Lab 5

3.

Question 1

```
(venv) student@vm04:~/lab5$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
```

La politique par défaut actuelle concernant le trafic entrant est ACCEPT.

Question 2

La politique à choisir est DROP sur la chaîne INPUT.
Commande : sudo iptables -P INPUT DROP

```
student@vm04:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate ESTABLISHED
ACCEPT     all  --  anywhere             anywhere
```

Question 3

On n'y parvient pas, car avec la commande utilisée pour la question 2, on a décidé de bloquer tous les paquets entrants pour lesquels il n'existe pas de règle. Nous n'avons pas encore de règle pour gérer le trafic http (qui passe par le port 80), les paquets que l'on reçoit du browser sont pour le moment bloqués.

Question 4

Commande : sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT

```
student@vm04:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
student@vm04:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate ESTABLISHED
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
student@vm04:~$
```

Ajout de la nouvelle règle pour le trafic http en rouge ci-dessus.

4.

Question 5

```
Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/vm04.secinf24.patu.re/fullchain.pem
Key is saved at:         /etc/letsencrypt/live/vm04.secinf24.patu.re/privkey.pem
This certificate expires on 2025-02-11.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the background.
```

Chemin vers la clé privée : /etc/letsencrypt/live/vm04.secinf24.patu.re/privkey.pem

Chemin vers le certificat : /etc/letsencrypt/live/vm04.secinf24.patu.re/fullchain.pem

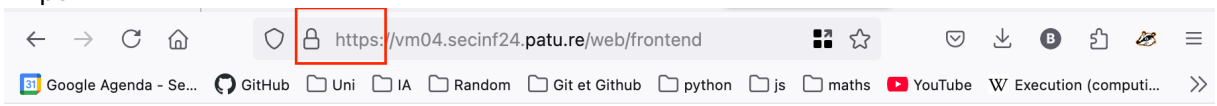
Question 6

On ne parvient pas à ouvrir la page car cette fois les paquets passent par le port 443. Les paquets sont bloqués à cause de notre politique par défaut sur le trafic entrant DROP. Il faut donc ajouter une règle permettant l'entrée de ces paquets par le port 443. Ceci se fait grâce à la commande suivante : sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT

```
student@vm04:~$ sudo systemctl reload nginx
student@vm04:~$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
student@vm04:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate ESTABLISHED
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
```

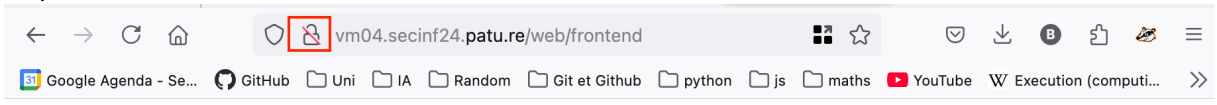
On remarque l'ajout de la règle pour le trafic https (qui utilise le port 443) sur la dernière ligne de l'image ci-dessus.

https



- Nom: pomme, Quantité: 10
- Nom: poires, Quantité: 20

http



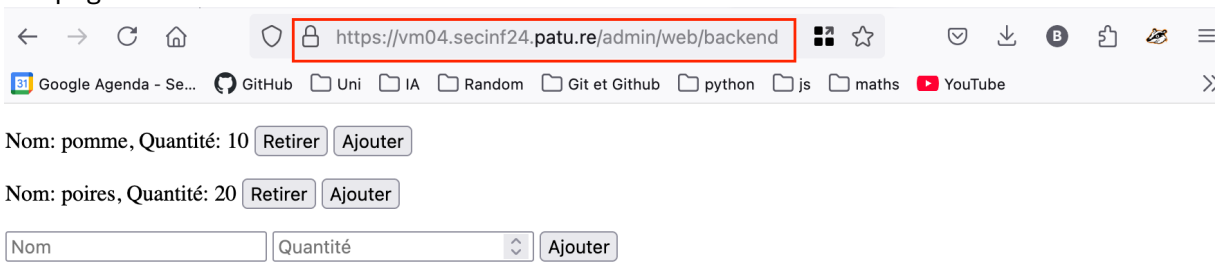
- Nom: pomme, Quantité: 10
- Nom: poires, Quantité: 20

On constate également la différence entre http et https, sur notre browser préféré (évidemment firefox)

5 (Bonus).

Avant d'importer le certificat sur notre navigateur on a une erreur 403 Forbidden qui nous empêche l'accès à la page. Le serveur comprend la requête mais refuse son exécution car on ne dispose pas du certificat ni de la clé nécessaire.

Lorsque l'on a importé le certificat et la clé privée sur notre navigateur. On a normalement accès à la page désormais sécurisé.



Ce qui rend l'accès plus pratique et sécurisé sans avoir à faire de redirection de port via SSH.