UNIVERSITÉ DE SHERBROOKE

Faculté de Génie - Département de Génie Informatique et Electrique

APP3 - Réseaux

Rapport

Yohanna Taptue – tapy2701
Solène Aboud – abos2601
16/10/2019

Analyse des PDUs

PDU 1

MAC destination : FF FF FF FF FF FF MAC source : F8 B1 56 A3 64 50

Type : 0806 -> ARP Type de matériel : 0001 Type de Protocol : 0800

Longueur de l'adresse physique : 06 Longueur de l'adresse logique : 04

Opération : 0001 *(Request)*

Adresse MAC source : F8 B1 56 A3 64 50

Adresse IP source : C0 A8 01 02 (192.168.1.2)

Adresse MAC destination : 00 00 00 00 00 00

Adresse IP source : C0 A8 01 01 (192.168.1.1)

PDU 2

MAC destination : F8 B1 56 A3 64 50 MAC source : F8 B1 56 A3 64 50

Type : 0806 -> ARP Type de matériel : 0001 Type de Protocol : 0800

Longueur de l'adresse physique : 06 Longueur de l'adresse logique : 04

Opération : 0002 *(Reply)*

Adresse MAC source : F8 B1 56 A3 64 50

Adresse IP source : C0 A8 01 02 (192.168.1.1)

Adresse MAC destination : F8 B1 56 A3 64 50

Adresse IP source : C0 A8 01 02 (192.168.1.2)

PDU3

MAC destination : F8 B1 56 A5 90 E1 MAC source : F8 B1 56 A3 59 E0 Type : 0800 -> IPv4

Version : 4 LET : 5

Services différenciés : 00 Longueur totale : 0028

Id: 01A1 Flag: 4 = 0100

TTL: 80 Protocol: 06->TCP Header: 77DA

Adresse source : C0 A8 01 01 (192.168.1.1)

Adresse destination : C0 A8 01 03 (192.168.1.3)

Port source : 0B DF Port destination : 04 1E N° de séquence : 68 FA A3 6F

N° accusé de réception : 4A 5B EF 58 longueur en-tête TCP : 5 Taille de la fenêtre : 010

PDU4

MAC destination : F8 B1 56 A5 90 E1 MAC source : F8 B1 56 A3 59 E0 Type : 0800 -> IPv4

Version : 4 LET : 5

Services différenciés : 00 Longueur totale : 0034

Id: 01DC Flag: 4 = 0100

TTL: 80 Protocole : 06->TCP Header : 68C2

Adresse source : 84 DD2 4A A2 (132.210.74.162)

Adresse destination : C0 A8 01 03 (192.168.1.3)

Port source : 0B E1 Port destination : 04 20 N° de séquence : 6F F5 0F 95

N° accusé de réception : 51 56 5F 36 longueur en-tête TCP : 5 Taille de la fenêtre : 018

Identification de l'adresse de la passerelle

Grâce à l'analyse des PDUs que nous avons effectuée précédemment nous avons pu identifier l'adresse IP de la passerelle de notre réseau. Il s'agit de l'adresse IP **192.168.1.3**.

Lors de cette analyse nous avons pu remarquer l'utilisation de 2 protocoles différents. Cela nous a permit de déterminer l'adresse source et l'adresse destination de chaque PDU.

Avec ces adresses nous avons remarqué qu'il y a trois adresses IP qui sont dans le même sous réseau et c'est uniquement l'adresse IP 192.168.1.3 qui communique avec une autre adresse IP externe.

Analyse de la session TCP

Le détournement de la session TCP est une technique consistant à intercepter une session TCP initiée entre deux machines afin de la détourner.

Pour analyser le fichier .CAP nous avons commencé par récupérer les adresses IP source et destination des machines du début des échanges ainsi que leurs adresses MAC. Ensuite nous avons appliqué un filtre pour pouvoir déterminer si d'autres adresses MAC étaient impliquées dans ces échanges. Deux paquets ont été filtrés et dans ces paquets nous avons remarqué que l'adresse MAC de source était différente mais celle de la destination n'avait pas changé.

Lorsque nous retirons les filtres et analysons les échanges, nous remarquons que juste avant les paquets filtrés l'échange est normal, avec les adresses IP et MAC correspondantes, ensuite un changement s'effectue au niveau de l'adresse MAC de source. Mais plus tard, l'échange redevient à nouveau normal. Nous pouvons donc en déduire qu'une personne tierce s'est introduite lors de la communication entre nos deux machines.