TP Sécurité

Table des matières

[TP 1.1 : Création d'une connexion « Client - Serveur » 2](#_Toc32767122)

[TP 1.1 (Suite) : Création d'un « Chat » 3](#_Toc32767123)

[TP 1.3 : Création d'un Cheval de Troie 3](#_Toc32767124)

[1.4 : T.P. Netstat 5](#_Toc32767125)

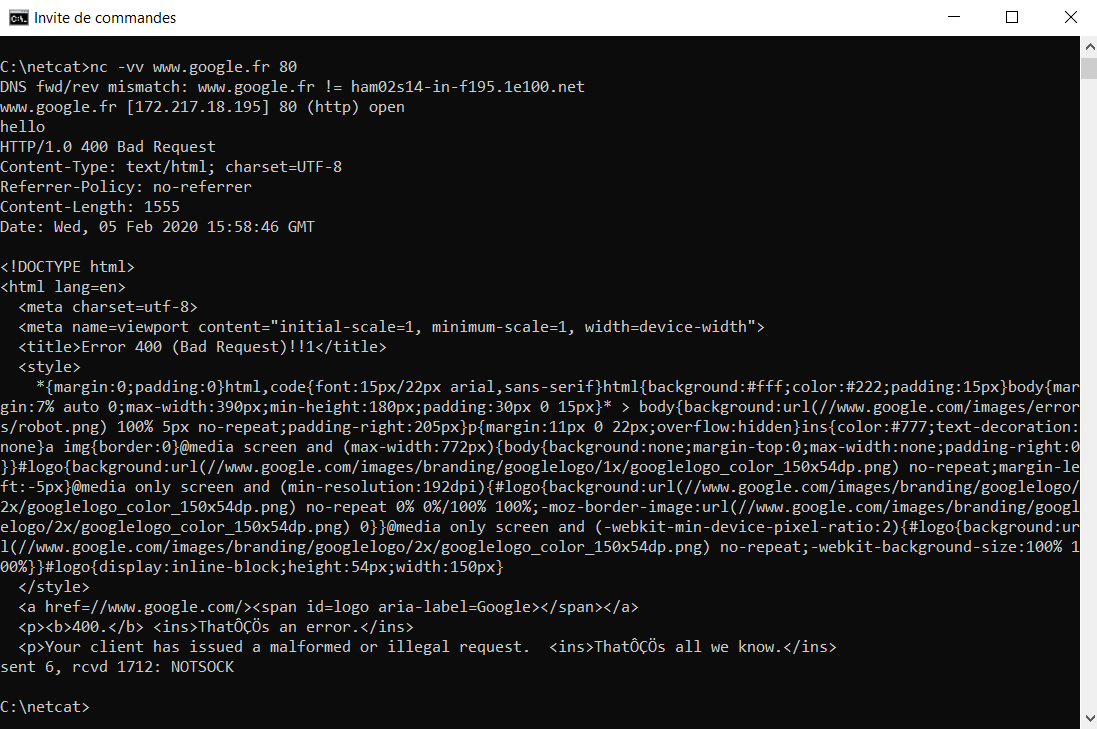
[T.P. 2.1 / Intégrité : 5](#_Toc32767126)

[T.P. : 2.2 / Hachage et Authentification 6](#_Toc32767127)

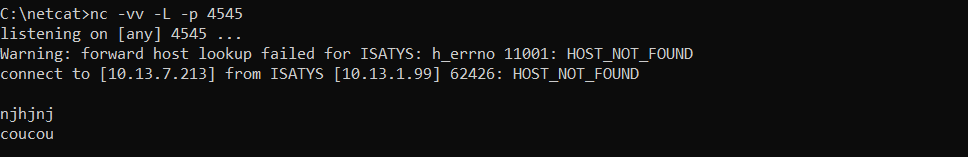
[T.P. 2.3 / Chiffrement 6](#_Toc32767128)

[T.P. 2.4 / Propriété des fonctions de Hash 6](#_Toc32767129)

# TP 1.1 : Création d'une connexion « Client - Serveur »



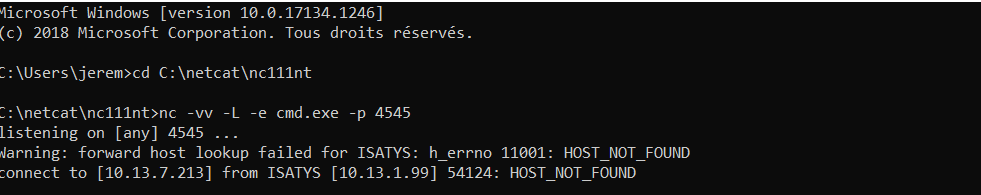
Je lance netcat et je me connecte sur le serveur de google, grâce à la commande nc -vv [www.google.fr](http://www.google.fr) 80. J’ai créé une commande qui n’est pas interprété je reçoi donc une erreur.

