1/ Établissement d’une communication orientée connexion :

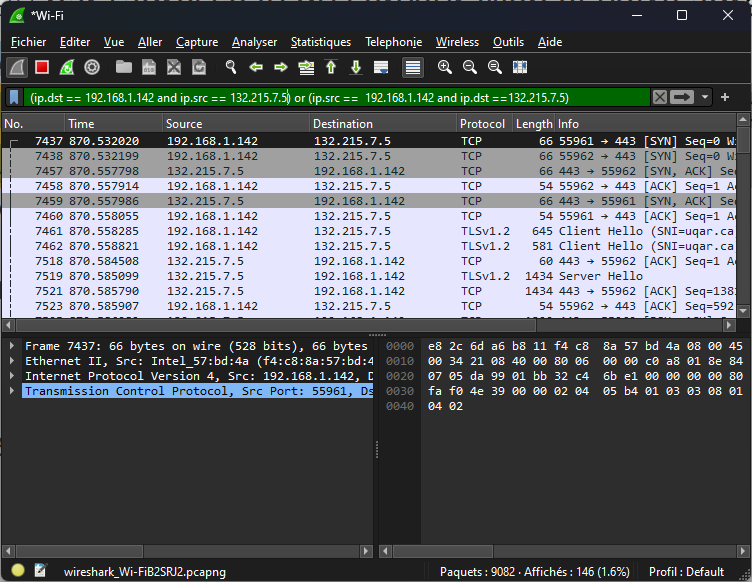
Mon adresse IP: 192.168.1.142

L’adresse IP de l’UQAR : 132.215.7.5

Une image contenant texte, capture d’écran, logiciel

Description générée automatiquement

Isolation d’une communication :



Numéro de séquence :

SYN (client): 0

SYN-ACK (serveur): 0

ACK (client): 1

Numéro d’acquittement :

SYN (client): /

SYN-ACK (serveur): 1

ACK (client): 1



La connexion n’a pas été établie du premier coup il en fallait 3 paquets pour établir la connexion TCP.

Teille de fenêtre :

SYN (client): 64240

SYN-ACK (serveur): 29200

ACK (client): 131072

Une image contenant capture d’écran, texte, Logiciel multimédia, Logiciel de graphisme

Description générée automatiquement

Oui la taille de la fenêtre change en fur et en mesure que la page charge

Le processus d'établissement de la connexion TCP observé dans la capture réseau correspond à la théorie vue en classe. La séquence SYN-SYN-ACK est utilisée pour établir une connexion

On identifie un paquet ‘Client-Hello’ du Protocol TLS-v1.2 envoyé du client vers le serveur



Trame Ethernet

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | | 1 | | 2 | | 3 | | 4 | | 5 | |
| **Adresse destination** | | | | | | | | | | | |
| 8 | 8 | d | 8 | 2 | e | f | 5 | d | 4 | 3 | 0 |
| 8=1000, troisième bit = 0 donc c’est une adresse globale. | | | | | | | | | | | |
| **Adresse source** | | | | | | | | | | | |
| 3 | c | 2 | 6 | e | 4 | 2 | 7 | e | 0 | f | f |
| C=1100, troisième bit = 0 donc c’est une adresse globale. | | | | | | | | | | | |
| **Type/Taille** | | | |  |  |  |  |  |  |  |  |
| 0 | 8 | 0 | 0 |  |  |  |  |  |  |  |  |
| Type IPv4 | | | |  |  |  |  |  |  |  |  |

En-tête IP

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | | | | | | | | 1 | | | | | | | | 2 | | | | | | | | 3 | | | | | | | |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| **Version** | | | | **IHL** | | | | **DSCP** | | | | | | **ECN** | | **Longueur totale** | | | | | | | | | | | | | | | |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 |
| Version 4 | | | | 20 bytes | | | | AF11(10)  Faible priorité | | | | | | desactivé | | Longueur total de 83 | | | | | | | | | | | | | | | |
| **Identification** | | | | | | | | | | | | | | | | **Flags** | | | **Décalage (offset)** | | | | | | | | | | | | |
| 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Identification : 0xfd6c (64876) | | | | | | | | | | | | | | | | 0x2  No frag | | | Pas eu de fragmentation | | | | | | | | | | | | |
| **TTL** | | | | | | | | **Protocole** | | | | | | | | **Somme de contrôle de l’en-tête (CRC)** | | | | | | | | | | | | | | | |
| 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| Durée de vie: 49s | | | | | | | | TCP (6) | | | | | | | | 0xa407 | | | | | | | | | | | | | | | |
| **Adresse IP Source** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 |
| 206.247.43.151 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Adresse IP Destination** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 10.10.163.112 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

B – i/ Non, il n’y a pas d’options car la taille de l’entête ne dépasse pas 20 octets. (4o x 5)

C -/ DSCP classe les paquets selon la priorité, ECN signale la congestion des du réseau avant la perte des paquets

En-tête TCP

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | | | | | | | | 1 | | | | | | | | 2 | | | | | | | | 3 | | | | | | | |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| **Port Source** | | | | | | | | | | | | | | | | **Port Destination** | | | | | | | | | | | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| 443 destiné pour HTTPS. | | | | | | | | | | | | | | | | 65066 une app ordi utilisant ce port | | | | | | | | | | | | | | | |
| **Numéro de séquence** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| 3411258760 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Numéro d’acquittement** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 11520041320 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Taille en-tête/**  **Décalage des données** | | | | **Réservé** | | | | **Codes** | | | | | | | | **Taille de la fenêtre glissante** | | | | | | | | | | | | | | | |
| 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 |
| 20bytes | | | |  | | | | Ack and push set | | | | | | | | Taille de 11 | | | | | | | | | | | | | | | |
| **Somme de contrôle** | | | | | | | | | | | | | | | | **Pointeur urgent** | | | | | | | | | | | | | | | |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0x802f | | | | | | | | | | | | | | | | 0 | | | | | | | | | | | | | | | |

E- i/ Il n’y a pas d’options car la taille de l’entête ne dépasse pas 20 bytes

F/ACK : Champ d'accusé de réception

Push : permet d'envoyer immédiatement des données à l'application réceptrice sans attendre d'accusé de réception.

H/ Il n’y a as de pointeur de données urgente configuré

H-i/ Premier octet : 0x3B sa valeur en HEX :ad

Dernier octet : 0x60 sa valeur en HEX : b4

Type de données reçu : application data (données application)