Protocols & Servers 2

Before going further lets address 2 very important security perspectives.
CIA TRIAD: DEFENCE

1. **Confidentiality**
2. **Integrity**
3. **Availability**

DAD TRIAD: OFFENCE

1. **Disclosure**
2. **Alteration**
3. **Destruction**

DAD is all about exploiting and causing damage, whereas CIA is a security model to protect against such attacks.
These attacks directly affect the security of the system, such as:

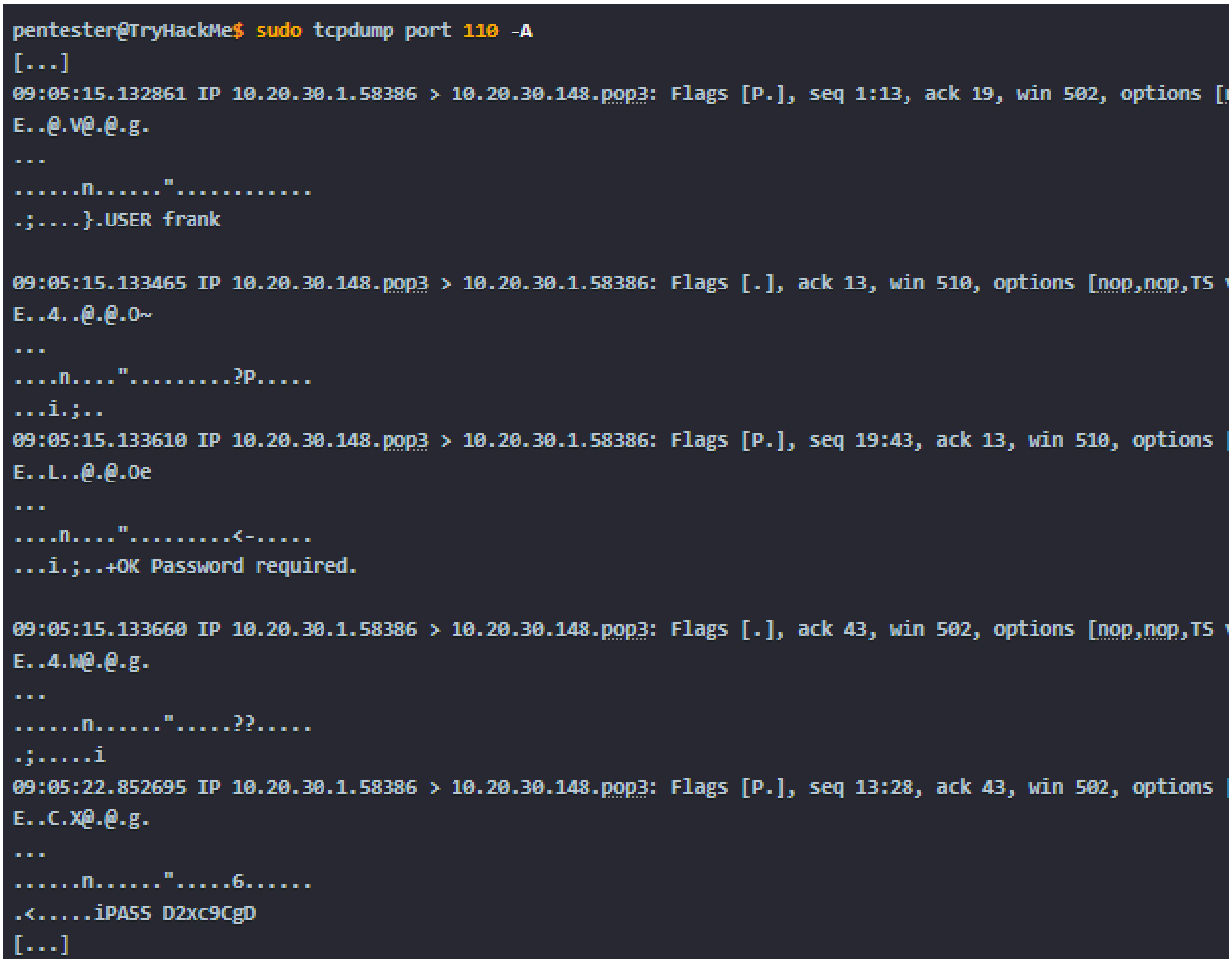
1. **Sniffing Attack (Network packet capture)**
2. **Man-In-The-Middle (MITM) Attack**
3. **Password Attack (Authentication Attack)**
4. **Vulnerabilities**

Sniffing Attack:
This attack refers to using a network capture packet tool eg. BURP SUITE, which we have used. To collect information about the target. When a protocol communicates in clear text the data exchanged is captured by third parties to analyse. This could be credentials, login information if the data is NOT encrypted in transit.

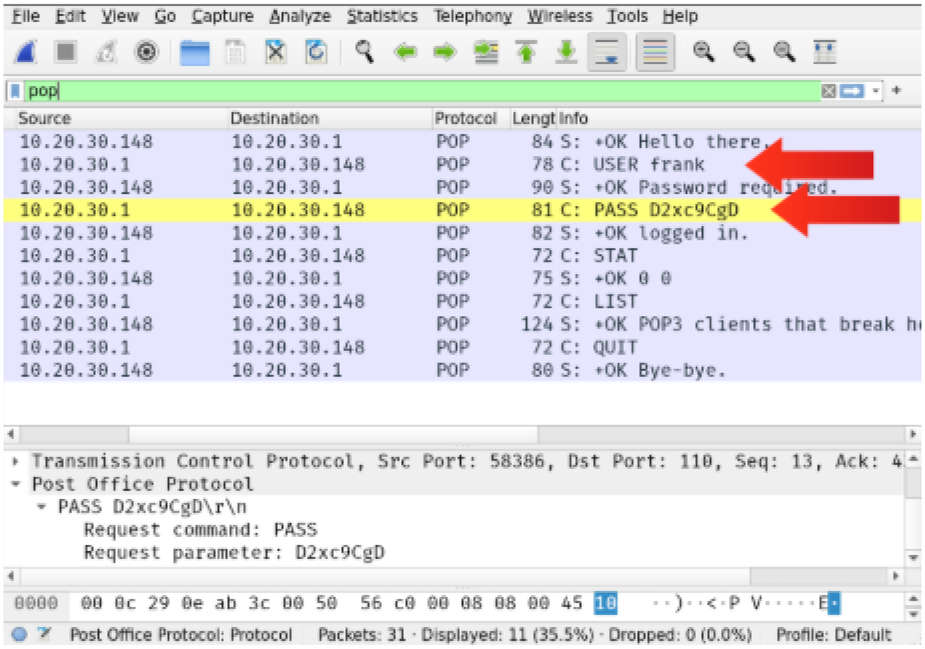
A sniffing attack can be conducted using an **ethernet (802.3) network card, that has proper permissions on Linux and administrator on MS windows.** Applications are:

1. **Tcpdump** free open source CLI that has been ported to many OS.
2. **Wireshark** familiar to me, GUI program available to capture network packets inc, Linux /MacOS and MS windows.
3. **Tshark** CLI alternative to wireshark.

