ÉCOLE POLYTECHNIQUE MONTRÉAL

INF4420/ 6420 – Sécurité informatique

Examen final - SOLUTIONS

8 décembre 2004

Profs. : *François-R Boyer & José M. Fernandez*

Directives : - La durée de l'examen est deux heures et demi
L'examen est **long**. Soyez bref, précis et travaillez efficacement.
- Toute documentation permise (quantité raisonnable)
- Calculatrice non programmable permise (mais ne sert à rien)
- 6 questions (15 sous-questions) à répondre pour un total possible de 40 points (les points sont entre crochets)

1. « Paranoïa » [4 points]

Le professeur de sécurité informatique est un peu paranoïaque (ça vient avec le métier!) et ne veut dévoiler les solutions de l'examen final à personne avant que l'examen ne soit fini. Par contre, pour montrer qu'il fait les choses correctement et pour s'assurer que ses questions sont possibles à répondre dans le temps requis, il veut pouvoir prouver au directeur qu'il a bel et bien fait le solutionnaire avant d'envoyer le questionnaire à l'imprimerie. Dites comment il peut le faire de manière informatique (pas de papier et autre), sans avoir à faire confiance au directeur ou au personnel de l'École, qui étant très mal payés, pourraient être tentés de faire une petite business « à côté » de ventes de solutions à l'avance …

Il va envoyer un message au directeur avant d'imprimer le questionnaire, avec preuve de date mise par le serveur de courriel à la réception. Ce message ne doit pas être lisible avant la fin de l'examen, mais il doit permettre de prouver que le solutionnaire existait à ce moment. Il peut contenir uniquement un hash cryptographique du solutionnaire et dans ce cas montrer le solutionnaire après l'examen permet de faire la vérification. Il pourrait aussi contenir une version encryptée dont la clé ne sera donnée qu'après l'examen.

2. Contenu des présentations [2 sous-questions ; 4 points].

(Veuillez donner des réponses courtes et précises).

QUESTIONS 2 POUR INF 4420 :

a) [2 pt] Donnez une méthode sécuritaire permettant à un ordinateur (ou puce) de s'authentifier à un autre. Cette méthode doit être immune entre autre contre le « replay » et contre l'analyse d'un enregistrement d'une grande quantité de communication d'authentification réussies, pour trouver comment se faire authentifier frauduleusement.

- *Preuve à connaissance nulle (« Zero-knowledge Proofs » ou ZKP)*
- *Des systèmes « challenge response » cryptographiques par logiciel ou par matériel*
- *Les générateurs de séquence à sens-unique (type « Secure ID »)*

b) [2 pt] À quoi sert un pot de miel (« Honeypot ») ?

C'est un leurre qui sert à attirer l'activité des hackers à un endroit particulier (p.ex. un serveur) de façon à pouvoir plus facilement les détecter, observer leurs méthodes et essayer de les retracer. C'est habituellement un serveur qu'on a « décoré » avec des services et des données fausses qui seraient susceptibles d'attirer l'attention des hackers.

QUESTION 2 POUR INF 6420 :

a) [2 pt] Comment la stéganographie pourrait être utile à un groupe terroriste?

Les terroristes pourrait se servir des techniques de stéganographie pour s'échanger des messages sur Internet (fichiers d'images ou MP3 sur des newsgroups, envoyées par courriel, etc.) de façon clandestine et secrète. Ainsi, ils éviteraient de se faire détecter et repérer par les agences de l'ordre ayant des mandats pour intercepter des communications sur Internet.

b) [2 pt] Nommez deux méthodes d'authentification biométriques parmi les plus utilisés présentement, ainsi que leurs principaux inconvénients.

Les méthodes les plus utilisées :

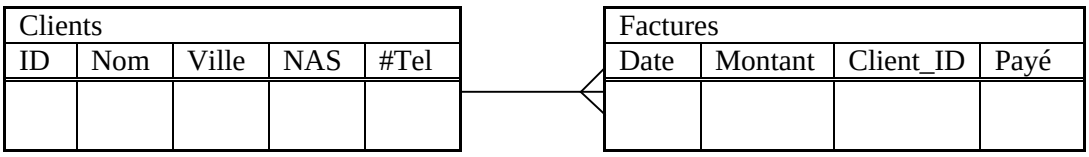
- *la reconnaissance d'empreinte digitale (p.ex. sur la souris),*
- *la reconnaissance de forme de la palme de la main (p.ex. au CEPSUM) et*
- *la reconnaissance de patrons de l'iris (dans l'œil).*

Désavantages principaux :

