Travaux pratiques sur SSL/TLS
Ahmed Serhrouchni

Question 1 :
Récupérer au moyen de la commande ***s_client*** le certificat du Crédit Lyonnais.

Réponse :
Openssl> s_client -host www.lcl.fr -port 443 -ssl3 -debug -state -showcerts

Question 2 :
Analyser et commenter les différents champs et extensions de ce certificat. Pour cela utiliser la commande x509.

Réponse :
Openssl> x509 -text -in nom_certificat

Question 3 :
Idem question 1 et 2 pour le site xxx.yyy.fr et également pour le serveur POP3 du domaine xxx.yyy.fr

Question 4 :
Analyser l'impact de ces certificats sur le fonctionnement de SSL.

Question 5 :
A l'aide de la commande ciphers déterminer les algorithmes supportés par TLS1_X. Interpréter le résultat, pour cela aidez-vous du document relatif à TLS1_2. Débrouillez-vous pour le retrouver !

Réponse :
Openssl> ciphers -TLS1_1 -s
Openssl> ciphers -TLS1_1 -s -stdname
Openssl> ciphers -TLS1_2 -s
Openssl> ciphers -TLS1_2 -s -stdname
Openssl> ciphers -TLS1_3 -s -stdname
Openssl> ciphers -TLS1_3 -s -stdname -psk

Question 6:
Déterminer pour les sites précédents les algorithmes de chiffrement et les tailles de clés supportés.

Question 7:
Déterminer pour une durée donnée le nombre d'établissent de session pour chaque cipher suite.
Repère:
OpenSSL> s_time -connect www.google.fr:443 -www / -new
Réponse:

```
IFS=":"
for cipher in $(openssl ciphers ALL); do
 echo $cipher ; openssl s_time -connect $1 -www / -new -time 10 -cipher $cipher 2>&1;
  echo
done
```

Question 8:

Générer une unique CA et installer son certificat sur l'ensemble des équipements.

Question 9:

En vous basant sur le fichier httpd.conf retrouver les différentes variables de configurations des certificats

Réponse :

SSLCertificateFile
SSLCertificateKeyFile
SSLCertificateChainFile
SSLCACertificatePath
SSLCARevocationPath
SSLVerifyClient require
SSLVerifyDepth 10

```
<Location />
SSLRequire (    %{SSL_CIPHER} !~ m/^(EXP|NULL)-/ \
        and %{SSL_CLIENT_S_DN_O} eq "Snake Oil, Ltd." \
        and %{SSL_CLIENT_S_DN_OU} in {"Staff", "CA", "Dev"} \
         and %{TIME_WDAY} >= 1 and %{TIME_WDAY} <= 5 \
         and %{TIME_HOUR} >= 8 and %{TIME_HOUR} <= 20       ) \
        or %{REMOTE_ADDR} =~ m/^192\.76\.162\.[0-9]+$/
</Location>
```

Question 10:

Configurer un serveur web apache avec une authentification par certificat uniquement du serveur.

Question 11:

Configurer un serveur web apache avec une authentification par certificat du serveur et du client.

Question 12:

Configurer vos clients de messagerie avec les différents certificats : clients et autorité de certification.

Question 13:

Vérifier les signatures sur Yahoo et Gmail !!!