antes de publicar en producción. Muy valioso para un Red Team porque podría tener menos seguridad que la versión final.
3. preprod.airbnb.com Similar al anterior, otro entorno de testing/preproducción. Suele contener versiones incompletas de servicios reales.
4. engineering.airbnb.com Usado probablemente por el equipo de ingeniería para compartir artículos técnicos, documentación interna o acceso a herramientas.
5. community.airbnb.com Plataforma de comunidad de usuarios/anfitriones. Puede revelar interacciones, flujos de usuarios y configuración de terceros.
6. karma.airbnb.com Nombre inusual; podría estar relacionado con reputación de usuarios, sistema de evaluación o herramienta interna. Merece revisión.
7. localhost.admin.airbnb.com Muy interesante: puede haber sido una mala configuración o prueba mal eliminada. Si resuelve públicamente, es un error serio.
8. git.airbnb.com Podría ser acceso al sistema GitLab/Gitea/Bitbucket interno. Si está expuesto, es una mina de oro para atacantes.

1. api.airbnb.com

¿Qué es?

Es el subdominio asociado a la API de Airbnb. Es probable que maneje peticiones REST o GraphQL para funcionalidades como búsqueda de alojamientos, reservas, login, datos de usuarios y anfitriones, etc.

¿Por qué es crítico?

Las APIs suelen ser muy sensibles porque exponen la lógica del backend. Si hay endpoints inseguros, mal autenticados o mal documentados, un atacante podría:

- Acceder a datos sin autorización (IDOR).
- Realizar ataques de enumeration (enumeración de usuarios, alojamientos, etc.).
- Encontrar endpoints ocultos o en desuso.
- Probar fuzzing o inyección en parámetros JSON o headers.

Acciones ejecutadas sobre api.airbnb.com:

Utilicé la herramienta **curl** para un primer análisis.

```
osboxes@osboxes:~/análisis_airbnb$ curl -i https://api.airbnb.com/
```

De la ejecución de fingerprinting **whatweb**:

```
osboxes@osboxes:~/análisis_airbnb$ whatweb https://api.airbnb.com
```

Verificar los headers:

```
osboxes@osboxes:~/análisis_airbnb$ curl -I https://api.airbnb.com
```

Conclusión clave de la ejecución del curl.

El subdominio api.airbnb.com está activo y respaldado por un backend en producción (Monorail) bajo Kubernetes. La respuesta 404 indica que se requieren rutas específicas y autenticadas para interacción válida.

Esto confirma que Airbnb está segmentando el acceso a su API por rutas y controladores internos. El servidor entrega información sensible en headers y cookies que podrían ser útiles en una fase de fingerprinting o análisis pasivo. Es un excelente candidato para pruebas dirigidas a: Enumeración de endpoints (/v1/users, /v2/listings, etc.), fuzzing con herramientas como ffuf, burp intruder, dirsearch, Validación de controles de acceso si se logra un token válido.

Subdominio: api.airbnb.com

Estado: Activo

Servidor: nginx + Monorail backend

Respuesta a /: 404 Not Found — "invalid_action"

Infraestructura: Kubernetes ('x-k8s-pod-name', 'x-k8s-app-name')

Cookies identificadas: jitney_client_session_id, everest_cookie

Seguridad activa: CSP, HSTS, X-Content-Type-Options, X-Frame-Options

Posibles riesgos:

- Exposición parcial de estructura interna ('BaseController', 'monorail').

- Cookies de sesión accesibles incluso en error.

- Oportunidad para enumeración de rutas y fuzzing de API endpoints.

Recomendación:

Realizar mapeo exhaustivo de rutas conocidas ('/v1/', '/v2/'), validar headers de autenticación requeridos, comprobar políticas de rate limit y analizar posibles endpoints accesibles sin token.

De la ejecución de whatweb

Conclusión general:

La salida muestra que el sitio está utilizando **nginx** y está configurado con varias cabeceras de seguridad avanzadas y cookies de sesión. El uso de **HTTP/3** y políticas de seguridad como **HSTS**, **X-Frame-Options** y **X-XSS-Protection** indica un enfoque robusto en la seguridad de las comunicaciones. Sin embargo, el recurso específico que se intentó acceder no existe (404 Not Found), lo que sugiere que la URL no es válida o que se requiere autenticación para acceder a información adicional.

El análisis de las cabeceras inusuales también sugiere que la infraestructura de Airbnb está utilizando mecanismos internos complejos para monitoreo y trazabilidad, lo que es común en sistemas de gran escala.

de la ejecución del curl -I para análisis de las cabeceras.

La respuesta a la solicitud muestra que el servidor de **Airbnb** está utilizando un conjunto avanzado de medidas de seguridad, políticas de rendimiento y gestión de sesiones para proteger tanto los datos de los usuarios como la infraestructura interna. Sin embargo, la URL consultada no está disponible, ya que se recibió un error **404**. Esto sugiere que puede ser necesario revisar la ruta de la API solicitada o autenticar la sesión para acceder a recursos específicos. Además, la presencia de cookies de sesión y el uso de HSTS indican un alto enfoque en la seguridad y la protección de los datos de usuario.

Utilicé la herramienta **ffuf** con diferentes parámetros, pero no obtuve ningún resultado para realizar ciertos análisis.

```
osboxes@osboxes:~/análisis_airbnb$ ffuf -w /home/osboxes/go/pkg/mod/github.com/projectdiscovery/shuffledns@v1.1
```

```
.0/tests/wordlist.txt -u https://api.airbnb.com/FUZZ -mc 200,301,302,404,500 -v
```



v2.1.0-dev

```
:: Method      : GET
:: URI       : https://api.airbnb.com/FUZZ
```

Comprobar si pide autenticación (tokens, API keys).

Conclusión:

El subdominio api.airbnb.com corresponde a la interfaz de comunicación entre **frontend** y **backend**. Este dominio puede ser una pieza clave en la superficie de ataque y debe protegerse con autenticación, validación de entrada y control de acceso estricto. Se recomienda realizar una validación exhaustiva de endpoints accesibles, headers de seguridad y métodos habilitados (GET, POST, PUT, DELETE).

Herramienta **HTTPX**.

HTTP 200

Se utilizó la herramienta `httpx` para validar la accesibilidad de los subdominios pertenecientes al dominio objetivo (airbnb.com). A través de esta validación, se identificaron múltiples subdominios que respondieron con un código HTTP 200, lo que indica disponibilidad activa y posibilidad de interacción por parte de un atacante o investigador.

Ejemplo de subdominio activo:

<https://da.airbnb.com> [200] [2.20.187.96]

Estos subdominios representan posibles vectores de ataque, ya que podrían albergar servicios web, aplicaciones legacy o recursos no suficientemente auditados. La información adicional obtenida (como servidor web, tecnologías detectadas y encabezados TLS) permite realizar una priorización para pruebas posteriores de seguridad (fingerprinting más profundo, detección de versiones vulnerables, testing de CORS, etc.).

Los dominios activos encontrados:

```
osboxes@osboxes:~/analisys_airbnb$ grep "200" httpx_airbnb | awk '{print $1, $5}'  
https://careers.airbnb.com Careers  
https://developer.airbnb.com [2.20.68.97]  
https://bg.next.airbnb.com Ваканционни  
https://de.airbnb.com Blockhäuser,  
https://cnr.next.airbnb.com Smještaji  
https://cs.airbnb.com chaty,  
https://cs.next.airbnb.com chaty,  
https://ar.airbnb.com أماكن  
https://da.next.airbnb.com Ferieboliger,  
https://ar.next.airbnb.com أماكن  
https://bs.next.airbnb.com Smještaji  
https://az.next.airbnb.com Tətil  
https://ca.next.airbnb.com Lloguers  
https://de.next.airbnb.com Blockhäuser,  
https://bg.airbnb.com Ваканционни  
https://da.airbnb.com Ferieboliger,  
https://el.airbnb.com
```

La información detallada incluida todos los IPs se encuentra en el archivo `httpx_airbnb`.

Herramienta CERO

Se utilizó la herramienta cero para identificar dominios relacionados con la infraestructura de Airbnb. Se encontraron más de 70 dominios activos vinculados al dominio principal airbnb.com, incluyendo versiones regionales (.fr, .es, [.co.uk](http://co.uk), .jp, etc.) y dominios corporativos como airbnb.org y airbnb.tools. Esta información amplía la superficie de ataque, ya que cada uno de estos dominios podría albergar aplicaciones web independientes, subdominios únicos o configuraciones específicas susceptibles a vulnerabilidades. En fases posteriores, se recomienda: Ejecutar reconocimiento pasivo y activo sobre estos dominios, identificar subdominios, servicios expuestos y certificados TLS, priorizar aquellos con menor grado de protección o mantenimiento visible.

```
analytics.txt    dnsvalidator    resultado_200.txt    shuffledns_verbose.txt    subs_airbnb.txt  
cero_airbnb     httpx_airbnb    resume.cfg        subdomains.txt  
cero_airbnb.txt resolvers.txt  shuffledns.txt    subfinder_airbnb  
osboxes@osboxes:~/analisis_airbnb$ cat cero_airbnb | wc  
76      76     901
```

Herramienta KATANA.

