Contrôle continu

Sécurité des SI

Génie informatique 2 durée 1h30

Questions de cours :

1. Pourquoi est-il important de sécuriser les communications sur IP ?
2. Un administrateur réseau identifie les utilisateurs par leurs adresses IP et demande un mot de passe envoyé en clair sur le réseau. A quels types d'attaque ce système est il exposé ? comment ce problème peut être évité
3. Un hacker utilise un ordinateur portable muni d'une carte réseau sans fil récupère les données qui circulent sur le réseau et réussi à se faire passer par un utilisateur légitime pour accéder à un service interne de l'entreprise. De quels types d'attaques s'agit-il ? quelle faille de sécurité a permis à ce hacker à récupérer les données qui circulent dans le réseau ?
4. Les utilisateurs sont identifiés par des empreintes digitales. Des certificats numériques sont générés sur la base de ces empreintes. Toutes communication avec le serveur doit être assurées par un algorithme de cryptage DES. S'agit-il d'une procédure ou une politique ? quels sont les principes appliqués dans cette règle de sécurité

Exercice 1 :

Sur un réseau local utilisant un hub ou les utilisateurs connectent leurs machines directement sur le hub peuvent accéder à internet ainsi qu'au réseau intranet. L'accès à la salle et par conséquence au hub se fait sans grande difficulté une personne sur dix y accède sans être contrôlé par les agents de sécurité. Les utilisateurs de l'intranet se connectent sur un serveur de données en utilisant un login et un mot de passe envoyé en clair sur le réseau et en traversant un pare feu qui ne laisse passé que les utilisateurs avec une adresse IP du réseau interne.

1) Quel sont les attaques auxquelles ce réseau est il exposés ?
2) Par quel moyen le mot de passe et le login peuvent être récupérés ?
3) Dresser l'arbre des événements pour qu'un hacker accède aux ressources de l'entreprise ou met le réseau hors service sachant que la probabilité de trouver le login et le mot de passe est de 1/50 et la probabilité de spoofé une adresse IP est de 1/100
4) Calculer la probabilité que l'une des deux attaques ait lieu
5) Proposer des mesures pour renforcer la sécurité de cette entreprise

Exercice 2 :

Décrire les ACL suivantes :

1) Access list 40 permit 115.1.13.0 0.0.127.255
2) Access-list 140 permit TCP host 193.1.1.1 gt 1001 host 193.1.1.2 eq 80
3) Acess-list 30 deny 192.168.1.0 0.0.0.127

   Access-list 30 permit any

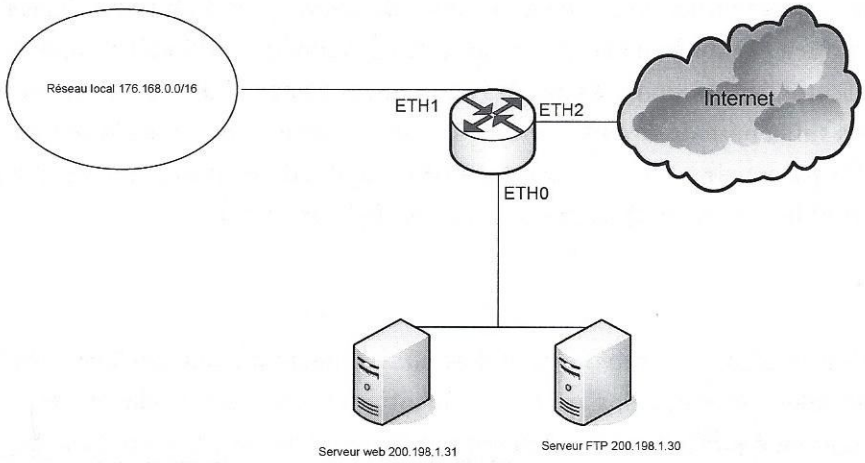
4) Access-list 150 permit ICMP any host 192.168.1.40
5) Access-list 179 permit TCP 192.168.1.0 0.0.0.255 any eq 80

   Acces-list 179 deny icmp any any

6) Quel est le résultat d'un ping de la machine 115.180.1.3 par rapport à l'ACL numéro 40 ?
7) Quel est le résultat d'une requete http venant de la machine 193.1.1.1 vers la machine 193.1.1.2 ?
8) Quel est le résultat d'une requete telnet de la machine 192.168.1.140 par rappot à l'ACL numéro 30 ?

Exercice 3:

Un administrateur dispose d'un réseau local 176.168.0.0/16. Il dispose également d'un serveur web d'adresse publique 200.198.1.30 et un serveur FTP d'adresse 200.198.1.31.



1. L'administrateur veut autoriser les machines du réseau local à utiliser internet sachant que pour autoriser internet il faut ouvrir le port du protocole http et le port du protocole DNS. Ecrire une ACL qui permet d'autoriser le flux sortant vers internet. Ou doit-il appliquer cette ACL ?
2. Dans le sens inverse seuls les paquets à destination du réseau local avec un port source DNS ou http doivent être acceptés. Ecrire une ACL qui permet de réaliser cette opération
3. Ecrire deux ACL (envoi et réception) qui permettent l'accès seulement aux serveurs Web et FTP aux machines d'internet. Sur quelle interface/direction doit-on les appliquer ?
4. Ecrire une ACL qui interdit aux utilisateurs du réseau local de spoofer des adresses IP
5. L'administrateur contrôle par Telnet les deux serveurs depuis une des machines des réseaux depuis un port source 10111. Ecrire une ACL qui autorise seulement l'accès à ce service pour l'administrateur et permettre les autres échanges de paquet IP
6. Est que l'utilisation du numéro de port pour authentifier l'administrateur est une manière sur d'authentification ? pourquoi ?