INSA de Toulouse – 5° R.T.

CORRIGÉ

Examen du 25 janvier 2008

Sécurité des systèmes informatiques

2ème partie

Exercice 1 *(2,5 points)*

Le logiciel d'authentification des systèmes d'exploitation usuels vérifie le mot de passe fourni par un utilisateur à l'aide d'une empreinte de ce mot de passe stockée par le système dans un fichier protégé.

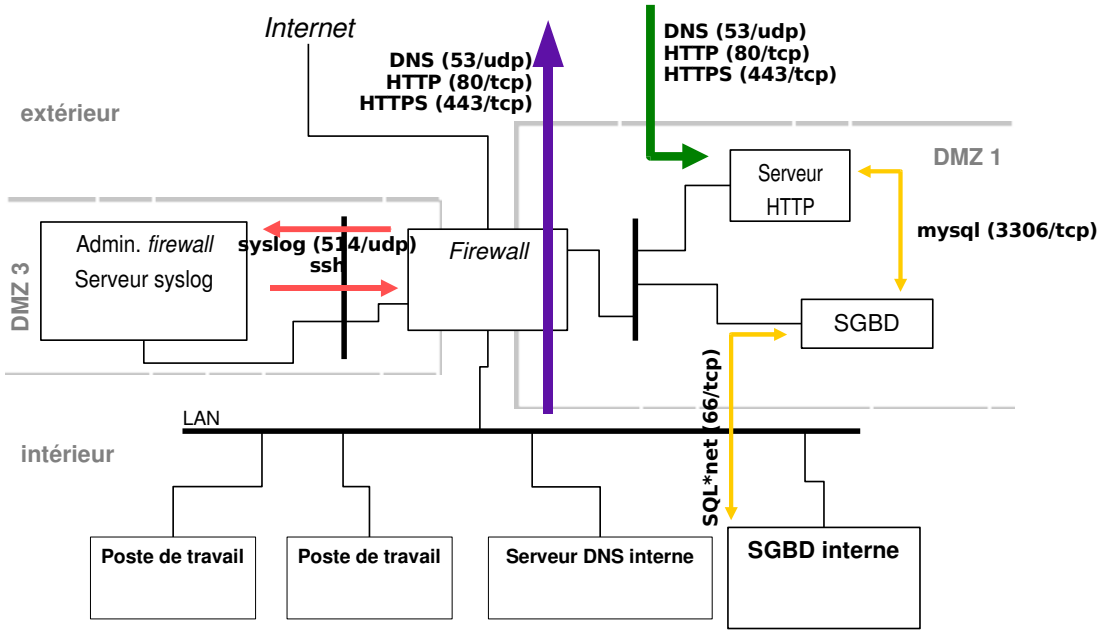
1. Pourquoi stocker des empreintes des mots de passe plutôt que les mots de passe eux-mêmes ?
2. Pourquoi doit-on protéger l'accès à ce fichier contenant les empreintes des mots de passe ?
3. Sous quelle condition cette précaution ne serait pas nécessaire ?

Stockage des empreintes des mots de passe :

1. *Étant donné que les empreintes des mots de passe sont générées à l'aide d'une fonction non-inversible (fonction de hachage ou algorithme de chiffrement utilisé dans un mode équivalent), le vol ou la consultation des empreintes ne divulgue pas les mots de passe.*
2. *Bien que la fonction qui ait généré les empreintes des mots de passe ne soit pas inversible, il est préférable de protéger l'accès à ce fichier car les mots de passe peuvent souvent être retrouvés à l'aide d'une attaque par dictionnaire ou via une recherche exhaustive si l'ensemble des mots de passe possibles est suffisamment petit et la fonction utilisée suffisament rapide (par exemple une chaîne de caractères alphabétiques de longueur inférieure ou égale à 6).*
3. *Si les mots de passe choisis par les utilisateurs étaient suffisamment complexes (et notamment, peu susceptibles d'apparaître dans un quelconque dictionnaire), cette protection de la confidentialité de l'empreinte pourrait être inutile. A notre connaissance, il n'y a pas de conditions d'utilisation réalistes, où l'on puisse faire cette hypothèse.*

Exercice 2 *(8 points)*

On étudie l'architecture de protection réseau suivante :



Question 1 *(2 points)* : Compte tenu du mode de fonctionnement suggéré par le schéma, expliquez le fonctionnement des différents services réseau fournis à l'organisation utilisant cette architecture. Indiquez les protections offertes par l'architecture.

Question 2 *(1 point)* : Compte tenu des flux identifiés, un autre service réseau devrait figurer en DMZ. Lequel ?

Question 3 *(1 point)* : Certains flux d'administration sont également absents. Indiquez lesquels vous semblent nécessaires et si on peut vraiment envisager de s'en passer dans un cas d'utilisation réaliste.

