TP3

Sommaire

1.Connexion Bureau à distance(RDP)

```
C:\Windows\System32>netstat -no

Connexions actives

  Proto  Adresse locale         Adresse distante       État
  TCP    172.17.2.2:7680        172.17.2.10:53474      TIME_WAIT       0
  TCP    172.17.2.2:50263       172.17.254.5:445       ESTABLISHED     4

C:\Windows\System32>
```

Je recupere mon adresse ip grâce a la commande nestat -no

```
:\Windows\System32>ping 172.17.2.1

nvoi d'une requête 'Ping'  172.17.2.1 avec 32 octets de données :
éponse de 172.17.2.1 : octets=32 temps=2 ms TTL=128
éponse de 172.17.2.1 : octets=32 temps=2 ms TTL=128
éponse de 172.17.2.1 : octets=32 temps=2 ms TTL=128
éponse de 172.17.2.1 : octets=32 temps=2 ms TTL=128

tatistiques Ping pour 172.17.2.1:
   Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
urée approximative des boucles en millisecondes :
   Minimum = 2ms, Maximum = 2ms, Moyenne = 2ms
```

je ping mon l'ordinateur de mon ami grâce a la commande ping

après avoir désactiver le pare feux Windows

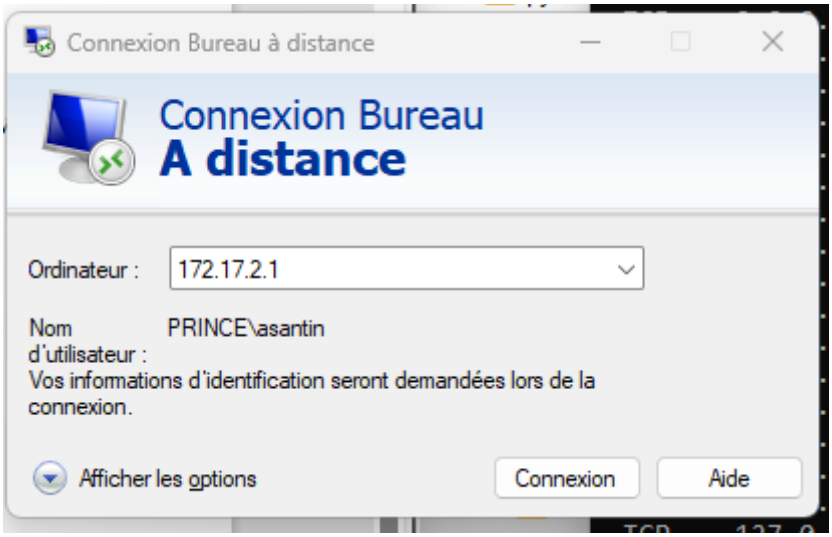
TP3

```
Proto  Adresse locale         Adresse distante       État
TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
TCP    0.0.0.0:902            0.0.0.0:0              LISTENING
TCP    0.0.0.0:912            0.0.0.0:0              LISTENING
TCP    0.0.0.0:2179           0.0.0.0:0              LISTENING
TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING
TCP    0.0.0.0:3307           0.0.0.0:0              LISTENING
TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49672          0.0.0.0:0              LISTENING
TCP    127.0.0.1:27017        0.0.0.0:0              LISTENING
TCP    172.17.2.2:139         0.0.0.0:0              LISTENING
TCP    172.17.2.2:49731       172.17.254.5:445       ESTABLISHED
TCP    172.17.2.2:51888       98.66.133.186:443      ESTABLISHED
TCP    172.17.2.2:51938       3.160.188.68:443       ESTABLISHED
TCP    172.17.2.2:51944       95.100.133.33:443      ESTABLISHED
TCP    172.17.2.2:51946       13.107.4.254:443       ESTABLISHED
TCP    172.17.2.2:51947       150.171.22.254:443     ESTABLISHED
TCP    172.17.2.2:51948       204.79.197.222:443     ESTABLISHED
TCP    172.17.2.2:51949       13.107.42.254:443      ESTABLISHED
TCP    172.17.2.2:51950       4.150.240.254:443      ESTABLISHED
TCP    172.17.2.2:51951       172.202.65.254:443     ESTABLISHED
TCP    172.17.2.2:51952       13.107.253.254:443     ESTABLISHED
TCP    172.17.2.2:51954       13.107.246.254:443     ESTABLISHED
TCP    172.17.2.2:51955       150.171.70.254:443     ESTABLISHED
TCP    172.26.208.1:139       0.0.0.0:0              LISTENING
```

j’ai effectuer la commande nestat -an

Quel est le port d’écoute du terminal serveur ?

