DS

Sécurité et cryptographie

Classes: 1ère année SSICE

Documents autorisés

Exercice 1 [4pts]:

1) Expliquer pourquoi il est plus facile d'écouter (sniffer) un réseau local partagé qu'un réseau commuté.
2) Expliquer pourquoi, dans un réseau local, les nœuds ayant des adresses routables (publiques) sont beaucoup plus exposés aux attaques externes que ceux ayant des adresses privées?
3) Certaines attaques ne peuvent être lancées qu'à partir de l'intérieur du réseau local. Donner une méthode permettant à un nœud externe au réseau local de lancer ce type d'attaque? Expliquer ?
4) Expliquer pourquoi les attaques externes sont plus difficiles à mener que les attaques internes ?
5) Expliquer pourquoi les attaques passives sont plus utiles (pour l'attaquant) dans un réseau partagé que dans un réseau commuté ?

Exercice 2 [5pts]:

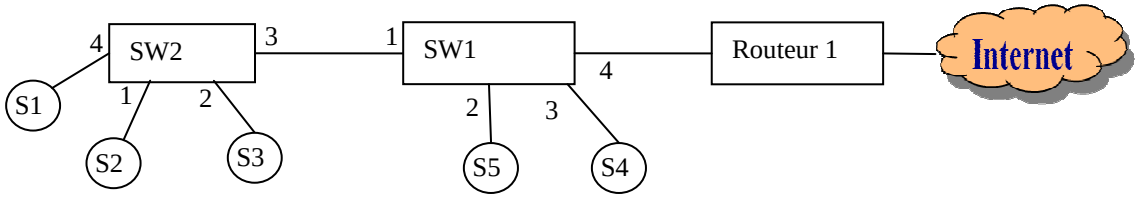
1) Expliquer comment un attaquant peut transformer un réseau Ethernet commuté en un réseau partagé? Donner une solution permettant de contrer cette attaque ?
2) En se basant sur DHCP, expliquer comment un attaquant peut faire passer le trafic destiné à Internet par lui ? Donner une solution permettant de contrer cette attaque ?
3) Donner une solution permettant de détecter et d'identifier les serveurs DHCP pirates.
4) Soit trois nœuds A, B et C relié à un commutateur. Donner une solution permettant à A d'intercepter les messages échangés entre B et C.?

Exercice 3 [5pts]:

1) Est-il nécessaire d'utiliser un canal sécurisé pour récupérer la clé publique (de chiffrement) dans un système à chiffrement asymétrique? Expliquer ?
2) Est-il nécessaire d'utiliser un canal authentifié pour récupérer la clé de chiffrement des donnés dans un système à chiffrement hybride? Expliquer ?
3) Expliquer l'utilité de changer la clé d'encryptage des données à chaque session pour un système à chiffrement hybride,?
4) Comparer les systèmes de chiffrement symétriques et asymétriques de point de vue problématique de gestions de clés (nombre et sécurité des clés, problématique de mise en place des clés…etc) ?
5) Comparer l'authentification par adresse IP à celle par signature de point de vue robustesse. Expliquer ?
6) Quel problème peut surgir si la clé privée du PKI est compromise par un attaquant?

Exercice 4 [6pts]:

Soit le réseau câblé suivant où les cercles sont des stations de travail :



1) Expliquer comment SW1 apprend que S5 se trouve sur son port 2?
2) Expliquer la réaction de SW2 lorsque S5 change de port (du port 2 vers le port 5 du même switch)?
3) Supposons que SW2 a appris les ports menant à S1, S2 et S3. Donner la nouvelle table de commutation de SW2 si S1 envoie une trame en spécifiant comme adresse MAC source celle de S2
4) Supposons que la taille de la table de commutation (TC) de SW2 est 8192 entrées. L'administrateur a limité le nombre d'adresses MAC par port à 200. Donner le nombre d'entrées libre de TC après l''exécution d'une attaque d'inondation de TC par les nœuds S2 et S5. Expliquer ?
5) En tenant compte des données et des résultats de la question précédente, S2 peut-il récupérer une copie des messages échangés entre S1 et S3? Si oui, comment ?
6) Supposons que S4 est un serveur DHCP légitime et que l'administrateur a utilisé le DHCP snooping seulement au niveau du switch SW2. Quel sont les nœuds qui peuvent jouer le rôle de serveurs DHCP sans être détecté. Expliquer ?