

# **INFORME RECOPIACION DE INFORMACION**

## **FOOTPRINTING, FINGERPRINTING Y OSINT**

Mi objetivo para esta practica es la empresa Booking.com.

Booking.com es una plataforma líder a nivel mundial dedicada a la reserva de alojamientos y servicios relacionados en línea. Fundada en 1996 en los Países Bajos, la empresa ha crecido hasta convertirse en una de las mayores agencias de viajes en línea del mundo. Su modelo de negocio se centra en proporcionar a los usuarios una amplia variedad de opciones de alojamiento, desde hoteles y apartamentos hasta casas vacacionales y otros tipos de hospedaje.

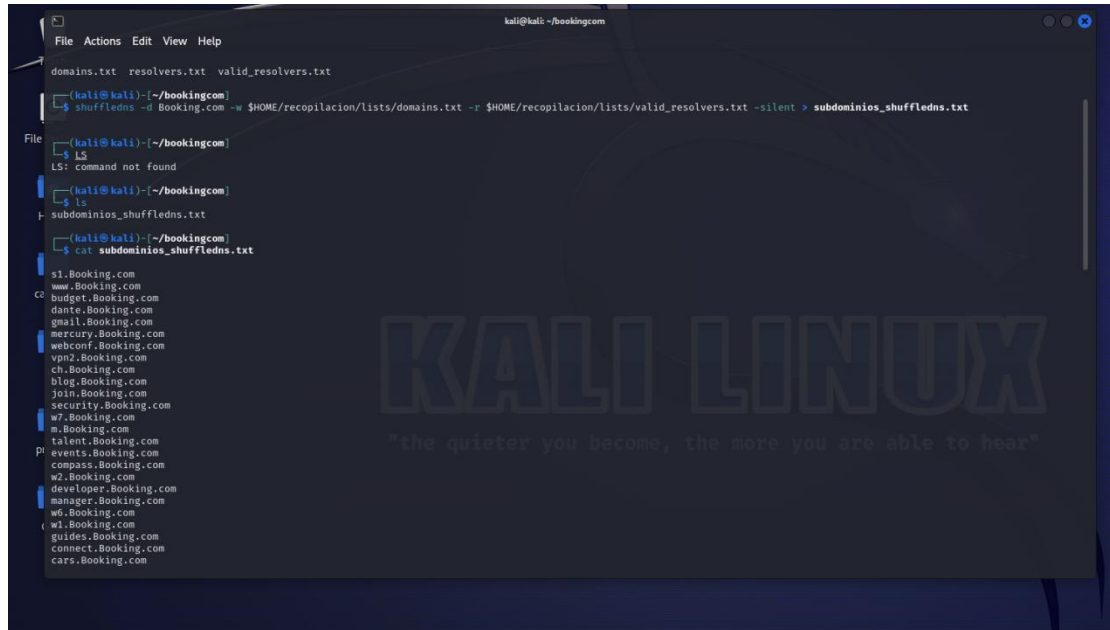
Principales puntos sobre Booking.com:

1. **Fundación y Crecimiento:** Booking.com fue fundada en Ámsterdam en 1996 y ha experimentado un rápido crecimiento desde entonces. A lo largo de los años, se ha expandido globalmente y ha diversificado su oferta de servicios.
2. **Oferta de Servicios:** La plataforma ofrece a los usuarios la posibilidad de reservar una amplia gama de alojamientos, así como servicios de transporte, alquiler de automóviles y experiencias turísticas. Proporciona opciones para todos los tipos de viajeros, desde aquellos que buscan comodidades de lujo hasta quienes prefieren opciones más económicas.
3. **Alcance Global:** Booking.com opera en todo el mundo y colabora con una extensa red de alojamientos, desde grandes cadenas hoteleras hasta propiedades independientes. Esta presencia global le permite ofrecer a los usuarios opciones en prácticamente cualquier destino.
4. **Plataforma en Línea:** La reserva de alojamientos se realiza a través de su plataforma en línea, que proporciona a los usuarios información detallada, comentarios y valoraciones de otros viajeros para ayudar en la toma de decisiones.
5. **Innovación y Tecnología:** Booking.com ha destacado por su enfoque innovador y la utilización de tecnología para mejorar la experiencia del usuario. Ha introducido características como la opción de reservar sin cargo por anticipado y la posibilidad de realizar cambios flexibles en las reservas.
6. **Impacto en la Industria:** La empresa ha tenido un impacto significativo en la industria de viajes y ha contribuido a la transformación digital del sector. Su modelo de reserva en línea ha cambiado la forma en que las personas planifican y reservan sus viajes.

# FOOTPRINTING

## SHUFFLEDNS (FUERZA BRUTA)

-He iniciado el reconocimiento horizontal de booking.com con un ataque de fuerza bruta utilizando esta herramienta y me ha devuelto varios subdominios, adjunto captura de pantalla



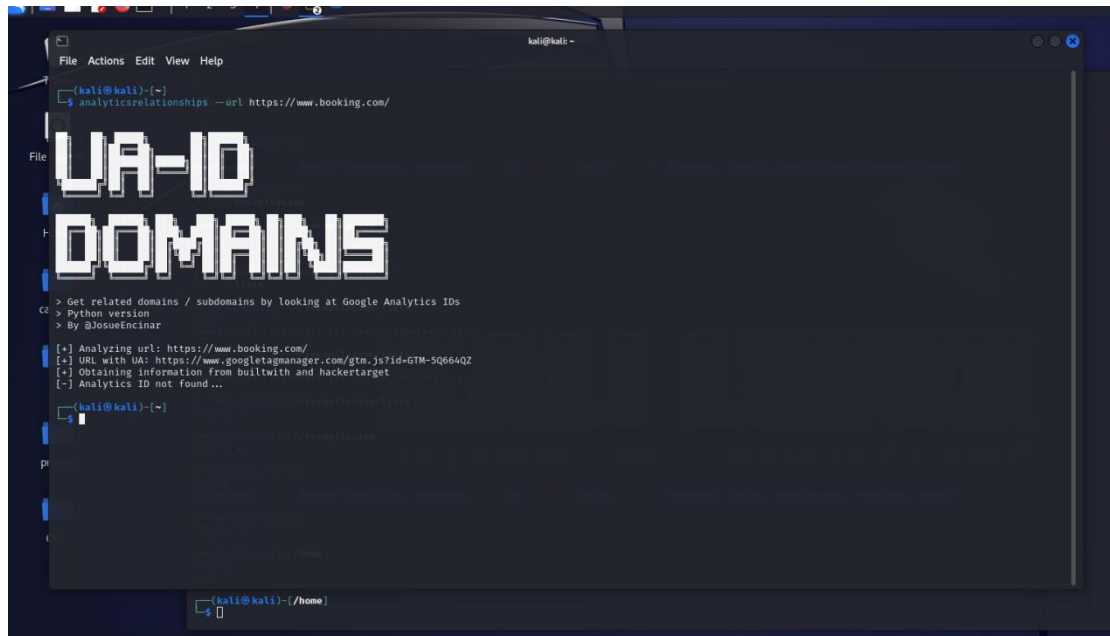
```
kali@kali: ~/booking.com
File Actions Edit View Help
domains.txt resolvers.txt valid_resolvers.txt
$ shuffledns -u Booking.com -w $HOME/recopilacion/lists/domains.txt -r $HOME/recopilacion/lists/valid_resolvers.txt -silent > subdominios_shuffledns.txt
File
$ ls
ls: command not found
$ ls
ls
subdominios_shuffledns.txt
$ cat subdominios_shuffledns.txt
s1.Booking.com
www.Booking.com
budget.Booking.com
dante.Booking.com
gmail.Booking.com
mercury.Booking.com
webconf.Booking.com
vpn2.Booking.com
ch.Booking.com
blog.Booking.com
join.Booking.com
security.Booking.com
w7.Booking.com
w.Booking.com
talent.Booking.com
events.Booking.com
compass.Booking.com
w2.Booking.com
developer.Booking.com
manager.Booking.com
w6.Booking.com
w1.Booking.com
guides.Booking.com
connect.Booking.com
cars.Booking.com
```

Una vez pasada la herramienta unfurl para limpiar la lista, me devuelve un total de 98 subdominios

## GOOGLE ANALYTICS (ANALISIS DE VULNERABILIDADES)

-He continuado usando una herramienta de analisis de google analytics, para intentar hacer una detección de subdominios pero lamentablemente en este dominio no ha encontrado nada porque no trabaja con google analytics.

Adjunto captura.



```
kali@kali: ~  
$ analyticsrelationships --url https://www.booking.com/  
  
> Get related domains / subdomains by looking at Google Analytics IDs  
> Python version  
> By @JosueEncinar  
  
[+] Analyzing url: https://www.booking.com/  
[+] URL with UA: https://www.googletagmanager.com/gtm.js?id=GTM-SQ664QZ  
[+] Obtaining information from builtwith and hackertarget  
[-] Analytics ID not found...  
  
kali@kali: ~  
$
```

## CERO (TLS PROBING)

Continuando con el proceso de footprinting he utilizado la herramienta CERO en kali linux, pero solo me ha devuelto el dominio principal como podemos ver en la captura

```
a5.booking.com
a3.booking.com
a4.booking.com
gp.booking.com
adfs.booking.com
+
(kali@kali)-[~/bookingcom]
└─$ cat subdominios_shuffledns.txt | wc
    98    98   1740
(kali@kali)-[~/bookingcom]
└─$ ls
subdominios_shuffledns.txt
C2 (kali@kali)-[~/bookingcom]
└─$ ls
subdominios_shuffledns.txt
(kali@kali)-[~/bookingcom]
└─$ cero -d booking.com
booking.com
(kali@kali)-[~/bookingcom]
└─$ cero -d www.booking.com
booking.com
(kali@kali)-[~/bookingcom]
└─$ cero
^C
pi (kali@kali)-[~/bookingcom]
└─$ cero -d booking.com > subdominios_cero
subdominios_cero: booking.com
(kali@kali)-[~/bookingcom]
└─$ cat subdominios_cero
booking.com
(kali@kali)-[~/bookingcom]
└─$
(kali@kali)-[~/home]
└─$
```

## KATANA (SCRAPPING)

He utilizado esta herramienta para hacer scraping sobre el objetivo y ver que subdominios nos encuentra de nuestro objetivo.

