

SRES TP3

SSL

Master 2 Cybersécurité

2018 - 2019

Encadré par:
Gwenn FEUNTEUN

Réalisé par:
Manon DEROCLES
Alexis LE MASLE

Table des matières

Configurer un service HTTPS	2
Configurer un service OpenVPN	6

Configurer un service HTTPS

Question 1:

Dans un répertoire temporaire, créez une autorité de certification (étape 3 et 4) avec les paramètres suivants :

- Clé RSA de 2048 bits (4096 seraient mieux, mais trop long à générer dans le cadre de ce TP) ;
- Valable 4 ans ;
- Country = FR, State = IEV, Locality = RENNES, Organization = ISTIC, Organizational Unit = SRES, Common Name = MonACPerso

Voici les deux commandes pour créer un certificat, crée la clé rsa puis crée le certificat avec cette clé générée.

Tout d'abord, on commence par générer l'autorité de certification.

```
openssl envt
derocles@derocles:~/Documents/SRES/TP3$ openssl genrsa -out ca.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
derocles@derocles:~/Documents/SRES/TP3$ openssl req -x509 -new -days 1461 -key ca.key -out ca.pem
Can't load /home/derocles/.rnd into RNG
140249817285056:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/rand/randfile.c:88:Filename=/home/derocles/.rnd
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]:FR
State or Province Name (full name) [Some-State]:IEV
Locality Name (eg, city) []:RENNES
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ISTIC
Organizational Unit Name (eg, section) []:SRES
Common Name (e.g. server FQDN or YOUR name) []:MonACPerso
Email Address []:
```

Création de l'autorité de certification

Question 2:

Créez un certificat serveur pour le site www.monsite.com , avec les mêmes caractéristiques.

On réalise les mêmes étapes pour créer un certificat client, pour le site www.monsite.com

```
Email Address []:
derocles@derocles:~/Documents/SRES/TP3$ openssl genrsa -out cert.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
derocles@derocles:~/Documents/SRES/TP3$ openssl req -new -days 1461 -key cert.key -out cert.csr
Ignoring -days; not generating a certificate
Can't load /home/derocles/.rnd into RNG
140504715264448:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/rand/randfile.c:
88:Filename=/home/derocles/.rnd
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]:FR
State or Province Name (full name) [Some-State]:IEV
Locality Name (eg, city) []:RENNES
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ISTIC
Organizational Unit Name (eg, section) []:SRES
Common Name (e.g. server FQDN or YOUR name) []:www.monsite.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
derocles@derocles:~/Documents/SRES/TP3$
```

Création du certificat

```
derocles@derocles:~/Documents/SRES/TP3$ openssl x509 -req -CAcreateserial -in cert.csr -CA ca.pem
CAkey ca.key -out cert.pem
Signature ok
subject=C = FR, ST = IEV, L = RENNES, O = ISTIC, OU = SRES, CN = www.monsite.com
Getting CA Private Key
```

Signature du certificat

Question 3:

Activez la prise en charge de HTTPS sur le service avec ce certificat.

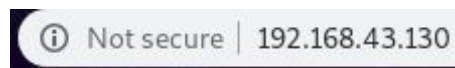
Nous créons un fichier *monsite.com* dans le dossier *etc/apache2/sites-available/* où nous mettons les configurations pour le port 80 (http) puis pour le port 443 pour le https.

```
GNU nano 2.7.4 Fichier : /etc/apache2/sites-available/monsite.com.conf
<VirtualHost *:80>
  ServerName monsite.com
  ServerAlias www.monsite.com
  ServerAdmin webmaster@monsite.com
  DocumentRoot /srv/web/monsite.com/www
  <Directory /srv/web/monsite.com/www>
    Options -Indexes +FollowSymLinks +MultiViews
    AllowOverride none
    Require all granted
  </Directory>
  ErrorLog /var/log/apache2/error.monsite.com.log
  CustomLog /var/log/apache2/access.monsite.com.log combined
</VirtualHost>

<VirtualHost *:443>
  ServerName monsite.com
  ServerAlias www.monsite.com
  ServerAdmin webmaster@monsite.com
  DocumentRoot /srv/web/monsite.com/www
  <Directory /srv/web/monsite.com/www>
    Options -Indexes +FollowSymLinks +MultiViews
    AllowOverride none
    Require all granted
  </Directory>
  # directives obligatoires pour TLS
  SSLEngine on
  SSLCertificateFile /etc/letsencrypt/live/monsite.com/fullchain.pem
  SSLCertificateKeyFile /etc/letsencrypt/live/monsite.com/privkey.pem
  Header always set Strict-Transport-Security "max-age=15768000"
  ErrorLog /var/log/apache2/error.monsite.com.log
  CustomLog /var/log/apache2/access.monsite.com.log combined
</VirtualHost>
```

