Lab packet-introspection

Présentation
Le format PCAP (Capture de paquets) est une représentation standard et portable du trafic réseau au niveau des paquets. Vous êtes probablement déjà familiarisé avec PCAP car à la fois Wireshark et TCPDump stockent et lisent des données au format PCAP. Ce laboratoire d'introduction est conçu pour familiariser les élèves avec les PCAPS et l'analyse de trafic à l'aide de Wireshark.
Wireshark comprend de nombreux outils puissants et convient le mieux à une analyse hautement ciblée sur des Captures de paquets de petite taille. Ce laboratoire est adapté de [1], qui est une ressource utile pour améliorer votre familiarité avec le système d'outils Wireshark.

Pré-requis
Les étudiants doivent avoir une connaissance de base de la ligne de commande Linux et la capacité d'éditer des fichiers et d'exécuter des scripts shell simples. Une certaine expérience avec Wireshark est également présumée, par exemple, l'étude du laboratoire d'introduction à wireshark.

Démarrer le laboratoire
Le laboratoire est lancé à partir du répertoire de travail labtainer sur votre hôte sur votre hôte ou votre machine virtuelle Linux. Exécutez la commande:

```
labtainer packet-introspection
```

Un lien vers ce manuel de laboratoire sera affiché.
Le terminal virtuel résultant comprend : un terminal (shell bash) connecté à un ordinateur **client** "ws".

Tâches

1 Trouver le flux TCP le plus actif

Une tâche d'analyse de réseau commune consiste à déterminer les principaux contributeurs au trafic réseau et à la potentielle congestion. Dans cette partie, vous allez isoler et examiner le plus grand débit TCP dans une capture de paquets. Réaliser les étapes suivantes et répondez aux questions.

1. Lancez **wireshark** et ouvrez le fichier `pcaps/http-misctraffic101.pcapng`
2. Sélectionnez **Statistics — Conversations.** Cliquez sur l'onglet **Ethernet**; remarquez qu'il n'y a qu'une paire d'hôtes qui communiquent sur le réseau local. Cochez la case de résolution de nom **« Name resolution »**.
   L'adresse MAC indiquée comme *Cadant* est celle du routeur local.
   L'hôte *HewlettP* est le client à partir duquel le trafic a été capturé.
3. Cliquez sur l'onglet **IPv4** pour examiner les conversations IPv4 dans ce fichier de trace. En vous basant sur le comptage des octets, identifiez les adresses IP qui participent à la conversation IPv4 la plus active.
   - Cliquez sur l'onglet TCP pour identifier la conversation TCP la plus active. Trier par octets en cliquant sur l'entête de colonne des octets « Bytes ».
   - Lorsque vous regardez le flux le plus actif, vous voyez que l'hôte Source 24.6.173.220 utilise un port aléatoire (61598) et l'hôte Destination: 209.177.86.18 utilise le port HTTP (80).
     (Si vous voyez des noms de service, vous pouvez décocher la zone de résolution de noms pour afficher les Numéros de port.)

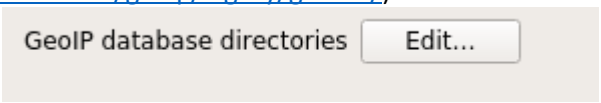
4. Cliquez avec le bouton droit de la souris sur la conversation TCP la plus active et sélectionnez Appliquer en tant que filtre « **Apply as a Filter—Selected—A<->B** ». Wireshark crée et applique automatiquement un filtre d'affichage pour cette conversation TCP. Cochez la case « **Limit to display filter** ». Combien de paquets correspondent à ce filtre?

Partie 1 Nettoyage : cliquez sur le bouton **Clear** ou Effacer (le X rouge à côté de l'expression du filtre) pour supprimer votre filtre avant de continuer. Basculez vers la fenêtre principale de Wireshark et cliquez sur Fermer.

