Lab Wireshark Introduction

Présentation
Cet exercice introduit l'outil d'analyse de trafic réseau Wireshark. L'étudiant utilisera Wireshark pour afficher le trafic réseau capturé dans un fichier "PCAP" et localiser un paquet spécifique. Les fichiers PCAP contiennent des copies du trafic réseau stockées dans un format pouvant être traité par divers outils d'analyse de réseau tels que Wireshark et TCPDump. PCAP est un raccourci pour "Capture de paquet".

Pré-requis
Cet exercice suppose que vous avez reçu une formation à TCP / IP et au réseau. Dans ce laboratoire, il vous sera demandé d'analyser des paquets d'une session Telnet. Telnet est un protocole de communication permettant à un utilisateur de délivrer des commandes shell à un hôte distant. Le trafic réseau Telnet n'est pas chiffré, ce qui simplifie l'analyse du trafic. Reportez-vous au TelnetLab pour plus d'informations.

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 wireshark-intro
```

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 Exploration

1. Utilisez la commande **ls -l** pour afficher le contenu du répertoire dans le terminal ouvert lorsque vous avez démarré le laboratoire. Un fichier `telnet.pcap` contient le trafic réseau que vous analyserez.
2. Utilisez la commande **file telnet.pcap** pour afficher des informations sur le fichier.

2. Exécutez Wireshark pour effectuer une analyse PCAP

3. Lancez **wireshark** avec la commande `wireshark`
4. Ouvrez le fichier `telnet.pcap` avec le menu **File->Open**

Remarque: si vous rencontrez une fenêtre noire ou corrompue lors de l'utilisation de Wireshark, essayez de redimensionner un peu la fenêtre. Si la fenêtre ne se redimensionne pas, essayez d'arrêter l'application et de la relancer.

3.Trouver un paquet spécifique

5. Localisez l'unique paquet contenant le mot de passe fourni lorsque l'utilisateur a tenté d'utiliser Telnet pour se connecter en tant qu'utilisateur «John».
   Astuce: Si vous tapez **telnet.data** dans le champ indiquant " Apply a display filter" pour ajouter un filtre d'affichage" (voir la figure 1), l'outil affiche uniquement les paquets de données Telnet. Appuyez sur Entrée pour appliquer le filtre.

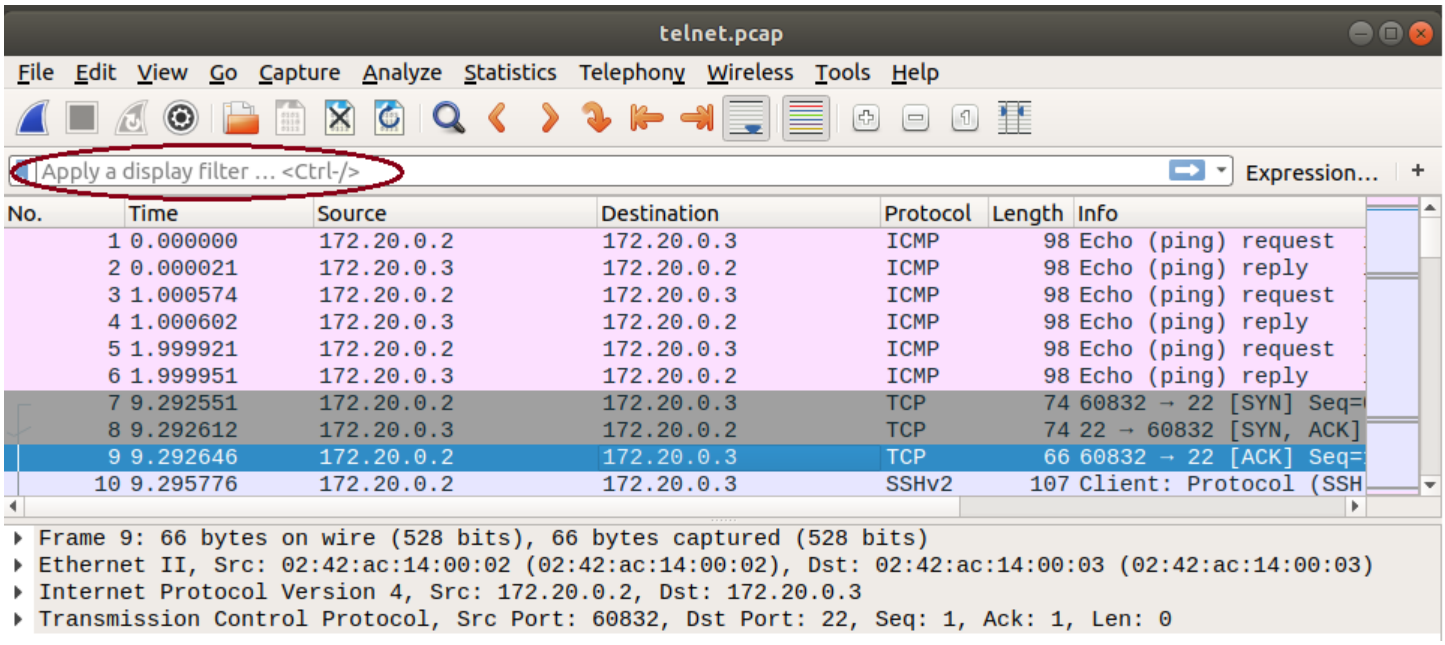

Figure 1- Fenêtre Wireshark - Filtre

6. Une fois que vous localisez le paquet unique contenant le mot de passe invalide, sélectionnez-le et utilisez **File=>Export specified packets** pour enregistrer le paquet unique. Enregistrez ce paquet unique comme « invalidpassword.pcap ». Assurez-vous de sélectionner le bouton radio **Selected packets only** dans la boîte de dialogue **Export** et d'écrire exactement le nom du fichier.

Après avoir enregistré le paquet, vous pouvez utiliser **File=>Open** pour ouvrir votre nouveau fichier PCAP pour confirmer qu'il bien contient le paquet correct.

7. 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 ». Wireshark crée et applique automatiquement un filtre d'affichage pour cette conversation TCP. Combien de paquets correspondent à ce filtre?

Poursuivre l'exploration

8. Observez d'autres paquets de cette capture et expérimentez des filtres. Essayez de sélectionner l'un des paquets TELNET et utilisez la fonction d'analyse de flux **Analyze=>Follow=>TCP stream** pour afficher l'ensemble du dialogue Telnet.
9. Explorez les paquets ICMP Echo/reply entre le serveur et le client.

Après avoir terminé ce laboratoire, envisagez d'effectuer le laboratoire d'introspection de paquets packet-introspection pour approfondir l'analyse du trafic avec Wireshark.

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.