Networking Core Protocols

DNS

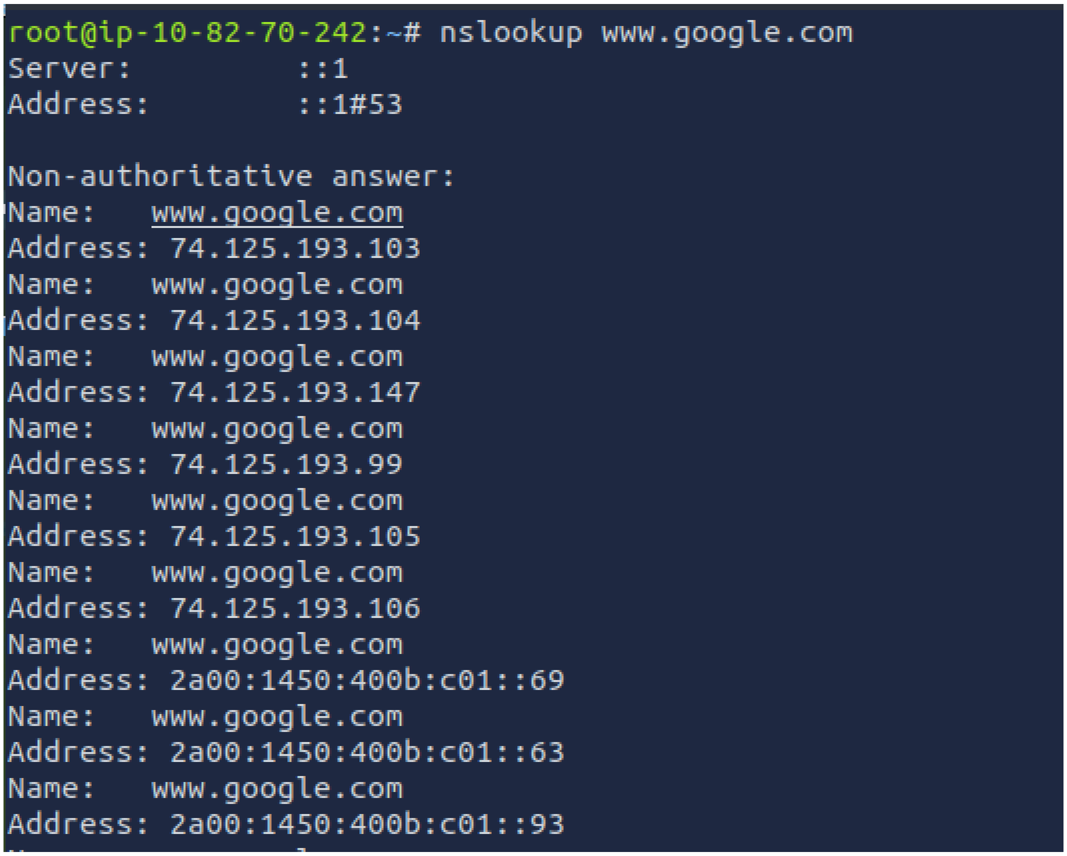
is responsible for properly mapping a domain name to an IP address.

DNS traffic uses UDP port 53 by default and TCP port 53

types of DNS records:

- **A record**: The A (Address) record maps a hostname to one or more IPv4 addresses. For example, you can set `example.com` to resolve to `172.17.2.172`.
- **AAAA Record**: The AAAA record is similar to the A Record, but it is for IPv6. Remember that it is AAAA (quad-A), as AA and AAA would refer to a battery size; furthermore, AAA refers to *Authentication, Authorization, and Accounting*; neither falls under DNS.
- **CNAME Record**: The CNAME (Canonical Name) record maps a domain name to another domain name. For example, `www.example.com` can be mapped to `example.com` or even to `example.org`.
- **MX Record**: The MX (Mail Exchange) record specifies the mail server responsible for handling emails for a domain.

