Protocols & Servers

Telnet:

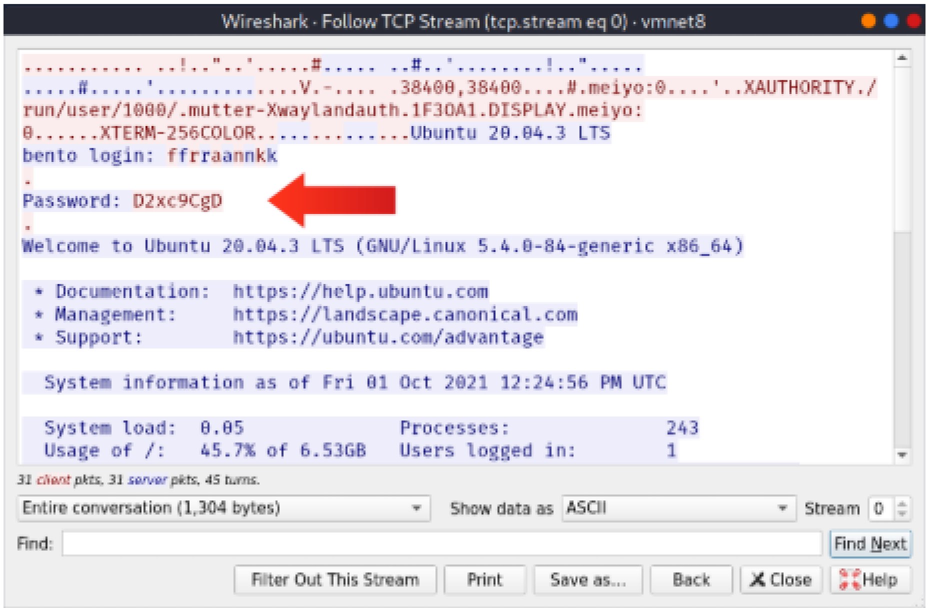
Application layer protocol used to connect to a virtual terminal of another computer. Telnet can allow us to log into another computer to run a program, start batch processes and perform system admin tasks remotely.

It's quite simple. When a user connects the terminal prompts a username and password. Once authorized the user will access the remote systems terminal. But when this connection does happen between the telnet client and telnet server **it is not encrypted, making it an easy target for attackers.**

Telnet server uses Telnet protocol to listen for incoming connections on Port 23. Let's say a user is connecting to the telnetd - Telnet server.

1. First he is asked to use username to login.
2. Then he is asked for a password to login.
3. Once the system checks login credentials he is greeted with a welcome message.
4. Remote server grants him command prompt eg: **frank@bento:~$ - $ means not root terminal.**

Although telnet gave us access to the remote terminal quickly, it is **not a reliable protocol for remote admin as all the data is sent via cleartext.**

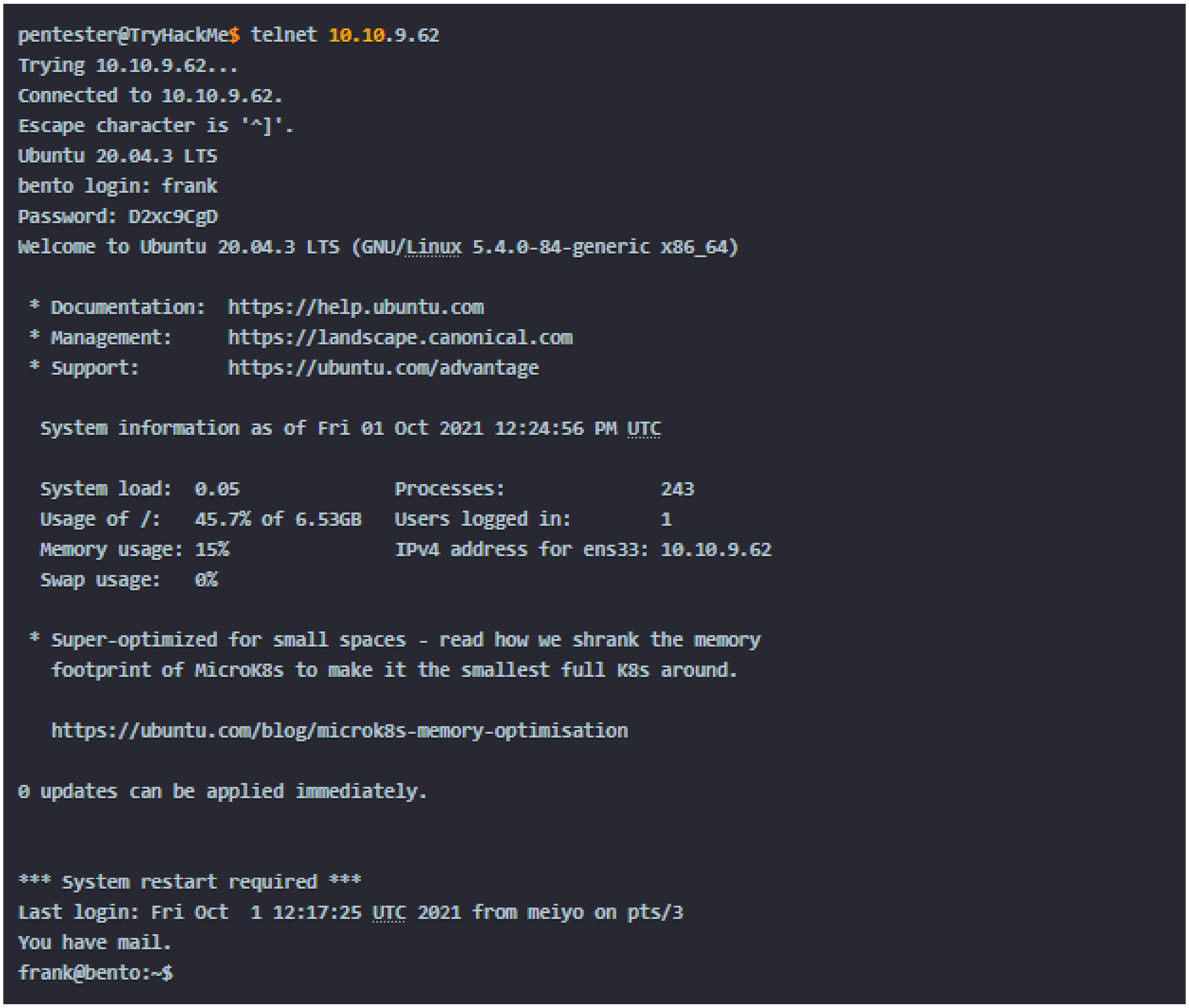


```
........... ..!.."..'.....#..... ..#..'........!..".....
.....#.....'.............V.-.... .38400,38400....#.meiyo:0....'..XAUTHORITY./
run/user/1000/.mutter-Xwaylandauth.1F30A1.DISPLAY.meiyo:
0......XTERM-256COLOR..............Ubuntu 20.04.3 LTS
bento login: ffrraannkk
.
Password: D2xc9CgD
.
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-84-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri 01 Oct 2021 12:24:56 PM UTC

  System load:  0.05              Processes:             243
  Usage of /:   45.7% of 6.53GB   Users logged in:       1
```

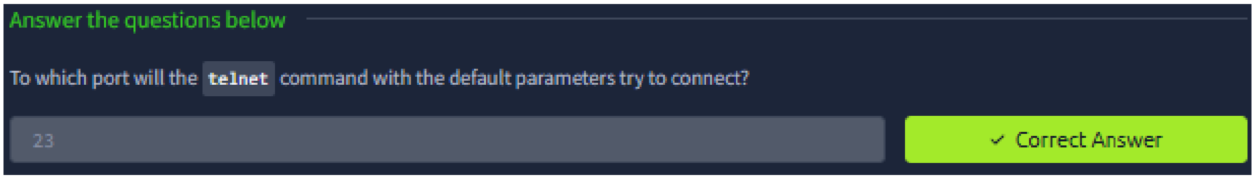
31 client pkts, 31 server pkts, 45 turns.