### LANZAMIENTO KATANA

```
kali@kali: ~/bookingcom
File Actions Edit View Help
$ echo booking.com | katana -silent -jc -o katana_output.txt -kf robotstxt,sitemapxml
https://booking.com/sitembk-incr-closed-index-hotel-reviews-https_2017-04-20.xml
https://booking.com/sitembk-reviews-index-hotel-review-https.xml
https://booking.com/sitembk-dsf-index-destinationfinder-https.xml
https://booking.com/sitembk-reviews-index-country-review-https.xml
https://booking.com/sitembk-reviews-index-region-review-https.xml
https://booking.com/sitembk-index-https.xml
https://booking.com/hotel_rt_onview
https://booking.com/sitembk-incr-closed-index-hotel-reviews-https_2017-04-21.xml
https://booking.com/sitembk-reviews-index-city-review-https.xml
https://booking.com/sitembk-articles-index-articles-https.xml
https://booking.com/sitembk-reviews-index-single-review-https.xml
https://booking.com/pbbook*
https://booking.com/pngo*
https://booking.com/hotel_attractions
https://booking.com/episode_times
https://booking.com/event
https://booking.com/track
https://booking.com/vpmlgdesktopscreensize
https://booking.com/sendlayoutevents
https://booking.com/join_js_tracking
https://booking.com/reviewlist.html
https://booking.com/product_header.html
https://booking.com/bas/*
https://booking.com/srcompset.*.html
https://booking.com/_frdtr
https://booking.com/srcompset.html
https://booking.com/fragment.json
https://booking.com/c360_v1_track
https://booking.com/hotel/us/the-airstream-van.*.html
https://booking.com/fragment.html
https://booking.com/asapi/*
https://booking.com/logrt_blocks_order
https://booking.com/squeak
https://booking.com/c360/v1/track
https://booking.com/js_tracking
https://booking.com/js_errors
https://booking.com/fragment.*.json
https://booking.com/fragment.*.html
https://booking.com/*_hi.html
https://booking.com/free-cancellation/index.*
https://booking.com/deals-special-offers/index.*
https://booking.com/we-speak-your-language/index.*
```

Hemos utilizado la herramienta unfurl para que nos filtre los resultados obtenidos y que solo son de los dominios únicos y el resultado lo hemos volcado en otro fichero.

```
kali@kali: ~/bookingcom
File Actions Edit View Help
(kali@kali)~$ ls
bookingcom  cero  Desktop  Documents  Downloads  gau  go  katana  Music  nuclei  Pictures  Public  recopilacion  Templates  Videos
(kali@kali)~$ cd bookingcom
(kali@kali)~/bookingcom$ ls
katana_output.txt  subdominios_cero  subdominios_shuffledns.txt
(kali@kali)~/bookingcom$ cat katana_output.txt | unfurl -u domains > subdominios_katana.txt
(kali@kali)~/bookingcom$ cat subdominios_katana.txt
booking.com
www.booking.com
secure.booking.com
business.booking.com
join.booking.com
partner.booking.com
account.booking.com
taxi-support.booking.com
taxi.booking.com
cars.booking.com
spadmin.booking.com
admin.booking.com
careers.booking.com
experiences.booking.com
news.booking.com
www.sustainability.booking.com
```

En total he obtenido 16 subdominios con esta herramienta.

## CTFR (BUSQUEDA EN REGISTROS DE CERTIFICADOS SSL)

Utilizamos esta herramienta para buscar certificados ssl en el registro.

### BUSQUEDA

```
kali@kali: ~/bookingcom
File Actions Edit View Help
(kali@kali)~(~/bookingcom)
$ ctfr -d booking.com

CTFR

Version 1.2 - Hey don't miss AXFR!
Made by Sheila A. Berta (UnaPiGeek)

[!] --- TARGET: booking.com --- [!]

[!] *2017--booking.com
2017--booking.com
[!] *ams4.dev.booking.com
ams4.dev.booking.com
Booking.com BV
[!] *ams4.dqs.booking.com
ams4.dqs.booking.com
Booking.com BV
[!] *ams4.lon.booking.com
ams4.lon.booking.com
Booking.com BV
[!] *ams4.prod.booking.com
ams4.prod.booking.com
Booking.com BV
[!] *anycast.dqs.booking.com
anycast.dqs.booking.com
Booking.com BV
[!] *anycast.prod.booking.com
anycast.prod.booking.com
Booking.com BV
[!] *api.booking.com
api.booking.com
[!] *api.booking.com
api.booking.com
[!] *artifactory.booking.com
artifactory.booking.com
```

### DOMINIOS OBTENIDOS

```
kali@kali: ~/bookingcom
File Actions Edit View Help
[!] vpn.booking.com
www.vpn.booking.com
[!] www.secure--booking.com

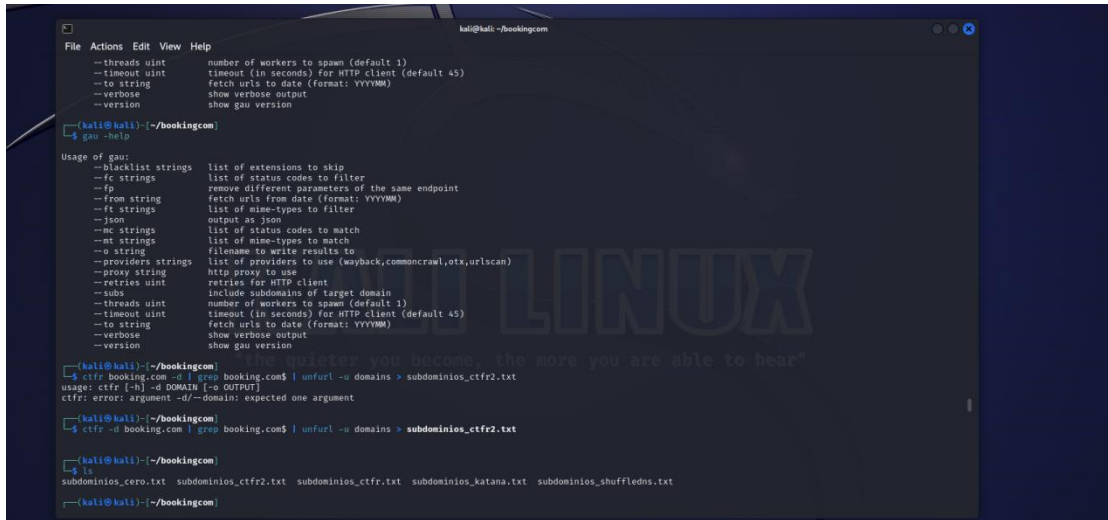
[!] Done. Have a nice day! ;).

(kali@kali)~(~/bookingcom)
$ cat subdominios_ctfr2.txt | unfurl -u domains > subdominios_ctfr.txt

(kali@kali)~(~/bookingcom)
$ ls
subdominios_cero.txt subdominios_ctfr2.txt subdominios_ctfr.txt subdominios_katana.txt subdominios_shuffledns.txt

(kali@kali)~(~/bookingcom)
$ cat subdominios_ctfr.txt
2017--booking.com
ams4.dev.booking.com
ams4.dqs.booking.com
ams4.lon.booking.com
ams4.prod.booking.com
anycast.dqs.booking.com
anycast.prod.booking.com
api.booking.com
artifactory.booking.com
*jfrog.booking.com
jfrog.booking.com
ashl.corp.booking.com
ashl.prod.booking.com
bk-eu-west4.prod.booking.com
BOOKING.COM
booking.com
bpad.booking.com
dev.booking.com
dev.taxi.booking.com
dxi.booking.com
insurance.booking.com
preview.suite.booking.com
publish.suite.booking.com
qa.taxi.booking.com
rm.booking.com
suite.booking.com
suiteoffice.booking.com
```

UTILIZAMOS GREP PARA QUE NOS SAQUE SOLO LOS RESULTADOS QUE ACABEN EN BOOKING.COM



```
kali@kali: ~/bookingcom
File Actions Edit View Help
--threads uint    number of workers to spawn (default 1)
--timeout uint    timeout (in seconds) for HTTP client (default 45)
--to string       fetch url's to date (format: YYYYMM)
--verbose         show verbose output
--version         show gau version

[kali@kali]~/bookingcom$ gau -help

Usage of gau:
--blacklist strings  list of extensions to skip
--fp strings         list of status codes to filter
--fp                remove different parameters of the same endpoint
--from string       fetch url's from date (format: YYYYMM)
--ft strings        list of mime-types to filter
--json              output as json
--mc strings        list of status codes to match
--mt strings        list of mime-types to match
--o string          filename to write results to
--providers strings list of providers to use (wayback,commoncrawl,otx,urlscan)
--proxy string      http proxy to use
--retries uint      retries for HTTP client
--subs             include subdomains of target domain
--threads uint     number of workers to spawn (default 1)
--timeout uint     timeout (in seconds) for HTTP client (default 45)
--to string        fetch url's to date (format: YYYYMM)
--verbose          show verbose output
--version          show gau version

[kali@kali]~/bookingcom$ ctfr booking.com | grep booking.com | unfurl -u domains > subdominios_ctfr2.txt
usage: ctfr [-h] -d DOMAIN [-o OUTPUT]
ctfr: error: argument -d/--domain: expected one argument

[kali@kali]~/bookingcom$ ctfr -d booking.com | grep booking.com | unfurl -u domains > subdominios_ctfr2.txt

[kali@kali]~/bookingcom$ ls
subdominios_cero.txt  subdominios_ctfr2.txt  subdominios_katana.txt  subdominios_shuffledns.txt

[kali@kali]~/bookingcom$
```

Después de este proceso hemos obtenido 945 subdominios.



## GAU (ANALISIS DE CACHE)

Realizamos un análisis de caché sobre nuestro objetivo utilizando la herramienta gau

