LinkedIn: Kelvin Kimotho

Fawn machine tier 0 HackTheBox

Question: What does the 3-letter acronym FTP stand for?

Answer: file transfer protocol

Question: Which port does the FTP service listen on usually?

Answer: 21

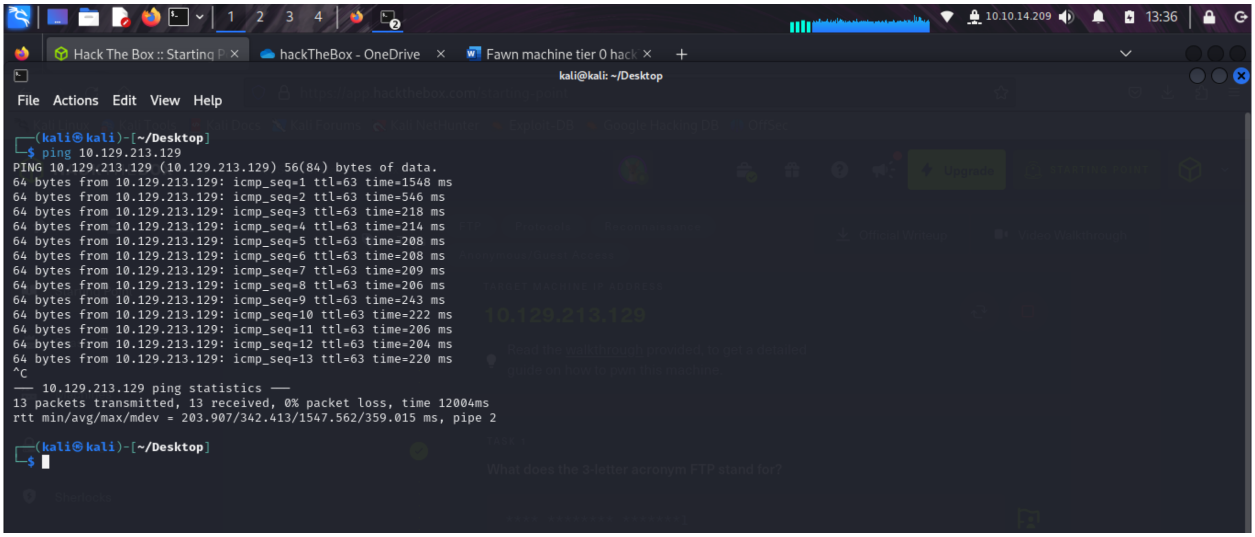
Question: FTP sends data in the clear, without any encryption. What acronym is used for a later protocol designed to provide similar functionality to FTP but securely, as an extension of the SSH protocol?

Answer: SFTP

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

Answer: ping

I ran ping <TargetIp> Command.

