Bloc 3
Cybersécurité des services informatiques

Surveillance du réseau

IDS – IPS - SNORT

Objectifs administratifs

- Tester le **niveau d'ouverture** d'un réseau
- Evaluer quantitativement la **sécurité** du réseau
- Disposer d'un outil permettant la **surveillance du réseau**
- Disposer d'un outil de **suivi d'activité**

Objectifs techniques

- Installer et configurer un logiciel de **découverte réseau**
- Installer et configurer un **service de surveillance** du réseau
- Installer, configurer et exploiter un **logiciel d'analyse de logs**

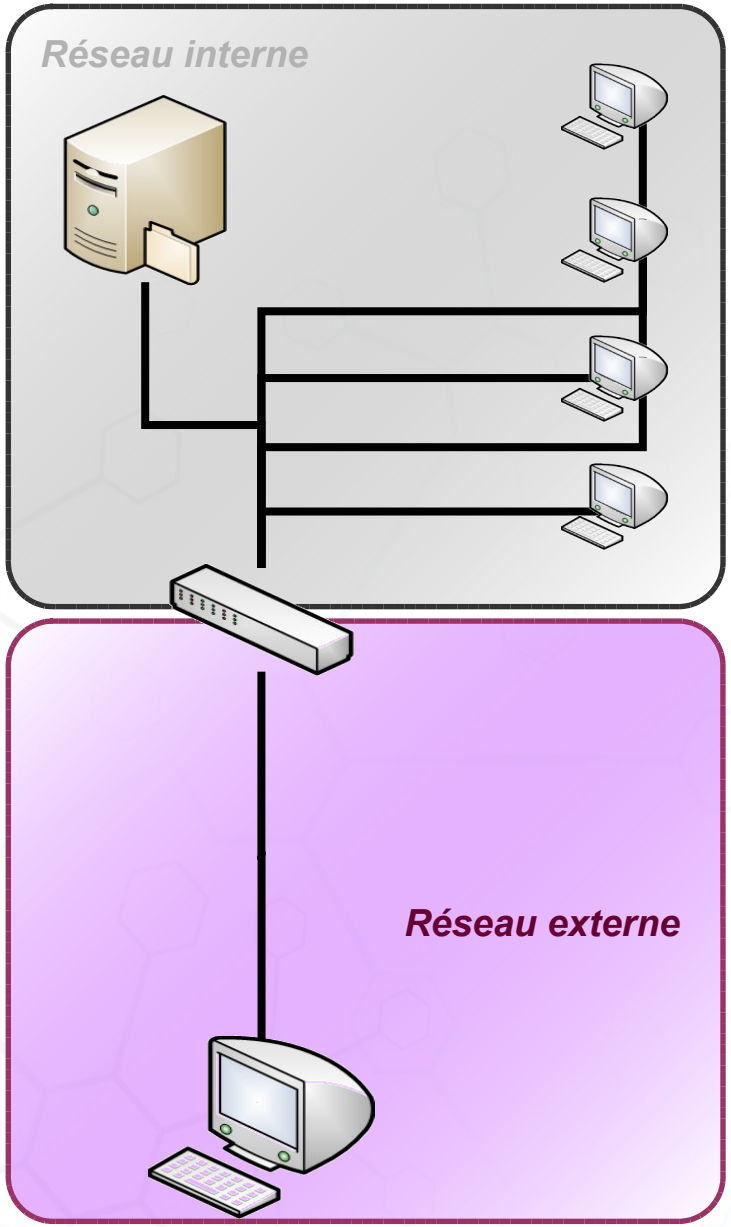
- **NIDS / NIPS**
- **Avantages**
  - Open source
  - Peu consommateur en ressources
  - Pas d'interface graphique
  - Mise à jour fréquente de la base de signatures
  - Langage de description des règles
- **Fonctionnalités**
  - Analyse protocolaire
  - Pattern matching
- **Fonctionnement selon 3 modes :**
  - Sniffer
  - Logger
  - Détection / Prévention d'intrusions

Matériel nécessaire

- ***Matériel :***
  - 1 Serveur
- ***Logiciels/services :***
  - Linux (Debian conseillé)
  - SNORT

- ***Matériel :***
  - Un réseau en état de fonctionnement

- ***Matériel :***
  - Un machine client
- ***Logiciels :***
  - Linux ou Windows
  - Outil de découverte réseau (nmap, netwag, kali, metasploit...)



