CentraleSupélec

Visualisation de traces réseaux

Thibault LENGAGNEet Nicolas NGÔ-MAÏ

Centrale Supélec - Campus de Rennes

2 février 2016

Plan

Rappel du Sujet

- Le but est de créer un outil destiné aux pentesters, permettant d'analyser efficacement une trace réseau.
- L'attaquant dispose d'une trace réseau mais n'a aucune connaissance de ce réseau.
- Un fichier pcap devient rapidement très volumineux et son analyse est laborieuse, nécessitant l'utilisation de plusieurs outils.

Rappel du Sujet

L'attaquant espère soutirer des informations sur le réseau :

- Les adresse IP identifiées (+ géolocalisation, résolution DNS)
- Les protocoles utilisés (en particulier non chiffrés ou mal configurés)
- Les noeuds importants du réseau (serveur de fichier, DNS, LDAP...)
- Extraire des traces réseaux filtrées, extraire les données sensibles

Retour sur les choix technologique

- Nous voulions à l'origine interfacer plusieurs outils (Ettercap, ChaosReader, tcptrace...)
- Finalement, Scapy nous permet de manipuler la trace réseau de façon satisfaisante.
- Enfin, le choix initial de PyQt a été remplacé par une interface web.

Resumé des choix technologiques

- Pour stocker les résultats, nous avons choisi d'utiliser une base de donnée PostGreSQL
- Nous avons trouvé un outil très puissant pour faire de la visualisation : D3.js
- Nous avons donc choisi de mettre en place un serveur web en python (Flask)

Retour sur les objectifs fixés

Nous avons d'ores et déjà remplis les objectifs suivants :

- Extraction de sessions, des utilisateurs, et des protocoles
- Création de statistiques, extraction des données en clair
- Visualisation en barre parallèle

Plan

Schéma fonctionnel de notre programme :

Analyse du fichier pcap

- Libraire Scapy permet de lire nos fichiers .pcap, puis de manipuler les packets.
- Une fonction parse parcourt tous les paquets. Des statistiques sont alors tirées du protocole en jeux,
- La fonction parse parcourt également tous les sessions, et enregistre les trames de chaque session

Performances du parser

- Les fichiers pcap peuvent atteindre plusieurs Giga assez rapidement.
- Le programme n'écrit dans la base de donnée qu'une seule fois, à la fin de la collecte des données
- Certaines tables sont simplement commit. Pour d'autre tables, le résultat est stocké dans un dictionnaire jusqu'à la fin.

Plan

Lancement de l'outil

Le projet est disponible sur
https ://github.com/lechinoix/Pcap-visualization-project
Après avoir suivi la procédure d'installation, on démarre le serveur pour accéder à l'interface web

CentraleSupélec

Question, remarques ?

Plan

Objectifs à remplir

- Ajouter les différents filtres possibles
- Extraire d'un pcap a partir des trames filtrées
- Extraire les données non chiffrées des protocoles SMTP,IMAP,POP,LDAP
- Ajouter la résolution DNS
- Ajouter d'autres mode de visualisation (carte des IP,..)

Plan

Merci de votre attention !