R5.B.09
≪ Cybersécurité ≫

TP 1 : Attaques Passives

L'objectif de ce TP est de prendre en main les activités de reconnaissance en cybersécurité. Vous allez examiner des traces réseau dans un premier temps pour extraire des informations précises et vous habituer à lire des captures de trafic. Ensuite, vous analyseriez d'autres traces pour étudier le comportement de votre victime, ici moi, et d'extraire des informations d'"espionnage", vous informant à la fois sur les activités de la victime, mais également leurs tendances, envies, mais également la topologie du réseau, les équipements, logiciels, etc. Dans ce TP, vous serez guidé dans l'analyse, mais ils seraient à vous de pousser votre analyse plus loin pour sortir le maximum d'informations possibles. À la fin du TP, vous devez rendre un rapport écrit (PDF) contenant les traces de cotre analyse, les preuves de vos suppositions/déductions, et surtout votre raisonnement de vos choix.

Bon courage cyber-guerriers !

Prise en main de Wireshark

Pour ce TP, vous allez étudier et analyser des traces réseau sous forme de fichier `pcap` via l'outil Wireshark. Wireshark est un très bon outil à la fois de capture et d'analyse de trafic puisqu'il fait beaucoup du travail a votre place, vous fournissant des informations sur le type du paquet, les sources et les destinations, etc.

Bien qu'il existe plusieurs méthodes pour vous aider dans votre analyse, deux d'entre eux sont particulièrement utiles : le filtre d'affichage, et les méthodes statistiques.

Filtres d'affichage

Sans doute l'outil le plus utilisé dans Wireshark est la capacité à filtrer les données selon divers éléments, tel que le type de paquet, l'adresse mac de source, l'adresse IP de destination, etc. Lorsque vous êtes devant une capture de plusieurs milliers de paquets, c'est ici que vous tournerez votre attention en premier Il y a plusieurs méthodes pour appliquer un filtre à votre capture. Dans un premier temps, vous pouvez utiliser des informations déjà présentes dans votre capture, par exemple l'adresse IP destination d'un paquet ICMP. Vous pouvez alors faire `clique droit --> appliquer filtre` pour n'afficher que les paquets à destination de cette adresse.

Vous pouvez trouver une documentation sur comment utiliser les filtres d'affichage [1], ainsi qu'une présentation comment utiliser le registre d'expressions de filtrage [2], accessible en `clique droite` sur la barre de recherche, sur le site web de Wireshark.

Enfin, un ≪ cheat sheet ≫ [3] est également disponible avec quelques filtres basiques.

Méthodes statistiques

Wireshark intègre quelques outils de représentation statistiques, disponibles à travers l'onglet `Statistiques`. Bien sûr, Wireshark est incapable de faire le travail à votre place, mais grâce à ces outils telle la hiérarchie protocolaire ou encore les conversations, vous pouvez trouver ce que vous cherchez plus facilement.

Wireshark fournit de nouveau une documentation sur ces différents méthodes [4].

1. https://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html
2. https://www.wireshark.org/docs/wsug_html_chunked/ChWorkFilterAddExpressionSection.html
3. https://cdn.comparitech.com/wp-content/uploads/2019/06/Wireshark-Cheat-Sheet.pdf
4. https://www.wireshark.org/docs/wsug_html_chunked/ChStatistics.html

1 Recherche d'informations

Pour cette partie, vous allez télécharger et ouvrir la capture `Exo1.pcap` fourni sur moodle. Vous verrez alors un ensemble de plus de 300 paquets capturés pour votre analyse. Ici, vous n'êtes pas demandé pas d'effectuer une analyse approfondie des données, mais plutôt de suivre la méthodologie semblable à l'« écoute clandestine » et extraire des informations ciblées, si possible.

Dans cette capture, il y a 4 échanges : HTTP, FTP et SSH.

1.1 HTTP

Un échange HTTP a eu lieu dans cette capture. Vous devez dans un premier temps identifier l'URL du site web ainsi que son adresse IP. Que pouvez-vous en dire sur ces éléments ?

Analyser l'échange pour extraire les informations de HTML. Quel type de « service » est fourni par ce site web ?

