

RECONOCIMIENTO DE LA EMPRESA

BOOKING.COM

INDICE:

1- NOMBRE E INFORMACION DE LA EMPRESA

2-ESCANEO DEL DOMINIO PRINCIPAL Y SUBDOMINIOS

3-HERRAMIENTAS OSINT

1-NOMBRE E INFORMACIÓN DE LA EMPRESA

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.

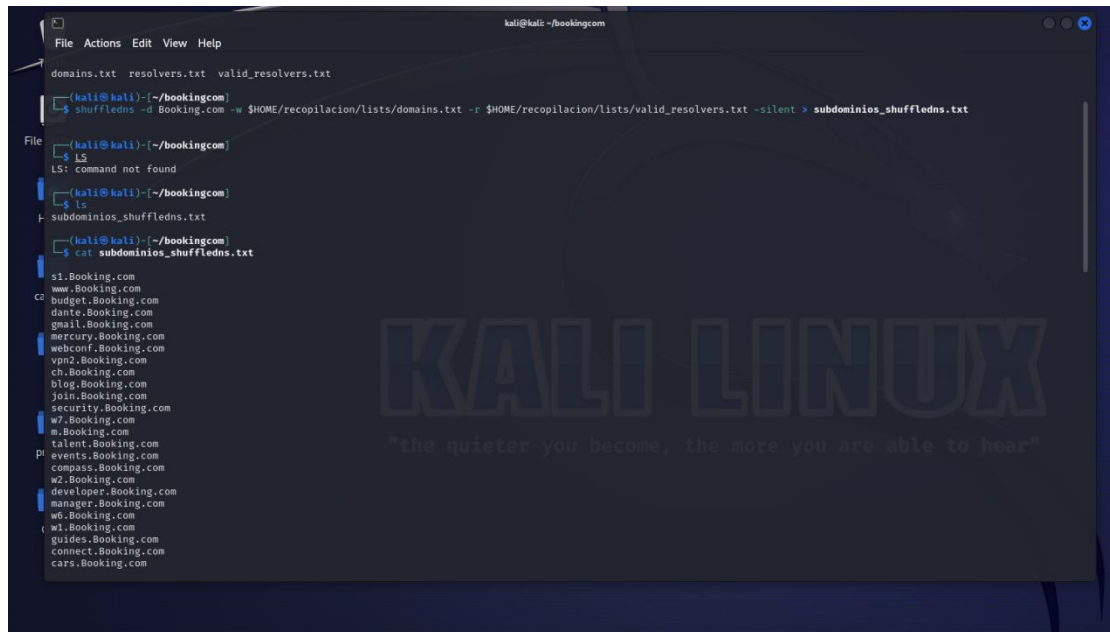
Principales puntos sobre Booking.com:

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.

2-ESCANEO DEL DOMINIO PRINCIPAL Y SUBDOMINIOS

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



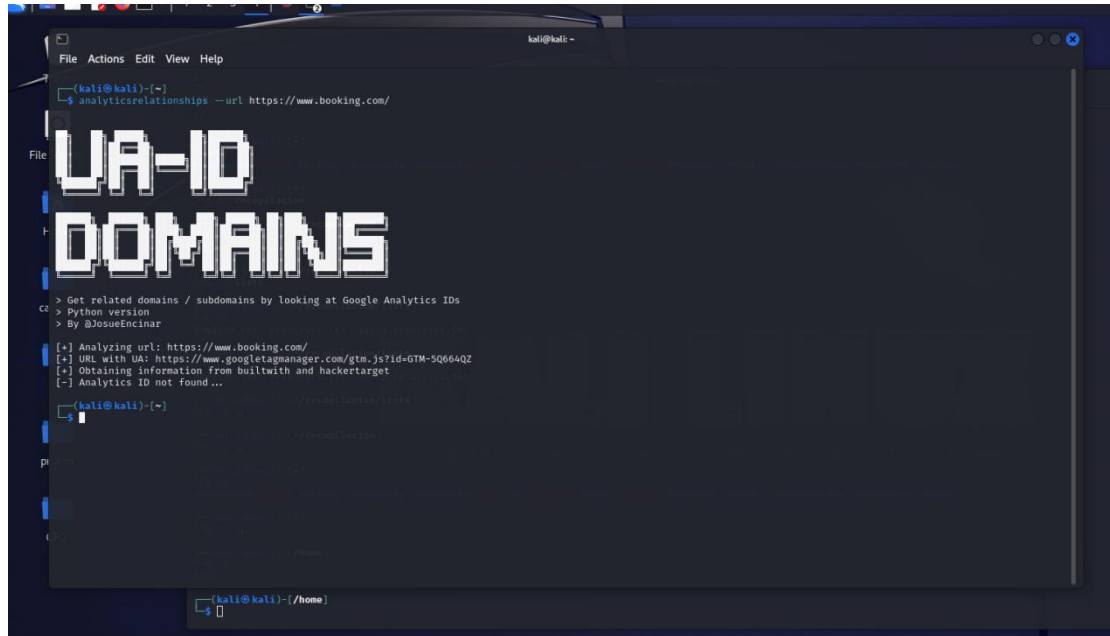
```
kali@kali: ~/bookingcom
File Actions Edit View Help
domains.txt resolvers.txt valid_resolvers.txt
$ shuffledns -d Booking.com -w $HOME/recopilacion/lists/domains.txt -r $HOME/recopilacion/lists/valid_resolvers.txt -silent > subdominios_shuffledns.txt
File
$ ls
ls: command not found
$ ls
subdominios_shuffledns.txt
$ 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
m.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/  
  
UA-ID  
DOMAINS  
  
> 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: ~  
$
```

