

Présentation Mini-Projet



Sujet N°1 : IDS + SDN dans ODL

Introduction



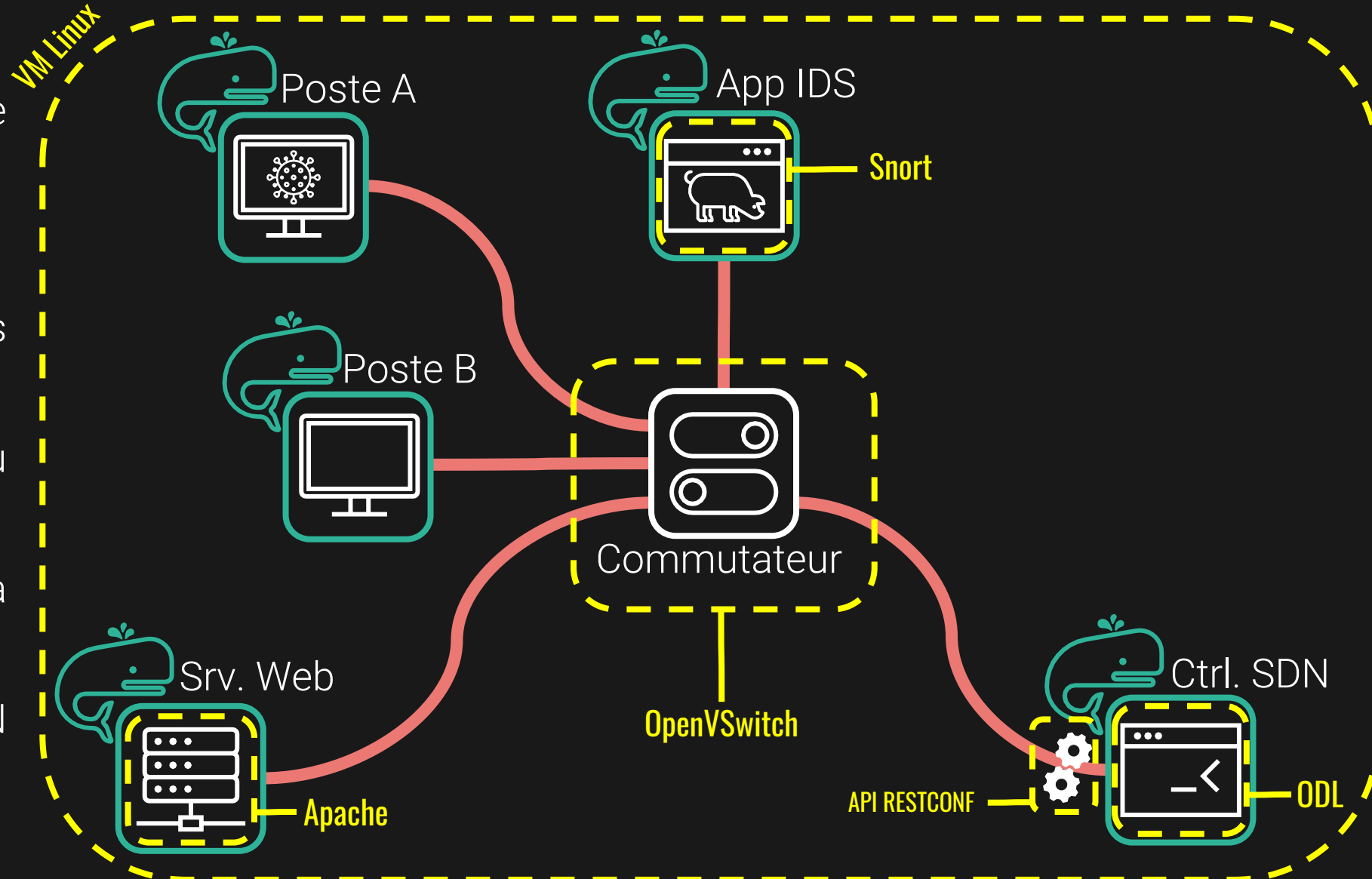
Rappel du sujet :

Injecter une attaque qui se fait détecter par un IDS. Ce dernier instruit le contrôleur afin de mettre à jour les tables de flux des commutateurs du réseau afin de bloquer l'attaquant.

