Projet 1 - HomeLab Cybersecurity

📄 RAPPORT – Mise en place d'un Mini Réseau Sécurisé avec pfSense

Auteur : Rosdel KONDELO

Date : 22 Novembre *2025*

Projet : Segmentation réseau & paramétrage du firewall avec pfSense

Environnement : HomeLab VirtualBox

🟦 1. Introduction

L'objectif de ce projet est de mettre en place un environnement réseau isolé et sécurisé dans un HomeLab, utilisant pfSense comme firewall et routeur.

Ce réseau sert de base pour les tests de cybersécurité, l'analyse réseau, les IDS et l'apprentissage des bonnes pratiques de segmentation.

L'environnement est volontairement simple :

- **LAN sécurisé** : machine d'analyse (Kali)
- **DMZ** : machine vulnérable (Metasploitable2)
- **pfSense** : segmentation + filtrage + IDS

🟩 2. Architecture réseau

L'infrastructure repose sur **3 machines virtuelles** connectées via des réseaux internes VirtualBox :

Détails techniques :

Machine	Rôle	Interface	Adresse IP	Réseau VirtualBox
Kali Linux	Machine d'audit / analyste	LAN	192.168.1.10	Réseau Interne
pfSense	Firewall / IDS / Routeur	LAN + DMZ	192.168.1.1 / 192.168.2.1	Réseau Interne
Metasploitable2	Machine vulnérable	DMZ	192.168.2.10	Réseau Interne
PfSense	Accès Internet pour MAJ pfSense	WAN	10.0.2.15	NAT

La communication est **contrôlée et limitée** entre les segments.

🟧 3. Mise en place des réseaux VirtualBox

3.1 Création des réseaux internes

Deux réseaux Interne VirtualBox ont été créés :

- LANHOME : utilisé par Kali et pfSense (interface LAN)
- DMZHOME : utilisé par Metasploitable2 et pfSense (interface DMZ)

3.2 Configuration des cartes réseau

- pfSense possède **deux interfaces** :
  - LAN → LANHOME
  - DMZ → DMZHOME
- Kali et Metasploitable2 possèdent **une seule interface** chacune, connectée à leur segment respectif.

🟥 4. Configuration de pfSense

Une fois pfSense installé :

4.1 Attribution des adresses IP

- **LAN** : 192.168.1.1 /24
- **DMZ** : 192.168.2.1 /24

4.2 DHCP

- DHCP activé uniquement sur le LAN pour Kali Linux
- DHCP désactivé sur la DMZ

🟦 5. Segmentation réseau : règles du firewall

Le firewall a été configuré selon des bonnes pratiques de segmentation.

5.1 Politique de sécurité appliquée

Flux	Autorisé ?	Raison
LAN → DMZ	✔️ Oui	Kali doit pouvoir attaquer / auditer Metasploitable2
DMZ → LAN	❌ Non	Empêche la compromission du LAN
LAN → Internet	✔️ Oui	Mise à jour Kali / téléchargement outils
DMZ → Internet	❌ Non	DMZ isolée
Internet → DMZ	❌ Non	DMZ non exposée
Internet → LAN	❌ Non	Réseau interne protégé

5.2 Exemples de règles dans pfSense

✳️ LAN → DMZ

Action : Pass
Source : LAN Subnet
Destination : DMZ Subnet
Port : any

⛔ DMZ → LAN

Action : Block
Source : DMZ Subnet
Destination : LAN Subnet
Port : any

⛔ DMZ → Internet

Action : Block
Source : DMZ Subnet
Destination : any
Port : any

Ces règles assurent une forte isolation de la DMZ.

🟩 6. Tests fonctionnels

Plusieurs tests ont été réalisés pour vérifier la segmentation.

6.1 Test ping

- Kali → Metasploitable2 = OK
- Metasploitable2 → Kali = BLOQUÉ

✔️ La segmentation fonctionne dans un seul sens.

6.2 Scan Nmap depuis Kali

`nmap -sV 192.168.2.10`

Les paquets passent correctement (autorisation LAN → DMZ).

6.3 Scan Nmap depuis Metasploitable2

→ BLOQUÉ par pfSense

→ comportement attendu

🟨 7. Activation d'un IDS

Snort a été installé via pfSense.

7.1 Objectif

- détecter les scans Nmap
- surveiller la DMZ
- générer des alertes dans l'interface pfSense

7.2 Résultats

Après un scan Nmap agressif :

`nmap -A 192.168.2.10`

pfSense affiche :

- Détection d'un SYN scan
- Alertes réseau (signature ET SCAN)
- Logs visibles dans "Alerts"

Cela montre que l'environnement est adapté au travail SOC.

🟪 8. Résultats observés

🔐 Sécurité du réseau

- La DMZ est complètement isolée du LAN
- Les flux entrants/sortants sont strictement contrôlés
- La surface d'attaque est réduite

🛡️ Détection d'intrusions

- Les scans Nmap sont correctement détectés
- Les journaux IDS permettent une analyse SOC basique

🧪 Fonctionnalités opérationnelles

- Kali peut auditer Metasploitable2 librement
- Le LAN reste protégé même si la DMZ est compromise

🟧 9. Conclusion

Ce projet met en place une architecture **réaliste**, similaire à celles utilisées dans des environnements professionnels.

Il démontre les compétences suivantes :

✔️ Installation et configuration d'un firewall pfSense

✔️ Mise en place d'une segmentation réseau LAN/DMZ

✔️ Écriture de règles de filtrage réseau

✔️ Tests pratiques (ping, Nmap, communication bloquée)

✔️ Configuration d'un IDS pour la détection de scans

✔️ Rédaction d'un rapport technique