


Practica de recopilacion, fingerprint, footprint, análisis de vulnerabilidades y OSSINT.

He cogido a nextcloud porque lo uso como servidor de ficheros para mi servidor web y quisiera comprobar su seguridad y cuanta información puedo obtener, también tiene un amplio scope

https://hackerone.com/nextcloud/policy_scopes?type=team



Nextcloud
Access, share and protect your files, calendars, contacts, communication & more at home and in your enterprise.
<https://nextcloud.com> · [@nextclouders](#)

Submit report

Bug Bounty Program
Launched in Jun 2016

Reports resolved
503

Assets in scope
93

Average bounty
\$100-\$187

Give feedback

Bookmark

Subscribe

Policy

Scope New!

Hackitivity

Thanks

Updates (2)

Search

Q Search

Scope

All scopes

Maximum severity

Any

Bounty eligibility

All

...

Download Burp Suite Project Configuration File

Download CSV

View changes (Last updated on January 15, 2024)

1-99 of 99

Asset name ↑	Type ↑	Coverage ↑	Max. severity ↓	Bounty ↑	Last update ↑
help.nextcloud.com This asset is running Discourse, and as such reports of newly discovered vulnerabilities should be submitted to their program instead: https://hackerone.com/discourse – Please use this scope only for reporting missing security updates on our Discourse installation.	Domain	In scope	Critical	Ineligible	15/06/2017
nextcloud/files_accesscontrol Code from https://github.com/nextcloud/files_accesscontrol – Note that some folders such as tests and so on will not be packaged. Please make sure that the referenced file is thus also existent in our final releases.	Source code	In scope	Critical	Eligible	15/06/2017
usercontent.apps.nextcloud.com Note that usercontent.apps.nextcloud.com serves					

Obtenemos los registros DNS

Viewdns.info

[Tools](#)[API](#)[Research](#)[Data](#)

[ViewDNS.info](#) > [Tools](#) > **DNS Record Lookup**

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

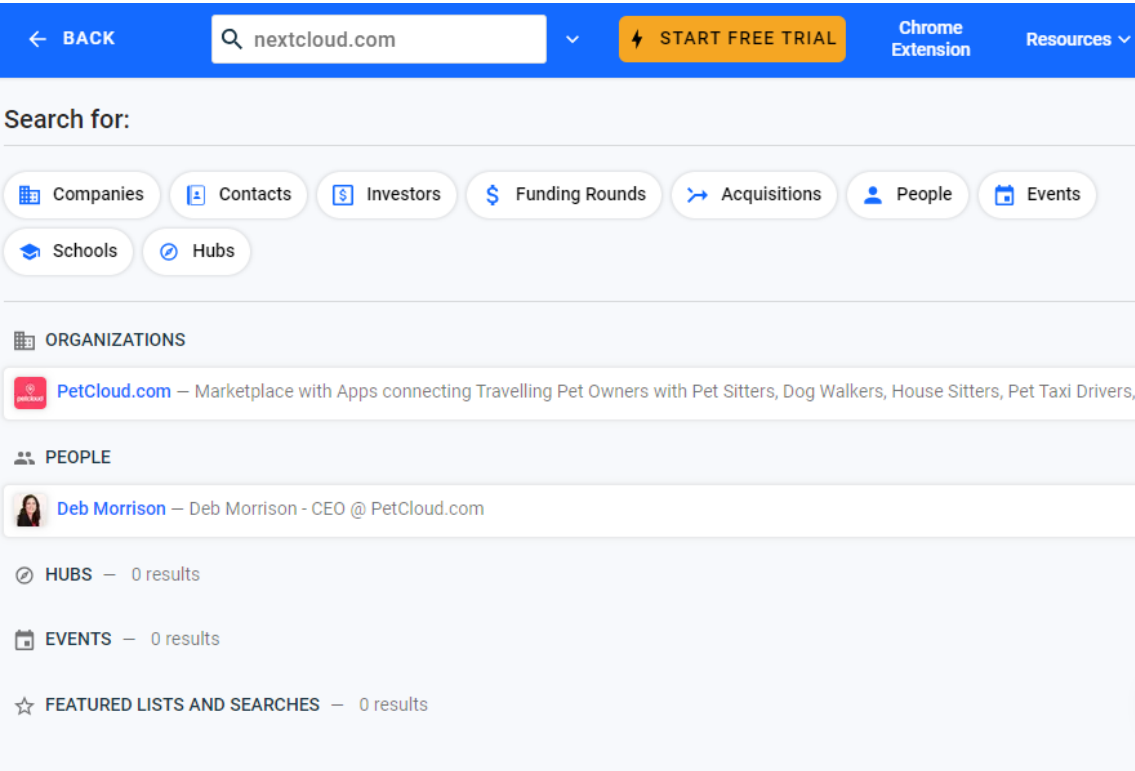
Domain (e.g. domain.com):

DNS Records for nextcloud.com
=====

Name	TTL	Class	Type	Priority	Data
nextcloud.com.	21019	IN	SOA		ns.inwx.de. hostmaster.inwx.de. 2024013101 10800 3600 604800 3600
nextcloud.com.	5654	IN	NS		ns.inwx.de.
nextcloud.com.	5654	IN	NS		ns2.inwx.de.
nextcloud.com.	5654	IN	NS		ns3.inwx.eu.
nextcloud.com.	300	IN	A		85.10.195.17
nextcloud.com.	89	IN	AAAA		2a01:4f8:a0:3068::2
nextcloud.com.	3600	IN	TXT		"MS=2FF4FDA4B4C49AE44213D37A308105AA0D4EBF39"
nextcloud.com.	3600	IN	TXT		"apple-domain-verification=dTWDbt2uCnxS9nIG"
nextcloud.com.	3600	IN	TXT		"google-site-verification=BRRA-GQB6KD9WDj8KhccsNho8-E0Feba52m3uuDZ5w"
nextcloud.com.	3600	IN	TXT		"v=spf1 mx include:sendgrid.net include:amazonses.com include:_spf.eu.sparkpostmail.com -all"
nextcloud.com.	3600	IN	MX	10	mx.nextcloud.com.

A través de Viewdns podemos obtener bastante información sobre el dominio, vemos que tiene su propio servidor de correo mx.nextcloud.com

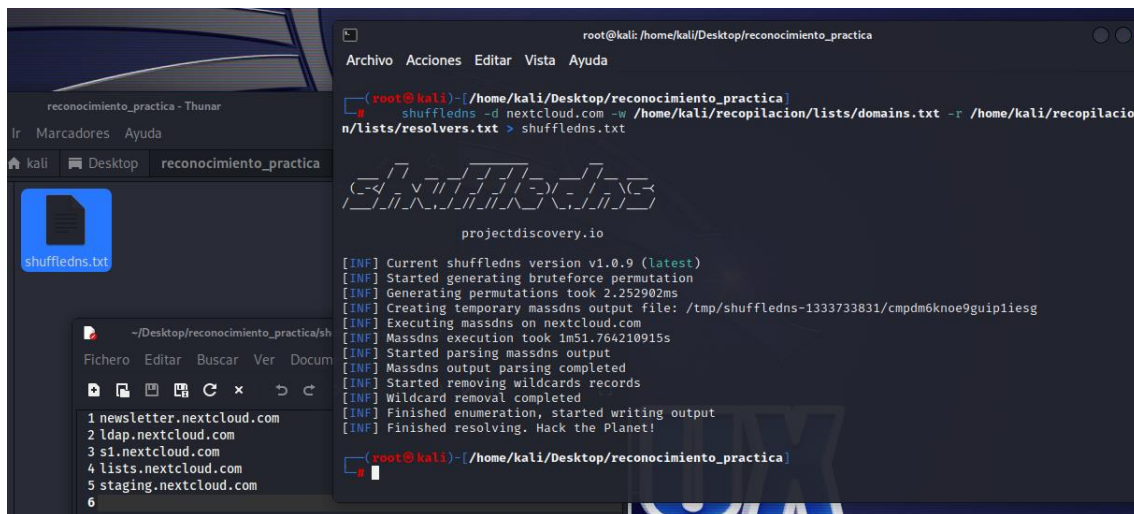
Obteniendo información de la empresa con crunchbase



