heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

iICT

Labo TIB

Wireshark

Objectifs d'apprentissage

1. Savoir utiliser les fonctions de base de Wireshark : capture de paquets et analyse de protocoles.
2. Savoir dessiner un diagramme en flèches.
3. Savoir utiliser Wireshark pour analyser du trafic de réseau.

Contenu

Ce premier laboratoire vous permet de vous familiariser avec l'analyser de protocoles Wireshark.

1. Wireshark pour la capture et l'analyse de trafic de réseau
2. Diagramme en flèches pour illustrer le fonctionnement d'un protocole
3. Analyses de trafic réseau.

Rapport à fournir

Un rapport de **2 pages au maximum** avec les éléments suivants :

1. Nom du laboratoire, noms des étudiants, date du laboratoire
2. **Objectif 1 : Wireshark et diagramme en flèches**
    a. Rappel de l'objectif d'apprentissage et du critère de succès.
    b. Diagramme en flèche qui documente la capture Wireshark de l'échange SSL avec https://www.gmail.com.
3. **Objectif 2 : image cachée**
    a. Rappel de l'objectif d'apprentissage et du critère de succès.
    b. L'image cachée.
    c. Explication comment trouver l'image, à l'aide de Wireshark.
4. **Objectif 3 : analyse forensique**
    a. Rappel de l'objectif d'apprentissage et du critère de succès.
    b. Réponses aux questions :
        i. Quelle est l'adresse email d'Ann ?
        ii. Quelle est l'adresse email de l'amant secret d'Ann ?
        iii. Quelles deux choses Ann demande-elle à son amant d'apporter ?
5. **Objectif 4 : analyse forensique à l'aide d'outils**
    a. Réponses aux questions :
        i. Quel est le mot de passe d'Anne ?
        ii. En quelle ville est le rendez-vous (nécessite l'extraction de l'attachement du mail) ?
6. Auto-évaluation : est-ce que vous avez atteint les objectifs d'apprentissage de la page 1 ?

Délai

Le fichier PDF du rapport doit être envoyé à l'aide du formulaire
http://iict-space.heig-vd.ch/jer/rendu-labo-tib/
avant le début du prochain laboratoire.

1 Introduction

L'objectif premier du cours Téléinformatique de base est de vous permettre de comprendre le fonctionnement des réseaux informatique. Que se passe-t-il quand on envoie des données à travers un réseau complexe ? Vous allez voir que beaucoup de mécanismes comme DHCP, DNS, le routage, les retransmissions, etc., sont nécessaire pour rendre ça possible.

Dans ce laboratoire, vous allez apprendre à utiliser un outil précieux : Wireshark. Wireshark est un analyseur de protocoles. Il capture les données envoyées sur le réseau, les analyse et les affiche d'une manière structurée. Ainsi il nous permet de comprendre ce qui se passe sur le réseau. Wireshark est précieux pour comprendre le fonctionnement de protocoles et pour le dépannage.

2 Matériel

Nous allons utiliser une configuration très simple : un PC Linux connecté à Internet, avec Wireshark installé.

3 Exercices

Objectif 1 : Wireshark

L'objectif de cette partie et d'apprendre à effectuer une capture Wireshark simple et de documenter les résultats.

L'objectif est atteint si vous savez :

- effectuer une capture Wireshark
- utiliser un filtre d'affichage
- réaliser un diagramme en flèche.

Pour commencer à utiliser Wireshark, lisez le document « Annexe – Wireshark ».

Puis, effectuez une capture Wireshark pendant que vous exécutez la commande

```
ping www.heig-vd.ch
```

dans un terminal.

Utilisez un filtre d'affichage « icmp », analysez les paquets capturés et complétez le diagramme en flèches ci-dessous.

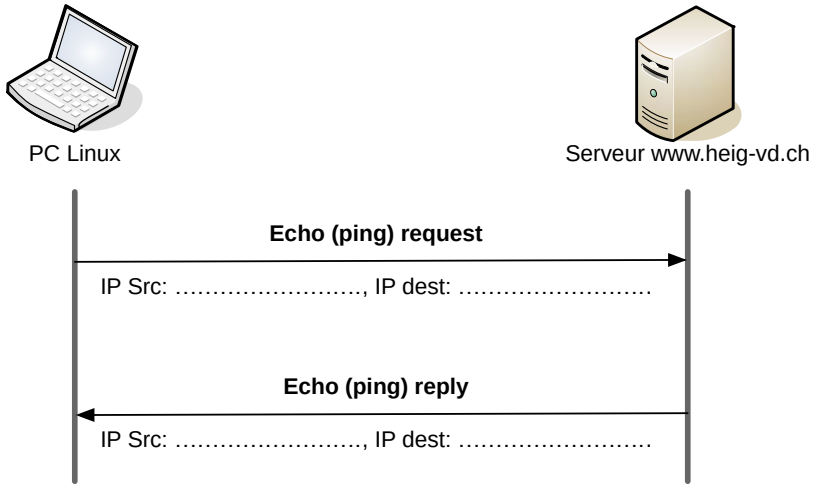

Figure 1: Diagramme en flèches à compléter

Diagramme en flèches

Les diagrammes en flèches montrent de manière claire les paquets échangés entre différents nœuds. Ils permettent ainsi d'illustrer le fonctionnement d'un protocole.

