Analyse de communication et cheval de Troie

Table des matières

[TP 1.1 : Création d’un connexion « Client-Serveur » 3](#_Toc26882406)

[TP 1.2 : Création d’un chat en Local 3](#_Toc26882407)

[TP1.3 créations d’un cheval de troie 4](#_Toc26882408)

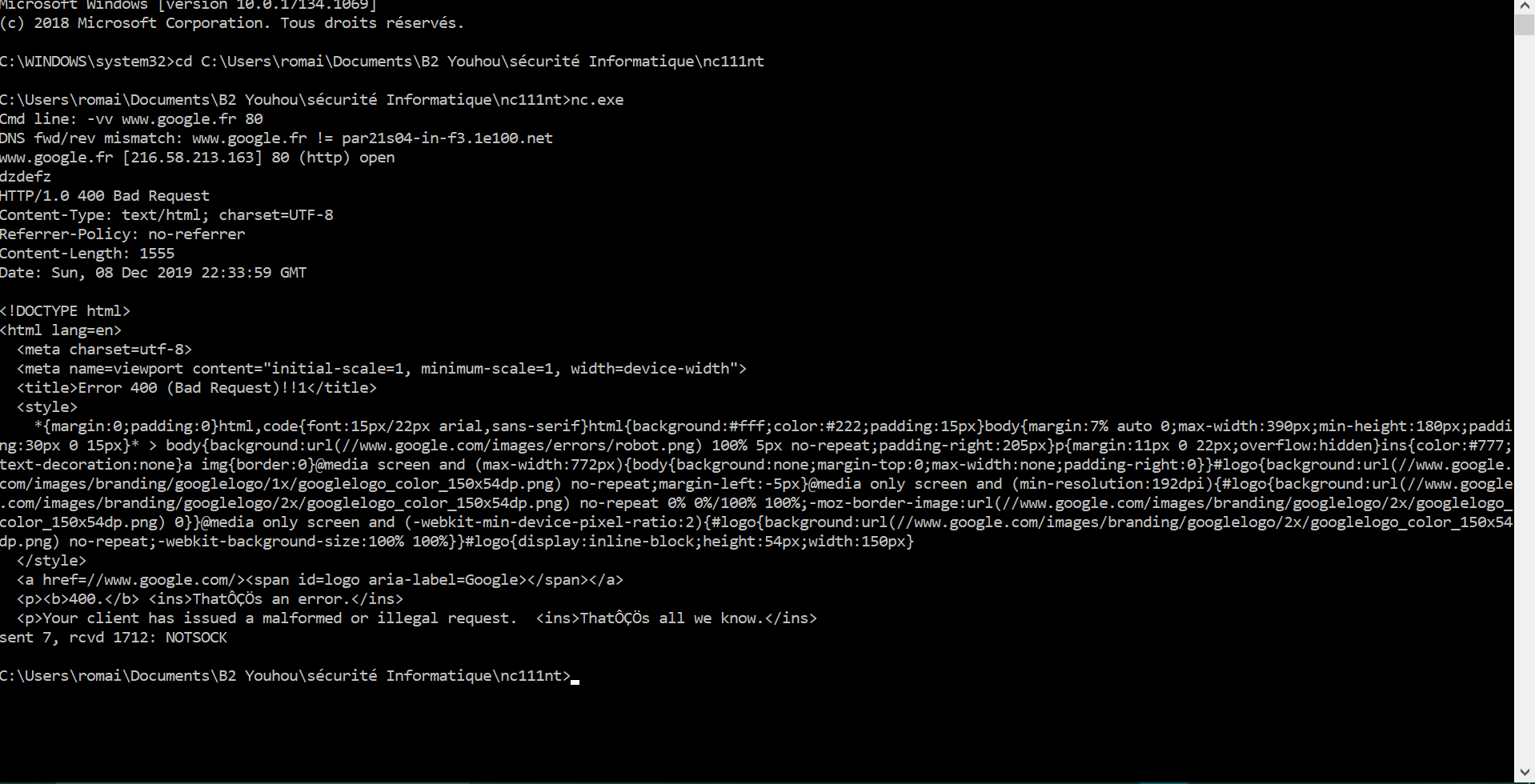
[TP 1.4 : Identifier un programme en cours de Fonctionnement 5](#_Toc26882409)