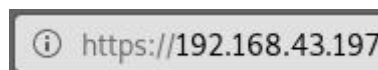
Fichier de configuration de *www.monsite.com* pour apache2

Nous réussissons à nous connecter au port 80.



Succès de la connexion au port 80 sur le serveur

Nous réussissons également à nous connecter en https



Succès de la connexion au port 443 sur le serveur

Pour vérifier que nous possédons le bon certificat nous l'affichons sur le navigateur. C'est bien le certificat que nous avons créé.¶¶



Certificat présent lors de la connexion sur le navigateur en https

Configurer un service OpenVPN

Question 2:

Créez un certificat pour le serveur et un autre pour le client VPN (avec les CN respectifs « serveur » et « client »).

Pour générer un certificat SSL server pour openvpn (respectivement client) on utilise les commandes suivante:

```
istic-web:/etc/openvpn# openssl genrsa -out server.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++
65537 (0x010001)

root@istic-web:/etc/openvpn# openssl req -new -key server.key -out server.csr
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]:FR
State or Province Name (full name) [Some-State]:IEV
Locality Name (eg, city) []:RENNES
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ISTIC
Organizational Unit Name (eg, section) []:SRES
Common Name (e.g. server FQDN or YOUR name) []:vpnServer
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
root@istic-web:/etc/openvpn# openssl x509 -req -CAcreateserial -in cert.csr -CA
root@istic-web:/etc/openvpn# openssl x509 -req -CAcreateserial -in server.csr -CA
A ca.pem -CAkey ca.key -out serveur.pem
Signature ok
subject=C = FR, ST = IEV, L = RENNES, O = ISTIC, OU = SRES, CN = vpnServer
Getting CA Private Key
```


Question 3:

Générez des paramètres Diffie-Hellman de 2048 bits dans dh2048.pem.

```
root@istic-vpn:/etc/openvpn# openssl genpkey -genparam -algorithm dh
-out dh2048.pem
.....+.....+.....
.+.....+.+.+.+.
.....
.....+.+.+.+.
.....
.....+.
.....+.+.++*++*++*
```

```
-----BEGIN DH PARAMETERS-----
MIGHAoGBALFTeYpCdIRvWEpcP9XsiyfDJT53zDk3nFkwDNmEHSHeQiWJsp/zcVf2
CiB4pk0C5BGoUS/Ijm5ZKq9lDzwCk2sldI3Eo+wExFmlztS26eisgI0R9+BQ1IDY
HtYCNge7zFTXpjeVjiHGRli87p0dXhwdWMI+HKmytaUGh0LKh5CTAgEC
-----END DH PARAMETERS-----
```

Question 4:

Mettez en place le serveur OpenVPN sur la machine serveur. Vous pourrez trouver un fichier de configuration déjà prêt dans le répertoire /usr/share/doc/openvpn/examples/sample-config-files/. Copiez le fichier de configuration serveur d'exemple.

Question 5:

Mettez en place le serveur OpenVPN sur la machine cliente. Vous pourrez trouver un fichier de configuration déjà prêt dans le répertoire /usr/share/doc/openvpn/examples/sample-config-files/. Copiez le fichier de configuration client d'exemple

Question 6:

Lancez le serveur et le client pour établir la connexion VPN :

- Sur le serveur : `openvpn /etc/openvpn/server.conf`
- Sur le client : `openvpn /etc/openvpn/client.conf`

