



Clubhouse

Recopilación de información - Clubhouse

[Información](#)

[Bug Bounty Program](#)

[Scope](#)

[Footprinting](#)

[Localización de subdominios](#)

[Permutaciones posibles](#)

[Subdominios desde AnalyticsRelationships](#)

[TLS probing](#)

[Scrapping](#)

[Certificate Transparency](#)

[Fuentes pasivas](#)

[Caches y archivos web](#)

[Github](#)

[Herramienta: ReconFTW](#)

[Herramienta: AMASS](#)

[Subdominios definitivos](#)

[Fingerprint](#)

[Descubrimiento de host](#)

[Descubrimiento de puertos y servicios](#)

[Descubrimiento de servicios](#)

[Detección de servicios mediante UDP](#)

[Firewall ByPass](#)

[Análisis Web](#)

[Evaluación de subdominios - Eyewitness](#)

[Web Application Firewall](#)

[Descubrimiento de contenido](#)

[BurpSuite Community](#)

[Dirsearch](#)

[Dirb](#)

[Análisis de vulnerabilidades.](#)

[Vulnerabilidades](#)

[Cifrados y seguridad](#)

[Correo electrónico](#)

[Subdomain takeover](#)

[OSINT](#)

[Motores de búsqueda](#)

[Búsqueda de contactos](#)

[Maltego / Intelligence X](#)

[Hunter.io](#)

[Spiderfoot](#)

[Inciso - clubhouseapi.com](#)

[Verificación de correos.](#)

[Correos comprometidos](#)

Conclusión

Autor: Jose Manuel González González. KeepCoding España


Información

ClubHouse es una red social nueva basada en la creación de salas donde el principal medio de comunicación es mediante mensajes de audio.

Bug Bounty Program

Clubhouse - Bug Bounty Program | HackerOne

The Clubhouse Bug Bounty Program enlists the help of the hacker community at HackerOne to make Clubhouse more secure. HackerOne is the #1 hacker-powered security platform, helping organizations find and fix critical vulnerabilities before they can be criminally exploited.

 <https://hackerone.com/clubhouse?type=team>



Scope

- *.clubhouseapi.com
- *.joinclubhouse.com
- *.clubhouse.com



Los dominios relacionados están acotados por el scope proporcionado en hacker1, por lo tanto, en nuestro análisis nos basaremos en el reconocimiento vertical.

Footprinting

Localización de subdominios

1. Obtenemos y verificamos una lista de DNS de cara a poder obtener los subdominios

```
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ dnsvalidator -tL https://public-dns.info/nameservers.txt -threads 100 -o resolvers.txt
>> Discovered 1785 servers
```




Archivo  resolvers.txt

2. Obtenemos a partir de los DNS obtenidos los posibles subdominios, para ello hemos seleccionado un diccionario de SecList "subdomains-top1million-5000" por su tamaño me ha parecido un tamaño comedido con buenos resultados (4989).

```
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ puredns bruteforce /home/kali/recopilacion-informacion/SecLists/Discovery/DNS/subdomains-top1million-5000.txt clubhouseapi.com -r resolvers.txt -w subdominios_clubhouseAPI.txt
```



Archivo  subdominios_clubhouseAPI.txt

Subdominios encontrados ▶ 2.

- images.clubhouseapi.com
- www.clubhouseapi.com

```
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ puredns bruteforce /home/kali/recopilacion-informacion/SecLists/Discovery/DNS/subdomains-top1million-5000.txt joinclubhouse.com -r resolvers.txt -w subdominios_joinclubhouse.txt
```



Archivo ▶ subdominios_joinclubhouse.txt

Subdominios encontrados ▶ 7

- welcome.joinclubhouse.com
- admin.joinclubhouse.com
- www.joinclubhouse.com
- support.joinclubhouse.com
- ios.joinclubhouse.com
- community.joinclubhouse.com
- staging.joinclubhouse.com

```
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ puredns bruteforce /home/kali/recopilacion-informacion/SecLists/Discovery/DNS/subdomains-top1million-5000.txt clubhouse.com -r resolvers.txt -w subdominios_clubhouse.txt
```



Archivo ▶ subdominios_clubhouse.txt



Subdominios encontrados ▶ 10.

- staging.clubhouse.com
- www.clubhouse.com
- admin.clubhouse.com
- ios.clubhouse.com
- go.clubhouse.com
- welcome.clubhouse.com
- share.clubhouse.com
- blog.clubhouse.com
- support.clubhouse.com
- community.clubhouse.com

Permutaciones posibles

```
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ gotator -sub subdominios_clubhouseAPI.txt -perm /home/kali/recopilacion-informacion/SecLists/Discovery/DNS/deepmagic.com-prefixes-top500.txt -depth 1 -numbers 10 -mindup -adv -md > subdominios_clubhouseAPI_perm.txt
```

```
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ puredns resolve subdominios_clubhouseAPI_perm.txt -r resolvers.txt > subdominios_clubhouseAPI_perm_clear.txt
```



 Archivo  subdominios_clubhouseAPI_perm_clear.txt

Solo nos ha localizado un subdominio, aunque ya contábamos con el y el propio dominio:

- images.clubhouseapi.com
- clubhouseapi.com

```
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ gotator -sub subdominios_joinclubhouse.txt -perm /home/kali/recopilacion-informacion/SecLists/Discovery/DNS/deepmagic.com-prefixes-top500.txt -depth 1 -numbers 10 -mindup -adv -md > subdominios_joinclubhouse_perm.txt
```

```
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ puredns resolve subdominios_joinclubhouse_perm.txt -r resolvers.txt > subdominios_joinclubhouse_perm_clean.txt
```



 Archivo  subdominios_joinclubhouse_perm_clean.txt

En este caso nos ha detectado 7 subdominios, todos ya localizados excepto estos dos:

- admin-staging.joinclubhouse.com
- ios-staging.joinclubhouse.com

```
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ gotator -sub subdominios_clubhouse.txt -perm /home/kali/recopilacion-informacion/SecLists/Discovery/DNS/deepmagic.com-prefixes-top500.txt -depth 1 -numbers 10 -mindup -adv -md > subdominios_clubhouse_perm.txt
```

```
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ puredns resolve subdominios_clubhouse_perm.txt -r resolvers.txt > subdominios_clubhouse_perm_clean.txt
```


 Archivo  subdominios_clubhouse_perm_clean.txt

En el caso de clubhouse.com, ha encontrado 4 dominios, de los cuales como novedad tenemos el siguiente:

- admin-staging.clubhouse.com

Concatenamos todas las fuentes que tenemos hasta ahora:

```
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ cat subdominios_clubhouse.txt subdominios_clubhouseAPI.txt subdominios_joinclubhouse.txt subdominios_clubhouse_perm_clean.txt subdominios_clubhouseAPI_perm_clean.txt subdominios_joinclubhouse_perm_clean.txt | uniq > subdominios_tot.txt
```

 Archivo subdominios_tot.txt

Subdominios desde AnalyticsRelationships

A través de la herramienta AnalyticsRelationships localizamos que el gtag de Google es: **UA-169630588**, y nos muestra los siguientes subdominios en todos los casos:

joinclubhouse.com	Existe
clubhouseapi.com	Existe
join.club	Fuera del scope
onlyon.ch	Fuera del scope
xn--jonclubhouse-6fb.com	Fuera del scope - Typesquatting
clubhouse-tou.wawa.jp	Fuera del scope
clubhouse.com	Existe
joinpillowfort.com	Fuera del scope
comeonbump.me	Fuera del scope
community.clubhouse.com	Existe
privacy.clubhouse.com	NUEVO
tos.clubhouse.com	NUEVO

```
(kali@kali)~/recopilacion-informacion/practica
└─$ analyticsrelationships --url clubhouse.com

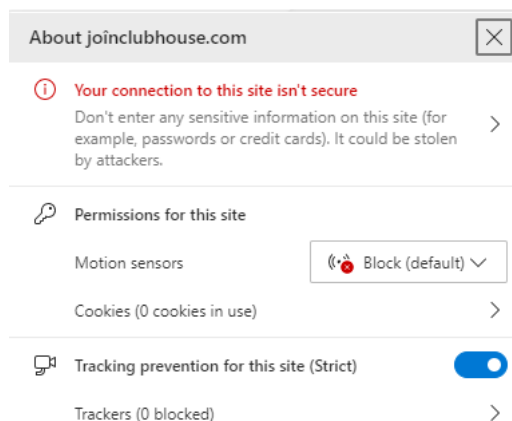
(kali@kali)~/recopilacion-informacion/practica
└─$ analyticsrelationships --url clubhouseapi.com

(kali@kali)~/recopilacion-informacion/practica
└─$ analyticsrelationships --url joinclubhouse.com
```



Archivo analyticsrelationships.txt

- El archivo lo he evaluado y limpiado a mano de forma de quedarme con los dos únicos nuevos subdominios.
- Llama especial atención que aparezca un subdominio typosquatting. He intentado revisar su certificado pero no tiene y la conexión no es segura.