- *Beaucoup considèrent que leur utilisation constitue une atteinte au droit à la vie privée de l'utilisateur, car le système doit stocker des informations médicales de caractère privé.*
- *Il y existe encore aujourd'hui des taux relativement élevés d'erreur dans certaines de ces méthodologies.*
- *Ces systèmes ne sont pas toujours convivial (« user-friendly »).*
- *etc.*

3. Sécurité des bases de données [3 sous-questions ; 9 points]

Une entreprise veut se monter une base de données relationnelle pour la facturation des clients. Il y a deux tables en relation, une qui tient tous les clients, et l'autre qui tient toutes les factures, chaque client pouvant avoir plusieurs factures, tel qu'illustré :



Alice et Bob, employés de la compagnie, sont des gérants de comptes et doivent pouvoir facturer (envoyer une facture) et modifier toutes les données des clients (y compris en ajouter). Charlie et Ève s'occupent des comptes à recevoir et doivent pouvoir consulter les factures d'un client, y inscrire si elles ont été payées. Ils ne doivent pas avoir accès aux données privées (numéro d'assurance sociale et #Tel), mais doivent être capable de retrouver toutes les factures d'un client déterminé à partir de son nom ou adresse.

Rappel de la structure des commandes pertinentes en SQL : (`GRANT` | `REVOKE`) (`SELECT` | `UPDATE` | `INSERT`) `ON` (<table> | <view>) `TO` (<user> | <group>)

Le système de gestion de la base de données (SGBD) supporte l'authentification d'usagers via le système d'exploitation. Donc, tel qu'indiqué par la syntaxe SQL, il est possible d'attribuer des droits d'accès soit à des usagers individuels du système d'exploitation, soit à des groupes d'usagers définis dans le système d'exploitation. *(Vous pouvez présumer que les noms d'utilisateurs des personnes ci-haut sont simplement leur prénom)*

a) [2 pt] Quelles groupes d'utilisateurs devrait-on créer (et avec quels membres)?

Il y a essentiellement deux rôles d'identifiés dans le problème avec lesquels on associera un groupe d'utilisateurs :

- *les gérants de comptes – qui feront parti du groupe* `vente_group` *et contient les usagers* `alice` *et* `bob`
- *les personnes des comptes à recevoir– qui feront parti du groupe* `comptab_group` *et contient* `charlie` *et* `eve.`

b) [4 pt] Dites ce qu'il faut faire pour donner l'accès minimum requis aux bonnes personnes? (commandes SQL si possible; des explications claires sont aussi acceptables).

1) Pour permettre aux gérants de compte de pouvoir accéder et modifier des données des clients et de facturer :

- ```
  CREATE VIEW ventes_view
        SELECT id, nom, ville, nas, #Tel, date, montant, client_id
  ```
  ```

```
        FROM clients, factures
        WHERE id = client_id
```

- ```
  GRANT SELECT ON ventes_view TO ventes_group ;
  GRANT INSERT ON ventes_view TO ventes_group ;
  GRANT UPDATE ON ventes_view TO ventes_group ;
  ```

Pour permettre aux personnes des comptes à recevoir de

2) visualiser les données d'un client et des factures correspondantes :

- ```
  CREATE VIEW comptab_view
          SELECT id, nom, ville, date, montant, client_id, payé
          FROM clients, factures
          WHERE id = client_id
  ```
- ```
  GRANT SELECT ON comptab_view TO comptab_group
  ```

3) Inscrire qu'une facture a été payée

- ```
  CREATE VIEW comptab_paye_view SELECT paye FROM factures
  ```
- ```
  GRANT UPDATE ON comptab_paye_view TO comptab_group
  ```

c) [3 pt] Bob a peur d'Alice et réussit à faire accepter à son patron qu'elle devrait s'occuper seulement des clients habitant à Laval. Que faut-il faire pour restreindre son accès? (Les choses/commandes à faire après lui avoir donné l'accès en b)).

Plusieurs solutions sont possibles :

a) La solution « rapide » :