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_et_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/pxbook?*>recopilacion
https://booking.com/pxgo?*>recopilacion
https://booking.com/hotel_attractions
https://booking.com/episode_times
https://booking.com/event*>recopilacion
https://booking.com/track
https://booking.com/vpmlgdeskscreensize
https://booking.com/sendlayoutevents
https://booking.com/join_js_tracking*>recopilacion/tiempo
https://booking.com/reviewlist.html*>recopilacion/tiempo
https://booking.com/product_header.html*>recopilacion/tiempo
https://booking.com/bas/**>recopilacion/tiempo
https://booking.com/srcompset.*.html*>recopilacion/tiempo
https://booking.com/frdtcr*>recopilacion/tiempo
https://booking.com/srcompset.html*>recopilacion/tiempo
https://booking.com/fragment.json*>recopilacion/tiempo
https://booking.com/c360_v1_track
https://booking.com/hotel/us/the-airstream-van.*.html
https://booking.com/fragment.html*>recopilacion/tiempo
https://booking.com/asapi/*
https://booking.com/log_r_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.*
(kali@kali)~/home
```

Hemos utilizado la herramienta unfurl para que nos filtre los resultados obtenidos y que solo nos deje 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

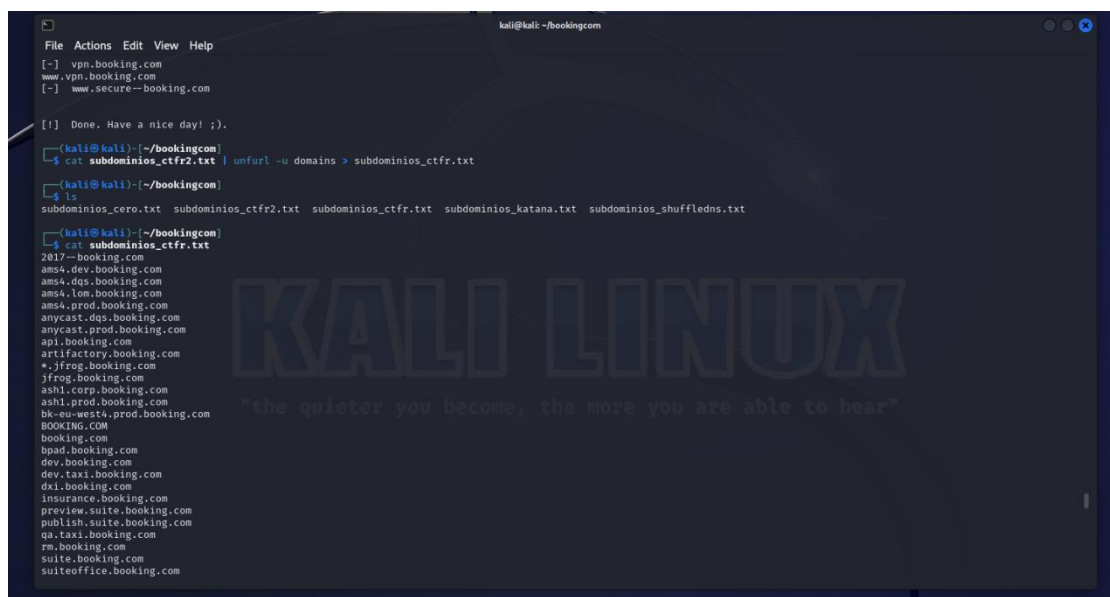
CTFR

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

[!] --- 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.lom.booking.com
ams4.lom.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
Booking.com BV
[-] *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.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
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 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
--fr strings         list of status codes to filter
--fp                remove different parameters of the same endpoint
--from string        fetch url from date (format: YYYYMM)
--ft strings         list of mime-types to filter
--json              output as json
--mc strings         list of status codes to watch
--mt strings         list of mime-types to watch
--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 to date (format: YYYYMM)
--verbose            show verbose output
--version            show gau version

[kali@kali]~/bookingcom$ ctfr booking.com -d | 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$
```


