Projet Visualisation de traces réseau

* **But**: Appliquer notre logiciel offline sur une trace (.pcap) pour créer une visualisation permettant de trouver des informations utiles à la découverte de vulnérabilité

1. **3 phases**:
   1. Dissection du réseau pour obtenir des métadonnées -> pcap puis XML
   2. Analyse de ces données pour trouver des infos
   3. Visualisation des données intelligentes
2. **Questions**
3. Quelles informations peut-on déterminer de cette manière ? -> Spectre large
   * Données sensibles : en clair, chiffrement faible, password hashes
   * Informations sur les protocoles utilisés (insecure one ?)
   * Mauvaise utilisation du réseau/des protocoles
   * Defaut de configuration
   * Architecture du réseau
4. Comment générer une trace réseau de test ? Quel protocole analyser ?
   * Trace toute faite dispo sur internet / Génération perso
   * IP, ICMP, Protocoles cryptées (analyse de la taille)
5. Quel format pour la trace réseau ?
   * XML généré à partir d’un .pcap.
6. Quelles technologie pour analyser des paquets ?
   * Techno Python pour manipuler des XML
7. Comment analyser ces traces ?
   * Reconstruire les flux à partir des fragments (Scalpel, tcpxtract, tcpflow, Scapy)
   * Extraire informations de ces flux (ettercap, NSM Console)
   * Préparer la visualisation (ggobi rumint)
8. Etat de l’art : Quelles logiciels, à quoi servent-ils, y-a-t-il un outil orienté pentest ?
9. Comment visualiser l’analyse ?
   * Analyse par services et par port : Représentation paralléle
   * Analyse spatio-temporelle : Ip source/Dest : carte
   * Caractérisation volumétrique
   * Paquets chiffrés : Diagramme de chaleur
10. Quelle technologie pour l’IHM ?
    * **PyQT4** (ou PySide, Camelot, Boa (wxPython), PyGTK)

1er séance : Définition du problème, Recherche bibliographique

2e séance : Lecture d’articles, recherche bibliographique, redéfinition du problème

Soutenance : Présentation générale, spécification (paliers techniques), état de l’art -> Solutions choisies

Taff :

1. créer un repository public pour le soft -> Nico
2. Etat de l’art : Visu, reconsitution des packets, analyse des paquets

Solutions retenues

1. Bibliographie : Lister les documents supports de nos travaux
2. Etablir précisément ce qu’on va chercher

Etablir des paliers technique par rapport aux espérance

1. Faire les slides -> mercredi