

SADEK  
ADEL  
SIO1

---

### TP03 apache

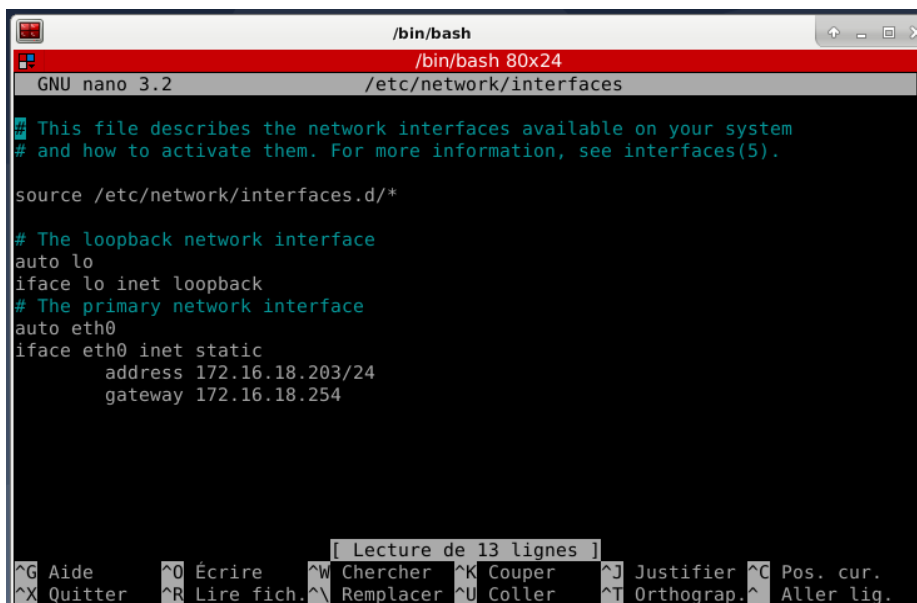
---

J'ai créé la VM comme demandé dans la consigne

J'ai modifié l'adresse IP et la passerelle de ma machine comme demandé en allant dans le fichier  
`/etc/network/interfaces`

Mon IP 172.16.18.203/24

Ma passerelle 172.16.18.254



```
GNU nano 3.2 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
# The primary network interface
auto eth0
iface eth0 inet static
    address 172.16.18.203/24
    gateway 172.16.18.254
```

Ensuite j'ai réinitialisé l'interface réseau pour que ça fonctionne en tapant la commande `systemctl restart networking`

Je vérifie ensuite si mon IP a bien été modifié  
Je ping mon adresse ensuite la passerelle et le DNS.

```
root@debTP3:~# ping 172.16.100.9
PING 172.16.100.9 (172.16.100.9) 56(84) bytes of data:
64 bytes from 172.16.100.9: icmp_seq=1 ttl=63 time=0.530 ms
64 bytes from 172.16.100.9: icmp_seq=2 ttl=63 time=0.890 ms
64 bytes from 172.16.100.9: icmp_seq=3 ttl=63 time=1.10 ms
64 bytes from 172.16.100.9: icmp_seq=4 ttl=63 time=0.911 ms
64 bytes from 172.16.100.9: icmp_seq=5 ttl=63 time=0.936 ms
64 bytes from 172.16.100.9: icmp_seq=6 ttl=63 time=0.784 ms
^C
--- 172.16.100.9 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 38ms
rtt min/avg/max/mdev = 0.530/0.857/1.095/0.176 ms
root@debTP3:~#
```

```
root@debTP3:/etc/apache2/sites-enabled# ping 172.16.100.10
PING 172.16.100.10 (172.16.100.10) 56(84) bytes of data:
64 bytes from 172.16.100.10: icmp_seq=1 ttl=63 time=0.504 ms
64 bytes from 172.16.100.10: icmp_seq=2 ttl=63 time=0.564 ms
64 bytes from 172.16.100.10: icmp_seq=3 ttl=63 time=0.465 ms
^C
--- 172.16.100.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 53ms
rtt min/avg/max/mdev = 0.465/0.511/0.564/0.040 ms
root@debTP3:/etc/apache2/sites-enabled#
```

