

```
C:\WINDOWS\system32>netstat -an | find /i "ESTABLISHED"
TCP    192.168.1.13:49202    192.168.1.18:445    ESTABLISHED
TCP    192.168.1.13:49214    157.56.124.164:443  ESTABLISHED
TCP    192.168.1.13:49264    64.15.116.121:443   ESTABLISHED
TCP    192.168.1.13:49373    192.168.1.10:3389   ESTABLISHED
TCP    192.168.1.13:49387    64.15.116.57:443    ESTABLISHED
TCP    192.168.1.13:49388    64.15.116.57:443    ESTABLISHED
TCP    192.168.1.13:49389    64.15.116.149:443   ESTABLISHED
TCP    192.168.1.13:49390    64.15.116.149:443   ESTABLISHED
TCP    192.168.1.13:49391    64.15.116.27:443    ESTABLISHED
TCP    192.168.1.13:49392    64.15.116.27:443    ESTABLISHED
TCP    192.168.1.13:49393    216.58.208.198:443  ESTABLISHED
TCP    192.168.1.13:49394    216.58.208.198:443  ESTABLISHED
TCP    192.168.1.13:49395    216.58.211.66:443   ESTABLISHED
TCP    192.168.1.13:49396    216.58.211.66:443   ESTABLISHED
TCP    192.168.1.13:49397    64.15.116.108:443    ESTABLISHED
TCP    192.168.1.13:49398    64.15.116.108:443    ESTABLISHED
TCP    192.168.1.13:49401    173.194.45.89:443   ESTABLISHED
TCP    192.168.1.13:49402    173.194.45.89:443   ESTABLISHED
TCP    192.168.1.13:49403    64.15.116.148:443    ESTABLISHED
TCP    192.168.1.13:49404    64.15.116.148:443    ESTABLISHED
TCP    192.168.1.13:49405    216.58.208.194:443  ESTABLISHED
TCP    192.168.1.13:49406    216.58.208.194:443  ESTABLISHED
TCP    192.168.1.13:49407    64.15.116.185:443    ESTABLISHED
TCP    192.168.1.13:49408    64.15.116.185:443    ESTABLISHED
TCP    192.168.1.13:49409    64.15.116.56:443    ESTABLISHED
TCP    192.168.1.13:49410    64.15.116.56:443    ESTABLISHED
TCP    192.168.1.13:49411    64.15.116.149:443    ESTABLISHED
TCP    192.168.1.13:49412    64.15.116.149:443    ESTABLISHED
TCP    192.168.1.13:49413    64.15.116.149:443    ESTABLISHED
TCP    192.168.1.13:49414    216.58.208.193:443  ESTABLISHED
TCP    192.168.1.13:49415    216.58.208.193:443  ESTABLISHED
TCP    192.168.1.13:49416    216.58.208.193:443  ESTABLISHED
```

À gauche sont énumérées les adresses locales et à droite les adresses distantes.

Dans cet exemple, nous nous rendons compte que l'adresse IP de l'ordinateur est 192.168.1.13. Une connexion est établie vers un ordinateur possédant l'adresse IP 64.15.116.57. Cela correspond au site français de Google. Par ailleurs, le port d'écoute est le 443 (utilisé pour l'affichage de pages web).

La commande `netstat -o` liste l'ID du processus utilisé pour chaque connexion.

Une vue complète est offerte par la commande `netstat -a` (ports fermés, ouverts et utilisés).

Afin d'afficher les applications qui communiquent vers l'extérieur, saisissez cette commande : `netstat -b 5 > log.txt`

Au bout de quelques minutes, appuyez sur les touches [Ctrl][C] afin d'interrompre l'exécution de la commande. Saisissez ensuite cette commande : `notepad log.txt`. Le fichier journal qui a été généré s'affichera dans le Bloc-notes Windows.

5. nbtstat

C'est l'équivalent de la commande `netstat` mais pour les connexions NetBIOS over TCP/IP. Il est également possible par cette commande de recharger le fichier `Lmhosts` dans le cache NetBIOS.

- `-a <nom distant>` : affiche la table des noms d'une station distante en utilisant son nom NetBIOS.
- `-A <adresse IP>` : idem que précédemment mais en utilisant son adresse IP.
- `-C` : affiche le contenu du cache de noms NetBIOS, la table de noms NetBIOS et les adresses IP correspondantes.
- `-n` : affiche la table de noms NetBIOS de l'ordinateur local.
- `-r` : affiche les statistiques de la résolution de noms NetBIOS.
- `-R` : purge et recharge le fichier `LmHosts` sans avoir à redémarrer l'ordinateur.
- `-RR` : libère puis actualise les noms NetBIOS pour l'ordinateur local inscrit par des serveurs WINS.