

Corrigé 5.2 Identification des services démarrés

1. Voici les ports que nous avons identifiés comme étant des services couramment utilisés. Ces informations ont été obtenues en téléchargeant le fichier suivant sur Internet (581Ko) : <http://www.iana.org/assignments/port-numbers>

tcpmux	1/tcp	TCP Port Service Multiplexer
tcpmux	1/udp	TCP Port Service Multiplexer
ftp	21/tcp	File Transfer [Control]
ftp	21/udp	File Transfer [Control]
telnet	23/tcp	Telnet
telnet	23/udp	Telnet
time	37/tcp	Time
time	37/udp	Time
gopher	70/tcp	Gopher
gopher	70/udp	Gopher
finger	79/tcp	Finger
finger	79/udp	Finger
pop2	109/tcp	Post Office Protocol - Version 2
pop2	109/udp	Post Office Protocol - Version 2
pop3	110/tcp	Post Office Protocol - Version 3
pop3	110/udp	Post Office Protocol - Version 3
sunrpc	111/tcp	SUN Remote Procedure Call
sunrpc	111/udp	SUN Remote Procedure Call
auth	113/tcp	Authentication Service
auth	113/udp	Authentication Service
netbios-ns	137/tcp	NETBIOS Name Service
netbios-ns	137/udp	NETBIOS Name Service
netbios-dgm	138/tcp	NETBIOS Datagram Service
netbios-dgm	138/udp	NETBIOS Datagram Service
netbios-ssn	139/tcp	NETBIOS Session Service
netbios-ssn	139/udp	NETBIOS Session Service
xdmcp	177/tcp	X Display Manager Control Protocol
xdmcp	177/udp	X Display Manager Control Protocol
exec	512/tcp	remote process execution;
#		authentication performed using
#		passwords and UNIX login names
comsat	512/udp	
biff	512/udp	used by mail system to notify users
#		of new mail received; currently
#		receives messages only from
#		processes on the same machine
login	513/tcp	remote login a la telnet;
#<+>		automatic authentication performed
#		based on privileged port numbers
#		and distributed data bases which
#		identify "authentication domains"
who	513/udp	maintains data bases showing who's
#		logged in to machines on a local
#		net and the load average of the
#		machine
shell	514/tcp	cmd

```
#           like exec, but automatic authentication
#           is performed as for login server
syslog      514/udp
printer     515/tcp      spooler
printer     515/udp      spooler
ftps        990/tcp      ftp protocol, control, over TLS/SSL
ftps        990/udp      ftp protocol, control, over TLS/SSL
telnet      992/tcp      telnet protocol over TLS/SSL
telnet      992/udp      telnet protocol over TLS/SSL
pop3s       995/tcp      pop3 protocol over TLS/SSL (was spop3)
pop3s       995/udp      pop3 protocol over TLS/SSL (was spop3)
```

L'examen du contenu du fichier sur Internet nous permet d'identifier les services suivants :

Port réseau	Service	Adresse(s) d'écoute	Complément
TCP 23	Telnet	172.17.0.2	
TCP 139	NetBIOS	172.16.0.2	
TCP 515	Spooler	Toutes (0.0.0.0)	
TCP 992	TelnetS	Toutes (0.0.0.0)	
TCP 901	SNMPNameRes	Toutes (0.0.0.0)	En fait ce port est utilisé par l'outil d'administration de Samba (SWAT)
TCP 98	TAC NEWS	Toutes (0.0.0.0)	
TCP 113	AUTH	Toutes (0.0.0.0)	Service d'authentification
TCP 37	TIME	Toutes (0.0.0.0)	
TCP 79	FINGER	Toutes (0.0.0.0)	
TCP 143	IMAP	Toutes (0.0.0.0)	
TCP 110	POP 3	Toutes (0.0.0.0)	
TCP 109	POP 2	Toutes (0.0.0.0)	
TCP 512	EXEC	Toutes (0.0.0.0)	
TCP 513	LOGIN	Toutes (0.0.0.0)	
TCP 514	SHELL	Toutes (0.0.0.0)	
TCP 70	GOPHER	Toutes (0.0.0.0)	
TCP 23	TELNET	Toutes (0.0.0.0)	
TCP 21	FTP CONTROL	Toutes (0.0.0.0)	
TCP 111	SUN RPC	Toutes (0.0.0.0)	Appels de procédures distantes
UDP 177	XDMCP	Toutes (0.0.0.0)	
UDP 137	NetBIOS Name Service	Toutes (0.0.0.0)	
UDP 138	NetBIOS Datagram Service	Toutes (0.0.0.0)	
UDP 2049	SHILP	Toutes (0.0.0.0)	
UDP 1000	Cadlock2	Toutes (0.0.0.0)	
UDP 177	XDMCP	Toutes (0.0.0.0)	
UDP 995	POP 3 Sécurisé	Toutes (0.0.0.0)	

UDP 990	FTP S	Toutes (0.0.0.0)	
UDP 37	TIME	Toutes (0.0.0.0)	
UDP 518	NTALK	Toutes (0.0.0.0)	
UDP 517	TALK	Toutes (0.0.0.0)	
UDP 111	SUNRPC	Toutes (0.0.0.0)	
RAW 1	ICMP	Toutes (0.0.0.0)	Le mode RAW correspond aux protocoles encapsulés dans Ethernet et en attente de sollicitation.
RAW 6	TCP	Toutes (0.0.0.0)	Le mode RAW correspond aux protocoles encapsulés dans Ethernet et en attente de sollicitation.

Attention, certains ports ouverts peuvent tout à fait être des ports clients attribués aléatoirement. Dans ce cas, il est possible que ces numéros puissent être confondus avec des ports bien connus.

2. Les seules adresses IP qui apparaissent ici sous "local address" sont 172.16.0.2 et 172.17.0.2 ; l'adresse 127.0.0.1 étant la boucle locale (localhost).
3. Le socket de l'ordinateur client qui est connecté en Telnet sur le serveur est 172.17.207.89 :TCP :3083.
4. Les adresses IP des ordinateurs qui disposent de connexions NetBIOS avec le serveur Linux apparaissent à travers les lignes ci-après.

```

tcp      0      0 172.17.0.2:139      172.17.207.89:2964    ESTABLISHED
tcp      0      0 172.16.0.2:139      192.168.8.7:1034      ESTABLISHED
tcp      0      0 172.16.0.2:139      172.16.206.254:3938   ESTABLISHED
tcp      0      0 172.16.0.2:139      192.168.8.254:4662    ESTABLISHED

```

On obtient donc : 172.17.207.89, 192.168.8.7, 172.16.206.254 et 192.168.8.254.

5. Cela veut dire que le service FTP est à l'écoute de toute demande cliente, et ce, sur n'importe quelle adresse IP de l'ordinateur matérialisé par 0.0.0.0. Le terme de pooling sera utilisé pour préciser que le service n'est pas lié à une adresse IP spécifique lorsque le serveur écoute sur toutes ses interfaces.
6. FTPS, TELNETs et POP3s.