Projet Programmation

Analyseur de Protocoles Réseau ‘Offline’

Présentation

L’objectif de ce projet est de programmer un analyseur de protocoles réseau ‘offline’. Il prend en entrée un fichier trace contenant les octets capturés préalablement sur un réseau Ethernet. Votre programme peut s’exécuter dans une fenêtre de commande (de type terminal) ou s’afficher dans une interface graphique.

La liste des protocoles que votre analyseur sera en mesure de comprendre sont les suivants :

- Couche 2: Ethernet
- Couche 3: IP
- Couche 4: UDP
- Couche 7: DNS et DHCP

Dans le cas de DNS, votre analyseur décodera les six (6) champs d’entête ainsi que les sections Questions, Réponses, Autorités et Additionnelles. Vous décoderez toutes les informations y compris les noms compressés.

Dans le cas de DHCP, votre analyseur décodera les huit (8) types de messages et l’ensemble des options définies pour chaque type de message.

A chaque exécution, le résultat de votre analyseur doit être sauvegardé dans un ficher texte formaté de façon à faciliter sa lecture.

Notation

- Ce projet sera réalisé en binôme.
- Vous êtes libres de choisir le langage de programmation.
- Date de soumission : **Vendredi 10 décembre 23:59:00**.
- Documents à soumettre :
    1. Une **archive zip** à soumettre sur le Moodle de l’UE :
        a. votre **code source**,
        b. un **fichier binaire** ou **makefile** pour lancer l’exécution de votre analyseur,
        c. un **fichier readme** qui décrit la structure de votre code,
        d. un **fichier howto** qui explique comment installer et lancer votre programme.

2. Une **presentation vidéo préenregistrée de 10 minutes** postée sur Youtube : Lien d'ajout de vidéo. (Votre vidéo sera ajouté à une liste de lecture privée). Ne cliquer pas sur “cette vidéo a été conçue pour les enfants”.

   Dans cette vidéo, vous présenterez :

   1. un **aperçu complet** de votre projet,
   2. une description de **vos choix, réalisations et contributions personnelles**,
   3. une **démonstration** de votre analyseur en action.

Instructions à suivre

1/ En entrée

Votre programme prend en entrée un fichier trace (format texte) contenant les octets ‘bruts’, tels que capturés sur le réseau. Ces octets sont présentés comme dans Wireshark dans le panneau ‘Octets capturés’. Ce fichier pourra contenir plusieurs trames Ethernet à la suite (sans préambule ni champ FCS) :

- Chaque octet est codé par deux chiffres hexadécimaux.
- Chaque octet est délimité par un espace.
- Chaque ligne commence par l’offset du premier octet situé à la suite sur la même ligne. L’offset décrit la positon de cet octet dans la trace.
- Chaque nouvelle trame commence avec un offset de 0 et l’offset est séparé d’un espace des octets capturés situés à la suite.
- L’offset est codé sur plus de deux chiffres hexadécimaux.
- Les caractères hexadécimaux peuvent être des majuscules ou minuscules.
- Il n’y a pas de limite concernant la longueur ou le nombre d’octets présents sur chaque ligne.
- Si des valeurs textuelles sont données en fin de ligne, elles doivent être ignorées, y compris si ces valeurs sont des chiffres hexadécimaux.
- Les lignes de texte situées entre les traces ou entrelacées entre les lignes d’octets capturés doivent être ignorées.
- Les lignes d’octets qui ne débutent pas un offset valide doivent être ignorées.
- Toute ligne incomplète doit être identifiée et soulever une erreur indiquant la position de la ligne en erreur.

2/ En sortie

Le résultat de votre programme doit être similaire aux informations produites par Wireshark dans le panneau ‘analyse des entêtes de message’.

Votre analyseur doit retourner la liste des entêtes pour chaque trame contenue dans le fichier trace en précisant :

- Pour chaque entête de protocole, la liste des champs d'entête et la valeur de ces champs donnée en hexadécimal et quand nécessaire convertie en décimal.

  Exemple: Champ IP Longueur totale : 0x05C8 (1500 octets).

- Pour les champs d'entête contenant un code, votre analyseur donnera la signification de ce code.

  Exemple: Champ Ethernet Type : 0x0806 (ARP).

- Les entêtes de protocole seront présentés sous forme arborescente : chaque entête pourra être développée (réduite) pour révéler (masquer) les champs et valeurs de l'entête. Sinon, l'utilisation d'indentations permettra de distinguer les champs et leur valeur selon l'entête de protocole à laquelle ils appartiennent.

Le résultat de votre analyseur sera sauvegardé dans un fichier texte formaté de façon à faciliter sa lecture.