Se utilizó Katana para recopilar URLs accesibles a través de archivos de configuración pública como robots.txt y sitemap.xml. Posteriormente, se usó unfurl para extraer dominios relacionados o referenciados. Esto permitió identificar posibles endpoints expuestos, dominios vinculados a terceros y áreas útiles para análisis de superficie de ataque. Se utilizó Katana para el scraping de rutas y endpoints de airbnb.com. Se identificaron 245 URLs únicas, incluyendo rutas administrativas, APIs expuestas y endpoints potencialmente sensibles como /login, /api/v2/explore_tabs y parámetros GET. Esta información es valiosa para priorizar vectores de ataque como brute-force, enum de usuarios o fuzzing.

Herramienta utilizada: Katana - En este caso se utilizó para obtener información a partir del dominio airbnb.com.

```
echo airbnb.com | katana -jc -o katana airbnb.txt -kf robotstxt,sitemapxml
```

Esto habilitó jc: crawling en JavaScript, kf_robotstxt,sitemapxml: inclusión de análisis de robots.txt y sitemap.xml, o katana_airbnb.txt: guardar la salida en un archivo.

Resultados obtenidos: Se recolectaron 245 URLs relacionadas a Airbnb desde robots.txt, sitemap.xml y crawling, algunas rutas encontradas incluyen: Endpoints para de suscripción de emails, Interfaces .well-known, como assetlinks.json y amphtml/apikey.pub, enlaces directos a funcionalidades como calendar/ical/, book/, y unsubscribe.

Utilidad para el análisis Red Team:

Las rutas encontradas pueden revelar: Potenciales puntos de acceso para pruebas de fuzzing o ingeniería social (como formularios públicos), archivos .well-known que pueden filtrar detalles sobre configuración de seguridad o vínculos con apps móviles, páginas sensibles como unsubscribe, que pueden estar mal protegidas, elementos relevantes para recolección pasiva y fingerprinting.

Herramienta UnFurl

```
osboxes@osboxes:~/analisis_airbnb$ cat katana_airbnb.txt | ~/go/bin/unfurl domains | sort -u > unfurl_domains.txt
osboxes@osboxes:~/analisis_airbnb$ ls
analytics.txt      httpx_airbnb      resultado_200.txt      subdomains.txt
cero_airbnb         katana_airbnb     resume.cfg          subfinder_airbnb
cero_airbnb.txt    katana_airbnb.txt  shuffledns.txt      subs_airbnb.txt
dnsvalidator        resolvers.txt    shuffledns_verbose.txt unfurl_domains.txt
osboxes@osboxes:~/analisis_airbnb$ cat unfurl_domains.txt
airbnb.com
ar.airbnb.com
bg.airbnb.com
community.withairbnb.com
es.airbnb.com
es-l.airbnb.com
he.airbnb.com
hr.airbnb.com
investors.airbnb.com
ka.airbnb.com
mk.airbnb.com
sk.airbnb.com
sq.airbnb.com
sw.airbnb.com
th.airbnb.com
www.airbnb.com
zh.airbnb.com
```

Este análisis permite:

- Identificar diferentes dominios y subdominios relacionados con Airbnb. Esto es útil para ver si hay sitios relacionados o si hay diferencias regionales o específicas de país.
 - Los parámetros en las URLs, como `utm_source` o `utm_campaign`, pueden indicar campañas de marketing o personalización de contenidos. Esta información es útil para comprender cómo se gestionan las interacciones y personalización de los usuarios.
 - Las rutas pueden revelar endpoints de interés, como rutas de suscripción, calendarios de eventos, o rutas relacionadas con configuraciones específicas. Esta información puede ser valiosa para la explotación de vulnerabilidades o pruebas de penetración.

Utilicé la herramienta katana para hacer un escaneo pasivo y automatizado de URLs públicas asociadas al dominio principal de Airbnb (airbnb.com), especialmente centrado en los archivos robots.txt y sitemap.xml, que suelen contener rutas expuestas o no indexadas de interés para una fase de reconocimiento. El resultado fue una lista extensa de más de 200 URLs.

Para procesar esa información y extraer datos útiles, utilice la herramienta unfurl, que permite descomponer y analizar masivamente URLs. En este caso, aplique el comando: `cat katana_airbnb.txt | unfurl domains | sort -u > unfurl_domains.txt`

Este comando permitió aislar y listar todos los subdominios únicos vinculados al ecosistema de Airbnb. Se identificaron subdominios interesantes como: community.withairbnb.com (posible foco de usuarios o foros), investors.airbnb.com (punto potencialmente sensible relacionado con temas financieros), subdominios regionales como ar.airbnb.com, zh.airbnb.com, es.airbnb.com, etc. Estos subdominios son importantes para el equipo Red Team porque pueden presentar superficies de ataque diferentes, tecnologías o configuraciones específicas por región o propósito. Por ejemplo, algunos pueden estar más desactualizados, contener servicios de prueba, ofrecer formularios expuestos o incluso estar parcialmente desatendidos por el equipo de seguridad. Además, la separación por idioma o región también puede implicar diferencias en la validación de entrada, flujos de autenticación o almacenamiento de datos. En resumen, esta fase permitió construir un mapa más detallado del entorno digital de Airbnb, que será clave para posteriores etapas de exploración activa.

Uní todos los archivos de dominios para ser utilizado en el analizados con herramientas como gau, etc.

```
osboxes@osboxes:~/analisis_airbnb$ cat shuffledns.txt subdominios.txt cero_airbnb katana_airbnb | sort -u > all_subs.txt
osboxes@osboxes:~/analisis_airbnb$ cat all_subs.txt | wc
      657      657    20132

osboxes@osboxes:~/analisis_airbnb$ cat all_subs.txt | wc
      657      657    20132
```

Herramientas AlterX y dnsX

```
osboxes@osboxes:~/analisis_airbnb$ cat all_subs.txt | alterx | dnsx -silent -o alterx.txt
[ INFO] Current alterx version v0.0.6 (latest)
[ INFO] Generated 205860 permutations in 0.3121s
8c9be.admin.airbnb.com
8c9be.staging.airbnb.com
acc-admin.dev.staging.airbnb.com
acc-api.dev.staging.airbnb.com

osboxes@osboxes:~/analisis_airbnb$ cat alterx.txt | wc
      8839      8839    307720
```

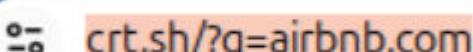
Fase de Permutaciones y Resolución DNS

Una vez obtenida una lista inicial de posibles subdominios (all_subs.txt), se emplean técnicas de **permutación de subdominios** para descubrir nuevos subdominios potenciales que no fueron detectados durante el reconocimiento pasivo inicial.

alterx: Genera permutaciones automáticas a partir de los subdominios conocidos. Esto permite encontrar subdominios mal configurados, entornos de staging o testeo, olvidados, etc. y **dnsx:** Es una herramienta de resolución DNS que verifica cuáles de esos subdominios realmente existen (es decir, responden a una consulta DNS). Solo los válidos se guardarán.

Comando utilizado: `cat all_subs.txt | alterx | dnsx -silent -o alterx.txt`

Este proceso permitió la superficie de ataque, ayudando a descubrir subdominios vivos que podrían contener vulnerabilidades o información sensible. El resultado del uso combinado de alterx y dnsx, que generó un total de 8.839 subdominios válidos y activos, representa un hallazgo significativo en términos de inteligencia ofensiva. Esta información no solo amplía de forma exponencial la superficie de ataque, sino que también permite identificar activos que probablemente no estén bien protegidos o incluso hayan sido olvidados por el equipo de TI del objetivo. Subdominios como dev., staging., old., backup., entre muchos otros, suelen estar menos vigilados o contar con configuraciones débiles, credenciales por defecto o versiones antiguas de aplicaciones. Además, al haber "barriendo el alfabeto completo", el proceso ha sido sistemático y exhaustivo, lo que garantiza una cobertura muy amplia. En un entorno real de Red Team, esta información podría ser utilizada para llevar a cabo ataques más dirigidos como la explotación de aplicaciones web, ingeniería social basada en nombres internos, o incluso como punto de entrada a redes internas. En resumen, este paso representa un **valor estratégico clave** para el análisis posterior y la planificación de futuras acciones ofensivas.



Como parte de la fase de reconocimiento pasivo, consulte los **Certificate Transparency Logs** a través de la plataforma [crt.sh](#), con el objetivo de identificar subdominios asociados al dominio principal airbnb.com y analizar los certificados SSL/TLS vinculados. La búsqueda arrojó una lista extensa de certificados, muchos de ellos del tipo SAN (*Subject Alternative Name*), que agrupan múltiples subdominios regionales bajo un único certificado. Un ejemplo representativo es el certificado con ID 18246188439, emitido el 25 de febrero de 2025 y válido hasta febrero de 2026, que incluye subdominios como es.airbnb.com, ar.airbnb.com, mt.airbnb.com, entre otros. Este enfoque facilita la administración de certificados en organizaciones con presencia global, pero desde la perspectiva de un Red Team, permite mapear parte de la infraestructura externa del objetivo sin interacción directa, manteniendo un perfil bajo durante el reconocimiento.