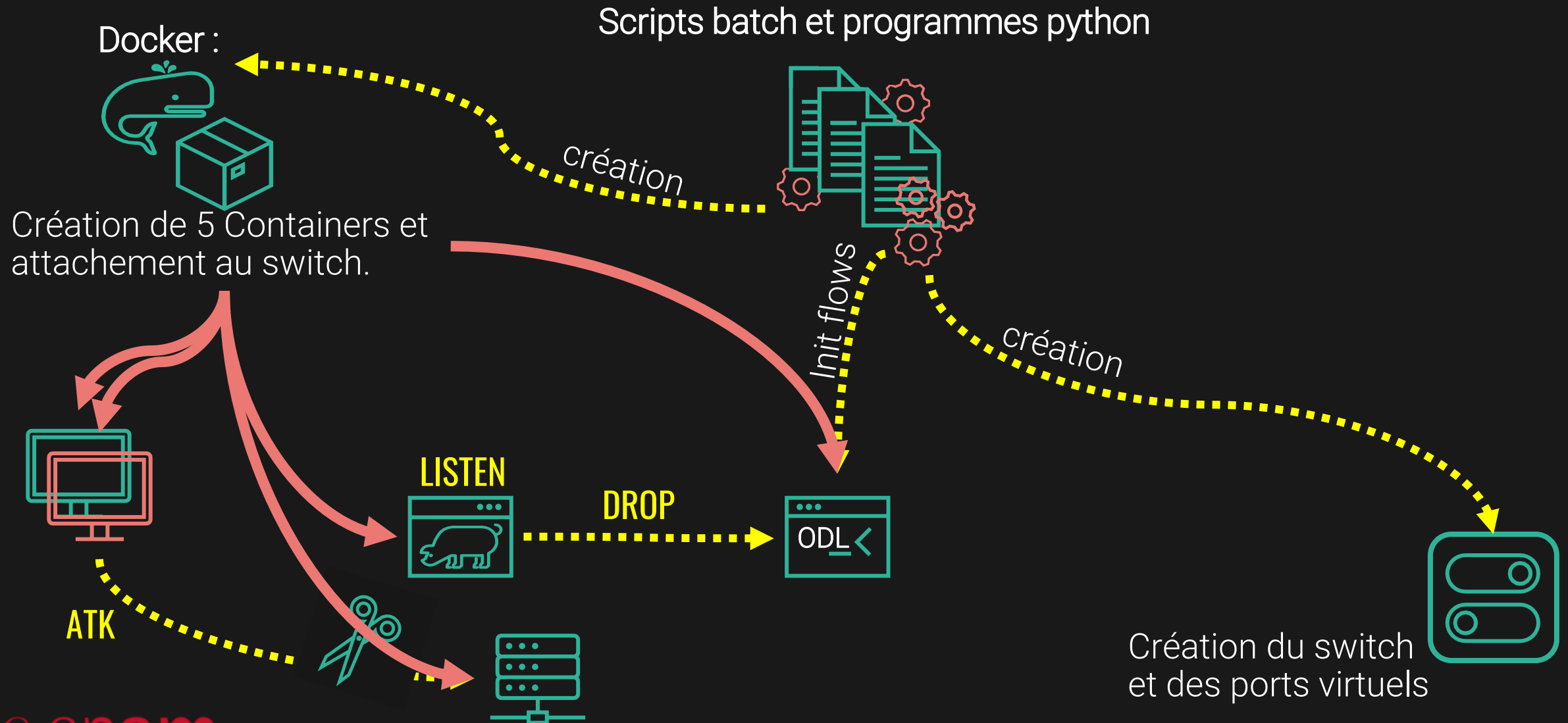
Présentation de l'environnement

Choix techniques :

- VM Linux hébergeant le projet
- Serveur Apache
- Applicatifs dans des containers Docker
- Commutation réseau via OpenVSwitch
- Ctrl. SDN pilote la topologie via Openflow
- Snort pilote le Ctrl. SDN via l'API RESTCONF



Réalisation du proof of concept



Difficultés

Tableau des difficultés :

Chantiers	Tâche	Indice de difficulté	
ODL	Configuration initiale du switch à travers le GUI ODL	4/5	<input checked="" type="checkbox"/>
	Mettre à jour une table de flow via API RESTCONF	4/5	<input checked="" type="checkbox"/>
Snort	Déclenchement d'une commande/script permettant de couper le flow via le contrôleur	3/5	<input checked="" type="checkbox"/>
	Implémentation des règles lors de la détection d'évènement	2/5	<input checked="" type="checkbox"/>
Docker / Openvswitch	Interconnecter les containers au sein d'un réseau OpenVSwitch	3/5	<input checked="" type="checkbox"/>
	Utilisation de Dockerfiles	1/5	<input checked="" type="checkbox"/>



Vidéo de présentation



Lien de la vidéo :

<https://www.youtube.com/watch?v=B52Z-F6vLvA>