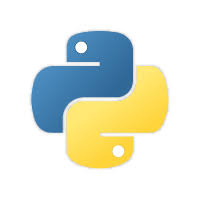


PYTHON : Projet ClicMed

Une image contenant mur, personne, homme, intérieur

Description générée avec un niveau de confiance très élevéUne image contenant homme, personne, verres, mur

Description générée avec un niveau de confiance très élevéUne image contenant mur, personne, homme, intérieur

Description générée avec un niveau de confiance très élevéUne image contenant mur, personne, intérieur, habits

Description générée avec un niveau de confiance très élevé

Philippe DA SILVA OLIVEIRA

Alexandre KOSTAS

Khartike EZHILARASAN

Benjamin BEYERLE

Sommaire :

[Contexte 2](#_Toc12668491)

[Besoins Exprimés par ClicMed 3](#_Toc12668492)

[Outils de communication 4](#_Toc12668493)

[Outil collaboratif 4](#_Toc12668494)

[Le projet 5](#_Toc12668495)

[Partie sauvegarde 5](#_Toc12668496)

[Gestion des utilisateurs 6](#_Toc12668497)

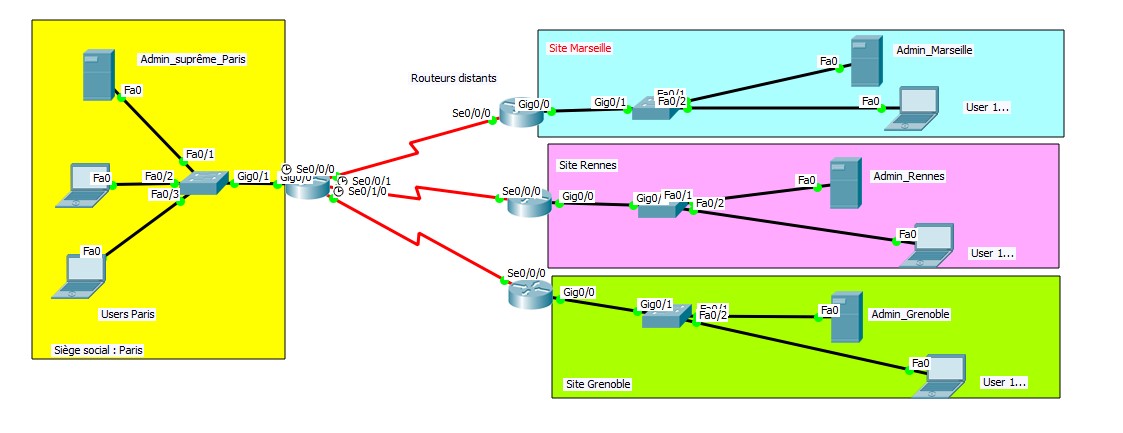
[Boite à outils 6](#_Toc12668498)

[Résultat 7](#_Toc12668499)

# 

# Contexte

La société ClicMed dont le siège se situe à Paris est spécialisée dans le secteur de la santé, cherche à définir sa politique de sécurité. Elle gère 4 cliniques privées (Paris, Marseille, Rennes, Grenoble).



Par souci de traçabilité, de qualité de ses services et de sécurité, le siège dispose d’un Datacenter (répliqué) qui centralise tous les documents et toute la gestion des utilisateurs/administrateurs de toute la plateforme de l’entreprise. Les clients de ClicMed sont des patients envoyés par des médecins traitants et des intervenants médicaux, médecins généralistes et spécialistes et des experts. Les patients peuvent obtenir auprès de ClicMed des analyses médicales, des expertises (en apportant éventuellement eux même des documents issus d’analyses antérieures, …).