TLS probing

Para ello utilizamos la herramienta cero.

```
(kali@kali)~/recopilacion-informacion/practica
└─$ cero -d clubhouse.com
clubhouse.com
```

```
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ cero -d clubhouseapi.com
sni.cloudflaressl.com
clubhouseapi.com
```

```
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ cero -d joinclubhouse.com
sni.cloudflaressl.com
joinclubhouse.com
```

Al visitar la web para TLS Probing no hemos encontrado nada nuevo, salvo:

- joinclubhouse.com  Redirige a Clubhouse.com

Scrapping

Para obtener subdominios a través de scraping utilizaremos dos herramientas: gospider y unfurl. gospider tiene la funcionalidad de buscar también en el archivo de Robots, con lo que evitamos revisarlo, como sucede con el sitemap.

```
GOSPIDER
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ gospider -s "https://clubhouse.com/" -t 5 -d 5 --blacklist jpg,jpeg,gif,css,tif,tiff,png,tf,woff,woff2,ico,pdf,svg --sitemap --robots
> gospiderout_1.txt


(kali@kali)-[~/recopilacion-informacion/practica]
└─$ gospider -s "https://joinclubhouse.com/" -t 5 -d 5 --blacklist jpg,jpeg,gif,css,tif,tiff,png,tf,woff,woff2,ico,pdf,svg --sitemap --robots
> gospiderout_2.txt

(kali@kali)-[~/recopilacion-informacion/practica]
└─$ gospider -s "https://clubhouseapi.com/" -t 5 -d 5 --blacklist jpg,jpeg,gif,css,tif,tiff,png,tf,woff,woff2,ico,pdf,svg --sitemap --robots
> gospiderout_3.txt

(kali@kali)-[~/recopilacion-informacion/practica]
└─$ cat gospiderout_1.txt gospiderout_2.txt gospiderout_3.txt > gospider_todos.txt

(kali@kali)-[~/recopilacion-informacion/ctfr]
└─$ cat gospider_todos.txt | grep -Eo '([http|https]://[^\s/]+)' | unfurl --unique domains > gospider_clean.txt
```



Archivo  gospider_clean.txt

Obtenemos los dominios con unfurl que ya han sido limpiados mediante expresiones regulares. Resultado:

```
www.clubhouse.com
fonts.googleapis.com
blog.clubhouse.com
clubhouse.app.link
support.clubhouse.com
welcome.clubhouse.com
creators.clubhouse.com
community.clubhouse.com
airtable.com
twitter.com
www.instagram.com
www.linkedin.com
privacy.clubhouse.com
tos.clubhouse.com
browser.sentry-cdn.com
joinclubhouse.com
clubhouseapi.com
drive.google.com
www.cloudflare.com
support.cloudflare.com
www.w3.org
jobs.lever.co
a16z.com
www.bloomberg.com
www.nytimes.com
```



No he encontrado nuevos subdominios en Bing, Google o Yandex.

```
site:joinclubhouse.com -www.joinclubhouse.com
```

Certificate Transparency

Vamos a obtener subdominios a traves de comprobar donde se han utilizado los certificados.

```
(kali@kali)-[~]
└─$ python3 ctfr.py -d 'clubhouse.com' -o ctfr1.txt

(kali@kali)-[~]
└─$ python3 ctfr.py -d 'clubhouseapi.com' -o ctfr2.txt

(kali@kali)-[~]
└─$ python3 ctfr.py -d 'joinclubhouse.com' -o ctfr3.txt

(kali@kali)-[~]
└─$ cat ctfr1.txt ctfr2.txt ctfr3.txt > ctfr.txt
```


Obtenemos 41 subdominios, la mayoría contábamos con ellos y vemos que algunos como los del * no nos son util.





Archivo  ctfr.txt

```
*.clubhouse.com
clubhouse.com
*.staging.clubhouse.com
staging.clubhouse.com
blog.clubhouse.com
community.clubhouse.com
creators.clubhouse.com
eng-blog.clubhouse.com
go.clubhouse.com
privacy.clubhouse.com
tos.clubhouse.com
*.clubhouseapi.com
clubhouseapi.com
*.staging.clubhouseapi.com
*.staging.clubhouseapi.com
staging.clubhouseapi.com
clubhouseapi.com
clubhouseapi.com
www.clubhouseapi.com
ultravox.staging.clubhouseapi.com
www.clubhouseapi.com
*.joinclubhouse.com
*.joinclubhouse.com
joinclubhouse.com
*.staging.joinclubhouse.com
*.staging.joinclubhouse.com
staging.joinclubhouse.com
bulletin.joinclubhouse.com
bulletinadd.joinclubhouse.com
community.joinclubhouse.com
incident.joinclubhouse.com
privacy.joinclubhouse.com
profilealert.joinclubhouse.com
staging.joinclubhouse.com
support.joinclubhouse.com
supportrequest.joinclubhouse.com
suspension.joinclubhouse.com
tos.joinclubhouse.com
welcome.joinclubhouse.com
whatsnew.joinclubhouse.com
www.joinclubhouse.com
```

Fuentes pasivas

- BinaryEdge  Hemos encontrado únicamente un nuevo subdominio:

```
incident.joinclubhouse.com
```

- RiskIQ  No hemos encontrado nuevos subdominios.
- Project Crobat  solo hemos encontrado subdominios para el dominio joinclubhouse.com.

```
└─(kali@kali)-[~/recopilacion-informacion/practica]
└─$ crobat -s joinclubhouse.com -u > crobat_sub.txt

└─(kali@kali)-[~/recopilacion-informacion/practica]
└─$ echo "incident.joinclubhouse.com" >> crobat_sub.txt
```

```
joinclubhouse.com
community.joinclubhouse.com
ios.joinclubhouse.com
o1.ptr382.joinclubhouse.com
o2.ptr102.joinclubhouse.com
privacy.joinclubhouse.com
support.joinclubhouse.com
tos.joinclubhouse.com
whatsnew.joinclubhouse.com
www.joinclubhouse.com
incident.joinclubhouse.com
```



Archivo  crobat_sub.txt

Caches y archivos web

Buscamos en el WayBackMachine subdominios posibles.

```
└─(kali@kali)-[~/recopilacion-informacion/practica]
└─$ cat dominios.txt | waybackurls > urls_last.txt
```

- Hemos obtenido 1573816 URLs antes de limpiar con furl.


```
cat urls_last.txt | grep -Eo '(http|https)://[^\s/]+)' | unfurl --unique domains > url_last_clean.txt
```



Muchos de las URL obtenidas no pertenecen a la organización. Por lo que son eliminadas.

- El resultado final son 40 subdominios.



