

# TP3 – Les ports logiciels

## Sommaire

- 1. *Connexion sécurisée à une machine Linux depuis un client SSH Windows* .....2
- 2. *Connexion Bureau à distance (RDP)*.....9
- 3. *Capture de trames HTTP*..... 12

# 1. Connexion sécurisée à une machine Linux depuis un client SSH Windows

→ On télécharge **putty.exe** depuis la machine hôte :



→ On vérifie que la carte réseau de la machine serveur soit en **accès par pont** et qu'elle récupère **automatiquement** son adresse IP auprès du **serveur DHCP ROI (172 .17.X.Y)** :

DEB12Server - Settings

Basic Expert

Search settings

Réseau

Adapter 1 Adapter 2 Adapter 3 Adapter 4

Activer l'interface réseau

Mode d'accès réseau : **Accès par pont**

Name: Realtek PCIe GbE Family Controller

Type d'interface : Intel PRO/1000 MT Desktop (82540EM)

Mode Promiscuité : Refuser

Adresse MAC : 080027FB5BD4

Câble branché

Ports séries

Port 1 Port 2 Port 3 Port 4

OK Annuler Aide

```
GNU nano 7.2 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
auto enp0s3
iface enp0s3 inet dhcp
```

```

root@DEB12Server: ~#ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:fb:5b:d4 brd ff:ff:ff:ff:ff:ff
    inet 172.17.110.17/16 brd 172.17.255.255 scope global dynamic enp0s3
        valid_lft 86046sec preferred_lft 86046sec
    inet6 fe80::a00:27ff:fe5b:5bd4/64 scope link
        valid_lft forever preferred_lft forever

```

→ On vérifie les paramètres IP de la carte réseau sur la **machine physique** avec **ipconfig /all** pour s'assurer que les deux machines sont dans le **même réseau** :

```

Carte Ethernet Ethernet :

Suffixe DNS propre à la connexion. . . . : prince.local
Description. . . . . : Realtek PCIe GbE Family Controller
Adresse physique . . . . . : 74-56-3C-2F-9C-F0
DHCP activé. . . . . : Oui
Configuration automatique activée. . . . : Oui
Adresse IPv6 de liaison locale. . . . . : fe80::6b83:74d3:2ac4:5035%9(préféré)
Adresse IPv4. . . . . : 172.17.2.21(préféré)
Masque de sous-réseau. . . . . : 255.255.0.0
Bail obtenu. . . . . : vendredi 11 octobre 2024 14:40:52
Bail expirant. . . . . : samedi 12 octobre 2024 04:53:56
Passerelle par défaut. . . . . : 172.17.250.2
Serveur DHCP . . . . . : 172.17.254.1
IAID DHCPv6 . . . . . : 326391356
DUID de client DHCPv6. . . . . : 00-01-00-01-2C-DF-41-0E-74-56-3C-2F-9C-F0
Serveurs DNS. . . . . : 172.17.254.1
                        172.17.244.1
                        80.10.246.2
                        8.8.8.8
NetBIOS sur Tcpip. . . . . : Activé

```

\*Elles sont bien toutes les deux dans le **réseau ROI**.

→ On teste la **connectivité** entre les deux machines avec un **ping** :

