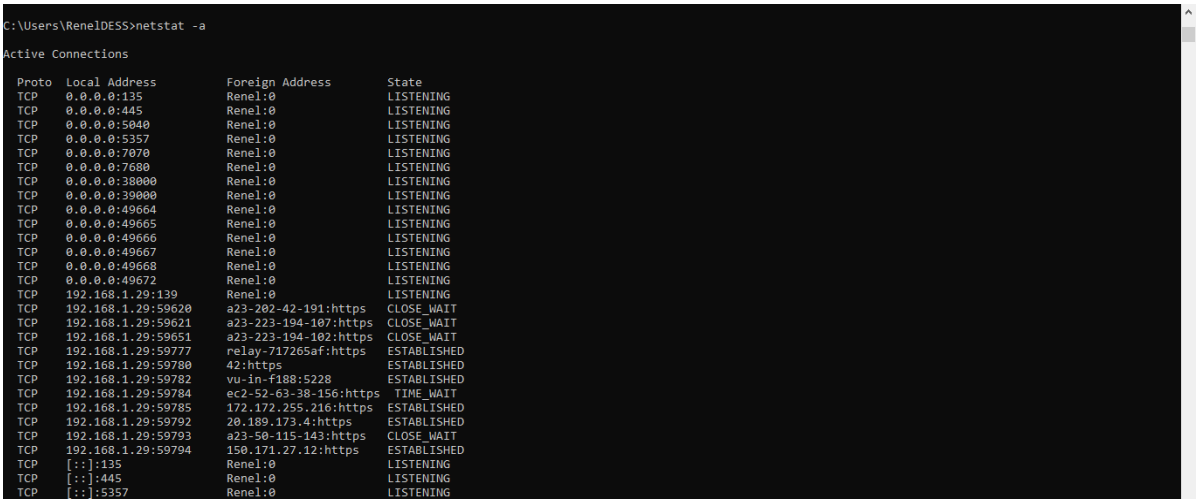
GESTION DES RISQUES INFORMATIQUES

DESS en Technologie de l'Informationion

RESOLUTION 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.

1. Lister toutes les connexions réseau actives



Netstat -a affiche toutes les connexions

2. Identifier les connexions établies

Netstat -a | findstr ESTABLISHED permet voir les connexions établies.

3. Identifier les ports en écoute

```
C:\Users\RenelDESS>netstat -ano | find "LISTENING"
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1192
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       7884
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:7070           0.0.0.0:0              LISTENING       4352
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       10824
  TCP    0.0.0.0:38000          0.0.0.0:0              LISTENING       3960
  TCP    0.0.0.0:39000          0.0.0.0:0              LISTENING       3960
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       560
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       852
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1504
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       2100
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       3928
  TCP    0.0.0.0:49672          0.0.0.0:0              LISTENING       556
  TCP    192.168.1.29:139       0.0.0.0:0              LISTENING       4
  TCP    [::]:135               [::]:0                 LISTENING       1192
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:5357              [::]:0                 LISTENING       4
  TCP    [::]:7070              [::]:0                 LISTENING       4352
  TCP    [::]:7680              [::]:0                 LISTENING       10824
  TCP    [::]:49664             [::]:0                 LISTENING       560
  TCP    [::]:49665             [::]:0                 LISTENING       852
  TCP    [::]:49666             [::]:0                 LISTENING       1504
  TCP    [::]:49667             [::]:0                 LISTENING       2100
  TCP    [::]:49668             [::]:0                 LISTENING       3928
  TCP    [::]:49672             [::]:0                 LISTENING       556
  TCP    [::1]:49669            [::]:0                 LISTENING       4684
```

Netstat -ano | findstr ”LISTENING affiche les ports en écoute.

