Semaine 6 : Analyse de paquets
IPL I317B Sécurité : labo

Olivier Choquet & Thibault Vanwersch

24 octobre 2023

Objectif

Ce labo abordera quelques bases de l'analyse de paquets réseaux, nous travaillerons ici sur un capture au format pcap mais nous pourrions aborder bon nombre de ces points sur une capture en direct.

Les exercices qui suive utilisent des paquets provenant de « *adversary.pcap* ».
Ce fichier est extrait du cours SANS SEC503: Intrusion Detection In-Depth. C'est un formation très spécialisé qui va en profondeur dans l'analyse réseau.
Nous allons ici effleurer le sommet de ce très large sujet.

Outil

Pour cet exercice, nous allons utiliser l'analyseur de paquet Wireshark que vous pouvez télécharger à l'adresse suivante pour Windows et Mac :

https://www.wireshark.org/index.html#_download_hfnhr_292

Si vous utilisez gnu/linux, vous devriez trouver Wireshark dans les dépôts de votre distribution.

Wireshark contient un système de filtre permettant de n'afficher que certains paquets. Dans certains exercices, vous trouverez des filtres à appliquer pour ne voir qu'un sous ensemble des paquets. Ces filtres seront écrit ici `avec cette police d'écriture`.

Questions

1. L’adresse ip 92.242.140.21 a eu une drôle d’activité, en regardant tous les paquets lié à cette ip, pouvez-vous en déduire son comportement ?
   `ip.addr==92.242.140.21`
   Indice : Quel est le type ICMP ?

2. Même question pour l’ip 192.168.11.62 avec le port source 52999.
   `ip.addr==192.168.11.62 and tcp.port==52999`
   Indice : Three-way handshake

3. Un paquet peut en cacher un autre …
   Pour cette exercice, nous allons nous intéresser aux paquets échangés entre 92.68.122.132 et 184.168.221.63.
   `ip.addr==184.168.221.63 and ip.addr==92.68.122.132`
   1. Quel est l’unique type de paquet échangé ?
   2. La taille de certains paquets ne vous semble-t-elle pas un peu grosse pour ce type de paquet ? Qu’y a-t-il dans les paquets plus gros ?
   3. Pourquoi donc quelqu’un ferait-il ça ?
4. La plupart du temps, les protocoles ont leur contenu séparé dans plusieurs paquets et les lire un par un pour essayer de dégager le sens général de l’échange est fastidieux. Pour régler ce problème, intéressons nous maintenant à la fonctionnalité de Wireshark « follow : tcp-stream ». Celle-ci permet de rassembler le contenu de plusieurs paquets.
   En scrollant un peu dans ce pcap, vous devriez voir des paquets du protocole IMAP (mail), effectuer un clique-droit, *follow : tcp-stream*. Que constatez-vous ?
5. Un peu plus loin, vous pouvez trouver du trafic SMB avec un serveur SMB qui semble se trouver sur 192.168.1.8, procédez à l’inspection du tcp-stream comme nous l’avons vu à l’exercice précédent.
   Protip : vidow.exe est un vrai malware, laissez le dans son pcap si vous utilisez Windows.

6. Avec quelques autres suivis de tcp-stream, vous pouvons continuez à analyser cette histoire, que ce passe-t-il ensuite …