An example, is someone checking their email messages using POP3, using Tcpdump to attempt to capture the username and password. If we put in the terminal: **sudo tcpdump port 110 -A** this attack requires access to network traffic, eg, using wiretap or switch with port mirroring
Sudo - **Captures root privileges. POP3 = port 110. -A = Ascii text format.**

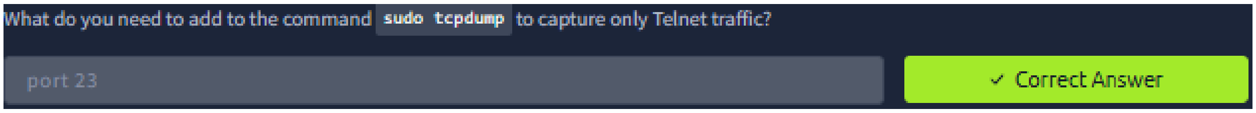


```
pentester@TryHackMe$ sudo tcpdump port 110 -A
[...]
09:05:15.132861 IP 10.20.30.1.58386 > 10.20.30.148.pop3: Flags [P.], seq 1:13, ack 19, win 502, options [
E..@.V@.@.g.
...
......n......"...........
.;....}.USER frank

09:05:15.133465 IP 10.20.30.148.pop3 > 10.20.30.1.58386: Flags [.], ack 13, win 510, options [nop,nop,TS
E..4..@.@.O~
...
....n...."........?P.....
...i.;..
09:05:15.133610 IP 10.20.30.148.pop3 > 10.20.30.1.58386: Flags [P.], seq 19:43, ack 13, win 510, options
E..L..@.@.Oe
...
....n...."........<-.....
...i.;..+OK Password required.

09:05:15.133660 IP 10.20.30.1.58386 > 10.20.30.148.pop3: Flags [.], ack 43, win 502, options [nop,nop,TS
E..4.W@.@.g.
...
......n......"....??.....
.;.....i
09:05:22.852695 IP 10.20.30.1.58386 > 10.20.30.148.pop3: Flags [P.], seq 13:28, ack 43, win 502, options
E..C.X@.@.g.
...
......n......"....6......
.<.....iPASS D2xc9CgD
[...]
```


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
pop

```
Source          Destination     Protocol Lengt Info
10.20.30.148    10.20.30.1      POP       84 S: +OK Hello there.
10.20.30.1      10.20.30.148    POP       78 C: USER frank
10.20.30.148    10.20.30.1      POP       90 S: +OK Password required.
10.20.30.1      10.20.30.148    POP       81 C: PASS D2xc9CgD
10.20.30.148    10.20.30.1      POP       82 S: +OK logged in.
10.20.30.1      10.20.30.148    POP       72 C: STAT
10.20.30.148    10.20.30.1      POP       75 S: +OK 0 0
10.20.30.1      10.20.30.148    POP       72 C: LIST
10.20.30.148    10.20.30.1      POP      124 S: +OK POP3 clients that break h
10.20.30.1      10.20.30.148    POP       72 C: QUIT
10.20.30.148    10.20.30.1      POP       80 S: +OK Bye-bye.

▸ Transmission Control Protocol, Src Port: 58386, Dst Port: 110, Seq: 13, Ack: 4
▾ Post Office Protocol
  ▾ PASS D2xc9CgD\r\n
      Request command: PASS
      Request parameter: D2xc9CgD

0000  00 0c 29 0e ab 3c 00 50  56 c0 00 08 08 00 45 10   ··)··<·P V·····E·

Post Office Protocol: Protocol   Packets: 31 · Displayed: 11 (35.5%) · Dropped: 0 (0.0%)   Profile: Default
```

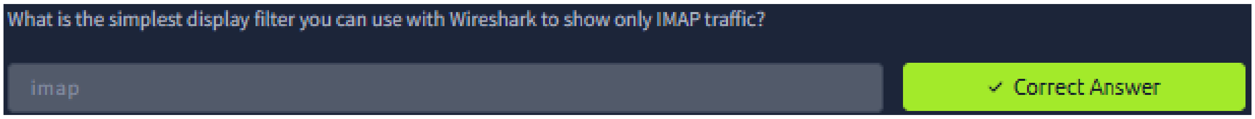
Wireshark capture: Being used in this example show us in raw form filtered to pop which is the protocol, allows us to filter packets being sent in a POP packet. In this case we now have access to the individuals username and password in cleartext form. Not good for the user. Excellent news for us.



What do you need to add to the command `sudo tcpdump` to capture only Telnet traffic?

port 23

If we remember telnet is on port 23.



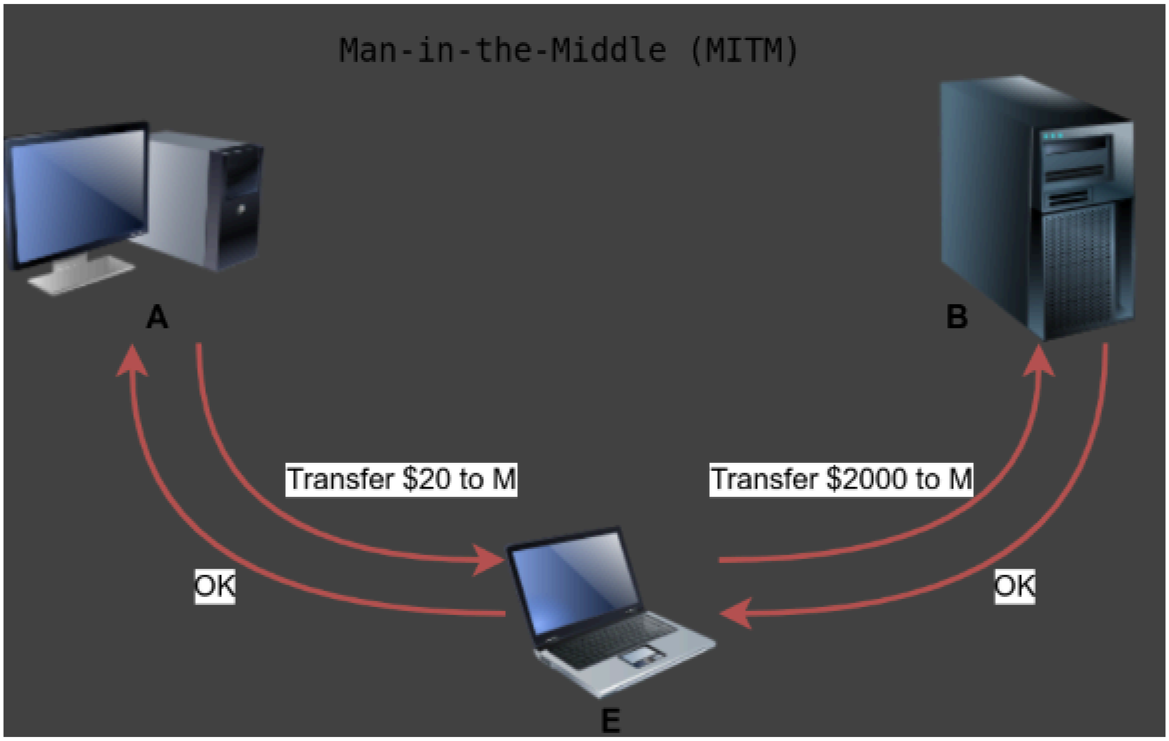
What is the simplest display filter you can use with Wireshark to show only IMAP traffic?

imap

If we want a filter for imap simply like in the pop example of wireshark we simply change it to imap! That will display only imap packets.

Man-In-The-Middle Attacks (MITM)

Which we have simulated using Burp Suite, it occurs when victim A believes they are communicating with a legitimate destination B but they are unknowingly communicating with an attacker E. See figure below.



Attack is simply to carry out if the two parties do **not** confirm the authenticity and integrity of each other. Sometimes the chosen protocol does not provide secure authentication or integrity checking. Those insecurities let loose attacks like this occur.

Any time you browse over HTTP, you are susceptible to a MITM attack. Scary thing is you cannot recognise it. Many tools aid this such as:

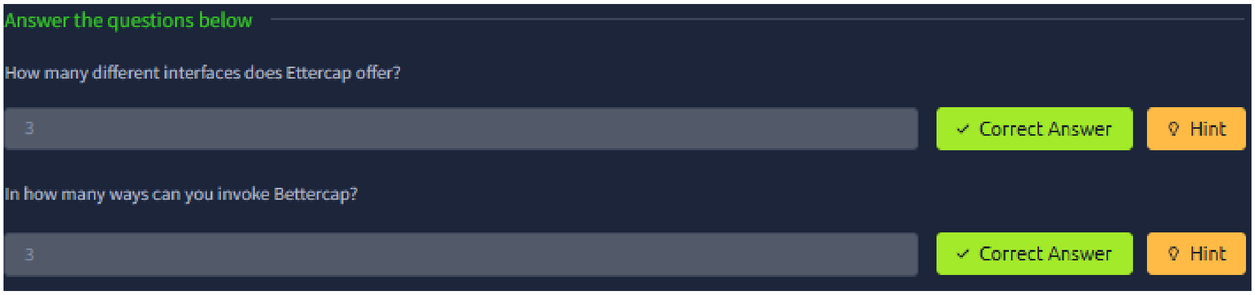
1. **Ettercap**
2. **Bettercap**

MITM also affect cleartext protocols such as:

1. **FTP**
2. **SMTP**
3. **POP3**

MITIGATION:

1. **Cryptology:** Using public key infrastructure **PKI** and trusted root certificates eg **TLS** (transport layer security). - HTTPS



Answer the questions below

How many different interfaces does Ettercap offer?

