


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

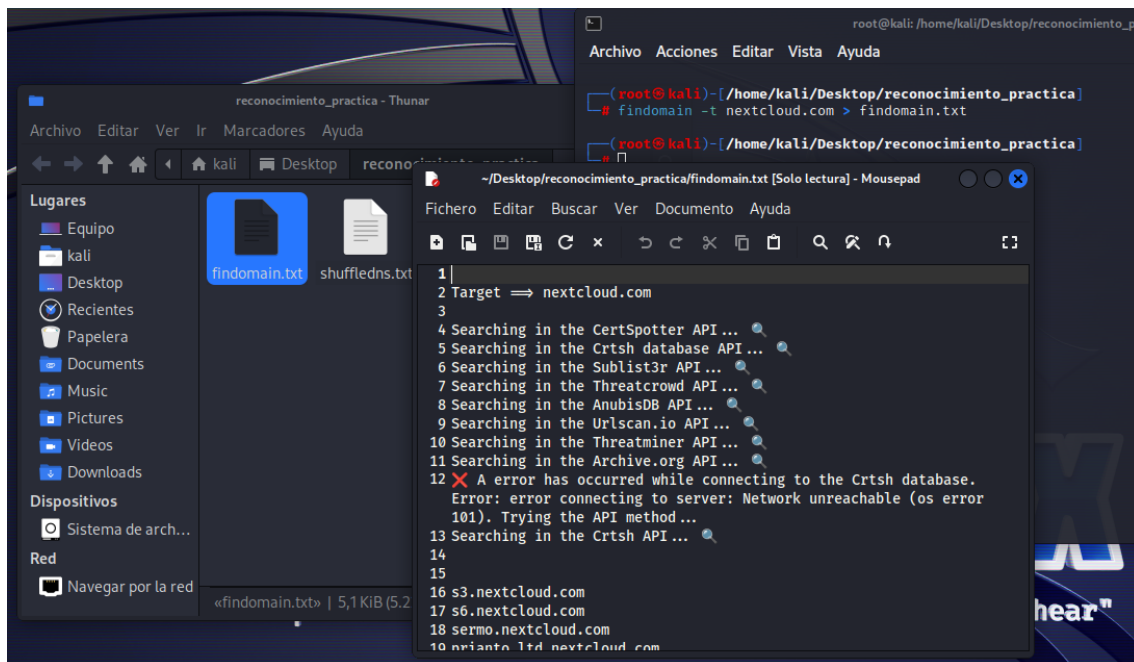
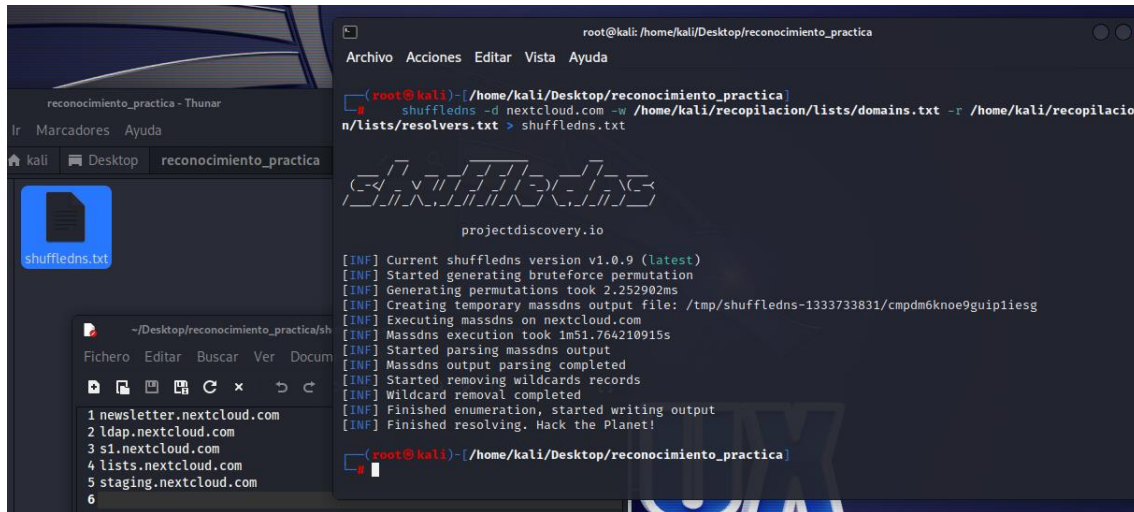
Download CSV

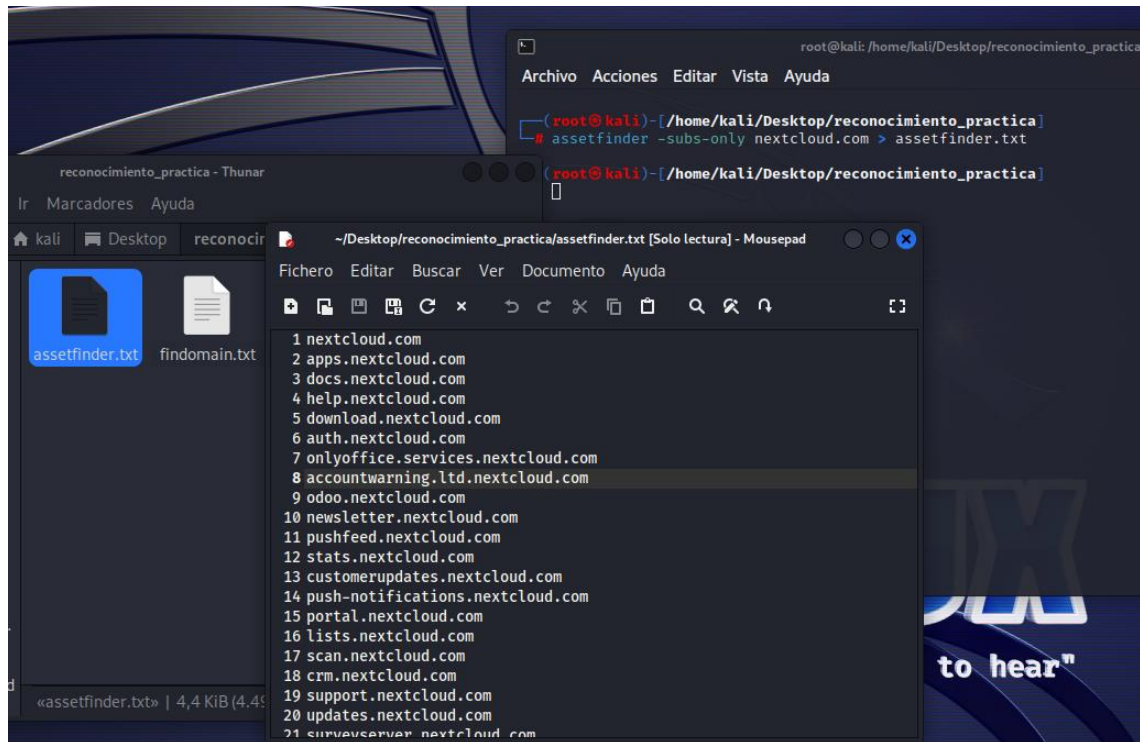
View changes (Last updated on January 15, 2024)