To look up the ip address of a domain you can use: nslookup



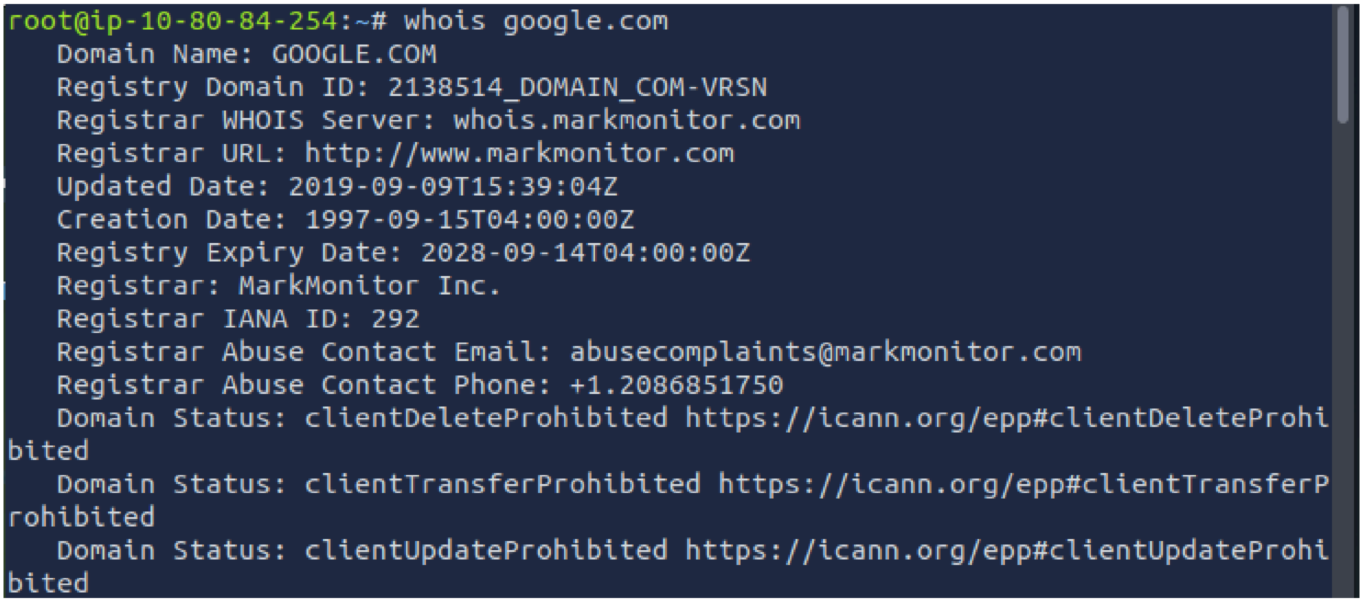
```
root@ip-10-82-70-242:~# nslookup www.google.com
Server:         ::1
Address:        ::1#53

Non-authoritative answer:
Name:   www.google.com
Address: 74.125.193.103
Name:   www.google.com
Address: 74.125.193.104
Name:   www.google.com
Address: 74.125.193.147
Name:   www.google.com
Address: 74.125.193.99
Name:   www.google.com
Address: 74.125.193.105
Name:   www.google.com
Address: 74.125.193.106
Name:   www.google.com
Address: 2a00:1450:400b:c01::69
Name:   www.google.com
Address: 2a00:1450:400b:c01::63
Name:   www.google.com
Address: 2a00:1450:400b:c01::93
```

WHOIS

can look up the WHOIS records of any registered domain name using one of the online services or via the command-line tool `whois`

you can find the registrant’s name, address, phone, and email.



```
root@ip-10-80-84-254:~# whois google.com
   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhi
bited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferP
rohibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhi
bited
```

With the following web protocols we can use wireshark to see the client messages and server responses for the web based protocols .

HTTP(S)