Entire conversation (1,304 bytes) — Show data as: ASCII — Stream: 0

Example of packet intercepted from Telnet. Show's ASCII text data. Red = What we are sending and blue = text remote system is sending. It was all echoed back to us.



```
pentester@TryHackMe$ telnet 10.10.9.62
Trying 10.10.9.62...
Connected to 10.10.9.62.
Escape character is '^]'.
Ubuntu 20.04.3 LTS
bento login: frank
Password: D2xc9CgD
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-84-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri 01 Oct 2021 12:24:56 PM UTC

  System load:  0.05              Processes:              243
  Usage of /:   45.7% of 6.53GB   Users logged in:        1
  Memory usage: 15%               IPv4 address for ens33: 10.10.9.62
  Swap usage:   0%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

0 updates can be applied immediately.


*** System restart required ***
Last login: Fri Oct  1 12:17:25 UTC 2021 from meiyo on pts/3
You have mail.
frank@bento:~$
```



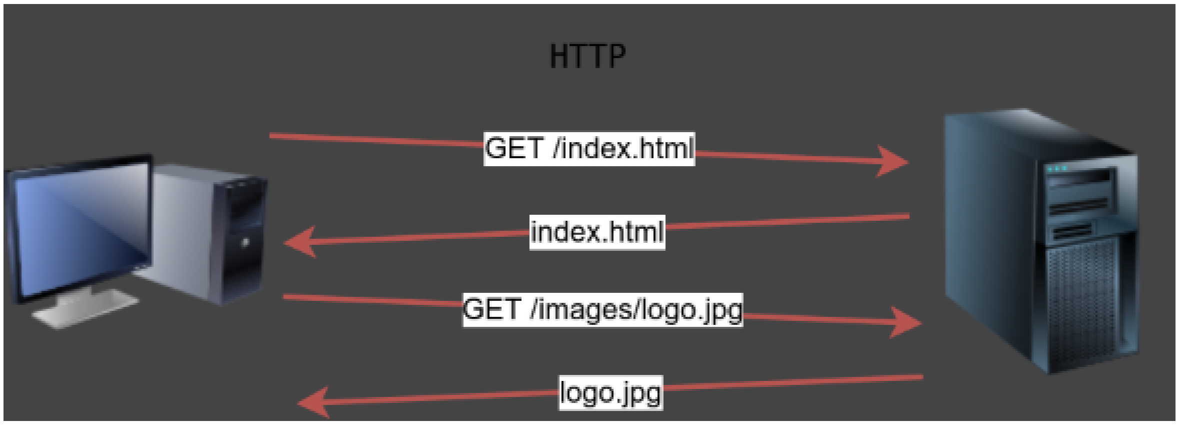
Answer the questions below

To which port will the `telnet` command with the default parameters try to connect?

23

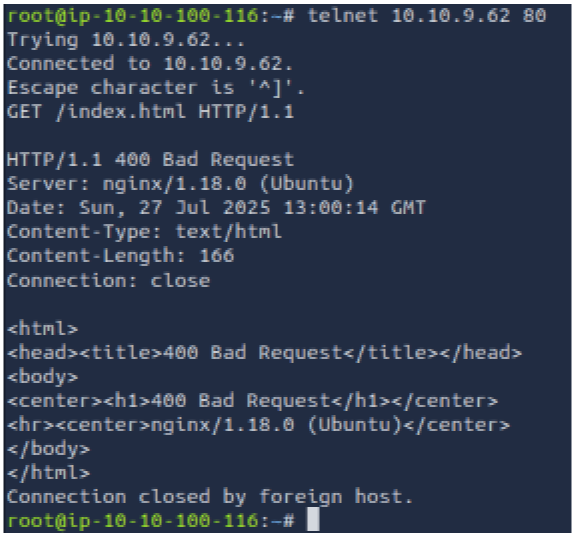
Hyper Text Transfer Protocol (HTTP)

This protocol is used for transferring web pages. Web browser connects to the web server and uses HTTP to request HTML pages. Anytime you access **WWW** you are using a HTTP protocol.



In the following example, we will see how we can request a page from a web server. Additionally we will discover the web server version. We need to use Telnet client, because it is a simple protocol makes using it easier.

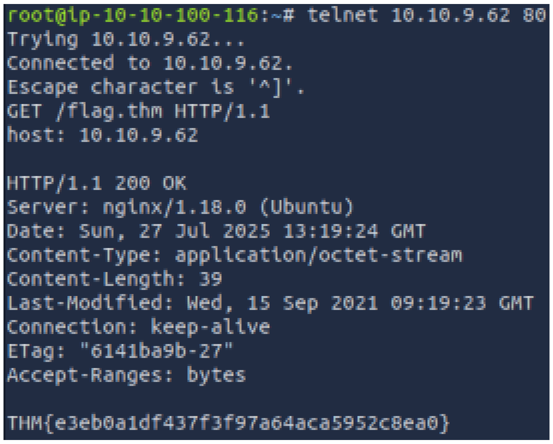
1. Connect to port 80 using **telnet 10.10.9.62 80**
2. Type **GET /index.html HTTP/1.1** to retrieve page index.html or GET / HTTP/1.1.
3. Finally you need to provide value for the host like **host: telnet and press “enter” twice.**



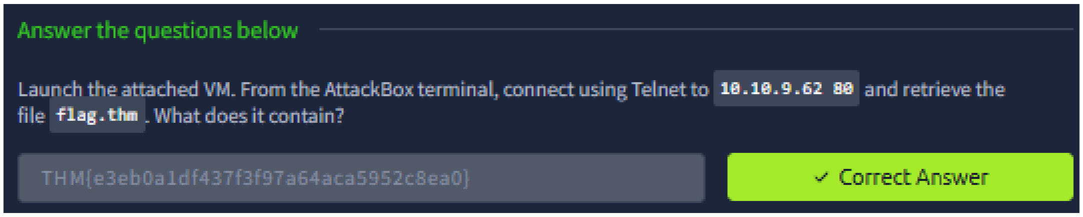
```
root@ip-10-10-100-116:~# telnet 10.10.9.62 80
Trying 10.10.9.62...
Connected to 10.10.9.62.
Escape character is '^]'.
GET /index.html HTTP/1.1

HTTP/1.1 400 Bad Request
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 27 Jul 2025 13:00:14 GMT
Content-Type: text/html
Content-Length: 166
Connection: close

<html>
<head><title>400 Bad Request</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx/1.18.0 (Ubuntu)</center>
</body>
</html>
Connection closed by foreign host.
root@ip-10-10-100-116:~# 
```

Now we need to retrieve the flag.thm on the virtual machine by connecting to 10.10.9.62 80 using Telnet. Let’s give it a go!

