Outil de visualisation de captures réseau

Encadrants: Guillaume Piolle Nicolas Prigent

Lors de l'audit d'un réseau (filaire ou wifi), on peut être amené à effectuer une capture du trafic en espérant y trouver des éléments exploitables (pour la poursuite d'un test d'intrusion, par exemple). Néanmoins, la forme de ces traces est rarement pratique pour y rechercher l'information pertinente. Le but de ce projet est de développer un outil de visualisation d'une capture réseau (éventuellement après dissection protocolaire, par Wireshark ou autre), de manière à pouvoir présenter les flux de manière lisible et graphiquement organisée, permettant le filtrage et l'identification rapide des informations. L'outil devra également être capable de reconstituer les éléments capturés dans tel ou tel flux, comme un e-mail et ses pièces jointes, une session de navigation web, un fichier échangé, une conversation de messagerie instantanée ...

Idéalement, l'outil devrait être capable d'identifier et de mettre en évidence automatiqeument certains éléments particulièrement utiles à l'évaluation de sécurité du réseau, comme la transmission d'identifiant dans un flux non chiffré ou l'utilisation de schémas de chiffrement déconseillés. Outre la détection des informations sensibles, un autre objectif peut être l'identification automatique (et passive) de vulnérabilités connues.

L'outil peut être envisagé comme fonctionnant en temps réel (sous la forme d'un plugin Wireshark, par exemple) ou bien hors ligne, sur une trace enregistrée en XML (ou autre). L'outil aura le bon goût d'être développé sous une licence libre sur une forge publique.

Références

[1]"Wireshark development." [Online]. Available: https://wiki.wireshark.org/Development

[2]"PyShark – Python packet parser using wireshark's tshark." [Online]. Available: http://kiminewt.github.io/pyshark/

[3]"PCAP parsing using Python with Pyshark." [Online]. Available: https://www.linkedin.com/pulse/daily-pulse-mcmuffins-dinner-reddit-gets-newsy-beam-me-katie-carroll

[4]"Chaosreader." [Online]. Available: http://chaosreader.sourceforge.net/