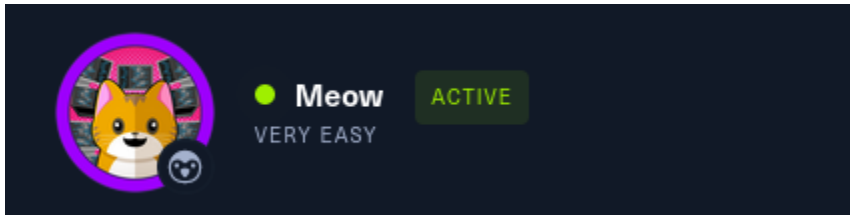


LinkedIn: [Kelvin Kimotho](#)



Questions

Task 1

What does the acronym VM stand for?

Answer: Virtual machine

Task 2

What tool do we use to interact with the operating system in order to issue commands via the command line, such as the one to start our VPN connection? It's also known as a console or shell.

Answer: Terminal

Task 3

What service do we use to form our VPN connection into HTB labs?

Answer: openvpn

Task 4

What tool do we use to test our connection to the target with an ICMP echo request?

Answer: ping

Task 5

What is the name of the most common tool for finding open ports on a target?

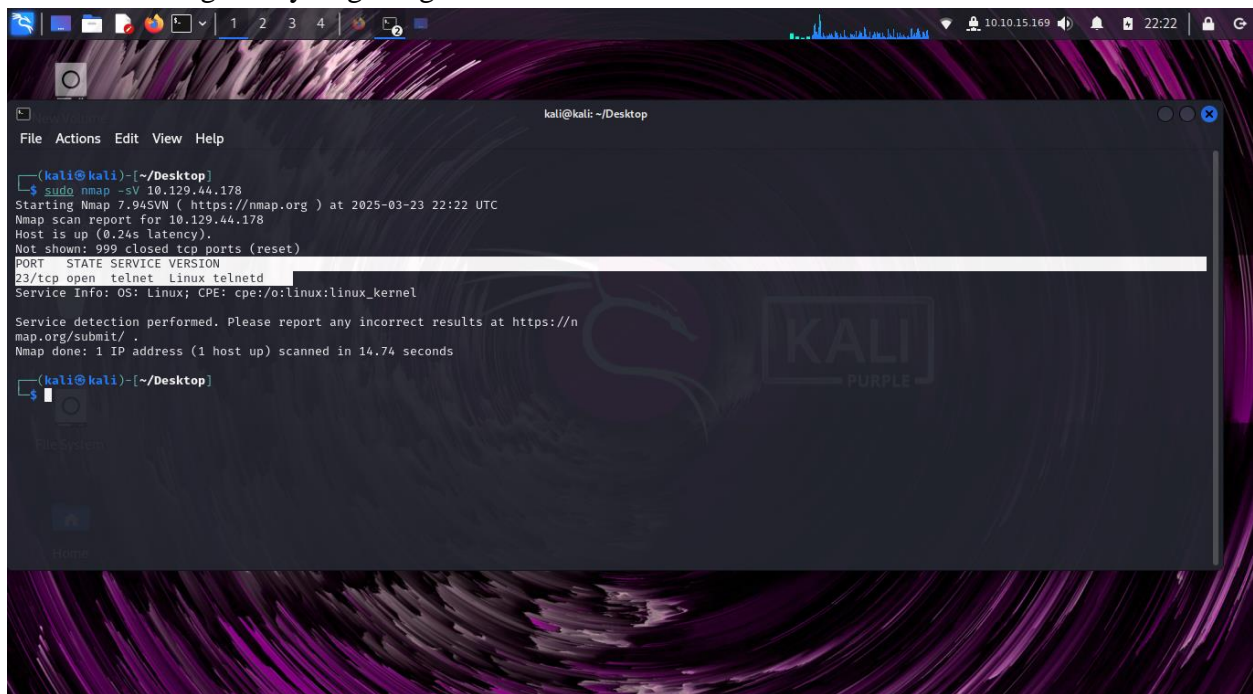
Answer: nmap

Task 6

What service do we identify on port 23/tcp during our scans?