Le port d’écoute du terminale serveur est 0



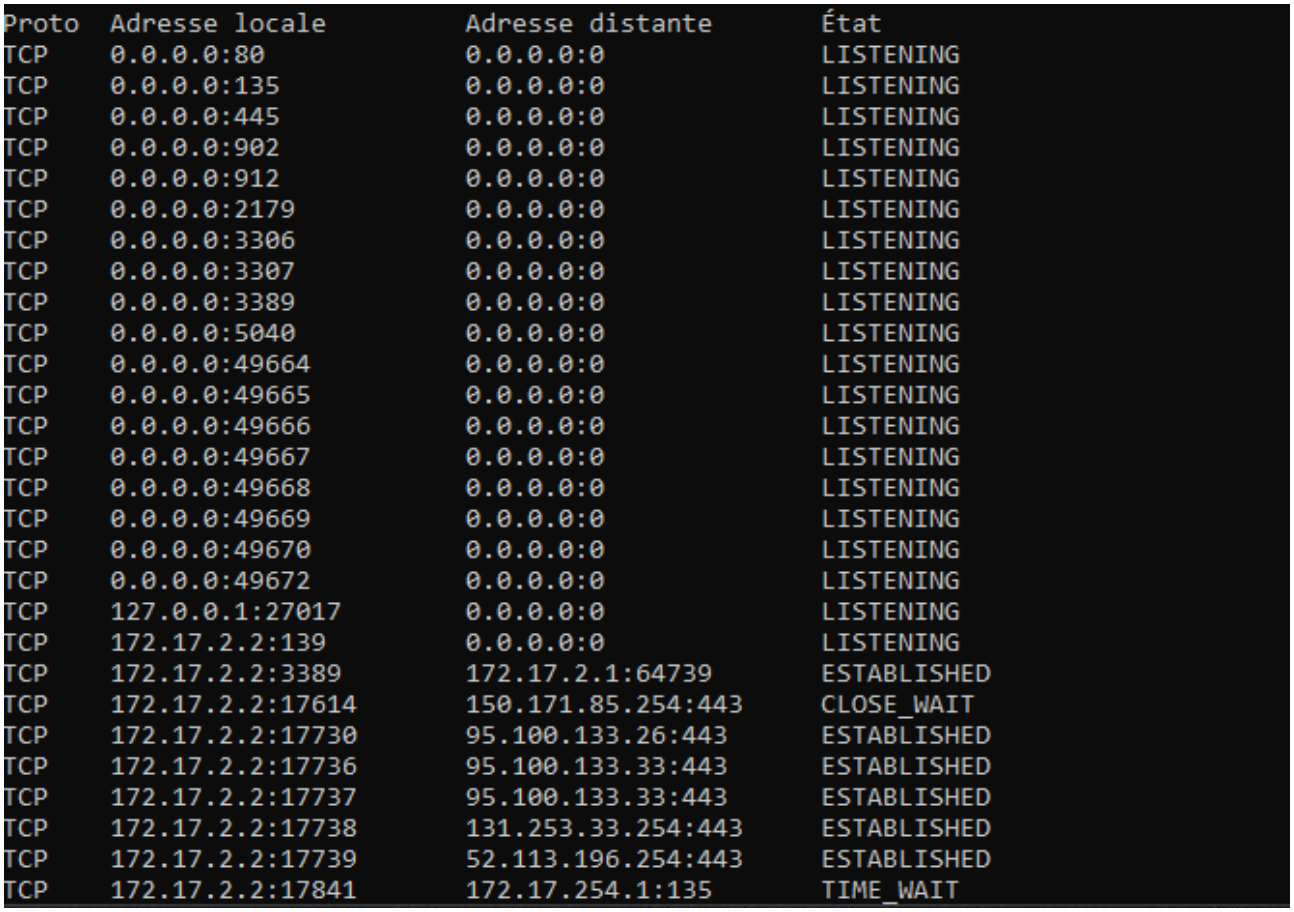
TP3

j’ai chercher mstc sur la zone de recherche et je l’ai ouverte

puis j’ai entre l’adresse ip de mon voisin

puis j’ai accéder a ca machine Windows

puis j’ai activer l’invite de commande puis taper nestat -an



```
Proto  Adresse locale         Adresse distante       État
TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
TCP    0.0.0.0:902            0.0.0.0:0              LISTENING
TCP    0.0.0.0:912            0.0.0.0:0              LISTENING
TCP    0.0.0.0:2179           0.0.0.0:0              LISTENING
TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING
TCP    0.0.0.0:3307           0.0.0.0:0              LISTENING
TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49672          0.0.0.0:0              LISTENING
TCP    127.0.0.1:27017        0.0.0.0:0              LISTENING
TCP    172.17.2.2:139         0.0.0.0:0              LISTENING
TCP    172.17.2.2:3389        172.17.2.1:64739       ESTABLISHED
TCP    172.17.2.2:17614       150.171.85.254:443     CLOSE_WAIT
TCP    172.17.2.2:17730       95.100.133.26:443      ESTABLISHED
TCP    172.17.2.2:17736       95.100.133.33:443      ESTABLISHED
TCP    172.17.2.2:17737       95.100.133.33:443      ESTABLISHED
TCP    172.17.2.2:17738       131.253.33.254:443     ESTABLISHED
TCP    172.17.2.2:17739       52.113.196.254:443     ESTABLISHED
TCP    172.17.2.2:17841       172.17.254.1:135       TIME_WAIT
```

comme on voit sur une ligne la connexion entre elle deux ordinateur a ete effectuer

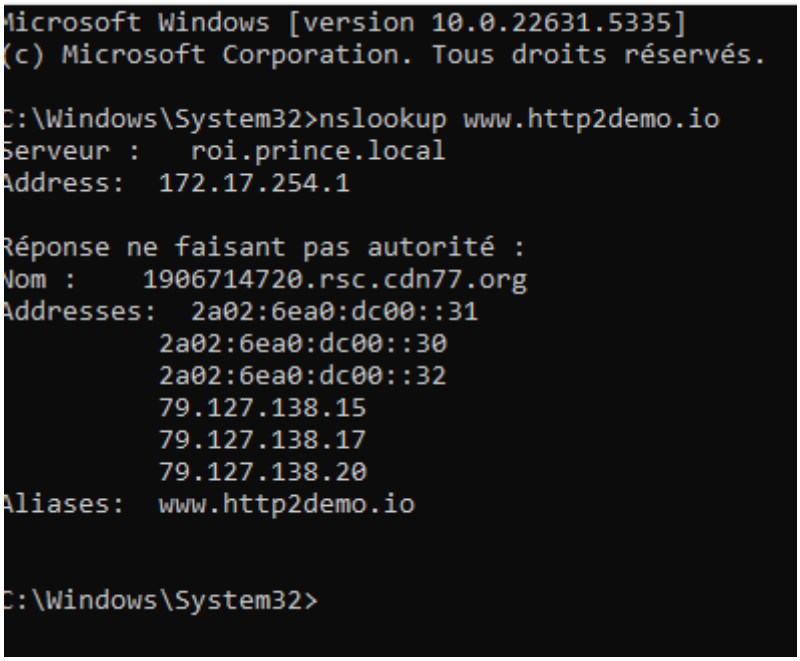
de l’ip 172.17.2.2 et 172.17.2.1

puis je me suis déconnecter

TP3

2.Capture de trames HTTP

