Devoir # 1 : Utilisation de Wireshark (INF3271 Été 2024)

Un projet pratique qui est composé deux parties. La première s'agit de l'installation et l'utilisation de l'outil Wireshark® et WinCap® et la deuxième partie représente une liste des questions sur votre compréhension de l'outil en question.

TABLE DES MATIÈRES

Première partie : L'un des renifleurs (Sniffers) de paquets les plus connus est Wireshark® (anciennement appelé Ethereal®). C'est un outil flexible et puissant. Tout administrateur réseau digne de ce nom saura exécuter Wireshark. La plupart des professionnels l'utilisent souvent. Wireshark s'est amélioré avec chaque version. Il restera probablement longtemps la norme de l'industrie.

Vous allez installer Wireshark et faire quelques exemples pour vous donner un petit aperçu de ce que Wireshark peut faire. En plus de télécharger Wireshark (j'espère que c'est déjà fait), vous devrez également télécharger WinPCap® afin de capturer réellement les paquets envoyés sur votre réseau.

Les informations à remettre via Moodle :

- Capture d'écran de l'outil Wireshark (comme quoi s'est bien installé)
- Capture d'écran de l'outil WinPCap (comme quoi s'est bien installé)
- Une capture des paquets avec Wireshark
- Une capture des paquets avec WinPCap

Remarque: vous venez de sélectionner des paquets sur votre réseau et de regarder leur contenu. Il se peut qu'il y ait eu beaucoup de trafics que vous ne pouviez pas interpréter. Ne vous inquiétez pas des informations sur votre écran qui sont difficiles à comprendre. Dans la deuxième partie, vous utiliserez un filtre pour capturer uniquement le trafic Web passant par le port 80.

Deuxième partie : Dans ce projet, vous allez filtrer tous les paquets « supplémentaires » que vous avez capturés et regarder simplement le trafic Web. Trop souvent, vous capturerez beaucoup plus d'informations que vous n'en voudrez ou n'en aurez jamais besoin. Être capable de filtrer le trafic que vous ne voulez pas est une compétence importante. Wireshark peut filtrer les paquets par adresse IP ou par numéro de port. Une compréhension approfondie de TCP / IP vous aidera grandement à comprendre comment fonctionne le filtrage de paquets. Il existe plusieurs excellents didacticiels en ligne qui vous apprendront les bases de TCP / IP.

Deuxième partie : Questions de réflexion?

1. Que signifient les différentes couleurs dans le journal Wireshark ?
2. Pourquoi votre ordinateur reçoit-il des paquets qui sont adressés à une autre machine ?
3. Combien de paquets votre ordinateur envoie / reçoit-il en un seul clic de souris lorsque vous visitez un site Web ?
4. Pourriez-vous organiser ou filtrer le trafic pour le rendre plus facile à comprendre ?
5. Pourquoi votre ordinateur envoie-t-il autant de paquets ? Pourquoi ne pas envoyer un seul très gros paquet ?
6. Que signifient SYN, ACK, FIN et GET ?
7. Pouvez-vous capturer tous les paquets pour un réseau entier ?
8. Wireshark peut-il résoudre automatiquement l'adresse IP en un nom de machine (hôte) ?