

Sommaire

1. Introduction à la sécurité des réseaux

- Définitions et enjeux
- Historique et évolution
- Principes fondamentaux

2. Les menaces et attaques réseau

- Types d'attaques : malware, phishing, DDoS, etc.
- Techniques d'attaque : injection, interception, etc.
- Études de cas

3. Les mécanismes de sécurité

- Authentification et contrôle d'accès
- Chiffrement et VPN
- Pare-feu, systèmes de détection d'intrusion (IDS/IPS)
- Sécurité des protocoles (SSL/TLS, IPsec)

4. Sécurisation des infrastructures réseaux

- Sécurité des réseaux locaux (LAN) et étendus (WAN)
- Segmentation réseau et VLAN
- Sécurité des périphériques réseau

5. Gestion des risques et politique de sécurité

- Analyse de risques
- Mise en place de politiques de sécurité
- Plan de continuité d'activité

6. Résilience et surveillance

- Monitoring et journalisation
- Mise en place de réactions en cas d'incident

- Tests de pénétration et audits de sécurité

7. Normes et réglementations

- Cadre légal et conformité
- Normes ISO/IEC
- Obligations légales et éthiques

8. Tendances et défis futurs

- Sécurité dans le cloud
- Internet des objets (IoT)
- Intelligence artificielle et sécurité