Challenge FIC 2015 : Guide introductif

20 janvier 2015

Bienvenue dans cette première épreuve du challenge *forensics* ! Votre première activité consiste à accéder au site dédié à cet événement ; ce guide est là pour vous y aider.

Important : La clef USB qui vous a été donnée contient des fichiers permettant votre authentification auprès de nos serveurs. Ne la laissez pas sans surveillance !

Table des matières

1 Installation du certificat client

Le certificat *client* est envoyé à notre serveur pour vous identifier et vous authentifier. Si votre numéro d'équipe était *X*, il s'agirait du fichier nommé `client_X.p12` sur votre clef USB. Il est protégé avec le mot de passe qui vous a été fourni sur papier.

1.1 Mozilla Firefox

1. Ouvrez la fenêtre des préférences du navigateur.
2. Choisissez la catégorie **Avancé**.
3. Sélectionnez l'onglet **Certificats**.

4. Cliquez sur **Afficher les certificats**.
5. Sélectionnez l'onglet **Vos certificats**.
6. Cliquez sur **Importer…** et sélectionnez votre certificat client.

1.2 Chromium/Google Chrome

1.2.1 Sous Microsoft Windows

Le navigateur utilise les paramètres du système ; suivez les instructions concernant Internet Explorer.

1.2.2 Sous Mac OS

1. Ouvrez le menu des préférences du navigateur.
2. Cliquez sur **Afficher les paramètres avancés**.
3. Dans la section **HTTPS/SSL**, cliquez sur **Gérer les certificats**. Le trousseau d'accès se lance.
4. Dans le menu **Fichier**, sélectionnez **Importer des éléments…** et sélectionnez votre certificat client.
5. Choisissez un trousseau.

1.2.3 Sous GNU/Linux, FreeBSD ou OpenBSD

1. Ouvrez le menu des préférences du navigateur.
2. Cliquez sur **Afficher les paramètres avancés**.
3. Dans la section **HTTPS/SSL**, cliquez sur **Gérer les certificats**.
4. Sélectionnez l'onglet **Vos certificats**.
5. Cliquez sur **Importer…** et sélectionnez votre certificat client.

1.3 Internet Explorer

1. Double-cliquez sur le fichier `client_X.p12`. L'*assistant d'importation du certificat* apparaît.
2. Cliquez sur **Suivant**.
3. Cliquez sur **Suivant**.
4. Entrez le mot de passe fourni sur papier puis cliquez sur **Suivant**.
5. Cliquez sur **Suivant** (le certificat sera automatiquement placé dans le magasin *Personnel*).
6. Cliquez sur **Terminer**.

Selon votre version de Windows, votre système peut ensuite vous demander de définir un mot de passe pour protéger ce certificat.

Microsoft Internet Explorer : Aucune version de *Microsoft Internet Explorer* (nom d'« Internet Explorer » jusqu'à sa version 9 comprise) n'est supportée par notre serveur.

1.4 Safari

1. **Double-cliquez** sur le fichier `client_X.p12`.
2. Entrez le mot de passe fourni sur papier puis cliquez sur **Suivant**.

2 Installation du certificat de l'autorité de certification du serveur

Pour ne pas rencontrer d'avertissement lors de vos connexions au serveur, c'est-à-dire être en mesure de **vérifier la validité** du certificat du serveur, nous vous **recommandons** d'ajouter également à votre navigateur le certificat de notre autorité de certification.

Sur votre clef USB, ce certificat est nommé `ca.der`.

Note : Ajouter un certificat d'autorité racine n'est pas anodin : si un certificat était forgé par cette autorité pour un site tiers (comme Twitter, Gmail, etc.), il serait considéré valide par votre navigateur, permettant ainsi un espionnage *man in the middle* de vos échanges avec ce site.

Pour cette raison, au cas où vous oublieriez de le supprimer après le challenge, ce certificat n'est valide que jusqu'à 23 h 59 ce soir.

2.1 Mozilla Firefox

Suivez la même procédure que pour le certificat client (cf. sous-section 1.1) mais choisissez l'onglet **Autorités** (au lieu de *Vos certificats*) et, lorsqu'on vous demande pour quelles actions faire confiance au certificat, sélectionnez **Confirmer cette AC pour identifier des sites web**.

2.2 Chromium/Google Chrome

2.2.1 Sous Microsoft Windows

Le navigateur utilise les paramètres du système ; suivez les instructions concernant Safari.

2.2.2 Sous Mac OS

1. Suivez la même procédure que pour le certificat client (cf. sous-section 1.2) mais sélectionnez cette fois-ci le fichier `ca.der`.
2. Cliquez sur **Toujours approuver**.

2.2.3 Sous GNU/Linux, FreeBSD ou OpenBSD

1. Ouvrez le menu des préférences du navigateur.
2. Cliquez sur **Afficher les paramètres avancés**.
3. Dans la section **HTTPS/SSL**, cliquez sur **Gérer les certificats**.
4. Sélectionnez l'onglet **Autorités**.
5. Cliquez sur **Importer...** et sélectionnez `ca.der`.
6. Choisissez **Faire confiance à ce certificat pour identifier les sites web**.

2.3 Internet Explorer

1. **Double-cliquez** sur le fichier `ca.der`.
2. Cliquez sur **Installer un certificat...**
3. Cliquez sur **Suivant**.
4. Sélectionnez **Placer tous les certificats dans le magasin suivant** et choisissez le magasin **Autorités de certification racines de confiance**. Cliquez enfin sur **Suivant**.
5. Cliquez sur **Terminer**.
6. Un avertissement de sécurité apparaît, reprenant notamment notre avertissement de début de section. Cliquez sur **Oui**.

2.4 Safari

1. **Double-cliquez** sur le fichier `ca.der`
2. Cliquez sur **Toujours approuvé**