Helec Bastien

TP1 : Capture de trames :

1. Initiation a wireshark :

montrer comment filtrer le trafic pour n'avoir que les messages qui partent ou qui arrive de la machine :

```
ip.src == 10.213.8.1 || ip.dst == 10.213.8.1
```

Capturer les trames emises et reçues lors de la consultation avec firefox du site : www.perdu.com

```
http.request.method == GET || http.request.method == POST
```

Les protocoles utilisés sont : Ethernet, IPV4, TCP, HTTP

Les champs que vous comprennez du PCI de chaque couche : couche 2: les adresses mac : dest= d0:7e:28:2d:84:8c src = 98:90:96:e0:85:29 le type = IPV4 couche 3: ip src = 10.213.8.1 ip dest = 34.107.221.82 la taille de l'entete = 20 bytes le protocole = TCP le TTL = 64 la taille total = 364 bytes couche 4: port dest = 80 port source = 34388 le flags = PSH, ACK

Prenez l'un des paquets de votre. Dans son analyse en couches, une couche apparait tout en haut indiquant 'Frame XXXX' où XXXX est un numéro. frame 525

Qu'elle couche du modele tcp/ip correspond a cette information ? couche 1

Que contient-elle ? le type de la couche 2

2. Analyse de trames ICMP Request :

   Quels paquets sont emis ? reçus ? Expliquez les paquets emis sont les paquets ICMP request les paquets recus sont les paquets ICMP reply ICMP request permet de savoir si une machine est joignable ICMP reply permet de repondre a un ICMP request

3. Follow TCP stream : Récupérez et ouvrez la capture effectuée par vos professeurs adorés à l'adresse suivante :

   ```
   http://www.lirm.fr/~druon/assets/pdf/r102_tp1_capture.pcapng
   ```

   Vous pourrez pour ce faire , utiliser la commande wget.

   Comment wireshark a-t-il réussi à isoler cette conversation des autres ? il a reconnu les paquets TCP et a recuperer toute la données qu'il a pu isoler grace au numéro du paquet

4. Graphique des flux : Que voyez vous ? Explorez les autres analyse possible On voit les flux sur le réseaux a qu'elle moment le paquet et a t'elle endroit entre le serveur et le client

5. Analyse de trames Ethernet : Dans l'en-tete Ethernet quel champ permet de dire ce que contient la trame ? le type (qui est situé juste apres l'adresse mac src) Quelle est la valeur de ce champ dans le cas d'un ARP ? ! 0x0806 (ARP)

6. Ecriture d'un filtre sous wireshark:

   Ecrivez un filtre permettant de ne visualiser que les paquets : émis pour votre machine en tcp a destination du port 80

```
ip.src == 10.213.8.1 && tcp && tcp.dstport == 80
```

Quelle est l'adresse Mac de destination : d0:7e:28:2d:84:8c Quelle est l'adresse IP de destination : 193.49.104.251

7. Decouverte de tcpdump:

   Capturez avec tcpdump une requete http vers le site htttps://www.lawifi.fr , vous donnerez : les actions et commandes utiliser la syntaxe du filtre permettant de faire la Capture

```
man tcpdump
man pcap
sudo tcpdump -A 'tcp port 80 and (((ip[2:2] - ((ip[0]&0xf)<<2)) -
((tcp[12]&0xf0)>>2)) != 0)'
```

2. La resolution ARP :

3. Il contient toute les adresses mac avec les adresses ip associer

4. j'emet des trames ping request et je recois des trames ping reply on peut voir alors l'adresse MAC de la machine destination

5. Il contient la nouvelle adresse mac de la machine destination

6. On peut observer que la machine destination a changé d'adresse mac

7. Je peux observer le status reachable qui a remplacer stale

8. On n'obtient pas la l'adresse MAC du serveur externe par contre l'adresse MAC du routeur passe en statut delay, a nouveau la meme information cela veut dire que la trame passe par le routeur avant d'aller sur le reseau externe

On ne voit pas l'adresse MAC du serveur externe car il n'est pas sur le meme reseau que la machine source c'est une histoire de couche 2-3

14. le status est STALE ce qui signifie que l'adresse MAC est valide fasse a l'adresse IP mais l'adresse IP a peut etre changer de MAC entre temps ce status et la table qui affiche si c'est recent ou non

15. Non car la machine a supprimer les informations de la table ARP en attente d'une nouvelle requete ARP

16. trouver le temps avant suppression de la table ARP cat /proc/sys/net/ipv4/neigh/eno1/gc_stale_time 60 ce qui indique que la table ARP est supprimer au bout de 60 secondes

17. Videz le cache ARP de votre machine. Si des entrées sont déclarer de façon statique supprimez les. Il faut que le cache ARP soit vide :

```
sudo ip neigh flush all
```

Effectuez la capture de trame lors d'un ping vers WWWW.google.fr

Quelles sont les entrées qui sont apparu dans votre cache ARP ? L'entrée qui est apparu est l'adresse ip et mac du routeur Est-ce compatible avec votre capture de trame ? Oui car on peut voir que la trame passe par le routeur avant d'aller sur le reseau externe Justifiez et illustrez vos réponses avec une capture d'écran.

18. Que se passe t'il si vous refaite une tentative pour joindre www.tf1.fr au bout d'une minute ?

Le cache arp du routeur est passer en status stale

Qu'elle influence cela peut avoir sur le trafic réseau ? Cela peut avoir une influence sur le trafic réseau car le routeur va devoir repondre a une requete ARP pour savoir si l'adresse MAC est toujours valide

19. On va maintenant entrer l'adresse de la passerelle en statique dans le cache ARP. Recuperez l'adresse MAC de la passerelle et entrez cette adresse de facon statique à l'aide de la commande ip neigh :

```
sudo ip neigh add d0:7e:28:2d:84:8c dev eno1 lladdr d0:7e:28:2d:84:8c nud
permanent
```

Que se passe t'il si vous refaite une tentative pour joindre une machine exterieur. Indiquez ce qui a changer
.

On peut voir que la trame passe directement sur le reseau externe sans passer par le routeur

20. Les switchs (partie optionnelle) :

Connectez vous a l'interface d'administration de l'un des switchs Cisco 2960 . Affichez la table de commutation du switch

```
show mac address-table
show mac address-table dynamic
```

Reliez votre switch au switch et de vos deux machines a votre switch.

tout en Fa0/10 est le cable réseau et Fa0/6 le cable de la machine