3

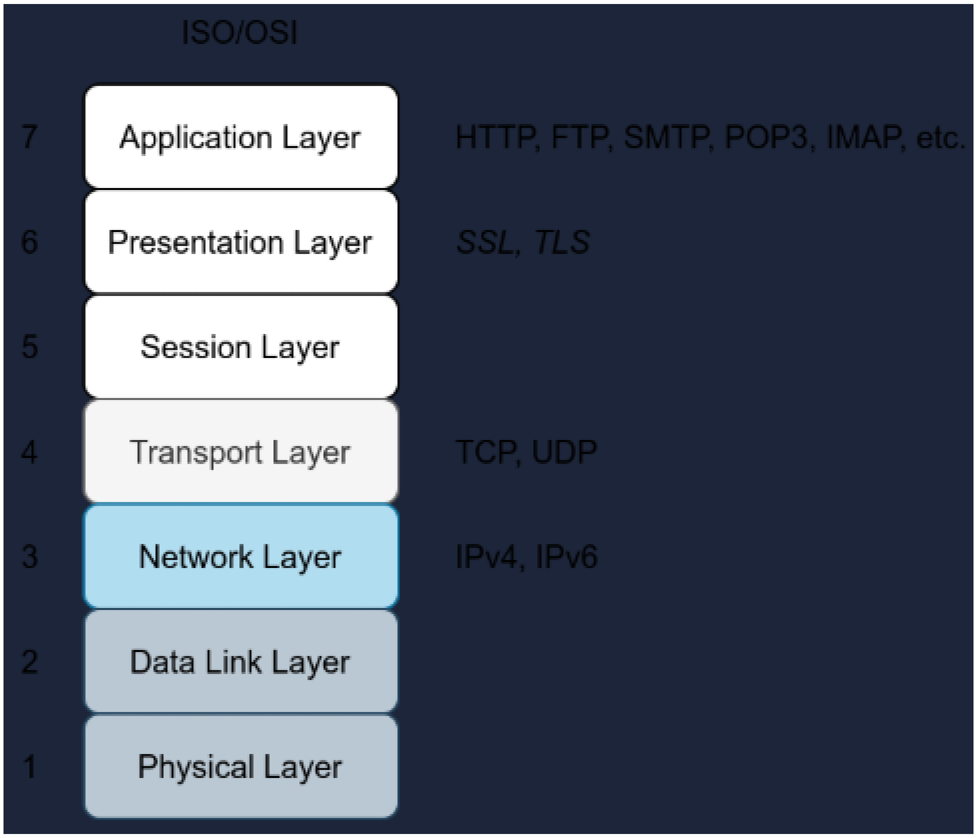
In how many ways can you invoke Bettercap?

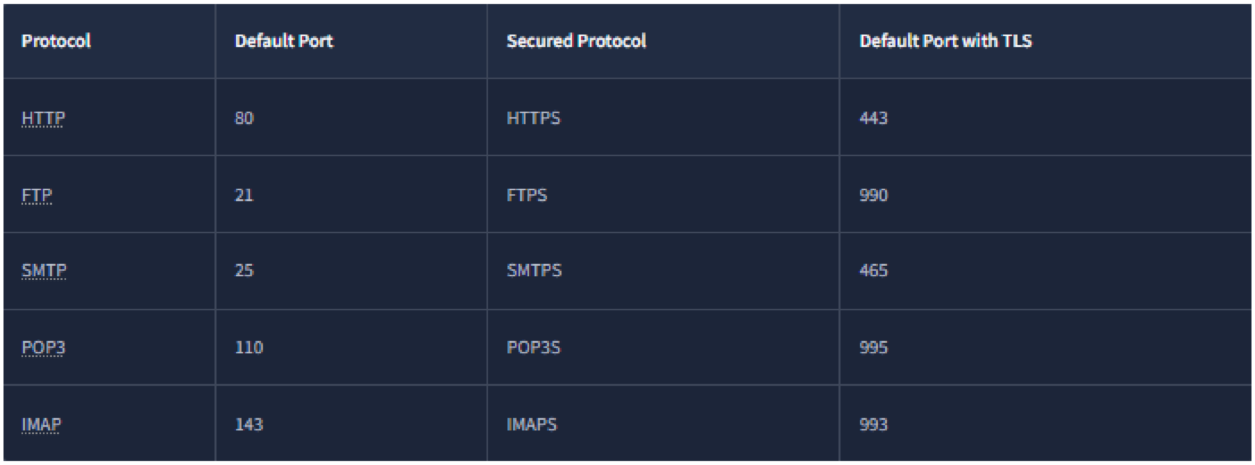
3

Transport Layer Security (TLS)

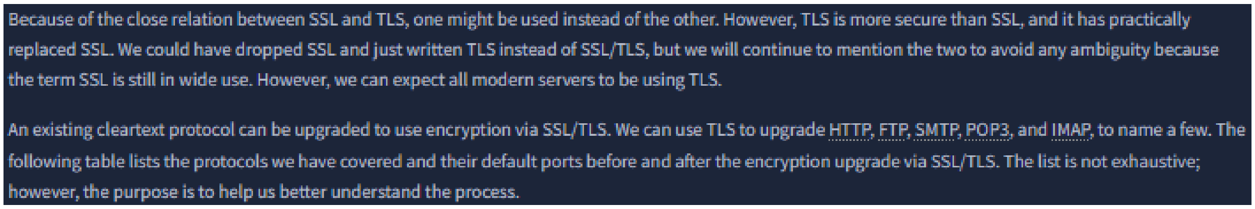
We did mention this briefly, protecting against MITM attacks. Protocols such as **SSL - Secure Sockets Layer** started when the world wide web was starting to see new applications such as online shopping and sending payments information.

Netscape introduced SSL in 1994 with SSL 3.0 being released in 1996. Eventually more security was needed and **TSL was introduced in 1999.**


ISO/OSI
7 Application Layer HTTP, FTP, SMTP, POP3, IMAP, etc.
6 Presentation Layer SSL, TLS
5 Session Layer
4 Transport Layer TCP, UDP
3 Network Layer IPv4, IPv6
2 Data Link Layer
1 Physical Layer



Protocol	Default Port	Secured Protocol	Default Port with TLS
HTTP	80	HTTPS	443
FTP	21	FTPS	990
SMTP	25	SMTPS	465
POP3	110	POP3S	995
IMAP	143	IMAPS	993



Because of the close relation between SSL and TLS, one might be used instead of the other. However, TLS is more secure than SSL, and it has practically replaced SSL. We could have dropped SSL and just written TLS instead of SSL/TLS, but we will continue to mention the two to avoid any ambiguity because the term SSL is still in wide use. However, we can expect all modern servers to be using TLS.

An existing cleartext protocol can be upgraded to use encryption via SSL/TLS. We can use TLS to upgrade HTTP, FTP, SMTP, POP3, and IMAP, to name a few. The following table lists the protocols we have covered and their default ports before and after the encryption upgrade via SSL/TLS. The list is not exhaustive; however, the purpose is to help us better understand the process.