Enfin, identifiez un échange d'authentification qui a eu lieu avec le serveur web. Est-ce qu'un nom d'utilisateur a été renseigné ? Si oui, lequel ? Est-ce qu'un mot de passe a été renseigné ? Si oui, lequel ? Que pouvez-vous en dire sur ce que vous avez trouvé par rapport aux consignes de sécurité que vous connaissez, et mentionnés en cours ?

1.2 FTP

Dans cette capture, une session FTP a été initiée vers un serveur distant. Suivez la même démarche que pour l'échange HTTP et identifier le domaine et l'adresse IP du serveur.

Que savez-vous sur le fonctionnement un échange FTP ? Reposez sur les traces FTP dans la capture pour présenter le fonctionnement. Notez si une authentification a eu lieu et le nom d'utilisateur et/ou mot de passe utilisé. Précisez également ce qui a été fait lors de la session FTP (upload, téléchargement, suppression, afficher, etc.).

1.3 SSH

Dans ce fichier, se trouve une session SSH. Avec quel serveur la session SSH a eu lieu ? Donnez le nom de domaine, l'adresse IP et votre analyse comme pour les deux précédentes questions.

Les sessions SSH peuvent être initiées via un mot de passe, ou via une clé. Lequel est utilisé ici et quelles informations pouvez-vous en tirer ? Est-ce que c'est possible de trouver un mot de passe dans une session SSH ?

1.4 SSH clandestine

Une autre session SSH se trouve également dans ce fichier, mais il est caché et pas reconnu par Wireshark. Parsez le fichier pour trouver le nom de domaine du serveur contacté avec son adresse IP. Est-ce que vous avez une idée de pourquoi Wireshark n'a pas reconnu la session SSH ? Expliquez l'avantage de cette approche, mais également les inconvénients.

Appelez l'enseignant pour afficher la session SSH une fois trouvée.

2 Analyse approfondi

Maintenant, que vous avez compris comment parser une capture de trafic avec Wireshark et vous avez pu extraire les informations recherchées, téléchargez et ouvrez le fichier `Exo2.pcap` sur moodle. Cette capture est un peu plus grande avec presque 23 000 paquets capturés. Cette capture comprend plusieurs échanges différents. Il y a également beaucoup de données chiffrées, liés à l'utilisation par exemple de HTTPS et d'autres méthodes de communication sécurisés.

Ici, vous avez deux taches : extraire le maximum d'informations possibles, et donner votre opinion des habitudes, envies et ce qu'aime faire l'utilisateur.

2.1 À la pêche à l'information

L'objectif de cet exercice est d'utiliser ce que vous avez vu à l'exercice précédent pour extraire le maximum d'informations possibles. Pour vous aider, voici quelques éléments qui sont disponibles dans cette capture que vous pouvez extraire :

- noms de domaine et adresses IP des sessions HTTP
- le navigateur utilisé
- Le système d'exploitation de l'utilisateur
- Le nom d'un logiciel de gestion de jeux
- Le lancement d'une session de jeu en ligne (nom du jeu, url du serveur & IP, port associé)
- le client mail utilisé
- les serveurs mail utilisés (poser des hypothèses sur les domaines des adresses mail)
- la plage d'adresses IP du réseau local du client (regardez les machines sur le même réseau du client)(
- le rôle des équipements du réseau local (essayez d'identifier la passerelle, la marque, les autres machines du réseau local qui sont sollicitées)

N'hésitez pas à regarder plus loin avec d'autres outils, par exemple Who.is sur certains domaines pour les associations mail. Vous pouvez également analyser certains éléments, comme les adresses MAC pour trouver leur fabriquant et avoir des informations sur le matériel, voir même le système d'exploitation (macvendors [5]).

2.2 Comportement utilisateur

À partir de ce que vous avez trouvé juste avant, donnez votre opinion de l'utilisateur surveillé, en vous reposant sur votre analyse. Reposez-vous sur les informations des échanges par l'utilisateur, mais aussi sur le réseau et les systèmes pour tirer une conclusion sur les envies et les motivations de l'utilisateur.

Bravo, vous êtes à présent des cyber-espions !

5. https://macvendors.com/