INSA – 5° R.T.

Sujet d'examen
12 janvier 2006

Sécurité des systèmes informatiques

2ème partie

Exercice 1 *(3 points)*

Question 1 *(1 point)* : Quelles valeurs le programme C ci-dessous va-t'il afficher ? Pourquoi ?

```
#include <stdio.h>

void main() {
      char buffer [10];
      char *ptr;

      buffer[0] = 'A';
      buffer[1] = 'B';
      buffer[2] = 'C';
      buffer[3] = 'D';

      ptr = buffer + 2;
      *ptr = 'Z';

      printf("%c %c %c %c \n", buffer[0], buffer[1],
                              buffer[2], buffer[3]);
}
```

Question 2 *(2 points)* : Une société est spécialisée dans la vente (légale) de fichiers musicaux sur Internet. Les personnes souhaitant acheter ces fichiers doivent avoir préalablement ouvert un compte sur le site de la société. Lorsqu'un client souhaite télécharger une nouvelle chanson, il exécute via son navigateur un script faisant appel à la fonction `buy()` ci-dessous. Cette fonction prend en argument l'identifiant du client `nickname`, son mot de passe `password`, son nom `name` ainsi que le numéro de la chanson désirée `song_num`. La fonction `debit()` comptabilise les fichiers que le client a téléchargés, la fonction `send()` retourne le fichier sur le navigateur du client et la fonction `authenticate()` permet de vérifier que le mot de passe indiqué est correct. On suppose que ces 3 fonctions, qui ne sont pas présentées ici, sont correctement implémentées.

```
void buy(const char* nickname, const char* password,
         const char* name,     const int song_num) {
      if (authenticate(nickname, password) == 1) {
                log_and_send(name, song_num);
                log_and_debit(nickname);
}

void log_and_send(const char* name, const int song_num) {
      char msg[100]="";
      strcat(msg, "Download initiated for ");
      strcat(msg, name);
      strcat(msg, ".\n");
      printf(msg);
      send(song_num);
}
```

```
void log_and_debit(const char* nickname) {
      debit(nickname);
      printf("Charged 3euros.\n");
}
```

a) Quelle vulnérabilité est fréquemment rencontrée dans les programmes, en particulier en C ?
b) Décrire comment cette technique peut être appliquée dans le cas présent afin qu'un client puisse récupérer un fichier sans être débité du montant de son achat.

Exercice 2 *(3 points)*

On donne ci-après une description du virus CIH (aussi connu sous le nom de Tchernobyl en raison de sa date d'activation), apparu en 1998.
Le virus CIH infecte les fichiers exécutables Windows 32 bits au format PE, caractéristiques de Windows 95. D'une taille de 1003 octets dans sa version originale, il fragmente son code pour le placer dans les zones vides (ou contenant des instructions nulles) des fichiers. La taille du fichier infecté n'est donc pas modifiée.
Chaque 26 du mois (pour la version originale de CIH), le programme entre dans sa phase destructive qui comprend deux aspects. D'une part, le virus corrompt le BIOS en modifiant des données dans la mémoire *flash* (cette procédure ne fonctionnant qu'avec certains types de BIOS). CIH empêche ainsi l'ordinateur de redémarrer puisque le BIOS sert à initialiser et à gérer les entrées/sorties des périphériques. D'autre part, le virus écrase avec des données aléatoires les 2048 premiers secteurs (1 Mo) de tous les disques durs de la machine infectée. Ce faisant, le virus détruit des informations essentielles au bon fonctionnement de la machine infectée (notamment la table des partitions et la table d'allocation des fichiers, ainsi que, éventuellement, sa copie, si celle-ci se situe par hasard dans ces 2048 secteurs).