No aparece Nextcloud así que interpreto que no es una empresa de gran alcance, los resultados que aparecen no tienen nada que ver con la empresa

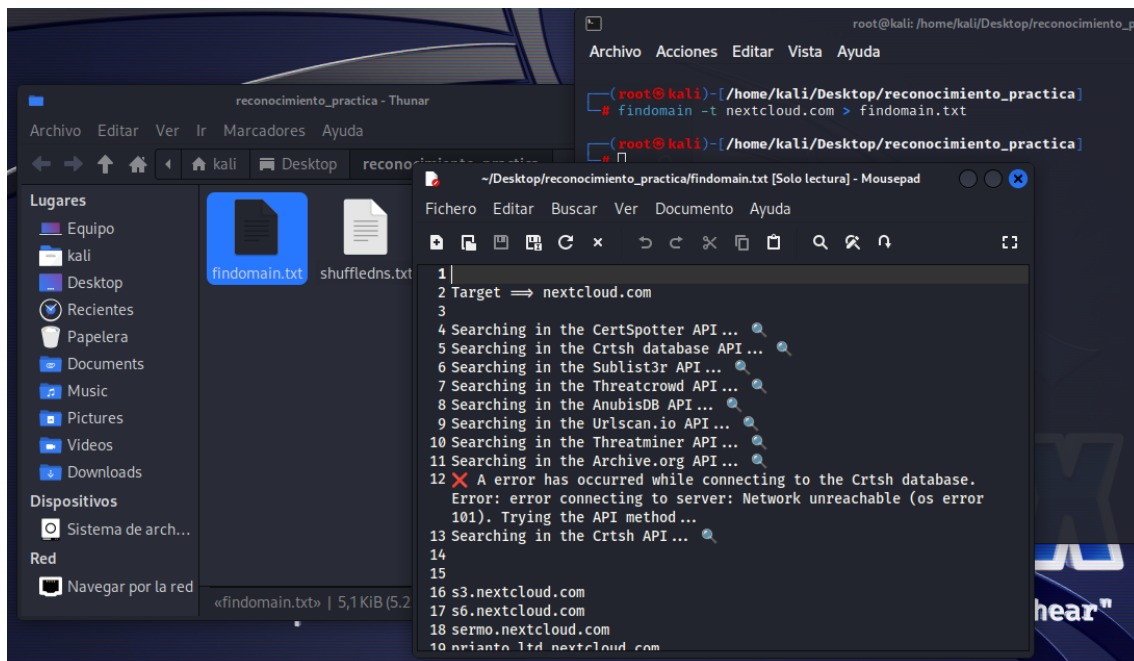
Tecnicas Footprinting

Se usan diferentes herramientas para la extracción de los subdominios que pueda tener nextcloud



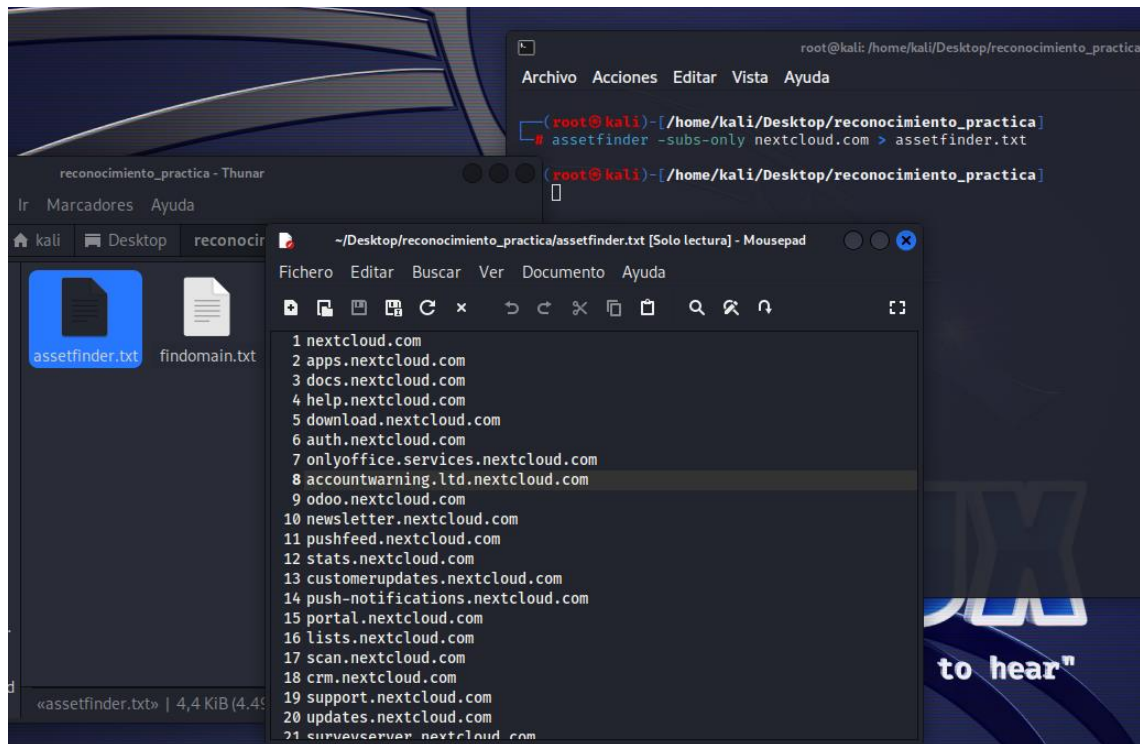
Con shuffledns conseguimos enumerar los dominios vivos que en este caso son 5

Probamos con findomain, en la practica nos devuelve mucho contenido pero que luego habrá que filtrar para poder automatizar

