Université Mohammed V- Agdal
Faculté des Sciences
Département de Mathématiques
et Informatique. Rabat

TP n° 5
Mise en place d'un IDS Snort

Objectifs :

L'objectif de ce TP est de mettre en place un système de détection d'intrusion en se basant sur le logiciel libre Snort. C'est un système de détection d'intrusion libre qui est capable d'effectuer en temps réel des analyses de trafic et de logger les paquets sur un réseau IP. Il peut effectuer des analyses de protocoles, recherche/correspondance de contenu et peut être utilisé pour détecter une grande variété d'attaques.

Dans le cadre de ce TP, nous nous intéressons essentiellement aux aspects suivants :

- Comprendre et assimiler le rôle d'un système de détection d'intrusion dans la sécurité des réseaux ;
- Installer du logiciel Snort et les logiciels requis;
- Effectuer les configurations nécessaires au bon fonctionnement de Snort ;
- Effectuer des tests avec Snort dans ses différents modes.
    - Utilisation de SNORT comme un simple sniffer :
    - Utilisation comme outil d'enregistrement de trafic réseau
    - Utilisation de SNORT comme un IDS
- Apprendre à écrire de nouvelles règles personnalisées.