

GESTION DES RISQUES INFORMATIQUES

DESS en Technologie de l'Information

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

```
C:\Users\RenelDESS>netstat -a
Active Connections
Proto Local Address           Foreign Address         State
TCP    0.0.0.0:135              Renel:0                 LISTENING
TCP    0.0.0.0:445              Renel:0                 LISTENING
TCP    0.0.0.0:5040             Renel:0                 LISTENING
TCP    0.0.0.0:5357             Renel:0                 LISTENING
TCP    0.0.0.0:7070             Renel:0                 LISTENING
TCP    0.0.0.0:7680             Renel:0                 LISTENING
TCP    0.0.0.0:39800            Renel:0                 LISTENING
TCP    0.0.0.0:39800            Renel:0                 LISTENING
TCP    0.0.0.0:49664            Renel:0                 LISTENING
TCP    0.0.0.0:49665            Renel:0                 LISTENING
TCP    0.0.0.0:49666            Renel:0                 LISTENING
TCP    0.0.0.0:49667            Renel:0                 LISTENING
TCP    0.0.0.0:49668            Renel:0                 LISTENING
TCP    0.0.0.0:49672            Renel:0                 LISTENING
TCP    192.168.1.29:139         Renel:0                 LISTENING
TCP    192.168.1.29:59620      a23-202-42-101:https    CLOSE_WAIT
TCP    192.168.1.29:59621      a23-223-194-107:https    CLOSE_WAIT
TCP    192.168.1.29:59651      a23-223-194-102:https    CLOSE_WAIT
TCP    192.168.1.29:59777      relay-717265af:https     ESTABLISHED
TCP    192.168.1.29:59780      42:https                 ESTABLISHED
TCP    192.168.1.29:59782      vu-in-f188:5228          ESTABLISHED
TCP    192.168.1.29:59784      ec2-52-63-38-156:https   TIME_WAIT
TCP    192.168.1.29:59785      172.172.255.216:https    ESTABLISHED
TCP    192.168.1.29:59792      20.109.173.4:https        ESTABLISHED
TCP    192.168.1.29:59793      a23-50-115-143:https     CLOSE_WAIT
TCP    192.168.1.29:59794      150.171.27.12:https       ESTABLISHED
TCP    [::]:135                 Renel:0                 LISTENING
TCP    [::]:445                 Renel:0                 LISTENING
TCP    [::]:5357                Renel:0                 LISTENING
```

Netstat -a affiche toutes les connexions

2. Identifier les connexions établies

```
operable program or batch file.
C:\Users\RenelDESS>netstat -a | findstr ESTABLISHED
TCP    192.168.1.29:59777      relay-717265af:https     ESTABLISHED
TCP    192.168.1.29:59782      vu-in-f188:5228          ESTABLISHED
TCP    192.168.1.29:59785      172.172.255.216:https    ESTABLISHED
TCP    192.168.1.29:59801      a23-50-115-146:https     ESTABLISHED
TCP    192.168.1.29:59803      52.167.164.84:https      ESTABLISHED
```

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

3. Identifier les ports en écoute

```
C:\Users\RenelDES>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 0.0.0.0:39000 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 [::]: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]
TCP 192.168.1.29:59822 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 0
```

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

6. Afficher la table de routage

```
C:\WINDOWS\system32>netstat -r
=====
Interface List
.....Intel(R) Ethernet Connection (4) I219-LM
.....Microsoft Wi-Fi Direct Virtual Adapter
.....Microsoft Wi-Fi Direct Virtual Adapter #2
.....Intel(R) Dual Band Wireless-AC 8265
.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway           Interface        Metric
0.0.0.0                    0.0.0.0          192.168.1.1       192.168.1.29     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
192.168.1.0                255.255.255.0    On-link          192.168.1.29     306
192.168.1.29               255.255.255.255  On-link          192.168.1.29     306
192.168.1.255              255.255.255.255  On-link          192.168.1.29     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          192.168.1.29     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          192.168.1.29     306
=====
Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1 331 ::1/128 On-link
17 306 fe80::/64 On-link
17 306 fe80::5f6a:e32b:aea3:5ae6/128 On-link
1 331 ff00::/8 On-link
17 306 ff00::/8 On-link
=====
Persistent Routes:
None
```

Netstat -r permet de voir la table de routage.

7. Actualiser l’affichage en temps réel

```
C:\WINDOWS\system32>netstat -an 15
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 0.0.0.0:7070             0.0.0.0:0               LISTENING
TCP 0.0.0.0:7680             0.0.0.0:0               LISTENING
TCP 0.0.0.0:38000            0.0.0.0:0               LISTENING
TCP 0.0.0.0:39000            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 0.0.0.0:49672            0.0.0.0:0               LISTENING
TCP 192.168.1.29:139        0.0.0.0:0               LISTENING
TCP 192.168.1.29:59620      23.202.42.191:443       CLOSE_WAIT
TCP 192.168.1.29:59621      23.223.194.107:443      CLOSE_WAIT
TCP 192.168.1.29:59777      92.223.66.46:443        ESTABLISHED
TCP 192.168.1.29:59782      173.194.216.188:5228    ESTABLISHED
TCP 192.168.1.29:59785      172.172.255.216:443     ESTABLISHED
TCP 192.168.1.29:59840      52.168.117.168:443      TIME_WAIT
TCP 192.168.1.29:59841      23.223.194.103:443      ESTABLISHED
TCP 192.168.1.29:59842      23.223.194.102:443      CLOSE_WAIT
TCP 192.168.1.29:59845      4.249.200.148:443       ESTABLISHED
```