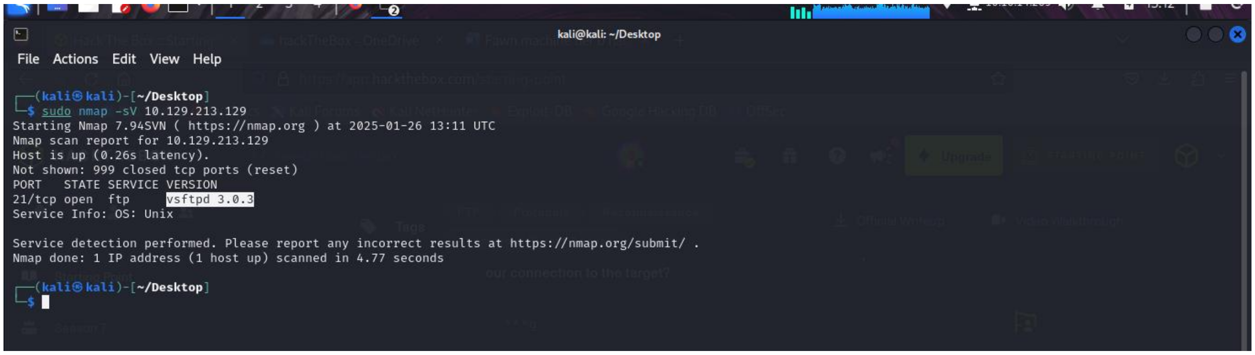


```
┌──(kali㉿kali)-[~/Desktop]
└─$ ping 10.129.213.129
PING 10.129.213.129 (10.129.213.129) 56(84) bytes of data.
64 bytes from 10.129.213.129: icmp_seq=1 ttl=63 time=1548 ms
64 bytes from 10.129.213.129: icmp_seq=2 ttl=63 time=546 ms
64 bytes from 10.129.213.129: icmp_seq=3 ttl=63 time=218 ms
64 bytes from 10.129.213.129: icmp_seq=4 ttl=63 time=214 ms
64 bytes from 10.129.213.129: icmp_seq=5 ttl=63 time=208 ms
64 bytes from 10.129.213.129: icmp_seq=6 ttl=63 time=208 ms
64 bytes from 10.129.213.129: icmp_seq=7 ttl=63 time=209 ms
64 bytes from 10.129.213.129: icmp_seq=8 ttl=63 time=206 ms
64 bytes from 10.129.213.129: icmp_seq=9 ttl=63 time=243 ms
64 bytes from 10.129.213.129: icmp_seq=10 ttl=63 time=222 ms
64 bytes from 10.129.213.129: icmp_seq=11 ttl=63 time=206 ms
64 bytes from 10.129.213.129: icmp_seq=12 ttl=63 time=204 ms
64 bytes from 10.129.213.129: icmp_seq=13 ttl=63 time=220 ms
^C
—— 10.129.213.129 ping statistics ——
13 packets transmitted, 13 received, 0% packet loss, time 12004ms
rtt min/avg/max/mdev = 203.907/342.413/1547.562/359.015 ms, pipe 2

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

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

Answer: vsftpd 3.0.3

After running the sudo nmap –sV <targetIp> command, I was able to retrieve information about the version of services running in the server as well as the version of the operating system running the ftp server.

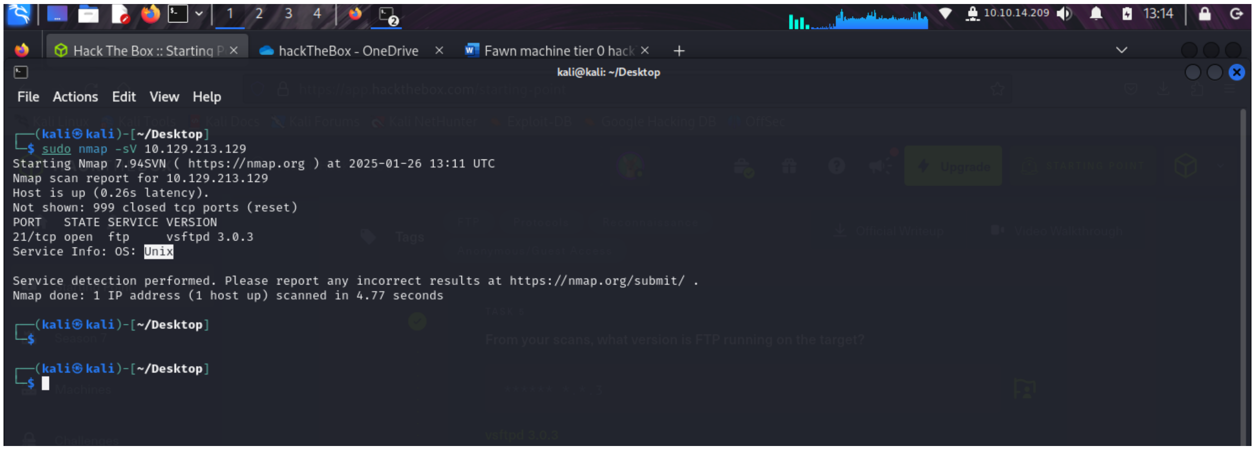


```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sV 10.129.213.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-26 13:11 UTC
Nmap scan report for 10.129.213.129
Host is up (0.26s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
Service 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 4.77 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