Considering HTTP, initially retrieves a webpage over HTTP the web browser would need at least perform the following 2 steps:

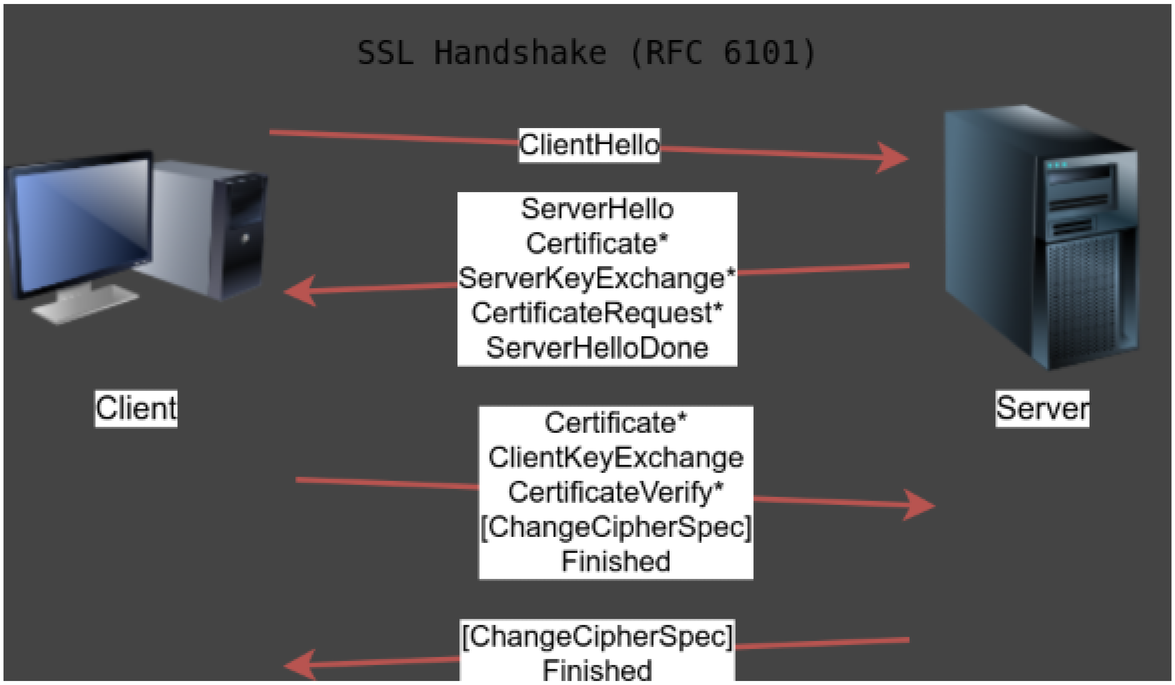
1. **Establish TCP connection**
2. **Send HTTP request to web server such as GET and POST requests**

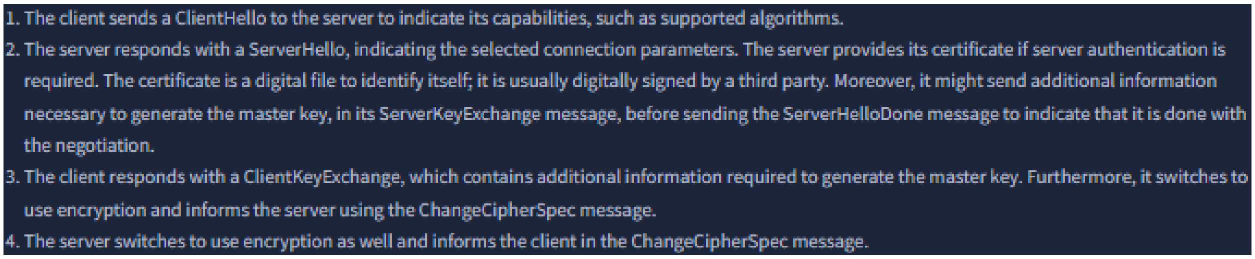
HTTPS on the other hand, needs an additional step to encrypt the traffic. They are:

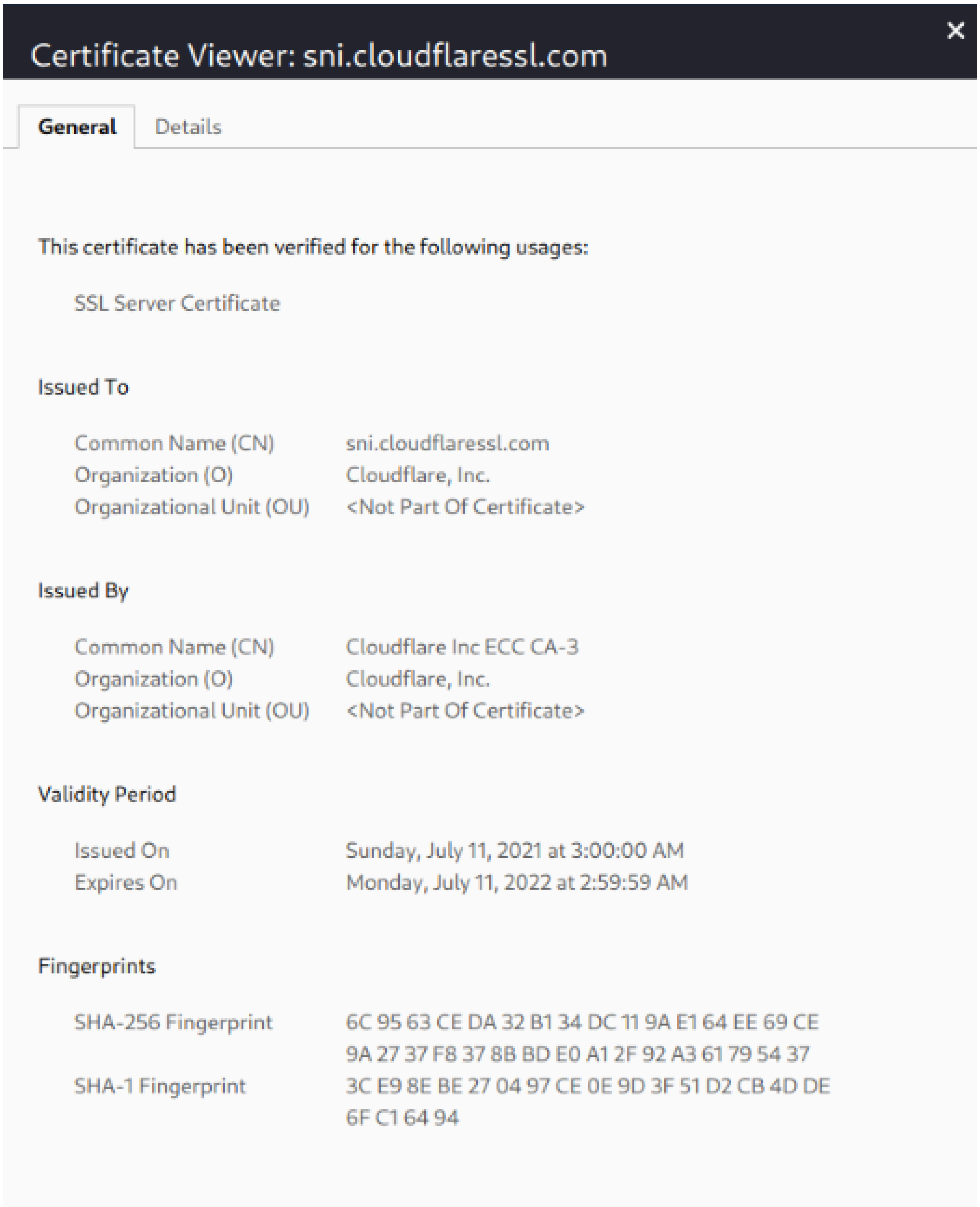
1. **Establish TCP connection**
2. **Establish SSL/TLS connection**
3. **Sent HTTP requests to web server.**

How to establish SSL/TSL connection:

Client needs to perform proper handshake with the server based off RFC 6101. See image below.