netstat -an 5 ou 15 actualise l’affichage

8. Lister les connexions réseau et exporter les résultats

```
C:\WINDOWS\system32>netstat -an > C:\raportConnections.txt
C:\WINDOWS\system32>
```

raportConnections - Notepad

File Edit Format View Help

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	0.0.0.0:7070	0.0.0.0:0	LISTENING
TCP	0.0.0.0:7680	0.0.0.0:0	LISTENING
TCP	0.0.0.0:38000	0.0.0.0:0	LISTENING
TCP	0.0.0.0:39000	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	0.0.0.0:49672	0.0.0.0:0	LISTENING
TCP	192.168.1.29:139	0.0.0.0:0	LISTENING
TCP	192.168.1.29:59620	23.202.42.191:443	CLOSE_WAIT
TCP	192.168.1.29:59621	23.223.194.107:443	CLOSE_WAIT
TCP	192.168.1.29:59777	92.223.66.46:443	ESTABLISHED
TCP	192.168.1.29:59782	173.194.216.188:5228	ESTABLISHED
TCP	192.168.1.29:59785	172.172.255.216:443	ESTABLISHED
TCP	192.168.1.29:59841	23.223.194.103:443	ESTABLISHED
TCP	192.168.1.29:59842	23.223.194.102:443	CLOSE_WAIT
TCP	192.168.1.29:59857	52.167.164.84:443	ESTABLISHED
TCP	[::]:135	[::]:0	LISTENING
TCP	[::]:445	[::]:0	LISTENING
TCP	[::]:5357	[::]:0	LISTENING
TCP	[::]:7070	[::]:0	LISTENING
TCP	[::]:7680	[::]:0	LISTENING
TCP	[::]:49664	[::]:0	LISTENING
TCP	[::]:49665	[::]:0	LISTENING
TCP	[::]:49666	[::]:0	LISTENING
TCP	[::]:49667	[::]:0	LISTENING

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

C:\WINDOWS\system32>netstat -o

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	192.168.1.29:59620	a23-202-42-191:https	CLOSE_WAIT	3596
TCP	192.168.1.29:59621	a23-223-194-107:https	CLOSE_WAIT	3596
TCP	192.168.1.29:59777	relay-717265af:https	ESTABLISHED	4352
TCP	192.168.1.29:59782	vu-in-f188:5228	ESTABLISHED	10948
TCP	192.168.1.29:59785	172.172.255.216:https	ESTABLISHED	4984
TCP	192.168.1.29:59842	a23-223-194-102:https	CLOSE_WAIT	5656
TCP	192.168.1.29:59863	a23-45-49-144:https	ESTABLISHED	10948

C:\WINDOWS\system32>

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
420	232.325182	BilianElectr_9e:8a:...	Broadcast	ARP	42	Who has 192.168.1.59? Tell 192.168.1.1
421	233.154185	192.168.1.29	92.223.66.46	TCP	55	[TCP Keep-Alive] 59777 → 443 [ACK] Seq=1516 Ack=872 Win=514 Len=1
422	233.180517	92.223.66.46	192.168.1.29	TCP	66	[TCP Keep-Alive ACK] 443 → 59777 [ACK] Seq=872 Ack=1517 Win=501 Len=0 SLE=1516 SRE=1517
423	233.348951	BilianElectr_9e:8a:...	Broadcast	ARP	42	Who has 192.168.1.59? Tell 192.168.1.1
424	234.179813	192.168.1.1	192.168.1.29	DNS	79	Standard query response 0x8951 Refused HTTPS accounts.google.com
425	234.270365	BilianElectr_9e:8a:...	Broadcast	ARP	42	Who has 192.168.1.59? Tell 192.168.1.1
426	235.397092	BilianElectr_9e:8a:...	Broadcast	ARP	42	Who has 192.168.1.59? Tell 192.168.1.1
427	236.318361	BilianElectr_9e:8a:...	Broadcast	ARP	42	Who has 192.168.1.59? Tell 192.168.1.1
428	237.280150	BilianElectr_9e:8a:...	Broadcast	ARP	42	Who has 192.168.1.59? Tell 192.168.1.1
429	238.165303	192.168.1.29	92.223.66.46	TLSv1.2	129	Application Data
430	238.189706	92.223.66.46	192.168.1.29	TCP	54	443 → 59777 [ACK] Seq=872 Ack=1592 Win=501 Len=0
431	238.337765	92.223.66.46	192.168.1.29	TLSv1.2	109	Application Data
432	238.366453	BilianElectr_9e:8a:...	Broadcast	ARP	42	Who has 192.168.1.59? Tell 192.168.1.1
433	238.382999	192.168.1.29	92.223.66.46	TCP	54	59777 → 443 [ACK] Seq=1592 Ack=927 Win=514 Len=0
434	239.390405	BilianElectr_9e:8a:...	Broadcast	ARP	42	Who has 192.168.1.59? Tell 192.168.1.1
435	240.414406	BilianElectr_9e:8a:...	Broadcast	ARP	42	Who has 192.168.1.59? Tell 192.168.1.1

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    200.50.246.138:443    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
```