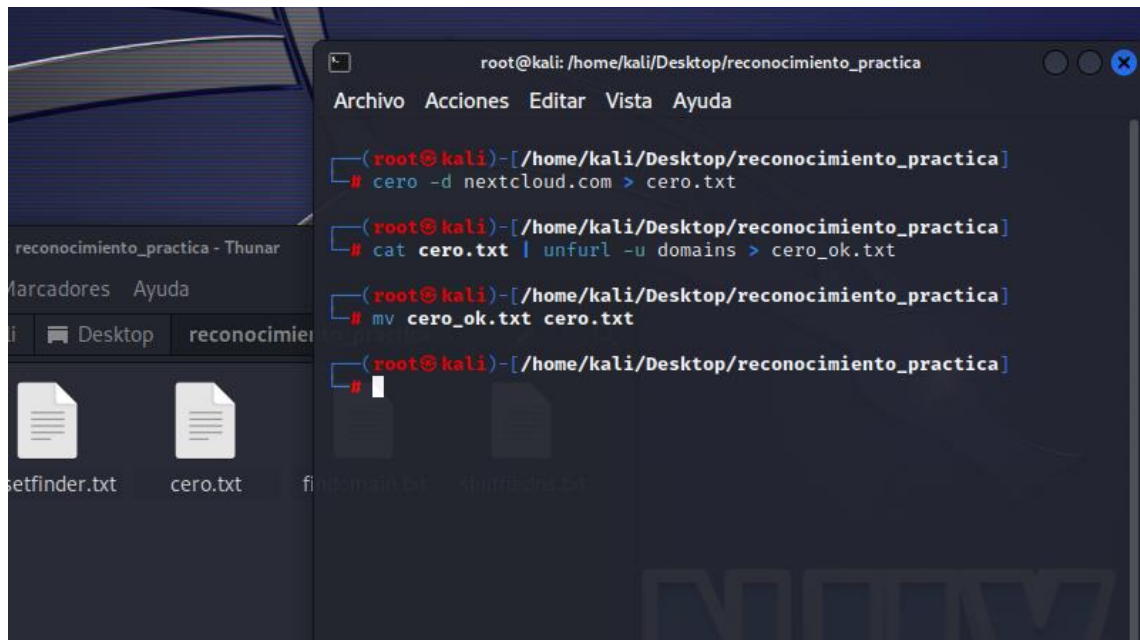


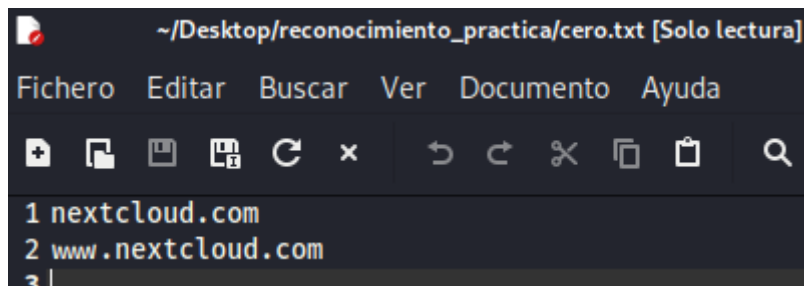
David Fernández Domingo

Con assetfinder obtengo una buena cantidad de subdominios



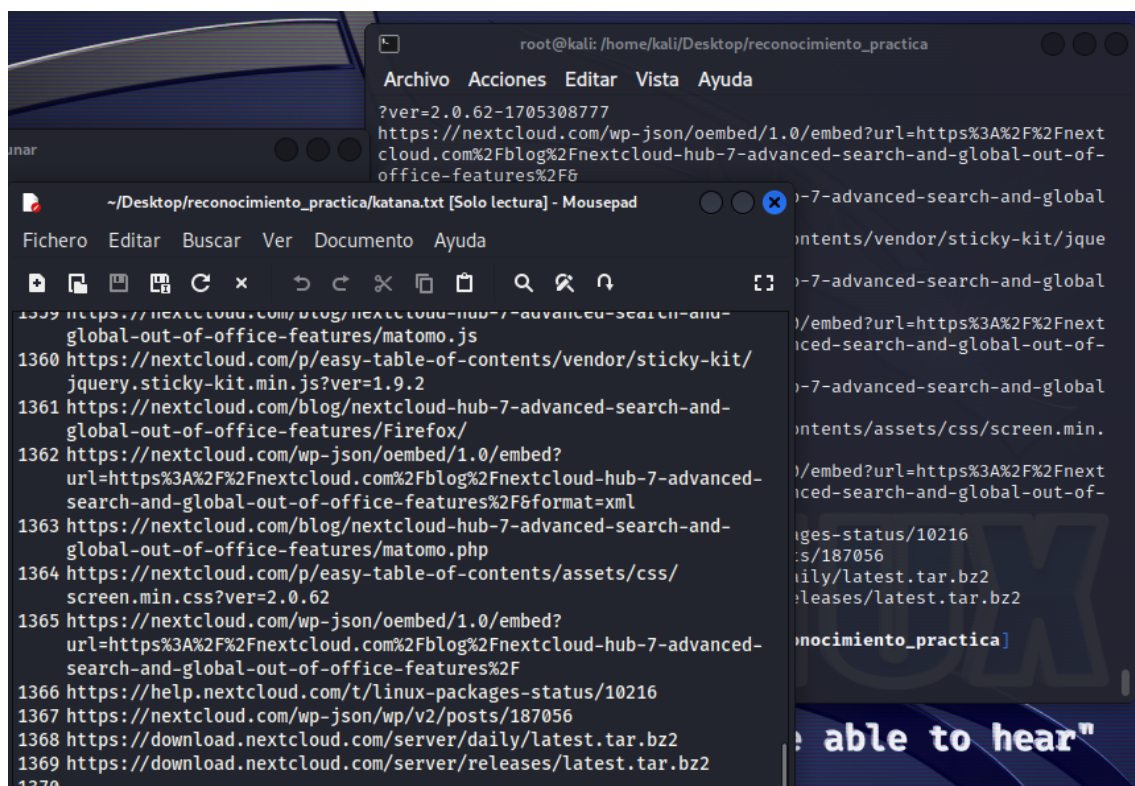
TLS probing con cero (comprobamos los dominios a través de los certificados)

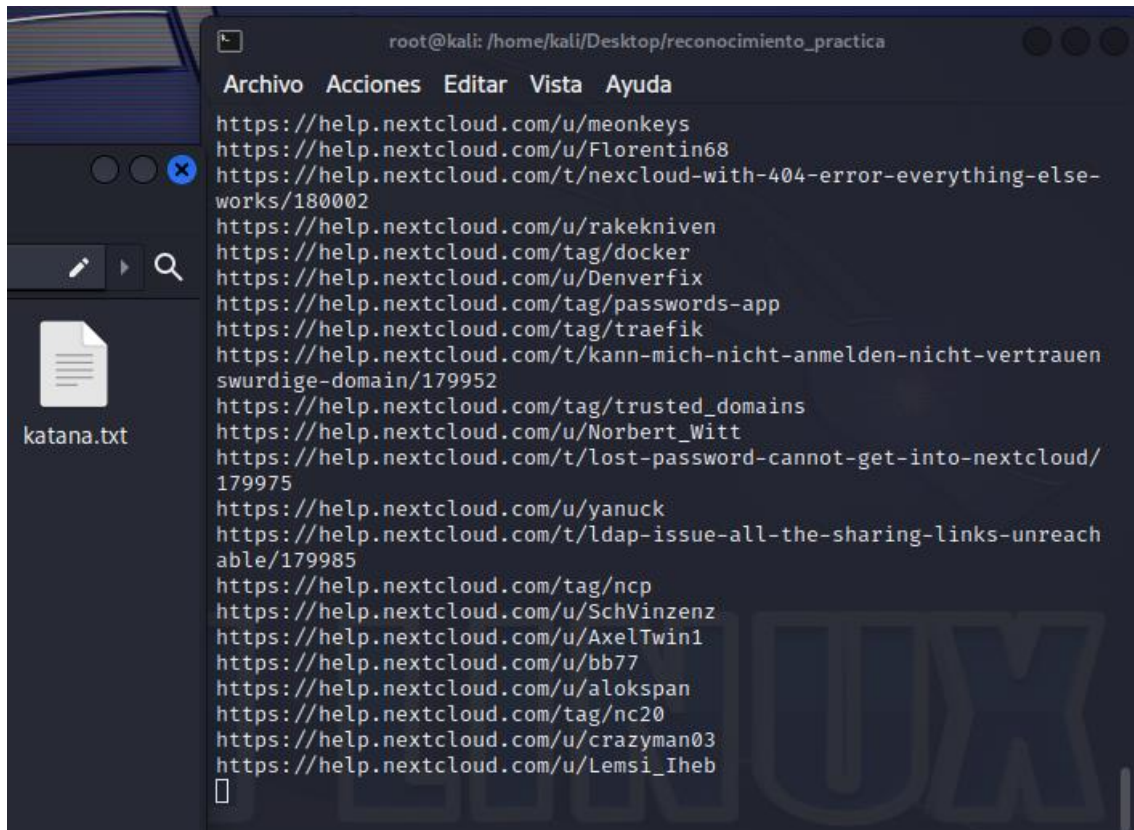




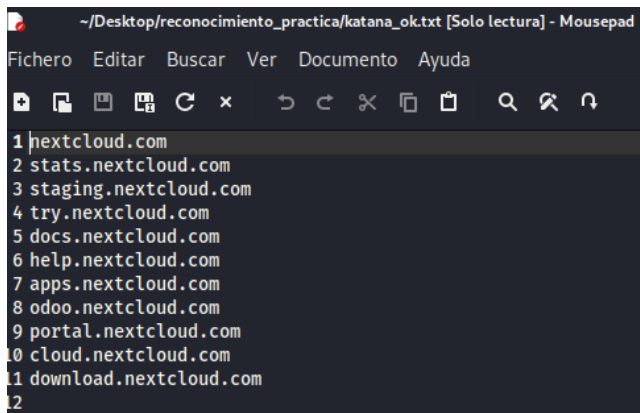
Tan solo obtengo uno, el de nextcloud.com