Archivo  url_last_clean.txt

Github

Utilizamos la herramienta github-search para localizar en GitHub subdominios a partir de los dominios datos, he localizado 6.

```
└─(kali@kali)-[~/recopilacion-informacion/github-search]
└─$ ./github-subdomains.py -t ghp_ussj1raCovKuDGb34IGIpLNx8TaFZ0qPAHW -d clubhouse.com > gsearch_clubhouse.txt

└─(kali@kali)-[~/recopilacion-informacion/github-search]
```



```

└─$ ./github-subdomains.py -t ghp_ussj1raCovKuDGb34IGIpLNx8TaFZ0qPAHW -d clubhouseapi.com > gsearch_clubhouseapi.txt

└─(kali@kali)-[~/recopilacion-informacion/github-search]
└─$ ./github-subdomains.py -t ghp_ussj1raCovKuDGb34IGIpLNx8TaFZ0qPAHW -d joinclubhouse.com > gsearch_joinclubhouse.txt

```



Archivo gsearch_todos.txt

Herramienta: ReconFTW

Hemos elegido esta herramienta por ser nueva y ver reportes positivos sobre ella.

```

└─(kali@kali)-[~/recopilacion-informacion/reconftw]
└─$ ./reconftw.sh -l ~/recopilacion-informacion/practica/dominios.txt -s --deep 2 -o ~/recopilacion-informacion/practica/reconftw_subd.txt

```

Herramienta: AMASS

Para el reconocimiento de subdominios, finalmente voy a utilizar AMASS.

```

└─(kali@kali)-[~/recopilacion-informacion/practica]
└─$ amass enum -active -brute -dir amass_CH -d clubhouse.com, joinclubhouse.com, clubhouseapi.com

```

Con el análisis hemos localizado 30 subdominios. Además hemos obtenido la siguiente información:

```

OWASP Amass v3.15.2                                     https://github.com/OWASP/Amass
-----
30 names discovered - archive: 3, alt: 10, api: 3, crawl: 3, brute: 5, cert: 6
-----
ASN: 14618 - AMAZON-AES - Amazon.com, Inc.
      54.144.0.0/14          9 Subdomain Name(s)
      52.72.0.0/15          1 Subdomain Name(s)
ASN: 16509 - AMAZON-02 - Amazon.com, Inc.
      76.76.21.0/24         8 Subdomain Name(s)
ASN: 13335 - CLOUDFLARENET - Cloudflare, Inc.
      104.16.0.0/14         26 Subdomain Name(s)
      2606:4700::/47        28 Subdomain Name(s)
ASN: 54113 - AS54113 - FASTLY
      146.75.32.0/22        1 Subdomain Name(s)
      2a04:4e42::/47        1 Subdomain Name(s)

```

Podemos observar como nos devuelve las direcciones IP de los subdominios y ninguno esta hosteado por el mismo Clubhouse.



Archivo /amass_CH/amass.txt

Subdominios definitivos

A continuación uniremos todos los ficheros resultantes para tener unificados todos los subdominios. Por ahora tenemos encontrado 148 subdominios relacionados con Clubhouse.

```

└─(kali@kali)-[~/recopilacion-informacion/practica]
└─$ cat subdominios_tot.txt ctf.txt gospider_clean.txt crobat_sub.txt analyticsrelationships.txt gsearch_todos.txt ./amass_CH/amass.txt
    | uniq > subdominios.txt

```



Archivo subdominios.txt

Para verificar que no se ha colado ninguno fuera comprobamos, eliminamos, volvemos a verificar que no estén duplicados:

```
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ sort subdominios.txt | uniq > subdominios2.txt
```

Finalmente tenemos 58 subdominios.



Archivo subdominios2.txt

Fingerprint

He lanzado un nmap, el cual me ha dado problemas al resolver algunas direcciones de subdominios, por lo consiguiente los he comprobado fuera de la maquina virtual y tenia el mismo problema, han sido los siguientes dominios, y han sido eliminados.

```
Failed to resolve "11tos.clubhouse.com".
Failed to resolve "bulletinadd.joinclubhouse.com".
Failed to resolve "bulletin.joinclubhouse.com".
Failed to resolve "eng-blog.clubhouse.com".
Failed to resolve "korea-www.clubhouse.com".
Failed to resolve "partnershipstesting.clubhouse.com".
Failed to resolve "sqlprivacy.clubhouse.com".
Failed to resolve "staging.clubhouseapi.com".
Failed to resolve "supportcms1.clubhouse.com".
Failed to resolve "supportrequest.joinclubhouse.com".
Failed to resolve "turk-go.clubhouse.com".
Failed to resolve "whatsnewboards.clubhouse.com".
Failed to resolve "www-nautilus.clubhouse.com".
Failed to resolve "www-nautiluskorea.clubhouse.com".
```



Procedo al borrado manual. Quedan 44 subdominios.



Archivo resultante subdominios3.txt

Descubrimiento de host

He lanzado un analisis de host localizando 43IPs, de las cuales 42 host estan conectados. Podemos deducir que la diferencia de IP y host es debido a que uno de ellos rechaza la conexión.

```
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ sudo nmap -sn -PE -iL subdominios3.txt -oA nmap_1
```

- -sn para el descubrimiento de host.
- -PE para trabajar con paquetes del protocolo ICMP
- -iL Para trabajar con los subdominios localizados.










Archivo nmap_1

Descubrimiento de puertos y servicios

Hemos localizado 43 IPs en 43host que estan funcionando.

```
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ sudo nmap -Pn -sS -sV -sC -T4 -iL subdominios3.txt -oA nmap_1
```

- -Pn  para tratar a todos como si estuvieran todos online
- -sS  Como técnica de escaneo TCP SYN, simulando un paquete de solicitud de conexion.
- -sV  Para conocer la version del sistema
- -sC  Para lanzar scripts
- -T4  Para aumentar la velocidad de escaneo
- -iL  para pasarle un fichero con los targets
- -oA  Para indicarle que nos guarde los resultados en tres formatos (nmap, xml, gnmap)

En muchas de las maquinas se repiten un mismo patron y solo en una el patron cambia:



- Las siguientes configuración es compartida por las siguientes máquinas:

Puerto	Servicio	Estado	Version	Info
80	http	open	Cloudflare http proxy	
443	ssl/http	open	Cloudflare http proxy	
8080	http	open	Cloudflare http proxy	
8443	ssl/http	open	Cloudflare http proxy	

```
admin.joinclubhouse.com (104.18.20.150)
admin-staging.clubhouse.com (104.18.13.12)
incident.joinclubhouse.com (104.18.21.150)
staging.joinclubhouse.com (104.18.14.204)
support.clubhouse.com (104.16.53.111)
admin-staging.joinclubhouse.com (104.18.20.150)
clubhouse.com (104.18.13.12)
cookies.clubhouse.com (104.18.12.12)
images.clubhouseapi.com (104.17.37.19)
ios-staging.joinclubhouse.com (104.18.21.150)
community.joinclubhouse.com (104.18.20.150)
creatorfirst.clubhouse.com (104.18.12.12)
ios-staging.clubhouse.com (104.18.13.12)
privacy.joinclubhouse.com (104.18.21.150)
www.clubhouseapi.com (104.17.37.19)
ios.clubhouse.com (104.18.12.12)
ios.joinclubhouse.com (104.18.20.150)
share.clubhouse.com (104.18.13.12)
support.joinclubhouse.com (104.18.21.150)
joinclubhouse.com (104.18.20.150)
partnerships.clubhouse.com (104.18.12.12)
suspension.clubhouse.com (104.18.13.12)
profilealert.joinclubhouse.com (104.18.20.150)
staging.clubhouse.com (104.18.12.12)
suspension.joinclubhouse.com (104.18.20.150)
welcome.clubhouse.com (104.18.12.12)
tos.joinclubhouse.com (104.18.20.150)
whatsnew.clubhouse.com (104.18.12.12)
welcome.joinclubhouse.com (104.18.20.150)
www.clubhouse.com (104.18.12.12)
whatsnew.joinclubhouse.com (104.18.20.150)
www.joinclubhouse.com (104.18.20.150)
clubhouseapi.com (104.17.37.19)
```

- blog.clubhouse.com  146.75.31.7

Puerto	Servicio	Estado	Version	Info
80	http/proxy	open	Varnish	
443	ssl/http	open	OpenResty web App Server	

- Los siguientes subdominios e IPs comparten configuracion:
 - community.clubhouse.com  76.223.121.104
 - creators.clubhouse.com  76.76.21.164

- privacy.clubhouse.com ▶ 76.223.121.104
- tos.clubhouse.com ▶ 76.76.21.164

Puerto	Servicio	Estado	Version	Info
80	http?	open		
443	ssl/http	open	Vercel	Parámetros para denegar la conexion.

Como nota, el certificado SSL caduca en marzo.

- creators.clubhouse.com ▶ 76.76.21.164

Puerto	Servicio	Estado	Version	Info
80	http	open	Apache httpd	
443	ssl/http	open	Apache httpd	

- ultravox.staging.clubhouseapi.com ▶ 15.197.203.241

Puerto	Servicio	Estado	Version	Info
443	ssl/http	open	awselb/2.0	Parámetros para denegar la conexion. El servicio no se le conoce exploit.