GAU (ANALISIS DE CACHÉ)

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

LANZAMIENTO GAU

```

kali@kali:~/bookingscom$ ls
subdomains_cero.txt  subdomains_ctfr.txt  subdomains_katana.txt  subdomains_shuffledns.txt

kali@kali:~/bookingscom$ cd ~
kali@kali:~$ ls
subdomains_cero.txt  subdomains_ctfr.txt  subdomains_katana.txt  subdomains_shuffledns.txt

kali@kali:~/bookingscom$ gau --threats 5 bookings.com --o subdomains_gau2.txt
unknown flag: --threats
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

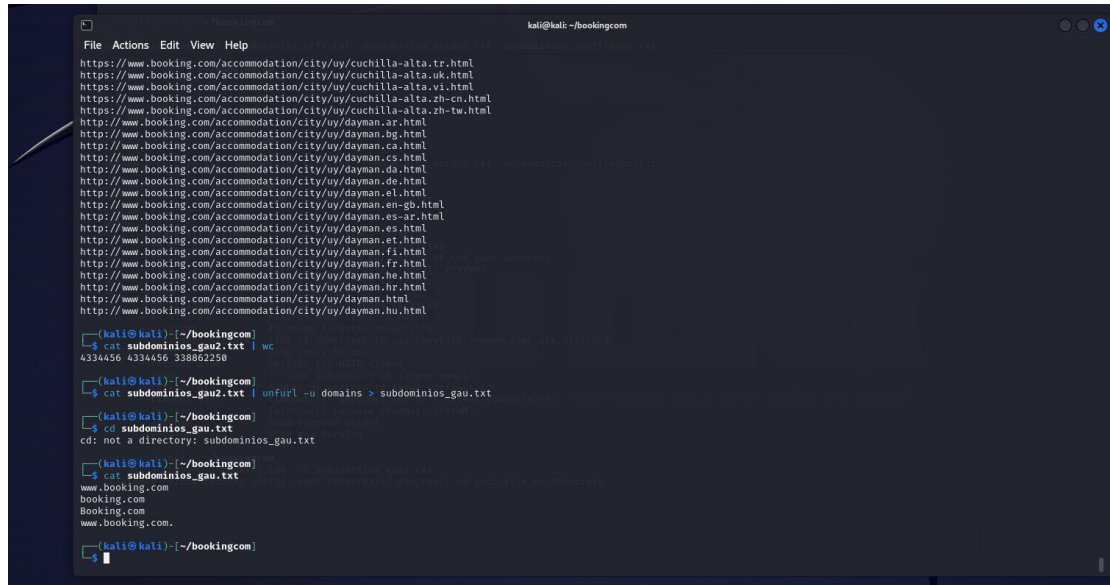
kali@kali:~/bookingscom$ gau --threads 5 bookings.com --o subdomains_gau2.txt
WARN[0000] error reading config: open /home/kali/.gau.toml: no such file or directory
ls