[TP2.1 :Intégrité 6](#_Toc26882410)

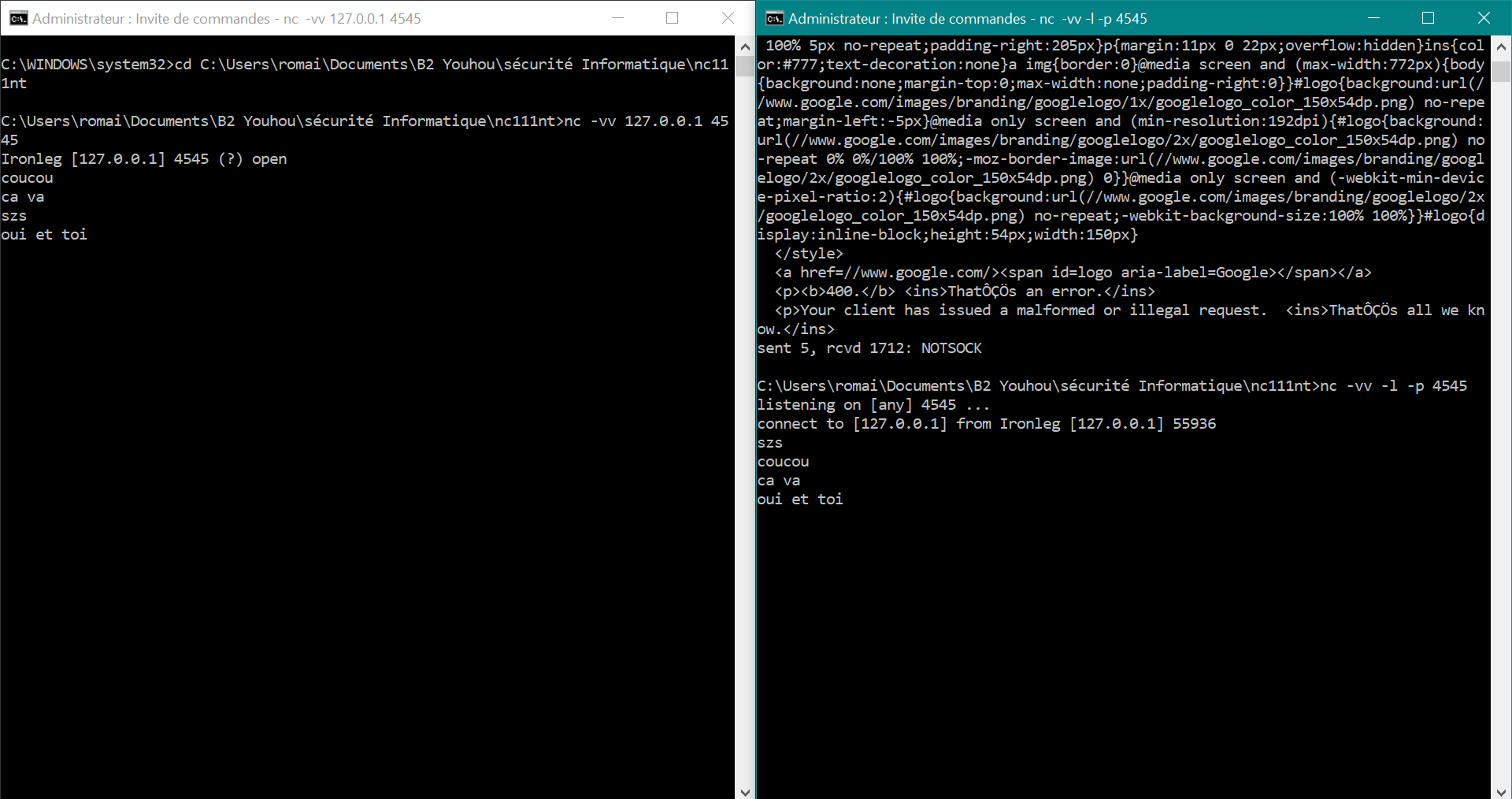
[TP2.2 : Hachage et Authentification 6](#_Toc26882411)

