Fiche savoir : la fragmentation IP

Présentation

La taille maximale d'un paquet IP qui est envoyé sur le réseau est définie par la valeur de la MTU (Maximum transmission unit) de l'interface de sortie.

Ce paramètre permet à l'interface de sortie d'un équipement :

- d'**adapter** la taille des paquets aux **capacités** de la couche 1 et 2 (Ethernet pour les réseaux locaux) pour un PC ou un routeur ;
- de tenir compte de l'utilisation d'encapsulation spécifiques (VPN, PPP, ...) pour un routeur.

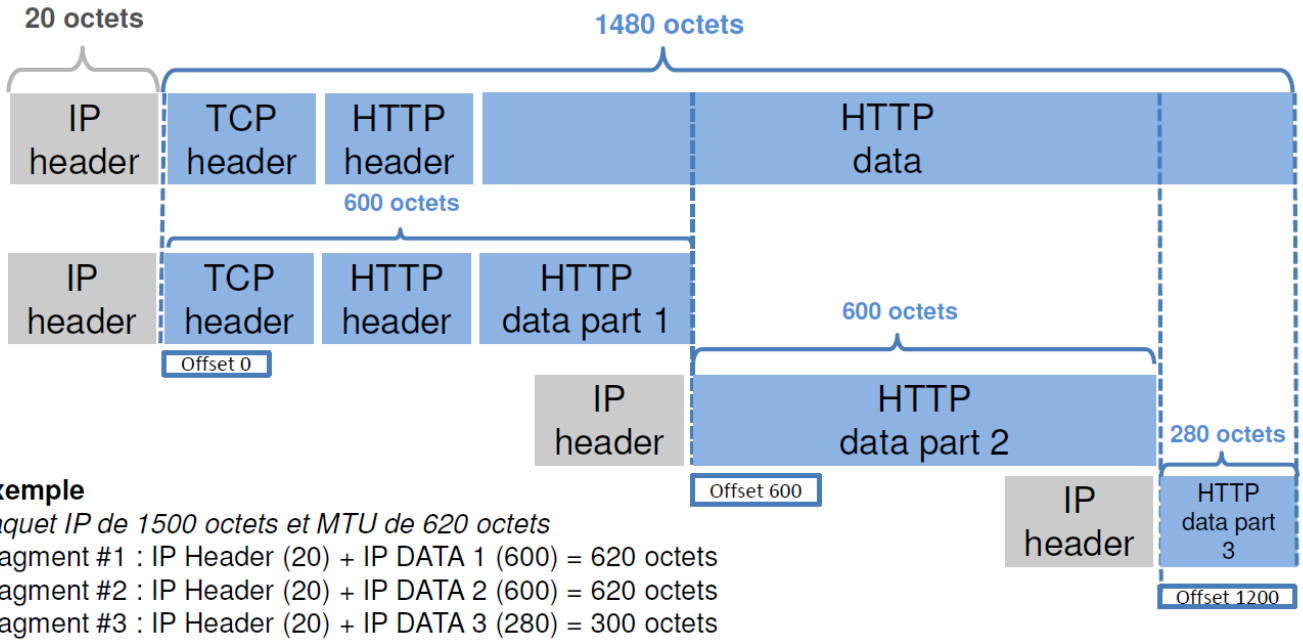
Lors de l'acheminement du paquet dans les différents traversés jusqu'à sa destination, des liens ayant une capacité de transmission inférieure peuvent être utilisés. Dans ces cas, le paquet IP est **fragmenté** par les routeurs intermédiaires qui ont une MTU plus petite :

- En IPv4, la fragmentation d'un paquet est **interdite*** lorsque le bit **DF** est positionné dans l'en-tête IP. La MTU minimale est de 576 octets.
- En IPv6, la fragmentation par un équipement intermédiaire est **interdite**. La MTU minimale est de 1280 octets.

> Un paquet IP qui ne peut être acheminé compte tenu de la MTU de l'interface d'entrée est détruit (**drop**).

> Une valeur **optimale** de MTU correspond à la valeur maximale que le réseau accepte. S'il est trop bas, cela ajoute de la **latence**.

L'option **offset** indique la position de chaque portion des données qui ont dû être fragmentées.