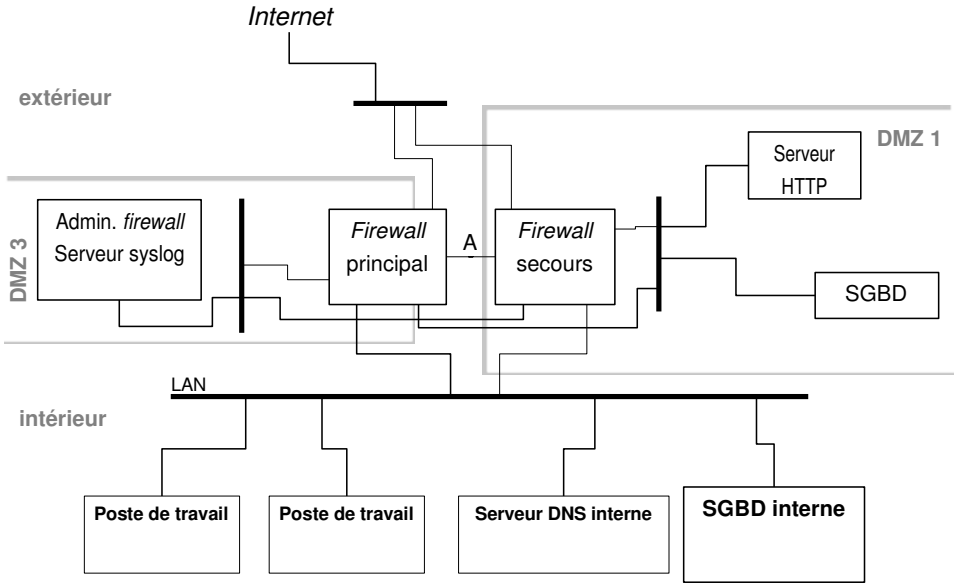
Description des services (question 1)

- *En DMZ 1, on voit d'abord apparaître un serveur HTTP (et probablement HTTPS compte tenu des flux entrants). Ce serveur Web intègre certainement des pages dynamiques ou des applications car il interagit avec un SGBD situé également dans la même DMZ (un serveur MySQL compte tenu du flux entre les deux machines). Ce serveur de base de données interagit également avec un SGBD situé sur le réseau local de l'entreprise via le protocole SQL*net (caractéristique d'Oracle).*
- *L'administration de l'équipement de protection est effectuée depuis une station présente en DMZ 3 à l'aide du protocole SSH. C'est également cette station qui est utilisée pour la collecte des traces produites par le firewall lui-même.*
- *Le firewall autorise les accès directs aux services DNS et HTTP ou HTTPS du réseau public depuis le réseau local de l'entreprise.*

(Question 2) Pour le bon fonctionnement du serveur Web offert par l'entreprise en DMZ 1, un service DNS est également nécessaire (notamment afin de référencer l'URL d'accès). Ce flux apparaît sur le schéma, mais le service DNS ne figure pas sur les machines identifiées dans la DMZ 1 (est-il sur une machine séparée, sur la même machine que le serveur HTTP, fourni par un prestataire extérieur – donc inutile au niveau du firewall, etc. ?).

(Question 3) Les flux d'administration du firewall apparaissent sur la figure, mais uniquement en provenance de la DMZ d'administration. Ce sont les seuls flux d'administration identifiés. Or, il est bien évident que des flux d'administration doivent également être prévus à destination des machines de la DMZ 1 (serveur HTTP ou SGBD MySQL).
Les flux d'administration à destination de ces machines, ou même à destination du firewall, sont habituellement nécessaires aussi à partir du réseau local (et pas seulement depuis les machines de la DMZ d'administration – fréquemment à isoler physiquement). De manière réaliste, ces flux sont quasiment incontournables, notamment en provenance des postes de travail des administrateurs eux-mêmes. Par contre, il est également fréquent que ces flux « secondaires » n'apparaissent pas dans la description du fonctionnement, même si, en nombre, ils peuvent représenter une majorité des types de communication à prendre en compte.

Pour améliorer la disponibilité de l'architecture, on propose l'évolution suivante visant à introduire de la redondance au niveau du *firewall*. (Il s'agit ici d'une redondance passive où l'équipement de secours ne fonctionne pas en situation normale et ne prend le relais de l'équipement principal qu'en cas de besoin.)



Question 4 *(1 point)* : Certains équipements nécessaires au fonctionnement du système n'apparaissent pas sur la figure. Lesquels ? Quel peut être l'impact de leur choix sur la disponibilité de l'ensemble ?
Question 5 *(1 point)* : Compte tenu de la gestion de la redondance et des informations gérées en interne par un *firewall*, quelles informations transitent sur le lien A ?
Question 6 *(1 point)* : A votre avis, du point de vue d'un utilisateur (ou d'un routeur) sur Internet, quelle est l'adresse IP du *firewall* ? Comment pourrait-on gérer ce type de cas ?

