Université Paris XII
UFR de Sciences et Technologie
Département Informatique
Master deuxième année
2007/2008

EXAMEN SERE DE RATTRAPAGE

2 heures

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

Exercice 1.- (Maryline, 9 points, **support de cours autorisé**)

Voir pages séparées.

Exercice 2.- (Olivier, 3 points, **transparents du cours autorisés**)

On considère l'attaque "TCP SYN Flooding" vue en cours. Donnez sa catégorisation en fonction des critères (taxonomie) généralement utilisés pour classer les attaques de dénis de service. Expliquez vos choix.

Exercice 3.- (Patrick, 9 points, **avec documents sur les formats**)

- 1^o) Expliquer comment on peut récupérer des informations confidentielles en analysant les trames et quelles sont les mesures de sécurité qui peuvent être prises pour contrer ceci.

- 2^o) On a récupéré avec Ethereal la trame de la figure 1 provenant d'une interface Ethernet. Analyser cette trame en commentant **tous** les octets.

Vous encadrerez en particulier vos commentaires concernant le nombre d'octets total de la trame, celui de chacun des en-têtes, l'adresse MAC de l'expéditeur, la longueur du paquet IP, le TTL, l'adresse IP de l'expditeur, le port de destination et la longueur de la fenêtre TCP, le nombre de fragments SSL, leur nature et le nom de l'agorithme de sécurité utilisé.

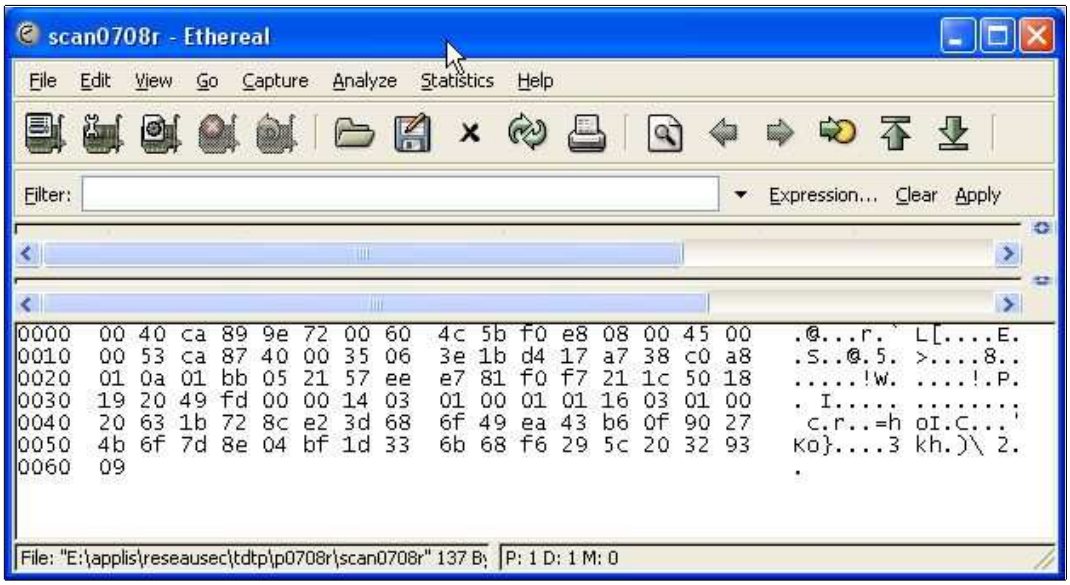

Figure 1: Trame Ethernet