Matériel / Logiciels nécessaires

Étape 1
- Désactiver le parefeu

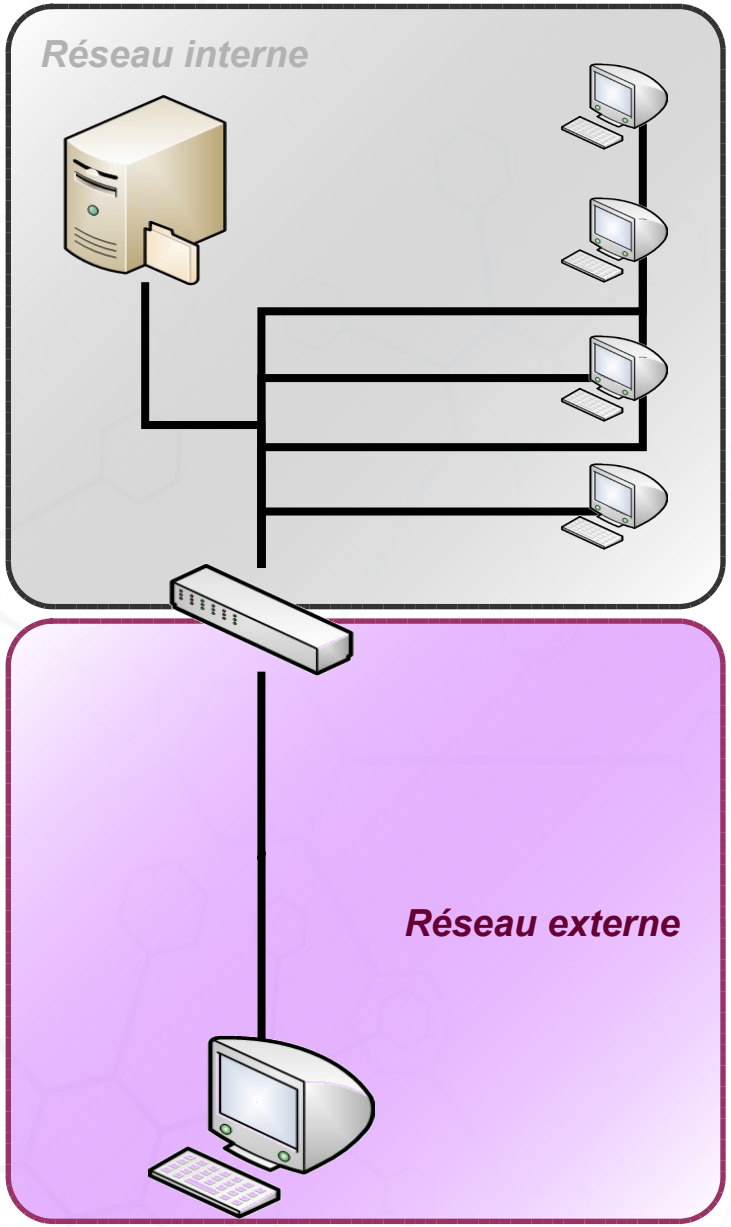
Étape 2
- Installer / configurer snort / démarrer le service

Étape 5
- Confronter les résultats des logs snort avec les attaques du test de vulnérabilité

Étape 3
- Configurer le port du switch en mode promiscuité

Étape 6 (Facultatif mais intéressant)
- Trouver un moyen d'alerter l'administrateur via email en cas d'intrusion
- Trouver un moyen de couper la connexion de l'attaquant via un parefeu ou une ACL (voir www.snortsam.net par exemple)

Étape 4
- Utiliser un outil de test de vulnérabilité pour générer des alertes snort



Étape 1
- Rendre le serveur SNORT visible sur le réseau du lycée

Étape 2
- Attaquer le serveur de votre binôme

Étape 3
- Confronter les résultats des logs snort avec les attaques pratiquées par votre binôme

Important
- Ne pratiquez que des attaques dirigées vers votre binôme (sinon risque de saturation du réseau)