Answer: telnet

I performed an nmap scan using nmap tool together with the `-v` option to enable reveal the services running on my target together with their version.



```
(kali@kali)-[~/Desktop]
$ sudo nmap -sV 10.129.44.178
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-23 22:22 UTC
Nmap scan report for 10.129.44.178
Host is up (0.24s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.74 seconds

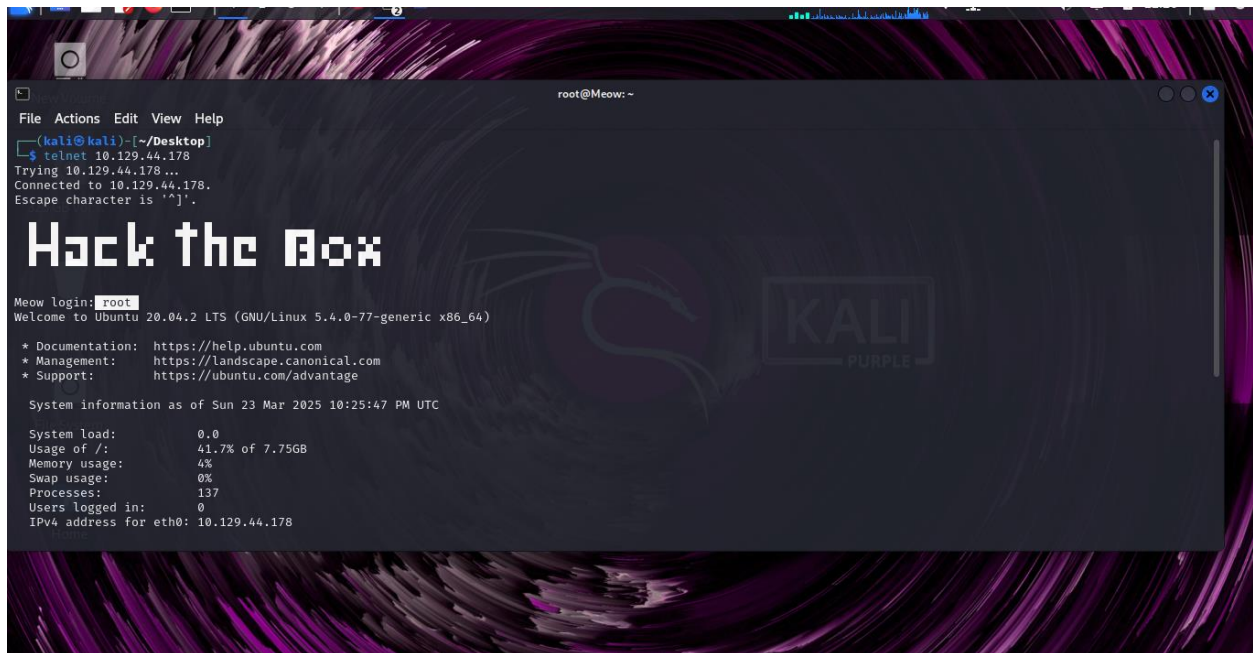
(kali@kali)-[~/Desktop]
$
```

Task 7

What username is able to log into the target over telnet with a blank password?

Answer: root

Root username with no password allowed me login into the machine.



Submit Flag

Flag: `b40abdfc23665f766f9c61ecba8a4c19`

After logging in via telnet i used the ls command to list the files in the directory i landed into after logging in, there was a flag.txt file. U used cat command to view its contents and that's how i captured the flag.



Fawn



Questions

Task 1

What does the 3-letter acronym FTP stand for?

Answer: File transfer protocol

Task 2

Which port does the FTP service listen on usually?