[TP2.3 :Cryptographie 6](#_Toc26882412)

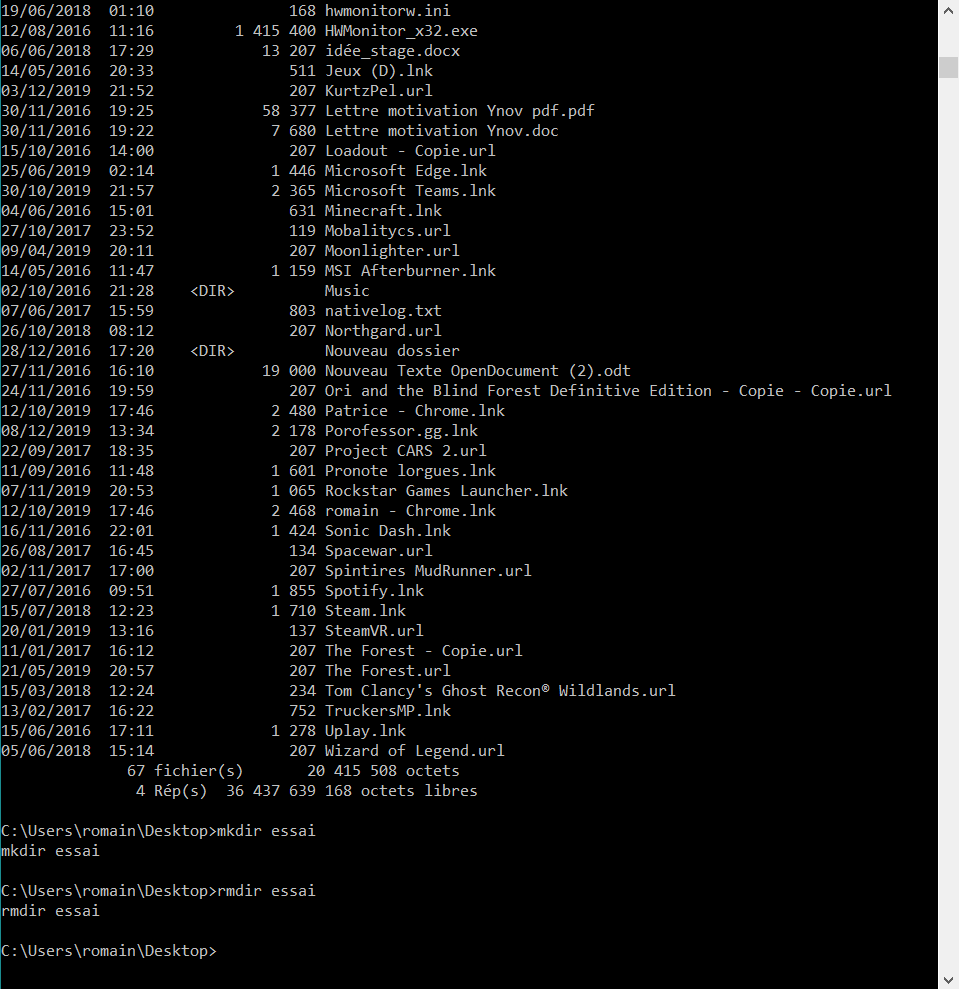
# TP 1.1 : Création d’un connexion « Client-Serveur »