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					

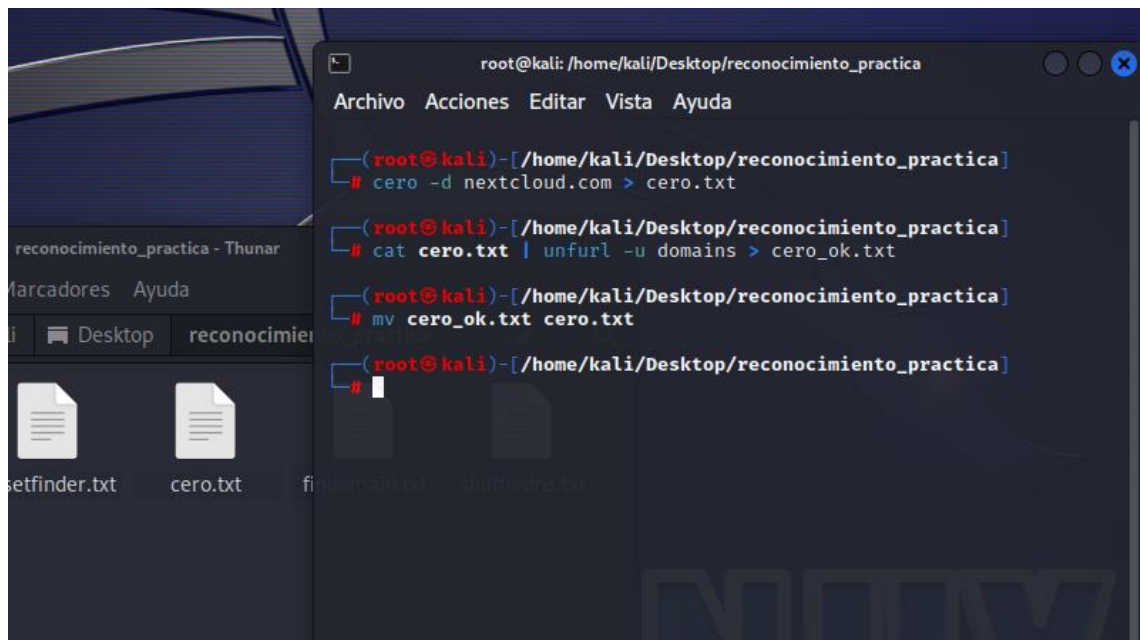
Tecnicas Footprinting

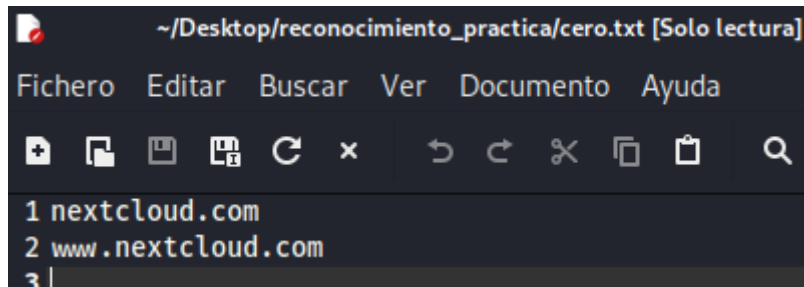




Obtenemos listado de subdominios con shuffledns, findomain y assetfinder

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

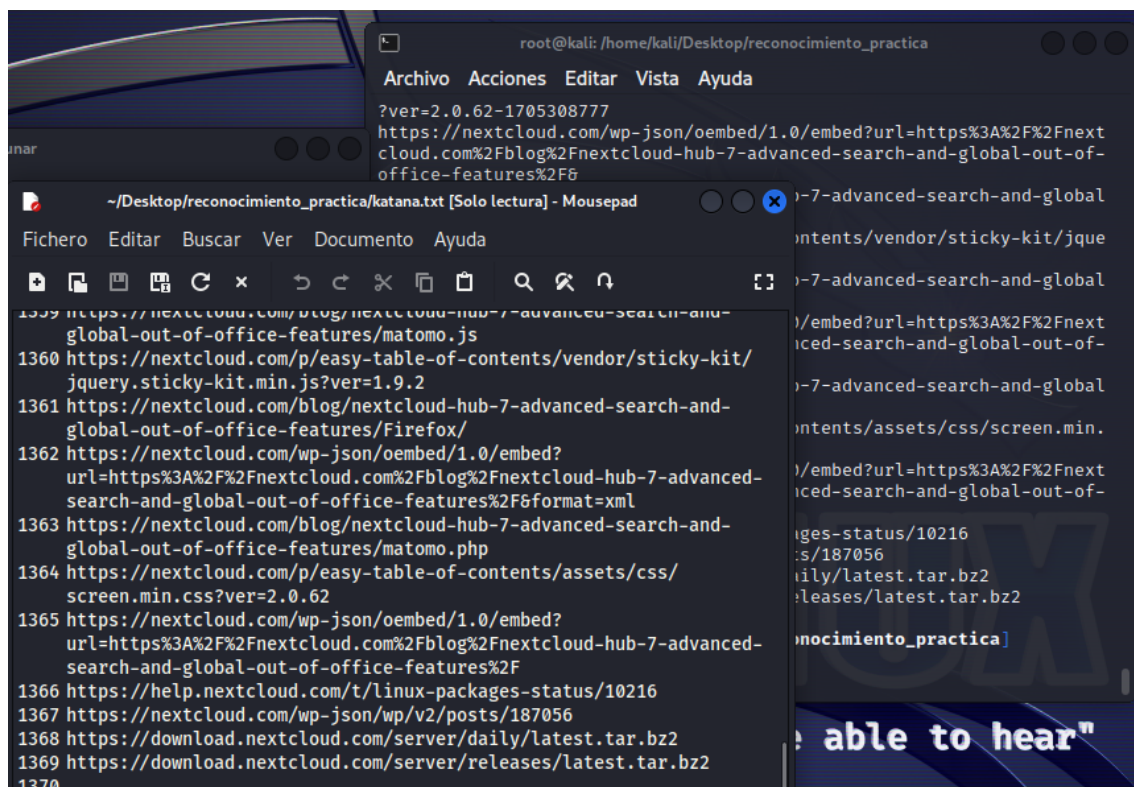




