Sécurité Informatique

Fascicule 5

Esprit 2024-2025

Pré-requis :

- Architecture mise en place (LAN,WAN,DMZ) .
- Le firewall Pfsense installé et configuré

Objectifs :

- Installer et configurer un IDS/IPS pour concrétiser les connaissances acquises dans le cours.
- Installer et configurer une solution VPN (client to site)
- Retester les attaques après la mise en place de l'architecture de sécurité et interpréter les résultats.

Partie 1 : Mettre en place une solution IDS / IPS [Snort]

1- Installer snort à partir des packages disponibles depuis Pfsense

2- Configurer une règle de sécurité qui permet de :
Détecter le flux icmp sortant de la zone LAN vers n'importe quelle zone et générer un message d'alerte « Année universitaire-Nom de la classe-numéro du groupe »*Exemple : 2425-4SAE6-G1*

3- Tester le fonctionnement et exporter le rapport d'alertes.

L'installation de Snort est recommandée à travers l'interface graphique de Pfsense.

Aller sur System > Package Manager> Available Packages et rechercer Snort

Les étapes de configuration détaillées de snort (règles et alertes) sont disponibles dans le tutorial suivant :https://youtu.be/SapAcfHbQSE

Partie 2 : Mettre en place une solution VPN [OpenVPN]

1. Installer et configurer **Openvpn** sur les deux machines LAN et WAN**.**

2. Tester l'authentification sécurisée des utilisateurs de la base locale **Openvpn**

a. Tester d'établissement du tunnel **VPN** entre les deux réseaux LAN et WAN.

b. Visualiser avec **Wireshark** le trafic échangé entre ces deux machines pour l'établissement du tunnel **VPN**.

Toutes les étapes d'installation et de configuration d'OpenVPN sont détaillées dans le document d'aide **« Tuto Pfsense-OpenVPN » à partir de la page 20**