Answer: 21

Task 3

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: http

Task 4

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

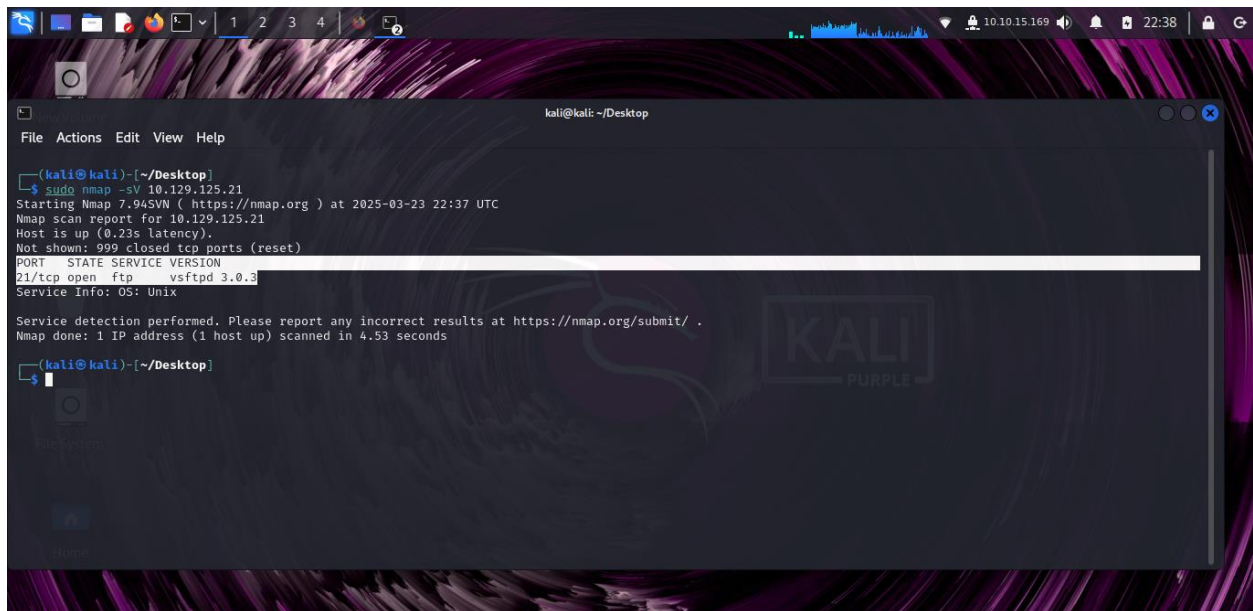
Answer: ping

Task 5

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

Answer: vsftpd 3.0.3

I carried out an nmap scan on my target trying to get services running together with their versions.



```
kali@kali: ~/Desktop
File Actions Edit View Help

(kali@kali)-[~/Desktop]
$ sudo nmap -sV 10.129.125.21
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-23 22:37 UTC
Nmap scan report for 10.129.125.21
Host is up (0.23s 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 4.53 seconds

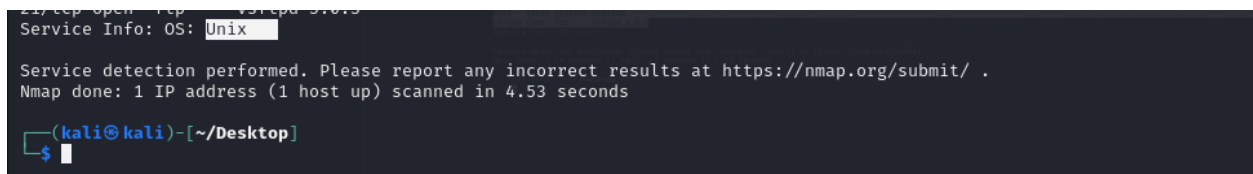
(kali@kali)-[~/Desktop]
$
```

Task 6

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

Answer: unix

The -V option when performing the scan disclosed the os running on the victim machine.



```
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 4.53 seconds

(kali@kali)-[~/Desktop]
$
```

Task 7

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

Answer: **ftp -?**

We ran the command ftp -? To get and learn the inputs and how the ftp tool works.