A screenshot of a text editor window titled `~/Desktop/reconocimiento_practica/cero.txt [Solo lectura]`. The menu bar includes `Fichero`, `Editar`, `Buscar`, `Ver`, `Documento`, and `Ayuda`. The toolbar shows icons for file operations. The text content is as follows:

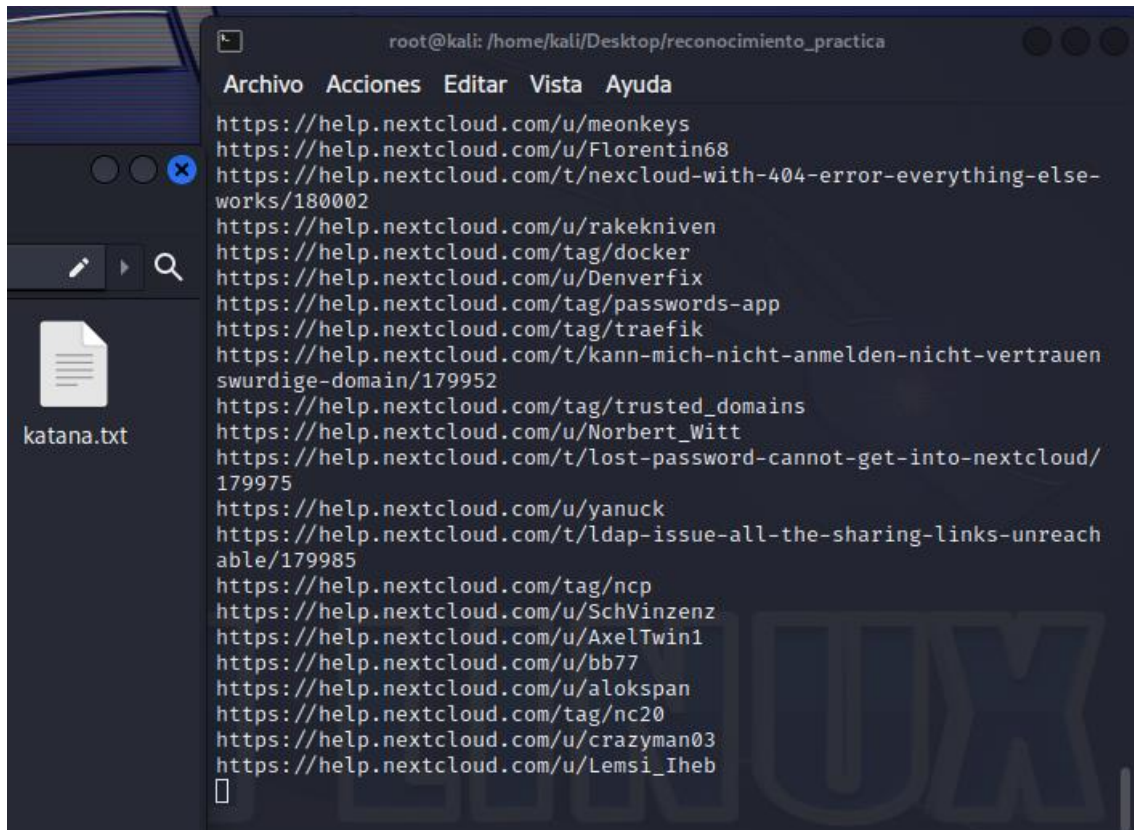
```
1 nextcloud.com
2 www.nextcloud.com
3 |
```