- En este caso todos los puertos escaneados estan cerrados cerrados (1000).
 - o1_ptr382.joinclubhouse.com ▶ 149.72.152.124
 - o1_ptr382.joinclubhouse.com ▶ 149.72.152.124

 Archivo ▶ nmap_2

Descubrimiento de servicios

He intentado descubrir mas servicios, pero no he encontrado nada mas. La unica cosa que remarcar de nuevo es lo indicado de awselb/2.0, pero no se le conoce exploit. Por lo demás me gustaría remarcar que todos ellos estan protegidos por Cloudflare.

```
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ sudo nmap -Pn -sS -sV -iL subdominios3.txt -oA nmap_3
```

 Archivo ▶ nmap_3

Detección de servicios mediante UDP

Utilizamos la detección de servicios mediante la capa de internet por si acaso pero no encontramos ningun servicio extra que respondiera.

```
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ sudo nmap -Pn -sU -F -iL subdominios3.txt -oA nmap_udp
```

 Archivo ▶ nmap_udp

Firewall ByPass

Al contar con Cloudflare, he intentado utilizar nmap para intentar obtener algun puerto mas mediante la fragmentacion de paquetes, pero no he tenido resultado.




```
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ sudo nmap -f -Pn -sS -iL subdominios3.txt -oA nmap_fire
```

 Archivo  nmap_fire

Analisis Web

A traves de HTTPX hemos comprobado como es el acceso a los subdominios, siendo todos en HTTPS, ademas algunos arrojan error 40X(errones), 30X(redirecciones) y 200(correcto).

```
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ cat subdominios3.txt | httpx -td -ip -sc > httpx.txt
```

- -td  Para ver de nuevo el servicio.
- -ip  Ver la IP
- -sc  Para ver el codigo de estado a la solicitud HTTPS

```
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ cat httpx.txt
https://admin.joinclubhouse.com [301] [104.18.20.150] [Cloudflare]
https://admin-staging.joinclubhouse.com [301] [104.18.20.150] [Cloudflare]
https://www.joinclubhouse.com [301] [104.18.21.150] [Cloudflare]
https://clubhouse.com [302] [104.18.13.12] [Cloudflare]
https://creatorfirst.clubhouse.com [302] [104.18.12.12] [Cloudflare]
https://cookies.clubhouse.com [302] [104.18.12.12] [Cloudflare]
https://community.joinclubhouse.com [301] [104.18.21.150] [Cloudflare]
https://go.clubhouse.com [301] [52.72.13.96] [Apache]
https://ios-staging.joinclubhouse.com [301] [104.18.20.150] [Cloudflare]
https://incident.joinclubhouse.com [301] [104.18.21.150] [Cloudflare]
https://images.clubhouseapi.com [403] [104.17.36.19] [Amazon Cloudfront,Amazon Web Services,Cloudflare,Cloudflare Bot Management]
https://suspension.clubhouse.com [302] [104.18.13.12] [Cloudflare]
https://ios.joinclubhouse.com [301] [104.18.21.150] [Cloudflare]
https://blog.clubhouse.com [200] [151.101.3.7] [Ghost,Google Font API,Nginx,Node.js,OpenResty,Varnish]
https://joinclubhouse.com [301] [104.18.21.150] [Cloudflare]
https://privacy.joinclubhouse.com [301] [104.18.21.150] [Cloudflare]
https://profilealert.joinclubhouse.com [301] [104.18.20.150] [Cloudflare]
https://support.joinclubhouse.com [301] [104.18.20.150] [Cloudflare]
https://admin-staging.clubhouse.com [200] [104.18.12.12] [Cloudflare,Google Font API,Google Tag Manager]
https://suspension.joinclubhouse.com [301] [104.18.21.150] [Cloudflare]
https://welcome.clubhouse.com [302] [104.18.12.12] [Cloudflare]
https://tos.joinclubhouse.com [301] [104.18.21.150] [Cloudflare]
https://welcome.joinclubhouse.com [301] [104.18.20.150] [Cloudflare]
https://whatsnew.clubhouse.com [302] [104.18.12.12] [Cloudflare]
https://partnerships.clubhouse.com [302] [104.18.13.12] [Cloudflare]
https://www.clubhouse.com [200] [104.18.12.12] [Cloudflare,Google Font API,Google Tag Manager,Sentry]
https://admin.clubhouse.com [200] [104.18.13.12] [Cloudflare,Google Font API,Google Tag Manager,Sentry]
https://ultravox.staging.clubhouseapi.com [404] [3.33.253.254]
https://whatsnew.joinclubhouse.com [301] [104.18.20.150] [Cloudflare]
https://support.clubhouse.com [301] [104.16.51.111] [Cloudflare,Cloudflare Network Error Logging]
https://clubhouseapi.com [200] [104.17.36.19] [Cloudflare,Cloudflare Bot Management,Google Font API,Google Tag Manager,Sentry]
https://staging.joinclubhouse.com [200] [104.18.15.204] [Cloudflare,Google Font API,Google Tag Manager]
https://ios.clubhouse.com [200] [104.18.12.12] [Cloudflare,Google Font API,Google Tag Manager,Sentry]
https://ios-staging.clubhouse.com [200] [104.18.13.12] [Cloudflare,Google Font API,Google Tag Manager]
https://staging.clubhouse.com [200] [104.18.12.12] [Cloudflare,Google Font API,Google Tag Manager]
https://www.clubhouseapi.com [200] [104.17.36.19] [Cloudflare,Cloudflare Bot Management,Google Font API,Google Tag Manager,Sentry]
https://share.clubhouse.com [200] [104.18.12.12] [Cloudflare,Google Font API,Google Tag Manager,Sentry]
https://creators.clubhouse.com [200] [76.223.123.94] [Google Font API,Next.js,Node.js,React,webpack]
https://privacy.clubhouse.com [200] [76.223.126.116] [Google Font API,Next.js,Node.js,React,webpack]
https://tos.clubhouse.com [200] [76.223.125.115] [Google Font API,Next.js,Node.js,React,webpack]
https://community.clubhouse.com [200] [76.76.21.142] [Google Font API,Next.js,Node.js,React,webpack]
```

 Archivo  httpx.txt

Lanzamos otra consulta para obtener solo las URL para pasárselas a EyeWitness y tener un análisis mas detallado.

```
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ httpx -l subdominios3.txt -silent > httpx_url.txt
```



Archivo  httpx_url.txt

```
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ cat httpx_url.txt
https://www.joinclubhouse.com
https://ios.joinclubhouse.com
https://ios-staging.joinclubhouse.com
https://admin-staging.joinclubhouse.com
https://admin.joinclubhouse.com
https://clubhouse.com
https://joinclubhouse.com
https://ios.clubhouse.com
https://admin-staging.clubhouse.com
https://partnerships.clubhouse.com
https://admin.clubhouse.com
https://community.joinclubhouse.com
https://clubhouseapi.com
https://privacy.joinclubhouse.com
https://creatorfirst.clubhouse.com
https://cookies.clubhouse.com
https://profilealert.joinclubhouse.com
https://privacy.clubhouse.com
https://community.clubhouse.com
https://go.clubhouse.com
https://incident.joinclubhouse.com
https://welcome.clubhouse.com
https://blog.clubhouse.com
https://ultravox.staging.clubhouseapi.com
https://welcome.joinclubhouse.com
https://support.joinclubhouse.com
https://suspension.clubhouse.com
https://share.clubhouse.com
https://staging.joinclubhouse.com
https://whatsnew.clubhouse.com
https://images.clubhouseapi.com
https://suspension.joinclubhouse.com
https://ios-staging.clubhouse.com
https://staging.clubhouse.com
https://whatsnew.joinclubhouse.com
https://tos.joinclubhouse.com
https://tos.clubhouse.com
https://www.clubhouseapi.com
https://www.clubhouse.com
https://support.clubhouse.com
https://creators.clubhouse.com
```

```
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ wc -l httpx_url.txt
41 httpx_url.txt
```

Evaluación de subdominios - Eyewitness

Vamos a lanzar Eyewitness para obtener una vista mas clara de cada subdominio y un analisis mas detallado de cara a poder conocer o categorizar los subdominios.

```
(kali@kali)-[~/recopilacion-informacion/Eyewitness/Python]
└─$ ./Eyewitness.py --web -f ~/recopilacion-informacion/practica/httpx_url.txt -d ~/recopilacion-informacion/practica/Eyewitness
```

Del reporte de EyeWitness, de un total de 41 host obtenemos la siguiente información:

Uncategorized	33
401/401 Unauthorized	1
404 Not found	1


Errors	6
Total	41

No he encontrado nada de lo que esperaba, logins o similar. Los subdominios admin no muestran nada mas allá que la pagina principal;

