TP1 : Cartographie des services

Objectif

Cartographier une infrastructure.

Contexte

Vous arrivez dans une nouvelle société au sein d'un incubateur d'entreprise.
Vous découvrez qu'une infrastructure avait déjà été mise en place pour le compte d'une société précédente, qui a fermé mais qui a tout laissé en place.Vous ne savez rien de ce qui peut tourner sur le réseau et sur les machines. Vous ne disposez d'aucun accès administrateur, en dehors d'une machine reliée à différents réseaux.

Dispositif

Un machine"obs" est connectée sur l'infrastructure à cartographier.
Elle servira de point d'observation : elle dispose de plusieurs interfaces réseau en mode "promiscuous" (nommées vport). Il est possible d'y capturer le trafic de différents réseaux.
De plus, elle possède une interface (eth1) qui porte une adresse IP dans un des réseaux internes. Depuis cette interface, vous pouvez faire des pings, des scan etc.
Enfin, elle dispose d'une interface de gestion (eth0, 192.168.57.98) qui permet d'accéder à la machine en ssh depuis l'hôte.

Méthode

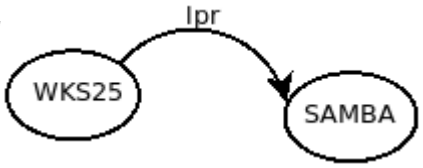
Vous aller devoir cartographier les différentes éléments d'infrastructures présents : sous-réseaux, adressage, postes de travail, serveurs, services.

Pour effectuer cette cartographie, utiliser les outils utiles évoqués en cours : ping, nmap, traceroute, nc, tcpdump etc.
Commencer par vous connecter en SSH sur la machine OBS :

```
ssh tprli@192.168.57.98
```

Faire un schéma du réseau et des machines, établir une matrice de flux (source/destination/service) et produire un graphe des dépendance entre chacune des machines (les arêtes du graphes indiquant le service).

Exemple : la machine "WKS25" dépend du serveur "SAMBA1" car elle utilise le service d'impression.



Rendu de TP

- schéma du réseau
- matrice de flux
- graphe de dépendance