INSA – 5° R.T.

Sujet d'examen
20 janvier 2004

Sécurité des systèmes d'information

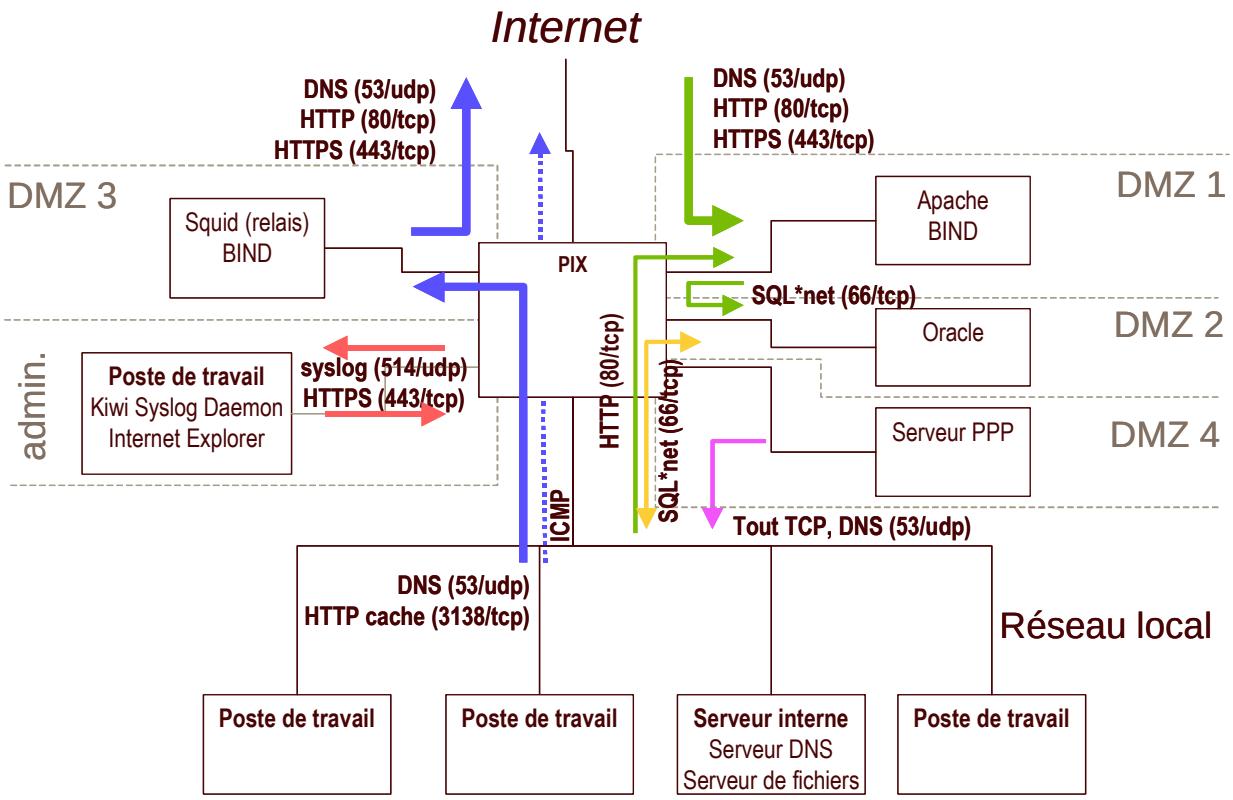
2ème partie

Exercice 1 *(3 pts)*

Donnez un exemple d'action concrète pour chacune des grandes fonctions d'un RSSI telles qu'elles vous ont été présentées :

1. Définition de la politique de sécurité
2. Analyse de risques
3. Sensibilisation et formation aux enjeux de la sécurité
4. Etude des moyens et préconisations
5. Audit et contrôle
6. Veille technologique et prospective

Exercice 2 *(4 pts)*



Question 1 *(3 pts)* : 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. Pour chaque fonction (ou à nouveau pour chaque DMZ si vous préférez), critiquez (avantages/inconvénients) la solution.

Question 2 *(1 pt)* : En ce qui concerne les flux entrants ou sortants du réseau local (depuis ou vers les DMZ ou Internet), indiquez les restrictions d'accès qu'il vous semblerait souhaitable d'appliquer.

Exercice 3 *(3 pts)*

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 choisis au hasard parmi les **36** symboles alphanumériques (en supposant que le système d'exploitation ne fait *pas* de distinction entre majuscules et minuscules).
   Exemple : `GB4F7BB`
2. Utilisation de 2 mots du dictionnaire français courant accolés ou éventuellement séparés ou suivis par des caractères spéciaux choisis parmi : `,;:!?.+-*/<>=`
   Exemples : `LUNE;MIEL` ou `ALLEZ-BLEUS!`
3. Utilisation de la première lettre d'une phrase comptant au moins douze mots. On fera aussi l'hypothèse qu'au plus deux signes de ponctuation (parmi 6 : `,;:!?.`) peuvent apparaître (n'importe où entre les douze mots) et qu'il est possible qu'au plus deux lettres soient en majuscules.
   Exemple : `Udlpld'upcamdm.` (1ère phrase ci-dessus)

Question 1 *(2 pts)* : 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 algébrique exacte la taille de l'espace considéré, mais essayez d'obtenir un ordre de grandeur *justifié* du nombre de mots de passe possibles (ou un minorant).

Question 2 *(1 pt)*: 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[1], suite à un vol de la forme chiffrée du mot de passe[2]. Considérez : un système Unix utilisant un chiffrement DES classique, un système Windows utilisant NT LM (DES) et un système utilisant MD5.

[1] Une attaque consistant à essayer systématiquement les mots d'un dictionnaire ou des combinaisons simples de ces mots entre eux ou avec des symboles courants.

[2] 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.).

Quelques information utiles :

- On pourra considérer qu'un lexique de français courant compte environ 4000 mots[3] (méthode 2).
- (*Pour simplifier, il est optionnel de considérer cette hypothèse.*) 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 (soit 20 mots au lieu de 4000), mais surtout qui ne représentent probablement 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[4]. Voici, sur une machine tout à fait banale (PII 266 MHz) les performances obtenues par un outil librement disponible :

```
# /home/ripper/john-1.6.36/run/john -test
Benchmarking: Traditional DES [64/64 BS MMX]... DONE
Many salts:     80230 c/s real, 80230 c/s virtual

Benchmarking: FreeBSD MD5 [32/32]... DONE
Raw:    644 c/s real, 644 c/s virtual

Benchmarking: NT LM DES [64/64 BS MMX]... DONE
Raw:    493030 c/s real[5], 492046 c/s virtual
```

[3] Le lexique Dubois-Buyse des mots français courants (enfants entre 0 et 16 ans) compte 3726 mots.

[4] La quasi-totalité des systèmes d'exploitation utilisent un « grain de sel » (*salt*) aléatoire pour ralentir les attaques par dictionnaire (c'est une valeur concaténée au mot de passe de l'utilisateur qui multiplie immédiatement le nombre de combinaisons à essayer pour une attaque par dictionnaire). Voir : crypt(3). Le temps nécessaire pour chiffrer et comparer un mot du dictionnaire à la valeur dérobée dépend bien sûr du type d'algorithme (DES, MD5, MD4, Blowfish, etc.), mais dépend aussi fortement de la longueur du « *salt* » (10 bits, 12 bits, ou plus).

[5] Pour votre information, il y a des cas où les machines Windows n'utilisent pas de « *salt* » avec NT LM (cf : note 4). Dans ces cas, expérimentalement, on atteint plus de 20 000 000 c/s sur cette machine…