```

Nos devuelve bastantes urls:

```
File Actions Edit View Help
kali@kali:~$ cd /root/.ssh
kali@kali:~/ssh$ ls
bookingscom
kali@kali:~/ssh/bookingscom$ ls
subdominios_cero.txt subdominios_cttfr.txt subdominios_gau2.txt subdominios_katana.txt subdominios_shuffledns.txt
kali@kali:~/ssh/bookingscom$ cat subdominios_gau2.txt
http://www.booking.com/80/
http://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/
https://www.booking.com/
https://www.booking.com/
http://booking.com/
https://www.booking.com/
https://www.booking.com/1%20hotel/au/curdieval-rieverfront-lodge-en-gb.html
https://www.booking.com/1%20hotel/au/curdieval-rieverfront-lodge-en-gb.html?aid=306395;label=istanbul-JviwZgVefvAHGvQ3_bzFhgS3227685239;sid=c8d512c2cc4e091e518be1fac291a9
http://booking.com/Igo
http://www.booking.com/80/RESTB_ERROR_NCURL_IGNORE_ALL
https://www.booking.com/x22
http://www.booking.com/x22x22
http://www.booking.com/x22x22x3C1X20X22_black
https://www.booking.com/x22_x22
https://www.booking.com/x22_x22alts
https://www.booking.com/x22_x22imageX22x22https://cnt/uploads/logos/booking-com.jpg?1606894191","aggregateRating":{"@type":"AggregateRating","ratingValue":"5.00","worstRati
ng":1,"bestRating":5,"ratingCount":2}}
https://www.booking.com/x22_x22x22x22x22
http://www.booking.com/x22https://e-c.bstatic.com/static/img/icons/circles/X7BK7Bb_class/XD7DX7B7Bb_class_hal/FK7Dsterren4.png/x22/
http://booking.com/80/x22rel_x22nofollow
https://www.booking.com/80/8
https://www.booking.com/$$$$767$$$$?cmd=get_file&arg=block_style.css&sid=85362f80d1CFE5BFCEFC940FAC6DDAABCA1AE542
https://www.booking.com/$$$$767$$$$?cmd=get_file&arg=block_style.css&sid=BC8BD3093618C45338ACAB93FA954F54BA68512
https://www.booking.com/$$$$767$$$$?cmd=get_file&arg=block_style.css&sid=EBC1D5D4BE090983570CBCE882162377D5088BAC
https://www.booking.com/$$$$767$$$$?cmd=get_file&arg=images/block.png&sid=A1FB0AAAEF2F2FA4E349021C4AF4A9DB28543
```

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

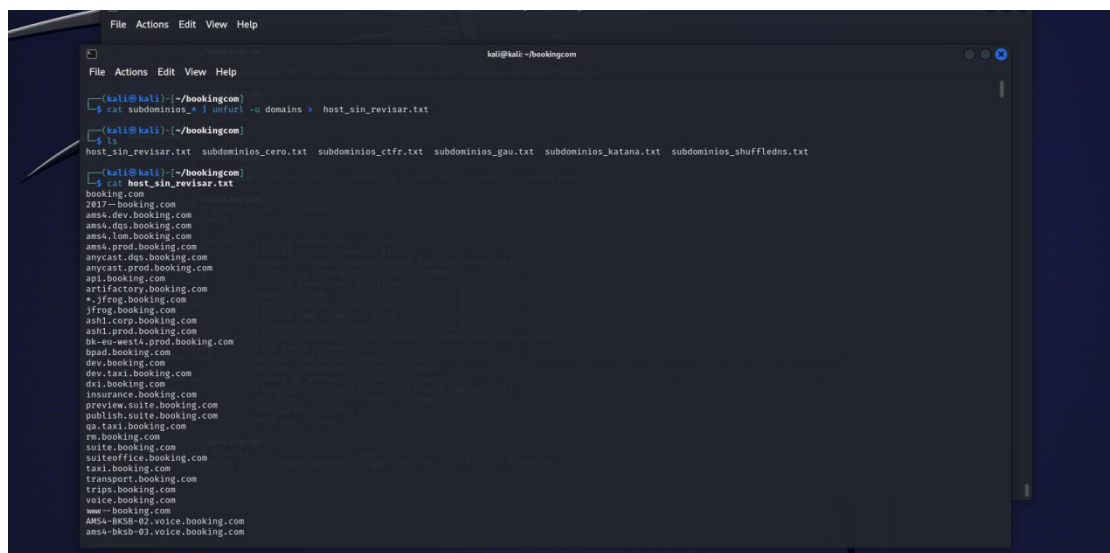
(kali@kali) [~/bookingcom]
$ cd subdominios_gau.txt
cd: not a directory: subdominios_gau.txt

