CentraleSupélec

Visualisation de traces réseaux

Thibault LENGAGNEet Nicolas NGÔ-MAÏ

Centrale Supélec - Campus de Rennes

4 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.
- L'analyse lui permet d'obtenir des mots de passe, la connaissance machines non sécurisées, du contenu non chiffré

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

Cela lui permettra d'attaquer plus facilement le réseau

Rappel du Sujet

Scénario d'utilisation

- Upload du fichier Pcap, affichage en continu des données analysées
- Liste des protocoles / hosts filtrables dans la sidebar.
- Vue treemap qui permet de caractériser les hosts
- Passage en coordonées parallèle avec seulement les hôtes filtrés qui permet de valider les hypothèses
- L'outil permet de trouver des machines mal configurées et d'extraire des informations.

Retour sur les choix technologiques

- 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.

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 coordonnées parallèles

Plan

Nos choix de technologies

- Le travail s'articule principalement autour de deux technologies : Scapy et D3.js
- Scapy est une librairie Python pour faire de la manipulation de trames réseaux
- D3.js est une librairie Javascript qui permet de faire de la manipulation de SVG lié à des données.

Nos choix de technologies

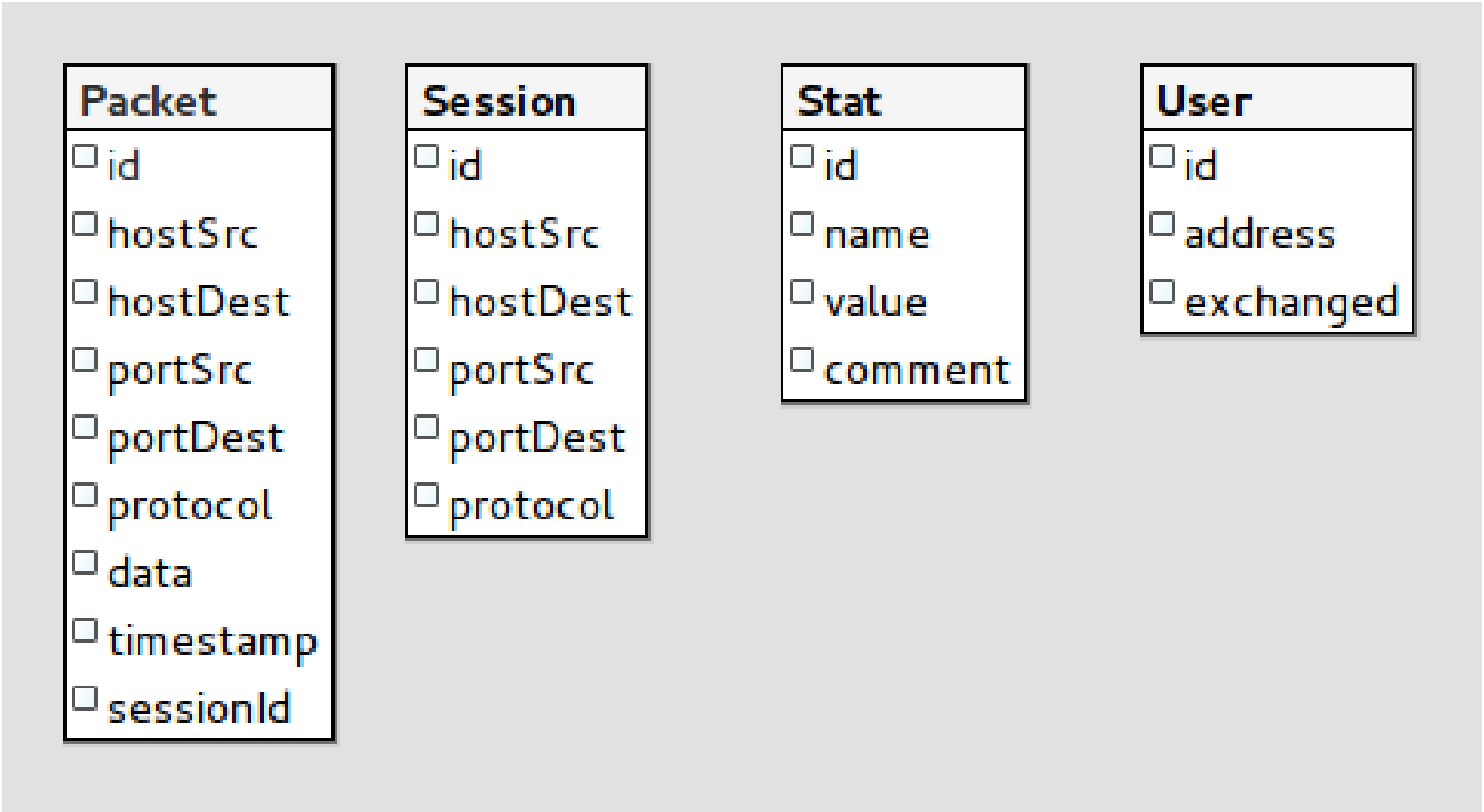
- Serveur web Flask (Python) associé à une base de données Postgres et un ORM python, SQLAlchemy
- Pour réaliser un update continu en fonction des données analysées par le serveur, nous avons installé SocketIO