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)~[~/Desktop]
$ ftp -?
usage: ftp [-46Aade fg in pRtVv] [-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
```

Task 8

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

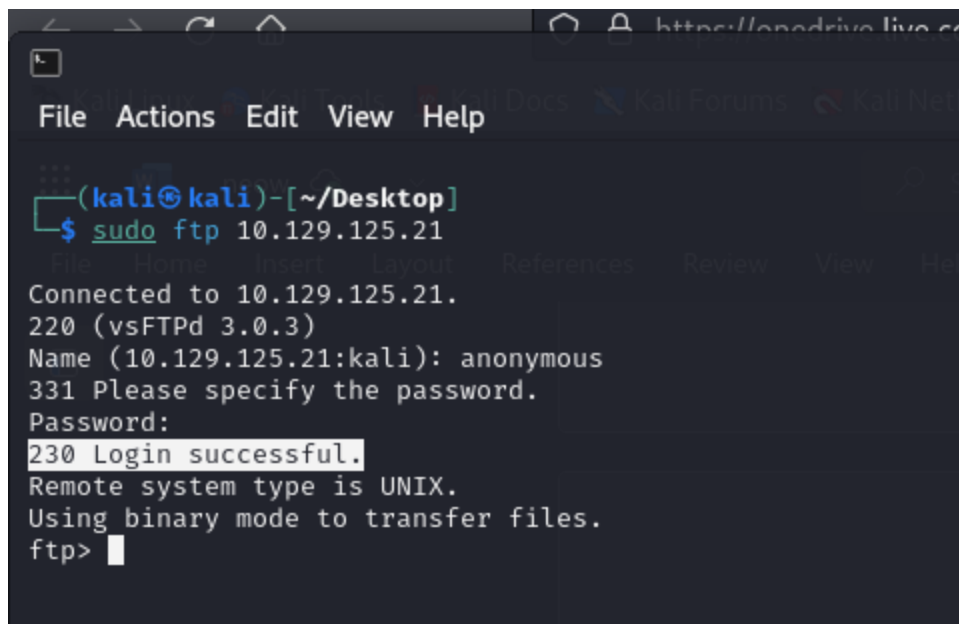
Answer: **anonymous**

```
(kali@kali)~[~/Desktop]
$ sudo ftp 10.129.125.21
Connected to 10.129.125.21.
220 (vsFTPD 3.0.3)
Name (10.129.125.21:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Task 9

