Université Paris Est Créteil
IUT de Sénart-Fontainebleau
Département Informatique
Licence BDISe
2009/2010

Premier partiel SRA

2 heures

Exercice 1.- (**Analyse de trame**)

Le responsable d'une entreprise ultra-sensible, dont les postes informatique sont tous sur le même réseau local Ethernet avec adresses IP données par DHCP, a récupéré avec Wireshark la trame de la figure 1. Il veut déterminer quel poste l'a envoyé ou reçu et à qui elle est adressée (ou d'où elle provient).

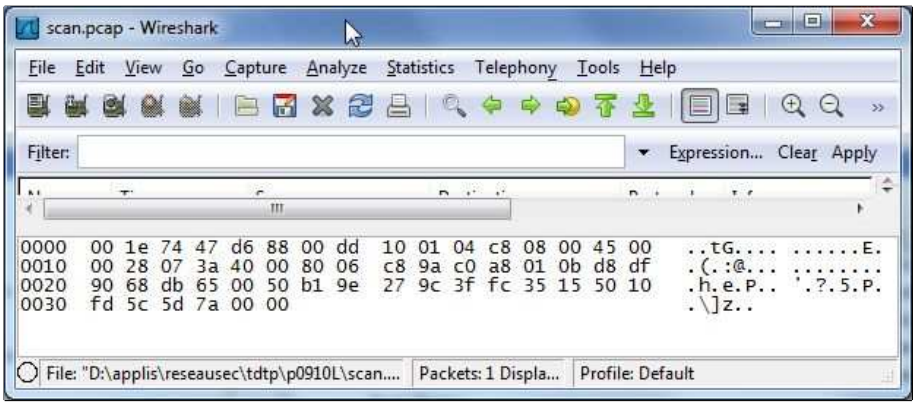

Figure 1: Trame Ethernet

- 1^o) Analyser cette trame en commentant **tous** les octets.

- 2^o) Donnez les détails du calcul de vérification de la première somme de contrôle.

- 3^o) Quels sont les deux données à remettre au responsable ? Justifiez votre choix et expliquez au responsable ce qu'il doit en faire.

[(Hors partiel) Le site concerné est-il compromettant ?]

Exercice 2.- (**Iptables**)

Le même responsable veut que vous configuriez un poste sous Linux pour que celui-ci n'accepte que les paquets provenant de l'hôte d'adresse IP 209.85.229.106 (correspondant au site délocalisé de la société) ainsi que du service de mail (pop3 de port 110) et qu'il ne permette d'envoyer que les paquets destinés à cette même adresse IP et au service de mail (smtp de port 25).

- 1^o) Écrire les commandes *iptables* correspondant à ces *desiderata*.

- 2^o) Améliorez votre réponse en critiquant positivement les *desiderata* et en suggérant des améliorations (sans écrire les commandes correspondantes).