<https://admin-staging.joinclubhouse.com>
Resolved to: 104.18.21.150

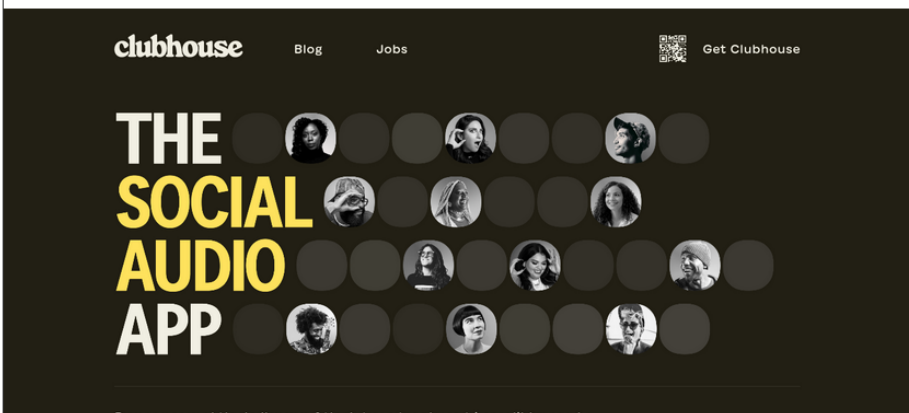
Page Title: Clubhouse: The Social Audio App
Date: Thu, 27 Jan 2022 13:41:37 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: close
x-frame-options: DENY
vary: Accept-Encoding, Origin
x-content-type-options: nosniff
referrer-policy: same-origin
CF-Cache-Status: DYNAMIC
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Server: cloudflare
CF-RAY: 6d42664c598d5c9a-IAD
Response Code: 200

[Source Code](#)



<https://admin.joinclubhouse.com>
Resolved to: 104.18.20.150

Page Title: Clubhouse: The Social Audio App
Date: Thu, 27 Jan 2022 13:41:41 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: close
x-frame-options: DENY
vary: Cookie, Accept-Encoding, Origin
x-content-type-options: nosniff
referrer-policy: same-origin
CF-Cache-Status: DYNAMIC
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Server: cloudflare
CF-RAY: 6d426664af068286-IAD
Response Code: 200




EI



Carpeta  EyeWitness ; analisis extendido  /EyeWitness/report.html

Web Application Firewall

Todos los subdominios recolectados he observado que estan detrás de Cloudflare web proxy, voy a utilizar wafwoof para confirmarlo.

```
(kali@kali) - [~/recopilacion-informacion/practica]
$ wafw00f -l
```

```
(kali@kali) - [~/recopilacion-informacion/practica]
$ wafw00f -i subdominios3.txt -o wafw00f_ch.txt
```

Observo que ademas de Cloudflare en algunos casos también usan AWS Elastic Load Balancer (Amazon) o no usan nada.

- Subdominios que estan protegidos por Cloudflare:

<https://admin.clubhouse.com> Cloudflare (Cloudflare Inc.)
<https://admin.joinclubhouse.com> Cloudflare (Cloudflare Inc.)
<https://admin-staging.clubhouse.com> Cloudflare (Cloudflare Inc.)
<https://admin-staging.joinclubhouse.com> Cloudflare (Cloudflare Inc.)
<https://clubhouseapi.com> Cloudflare (Cloudflare Inc.)
<https://clubhouse.com> Cloudflare (Cloudflare Inc.)
<https://images.clubhouseapi.com> Cloudflare (Cloudflare Inc.)
<https://ios.clubhouse.com> Cloudflare (Cloudflare Inc.)
<https://ios.joinclubhouse.com> Cloudflare (Cloudflare Inc.)
<https://ios-staging.clubhouse.com> Cloudflare (Cloudflare Inc.)
<https://ios-staging.joinclubhouse.com> Cloudflare (Cloudflare Inc.)
<https://joinclubhouse.com> Cloudflare (Cloudflare Inc.)
<https://share.clubhouse.com> Cloudflare (Cloudflare Inc.)
<https://staging.clubhouse.com> Cloudflare (Cloudflare Inc.)
<https://staging.joinclubhouse.com> Cloudflare (Cloudflare Inc.)
<https://support.clubhouse.com> Cloudflare (Cloudflare Inc.)
<https://support.joinclubhouse.com> Cloudflare (Cloudflare Inc.)
<https://suspension.clubhouse.com> Cloudflare (Cloudflare Inc.)
<https://suspension.joinclubhouse.com> Cloudflare (Cloudflare Inc.)
<https://welcome.clubhouse.com> Cloudflare (Cloudflare Inc.)
<https://welcome.joinclubhouse.com> Cloudflare (Cloudflare Inc.)
<https://www.clubhouseapi.com> Cloudflare (Cloudflare Inc.)
<https://www.clubhouse.com> Cloudflare (Cloudflare Inc.)
<https://www.joinclubhouse.com> Cloudflare (Cloudflare Inc.)

- AWS Elastic Load Balancer (Amazon)

<https://cookies.clubhouse.com> AWS Elastic Load Balancer (Amazon)
<https://partnerships.clubhouse.com> AWS Elastic Load Balancer (Amazon)
<https://profilealert.joinclubhouse.com> AWS Elastic Load Balancer (Amazon)
<https://ultravox.staging.clubhouseapi.com> AWS Elastic Load Balancer (Amazon)
<https://whatsnew.clubhouse.com> AWS Elastic Load Balancer (Amazon)
<https://whatsnew.joinclubhouse.com> AWS Elastic Load Balancer (Amazon)

- Desconocido

<https://creatorfirst.clubhouse.com> Generic (Unknown)

- Sin firewall

<https://blog.clubhouse.com> None (None)
<https://community.clubhouse.com> None (None)
<https://community.joinclubhouse.com> None (None)
<https://creators.clubhouse.com> None (None)
<https://go.clubhouse.com> None (None)
<https://privacy.clubhouse.com> None (None)
<https://privacy.joinclubhouse.com> None (None)
<https://tos.clubhouse.com> None (None)
<https://tos.joinclubhouse.com> None (None)



Los subdominios sin firewall pueden ser blanco de ataque.



Archivo wafw00f_ch.txt

Descubrimiento de contenido

Para intentar localizar contenido he lanzado simultaneamente BurpSuite Community y Dirseach.

BurpSuite Community

Para BurpSuite he lanzado 3 escáneres, uno por cada dominio principal.

- Configuración de *BurpSuite* para que no salga del *Scope* en el *Target*.
- Utilizamos y personalizamos una petición *GET* para obtener el *Payload*.

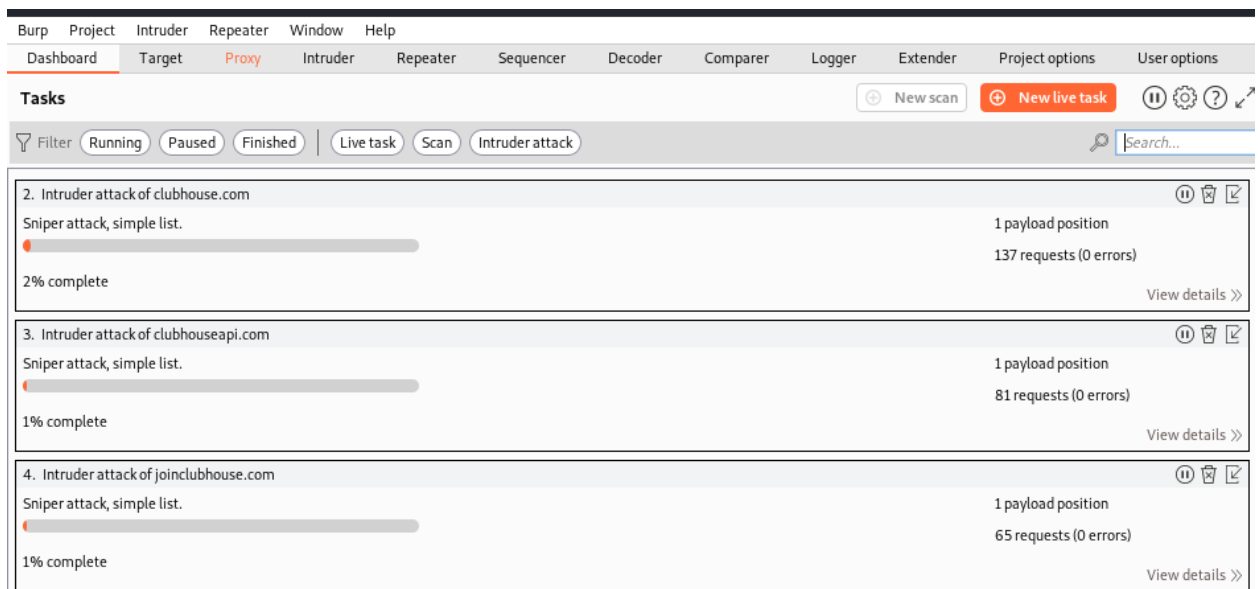
Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
1 GET /$S HTTP/1.1
2 Host: clubhouse.com
3 Sec-Ch-Ua: "Chromium";v="95", ";Not A Brand";v="99"
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: "Linux"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
```

- Utilizamos el diccionario de SecList common.txt
- Lanzamos el ataque.



The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The 'Tasks' panel displays three active intruder attacks:

Task Name	Attack Type	Payload Positions	Requests	Errors	Progress
2. Intruder attack of clubhouse.com	Sniper attack, simple list.	1 payload position	137 requests	0 errors	2% complete
3. Intruder attack of clubhouseapi.com	Sniper attack, simple list.	1 payload position	81 requests	0 errors	1% complete
4. Intruder attack of joinclubhouse.com	Sniper attack, simple list.	1 payload position	65 requests	0 errors	1% complete

En analisis me ha llevado ~15hrs, posteriormente el pc colapso y no pudo continuar.

Dirsearch

Con Dirsearch vamos a analizar los subdominios utilizando su diccionario default. En este caso nos centraremos en los puertos donde la conexión es correcta (200).



Anteriormente hemos lanzado otro análisis en Dirsearch incluyendo los puertos 200 y 300-399. Hemos observado que los aquellas direcciones que emitían mensajes 300-X eran siempre redirecciones a direcciones fuera del scope deseado.