## LANZAMIENTO GAU

```

kali@kali:~/bookimgcom]
$ ls
subdominios_cero.txt  subdominios_ctfr.txt  subdominios_katana.txt  subdominios_shuffledns.txt

kali@kali:~/bookimgcom]
$ cd ~
kali@kali:~]
bookimgcom
kali@kali:~/bookimgcom]
$ ls
subdominios_cero.txt  subdominios_ctfr.txt  subdominios_katana.txt  subdominios_shuffledns.txt

kali@kali:~/bookimgcom]
$ gau --threat 5 booking.com --o subdominios_gau2.txt
unknown flag: --threat
Usage of gau:
  -blacklist strings  list of extensions to skip
  -fc strings         list of status codes to filter
  -fp                remove different parameters of the same endpoint
  -from string        fetch urls from date (format: YYYYMM)
  -ft strings         list of mime-types to filter
  -json              output as json
  -mc strings         list of status codes to match
  -mt strings         list of mime-types to match
  -o string           filename to write results to
  -providers strings  list of providers to use (wayback,commoncrawl,otx,urlscan)
  -proxy string       http proxy to use
  -retries uint       retries for HTTP client
  -subs              include subdomains of target domain
  -threads uint       number of workers to spawn (default 1)
  -timeout uint       timeout (in seconds) for HTTP client (default 45)
  -to string          fetch urls to date (format: YYYYMM)
  -verbose            show verbose output
  -version            show gau version

kali@kali:~/bookimgcom]
$ gau --threads 5 booking.com --o subdominios_gau2.txt
WARN[0000] error reading config: open /home/kali/.gau.toml: no such file or directory
ls

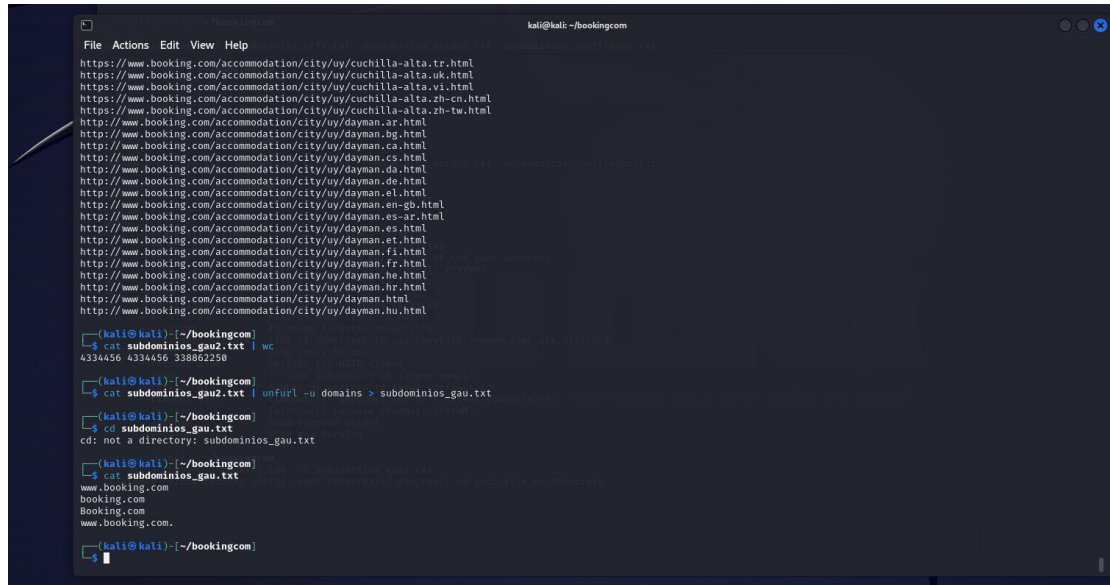
```

Nos devuelve bastantes urls:

```
File Actions Edit View Help
kali@kali:~$ cd /root/.ssh/
cd bookingcom
kali@kali:~/bookingcom$ ls
subdominios_cero.txt subdominios_cttfr.txt subdominios_gau2.txt subdominios_katana.txt subdominios_shuffledns.txt
kali@kali:~/bookingcom$ cat subdominios_gau2.txt
http://www.booking.com/80/
https://www.booking.com/
https://www.booking.com/
https://www.booking.com/
https://www.booking.com/
https://www.booking.com/
http://booking.com/
https://booking.com/
https://booking.com/
https://www.booking.com/
http://booking.com/
https://www.booking.com/
https://www.booking.com/
https://www.booking.com/6go
http://www.booking.com/80/!RSTB_ERROR_NCURL_IGNORE_ALL
https://www.booking.com/?z22
http://www.booking.com/?z22&z22
http://www.booking.com/?z22&Z%3C%7A%2D_black
https://www.booking.com/?z22_z22
https://www.booking.com/?z22_z22alts
https://www.booking.com/?z22_z22imageX&z22=https://cnt/uploads/logos/booking-com.jpg?f60694191","aggregateRating":{"type":"AggregateRating"},"ratingValue":5.00},"worstRating":1,"bestRating":5","ratingCount":2}
https://booking.com/z22_z22&z22=z22bstatic.com
http://www.booking.com/z22htts://e-ec.bstatic.com/static/img/icons/circles/X7BK7eb_blockX7DK7DX7K7Bb_class_halF7DK7ToxTerrenn.png?z22/
http://booking.com/80/X22rel-X22nofollow
https://www.booking.com/80/8
https://www.booking.com/$$$8767$$$?cmd=get_file&arg=block_style.css&suid=85362E8D1CFE5ECFCFE40FAC6DD1ABCA1AE542
https://www.booking.com/$$$8767$$$?cmd=get_file&arg=block_style.css&suid=CBCBD3093618C45338AACBP93F495F54B68512
https://www.booking.com/$$$8767$$$?cmd=get_file&arg=block_style.css&suid=EBC1D5D4BEED99098357DC8E8821652377D508BBAC
https://www.booking.com/$$$8767$$$?cmd=get_file&arg=images/block_png&suid=A1FB8DAEA9EF2F2FA434902C43AF4ADDB2854
```

ENRIQUE LÓPEZ PASCUAL  
RECOPILACION DE INFORMACIÓN

## SACAMOS LOS DOMINIOS UNICOS Y LIMPIAMOS EL ARCHIVO



```
kali@kali: ~/bookingcom
File Actions Edit View Help
https://www.booking.com/accommodation/city/uy/cuchilla-alta.tr.html
https://www.booking.com/accommodation/city/uy/cuchilla-alta.uk.html
https://www.booking.com/accommodation/city/uy/cuchilla-alta.vi.html
https://www.booking.com/accommodation/city/uy/cuchilla-alta.zh-cn.html
https://www.booking.com/accommodation/city/uy/cuchilla-alta.zh-tw.html
http://www.booking.com/accommodation/city/uy/dayman.ar.html
http://www.booking.com/accommodation/city/uy/dayman.bg.html
http://www.booking.com/accommodation/city/uy/dayman.ca.html
http://www.booking.com/accommodation/city/uy/dayman.cs.html
http://www.booking.com/accommodation/city/uy/dayman.da.html
http://www.booking.com/accommodation/city/uy/dayman.de.html
http://www.booking.com/accommodation/city/uy/dayman.el.html
http://www.booking.com/accommodation/city/uy/dayman.en-gb.html
http://www.booking.com/accommodation/city/uy/dayman.es-ar.html
http://www.booking.com/accommodation/city/uy/dayman.es.html
http://www.booking.com/accommodation/city/uy/dayman.et.html
http://www.booking.com/accommodation/city/uy/dayman.fi.html
http://www.booking.com/accommodation/city/uy/dayman.fr.html
http://www.booking.com/accommodation/city/uy/dayman.he.html
http://www.booking.com/accommodation/city/uy/dayman.hr.html
http://www.booking.com/accommodation/city/uy/dayman.html
http://www.booking.com/accommodation/city/uy/dayman.hu.html

(kali@kali) [~/bookingcom]
$ cat subdominios_gau2.txt | wc
4334456 4334456 33886258

(kali@kali) [~/bookingcom]
$ cat subdominios_gau2.txt | unfurl -u domains > subdominios_gau.txt

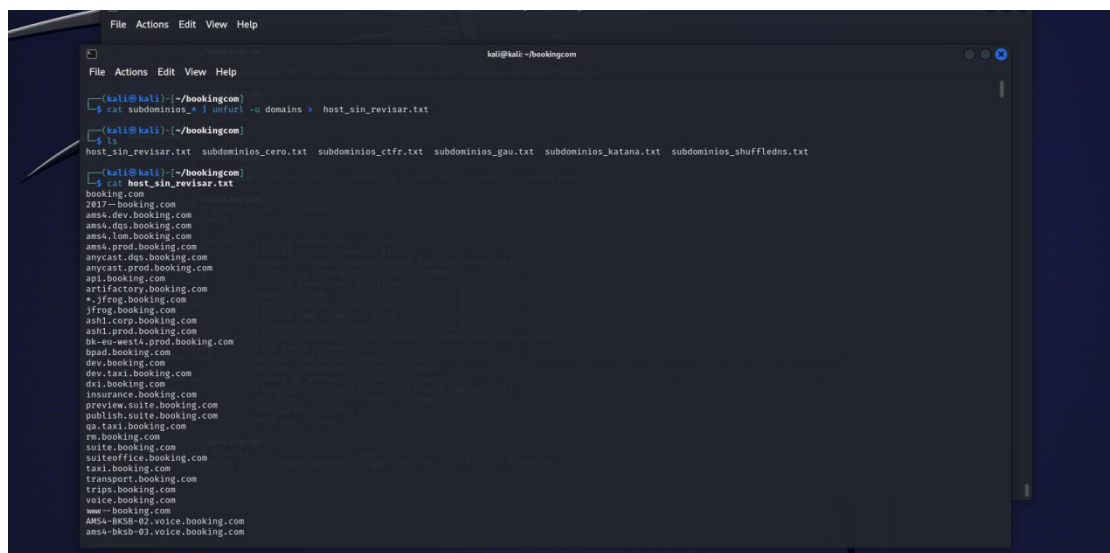
(kali@kali) [~/bookingcom]
$ cd subdominios_gau.txt
cd: not a directory: subdominios_gau.txt

(kali@kali) [~/bookingcom]
$ cat subdominios_gau.txt
www.booking.com
booking.com
Booking.com
www.booking.com.

(kali@kali) [~/bookingcom]
$
```

Una vez limpia nuestra lista de subdominios obtenida anteriormente, solo obtenemos 4 subdominios.

## LLEGADOS A ESTE PUNTO, JUNTAMOS TODOS LOS ARCHIVOS Y LIMPIAMOS LOS DOMINIOS DUPLICADOS



```
kali@kali: ~/bookingcom
File Actions Edit View Help
(kali@kali) [~/bookingcom]
$ cat subdominios_* | unfurl -u domains > host_sin_revisar.txt

(kali@kali) [~/bookingcom]
$ ls
host_sin_revisar.txt subdominios_cero.txt subdominios_ctfr.txt subdominios_gau.txt subdominios_katana.txt subdominios_shuffledns.txt

(kali@kali) [~/bookingcom]
$ cat host_sin_revisar.txt
booking.com
2817-booking.com
ams4.dev.booking.com
ams4.dqs.booking.com
ams4.lom.booking.com
ams4.prod.booking.com
anycast.dqs.booking.com
anycast.prod.booking.com
api.booking.com
artifactory.booking.com
*.jfrog.booking.com
jfrog.booking.com
ash1.corp.booking.com
ash1.prod.booking.com
bk-eu-west4.prod.booking.com
bpad.booking.com
dev.booking.com
dev.taxi.booking.com
dx1.booking.com
insurance.booking.com
preview.suite.booking.com
publish.suite.booking.com
qa.taxi.booking.com
rm.booking.com
suite.booking.com
suiteoffice.booking.com
taxi.booking.com
transport.booking.com
trips.booking.com
voice.booking.com
www-booking.com
ams4-bkcs-02.voice.booking.com
ams4-bkcs-03.voice.booking.com
```

