TP1-1 : Analyse de trames
M1-DNR2I

Gaétan Richard

2 janvier 2012

Dans ce TP, nous allons procéder à l'analyse de trames. Pour cela, nous allons utiliser le logiciel **wireshark** qui permet d'afficher de façon lisible le contenu des trames.

Télécharger la capture disponible à l'adresse `http://richardg.users.greyc.fr/tmp/Capture.cap`.

1 Un paquet DNS

Dans un premier temps, obersevez le paquet numéro 99.

Question 1 *Quelles sont les adresses MAC des machines en jeu ?*

Question 2 *Quelles sont les adresses IPv4 des machines impliqués dans ce paquet ?*

Question 3 *Trouver le paquet émis en réponse. Oberservez la valeur du champ `hop limit`. Déduisez-en combien de routeurs sont traversés.*

Question 4 *Indiquer quels ports sont mis en jeu dans cet échange. Le traffic est-il de type UDP ou TCP ?*

2 Un échange HTTP

On va maintenant se concentrer sur le paquet numéro 17.

Question 5 *Quels sont les adresses MAC des machines mises en jeu ? Comparer avec celles obtenues précédemment.*

Question 6 *Même question avec les adresses IPv4.*

Question 7 *Quel est le type (TCP / UDP) de ce paquet ? Quels sont les ports impliqués ?*

Question 8 *Listez les différents paquets appartenant à cette connection. Oberservez les numéro de séquence et ceux des acquittements et dessinez les 10 premiers échanges.*

3 Autres trafics

Question 9 *Trouver un paquet ICMP. Quelle est alors la chaîne d'inclusion des protocoles ?*

Question 10 *Trouver un paquet https. Que pouvez-vous dire du contenu de ce paquet ?*

Question 11 *Expliquer alors pourquoi il ne faut pas rentrer son mot de passe sur une page http.*

4 Faites le vous-même

La capture qui vous a été fournie a été réalisée à l'aide du logiciel **tcpdump**. Pour des raisons de sécurité, cette commande n'est normalement accessible qu'au super-utilisateur. Cependant, pour ce TP, les administrateurs vous ont exceptionnellement autorisé à capturer les paquets par l'intermédiaire de la commande **sudo netdump-tp**.

Pour vérifier que cela est la cas et avant toute utilisation de **sudo**, utiliser la commande **sudo -l**

Lancer cette commande et effectuer les actions suivantes :

- Consultation d'une page web en http
- Consultation d'une page web en https
- Lancer la commande **ping mike**
- ...

(si vous n'avez pas le temps de tout faire en une fois, vous pouvez faire plusieurs captures successives).

Question 12 *Retrouvez la trace de ces opérations sur la capture obtenue.*