Je lance Wireshark en tant-que administrateur



j’effectue la commande nslookup pour obtenir l’adresse ip du serveur web

Développez la section correspondant à l’en-tête Transport :

-Développez la section correspondant à l’en-tête Transport :

protocole port

-Quel est le nom du PDU encapsulant les données applicatives HTTP ?

Segment

-Quelle est la longueur de l’en-tête de transport ?

20 octet

-Quelles sont les valeurs décimale et hexadécimale correspondant aux ports source et destination ?

Source:
décimal=192.168.1.11
hexadécimal=9c:b6:d0:ee:c1:fd
destinataire:
décimal=89.187.167.42
hexadécimal=24:7f:20:1a:99:20

TP3

Développez la section correspondant à l'en-tête Réseau :

-Quelle est la longueur de l'en-tête de réseau ?

20 octet

-Repérez le champ Protocole figurant dans l'en-tête Réseau. Quelle est la valeur présente ?

La valeur est 6

-Que signifie-t-elle ?

Elle représente le protocole TCP

-Quelles sont les valeurs décimales et hexadécimales des adresses IP source et destination ?

Source:
décimale=192.168.1.11
hexadécimale=9c:b6:d0:ee:c1:fd
destinataire:
décimale=89;187.167.42
hexadécimale=24:7f:20:1a:99:20

Développez la section correspondant à l'en-tête Ethernet :

-Repérez le champ EtherType. Quel est la valeur contenue ?

La valeur est 0800

-Que signifie-t-elle ?

C'est le protocole IPV4

-Quelles sont les valeurs des adresses MAC destination et source ?

mac source =24:7f:20:1a:99:20
mac destination =9c:b6:d0:ee:c1:fd

Que signifie le contenu de ce champ pour chacun des 3 segments TCP ? Quelle est la raison de la mise en place de ce mode connecté ?

pour pouvoir récupéré les trame dans l'ordre et être sur d'avoir ressue tout les trame