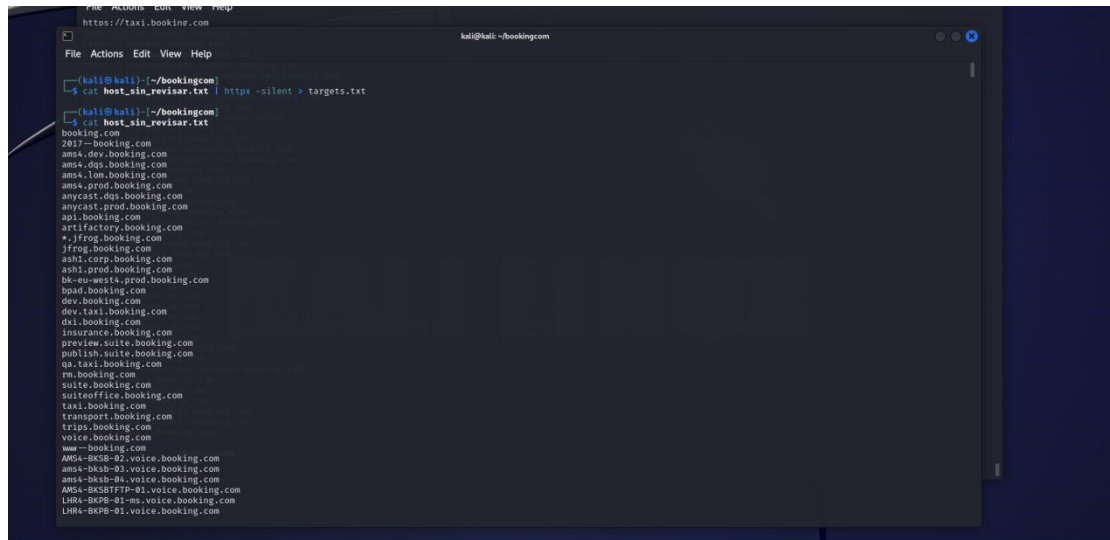
Con el código que vemos en la imagen, hemos juntado todos los subdominios obtenidos hasta ahora en un mismo fichero, en total contamos ahora mismo con 1048 subdominios de los cuales vamos a comprobar cuales de todos son válidos.

# FINGERPRINTING

## HTTPX (COMPROBACION VALIDEZ DE LOS DOMINIOS)

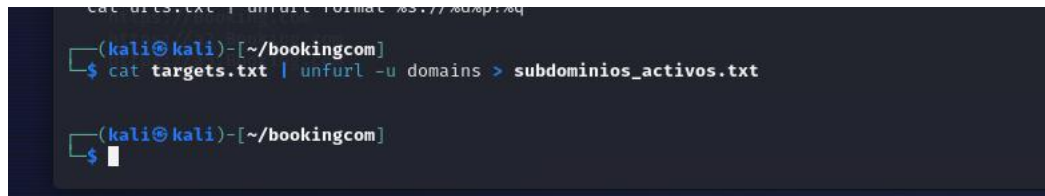
Esta herramienta nos permite hacer fingerprinting sobre HTTP. También nos permite validar de una lista de dominios cuales están activos y cuales no.

Al fichero que hemos creado, juntando todos y limpiando los dominios duplicados, le pasamos esta herramienta para comprobar la validez de los dominios y guardamos los resultados en un fichero nuevo.



```
https://taxi.booking.com
File Actions Edit View Help
kali@kali: ~/bookingcom
kali@kali:~/bookingcom$ httpx -silent > targets.txt
kali@kali:~/bookingcom$ cat host_in_revisar.txt
booking.com
2017--booking.com
amss-dev.booking.com
amss-dqs.booking.com
amss-lon.booking.com
amss-prod.booking.com
anycast-dqs.booking.com
anycast-prod.booking.com
api.booking.com
artifactory.booking.com
*.jfrog.booking.com
jfrog.booking.com
ash1.corp.booking.com
ash1-prod.booking.com
bk-eu-west-1-prod.booking.com
bpad.booking.com
dev.booking.com
dev-taxi.booking.com
dxi.booking.com
insurance.booking.com
preview-suite.booking.com
publish-suite.booking.com
qa-taxi.booking.com
rm.booking.com
suite.booking.com
suiteoffice.booking.com
taxi.booking.com
transport.booking.com
trips.booking.com
voice.booking.com
www--booking.com
AMS4-BKPB-02.voice.booking.com
AMS4-BKPB-03.voice.booking.com
AMS4-BKPB-04.voice.booking.com
AMS4-BKPB-TTP-01.voice.booking.com
LHR4-BKPB-01-ms.voice.booking.com
LHR4-BKPB-01.voice.booking.com
```

Pasamos la herramienta “unfurl” a los resultados para quedarnos solo con los dominios unicos



```
cat targets.txt | unfurl -u domains > subdominios_activos.txt
kali@kali:~/bookingcom$ cat targets.txt | unfurl -u domains > subdominios_activos.txt
kali@kali:~/bookingcom$
```

En total contamos ahora mismo con 108 dominios activos.

Esta herramienta nos da los siguientes resultados:

```
subdominios_activos.txt subdominios_ciffr.txt subdominios_katamrkt.txt targets.txt
(kali@kali)~/bookingcom$ cat subdominios_activos.txt
admin.booking.com
admin.booking.com
a1.booking.com
Booking.com
a2.booking.com
a5.booking.com
a2.booking.com
a4.booking.com
account.booking.com
affiliates.booking.com
account.booking.com
about.booking.com
api.booking.com
api.booking.com
b3.booking.com
b2.booking.com
b1.booking.com
b5.booking.com
booking.com
bookingmcm.itspublic.booking.com
budget.booking.com
bugs.booking.com
blog.booking.com
c.booking.com
cares.booking.com
calendar.booking.com
cars.booking.com
cars.booking.com
business.booking.com
business.booking.com
chat.booking.com
ch.booking.com
click.booking.com
click.booking.com
chainssupport.booking.com
careers.booking.com
careers.booking.com
compliance.booking.com
connectivity.booking.com
```

Podemos observar algun dominio interesante, como estos, que contienen la palabra admin:

<https://admin.booking.com>

<https://admin.Booking.com>

<http://spadmin.booking.com>

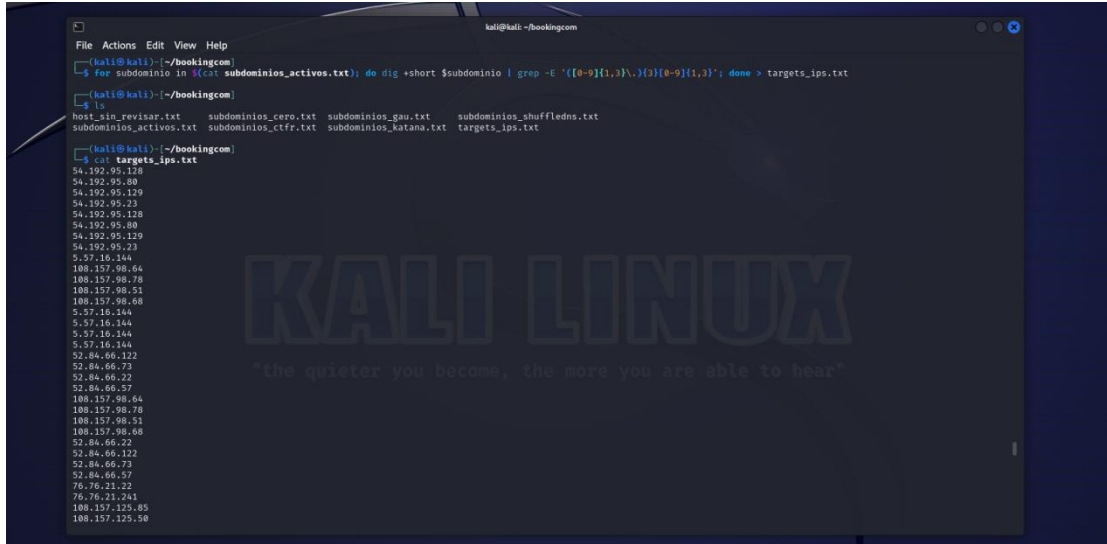
O estos otros que contiene la palabra developers (desarrolladores)

<https://developer.Booking.com>

<https://developers.Booking.com>

EN EL SIGUIENTE PASO VAMOS A CONVERTIR LOS DOMINIOS A IPS PARA PODER EMPEZAR CON LOS ESCANEOS DE LOS DOMINIOS CON LA HERRAMIENTA MASSCAN, PARA ELLO EJECUTAMOS EL SIGUIENTE CODIGO:

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



The screenshot shows a Kali Linux terminal window with the following content:

```
kali@kali:~/bookngcom
File Actions Edit View Help
kali@kali:~/bookngcom
$ for subdominio in $(cat subdominios_activos.txt); do dig +short $subdominio | grep -E '([0-9]{1,3}\.){3}[0-9]{1,3}'; done > targets_ips.txt
kali@kali:~/bookngcom
$ ls
host_sin_revisar.txt  subdominios_cero.txt  subdominios_gau.txt  subdominios_shuffledns.txt
subdominios_activos.txt  subdominios_ctfr.txt  subdominios_katana.txt  targets_ips.txt
kali@kali:~/bookngcom
$ cat targets_ips.txt
54.192.95.128
54.192.95.80
54.192.95.129
54.192.95.23
54.192.95.128
54.192.95.80
54.192.95.129
54.192.95.23
5.57.16.144
188.157.98.64
188.157.98.78
188.157.98.51
188.157.98.68
5.57.16.144
5.57.16.144
5.57.16.144
5.57.16.144
52.84.66.122
52.84.66.73
52.84.66.22
52.84.66.57
188.157.98.64
188.157.98.78
188.157.98.51
188.157.98.68
52.84.66.22
52.84.66.122
52.84.66.73
52.84.66.57
76.76.21.22
76.76.21.241
188.157.125.85
188.157.125.50
```

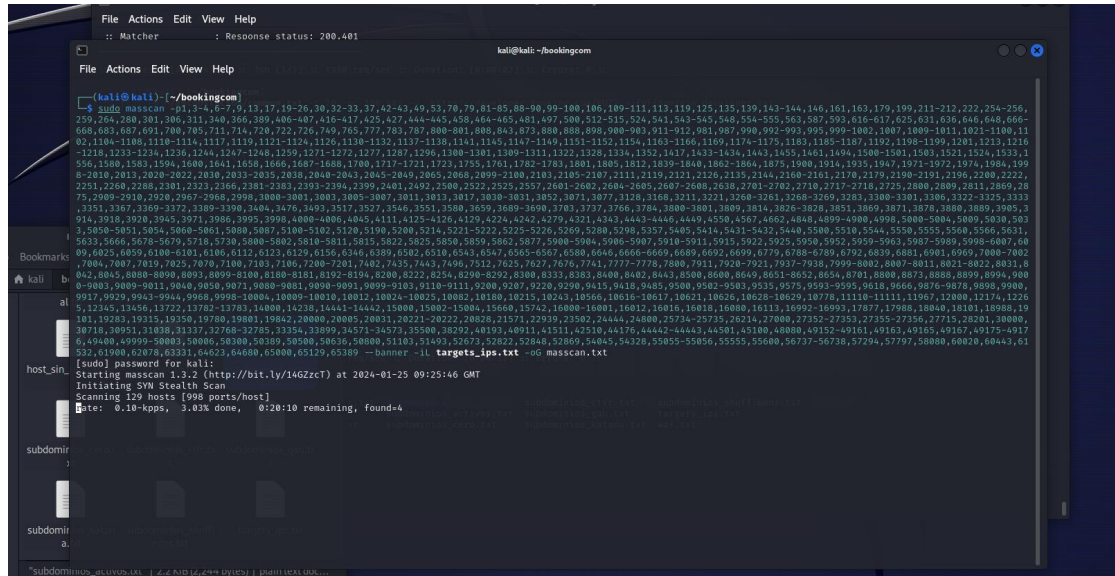
## MASSCAN (ESCANEEO DE PUERTOS)

Realizamos escaneo de los dominios activos con la herramienta masscan.

