Petit Wesley

TP1 – Sécurité des réseaux et du Web

1. [2 pts] Cette capture contient un échange où utilisateur tente de se connecter à localhost via TELNET. Donnez son nom d'utilisateur et son mot de passe.

On sait que l'utilisateur tente de se connecter à localhost (127.0.0.1) via Telnet, d'où le filtre suivant : telnet and ip.src == 127.0.0.1. En regardant les différentes trames obtenues, on trouve le compte utilisateur et le mot de passe dans les lignes 559 à 664 (avant il y a un login incorrect) sur la machine Satchmo.

Nom d'utilisateur : sigmundfreud

Mot de passe : a63!9w

2. [1 pt] De quelle marque est le routeur auquel est connecté l'ordinateur durant tout cet échange ?

Le routeur est de la marque Cisco, on peut le trouver avec le filtre ospf. Ce filtre met en avant les connexions entre l'ordinateur et le routeur.

3. [1 pt] Combien de temps a pris le chargement du site web perdu.com?

Le chargement d'un site web se fait via le protocole HTTP, on a l'IP du client 10.43.136.144 et l'IP du serveur HTTP est 208.97.177.124 (réponse DNS de perdu.com ligne 460). On peut voir avec le filtre suivant : http and ip.src == 208.97.177.124 and ip.dst == 10.43.136.144, en regardant le champ « Time since request » le temps de chargement. Le chargement du site web perdu.com a mis 0.032267000 seconde.

4. [4 pts] Le même navigateur a tenté d'envoyer une requête HTTP au site allmusic.com. Cette requête correspond à l'élément numéro 190 dans la trace capturée.

a) [1 pt] Donnez une expression de filtrage qui affiche tous les segments TCP échangés entre le client et allmusic.com (et rien d'autre).

En regardant la réponse DNS à les lignes 185 - 186, on a l'IP du serveur contenant allmusic.com : 144.198.225.72. Dans la requête HTTP au numéro 190, l'IP du client est 10.43.136.144. Des paquets sont présents avec le protocole HTTP, car elles contiennent un en-tête TCP.

Filtre : tcp and ((ip.src == 10.43.136.144 and ip.dst == 144.198.225.72) or (ip.src == 144.198.225.72 and ip.dst == 10.43.136.144))

b) [1 pt] Dans la vue ainsi obtenue, à quoi correspondent les éléments qui se trouvent avant le numéro 190 ?

Avant le numéro 190, les éléments sont des segments TCP servant à synchroniser le allmusic.com et le client (ouverture de connexion avec le « three-way handshake »). Cela correspond au SYN, SYN ACK et ACK aux éléments 187 - 189.

c) [1 pt] Quel numéro de port le client utilise-t-il pour identifier la connexion TCP entre lui et www.allmusic.com?

Pour identifier la connexion entre le client et allmusic.com, le client utilise le port 54552 (port pris à la volée) pour aller au port 80 pour allmusic.com (port standard pour le protocole http/web). On peut voir ces ports avec les segments TCP (Ex : de la ligne 193).

d) [1 pt] À un moment, l'utilisateur du navigateur a appuyé sur la touche Esc pour arrêter le chargement. Pouvez-vous identifier un segment TCP de l'échange qui le révèle ?

Le segment TCP qui montre l'arrêt du chargement est à la ligne 412, car il possède FIN comme « Flags ». Il s'agit donc de la demande de transmissions de segments.

5. [3 pts] On s'intéresse maintenant au trafic DNS échangé durant la capture.

a) [1 pt] Lorsqu'il envoie une requête, le système d'exploitation du client préfère-t-il recevoir comme réponse des adresses IPv4 ou IPv6 ?

On sait qu'on cherche des réponses DNS en provenance du client (10.43.136.144), d'où le filtre suivant : dns and ip.src == 10.43.136.144. Avec ce filtre, les différents DNS possèdent un champ type (dans Queries) qui contient soit le type A (Host Address), soit AAAA (IPv6). Le système d'exploitation préfère donc recevoir une réponse en IPv6. La ligne 12 et 124 montre ces deux types.

b) [2 pts] Le système d'exploitation sur lequel a été réalisé la capture possède un bug qui peut être révélé en observant le trafic DNS concernant le domaine daisy.ubuntu.com. Quel est le problème ?

6. [6 pts] Un paquet IP arrive au routeur dont l'adresse IP est 10.10.10.1 avec les champs suivants (les bits sont disposés de la même manière que dans les diapositives du cours) :

a) [1 pt] À qui (i.e. quelle adresse) est destiné ce paquet ?

Selon le cours, on connait l'adresse source avec la 4ème ligne et l'adresse de destination avec la 5ème ligne. En convertissant les différents bits, on obtient :

Adresse Source : 56.2.3.190

Adresse Destination : 10.10.10.3

b) [2 pts] Votre collègue Alice prétend que ce paquet transporte un segment UDP. Au contraire, Bob affirme qu'il est impossible de savoir ce que transporte ce paquet, puisqu'on n'en voit que l'en-tête. L'un des deux a-t-il raison ? Expliquez votre réponse.

Dans le cours, on a vu que l'en-tête IP contient le protocole du niveau supérieur (ligne 3, colonne 2). En comptant ce bit, on tombe sur 6 qui reviens au protocole TCP. Ainsi, aucun n'a raison puisqu'on peut déterminer le protocole TCP et non UDP.

c) [6 pts] Vous disposez d'un appareil qui peut intercepter les chaînes binaires juste avant qu'elles n'arrivent au routeur 10.10.10.1. Cet appareil peut remplacer n'importe quel bit 0 par un bit 1 (et vice versa), mais ne peut ajouter ou supprimer des bits de la transmission, laquelle aboutit toujours au routeur.

Au moyen de cet appareil, on vous demande de faire en sorte que les données transportées par ce paquet n'arrivent pas jusqu'à la couche application de son destinataire (i.e. aucun bit des données n'est relayé à la couche application). Donnez trois manières différentes d'altérer les bits de l'en-tête IP du paquet pour arriver à vos fins. Dans chaque cas, indiquez quels sont les bits que vous modifiez (i.e. dans quel(s) champ(s) de l'en-tête et quelle valeur vous souhaitez obtenir), et pourquoi les données n'arriveront pas à l'application. (2 points bonus si vous en identifiez une quatrième.)

L'une des manières est d'intervenir sur le Checksum (contrôle d'erreur) du paquet. Si on le modifie, la prochaine machine qui reçoit le paquet verra qu'il a été modifié et effacera le paquet. On prend les bits de la 3ème ligne / 3ème colonne (selon le schéma du cours), on les modifie de cette façon (différent de celui de base) : 00000000 00000111.

Une autre façon est de réduire le TTL à zéro. Quand le TTL tombe à zéro, alors le paquet est détruit au prochain routeur afin de ne pas surcharger le réseau avec des paquets perdus. On prend le bit de la 3ème ligne / 1ère colonne. On transforme ce bit en 00000000.

Une troisième manière consiste à change l'adresse utilisateur de destination. Ainsi, le paquet n'atteindra jamais l'adresse de destination de base. On prend les bits de la 5ème ligne, on les transforme par exemple en 00111000 00000010 00000011 10111110 (adresse source par exemple).