8.1 Activité 1

# 1. en ce qui concerne le scénario, impliquant le protocole HTTP:

(a) quel fureteur, ainsi que sa version, a été utilisé?

Firefox 5.0

(b) quelle page le fureteur voulait-il récupérer et laquelle a-t-il affiché?

http://www.usherbrooke.ca/monportail

(c) s’il ne l’avait pas fait automatiquement, qu’aurait-il été affiché?

404?

# 2. en ce qui concerne le client:

(a) d’où croyez-vous qu’origine la requête, selon l’adresse source des messages?

De l’université ou d’un ordi connecté en VPN à l’université à cause de l’adresse source 10.\*\*\*…

(b) quel version de SSL/TLS est utilisée?

TLSv1

(c) combien de suites de chiffrement peut supporter le fureteur?

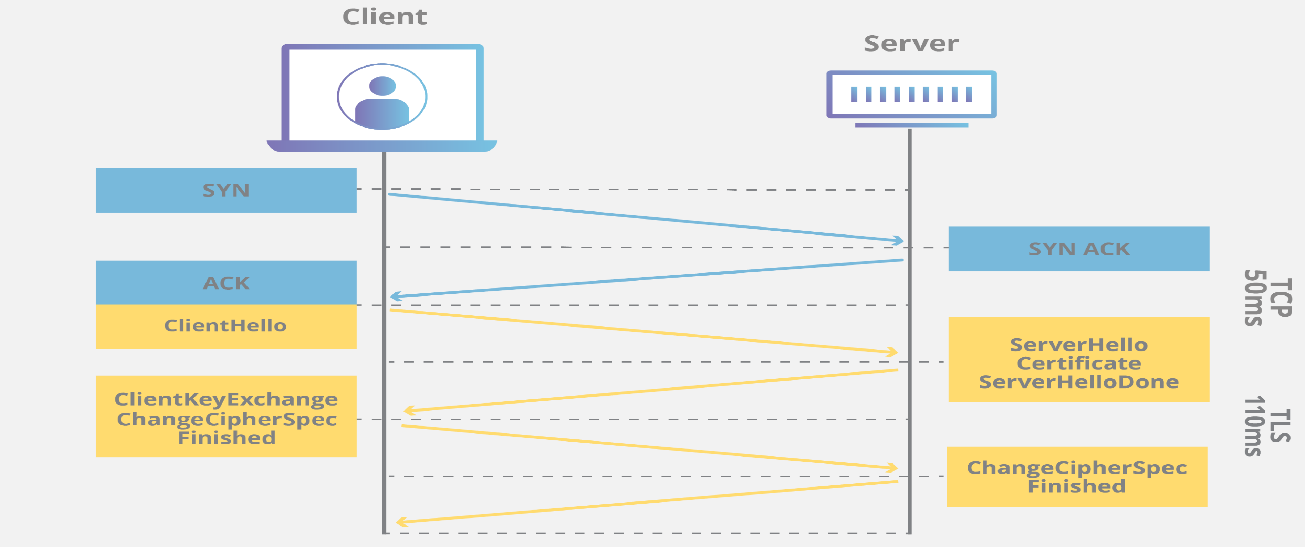
11, voir Cipher Suites

(d) a-t-il utilisé une cache de session?

Non car le session ID est 0

(e) où se situe le message Finished, de type Handshake?

Dans le dernier ChangeCypherSpec provenant du client ( Souvent les dernier encrypted handshake message )



# 3. en ce qui concerne le serveur:

(a) quel algorithme assure l’authentification?

Le certificat SSL

(b) quel algorithme assure la confidentialité de l’échange?

TLS\_RSA\_WITH\_RC4\_128\_MD5

(c) quel algorithme assure l’intégrité des messages?

MD5

(d) où se situe le message Finished, de type Handshake?

Dans le dernier ChangeCypherSpec provenant du serveur

L’algorithme choisi est insécure

# 4. en ce qui concerne le certificat du serveur:

(a) à qui appartient le certificat?

www.usherbrooke.ca

(b) qui a signé le certificat?

Thawte Consulting CC ( Certification Services Division )

(c) quelle est sa date d’activation?