1. The client sends a ClientHello to the server to indicate its capabilities, such as supported algorithms.
2. The server responds with a ServerHello, indicating the selected connection parameters. The server provides its certificate if server authentication is required. The certificate is a digital file to identify itself; it is usually digitally signed by a third party. Moreover, it might send additional information necessary to generate the master key, in its ServerKeyExchange message, before sending the ServerHelloDone message to indicate that it is done with the negotiation.
3. The client responds with a ClientKeyExchange, which contains additional information required to generate the master key. Furthermore, it switches to use encryption and informs the server using the ChangeCipherSpec message.
4. The server switches to use encryption as well and informs the client in the ChangeCipherSpec message.



Certificate Viewer: sni.cloudflaressl.com

This certificate has been verified for the following usages:

SSL Server Certificate

Issued To

Common Name (CN)	sni.cloudflaressl.com
Organization (O)	Cloudflare, Inc.
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	Cloudflare Inc ECC CA-3
Organization (O)	Cloudflare, Inc.
Organizational Unit (OU)	<Not Part Of Certificate>

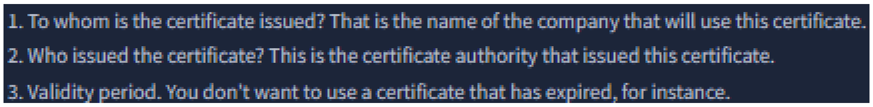
Validity Period

Issued On	Sunday, July 11, 2021 at 3:00:00 AM
Expires On	Monday, July 11, 2022 at 2:59:59 AM

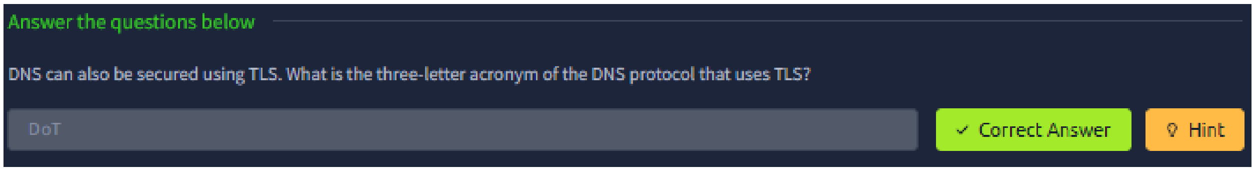
Fingerprints

SHA-256 Fingerprint	6C 95 63 CE DA 32 B1 34 DC 11 9A E1 64 EE 69 CE 9A 27 37 F8 37 8B BD E0 A1 2F 92 A3 61 79 54 37
SHA-1 Fingerprint	3C E9 8E BE 27 04 97 CE 0E 9D 3F 51 D2 CB 4D DE 6F C1 64 94

Above figure shows:



1. To whom is the certificate issued? That is the name of the company that will use this certificate.
2. Who issued the certificate? This is the certificate authority that issued this certificate.
3. Validity period. You don't want to use a certificate that has expired, for instance.



Answer the questions below

DNS can also be secured using TLS. What is the three-letter acronym of the DNS protocol that uses TLS?

DoT

DOT = **DNS over TSL.**

SSH - Secure Shell

Created to provide a secure way for remote system admin. Lets you securely connect to another system over the network and execute commands on a remote system. **SH = Shell and S = Secure.**

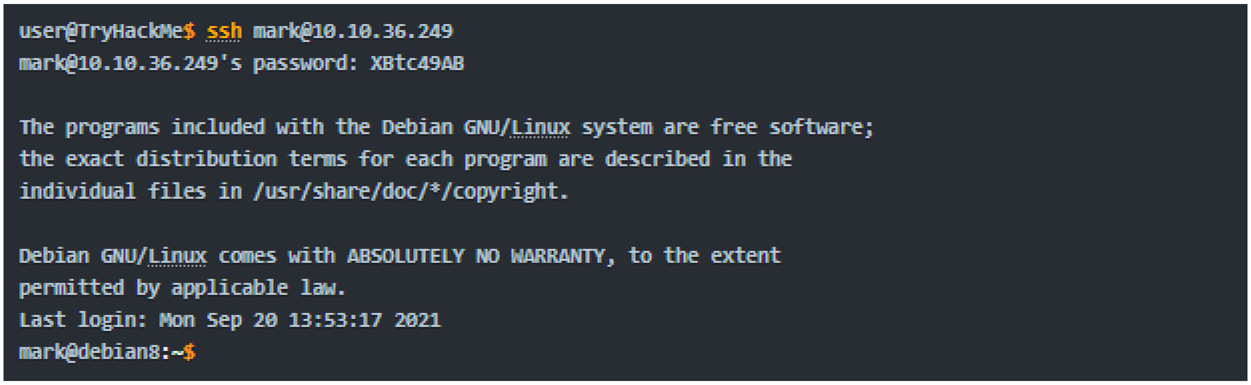
Can be summarized as:

1. **Confirm identity of remote server**
2. **Exchanged messages are encrypted and only decrypted by intended recipient**
3. **Both sides can detect any modification in the messages**

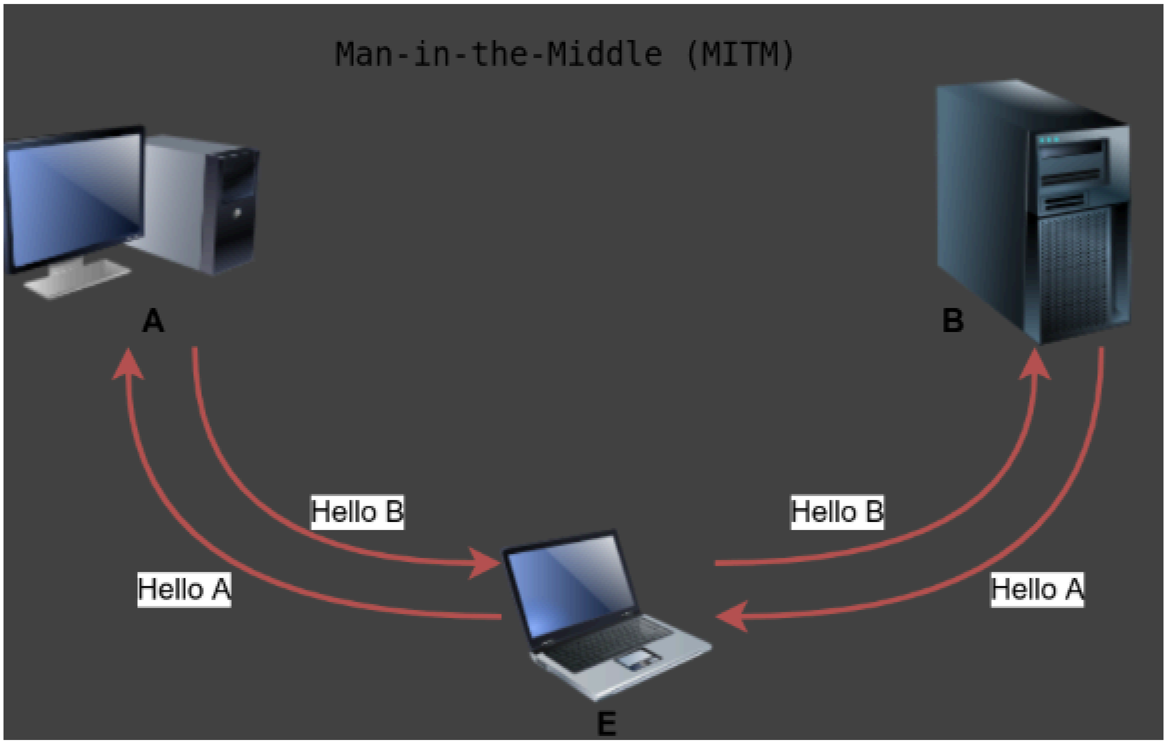
These 3 points are ensured by **cryptology. Part of Confidentiality and integrity.**

