

# Visualisation de traces réseaux

**Thibault LENGAGNE et Nicolas NGÔ-MAÏ**

Centrale Supélec - Campus de Rennes

4 février 2016

- 1 Retour sur les choix technologiques
- 2 Détails techniques
- 3 Démonstration
- 4 Travail à venir
- 5 Conclusion

- 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.

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

- Nous voulions à l'origine interfacier 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.

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

- 1 Retour sur les choix technologiques
- 2 Détails techniques**
- 3 Démonstration
- 4 Travail à venir
- 5 Conclusion

- 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.



- 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

- 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



# Démonstration D3.js

Quatres tables dans la base de données :

Packet
<input type="checkbox"/> id
<input type="checkbox"/> hostSrc
<input type="checkbox"/> hostDest
<input type="checkbox"/> portSrc
<input type="checkbox"/> portDest
<input type="checkbox"/> protocol
<input type="checkbox"/> data
<input type="checkbox"/> timestamp
<input type="checkbox"/> sessionId

Session
<input type="checkbox"/> id
<input type="checkbox"/> hostSrc
<input type="checkbox"/> hostDest
<input type="checkbox"/> portSrc
<input type="checkbox"/> portDest
<input type="checkbox"/> protocol

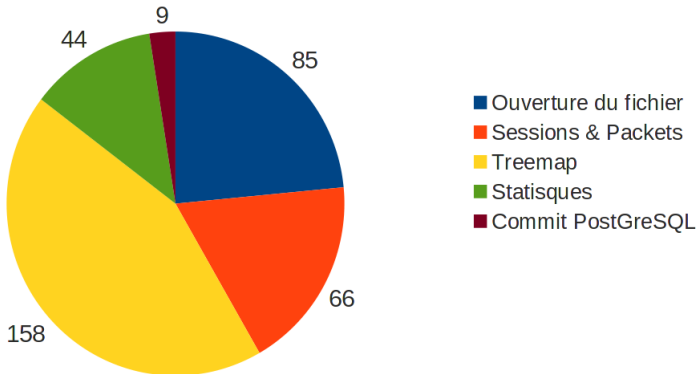
Stat
<input type="checkbox"/> id
<input type="checkbox"/> name
<input type="checkbox"/> value
<input type="checkbox"/> comment

User
<input type="checkbox"/> id
<input type="checkbox"/> address
<input type="checkbox"/> exchanged

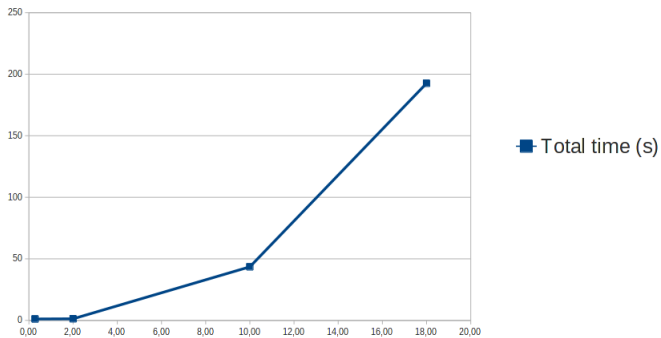
- La librairie Scapy permet de lire nos fichiers, puis de manipuler les packets.
- Une fonction parcourt tous les paquets. Les tables User et Stats sont alimentées
- Une fonction parcourt tous les sessions. Les tables Session et Trames sont alimentées

- Les fichiers pcap peuvent atteindre plusieurs Giga assez rapidement.
- L'écriture dans la base de donnée étant coûteuse, 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/](ftp://ftp.bro-ids.org/enterprise-traces/hdr-traces05/))

## Analyse d'un fichier de 18 MO



Temps de Parsing =  $f(\text{Taille})$





- 1 Retour sur les choix technologiques
- 2 Détails techniques
- 3 Démonstration**
- 4 Travail à venir
- 5 Conclusion

- 1 Retour sur les choix technologiques
- 2 Détails techniques
- 3 Démonstration
- 4 Travail à venir**
- 5 Conclusion

## Scénario d'utilisation

- Upload du fichier Pcap, affichage en continu des données analysées
- Liste des protocoles / hosts avec des chiffres dans la sidebar
- Vue treemap qui permet de caractériser les hosts, filtrage dans la barre à gauche
- Passage en coordonnées parallèle avec seulement les hôtes filtrés qui permet de valider les hypothèses
- Vue géographique ?

## 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

## 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,..)

- 1 Retour sur les choix technologiques
- 2 Détails techniques
- 3 Démonstration
- 4 Travail à venir
- 5 Conclusion**

Merçi de votre attention !