Université Paris Diderot
M1 informatique
Protocoles réseaux 2011-2012

TP: Couche liaison

1 Mise en oeuvre

Wireshark est un "packet sniffer" qui enregistre les messages envoyés et reçus par votre ordinateur. Il permet aussi d'analyser les paquets. Lancer Wireshark pour écouter toutes les communications de l'interface `eth0`, lancer par X11 une connection sécurisée à distance `ssh <une autre machine>` arrêter la capture. La fenêtre Wireshark comprend une liste de paquets capturés, une fenêtre dans lequel les paquets sont analysés et une fenêtre contenant les données brutes du paquet.

Reperer dans la liste des paquets capturés un paquet dont le protocole correspond à ssh et selectionner ce paquet. Dans la fenêtre où Wireshrak analyse le paquet on trouve des informations sur la frame EThernet correspondante, sur le datagramme IP correspondant. Si le paquet a été transporté via TCP ou UDP on trouve aussi des détails concernant ces protocoles et enfin des détails portant sur le protocole de plus haut niveau pour lequel le paquet a été envoyé /recu (dans notre exemple Ethernet, IP, TCP, SSH). Repérer ces différents éléments (les informations peuvent être étendues par l'onglet en triangle).

Dans la partie correspondant aux données brutes , en cliquant sur les données on obtient la correspondance avec une valeur dans l'analyse faite plus haut (par exemple dans un des paquets correspondant à ssh vous devez retrouver dans les données `ssh-rsa,ssh-dss` qui correspond à la valeur de `server_host_key_algorithm` pour le protocole `ssh` Ici on s'interresse aux protocoles de la couche liaison. On va demander à Wireshark de n'afficher que ceux la. Dans le menu `Analyse` dans `EnabledProtocols` retirer IPv4 et IPv6. L'affichage donne alors uniquement des infos sur les protocoles de la ouche liaison.

Dans le menu `file`, `Print` permet de sauvegarder le contenu d'une trame dans un fichier.

2 Ce qu'il faut rendre

Dans les 2 sections suivantes vous aller devoir chercher des paquets particuliers et on vous posera des questions dessus. Vous devrez déposer sur Didel à la fin du TP les fichiers contenant les paquets que vous avez analysés et les réponses aux questions.

3 Ethernet

Vider le cache de votre navigateur. Lancer une capture par Wireshark et faites une requête sur votre navigateur `www.liafa.jussieu.fr`. Trouver le premier paquet contenant le message `HTTP GET` envoyé de votre ordinateur et le premier paquet de réponse de `liafa`.

Répondez aux questions suivantes à partir de l'analyse du paquet correspondant à `HTTP GET`

1. Ou se trouve l'adresse ethernet de votre ordinateur dans le paquet? Quelle est l'adresse Ethernet de votre ordinateur ?
2. Ou se trouve l'adresse ethernet de destination dans le paquet? Quelle est l'adresse Ethernet de destination ? Est ce l'adresse ethernet de `www.liafa.jussieu.fr`? A quoi correspond l'adresse ethernet de destination?
3. Quelle est la valeur de "type field" de la frame ethernet ?
4. Combien y a t il de bytes après le "type field" et le mot GET? A quoi sont-ils utilisés?

Répondez aux questions suivantes à partir de l'analyse du paquet correspondant à la réponse

1. Quelle est l'adresse Ethernet de la source?
2. Quelle est l'adresse Ethernet de destination ?

4 ARP

Le protocole `ARP` maintient une table qui fait la correspondance entre les adresses IP et les adresses Ethernet. Vous pouvez visulaliser cette table sur votre ordinateur par la commande `arp`-a+. Dans Wirechark, vous pouvez filtrer les paquets pour ne voir que ceux qui concernent le protocole ARP par les filtres (il suffit de tapper `ARP` dans la boite `Filter`). Lancer la capture par Whireshrak en filtrant pour ARP.

Repérer dans la table ARP une machine de la salle qui n'a pas sa correspondance. Faites un `ssh` sur cette machine. Une fois le `ssh` réussi, consultez la table `ARP` et vérifier que la machine y est maintenant présente. Arreter la capture. Chercher dans les paquets pour `ARP` les 2 messages correspondant à l'acquisition de l'adresse Mac de cette machine.

Répondez aux questions suivantes à partir de l'analyse du paquet "who has...."

1. Quelle est l'adresse Ethernet de la source?
2. Quelle est l'adresse Ethernet de destination ?

3. Quelle est la valeur de "type field" de la frame ethernet ? A quoi sert le "field type"?

4. Dans les données correspondants au protocole ARP quelle est la valeur de `opocode`?

5. Ce message contient l'adresse IP de l'émetteur?

6. Dans ce message où se trouve l'adresse IP pour laquelle on veut connaitre l'adresse MAC?

Répondez aux questions suivantes à partir de l'analyse du paquet de réponse

1. Quelle est l'adresse Ethernet de la source?

2. Quelle est l'adresse Ethernet de destination ?

3. Quelle est la valeur de "type field" de la frame Ethernet ?

4. Dans les données correspondants au protocole ARP quelle est la valeur de `opocode`? à quoi sert le `opcode`?

5. Ce message contient-il les adresses IP de l'émetteur et du récepteur?

Faites une capture assez longue des paquets correspondants à ARP. Mis à part les paquets correspondant à des demandes explicitent de votre machine (comme ceux causés par le ssh précédent) y a t il d'autre paquets à ARP. Quels sont ils ? A quoi peuvent-ils correspondre?