First thing I tried was GET / HTTP/1.1 host: 10.10.9.62 But did not get the flag yet.
Next I tried GET /flag.thm HTTP/1.1 host: 10.10.9.62 and it was it! I also learnt a very valuable lesson, to make sure the format is correct capitals will not work! Silly mistake.



```
root@ip-10-10-100-116:~# telnet 10.10.9.62 80
Trying 10.10.9.62...
Connected to 10.10.9.62.
Escape character is '^]'.
GET /flag.thm HTTP/1.1
host: 10.10.9.62

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 27 Jul 2025 13:19:24 GMT
Content-Type: application/octet-stream
Content-Length: 39
Last-Modified: Wed, 15 Sep 2021 09:19:23 GMT
Connection: keep-alive
ETag: "6141ba9b-27"
Accept-Ranges: bytes

THM{e3eb0a1df437f3f97a64aca5952c8ea0}
```



Answer the questions below

Launch the attached VM. From the AttackBox terminal, connect using Telnet to `10.10.9.62 80` and retrieve the file `flag.thm`. What does it contain?

THM{e3eb0a1df437f3f97a64aca5952c8ea0}

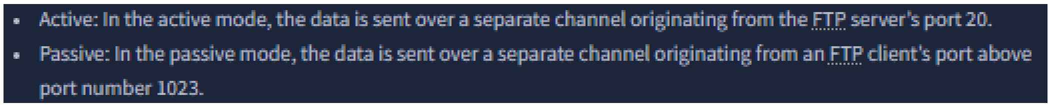
File Transfer Protocol (FTP)

This particular protocol was actually designed for allowing the transferring of files between different computers with different systems efficiently.

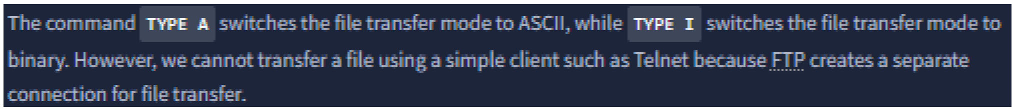
FTP also receives data as clear text, therefore we can use Telnet or Netcat to communicate with the FTP server and act as an FTP client.

1. Connect to FTP server using Telnet client, since FTP server listens on Port 21 by default we had to specify to our client to attempt connection on Port 21 instead.
2. We needed to provide the user name
3. We need to provide the password
4. Then we are logged in!

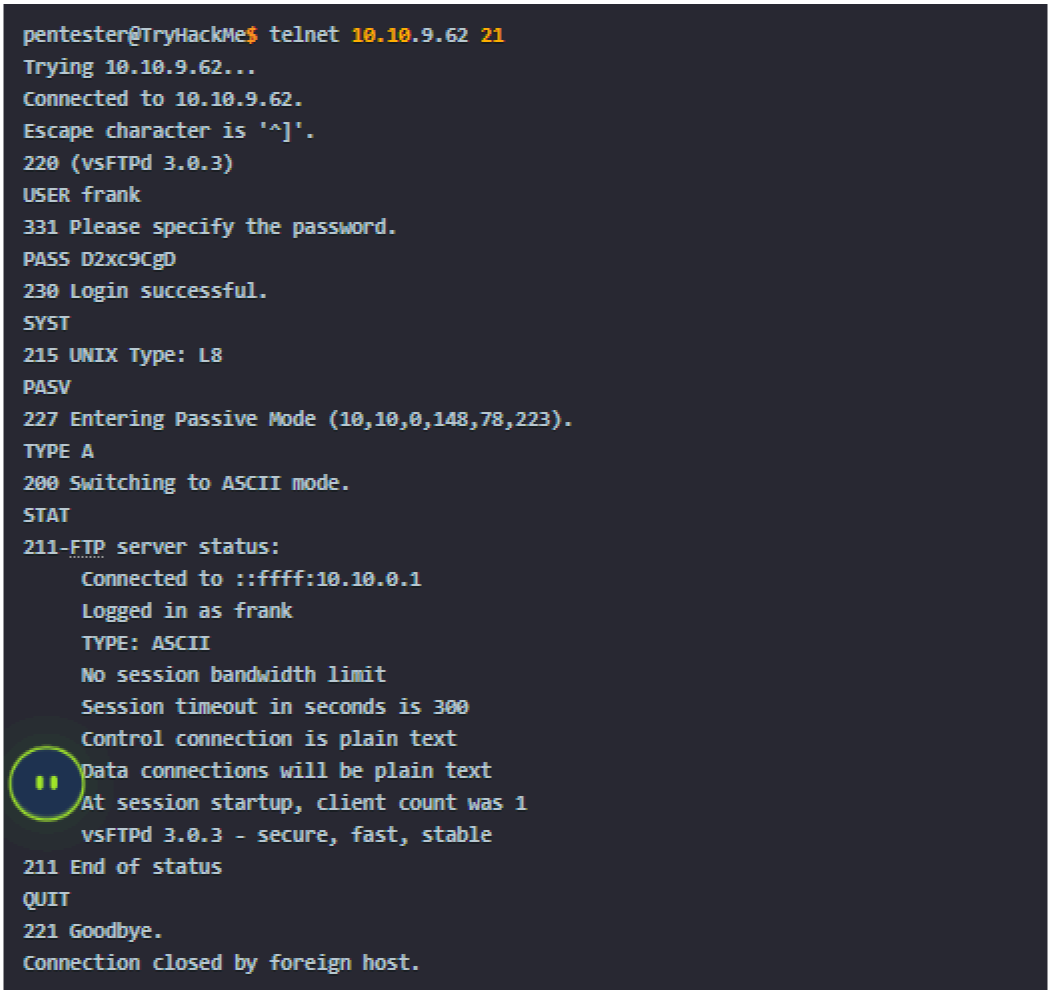
Command like **STAT** can provide additional information the **SYST** command shows the system type of the target, **PASV** switches mode to passive.



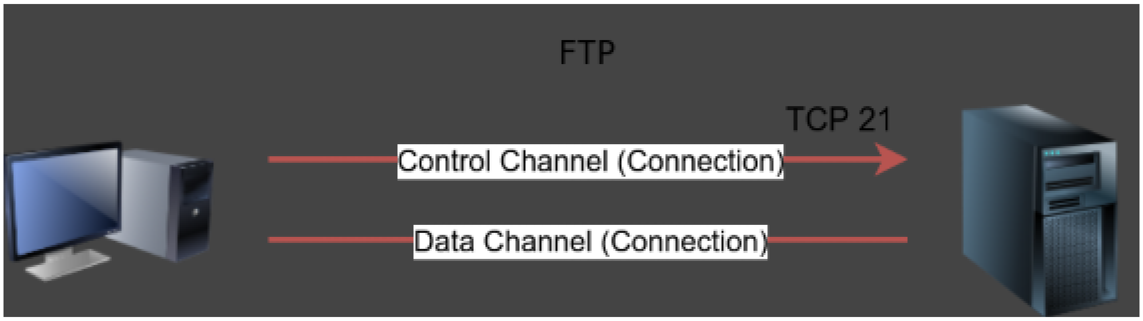
- Active: In the active mode, the data is sent over a separate channel originating from the FTP server's port 20.
- Passive: In the passive mode, the data is sent over a separate channel originating from an FTP client's port above port number 1023.