Question 7 *(1 point)* : On envisage de basculer dans une autre configuration où les deux firewall fonctionnent en régime normal en se partageant le trafic. Pointer les difficultés que ce type de fonctionnement peut poser au niveau du fonctionnement habituel d'un réseau ?

(Question 4) Les équipements de communication de niveau 2 (commutateurs) n'apparaissent pas sur la figure. Ils sont pourtant nécessaires pour l'interconnexion des 2 firewall entre eux et avec les réseaux les entourant. Si ces équipements ne sont pas redondants (ou dotés de garanties de disponibilité particulières comme des composants internes redondants), ils risquent de jouer un rôle dominant vis à vis de l'(in)disponibilité de l'ensemble de l'architecture en présentant des taux de défaillance supérieurs au couple de firewall.

(Question 5) Sur le lien A, plusieurs types d'information doivent transiter :

- *des informations de contrôle de l'état des firewall permettant à l'un d'entre eux de détecter la défaillance de l'autre (heartbeat par exemple) ;*
- *des transmissions régulières de l'état interne du firewall principal vers le firewall de secours doivent également avoir lieu afin que celui-ci soit en mesure de reprendre correctement le transport des flux en cas de défaillance (table des connexions en cours, table des translations d'adresses actives par exemple).*

NB: Ces informations peuvent également transiter par d'autres liens de connexion entre les deux firewall qu'un lien direct. (Mais il est plus facile d'étudier ces flux sur un lien spécifique.)

(Question 6) En fait, deux cas de figure sont envisageables :

- *les deux firewall possèdent chacun une adresse IP distincte, visibles depuis le réseau extérieur ;*
- *les deux firewall partagent une même adresse IP (un seul d'entre eux étant effectivement actif à l'adresse en question à un instant donné).*

Le premier cas peut néanmoins permettre d'assurer un basculement du firewall principal vers le firewall primaire en utilisant la coopération avec les routeurs en amont ou en aval des firewall via des protocoles de routage dynamiques. De tels routeurs doivent bien sûr être présents (y compris en DMZ) pour que cette approche puisse être envisagée.
Dans le deuxième cas, des protocoles spécifiques (HSRP, CARP par exemple) doivent être utilisés afin de permettre ce partage effectif d'une seule adresse IP entre deux équipements (possédant des interfaces réseaux différentes). Ces protocoles permettent alors généralement d'utiliser une adresse IP « virtuelle » dont l'association avec l'adresse MAC est susceptible de changer pour basculer dynamiquement d'un firewall vers l'autre en cas de besoin. Dans ce cas, les firewall possèdent alors généralement aussi chacun une autre adresse IP (personnelle), notamment pour l'administration ou leurs échanges en fonctionnement nominal.

(Question 7) Si les firewall se partagent le trafic réseau, la principale difficulté est liée au cheminement des paquets IP constituant le flux aller et le flux retour d'une connexion TCP. Il est habituellement nécessaire de garantir que les paquets IP allers et retour d'une même connexion transitent par le même firewall (pour éviter que l'un d'entre eux ne rejette ces paquets en les croyant non-associés à une connexion en cours). Ceci nécessite alors souvent de disposer de fonctions de distribution des paquets dans les équipements d'interconnexion de niveau 2 interconnectant les firewall, qui assurent alors une partie de la distribution de charge entre les deux équipements.

Exercice 3 *(1,5 points)*

Un employé télécharge de la musique grâce à un logiciel *peer-to-peer* pendant ses heures de travail. Il reçoit et lance malencontreusement une copie d'un virus *VisualBasic* qui se propage automatiquement sous forme de courrier électronique à tous les contacts inscrits dans son carnet d'adresses. Le serveur de messagerie interne étant doté d'un antivirus, la pièce jointe est heureusement automatiquement éliminée. Quels principes de base ne sont pas respectés dans l'architecture informatique de cette entreprise ?

Par exemple:
Si la machine de l'employé était équipée d'un antivirus (similaire à celui utilisé par le serveur de messagerie), le virus n'aurait pas pu tenter de se propager à toute l'entreprise. Ajouter un moyen de protection apparemment redondant permet parfois de pallier à des défaillances de sécurité difficiles à prévenir (comme les actions malencontreuses d'un utilisateur autorisé) : c'est le principe de défense en profondeur.
A moins d'un domaine professionnel bien spécifique, il va falloir de bons arguments à l'employé pour justifier le téléchargement de musique pendant le temps de travail. L'administrateur aurait dû interdire ce type d'accès peer-to-peer : c'est le principe du moindre privilège.