Exemple
paquet IP de 1500 octets et MTU de 620 octets
Fragment #1 : IP Header (20) + IP DATA 1 (600) = 620 octets
Fragment #2 : IP Header (20) + IP DATA 2 (600) = 620 octets
Fragment #3 : IP Header (20) + IP DATA 3 (280) = 300 octets

> Lors de la fragmentation d'un paquet, seul le **premier fragment contient les ports (TCP/UDP) utilisés** par la connexion. Pour que le pare-feu puisse analyser tous les fragments celui-ci doit reconstituer le paquet original.

MTU discovery (PMTUD)

Lien : https://www.malekal.com/quest-ce-que-le-mtu-et-mss-et-optimiser/

MTU discovery (PMTUD) est une méthode qui permet d'obtenir le MTU de tous les équipements que traversent un paquet :

- on envoie des paquets jusqu'à ce que ce dernier ne soit plus droppé par un des routeurs le long du chemin.
    - Lorsqu'un périphérique le long du chemin abandonne le paquet, il renvoie un message ICMP avec son MTU.
    - Le périphérique source abaisse son MTU et envoie un autre paquet de test.
    - Ce processus est répété jusqu'à ce que les paquets de test soient suffisamment petits pour traverser tout le chemin du réseau sans être abandonnés.

Le site speedguide permet d'obtenir les réglages MTU et MSS d'un PC ainsi que d'autres paramètres TCP/IP.

Des ajustements supplémentaires doivent alors être faits pour la partie **Données utiles**.

Optimiser le MTU

La commande **ping** permet de déterminer le meilleur **MTU**, en utilisant le même principe que le **path MTU discovery** : envoyer des paquets **fragmentés de différentes tailles** pour voir si un équipement **drop** ou **fragmente** le paquet.

Paramètres de la commande ping :

- envoyer des paquets **non fragmentés** avec l'option -f
- envoyer des paquets avec une taille de MTU différente avec -l

```
ping www.yahoo.com -f -l 1500
```

La commande netsh de Windows permet de modifier la valeur de la MTU du PC.

Attaque par fragmentation IP

Le mécanisme de fragmentation IP peut être détourné pour véhiculer des attaques :

- la menace est répartie sur plusieurs fragments.
- Le code malveillant est découpé puis inséré dans des fragments consécutifs ,
- l'analyse unitaire des fragments par le PC ou le serveur pare-feu ne révèle pas l'attaque.
- C'est au moment du réassemblage des fragments que la menace est reconstituée.

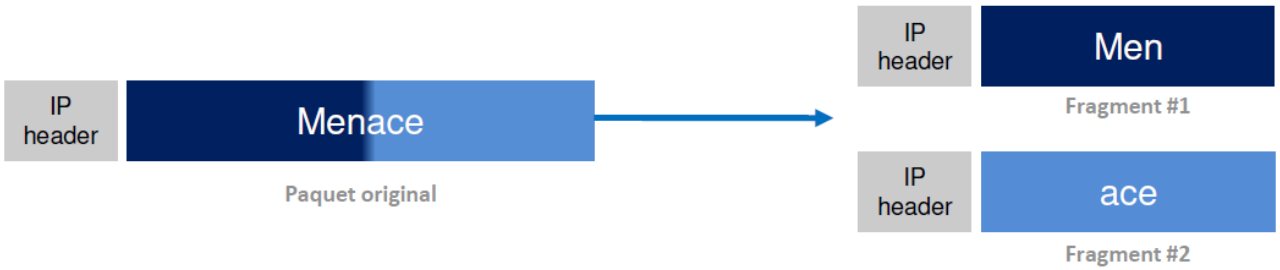
Attaque par recouvrement

L'usage de l'option **offset** est détourné" :

- définission de deux fragments consécutifs des valeurs d'offset qui se chevauchent ,
- mécanisme de chevauchement non standardisé, car non conforme,
- l'acceptation et la reconstitution du paquet dépend du comportement de l'implémentation de la pile IP destinataire :
    - Premier cas : si la pile IP destinataire place le 2nd fragment à l'offset indiqué,

l'atta□□ua□□t ayant forgé un second fragment contenant 100 octets de bourrage en début de fragment, le 1er fragment écrase le début du 2nd fragment et l'atta□□ue est reconstituée. • Second cas : l'atta□□ua□□t a inversé la place du bourrage (en fin de premier fragment) et la seconde partie de la menace pour parvenir à ses fins, parce que le second fragment écrase la fin du premier fragment dans l'i□□pl□□□□e□□tatio□□ de la pile IP destinataire.

- Exemple d'attaque par fragmentation



- Exemples d'attaque par recouvrement