# 

# Besoins Exprimés par ClicMed

* Assurer la disponibilité de ses services de connexion et de stockage pour des accès en local et à distance
* Identifier les types d’attaque pour renforcer la sécurité des données médicales des patients (DMP)
* Développer ses propres outils pour renforcer la sécurité des données médicales au sens de la confidentialité dont :
  + La gestion des utilisateurs
  + La gestion du serveur FTP
  + Le scan de ports au quotidien sur les serveurs et solution
  + Simulation d’une attaque par Force Brute pour tester la fiabilité des mots de passe avec les solutions
  + Un journal d’activité (log) sera mis en place pour éviter les erreurs et retracer l’activité du réseau

# Outils de communication

Pour mener à bien ce projet, des outils de communications ont été nécessaires :

Afin de pouvoir communiquer rapidement par message, nous avions besoin d’utiliser une application sur smartphone. Nous avons donc choisi WhatsApp étant donné que tout le monde la possédait.

De plus, il peut aussi être utilisé via un navigateur sur un ordinateur, via WhatsApp Web.

Grâce à cette application, nous sommes en mesure d’échanger avec tout le monde via un groupe pour partager une idée ou poser une question par exemple.

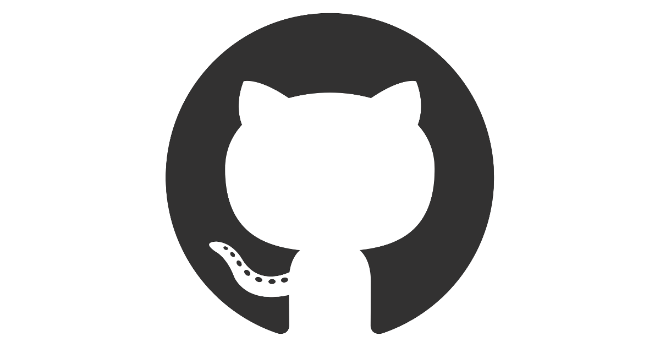


Nous avons également choisi Discord, un outil développé par Discord Inc. Grâce à cet outil nous étions en mesure également d’envoyer des messages instantanés lors des réunions mais aussi de réaliser des partages d’écrans.

# Outil collaboratif

Travailler sur un projet en commun permet de partager les tâches ainsi que nos connaissances. L’inconvénients du travail collaboratif est que dans notre cas par exemple, les scripts python pourraient être amené à avoir des bugs si tout le monde procédait à des modifications en même temps. C’est pour cela que nous avons utilisé la plateforme GitHub.

GitHub est utilisé pour stocker le code source d'un projet et suivre l'historique complet de toutes les modifications apportées à ce code. Il permet aux développeurs de collaborer plus efficacement sur un projet en fournissant des outils de gestion des modifications éventuellement conflictuelles de la part de plusieurs développeurs. GitHub permet aux développeurs de modifier, d'adapter et d'améliorer les logiciels de ses référentiels publics gratuitement.



# Le projet

Ce projet a été conçu avec une interface graphique permettant une meilleure visualisation du programme ainsi qu’une facilité d’utilisation. Cette interface a pu être créée grâce au module python « Tkinter ».

Le module « Tkinter » ("Tk interface") permet de créer des interfaces graphiques. De nombreux composants graphiques sont disponibles : fenêtre, bouton, case à cocher, étiquette, zone de texte simple, menu, zone graphique etc... On peut également gérer de nombreux événements : clic sur la souris, déplacement de la souris, appui sur une touche du clavier.

# 

# Partie sauvegarde

Il a été demandé de stocker les différents documents de chaque patient sur un serveur distant. La solution est donc de stocker ces documents via un serveur FTP (File Transfer Protocol) situé au siège à Paris. Les Cliniques disposent donc d’un client FTP permettant de transférer les documents des patients mais aussi de créer ou supprimer des répertoires selon leurs droits.

Une solution de backup est mise en place afin d’obtenir une sécurité supplémentaire en ayant une copie des données du client.

Pour cela, les modules OS, datetime, shutil ont dû être utilisés.

Python fournit deux modules permettant de gérer les fichiers et les répertoires. Le module OS qui permet de lister des fichiers et des répertoires. Le module shutil permet de copier, déplacer, supprimer des éléments sur les systèmes de fichiers. Quant à datetime, il permet seulement de sauvegarder les documents avec une date.

