Université Paris XII
UFR de Sciences et Technologie
Département Informatique
Master deuxième année
2005/2006

EXAMEN SERE DE RATTRAPAGE

1 heure 30

Attention ! Chacun des quatre exercices devra être rédigé sur une copie double indépendante (correcteurs différents) en spécifiant bien l'exercice.

Les documents ne sont pas autorisés sauf pour le quatrième exercice.

Exercice 1.- (Maryline, 3 points, **sans support de cours**)

- 1^o) Quelles sont les difficultés d'utiliser la cryptographie symétrique pour protéger des échanges sur un réseau?

- 2^o) Est-il possible de regénérer une clé privée à partir de la clé publique complémentaire ? Expliquez.

- 3^o) Quels sont les services de sécurité rendus par le sous-protocole ESP ?

- 4^o) Comment les passerelles IPsec gèrent-elles la mise en place d'une association de sécurité? Quel est le protocole impliqué ? Expliquez.

- 5^o) Citez une technique permettant d'authentifier une entité (utilisateur, passerelle IPsec, serveur...)

Exercice 2.- (Olivier, 3 points, **sans support de cours**)

Donnez les différentes classes de techniques existantes pour le "traçage" d'attaques. Expliquez les différences générales, les avantages et les inconvénients de chacune d'entre elles.

Exercice 3.- (Alexander, 6 points, **sans support de cours**)

- 1^o) Expliquer et donner des exemples des actions de prévention et d'audit avant les attaques contre la sécurité des SI bancaires. Différencier dans ce contexte les menaces et les risques avec des exemples.

- 2^o) Dans le contexte de fiabilisation des services de transmission d'un opérateur de télécommunication, présenter les notions de **GTD** (*Garantie de Temps Déplacement*), **GTI** (*Garantie de Temps d'Intervention*) et **GTR** (*Garantie de Temps de Rétablissement du service*) en relation avec ses clients.

- 3^o) Caractériser les structures de réseau optique de transport et les nouveaux réseaux à deux couches du point de vue de la sécurité de fonctionnement.

Exercice 4.- (Patrick, 8 points, **avec documents sur les formats**)

On a récupéré avec Ethereal la trame suivante provenant d'une interface Ethernet. Analyser cette trame.

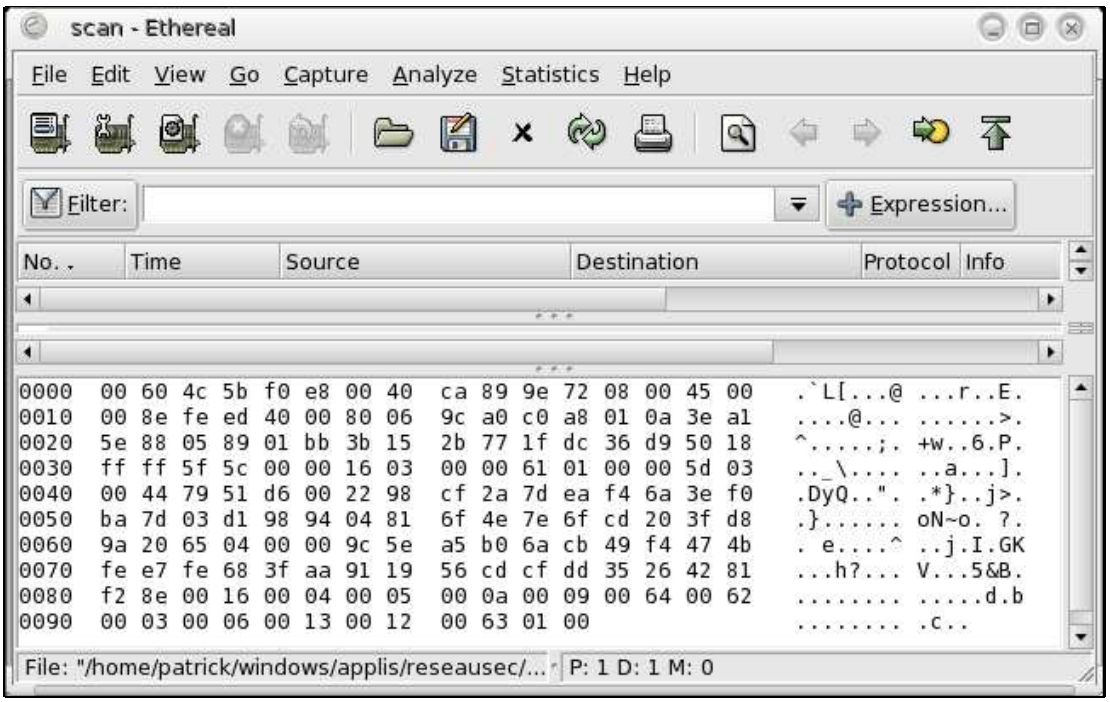

Figure 1: Trame Ethernet

On précisera en particulier le nombre d'octets de cette trame, on entourera l'adresse MAC de l'émetteur, son adresse IP, le port de destination, la version SSL utilisée et un des algorithmes de sécurité.