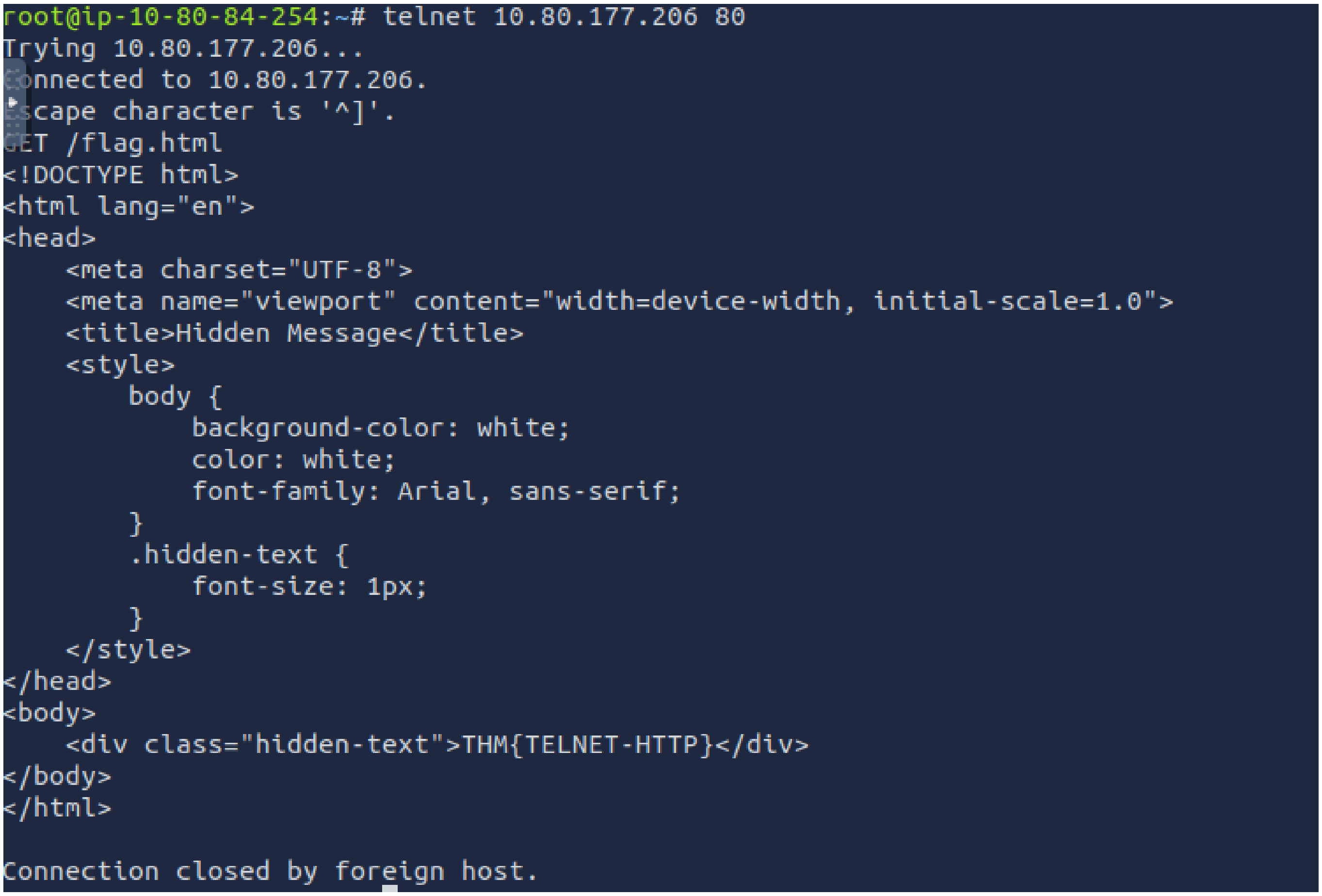
Browsers mainly use HTTP and HTTPS protocols. They rely on TCP connections and it defines how the web browser communicates with the web servers

Here are commands that the web browsers issue to the webserver:

- `GET` retrieves data from a server, such as an HTML file or an image.
- `POST` allows us to submit new data to the server, such as submitting a form or uploading a file.
- `PUT` is used to create a new resource on the server and to update and overwrite existing information.
- `DELETE` , as the name suggests, is used to delete a specified file or resource on the server.

HTTP and HTTPS commonly use TCP ports **80** and **443**, respectively, and less commonly other ports such as **8080** and **8443**

using telnet to access a file/any page



```
root@ip-10-80-84-254:~# telnet 10.80.177.206 80
Trying 10.80.177.206...
Connected to 10.80.177.206.
Escape character is '^]'.
GET /flag.html
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Hidden Message</title>
    <style>
        body {
            background-color: white;
            color: white;
            font-family: Arial, sans-serif;
        }
        .hidden-text {
            font-size: 1px;
        }
    </style>
</head>
<body>
    <div class="hidden-text">THM{TELNET-HTTP}</div>
</body>
</html>

Connection closed by foreign host.
```

I used telnet [ip of target] [port]
then sent a get request to the page i wanted which displayed a flag