Ping du DNS

```
root@debTP3:~# ping 172.16.18.203
PING 172.16.18.203 (172.16.18.203) 56(84) bytes of data:
64 bytes from 172.16.18.203: icmp_seq=2 ttl=64 time=0.068 ms
64 bytes from 172.16.18.203: icmp_seq=3 ttl=64 time=0.034 ms
^C
--- 172.16.18.203 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 37ms
rtt min/avg/max/mdev = 0.021/0.041/0.068/0.019 ms
root@debTP3:~# nslookup
> deb.sio.jjr
Server:      172.16.100.12
Address:     172.16.100.12#53

deb.sio.jjr canonical name = miroirdeb10.sio.jjr.
Name:       miroirdeb10.sio.jjr
Address:    172.16.100.9
> www.google.com
Server:      172.16.100.12
Address:     172.16.100.12#53

Non-authoritative answer:
Name:       www.google.com
Address:    216.58.213.164
Name:       www.google.com
Address:    2a00:1450:4007:811::2004
```

Je teste la résolution DNS avec la commande nslookup lorsque je tape un site en manière FQDN donc nom Machine>domaine>domaine sa m'affiche l'adresse ip de ce dernier

La commande nslookup deb.sio.jjr m'affiche bien 172.16.100.9

**Le fichier /etc/passwd contient toutes les informations relatives aux utilisateur login mdp etc**

```

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sb
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
apt:x:100:65534:./nonexistent:/usr/sbin/nologin

```

Le fichier `/etc/group` la liste des utilisateurs appartenant aux différents groupes  
`/etc/shadow` contient mdp codé et autres infos tel que l'expiration du compte  
Je créer un utilisateur comme ceci  
**useradd Adel**

J'ai installé les **paquets apache2, apache2-utils mariadb-server php7.3 et php7.3-mysql**

Je créer le répertoire `/var/www/booktic`  
Comme ceci **mkdir /var/www/booktic**

Je créer 2 pages html

Avec écrit seulement page html dedans

Je vais configurer VirtualHost, ServerName, DocumentRoot etc  
En suivant l'exemple du TP

```

/bin/bash
/bin/bash 80x24
GNU nano 3.2 booktic.conf Modifié
<VirtualHost *:80>
  ServerName booktic.<Sadek>.local
  DocumentRoot /var/www/booktic
  <Directory /var/www/booktic>
    Require all granted
  </Directory>
</VirtualHost>

```

La commande `a2ensite booktic.conf` me demande d'exécuter la commande `systemctl reload apache2` pour que le site soit activé (soit redémarrer le service)

