

Preguntas

What does the 3-letter acronym FTP stand for?

file transfer protocol

Which port does the FTP service listen on usually?

21

What acronym is used for the secure version of FTP?

sftp

What is the command we can use to send an ICMP echo request to test our connection to the target?

ping

From our scans, what version is FTP running on the target?

vsftpd 3.0.3

From your scans, what OS type is running on the target?

unix

What is the command we need to run in order to display the 'ftp' client help menu?

ftp -h

What is username that is used over FTP when you want to log in without having an account?

anonymous

Proceso

Realizar nmap

Sudo nmap -sS -sV -p- -Pn -vvv -O 10.129.32.252

```
> sudo nmap -sS -sV -p- -Pn -vvv -O 10.129.32.252
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-19
NSE: Loaded 45 scripts for scanning.
Initiating Parallel DNS resolution of 1 host. at 00:24
Completed Parallel DNS resolution of 1 host. at 00:24
Host is up, received user-set (0.12s latency).
Scanned at 2022-06-19 00:24:41 CEST for 583s
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE REASON          VERSION
21/tcp    open  ftp      syn-ack ttl 63 vsftpd 3.0.3
No exact OS matches for host (If you know what OS is
https://nmap.org/submit/ ).
```

Entrar en el servidor ftp como anónimo con el comando
ftp 10.129.32.252

```
> ftp 10.129.32.252
Connected to 10.129.32.252.
220 (vsFTPd 3.0.3)
Name (10.129.32.252:zom): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> |
```

Listar el contenido del servidor con el comando ls

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0          0          32 Jun 04  2021 flag.txt
226 Directory send OK.
ftp> |
```

Descargar el archivo flag.txt al equipo con el comando `get flag.txt`

```
ftp> get flag.txt
local: flag.txt remote: flag.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for flag.txt (32 bytes).
226 Transfer complete.
32 bytes received in 0.00 secs (13.8766 kB/s)
ftp> |
```

Leer el archivo desde el directorio personal que es donde se encuentra

```
> ls
Desktop    flag.txt  powerlevel10k  TheZombrex.ovpn
Documents  Music     Public         Videos
Downloads  Pictures  Templates      videos_obs
> cat flag.txt
035db21c881520061c53e0536e44f8159%
```