Présentation de D3.js

- Framework JS pour faire de la manipulation d'objets du DOM en les liant à des données
- On peut ainsi faire apparaître des balises html ou SVG en fonction d'une donnée arbitraire
- Du coup, les graphes s'adaptent aux données de façon automatique
  -> La structure des données est ce qui détermine le graphe

Démonstation D3.js

Quatres tables dans la base de données :

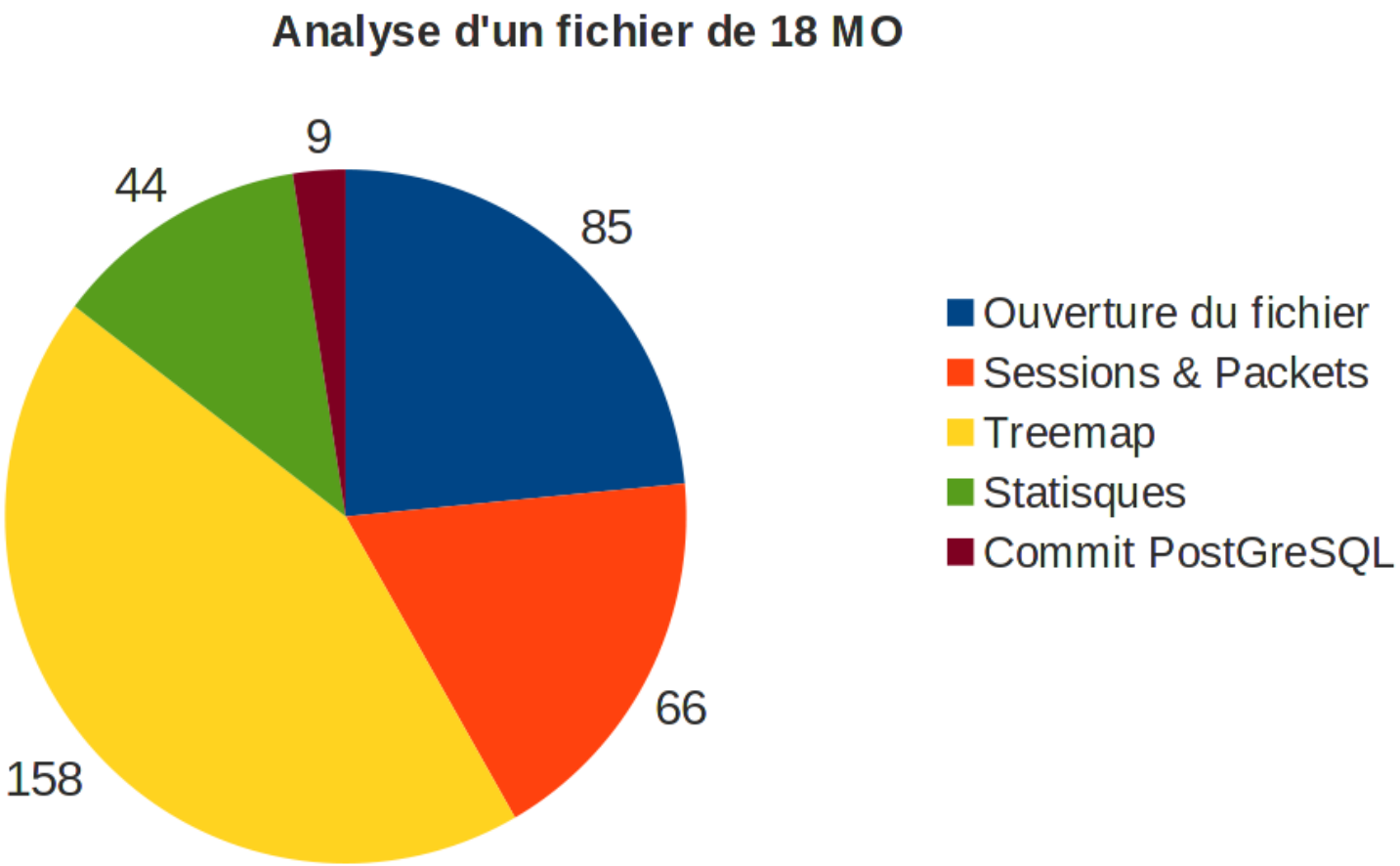


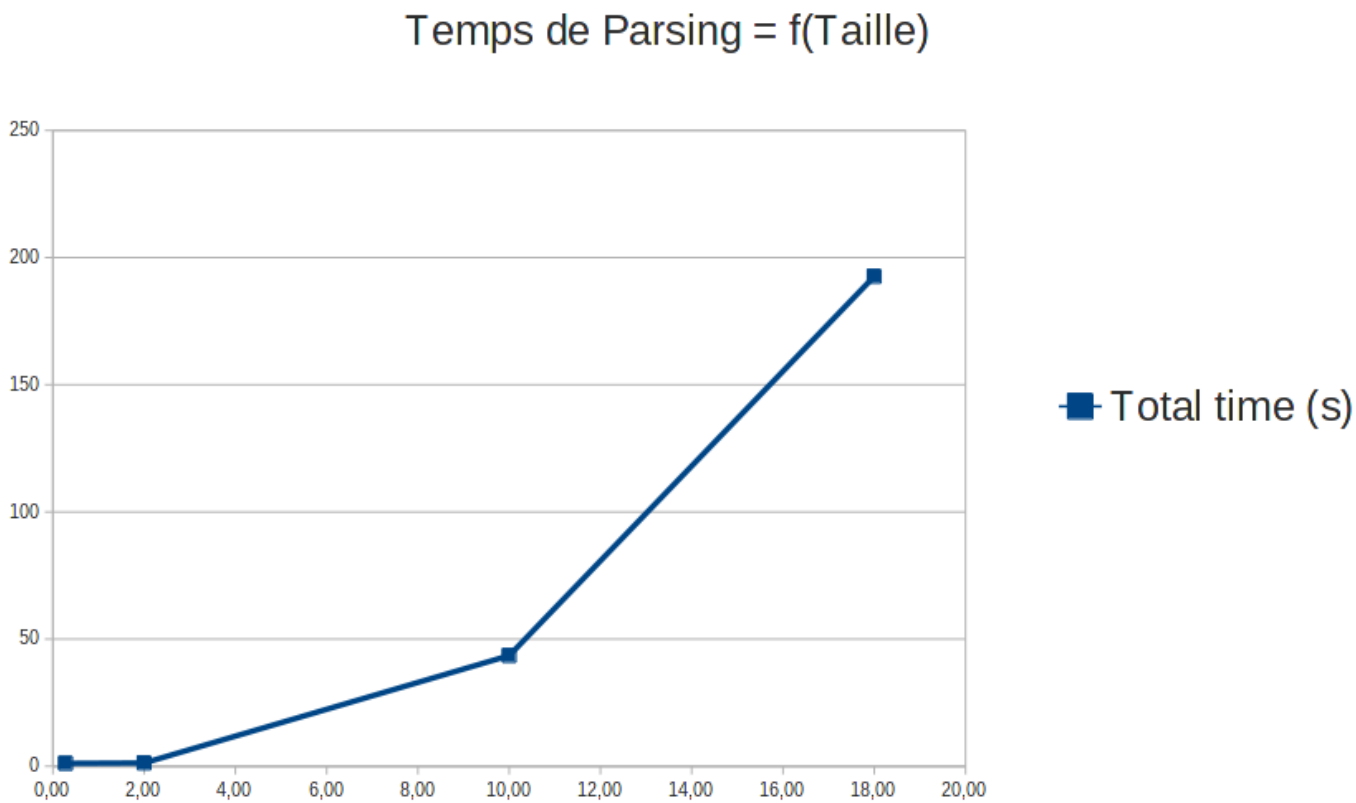
Analyse du fichier pcap

- La libraire Scapy permet de lire nos fichiers, puis de manipuler les packets.
- Une fonction parcourt tous les paquets. Les tables User et Stats sont alimentées
- Une fonction parcourt tous les sessions. Les tables Session et Trames sont alimentées

Performances du parser

- Les fichiers pcap peuvent atteindre plusieurs Giga assez rapidement.
- L'écriture dans la base de donnée étant couteuse,le programme écrit dans la base de donnée une seule fois, à la fin de la collecte des données
- Nous réalisons nos tests sur des traces d'entreprise anonymisées (ftp ://ftp.bro-ids.org/enterprise-traces/hdr-traces05/)


Analyse d'un fichier de 18 MO
9
44
85
