GESTION DES RISQUES INFORMATIQUES

DESS en Technologie de l'Information

Lamarre JOSEPH

lamarrejoseph@gmail.com

APRIL 1, 2025

UNITECH

Professeur: Austin WaffoKouhoué

GESTION DES RISQUES INFORMATIQUES

DESS en Technologie de l'Information

EXERCICES D'APPLICATION

En utilisant la commande **netstat help**, pour découvrir le manuel sur netstat. On utilise le manuel pour répondre aux questions suivantes.

1. **Lister toutes les connexions réseaux actives**

Active Connections `netstat -a`

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	PC-DESS:0	LISTENING
TCP	0.0.0.0:445	PC-DESS:0	LISTENING
TCP	0.0.0.0:623	PC-DESS:0	LISTENING
TCP	0.0.0.0:5040	PC-DESS:0	LISTENING
TCP	0.0.0.0:16992	PC-DESS:0	LISTENING
TCP	0.0.0.0:49664	PC-DESS:0	LISTENING
TCP	0.0.0.0:49665	PC-DESS:0	LISTENING
TCP	0.0.0.0:49666	PC-DESS:0	LISTENING
TCP	0.0.0.0:49667	PC-DESS:0	LISTENING
TCP	0.0.0.0:49668	PC-DESS:0	LISTENING
TCP	0.0.0.0:49670	PC-DESS:0	LISTENING
TCP	127.0.0.1:57907	PC-DESS:57908	ESTABLISHED
TCP	127.0.0.1:57908	PC-DESS:57907	ESTABLISHED
TCP	127.0.0.1:58169	PC-DESS:58170	ESTABLISHED
TCP	127.0.0.1:58170	PC-DESS:58169	ESTABLISHED
TCP	127.0.0.1:58171	PC-DESS:58172	ESTABLISHED
TCP	127.0.0.1:58172	PC-DESS:58171	ESTABLISHED
TCP	192.168.0.40:139	PC-DESS:0	LISTENING
TCP	192.168.0.40:57894	172.172.255.218:https	ESTABLISHED
TCP	192.168.0.40:57896	172.172.255.218:https	ESTABLISHED

```
TCP    192.168.0.40:58195     34.107.243.93:https    ESTABLISHED
TCP    192.168.0.40:58302     23.223.194.111:https   CLOSE_WAIT
TCP    192.168.0.40:58305     23.13.145.132:http     CLOSE_WAIT
TCP    192.168.0.40:58306     123:https              TIME_WAIT
TCP    192.168.0.40:58307     204.79.197.222:https   ESTABLISHED
TCP    192.168.0.40:58366     40.74.98.192:https     FIN_WAIT_1
TCP    192.168.0.40:58367     45.68.42.101:http      ESTABLISHED
TCP    192.168.0.40:58422     8.243.166.77:http      ESTABLISHED
TCP    192.168.0.40:58441     8.243.166.77:http      ESTABLISHED
TCP    192.168.0.40:58446     23.13.145.132:http     ESTABLISHED
TCP    192.168.0.40:58447     45.68.42.101:http      ESTABLISHED
TCP    192.168.0.40:58448     13.89.179.11:https     ESTABLISHED
TCP    192.168.0.40:58449     45.68.42.101:http      ESTABLISHED
TCP    192.168.0.40:58450     45.68.42.101:http      ESTABLISHED
TCP    [::]:135               PC-DESS:0              LISTENING
TCP    [::]:445               PC-DESS:0              LISTENING
TCP    [::]:623               PC-DESS:0              LISTENING
TCP    [::]:16992             PC-DESS:0              LISTENING
TCP    [::]:49664             PC-DESS:0              LISTENING
TCP    [::]:49665             PC-DESS:0              LISTENING
TCP    [::]:49666             PC-DESS:0              LISTENING
TCP    [::]:49667             PC-DESS:0              LISTENING
TCP    [::]:49668             PC-DESS:0              LISTENING
TCP    [::]:49670             PC-DESS:0              LISTENING
TCP    [::1]:49669            PC-DESS:0              LISTENING
UDP    0.0.0.0:5050           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5355           *:*
```

```
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:49664        *:*
  UDP    127.0.0.1:61130        *:*
  UDP    127.0.0.1:63187        *:*
  UDP    192.168.0.40:137       *:*
  UDP    192.168.0.40:138       *:*
  UDP    192.168.0.40:1900      *:*
  UDP    192.168.0.40:63186     *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5355              *:*
  UDP    [::1]:1900             *:*
  UDP    [::1]:63185            *:*
  UDP    [fe80::6639:9b6c:ad28:9f64%10]:1900  *:*
  UDP    [fe80::6639:9b6c:ad28:9f64%10]:63184  *:*
```

