

**DÉPARTEMENT DES SCIENCES APPLIQUÉES**

**RÉSEAUX D’ORDINATEURS**

**6GEN723-01**

**Instructions pour l’exécution des programmes du devoir 5**

**Remis à**

**M. Daniel Audet**

**Par**

**Marc-Antoine Plourde**

**REMIS LE**

**21/04/2020**

**Instructions pour l’exécution des programmes du devoir 5**

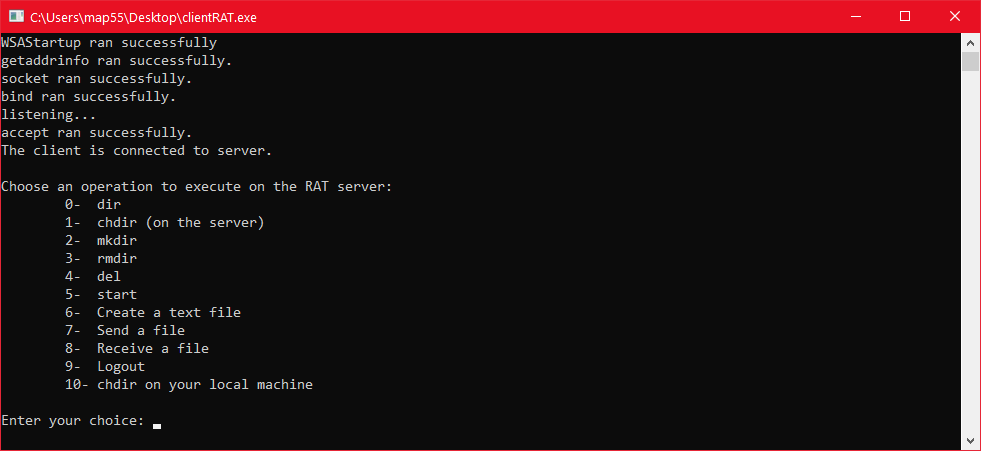
**Préalable**

Tout d’abord, il est question d’ouvrir le projet Visual Studio du serveur de l’injecteur (« ServerInjecter.sln » dans le dossier « ServerInjecter »). Ensuite, vous devez modifier la valeur de « MASTER\_IP » situé au début du code source par l’adresse IP de l’ordinateur « maître » (celui qui prendra le contrôle) et recompiler en mode « release ». Puis, ouvrez le projet du serveur du RAT (« ServerRAT.sln » dans le dossier « ServerRAT ») et effectuez la même chose qu’avec le serveur de l’injecteur.

