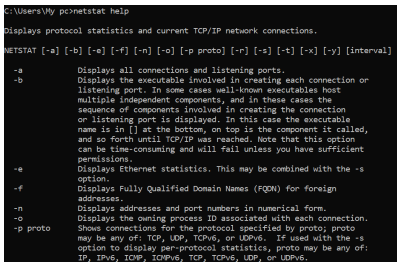
Nom : **LAGUERRE**
Prénom : **Rithler**
Université : **UNITECH**
Concentration : **CyberSecurity**
Cours : **GESTION DES RISQUES INFORMATIQUES**
Professeur : **Austin Waffo Kouhoué**

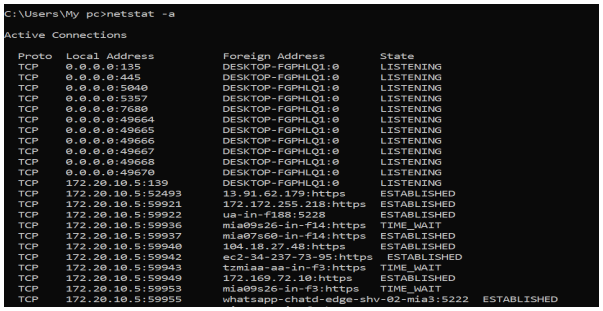
DESS en Technologie de l'Information

EXERCICES D'APPLICATION

netstat est un outil puissant pour surveiller les connexions réseau, les ports ouverts et les statistiques réseau. Voici des exercices pratiques avec corrections pour mieux comprendre son utilisation.
La commande **netstat help**, pour découvrir le manuel sur netstat.

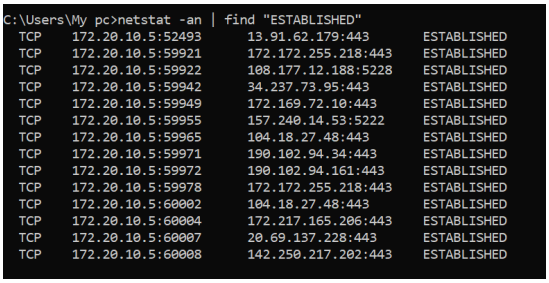


1. Lister toutes les connexions réseau actives. : **netstat -a**



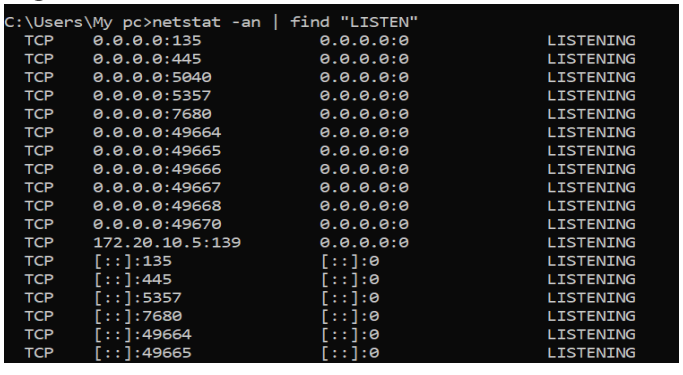
2. Identifier les connexions établies :

Lister uniquement les connexions établies sur ta machine : **netstat -an | find "ESTABLISHED"**



3. Identifier les ports en écoute

Voir quels services écoutent les connexions entrantes sur ta machine : **netstat -an | find "LISTEN"**



4. Afficher les connexions avec les noms des processus : **netstat -ano**

Associer les connexions réseau aux processus en cours d'exécution.

. chrome.exe utilise le port 55023 pour communiquer avec 93.184.216.34 (probablement un site web).

. firefox.exe utilise le port 54012 pour communiquer avec Google.

je n'ai pas trouvé les lignes correspondant aux ports 55023 et 54012 pour confirmer les connexions

tasklist /FI "PID eq 1060" & tasklist /FI "PID eq 7676"

```
C:\Users\My pc>tasklist /FI "PID eq 1060"

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
svchost.exe                   1060 Services                   0     21,084 K

C:\Users\My pc>tasklist /FI "PID eq 5355"
INFO: No tasks are running which match the specified criteria.

C:\Users\My pc>tasklist /FI "PID eq 7676"

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
chrome.exe                    7676 Console                    9    260,396 K

C:\Users\My pc>
```

5. Afficher les statistiques réseaux

Obtenir des informations sur les paquets envoyés et reçus : **netstat -s**

```
TCP Statistics for IPv4

  Active Opens                        = 10920
  Passive Opens                       = 136
  Failed Connection Attempts          = 2070
  Reset Connections                   = 2007
  Current Connections                 = 14
  Segments Received                   = 886705
  Segments Sent                       = 686911
  Segments Retransmitted              = 27830

TCP Statistics for IPv6

  Active Opens                        = 131
  Passive Opens                       = 81
  Failed Connection Attempts          = 45
  Reset Connections                   = 30
  Current Connections                 = 0
  Segments Received                   = 5141
  Segments Sent                       = 5043
  Segments Retransmitted              = 108
```

```
UDP Statistics for IPv4

  Datagrams Received    = 1018744
  No Ports              = 10887
  Receive Errors        = 1
  Datagrams Sent        = 725371

UDP Statistics for IPv6

  Datagrams Received    = 4243
  No Ports              = 0
  Receive Errors        = 0
  Datagrams Sent        = 3313

C:\Users\My pc>
```