# Gestion des utilisateurs

Pour se connecter à la solution de ClicMed, des utilisateurs doivent être créée. Ces derniers sont stockés dans une base de données avec des mots de passe hasher. Selon le profil, l’utilisateur disposera de diverses options comme la consultation, création, suppression, mail bombing, scan de ports etc.

Pour ce faire, Les modules « sys » et « OS » ont été utilisés. Ils constituent le cœur de la plupart des outils système de Python. Puis, le module « mysql-connector » qui permet de se connecter à la base de données contenant les utilisateurs. Enfin, le module « hashlib » permet de chiffrer les mots de passe.

# Boite à outils

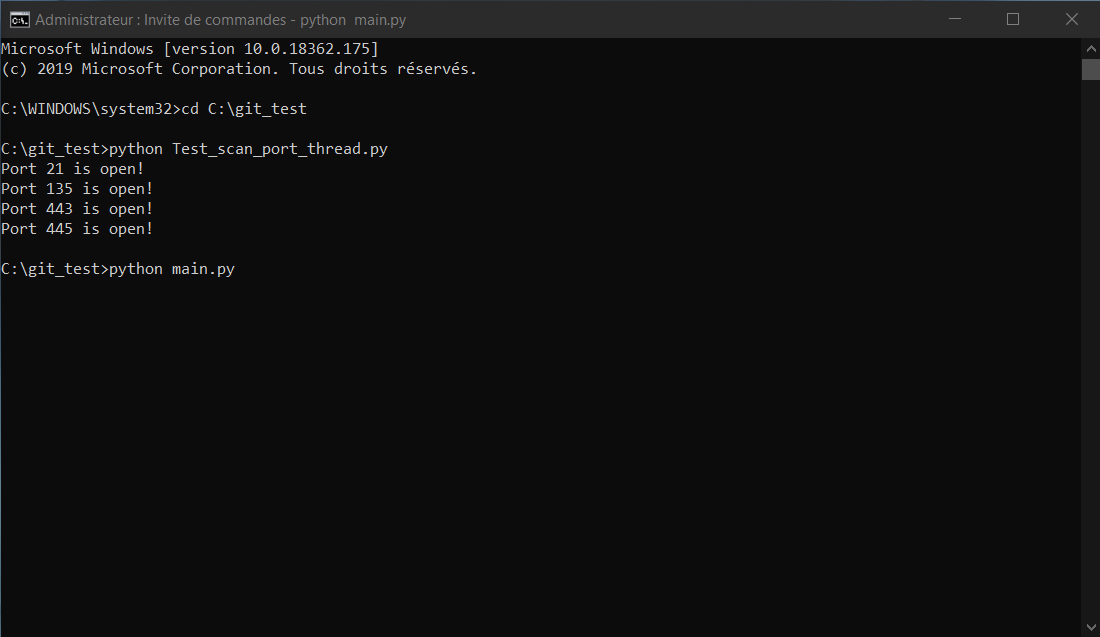
Les utilisateurs ayant les droits administrateurs disposent d’une boite à outils permettant le scan de port et de réseaux, mais aussi un outil de brute force permettant de voir la fiabilité des mots de passe ainsi qu’un outil de mail-bombing.

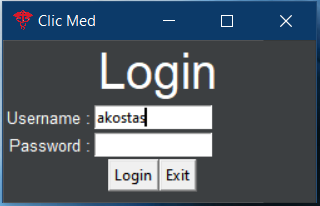
Les modules utilisés sont :

* Bruteforce : Module « Time » qui permet d’afficher le temps que mets le programme à déchiffrer le mot de passe, ainsi que le module « itertools » qui lui permet de procéder à des calculs plus rapidement et « String » permettant d’obtenir tous les caractères ASCII afin de récupérer le mot de passe en clair. Enfin, les modules « Hashlib » et « Sys ».
* Scan de port et Scan de réseaux : Module « Socket » qui permet de se connecter à une machine ou en local grâce à une adresse IP et un port, puis le Module « Thread » permettant de faire de la programmation parallèle. Enfin le Module « Queue » permettant la gestion des files d’attente.
* Mail bombing : Module « SMTP » qui permet d’envoyer des mails
* Logs : Nous allons utiliser le module « logging » pour cette partie et l’implémenter la où nous le souhaitons.

