****

**Prosit 3 : SECURITE**

# Contexte :

Sécuriser le réseau des menaces informatiques extérieures

# Mot clés :

ACL : « Access control list » Ensemble de règles qui définissent les opérations (lire, écrire, exécuter…) que pourra réaliser un utilisateur sur une ressource (un fichier, le plus souvent, mais aussi une adresse ou un port réseau).

Proxy : Un proxy est un serveur intermédiaire qui agit en tant qu'intermédiaire entre un utilisateur et un serveur de destination. Il peut être utilisé pour diverses raisons, notamment pour la sécurité, la gestion du cache, ou l'anonymat (en masquant l’ip).

Zone démilitarisée (DMZ) : DMZ: En informatique, une zone démilitarisée est un sous-réseau séparé du réseau local et isolé de celui-ci ainsi que d'Internet par un pare-feu.

Filtrage : Le filtrage fait référence au processus de surveillance et de gestion du trafic réseau en fonction de certaines règles prédéfinies. Cela peut inclure le filtrage du contenu web, le filtrage des e-mails indésirables, etc.

Bac à sable : Un bac à sable (sandbox en anglais) est un environnement sécurisé et isolé où les fichiers ou les applications peuvent être exécutés et analysés sans risque pour le système hôte. Il est souvent utilisé pour tester des logiciels potentiellement dangereux.

UTM : UTM signifie "Unified Threat Management". C'est une approche de la sécurité réseau qui combine plusieurs fonctions de sécurité, telles que le pare-feu, l'antivirus, le filtrage web, etc., dans un seul appareil ou système.

DMZ : Veuillez noter que "DMZ" a déjà été défini comme "Zone démilitarisée". Il s'agit d'une redondance dans votre liste.

IPS/IDS : IPS (Système de Prévention d'Intrusion) et IDS (Système de Détection d'Intrusion) sont des technologies de sécurité réseau. IDS détecte les activités suspectes, tandis que IPS tente de bloquer activement les intrusions ou les menaces.

NAT/PAT : NAT (Traduction d'Adresse Réseau) et PAT (Traduction d'Adresse Port) sont des techniques utilisées pour attribuer des adresses IP et des ports aux appareils sur un réseau privé, permettant ainsi la communication avec le réseau public, généralement via un seul adresse IP publique.

Firewall : Un pare-feu est un dispositif ou un logiciel qui contrôle le trafic réseau en fonction de règles de sécurité définies, en permettant ou en bloquant le trafic en fonction de ses caractéristiques.

SOC : SOC signifie "Centre de Sécurité Opérationnelle". Il s'agit d'une équipe ou d'un centre qui surveille en permanence la sécurité informatique, détecte les menaces et réagit en temps réel pour protéger les systèmes informatiques.

SIEM : SIEM signifie "Système de Gestion des Informations et des Événements de Sécurité". C'est une solution logicielle ou matérielle qui permet de collecter, d'analyser et de gérer les données de sécurité pour détecter les menaces.

PFsense : pfSense est un système d'exploitation open-source basé sur FreeBSD, principalement utilisé comme pare-feu et routeur pour les réseaux informatiques.

Malwares : Les malwares sont des logiciels malveillants, tels que les virus, les vers, les chevaux de Troie, les spywares, etc., conçus pour causer des dommages ou voler des informations sur un système informatique.

# Problématique :

**Comment sécuriser le réseau des menaces informatique extérieure**

# Contraintes :

Rien de trouver

# Généralisation :

Mettre en place un filtrage firewall

Sécuriser un réseau

# Livrables :

VMs configurées pour la sécurité

Schéma adapter à nos VMs

# Pistes de solution :

Utiliser une VM comme firewall (PFsense ?)

ACL pour filtrage ?

# Plan d’action :

Comprendre la théorie (faire le point vendredi)

Adapter le schéma aux VM

# Réalisation du plan d’action :

Pendant le workshop, nous avons configurer un firewall tournant sur PFsense qui est un os basé sur Unix et configuré sur une VM FreeBSD.

Grâce a lui nous pouvons créer des règles pfsense :

Une image contenant texte, nombre, Police, capture d’écran

Description générée automatiquement

Grace a ces règles nous allons créer un réseau virtuel, comme suis :

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

Description générée automatiquement

Grace au firewall on va pouvoir envoyer les choses potentiellement dangereuses, vers la DMZ « Zone démilitarisée » et plus précisément dans la SandBox. Tandis que les choses « safe », vont pouvoir être envoyer sur le LAN.