2. Identifier les connexions établies

Lister uniquement les connexions établies sur ta machine.

```
netstat -bano | find "ESTABLISHED"
```

```
C:\windows\system32>netstat -bano | find "ESTABLISHED"
  TCP    10.65.10.78:54076      172.172.255.216:443    ESTABLISHED     4436
  TCP    10.65.10.78:54297      34.107.243.93:443      ESTABLISHED     6720
  TCP    10.65.10.78:54375      31.13.80.53:443        ESTABLISHED     6720
  TCP    10.65.10.78:54497      35.174.127.31:443      ESTABLISHED     6720
  TCP    10.65.10.78:54870      54.175.249.133:443     ESTABLISHED     13464
  TCP    10.65.10.78:55001      104.18.26.90:443       ESTABLISHED     6720
  TCP    10.65.10.78:55011      8.8.8.8:443            ESTABLISHED     7224
  TCP    10.65.10.78:55036      20.189.173.28:443      ESTABLISHED     1680
  TCP    127.0.0.1:53893        127.0.0.1:53894        ESTABLISHED     4340
  TCP    127.0.0.1:53894        127.0.0.1:53893        ESTABLISHED     4340
  TCP    127.0.0.1:54282        127.0.0.1:54283        ESTABLISHED     6720
  TCP    127.0.0.1:54283        127.0.0.1:54282        ESTABLISHED     6720
  TCP    127.0.0.1:54284        127.0.0.1:54285        ESTABLISHED     13656
  TCP    127.0.0.1:54285        127.0.0.1:54284        ESTABLISHED     13656
```

3. Identifier les ports en écoute

Voir quels services écoutent les connexions entrantes sur ta machine.

```
C:\windows\system32>netstat -ano | find "LISTENING"
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1036
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:623            0.0.0.0:0              LISTENING       4340
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       4148
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       4604
  TCP    0.0.0.0:16992          0.0.0.0:0              LISTENING       4340
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       888
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       808
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1596
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       2480
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       3836
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       880
  TCP    10.65.10.78:139        0.0.0.0:0              LISTENING       4
  TCP    [::]:135               [::]:0                 LISTENING       1036
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:623               [::]:0                 LISTENING       4340
  TCP    [::]:7680              [::]:0                 LISTENING       4604
  TCP    [::]:16992             [::]:0                 LISTENING       4340
  TCP    [::]:49664             [::]:0                 LISTENING       888
  TCP    [::]:49665             [::]:0                 LISTENING       808
  TCP    [::]:49666             [::]:0                 LISTENING       1596
  TCP    [::]:49667             [::]:0                 LISTENING       2480
  TCP    [::]:49668             [::]:0                 LISTENING       3836
  TCP    [::]:49670             [::]:0                 LISTENING       880
  TCP    [::1]:49669            [::]:0                 LISTENING       4288
```

4. Afficher les connexions avec les noms des processus

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

netstat -bano

 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.

```
  TCP    10.65.10.78:54076      172.172.255.216:443    ESTABLISHED     4436
  WpnService
 [svchost.exe]
  TCP    10.65.10.78:54297      34.107.243.93:443      ESTABLISHED     6720
 [firefox.exe]
  TCP    10.65.10.78:54375      31.13.80.53:443        ESTABLISHED     6720
 [firefox.exe]
  TCP    10.65.10.78:54497      35.174.127.31:443      ESTABLISHED     6720
 [firefox.exe]
  TCP    10.65.10.78:54827      108.174.10.24:443      CLOSE_WAIT      5456
 [SearchApp.exe]
  TCP    10.65.10.78:54870      54.175.249.133:443     ESTABLISHED     13464
 [AcroCEF.exe]
  TCP    10.65.10.78:54920      34.120.208.123:443     TIME_WAIT       0
  TCP    10.65.10.78:54940      104.18.26.90:443       ESTABLISHED     6720
 [firefox.exe]
```

5. Afficher les statistiques réseaux

Obtenir des informations sur les paquets envoyés et reçus.

