

TP OPENSLL 3

- Afin de se connecter un serveur, nous devons avoir son hostname et son port, par exemple :

- Utiliser cette ligne de commande "openssl s_client -connect www.laposte.tn:443" pour avoir le

- ```
kali@kali:~$ openssl s_client -connect www.laposte.fr:443
```

```
kali@kali:~$ openssl s_client -connect www.taoposte.cn:443
CONNECTED(00000003)
depth=0 CN = *.poste.tn
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 CN = *.poste.tn
verify error:num=21:unable to verify the first certificate
verify return:1
```

- ```
kali@kali:~/Desktop/or3$ cat certificat_lăcose
```

```

kali@kali:~/Desktop/ops$ cat certificate_tacoste
-----BEGIN CERTIFICATE-----
MIIFrjCCBJagAwIBAgIQecVFfPfuWUW08Qc9aHjZLDANBgkqhkiG9w0BAQsFADCB
jzELMAkGA1UEBhMCRC0xGzAZBgNVBAGTEkdyZWf0ZXIgdWV2Y2hlc3RlcjEQAQA4G
A1UEBxMHU2FsZm9yZDEYMBYGA1UEChMPU2VjdGlnbyBMaW1pdGVkMTcwNQYDVQQD
Ey5TZWN0aWdvIFJFTQSEB21haW4gVmFsaWRhdGlvbiBTZWN1cmUgU2VydmdVYIENB
MB4XDTIwMDIxOTAwMDAwMFoXDTEwMDIxODIzNTk1OVowFTETMBEGA1UEAwwKKi5w
b3N0ZS50b3RlY2V0eXJkeXZlbycNAQFBR0ADggEFAADCCAQeCggEFAhuhD1pFAleZ

```

```
kali@kali:~/Desktop/op3$ openssl x509 -noout -in certificat_lacoste -issuer
-subject -dates -hash -fingerprint
issuer=C = GB, ST = Greater Manchester, L = Salford, O = Sectigo Limited, C
N = Sectigo RSA Domain Validation Secure Server CA
subject=CN = *.poste.tn
notBefore=Feb 19 00:00:00 2020 GMT
notAfter=Feb 28 23:59:59 2021 GMT
febd681b
SHA1 Fingerprint=F7:75:28:43:DA:1C:93:EF:D6:67:81:B7:F2:95:77:53:AA:B0:4D:D
9
```

— Le format pem est un type de format pour les certificats, c'est un certificat codé en ASCII (en Base 64). Il en existe trois principaux formats : DER, PKCS7 et PKCS12. Convertir le certificat .pem au format DER "openssl x509 -outform der -in certificat.pem -out certificat.der". Puis, lisez ce format en utilisant "openssl x509 -in certificat.der -inform der -text".

```
kali@kali:~/Desktop/op3$ file certificat_lacoste
certificat_lacoste: PEM certificate
```

```
kali@kali:~/Desktop/op3$ openssl x509 -outform der -in certificat_lacoste -out certificat.der
kali@kali:~/Desktop/op3$ openssl x509 -in certificat.der -inform der -text
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      79:c5:45:94:f7:ee:59:45:b4:f1:07:3d:68:78:d9:2c
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C = GB, ST = Greater Manchester, L = Salford, O = Sectigo Limited, CN = Sectigo RSA Domain Validation Secure Server CA
    Validity
```

APRES AVOIR FAIT LE TOUR SUR LES DIFFERENTS FORMATS DES CERTIFICATS, COMMENÇONS PAR INSTAURER NOTRE PKI.

1. ETAPE1 : CREATION DU CERTIFICAT DE L'AUTORITE DE CERTIFICATION AC :

(a) Générer la paire de clef de l'autorité : "CLEF_AC" (protéger toutes vos clefs par un pwd)

```
kali@kali:~/Desktop/op3$ openssl genrsa -out CLEF_AC -des3 4092
Generating RSA private key, 4092 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
Enter pass phrase for CLEF_AC:
Verifying - Enter pass phrase for CLEF_AC:
kali@kali:~/Desktop/op3$
```