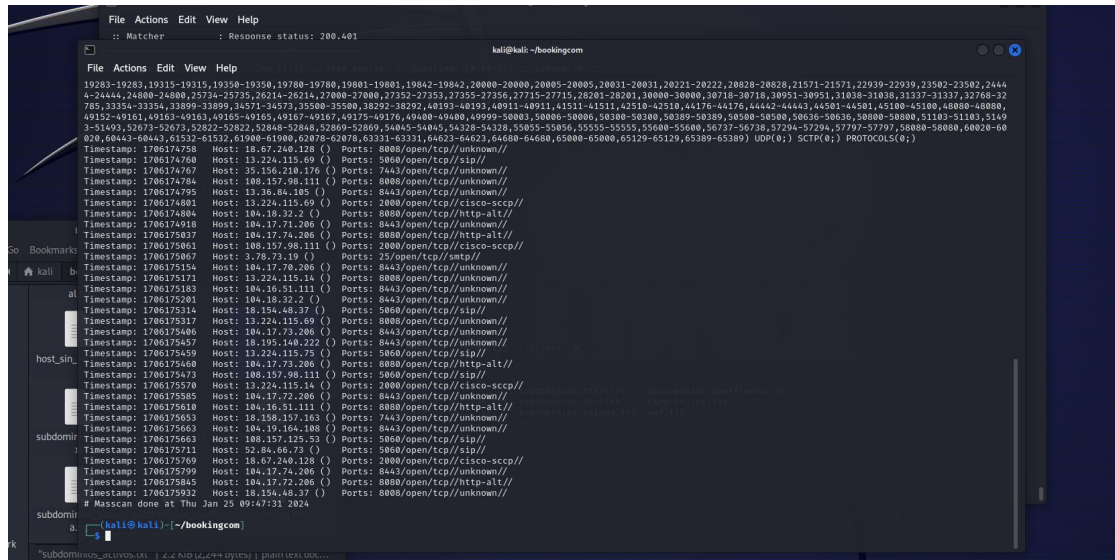
Hemos quitado los puertos 80 y 443 para que solo nos devuelva puertos destacables.

Con esta herramienta buscamos escanear el máximo numero de ips e el menos tiempo posible.

## LANZAMIENTO



## OUTPUT (PUERTOS ENCONTRADOS)



Algunos puertos que podrían ser de interés son:

1. Puertos 8008, 7443, 8443:

- Etiquetado como "unknown". Puede ser interesante investigar para determinar qué aplicación o servicio utiliza este puerto. Los puertos etiquetados como "unknown" a menudo requieren una mayor atención, ya que podrían ser utilizados por servicios no estándar.

2. Puerto 5060:

- Utilizado para SIP (Session Initiation Protocol) en comunicaciones VoIP. Podría ser de interés para evaluar la seguridad de las comunicaciones VoIP si se utilizan en el entorno analizado.

4. Puerto 8080:

- Etiquetado como "http-alt". Podría ser de interés para revisar servicios web alternativos en el sistema. Asegúrate de que los servicios configurados en este puerto estén debidamente protegidos.

6. Puerto 2000:

- Etiquetado como "cisco-sccp". Este puerto se asocia con el protocolo Skinny Client Control Protocol de Cisco. Si no se están utilizando dispositivos de telefonía IP de Cisco, podría ser interesante investigar por qué este puerto está abierto.

7. Puerto 25:

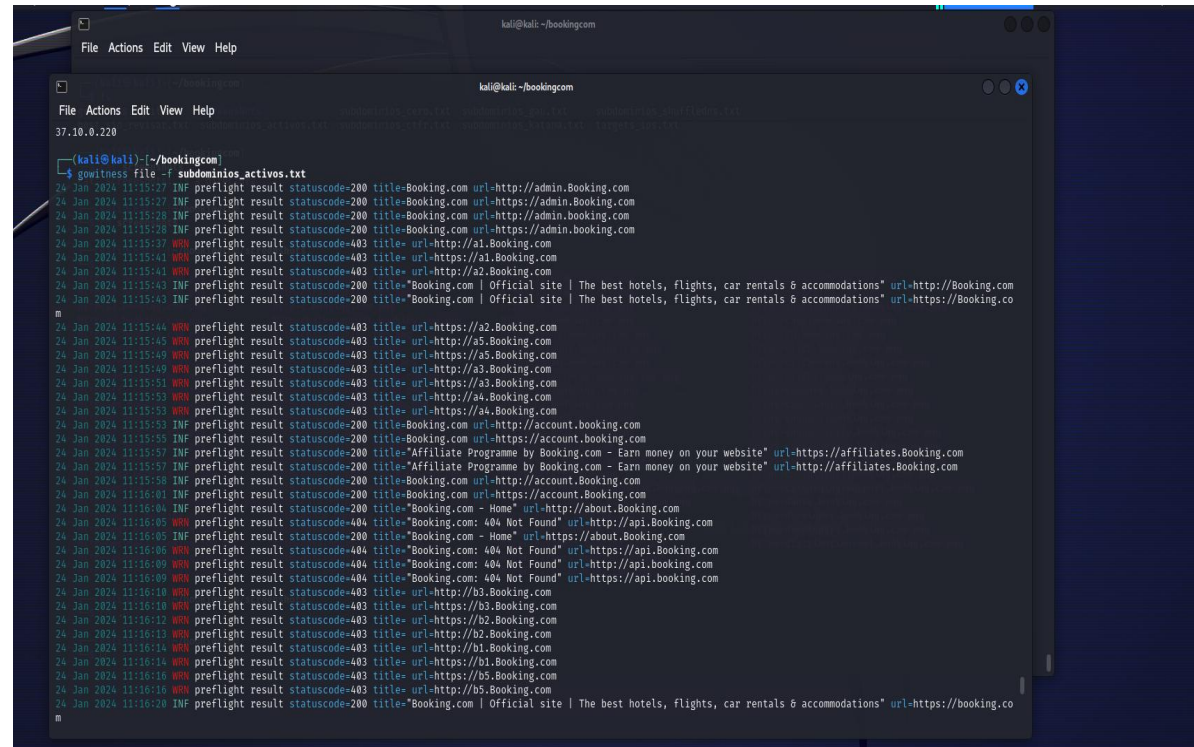
- Utilizado para SMTP. Podría ser de interés para evaluar la seguridad del servidor de correo si está presente en el entorno analizado.



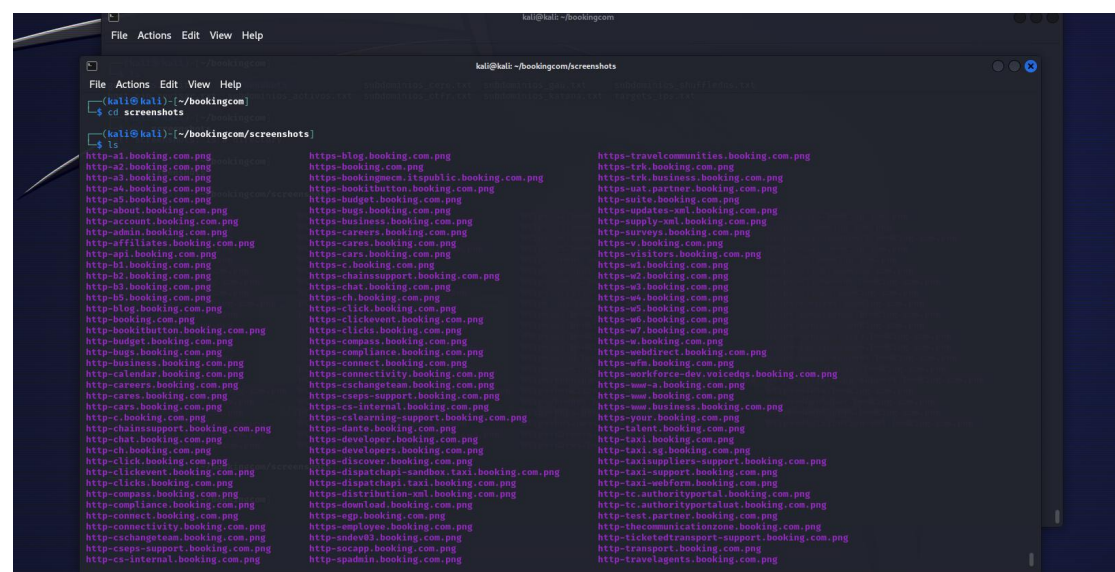
## GOWITNESS

Esta herramienta trabaja con subdominios de nuestra lista de subdominios. Vamos a realizar un análisis que incluye capturas de pantalla.

