Groupe-Projet P4

Enseignant : M.MAY

Projet n°4 : Système d'observation de réseau Ethernet **Dossier d'initialisation**

Groupe Projet :

ZHANG Zuhoran N'GASSA Nérice SCHMITT Alexandre QUESNEY Dany

_____

Année 2014-2015

1- Périmètre de sécurité :

Définir les aspects sécuritaires de votre dispositif. Soyez précis. Il est inutile de citer des choses génériques.
Autrement dit, sur le plan sécuritaire, contre quoi votre dispositif va aider l'utilisateur à combattre ?
A titre d'information, sur le plan scientifique, chaque point cité est appelé "verrou technique/scientifique".

I – Vision global

Type de protection :

- Ordinateur câblé réseau/ Relié sans fil ?
  - Connexion physique d'appareils ?
  - Bon nombre de machines sur le réseau/sous-réseau ?
  - Adresses MAC correcte ?
- Type de transmission des données ?
  - En clair
  - Crypté

II – Précisions :

1. **Détection de connexion.**
   Le but de ce dispositif est de vérifier les machines présentes sur le réseau, quel que soit le mode de connexion (Ethernet ou wifi).

2. **Disposer d'un tableau de bord du système.**
   Le système doit disposer d'une interface graphique performante permettant des répartir sous la forme de différentes salles, les machines du/des réseaux. Il sera possible de visualiser si des trames « non conventionnelles » sont émises (débit trop important, machine non autorisée, scan de ports, informations sensible en claire …)

3. **Attribution du bon réseau/ sous-réseau.**
   Lors de la connexion à un réseau, il se peut que l'ordinateur soit mal placé dans la configuration du réseau, surtout si celui-ci possède plusieurs sous-réseaux. Le but sera donc de signaler le problème.

4. **Prévention des attaques réseau.**
   Afin d'éviter que le réseau devienne inutilisable, un module de prévention d'attaques pourra être mis en place. Dans un premier temps, le but sera de signaler la présence d'un flux massif de requêtes anormal. Puis, il pourra être envisagé de mettre en place un moyen de bloquer/filtrer ces attaques.

Groupe-Projet P4

Enseignant : M.MAY

Projet n°4 : Système d'observation de réseau Ethernet **Dossier d'initialisation**

Groupe Projet :

ZHANG Zuhoran N'GASSA Nérice SCHMITT Alexandre QUESNEY Dany

_____

Année 2014-2015

2- Approche proposée

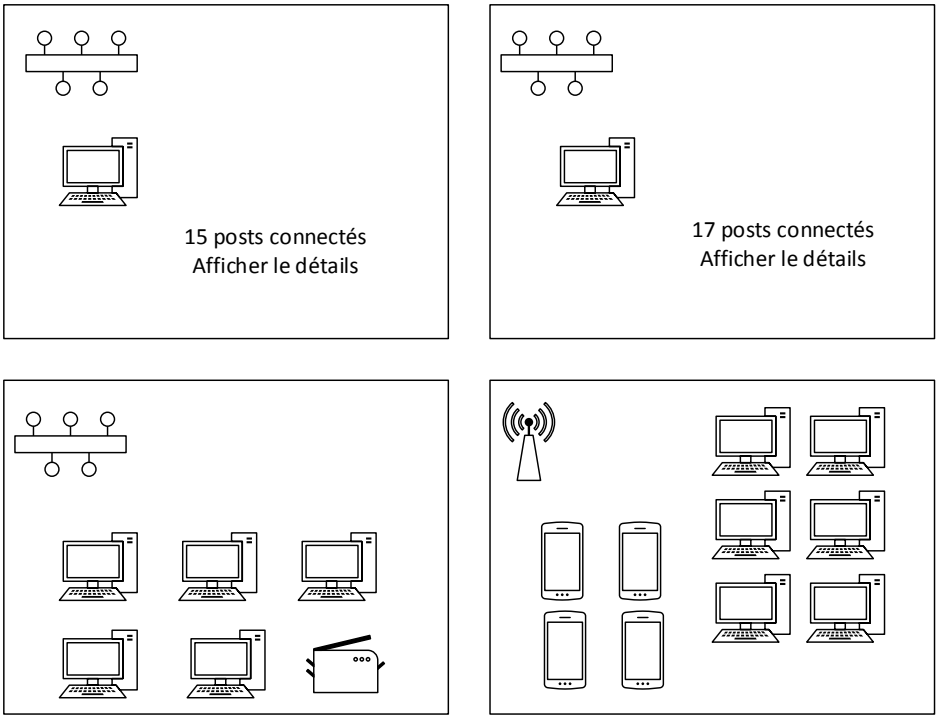
Comment allez-vous faire pour relever les verrous techniques identifiés dans le point précédent.
Pour vous, qui aimerez relever le défi :) vous pouvez présenter votre approche sous deux angles :
- scientifique : originalité, idée expérimentale, ou pof (proof of concept) de votre approche
- économique : impact de votre approche sur l'existant, ce qui peut apporter comme valeur ajoutée…
(pas obligatoire si vous ne voulez pas trop réfléchir sur ces deux points, présentez à votre manière votre approche)

Il apparait que le travail à réaliser semble être conséquent, l'idée de vouloir tout réaliser d'un coup semble donc ne pas être une bonne chose.

Nous essayerons dans un premier temps de penser à une interface la plus simple possible tout en essayant d'y afficher un maximum d'informations.