Con Katana me devuelve un mapa de todas las urls para los subdominios

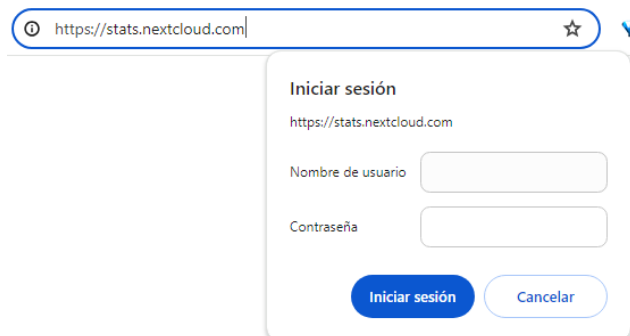




Con unfurl limpiamos y nos quedamos con los subdominios validos



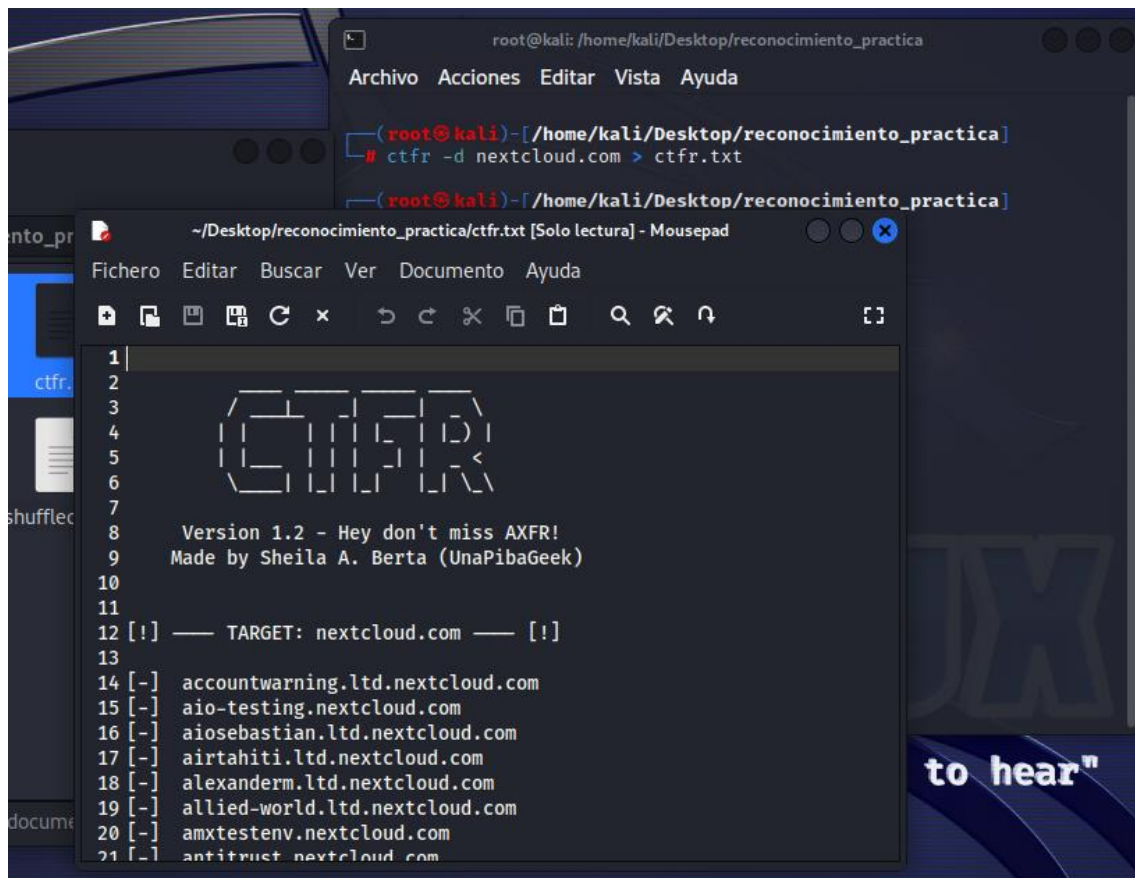
Compruebo algunas de las paginas



David Fernández Domingo

Compruebo que dicha pagina, podría llegar a ser propensa a alguna vulnerabilidad realizando ataque de fuerza bruta u otra vulnerabilidad

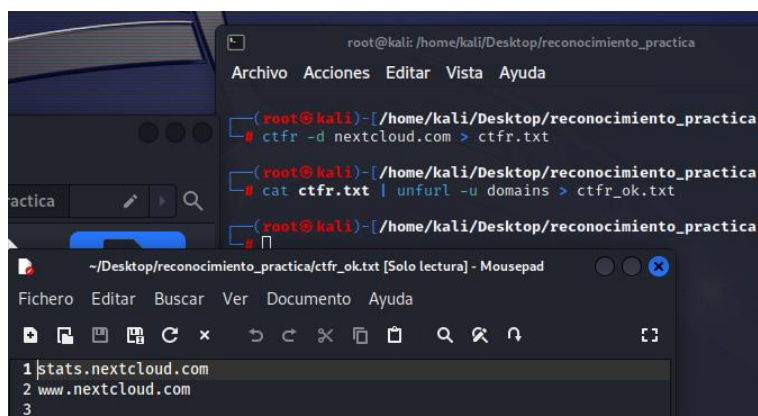
Con CTFR



```
root@kali: /home/kali/Desktop/reconocimiento_practica
Archivo Acciones Editar Vista Ayuda
root@kali)~[/home/kali/Desktop/reconocimiento_practica]
# ctfr -d nextcloud.com > ctfr.txt
root@kali)~[/home/kali/Desktop/reconocimiento_practica]

~/Desktop/reconocimiento_practica/ctfr.txt [Solo lectura] - Mousepad
Fichero Editar Buscar Ver Documento Ayuda
1
2
3
4
5
6
7
8  Version 1.2 - Hey don't miss AXFR!
9  Made by Sheila A. Berta (UnaPibaGeek)
10
11
12 [!] — TARGET: nextcloud.com — [!]
13
14 [-] accountwarning.ltd.nextcloud.com
15 [-] aio-testing.nextcloud.com
16 [-] aiosebastian.ltd.nextcloud.com
17 [-] airtahiti.ltd.nextcloud.com
18 [-] alexanderm.ltd.nextcloud.com
19 [-] allied-world.ltd.nextcloud.com
20 [-] amxtestenv.nextcloud.com
21 [-] antitrust.nextcloud.com
```

Al limpiar con unfurl, nos quedamos con los subdominios

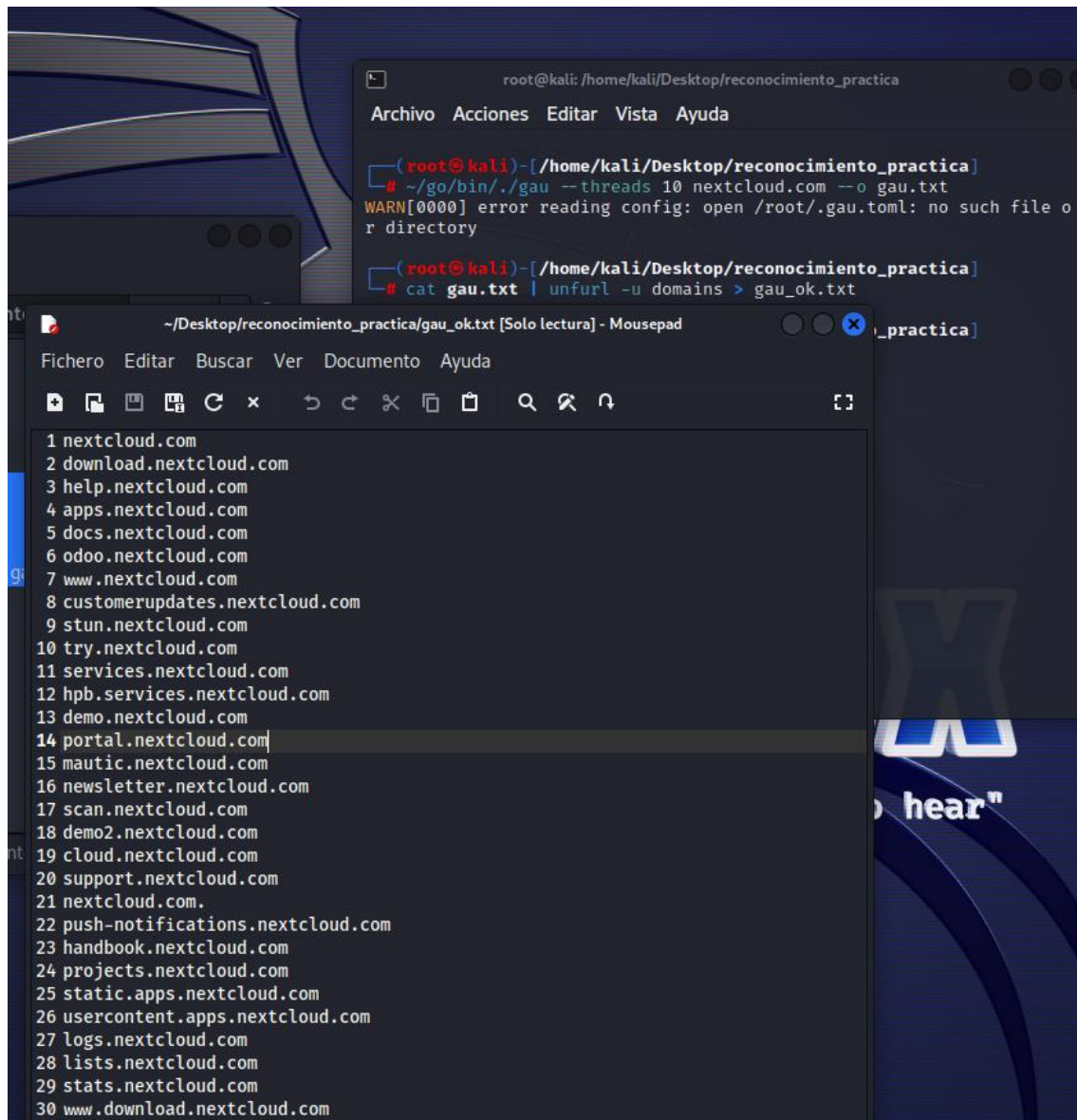


```
root@kali: /home/kali/Desktop/reconocimiento_practica
Archivo Acciones Editar Vista Ayuda
root@kali)~[/home/kali/Desktop/reconocimiento_practica]
# ctfr -d nextcloud.com > ctfr.txt
root@kali)~[/home/kali/Desktop/reconocimiento_practica]
# cat ctfr.txt | unfurl -u domains > ctfr_ok.txt
root@kali)~[/home/kali/Desktop/reconocimiento_practica]

~/Desktop/reconocimiento_practica/ctfr_ok.txt [Solo lectura] - Mousepad
Fichero Editar Buscar Ver Documento Ayuda
1 stats.nextcloud.com
2 www.nextcloud.com
3
```