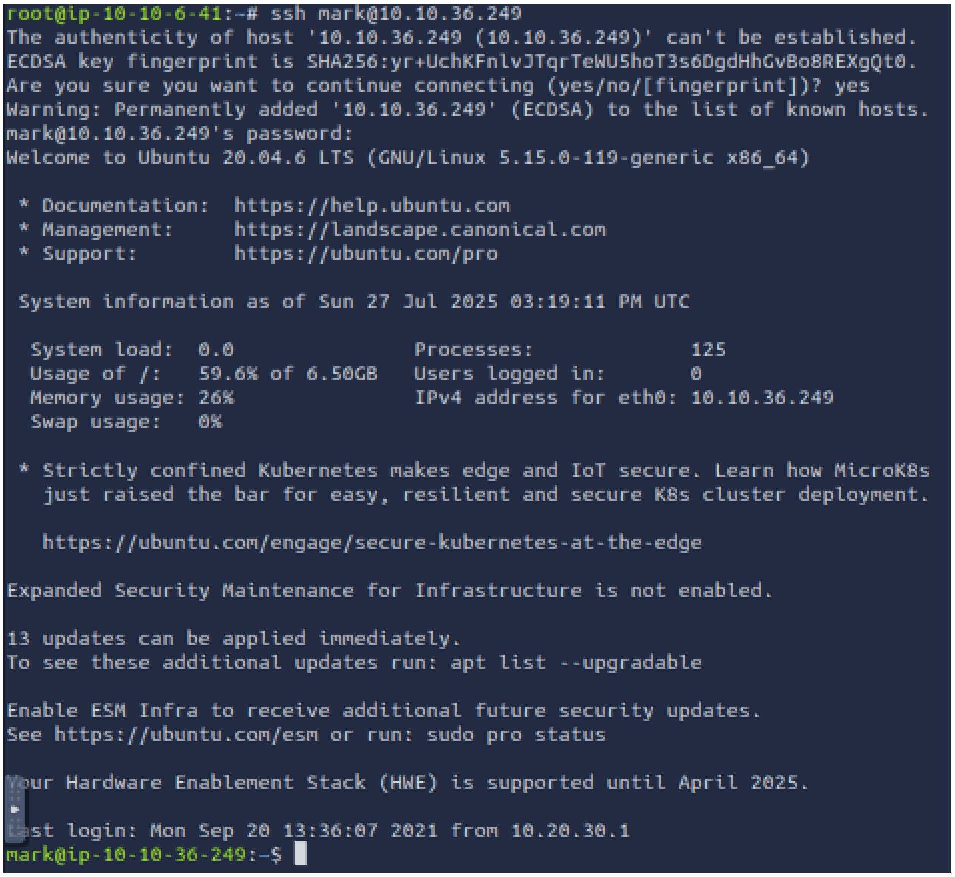
To use SSH you need an SSH server and an SSH client. SSH listens on port 22 by default and requires

1. **A username and password**
2. **Private and public key**



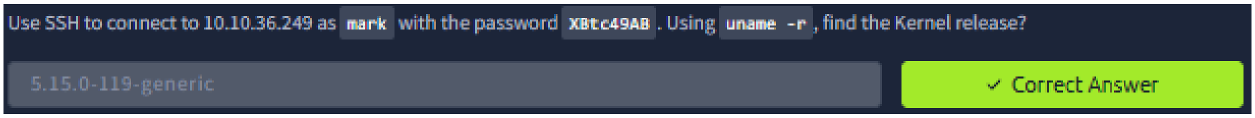
```
user@TryHackMe$ ssh mark@10.10.36.249
mark@10.10.36.249's password: XBtc49AB

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Sep 20 13:53:17 2021
mark@debian8:~$
```





```
root@ip-10-10-6-41:~# ssh mark@10.10.36.249
The authenticity of host '10.10.36.249 (10.10.36.249)' can't be established.
ECDSA key fingerprint is SHA256:yr+UchKFnlvJTqrTeWU5hoT3s6DgdHhGvBo8REXgQt0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.36.249' (ECDSA) to the list of known hosts.
mark@10.10.36.249's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-119-generic x86_64)

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

 System information as of Sun 27 Jul 2025 03:19:11 PM UTC

  System load:  0.0               Processes:             125
  Usage of /:   59.6% of 6.50GB   Users logged in:       0
  Memory usage: 26%               IPv4 address for eth0: 10.10.36.249
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Infrastructure is not enabled.

13 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Infra to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Your Hardware Enablement Stack (HWE) is supported until April 2025.

Last login: Mon Sep 20 13:36:07 2021 from 10.20.30.1
mark@ip-10-10-36-249:~$
```

Here in this example we have securely logged in as a user.

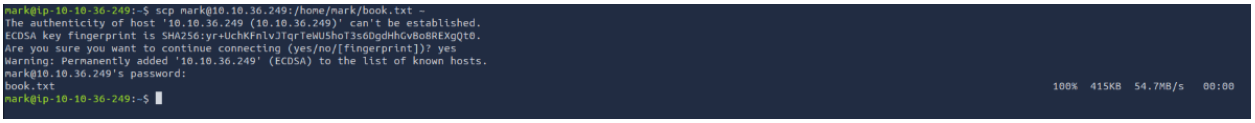


Use SSH to connect to 10.10.36.249 as `mark` with the password `XBtc49AB`. Using `uname -r`, find the Kernel release?

5.15.0-119-generic

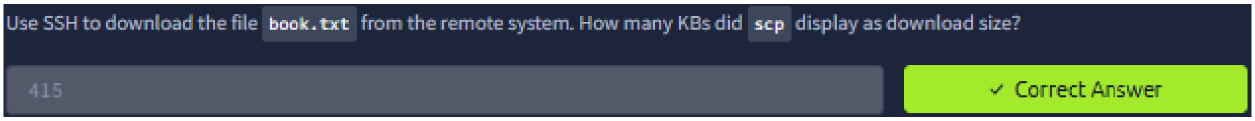
We can see this is identified in the top GNU/Linux area, that shows the kernel version.

scp mark@10.10.36.249:/home/mark/book.txt ~



```
mark@ip-10-10-36-249:~$ scp mark@10.10.36.249:/home/mark/book.txt ~
The authenticity of host '10.10.36.249 (10.10.36.249)' can't be established.
ECDSA key fingerprint is SHA256:yr+UchKFnlvJTqrTeWUShoT3s6DgdHhGvBo8REXgQt0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.36.249' (ECDSA) to the list of known hosts.
mark@10.10.36.249's password:
book.txt                                                                     100%  415KB  54.7MB/s   00:00
mark@ip-10-10-36-249:~$
```

So what’s interesting here is I needed to enter the credentials in before it would allow me to download it. This is much different than when we were using telnet. There wasn’t nearly as much security. I can certainly tell the difference here.