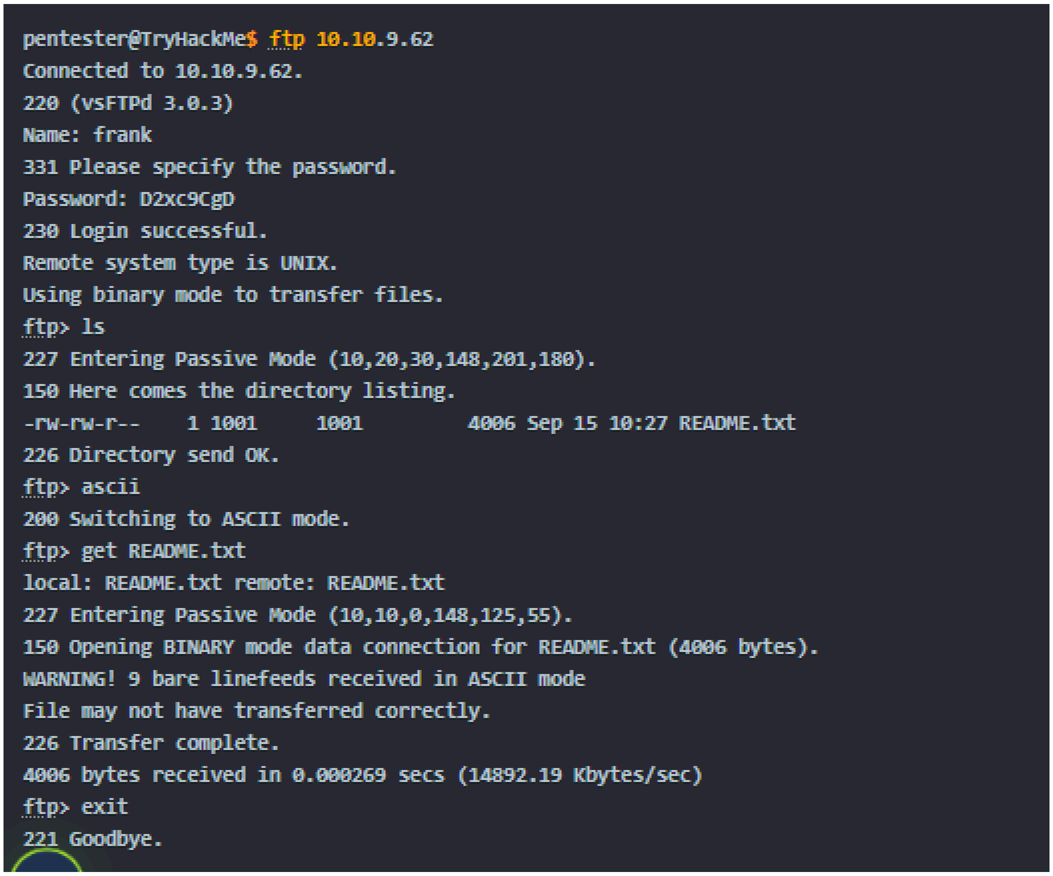


The command `TYPE A` switches the file transfer mode to ASCII, while `TYPE I` switches the file transfer mode to binary. However, we cannot transfer a file using a simple client such as Telnet because FTP creates a separate connection for file transfer.

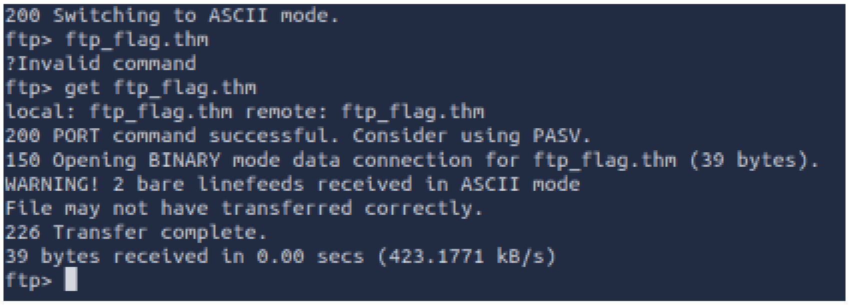


```
pentester@TryHackMe$ telnet 10.10.9.62 21
Trying 10.10.9.62...
Connected to 10.10.9.62.
Escape character is '^]'.
220 (vsFTPd 3.0.3)
USER frank
331 Please specify the password.
PASS D2xc9CgD
230 Login successful.
SYST
215 UNIX Type: L8
PASV
227 Entering Passive Mode (10,10,0,148,78,223).
TYPE A
200 Switching to ASCII mode.
STAT
211-FTP server status:
     Connected to ::ffff:10.10.0.1
     Logged in as frank
     TYPE: ASCII
     No session bandwidth limit
     Session timeout in seconds is 300
     Control connection is plain text
     Data connections will be plain text
     At session startup, client count was 1
     vsFTPd 3.0.3 - secure, fast, stable
211 End of status
QUIT
221 Goodbye.
Connection closed by foreign host.
```



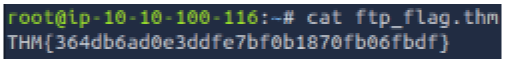


```
pentester@TryHackMe$ ftp 10.10.9.62
Connected to 10.10.9.62.
220 (vsFTPd 3.0.3)
Name: frank
331 Please specify the password.
Password: D2xc9CgD
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (10,20,30,148,201,180).
150 Here comes the directory listing.
-rw-rw-r--    1 1001     1001         4006 Sep 15 10:27 README.txt
226 Directory send OK.
ftp> ascii
200 Switching to ASCII mode.
ftp> get README.txt
local: README.txt remote: README.txt
227 Entering Passive Mode (10,10,0,148,125,55).
150 Opening BINARY mode data connection for README.txt (4006 bytes).
WARNING! 9 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
4006 bytes received in 0.000269 secs (14892.19 Kbytes/sec)
ftp> exit
221 Goodbye.
```



```
200 Switching to ASCII mode.
ftp> ftp_flag.thm
?Invalid command
ftp> get ftp_flag.thm
local: ftp_flag.thm remote: ftp_flag.thm
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for ftp_flag.thm (39 bytes).
WARNING! 2 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
39 bytes received in 0.00 secs (423.1771 kB/s)
ftp> █
```

This is our prompt! So we have transferred the file successfully. Now we must exit.