```
(kali@kali)-[~/recopilacion-informacion/dirsearch]
└─$ python3 dirsearch.py -l ~/recopilacion-informacion/practica/subdominios3.txt -i 200,300-399 -t 10 -o ~/recopilacion-informacion/practica/dirsearch_1.txt
```

 Archivo  dirsearch_1.txt

- Conexión correcta (200):

```
(kali@kali)-[~/recopilacion-informacion/dirsearch]
└─$ python3 dirsearch.py -l ~/recopilacion-informacion/practica/subdominios3.txt -i 200 -t 10 -o ~/recopilacion-informacion/practica/dirsearch_200.txt
```



Archivo  dirsearch_200.txt

- He comprobado los siguientes resultados manualmente, entre ellos destaca el enlace <https://creators.clubhouse.com:443/explore> lleva a una web y vamos a usar dirb para analizar la url.

```
https://clubhouseapi.com:443/.well-known/apple-app-site-association
https://clubhouseapi.com:443/.well-known/assetlinks.json
https://community.clubhouse.com:443/index
https://community.clubhouse.com:443/robots.txt
https://creators.clubhouse.com:443/explore
https://creators.clubhouse.com:443/index
https://creators.clubhouse.com:443/robots.txt
https://privacy.clubhouse.com:443/index
https://privacy.clubhouse.com:443/robots.txt
https://tos.clubhouse.com:443/index
https://tos.clubhouse.com:443/robots.txt
https://www.clubhouseapi.com:443/.well-known/assetlinks.json
https://www.clubhouseapi.com:443/.well-known/apple-app-site-association
```

Dirb

Vamos a usar Dirb para analizar una URL que parece un directorio y puede contener más información. Ha utilizado su diccionario por default basado en 4612 palabras.

```
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ dirb https://creators.clubhouse.com:443/explore -o dirb.txt
```



Archivo  dirb.txt

El análisis ha dado como dirección otra dirección, la cual indica que no existe cuando se visita:

<https://creators.clubhouse.com:443/explore/cgi-bin/>.

He lanzado otro análisis pero no ha localizado nada más.

Analisis de vulnerabilidades.

Voy a utilizar GreenBone para localizar vulnerabilidades. Hemos configurado el análisis utilizando todos los subdominios recolectados, y escaneando todos los puertos TCP y los mas usados de UDP.

New Task

Name

clubhouse

Comment

Scan Targets

Clubhouse ▼ ★

Add results to Assets

☒ Yes ☐ No

Apply Overrides

☒ Yes ☐ No

Min QoD

70 ▲ ▼ %

Alterable Task

☐ Yes ☒ No

Auto Delete Reports

☒ Do not automatically delete reports
☐ Automatically delete oldest reports but always keep newest 5 ▲ ▼ reports

Scanner

OpenVAS Default ▼

Scan Config

Full and fast ▼

Network Source Interface

Order for target hosts

Sequential ▼

Cancel

Save



Finalmente no he podido completar el analisis pese a intentarlo de diferentes formas y lugares. La maquina se desconectaba continuamente, perdía la conexion y tenia que reiniciarla para reanudar el analisis.

Vulnerabilidades

Ante la imposibilidad en un principio de utilizar GSM, hice uso de Nuclei:

```
(kali@kali)-[~/recopilacion-informacion/practica]
└─$ nuclei -l subdominios3.txt -o nuclei_analisis.txt
```


Entre los resultados que he obtenido no he podido obtener mucha informacion. Todo esta protegido por un firewall y apuntando a direcciones externas al scope.

```
(kali@kali)-[~/recopilacion-informacion/practica]
$ cat nuclei_analysis

(kali@kali)-[~/recopilacion-informacion/practica]
$ cat nuclei_analysis.txt
[2022-01-28 23:39:52] [dns-waf-detect:cloudflare] [dns] [info] admin.joinclubhouse.com
[2022-01-28 23:39:52] [dns-waf-detect:cloudflare] [dns] [info] incident.joinclubhouse.com
[2022-01-28 23:39:52] [dns-waf-detect:cloudflare] [dns] [info] clubhouseapi.com
[2022-01-28 23:39:52] [dns-waf-detect:cloudflare] [dns] [info] images.clubhouseapi.com
[2022-01-28 23:39:52] [dns-waf-detect:cloudflare] [dns] [info] ios-staging.clubhouse.com
[2022-01-28 23:39:52] [dns-waf-detect:cloudflare] [dns] [info] clubhouse.com
[2022-01-28 23:39:52] [dns-waf-detect:cloudflare] [dns] [info] cookies.clubhouse.com
[2022-01-28 23:39:52] [dns-waf-detect:cloudflare] [dns] [info] creatorfirst.clubhouse.com
[2022-01-28 23:39:52] [dns-waf-detect:cloudflare] [dns] [info] admin-staging.clubhouse.com
[2022-01-28 23:39:52] [dns-waf-detect:cloudflare] [dns] [info] admin-staging.joinclubhouse.com
[2022-01-28 23:39:52] [dns-waf-detect:cloudflare] [dns] [info] privacy.joinclubhouse.com
[2022-01-28 23:39:52] [dns-waf-detect:cloudflare] [dns] [info] community.joinclubhouse.com
[2022-01-28 23:39:52] [dns-waf-detect:cloudflare] [dns] [info] joinclubhouse.com
[2022-01-28 23:39:52] [dns-waf-detect:cloudflare] [dns] [info] admin.clubhouse.com
[2022-01-28 23:39:52] [dns-waf-detect:cloudflare] [dns] [info] ios-staging.joinclubhouse.com
[2022-01-28 23:39:52] [dns-waf-detect:cloudflare] [dns] [info] ios.joinclubhouse.com
```

Extracto ejemplo de los resultados obtenidos de Nuclei.



Archivo  nuclei_analysis.txt

Cifrados y seguridad

He utilizado TestSSL para conocer si existe alguna vulnerabilidad SSL y ademas comprobar los algoritmos de cifrado e intercambio de claves.