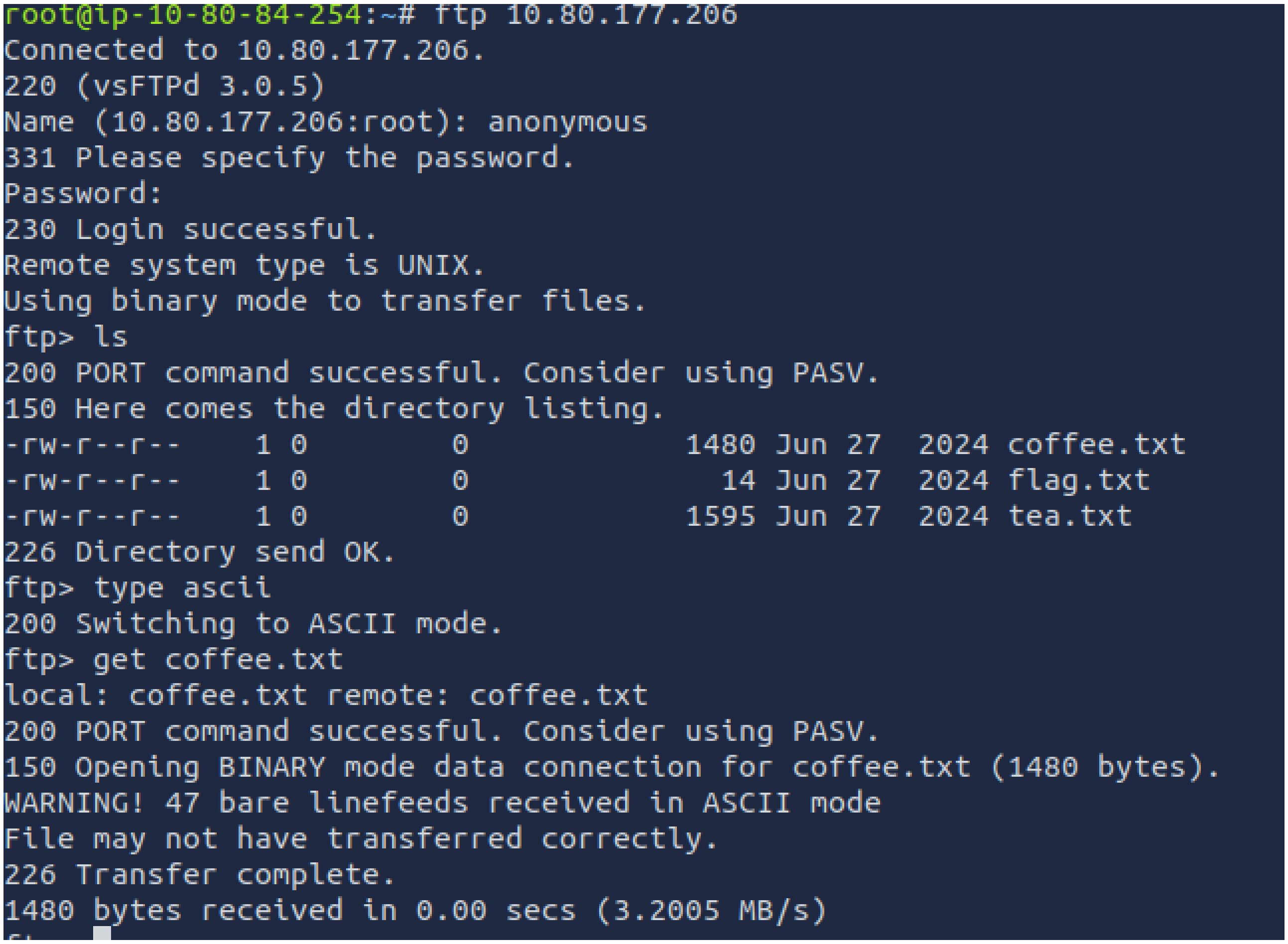
FTP (File Transfer Protocol)

is designed to transfer files. its efficient for file transfer and when all conditions are equal can achieve higher speeds than HTTP

Example commands defined by the FTP protocol are:

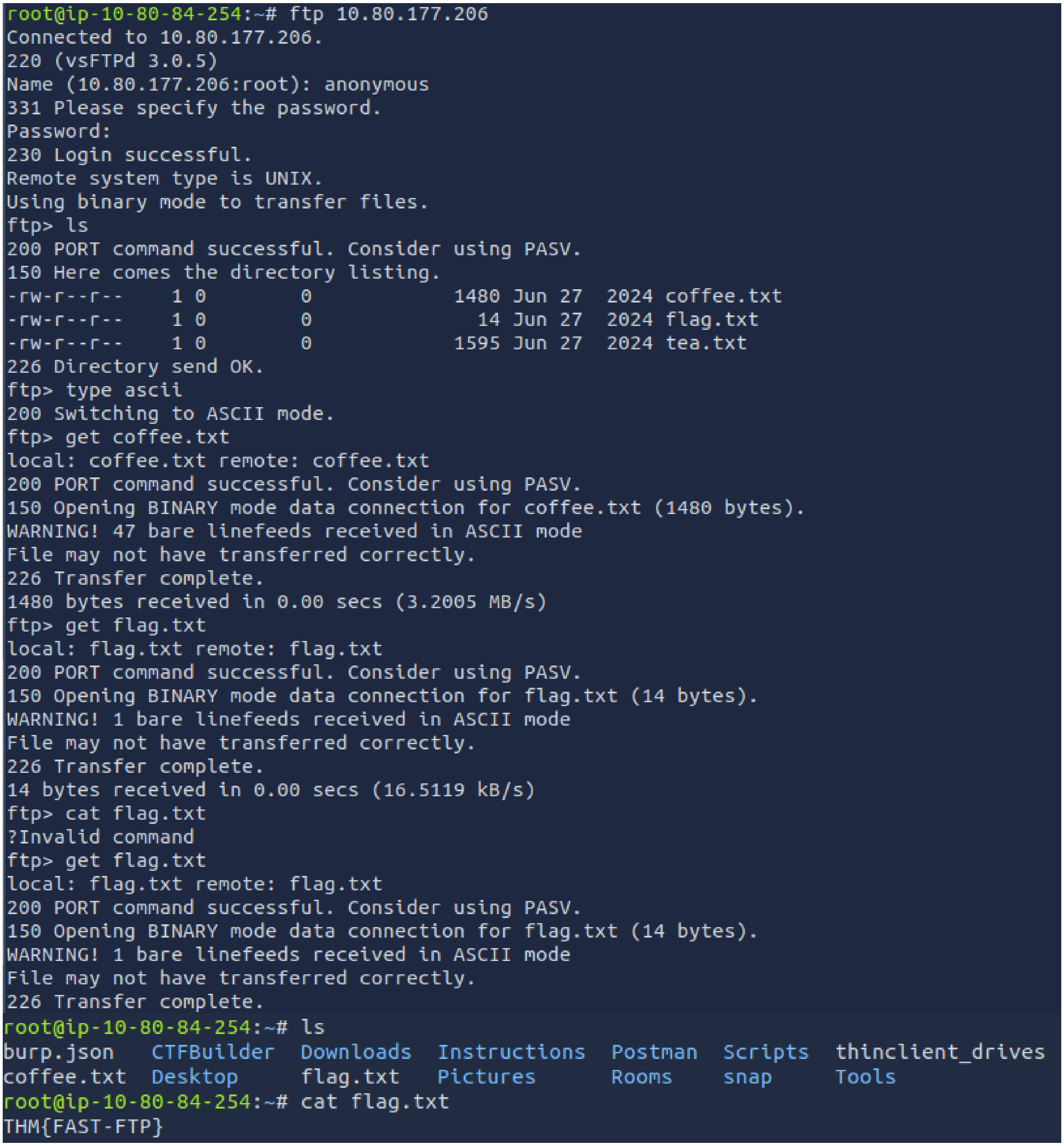
- `USER` is used to input the username
- `PASS` is used to enter the password
- `RETR` (retrieve) is used to download a file from the FTP server to the client.
- `STOR` (store) is used to upload a file from the client to the FTP server.

FTP server listens on TCP port **21** by default; data transfer is conducted via another connection from the client to the server.



```
root@ip-10-80-84-254:~# ftp 10.80.177.206
Connected to 10.80.177.206.
220 (vsFTPd 3.0.5)
Name (10.80.177.206:root): 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            1480 Jun 27  2024 coffee.txt
-rw-r--r--    1 0        0              14 Jun 27  2024 flag.txt
-rw-r--r--    1 0        0            1595 Jun 27  2024 tea.txt
226 Directory send OK.
ftp> type ascii
200 Switching to ASCII mode.
ftp> get coffee.txt
local: coffee.txt remote: coffee.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for coffee.txt (1480 bytes).
WARNING! 47 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
1480 bytes received in 0.00 secs (3.2005 MB/s)
```

we connected to the ftp server using credentials, then used ls command to list contents in directory, I used the type command to switch to ascii as this is a text file then used get [filename] to retrieve the file I want



```
root@ip-10-80-84-254:~# ftp 10.80.177.206
Connected to 10.80.177.206.
220 (vsFTPd 3.0.5)
Name (10.80.177.206:root): 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            1480 Jun 27  2024 coffee.txt
-rw-r--r--    1 0        0              14 Jun 27  2024 flag.txt
-rw-r--r--    1 0        0            1595 Jun 27  2024 tea.txt
226 Directory send OK.
ftp> type ascii
200 Switching to ASCII mode.
ftp> get coffee.txt
local: coffee.txt remote: coffee.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for coffee.txt (1480 bytes).
WARNING! 47 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
1480 bytes received in 0.00 secs (3.2005 MB/s)
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 (14 bytes).
WARNING! 1 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
14 bytes received in 0.00 secs (16.5119 kB/s)
ftp> cat flag.txt
?Invalid command
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 (14 bytes).
WARNING! 1 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
root@ip-10-80-84-254:~# ls
burp.json   CTFBuilder  Downloads  Instructions  Postman  Scripts  thinclient_drives
coffee.txt  Desktop     flag.txt   Pictures      Rooms    snap     Tools
root@ip-10-80-84-254:~# cat flag.txt
THM{FAST-FTP}
```