Pwd : CLEF_AC

(b) A partir de "CLEF_AC", créer un certificat x509 pour une durée de validité de 10 ans : "AC_cert".

```
kali@kali:~/Desktop/op3$ openssl req -new -x509 -days 3650 -key CLEF_AC -out AC_cert
Enter pass phrase for CLEF_AC:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:TN
State or Province Name (full name) [Some-State]:Tunis^[[C
Locality Name (eg, city) []:Mutuelville
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:AC
Common Name (e.g. server FQDN or YOUR name) []:AC
Email Address []:
kali@kali:~/Desktop/op3$
```

(c) Le résultat obtenu est le certificat de l'autorité de certification qui va permettre de signer les certificats créés.

```
kali@kali:~/Desktop/op3$ cat AC_cert
-----BEGIN CERTIFICATE-----
MIIFxjCCA66gAwIBAgIUUN/U5cWaBT0cR4E5BuDNHybJEswDQYJKoZIhvcNAQEL
BQAwczELMAkGA1UEBhMCVE4xETAPBgNVBAGMCFR1bmZG1tDMRQwEgYDVQQHDAtn
dXR1ZWx2aWxsZTEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMQsw
CQYDVQQLDAJBQzELMAkGA1UEAwwCQUMwHhcNMjAxMTEwMjExNTMxWhcNMzAxMTA5
MjExNTMxWjBzMQswCQYDVQQGEwJUTjERMA8GA1UECAwIVHVuaXBW0MxFDASBgNV
BACMC011dHVlbHZpbGx1MSEwHwYDVQQKDBhJbnRlcml5dCBXaWRnaXRzIFB0eSBM
dGQxChAJBgNVBAsMAkFDMQswCQYDVQQDDAJBQzCCAiEwDQYJKoZIhvcNAQEBBQAD
```

2. ETAPE2 : CREATION DU CERTIFICAT DU SERVEUR (DANS NOTRE CAS DE FIGURE APACHE2)

(a) Générer la clef privée "CLEF_apache". Tachez à donner un pwd à votre clef pour une éventuelle vérification de l'exactitude de votre manipulation lors du redémarrage du serveur.

```
kali@kali:~/Desktop/op3$ openssl genrsa -out CLEF_apache -des3 4092
Generating RSA private key, 4092 bit long modulus (2 primes)
.....
++++
.....++++
e is 65537 (0x010001)
Enter pass phrase for CLEF_apache:
Verifying - Enter pass phrase for CLEF_apache:
kali@kali:~/Desktop/op3$ █
```

Pwd : CLEF_apache

(b) Générer une demande de signature de certificat (CSR Certificate Signing Request) de votre serveur. Vous pouvez identifier votre institut (Tekup) comme serveur.

```
kali@kali:~/Desktop/op3$ openssl req -new -key CLEF_apache -out demande_serveur
Enter pass phrase for CLEF_apache:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:TN
State or Province Name (full name) [Some-State]:Tunis
Locality Name (eg, city) []:Mutuelleville^[D
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Tekup
Organizational Unit Name (eg, section) []:Tekup
Common Name (e.g. server FQDN or YOUR name) []:Tekup
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:certif_apache
An optional company name []:
kali@kali:~/Desktop/op3$ █
```

(c) AC signe la demande de certificat du serveur, on obtient "Apache_cert".

```
kali@kali:~/Desktop/op3$ openssl x509 -req -in demande_serveur -out Apache_cert -CA A
C_cert -CAkey CLEF_AC -CAcreateserial -CAserial serveur.srl
Signature ok
subject=C = TN, ST = Tunis, L = Mutuelleville\1B[D, O = Tekup, OU = Tekup, CN = Tekup
Getting CA Private Key
Enter pass phrase for CLEF_AC:
kali@kali:~/Desktop/op3$
```

3. ETAPE3 : CREATION DU CERTIFICAT DU CLIENT

(a) Générer la clef privée "CLEF_client".

```
kali@kali:~/Desktop/op3$ openssl genrsa -out CLEF_client -des3 4092
Generating RSA private key, 4092 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
Enter pass phrase for CLEF_client:
Verifying - Enter pass phrase for CLEF_client:
kali@kali:~/Desktop/op3$
```