- ```
  CREATE VIEW ventes_hors_laval_view
          SELECT * FROM ventes_view WHERE ville <> "Laval" ;
  ```
- ```
  REVOKE SELECT ON ventes_hors_laval_view TO alice ;
  REVOKE INSERT ON ventes_hors_laval_view TO alice ;
  REVOKE UPDATE ON ventes_hors_laval_view TO alice ;
  ```

b) La solution « selon les règles de l'art »

- Retirer l'usager `alice` du groupe `ventes`
- Créer un groupe `ventes_laval_group` et y ajouter l'usager `alice`
- ```
  CREATE VIEW ventes_laval_view
          SELECT * FROM ventes_view WHERE ville = "Laval" ;
  ```
- ```
  GRANT SELECT ON ventes_lavel_view TO ventes_laval_group ;
  GRANT INSERT ON ventes_laval_view TO ventes_laval_group ;
  GRANT UPDATE ON ventes_laval_view TO ventes_laval_group ;
  ```

4. Gestion de la sécurité [2 sous-questions ; 7 points]

La personne s'occupant de la sécurité informatique d'une entreprise s'assure que toutes les mises à jour des systèmes (système d'exploitation, applications, anti-virus, etc.) sont toutes faites la journée même où elles sont disponibles.

a) [3 pt] Quels problèmes de sécurité principaux sont toujours présents (nommez-en trois types) ?

- *Les attaques venant de l'intérieur*
- *Les failles qui ne sont pas encore connues (vulnérabilités non-découvertes, nouveaux virus, etc.)*
- *Les erreurs de procédures des usagers*
- *Une politique de sécurité dont l'analyse de risques n'a pas identifié les risques les plus importants, et qui ne prévoit aucune contre-mesure procédurale ou technique pour les réduire.*
- *etc.*
  ```

b) [4 pt] Un exécutif de l'entreprise ayant à finir rapidement une soumission pour un contrat de plusieurs centaines de millions de dollars demande à son assistant de régler quelques détails pour le lendemain matin. L'assistant apporte la soumission chez lui, sur un ordinateur portatif, et envoie par courriel le fichier final au patron après avoir fait les modifications. Une compagnie concurrente intercepte le message et fait une soumission légèrement moins élevée, et obtient le contrat. Qui devrait-on blâmer dans cette affaire?

N'importe quelle de ces réponses est acceptable (en dépendant des hypothèses que vous faites) :

- *Les dirigeants et décideurs de la compagnie (y compris l'exécutif) car ils n'ont pas identifié ni correctement évaluer la menace (le compétiteur) et les impacts (pertes de revenus).*
- *Le responsable (administratif) de la sécurité informatique qui, les risques et impacts étant bien identifiés par ses patrons, n'a pas établi clairement dans la politique de sécurité que ce genre d'information ne devrait pas circuler via l'Internet.*
- *L'utilisateur (l'assistant) qui, malgré que la politique de sécurité indiquait clairement le contraire, a quand même envoyé des informations confidentielles par l'Internet.*
- *Le responsable (technique) de la sécurité informatique qui, connaissant les risques technologiques associés à l'utilisation d'Internet et sachant qu'il y a un besoin réel et légitime d'envoyer des données confidentielles par Internet, n'a pas soit a) déconseillé aux décideurs de permettre cette pratique ou b) prévu des contre-mesures (VPN, chiffrement, etc.) pour en réduire les risques.*

5. Réseau bien protégé [4 sous-questions ; 10 points]

Une moyenne entreprise, n'oeuvrant pas dans un domaine informatique mais en ayant besoin comme outil, veut un réseau local bien protégé de l'extérieur mais permettant tout de même l'accès web et la communication par courriel sur Internet. L'entreprise place donc un pare-feu (« firewall ») et un IDS à l'extérieur de celui-ci. Les adresses externes de l'entreprise attribuées par le fournisseur de service Internet (ISP) sont dans le sous-domaine 123.45.67.*. À l'interne, les adresses utilisées sont les adresses privées 192.168.*.*

a) [2 pt] Pourquoi placer le IDS entre l'Internet et le pare-feu? Quel est l'avantage principal ? Quels sont les désavantages (nommez-en deux) ?

Avantages :

- *Permet de voir toutes les attaques, incluant celles visant le pare-feu lui-même, et donc on obtient plus d'informations sur la menace.*

Désavantages (en nommer 2 est suffisant) :

- *Si l'IDS n'est pas bien protégé il peut être attaqué…*
- *La grosseur des logs peut être énorme, étant donné qu'il n'y a aucun filtrage.*
- *L'IDS pourrait être en train d'intercepter des paquets qui ne sont pas destinés à l'entreprise, ce qui pourrait la mettre dans une situation illégale.*

b) [3 pt] Le IDS utilisé, GNUIDS, est gratuit et à code source ouvert. Celui-ci envoie les alarmes à mesure qu'elles se produisent, par une deuxième carte réseau via le port par défaut qui est 3838, la première carte étant en mode espion (« promiscuous »). Dans cette entreprise, et pour sauver des coûts, la compagnie NETSecurity Enr. spécialisée en sécurité informatique a été engagé pour faire l'analyse des données de l'IDS. La première carte écoute sur le sous-réseau 123.45.67.* et a été trafiquée pour qu'elle ne puisse pas transmettre. La deuxième carte est aussi connectée sur le même sous-réseau, ce qui permet à NETSecurity Enr. de recevoir les alarmes via l'Internet. Malgré le fait que les alarmes soient chiffrées, en quoi cette architecture avantage un potentiel pirate informatique (« hacker ») qui voudrait attaquer la compagnie? Le pirate n'a a priori aucune information sur la configuration du réseau de l'entreprise.