## LANZAMIENTO



## COMPROBAMOS QUE NOS HA GENERADO LAS IMAGENES



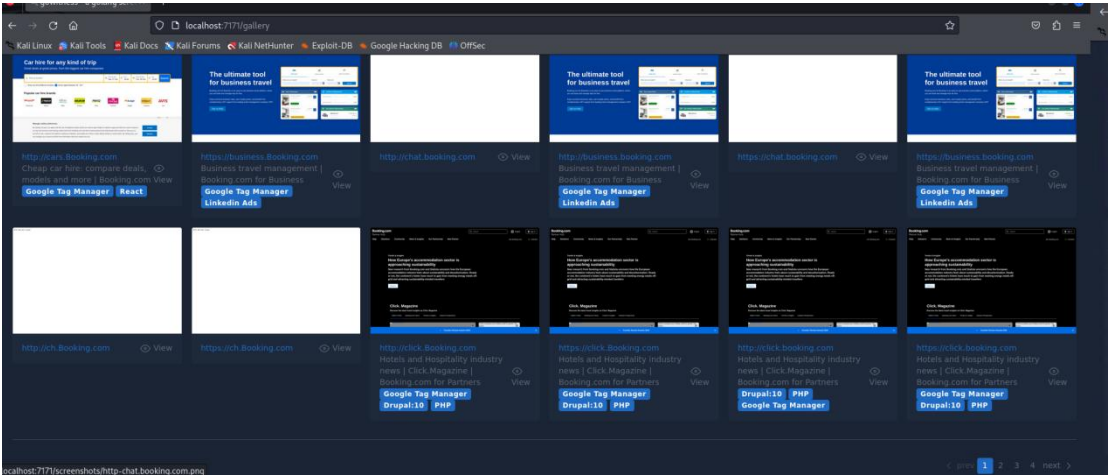
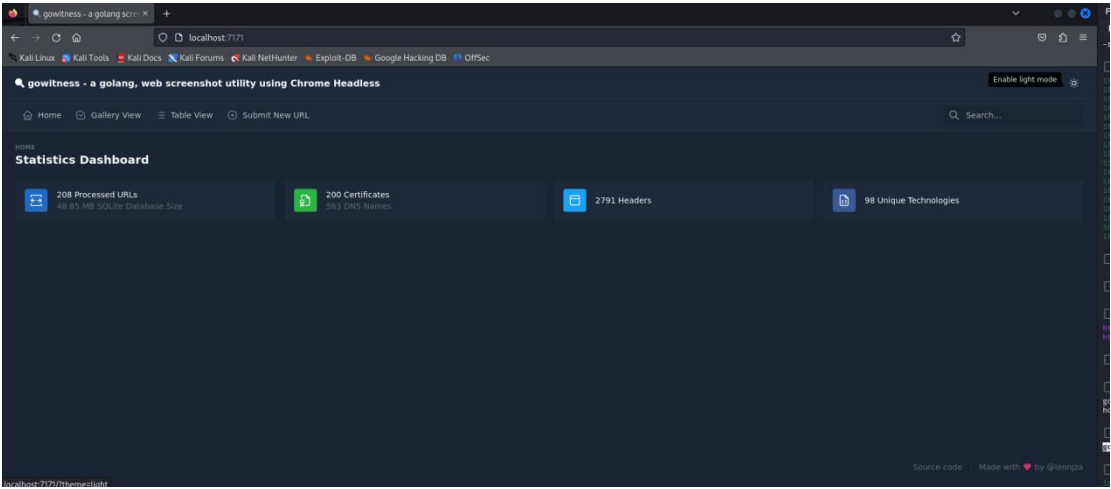


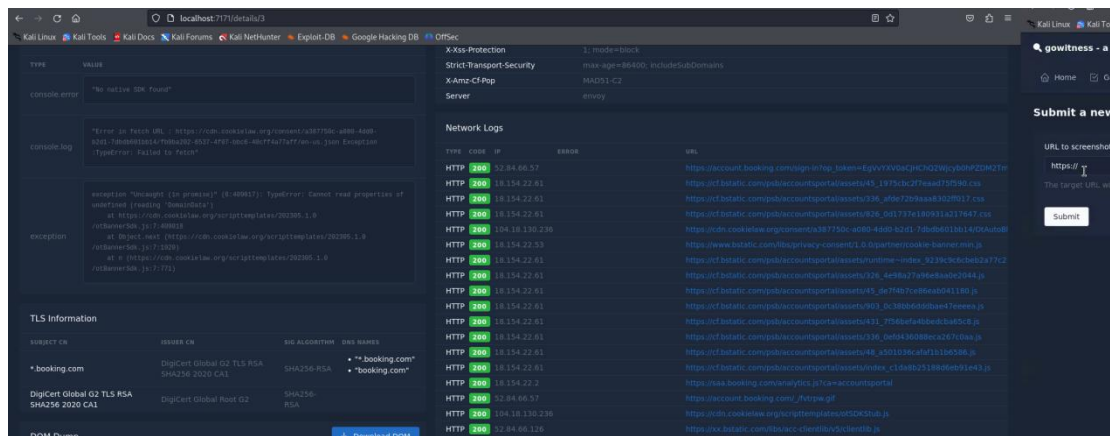
Ahora vamos a crear un servidor web local, al ejecutar el siguiente codigo, con lo que podremos acceder a la web y consultar las capturas y demás detalles

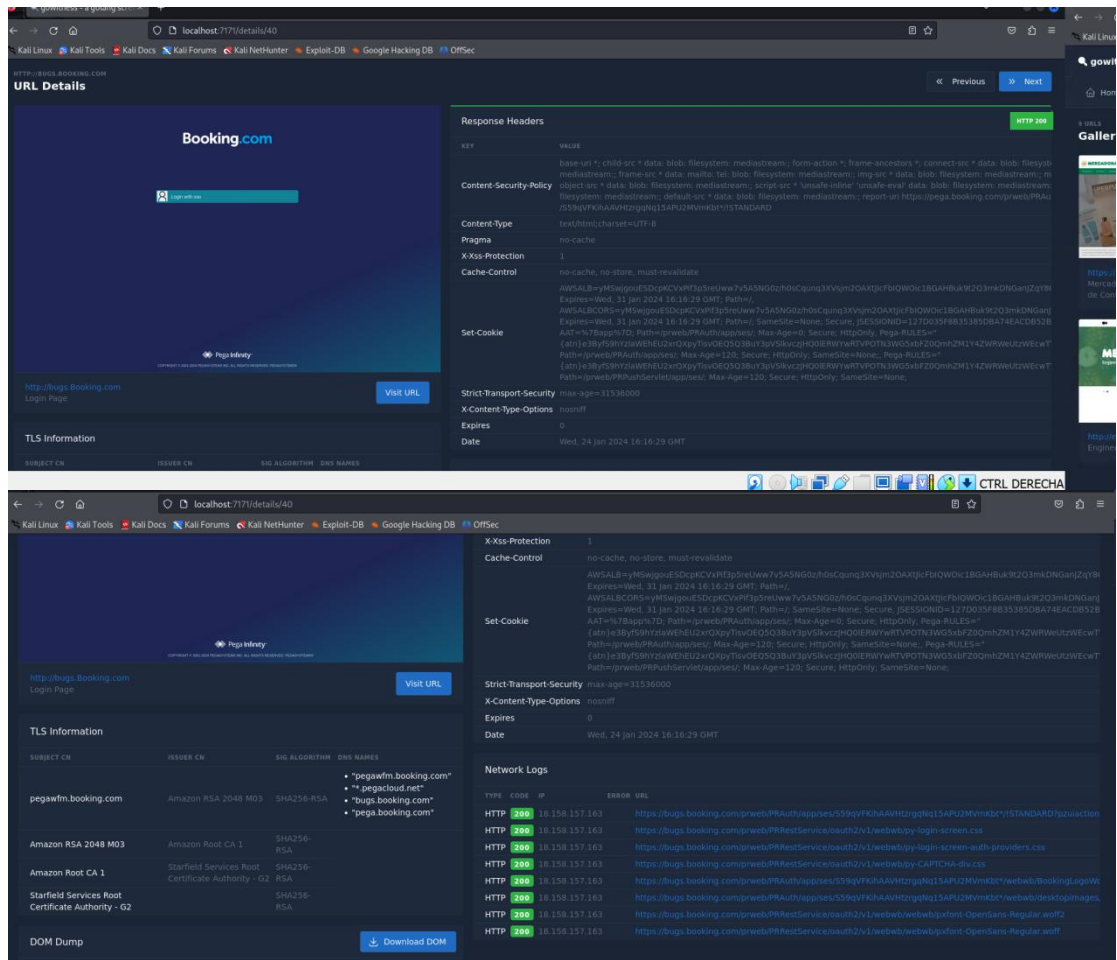
gowitness server <http://localhost:7171>

```
(kali@kali)-[~/bookingcom]
└─$ gowitness server http://localhost:7171

24 Jan 2024 11:43:45 INF db path path=sqlite://gowitness.sqlite3
24 Jan 2024 11:43:45 INF screenshot path path=screenshots
24 Jan 2024 11:43:45 INF basepath base-path=/
24 Jan 2024 11:43:45 INF server listening address=localhost:7171
[GIN] 2024/01/24 - 11:44:02 | 200 | 3.632157ms | 127.0.0.1 | GET | "/"
[GIN] 2024/01/24 - 11:44:02 | 200 | 2.62797ms | 127.0.0.1 | GET | "/assets/js/tabler.min.js"
[GIN] 2024/01/24 - 11:44:02 | 200 | 4.136463ms | 127.0.0.1 | GET | "/assets/css/tabler.min.css"
[GIN] 2024/01/24 - 11:44:02 | 404 | 3.121µs | 127.0.0.1 | GET | "/favicon.ico"
```







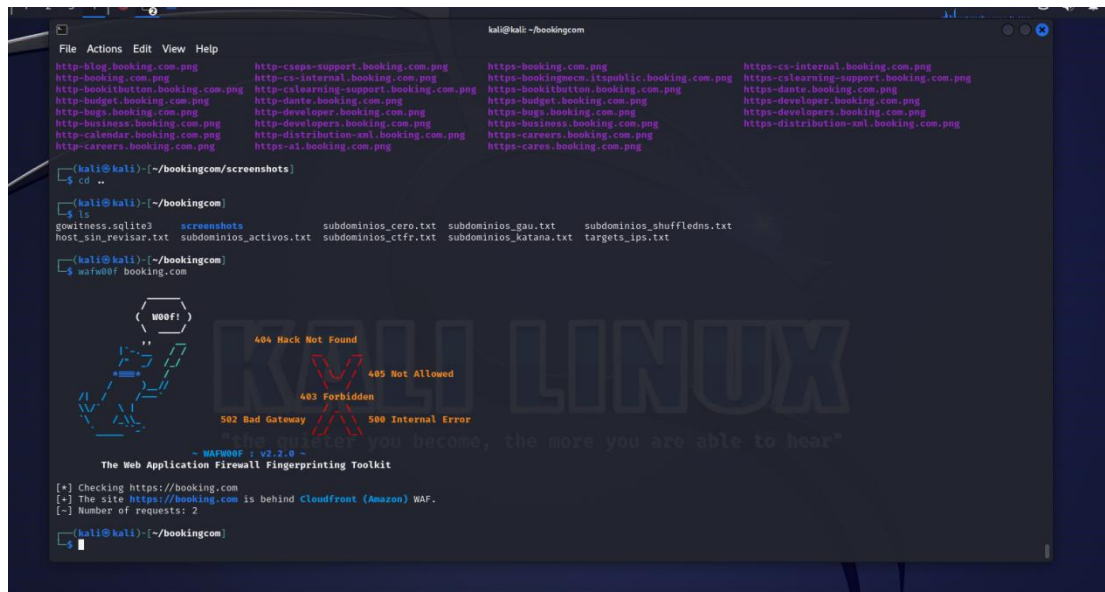
Encontramos capturas de pantalla que pueden ser interesantes, alguna con la palabra admin donde encontramos un login.

## WAFF (DETECTOR WEB APPLICATION FIREBALL)

Para el siguiente paso, vamos a comprobar si en el dominio objetivo hay waff o no.

Es un firewall que analiza las peticiones que le llega a un servidor web y esas peticiones las bloquea o las deja pasar.

En el caso de que tenga waff, es importante detectar cual es.



Como vemos en la imagen, comprobamos que efectivamente el dominio booking.com tiene waf, en este caso Cloudfront (Amazon).

