SMTP

↳ Simple mail transfer protocol

↳ To support email services, SMTP & POP/IMAP is used.

eg:) It is similar to post service, where SMTP is like post sorting office

Pop/IMAP:

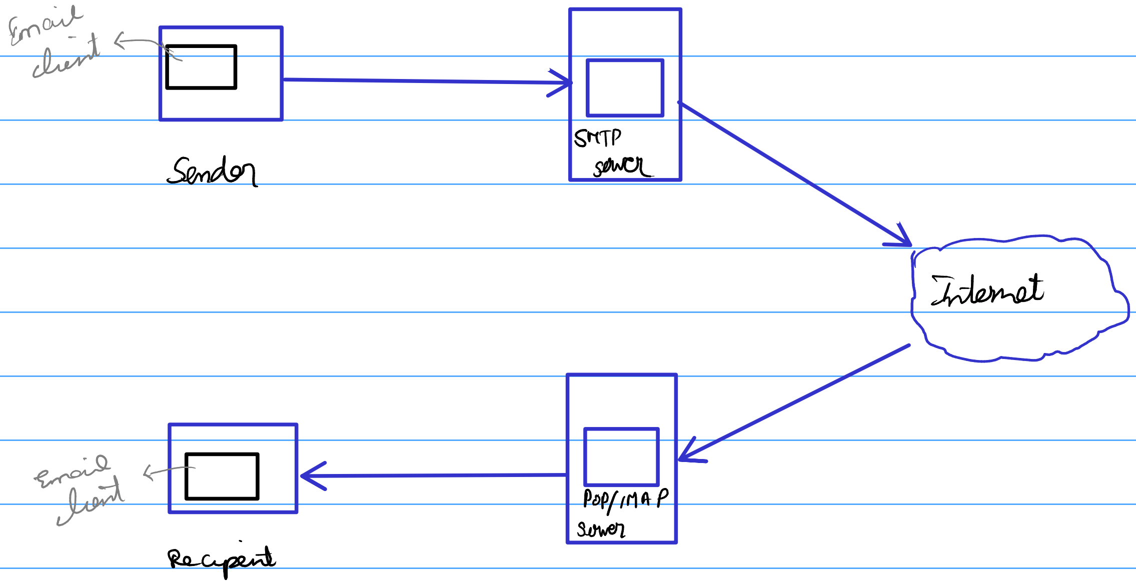
POP, or "Post Office Protocol" and IMAP, "Internet Message Access Protocol" are both email protocols who are responsible for the transfer of email between a client and a mail server. The main differences is in POP's more simplistic approach of downloading the inbox from the mail server, to the client. Where IMAP will synchronise the current inbox, with new mail on the server, downloading anything new.

Email delivery is same as the physical mail delivery, User sent email (letter) and the service (the postal delivery Servic), After a series of steps the email will reach the inbox (recepent post box)

Note:

The role of the SMTP server in this service, is to act as the sorting office, the email (letter) is picked up and sent to this server, which then directs it to the recipient.

Rough Architecture:



SMTP - Working :

i) https://computer.howstuffworks.com/e-mail-messaging/email3.htm - in simpler way

ii) https://www.afternerd.com/blog/smtp/ - In advanced way .

Enumeration :

↳ As usual, NMAP for port Scanning .

↳ SMTP_version in metasploit (Auxillary modules) scans the range of ipadd & return The versions.

↳ we can manually enumerate the user's mail address using URFY and EXPN like SMTP Commands. But it can automated by using SMTP_enum. (After Setting the param & running the module returns the usernames (i.e) email ID's).

↳ confirm the existence of that email ID

Here, for this model we need to give username wordlist file to bruteforce.

↳ SMTP_user_enum → non metasploit tool may also used

During pentesting we need to pivot the vulnerablites & exploit it further

↳ Here, in this THM eg) During nmap Scan we came to know that other services (SSH) is running the vulnerable machine.

↳ So, we try to use username we got from SMTP for login into SSH & bruteforce the password.

↳ We use HYDRA to achieve that,

Hydra :

Usage : Hydra <options> <ip> <protocol>

hydra --help for more info

eg) hydra -t 5 -l user -P /wordlist.txt -vV 10.1.2.3 SSH

-t: Thread
-l: username
-P: path to wordlist
-vV: verbose to high
10.1.2.3: ip
SSH: Protocol