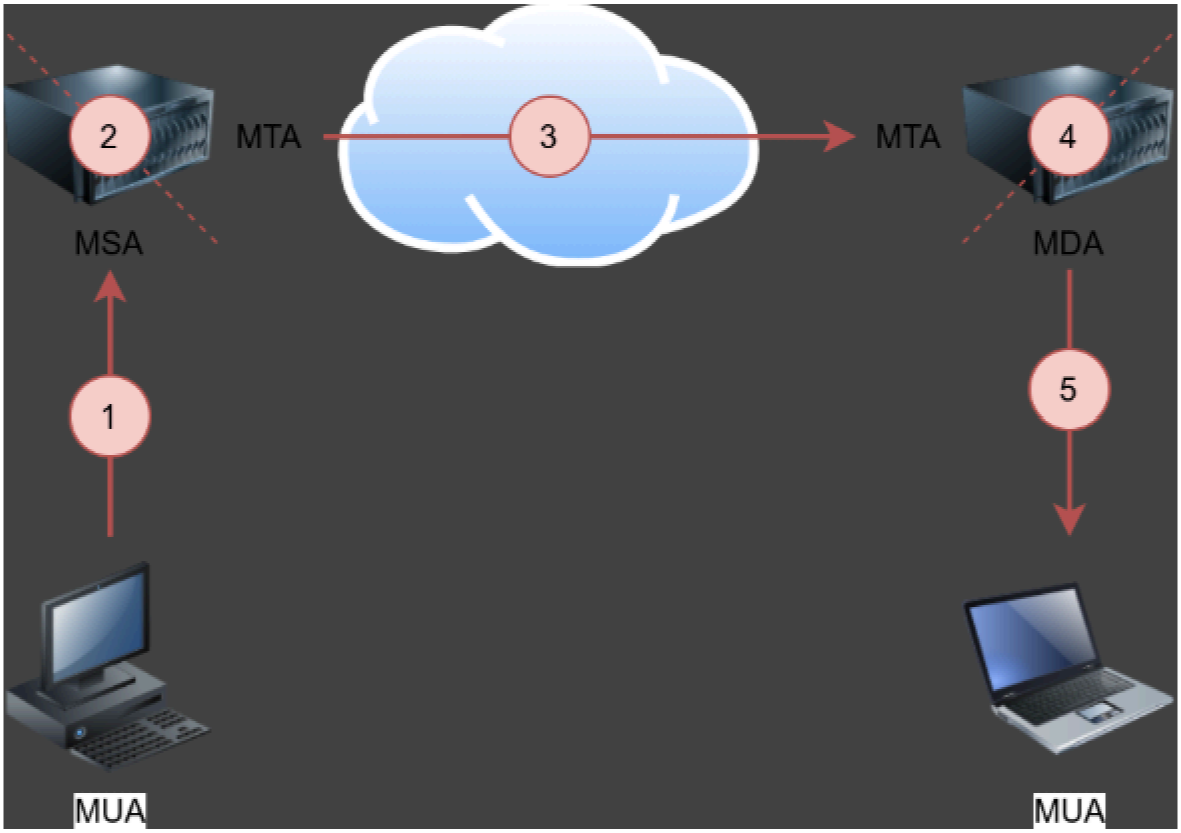
```
root@ip-10-10-100-116:~# cat ftp_flag.thm
THM{364db6ad0e3ddfe7bf0b1870fb06fbdf}
```

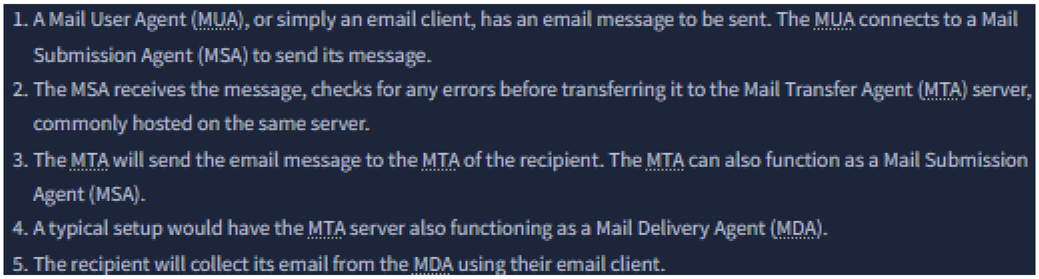
Boom! Success.

Simple Mail Transfer Protocol (SMTP)

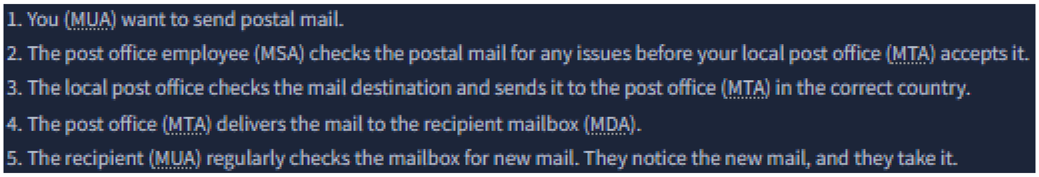
Email is one of the most used services on the internet. The email delivery over the internet requires the following components:

1. Mail Submission Agent (MSA)
2. Mail Transfer Agent (MTA)
3. Mail Delivery Agent (MDA)
4. Mail User Agent (MUA)

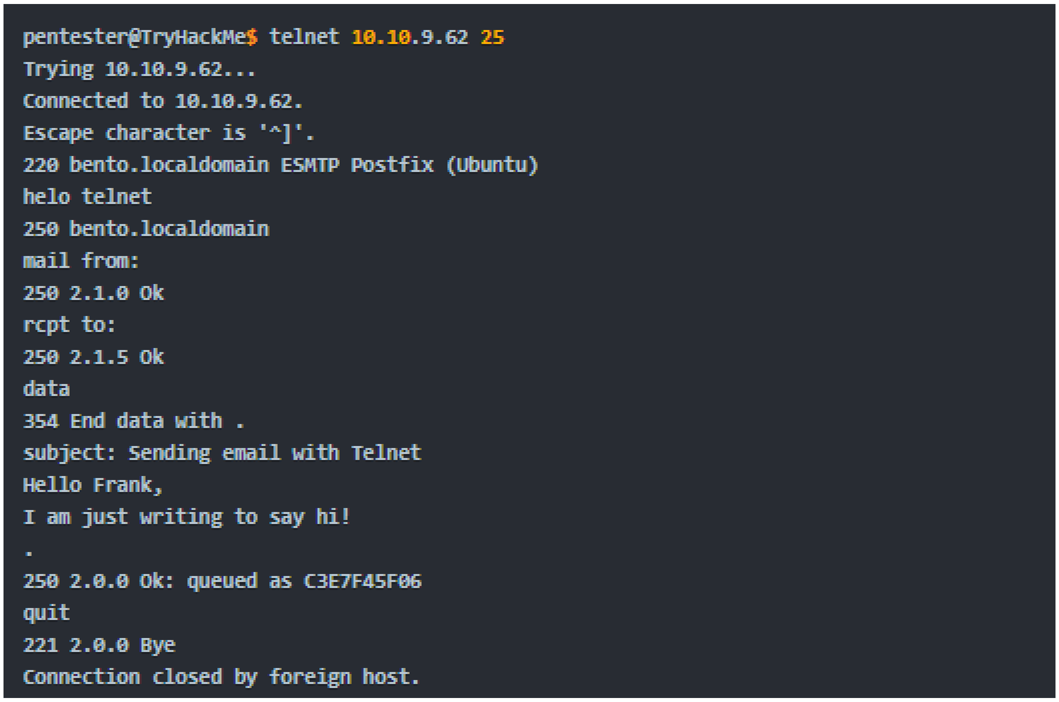




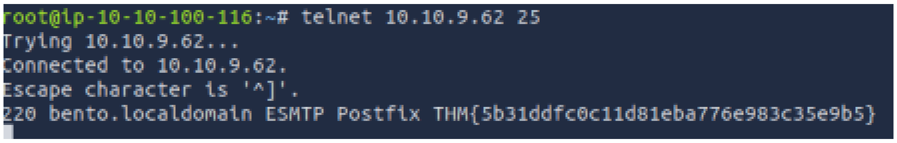
1. A Mail User Agent (MUA), or simply an email client, has an email message to be sent. The MUA connects to a Mail Submission Agent (MSA) to send its message.
2. The MSA receives the message, checks for any errors before transferring it to the Mail Transfer Agent (MTA) server, commonly hosted on the same server.
3. The MTA will send the email message to the MTA of the recipient. The MTA can also function as a Mail Submission Agent (MSA).
4. A typical setup would have the MTA server also functioning as a Mail Delivery Agent (MDA).
5. The recipient will collect its email from the MDA using their email client.



