DOCUMENTATION N°4

Est-ce une bonne idée ?

Table des matières

1. Ce qui a été fait

Toutes les fonctionnalités demandées ont été réalisées, l'interface est assez simpliste et facile à prendre en main. Les utilisateurs peuvent s'enregistrer eux-mêmes.

Le stockage des messages est bien effectué sur la base de données, et l'on peut bannir/kick des utilisateurs.

Les différents channels demandés ont été ajouté et sont fonctionnels.

Pour ce qui est de l'interface, je voulais faire mes propres styles pour les différents éléments mais par manque de temps j'ai utilisé un thème déjà existant appelé **Forest Theme** trouvable sur Github à l'adresse suivante :

https://github.com/rdbende/Forest-ttk-theme

2. Pistes d'améliorations

Il y a de nombreuses choses à améliorer, d'un point de vue sécurité comme fonctionnel :

- Les échanges clients/serveur et base de données/serveur ne sont pas chiffrés :
  Voici par exemple une capture faite avec Wireshark :

```
0000  02 00 00 00 45 00 00 be  17 5b 40 00 80 06 00 00   ····E··· ·[@·····
0010  7f 00 00 01 7f 00 00 01  d7 aa 0c ea 56 0f 43 26   ········ ····V·C&
0020  a0 4a 44 d7 50 18 27 f5  f6 3f 00 00 92 00 00 00   ·JD·P·'· ·?······
0030  03 49 4e 53 45 52 54 20  49 4e 54 4f 20 6d 65 73   ·INSERT  INTO mes
0040  73 61 67 65 28 63 68 61  6e 6e 65 6c 5f 6e 61 6d   sage(cha nnel_nam
0050  65 2c 20 75 73 65 72 5f  6e 61 6d 65 2c 20 63 6f   e, user_ name, co
0060  6e 74 65 6e 74 2c 20 74  69 6d 65 73 74 61 6d 70   ntent, t imestamp
0070  29 20 56 41 4c 55 45 53  28 27 67 65 6e 65 72 61   ) VALUES ('genera
0080  6c 27 2c 20 27 61 64 6d  69 6e 27 2c 20 27 63 65   l', 'adm in', 'ce
0090  63 69 20 65 73 74 20 75  6e 20 6d 65 73 73 61 67   ci est u n messag
00a0  65 20 65 78 74 72 c3 aa  6d 65 6d 65 6e 74 20 73   e extr·· mement s
00b0  c3 a9 63 75 72 69 73 c3  a9 27 2c 20 4e 4f 57 28   ··curis· ·', NOW(
00c0  29 29                                             ))
```

  Celle-ci correspond à l'insertion du message suivant dans la base de données :

```
Moi->ceci est un message extrêmement sécurisé
```

  On peut constater que le message est complètement lisible sur le réseau.

  Idem pour les trames TCP entre le client et le serveur :

```
0000  02 00 00 00 45 00 00 53  17 59 40 00 80 06 00 00   ····E··S ·Y@·····
0010  7f 00 00 01 7f 00 00 01  d7 ab 2f be 80 eb 2c 7c   ········ ··/···,|
0020  94 f6 3c 01 50 18 27 f9  b5 a9 00 00 63 65 63 69   ··<·P·'· ····ceci
0030  20 65 73 74 20 75 6e 20  6d 65 73 73 61 67 65 20    est un  message
0040  65 78 74 72 c3 aa 6d 65  6d 65 6e 74 20 73 c3 a9   extr··me ment s··
0050  63 75 72 69 73 c3 a9                              curis··
```

  Encore faut-il avoir les outils pour intercepter les communications comme je viens de le faire, mais cela reste assez facile à mettre en œuvre.

- Ensuite les informations comme les mots de passe ne sont pas chiffrées dans la base de données :

user_name	channel_name	is_admin	is_banned	kick_date	kick_time	current_ip	password
admin	["comptabilite", "informatique", "blabla", "general"]	1	0	NULL	NULL	127.0.0.1	passwd

- Enfin les utilisateurs peuvent très facilement lire le code du client et comprendre la logique des connexions et des échanges entre le serveur et le client, il faudrait compiler le code pour au moins empêcher sa lecture sans outils dédiés.
- Et pour finir il est très probable que l'on puisse « rejouer » et fabriquer des messages TCP ou MySQL pour envoyer ou récupérer des données sans clients dans un but malveillant.

Pour ce qui est de l'interface, il faudrait pouvoir rajouter des canaux de discussion via un menu dédié par exemple, ou encore avoir accès à l'historique des messages et pouvoir en supprimer certains via l'interface serveur.

Un point non négligeable est que l'outil ne permet que de partager du texte : impossible d'insérer des images, des pièces jointes…

3. Maintenance et mises à jour

C'est très laborieux de maintenir cet outil à jour, car lorsque l'on implémente des choses côté serveur il faut s'assurer qu'elles sont aussi interprétables côté client et vice-versa. De plus, il suffit qu'un client ne mette pas à jour sa version pour que ça cause des problèmes en cascade.

Je pense qu'un site web serait plus facile à maintenir à jour et à améliorer, c'est un moyen plus flexible pour faire des interfaces, et cela n'implique pas d'installations côté client.

De plus il est plus facile de mettre en œuvre des moyens de chiffrements comme l'HTTPS par exemple.

Grâce à un site, on s'assure aussi d'une plus grande variété d'environnements où l'outil est compatible, car dans notre cas on ne peut pas vraiment en faire une version mobile par exemple.

4. Conclusion

Cet outil pourrait être utilisable dans un environnement restreint et contrôlé, mais une mise en production sécurisé serait difficile en vue des différents points évoqués plus haut.

Une interface sous forme de site web serait sûrement plus adapté et plus facile à mettre en œuvre de manière sécurisée.