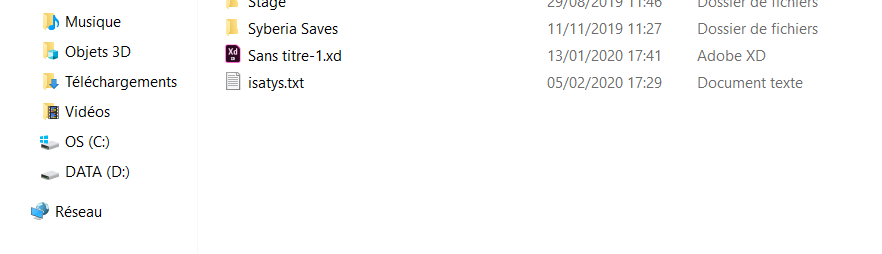
TP 1.1 (Suite) : Création d'un « Chat »



Avec l’aide d’Isatys Rivière nous avons communiqué sur le même réseau, ce qui nous permet de nous envoyer des messages.

# TP 1.3 : Création d'un Cheval de Troie



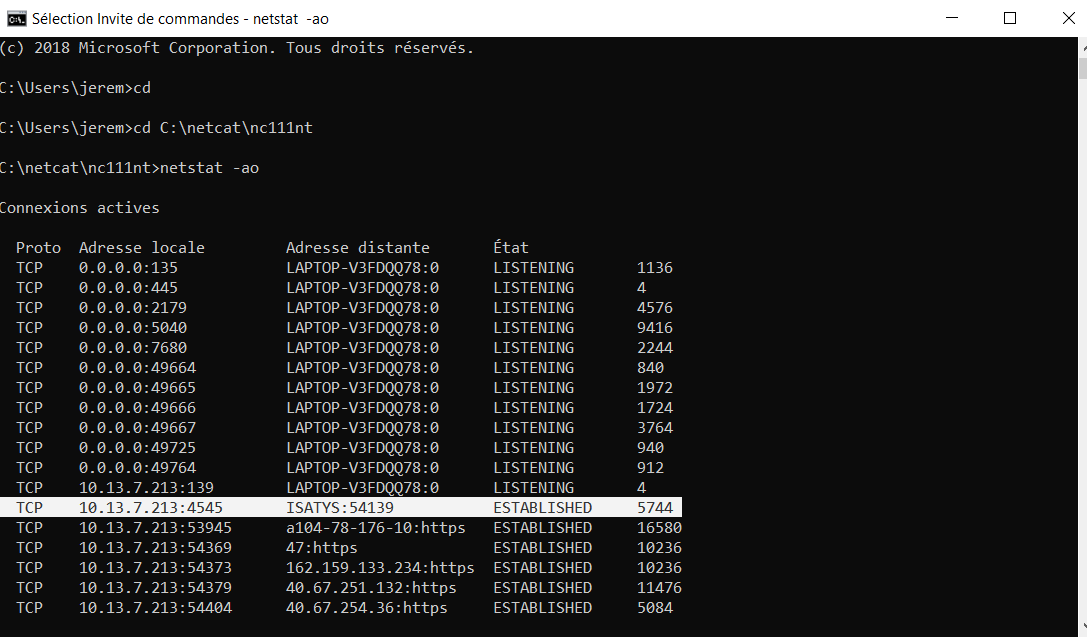




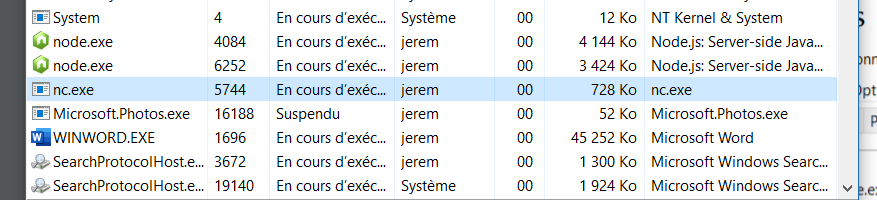


Pour cette partie du TP j’ai travaillé avec Isatys Rivière. Elle a pris contrôle de mon ordinateur, elle a pu renommer un fichier txt.txt en isatys.txt et a pu également le supprimer. En effectuant cette commande elle peut utiliser l’invite de commande de mon ordinateur.