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

Answer: Unix

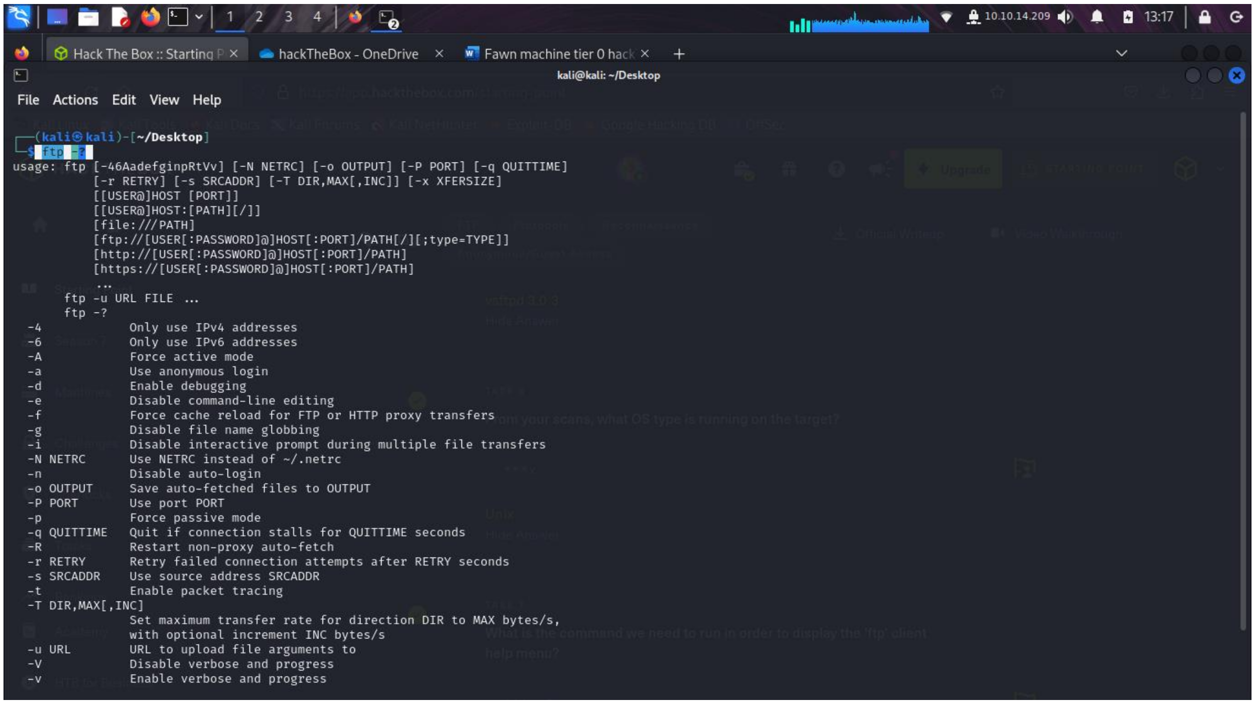
After running the sudo nmap –sV <targetIp> command, I was able to retrieve information about the version of services running in the server as well as the version of the operating system running the ftp server.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sV 10.129.213.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-26 13:11 UTC
Nmap scan report for 10.129.213.129
Host is up (0.26s latency).
Not shown: 999 closed tcp ports (reset)
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 4.77 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

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

Answer: ftp -?