Seria interesante comprobar el resto de subdominios para comprobar si hay alguno sin waf

## FUFF (DESCUBRIMIENTO DE CONTENIDO)

Vamos a descargar una lista de carpetas o archivos que puedan contener información sensible, y comprobar si esa lista está en uno de nuestros subdominios.

En este caso lo vamos a realizar sobre el dominio principal y sobre los dominios sensibles.

### LANZAMIENTO CONTRA BOOKING.COM

```
(kali@kali)-[~/bookingcom]
└─$ ffuf -w ~/recopilacion/common.txt -t 20 -mc 200,401 -u https://booking.com/FUZZ > fuff.txt

v2.1.0-dev

:: Method      : GET
:: URL         : https://booking.com/FUZZ
:: Wordlist     : FUZZ: /home/kali/recopilacion/common.txt
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 20
:: Matcher     : Response status: 200,401

:: Progress: [4727/4727] :: Job [1/1] :: 152 req/sec :: Duration: [0:00:22] :: Errors: 0 ::

(kali@kali)-[~/bookingcom]
└─$ ls
fuff.txt      host_sin_revisar.txt  subdominios_activos.txt  subdominios_ctfr.txt  subdominios_katana.txt  targets_ips.txt
gowitness.sqlite3  screenshots          subdominios_cero.txt    subdominios_gau.txt   subdominios_shuffledns.txt  waf.txt

(kali@kali)-[~/bookingcom]
└─$ cat ffuf.txt
cat: ffuf.txt: No such file or directory

(kali@kali)-[~/bookingcom]
└─$ cat fuff.txt
[Status: 200, Size: 9850, Words: 4992, Lines: 475, Duration: 76ms]
[Status: 200, Size: 5666, Words: 1, Lines: 75, Duration: 100ms]
[Status: 200, Size: 602, Words: 127, Lines: 26, Duration: 149ms]
```

### LANZAMIENTO CONTRA <https://admin.booking.com>

```
(kali@kali)-[~/bookingcom]
└─$ ffuf -w ~/recopilacion/common.txt -t 20 -mc 200,401 -u https://admin.booking.com/FUZZ > fuffdominio_admin.txt

v2.1.0-dev

:: Method      : GET
:: URL         : https://admin.booking.com/FUZZ
:: Wordlist     : FUZZ: /home/kali/recopilacion/common.txt
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 20
:: Matcher     : Response status: 200,401

:: Progress: [4727/4727] :: Job [1/1] :: 442 req/sec :: Duration: [0:00:10] :: Errors: 0 ::

(kali@kali)-[~/bookingcom]
└─$
```

LANZAMIENTO CONTRA <http://spadmin.booking.com>

```
(kali@kali)~[/bookingcom]
$ ffuf -w ~/recopilacion/common.txt -t 20 -mc 200,401 -u http://spadmin.booking.com/FUZZ -p fuffdominio_spadmin.txt

v2.1.0-dev

:: Method      : GET
:: URL         : http://spadmin.booking.com/FUZZ
:: Wordlist     : FUZZ: /home/kali/recopilacion/common.txt
:: Follow redirects : false
:: Calibration  : false
:: Timeout      : 10
:: Threads     : 20
:: Matcher     : Response status: 200,401

:: Progress: [4727/4727] :: Job [1/1] :: 1960 req/sec :: Duration: [0:00:02] :: Errors: 0 ::
```

LANZAMIENTO CONTRA <https://developer.booking.com>

```
(kali@kali)~[/bookingcom]
$ ffuf -w ~/recopilacion/common.txt -t 20 -mc 200,401 -u https://developer.booking.com/FUZZ -p fuffdominio_developer.txt

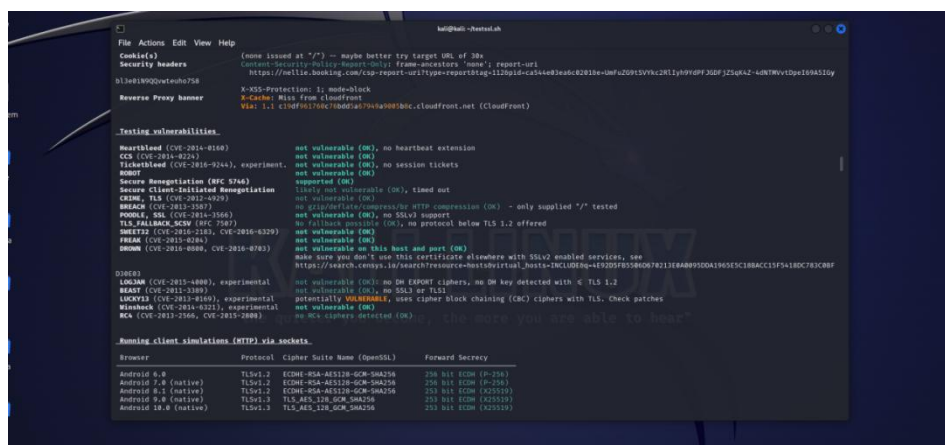
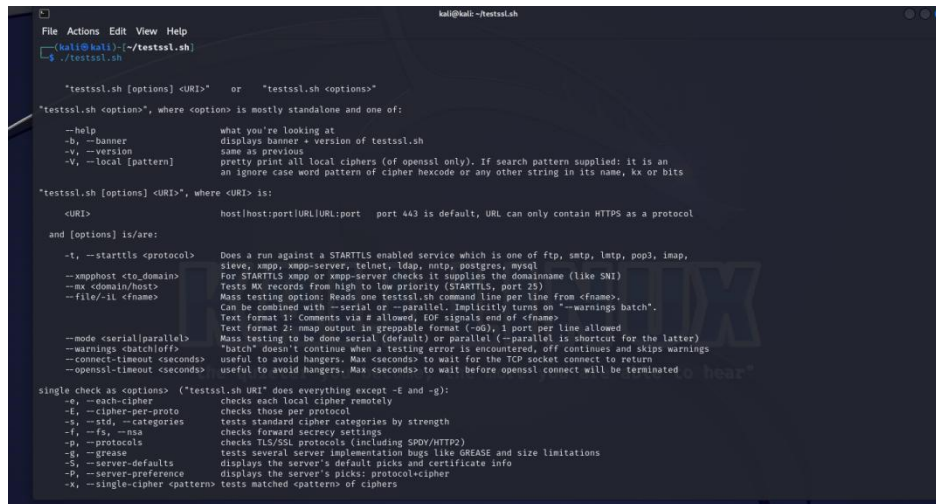
v2.1.0-dev

:: Method      : GET
:: URL         : https://developer.booking.com/FUZZ
:: Wordlist     : FUZZ: /home/kali/recopilacion/common.txt
:: Follow redirects : false
:: Calibration  : false
:: Timeout      : 10
:: Threads     : 20
:: Matcher     : Response status: 200,401

:: Progress: [4727/4727] :: Job [1/1] :: 473 req/sec :: Duration: [0:00:11] :: Errors: 0 ::
```

No hemos encontrado nada en ninguno de los dominios

Con esta herramienta detectamos vulnerabilidades en la configuracion SSL de un servidor web, como versiones antiguas SSL/TLS, algoritmos cifrados e intercambios de claves obsoletos, configuraciones inadecuadas o vulnerabilidades en el certificado





## SPOOFCHECK

```
(kali@kali) ~/spoocheck
$ python spoofcheck.py booking.com
[*] Found SPF record:
[*] v=spf1 include:_spf._has.pphosted.com -all
[*] SPF record contains an All item: -all
[*] Found DMARC record:
[*] v=DMARC1; p=reject; rua=mailto:dmARC_rua@emaildefense.proofpoint.com,mailto:booking@dmARC.postmastery.eu; ruf=mailto:dmARC_ruf@emaildefense.proofpoint.com
[*] DMARC policy set to reject
[*] Aggregate reports will be sent: mailto:dmARC_rua@emaildefense.proofpoint.com,mailto:booking@dmARC.postmastery.eu
[*] Forensics reports will be sent: mailto:dmARC_ruf@emaildefense.proofpoint.com
[*] Spoofing not possible for booking.com
(kali@kali) ~/spoocheck
```

la política DMARC configurada para este dominio es bastante estricta, lo que significa que los correos electrónicos que no pasen la autenticación DMARC serán rechazados por los servidores de correo receptor. Además, se han configurado direcciones de correo electrónico específicas para recibir informes de actividad y fallos relacionados con DMARC. Esto ayuda a los administradores del dominio a monitorear y mejorar la seguridad de los correos electrónicos enviados desde su dominio.



# OSINT

HERRAMIENTAS UTILIZADAS: FOCA Y MALTEGO

## FOCA:

DESCRAGA DE ARCHIVOS ENCONTRADOS:

The screenshot shows the Foca Open Source application interface. The top menu includes Project, Plugins, Options, TaskList, and About. The left sidebar shows a tree view with categories like BOOKING, Network, Domains, and Document Analysis. The main area displays a list of files with columns: Id, Type, URL, Download, Download Date, Size, Metadata E..., Malware An..., and Modified Date. The list contains 10 items, mostly PDF files from various booking.com URLs. Below the list, a message box indicates an error: "An error has occurred on GoogleWeb: Error en el servidor remoto: (429) Too Many Requests...". The bottom status bar shows "Downloading 105/320" and a progress bar.

Id	Type	URL	Download	Download Date	Size	Metadata E...	Malware An...	Modified Date
307	pdf	https://partner.booking.com/sites/default/files/2020-08/...	X	-	3.83 MB	X	X	-
308	pdf	https://partner.booking.com/sites/default/files/2020-08/...	X	-	1.74 MB	X	X	-
309	pdf	https://partner.booking.com/sites/default/files/2020-08/...	X	-	3.82 MB	X	X	-
310	pdf	https://partner.booking.com/sites/default/files/2020-08/...	X	-	4.32 MB	X	X	-
311	pdf	https://partnerships.booking.com/sites/default/files/202...	X	-	12.14 MB	X	X	-
312	pdf	https://image.email.partnerships.booking.com/ib-fe3011...	X	-	264.49 KB	X	X	-
313	pdf	https://partnerships.booking.com/sites/default/files/202...	X	-	3.34 MB	X	X	-
314	pdf	https://partnerships.booking.com/sites/default/files/202...	X	-	953 KB	X	X	-
315	pdf	https://go.partners.booking.com/rs/261-NRZ-371/image...	X	-	772.37 KB	X	X	-
316	pdf	https://insurance.gw.booking.com/document/policy/35...	X	-	-	X	X	-
317	pdf	https://go.partners.booking.com/rs/261-NRZ-371/image...	X	-	1.04 MB	X	X	-
318	pdf	https://partner.booking.com/sites/default/files/2021-03/...	X	-	281.21 KB	X	X	-
319	pdf	https://partner.booking.com/sites/default/files/2022-02/...	X	-	439.88 KB	X	X	-

EXTRACCION DE METADATOS:

The screenshot shows the Foca Open Source application interface. The top menu includes Project, Plugins, Options, TaskList, and About. The left sidebar shows a tree view with categories like BOOKING, Network, Domains, and Document Analysis. The main area displays a list of files with columns: Id, Type, URL, Download, Download Date, Size, Metadata E..., Malware An..., and Modified Date. The list contains 21 items, mostly PDF files from various booking.com URLs. Below the list, a message box indicates an error: "An error has occurred on GoogleWeb: Error en el servidor remoto: (429) Too Many Requests...". The bottom status bar shows "All documents were analyzed" and a progress bar.

