Sécurité réseau
Sylvain Meignier

Question 1

Une entreprise éditrice de logiciels vous confie la mise en place de son réseau. L'entreprise est divisée en 5 services :

- Direction : un directeur (bureau 1, un poste de travail, 1 téléphone), une assistante de direction (bureau 2, un poste de travail, 1 téléphone)
- Administratif : facturation, salaire, expédition des produits (bureau 3, 4 postes de travail, 4 téléphones),…
- Commerciaux : 5 ingénieurs et une personne chargée de la communication et du marketing (bureau 4, 6 postes de travail, 6 téléphones).
- Maintenance et Assistance : un ingénieur et 5 techniciens installation, maintenance et assistance des clients (bureau 5, 6 postes de travail, 6 téléphones).
- R&D : un chef de projet et 4 ingénieurs. Ils sont chargés du développement des nouveaux produits (bureau 6, 1 poste de travail ; bureau 7, 4 postes de travail, 2 téléphones).

Besoin à satisfaire :

- Le réseau de données interne doit avoir un bon débit pour permettre le partage des ressources (1 serveur de fichiers, 2 imprimantes, etc.). Les stations de travail sont hétérogènes (75% Windows, 25% Macintosh).
- Les services disponibles sur le réseau sont :
    - Service de mail
    - Service DNS
    - Services web :
        - un site pour la promotion de la société à l'extérieur de l'entreprise, le site est accessible de l'extérieur et de l'intérieur.
        - un site consultable uniquement depuis l'entreprise, il héberge un logiciel de « groupware » permettant de partager un agenda et un calendrier entre les employés.
- Les employés de l'entreprise ont un accès à l'Internet (web et mail uniquement).
- Les serveurs web, mail et DNS sont accessibles depuis l'Internet.

Questions : lire toutes les questions avant de répondre !

a : Sachant que l'entreprise cherche à minimiser les coûts, elle souhaite une solution faisant intervenir un seul routeur. Définissez la structure physique du réseau qui réponde à l'ensemble des besoins : type de matériels, serveur(s)... Donnez un schéma de l'infrastructure réseau, commentez.

b : Proposez un plan d'adressage complet (serveur(s), machines et routeur). Proposez la liste des services / logiciels disponibles sur le routeur, les serveurs. On supposera que l'entreprise n'a pas acheté de classe d'adresse publique ; par contre son fournisseur d'accès à l'internet lui a alloué 2 adresses publiques de 194.57.216.100 et 194.57.216.101.

c : Donnez les règles de filtrage. Faire un tableau avec les informations utiles.

Question 2

Les réseaux locaux sans fil utilisent des transmissions radio plutôt que des câbles. Ainsi, au lieu de tirer des fils dans tous les locaux d'une entreprise on peut installer quelques bornes radio et équiper tous les ordinateurs de cartes réseaux sans fil.

a : A quelle menace s'expose-t-on en utilisant un tel dispositif au lieu d'un système avec des câbles et en quoi cette menace est-elle pire que dans le cas d'un système avec des câbles ?

b : Donner une méthode pour diminuer la menace tout en gardant la technologie sans fil ?

c : Dans un réseau sans fil, la bande passante est partagée entre les différentes machines. Ce type de fonctionnement s'apparente-t-il au fonctionnement d'un Hub ou d'un Switch ?

c : Pour une grande entreprise, est-il raisonnable de munir les serveurs de fichiers de carte sans fil sachant que le débit théorique de la norme IEEE 802.11g est de 54Mbps sur une distance de plusieurs centaines de mètres ?

Question 3

Un pirate a remarqué qu'une requête de transfert de zone DNS (utilisée notamment pour fournir à un serveur DNS l'information qu'il doit connaître concernant la ou les zones qu'il doit desservir) fait toujours 16 octets de long, et que la réponse du serveur DNS dns.foo.fr fait 768 octets. On admettra que les communications se font en UDP.

a: Comment le pirate peut-il réaliser une attaque par déni de service depuis machine.pirate.com contre le serveur cible.victime.fr ? Expliquez, illustrez par un schéma.
b: Si le pirate possède une bande passante de 256 kilo bits par seconde et qu'il est capable de l'utiliser à 100% pour son attaque, l'attaque saturera-t-elle la bande passante de 2 méga bits par seconde de cible.victime.fr (on considère que dns.foo.fr a une bande passante infinie) ?