Sécurisation du réseau et défense contre les attaques DDoS à l'aide de pare-feu sous Linux

Objectif du projet : Configurer un pare-feu sous Linux pour limiter les connexions entrantes et sécuriser le réseau.

Livraison attendue :

- Une présentation détaillée du projet en format poster scientifique
- Le code source du projet hébergé sur GitHub.

Partie 0 : Comparatif des solutions de pare-feu

1. Recherche : Explorez 2 à 4 solutions de pare-feu disponibles pour Linux. Incluez nécessairement iptables dans votre comparaison.
2. Analyse : Pour chaque solution, listez ses principales caractéristiques, ainsi que les similitudes et différences.
3. Rendu : Présentez un comparatif structuré, mettant en évidence les avantages et inconvénients de chaque solution.

Partie 1 : Configuration du pare-feu

1. Installation : Installez et configurez un pare-feu sur un système Linux (sur une VM VirtualBox, WSL, ou une VM cloud).
2. Règles à appliquer :
    - Autorisez uniquement les connexions entrantes sur les ports SSH (22), HTTP (80) et HTTPS (443).
    - Bloquez tous les autres ports.
    - Autorisez uniquement les connexions sortantes vers l'adresse IP 51.12.247.156, pour empêcher l'exfiltration de données vers d'autres systèmes.
3. Tests de validation :
    - Installez un serveur SSH et un serveur web (Nginx, Flask, ou autre) sur votre machine.
    - Ajoutez un service écoutant sur un autre port, pour tester le blocage par le pare-feu.
    - Vérifiez que les services SSH et web sont accessibles, et que le service sur l'autre port est bloqué par le pare-feu.
    - Assurez-vous qu'il est impossible d'effectuer des requêtes réseau (HTTP ou autres) vers d'autres adresses que l'IP autorisée.

- Utilisez des outils comme nmap (ou autres) pour vos tests. Automatisez ces tests et l'installation des services avec des scripts (Python ou Bash).

Partie 2 : Gestion des attaques DDoS

1. Simulation d'attaque DDoS : Utilisez un outil de test de charge (comme ApacheBench ab, Vegeta, ou un autre) pour simuler une attaque DDoS sur votre serveur web.
2. Objectif : Configurez votre pare-feu pour rejeter (drop) automatiquement les requêtes si un nombre excessif de connexions entrantes provient de la même adresse IP.

Partie 3 : Amélioration de la défense

1. Analyse : Identifiez les limites de votre configuration actuelle de pare-feu face aux attaques DDoS.
2. Recherche de solutions : Proposez des stratégies plus sophistiquées pour améliorer la défense contre les attaques DDoS. Décrivez les options envisagées pour répondre aux limites identifiées.