2. Géolocaliser des Adresses IP

Faire la corrélation entre les adresses IP des interfaces réseau et leurs emplacements physiques est souvent une tâche utile. Wireshark comprend une fonctionnalité de base à cet égard, qui utilise les versions gratuites de la base de données MaxMind2. Il est important de reconnaître qu'aucune base de données de Géolocalisation IP n'est sans erreur. En effet, diverses approches permettent de géolocaliser des adresses IP et ces processus ont des complexités associées plus importantes que nous n'étudierons pas ici.

1. Lancez **wireshark** et ouvrez le fichier `pcaps/http-browse101c.pcapng`
2. Sélectionnez **Edit — Preferences — Name Resolution** et cliquez le bouton modifier **Edit** des répertoires de base de données GeoIP, cliquez sur Nouveau  et pointez sur le répertoire `/home/ubuntu/MaxMind` (qui dispose de fichiers de base de données téléchargés à partir de :http://dev.maxmind.com/geoip/legacy/geolite/).



puis **OK** et **OK**.
3. Sélectionnez **Statistics — Endpoints** et cliquez sur l'onglet **IPv4**. Vous devriez voir des informations dans les colonnes pays, ville, latitude et longitude (**Country, City, Latitude,** et **Longitude**).
4. Cliquez sur le bouton **Map**, Wireshark lancera une vue cartographique dans votre navigateur avec les adresses IP connues tracées sous forme de points sur la carte. Cliquez sur l'un des points pour trouver plus d'informations sur l'adresse IP.
    - Combien de trafic agrégé est allé à / provient de Santa Clara, CA?

Partie 2 Nettoyage : Fermez l'onglet / la fenêtre du navigateur lorsque vous avez terminé. Basculez vers la fenêtre Wireshark et cliquez sur Fermer.

3. Réassembler un texte à partir du flux TCP capturé

En tant que protocole orienté « flux d'octets », les données de segments TCP sont basées sur ses MSS, et non sur la sémantique de la langue anglaise, voire même sur le formatage des données d'application. Ainsi, il peut être utile de réassembler ces données avant de les inspecter manuellement.

1. Lancez **wireshark** et ouvrez le fichier `pcaps/http-wiresharkdownload101.pcapng`
   Les trois premiers paquets sont la poignée de main ou « handshake TCP » pour la connexion au Server Web. La trame 4 contient les requêtes GET des clients pour la page Download.html.
2. Cliquez avec le bouton droit de la souris sur la **trame 4** et sélectionnez **Follow — TCP stream** pour suivre le flux TCP. Le trafic du premier hôte vu dans le fichier de trace, le client dans notre cas, est coloré en rouge. Le trafic du deuxième hôte vu dans le fichier de trace, le serveur dans notre cas est coloré en bleu.
3. Wireshark affiche la conversation sans les en-têtes Ethernet, IP ou TCP. Faites défiler le flux pour rechercher le message caché de Gerald Combs, créateur de Wireshark. Il est situé dans le flux du serveur et commence par **X-Slogan**. Quel est le message?
   Ce n'est pas le seul message masqué dans la session de navigation sur le Web. Maintenant que vous savez que le message commence par X-slogan, vous pouvez afficher dans WireShark chaque trame comprenant cette chaîne ASCII. Cliquez sur le bouton **Close** pour fermer, puis sur le bouton **Clear** pour supprimer le filtre de flux TCP.
4. Appliquer le filtre d'affichage qui contient " **X-Slogan**" sur les trames.

Astuce : repérez dans la zone Hypertext Transfer Protocol, le texte xslogan, cliquez avec le bouton droit et sélectionnez **Apply as Filter—Selected** afin de voir la syntaxe du filtre et le modifier.

5. Cliquez avec le bouton droit sur les deux autres trames affichées et sélectionnez **Follow — TCP stream** pour examiner les en-têtes HTTP échangés entre les hôtes. Avez-vous trouvé l'autre message? Notez que vous ne pouvez suivre qu'un seul flux à la fois en utilisant cette méthode de clic droit. Vous devrez effacer votre filtre d'affichage avant de suivre le prochain flux.
   Quel autre message avez-vous trouvé (différent de Q3)?