No mostramos aquí toda la información de certificados porque es una lista muy amplia que puede consultarse fácilmente y es por ello que solo aparece una muestra.

crt.sh Identity Search							
Criteria		Type: Identity	Match: ILIKE	Search: 'airbnb.com'	Group by Issuer		
Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	18246188439	2025-05-06	2025-02-25	2026-02-25	www.airbnb.com	ar.airbnb.com bg.airbnb.com es.airbnb.com mt.airbnb.com	C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
18129745171	2025-04-29	2025-02-07	2025-06-06	airbnb.com	airbnb.com airbnb.com.ar airbnb.com.au airbnb.com.bo		C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
17935712346	2025-04-19	2024-05-22	2025-05-21	ci.airbnb-web.production.certs.akamai.airbnb.net	akamai-ci.airbnb.com		C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
17910132434	2025-04-17	2025-04-17	2026-04-14	homere-lac-dev.airbnb.com	grafana.lac-dev.airbnb.com grafana-lac-dev.airbnb.com homere-lac-dev.airbnb.com homere-lac-dev.airbnb.com		C=US, O=DigiCert Inc, CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1
17902295348	2025-04-17	2024-05-06	2025-05-06	ci.airbnb-api.production.certs.akamai.airbnb.net	api.akamai-ci.airbnb.com		C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
17791228139	2025-04-11	2025-04-11	2025-08-08	1.telemetry.integration.ingress.airbnb.net	origin-events.airbnb.com		C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
17789497553	2025-04-11	2025-04-11	2025-04-17	1.telemetry.integration.ingress.airbnb.net	origin-events.airbnb.com		C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
17586717607	2025-04-02	2025-04-02	2026-04-01	akamai-dev.airbnb.com	akamai-dev.airbnb.com api.akamai-dev.airbnb.com www.akamai-dev.airbnb.com		C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
17586717376	2025-04-02	2025-04-02	2026-04-01	ci.airbnb-web.production.certs.akamai.airbnb.net	www.akamai-ci.airbnb.com		C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
17585514545	2025-04-02	2025-04-02	2026-04-01	akamai-dev.airbnb.com	akamai-dev.airbnb.com api.akamai-dev.airbnb.com www.akamai-dev.airbnb.com		C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
17585509436	2025-04-02	2024-06-11	2025-05-22	ci.airbnb-web.production.certs.akamai.airbnb.net	www.akamai-ci.airbnb.com		C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
17585486829	2025-04-02	2025-04-02	2026-04-01	ci.airbnb-web.production.certs.akamai.airbnb.net	www.akamai-ci.airbnb.com		C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
17594522574	2025-04-01	2025-04-01	2025-06-30	developer.airbnb.com	developer.airbnb.com		C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
17567347417	2025-04-01	2025-04-01	2025-06-30	developer.airbnb.com	developer.airbnb.com		C=US, O=Let's Encrypt, CN=ES
17567368411	2025-04-01	2025-04-01	2025-06-30	developer.airbnb.com	developer.airbnb.com		C=US, O=Let's Encrypt, CN=ES
17567374689	2025-04-01	2025-04-01	2025-06-30	developer.airbnb.com	developer.airbnb.com		C=US, O=Let's Encrypt, CN=R11
17564850952	2025-04-01	2025-04-01	2026-03-31	akamai-dev.airbnb.com	akamai-dev.airbnb.com api.akamai-dev.airbnb.com www.akamai-dev.airbnb.com		C=US, O=Let's Encrypt, CN=R11
17563589553	2025-04-01	2024-09-13	2025-09-12	akamai-dev.airbnb.com	akamai-dev.airbnb.com api.akamai-dev.airbnb.com www.akamai-dev.airbnb.com		C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
17563590738	2025-04-01	2025-04-01	2026-03-31	akamai-dev.airbnb.com	akamai-dev.airbnb.com api.akamai-dev.airbnb.com www.akamai-dev.airbnb.com		C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
17070787143	2025-03-12	2025-03-12	2026-03-11	ci.airbnb-api.production.certs.akamai.airbnb.net	api.akamai-ci.airbnb.com		C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1

Herramienta GAU.

gau (GetAllUrls) es una herramienta muy útil en el campo del hacking ético, el bug bounty y las auditorías de seguridad web. Su propósito principal es enumerar URLs asociadas a un dominio a partir de múltiples fuentes públicas. Es muy útil en auditorías de ciberseguridad para descubrir endpoints antiguos, ocultos o abandonados, identificar archivos potencialmente sensibles como: Backups: .zip, .tar.gz, .bak, etc., Configuraciones: .env, .json, .xml, Scripts obsoletos: .js, .php, .asp, etc., Analizar el historial del sitio (por ejemplo, si alguna vez tuvo un panel de administración accesible).

Es especialmente útil para encontrar puntos de entrada que no aparecen en la versión actual del sitio web, pero que existieron antes y pueden seguir accesibles si no fueron correctamente eliminados.

```
osboxes@osboxes:~/analisis_airbnb$ gau --threads 5 airbnb.com --o gauoutput.txt
```

```
osboxes@osboxes:~/analisis_airbnb$ cat gauoutput.txt | wc
45703 45703 3361666
```

```
https://www.airbnb.com/rooms/8382747?guests=1&adults=1&s=66&source=embed_widget
https://www.airbnb.com/rooms/838382727394919144?adults=1&s=42&unique_share_id=C92AFF07-88A7-43E5-A57C-E123DF0CCAF1&_branch_match_id=1177881775160206091&_branch_referrer=H4sIAAAAAAAAA8soKSkottLXT0zKS9LLTdUvd828TLMKTvTAIAvoPMuxsAAAA%3D&source_impression_id=p3_1682067126_Us32H1L%2BcpZ%2Bbmxf
https://www.airbnb.com/rooms/838449661106063281?adults=2&location=Washington%20Island%2C%20Washington%20WI%20USA&search_mode=regular_search&check_in=2024-05-29&check_out=2024-05-31&source_impression_id=p3_1715994907_5YovU9XV2e2vu3DL&previous_page_section_name=1001&federated_search_id=08bc6003-8ecd-4764-b813-6131a6b49fed
```

A través de la herramienta **gau** se identificaron URLs que contienen múltiples parámetros dinámicos, incluyendo IDs únicos, referencias codificadas, fechas, datos de localización y seguimiento de impresiones. Estos elementos pueden ser analizados más a fondo para: Realizar pruebas de manipulación de parámetros, Detectar posibles vulnerabilidades de inyección, Extraer información codificada que pueda revelar datos internos o lógicas de sesión, Identificar puntos que podrían ser explotables o revelar información sensible. En particular, el uso de `_branch_referrer` con cadenas codificadas puede indicar contenido comprimido o encriptado que merece ser decodificado para entender su propósito. A continuación, utilice la herramienta **unfurl** para analizar las URLs recolectadas con **gau**, extrayendo de forma precisa los **dominios únicos** involucrados. Esta operación permitió identificar si existían **subdominios internos** de Airbnb o **servicios externos** vinculados. El resultado mostró que todas las URLs provenían exclusivamente del dominio principal

(airbnb.com) o su forma con www, sin presencia de subdominios adicionales ni referencias a dominios de terceros. Esto indica una arquitectura más cerrada en cuanto a exposición web, lo cual puede reducir la superficie de ataque en esta fase inicial del análisis.

```
osboxes@osboxes:~/análisis_airbnb$ cat gauoutput.txt | unfurl --unique domains > gau_unique.txt
```

```
osboxes@osboxes:~/análisis_airbnb$ cat gau_unique.txt | wc -l
3      3     37
osboxes@osboxes:~/análisis_airbnb$ cat gau_unique.txt
www.airbnb.com
airbnb.com
Airbnb.com
```

El uso de la herramienta gau permitió obtener un histórico de URLs relacionadas con el dominio airbnb.com desde fuentes públicas. Este paso es fundamental en auditorías web ya que ayuda a descubrir rutas obsoletas, archivos de configuración, endpoints de API o recursos JavaScript que podrían contener información sensible o vectores de ataque. Al analizar estos resultados, se pueden detectar errores de configuración o accesos no autorizados, mejorando así la postura de seguridad del sitio.

Análisis con urlscan.io

Como parte del reconocimiento pasivo, se utilizó la plataforma urlscan.io para obtener información adicional sobre el dominio airbnb.com. Esta herramienta permite analizar el comportamiento de una URL al ser cargada en un entorno controlado, proporcionando tanto datos históricos como en tiempo real (*live information*) sobre las solicitudes realizadas, recursos cargados, tecnologías utilizadas y posibles conexiones externas. A través de este análisis, se recopilaron evidencias visuales y técnicas relevantes que permiten comprender mejor la superficie expuesta del objetivo, sin generar interacción directa desde nuestra infraestructura. A continuación, se presentan capturas de pantalla y hallazgos destacados del escaneo.

www.airbnb.es
95.100.110.14 Public Scan

Submitted URL: <http://airbnb.com/>
Effective URL: https://www.airbnb.es/?_set_bev_on_new_domain=1747068117_EAYTc2MDM0NDUxMT
Submission: On May 12 via manual from ES - Scanned from ES

Behaviour Indicators Similar DOM Content API Verdicts

Summary

This website contacted 4 IPs in 3 countries across 5 domains to perform 235 HTTP transactions. The main IP is 95.100.110.14, located in Netherlands and belongs to AKAMAI-ASN1 Akamai International B.V., NL. The main domain is www.airbnb.es. The Cisco Umbrella rank of the primary domain is 607470. TLS certificate: Issued by DigiCert Global G2 TLS RSA SHA256 202... on February 25th 2025. Valid for: a year.