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

                           Received            Sent

Bytes                     158766307       151824484
Unicast packets              164332          129444
Non-unicast packets               0            1617
Discards                          0               0
Errors                            0               0
Unknown protocols                 0
```

6. Afficher la table de routage

Voir les routes utilisées par ton PC pour communiquer avec d'autres réseaux.

```
C:\Users\Lamarre Joseph>netstat -e
Interface Statistics

                           Received            Sent

Bytes                      8129583          3553592
Unicast packets              16387            14455
Non-unicast packets             21              504
Discards                         0                0
Errors                           0                0
Unknown protocols                0

C:\Users\Lamarre Joseph>netstat -r
===========================================================================
Interface List
 14...e8 6a 64 fe 6a 54 ......Intel(R) Ethernet Connection (4) I219-LM
  9...48 89 e7 2a 5c 43 ......Microsoft Wi-Fi Direct Virtual Adapter
 15...4a 89 e7 2a 5c 42 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 10...48 89 e7 2a 5c 42 ......Intel(R) Dual Band Wireless-AC 8265
  7...48 89 e7 2a 5c 46 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.150.1  192.168.150.102     50
        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
    192.168.150.0    255.255.255.0         On-link   192.168.150.102    306
  192.168.150.102  255.255.255.255         On-link   192.168.150.102    306
  192.168.150.255  255.255.255.255         On-link   192.168.150.102    306
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link   192.168.150.102    306
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link   192.168.150.102    306
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
 10    306 fe80::/64                On-link
 10    306 fe80::6639:9b6c:ad28:9f64/128
                                    On-link
  1    331 ff00::/8                 On-link
 10    306 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

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)

```
C:\windows\system32>netstat -ano 2

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1036
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:623            0.0.0.0:0              LISTENING       4340
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       4148
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       4604
  TCP    0.0.0.0:16992          0.0.0.0:0              LISTENING       4340
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       888
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       808
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1596
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       2480
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       3836
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       880
  TCP    10.65.10.78:139        0.0.0.0:0              LISTENING       4
  TCP    10.65.10.78:54076      172.172.255.216:443    ESTABLISHED     4436
  TCP    10.65.10.78:54297      34.107.243.93:443      ESTABLISHED     6720
  TCP    10.65.10.78:54375      31.13.80.53:443        ESTABLISHED     6720
  TCP    10.65.10.78:54497      35.174.127.31:443      ESTABLISHED     6720
  TCP    10.65.10.78:54827      108.174.10.24:443      CLOSE_WAIT      5456
  TCP    10.65.10.78:55109      104.18.26.90:443       ESTABLISHED     6720
  TCP    10.65.10.78:55110      104.18.20.157:443      ESTABLISHED     6720
  TCP    10.65.10.78:55111      8.45.52.230:443        TIME_WAIT       0
  TCP    10.65.10.78:55112      8.45.52.230:443        TIME_WAIT       0
  TCP    10.65.10.78:55114      8.45.52.230:443        ESTABLISHED     6720
  TCP    10.65.10.78:55115      8.45.52.230:443        TIME_WAIT       0
  TCP    10.65.10.78:55116      8.45.52.230:443        ESTABLISHED     6720
  TCP    10.65.10.78:55119      151.101.16.193:443     ESTABLISHED     6720
  TCP    10.65.10.78:55139      34.149.100.209:443     ESTABLISHED     6720
  TCP    10.65.10.78:55140      34.160.144.191:443     ESTABLISHED     6720
  TCP    10.65.10.78:55141      34.107.221.82:80       SYN_SENT        6720
  TCP    10.65.10.78:55142      34.117.188.166:443     ESTABLISHED     6720
  TCP    10.65.10.78:55143      34.107.221.82:80       SYN_SENT        6720
  TCP    127.0.0.1:53893        127.0.0.1:53894        ESTABLISHED     4340
  TCP    127.0.0.1:53894        127.0.0.1:53893        ESTABLISHED     4340
  TCP    127.0.0.1:54282        127.0.0.1:54283        ESTABLISHED     6720
  TCP    127.0.0.1:54283        127.0.0.1:54282        ESTABLISHED     6720
  TCP    127.0.0.1:54284        127.0.0.1:54285        ESTABLISHED     13656
  TCP    127.0.0.1:54285        127.0.0.1:54284        ESTABLISHED     13656
  TCP    [::]:135               [::]:0                 LISTENING       1036
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:623               [::]:0                 LISTENING       4340
  TCP    [::]:7680              [::]:0                 LISTENING       4604
  TCP    [::]:16992             [::]:0                 LISTENING       4340
  TCP    [::]:49664             [::]:0                 LISTENING       888
  TCP    [::]:49665             [::]:0                 LISTENING       808
  TCP    [::]:49666             [::]:0                 LISTENING       1596
  TCP    [::]:49667             [::]:0                 LISTENING       2480
  TCP    [::]:49668             [::]:0                 LISTENING       3836
  TCP    [::]:49670             [::]:0                 LISTENING       880
  TCP    [::1]:49669            [::]:0                 LISTENING       4288
```

