

COMPTE-RENDU TP2 RÉSEAU

Messagerie

Objectif : Compréhension des flux de messagerie électronique et des protocoles associés.

Exercice 2 : SMTP

4) La commande **telnet univ-rouen.fr 25** ne fonctionne pas, donc, avec la commande dig, en rajoutant l'option mx nous avons la liste des serveurs sur lesquels on peut envoyer des mails au domaine univ-rouen.fr.

dig mx univ-rouen.fr nous permet de savoir que le serveur de mail de l'université de Rouen est **smtp.univ-rouen.fr**. Par conséquent, pour envoyer un mail à une adresse universitaire, il faut utiliser la commande **telnet smtp.univ-rouen.fr 25**.

Voici le résultat obtenu :

```
habibah@ummhabibah:~$ telnet smtp.univ-rouen.fr 25
Trying 10.0.128.66...
Connected to mailhoc.univ-rouen.fr.
Escape character is '^]'.
220 mailhoc.univ-rouen.fr ESMTP
helo umm-habibah
250 mailhoc.univ-rouen.fr
mail from: <dupond@gmail.com>
250 2.1.0 Ok
rcpt to: <umm-habibah.ouattara@etu.univ-rouen.fr>
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: Question 4 TP2 de réseau
C'est un envoi de mail,
Umm-Habibah
.
250 2.0.0 Ok: queued as 73FBD231F
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

Marche à suivre :

- helo unnom
- mail from : <mail expéditeur>
- rcpt to : <mail destinataire>
- data
- subject
- contenu du message
- un point sur une autre ligne
- quit

5) On a plusieurs en-têtes

- **return-path** : adresse mail source SMTP utilisée pour les erreurs générées, renvoie du mail à l'adresse indiqué
- **delivered-to** :
- **received** : toutes les destinations auxquelles le message a été envoyé
- **message-id** : identifiant unique pour les messages
- **date** : date et heure de l'envoi du mail
- **from** : expéditeur à l'origine du message
- **subject** : objet du message
- **MIME-Version** :
- **User-Agent** :

6) On remarque que l'on voit les échanges entre le client (SYN) et le serveur (ACK). Il y a un établissement d'une connexion au niveau du protocole IMAP : la machine locale demande la connexion.

Le mot de passe est bien visible mais est encodé, on le voit grâce à la deuxième ligne **authenticate PLAIN**. Pour savoir quel est le mot de passe utilisé il faut faire la commande **echo mdp | base64 -d**

```
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS AUTH=PLAIN] Dovecot ready.
36 authenticate PLAIN
+
AGRIbw9yZXNvAG1vdGRlcGFzc2U=
36 OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE SORT SORT=DISPLAY THREAD=REFERENCES THREAD=REFS THREAD=ORDEREDSUBJECT
MULTIAPPEND URL-PARTIAL CATENATE UNSELECT CHILDREN NAMESPACE UIDPLUS LIST-EXTENDED I18NLEVEL=1 CONDSTORE QRESYNC ESEARCH ESORT SEARCHRES WITHIN
CONTEXT=SEARCH LIST-STATUS BINARY MOVE NOTIFY COMPRESS=DEFLATE QUOTA ACL RIGHTS=texk] Logged in
37 COMPRESS DEFLATE
37 OK Begin compression (0.001 + 0.000 secs).
2.P.tQ.P.K.MURP
.(KI-J,J..R.3...,C.#=-=%M^.....R.tQ.P.K.MURP./KM./Q...2.P...I&.....(h.....*h+.h.....bM=^.....2.Tp.st.qU.
q..utvv
.....2...t.KL.....21P(N.IM.QP
N.+Q.....
..0.E...0K+.m}.2..
h.M)a.(.kA..A.].].\e2..s..a2%..VL...KM...s.e....R.[.Ge...1.....m+.Tp.%W...8.....{.....2.....n..0@+.....E....&.j7...(.C..
.....r\.....T...k BB;..L...+.p..dY.....21T...L.(.....R...Z...W..ST^Y...t...].].%.c.....21RH0-),./
I...G...R...q...Z.ZTX...C.)h...9.*+.X.....d.{j XMQ~>_X.....21V...#-.$9C..JKA...=.h.....k....0.@.h,Cb2(5...M...RK.3..
.....L...
..0.E.e..H...I...*I>pQ.X*..E.&.n.....DU.....b...]}^%.V5.0.1<.5P*(.9]...u#...z$....a.p..S.
.j.v...3..PK">.IP..0...%Z...t.[0.0...;w-...N!...A;..FV...w..H...&'.....*=[.Z....aX...@?...o...x<.w|.N...y..'N.#.Q.Q....b.HDD...
4..P.c...i|M.$a...a@.].].]a.f.f.4.U.....;[&g..2.0P...o[({.....e...PY4<oe...
...;@~
t
..4.M.tP..4...EU.Y...*Z.o...'D...8...#...I..O.eR...V.b...s.{ ^.7.'a..^}..k1oD...|. {...b...}T.....=(-K;..c...M..>|....21..j.{A....."....
1..w .....ZT...g`.....1].t`X)..We..$....(hD..Z+.d..v(TX...X+..Y...h.3]rv...TC.C^.....}...=#D..$....=h.....p)E.y.i.
0r.K.O..K.R00...TbJB...21.F..+/.V.L.....r.....21.Wz)9.....3..f.....21wH,(H.K...FLpj.j..B...v-/.....t..N.
0.....F;...(.
..@.#]...nC...b..o0{...|'.....w8C!...4D-..((.....,e.E&..N.o. ....V..I.....!O..W...Z.
.....cJ.Rht...F.3/
.....o...a...@oI...'.U.kT].....:e[...2..&..T..L...r..V.o..j.K.F.E.F..t4...a6/-V...B....#. 'I4.e....)=yknM.....X.
{.WL...=H..^.....Y.f.4@...eF.....s..Z...Q/+..yy<...
...})|.....R0B.R..U
0a..X...W?.p..(.....5/..}&.....>C.....2.P.../.....2.W..~.....2.T..0./.....Rp.tU..00.zH!..T...g...G.....
```

7) Sur le port 143, on obtient le même résultat, nous récupérons le mot de passe mais encodé.

8) La ligne qui indique qu'on s'est bien authentifié est : **Authentication-Results**

9) On peut remarquer qu'il y a de nouveaux headers

- **content-type** : sert à indiquer le type MIME de la ressource
- **content-transfer-encoding** :

Et en bas du mail, on apprend plus sur le type de la pièce jointe, si c'est une image, un fichier, le nom de l'image ou le nom du fichier.