Live information

Google Safe Browsing: No classification for www.airbnb.es
Current DNS A record: 104.126.37.147 (AS20940 - AKAMAI-ASN1 Akamai International B.V., NL)

Domain & IP information

IP/ASNs	IP Detail	Domains	Domain Tree	Links	Certs	Frames
			IP Address	AS Autonomous System		
1 1			54.243.237.216	14618 (AMAZON-AES)		
1 43			95.100.110.14	20940 (AKAMAI-ASN1 Akamai International B.V.)		
189			95.100.110.24	20940 (AKAMAI-ASN1 Akamai International B.V.)		
3	2a00:1450:4001:80e::2008			15169 (GOOGLE)		
1	142.250.186.130			15169 (GOOGLE)		
235			4			

Utilicé el resultado del escaneo con httpx, filtrando únicamente los hosts activos (códigos 200), y posteriormente se extrajeron los dominios únicos utilizando unfurl. Este análisis permitió identificar los subdominios activos al momento de este análisis, del entorno de Airbnb, facilitando una visión clara de la superficie de ataque expuesta públicamente.

```
osboxes@osboxes:~/analisis_airbnb$ cut -d ' ' -f1 httpx_airbnb | unfurl --unique domains > subd_final.txt
osboxes@osboxes:~/analisis_airbnb$ cat subd_final.txt | wc
    17      17    296
osboxes@osboxes:~/analisis_airbnb$ cat subd_final.txt
careers.airbnb.com
developer.airbnb.com
bg.next.airbnb.com
de.airbnb.com
cnn.next.airbnb.com
cs.airbnb.com
cs.next.airbnb.com
ar.airbnb.com
da.next.airbnb.com
ar.next.airbnb.com
bs.next.airbnb.com
az.next.airbnb.com
ca.next.airbnb.com
de.next.airbnb.com
bg.airbnb.com
da.airbnb.com
el.airbnb.com
```

Se utilizó el resultado del escaneo con **httpx**, filtrando únicamente los hosts activos (códigos 200), y posteriormente se trajeron los dominios únicos utilizando **unfurl**. Este análisis permitió identificar los subdominios activos del entorno de Airbnb, facilitando una visión clara de la superficie de ataque expuesta públicamente.

Resolución de Subdominios a Direcciones IP.

Con el objetivo de obtener las direcciones IP asociadas a cada uno de los subdominios previamente identificados como activos mediante httpx, se ejecutó un bucle que automatiza la resolución DNS utilizando la herramienta dig. Esto permitió recopilar únicamente las direcciones IP válidas para su posterior análisis, como escaneo de puertos con masscan.

```
osboxes@osboxes:~/analisis_airbnb$ for subdominio in $(cat subd_final.txt); do dig +short $subdominio | grep -E '([0-9]{1,3}\.){3}[0-9]{1,3}'; done > subdominios
```

```
osboxes@osboxes:~/analisis_airbnb$ cat subdominios | wc
    44      44    568
```

Escaneo de Puertos con Masscan

Con el objetivo de identificar puertos abiertos en los activos previamente descubiertos, se utilizó la herramienta masscan, conocida por su alta velocidad de escaneo. La entrada para este análisis fue el archivo subdominios, que contiene las direcciones IP extraídas mediante resolución DNS de los subdominios activos.

```
osboxes@osboxes:~/analisis_airbnb$ sudo masscan -iL subdominios -p0-65535 --rate=1000 -oG puertos_abiertos.txt
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-05-12 17:39:28 GMT
Initiating SYN Stealth Scan
Scanning 16 hosts [65536 ports/host]
osboxes@osboxes:~/analisis_airbnb$ cat puertos_abiertos.txt | wc
    23     166   1600
```

```
osboxes@osboxes:~/analisis_airbnb$ cat puertos_abiertos.txt
# Masscan 1.3.2 scan initiated Mon May 12 17:39:28 2025
# Ports scanned: TCP(65536;0-65535) UDP(0;) SCTP(0;) PROTOCOLS(0;)
Timestamp: 1747071694 Host: 2.20.68.78 () Ports: 80/open/tcp//http/
Timestamp: 1747071726 Host: 95.101.38.16 () Ports: 80/open/tcp//http/
Timestamp: 1747071833 Host: 96.16.88.136 () Ports: 80/open/tcp//http/
Timestamp: 1747071836 Host: 96.16.88.142 () Ports: 443/open/tcp//https//
Timestamp: 1747071856 Host: 95.101.38.38 () Ports: 443/open/tcp//https//
Timestamp: 1747072017 Host: 95.101.38.18 () Ports: 443/open/tcp//https//
Timestamp: 1747072054 Host: 95.101.38.41 () Ports: 80/open/tcp//http/
Timestamp: 1747072083 Host: 96.16.88.165 () Ports: 80/open/tcp//http/
Timestamp: 1747072098 Host: 95.101.38.58 () Ports: 443/open/tcp//https//
Timestamp: 1747072150 Host: 95.101.38.58 () Ports: 80/open/tcp//http/
Timestamp: 1747072255 Host: 96.16.88.133 () Ports: 443/open/tcp//https//
Timestamp: 1747072256 Host: 95.101.38.47 () Ports: 80/open/tcp//http/
Timestamp: 1747072398 Host: 95.101.38.13 () Ports: 443/open/tcp//https//
Timestamp: 1747072415 Host: 95.101.38.41 () Ports: 443/open/tcp//https//
Timestamp: 1747072419 Host: 96.16.88.133 () Ports: 80/open/tcp//http/
Timestamp: 1747072421 Host: 2.20.68.78 () Ports: 443/open/tcp//https//
Timestamp: 1747072489 Host: 95.101.38.47 () Ports: 443/open/tcp//https//
Timestamp: 1747072534 Host: 95.101.38.13 () Ports: 80/open/tcp//http/
Timestamp: 1747072556 Host: 95.101.38.38 () Ports: 80/open/tcp//http/
Timestamp: 1747072598 Host: 95.101.38.23 () Ports: 80/open/tcp//http/
```

Conclusión del Escaneo de Puertos

El escaneo de puertos realizado con masscan reveló un total de 19 servicios expuestos, todos en los puertos TCP 80 (HTTP) y 443 (HTTPS), lo cual indica que los sistemas descubiertos están orientados principalmente a la provisión de servicios web. La ausencia de otros puertos abiertos reduce la superficie de ataque desde el punto de vista de servicios accesibles directamente, aunque no elimina la necesidad de análisis adicionales en capas superiores (aplicativas) y en configuraciones internas. Este hallazgo sugiere que la infraestructura utiliza prácticas de exposición controlada, limitando los servicios públicos únicamente a los esenciales para la navegación y la entrega de contenido seguro.

Uso de nmap

Conclusión técnica preliminar (Airbnb.com)

El dominio principal airbnb.com está alojado en AWS y utiliza nginx como servidor web. Se observa una política de redirección forzada a HTTPS (buen estándar de seguridad). El certificado TLS es amplio y válido, lo que respalda su uso internacional. No se han detectado servicios innecesarios ni puertos abiertos fuera de los esperados (80 y 443), lo que indica una superficie de ataque bien controlada.

```
osboxes@osboxes:~/análisis_airbnb$ sudo nmap -Pn -sS -sV -sC -p- airbnb.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-12 16:46 EDT
Nmap scan report for airbnb.com (54.243.237.216)
Host is up (0.12s latency).
Other addresses for airbnb.com (not scanned): 44.223.197.210 34.231.2.231
rDNS record for 54.243.237.216: ec2-54-243-237-216.compute-1.amazonaws.com
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http   nginx
|_http-title: Did not follow redirect to https://airbnb.com/
443/tcp   open  ssl/http nginx
|_http-title: Did not follow redirect to https://www.airbnb.com/
| tls-alpn:
|   http/1.1
|   http/1.0
|_http/0.9
|_ssl-date: TLS randomness does not represent time
|_ssl-cert: Subject: commonName=airbnb.com/organizationName=Airbnb, Inc./stateOrProvinceName=California/countryName=US
```

Conclusión técnica preliminar (api)

El subdominio api.airbnb.com está protegido detrás de la red Akamai, lo que limita los vectores de ataque directos. Los puertos visibles son los típicos para servicios web (80 y 443), bien configurados y redirigiendo correctamente a HTTPS. El uso de un CDN y certificados SSL válidos muestra buenas prácticas de seguridad. Sin embargo, el flag `httponly` ausente en una cookie identificada puede ser un punto a revisar más a fondo en un análisis web detallado.

```
osboxes@osboxes:~/análisis_airbnb$ sudo nmap -Pn -sS -sV -sC -p- api.airbnb.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-12 14:28 EDT
Nmap scan report for api.airbnb.com (23.211.15.162)
Host is up (0.033s latency).
Other addresses for api.airbnb.com (not scanned): 23.211.15.143 23.211.15.160 23.211.15.144 23.211.15.156 23.211.15.148 23.211.15.135
rDNS record for 23.211.15.162: a23-211-15-162.deploy.static.akamaitechnologies.com
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
53/tcp    closed domain
80/tcp    open  http   AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
|_http-title: Did not follow redirect to https://api.airbnb.com/
|_http-server-header: nginx
443/tcp   open  ssl/http AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
|_http-title: Site doesn't have a title (application/json;charset=utf-8).
|_http-server-header: nginx
| http-cookie-flags:
|   :
|     jitney_client_session_id:
|       httponly flag not set
|_ssl-cert: Subject: commonName=api.airbnb.com/organizationName=Airbnb, Inc./stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:api.airbnb.com
| Not valid before: 2025-02-19T00:00:00
| Not valid after:  2026-02-18T23:59:59
```

Herramienta Gowitness.