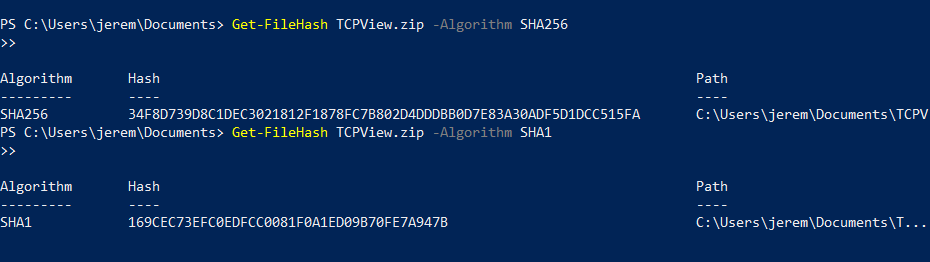
# 1.4 : T.P. Netstat



Je remarque l’adresse distante d’Isatys qui a pris contrôle de mon ordinateur, je remarque également qu’elle se trouve sur le port 4545, cette connexion est également établie ce qui veut dire qu’elle est actuellement connectée à mon ordinateur. Je remarque que le PID (l’ID du processus) est le 5744, grâce au gestionnaire des tâches je vois que ce processus correspond à nc.exe.



# T.P. 2.1 / Intégrité :



En utilisant la commande que vous pouvez voir si dessus, j’ai pu vérifier l’intégrité du document fourni, en effet comme vous pouvez le remarquer le hash trouvé pour le SHA1 et le SHA256 est exactement le même que celui fourni en référence. Sans vérifier cela le fichier pourrait contenir un malware ou autre.

# T.P. : 2.2 / Hachage et Authentification

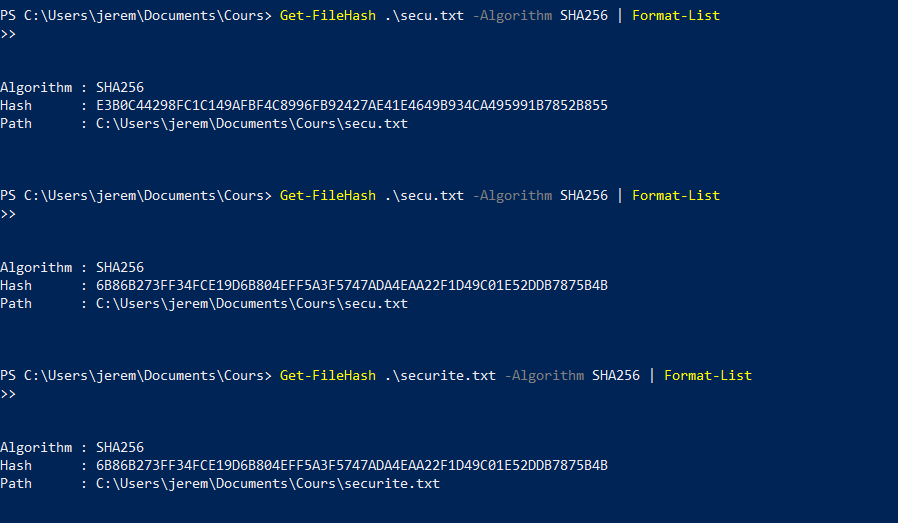
Nous avons le hash du mot de passe : 8a29aaf5687129c1d27b90578fc33ecc49d069dc, ce qui nous permet d’obtenir le mot de passe qui est : badpassword. On a pu obtenir ce mot de passe car on a récupéré son hash depuis la base de données.

# T.P. 2.3 / Chiffrement

Le message en clair est : Il ne faut pas confondre Codage et Chiffrement !

La base 64 n’est pas un système de chiffrement mais un système de codage ce qui le rend facilement réversibles car il ne nécessite pas de clé de chiffrement.

# T.P. 2.4 / Propriété des fonctions de Hash



La première commande montre le hash du fichier secu.txt, la deuxième son hash une fois sa taille modifier et la troisième une fois le fichier renommé. On peut voir que modifier un document change le hash du fichier alors que le renommer ne le change pas.