i did the same for the flag.txt file to retrieve the flag once i downloaded i went back to my root and the file had downloaded and i could open it up with the cat command

SMTP (Simple Mail Transfer Protocol)

defines how a mail client talks with a mail server and how a mail server talks with another.

some of the commands used by your mail client when it transfers an email to an SMTP server:

- `HELO` or `EHLO` initiates an SMTP session
- `MAIL FROM` specifies the sender’s email address

- `RCPT TO` specifies the recipient’s email address
- `DATA` indicates that the client will begin sending the content of the email message
- `.` is sent on a line by itself to indicate the end of the email message

The SMTP server listens on TCP port **25** by default.

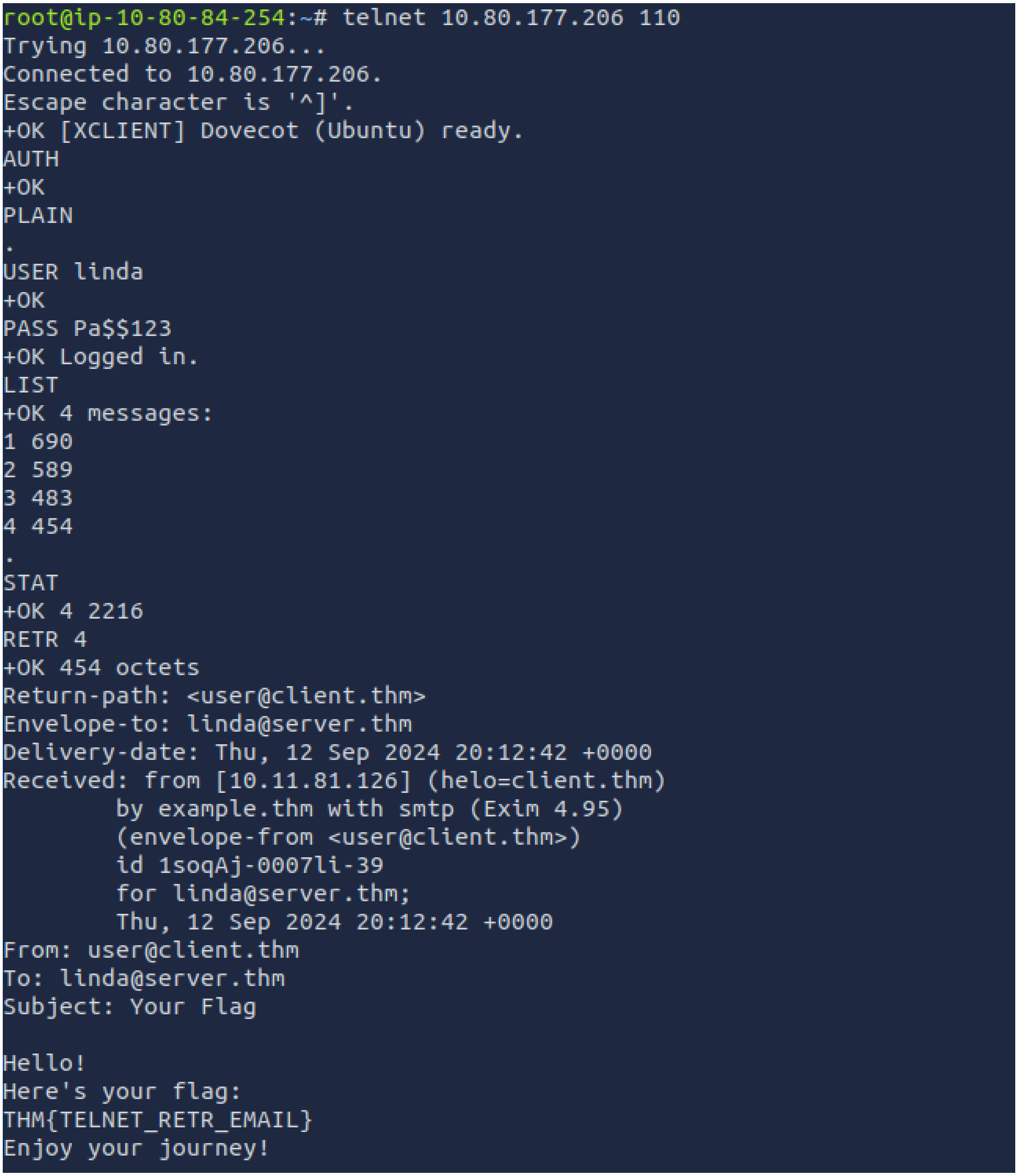
POP3 - The Post Office Protocol version 3