GoWitness es una herramienta de código abierto diseñada para capturar automáticamente capturas de pantalla de servicios web expuestos en un escaneo de red. Resulta especialmente útil en auditorías de seguridad y ejercicios de reconocimiento, ya que permite visualizar de forma rápida y masiva las interfaces web que están activas en los puertos detectados.

```
osboxes@osboxes:~/análisis_airbnb$ gowitness scan file -f subdominiostxt
2025/05/12 17:18:00 WARN no writers have been configured. to persist probe results, add writers using --write-* flags
2025/05/12 17:18:09 INFO result 📸 target=http://ar.next.airbnb.com:443 status-code=429 title="503 Service Unavailable - Airbnb" have-screenshot=true
```

```
osboxes@osboxes:~/análisis_airbnb$ ls
all_subs.txt    clean_subs.txt  katana_airbnb        resume.cfg          subdominiostxt
alterx.txt      dnsvalidator    katana_airbnb.txt    screenshots         subdominiostxt
analytics.txt   gaouput.txt    puertos_abiertos.txt  shuffledns.txt    subfinder_airbnb
```

Estas imágenes representan cómo se ve cada sitio/subdominio cuando se accede desde un navegador web.

```
osboxes@osboxes:~/análisis_airbnb/screenshots$ ls
http---ar.next.airbnb.com-443.jpeg  http---id.airbnb.com-80.jpeg      https---id.airbnb.com-443.jpeg
http---ar.next.airbnb.com-80.jpeg    http---mk.next.airbnb.com-443.jpeg  https---mk.next.airbnb.com-443.jpeg
http---fastly.airbnb.com-443.jpeg   http---mk.next.airbnb.com-80.jpeg   https---sv.airbnb.com-443.jpeg
http---fastly.airbnb.com-80.jpeg    https---ar.next.airbnb.com-443.jpeg  http---sv.airbnb.com-443.jpeg
http---id.airbnb.com-443.jpeg      https---fastly.airbnb.com-443.jpeg  https---sv.airbnb.com-80.jpeg
```

En este proyecto, GoWitness se utilizó para realizar capturas de pantalla de los servicios web de los subdominios de Airbnb, permitiendo obtener una representación visual de las páginas accesibles en los puertos HTTP (80) y HTTPS (443). La herramienta se ejecutó de manera eficiente y proporcionó un análisis visual complementario a los escaneos de puertos previos.

Herramienta WafW00f

Para complementar la fase de reconocimiento pasivo, se utilizó la herramienta WafW00f con el objetivo de detectar la presencia de firewalls de aplicaciones web (WAF) en los subdominios analizados. Esta herramienta permite identificar el tipo y fabricante del WAF implementado, proporcionando información clave sobre las medidas de defensa empleadas por la infraestructura web del objetivo. Para

ello, se empleó el siguiente comando: `wafw00f -l subd_final.txt > wafw00f_waf.txt`, lo que permitió automatizar el análisis de una lista de subdominios recopilada en fases anteriores. Esta técnica es especialmente útil en escenarios de Red Team, ya que permite detectar defensas perimetrales que podrían bloquear o dificultar ataques posteriores. Los resultados se almacenaron en un archivo de texto (wafw00f_waf.txt) para su posterior análisis y documentación.

```
(waf-env) osboxes@osboxes:~/análisis_airbnb$ wafw00f -l subd_final.txt > wafw00f_waf.txt
```

```
(waf-env) osboxes@osboxes:~/análisis_airbnb$ cat wafw00f_waf.txt | wc  
184 894 15834
```

Como resultado parcial del escaneo con WafW00f, se identificaron múltiples tecnologías de WAF (Web Application Firewall) activas en los subdominios analizados. Entre las soluciones detectadas se encuentran productos ampliamente utilizados como AWS Elastic Load Balancer de Amazon, Airlock de Ergon, AppWall de Radware, y 360WangZhanBao de 360 Technologies, entre otros. Esta información es valiosa para comprender el entorno de defensa de los sistemas objetivo, ya que permite anticipar qué mecanismos de filtrado o bloqueo podrían interferir en futuras fases de evaluación de seguridad o explotación.

```
~ WAFW00F : v2.3.1 ~  
The Web Application Firewall Fingerprinting Toolkit  
[+] Can test for these WAFs:  


| WAF Name                  | Manufacturer            |
|---------------------------|-------------------------|
| 360WangZhanBao            | 360 Technologies        |
| ACE XML Gateway           | Cisco                   |
| ASP-.NET Generic          | Microsoft               |
| ASPA Firewall             | ASPA Engineering Co.    |
| AWS Elastic Load Balancer | Amazon                  |
| AireecDN                  | Airee                   |
| Airlock                   | Phion/Ergon             |
| Alert Logic               | Alert Logic             |
| AliYunDun                 | Alibaba Cloud Computing |
| AnYu                      | AnYu Technologies       |


```

Herramienta FFUF

FFUF (Fuzz Faster U Fool) es una herramienta de línea de comandos utilizada para descubrir directorios y archivos ocultos en servidores web mediante técnicas de fuzzing. Es ampliamente empleada en tareas de recolección de información y pruebas de penetración, ya que permite enviar múltiples solicitudes HTTP modificando partes de la URL (como rutas o parámetros) con palabras tomadas de diccionarios predefinidos. Esto facilita identificar recursos expuestos o no documentados, como paneles de administración, archivos sensibles o APIs internas, que podrían representar posibles vectores de ataque. Su velocidad, flexibilidad y compatibilidad con múltiples opciones de filtrado y salida la convierten en una herramienta esencial dentro del arsenal de cualquier red teamer o auditor de seguridad.

El siguiente comando descarga el archivo common.txt desde el repositorio [Seclists](#), que es una colección muy completa de listas para pentesting (subdominios, directorios, contraseñas, etc.). El archivo common.txt contiene nombres comunes de directorios y archivos web que luego puedes usar para fuzzing con FFUF.

```
(waf-env) osboxes@osboxes:~/análisis_airbnb$ wget https://raw.githubusercontent.com/danielmiessler/SecLists/re  
fs/heads/master/Discovery/Web-Content/common.txt
```

```
(waf-env) osboxes@osboxes:~/análisis_airbnb$ cat common.txt | wc  
4746 4750 38467
```

```
(waf-env) osboxes@osboxes:~/análisis_airbnb$ ffuf -w common.txt -u https://airbnb.com/FUZZ -t 10 -mc 200,401,4  
03 -o ffuf_dir-file.txt  
/___\ /___\ /___\
```

```
(waf-env) osboxes@osboxes:~/análisis_airbnb$ cat ffuf_dir-file.txt | wc  
0 21 1960
```

Tras ejecutar FFUF utilizando la lista común de rutas (common.txt), no se identificaron directorios o archivos accesibles en el dominio objetivo que respondieran con códigos HTTP relevantes como 200, 401 o 403. Esto podría indicar que el servidor está bien configurado, no expone rutas sensibles comunes o utiliza mecanismos de defensa como redireccionamientos, respuestas uniformes ante errores o un WAF que bloquea los intentos de enumeración. También es posible que se requiera una lista de diccionario más amplia o específica para el objetivo en cuestión, o ajustar parámetros como los códigos de respuesta a filtrar.

El escaneo con FFUF reveló la presencia de un único recurso accesible en el dominio <https://airbnb.com>: la ruta /.well-known/assetlinks.json, que respondió con un código **HTTP 200**. Este archivo es comúnmente utilizado para la verificación de vínculos entre aplicaciones móviles y dominios web, como parte del protocolo de asociación de apps en Android. Aunque no constituye una

vulnerabilidad en sí misma, su presencia puede ser aprovechada para obtener información adicional sobre integraciones móviles o para confirmar la legitimidad de ciertas aplicaciones asociadas con el dominio. Una ligera muestra de su contenido a continuación.

```
(waf-env) osboxes@osboxes:~/análisis_airbnb$ cat ffuf_dir-file.txt
{"commandline": "ffuf -w common.txt -u https://airbnb.com/FUZZ -t 10 -mc 200,401,403 -o ffuf_dir-file.txt", "time": "2025-05-13T06:45:18-04:00", "results": [{"input": {"FFUFHASH": "683c92e", "FUZZ": ".well-known/assetlinks.json"}, "position": 46, "status": 200, "length": 11285, "words": 2652, "lines": 565, "content-type": "application/json", "redirect": null}], "error": null}
```

Herramienta WhatWeb.