8. Lister les connexions réseau et exporter les résultats

Générer un fichier de rapport contenant toutes les connexions actives.

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	1036
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:623	0.0.0.0:0	LISTENING	4340
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING	4148
TCP	0.0.0.0:7680	0.0.0.0:0	LISTENING	4604
TCP	0.0.0.0:16992	0.0.0.0:0	LISTENING	4340
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	888
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	808
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	1596
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	2480
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	3836
TCP	0.0.0.0:49670	0.0.0.0:0	LISTENING	880
TCP	10.65.10.78:139	0.0.0.0:0	LISTENING	4
TCP	10.65.10.78:54076	172.172.255.216:443	ESTABLISHED	4436
TCP	10.65.10.78:54375	31.13.80.53:443	ESTABLISHED	6720
TCP	10.65.10.78:54497	35.174.127.31:443	ESTABLISHED	6720
TCP	10.65.10.78:54827	108.174.10.24:443	CLOSE_WAIT	5456
TCP	10.65.10.78:55210	104.18.26.90:443	TIME_WAIT	0
TCP	10.65.10.78:55211	8.8.4.4:443	TIME_WAIT	0
TCP	10.65.10.78:55225	8.45.52.230:443	TIME_WAIT	0
TCP	10.65.10.78:55227	8.45.52.230:443	TIME_WAIT	0
TCP	10.65.10.78:55232	34.110.207.168:443	TIME_WAIT	0
TCP	10.65.10.78:55233	34.117.14.220:443	TIME_WAIT	0
TCP	10.65.10.78:55234	34.107.141.31:443	TIME_WAIT	0