designed to allow the client to communicate with a mail server and retrieve email messages. An email client sends its messages by relying on SMTP and retrieves them using POP3.

Some common POP3 commands are:

- `USER <username>` identifies the user
- `PASS <password>` provides the user’s password
- `STAT` requests the number of messages and total size
- `LIST` lists all messages and their sizes
- `RETR <message_number>` retrieves the specified message
- `DELE <message_number>` marks a message for deletion
- `QUIT` ends the POP3 session applying changes, such as deletions

POP3 server listens on TCP port **110** by default



```
root@ip-10-80-84-254:~# telnet 10.80.177.206 110
Trying 10.80.177.206...
Connected to 10.80.177.206.
Escape character is '^]'.
+OK [XCLIENT] Dovecot (Ubuntu) ready.
AUTH
+OK
PLAIN
.
USER linda
+OK
PASS Pa$$123
+OK Logged in.
LIST
+OK 4 messages:
1 690
2 589
3 483
4 454
.
STAT
+OK 4 2216
RETR 4
+OK 454 octets
Return-path: <user@client.thm>
Envelope-to: linda@server.thm
Delivery-date: Thu, 12 Sep 2024 20:12:42 +0000
Received: from [10.11.81.126] (helo=client.thm)
        by example.thm with smtp (Exim 4.95)
        (envelope-from <user@client.thm>)
        id 1soqAj-0007li-39
        for linda@server.thm;
        Thu, 12 Sep 2024 20:12:42 +0000
From: user@client.thm
To: linda@server.thm
Subject: Your Flag

Hello!
Here's your flag:
THM{TELNET_RETR_EMAIL}
Enjoy your journey!
```

Here I used telnet [target ip] and pop3 portnumber to access the POP3 server
i used the AUTH command to authorise the server connection and then used USER and PASS commands with credentials provided to log in. I then could use the LIST command to see the amount of messages and then the RETR command followed by the number of the message i wanted to open which provided me the flag.