4. Afficher les connexions avec les noms des processus

```
C:\WINDOWS\system32>netstat -b

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.29:59620     a23-202-42-191:https   CLOSE_WAIT
 [SystemSettings.exe]
  TCP    192.168.1.29:59621     a23-223-194-107:https  CLOSE_WAIT
 [SystemSettings.exe]
  TCP    192.168.1.29:59777     relay-717265af:https   ESTABLISHED
 [AnyDesk.exe]
  TCP    192.168.1.29:59782     vu-in-f188:5228        ESTABLISHED
 [chrome.exe]
  TCP    192.168.1.29:59785     172.172.255.216:https  ESTABLISHED
  WpnService
 [svchost.exe]
  TCP    192.168.1.29:59811     a23-223-194-102:https  ESTABLISHED
 [chrome.exe]
  TCP    192.168.1.29:59812     a23-223-194-102:https  ESTABLISHED
 [SearchApp.exe]
  TCP    192.168.1.29:59813     a23-223-194-102:https  ESTABLISHED
 [SearchApp.exe]
  TCP    192.168.1.29:59814     a23-223-194-102:https  ESTABLISHED
 [SearchApp.exe]
  TCP    192.168.1.29:59815     a23-4-43-62:http       ESTABLISHED
 [SearchApp.exe]
  TCP    192.168.1.29:59816     a23-223-194-107:https  ESTABLISHED
 [SearchApp.exe]
  TCP    192.168.1.29:59817     a23-223-194-107:https  ESTABLISHED
 [SearchApp.exe]
  TCP    192.168.1.29:59818     a23-223-194-107:https  ESTABLISHED
 [SearchApp.exe]
  TCP    192.168.1.29:59819     a23-223-194-107:https  ESTABLISHED
 [SearchApp.exe]
  TCP    192.168.1.29:59820     a23-223-194-107:https  ESTABLISHED
 [SearchApp.exe]
  TCP    192.168.1.29:59821     a23-223-194-107:https  ESTABLISHED
 [SearchApp.exe]
```

Netstat -b affiche les connexions avec les noms des processus

5. Afficher les statistiques réseaux

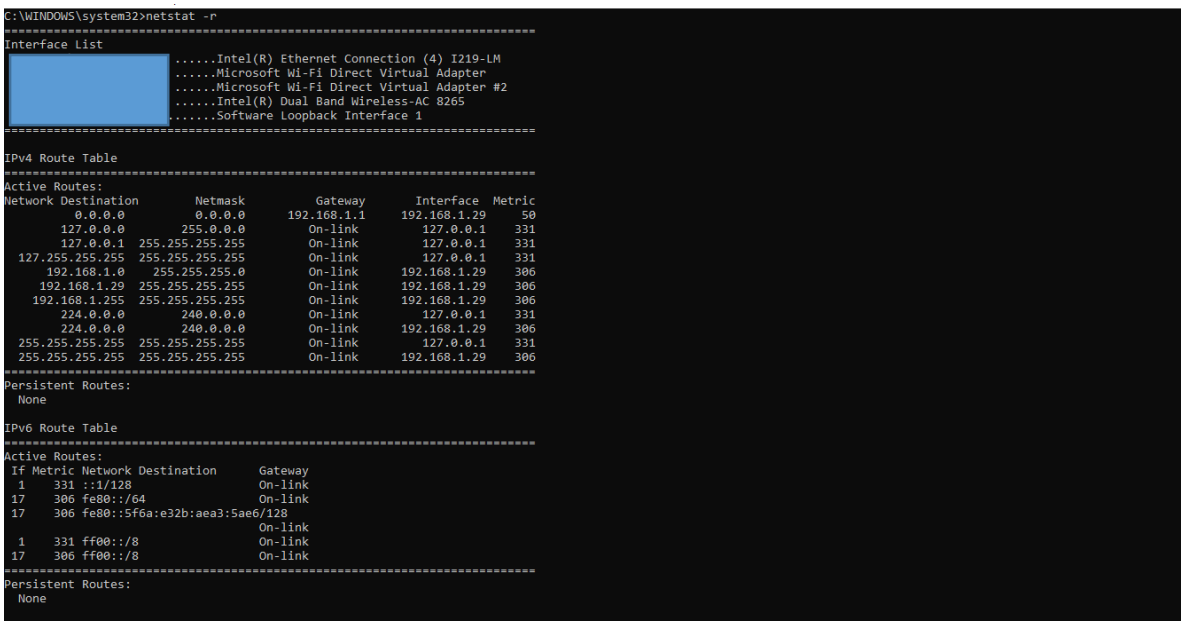
```
C:\WINDOWS\system32>netstat -e
Interface Statistics

                           Received            Sent

Bytes                     981256101        57399706
Unicast packets              435036          347011
Non-unicast packets           67599            5089
Discards                          0               0
Errors                            0               0
Unknown protocols                 0
```