Notre logiciel ne pourra trouver sa place qu'au sein de réseau important et donc s'adressera majoritairement à des professionnels du réseau (administrateur, DSI, …) C'est donc dans cette optique que l'interface ce doit d'être relativement exhaustive dans les informations affichées.

Une seconde étape sera de déterminer quelles sont les machines connectées sur le réseau et de les représenter sous la forme de différentes pièces dans le bâtiment.



Une troisième étape sera la détection et l'analyse de trames suspectes, afin de déterminer les éventuel attaque ou anticiper des problèmes de sécurité sur le réseau ou sur des machines du réseau.

Après avoir parcourus une partie du net nous nous sommes rendu compte qu'il n'y pas vraiment de produit réalisant ce genre de chose. Beaucoup de logiciel supervision réseau sont assez complexe et ne permettent pas d'identifier rapidement un problème sur un réseau important.

3- Environnement technique

Même si vous n'allez pas développer votre dispositif de A-Z, j'aimerais quand-même voir comment vous allez implémenter votre approche. Définir l'architecture technique, plateforme/OS sur lesquels vous allez travailler, les langages de développement, etc.

Logiciel :

- Langage : JAVA.
- OS : Linux, pour le début. Windows si possible.

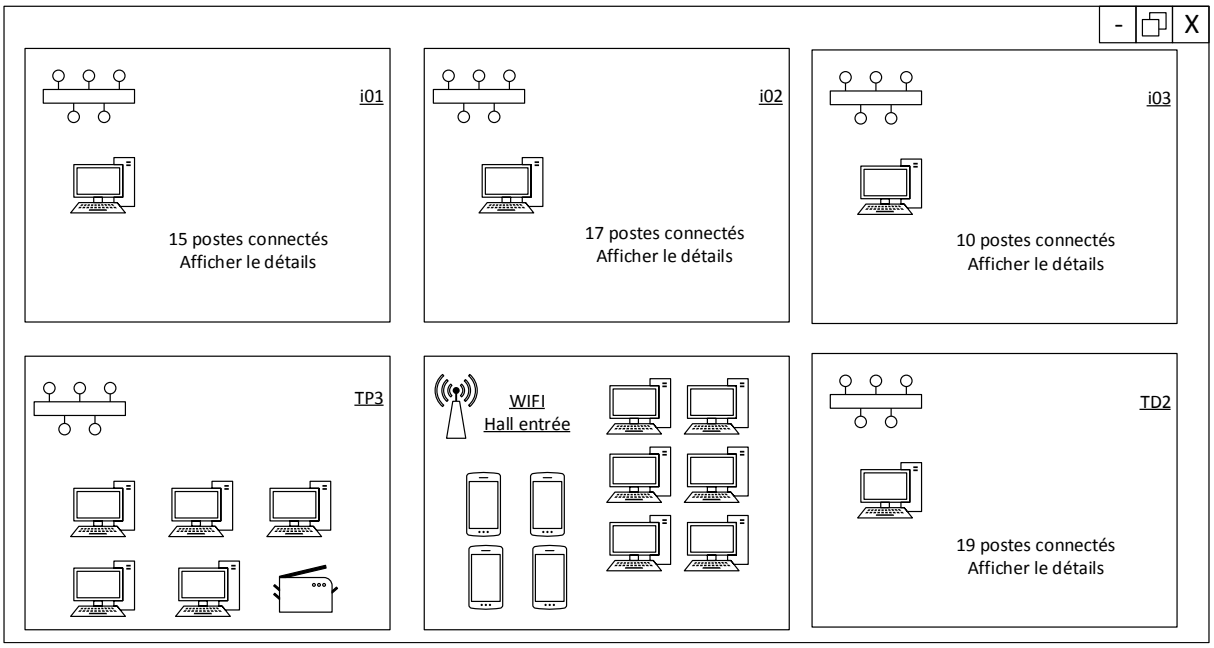
Le JAVA semble être plutôt bien adaptée pour la gestion du réseau. De plus nous commençons l'apprentissage du JAVA et nous aimerions tous progresser dans la maitrise de ce langage.

De plus un logiciel Open source Nmap dédié à l'analyse réseau sur linux existe et semble être extrêmement performant, cependant il n'existe pas d'interface graphique performante pour ce logiciel. Nous aimerions pouvoir l'utiliser en tache de fond afin de gagner du temps et ne pas avoir à réinventer quelque chose qui existe déjà. C'est donc pour cela que nous nous dirigeons plus sur une solution fonctionnel sur Linux.

Nous ne pensons pas restreindre énormément notre public en passant par Linux plutôt que Windows car la plupart des administrateurs réseau utilise Linux pour l'administration réseau.

4-Cas concret d'une utilisation du logiciel

Utilisation au sein de l'ENSIM.



Grâce aux sous réseau il est possible de pouvoir déterminer quels machine est dans qu'elle salle. Avec cette possibilité, nous pourrions donc présenter toutes les machines de l'école et voir si tout se passe correctement. Dans le cas où il y aurait trop de machines à afficher, l'utilisateur pourrait cliquer sur la salle de son choix et en afficher plus d'informations. Exemple de la salle i01.

Il est possible qu'en cas de détection de problème sur le réseau, le post ou la salle s'affiche en rouge ou orange et en cliquant dessus l'utilisateur aurait un diagnostic du problème pour pouvoir le résoudre.