**Instructions pour l’exécution des programmes**

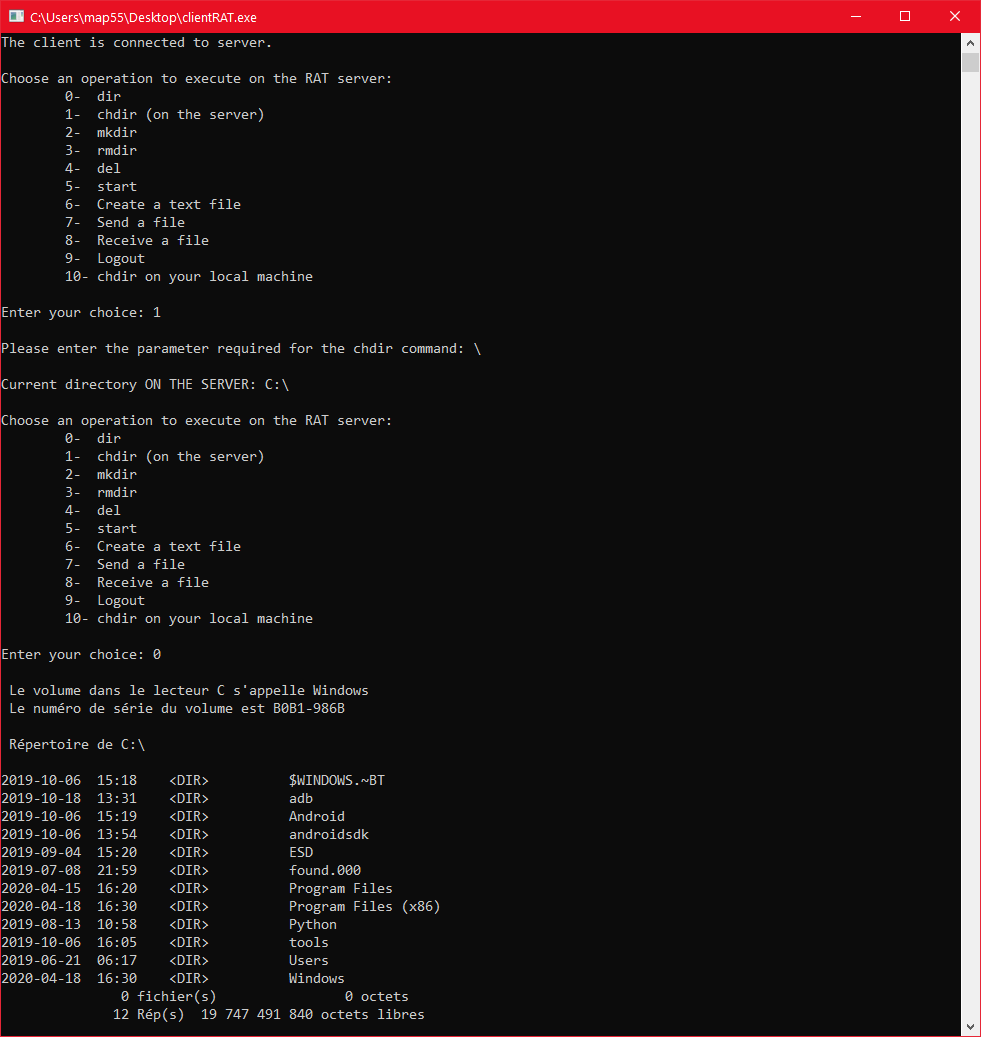
1. Placez l’exécutable du client de l’injecteur, du client du RAT et du serveur du RAT sur la machine « maître » et l’exécutable du serveur de l’injecteur sur la machine « esclave » (celle qui se fait contrôler). Veuillez prendre note que les exécutables (.exe) se retrouvent dans le dossier « Release » du dossier de chaque projet.
2. Sur le maître, lancer le client de l’injecteur ainsi que le client du RAT.
3. Sur l’esclave, lancer le serveur de l’injecteur.
4. Lorsque la connexion sera établie entre le client et le serveur de l’injecteur, veuillez entrer le chemin de fichier de l’exécutable du serveur du RAT (ne pas oublier de rentrer le « .exe »).
5. Lorsque la connexion aura été établie entre le client et le serveur du RAT, une liste d’opérations pouvant être exécutée par l’esclave (à l’exception de la dixième opération) sera affichée dans la fenêtre du programme client. Vous aurez donc à entrer le numéro de l’opération que vous désirez effectuer. Après chaque opération, la liste d’opérations réapparaîtra tant et aussi longtemps que vous ne vous déconnectez pas du serveur du RAT (opération 9). De plus, la dixième opération a été ajoutée afin de faciliter l’envoi de fichier vers l’esclave. Dans ce sens, la dixième opération consiste à changer le répertoire courant (« current directory ») sur le maître.

**Précisions sur le fonctionnement des commandes:**

* Toutes les opérations se font sur le répertoire courant, et ce pour chacune des deux machines. Tel qu’il est indiqué dans le menu principal du client, il y a un chdir serveur et un chdir client à cet effet.

**Figure 1: Capture d'écran le menu du programme du client du rat comportant deux chdir (un client (machine locale) et un serveur (machine distante)).**

* Les fichiers transférés entre les deux ordinateurs doivent avoir une taille inférieure à 1000000 bits.
* Lorsqu’il est spécifié de ne pas mettre l’extension du fichier, seul le nom du fichier (ce qui est avant le « .quelquechose ») doit être entré. Lorsque l’extension du fichier est demandée, l’utilisateur doit entrer, selon la commande, soit le nom du fichier avec son extension (ex. « fichier.txt »), soit le chemin vers le fichier n’oubliant pas d’inscrire le nom du fichier avec son extension à la fin (cette dernière possibilité est spécifique au programme client de l’injecteur qui demande le chemin de fichier de l'exécutable du serveur du RAT avec le fichier « .exe » à la fin du chemin (ex. « C:\CheminVersL'Exécutable\ServerRAT.exe »)).
* Lorsqu’une commande ne demande pas de paramètre (ex. effectuer un dir), seul le numéro de la commande doit être entré par l’utilisateur. Si une commande demande des paramètres, le client du rat invitera l’utilisateur à entrer les paramètres de la commande seulement et non la commande et le(s) paramètre(s) (après avoir préalablement sélectionné une commande).



**Figure 2: Capture d'écran du programme client du rat montrant que comme exécuter une commande avec paramètre et une commande sans paramètre. D’abord, celles nécessitant un paramètre demandent à entrer le numéro de la commande puis SEULEMENT le paramètre associé à la commande. Ainsi, pour la commande 1, l’utilisateur doit seulement entrer « \ » afin que le répertoire courant soit à la racine du disque et non « chdir \ » comme dans un terminal. Ensuite, une commande ne demandant pas de paramètres nécessite seulement d'entrer le numéro de la commande. Ici, on peut voir que la commande 0 ne nécessite que d’entrer « 0 » afin qu’elle s’exécute.**