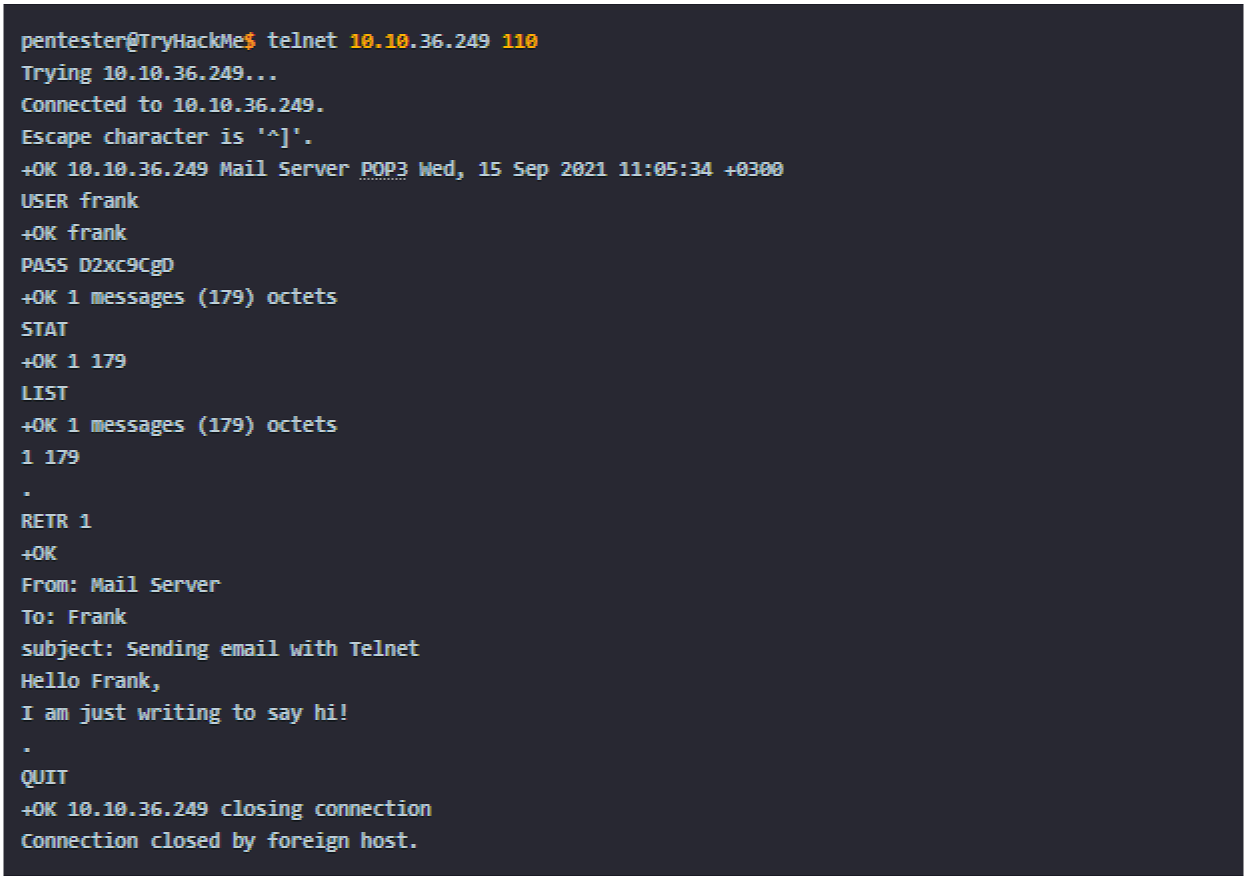


Use SSH to download the file `book.txt` from the remote system. How many KBs did `scp` display as download size?

415

Password Attack:

Many protocols require authentication proving you are who you claim to be. When using protocols such as POP3 we should not be given access to the mailbox before verifying our identity.



```
pentester@TryHackMe$ telnet 10.10.36.249 110
Trying 10.10.36.249...
Connected to 10.10.36.249.
Escape character is '^]'.
+OK 10.10.36.249 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 10.10.36.249 closing connection
Connection closed by foreign host.
```

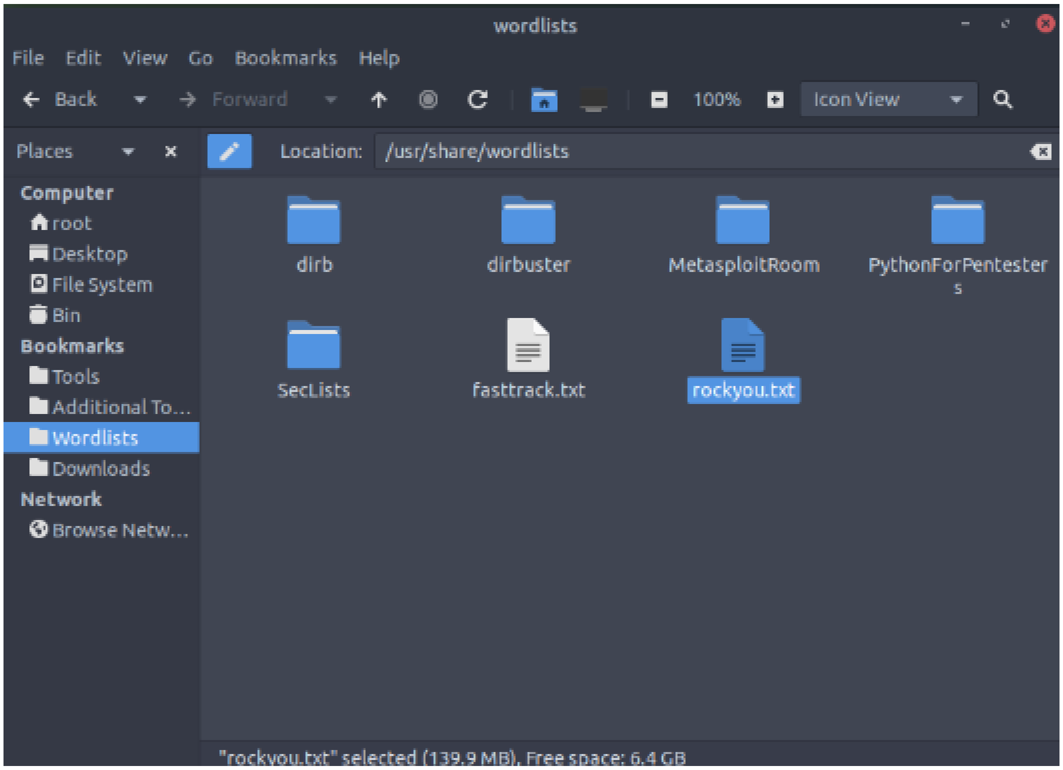
Authentication can be achieved through one of the following or combination of 2:

1. **Something you know, password and pincode**
2. **Something you have, SIM card, RFID card and USB dongle**
3. **Something you are, such as fingerprints and iris**

This task will focus on passwords. I.e something the target knows. Attacks against passwords are usually carried out by:

1. **Password guessing**
2. **Dictionary attacks**
3. **Brute Force attacks**

Let's focus on dictionary attacks, eg using RockYou's list of breached passwords.

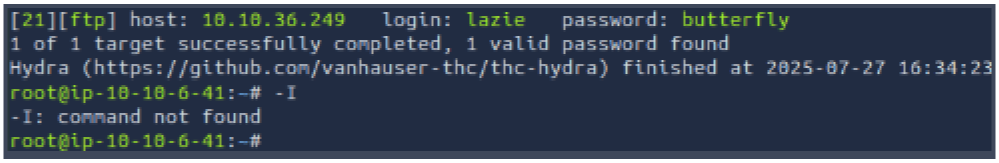


Location: /usr/share/wordlists

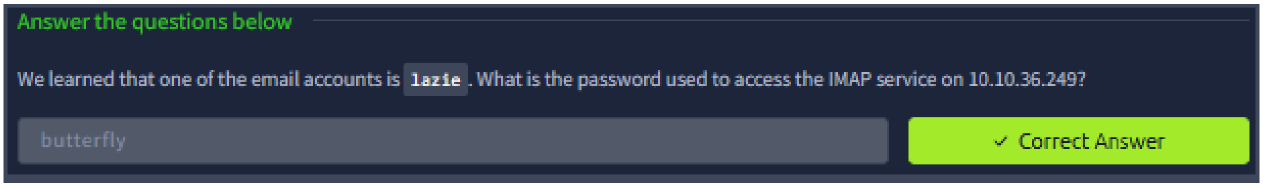
"rockyou.txt" selected (139.9 MB), Free space: 6.4 GB

```
hydra -l mark -P /usr/share/wordlists/rockyou.txt 10.10.36.249 ftp
```

```
hydra -l lazie -P /usr/share/wordlists/rockyou.txt 10.10.36.249 ftp
```



```
[21][ftp] host: 10.10.36.249   login: lazie   password: butterfly
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-27 16:34:23
root@ip-10-10-6-41:~# -I
-I: command not found
root@ip-10-10-6-41:~#
```

