Atelier 4: Dispositifs de sécurité

Objectif :

Partie 1 : les étudiants seront amenés à configurer un pare-feu « **Netfilter/iptable** » pour un réseau d'entreprise avec des exigences de sécurité strictes.
Partie 2 : Les étudiants seront initiés à la configuration de « **Snort** » en tant que système de détection d'intrusion (IDS) pour surveiller et détecter les attaques sur un réseau.

Partie 1 : Pare-feu iptables

Exercice 1 :

1. Bloquez tout le trafic entrant par défaut.
2. Autorisez uniquement le trafic HTTP (port 80) entrant.
3. Vérifier les règles iptables

Exercice 2 :

1. Bloquez tout le trafic entrant et sortant par défaut.
2. Autorisez uniquement le trafic suivant :
    - SSH (port 22) depuis l'adresse IP interne du réseau local.
    - HTTP (port 80) et HTTPS (port 443) pour tout le trafic sortant.
    - DNS (port 53) pour les requêtes sortantes uniquement vers les serveurs DNS autorisés.
    - ICMP (ping) pour permettre la connectivité de base.
3. Configurez une règle de journalisation pour enregistrer les paquets rejetés ou acceptés.
4. Testez la configuration en essayant d'accéder à différents services depuis le réseau local et en vérifiant les journaux pour les activités autorisées et rejetées.

Partie 2 : Configuration de Snort en mode IDS

1. Configurez Snort pour utiliser une base de données de règles (règles de la communauté) pour détecter les attaques courantes.
2. Démarrez Snort en mode écoute pour capturer et analyser le trafic réseau en temps réel.
3. Simulez des attaques ciblant le réseau surveillé (par exemple, des scans de ports, ARP poinsing, Ping of Death, etc.).