# TP 1.2 : Création d’un chat en Local



# TP1.3 créations d’un cheval de troie

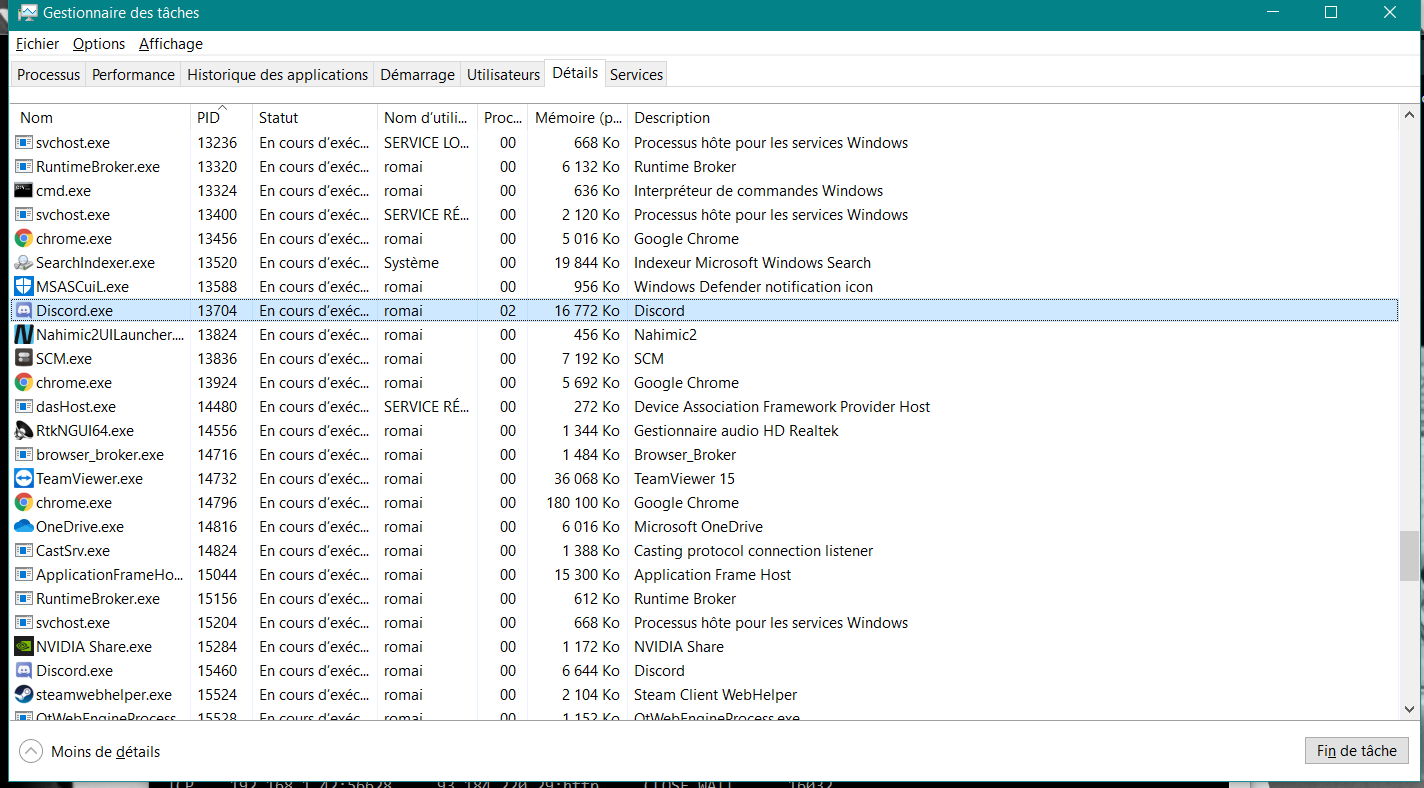


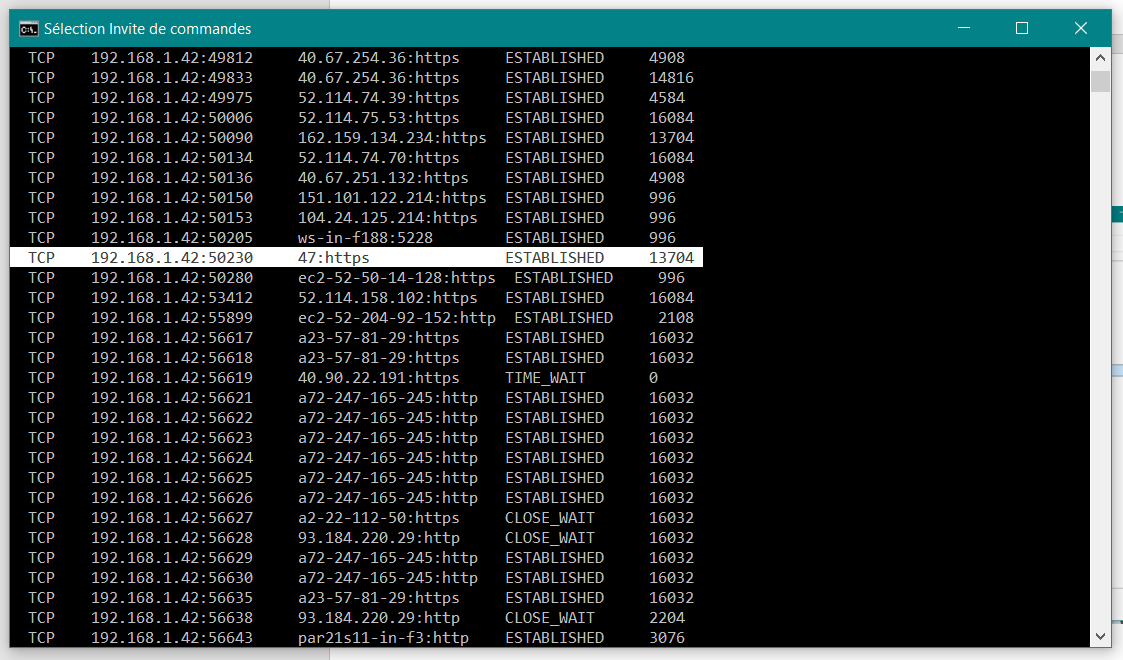
Grace a cette manipulation, l’attaquant a de façon assez général accès au CMD de la victime. Ce qui signifie qu’il a accès à toutes les données de l’ordinateur attaquer, et ce sans déclencher l’anti-virus.

Voici une liste non exhaustive des commande que l’attaquant peut utiliser sur la victime :

<https://fr.wikibooks.org/wiki/DOS/Liste_des_commandes>

# TP 1.4 : Identifier un programme en cours de Fonctionnement





Avec la commande Netstat -ao je peux scanner le réseau tcp de mon ordi et ainsi repéré tous les transferts de donné. J’ai pu donc retrouver la connexion réseau Discord.

# TP2.1 :Intégrité

Malheureusement a l’heure ou je veux faire ce Tp moodle est inaccesseoble. Je ne peux donc pas télécharger TCPview de l’archive moodle. J’ai donc essayer de le télécharger sur le web mais impossible de le lancer.

Pour vérifier l’intégriter d’un fichier, je peux tout de même me référer a ce tutoriel.

<https://lecrabeinfo.net/verifier-integrite-calculer-empreinte-checksum-md5-sha1-sha256-fichier-windows.html>

# TP2.2 : Hachage et Authentification

Le mot de passe est badpassword.

Le mot de passe étant déjà utilisé, il a été stocker dans une basse de donnée ce qui a permis a l’algorithme d’etre décrypté.

# TP2.3 :Cryptographie

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

J’ai pu déchiffrer facilement ce message car la base64 est un moyen de conversion générique, tandis que le hachage est fait en fonction d’une clé spécifique défini par chaque algorithme.