TP Numéro 4: Wireshark

1. Téléchargez le fichier Captures.zip du site web :
2. Allez à http://www-scf.usc.edu/~csci571/Special/Tutorials/wireshark_html/wireshark.html et trouvez la section sur le trafic HTTP « Examining HTTP Traffic »
3. Filtrez, dans le fichier capture1 , les paquets http. Dans une requête « Get » dans la liste de paquets filtrés, notez les détails dans le volet « Hypertext Transfer Protocol » sur :
    a. Host
    b. User-Agent
    c. Accepts
    d. Et d'autres informations pertinentes.
4. Trouvez une réponse à la requête GET. Notez les informations les plus intéressantes pour la requête. Détaillez puis la partie « HTTP chuncked response ». Si vous regardez maintenant le volet en bas quand vous examinez la partie « Data »dans le « chunked response » qu'est-ce que vous pouvez retrouver ?
5. Filtrez dans la liste de tous les paquets seulement les paquets HTTP. Pour faire ceci, il faut écrire « http » dans le champ marqué « Filtre » au-dessus de la liste de paquets. Est-ce que vous pouvez récupérer une liste avec les sites visités ? Comment est-ce que vous pouvez trouver le contenu (text, images, etc.) du site web visité ?
6. Le protocole TLS/SSL rassure la sécurité des échanges de messages en-ligne. Pour filtrer les messages TLS/SSL il faut mettre ssl dans le champ « Filtre » . En filtrant les messages SSL dans le fichier capture 1, trouvez une suite de messages qui commence par « Client Hello » et qui finit par « Application Data ».
7. Détaillez les contenus de ces messages. Notez les informations les plus pertinentes, en particulier les valeurs aléatoires, la suite de chiffres, les certificats (par exemple la méthode de certification, l'autorité de certification, etc.). Essayez de trouver, avec l'aide de l'Internet et du contenu du paquet « Client Key Exchange » quelle méthode a été utilisé pour l'échange de clés.
8. Ouvrez maintenant le fichier capture2 et filtrez par ssl. Trouvez les messages de Handshake avec 173.194.45.255. En tapant « host google.com » dans votre terminal essayez d'identifier quel site a été visité quand la handshake a eu lieu. Quelle est la version de TLS utilisée ? Quel est la chaine de certification ?
9. En utilisant les messages capturés par Wireshark, est-ce que vous pouvez déduire la structure du protocole TLS/SSL ? Comparez vos résultats avec les informations à trouver sur ce protocole en-ligne.
10. Tapez dans le terminal la commande « ssh –v cassius.istic.univ-rennes1.fr » . Qu'est-ce que se passe ? Identifiez les informations les plus importantes dans le log. Pour sortir, tapez CTRL + C. Pour avoir plus de détails vous pouvez également taper « ssh –vv <serveur SSH> » où la même commande avec -vvv.
11. Dans OpenSSL la commande « openssl s.client –connect <site web> : 443 » vous permette d'ouvrir une connexion sécurisé au site indiqué. Essayez d'introduire www.google.com pour le site. Quelle est la version de TLS utilisé ? Quel est la chaine de signatures pour le certificat du serveur ? Quels sont les chiffres choisis pour la communication sécurisée ?

12. En ajoutant la commande –no_ssl2 par exemple, on garantit que la connexion sécurisé ne va pas utiliser le protocole SSL en version SSL v2 (une version très vulnérable). La version la plus sécurisé du protocole est TLS v 1.2. Essayez maintenant de taper la commande : « openssl s.client –connect www.google.com:443 –no_ssl2, -no_ssl3, -no_tls1, -no_tls1_1, -no_tls1_2. Pourquoi est-ce que vous avez une erreur ?
13. On va utiliser la commande « openssl s.client –connect » avec les paramètres -no_ssl2, -no_ssl3, -no_tls1, -no_tls1_1 pour détecter quels sites web implémentent une version ancienne de TLS. Si le site ne permet pas une connexion de TLS 1.2, alors on va avoir un message d'erreur quand on roule la commande openssl s.client. Essayez la prochaine liste de sites web, en indiquant pour chacune quelle est la version la plus haute de TLS qu'elle permet :

    osur.univ-rennes1.fr
    www.chd.univ-rennes1.fr
    ipr.univ-rennes1.fr
    www.lhotellerie-restauration.fr
    asap2010.inria.fr
    ewshm2014.inria.fr
    dtk.inria.fr