Plusieurs réponses sont possibles:

- *Le hacker peut possiblement trouver le IDS, en faisant une recherche d'une machine répondant sur le port 3838 (« horizontal scan » sur le port 3838). Il peut ensuite voir si cet IDS a des failles et les utiliser pour faire ses attaques sans être détecté.*

- *Le hacker peut détecter la présence d'un IDS en observant que des attaques évidentes génèrent automatiquement du trafic chiffré à partir de l'adresse de l'IDS…*

c) [2 pt] Étant donné que l'entreprise n'a pas les compétences pour faire l'analyse des données de l'IDS, elle a le choix entre engager quelqu'un pour le faire sur place à 100k$/année, ou de laisser cette analyse externe pour 1k$/mois. Quel devrait être son choix et pourquoi?

La probabilité d'une attaque sur l'IDS causée par le fait qu'il peut répondre sur Internet est très faible. L'entreprise devrait donc laisser cette analyse à l'extérieur, à moins qu'une telle brèche puisse causer des dommages énormes.

d) [5 pt] La même entreprise décide d'implémenter une DMZ (zone démilitarisée). Faites le schéma de son réseau en y plaçant les éléments suivants :

Un LAN interne ; un serveur web Intranet ; un serveur de courriel Internet ; une base de données corporative ; un serveur mandataire (proxy) pour l'accès HTTP sur Internet ; la connexion Internet.

Sur votre schéma, indiquez des numéros de connections au(x) routeur(s), et donnez les tables de routage selon le format de l'exemple suivant (ou équivalent) :

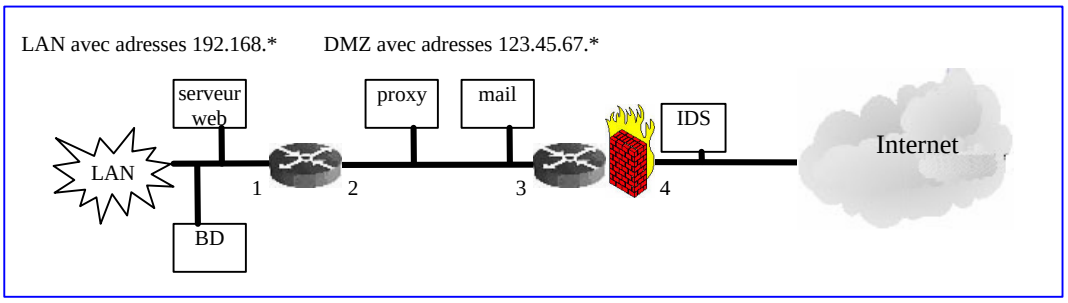
Sous-réseau	Router vers connexion
192.168.*.*	1
...	...

Routage :

- *Le routeur interne : 192.168.*.* ® 1 ; 123.45.67.* ® 2 ; autre ® rejeté*
- *Le routeur externe : 123.45.67.* ® 3 ; autre ® 4*

(le NAT pourrait aussi être placé sur l'autre routeur si aucun ordinateur de la DMZ a besoin d'ouvrir des connexions vers le LAN interne)

Schéma de réseau :



6. Pare-feu (firewall) [3 sous-questions ; 4 points]

a) [2 pt] Quelle est la différence fondamentale entre un pare-feu de réseau et un pare-feu sur un ordinateur client? (outre le fait qu'ils ne soient pas installés sur la même machine, bien sûr)

Un pare-feu sur un ordinateur client peut savoir de quelle application vient une requête de connexion et bloquer toutes les applications qui ne sont pas connus comme ayant besoin de l'accès réseau. Un pare-feu de réseau ne peut bloquer que sur ce qu'il y a d'écrit dans les paquets.

b) [1 pt] Quels sont les paramètres principaux qu'un pare-feu de réseau examine sur un paquet IP? (nommez-en au moins trois)

IP source et destination; port; protocole; flags TCP; contenu de la charge utile du paquet.

c) [1 pt] Dans un IDS, que peut-on inclure légalement dans un journal (« log ») et pourquoi ? (Qu'est-ce qu'on ne peut pas inclure?)

On ne peut pas inclure la charge utile du paquet puisqu'elle pourrait contenir des informations privées.