Documentation

L’entreprise cliente, son mode d’organisation

**Comment le script est-il structuré ?**

Le script est divisé en 2 parties :

* Script client
  + Il s’exécute sur la machine des clients, il permet d’établir la communication et s’authentifier sur le serveur, il fournit l’interface pour voir la liste des tâches qui lui sont autorisées (ftp, sauvegardes, panneau d’administration…)
* Script serveur
  + Reçoit les connexions des clients
  + Il vérifie si l’utilisateur existe dans la BDD, si oui il autorise la connexion
  + Il vérifie les droits de l’utilisateur connecté
  + Il donne accès à des ressources

**Comment le script est-il organisé ?**

**Serveur :** Le script qui doit être exécuté sur le serveur est nommé main.py, ce script permet d’initialiser l’écoute du serveur sur le port custom dans notre cas 3401.

Une image contenant texte

Description générée automatiquement

Lorsqu’une connexion va être établie sur ce port, un thread sera créer et redirigé vers la fonction « Instruction » de la classe « Server ». Ce thread permet des connexions simultanés de clients et isole le client dans cette fonction.

**Client :** Lorsqu’un client initialise une connexion avec le serveur, il utilise un port source aléatoire défini par le système, ce port sera utilisé par le serveur comme port destination pour le message de réponse.

Lors de la connexion, le client indique son login et son password.

**Serveur :** il va vérifier si la BDD contenant les utilisateurs existe, dans le cas où celle-ci n’est pas présente, il va créer une nouvelle BDD en créant la table « Utilisateur », cette table contient l’ID auto incrémenté, le login, le password, le rôle, le nom, prénom et le site.

Une fois fait, il va générer l’utilisateur par défaut root avec le password root, rôle « 1 » qui correspond à un superutilisateur/admin, avec comme site de rattachement « SIEGE ».

Il va vérifier que l’utilisateur connecté existe bien dans la base de données, si c’est le cas il autorise le client à poursuivre la connexion, sinon il ferme la connexion. Il lui envoie les informations relatives à son statut : rôle, nom, prénom, site.

**Client :** il reçoit les informations et va vérifier s’il est admin, en fonction de ses droits il aura accès à un panel d’options différent.

Panel administrateur :

Une image contenant texte

Description générée automatiquement

Panel utilisateur :

Une image contenant texte

Description générée automatiquement

Principe :

* Une infinité de clients peuvent se connecter à l’infrastructure
* Chaque session de connexion d’un client correspond à un thread dans le serveur

Rôle du serveur : contrôle d’accès des clients

**Process général de connexion des clients (étapes)**

* Le client se connecte avec son login et pwd
* Le serveur va vérifier si cet user est connu dans la BDD
  + Connu : connexion acceptée
    - Renvoi :
      * Login
      * Rôle (admin ou non)
      * Site géographique
  + Inconnu : indique au client qu’il n’existe pas, ferme la session de connexion

**Quels sont les éléments de l’infrastructure ?**

* Un serveur d’administration
* Un serveur FTP
* Un serveur de sauvegardes (dans notre archi, le serveur d’administation également)

**Fonctionnement, les fonctionnalités du FTP**

* Il y a un utilisateur FTP dédié pour chaque site, qui a les droits sur le dossier FTP de son site uniquement
* Un superutilisateur (admin) a accès à l’ensemble des sites FTP
* L’adresse IP du ou des serveurs FTPs est détenue par le serveur d’administration, ainsi que les logins et passwords des utilisateurs FTP de chaque site

**Panel d’options FTP admin :**

Une image contenant texte

Description générée automatiquement

**Panel d’options FTP utilisateur :**

Une image contenant texte

Description générée automatiquement

**Fonctionnement, les fonctionnalités de la Toolbox**

* Les fonctionnalités de la toolbox sont exécutés par le serveur pour le compte des clients
* Tous les outils sont multithreadés pour accélérer l’exécution des tâches et rester disponibles pour d’autres tâches demandées par les clients

Une image contenant texte

Description générée automatiquement

**Fonctionnement scan de port :**

* Le client indique une machine cible, ainsi qu’un port unique ou une plage de port à scanner
* Le serveur d’administration lance le scan, un thread sera créer pour chaque port à scanner
* La date et l’heure de lancement du script est mémorisée
* Si un port est ouvert, un rapport sera généré dont le titre sera la date et l’heure de lancement du scan et contenant uniquement les numéros de port ouverts
* Si aucun port ouvert n’est trouvé, le rapport ne sera pas généré

Une image contenant texte

Description générée automatiquement

**Fonctionnement bruteforce :**

**Bruteforce mode combinaison :**

Principe de la combinaison : va tester à partir de l’alphabet et des nombres de 0 à 9, sur 6 caractères, toutes les combinaisons possibles, cette opération est longue et fastidieuse

* Le client indique une machine cible et un username
* Le serveur d’administration va tester les possibilités dans l’ordre : a, aa, aaa…
* Si un mot de passe est trouvé, un rapport sera généré avec l’IP de la machine cible, l’username et le mot de passe

**Bruteforce mode dico :**

Principe du dictionnaire : va tester l’ensemble des mots de passe (souvent les plus courants) contenus dans un fichier, appelé dictionnaire.

* Le client indique une machine cible et un username
* Le serveur d’administration va tester les possibilités dans l’ordre : a, aa, aaa…
* Si un mot de passe est trouvé, un rapport sera généré avec l’IP de la machine cible, l’username et le mot de passe

Une image contenant texte

Description générée automatiquement

**Comment fonctionne la solution de sauvegarde (de backup) ? :**

* Le client va demander a effectuer une sauvegarde sur le FTP en fonction de ses accès
* Le client aura différentes options de sauvegardes plus ou moins étendues selon ses autorisations (sauvegarde de tous les sites ou son site de rattachement uniquement)
* Le serveur de backup va se connecter au serveur FTP et copier tous les fichiers du répertoire de l’utilisateur FTP dans le répertoire backup et générer un dossier de sauvegarde selon la nomenclature suivante : SITE\_JJ\_MM\_AAAA\_HH
* Créer un dossier compressé à partir du dossier initial
* Supprime le dossier initial

**Panel d’options admin backup (le menu est le même que l’utilisateur mais l’admin peut backup d’autres sites) :**

Une image contenant texte

Description générée automatiquement

**Panel d’options utilisateur backup :**

Une image contenant texte

Description générée automatiquement