Je l'exécute

La différence entre les deux c'est que dans le fichier `/etc/apache2/sites-enabled` c'est que il y a une fleche vers le fichier `/etc/apache2/sites-available` (lien symbolique)

```
root@debTP3:~# a2ensite booktic.conf
Enabling site booktic.
To activate the new configuration, you need to run:
. systemctl reload apache2
root@debTP3:~# systemctl reload apache2
root@debTP3:~# cd /etc/apache2
root@debTP3:/etc/apache2# ls
apache2.conf  conf-enabled  magic          mods-enabled  sites-available
conf-available  envvars      mods-available  ports.conf    sites-enabled
root@debTP3:/etc/apache2# systemctl stop apache2
root@debTP3:/etc/apache2# ls
apache2.conf  conf-enabled  magic          mods-enabled  sites-available
conf-available  envvars      mods-available  ports.conf    sites-enabled
root@debTP3:/etc/apache2# systemctl start apache2
root@debTP3:/etc/apache2# nano /etc/apache2/sites-available/available
root@debTP3:/etc/apache2# cd /etc/apache2/sites-available
root@debTP3:/etc/apache2/sites-available# ls -l
bash: ls -l : commande introuvable
root@debTP3:/etc/apache2/sites-available# ls -l
total 16
-rw-r--r-- 1 root root 1332 août  8 09:47 000-default.conf
-rw-r--r-- 1 root root 164 déc. 14 14:45 booktic.conf
-rw-r--r-- 1 root root 6338 août  8 09:47 default-ssl.conf
root@debTP3:/etc/apache2/sites-available#
```

```
root@debTP3:/etc/apache2/sites-enabled# ls -l
total 0
lrwxrwxrwx 1 root root 35 déc. 14 14:07 000-default.conf -> ../sites-available/000-default.conf
lrwxrwxrwx 1 root root 31 déc. 14 14:45 booktic.conf -> ../sites-available/booktic.conf
root@debTP3:/etc/apache2/sites-enabled#
```

```
root:$6$XGzUMgdL9.zph/Xs$KLzK4AGGn8Smvn/yYh6sj6gitkVvHS1P82DpD2uRBDfaQjpuY5xdXr$
daemon*:18609:0:99999:7:::
bin*:18609:0:99999:7:::
sys*:18609:0:99999:7:::
sync*:18609:0:99999:7:::
games*:18609:0:99999:7:::
man*:18609:0:99999:7:::
lp*:18609:0:99999:7:::
mail*:18609:0:99999:7:::
news*:18609:0:99999:7:::
uucp*:18609:0:99999:7:::
proxy*:18609:0:99999:7:::
www-data*:18609:0:99999:7:::
backup*:18609:0:99999:7:::
list*:18609:0:99999:7:::
irc*:18609:0:99999:7:::
gnats*:18609:0:99999:7:::
nobody*:18609:0:99999:7:::
_apt*:18609:0:99999:7:::
[ Lecture de 32 lignes ]
```

```
127.0.0.1    localhost
127.0.1.1    debTP3
# The following lines are desirable for IPv6 capable hosts
::1         localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
172.16.18.203 booktic.Sadek.local
```

## Sécurisation du serveur avec https

J'ai saisi dans la ligne de commande `apt-get install openssl`

J'ai créé le répertoire Secure dans `var/www/secure`

J'ai créé le fichier `serial` et j'y ai inséré 01 (Sur les nouvelles versions ceci ne change rien, à ne pas faire)

J'ai créé le fichier `index.txt` qui ne contient rien

J'ai ouvert le fichier `etc/sl/openssl.cnf`

Je l'ai modifier a la ligne `dir` et j'y ai insérer le chemin du répertoire `var/www/secure` ( on peut aussi simplement rester dans le dossier `secure` et saisir les prochaines commandes)

*J'ai exécuté la commande pour générer un certificat*

*Openssl genrsa 4096 > clef.key (on génère d'abord la clef privée)*

*Ensuite le certificat basé sur la clef privée*

*Openssl req -x509 -days 365 -nodes -key clef.key -out clef.crt*

*Plusieurs questions m'ont été poser ma ville région nom du site (FQDN) et mon mail*

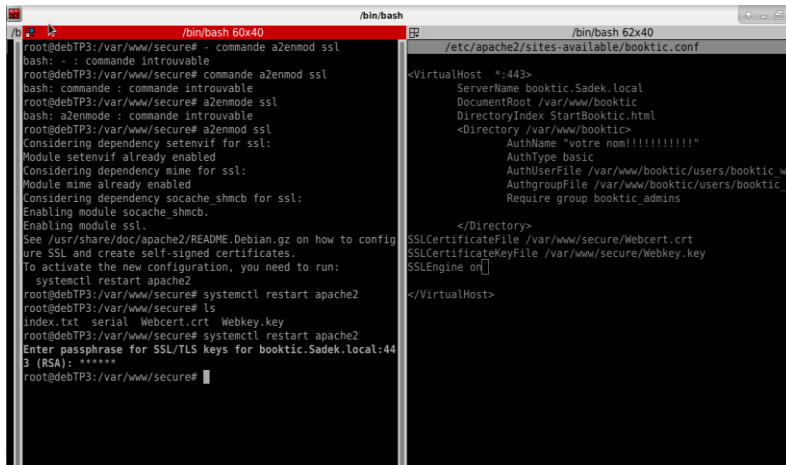
*Le rsa :2048 c'est un chiffrement qui est baser sur 2048 bit*

*Le fichier `Webcert.crt` c'est le certificat qui est chiffrer*

*Le fichier `Webkey.key` est un fichier chiffrer qui contient la clé de chiffrement*