Ejecutamos Katana para conseguir un mapa de todo el dominio

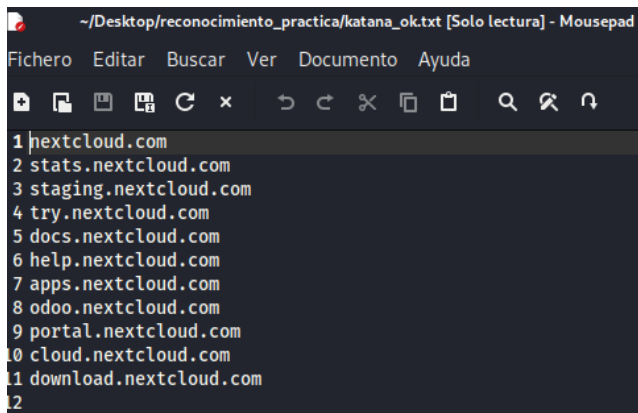


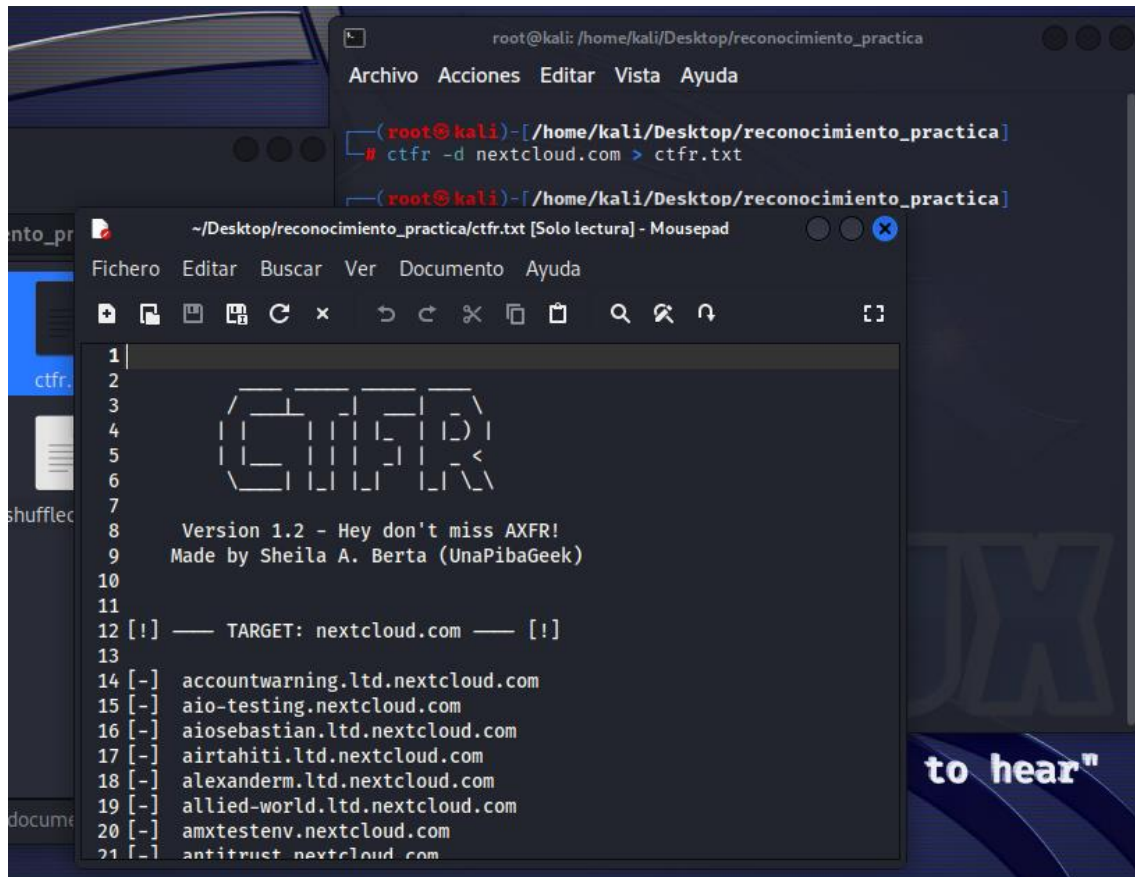
A screenshot of a terminal window titled `root@kali: /home/kali/Desktop/reconocimiento_practica`. The terminal shows the output of a Katana scan. The menu bar includes `Archivo`, `Acciones`, `Editar`, `Vista`, and `Ayuda`. The output is as follows:

```
?ver=2.0.62-1705308777
https://nextcloud.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fnextcloud.com%2Fblog%2Fnextcloud-hub-7-advanced-search-and-global-out-of-office-features%2F&format=xml
1359 https://nextcloud.com/blog/nextcloud-hub-7-advanced-search-and-global-out-of-office-features/matomo.js
1360 https://nextcloud.com/p/easy-table-of-contents/vendor/sticky-kit/jquery.sticky-kit.min.js?ver=1.9.2
1361 https://nextcloud.com/blog/nextcloud-hub-7-advanced-search-and-global-out-of-office-features/Firefox/
1362 https://nextcloud.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fnextcloud.com%2Fblog%2Fnextcloud-hub-7-advanced-search-and-global-out-of-office-features%2F&format=xml
1363 https://nextcloud.com/blog/nextcloud-hub-7-advanced-search-and-global-out-of-office-features/matomo.php
1364 https://nextcloud.com/p/easy-table-of-contents/assets/css/screen.min.css?ver=2.0.62
1365 https://nextcloud.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fnextcloud.com%2Fblog%2Fnextcloud-hub-7-advanced-search-and-global-out-of-office-features%2F
1366 https://help.nextcloud.com/t/linux-packages-status/10216
1367 https://nextcloud.com/wp-json/wp/v2/posts/187056
1368 https://download.nextcloud.com/server/daily/latest.tar.bz2
1369 https://download.nextcloud.com/server/releases/latest.tar.bz2
1370
```



Con unfurl limpiamos y nos quedamos con los subdominios





The screenshot shows a Kali Linux terminal window with the command `ctfr -d nextcloud.com > ctfr.txt` executed. A text editor window (Mousepad) is open, displaying the contents of `ctfr.txt`. The file contains a ASCII art logo for 'CTFR', version information, and a list of subdomains for nextcloud.com.

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

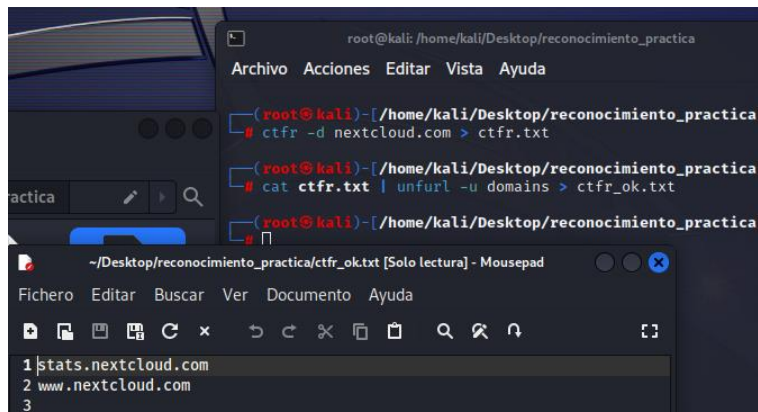
(root@kali)-[/home/kali/Desktop/reconocimiento_practica]
# ctfr -d nextcloud.com > ctfr.txt

(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
```

Con unfurl limpiamos y nos quedamos con los subdominios



The screenshot shows a Kali Linux terminal window with the command `cat ctfr.txt | unfurl -u domains > ctfr_ok.txt` executed. A text editor window (Mousepad) is open, displaying the contents of `ctfr_ok.txt`, which contains a cleaned list of subdomains.