(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

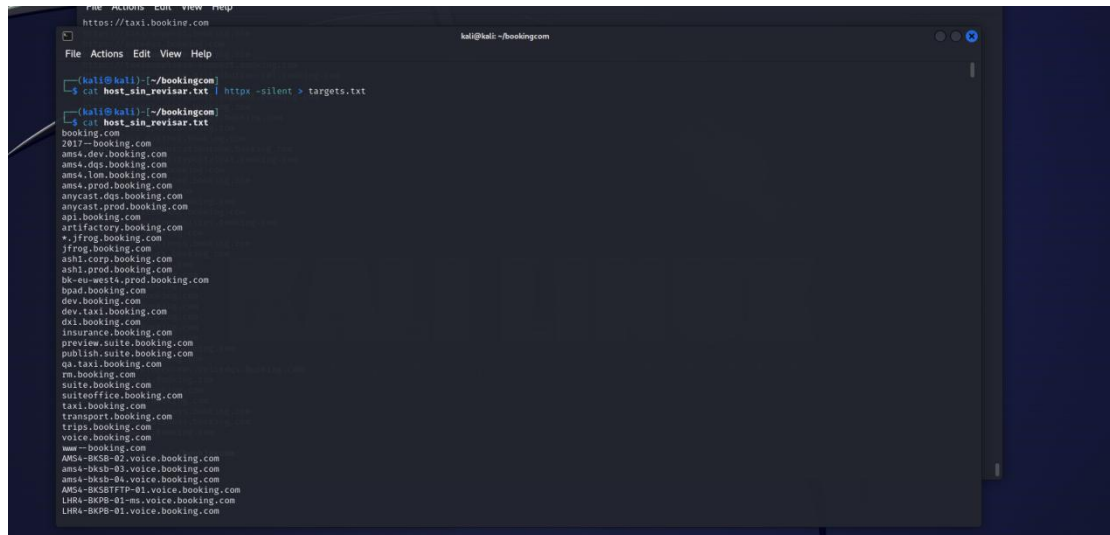
(kali@kali) [~/bookingcom]
$ cat host_sin_revisar.txt
booking.com
2817-booking.com
ams4.dev.booking.com
ams4.dqs.booking.com
ams4.lom.booking.com
ams4.prod.booking.com
anycast.dqs.booking.com
anycast.prod.booking.com
api.booking.com
artifactory.booking.com
*-jfrog.booking.com
jfrog.booking.com
ash1.corp.booking.com
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, hemos obtenido varios subdominios, vamos a comprobar cuales de todos son válidos.

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.



```
File Actions Edit View Help
https://taxi.booking.com

(kali@kali) [~/bookingcom]
$ cat host_sin_revisar.txt | httpx -silent > targets.txt

(kali@kali) [~/bookingcom]
$ cat host_sin_revisar.txt
booking.com
2017-booking.com
amss4.dev.booking.com
amss4.dqs.booking.com
amss4.tom.booking.com
amss4.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
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-BKSB-02.voice.booking.com
amss4-bksh-03.voice.booking.com
amss4-bksh-04.voice.booking.com
AMS4-BKSB7FTP-01.voice.booking.com
LHRA-BKPB-01-ms.voice.booking.com
LHRA-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]
$
```

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>

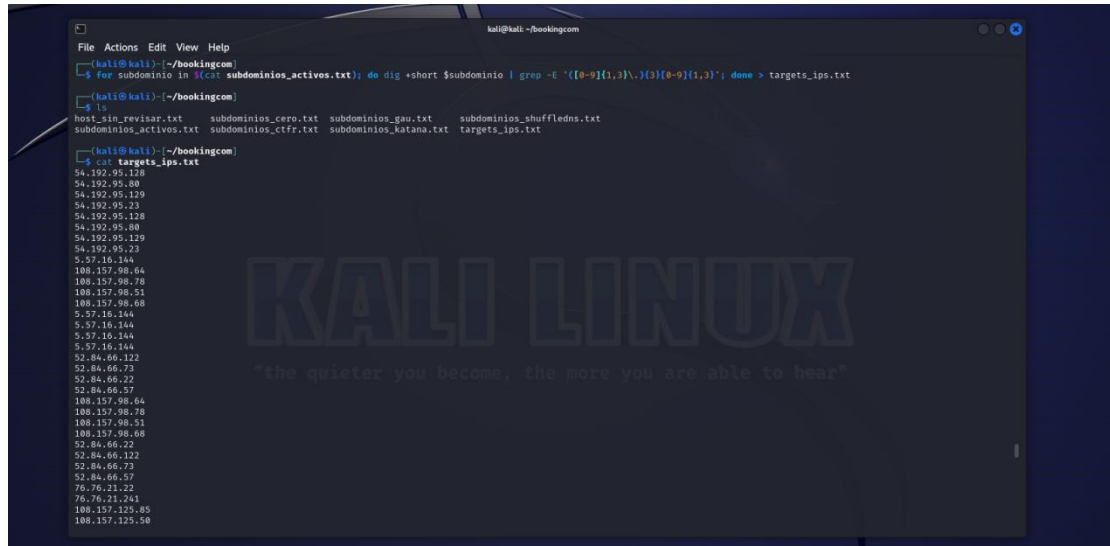
O estos otros que contiene la palabra developers (desarrolladores)

