Architecture technique – Projet NetShield

1. Présentation générale

Le projet NetShield repose sur une infrastructure locale virtualisée composée de trois machines virtuelles (VM) interconnectées au sein d’un réseau privé. Il simule un environnement réaliste d’attaque DDoS et met en œuvre une chaîne complète de détection, visualisation et réponse automatique.

1. Infrastructure réseau

Une image contenant texte, capture d’écran, diagramme, conception

Le contenu généré par l’IA peut être incorrect.

1. Composants logiciels

Sur la VM vm-monitor :

* Suricata : IDS (Intrusion Detection System) en écoute sur l’interface réseau
* Python script (auto\_block.py) : Analyse le log eve.json en temps réel et bloque les IP via iptables
* Streamlit (dashboard.py) : Affiche en direct les alertes et les IP bloquées
* Environnement virtuel (venv) : Isole les dépendances Python pour le dashboard

Sur la VM vm-kali :

* Docker & hping3 : Génère les paquets DDoS via plusieurs conteneurs simulant une attaque distribuée

1. Fonctionnement global
2. Lancement d’une attaque DDoS via start\_attack.sh (Docker + hping3)
3. Détection des paquets suspects par Suricata (règles locales personnalisées
4. Écriture dans eve.json (log JSON de Suricata)
5. Script Python lisant en continu le log → bloque les IP malveillantes
6. Dashboard Streamlit affiche :
   * Les alertes en temps réel
   * Les IP bloquées automatiquement