WhatWeb es una herramienta de análisis de aplicaciones web que permite identificar tecnologías, frameworks y herramientas utilizadas por los sitios web. Utiliza una base de datos extensa de firmas para detectar diversos componentes como servidores web, sistemas de gestión de contenido (CMS), bibliotecas JavaScript, plataformas de análisis web y más. Esta herramienta es útil para realizar un *reconocimiento* detallado de las tecnologías que componen un sitio web, lo cual es esencial en pruebas de penetración y evaluaciones de seguridad. En este caso, WhatWeb se utilizó para obtener información sobre la infraestructura tecnológica detrás de airbnb.com, proporcionando una visión general de las plataformas y servicios.

```
(waf-env) osboxes@osboxes:~/análisis_airbnb$ whatweb airbnb.com
http://airbnb.com [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[nginx], IP[54.243.237.216], RedirectLocation[https://airbnb.com/], Title[301 Moved Permanently], UncommonHeaders[x-airbnb-sureride,x-server-name, nginx]
https://airbnb.com/ [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[nginx], IP[44.223.197.210], RedirectLocation[https://www.airbnb.com/], Strict-Transport-Security[max-age=31536000; includeSubDomains; preload], Title[301 Moved Permanently], UncommonHeaders[x-airbnb-sureride,x-server-name, nginx]
https://www.airbnb.com/ [200 OK] Bootstrap, Cookies[_user_attributes,ak_bmsc,bev,cdn_exp_5d4847f3128303184,country,everest_cookie], Country[UNITED STATES][US], HTML5, HTTPServer[nginx], IP[96.16.88.134], Open-Graph-Protocol[website][138566025678], OpenSearch[/opensearch.xml], Script[application/json,application/ld+json], Strict-Transport-Security[max-age=10886400; includeSubdomains], Title[Airbnb | Vacation rentals, cabins, beach houses, & more], UncommonHeaders[x-instrumentation,x-server-lifecycle-phase,x-kraken-loop-name,accept-ch-lifetime,content-security-policy,x-airbnb-kraken-flush-body,x-envoy-upstream-service-time,accept-ch,x-content-type-options,link,x-airbnb-internal-trace-id,x-server-name,alt-svc,akamai-request-bc,x-airbnb-sureride,cacheStatus,server-timing,origin-trial,x-browser-type,x-erf-bev-bev-is-generated,x-erf-bev-bev,x-airbnb-everest-device-id], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[1; mode=block], nginx
```

El análisis realizado con WhatWeb para airbnb.com reveló detalles sobre la infraestructura del sitio web, incluyendo información sobre el servidor web, redirecciones y tecnologías utilizadas. Se identificaron múltiples redirecciones HTTP, primero desde,

<http://airbnb.com> hacia <https://airbnb.com>, y luego hacia <https://www.airbnb.com>.

El servidor web en uso es nginx, con varias cabeceras personalizadas como x-airbnb-sureride y x-server-name. Además, el sitio utiliza Strict-Transport-Security para garantizar conexiones seguras y ha implementado políticas de seguridad como X-Frame-Options y X-XSS-Protection. En la versión final de la página, se observó que Airbnb utiliza tecnologías como Bootstrap y varios encabezados JSON-LD para representar datos estructurados. La respuesta HTTP fue 200 OK, indicando que la página fue cargada exitosamente, mientras que la página titulada "Airbnb | Vacation rentals, cabins, beach houses, & more" muestra una interfaz accesible para los usuarios.

Después de analizar Airbnb.com también realice el proceso para los subdominios vivos.

```
(waf-env) osboxes@osboxes:~/análisis_airbnb$ whatweb -i subd_final.txt > whatweb_subd.txt
(waf-env) osboxes@osboxes:~/análisis_airbnb$ cat whatweb_subd.txt | wc
 34    748   31277
```

El análisis de los subdominios de airbnb.com mediante la herramienta WhatWeb ha permitido obtener información valiosa sobre la infraestructura de los mismos. Se ha identificado que los subdominios, como ar.airbnb.com, de.airbnb.com, cs.airbnb.com, entre otros, redirigen a URLs específicas con códigos de estado 301 (Movido Permanentemente), lo que indica que las páginas han sido reubicadas permanentemente a nuevas direcciones. Además, se detectaron servidores web de AkamaiGHost que gestionan el tráfico, con cabeceras inusuales como akamai-request-bc y x-airbnb-sureride, así como el uso de cookies como bev y everest_cookie. Estos resultados sugieren el uso de una infraestructura de distribución de contenido (CDN) y medidas de seguridad asociadas. Para más información y detalles completos del análisis de los subdominios, se puede consultar el archivo whatweb_subd.txt.

Análisis de vulnerabilidades.

Nuclei es una herramienta de código abierto utilizada en el análisis de vulnerabilidades automatizado, que permite identificar de forma rápida y precisa fallos de seguridad en aplicaciones web, servidores y servicios expuestos. Gracias a su enfoque basado en plantillas YAML, Nuclei facilita la ejecución de pruebas específicas como detección de CVEs, exposición de información sensible, configuraciones erróneas, y otros vectores comunes de ataque. Esta herramienta es ampliamente utilizada en auditorías de ciberseguridad debido a su velocidad, modularidad y capacidad de personalización, lo que la convierte en una opción ideal para análisis estándar en entornos controlados o reales.

Resumen técnico de hallazgos – Nuclei Scan (airbnb.com)

Tecnologías detectadas: Se identificó el uso del servidor NGINX ([tech-detect:nginx]) y presencia de formularios en la página principal ([form-detection]), el sitio está utilizando TLS 1.2 ([tls-version]), lo cual es seguro pero no el estándar más actual (TLS 1.3), se halló un patrón de detección de WAF genérico de NGINX ([waf-detect:nginxgeneric]), lo que indica la posible presencia de protección básica contra ataques web.

Recursos y scripts cargados: La URL principal carga más de 40 archivos JavaScript y CSS desde el subdominio a0.muscache.com. Esto puede ser útil para análisis de fingerprinting, rutas internas y endpoints JS.

Configuración DNS y correo: SPF y DMARC están correctamente configurados, apuntando a protección activa contra spoofing de correo, MX gestionado por Google Workspace, confirmando integración con servicios empresariales de Google ([mx-service-detector:Google Apps]). Registros TXT adicionales indican integraciones con servicios de terceros como Miro, BetterComp, Yahoo, etc.

Registro del dominio: Registro activo desde 2008 y vigente hasta 2026 ([rdap-whois:expirationDate]), última modificación del WHOIS: octubre 2024, el campo secureDNS está marcado como falso, lo cual indica que no tiene DNSSEC habilitado, una práctica recomendada para integridad DNS.

Integración con Azure AD: Se detectó un endpoint OIDC en Azure Active Directory ([azure-domain-tenant]) con un tenant_id, lo que revela que Airbnb utiliza Microsoft Azure para autenticación, potencialmente en entornos internos o para servicios SSO.

La ejecución de Nuclei contra el dominio airbnb.com reveló una configuración sólida desde el punto de vista de tecnologías y seguridad pasiva, con buenas prácticas en registros DNS (SPF, DMARC) y uso de WAF. Sin embargo, la falta de DNSSEC podría ser un vector menor de mejora. Además, la gran cantidad de scripts externos y la integración con Azure Active Directory ofrecen posibles puntos de análisis en pruebas posteriores, especialmente en escenarios de fingerprinting, recolección de endpoints o ingeniería inversa de código JS. No se detectaron vulnerabilidades críticas ni configuraciones peligrosas expuestas.

Herramienta testssl.sh.

Análisis SSL/TLS con testssl.sh

testssl.sh es una herramienta de línea de comandos escrita en Bash que permite auditar y evaluar la configuración SSL/TLS de un servidor remoto. Es especialmente útil para detectar protocolos inseguros, suites de cifrado obsoletas, problemas de configuración en certificados, vulnerabilidades conocidas (como Heartbleed, ROBOT, BEAST, etc.) y verificar el cumplimiento con estándares modernos de seguridad. No requiere instalación previa ni acceso root, ya que funciona de forma autónoma en cualquier sistema Unix/Linux que tenga bash y openssl. Esto la convierte en una opción rápida, portable y eficaz para auditores de ciberseguridad, administradores de sistemas y desarrolladores preocupados por la seguridad de sus servicios web.

```
(waf-env) osboxes@osboxes:~/analisis_airbnb$ cd testssl.sh
(waf-env) osboxes@osboxes:~/analisis_airbnb/testssl.sh$ ./testssl.sh https://airbnb.com > testssl_airbnb.txt
(waf-env) osboxes@osboxes:~/analisis_airbnb/testssl.sh$ ls
bin           CREDITS.md      Dockerfile.md      README.md      utils
CHANGELOG.md   doc           etc              t
Coding_Convention.md Dockerfile      LICENSE          testssl_airbnb.txt
CONTRIBUTING.md  Dockerfile.alpine openssl-iana.mapping.html testssl.sh
(waf-env) osboxes@osboxes:~/analisis_airbnb/testssl.sh$ cat testssl_airbnb.txt | wc
    669    4243   49893
```

LUCKY13 (CVE-2013-0169), experimental potentially **VULNERABLE**, uses cipher block chaining (CBC) ciphers with TLS. Check patches

Vulnerabilidad: LUCKY13 (CVE-2013-0169)

Elemento	Detalle
Nombre	LUCKY13
CVE	CVE-2013-0169
Clasificación	Vulnerabilidad de canal lateral (side-channel attack)
Descripción	Explotación basada en el tiempo de procesamiento de mensajes TLS cifrados con CBC. Permite recuperar fragmentos del contenido cifrado bajo ciertas condiciones muy precisas.

