# TP Sécurité

#### Table des matières

TP 1.1 : Création d'une connexion « Client - Serveur »	. 2
TP 1.1 (Suite) : Création d'un « Chat »	. 3
TP 1.3 : Création d'un Cheval de Troie	. 3
1.4 : T.P. Netstat	. 5
T.P. 2.1 / Intégrité :	. 5
T.P.: 2.2 / Hachage et Authentification	. 6
T.P. 2.3 / Chiffrement	. 6
T.P. 2.4 / Propriété des fonctions de Hash	. 6

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

```
Invite de commandes
                                                                                                                                                                                                                                                                                                                                                                                          :\netcat>nc -vv www.google.fr 80
  DNS fwd/rev mismatch: www.google.fr != ham02s14-in-f195.1e100.net
www.google.fr [172.217.18.195] 80 (http) open
  HTTP/1.0 400 Bad Request
  Content-Type: text/html; charset=UTF-8
  Referrer-Policy: no-referrer
Content-Length: 1555
   Date: Wed, 05 Feb 2020 15:58:46 GMT
  <!DOCTYPE html>
       <meta charset=utf-8>
       <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width">
      <title>Error 400 (Bad Request)!!1</title>

<title>Error 400 (Bad Request)!!!</title>
<tstyle>

*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{mar
gin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/error
s/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:
none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}
}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-le
ft:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/
2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/google
logo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/branding/google
logo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/branding/google
logo/2x/googlelogo_color_150x54dp.png) no-repeat;-webkit-background-size:100% 1
0///www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat;-webkit-background-size:100% 1
0///www.google.c
     0%}}#logo{display:inline-block;height:54px;width:150px}
      </style>
       <a href=//www.google.com/><span id=logo aria-label=Google></span></a>
       <b>400.</b> <ins>ThatÔÇÖs an error.</ins>
       Your client has issued a malformed or illegal request. <ins>ThatÔÇÖs all we know.</ins>
    sent 6, rcvd 1712: NOTSOCK
     :\netcat>
```

Je lance netcat et je me connecte sur le serveur de google, grâce à la commande nc -vv 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 »

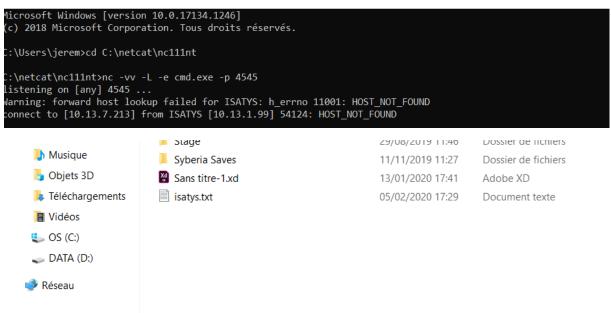
```
C:\netcat>nc -vv -L -p 4545
listening on [any] 4545 ...
Warning: forward host lookup failed for ISATYS: h_errno 11001: HOST_NOT_FOUND
connect to [10.13.7.213] from ISATYS [10.13.1.99] 62426: HOST_NOT_FOUND

njhjnj
coucou

C:\Users\zazar\Documents\Netcat>Nc -vv 10.13.7.213 4545
Warning: forward host lookup failed for LAPTOP-V3FDQQ78: h_errno 11001: HOST_NOT_FOUND
LAPTOP-V3FDQQ78 [10.13.7.213] 4545 (?) open
njhjnj
coucou
```

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

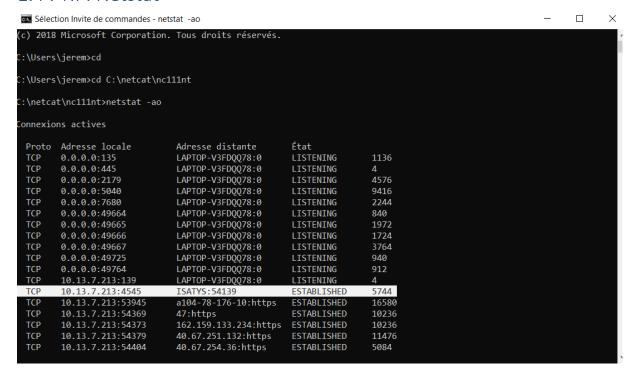


```
C:\netcat>cd C:\Users\jerem\Documents
cd C:\Users\jerem\Documents
C:\Users\jerem\Documents>ls
ls
'ls' n'est pas reconnu en tant que commande interne
ou externe, un programme exécutable ou un fichier de commandes.
C:\Users\jerem\Documents>dir
dir
 Le volume dans le lecteur C s'appelle OS
Le numéro de série du volume est C678–4E5D
 Répertoire de C:\Users\jerem\Documents
05/02/2020
05/02/2020
10/11/2019
29/08/2019
29/08/2019
                17:29
17:29
                              <DIR>
                 18:50
                                                   American Truck Simulator
                              <DIR>
                 10:44
                              <DIR>
                                                   Arduino
                                                   ArduinoData
                 10:45
                              <DIR>
29/08/2019
29/08/2019
29/08/2019
17/09/2019
03/11/2019
02/10/2019
                                                   build-test-Desktop_Qt_5_11_2_MinGW_32bit-Debug
build-untitled-Desktop_Qt_5_11_2_MinGW_32bit-Debug
                 10:45
10:45
                              <DIR>
                              <DIR>
                 11:41
22:29
                              <DIR>
                                                   Camera Roll
                              <DIR>
                                                   Downloads
                 18:44
                              <DIR>
                                                   Electronic Arts
                                                   Frontier Developments
Modèles Office personnalisés
19/11/2019
01/10/2019
                 16:34
                              <DIR>
10/12/2019
15/01/2020
02/10/2019
13/01/2020
29/08/2019
                 10:48
10:40
08:23
                             <DIR>
                                                   My Cheat Tables
My Games
                              <DIR>
                                                   Processing
                                         65 294 Sans titre-1.xd
                 17:41
                 10:46
11:27
                              <DIR>
                                                   Stage
11/11/2019
                              <DIR>
                                                   Syberia Saves
                   29 0 txt.txt
2 fichier(s) 65 294 octets
17 Rép(s) 15 991 283 712 octets libres
05/02/2020
                17:29
C:\Users\jerem\Documents>ren txt.txt isatys.txt
ren txt.txt isatys.txt
C:\Users\jerem\Documents>
```

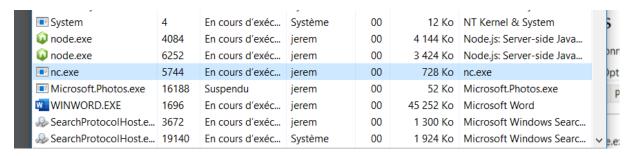
# C:\Users\jerem\Documents>del isatys.txt del isatys.txt

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

```
Algorithm : SHA256
        : E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
Hash
        : C:\Users\jerem\Documents\Cours\secu.txt
Path
PS C:\Users\jerem\Documents\Cours> <mark>Get-FileHash .\</mark>secu.txt -Algorithm SHA256 | Format-List
Algorithm : SHA256
        : 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
Hash
Path
        : C:\Users\jerem\Documents\Cours\secu.txt
PS C:\Users\jerem\Documents\Cours> Get-FileHash .\securite.txt -Algorithm SHA256 | Format-List
Algorithm : SHA256
        : 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
Hash
Path
        : C:\Users\jerem\Documents\Cours\securite.txt
```

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.