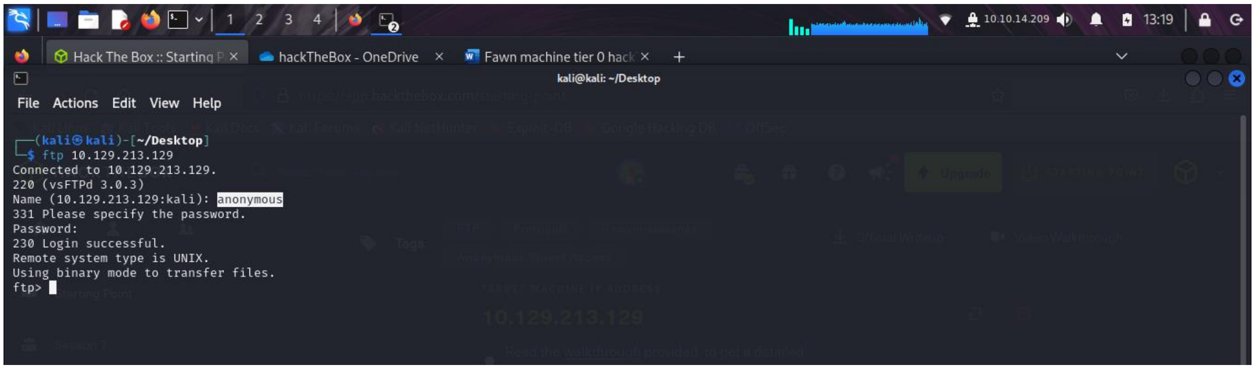


```
┌──(kali㉿kali)-[~/Desktop]
└─$ ftp -?
usage: ftp [-46AadefginpRtVv] [-N NETRC] [-o OUTPUT] [-P PORT] [-q QUITTIME]
           [-r RETRY] [-s SRCADDR] [-T DIR,MAX[,INC]] [-x XFERSIZE]
           [[USER@]HOST [PORT]]
           [[USER@]HOST:[PATH][/]]
           [file:///PATH]
           [ftp://[USER[:PASSWORD]@]HOST[:PORT]/PATH[/][;type=TYPE]]
           [http://[USER[:PASSWORD]@]HOST[:PORT]/PATH]
           [https://[USER[:PASSWORD]@]HOST[:PORT]/PATH]
           ...
       ftp -u URL FILE ...
       ftp -?
  -4            Only use IPv4 addresses
  -6            Only use IPv6 addresses
  -A            Force active mode
  -a            Use anonymous login
  -d            Enable debugging
  -e            Disable command-line editing
  -f            Force cache reload for FTP or HTTP proxy transfers
  -g            Disable file name globbing
  -i            Disable interactive prompt during multiple file transfers
  -N NETRC      Use NETRC instead of ~/.netrc
  -n            Disable auto-login
  -o OUTPUT     Save auto-fetched files to OUTPUT
  -P PORT       Use port PORT
  -p            Force passive mode
  -q QUITTIME   Quit if connection stalls for QUITTIME seconds
  -R            Restart non-proxy auto-fetch
  -r RETRY      Retry failed connection attempts after RETRY seconds
  -s SRCADDR    Use source address SRCADDR
  -t            Enable packet tracing
  -T DIR,MAX[,INC]
                Set maximum transfer rate for direction DIR to MAX bytes/s,
                with optional increment INC bytes/s
  -u URL        URL to upload file arguments to
  -V            Disable verbose and progress
  -v            Enable verbose and progress
```

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

Answer: anonymous

I used anonymous as the username to gain access to the ftp server since i had no account.

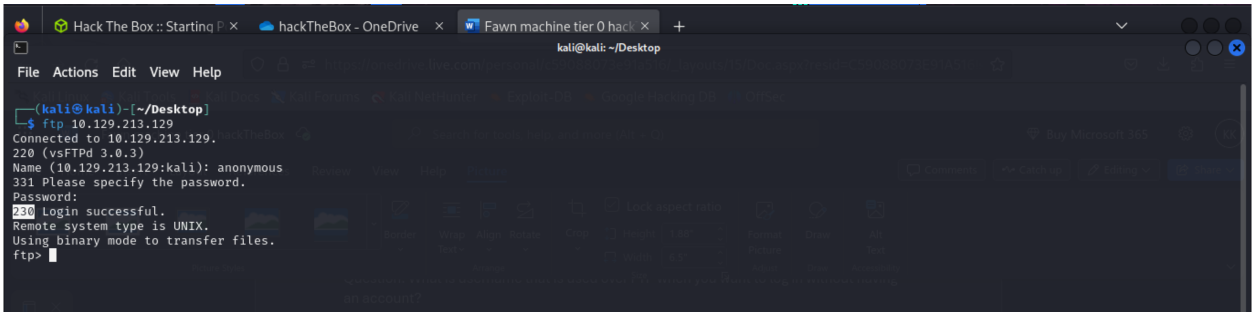


```
┌──(kali㉿kali)-[~/Desktop]
└─$ ftp 10.129.213.129
Connected to 10.129.213.129.
220 (vsFTPd 3.0.3)
Name (10.129.213.129:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

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

Answer: 230

After a successful login with username anonymous with no password, a login success message was returned together with the code 230.

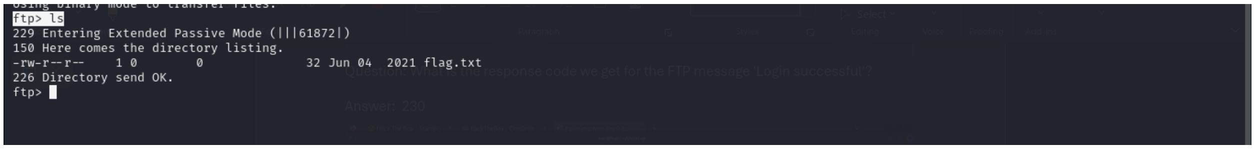