Elemento	Detalle
Protocolos afectados	TLS 1.0, TLS 1.1 y algunas implementaciones de TLS 1.2 que usan cifrados CBC.
Resultado de testssl.sh	potentially VULNERABLE
Condición técnica	El servidor acepta cifrados CBC en protocolos vulnerables.
Impacto potencial	Filtración de información sensible. Compromete la confidencialidad del canal.
Dificultad de explotación	Alta (requiere entorno controlado y medición precisa de tiempos de respuesta)

Recomendaciones de mitigación

- Eliminar soporte para TLS 1.0 y 1.1:

Limitar los protocolos a TLS 1.2 o TLS 1.3, mucho más seguros y modernos.

- Eliminar cifrados CBC:

Configurar el servidor para usar únicamente cifrados AEAD (como AES-GCM o ChaCha20-Poly1305).

- Actualizar bibliotecas criptográficas:

Asegurarse de estar usando versiones actualizadas de OpenSSL, GnuTLS o NSS que corren la implementación CBC con técnicas de tiempo constante.

- Verificación de compatibilidad:

Realizar pruebas con clientes antiguos antes de aplicar cambios si existen usuarios que usan navegadores o sistemas antiguos.

La presencia de esta vulnerabilidad indica una configuración TLS desactualizada que no cumple con las recomendaciones de seguridad actuales, como las publicadas por NIST, Mozilla o la OWASP Foundation. Aunque el riesgo de explotación práctica es bajo, su existencia es motivo suficiente para aplicar medidas preventivas.

```
Trust (hostname)          Ok via SAN and CN (works w/o SNI)
                           wildcard certificate could be problematic, see other hosts at
                           https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=839DE71D995
```

Aunque los certificados wildcard son prácticos, presentan riesgos de seguridad y de gestión:

1. Punto único de fallo:

Si la clave privada del certificado se ve comprometida, todos los subdominios protegidos por él también lo estarán. Es decir, una sola brecha pone en riesgo múltiples servicios.

2. Distribución amplia de la clave privada:

Para que el wildcard funcione en múltiples servidores/subdominios, es habitual que la misma clave privada se copie y distribuya entre sistemas. Esto aumenta la superficie de ataque.

3. Falta de granularidad en la revocación:

Si se compromete el certificado, no se puede revocar un solo subdominio. Hay que revocar y reemplazar todo el wildcard, lo que puede afectar a decenas de servicios.

4. Dificultad visibilidad y control:

Al haber un solo certificado para múltiples subdominios, puede ser más difícil auditar qué subdominios están protegidos correctamente o si se están usando certificados expirados o mal configurados en servidores no controlados.

```
Rating (experimental)

Rating specs (not complete)  SSL Labs's 'SSL Server Rating Guide' (version 2009q from 2020-01-30)
Specification documentation https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide
Protocol Support (weighted)  100 (30)
Key Exchange (weighted)     90 (27)
Cipher Strength (weighted)  90 (36)
Final Score                 93
Overall Grade               A+

Done 2025-05-13 13:42:25 [ 369s ] --> 54.243.237.216:443 (airbnb.com) <<-- 

----- 
Done testing now all IP addresses (on port 443): 34.231.2.231 44.223.197.210 54.243.237.216
```

Análisis Final del Estado de Seguridad TLS/SSL del dominio airbnb.com

El análisis realizado sobre airbnb.com mediante la herramienta testssl.sh muestra que el sitio mantiene una configuración TLS/SSL robusta y alineada con buenas prácticas de seguridad. El servidor obtuvo una calificación global A+, según la guía de evaluación de SSL Labs, con un puntaje final de 93 sobre 100. Destaca el soporte exclusivo de protocolos seguros, claves RSA de 2048 bits, extensiones TLS estándar bien configuradas y el uso de algoritmos de firma modernos como SHA256. Sin embargo, se identificó una vulnerabilidad potencial: la exposición a LUCKY13 (CVE-2013-0169) debido al uso de cifrados basados en CBC, lo que podría permitir ataques de canal

lateral si no se aplican mitigaciones adecuadas a nivel de sistema. Aunque esta vulnerabilidad es teórica en muchos entornos modernos, se recomienda verificar la aplicación de parches de seguridad correspondientes. En general, la configuración de TLS de airbnb.com es segura y madura, con prácticas sólidas de cifrado y autenticación, aptas para el tráfico de datos sensibles como los que maneja la plataforma.

Autenticación de Servidores de Correo (SPF, DKIM y DMARC)

- SPF (Sender Policy Framework): SPF es un mecanismo de autenticación que permite al propietario de un dominio especificar qué servidores están autorizados para enviar correos electrónicos en nombre de ese dominio. Esto ayuda a prevenir la suplantación de identidad por correo electrónico (email spoofing), donde un atacante envía correos haciéndose pasar por una dirección legítima. SPF verifica si el correo proviene de un servidor autorizado para enviar mensajes en nombre del dominio especificado.
- DKIM (DomainKeys Identified Mail): DKIM utiliza firmas digitales para autenticar que un correo electrónico no ha sido modificado durante su tránsito y que realmente proviene del dominio que dice representarlo. Cada mensaje enviado desde un servidor que utiliza DKIM se firma con una clave privada, y el servidor receptor puede verificar esa firma utilizando la clave pública disponible en los registros DNS del dominio. Esto garantiza la integridad y autenticidad del mensaje.
- DMARC (Domain-based Message Authentication, Reporting, and Conformance): DMARC se basa en SPF y DKIM, pero añade una capa adicional de políticas que indican al servidor receptor cómo debe manejar los correos que no superan estas verificaciones. DMARC también permite a los propietarios del dominio recibir informes sobre los correos que no han pasado la autenticación, ayudándoles a entender y tomar medidas contra intentos de suplantación de identidad o el uso no autorizado de su dominio.

Estos tres mecanismos—SPF, DKIM y DMARC—trabajan en conjunto para mejorar la seguridad del correo electrónico, autenticando el origen y la integridad de los mensajes, previniendo la suplantación, y ayudando a los propietarios del dominio a monitorear la eficacia de la autenticación de sus correos.

Primero accedí a la página web <https://dmarcian.com/domain-checker/?domain=bill.com> y obtuve los siguientes resultados:

SPF

Great job! You have a valid SPF record, which specifies a hard fail (-all).

Details

v=spf1 include:spf1.airbnb.com ip6:2c0f:fb50:4000::/36 ip6:2a00:1450:4000::/36 ip6:2800:3f0:4000::/36 ip6:2607:f8b0:4000::/36 ip6:2404:6800:4000::/36 ip6:2001:4860:4000::/36 ip4:87.253.232.0/21 ip4:76.223.176.0/20 ip4:76.223.128.0/19 -all

To understand and fix the specific errors, use our [SPF Surveyor](#).

DKIM

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.

Details

v=DKIM1; k rsa;

p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCf/XaKSG0J1epRu28cB3wCG5T38NAx/YAgQKU5QWYbvGICu9OQtWnw+BtmVJ4JemM751Z8vGkoAYjE9AQeSvliN8QvBmRrK6PO5PesFNLwVZ/lvM4/VuSYltQB14INx/uNnEqHVDgG2NILsZNZSIB1MnEgEdTDppkUpBjal+PbQIDAQAB

El dominio airbnb.com presenta una configuración sólida de seguridad de correo electrónico, con políticas DMARC, SPF y DKIM bien implementadas. Estas medidas protegen contra suplantación de identidad (phishing) y aseguran la autenticidad de los correos enviados desde el dominio.

Herramienta SpoofCheck. SpoofCheck puede ser utilizado para ataques de phishing, envío de spam u otras actividades maliciosas.

```
(waf-env) osboxes@osboxes:~/analisis_airbnb/spoofcheck$ python spoofcheck.py airbnb.com > spoofcheck_airbnb.txt
```

```
(waf-env) osboxes@osboxes:~/analisis_airbnb/spoofcheck$ ls
dns_dump.py LICENSE README.md requirements.txt spoofcheck_airbnb.txt spoofcheck.py
(waf-env) osboxes@osboxes:~/analisis_airbnb/spoofcheck$ cat spoofcheck_airbnb.txt | wc
      9      57     685
(waf-env) osboxes@osboxes:~/analisis_airbnb/spoofcheck$ cat spoofcheck_airbnb.txt
[*] Found SPF record:
[*] v=spf1 include:spf1.airbnb.com ip6:2c0f:fb50:4000::/36 ip6:2a00:1450:4000::/36 ip6:2800:3f0:4000::/36 ip6:2607:f8b0:4000::/36 ip6:2404:6800:4000::/36 ip6:2001:4860:4000::/36 ip4:87.253.232.0/21 ip4:76.223.176.0/20 ip4:76.223.128.0/19 -all
[*] SPF record contains an All item: -all
[*] Found DMARC record:
[*] v=DMARC1;p=reject;sp=reject;pct=100;ruf=mailto:dmarc.forensic@airbnb.com;rua=mailto:dmarc.aggregate@airbnb.com;aspf=r;adkim=r;fo=1;ri=3600
[-] DMARC policy set to reject
[*] Aggregate reports will be sent: mailto:dmarc.aggregate@airbnb.com
[*] Forensics reports will be sent: mailto:dmarc.forensic@airbnb.com
[-] Spoofing not possible for airbnb.com
```

El análisis realizado con *Spoofcheck* confirmó que el dominio airbnb.com cuenta con mecanismos de autenticación de correo electrónico correctamente implementados. Se detectó un registro SPF que especifica claramente qué direcciones IP están autorizadas para enviar correos en nombre del dominio, incluyendo una política estricta con -all, lo que indica un "hard fail" para cualquier servidor no autorizado. Asimismo, se encontró un registro DMARC con una política de rechazo (p=reject) tanto para el dominio principal como para los subdominios (sp=reject), lo que refuerza la protección contra suplantación de identidad. Además, se especificaron direcciones para el envío de reportes agregados y forenses, lo que sugiere un monitoreo activo. En conjunto, estos mecanismos hacen que la suplantación del dominio sea inviable, garantizando un nivel alto de protección frente a ataques de *spoofing*.