Exceptuando al subdominio de stats.nextcloud.com, no he encontrado ningún otro subdominio oculto que pueda albergar información sensible o estar expuesta.

Lanzamos GAU (consigue todas las urls pertenecientes al dominio que indiquemos)



The screenshot shows a Kali Linux desktop environment. In the background, a terminal window is open with the following commands and output:

```
root@kali: /home/kali/Desktop/reconocimiento_practica
Archivo Acciones Editar Vista Ayuda

(root@kali)-[/home/kali/Desktop/reconocimiento_practica]
# ~/go/bin/./gau --threads 10 nextcloud.com --o gau.txt
WARN[0000] error reading config: open /root/.gau.toml: no such file or directory

(root@kali)-[/home/kali/Desktop/reconocimiento_practica]
# cat gau.txt | unfurl -u domains > gau_ok.txt
```

In the foreground, a text editor window titled "~/Desktop/reconocimiento_practica/gau_ok.txt [Solo lectura] - Mousepad" is open, displaying a list of 30 subdomains found by GAU:

```
1 nextcloud.com
2 download.nextcloud.com
3 help.nextcloud.com
4 apps.nextcloud.com
5 docs.nextcloud.com
6 odoo.nextcloud.com
7 www.nextcloud.com
8 customerupdates.nextcloud.com
9 stun.nextcloud.com
10 try.nextcloud.com
11 services.nextcloud.com
12 hpb.services.nextcloud.com
13 demo.nextcloud.com
14 portal.nextcloud.com
15 mautic.nextcloud.com
16 newsletter.nextcloud.com
17 scan.nextcloud.com
18 demo2.nextcloud.com
19 cloud.nextcloud.com
20 support.nextcloud.com
21 nextcloud.com.
22 push-notifications.nextcloud.com
23 handbook.nextcloud.com
24 projects.nextcloud.com
25 static.apps.nextcloud.com
26 usercontent.apps.nextcloud.com
27 logs.nextcloud.com
28 lists.nextcloud.com
29 stats.nextcloud.com
30 www.download.nextcloud.com
```

Al limpiar con unfurl vemos que con GAU ha conseguido muchos más subdominios que con otras herramientas

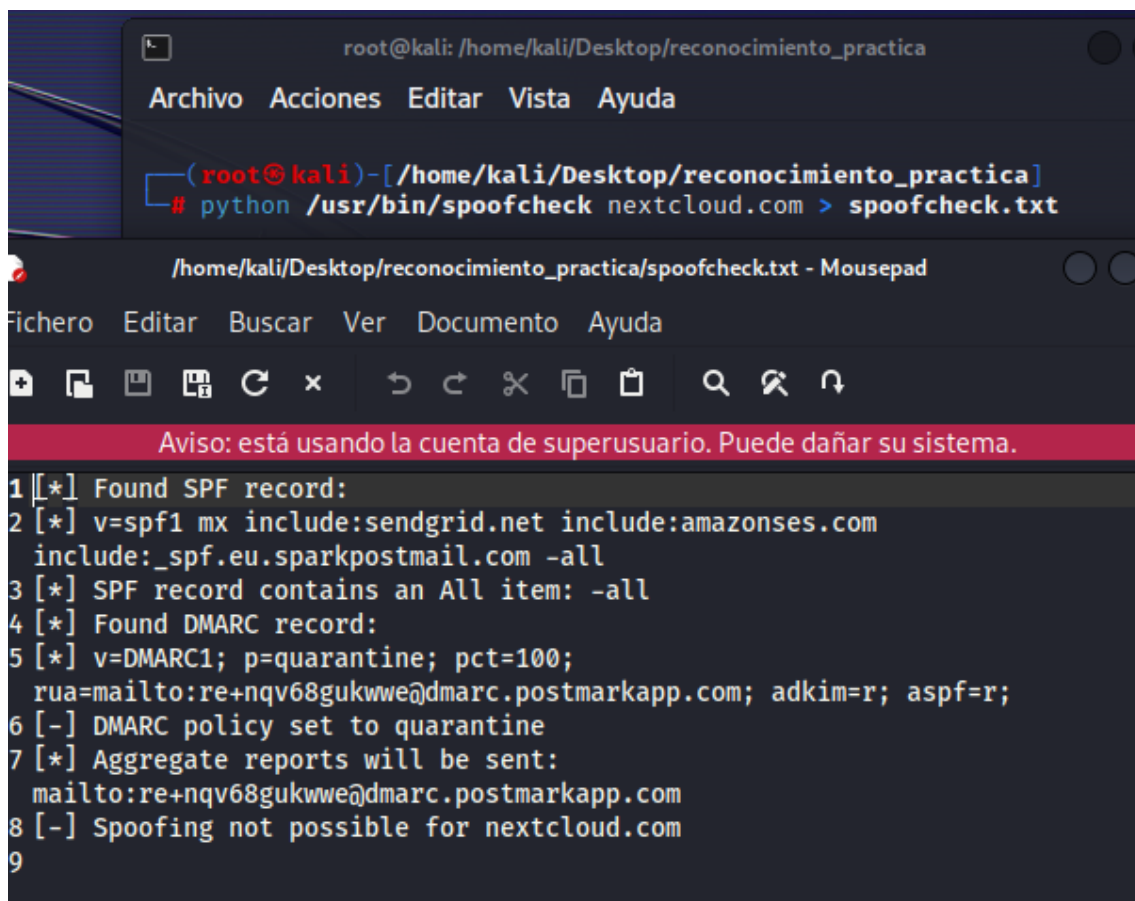
Unimos todos los resultados en subdominios.txt y parseamos todas las mayúsculas a minúsculas para no tener problemas después

```
(root@kali)-[/home/kali/Desktop/reconocimiento_practica]
# cat shuffledns.txt findomain.txt assetfinder.txt cero.txt katana_
ok.txt ctfr_ok.txt gau_ok.txt > subdominios.txt

(root@kali)-[/home/kali/Desktop/reconocimiento_practica]
# cat subdominios.txt | grep -E "$1\$" | tr '[:upper:]' '[:lower:]'
| unfurl --unique domains > subdominios_ok.txt

(root@kali)-[/home/kali/Desktop/reconocimiento_practica]
# mv subdominios_ok.txt subdominios.txt
```