Id	Type	URL	Download	Download Date	Size	Metadata E...	Malware An...	Modified Date
9	pdf	https://business.booking.com/storage/c-4b7e98314184...	•	01/29/2024 17:24:53	1 MB	•	X	07/31/2018 13:54:52
10	pdf	https://business.booking.com/storage/a359397e514b1...	•	01/29/2024 17:24:54	1.45 MB	•	X	04/05/2018 18:53:19
11	pdf	https://business.booking.com/starter-kit-download/...	•	01/29/2024 17:26:32	16.5 KB	•	X	-
12	pdf	https://business.booking.com/storage/f369d55fbc490...	•	01/29/2024 17:24:54	894.17 KB	•	X	07/31/2018 13:16:10
13	pdf	https://business.booking.com/storage/07334ae7020b4...	•	01/29/2024 17:26:32	2.15 MB	•	X	02/06/2018 09:11:41
14	pdf	https://business.booking.com/storage/b13d37cddc389...	•	01/29/2024 17:24:54	127.66 KB	•	X	02/06/2018 15:41:58
15	pdf	https://business.booking.com/storage/e3622aa59f2c7...	•	01/29/2024 17:26:31	161.5 KB	•	X	05/03/2021 15:39:04
16	pdf	https://business.booking.com/storage/2d678dbd2416...	•	01/29/2024 17:24:54	254.4 KB	•	X	05/03/2021 15:38:47
17	pdf	https://business.booking.com/storage/f2e429b28d140...	•	01/29/2024 17:26:32	195.97 KB	•	X	01/02/2018 13:00:54
18	pdf	https://business.booking.com/storage/b4e722107d477...	•	01/29/2024 17:24:54	260.07 KB	•	X	05/03/2021 15:39:20
19	pdf	https://business.booking.com/storage/bd6e3d15d7d5b...	•	01/29/2024 17:26:34	7.12 MB	•	X	09/03/2018 13:41:10
20	pdf	https://business.booking.com/storage/25758d74616b3...	•	01/29/2024 17:24:55	614.45 KB	•	X	02/02/2018 16:14:19
21	pdf	https://business.booking.com/storage/5b024b71c8451...	•	01/29/2024 17:26:43	11.34 MB	•	X	01/03/2018 16:06:59

ENRIQUE LÓPEZ PASCUAL  
RECOPIACION DE INFORMACIÓN

SOFTWARES:

The screenshot shows the 'TaskList' window with the following content:

**Project Structure (Left Pane):**

- BOOKING
  - Network
  - Domains
  - booking.com
    - Document Analysis
      - Files (320/320)
        - docx (6)
        - .pdf (306)
        - pptx (2)
        - Unknown (5)
      - Metadata Summary
        - Users (37)
        - Folders (609)
        - Printers (0)
        - Software (327)
        - Emails (1)
        - Operating Systems (0)
        - Passwords (0)
        - Servers (0)
        - Malware Summary (DIARIO)

**TaskList (Right Pane):**

Attribute	Value	Software
Attribute	Value	
software	Adobe InDesign CC 2017 (Macintosh)	
Software	Adobe PDF Library 15.0	
Software	Adobe InDesign CC 13.0 (Macintosh)	
Software	Adobe PDF Library 15.0	
Software	Microsoft Office	
Software	Adobe InDesign CC 2015 (Macintosh)	
Software	Adobe PDF Library 15.0	
Software	Adobe InDesign CC 13.0 (Macintosh)	
Software	Adobe PDF Library 15.0	
Software	Adobe InDesign CC 2017 (Macintosh)	
Software	Adobe PDF Library 15.0	
Software	Adobe InDesign 14.0 (Macintosh)	
Software	Adobe PDF Library 15.0	
Software	Microsoft Office	
Software	Adobe InDesign CC 13.1 (Macintosh)	
Software	Adobe PDF Library 15.0	
Software	Microsoft Office	
Software	Adobe InDesign CC 2017 (Macintosh)	
Software	Adobe PDF Library 15.0	

Podrían tener algún software desactualizado y por lo tanto vulnerable.

## EMAIL ENCONTRADO:

Project

Plugins

Options

TaskList

About

BOOKING

Network

Domains

Document Analysis

Files (320/320)

Unknown (6)

Metadata Summary

Users (10)

Folders (159)

Printers (0)

Software (22)

Emails (11)

Operating Systems (0)

Passwords (0)

Servers (0)

Malware Summary (DIARIO)

Attribute

Value

All emails found (1) - Times found

Emaildataprotectionoffice@booking.com

Time	Source	Severity	Message
17:24:14	MetadataSearch	error	An error has occurred on GoogleWeb: Error en el servidor remoto: (429) Too Many Requests.

Settings

Deactivate AutoScroll

Clear

Save log to File

USUARIOS:

The screenshot shows the NetworkMiner tool interface. On the left, a file tree is displayed under the 'BOOKING' category. The tree structure is as follows:

- BOOKING
  - Network
  - Domains
    - booking.com
  - Document Analysis
  - Files (320/320)
    - docx (6)
    - pdf (306)
    - psbt (2)
    - Unknown (6)
  - Metadata Summary
    - Users (17)
    - Folders (609)
    - Printers (0)
    - Software (327)
    - Emails (1)
    - Operating Systems (0)
    - Passwords (0)
    - Severs (0)
    - Malware Summary (DIARIO)

On the right, a table lists attributes and their corresponding values:

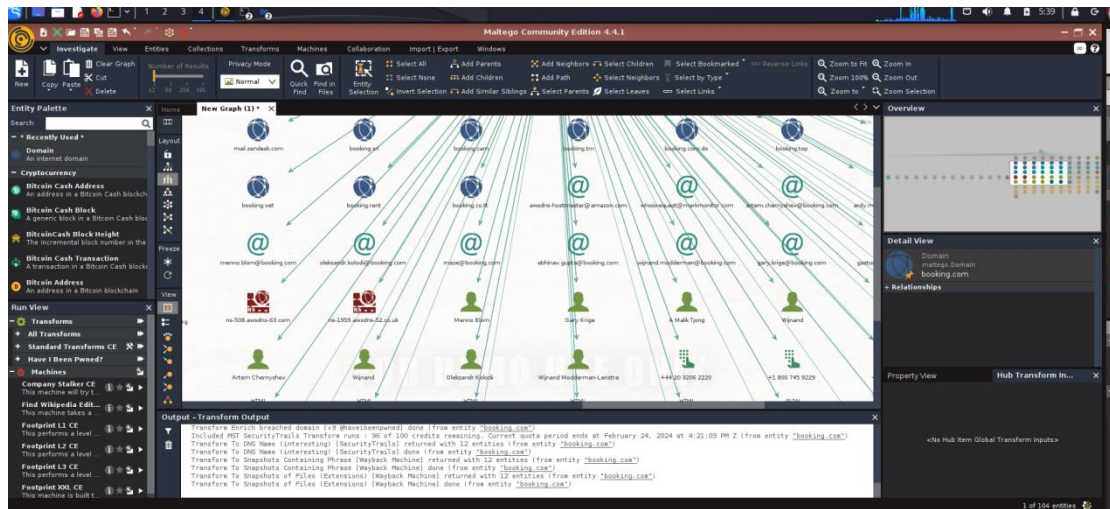
Attribute	Value
Name	Znaida Kovaleva
Name	Feyzanur Manay
Name	Znaida Kovaleva
Name	Znaida Kovaleva
Name	Znaida Kovaleva
Name	Znaida Kovaleva
Name	Znaida Kovaleva
Name	Vicky Lampidi
Name	Brida Mattio
Name	Antonella Ponce
Name	Luciana Brad
Name	Ferd de Jong
Name	Feyzanur Manay
Name	Kyueun Chung
Name	Znaida Kovaleva
Name	Arte Poljak
Name	Vicky Lampidi
Name	Kyueun Chung
Name	Nick Whitehead
Name	Nick Whitehead
Name	Nick Whitehead

At the bottom of the interface, there are four tabs: 'Time', 'Source', 'Severity', and 'Message'.

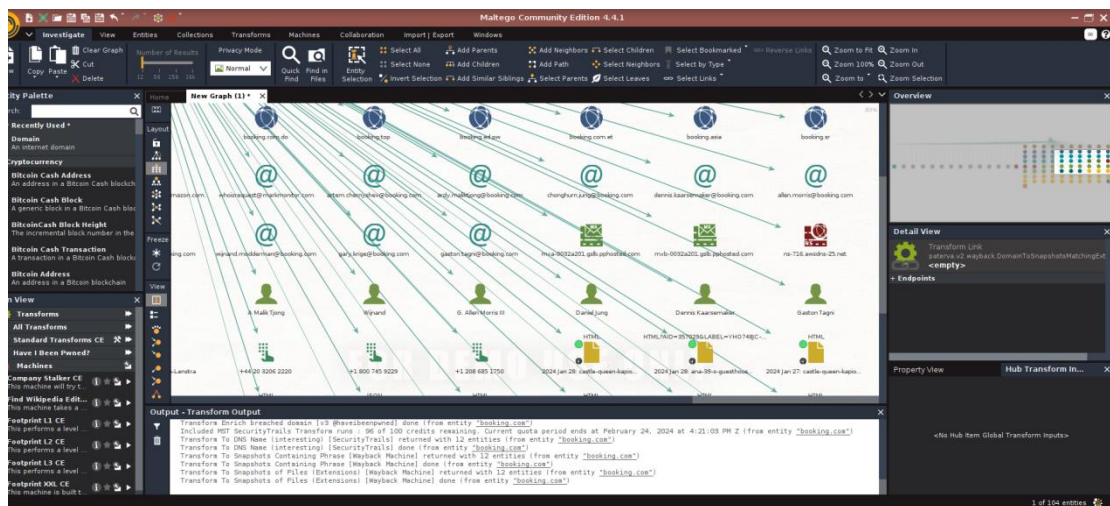
ENRIQUE LÓPEZ PASCUAL  
RECOPIACION DE INFORMACIÓN

## MALTEGO

Vamos a utilizar la herramienta maltego que es un software especializado en tareas OSINT.  
Vamos a intentar extraer correos electronicos y usuarios de nuestro objetivo



Con esta herramienta hemos obtenido varios correos electrónicos y nombres de usuario.



He pasado la herramienta Have I Been Pwned por cada uno de los correos que hemos encontrado con maltego, observamos que varios de ellos fueron afectados por el hackeo Apollo.