Pwd : CLEF_client

(b) Générer une demande de signature de certificat de votre client. Vous pouvez identifier votre filière SSIR. Le common Name de cette demande est SSIR.tn.

```
kali@kali:~/Desktop/op3$ openssl req -new -key CLEF_client -out demande_client
Enter pass phrase for CLEF_client:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:TN
State or Province Name (full name) [Some-State]:Tunis
Locality Name (eg, city) []:Mutuelville
Organization Name (eg, company) [Internet Widgits Pty Ltd]:SSIR
Organizational Unit Name (eg, section) []:SSIR
Common Name (e.g. server FQDN or YOUR name) []:SSIR.tn
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:client_cert
An optional company name []:SSIR
kali@kali:~/Desktop/op3$
```


(c) AC signe la demande de certificat du client, on obtient "client_cert".

```
Enter pass phrase for CLEF_AC:
kali@kali:~/Desktop/op3$ openssl x509 -req -in demande_client -out client_cert -CA AC
_cert -CAkey CLEF_AC -CAcreateserial -CAserial serveur.srl
Signature ok
subject=C = TN, ST = Tunis, L = Mutuelville, O = SSIR, OU = SSIR, CN = SSIR.tn
Getting CA Private Key
Enter pass phrase for CLEF_AC:
kali@kali:~/Desktop/op3$
```

(d) Générer votre enveloppe pkcs12 de votre client "client_pfx". Donner un pwd différent de celui de la clef pour mieux comprendre les différentes étapes.

```
kali@kali:~/Desktop/op3$ openssl pkcs12 -export -out client_cert.pfx -in client_cert
-inkey CLEF_client -name "client_pfx"
Enter pass phrase for CLEF_client:
Enter Export Password:
Verifying - Enter Export Password:
```

Pwd : Export_cert

LE BUT DE CE TP EST DE SECURISER L'ACCES A NOTRE SITE WWW.SSIR.TN.

1. CONFIGURATION DE APACHE :

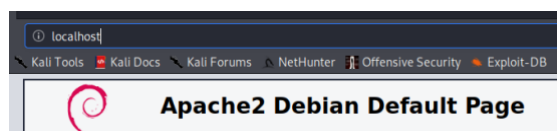
(a) Installation de apache2 : apt-get install apache2

```
kali@kali:~/Desktop/op3$ sudo apt-get install apache2
[sudo] password for kali:
Reading package lists... Done
Building dependency tree
Reading state information... Done
apache2 is already the newest version (2.4.43-1).
apache2 set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
kali@kali:~/Desktop/op3$
```

```
kali@kali:~$ sudo systemctl start apache2
```

(b) Tester votre localhost

```
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
kali@kali:~/Desktop/op3$ ping localhost
PING localhost (localhost (:::1)) 56 data bytes
64 bytes from localhost (:::1): icmp_seq=1 ttl=64 time=0.024 ms
64 bytes from localhost (:::1): icmp_seq=2 ttl=64 time=0.037 ms
```



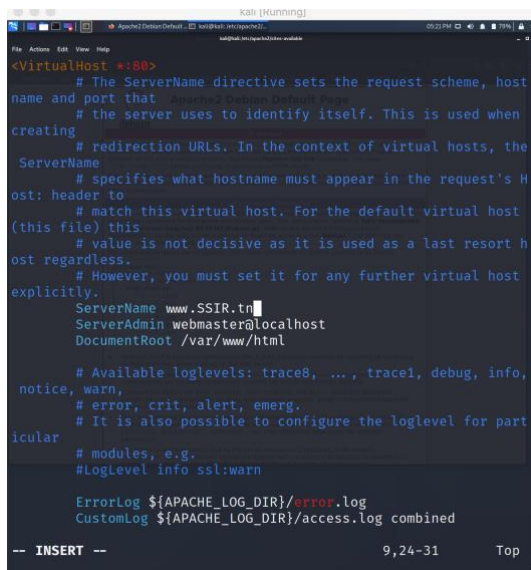
(c) En ajoutant à votre hosts, le Domain Name Server www.SSIR.tn, tester votre site.