```
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

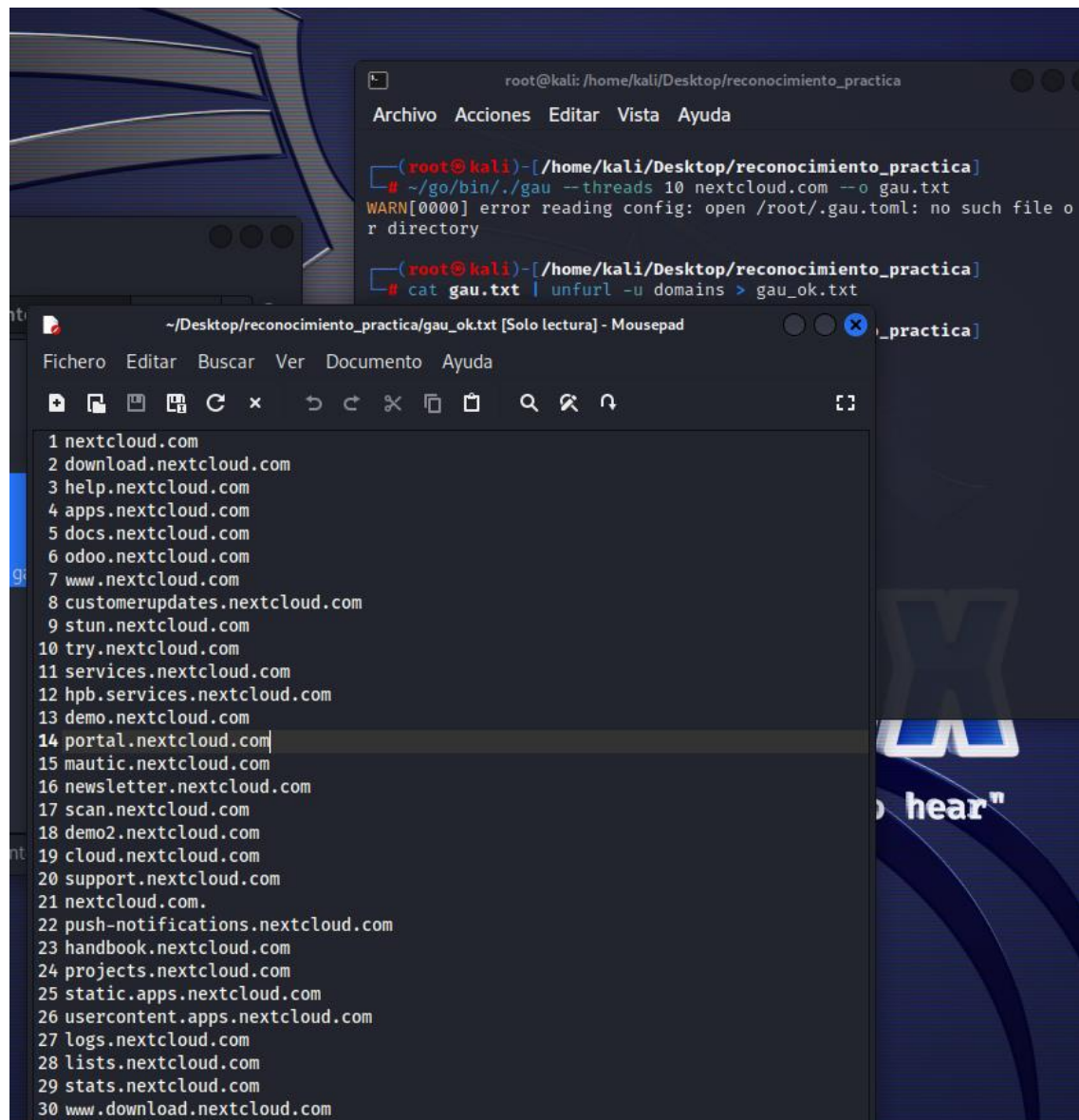
(root@kali)-[/home/kali/Desktop/reconocimiento_practica]
# cat ctfr.txt | unfurl -u domains > ctfr_ok.txt

(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
```

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
```

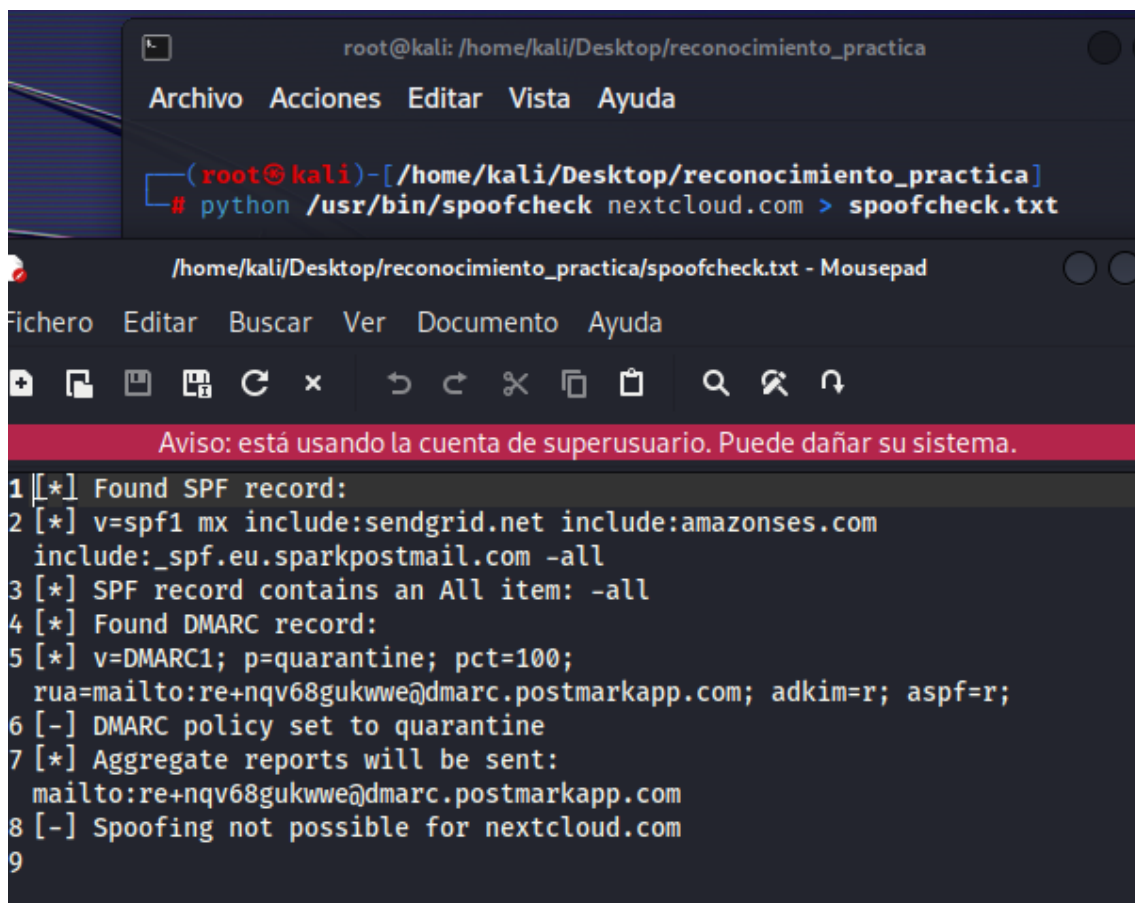
Al limpiar con unfurl vemos que con GAU ha conseguidos muchos más subdominios que con otras herramientas

