

CyberSécurité

Sécurité des réseaux (36 heures)

26_27_4IRC_08_CYBER_UE9_091_MAJ

ACQUIS

- Analyser le rôle des protocoles TCP, UDP dans les réseaux.
- Maîtriser les techniques de filtrage et de contrôle d'accès dans un réseau.
- Configurer et gérer des firewalls pour sécuriser les communications réseau.
- Implémenter des solutions de sécurité basées sur IPsec pour les communications sécurisées.
- Appliquer les concepts de sécurité pour protéger les réseaux contre les menaces externes et internes.

CONTENU

- Protocoles de Communication
- Rappel sur le protocole TCP (Transmission Control Protocol) : modèle en couches, fiabilité, contrôle de flux, gestion de congestion, séquençement, structure des segments.
- Rappel sur le protocole UDP (User Datagram Protocol) : transmission non fiable, applications utilisant UDP (streaming, jeux en ligne, DNS), en-tête UDP, différences avec TCP.
- Listes de Contrôle d'Accès (ACL
- Access Control Lists)
- Rappel sur les ACL : objectifs et types (standard et étendues), règles de filtrage selon adresse, protocole, etc.
- Configuration et gestion des ACL : implémentation sur routeurs et switches, applications pratiques pour sécuriser les réseaux internes.
- Firewalls
- Rappel sur les Firewalls : rôle et types (filtrage de paquets, inspection dynamique, NGFW).
- Stratégies de filtrage : filtrage par IP, protocole, port et par application, firewalls de niveau application.
- Configuration d'un firewall : outils de gestion, création de règles de sécurité.
- IPsec (Internet Protocol Security)
- Rappel sur IPsec : objectifs de sécurité (confidentialité, intégrité, authentification), modes (transport et tunnel).
- Protocoles et algorithmes d'IPsec : AH et ESP, cryptographie (AES, 3DES, HMAC, SHA).
- Mise en oeuvre d'IPsec : création de tunnels VPN, étapes de configuration.
- Applications d'IPsec : sécurisation des communications inter-sites, accès sécurisé aux réseaux distants.
- Cas Pratiques et Applications
- Configuration d'un réseau avec ACL et Firewalls.
- Création d'un tunnel VPN sécurisé avec IPsec.
- Analyse des performances des protocoles TCP et UDP dans un réseau sécurisé.

PRÉREQUIS

- Notions de base en réseaux : modèle OSI, TCP/IP, et fonctionnement des équipements réseau.
- Connaissance des protocoles : TCP, UDP, et IP.
- Bases de la sécurité informatique : concepts de chiffrement, authentification et intégrité des données.
- Compétences en systèmes d'exploitation : maîtrise des commandes sur Linux ou Windows pour la configuration des outils de sécurité réseau.

PÉDAGOGIE

ÉVALUATION

BIBLIOGRAPHIE