<https://developer.Booking.com>

<https://developers.Booking.com>

EN EL SIGUIENTE PASO VAMOS A CONVERTIR LOS DOMINIOS A IPs, PARA 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
```



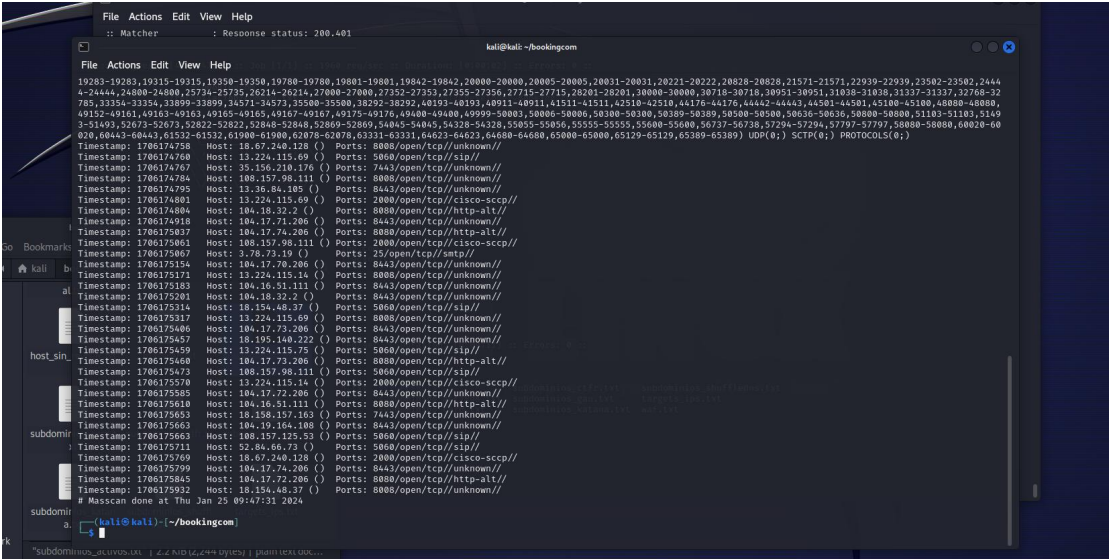
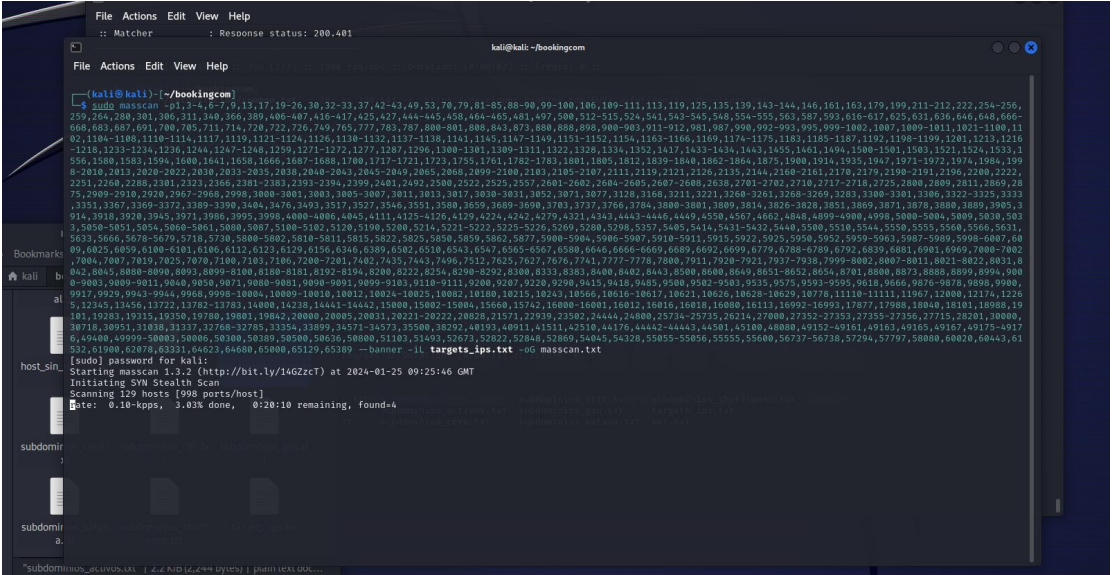
The screenshot shows a Kali Linux terminal window with the following content:

```
kali@kali:~/bookingscom
File Actions Edit View Help
kali@kali:~/bookingscom
$ 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:~/bookingscom
$ 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:~/bookingscom
$ 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
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 (ESCANEO 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