Comprobando si el dominio es spoofeable:



The screenshot shows a terminal window and a text editor. The terminal window is titled 'root@kali: /home/kali/Desktop/reconocimiento_practica' and shows the command `python /usr/bin/spooofcheck nextcloud.com > spooofcheck.txt` being executed. The text editor, titled '/home/kali/Desktop/reconocimiento_practica/spooofcheck.txt - Mousepad', displays the output of the command. The output includes SPF and DMARC record details for nextcloud.com, concluding with 'Spoofing not possible for nextcloud.com'.

```
root@kali: /home/kali/Desktop/reconocimiento_practica
Archivo Acciones Editar Vista Ayuda

(root@kali)-[/home/kali/Desktop/reconocimiento_practica]
# python /usr/bin/spooofcheck nextcloud.com > spooofcheck.txt

/home/kali/Desktop/reconocimiento_practica/spooofcheck.txt - Mousepad
Fichero Editar Buscar Ver Documento Ayuda

Aviso: está usando la cuenta de superusuario. Puede dañar su sistema.

1 [*] Found SPF record:
2 [*] v=spf1 mx include:sendgrid.net include:amazonses.com
   include:_spf.eu.sparkpostmail.com -all
3 [*] SPF record contains an All item: -all
4 [*] Found DMARC record:
5 [*] v=DMARC1; p=quarantine; pct=100;
   rua=mailto:re+nqv68gukwwe@dmARC.postmarkapp.com; adkim=r; aspf=r;
6 [-] DMARC policy set to quarantine
7 [*] Aggregate reports will be sent:
   mailto:re+nqv68gukwwe@dmARC.postmarkapp.com
8 [-] Spoofing not possible for nextcloud.com
9
```

En conclusión, en este caso para el correo de nexcloud no es posible una suplantación

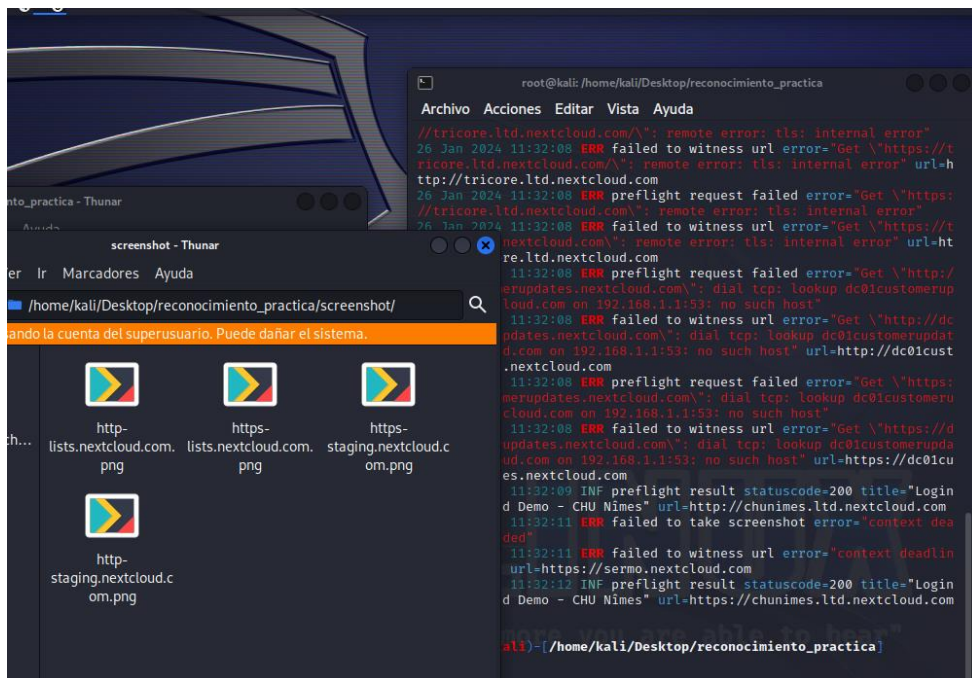
Tecnicas de footprint

Validamos los subdominios

```
root@kali: /home/kali/Desktop/reconocimiento_practica
Archivo Acciones Editar Vista Ayuda
(root@kali)-[/home/kali/Desktop/reconocimiento_practica]
# cat subdominios.txt | httpx -silent -mc 200,401,403 -t 10 -rl 50
-o subdominios_ok.txt
https://antitrust.nextcloud.com
https://apps.nextcloud.com
https://collabora.nextcloud.com
https://collabora.perftesting.nextcloud.com
https://collabora.services.nextcloud.com
https://cool.amxtestenv.nextcloud.com
https://customerupdates.nextcloud.com
https://docs.nextcloud.com
https://download.nextcloud.com
https://drone.nextcloud.com
https://go.nextcloud.com
https://hpb.services.nextcloud.com
https://help.nextcloud.com
https://nextcloud.com
https://nextcloud.com.
https://odoo.nextcloud.com
https://portal.nextcloud.com
https://pushfeed.nextcloud.com
https://s4.nextcloud.com
https://scan.nextcloud.com
https://services.nextcloud.com
https://staging.collabora.nextcloud.com
https://staging.nextcloud.com
https://stats.nextcloud.com
https://surveyserver.nextcloud.com
https://support.nextcloud.com
https://try.nextcloud.com
https://updates.nextcloud.com
https://usercontent.apps.nextcloud.com
http://turn.services.nextcloud.com
(root@kali)-[/home/kali/Desktop/reconocimiento_practica]
```

David Fernández Domingo

Con Gowitness nos ha permitido obtener varios screenshots con sus cabeceras para un análisis rápido de identificar mediante imágenes si damos con alguna pagina de login o con algún acceso visible y poder encontrar alguna vulnerabilidad

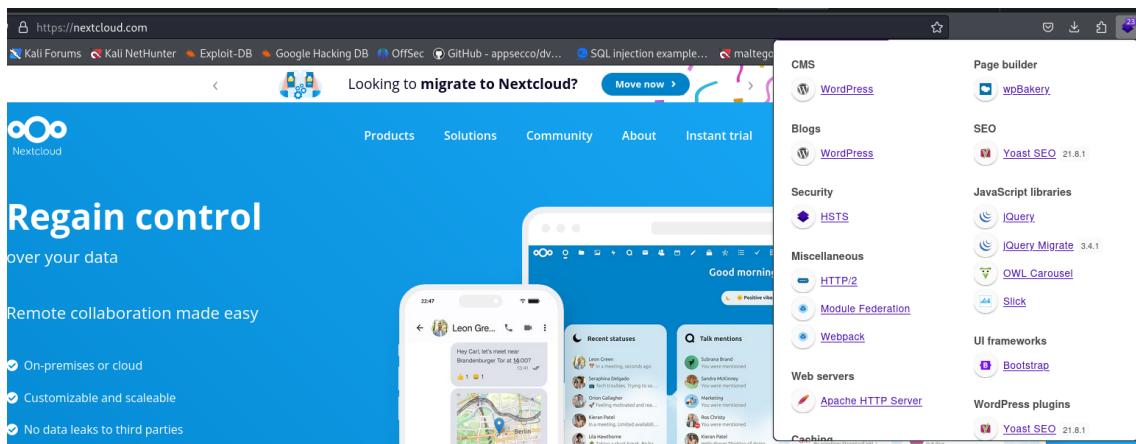


Para masscan y woof, se ha creado un script (masscan_woof.sh) para hacer el escaneo por subdominio. He comentado la línea cuando va a utilizar Nuclei porque se me corta la conexión y cuelga la máquina virtual (tengo que reiniciar Kali.)