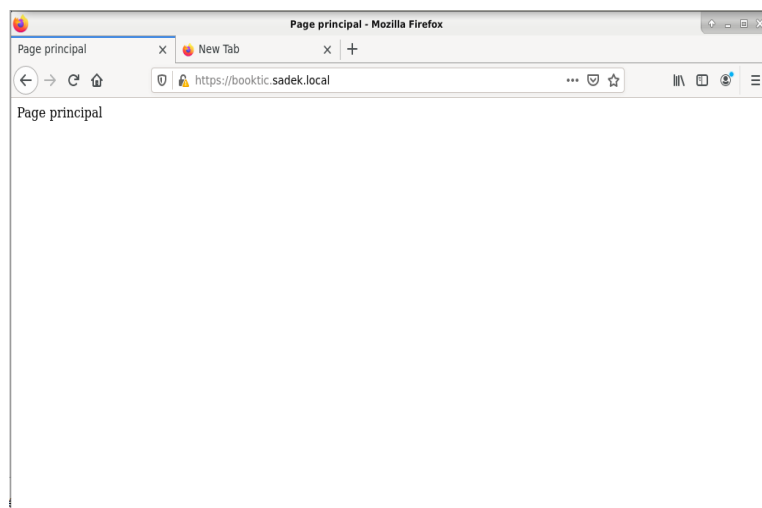
J'ai modifié le fichier de conf de mon serveur comme ceci et j'ai redémarrer apache2 qui ma demander mon mdp que j'avais configurer au début

### Virtual host après changement :



```
root@debTP3:/var/www/secure# - commande a2enmod ssl
bash: - : commande introuvable
root@debTP3:/var/www/secure# commande a2enmod ssl
bash: commande : commande introuvable
root@debTP3:/var/www/secure# a2enmod ssl
bash: a2enmod : commande introuvable
root@debTP3:/var/www/secure# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
systemctl restart apache2
root@debTP3:/var/www/secure# systemctl restart apache2
root@debTP3:/var/www/secure# ls
index.txt  serial  Webcert.crt  Webkey.key
root@debTP3:/var/www/secure# systemctl restart apache2
Enter passphrase for SSL/TLS keys for booktic.Sadek.local:443 (RSA): *****
root@debTP3:/var/www/secure#
```

```
/etc/apache2/sites-available/booktic.conf
<VirtualHost *:443>
    ServerName booktic.Sadek.local
    DocumentRoot /var/www/booktic
    DirectoryIndex StartBooktic.html
    <Directory /var/www/booktic>
        AuthName "votre nom!!!!!!!!!!!!!!"
        AuthType basic
        AuthUserFile /var/www/booktic/users/booktic_w
        AuthgroupFile /var/www/booktic/users/booktic_
        Require group booktic_admins
    </Directory>
    SSLCertificateFile /var/www/secure/Webcert.crt
    SSLCertificateKeyFile /var/www/secure/Webkey.key
    SSLEngine on
</VirtualHost>
```



Tout fonctionne et j'avais un message d'alerte qui c'était afficher car j'ai auto signer mon certificat ce n'est pas une autorité reconnue comme LetsEncrypt qui a signé mon certificat donc Firefox a remis en doute mon certificat on peut l'éviter en faisant signer son certificat par une autorité reconnue tel que LetsEncrypt

---

## Sécurité supplémentaire sur le serveur web

---

Faire en sorte qu'apache n'écoute pas sur le port 80 aller dans le fichier port.conf et commenter la directive Listen 80

Authentification utilisateur :

```
<Directory directory-path >
  AuthType Basic
  AuthName "text"
  AuthUserFile fichier/utilisateur
  Require valid-user
</Directory>
```

Il faut installer le paquet apache2-utils et activer le module auth\_basic

Cryptage avec certificat et clef public normalement c'est maîtrisé.

Masquer la version de mon serveur apache en GUI

```
ServerSignature Off
```

En cli avec wget on peut toujours récolter des informations sur le serveur web notamment avec la commande wget

ServerTokens doit être mis après le virtualhost

```
ServerTokens Prod[uctOnly] | Min[imal] | OS | Full
```

C'est pour ça il faut rajouter cette directive et mettre Productonly