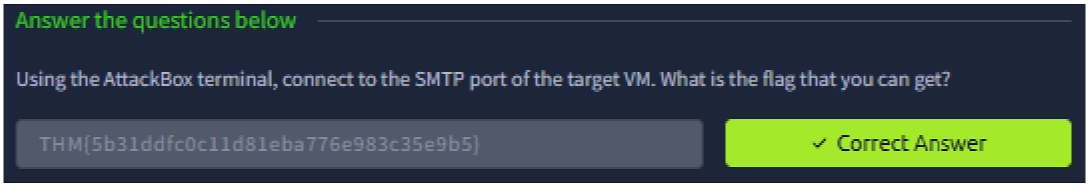
1. You (MUA) want to send postal mail.
2. The post office employee (MSA) checks the postal mail for any issues before your local post office (MTA) accepts it.
3. The local post office checks the mail destination and sends it to the post office (MTA) in the correct country.
4. The post office (MTA) delivers the mail to the recipient mailbox (MDA).
5. The recipient (MUA) regularly checks the mailbox for new mail. They notice the new mail, and they take it.



```
pentester@TryHackMe$ telnet 10.10.9.62 25
Trying 10.10.9.62...
Connected to 10.10.9.62.
Escape character is '^]'.
220 bento.localdomain ESMTP Postfix (Ubuntu)
helo telnet
250 bento.localdomain
mail from:
250 2.1.0 Ok
rcpt to:
250 2.1.5 Ok
data
354 End data with .
subject: Sending email with Telnet
Hello Frank,
I am just writing to say hi!
.
250 2.0.0 Ok: queued as C3E7F45F06
quit
221 2.0.0 Bye
Connection closed by foreign host.
```



```
root@ip-10-10-100-116:~# telnet 10.10.9.62 25
Trying 10.10.9.62...
Connected to 10.10.9.62.
Escape character is '^]'.
220 bento.localdomain ESMTP Postfix THM{5b31ddfc0c11d81eba776e983c35e9b5}
```