Partie 3 Nettoyage : Cliquez sur le bouton **Close** pour fermer, puis sur le bouton **Clear** pour supprimer le filtre de flux TCP. Basculez vers la fenêtre principale de Wireshark et cliquez sur Fermer.

4. Extraire un fichier binaire d'une session FTP

Dans la section précédente, nous avons extrait des messages ASCII-text des paquets. Qu'en est-il des données binaires? Wireshark a également des outils pour cela.

1. Lancez **wireshark** et ouvrez le fichier `pcaps/ftp-clientside101.pcapng`
2. Faites défiler le début du fichier de trace. Vous verrez de nombreuses commandes **FTP** utilisées pour se connecter, demander un répertoire, définir un numéro de port pour le transfert de données et récupérer un fichier.
   Il existe deux connexions de données dans ce fichier de trace : une pour la liste des répertoires et une autre pour le transfert de fichier. Nous ne sommes intéressés que par ces deux flux de données et non par le flux de canal de commandes.
   - Choisissez une trame de flux de canal de commandes puis cliquez avec le bouton droit **Follow — TCP stream**, cliquez sur le bouton **Hide This Stream**. Ceci ferme la fenêtre du flux TCP et applique un filtre d'exclusion.

   Maintenant, vous ne voyez que le trafic de canal de données. Les trames 16 à 18 et 22 à 24 sont des paquets de poignée de main ou « handshake TCP » pour établir les deux canaux de données requis.
   - Cliquez avec le bouton droit de la souris sur la trame 16 et sélectionnez **Follow — TCP stream**. Cette liste de flux indique qu'il n'y a qu'un seul fichier dans le répertoire. Quel est son nom? (Vous allez l'utiliser ensuite.)
   - Cliquez sur le bouton **Hide This Stream**. Ceci ferme la fenêtre du flux TCP et l'ajoute au filtre d'exclusion existant.

   Le seul trafic restant affiché est le trafic de transfert de fichier.
   - Cliquez avec le bouton droit de la souris sur n'importe quelle trame et sélectionnez **Follow — TCP stream**.

   Vous pouvez afficher l'identifiant de fichier qui indique qu'il s'agit d'un fichier .jpg (JFIF) et des métadonnées contenues dans le fichier graphique.

- Pour réassembler l'image graphique transférée dans cette communication FTP, dans la liste déroulante **Show and save data** choisissez le format **RAW**, puis cliquez sur le bouton **Save As**, sélectionnez un répertoire cible pour le fichier et définissez le nom du fichier avec celui que vous avez trouvé quelques étapes plus haut. Cliquez sur **Save** pour l'enregistrer.
- Accédez au répertoire cible et ouvrez le fichier que vous avez enregistré à l'étape précédente à l'aide du navigateur **firefox** installé sur le client **ws**. Inclure l'image dans votre rapport.

Partie 4 Nettoyage : Lorsque vous avez fini d'examiner l'image que vous avez extraite, fermez votre visionneuse d'image. Cliquez sur le bouton **Close** pour fermer, puis sur le bouton **Clear** pour supprimer le filtre de flux TCP. Basculez vers la fenêtre principale de Wireshark et cliquez sur Fermer.

Arrêter le labtainer

Lorsque le laboratoire est terminé, ou si vous souhaitez arrêter de travailler pendant un certain temps, dans le terminal qui vous a permis de le lancer, exécutez : stoplab

Vous pouvez toujours redémarrer le Labtainer et continuer votre travail. Lorsque le Labtainer est arrêté, un fichier zip est créé et copié dans un emplacement affiché par la commande « stoplab ». Une fois le laboratoire terminé, vous pouvez envoyer ce fichier zip au formateur pour correction éventuelle.

Références

[1] Wireshark 101: Essential Skills for Network Analysis, by Laura Chappell and Gerald Combs. Published by Protocol Analysis Institute, 2013. ISBN: 1893939723, 9781893939721