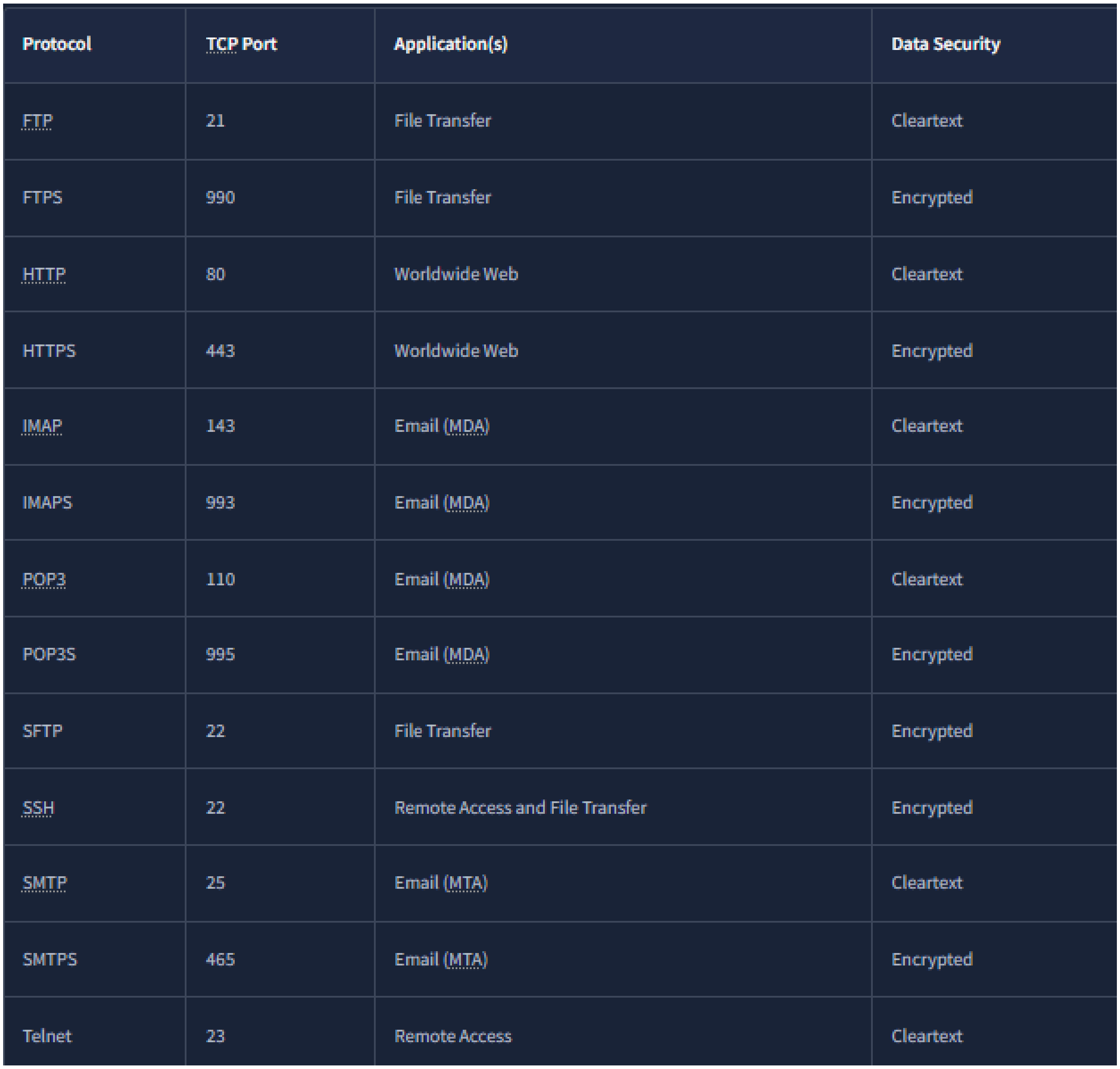


Answer the questions below

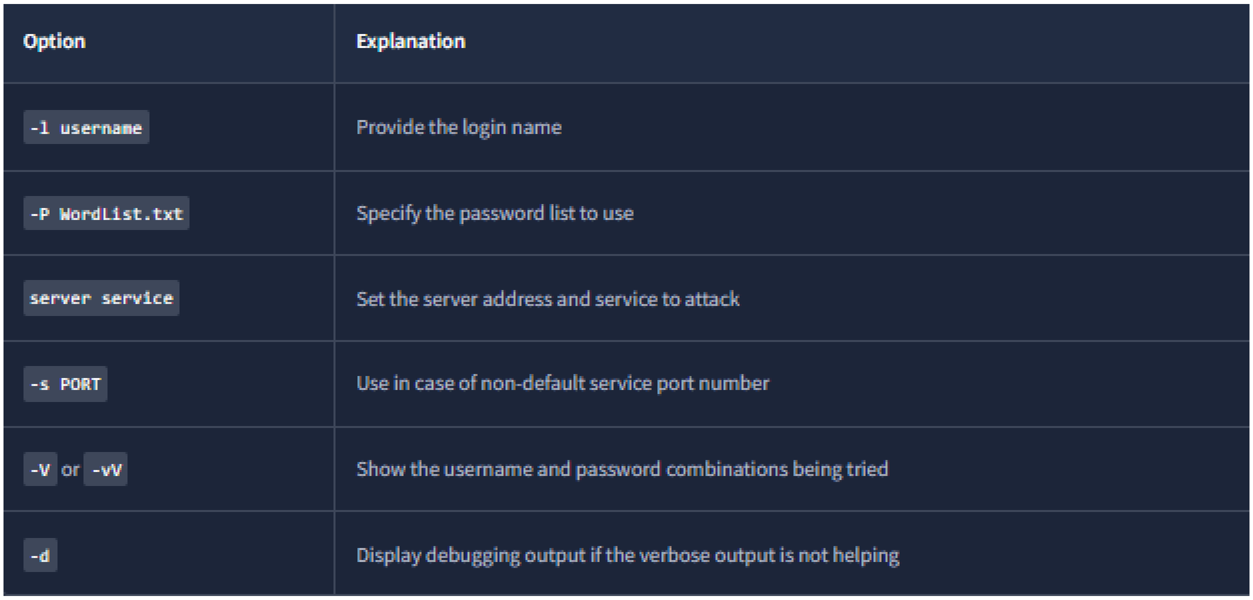
We learned that one of the email accounts is `lazie`. What is the password used to access the IMAP service on 10.10.36.249?

butterfly

Hahaha… So using the prebuilt fabricated wordlist we were able to launch an attack using the users username as the default and then using the wordlists/rockyou.txt to go through all the commonly used nicknames. I also took initiative and picked up a wordlist 100k password for myself to add to my tool box.



Protocol	TCP Port	Application(s)	Data Security
FTP	21	File Transfer	Cleartext
FTPS	990	File Transfer	Encrypted
HTTP	80	Worldwide Web	Cleartext
HTTPS	443	Worldwide Web	Encrypted
IMAP	143	Email (MDA)	Cleartext
IMAPS	993	Email (MDA)	Encrypted
POP3	110	Email (MDA)	Cleartext
POP3S	995	Email (MDA)	Encrypted
SFTP	22	File Transfer	Encrypted
SSH	22	Remote Access and File Transfer	Encrypted
SMTP	25	Email (MTA)	Cleartext
SMTPS	465	Email (MTA)	Encrypted
Telnet	23	Remote Access	Cleartext



Option	Explanation
`-l username`	Provide the login name
`-P WordList.txt`	Specify the password list to use
`server service`	Set the server address and service to attack
`-s PORT`	Use in case of non-default service port number
`-V` or `-vV`	Show the username and password combinations being tried
`-d`	Display debugging output if the verbose output is not helping

Conclusion:

I must say this is beginning to really open my eyes at the very real threat when it comes to hacking. Not only that but how easy it is to at least try to brute force into someone else's account by just knowing the nickname alone. I am a little concerned but at the same time amazed by how adaptable I have become at learning all this information, and seeing how it can be used for good, and for bad. But in the ethical mindset both are needed to understand the offensive and defensive strategies that stem from them.