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:

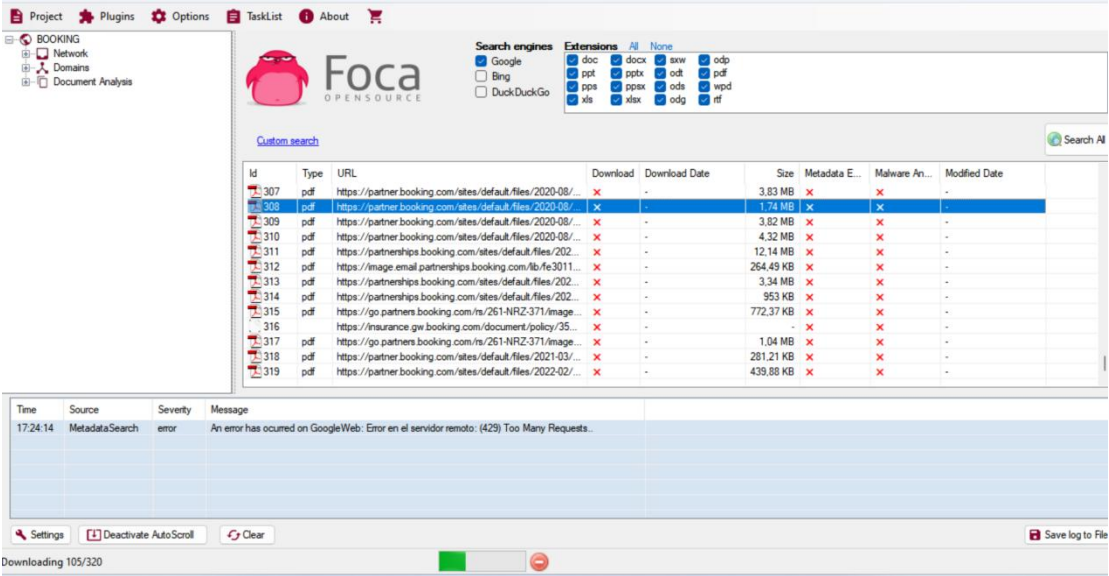
- Utilizado para SMTP. Podría ser de interés para evaluar la seguridad del servidor de correo si está presente en el entorno analizado.

3-HERRMIENTAS OSINT

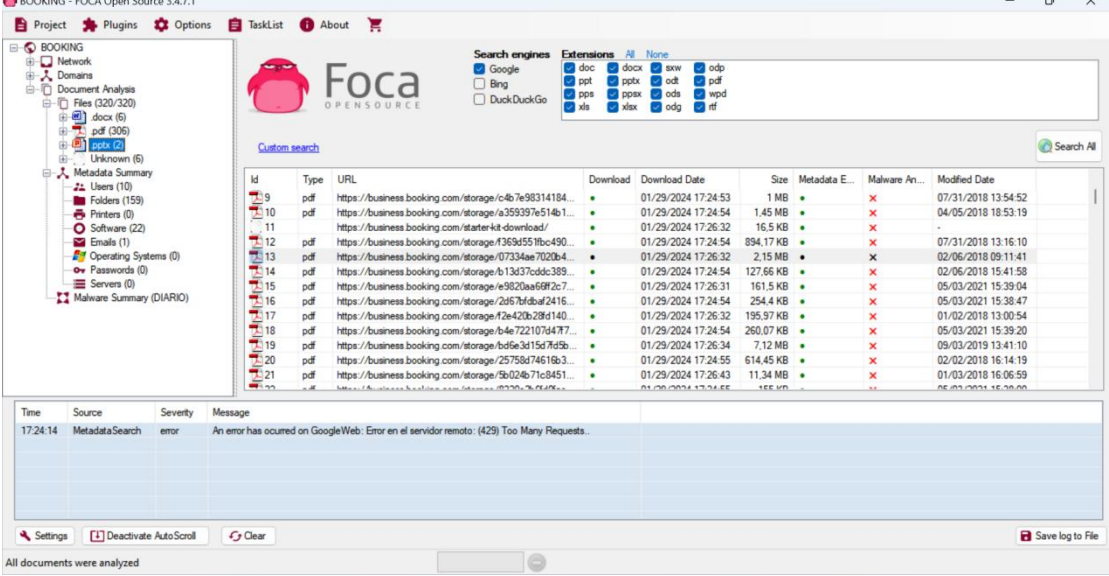
HERRAMIENTAS UTILIZADAS: FOCA Y MALTEGO

FOCA:

