Compte rendu : AP VPN

Nom : CHARTIER Carmine / Dumond Camille
Date de l'AP : Octobre 2024

Objectif de l'atelier :

L'objectif de cet AP était de **concevoir et sécuriser une infrastructure réseau virtuelle** complète en utilisant **pfSense** comme pare-feu et gestionnaire de trafic. Cette architecture inclut une **gestion de DMZ**, la mise en place d'un **serveur LAMP leurre (honeypot)**, un **VPN avec règles QoS**, et la **configuration d'un utilisateur distant**.

Machines virtuelles utilisées :

1. **pfSense (pare-feu + routeur)**
    - Interfaces configurées :
        - **WAN** : accès à Internet
        - **LAN** : réseau interne sécurisé
        - **DMZ Interne** : héberge un serveur de fichiers accessible uniquement via SSH
        - **DMZ Externe** : héberge un **serveur LAMP sans site web**, servant de honeypot
    - Services :
        - Firewall avec redirections de ports
        - Gestion VPN sortant avec limites et priorités
        - Règles QoS et traffic shaping
        - NAT, DNS Resolver, DHCP
2. **Ubuntu Server – Serveur LAMP (Honeypot)**
    - Installé dans la DMZ externe
    - Aucun site web actif, utilisé pour capturer/observer les connexions anormales

- Port 80 ouvert en façade publique, mais sans service réel

3. **Ubuntu Server – Serveur de fichiers**
    - Installé dans la DMZ interne
    - Accessible uniquement en SSH depuis le LAN
    - Port SSH contrôlé par règles pfSense
4. **Utilisateur distant (VPN)**
    - Accès via OpenVPN ou IPsec configuré dans pfSense
    - Droits restreints, accès au LAN uniquement pour supervision ou maintenance

---

Configuration réseau sur pfSense :

1. **Redirection de trafic vers le honeypot** :
    - Port 80 (HTTP) redirigé vers la DMZ externe
    - Surveillance des tentatives d'accès (préparation à une analyse réseau de type IDS)
2. **Traffic shaping / QoS sur le VPN sortant :**
    - **Limitation du débit global VPN à 2 Mbps**
    - **Priorité maximale pour :**
        - **ICMP** (surveillance réseau)
        - **SSH** (accès admin)
    - **Garantie de 1 Mbps pour le trafic HTTP**
    - Files de trafic configurées via la QoS de pfSense
3. **Utilisation du VPN :**
    - Création d'un accès distant avec utilisateur spécifique
    - Authentification par certificat ou mot de passe

- Accès restreint au LAN et logs activés pour suivi

4. **Sécurisation et cloisonnement des zones :**
    - DMZ interne isolée, accès SSH uniquement depuis LAN ou VPN
    - DMZ externe visible depuis l'extérieur uniquement pour le port HTTP
    - Aucun accès entre DMZ externe et interne

Compétences mobilisées :

- Architecture réseau complexe avec segmentation (LAN / DMZ / VPN)
- Sécurisation et filtrage via pare-feu (pfSense)
- Mise en œuvre de QoS (traffic shaping, priorisation)
- Déploiement d'un honeypot (simulation d'un serveur vulnérable)
- Administration d'utilisateurs distants et VPN
- Analyse de sécurité réseau (règles, logs, redirections)

Conclusion / Prochaines étapes :

Cette activité m'a permis de me familiariser avec des concepts avancés de **sécurité réseau et de virtualisation**, tout en mettant en œuvre un environnement simulant une situation réelle en entreprise. Le projet m'a aussi sensibilisé aux notions de **cloisonnement**, de **détection proactive** (honeypot), et de **gestion de bande passante critique**.

Ce projet sera intégré à mon **portfolio pour l'épreuve E5**, accompagné de la documentation complète et du schéma réseau.