66
158
Ouverture du fichier
Sessions & Packets
Treemap
Statisques
Commit PostGreSQL


Temps de Parsing = f(Taille)
250
200
150
100
50
0
0,00
2,00
4,00
6,00
8,00
10,00
12,00
14,00
16,00
18,00
20,00
Total time (s)

CentraleSupélec

Plan

Plan

Objectifs à remplir

- Ajouter les différents filtres possibles
- Extraire un .pcap a partir de 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,..)

Problématiques à venir

- Technos suffisantes ? Tests de performance à venir
- Morcellement de l'analyse du Pcap
- Création de vues interactives, et donc d'une belle architecture de données

Plan

Merci de votre attention !

https ://github.com/lechinoix/Pcap-visualization-project

Détail du champs exchanged de Users


```
{
   "Volume": 28284,
   "Protocole": {
      "AUTRE": {
         "Nombrein": 291,
         "Volumeout": 12732,
         "Nombreout": 284,
         "Volumein": 13494
      },
      "POP3S": {
         "Nombrein": 9,
         "Volumeout": 386,
         "Nombreout": 7,
         "Volumein": 510
      },
      "ICMP": {
         "Nombrein": 14,
         "Volumeout": 546,
         "Nombreout": 13,
         "Volumein": 616
      }
   }
}
```