```
(kali@kali)-[~/recopilacion-informacion/testssl.sh]
$ ./testssl.sh -iL ~/recopilacion-informacion/practica/subdominios3.txt --json
```

- Todos los dominios mostrados a continuación estan agrupados en funcion de sus vulnerabilidades:

Dominio + Puntuación	Vulnerabilidades compartidas
admin.clubhouse.com  B	SWEET32 (CVE-2016-2183, CVE-2016-6329)
admin.joinclubhouse.com  B	LUCKY13 (CVE-2013-0169)
http://admin-staging.clubhouse.com/  B	BEAST (CVE-2011-3389)
admin-staging.joinclubhouse.com  B	
clubhouseapi.com  B	
clubhouse.com  B	
community.joinclubhouse.com  B	
cookies.clubhouse.com  B	
creatorfirst.clubhouse.com  B	
images.clubhouseapi.com  B	
incident.joinclubhouse.com  B	
ios.joinclubhouse.com  B	
ios-staging.joinclubhouse.com  B	
joinclubhouse.com  B	
partnerships.clubhouse.com  B	
privacy.joinclubhouse.com  B	
profilealert.joinclubhouse.com  B	
support.clubhouse.com  B	
support.joinclubhouse.com  B	
suspension.clubhouse.com  B	

Dominio + Puntuación	Vulnerabilidades compartidas
suspension.joinclubhouse.com ▶ B	
tos.joinclubhouse.com ▶ B	
welcome.clubhouse.com ▶ B	
welcome.joinclubhouse.com ▶ B	
whatsnew.clubhouse.com ▶ B	
whatsnew.joinclubhouse.com ▶ B	
www.joinclubhouse.com ▶ B	

Dominio + Puntuación	Vulnerabilidades compartidas
ios.clubhouse.com ▶ B	BREACH (CVE-2013-3587) ▶ Potencial
ios-staging.clubhouse.com ▶ B	RC4 (CVE-2013-2566, CVE-2015-2808)
share.clubhouse.com ▶ B	LUCKY13 (CVE-2013-0169)
staging.clubhouse.com ▶ B	SWEET32 (CVE-2016-2183, CVE-2016-6329)
staging.joinclubhouse.com ▶ B	
staging.joinclubhouse.com ▶ B	
www.clubhouseapi.com ▶ B	
www.clubhouse.com ▶ B	

- A continuación, dominios y vulnerabilidades.

Dominio + Puntuación	Vulnerabilidad
go.clubhouse.com ▶ B	Error de certificado
	RC4 (CVE-2013-2566, CVE-2015-2808)
	LUCKY13 (CVE-2013-0169)
	SWEET32 (CVE-2016-2183, CVE-2016-6329)
blog.clubhouse.com ▶ A	LUCKY13 (CVE-2013-0169)
privacy.clubhouse.com ▶ A+	BREACH (CVE-2013-3587) ▶ Potencial
tos.clubhouse.com ▶ A+	BREACH (CVE-2013-3587) ▶ Potencial
ultravox.staging.clubhouseapi.com ▶ B	LUCKY13 (CVE-2013-0169)
	BEAST (CVE-2011-3389)



Todas las vulnerabilidades estan relacionadas con la criptografía, cifrado de claves.

Correo electrónico

He evaluado si seria posible suplantar los correos electrónicos de la organización pertenecientes al scope utilizando la herramienta spoofcheck. En los tres casos he encontrado que es posible enviar mensajes suplantando la identidad de la organización al no tener DMARC o no configurado o configurado a None.

```

(kali@kali)-[~/recopilacion-informacion/spoofcheck]
└─$ python3 spoofcheck.py clubhouse.com
[*] Found SPF record:
[*] v=spf1 include:_spf.google.com include:sendgrid.net include:mail.zendesk.com ~all
[*] SPF record contains an All item: ~all
[*] Found DMARC record:
[*] v=DMARC1; p=none; rua=mailto:rohan@alphaexplorationco.com, mailto:dmarc_agg@vali.email;
[+] DMARC policy set to none
[*] Aggregate reports will be sent: mailto:rohan@alphaexplorationco.com, mailto:dmarc_agg@vali.email
[+] Spoofing possible for clubhouse.com!

(kali@kali)-[~/recopilacion-informacion/spoofcheck]
└─$ python3 spoofcheck.py clubhouseapi.com
[+] clubhouseapi.com has no SPF record!
[*] No DMARC record found. Looking for organizational record
[+] No organizational DMARC record
[+] Spoofing possible for clubhouseapi.com!

(kali@kali)-[~/recopilacion-informacion/spoofcheck]
└─$ python3 spoofcheck.py joinclubhouse.com
[*] Found SPF record:
[*] v=spf1 include:_spf.google.com include:mail.zendesk.com ~all
[*] SPF record contains an All item: ~all
[*] Found DMARC record:
[*] v=DMARC1; p=none; rua=mailto:rohan@alphaexplorationco.com, mailto:dmarc_agg@vali.email;
[+] DMARC policy set to none
[*] Aggregate reports will be sent: mailto:rohan@alphaexplorationco.com, mailto:dmarc_agg@vali.email
[+] Spoofing possible for joinclubhouse.com!

```

- [clubhouseapi.com](#) 🟡 No esta configurado ni el SPF ni el DMARC
- [clubhouse.com](#) 🟡 DMARC no esta configurado correctamente (verificado por dmarcian.com)
- [joinclubhouse.com](#) 🟡 DMARC no esta configurado correctamente (verificado por dmarcian.com)

Subdomain takeover

En la ultima parte voy a examinar si existe la posibilidad de que el servidor que esta alojando el dominio pueda ser configurado de forma que re-direccione a una direccion maliciosa.

```

(kali@kali)-[~/recopilacion-informacion/practica]
└─$ subzy -targets subdominios3.txt

```



En ninguno de los casos se ha encontrado vulnerabilidad alguna de cara a sufrir un subdomain takeover.



Archivo 🟡 subzy_takeover.txt

OSINT

Vamos a intentar obtener informacion de las fuentes abiertas, me gustaría haber usado Lampyre junto con Maltego pero la primera, ma daba error al acceder.

Motores de búsqueda

Voy a utilizar los motores de busqueda de cara a encontrar documentos o archivos que me permitan analizar los metadatos y localizar a algún contacto de la organización.



He accedido a [exploit-db.com](#) para obtener dorcks aplicables de cara a obtener informacion de la organización:

```
site:clubhouse.com ext:pdf
url:clubhouse.com intext:"Index of" "email.txt"
url:clubhouse.com ext:(doc | pdf | xls | txt |) inurl:confidential
url:clubhouse.com intitle:"index of" "/usernames"
```

✗ No he encontrado nada interesante.

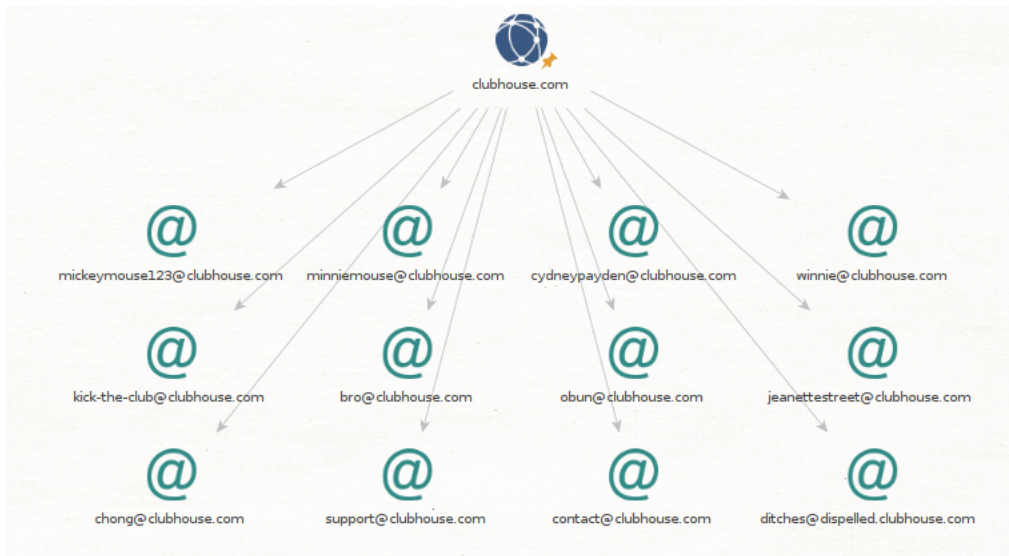
Busqueda de contactos

Voy a utilizar diferentes herramientas para localizar diferentes contactos y/o emails.

✗ Los emails que aparezcan repetidos en diferentes herramientas serán obviados y para no repetirlos.

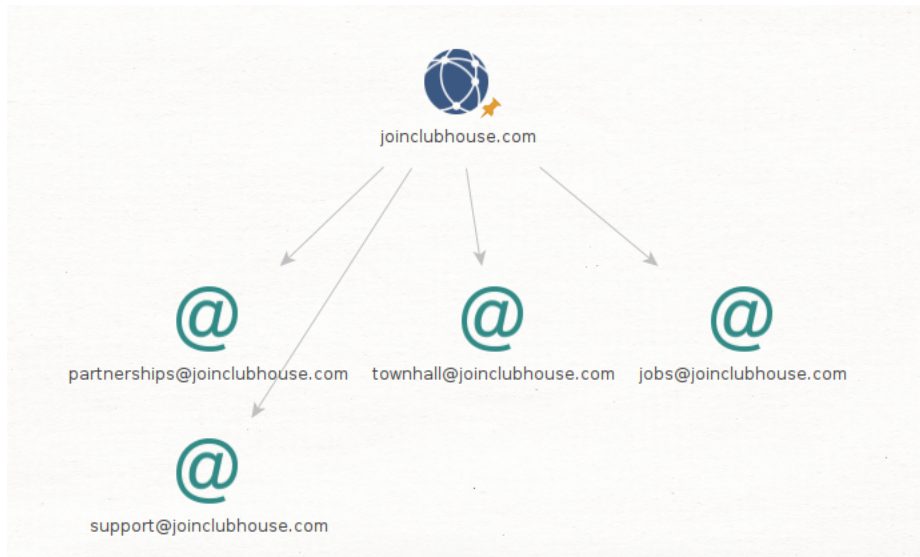
Maltego / Intelligence X

Voy a utilizar Maltego con la utilidad de buscar mails de IntelIX.



- Hemos obtenido los siguientes correos del dominio clubhouse.com