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

```
(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
```



The screenshot shows a Kali Linux terminal window and a text editor (Mousepad) displaying the output of the `spooofcheck` tool. The terminal window title is `root@kali: /home/kali/Desktop/reconocimiento_practica` and the command executed is `python /usr/bin/spooofcheck nextcloud.com > spooofcheck.txt`. The text editor window title is `/home/kali/Desktop/reconocimiento_practica/spooofcheck.txt - Mousepad`. The output of the tool is as follows:

```
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
```


Tecnicas de footprint

Validamos los subdominios

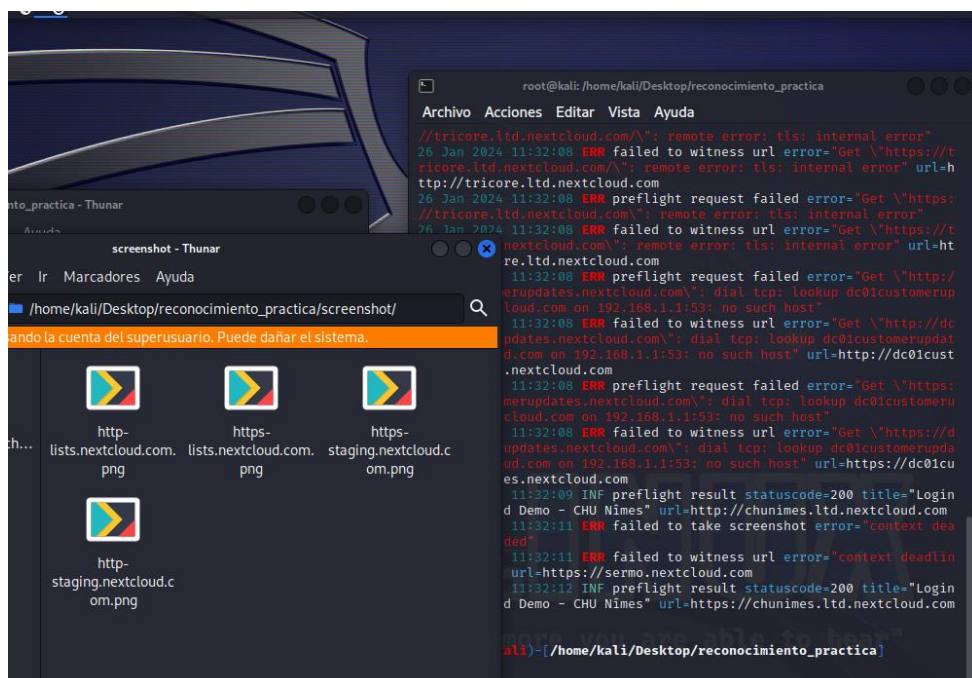
```
root@kali: /home/kali/Desktop/reconocimiento_practica

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]
```

Gowitness para sacar screenshot de las paginas



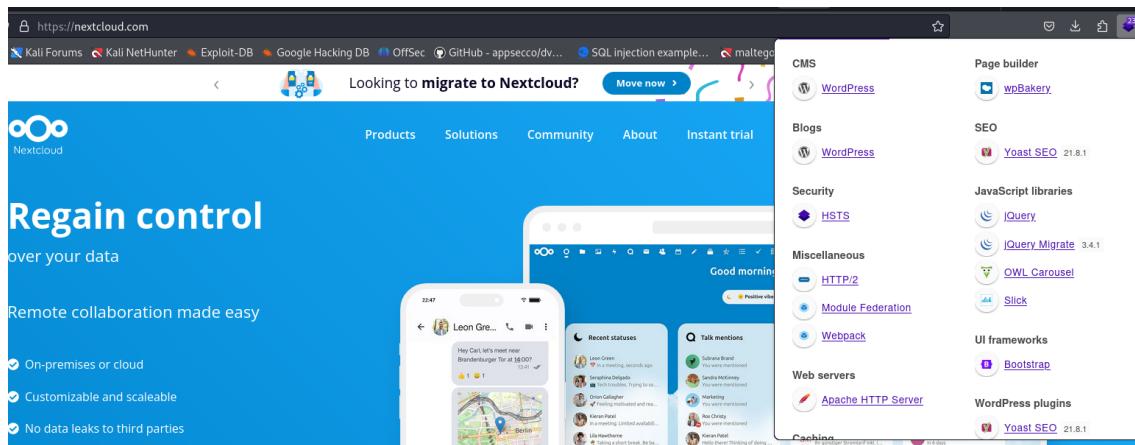
David Fernández Domingo

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 bloquea la conexión y tengo que reiniciar Kali.