6. Afficher la table de routage

Voir les routes utilisées par ton PC pour communiquer avec d'autres réseaux: **`netstat -r`**

```
C:\Users\My pc>netstat -r
===========================================================================
Interface List
  7...10 65 30 ea 0a 8a ......Intel(R) Ethernet Connection (4) I219-LM
 23...20 79 18 a5 73 92 ......Microsoft Wi-Fi Direct Virtual Adapter #5
  6...22 79 18 a5 73 91 ......Microsoft Wi-Fi Direct Virtual Adapter #6
 16...20 79 18 a5 73 91 ......Intel(R) Dual Band Wireless-AC 8265
 11...20 79 18 a5 73 95 ......Bluetooth Device (Personal Area Network) #2
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     172.20.10.1     172.20.10.5     55
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      172.20.10.0  255.255.255.240         On-link      172.20.10.5    311
      172.20.10.5  255.255.255.255         On-link      172.20.10.5    311
```

7. Actualiser l'affichage en temps réel

Surveiller les connexions réseau en direct (voir les connexions qui s'ouvrent et se ferment en temps réel) : **`netstat -an 4`**

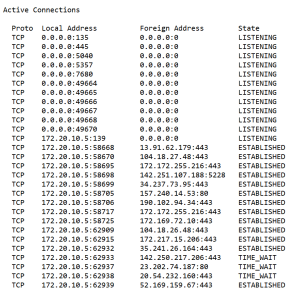
```
  TCP    [::]:49665             [::]:0                 LISTENING
  TCP    [::]:49666             [::]:0                 LISTENING
  TCP    [::]:49667             [::]:0                 LISTENING
  TCP    [::]:49668             [::]:0                 LISTENING
  TCP    [::]:49670             [::]:0                 LISTENING
  TCP    [::1]:49669            [::]:0                 LISTENING
  UDP    0.0.0.0:123            *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:5050           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5355           *:*
```

8. Lister les connexions réseau et exporter les résultats

Générer un fichier de rapport contenant toutes les connexions actives : **netstat -an > connections.txt**

9. Trouver la connexion réseau la plus active

Identifier quelle connexion génère le plus de trafic sur ta machine, après les avoir généré dans un fichier.



```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING
  TCP    172.20.10.5:139        0.0.0.0:0              LISTENING
  TCP    172.20.10.5:58668      13.91.62.179:443       ESTABLISHED
  TCP    172.20.10.5:58670      104.18.27.48:443       ESTABLISHED
  TCP    172.20.10.5:58695      172.172.255.216:443    ESTABLISHED
  TCP    172.20.10.5:58698      142.251.107.188:5228   ESTABLISHED
  TCP    172.20.10.5:58699      34.237.73.95:443       ESTABLISHED
  TCP    172.20.10.5:58705      157.240.14.53:80       ESTABLISHED
  TCP    172.20.10.5:58706      190.102.94.34:443      ESTABLISHED
  TCP    172.20.10.5:58717      172.172.255.216:443    ESTABLISHED
  TCP    172.20.10.5:58725      172.169.72.10:443      ESTABLISHED
  TCP    172.20.10.5:62909      104.18.26.48:443       ESTABLISHED
  TCP    172.20.10.5:62915      172.217.15.206:443     ESTABLISHED
  TCP    172.20.10.5:62932      35.241.26.164:443      ESTABLISHED
  TCP    172.20.10.5:62933      142.250.217.206:443    TIME_WAIT
  TCP    172.20.10.5:62937      23.202.74.187:80       TIME_WAIT
  TCP    172.20.10.5:62938      20.54.232.160:443      TIME_WAIT
  TCP    172.20.10.5:62939      52.169.159.67:443      ESTABLISHED
```

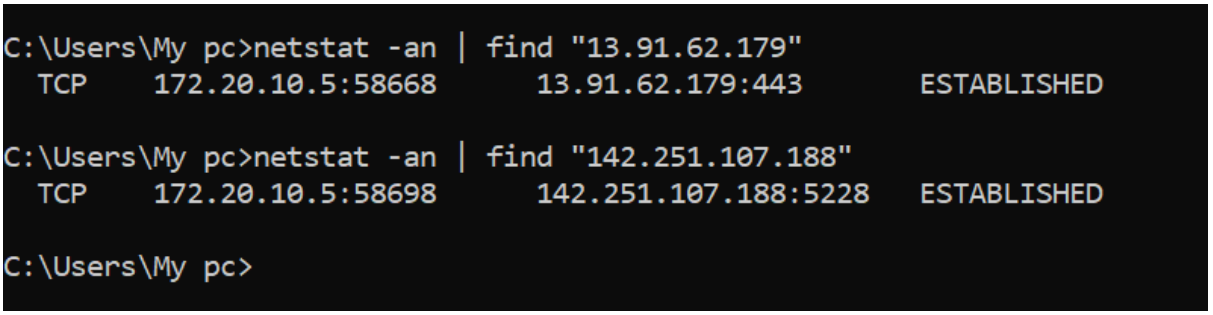
il est difficile de Trouver la connexion réseau la plus active

10. Trouver si une machine du réseau envoie trop de requêtes

Identifier un appareil qui effectue trop de connexions simultanées (ex : infection par un botnet).

Si le nombre de connexions est très élevé (+100), c'est anormal.

Vérifie quelles IP sont concernées avec : **netstat -an | find "13.91.62.179"**



```
C:\Users\My pc>netstat -an | find "13.91.62.179"
  TCP    172.20.10.5:58668      13.91.62.179:443       ESTABLISHED

C:\Users\My pc>netstat -an | find "142.251.107.188"
  TCP    172.20.10.5:58698      142.251.107.188:5228   ESTABLISHED

C:\Users\My pc>
```