Projet Privacité et Sécurité des Données

Table of Contents

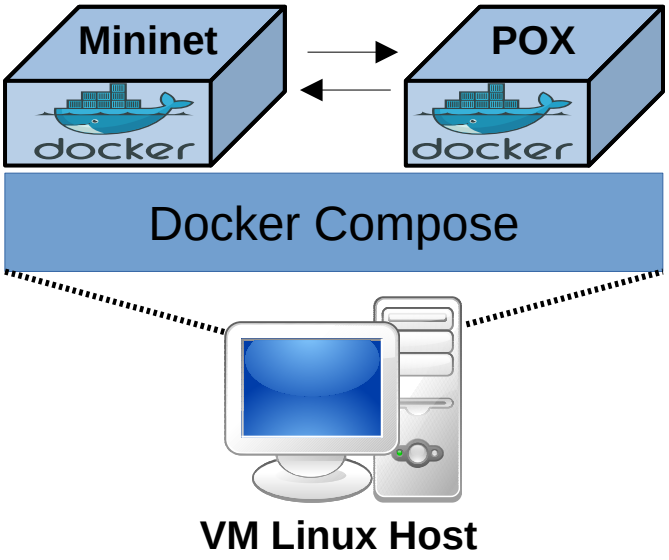
Motivation

Ce projet a pour objectif de rassembler et mettre en œuvre les connaissances acquises en cours de Privacité et Sécurité des Données. Le projet comporte trois parties principales :

1. La mise en œuvre d'un environnement virtualisé en utilisant des conteneurs Docker. La gestion et le déploiement de l'environnement sont assurés à l'aide du framework Docker Compose.
2. La simulation et la gestion d'un réseau en utilisant *mininet* et le controller SDN POX. Deux scénarios d'attaque sont définis dans ce projet et les étudiants pourront proposer d'autres scénarios :
   a) Attaque d'empoisonnement des tables ARP (ARP spoofing)
   b) Attaque par denis de service (DoS)

Description du projet

Voici une image montrant l'environnement virtualisé qui doit être déployé durant ce projet :



La figure 1 montre la mise en œuvre d'un environnement virtualisé. L'environnement est décrit comme suit :

1. **Docker Container Mininet**: ce conteneur sert à simuler la topologie du réseau qui doit être mis en place. Le réseau est simulé via *mininet* en utilisant son API Python afin de faciliter la gestion des différents scénarios. La topologie demandée par défaut est illustrée dans la figure suivante.

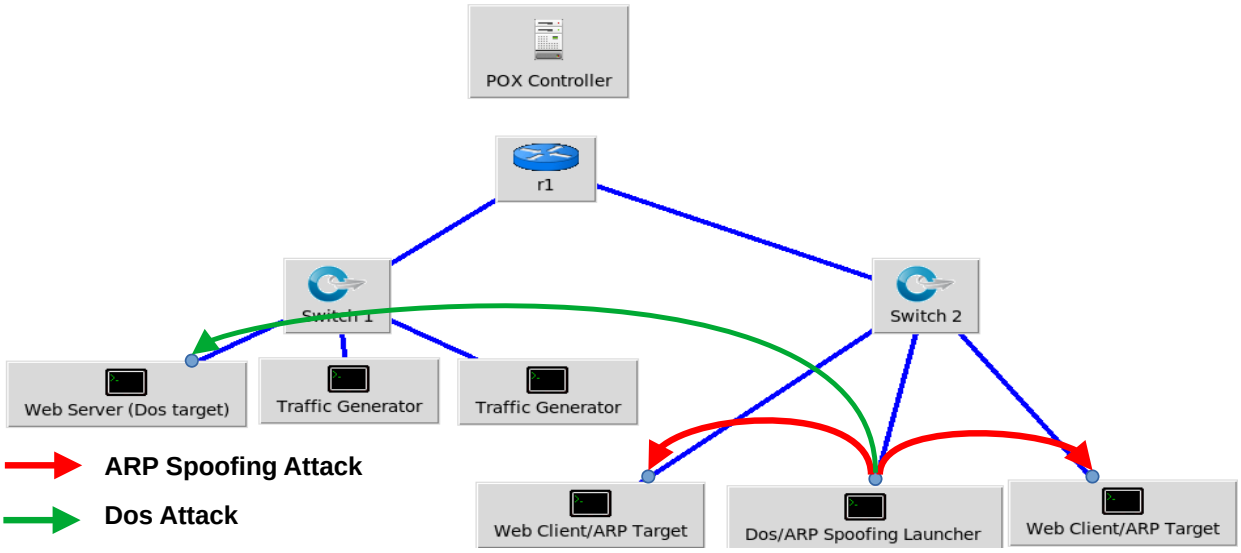


Illustration 1: Topologie du réseau simulé

Ce réseau comporte deux sous-réseaux interconnectés à l'aide d'un routeur afin de séparer les deux sous-réseaux.

1. Le premier sous réseau comporte un serveur web qui représente la cible de l'attaque (D)DoS, et deux générateurs de trafic réseaux (e.g. Flux TCP). Les trois entités sont connectées à un switch openflow.
2. Le deuxième sous-réseau comporte deux clients HTTP et le lanceur de l'attaque (D)DoS et ARP Spoofing, les trois connectés à un switch openflow.

La topologie est connecté à un contrôleur SDN POX distant (il s'exécute sur le container Docker POX).

2. **Docker Container POX :** ce conteneur exécute le contrôleur SDN POX qui gère les switchs OpenFlow du conteneur **Mininet**. La détection de l'attaque se fait au niveau du contrôleur en capturant et analysant le trafic et en appliquant apr exemple des techniques de Machine Learning (e.g. KNN, SVM, Decision Trees, etc.). Le blocage de l'attaque et la configuration des switchs OpenFlow se fait exclusivement via le contrôleur SDN.
   Le contrôleur pourrait également alimenter les deux conteneurs Docker pour l'analyse du trafic.

NOTE

tout le travail demandé doit être complètement automatisé en utilisant des scripts Shell et/ou Python (i.e. via les APIs Python).

À rendre

1. Un rapport détaillant la mise en œuvre de l'environnement, des attaques, et les solutions de détection et de blocage des attaques (10 pages max, 12pt taille de caractères).
2. Une présentation résumant le travail (5 slides max) ainsi qu'une démo montrant les scénarios, avant et après la mise en œuvre des algorithmes de détection.
3. Les codes sources des scripts d'automatisation, mininet, et POX.