Pràctica Complement: Wireshark TLS

Aplicacions i serveis d'internet — iTIC

Francisco del Águila López

19 d'abril de 2020

Índex

Resum

Captura de comunicació HTTP amb xifrat.

1 Introducció

Una bona eina per comprovar el funcionament de les comunicacions és **Wireshark**. La seva correcta instal·lació implica que l'usuari que executa el **Wireshark** formi part del grup *wireshark*. Quan es llença l'aplicació cal escollir la interfície que farà la captura de paquets.

Algunes funcionalitats importants per gestionar la captura són

1. Els filtres tant de captura com de visualització. Aquests filtres poden ser complexos ja que es poden combinar amb operadors lògics.
2. L'exportació d'objectes. D'aquesta manera es poden guardar localment en fitxers alguns del objectes transferits a través d'algun *stream* de comunicació. Per exemple, es podria guardar el contingut d'un fitxer *jpeg* que es transfereix en una comunicaicó HTTP.
3. Una altra funcionalitat molt interessant consisteix en fer el seguiment d'un *stream* concret. Això mostra tota la conversa amb els 2 interlocutors d'una manera clara, neta i simplificada. Aquesta funcionalitat es troba al menú desplegable del botó dret del ratolí, marcant la opció *follow* i escollint el tipus de *stream* desitjat.

Avui en dia gairebé la totalitat de les comunicacions HTTP en realitat són HTTPS, es a dir, estan xifrades. En aquest cas, la informació que intercanvien els dos interlocutors és confidencial i només aquests 2 interlocutors (client web i servidor web) són els únics que poden desxifrar-la. Per poder desxifrar aquesta informació cal disposar de les claus de xifrat que s'està fent servir. Per aquest motiu, el **Wireshark**, que és un tercer enmig de la conversa, no pot veure el contingut dels missatges que s'intercanvien. Per contra, si les claus de xifrat són proporcionades al **Wireshark**, llavors sí que podrà accedir al contingut d'aquests missatges.

2 Procediment de desxifrat

Tant Firefox com Chromium, i possiblement altres navegadors, suporten registrar les claus que es fan servir durant les sessions mantingudes per les capes de seguretat TLS. El registre d'aquestes claus es fa en un fitxer. Proporcionant aquest fitxer al **Wireshark** es pot desxifrar aquest trànsit.

El mecanisme utilitzat per crear aquest fitxer amb les claus de les sessions es fa definint una variable d'entorn que es passa als navegadors. Aquesta variable d'entorn és **SSLKEYLOGFILE**. Es crida al navegador web passant-li aquesta variable d'entorn apuntant a un fitxer definit amb un PATH absolut. Per passar aquesta variable d'entorn a través de la *shell* i que es mantingui en els processos fills cridats des d'ella es fa servir la comanda *export*.

La crida des d'un terminal seria el següent:

```
export SSLKEYLOGFILE=~/pathto/sslfile.log
firefox
```

Degut a com està dissenyat Firefox, cal que no hagi cap instancia prèvia de Firefox executant-se. En cas contrari no tindria efecte aquesta variable d'entorn.

El mecanisme per informar a **Wireshark** sobra la existència d'aquest fitxer és a través de les *preferències*. Allà s'ha de buscar el protocol *SSL* i proporcionar a l'opció de *(Pre)-Master-Secret log filename* la localització del fitxer definit a la variable d'entorn. Un cop fet això, totes les comunicacions HTTPS passaran a estar desxifrades, mostrant tot el contingut de la conversa HTTP.

Informació de referència sobre aquest procediment la podeu trobar a [Wir20].

Referències

[Wir20] Wireshark. *Wireshark TLS*. 2020. URL: `https://wiki.wireshark.org/TLS` (consultat 19 d'abr. de 2020).