TCP	10.65.10.78:55235	35.186.227.140:443	TIME_WAIT	0
TCP	10.65.10.78:55239	34.107.243.93:443	TIME_WAIT	0
TCP	10.65.10.78:55240	34.107.243.93:443	ESTABLISHED	6720
TCP	10.65.10.78:55241	34.149.100.209:443	TIME_WAIT	0
TCP	10.65.10.78:55262	34.120.208.123:443	ESTABLISHED	6720
TCP	10.65.10.78:55273	20.189.173.15:443	TIME_WAIT	0
TCP	10.65.10.78:55274	40.69.42.241:443	TIME_WAIT	0
TCP	10.65.10.78:55276	52.183.205.142:443	TIME_WAIT	0
TCP	10.65.10.78:55279	23.43.46.149:443	ESTABLISHED	4604
TCP	10.65.10.78:55280	8.8.4.4:443	ESTABLISHED	7224
TCP	10.65.10.78:55282	23.223.194.112:443	ESTABLISHED	7224
TCP	10.65.10.78:55284	23.219.155.144:443	ESTABLISHED	7224
TCP	10.65.10.78:55287	23.43.46.149:443	ESTABLISHED	4604
TCP	10.65.10.78:55288	23.43.46.149:443	ESTABLISHED	4604
TCP	10.65.10.78:55289	23.219.155.143:443	ESTABLISHED	7224
TCP	10.65.10.78:55292	23.221.212.210:443	ESTABLISHED	2076
TCP	10.65.10.78:55293	23.221.212.210:443	ESTABLISHED	2076
TCP	10.65.10.78:55301	52.109.6.63:443	TIME_WAIT	0
TCP	10.65.10.78:55304	104.18.26.90:443	ESTABLISHED	6720
TCP	10.65.10.78:55305	8.45.52.230:443	ESTABLISHED	6720
TCP	10.65.10.78:55306	8.45.52.230:443	ESTABLISHED	6720
TCP	10.65.10.78:55307	104.18.20.157:443	ESTABLISHED	6720
TCP	10.65.10.78:55343	23.43.46.149:443	ESTABLISHED	4604
TCP	10.65.10.78:55344	23.43.46.149:443	ESTABLISHED	4604
TCP	10.65.10.78:55345	23.43.46.149:443	ESTABLISHED	4604
TCP	127.0.0.1:53893	127.0.0.1:53894	ESTABLISHED	4340
TCP	127.0.0.1:53894	127.0.0.1:53893	ESTABLISHED	4340
TCP	127.0.0.1:54282	127.0.0.1:54283	ESTABLISHED	6720

```
TCP    127.0.0.1:54283        127.0.0.1:54282        ESTABLISHED     6720
TCP    127.0.0.1:54284        127.0.0.1:54285        ESTABLISHED     13656
TCP    127.0.0.1:54285        127.0.0.1:54284        ESTABLISHED     13656
TCP    [::]:135               [::]:0                 LISTENING       1036
TCP    [::]:445               [::]:0                 LISTENING       4
TCP    [::]:623               [::]:0                 LISTENING       4340
TCP    [::]:7680              [::]:0                 LISTENING       4604
TCP    [::]:16992             [::]:0                 LISTENING       4340
TCP    [::]:49664             [::]:0                 LISTENING       888
TCP    [::]:49665             [::]:0                 LISTENING       808
TCP    [::]:49666             [::]:0                 LISTENING       1596
TCP    [::]:49667             [::]:0                 LISTENING       2480
TCP    [::]:49668             [::]:0                 LISTENING       3836
TCP    [::]:49670             [::]:0                 LISTENING       880
TCP    [::1]:49669            [::]:0                 LISTENING       4288
UDP    0.0.0.0:123            *:*                                    13420
UDP    0.0.0.0:5050           *:*                                    4148
UDP    0.0.0.0:5353           *:*                                    3420
UDP    0.0.0.0:5355           *:*                                    3420
UDP    10.65.10.78:137        *:*                                    4
UDP    10.65.10.78:138        *:*                                    4
UDP    10.65.10.78:1900       *:*                                    11840
UDP    10.65.10.78:64167      *:*                                    11840
UDP    127.0.0.1:1900         *:*                                    11840
UDP    127.0.0.1:49664        *:*                                    4940
UDP    127.0.0.1:61130        *:*                                    2364
UDP    127.0.0.1:64168        *:*                                    11840
UDP    [::]:123               *:*                                    13420
```

UDP [::]:5353 *:* 3420

UDP [::]:5355 *:* 3420

UDP [::1]:1900 *:* 11840

UDP [::1]:64166 *:* 11840

UDP [fe80::6639:9b6c:ad28:9f64%10]:1900 *:* 11840

UDP [fe80::6639:9b6c:ad28:9f64%10]:64165 *:* 11840

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

La connexion qui génère le plus de trafic sur ma machine est :

TCP 10.65.10.78:55527 57.144.163.32:443 ESTABLISHED 6720 [firefox.exe]

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 :

Aucune machine suspecte détectée (seuil = 100 connexions)