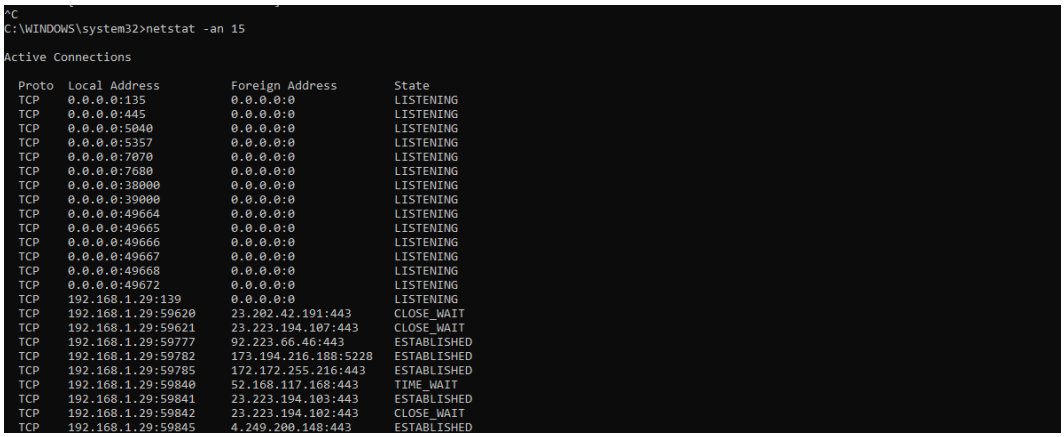
Netstat –e permet de voir les paquets envoyés et reçus.

6. Afficher la table de routage



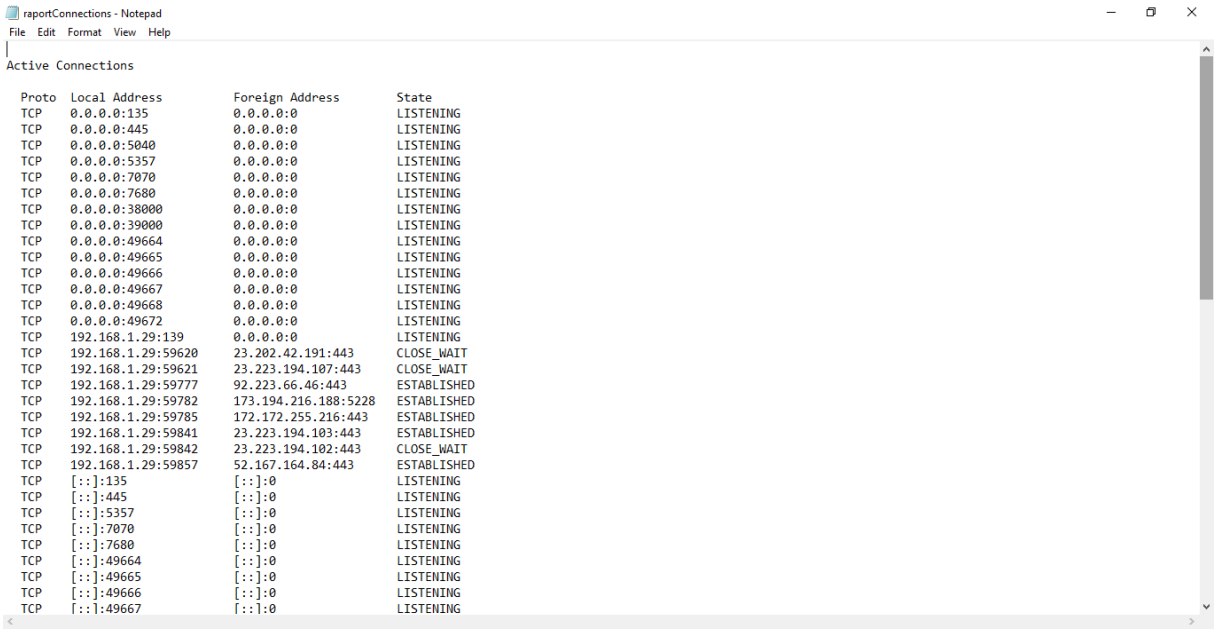
Netstat –r permet de voir la table de routage.