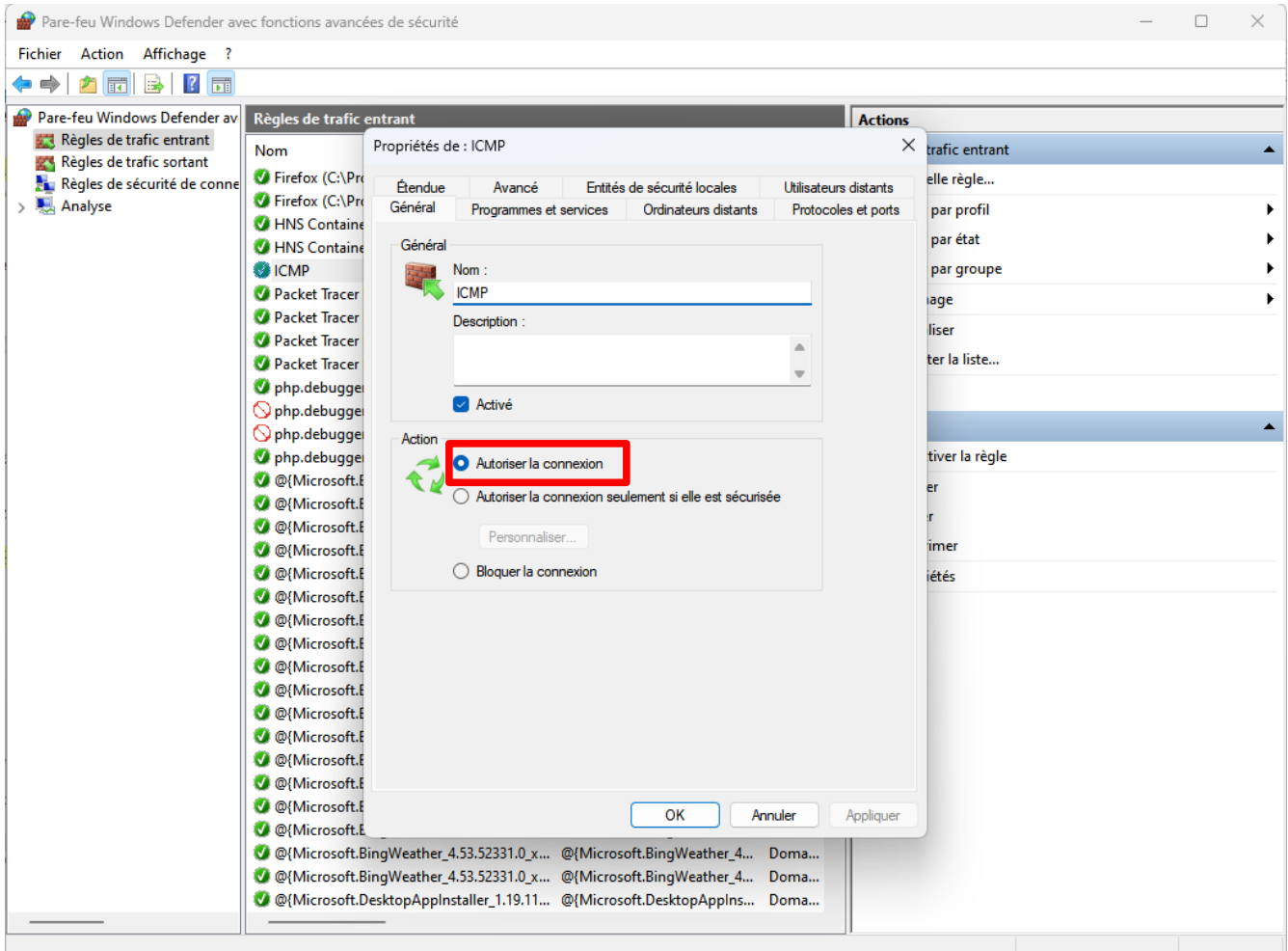
```

root@DEB12Server: ~#ping 172.17.2.21
PING 172.17.2.21 (172.17.2.21) 56(84) bytes of data.
64 bytes from 172.17.2.21: icmp_seq=1 ttl=128 time=0.932 ms
64 bytes from 172.17.2.21: icmp_seq=2 ttl=128 time=0.432 ms
64 bytes from 172.17.2.21: icmp_seq=3 ttl=128 time=0.360 ms
64 bytes from 172.17.2.21: icmp_seq=4 ttl=128 time=0.505 ms
^C
--- 172.17.2.21 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3069ms
rtt min/avg/max/mdev = 0.360/0.557/0.932/0.222 ms

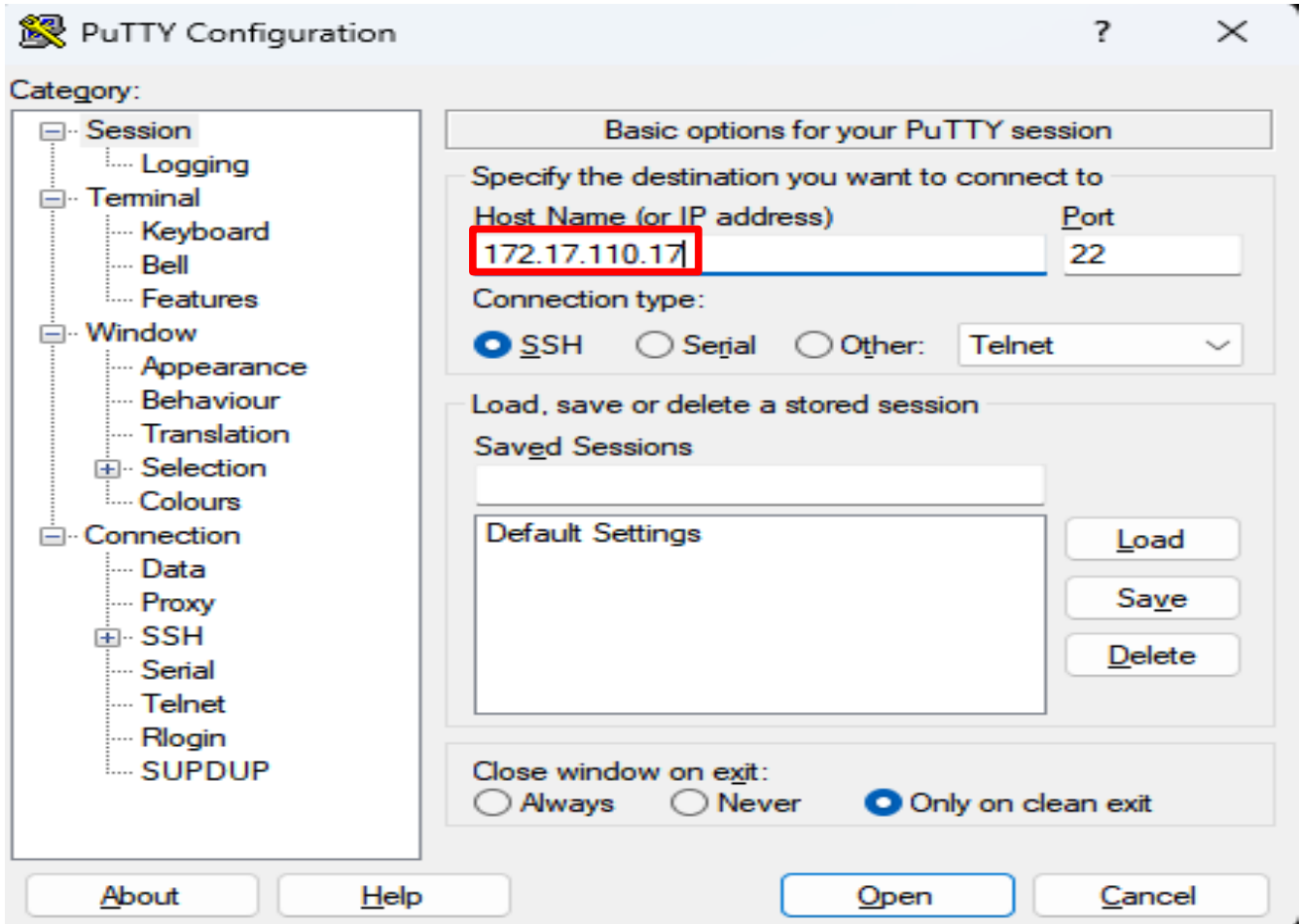
```