Análisis de vulnerabilidades

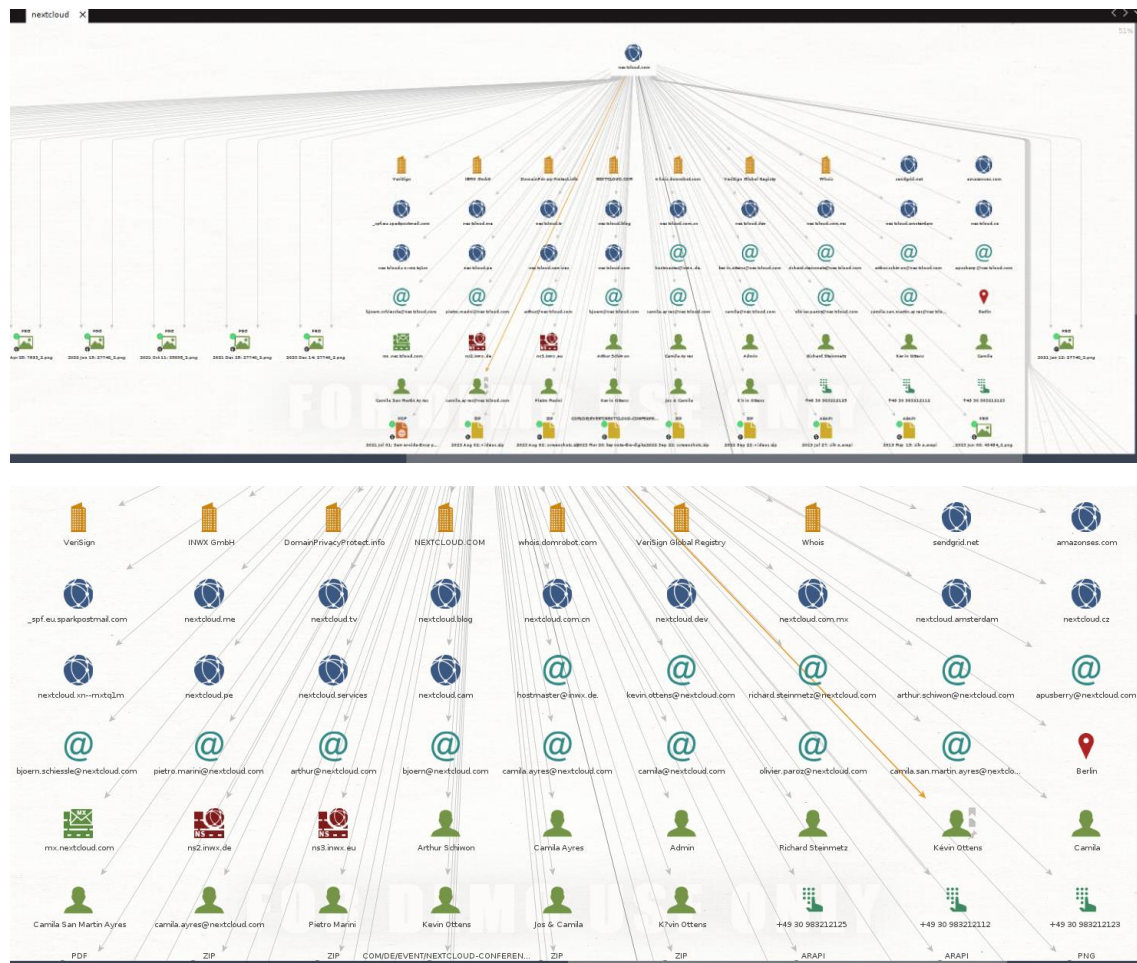
Se ha usado woof y Testssl para detectar las debilidades o vulnerabilidades a través de los certificados SSL

Usamos wappalyzer para detectar que software utiliza y que versiones



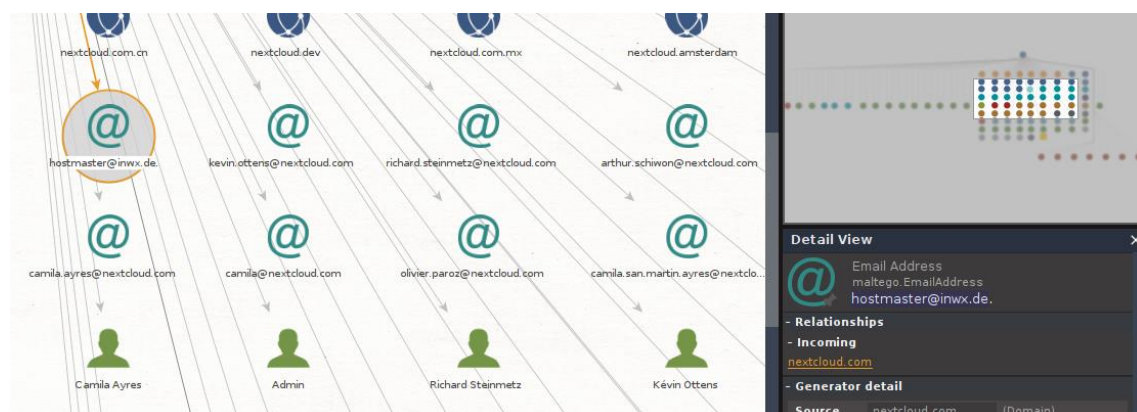
OSSINT

Usamos maltego para obtener directorios, recursos, empleados



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

Encontramos varias cuentas de correo




Comprobamos una de ellas con ihavepwned

';--have i been pwned?

Check if your email address is in a data breach

pwned?

Using Have I Been Pwned is subject to [the terms of use](#)

 Generate secure, unique passwords for every account [Learn more at 1Password.com](#)

[Why 1Password?](#)

Oh no — pwned!

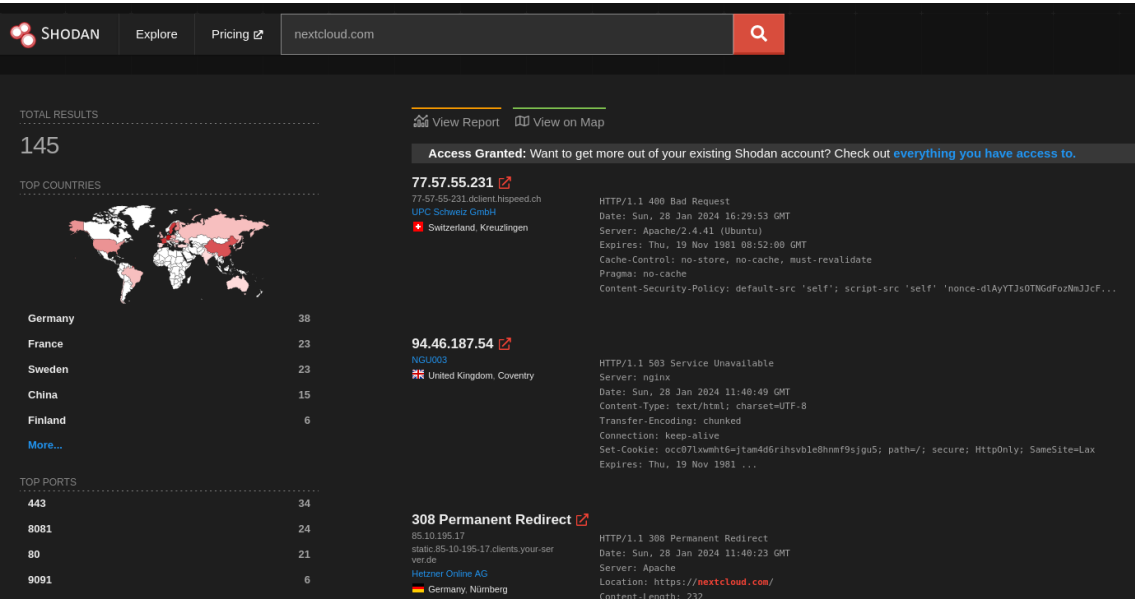
Pwned in [8 data breaches](#) and found [6 pastes](#) ([subscribe](#) to search sensitive breaches)