```
► mickeymouse123@clubhouse.com
► minniemouse@clubhouse.com
► cydney payden@clubhouse.com
► winnie@clubhouse.com
► kick-the-club@clubhouse.com
► bro@clubhouse.com
► obun@clubhouse.com
► jeannetestreet@clubhouse.com
► chong@clubhouse.com
► support@clubhouse.com
► contact@clubhouse.com
► ditches@dispelled.clubhouse.com
```



```
► partnerships@joinclubhouse.com
► townhall@joinclubhouse.com
► jobs@joinclubhouse.com
► support@joinclubhouse.com
```

✗ Del dominio clubhouseapi.com no he obtenido ningún email.

Hunter.io

La herramienta online Hunter.io permite obtener mail relacionados con los dominios.

```
► luke@clubhouse.com
► reception@clubhouse.com
► partnerships@clubhouse.com
► press@clubhouse.com
► townhall@clubhouse.com
► westyellowstone@clubhouse.com
► international@clubhouse.com




► security@joinclubhouse.com
► press@joinclubhouse.com
```



✗ Del dominio clubhouseapi.com en esta herramienta no he encontrado mail alguno.

Spiderfoot

- clubhouse.com

```
└─(kali@kali)-[~/recopilacion-informacion/spiderfoot-3.5]
└─$ ./sf.py -s clubhouse.com -t EMAILADDR -f -x -q > spider_OSINT_1.txt
```



- -s  Objetivo
- -t  Informacion a recolectar
- -f  Obtener la informacion solo recogida en la informacion a recolectar

- -x  Modo estricto: Solo los módulos activos o seleccionados.
- -q  Deshabilitar registro.

```

▶ cydneypayden@clubhouse.com
▶ sexygirl@clubhouse.com
▶ cym46@clubhouse.com
▶ six@clubhouse.com
▶ zentrelthibodaux@clubhouse.com
▶ dees@clubhouse.com
▶ george.porcella@clubhouse.com
▶ rsvp@clubhouse.com
▶ filmchenelle77@clubhouse.com

```

 Archivo con los mails recopilados por spiderfoot  spider_OSINT_1.txt

- joinclubhouse.com

```



└─(kali@kali)-[~/recopilacion-informacion/spiderfoot-3.5]
└─$ ./sf.py -s joinclubhouse.com -t EMAILADDR -f -x -q > spider_OSINT_3.txt

```

```

▶ suspensions@joinclubhouse.com
▶ suspension@joinclubhouse.com
▶ jobs@joinclubhouse.com

```


 Archivo con los mails recopilados por spiderfoot  spider_OSINT_3.txt


- clubhouseapi.com

```

└─(kali@kali)-[~/recopilacion-informacion/spiderfoot-3.5]
└─$ ./sf.py -s clubhouseapi.com -t EMAILADDR -f -x -q > spider_OSINT_2.txt

```

 No se han encontrado correos relacionados con clubhouseapi.com

 Archivo con todos los mails recopilados  emails.txt

Inciso - clubhouseapi.com

Debido a que no he encontrado emails relacionados con el dominio clubhouseapi.com he investigado a través de GitHub por si pudiera localizar algún email desde algún commit del repositorio de Clubhouse, pero éste no existe.

Otra idea posible es analizar desde la cuenta de LinkedIn de la organización aquellas personas que trabajan en IT e intentar cruzar sus datos con los resultados de búsqueda de GitHub y así conocer el mail de la empresa en caso de haber realizado algún commit con él.

Verificación de correos.

He utilizado la herramienta online hunter.io que permite verificar hasta 200 mails desde una cuenta gratuita y obtener una visión general de la verificación.



Verification statuses

- Accept all (97.1% • 34 email addresses)
- Invalid (2.9% • 1 email address)

- Observaciones:

✖ No validos
- ditches@dispelled.clubhouse.com

>45%
- sexygirl@clubhouse.com
- cym46@clubhouse.co
- six@clubhouse.com
- rsvp@clubhouse.com



Archivo con todos los mails verificados ▶ verificacion_de_emails.csv

Correos comprometidos

Vamos a verificar si alguno de los correos de los dominios de la organización han aparecido en alguna brecha o alguna filtración de datos.

```
(kali@kali) - [~/recopilacion-informacion/spiderfoot-3.5]
$ ./sf.py -m sfp_spider,sfp_hunter,sfp_fullcontact,sfp_pgp,sfp_emailformat,sfp_email,sfp_citadel,sfp_intelx,sfp_scylla -s clubhouse.com
-q -F EMAILADDR,EMAILADDR_COMPROMISED

(kali@kali) - [~/recopilacion-informacion/spiderfoot-3.5]
$ ./sf.py -m sfp_spider,sfp_hunter,sfp_fullcontact,sfp_pgp,sfp_emailformat,sfp_email,sfp_citadel,sfp_intelx,sfp_scylla -s clubhouseapi.com
-q -F EMAILADDR,EMAILADDR_COMPROMISED

(kali@kali) - [~/recopilacion-informacion/spiderfoot-3.5]
$ ./sf.py -m sfp_spider,sfp_hunter,sfp_fullcontact,sfp_pgp,sfp_emailformat,sfp_email,sfp_citadel,sfp_intelx,sfp_scylla -s joinclubhouse.com
-q -F EMAILADDR,EMAILADDR_COMPROMISED
```

sexygirl@clubhouse.com
westyellowstone@clubhouse.com
cym46@clubhouse.com
six@clubhouse.com
dees@clubhouse.com
mickeymouse@clubhouse.com
cydney payden@clubhouse.com
zentrelthibodaux@clubhouse.com
copyright@clubhouse.com
creatorfirstindia@clubhouse.com
creatorfirstbrazil@clubhouse.com
creatorfirstindia@clubhouse.com
creatorfirstbrazil@clubhouse.com



De nuevo ningún mail correspondiente del dominio clubhouseapi.com aparece. En este caso, si tuviéramos algún mail y no apareciera sería positivo.



No aparece ningún mail comprometido del dominio joinclubhouse.com.

- Posteriormente verificado los mail que acabamos de obtener y todos ellos los considera aceptable, teniendo una puntuación alrededor de 70%, excepto sexygirl@clubhouse.com que tiene 43%.

Conclusión

He utilizado todas las herramientas que he creído oportuno, en algunos casos repitiendo intentado obtener mas informacion. Otras muchas online las he utilizado a modo de comprobación o intentado obtener mas informacion, sobre todo emails, aunque no obtuve informacion relevante. Me hubiera gustado utilizar GreenBone sin que se me bloqueara el analisis o ver los resultados de BurpSuite a la hora de obtener versiones y sistemas, de forma de obtener mas ingormacion. Por otra parte me hubiera gustado contar con un perfil en LinkedIn preparado para poder analizar trabajadores de clubhouse y expandir mas la rama de OSINT, cruzando datos entre GitHub, mails obtenidos y nombre de trabajadores.