

Chapitre 5 : Sécurité réseau

Objectifs

- Comprendre les enjeux de la sécurité des réseaux dans un environnement informatique.
- Identifier les menaces courantes ciblant les infrastructures réseau.
- Appréhender les meilleures pratiques et les mesures de sécurité à mettre en œuvre pour protéger les réseaux.

A. Introduction

La sécurité des réseaux est une composante essentielle de la sécurité informatique, visant à protéger les données et les ressources transitant par les réseaux internes et externes. Dans un monde de plus en plus connecté, les réseaux sont exposés à diverses menaces, telles que les cyberattaques, les intrusions et les violations de données. Ce chapitre se concentre sur les concepts fondamentaux de la sécurité réseau et les pratiques recommandées pour assurer une protection efficace.

B. Concepts

B.1 : Menaces à la Sécurité Réseau :

- **Intrusions et Attaques :**
 - Les intrusions peuvent provenir de l'extérieur (hackers) ou de l'intérieur (employés malveillants). Les types d'attaques incluent les attaques par déni de service (DDoS), les sniffers de réseau et les attaques par injection.
- **Malware :**
 - Les logiciels malveillants peuvent se propager à travers le réseau, compromettant les systèmes et dérobant des informations sensibles.
- **Vulnérabilités des Protocoles :**
 - Les failles dans les protocoles réseau peuvent être exploitées par des attaquants pour accéder à des données non sécurisées.

B.2 : Mesures de Sécurité Réseau :

- **Firewalls :**
 - Les pare-feu sont des dispositifs de sécurité qui surveillent et contrôlent le trafic réseau entrant et sortant, en appliquant des règles de sécurité.
- **Systèmes de Détection et de Prévention des Intrusions (IDS/IPS) :**
 - Ces systèmes surveillent le réseau pour détecter des activités suspectes et peuvent réagir en temps réel pour bloquer les menaces.
- **VPN (Réseau Privé Virtuel) :**
 - Les VPN créent des tunnels sécurisés pour le trafic réseau, permettant aux utilisateurs d'accéder à des ressources distantes en toute sécurité.

B.3 : Segmentation du Réseau

- **Importance de la Segmentation :**
 - La segmentation du réseau consiste à diviser un réseau en sous-réseaux plus petits pour limiter les mouvements latéraux des attaquants en cas d'intrusion. Cela permet de protéger les données sensibles et d'isoler les systèmes critiques.
- **Mise en œuvre de la Segmentation :**
 - Utilisation de VLANs (Virtual Local Area Networks) pour séparer le trafic et appliquer des politiques de sécurité spécifiques à chaque segment.

C. Référentiel

- **Normes et Cadres de Référence :**
 - **ISO/IEC 27033 :**
 - Norme qui fournit des lignes directrices pour la sécurité des réseaux et la gestion des risques associés.
 - **NIST SP 800-115 :**
 - Publication qui fournit des directives pour les tests de pénétration et les évaluations de la sécurité des réseaux.
- **Meilleures Pratiques :**
 - **Audit de Sécurité Réseau :**
 - Réalisation d'audits réguliers pour évaluer la sécurité des réseaux, identifier les vulnérabilités et mettre en place des mesures correctives.
 - **Mise à Jour des Équipements :**
 - S'assurer que tous les équipements réseau (routeurs, commutateurs, pare-feu) sont régulièrement mis à jour pour corriger les failles de sécurité.