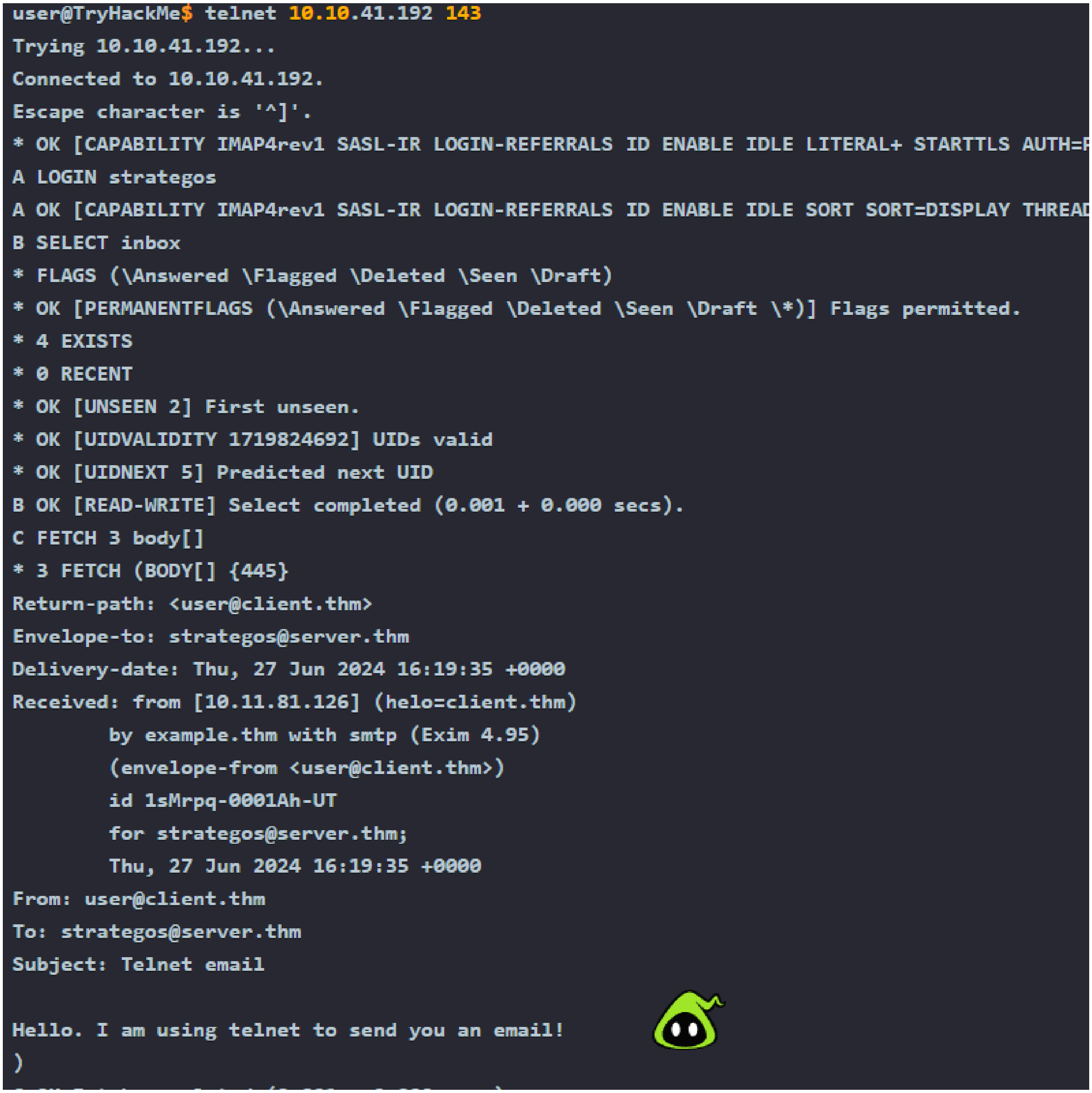
IMAP - Internet Message Access Protocol

Allows synchronizing read, moved, and deleted messages. Convenient when you check your email via multiple clients.

The IMAP protocol commands are more complicated than the POP3 protocol commands.

- `LOGIN <username> <password>` authenticates the user
- `SELECT <mailbox>` selects the mailbox folder to work with
- `FETCH <mail_number> <data_item_name>` Example `fetch 3 body[]` to fetch message number 3, header and body.
- `MOVE <sequence_set> <mailbox>` moves the specified messages to another mailbox
- `COPY <sequence_set> <data_item_name>` copies the specified messages to another mailbox
- `LOGOUT` logs out

IMAP server listens on TCP port **143** by default



```
user@TryHackMe$ telnet 10.10.41.192 143
Trying 10.10.41.192...
Connected to 10.10.41.192.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE LITERAL+ STARTTLS AUTH=P
A LOGIN strategos
A OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE SORT SORT=DISPLAY THREAD
B SELECT inbox
* FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
* OK [PERMANENTFLAGS (\Answered \Flagged \Deleted \Seen \Draft \*)] Flags permitted.
* 4 EXISTS
* 0 RECENT
* OK [UNSEEN 2] First unseen.
* OK [UIDVALIDITY 1719824692] UIDs valid
* OK [UIDNEXT 5] Predicted next UID
B OK [READ-WRITE] Select completed (0.001 + 0.000 secs).
C FETCH 3 body[]
* 3 FETCH (BODY[] {445}
Return-path: <user@client.thm>
Envelope-to: strategos@server.thm
Delivery-date: Thu, 27 Jun 2024 16:19:35 +0000
Received: from [10.11.81.126] (helo=client.thm)
        by example.thm with smtp (Exim 4.95)
        (envelope-from <user@client.thm>)
        id 1sMrpq-0001Ah-UT
        for strategos@server.thm;
        Thu, 27 Jun 2024 16:19:35 +0000
From: user@client.thm
To: strategos@server.thm
Subject: Telnet email

Hello. I am using telnet to send you an email!
)
```

Protocols covered and their ports

Protocol	Transport Protocol	Default Port Number
TELNET	TCP	23
DNS	UDP or TCP	53
HTTP	TCP	80
HTTPS	TCP	443
FTP	TCP	21
SMTP	TCP	25

Protocol	Transport Protocol	Default Port Number
POP3	TCP	110
IMAP	TCP	143