\* Les **trames** sont reçues par la machine hôte, la **connectivité** est bien présente.

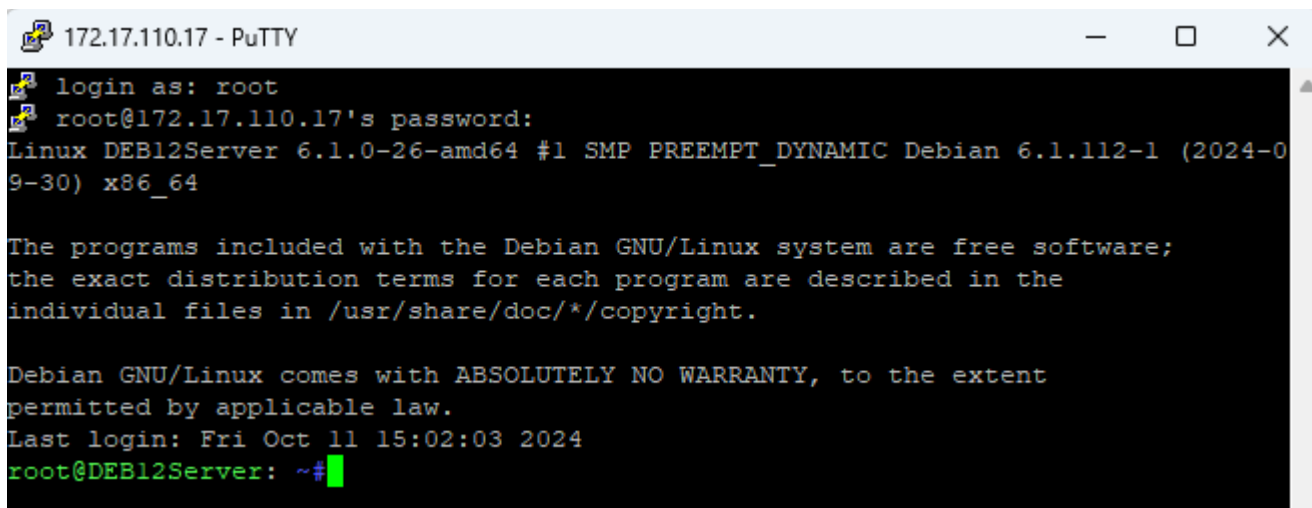
→ On autorise le **protocole ICMP** dans le **pare-feu Windows** en trafic entrant et sortant :



→ On lance **putty** depuis la machine hôte et on saisit l'IP de la machine serveur :



→ On ouvre une **session SSH** puis on saisit le **login** et le **mot de passe** :



→ On observe la **connexion TCP** qui a été établie avec la commande **ss -tan4** sur cette console :

```
root@DEB12Server: ~#ss -tan4
State  Recv-Q  Send-Q   Local Address:Port   Peer Address:Port   Process
LISTEN  0        128      0.0.0.0:22           0.0.0.0:*
ESTAB  0        64      172.17.110.17:22    172.17.2.21:50938
```

\* Le **port d'écoute** du **serveur SSH DEB12Server** est le port **22**.