Mettez une machine en écoute avec netcat et connectez-vous avec l'autre en utilisant les adresses IP attribuées par le VPN, vous devez pouvoir vous échanger des messages.


```
Fri Nov 16 15:08:29 2018 169.254.8.73:58614 peer info: IV_L24v2=1
Fri Nov 16 15:08:29 2018 169.254.8.73:58614 peer info: IV_L20=1
Fri Nov 16 15:08:29 2018 169.254.8.73:58614 peer info: IV_COMP_STUB=1
Fri Nov 16 15:08:29 2018 169.254.8.73:58614 peer info: IV_COMP_STUBv2=
Fri Nov 16 15:08:29 2018 169.254.8.73:58614 peer info: IV_TCPNL=1
Fri Nov 16 15:08:29 2018 169.254.8.73:58614 Control Channel: TLSv1.2,
v1/SSLv3 ECDHE-RSA-AES256-GCM-SHA384, 2048 bit RSA
Fri Nov 16 15:08:29 2018 169.254.8.73:58614 [clientVpn] Peer Connection
Initiated with [AF_INET]169.254.8.73:58614
Fri Nov 16 15:08:29 2018 clientVpn/169.254.8.73:58614 MULTI_sva: pool
Pv4=10.8.0.2, IPv6=(Not enabled)
Fri Nov 16 15:08:29 2018 clientVpn/169.254.8.73:58614 MULTI: Learn: 10
clientVpn/169.254.8.73:58614
Fri Nov 16 15:08:29 2018 clientVpn/169.254.8.73:58614 MULTI: primary v
for clientVpn/169.254.8.73:58614: 10.8.0.2
Fri Nov 16 15:08:30 2018 clientVpn/169.254.8.73:58614 PUSH: Received c
sage: 'PUSH_REQUEST'
Fri Nov 16 15:08:30 2018 clientVpn/169.254.8.73:58614 SENT CONTROL [cl
'PUSH_REPLY,route-gateway 10.8.0.1,topology subnet,ping 10,ping-restart
nfig 10.8.0.2 255.255.255.0,peer-id 0,cipher AES-256-GCM' (status=1)
Fri Nov 16 15:08:30 2018 clientVpn/169.254.8.73:58614 Data Channel Enc
er 'AES-256-GCM' initialized with 256 bit key
Fri Nov 16 15:08:30 2018 clientVpn/169.254.8.73:58614 Data Channel Dec
er 'AES-256-GCM' initialized with 256 bit key
```

Serveur VPN

```
AES256-GCM-SHA384, 2048 bit RSA
Fri Nov 16 15:08:28 2018 [serverVpn] Peer Connection Initiated with [AF_INET]169
.254.5.22:1194
Fri Nov 16 15:08:29 2018 SENT CONTROL [serverVpn]: 'PUSH_REQUEST' (status=1)
Fri Nov 16 15:08:30 2018 PUSH: Received control message: 'PUSH_REPLY,route-gatew
ay 10.8.0.1,topology subnet,ping 10,ping-restart 120,ifconfig 10.8.0.2 255.255.2
55.0,peer-id 0,cipher AES-256-GCM'
Fri Nov 16 15:08:30 2018 OPTIONS IMPORT: timers and/or timeouts modified
Fri Nov 16 15:08:30 2018 OPTIONS IMPORT: --ifconfig/up options modified
Fri Nov 16 15:08:30 2018 OPTIONS IMPORT: route-related options modified
Fri Nov 16 15:08:30 2018 OPTIONS IMPORT: peer-id set
Fri Nov 16 15:08:30 2018 OPTIONS IMPORT: adjusting link_mtu to 1624
Fri Nov 16 15:08:30 2018 OPTIONS IMPORT: data channel crypto options modified
Fri Nov 16 15:08:30 2018 Data Channel Encrypt: Cipher 'AES-256-GCM' initialized
with 256 bit key
Fri Nov 16 15:08:30 2018 Data Channel Decrypt: Cipher 'AES-256-GCM' initialized
with 256 bit key
Fri Nov 16 15:08:30 2018 TUN/TAP device tun0 opened
Fri Nov 16 15:08:30 2018 TUN/TAP TX queue length set to 100
Fri Nov 16 15:08:30 2018 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Fri Nov 16 15:08:30 2018 /sbin/ip link set dev tun0 up mtu 1500
Fri Nov 16 15:08:30 2018 /sbin/ip addr add dev tun0 10.8.0.2/24 broadcast 10.8.0
.255
Fri Nov 16 15:08:30 2018 Initialization Sequence Completed
```

Client VPN

Grâce aux commandes `openvpn /etc/openvpn/server.conf` et `openvpn /etc/openvpn/client.conf`, nous lançons le serveur VPN et le client associé. Ces captures d'écran nous montre que la liaison s'est bien faite entre les deux machines.