Análisis de vulnerabilidades

Se ha usado woof y Testssl para detectar las debilidades o vulnerabilidades a través de los certificados SSL

Usamos wappalyzer para detectar que software utiliza y que versiones



Reviso si tiene alguna versión vulnerable, compruebo un plugin de wordpress

exploit-db.com

Verified

Has App

Filters

Show15

Search:yoast seo

Date

D

A

V

Title

Type

Platform

2015-03-16

WordPress Plugin SEO by Yoast 1.7.3.3 - Blind SQL Injection

WebApps

PHP

Showing 1 to 1 of 1 entries (filtered from 45,811 total entries)

FIRST

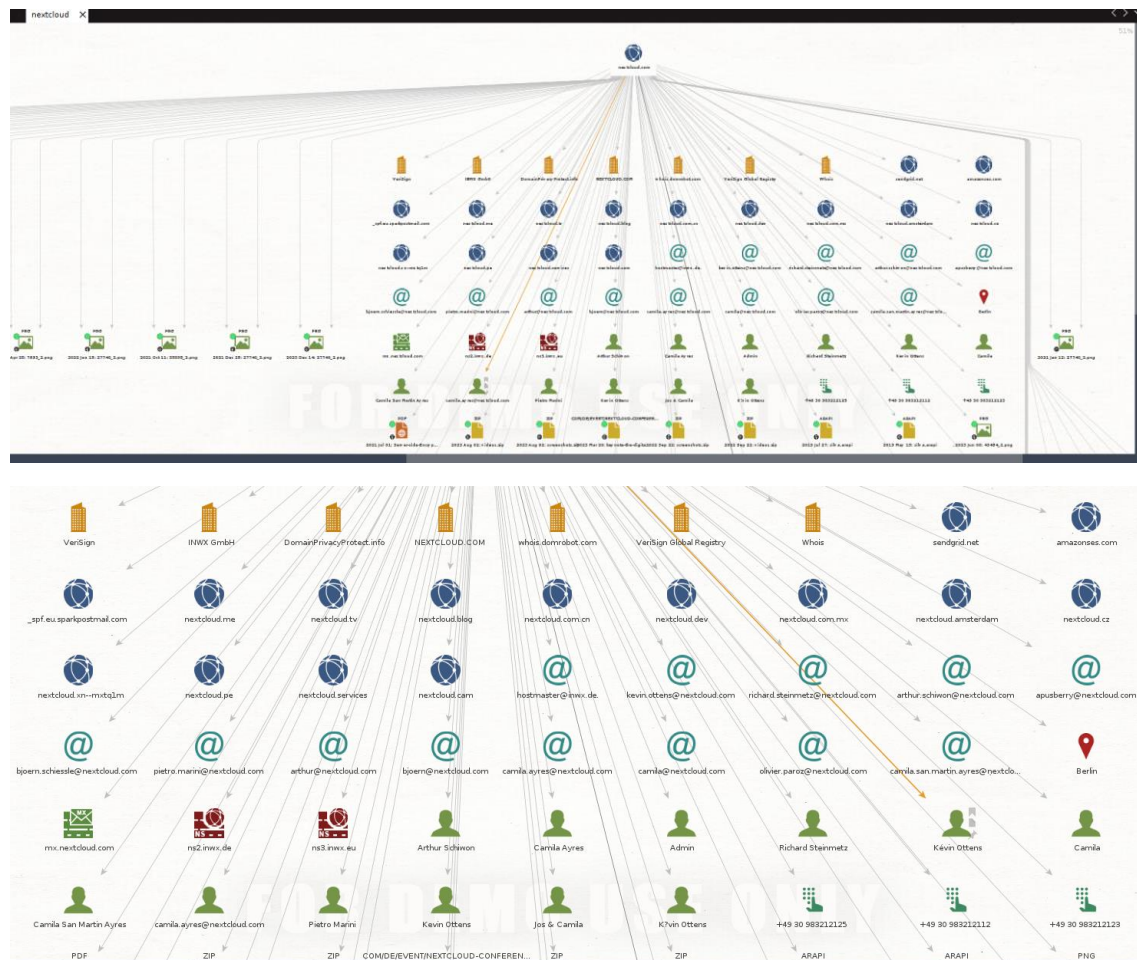
PREVIOUS

1

En exploit-db existe pero una versión anterior a la que tiene, por tanto no nos sirve.

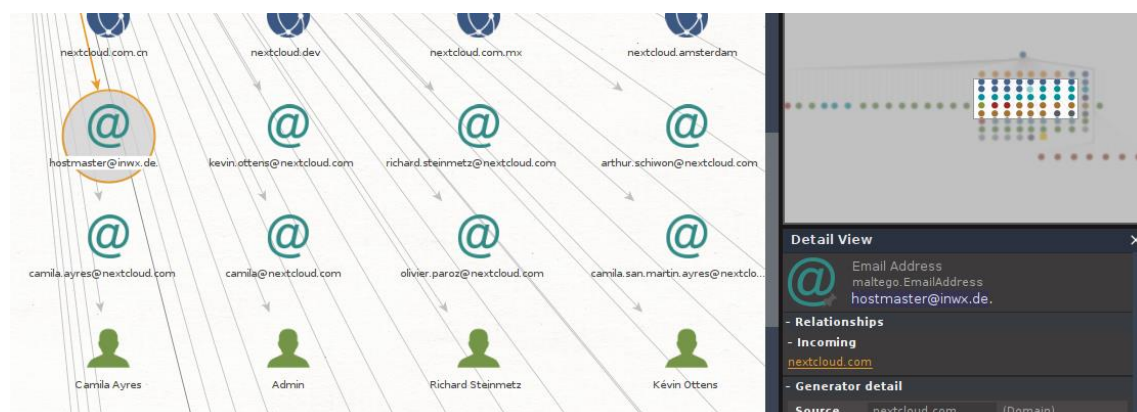
OSSINT

Usamos maltego para obtener directorios, recursos, empleados



Vemos que hay varios usuarios, podemos ver que hay un usuario admin

Encontramos varias cuentas de correo



Me gusta maltego por la cantidad de información que se puede obtener así como datos sensibles, lo que hay que tener en cuenta que la experiencia es más limitada en su versión de comunidad, para que los transformados sean útiles se han de usar las APIs de las aplicaciones por tanto en algunas nos obliga a tener cuenta.

Compruebo uno de los correos, hostmaster@inwx.de en ihavepwned

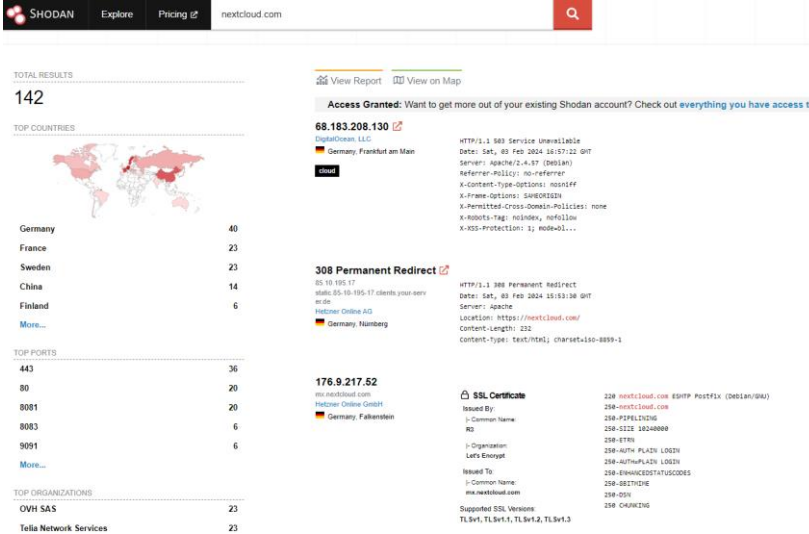
The screenshot shows the 'Have I Been Pwned' website interface. At the top, a large white box contains the text 'have i been pwned?'. Below this, a subtitle reads 'Check if your email address is in a data breach'. A search bar contains the email 'hostmaster@inwx.de' and a button labeled 'pwned?'. Below the search bar, a small link says 'Using Have I Been Pwned is subject to the [terms of use](#)'. Further down, there is a section for 1Password with the text 'Generate secure, unique passwords for every account' and a button 'Learn more at 1Password.com'. Below this is a link 'Why 1Password?'. The bottom section of the screenshot is a dark red banner with the text 'Oh no — pwned!' and 'Pwned in 8 [data breaches](#) and found 6 [pastes](#) (subscribe to search sensitive breaches)'.

