

Exercice 1 (8 points)

1. Donnez et expliquez les attaques qui peuvent être faites contre la sécurité des couches 1, 2 et 3 du modèle OSI (Une attaque par couche).
2. Pourquoi est-il désirable que le(s) responsable(s) de la sécurité informatique et le(s) responsable(s) de systèmes d'information ne soit pas la même personne ?
3. Qu'est-ce qu'une zone démilitarisée (DMZ) et à quoi sert-elle ?
4. Un responsable de sécurité informatique souhaite mettre en place l'application PGP, expliquez lui son fonctionnement, quelles sont les attaques que peut éviter cet outil ?

Exercice 2 (12 Points)

Vous devez établir l'architecture du réseau d'une petite entreprise. Le réseau sera divisé en trois parties : réseau interne, DMZ et réseau externe. Les équipements suivants doivent être installés sur le réseau :

- Stations de travail des employés
- Serveur IMAP/POP3
- Serveur passerelle SMTP (entrant et sortant)
- Serveur de base de données
- Serveur Web
- Serveur DNS
- Passerelle VPN
- Serveur mandataire Web (« proxy » Web)
- Console de travail de l'administrateur du serveur Web

1. Dessinez le schéma du réseau et justifiez l'emplacement de chaque équipement.
2. Les serveurs DNS et SMTP doivent être sécurisés plus que les autres équipements, Pourquoi ?
3. Appliquez un système de translation d'adresses (NAT) utilisant l'adresse publique 44.22.15.103.
4. Donnez la table de filtrage qui permet l'accès aux serveurs Web et IMAP.
5. L'équipe informatique souhaite mettre en place un serveur reverse-proxy http ; Quelles sont les types d'attaque que peut détecter ce serveur ? Quelles sont les fonctionnalités de ce serveur ?
6. Les employés de l'entreprise accèdent à Facebook et utilisent les logiciels P2P durant leur travail, dans quelle mesure l'usage de ces outils à des fins privées par les employés de l'entreprise peut générer des problèmes de sécurité pour celle-ci ?

L'entreprise offre des services bancaires par Internet à ses clients. Auparavant, ce service permettait seulement de consulter les transactions du compte et de payer des factures de services publics (électricité, Gaz, etc.). À la demande de ses clients, la société a ajouté la possibilité d'effectuer des transferts interbancaires sur des comptes de particulier via leur interface internet.

7. Faites l'analyse du risque dans les deux situations.
8. Donnez et expliquez les attaques qui peuvent être appliquées dans les deux situations.