Detección de Secuestro de Subdominios (Subzy)

Esta técnica dentro de la fase de recolección de información se refiere al proceso de identificar posibles vulnerabilidades donde un atacante podría tomar el control de un subdominio que apunta a un recurso que ya no está en uso o que está mal configurado.

```
(waf-env) osboxes@osboxes:~/análisis_airbnb$ subzy run --targets subdominios.txt > subzy_subd.txt  
(waf-env) osboxes@osboxes:~/análisis_airbnb$ cat subzy_subd.txt | wc  
313 1876 16541
```

```
[ ESC[32mVULNERABLEESC[0m ] - ws.next.airbnb.com [ Cargo Collective ]  
[ ESC[34mDISCUSSIONESC[0m ] - [Issue #152](https://github.com/EdOverflow/can-i-take-over-xyz/issues/152)  
[ ESC[34mDOCUMENTATIONESC[0m ] - [Cargo Support Page](https://support.2.cargocollective.com/Using-a-Third-Part  
y-Domain)  
[ ESC[31mHTTP ERRORESC[0m ] - rtpe-euwest1-01.iac.airbnb.com  
[ ESC[32mVULNERABLEESC[0m ] - email.airbnb.com [ Cargo Collective ]
```

En el resultado de subzy, los dos subdominios que se marcan como vulnerables son:

1. ws.next.airbnb.com

- ❖ Descripción de vulnerabilidad: Este subdominio parece estar asociado con el servicio Cargo Collective, el cual permite que los usuarios utilicen su propio dominio personalizado. Esto puede ser un vector de ataque si no se gestionan correctamente los dominios o la configuración DNS, permitiendo que un atacante pueda tomar control del subdominio si los registros no están correctamente asegurados.
- ❖ Referencia: Se menciona un Issue #152 en GitHub, lo que indica que ya se ha identificado este problema en otros casos similares. Esto permite una mayor comprensión sobre la naturaleza de la vulnerabilidad.
- ❖ Documentación adicional: También se menciona una página de soporte de Cargo Collective, lo que podría proporcionar más detalles sobre cómo mitigar este tipo de vulnerabilidad.

2. email.airbnb.com

- ❖ Descripción de vulnerabilidad: Al igual que el primero, este subdominio está vinculado a Cargo Collective, y como tal, podría ser vulnerable a un ataque si el control de dominio no está asegurado. En este caso, la vulnerabilidad podría permitir que un atacante se haga pasar por email.airbnb.com para enviar correos electrónicos maliciosos, afectando la reputación y seguridad de la marca.
- ❖ Referencia: Aunque no se proporcionan más detalles en la línea, esta vulnerabilidad está relacionada con la configuración de registros de dominio de Cargo Collective.

Se identificaron dos subdominios vulnerables en la infraestructura de airbnb.com. Los subdominios ws.next.airbnb.com y email.airbnb.com están asociados con Cargo Collective, un servicio de terceros para la personalización de dominios. Si la configuración de los registros DNS no está correctamente asegurada, estos subdominios podrían ser tomados por atacantes, lo que representa un riesgo potencial para la seguridad de la comunicación y la reputación de Airbnb. Es recomendable revisar y ajustar la configuración de estos dominios para mitigar el riesgo de suplantación de identidad o ataques relacionados.

Técnicas OSINT

OSINT permite el proceso de recopilar, analizar y utilizar datos disponibles públicamente desde una variedad de fuentes para obtener información o inteligencia. Estas fuentes pueden incluir sitios web, redes sociales, medios de comunicación, informes gubernamentales, blogs, foros y otras plataformas de acceso público.

La clave es que toda la información recopilada proviene de fuentes accesibles públicamente, lo que significa que es legal acceder a ella y utilizarla. Ejemplos muy utilizados para este fin son Maltego, DuckDuckGo, Spiderfoot, GoogleDorking y LinkedIn.



Brian Chesky  Co-founder, CEO @ Airbnb
San Francisco, California, United States - [Contact info](#)
500+ connections

+ Follow [Message](#) More

About
I am one of the founders and CEO of Airbnb.

Activity
268,364 followers
Brian hasn't posted yet
Recent posts Brian shares will be displayed here.



Joe G.  Co-founder of Airbnb and Samara
Austin, Texas, United States - [Contact info](#)
Samara 
21,935 followers - 500+ connections

+ Follow [Connect](#) More

About
Joe Gebbia is the co-founder of Airbnb and Samara. An entrepreneur from an early age, he is obsessed with igniting new ideas. Most people don't know that Joe began his life as an artist eventually double majoring in graphic design and industrial design. Airbnb's groundbreaking service began in his San Francisco living room and spread to nearly 7 million listings in more than 191 countries, changing how people trust each other. Joe has spoken globally about both entrepreneurship and design, and received numerous distinctions such as the Inc 30 under 30, and speaking at TED, Wired, and 99U. Airbnb was selected as one of the top 50 innovative companies by Fast Company, and company of the year by Inc.



Jake Kitchener  He/Him · 3rd
Compute Lead @ Airbnb
Raleigh, North Carolina, United States - [Contact info](#)
2,230 followers - 500+ connections

+ Follow [Message](#) More

About
Jake Kitchener has been closely aligned to systems management and cloud throughout his career in tech, and enjoys leadership roles focused on DevOps, cloud architecture, and shipping products. He is a coauthor of Kubernetes in the Enterprise and Hybrid Cloud Apps with OpenShift and Kubernetes. Jake dreams of team organization, pipeline, culture, and operations, with the hope of one day realizing cloud platform nirvana.



Wendy Jin  She/Her · 3rd
Engineering Manager, Security and Privacy, Data Governance in AI, Observability, Infrastructure & Product
San Francisco Bay Area - [Contact info](#)
500+ connections

+ Connect [Message](#) More

Wendy Jin

Swe Engineering
Manager in Data...



Airbnb

San Francisco, California, United States



wendy.jin@airbnb.com



wendyjinjing@gmail.com

[ceoemail.com/s.php?id=ceo-9901](#)

cholarships | Red R... Work Study and Stu... Levels in the Germa... Amazon

Airbnb, Inc. CEO Email and Telephone	
Mr Brian Chesky	CEO
Email	brian.chesky@airbnb.com
Advice from CEOemail.com	How to write your email to the CEO
Telephone Switchboard	415.800.5959 (Direct) 415-800-5959
Website	https://www.airbnb.com
Personal Twitter	@bchesky
Social Media	
Postal Address	888 Brannan St., San Francisco, CA, 94103
CIK	0001559720

Email from Corporate (High up in the chain): Catherine.powell@airbnb.com, Brian.chesky@airbnb.com, Tara.brunch@airbnb.com, David.bernstien@airbnb.com, Joe.gebbia@airbnb.com, Mike.liberatore@airbnb.com

Existe muchísima información sobre AIRBNB al ser una compañía muy grande pero la de arriba muestra los fundadores, dos o tres empleados con cargos importantes, el email personal de una empleada con un cargo clave, el telf. directo para comunicarse con el CEO, y algunos correos de los mas arriba en el escalafón de puestos de AIRBNB.

The screenshot shows the LinkedIn company profile for Airbnb. At the top, there's a navigation bar with icons for Home, My Network, Jobs, Messaging, and Notifications. Below that is a section titled 'Overview' which contains the following information:

- Website:** <http://airbnb.com>
- Verified page:** August 16, 2023
- Industry:** Software Development
- Company size:** 5,001-10,000 employees
54,748 associated members
- Headquarters:** San Francisco, CA
- Founded:** 2007
- Specialties:** travel accommodations, collaborative economy, and hospitality

Conclusiones del Ejercicio 1 – Planificación y Reconocimiento de una Organización

En este ejercicio se ha llevado a cabo la fase inicial de un engagement Red Team mediante un proceso estructurado de planificación y reconocimiento pasivo sobre la AIRBNB. La actividad incluyó la identificación de activos clave como nombres de la empresa matriz y empresas relacionadas, sistemas autónomos (ASNs), rangos de red, dominios y subdominios, cumpliendo con los objetivos establecidos.

Durante la investigación se utilizaron fuentes OSINT. Se identificaron varios dominios principales y subdominios relevantes, priorizándolos en función de su visibilidad, sensibilidad y potencial uso como vectores de acceso. Aunque no se realizaron pruebas activas agresivas, se analizaron posibles vectores de ataque considerando el tipo de servicios expuestos y la superficie de ataque observada.

Gracias a esta primera aproximación, se definió un alcance claro y realista para futuras fases del ejercicio, permitiendo estimar tiempos y recursos necesarios. En conjunto, se cumplió con éxito el objetivo de establecer las bases de una operación Red Team realista, demostrando la importancia del reconocimiento temprano y la correcta planificación antes de iniciar cualquier actividad ofensiva más avanzada.