Sudo vi /etc/host

```
127.0.0.1 www.SSIR.tn
```

(d) Sous sites-available, éditer le fichier de configuration du port 80. Avec le ServerName est www.SSIR.tn

```
kali@kali:/etc/apache2/sites-available$ sudo vi /etc/apache2/sites-available/000-default.conf
```



```
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, host
    # name and port that the server uses to identify itself. This is used when
    # creating
    # redirection URLs. In the context of virtual hosts, the
    # ServerName
    # specifies what hostname must appear in the request's Host
    # header to
    # match this virtual host. For the default virtual host
    # (this file) this
    # value is not decisive as it is used as a last resort host
    # regardless.
    # However, you must set it for any further virtual host
    # explicitly.
    ServerName www.SSIR.tn
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

    # Available loglevels: trace8, ..., trace1, debug, info,
    # notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for part
    # icular
    # modules, e.g.
    # LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
-- INSERT --
```

(e) Activer SSL et default-ssl /*a2enmod et a2ensite*/

```
kali@kali:/etc/apache2/sites-available$ sudo 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
```

(f) Sur la configuration du port 443, modifier le chemin de la clef du serveur, le certificat du serveur ainsi que celui de l'autorité : SSLCertificateFile, SSLCertificateKeyFile et SSLCertificateChainFile.

```
kali@kali:/etc/apache2/sites-available$ sudo vi default-ssl.conf
```

```
# SSLCertificateFile directive is needed.  
SSLCertificateFile /home/kali/Desktop/op3/Apache_cert  
SSLCertificateKeyFile /home/kali/Desktop/op3/CLEF_apache
```

```
SSLCertificateChainFile /home/kali/Desktop/op3/Apache_cert
```

(g) Redémarrer le service apache, vous serez amené à donner le pwd de votre serveur.

```
kali@kali:/etc/apache2/sites-available$ systemctl restart apache2
```

(h) Authentification ssl mutuelle :

i. Ajouter le certificat de l'AC : SSLCACertificateFile

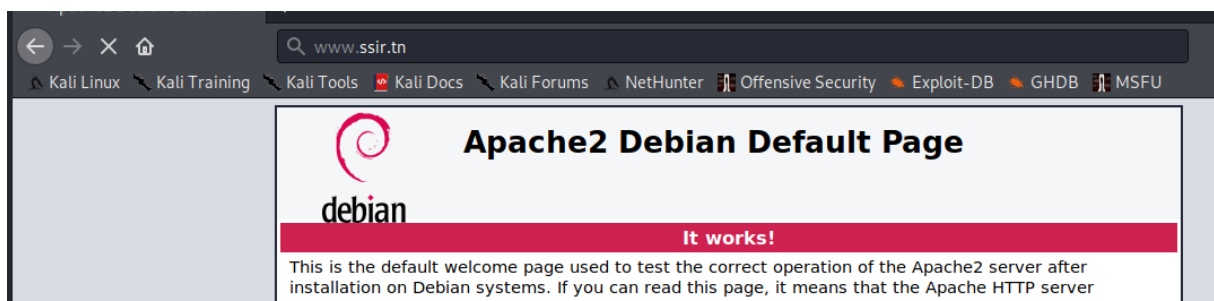
```
SSLCACertificatePath /etc/ssl/certs/  
SSLCACertificateFile /home/kali/Desktop/op3/AC_cert
```

ii. Décommenter SSLVerifyClient require et SSLVerifyDepth 1 2

```
SSLVerifyClient require  
SSLVerifyDepth 10
```

2. TEST D'ACCES :

(a) Accéder à votre site en http et en https (apachectl pourrait être utilisé pour viser une éventuelle erreur)



3. REDIRECTION :

(a) Sur le fichier de configuration du port 80, on oblige le passage par le port 443.

```
kali@kali:/etc/apache2/sites-available$ sudo vi /etc/apache2/sites-available/000-default.conf
```

(b) RedirectMatch permanent ^(.*)\$ https://www.SSIR.tn\$1

```
RedirectMatch permanent ^(.*)$ https://www.SSIR.tn$1
```

(c) ou bien :

RewriteEngine On

RewriteCond %{SERVER PORT} !^443\$

RewriteRule ^/(.*) https ://%{SERVER NAME}/\$1

```
RewriteEngine On
RewriteCond %{SERVER PORT} !^443$
RewriteRule ^/(.*) https ://%{SERVER NAME}/$1 # Available
loglevels: trace8, ... , trace1, debug, info, notice, warn,
```