UVS	Sécurité des Systèmes Informatiques	2021-2022
L2	Par M. NDIAYE	Projet

Projet : IDS/IPS

Objectif :

Les IDS/IPS sont des mécanismes destinés à surveiller un réseau ou un hôte (machine) afin de détecter et d'empêcher d'éventuelles attaques. Ils peuvent se présenter sous forme :

- matérielle

- module (carte) pouvant être installé dans un : switch, routeur, firewall

- logiciel

Snort est un système de détection et de prévention (IDS/IPS) open source développée par sourcefire. Il est l'une des technologies IDS/IPS les plus largement utilisées dans le monde.

L'objectif du projet est d'installer et de configurer un IDS/IPS et de voir sa réaction en cas de violation d'une règle définie.

NB : ce projet comporte trois (03) activités et doit être rendu **au plus tard le 8 janvier 2023**

Prérequis : disposer d'un logiciel de virtualisation VMWare ou VirtualBox, des machines virtuelles (Ubuntu et Kali linux) et d'un logiciel de simulation réseau (Gns3 ou Packet Tracer)

Activité 1 : Installation et configuration de Snort dans Linux

1- Installer les machines virtuelles Ubuntu et Kali

2- Installer et configurer Snort dans la machine virtuelle Ubuntu

3- Lancer Snort

4- Montrer les réactions de Snort en cas d'intrusions (utiliser Kali pour les tests d'intrusions)

Activité 2 : Installation et configuration de Snort dans un Firewall (pfsense)

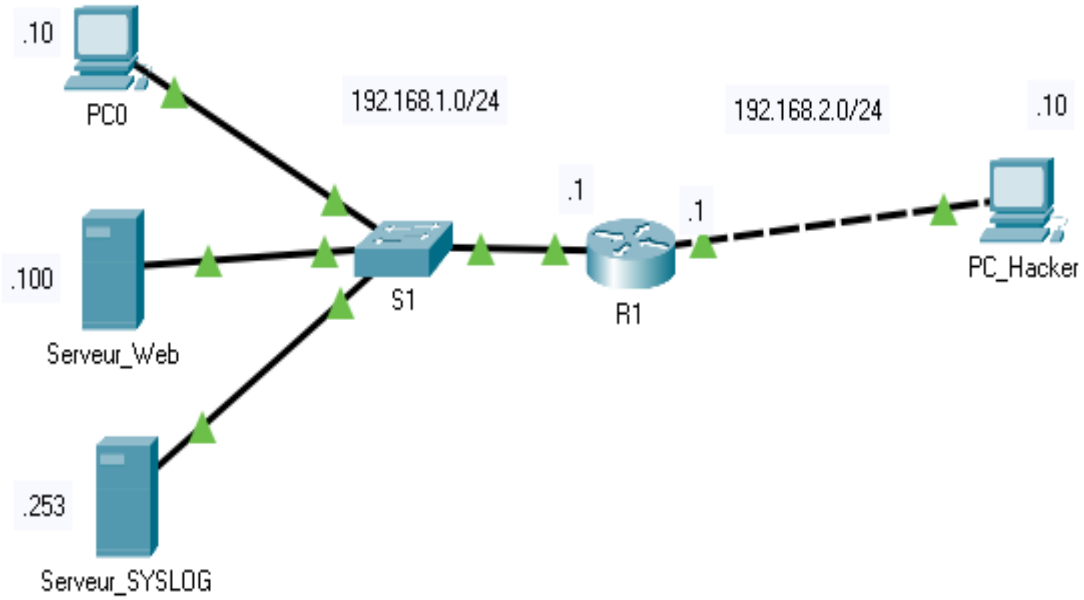
1- Installer Pfsense dans VMware ou Virtual box

2- Y installer et configurer Snort

3- Montrer les comportements de Snort en cas de violations (intrusions).

<u>Activité 3</u> : Configuration IDS/IPS dans un routeur (Cisco)

1- Reproduire le schéma ci-après :



2- Configurer IDS/IPS dans le routeur

3- Faire des tests d'intrusions au niveau du Serveur Web et visualiser les alertes au niveau du serveur Syslog