```
┌──(kali㉿kali)-[~/Desktop]
└─$ ftp 10.129.213.129
Connected to 10.129.213.129.
220 (vsFTPd 3.0.3)
Name (10.129.213.129:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

Question: 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.

Answer: ls

I used the ls command to list all the files within the ftp server directory.

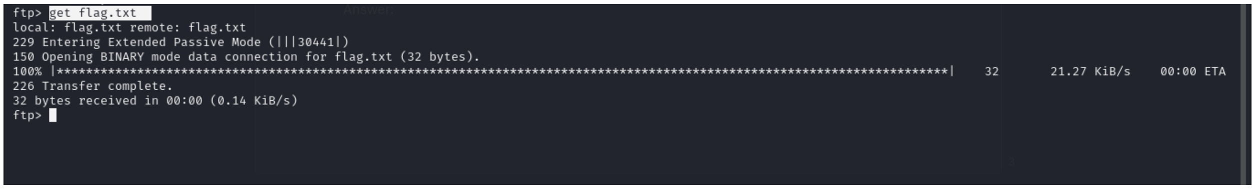


```
ftp> ls
229 Entering Extended Passive Mode (|||61872|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0              32 Jun 04  2021 flag.txt
226 Directory send OK.
ftp> 
```

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

Answer: get

I use the get command to download the flag.txt file from the ftp server to my attack machine for further analysis.

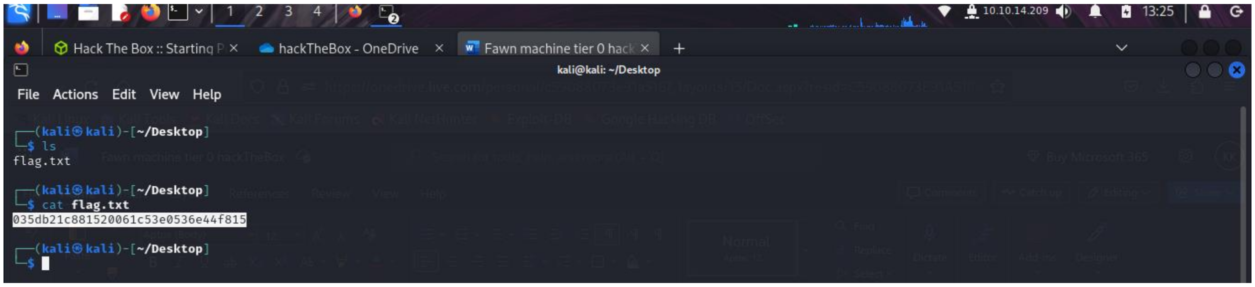


```
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||30441|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100% |************************************************************************************************************************|    32       21.27 KiB/s    00:00 ETA
226 Transfer complete.
32 bytes received in 00:00 (0.14 KiB/s)
ftp> 
```

Question: Submit Flag

Answer: 035db21c881520061c53e0536e44f815

After the downloading from the ftp server using get command, I used cat command to view the content of the file. And that's how I retrieved the root flag.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls
flag.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ cat flag.txt
035db21c881520061c53e0536e44f815

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```