TD 4

Exercice 1

Dans l'annexe A vous allez trouver une capture sur Wireshark. A partir de cette capture, répondez aux questions suivantes.

1. Trouvez les éléments suivants :

    - L'adresse IP du client
    - L'adresse IP du serveur
    - Le port utilisé par le client
    - Le port utilisé par le serveur
    - Le protocole utilisé

2. Expliquez le fonctionnement du protocole TCP.

3. Expliquez les notions de Seq et Ack pour chacun des participants au protocole TCP

4. Complétez la trame dans l'annexe en conséquence

5. Pouvez-vous estimer la taille du message #4 ? Justifiez votre réponse.

Exercice 2

Cet exercice concerne le protocole FTP et la capture d'écran montrée dans l'annexe B. Ce protocole permet le transfert de fichiers d'une machine à un autre.

1. Relevez les adresses IP du client et du serveur FTP, ainsi que les ports utilisés.

2. Pour chaque question et réponse FTP dans la capture mise dans l'annexe :
    - Trouvez le code (numérique ou en texte) associée
    - Indiquez si la commande vient du client ou du serveur
    - Expliquez le rôle du message

3. Pour le serveur dans la capture de l'annexe B trouvez :

    - Le login utilisé pour accéder à l'FTP
    - Le mot de passe utilisé :
    - Le répertoire courant :

Exercice 3

1. Pour chacune des commandes listées ci-dessous expliquez que fait la règle obtenue.
    - `iptables -F`
    - `iptables -P INPUT DROP`
    - `iptables -A INPUT -p -tcp --dport 80 -j ACCEPT`
    - `iptables -I INPUT -i eth0 -p tcp --dport 80 -j DROP`

- `iptables -A INPUT -p tcp -s 192.168.1.0/24 --dport 22 -j ACCEPT`

- `iptables -I OUTPUT -o eth3 -p udp --dport 53 -d 8.8.8.8 -j ACCEPT`

2. Pour un tableau vierge de filter d'un serveur on écrit la commande :

   `iptables -A INPUT -s 53.126.0.0/16 -j DROP`

   - Expliquez la politique qui résulte si on tape ensuite :
     `iptables -A INPUT -s 53.126.4.92 -j ACCEPT`

   - Et si, au lieu de taper la commande ci-dessus, on tapait :
     `iptables -I INPUT -s 53.126.4.92 -j ACCEPT`

Exercice 3

Regardez le tableau de filtrage ci-dessous. Donnez les commandes qu'on a dû taper pour l'obtenir (règle par règle).

```
root@PCA:~# iptables -L -v -n
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
          tcp spt:80
    0     0 ACCEPT     tcp  --  *      *       192.168.1.0/24       0.0.0.0/0
          tcp spt:22
    0     0 ACCEPT     icmp --  *      *       192.168.1.0/24       0.0.0.0/0


Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

    0     0 DROP       all  --  *      *       0.0.0.0/0            10.0.0.0/8
```

Annexe A

No.	Source	Destination	Protocol	Length	Info
1	192.168.56.1	192.168.56.101	TCP	74	51651→80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PE
2	192.168.56.101	192.168.56.1	TCP	74	80→51651 [SYN, ACK] Seq=0 Ack= in=5792 Len=0 MSS=14
3	192.168.56.1	192.168.56.101	TCP	66	51651→80 [ACK] Seq=1 Ack= in=29312 Len=0 TSval=5155
4	192.168.56.1	192.168.56.101	HTTP	350	GET / HTTP/1.1
5	192.168.56.101	192.168.56.1	TCP	66	80→51651 [ACK] Seq=1 Ack=285 Win=6880 Len=0 TSval=170
6	192.168.56.101	192.168.56.1	HTTP	557	HTTP/1.1 200 OK (text/html)
7	192.168.56.1	192.168.56.101	TCP	66	51651→80 [ACK] Seq=285 Ack=492 Win=30336 Len=0 TSval=
8	192.168.56.1	192.168.56.101	HTTP	331	GET /favicon.ico HTTP/1.1
9	192.168.56.101	192.168.56.1	TCP	66	80→51651 [ACK] Seq=492 Ack=550 Win=7936 Len=0 TSval=1
10	192.168.56.101	192.168.56.1	HTTP	569	HTTP/1.1 404 Not Found (text/html)
11	192.168.56.1	192.168.56.101	TCP	66	51651→80 [ACK] Seq=550 Ack=995 Win=31360 Len=0 TSval=
12	192.168.56.1	192.168.56.101	HTTP	361	GET /favicon.ico HTTP/1.1
13	192.168.56.101	192.168.56.1	HTTP	569	HTTP/1.1 404 Not Found (text/html)
14	192.168.56.1	192.168.56.101	TCP	66	51651→80 [ACK] Seq=845 Ack=1498 Win=32512 Len=0 TSval=
15	192.168.56.1	192.168.56.101	HTTP	359	GET /page.html HTTP/1.1
16	192.168.56.101	192.168.56.1	HTTP	556	HTTP/1.1 200 OK (text/html)
17	192.168.56.1	192.168.56.101	TCP	66	51651→80 [ACK] Seq=1138 Ack=1988 Win=33536 Len=0 TSval
18	192.168.56.101	192.168.56.1	TCP	66	80→51651 [FIN, ACK] Seq=1988 Ack=1138 Win=10080 Len=0
19	192.168.56.1	192.168.56.101	TCP	66	51651→80 [FIN, ACK] Seq=1138 Ack= Win=33536 Len=0
20	192.168.56.101	192.168.56.1	TCP	66	80→51651 [ACK] Seq=1989 Ack= Win=10080 Len=0 TSval