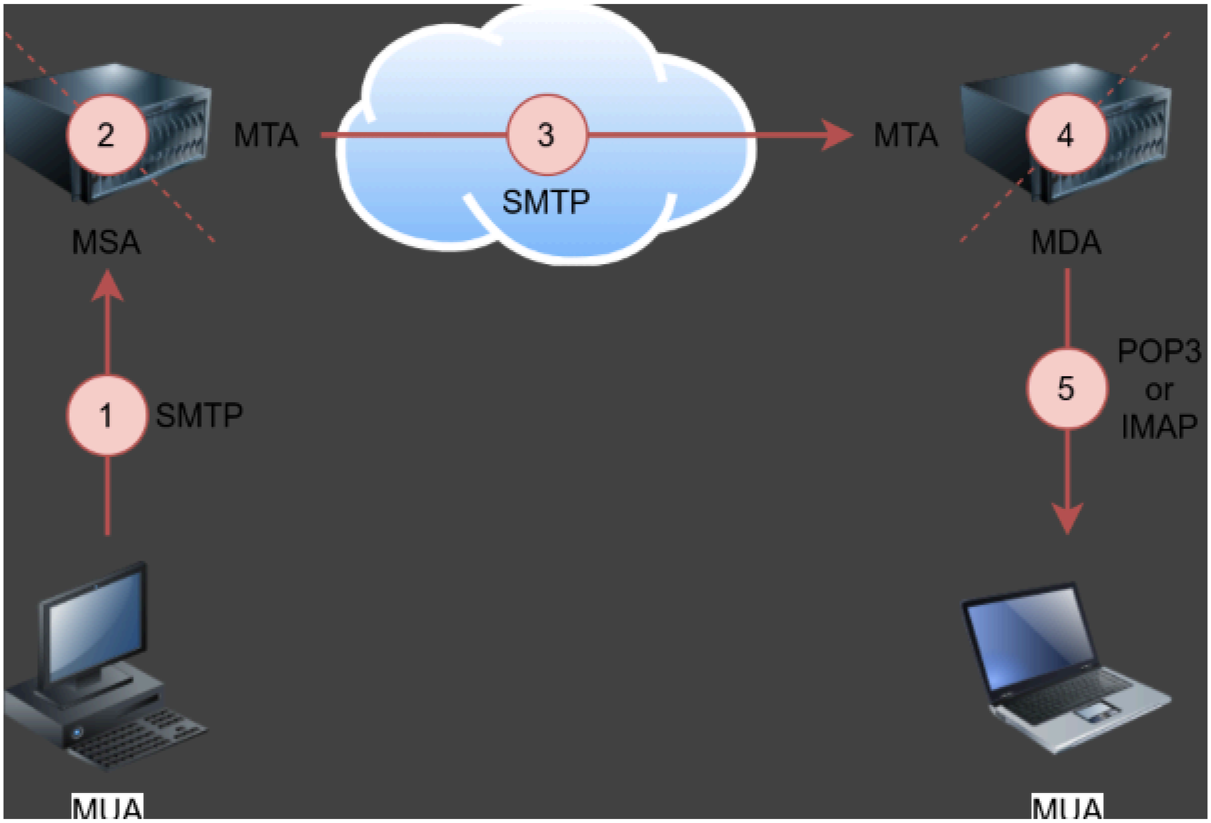
Answer the questions below

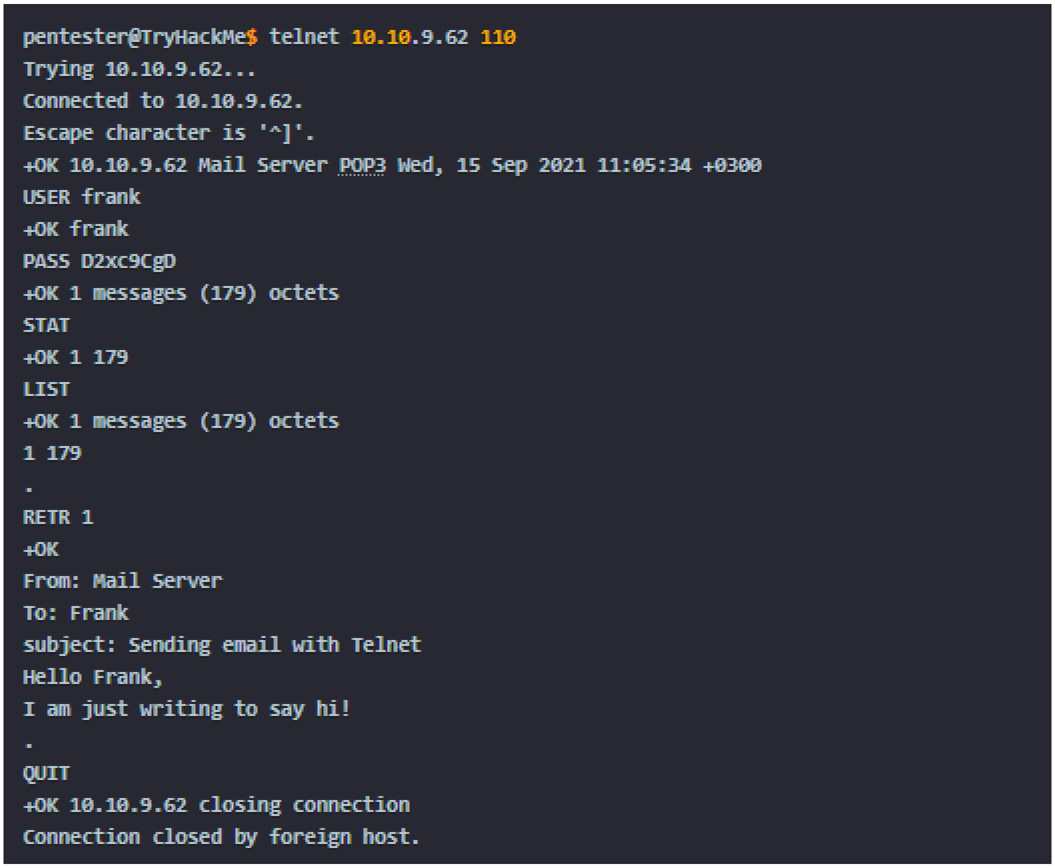
Using the AttackBox terminal, connect to the SMTP port of the target VM. What is the flag that you can get?

THM{5b31ddfc0c11d81eba776e983c35e9b5}

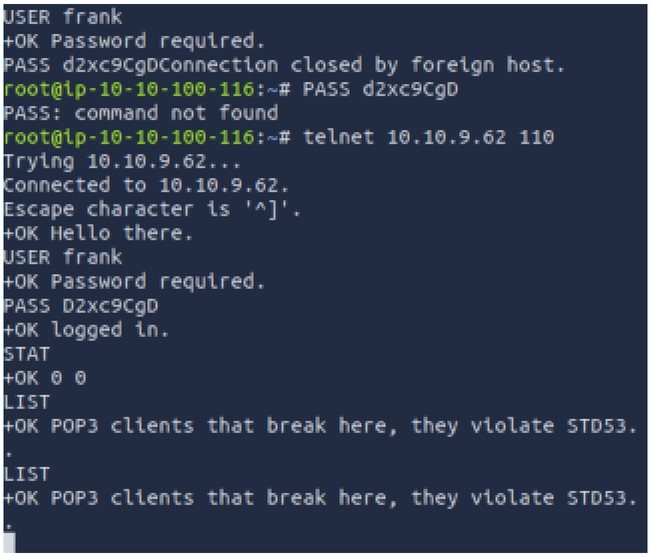
Post Office Protocol 3 (POP3)

Used to download email messages from a mail delivery agent MDA server.

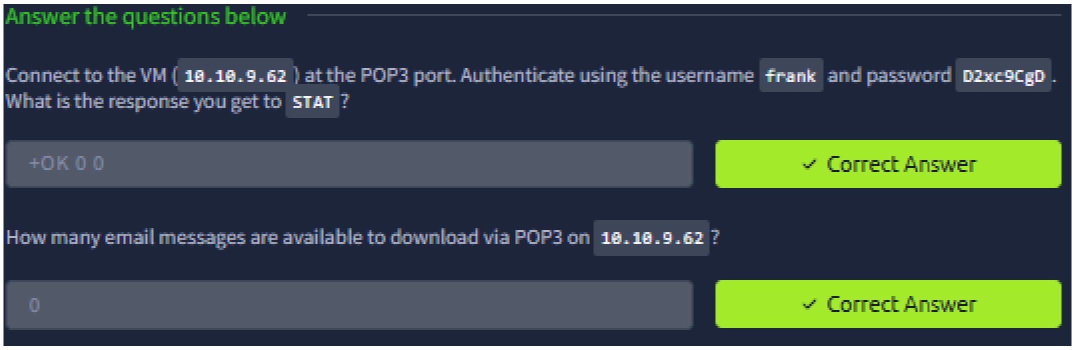




```
pentester@TryHackMe$ telnet 10.10.9.62 110
Trying 10.10.9.62...
Connected to 10.10.9.62.
Escape character is '^]'.
+OK 10.10.9.62 Mail Server POP3 Wed, 15 Sep 2021 11:05:34 +0300
USER frank
+OK frank
PASS D2xc9CgD
+OK 1 messages (179) octets
STAT
+OK 1 179
LIST
+OK 1 messages (179) octets
1 179
.
RETR 1
+OK
From: Mail Server
To: Frank
subject: Sending email with Telnet
Hello Frank,
I am just writing to say hi!
.
QUIT
+OK 10.10.9.62 closing connection
Connection closed by foreign host.
```



```
USER frank
+OK Password required.
PASS d2xc9CgDConnection closed by foreign host.
root@ip-10-10-100-116:~# PASS d2xc9CgD
PASS: command not found
root@ip-10-10-100-116:~# telnet 10.10.9.62 110
Trying 10.10.9.62...
Connected to 10.10.9.62.
Escape character is '^]'.
+OK Hello there.
USER frank
+OK Password required.
PASS D2xc9CgD
+OK logged in.
STAT
+OK 0 0
LIST
+OK POP3 clients that break here, they violate STD53.
.
LIST
+OK POP3 clients that break here, they violate STD53.
.
```


Answer the questions below

Connect to the VM (`10.10.9.62`) at the POP3 port. Authenticate using the username `frank` and password `D2xc9CgD` . What is the response you get to `STAT` ?

