Master 2 SeCReTS

Module "Concepts de sécurité & réseaux"

Sécurité des couches TCP/IP

Les supports de cours et autres documents ne sont pas autorisés. Seules les notes sont autorisées dans la limite d'une feuille recto/verso

Chaque question est notée sur un ou deux points, et seule une réponse complète avec des explications claires et suffisament détaillées se verra accorder la totalité des points.

1 Sécurité de la couche 2

Vous êtes dans une chambre d'un hôtel offrant une connexion à Internet au travers d'une liaison filaire. Vous raccordez votre PC portable avec le câble RJ45 fourni, et, une fois la connexion réseau établie vous êtes en mesure de surfer sur le net et de consulter votre messagerie.

Les paramètres de l'interface réseau de votre PC portable sont :

- Adresse IP : `172.16.23.56`
- Masque de sous-réseau : `255.255.255.0`
- Passerelle par défaut : `172.16.23.1`

▷ *(1 point)* Dans cette situation, quels sont les dangers auxquels vous êtes exposé ?

▷ *(1 point)* Comment feriez-vous pour détecter des tentatives d'attaques ?

▷ *(1 point)* Quels sont les mécanismes de protection possibles ?

2 La couche de niveau 3 / IP

2.1 A propos du TTL

On observe le trafic réseau en un point donné (par exemple, en se plaçant au niveau du lien entre deux routeurs successifs et en *écoutant* le trafic avec `tcpdump`). Cela permet de voir notamment différents paquets IP faisant partie d'une même connexion (par exemple, le trafic d'une session SSH entre un client et un serveur).

▷ *(1 point)* Que représente la valeur du champ TTL ? Est-ce la même valeur pour tous les paquets de la session SSH observée ?

2.2 Format des datagrammes IP

▷ *(1 point)* Quelle est la taille maximale (en octets) de la PCI ("*Protocol Control Information*" dans le vocabulaire OSI) contenue dans un fragment IP ? Justifiez votre réponse.

2.3 Découpage `CIDR`

Une entreprise décide de louer un bloc d'adresses IP auprès d'un opérateur. Ce dernier lui alloue le bloc `201.20.0.128/25`. L'entreprise en question choisit de découper son ensemble d'adresses en 4 sous-réseaux.

▷ *(2 points)* Proposer une découpage possible et donner pour chaque sous-réseau l'adresse et le masque. Il ne doit pas y avoir de gaspillage (*i.e.* toutes les adresses IP doivent être utilisées).