The screenshot shows a security breach notification. On the left is a red square icon with white horizontal lines. To the right, the text reads: 'Naz.API: In September 2023, [over 100GB of stealer logs and credential stuffing lists titled "Naz.API" was posted to a popular hacking forum](#). The incident contained a combination of email address and plain text password pairs alongside the service they were entered into, and standalone credential pairs obtained from unnamed sources. In total, the corpus of data included 71M unique email addresses and 100M unique passwords.' Below this, it says 'Compromised data: Email addresses, Passwords'.

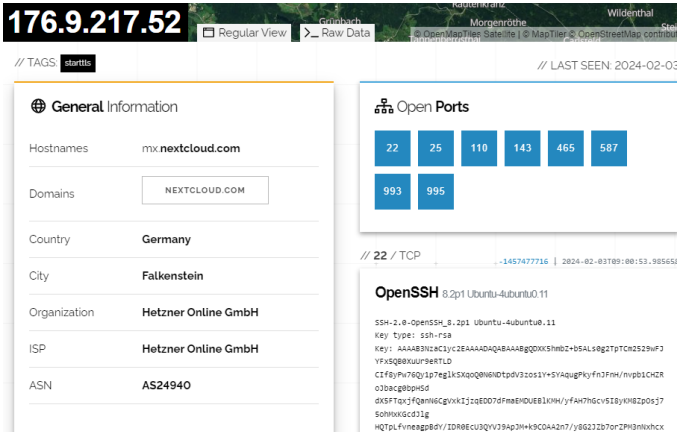
Encuentro que la ultima brecha de seguridad que hubo en la empresa fue en Septiembre de 2023, en un robo de datos de 100gb en los que contienen contraseñas y correos, seguramente todavía haya información que no hayan actualizado y se pueda usar para acceder.

David Fernández Domingo

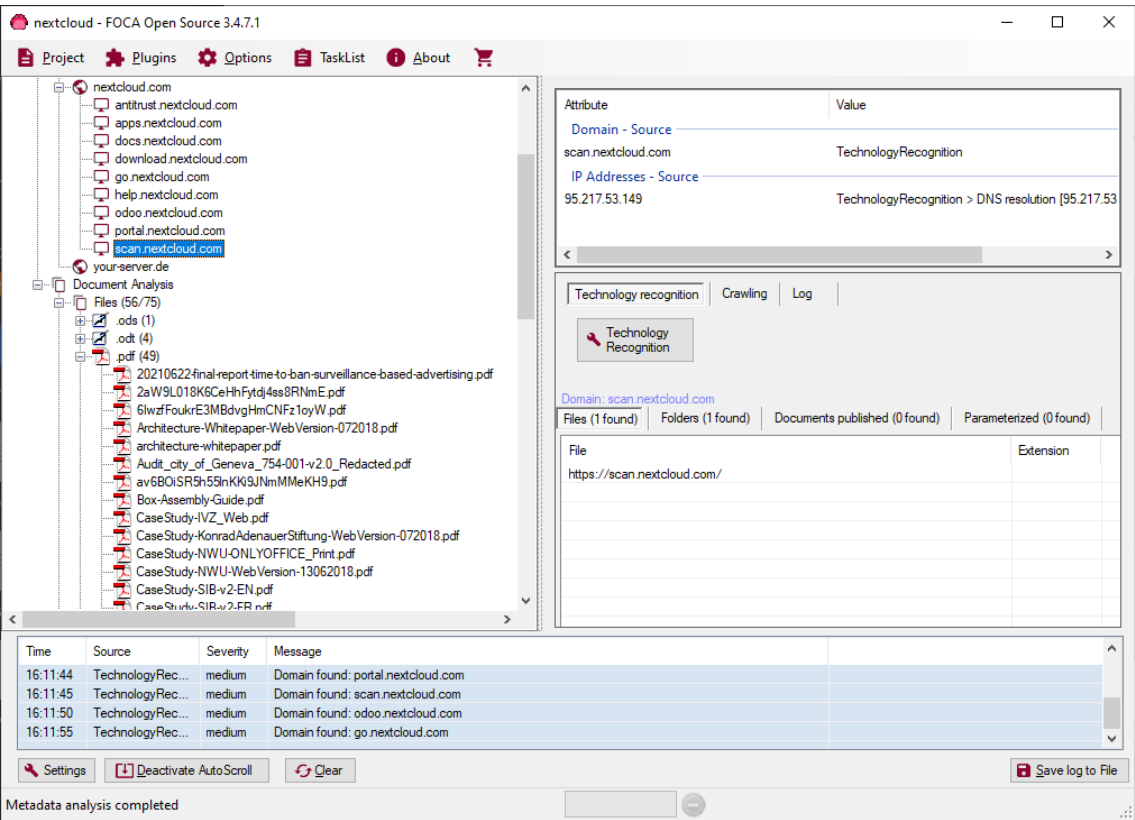
Compruebo con shodan para ver qué resultados da:



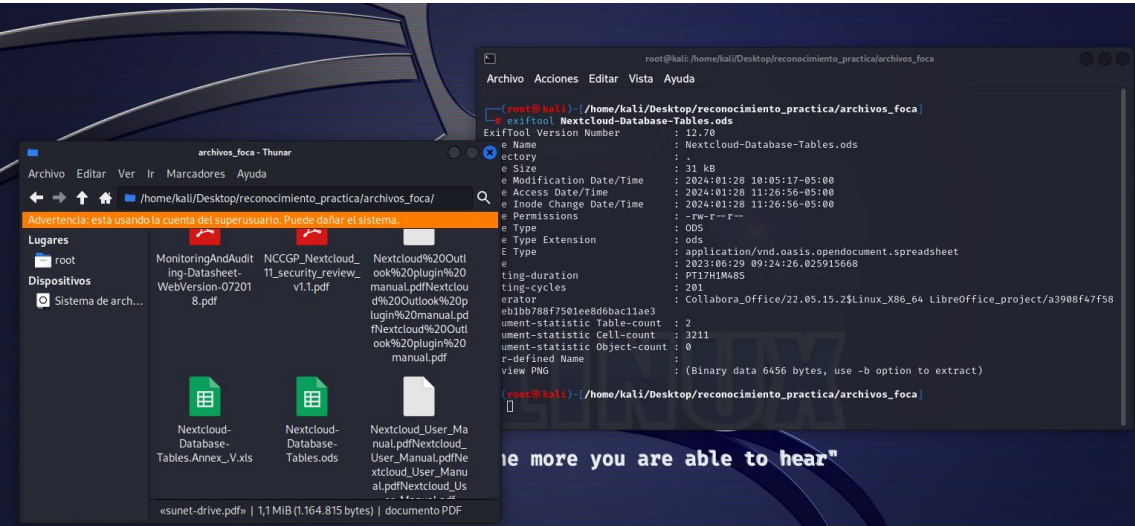
Con shodan me muestra alguna paginas las cuales utilizan nextcloud, la que me interesa es la oficial



Análisis de datos con Foca



Extraigo varia documentación en diferentes formatos, la opción de metadatos no me funciona, así que uso la herramienta Exiftool



David Fernández Domingo

En linkedin veo que es una manera más practica para conseguir contactos y miembros actuales de la empresa



Nextcloud

Servicios y consultoría de TI
Stuttgart, Baden-Württemberg

15 mil seguidores

+ Seguir

Ver página

Personas

1er

2º

3er y demás

En busca de personal



Miembro de LinkedIn

SQA technikus | Minőségbiztosítás | Metrológia | Nextcloud
Tiszalök



Oleg Sidokhmetov • 2º

DevOps Engineer
Valencia

Extracto: ..., Confluence, **NextCloud**. I really like what I do, I like...

Conectar



Carlos Rodríguez • 3er+

Nextcloud - GNU/Linux SysAdmin - Cibersecuri...
Spain

Actual: CEO en Librebit - **Nextcloud** partner, Linux specialist, Software Libre and migration to LibreOffice.

Ofrece servicios: Gestión de la información, Gestión en la nube, Seguridad de la información

Enviar mensaje

David Fernández Domingo

Enlace de github con los ficheros:

https://github.com/k43lthas/main/blob/practica_recopilacion/reconocimiento_practica.zip

El fichero con todo (capturas y archivos de foca) lo adjunto en wetransfer

<https://we.tl/t-S39g3EXIUy>

El zip se llama reconocimiento_practica.zip

Dentro estan archivos de foca en la carpeta archivos_foca y fichero de maltego se llama nextcloud.mtgI