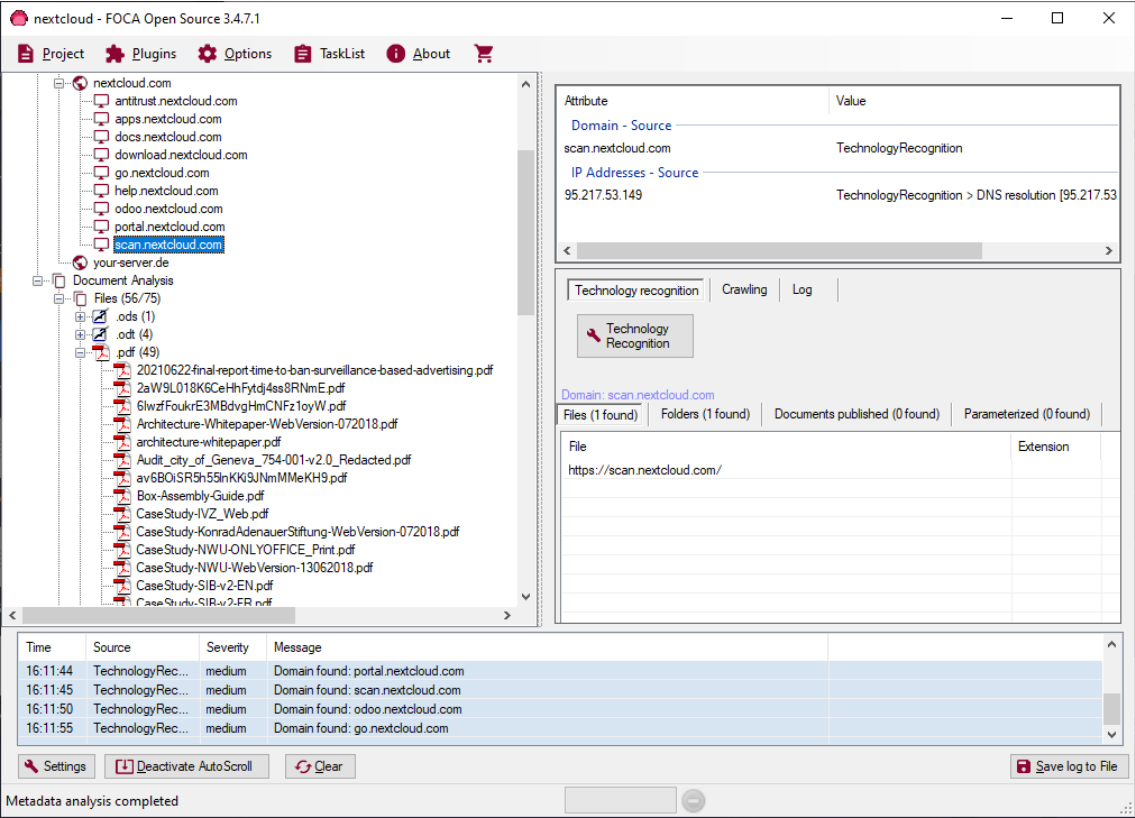
Naz.API: In September 2023, over 100GB of stealer logs and credential stuffing lists titled "Naz.API" was posted to a popular hacking forum. The incident contained a combination of email address and plain text password pairs alongside the service they were entered into, and standalone credential pairs obtained from unnamed sources. In total, the corpus of data included 71M unique email addresses and 100M unique passwords.

Compromised data: Email addresses, Passwords

Comprobamos con shodan para ver que resultados nos da:

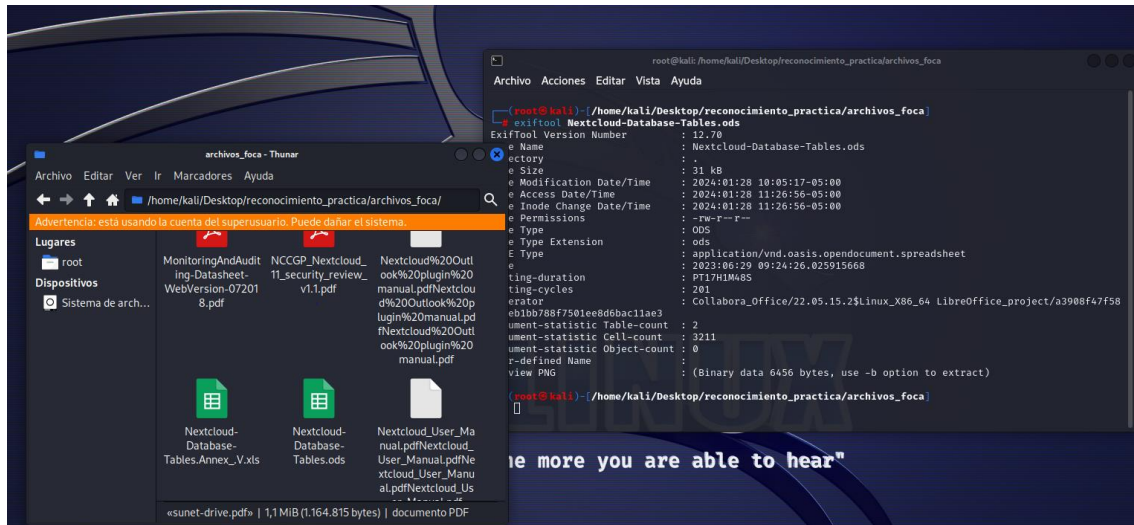


Foca



David Fernández Domingo

Herramienta Exiftool



Dado que github no deja adjuntar ficheros mayores a 25MB, utilizo wetransfers, aquí dejo el enlace:

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

El zip se llama reconocimiento_practica.zip

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