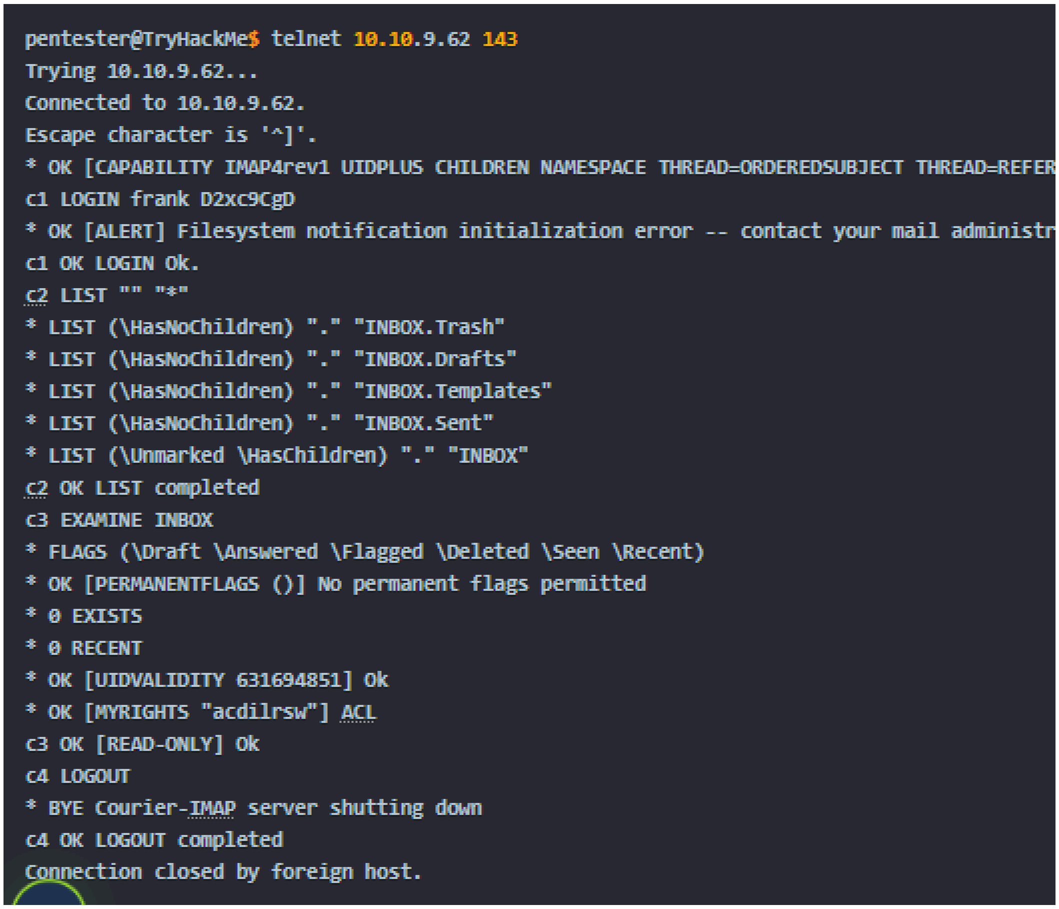
+OK 0 0

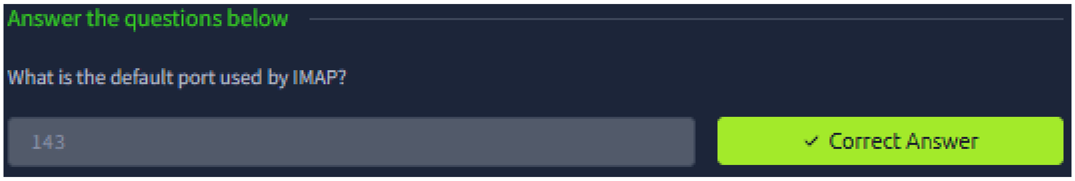
How many email messages are available to download via POP3 on `10.10.9.62` ?

0

Internet Message Access Protocol (IMAP)

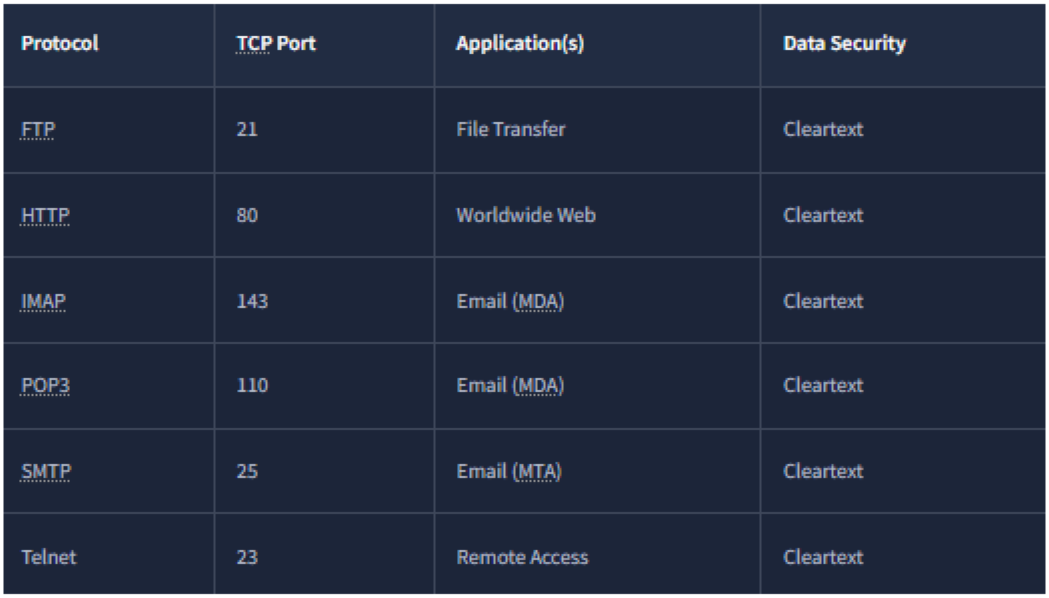
More sophisticated makes it possible to synchronize across multiple devices and mail clients. Eg if you mark an email as read when checking your email, the change will be saved on the IMAP (MDA) and replicated on your laptop when you review it on that separate device.


```
pentester@TryHackMe$ telnet 10.10.9.62 143
Trying 10.10.9.62...
Connected to 10.10.9.62.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFER
c1 LOGIN frank D2xc9CgD
* OK [ALERT] Filesystem notification initialization error -- contact your mail administr
c1 OK LOGIN Ok.
c2 LIST "" "*"
* LIST (\HasNoChildren) "." "INBOX.Trash"
* LIST (\HasNoChildren) "." "INBOX.Drafts"
* LIST (\HasNoChildren) "." "INBOX.Templates"
* LIST (\HasNoChildren) "." "INBOX.Sent"
* LIST (\Unmarked \HasChildren) "." "INBOX"
c2 OK LIST completed
c3 EXAMINE INBOX
* FLAGS (\Draft \Answered \Flagged \Deleted \Seen \Recent)
* OK [PERMANENTFLAGS ()] No permanent flags permitted
* 0 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 631694851] Ok
* OK [MYRIGHTS "acdilrsw"] ACL
c3 OK [READ-ONLY] Ok
c4 LOGOUT
* BYE Courier-IMAP server shutting down
c4 OK LOGOUT completed
Connection closed by foreign host.
```


Answer the questions below

What is the default port used by IMAP?

143



Protocol	TCP Port	Application(s)	Data Security
FTP	21	File Transfer	Cleartext
HTTP	80	Worldwide Web	Cleartext
IMAP	143	Email (MDA)	Cleartext
POP3	110	Email (MDA)	Cleartext
SMTP	25	Email (MTA)	Cleartext
Telnet	23	Remote Access	Cleartext

Conclusion:
By understanding how I can use the various different protocols I can understand how to interact with the interface over the command prompt selecting the appropriate ports and configuration information. By doing this I can remote login to different protocols gaining access to information. This means that by having a targets information such as username and password, which could potentially be intercepted by using a MITM attack, as it is unsecured and has cleartext packets being sent, these packets could theoretically be intercepted by applications such as wireshark and expose the credentials.
If this is done, I could as the attacker essentially save those credentials and login remotely using those credentials to gain access to the targets system, accessing their files and data as well as being able to send it back to my device.