Annexe B

No.	Time	Source	src	Destination	dst	Protocol	Length	Info
1	0.000000	164.81.20.108	1156	164.81.20.1	21	TCP	62	1156→21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SA
2	0.000473	164.81.20.1	21	164.81.20.108	1156	TCP	62	21→1156 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 M
3	0.000525	164.81.20.108	1156	164.81.20.1	21	TCP	54	1156→21 [ACK] Seq=1 Ack=1 Win=65535 Len=0
4	0.002798	164.81.20.1	21	164.81.20.108	1156	FTP	74	Response: 220 (vsFTPd 2.0.7)
5	0.129295	164.81.20.108	1156	164.81.20.1	21	TCP	54	1156→21 [ACK] Seq=1 Ack=21 Win=65515 Len=0
6	1.450836	164.81.20.108	1156	164.81.20.1	21	FTP	68	Request: USER reseaul
7	1.451375	164.81.20.1	21	164.81.20.108	1156	TCP	60	21→1156 [ACK] Seq=21 Ack=15 Win=5840 Len=0
8	1.451386	164.81.20.1	21	164.81.20.108	1156	FTP	88	Response: 331 Please specify the password.
9	1.571045	164.81.20.108	1156	164.81.20.1	21	TCP	54	1156→21 [ACK] Seq=15 Ack=55 Win=65481 Len=0
10	2.940956	164.81.20.108	1156	164.81.20.1	21	FTP	67	Request: PASS TQrtue
11	2.972536	164.81.20.1	21	164.81.20.108	1156	FTP	77	Response: 230 Login successful.
12	3.103105	164.81.20.108	1156	164.81.20.1	21	TCP	54	1156→21 [ACK] Seq=28 Ack=78 Win=65458 Len=0
13	4.700383	164.81.20.108	1156	164.81.20.1	21	FTP	60	Request: XPWD
14	4.700826	164.81.20.1	21	164.81.20.108	1156	FTP	75	Response: 257 "/home/reseaul"
15	4.815155	164.81.20.108	1156	164.81.20.1	21	TCP	54	1156→21 [ACK] Seq=34 Ack=99 Win=65437 Len=0
16	6.736881	164.81.20.108	1156	164.81.20.1	21	FTP	66	Request: CWD Socket
17	6.750319	164.81.20.1	21	164.81.20.108	1156	FTP	91	Response: 250 Directory successfully changed.
18	6.887716	164.81.20.108	1156	164.81.20.1	21	TCP	54	1156→21 [ACK] Seq=46 Ack=136 Win=65400 Len=0
19	8.180203	164.81.20.108	1156	164.81.20.1	21	FTP	60	Request: XPWD
20	8.180722	164.81.20.1	21	164.81.20.108	1156	FTP	82	Response: 257 "/home/reseaul/Socket"
21	8.329502	164.81.20.108	1156	164.81.20.1	21	TCP	54	1156→21 [ACK] Seq=52 Ack=164 Win=65372 Len=0
22	9.300656	164.81.20.108	1156	164.81.20.1	21	FTP	60	Request: QUIT
23	9.301418	164.81.20.1	21	164.81.20.108	1156	FTP	68	Response: 221 Goodbye.
24	9.302019	164.81.20.1	21	164.81.20.108	1156	TCP	60	21→1156 [FIN, ACK] Seq=178 Ack=58 Win=5840 Len=
25	9.302041	164.81.20.108	1156	164.81.20.1	21	TCP	54	1156→21 [ACK] Seq=58 Ack=179 Win=65358 Len=0
26	9.303508	164.81.20.108	1156	164.81.20.1	21	TCP	54	1156→21 [FIN, ACK] Seq=58 Ack=179 Win=65358 Len
27	9.303985	164.81.20.1	21	164.81.20.108	1156	TCP	60	21→1156 [ACK] Seq=179 Ack=59 Win=5840 Len=0