Module : Applications client/serveur

Classe : 2LT

Commandes TCP/IP et analyse de la suite protocolaire TCP/IP sur Wireshark

Objectif

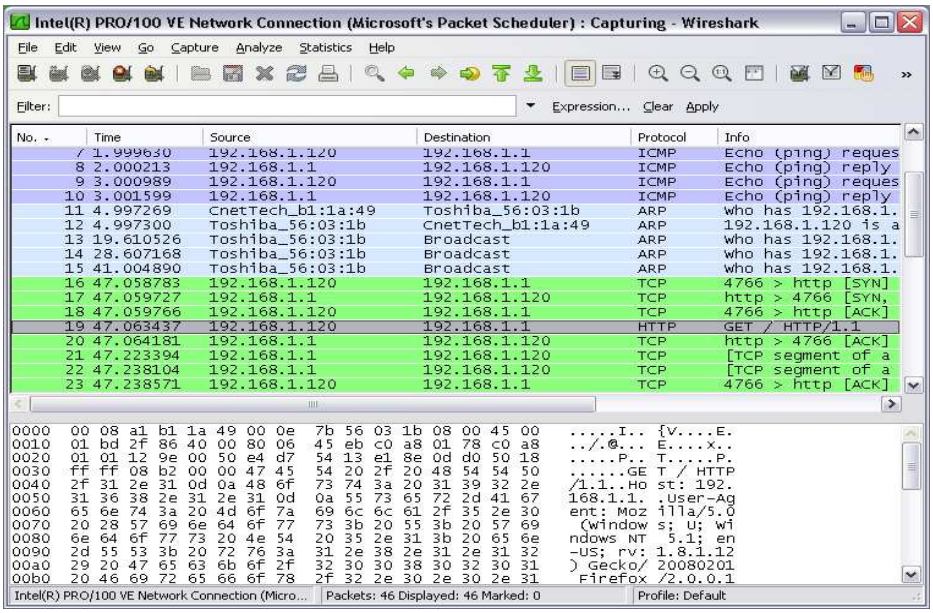
Le but de cette partie du TP est d'analyser des trames Ethernet en vue de comprendre le fonctionnement de quelques protocoles standard de la pile TCP/IP. Les analyseurs de trames Wireshark
Ce TP fera l'objet d'un compte rendu comportant la démarche suivie à chaque étape, les résultats obtenus et leurs interprétations de façon claire et précise.

1. Présentation de l'analyseur de trafic Wireshark

Ethereal est un analyseur de trafic réseau ou "packet sniffer", utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation,etc. C'est un analyseur multi-plateformes, fonctionnel sous Windows, Mac OS X, Linux, Solaris, ainsi que sous FreeBSD. Une récente version d'Ethereal portant le nom de Wireshrak bien d'apparaître. Pour des raisons de compatibilité avec le système Linux installé sur les machines, nous nous contentons d'utiliser Ethereal. Le travail demandé dans ce TP pourra être réalisé de la même façon en utilisant l'analyseur Wireshark.
Ethereal permet d'examiner les données qui transitent sur un réseau ou capturées dans un fichier sur un disque. Il est possible de visualiser le contenu des paquets transmis en direct et en détail. Il permet également le filtrage pour n'afficher que des paquets venant d'une destination ou un protocole par exemple. Plusieurs protocoles sont supportés par Ethereal tels que HTTP, TCP, DNS, FTP, MSN(P), IRC, AIM, ICQ, et POP, qu'il peut visualiser et décoder à partir des paquets capturés.

2. Capture de paquet avec Wireshark

Pour lancer une capture, il faut aller dans le menu Capture / Interface (ou cliquer sur le bouton correspondant). Une nouvelle fenêtre comportant la liste des interfaces réseaux disponibles va apparaître. Il est possible de configurer certaines options de la capture en choisissant le bouton «Options» de l'interface en question. Ces options permettent le filtrage de capture affin de ne capturer que les paquets correspondant aux choix réalisés.
Le filtre de capture dois être spécifié dans le champ "Capture Filter" ou bien cliquez sur le bouton "Capture Filter" pour choisir un des filtres existants ou définir votre filtre et pouvoir le réutiliser pour des captures ultérieures. Ethereal utilise la librairie Libpcap ou Winpcap pour la capture. La syntaxe de filtre de capture utilisé est la même utilisée par ces librairies et est identique à celle de la commande TCPdump.



