INSA – 5° R.T.

Sujet d'examen
19 janvier 2005

Sécurité des systèmes d'information

2ème partie

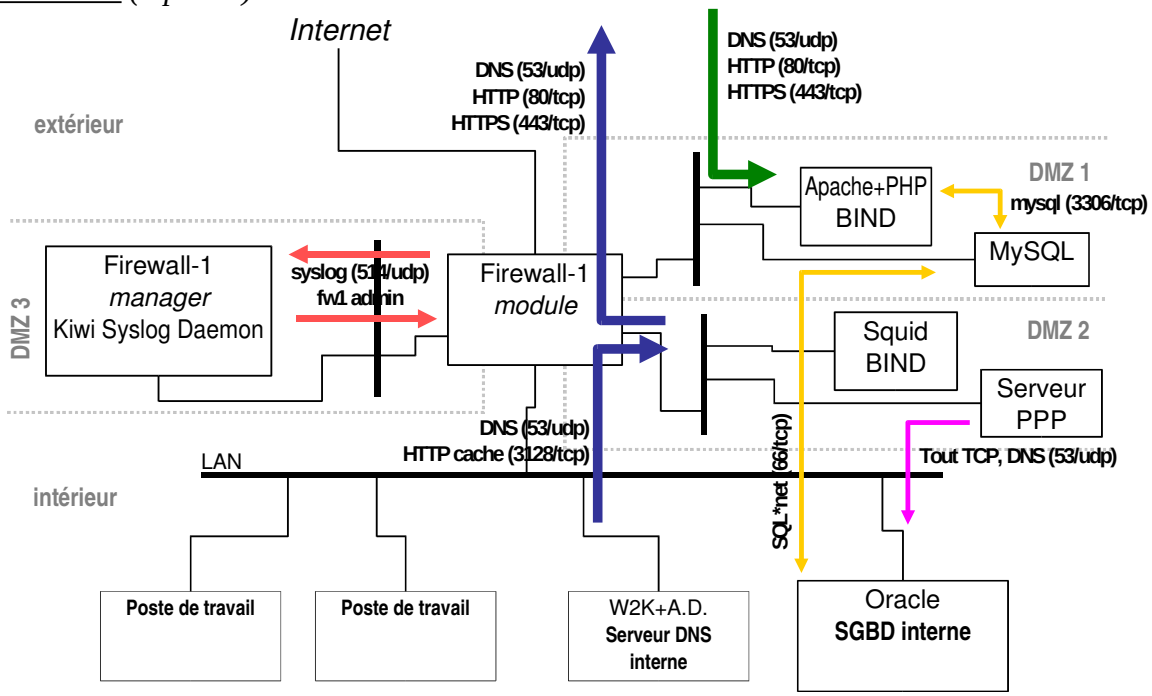
Exercice 1 *(3 points)*

Rédigez des exemples fictifs mais réalistes de règles de sécurité pouvant figurer dans chacun des documents suivants (6 règles en tout) :

A) 2 règles de la « Politique de Sécurité du Système d'Information » (PSSI)
B) 2 règles appartenant aux « Spécifications de sécurité réseau » (B.1) ou « Spécifications de sécurité des systèmes » (B.2)
C) 2 règles pour les « Cahier de recette de configuration d'Apache v.1.3 » (C.1) ou « Cahier de recette de configuration de Windows 2000 » (C.2)

Identifiez bien dans lequel de ces 5 documents figure selon vous chacune de vos 6 propositions.

Exercice 2 *(4 points)*



Question 1 *(2 points)* : Compte tenu du mode de fonctionnement suggéré par le schéma, indiquez l'usage de chacune des DMZ et la (les) fonction(s) qu'elle apporte à l'organisation utilisant cette architecture.

Question 2 *(2 points)* : Critiquez (avantages/inconvénients) l'architecture utilisée (notamment en terme de sécurité). Proposez des évolutions de l'architecture permettant de pallier certains inconvénients et éventuellement précisez les nouveaux inconvénients associés à vos préconisations.

Exercice 3 *(3 points)*

Voici 3 exemples de méthode utilisables par un utilisateur pour choisir un mot de passe :

1. Utilisation d'un mot de passe de 7 symboles exactement choisis au hasard parmi les **36** symboles alphanumériques (ce qui suppose que le système d'exploitation ne fait *pas* de distinction entre majuscules et minuscules).
   Exemple : `8PER2ZZ`
2. Utilisation de 2 mots du dictionnaire français courant accolés ou éventuellement séparés ou suivis par des caractères spéciaux choisis parmi : `,;:!?-`
   Exemples : `EMPORTE,VENT` ou `VIVE-MOI!`
3. Utilisation de la première lettre d'une phrase comptant au moins douze mots. On fera aussi l'hypothèse que toutes les lettres sont mises en minuscule pour constituer le mot de passe et qu'on n'inclut pas les signes de ponctuation.
   Exemple : `udlpldupcamdm` (1ère phrase ci-dessus)

Question 1 *(2 points)* : Comparez ces méthodes en évaluant *quantitativement* la taille de l'espace de recherche associé à chaque méthode, en vous servant si besoin des informations indiquées ci-dessous. Il n'est pas indispensable de calculer de manière exacte la taille de l'espace considéré, mais essayez d'obtenir un *ordre de grandeur* utile et justifié du nombre de mots de passe possibles (ou d'un minorant).
Question 2 *(1 point)*: Ensuite, en vous appuyant sur les informations expérimentales fournies ci-dessous, calculez (en jours) la durée espérée de résistance d'un mot de passe de type 1, 2 ou 3 face à un outil d'attaque par dictionnaire, suite à un vol de la forme chiffrée du mot de passe[1]. Considérez : un système Unix utilisant un chiffrement DES classique, un système Windows utilisant NT LM (DES) et un système OpenBSD utilisant Blowfish et un *salt* de grande taille.

Informations utiles :

- On pourra considérer qu'un lexique de français courant compte environ 4000 mots[2] (méthode 2 ou 3).
- Pour plus de réalisme, on pourra considérer (méthode 3) qu'une phrase est composée à 50% de « mots outils » qui ne représentent que 0,5% du lexique total mais surtout qui ne représentent que 25% des lettres de l'alphabet (pour leur première lettre), soit seulement 6 lettres.
- Le plus sûr est souvent d'évaluer expérimentalement le nombre de combinaisons par seconde (c/s) qu'une machine peut essayer. Voici, sur une machine moderne (P4 2,66 GHz) les performances obtenues par un outil librement disponible :

```
$ john -test
Benchmarking: Standard DES [48/64 4K]... DONE
Many salts:     192409 c/s real, 193182 c/s virtual

Benchmarking: OpenBSD Blowfish (x32) [32/32]... DONE
Raw:    380 c/s real, 381 c/s virtual

Benchmarking: NT LM DES [48/64 4K]... DONE
Raw:    1808998 c/s real, 1816263 c/s virtual
```

[1] Contenue dans /etc/passwd ou /etc/shadow sur un système Unix, ou dans la base SAM d'une machine Windows, ou transitant sur le réseau pour certaines applications (VNC, etc.).
[2] Le lexique Dubois-Buyse des mots français courants (enfants entre 0 et 16 ans) compte 3726 mots.