2023-2024

**Workshop Sécurité**

**Informatique**

Table des matières

I. Objectif ................................................................................................................................................. 2 II. Méthode d’évaluation............................................................................................................................ 2 III. Description........................................................................................................................................ 2 IV. Travail demandé................................................................................................................................ 4

A. Mise en place de l’architecture ......................................................................................................... 4 B. Tests des Attaques............................................................................................................................. 4 C. Sécuriser l’architecture réseau .......................................................................................................... 4

2023-2024 **I. Objectif**

L’objectif global de ce projet est de concrétiser les connaissances acquises dans le module sécurité informatique.

- Analyser le trafic entrant sortant d’une architecture réseau via un firewall ⚫ Concevoir, configurer et activer les règles de filtrage

- Mettre en place un IDS/IPS

⚫ Configurer un outil de détection d’intrusion Snort

- Etablir un réseau Privé virtuel VPN

⚫ Déployer **Openvpn**

- Tester quelques vulnérabilités des applications Web

⚫ Appliquer une ou deux attaques parmi les 10 attaques OWASP afin de vérifier la résistance de la politique de sécurité et du système de détection-prévention des attaques misent en place

**II. Méthode d Evaluation**

- Travail par groupe : au maximum 4 étudiants/groupe

- Un rapport (de 8 à 10 pages au maximum) illustrant les différents résultats et interprétations doit être élaboré.

- La validation sur machines aura lieu la 7ème semaine pendant la séance de cours. Un planning détaillé vous sera communiqué à temps.

- **Note de groupe** : validation de différentes fonctionnalités des services demandés. - **Note individuelle** : des questions d'ordre théorique

**III. Description**

Une entreprise souhaite sécuriser son réseau dont l’architecture est décrite comme suit : • Un réseau LAN : regroupe l’ensemble des machines des employés (utilisateurs internes)

• Un réseau DMZ : regroupe les différents serveurs hébergeant les applications des services métiers de l’entreprise

• Un réseau WAN : regroupe toutes les machines du réseau externe à l’entreprise

2023-2024 **Le plan d’adressage est fourni dans un document séparé (un plan d’adressage / groupe).**

Pour protéger l’architecture ci-dessus, l’administrateur de sécurité réseau a proposé de mettre en place ; comme première étape ; un pare-feu (voir figure). Les règles d’accès sont décrites comme suit :

**Politique de sécurité :**

- **Règle1 :** Les employés de l’entreprise sont autorisés à naviguer sur le web. - **Règle2** : Les clients ont toujours un accès vers le serveur Web.

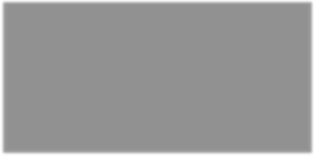
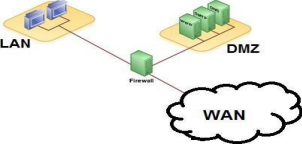
- **Règle3** : Les employés de l’entreprise peuvent échanger des e-mails en utilisant un serveur mail implémenté en local.

- **Règle4** : Les employés de l’entreprise peuvent travailler à distance (télétravail) en utilisant une connexion sécurisée à travers un **VPN.**

- **Règle5** : L’administrateur réseau doit accéder depuis la machine LAN vers la zone DMZ moyennant le protocole SSH.

- **Règle6** : L’authentification entre le serveur SSH et son client doit se faire avec des clés pas avec des mots de passes.

- **Règle7** : Interdire tout autre accès applicatif aux serveurs



*Figure 1 Architecture réseau sécurisée*

**2023-2024

**IV. Travail demandé **

**A. Mise en place de l’architecture**

1. Reproduire l’architecture de réseau en utilisant des machines virtuelles**sous Linux**.

2. Faire la configuration nécessaire (adressage, routage, etc.) et tester la connectivité entre lestrois zones (LAN, WAN et DMZ).

3. Visualiser le trafic échangé sur le réseau avec Whireshark.

**B. Tests des Attaques :**

En tant qu’attaquant éthique (white hacker), réaliser quelques attaques afin d’analyser la sécurité de l’architecture réseau pas encore protégé :

a) Tester une attaque de chapitre 2 à votre choix : visualiser et Interpréter le résultat

b) Tester une ou deux attaque(s) parmi les 10 attaques de Web Application Security Project (OWAP) : visualiser et Interpréter le résultat

**Que proposer-vous comme solution à chaque attaque testée ?**

**C. Sécuriser l’architecture réseau :**

**Partie 1 : Filtrage Firewall/ Accès à distance**

1. Installer et configurer **Pfsense** comme firewall pour sécuriser l’accès à travers les différentes zones.

2. Etablir la politique de filtrage à adopter pour contrôler l’accès vers les différentes zones.

3. Tester l’accès aux différents services suivant à partir des différentes zones : Accès vers leweb à partir du LAN, accès vers les serveurs publics à partir du LAN et d WAN.

**4.** Tester l’ouverture d’un accès à distance à travers **SSH** depuis la machine **LAN**

****2023-2024 versla **DMZ** avec une authentification par clé publique.

**Partie 2 : Détection d’intrusion**

1. Installer et configurer le logiciel Snort au niveau de réseau.

2. Effectuer des tests avec Snort : simple sniffer, des alertes etc.

**Partie 3 : Réseau privé Virtuel**

**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**.

**Partie 4 : test de niveau de sécurité améliorée**

L’administrateur réseau désire vérifier le niveau de sécurité amélioré :

a) Essayer de refaire les attaques précédemment testées.

b) Interpréter les résultats

c) De façon générale, Est-ce que la sécurité est garantie à 100% même en présence de Firewall, IDS/IPS et échanges du trafic via VPN OU ssh ?