Il est aussi possible de filtrer les paquets après capture en utilisant le filtre d'affichage.
Après le choix de l'interface et la définition du filtre s'il existe, lancez la capture des paquets en cliquant sur Start.

3. Analyse de la capture

Après capture, la liste des paquets capturés à travers le filtre peuvent être consultée à partir de la fenêtre principale. Pour analyser le contenu de l'un de ces paquets, il faut d'abord le sélectionner dans la liste des paquets. Les informations intéressantes sont disponibles dans la fenêtre des détails. Cette fenêtre affiche une ligne (extensible) par couche réseau. La capture d'un traffic http de retrouver les couches suivantes:

- couche 2 (Ethernet - MAC)
- couche 3 (Internet Protocol - IP)
- couche 4 (Transmission control protocol - TCP)
- couche 7 (HyperText Transfert Protocol - HTTP)

Il suffit de cliquer sur la ligne en question pour avoir plus de détail.

4. Filtrage après capture

Il est aussi possible de capturer la totalité d'un flux, puis, par la suite, effectuer un filtrage pour n'avoir qu'une partie précise. Voire annexe pour la syntaxe de filtrage.

5. Travail demandé :

A. <u>Questions théoriques</u>

1) Expliquer le principe de capture de trames dans un réseau Ethernet.
2) Que peut-on dire sur la sécurité d'un réseau Ethernet.
3) Etant donné le réseau auquel vous êtes connecté. En utilisant le logiciel de capture de trame sur une machine A, est ce que vous êtes capable d'observer une conversation entre deux machines B et C ?
4) Dans quelles conditions votre machine sera capable de visualiser le trafic émanant d'une autre machine sur le même réseau.

B. Analyse de trafic ARP

1) Expliquez dans quelle condition votre machine génère t'elle une trame ARP ?
2) Choisir une adresse IP destination et faire en sorte que votre machine émettra une requête ARP dès lors qu'elle commencera à communiquer avec cette dernière.
3) Créer un filtre de façon à ce que votre analyseur de trames ne captera que les datagrammes ARP.
4) Démarrer la capture, lancer la commande « ping » vers l'adresse IP choisie, puis arrêter la capture.
5) Vérifier que vous avez capturé les bonnes trames (la requête ARP émise/reçue depuis/vers votre machine). Expliquer votre démarche.
6) Expliquer comment votre analyseur arrive à détecter que les trames capturées encapsulent des datagrammes ARP (indiquer le champ utilisé et sa valeur).
7) Déterminer l'adresse Ethernet de votre machine à partir des trames capturées.
8) Vers quelle adresse Ethernet la requête ARP a été envoyée. Interpréter cette valeur.
9) Analyser le datagramme ARP de réponse et expliquer comment votre machine arrive à déterminer l'adresse MAC relative à votre correspondant.
10) Lancer de nouveau l'analyseur de paquets pour qu'il n'affiche que les paquets ARP.
11) Choisir une autre machine et changer son adresse IP avec la même adresse IP que celle attribué à votre machine. Utiliser la commande « arping » pour envoyer des paquets ARP reply (avec les adresses IP source et destination la même adresse utilisé par les deux machines). Observer les paquets capturés et expliquer.

C. Analyse de trafic ICMP et HTTP

1) Créer un filtre de façon à ce que votre analyseur de trames ne capte que les datagrammes ICMP.
2) Démarrer la capture, lancer la commande « ping » vers une adresse IP choisie. Arrêter la capture.
3) Retrouver dans le buffer de capture les trames générées par la commande « ping ».
4) Quel type de message ICMP (en émission et en réception) a été généré par la commande ping ? Indiquer les champs spécifiques qui vous ont permis de déduire cette valeur.
5) En combien de paquets IP a été décomposée la requête émise ? Conclure.
6) Quel est le nombre de trames générées par la commande « ping » ? Montrer qu'il est cohérent avec ce qui a été affiché lors de l'exécution de la commande.
7) Expliquer comment votre analyseur arrive à détecter qu'il s'agit d'un message ICMP encapsulé dans un paquet IP, qui est lui aussi encapsulé dans une trame Ethernet.
8) Interpréter les valeurs des champs IP suivants: FLAG, Offset, et identification relatives aux requêtes ICMP.
9) Quelle est la valeur TTL des paquets relatifs aux requêtes ICMP ? Conclure.