7. Actualiser l’affichage en temps réel



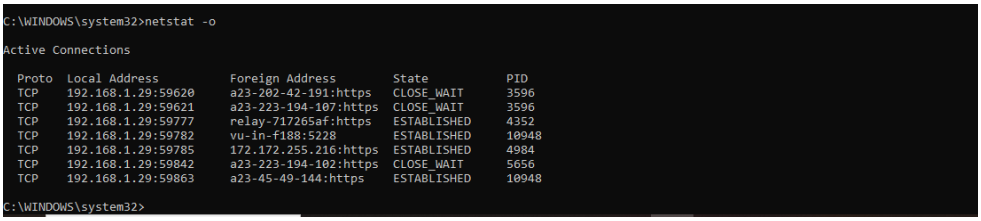
netstat –an 5 où 15 actualise l’affichage

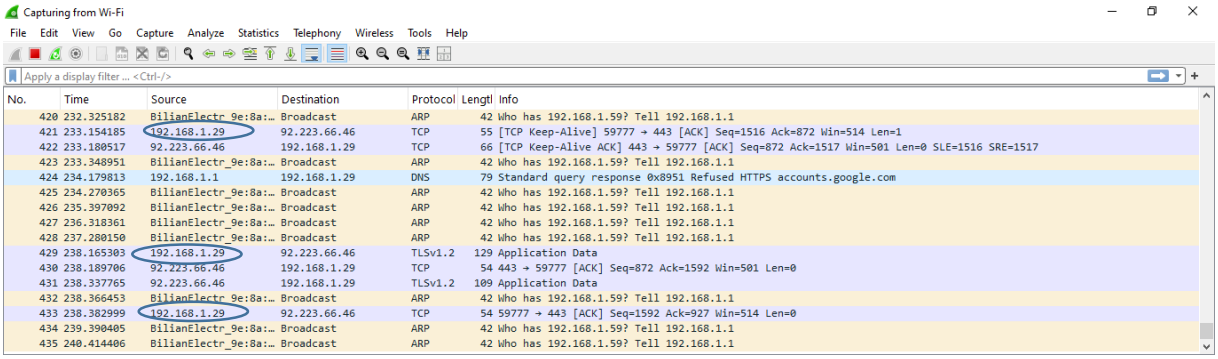
8. Lister les connexions réseau et exporter les résultats



Netstat –an permet d'exporter les résultats C:\raportConnections c'est le chemin parcourus pour stockés les résultats.

9. Trouver la connexion réseau la plus active





Netstat -o fait connaitre la connexion la plus active

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

```
C:\WINDOWS\system32>netstat -ano | findstr 192.168.1.29
  TCP    192.168.1.29:139       0.0.0.0:0              LISTENING       4
  TCP    192.168.1.29:59620     23.202.42.191:443      CLOSE_WAIT      3596
  TCP    192.168.1.29:59621     23.223.194.107:443     CLOSE_WAIT      3596
  TCP    192.168.1.29:59777     92.223.66.46:443       ESTABLISHED     4352
  TCP    192.168.1.29:59782     173.194.216.188:5228   ESTABLISHED     10948
  TCP    192.168.1.29:59785     172.172.255.216:443    ESTABLISHED     4984
  TCP    192.168.1.29:59842     23.223.194.102:443     CLOSE_WAIT      5656
  TCP    192.168.1.29:59871     23.223.194.102:443     ESTABLISHED     10948
  TCP    192.168.1.29:59880     23.221.212.208:443     ESTABLISHED     5124
  TCP    192.168.1.29:59884     200.58.246.138:443     ESTABLISHED     5124
  UDP    192.168.1.29:137       *:*                                    4
  UDP    192.168.1.29:138       *:*                                    4
  UDP    192.168.1.29:1900      *:*                                    7408
  UDP    192.168.1.29:2177      *:*                                    9900
  UDP    192.168.1.29:57120     *:*                                    7408
```