CentraleSupélec

# Visualisation de traces réseaux

**Thibault LENGAGNEet Nicolas NGÔ-MAÏ**

Centrale Supélec - Campus de Rennes

30 janvier 2016

# Plan

1 Sujet - Objectifs - Choix

2 Démonstration

3 Travail à venir

4 Conclusion

# Rappel du Sujet

Créer un outils pour pentester, permettant d'analyser efficacement une trace 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 interfacer plusieurs outils (Ettercap, ChaosReader, tcptrace...) -> Finalement, nous utilisons uniquement Scapy Pour stocker les résultats, la manipulation des JSON étant laborieuse, nous avons choisi d'utiliser une base de donnée PostGreSQL Nous avons trouvé un outil très puissant de visualisation : D3.js -> Nous avons donc créer une interface web (Flask, SQLAlchemy) connectée à PostgreSQL

Schéma fonctionnel :

# Retour sur les objectifs fixés

Nous avons remplis les objectifs suivants :

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

# Plan

1 Sujet - Objectifs - Choix

2 Démonstration

3 Travail à venir

4 Conclusion

# 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
Il suffit de disposer d'un fichier .pcap à analyser

CentraleSupélec

# Question, remarques ?

# Plan


1. Sujet - Objectifs - Choix
2. Démonstration
3. Travail à venir
4. Conclusion

Nous devons encore remplir ces objectifs

- 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


1. Sujet - Objectifs - Choix
2. Démonstration
3. Travail à venir
4. Conclusion

Merci de votre attention !