Dans cet exercice, vous devez dessiner un diagramme en flèches selon une capture Wireshark.

Vous pouvez utiliser par exemple les logiciels suivants pour dessiner un diagramme en flèches :

- Microsoft Visio (Windows)
- Omnigraffle (Mac)
- Microsoft Powerpoint
- OpenOffice/LibreOffice Drawing
- Dia (open source, multi-plateforme, http://projects.gnome.org/dia/)

Effectuez une capture Wireshark, avec le filtre d'affichage « ssl ». SSL est un protocole de sécurité qui permet de crypter des connexions. Une connexion HTTP transmet les informations en clair, une connexion HTTPS chiffre les données.

Pendant la capture Wireshark, connectez-vous au site https://www.gmail.com (https, donc crypté).

Puis, dessinez un diagramme en flèches pour les 6 premiers paquets. Indiquez les informations suivantes :

- Adresses IP source et destination
- Type du paquet (par exemple « Client Hello »)
- L'instant d'envoi, en secondes (temps affiché par Wirkeshark)

Objectif 2 : trouver l'image cachée

L'objectif de cette partie est d'apprendre à utiliser Wireshark pour analyser le trafic réseau.

L'objectif est atteint si vous trouvez les indices et l'image cachés.

Wireshark peut aussi être utile dans des analyses de sécurité. Votre tâche est maintenant de trouver une image cachée.

Voici les instructions :

1. Lancez Wireshark
2. Visitez le site Web http://iict-space.heig-vd.ch/jer/wschallenge/
3. Choisissez un filtre d'affichage pour montrer le trafic Web.
4. Analysez le contenu des paquets.
5. Est-ce que vous trouvez l'indice et l'image ?

Objectif 3 : analyse forensique

L'objectif de cette partie est d'apprendre à utiliser des fonctions avancées (conversations, flux) de Wireshark.

L'objectif est atteint si vous arrivez à effectuer l'analyse ci-dessous et à répondre aux questions.

Wireshark ne permet pas seulement d'effectuer des captures en temps réel, mais aussi d'enregistrer une capture dans un fichier .pcap et de l'utiliser après-coup.

Votre tâche est d'analyser un email envoyé d'Ann à son amant secret.

Voici les instructions :

1. Lisez les instructions sur la page https://www.hacking-lab.com/cases/3029-network-forensic-challenge/index.html
2. Téléchargez le fichier PCAP evidence02.pcap de la page : http://iict-space.heig-vd.ch/jer/enseignements/tib/labos/
3. Ouvrez le fichier PCAP avec Wireshark
4. Utilisez comme filtre d'affichage « SMTP » (le protocole pour l'échange d'emails).
5. Utilisez le menu « Statistics » → « Conversations » pour afficher les connexions.
6. Sélectionnez les connexions TCP.
7. Puis analysez chacune des connexions TCP à l'aide du bouton « Follow stream ».
8. Vous verrez les données envoyées entre le client email d'Ann et un serveur mail.

Répondez aux questions :

- Quelle est l'adresse email d'Ann ?
- Quelle est l'adresse email de l'amant secret d'Ann ?
- Quelles deux choses Ann demande-elle à son amant d'apporter ?

Objectifs 4 : Analyse forensiques avec des outils

Le site « Hacking Lab » utilisé pour le dernier exercice pose encore deux autre questions à répondre :

- Quel est le mot de passe d'Anne ?
- En quelle ville est le rendez-vous (nécessite l'extraction de l'attachement du mail) ?

Essayez de répondre à ces questions ! Voici quelques pistes :

Le login et le mot de passe d'Ann sont transmis lors de l'échange avec le serveur email. Ils apparaissent de manière codée dans le texte marqué en gras ci-dessous.

Ces textes semblent encryptés, mais ils ne sont que codés, et peuvent être décodés facilement.

Utilisez la commande *base64* (voir la page man) pour les décoder.

```
220 cia-mc07.mx.aol.com ESMTP mail_cia-mc07.1; Sat, 10 Oct 2009
15:37:56 -0400
EHLO annlaptop
250-cia-mc07.mx.aol.com host-69-140-19-190.static.comcast.net
250-AUTH=LOGIN PLAIN XAOL-UAS-MB
250-AUTH LOGIN PLAIN XAOL-UAS-MB
250-STARTTLS
250-CHUNKING
250-BINARYMIME
250-X-AOL-FWD-BY-REF
250-X-AOL-DIV_TAG
250-X-AOL-OUTBOX-COPY
250 HELP
AUTH LOGIN
334 VXNlcm5hbWU6
c25lYWt5ZzMza0Bhb2wuY29t
334 UGFzc3dvcmQ6
NTU4cjAwbHo=
235 AUTHENTICATION SUCCESSFUL
```

Pour extraire le fichier attaché au mail, vous pouvez utiliser la commande munpack.