2008-08-25, 20:12:44 (UTC)

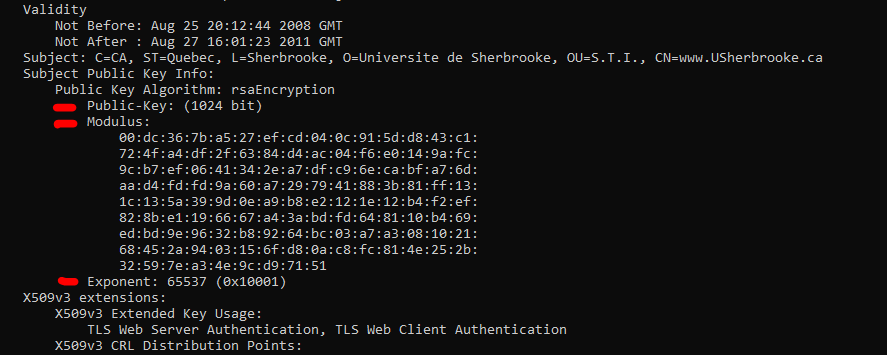
(d) quelle est sa date d’expiration?

2011-08-27, 16:01:23 (UTC)

8.2 Activité 2

Use ca -config \*filePath\* to use config file

# En utilisant la commande x509 de l’environnement OpenSSL, vous pourrez répondre aux questions suivantes, en considérant que les données qui vous avez sauvegardées sont un certificat X.509 encodé en format DER (le format binaire dont on se sert pour envoyer des certificats sur le réseau):



x509 -inform DER -in [certificate] -text -noout

(a) cette clef sert pour quel algorithme à clef publique?

rsaEncryption

(b) quelle est la dimension de la clef et du modulo?

1024 bits

(c) quelle est l’exposant?

65537

8.3 Activité 3

# 1. utilisez la commande windows nslookup pour connaître l’adresse IP associée au nom de domaine

Nslookup [domain name no http] => 132.210.4.144

# 2. utilisez l’argument -connect au port 443 (le port normalisé pour les connexions HTTPS) pour démarrer la négocation

Openssl s\_client -connect [ip\_address]:[port]

# 3. qui a émis le certificat?

Une chaine de 2 parties

1 : Sectigo Limited

2 : THE USERTRUST Network

# 4. quelle version du protocole a été utilisé pour la négociation?

TSLv1.2

# 5. quel jeu de chiffrement a été négocié?

ECDHE-RSA-AES128-GCM-SHA256

# 6. peut-on savoir la valeur la clef maîtresse?

Pas exactement puisqu’elle est encryptée? Sinon c’est :

3CF1FB70B15827810B0F35CEF95A2ECB6B3F4F931D3418B132DBC235AAF85837534C0336439747AD541BDCD664838177

8.4 Activité 4

# 1. générer la paire de clefs avec la commande genpkey (sans oublier de spécifier une dimension appréciable pour la clef)

openssl genpkey -algorithm RSA -out private\_key.pem -pkeyopt rsa\_keygen\_bits:2048

# 2. générer la demande de certificat avec la commande req (sans oublier de passer le fichier de configuration en paramètre)

Il faut préalablement extraire l’autorité

Pkcs12 -in autorite.pfx -out autorite.clef.pem

(Manuelment extract le pem en deux fichiers)

req -config gei761.conf -out cert\_request.pem -new -keyform PEM -key [key\_name]

# 3. signer la demande avec la commande ca (sans oublier de passer le fichier de configuration en paramètre)

ca -config gei761.conf -in cert\_request.pem -out cert\_signed.pem

# 4. Pour voir le certificat on peut utiliser

x509 -inform PEM -in cert\_signed.cer -text -noout

8.5 Activité 5

# 1. Quelle est l’adresse IPv4 de www.usherbrooke.ca ?

Dig [www.sherbrooke.ca](http://www.sherbrooke.ca) 132.210.3.136

# 2. Quelle est le nom de domaine et l’adresse IPv4 du serveur de courriel de usherbrooke.ca ?

Dig usherbrooke.ca MX

Et

Dig usherbrooke-ca.mail.protection.outlook.com

Domain: usherbrooke-ca.mail.protection.outlook.com

IP : 104.47.60.36

# 3. Quelle est l’adresse IPv6 de www.google.com ?

IPv6 : 2607:f8b0:4020:806::200e

DNSSEC. Sachant que les clés DNSSEC sont de type DNSKEY:

dig DNSKEY [ZONE]

# 1. Combien de clés possèdent la zone racine du DNS? [Zone «.»]

2 clés

# 2. Combien de clés possèdent la zone ca? [Zone “ca”]

2 clés

# 3. Combien de clés possèdent la zone usherbrooke.ca?

1 clé

Préparez-vous à utliser un serveur récursif local

1. tirez sur l’image docker internetsystemsconsortium/bind9:9.16

2. démarrez-la comme server DNS récursif2

Partir docker avec port UDP et TCP lier a un port local (comme 9000)

Ensuite sur WSL utiliser la commande : dig @127.0.0.1 -p 9000 www.google.ca

3. résolvez quelques noms de domaines pour connaître leur adresses IPv4 et IPv6 et leurs serveurs de courriels