# Résultat

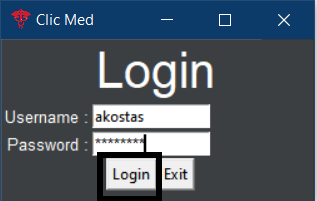
Voici un récapitulatif du fonctionnement du programme :

Tout d’abord lançons le programme :

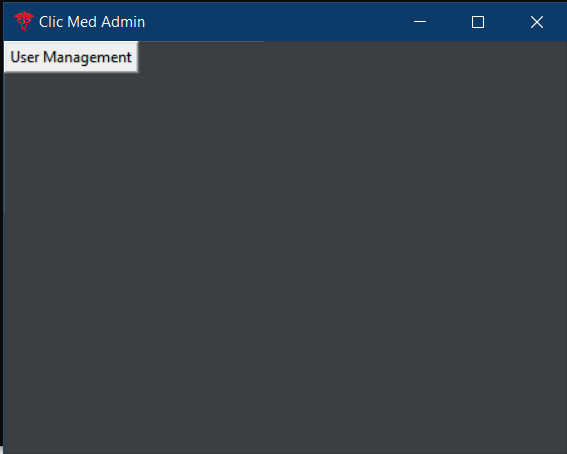
La fenêtre d’authentification apparaît

Nous rentrons nos

Identifiants

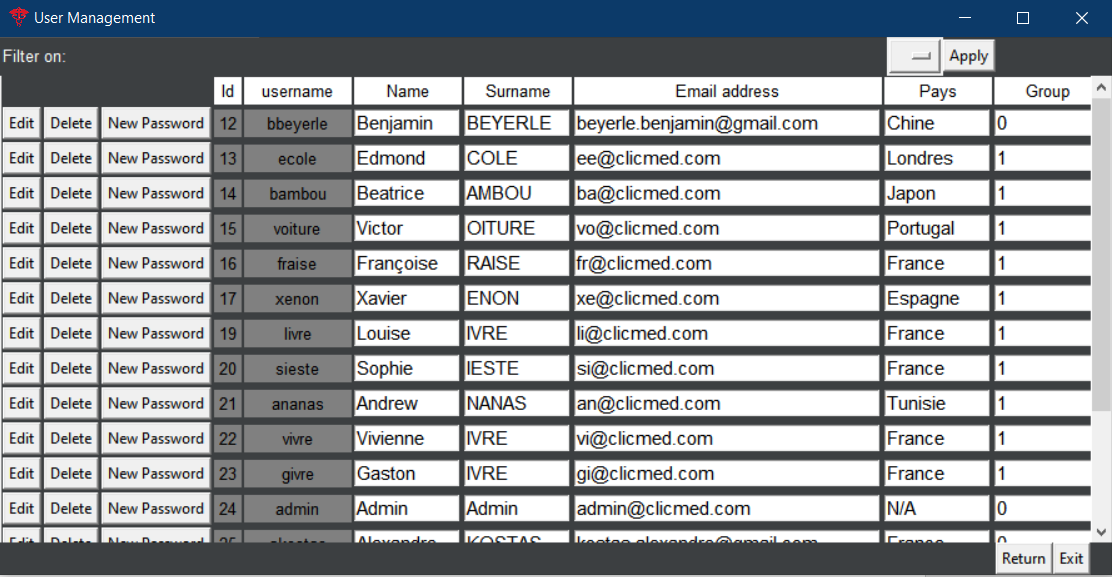


Login / Password

Nous cliquons sur

User Management

La fenêtre des User managements apparait :



C:\Users\Syu\.ClicMed

Voir les scripts et le fichier « readme ».