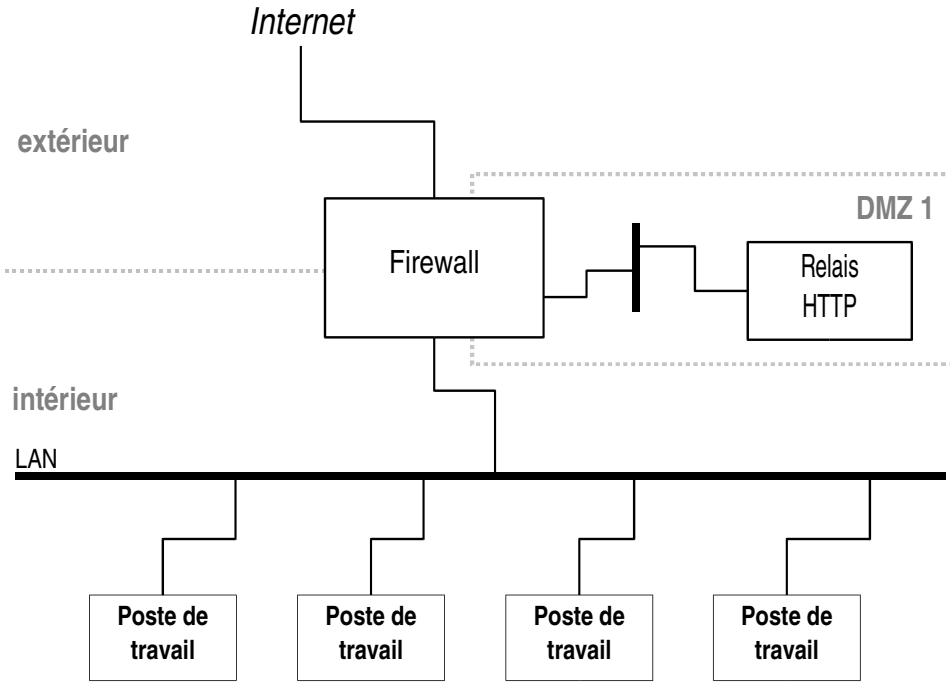
On considère ensuite Jacques Dupond, l'administrateur d'un parc informatique à cette période, constitué de machines utilisant le système Windows 95 (généralement les postes de travail) et de machines utilisant le système Windows NT (généralement pour les serveurs). La plupart des serveurs sont sauvegardés sur bandes magnétiques, sur une base hebdomadaire.

Répondez aux questions suivantes en justifiant votre réponse.

A) Est-il nécessaire que l'administrateur nettoie l'ensemble du parc informatique avec un antivirus puisque CIH ne s'attaque qu'à Windows 95/98 ?
B) On suppose que le virus a déjà agi sur la machine faisant office de serveur de messagerie. En démarrant, la machine affiche le message « Insérer une disquette de démarrage ». Quelles données le virus a-t'il corrompues ?
C) On suppose maintenant que le virus a également agi sur le serveur HTTP. En démarrant la machine, plus rien ne s'affiche à l'écran. Quelles données le virus a-t'il corrompues ?
D) Peut-on espérer récupérer des données du disque dur du serveur de messagerie ?
E) Comment remettre en fonctionnement le serveur Web ?
F) Est-il possible de se prémunir des virus s'attaquant au BIOS ?

Exercice 3 *(2 points)*

On considère le réseau décrit dans la figure ci-après. Le relais HTTP (*proxy*) écoute sur le port 8080. Quels sont les traitements que doivent effectuer le pare-feu et le *proxy* pour offrir un service de *proxy* HTTP transparent ?



Exercice 4 *(2 points)*

Les traces d'un serveur Web contiennent une série de lignes du type suivant (mentionnant l'adresse source, la date, la requête, le résultat et le nombre d'octets transférés) :

```
128.178.146.216 - - [24/Sep/2003:16:50:42 +0200] "GET /
default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXX%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%
u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00%
uu531b%u53ff%u0078%u0000%u00=a %HTTP/1.0" 404 209
```

1. De quoi peut-il bien s'agir ?
2. Comment faudrait-il configurer un système de détection d'intrusion pour détecter ces attaques ?
3. En supposant que le serveur Web se trouve derrière un proxy inverse, comment le *proxy* pourrait-il aider à éviter ces attaques ?
4. Laquelle de ces solutions, IDS ou *proxy* inverse, est-elle préférable ?