PLATYPUS

TP 3A S1 SECU
Sécurité Réseau - Wireshark

V1, Louis Cherel, Léonard Benedetti, François Déchelle

Installation de Wireshark

Téléchargez wireshark depuis le site officiel. Si vous êtes sur une machine dont vous n'avez pas les droits administrateur, téléchargez la version portable, sans installation.

Ouverture d'un .pcap

1) Qu'est-ce qu'un .pcap ?
2) Que contient-il ?

Analyse d'un trafic réseau

Scénario

Vous êtes dans votre entreprise depuis maintenant 5 ans, et vous sentez que vous êtes sur la sellette. Vos résultats sont en baisse, vos "stats ne sont sont plus assez disruptives". Votre manager ne vous donne plus de travail depuis plusieurs semaines et vos collègues vous narguent.

Un concurrent de votre entreprise, qui vous a repéré après quelques échanges véhéments sur les réseaux sociaux, vous sollicite car il a besoin de vos compétences, sous-exploitées par votre entreprise actuelle.

Il vous demande, pour preuve de votre bon vouloir, d'avoir accès à la liste de tous les clients de votre boîte. Seul problème, vous n'avez pas les droits d'accès.

Vous vous rappelez cette discussion avec le personnel informatique qui vous a expliqué que le réseau interne de l'entreprise est particulièrement vétuste, notamment les services CRM qui sont assez peu sécurisés. Mais, manque de budget, on fait au mieux, et de toute façon le minimum est quand même fait !

Le fichier client est sauvegardé très régulièrement, et il est imprenable car il circule de manière sécurisée.

Vous prenez votre mal en patience et branchez un petit boitier derrière le bureau de Jean Claude, le CRM Manager, entre son câble Ethernet et son ordinateur.

Analyse

Une semaine après, vous retournez chercher votre appareil, vous ouvrez le fichier enregistré avec Wireshark, et vous ne gardez que les échanges réalisés avec la machine qui s'occupe du CRM. Vous avez sauvegardé ce fichier sous le nom "capture.pcap".

Ouvrez ce fichier avec Wireshark.

Étudiez la requête n°4

Tout d'abord, cherchez à comprendre ce que vous avez sous les yeux.

3) Quelle adresse IP est la source ?
4) Quelle adresse IP est la destination ?
5) Quel est le protocole utilisé ?
6) Quel navigateur web a émis la requête ?
7) Quelle est la langue configurée par défaut dans ce navigateur ?
8) À quoi correspondent les 3 échanges qui précèdent cette requête ?

Allons plus loin

9) Quel est le n° de frame de la réponse HTTP ?
10) Que contient la réponse ?

Challenge

Trouvez le fichier client. Plusieurs étapes sont nécessaires pour y accéder. Lorsque vous tomberez dessus, aucun doute ne sera permis quant au fait que ce soit bien ce que vous cherchiez.

11) Quel est le **flag** ?

Conclusion

12) Comment le service informatique aurait-il pu éviter cette fuite de données ?
13) Le HTTP est-il un protocole sécurisé ? Pourquoi ? Qu'est-ce qui le remplace actuellement ?

Quelques tutoriels Wireshark

Dans les tutoriels, la partie qui vous sera utile concerne l'analyse. La partie "capture" ne vous concerne pas dans ce TP.

- https://blog.nicolargo.com/2011/05/capturer-et-analyser-un-trafic-reseau-avec-wireshark.html
- http://www.machaon.fr/isn/reseaux/Fiche-Wireshark.pdf
- https://inetdoc.developpez.com/tutoriels/analyse-reseau-wireshark/

Une dernière remarque

Les techniques décrites dans ce document ne doivent pas être utilisées à des fins frauduleuses. Le scénario proposé serait bien sûr illégal en pratique.

À toutes fins utiles, nous rappelons que l'article 323-1 du Code pénal punit de deux ans d'emprisonnement et de 60 000 € d'amende le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données.