

Exercice 1 généralités

expliquez les termes suivants : intégrité, authentification, authentification forte et non répudiation

Exercice 2 domaines d'application de la sécurité

Donner une définition succincte des 5 domaines d'application de la sécurité suivants : sécurité physique, sécurité de l'exploitation, sécurité logique, sécurité applicative, sécurité des télécommunications. Pour chacun d'eux, vous donnerez quelques points clefs sur lesquels ils reposent.

Exercice 3 chiffrement

Question 1

Expliquez le fonctionnement et comparez le principe général du chiffrement symétrique et du chiffrement asymétrique.

Question 2

Citez au moins 4 services offerts par le chiffrement.

Exercice 4 contrôle d'accès réseau

Question 1

Après avoir expliqué brièvement en quoi ils consistent, donnez les points forts et les points faibles des 3 modes de contrôle d'accès réseau suivant :

- brassage et activation de ports à la demande
- contrôle des adresses MAC
- utilisation d'un équipement en coupure

Question 2

Dans quel contexte et à quoi sert 802.1X ? Quel couche est-elle concernée. On ne vous demande une description détaillée du fonctionnement du protocole.

Question 3 Coupe feu, sécurité périmétrique

Dans le cadre d'une architecture de sécurité reposant notamment sur des coupes feux de niveau 3 et 4, expliquez ce que l'on entend par « sécurité périmétrique ». Quelles en sont les limitations ?

Question 4

En vous appuyant sur l'exemple du proxy WeB, expliquer ce qu'est un mandataire (proxy). Indiquer l'intérêt d'un tel outil (proxy WeB) et dans quel contexte on l'utilise.

Question 5

Qu'est-ce qu'un « reverse proxy » ? A quoi cela sert-il ?

Question 5

Expliquez ce que recouvrent les termes: surface d'attaque et sécurité en profondeur.

Question 5

Qu'est-ce qu'un CSIRT ?

Question 5

qu'appelle-t-on une analyse post mortem ?

Exercice 5 contrôle d'accès réseau

la société thebest.com possède le domaine dns thebest.com. Elle a un unique serveur de courrier qui fait office de serveur de courrier entrant, de courrier sortant et de serveur de boîtes aux lettres.

Après avoir critiqué cette architecture, vous en proposerez une autre dans laquelle vous pouvez utiliser en autant d'exemplaire que nécessaire :

- serveur de courrier entrant (plusieurs peuvent être chaînés les uns aux autres)
- serveur de boîtes aux lettres (c'est là que finit par arriver le courriers entrant)
- serveur de courrier sortant (plusieurs peuvent être chaînés les uns aux autres si nécessaire)
- routeur, coupe feu

Pour les coupes feux, vous pourrez préciser en français quel service sur quel serveur est accessible à partir de quel(lles) sources et ce qui est interdit.