DESCRAGA DE ARCHIVOS ENCONTRADOS:



EXTRACCION DE METADATOS:



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 13.1 (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:

Booking - Data Protection Suite 3.4.7.1

Project Plugins Options TaskList About

BOOKING

- Network
- Domains
- Document Analysis
 - Files (320/320)
 - docx (6)
 - pdf (306)
 - pptx (2)
 - 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	
Email	dataprotectionoffice@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)

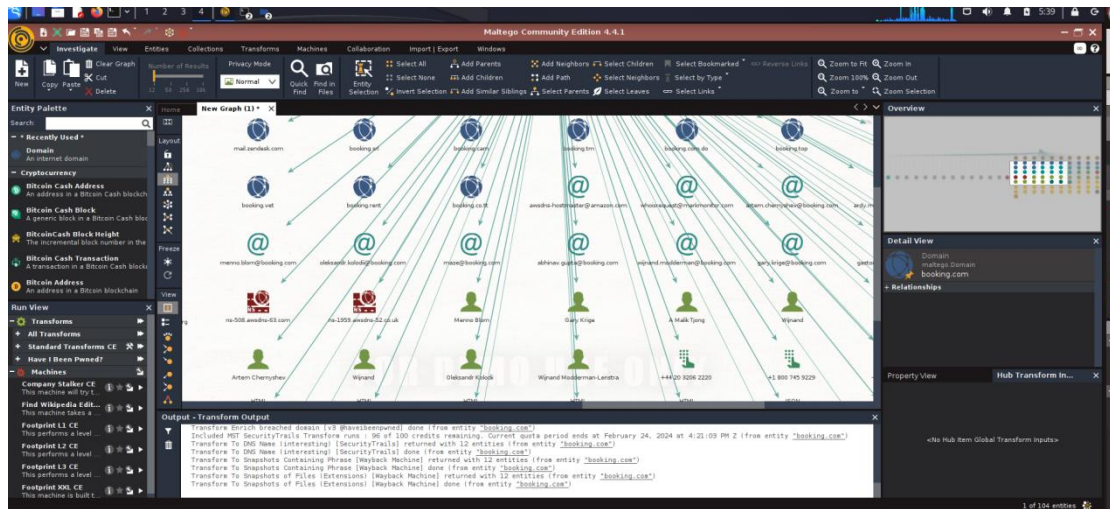
On the right, a table lists attributes and their corresponding values:

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 Matto
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

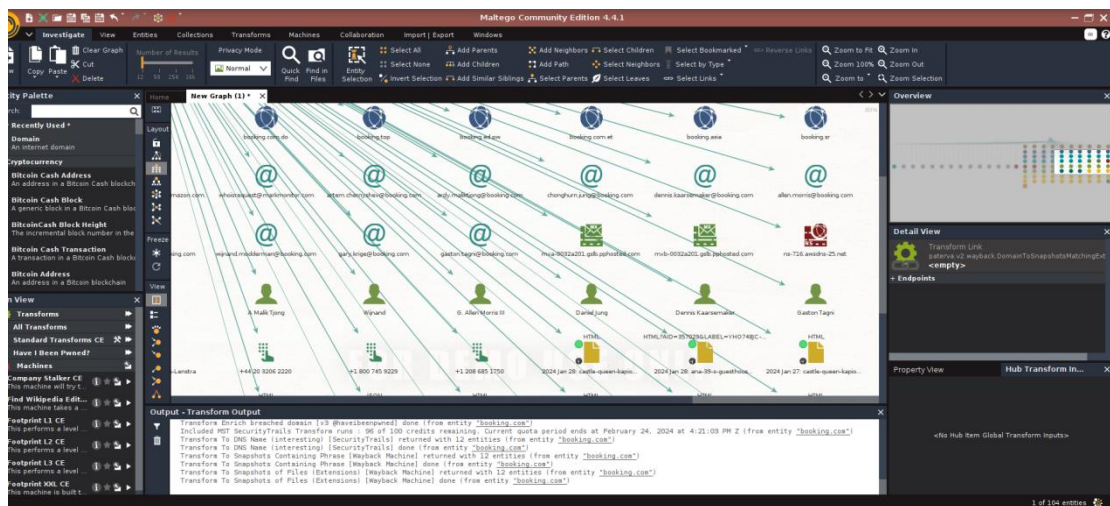
At the bottom of the interface, there are four tabs: 'Time', 'Source', 'Severity', and 'Message'.

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.