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

Answer: **230**

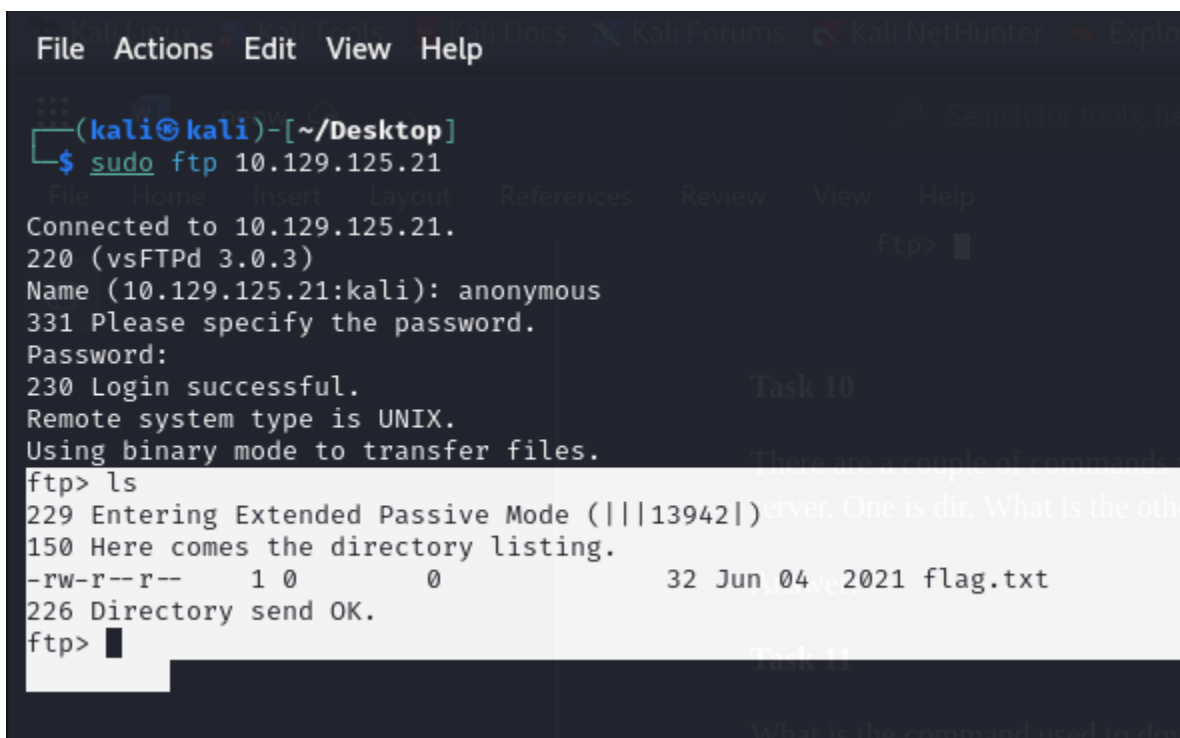
A terminal window with a dark background and light-colored text. The window title bar shows a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. Below the menu bar, the prompt is '(kali㉿kali)-[~/Desktop]'. The user enters '\$ sudo ftp 10.129.125.21'. The output shows a successful connection to 10.129.125.21 using vsFTPD 3.0.3. The user is prompted for a password and logs in successfully. The remote system type is UNIX, and binary mode is used for file transfers. The prompt is now 'ftp>'.

```
(kali㉿kali)-[~/Desktop]
$ sudo ftp 10.129.125.21
Connected to 10.129.125.21.
220 (vsFTPd 3.0.3)
Name (10.129.125.21:kali): 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.

Answer: `ls`

A terminal window showing the continuation of the FTP session. The user enters 'ftp> ls'. The output shows the directory listing for the remote system. The listing includes permissions, file size, date, and filename. The file 'flag.txt' is listed with permissions '-rw-r--r--', size '10', date '32 Jun 04 2021', and filename 'flag.txt'. The prompt is now 'ftp>'.

```
(kali㉿kali)-[~/Desktop]
$ sudo ftp 10.129.125.21
Connected to 10.129.125.21.
220 (vsFTPd 3.0.3)
Name (10.129.125.21:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||13942|)
150 Here comes the directory listing.
-rw-r--r-- 10 0 32 Jun 04 2021 flag.txt
226 Directory send OK.
ftp>
```

Task 11

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

Answer: **get**

I used the get command to download the flag.txt file from the ftp server to my attacker machine.

```
(kali@kali)-[~/Desktop]
$ sudo ftp 10.129.125.21

Connected to 10.129.125.21.
220 (vsFTPD 3.0.3)
Name (10.129.125.21:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||13942|)
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
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||11572|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100% |*****|
226 Transfer complete.
32 bytes received in 00:00 (0.14 KiB/s)
ftp>
```

Submit Flag

Root flag: **035db21c881520061c53e0536e44f815**

```
(kali@kali)-[~/Desktop]
$ ls
flag.txt

(kali@kali)-[~/Desktop]
$ cat flag.txt
035db21c881520061c53e0536e44f815

(kali@kali)-[~/Desktop]
$
```

To get the root flag i just used the cat command on the flag.txt file i downloaded from the server and that's how i captured the flag.