\* Le **port dynamique** assigné par **Windows** au **client SSH** durant la connexion TCP est le port **50938**.

→ On saisit la commande **netstat** puis **netstat -an** sur la machine hôte :

```
C:\Windows\System32>netstat
Connexions actives

Proto  Adresse locale      Adresse distante    État
TCP    172.17.2.21:7680    G102-GB11:49479    TIME_WAIT
TCP    172.17.2.21:7680    G102-GB11:49481    TIME_WAIT
TCP    172.17.2.21:7680    G102-GB19:51108    TIME_WAIT
TCP    172.17.2.21:7680    G102-GB19:51114    TIME_WAIT
TCP    172.17.2.21:7680    G102-GB02:57645    TIME_WAIT
TCP    172.17.2.21:7680    G102-GB02:57648    TIME_WAIT
TCP    172.17.2.21:7680    G102-GB02:57650    TIME_WAIT
TCP    172.17.2.21:7680    G102-GB02:57651    TIME_WAIT
TCP    172.17.2.21:7680    G102-GB02:57653    TIME_WAIT
TCP    172.17.2.21:50311    20.199.120.151:https ESTABLISHED
TCP    172.17.2.21:50431    aviateur:microsoft-ds ESTABLISHED
TCP    172.17.2.21:50902    aviateur:microsoft-ds ESTABLISHED
TCP    172.17.2.21:50910    150.171.85.254:https CLOSE_WAIT
TCP    172.17.2.21:50912    13.107.226.254:https CLOSE_WAIT
TCP    172.17.2.21:50921    13.107.246.254:https CLOSE_WAIT
TCP    172.17.2.21:50926    13.107.252.254:https CLOSE_WAIT
TCP    172.17.2.21:50938    172.17.110.17:ssh    ESTABLISHED
TCP    172.17.2.21:50950    21.111.192.150:https ESTABLISHED
TCP    172.17.2.21:50957    52.123.242.159:https ESTABLISHED
TCP    172.17.2.21:50958    192.229.221.95:http  ESTABLISHED
TCP    172.17.2.21:50959    a95-100-200-73:https ESTABLISHED
TCP    172.17.2.21:50961    52.168.117.171:https ESTABLISHED
TCP    172.17.2.21:50962    13.107.18.254:https  ESTABLISHED
TCP    172.17.2.21:50963    150.171.73.254:https ESTABLISHED
TCP    172.17.2.21:50964    13.107.213.254:https ESTABLISHED
TCP    172.17.2.21:50965    204.79.197.222:https ESTABLISHED
TCP    172.17.2.21:50966    152.199.19.161:https ESTABLISHED
TCP    172.17.2.21:50967    13.107.246.43:https  ESTABLISHED
TCP    172.17.2.21:50968    20.187.64.58:https   ESTABLISHED
TCP    172.17.2.21:50969    152.199.19.161:https ESTABLISHED
TCP    172.17.2.21:50970    172.202.65.254:https ESTABLISHED
TCP    172.17.2.21:50971    40.112.186.181:https ESTABLISHED

TCP    172.17.2.21:50938    172.17.110.17:22    ESTABLISHED
```

# 7

→ On se **déconnecte** de la **session SSH** :

```
root@DEB12Server: ~#logout
```

## 2. Connexion Bureau à distance (RDP)

→ On récupère l'adresse IP de la machine physique du **voisin** :

**172.17.2.19**

→ On **ping** sa machine pour s'assurer de la connectivité entre nos machines :

```
C:\Users\nflavigny>ping 172.17.2.19

Envoi d'une requête 'Ping' 172.17.2.19 avec 32 octets de données :
Réponse de 172.17.2.19 : octets=32 temps<1ms TTL=128
Réponse de 172.17.2.19 : octets=32 temps=1 ms TTL=128
Réponse de 172.17.2.19 : octets=32 temps<1ms TTL=128
Réponse de 172.17.2.19 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 172.17.2.19:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
```

→ On saisit la commande **netstat -an** sur la machine hôte :

```
C:\Users\nflavigny>netstat -an

Connexions actives

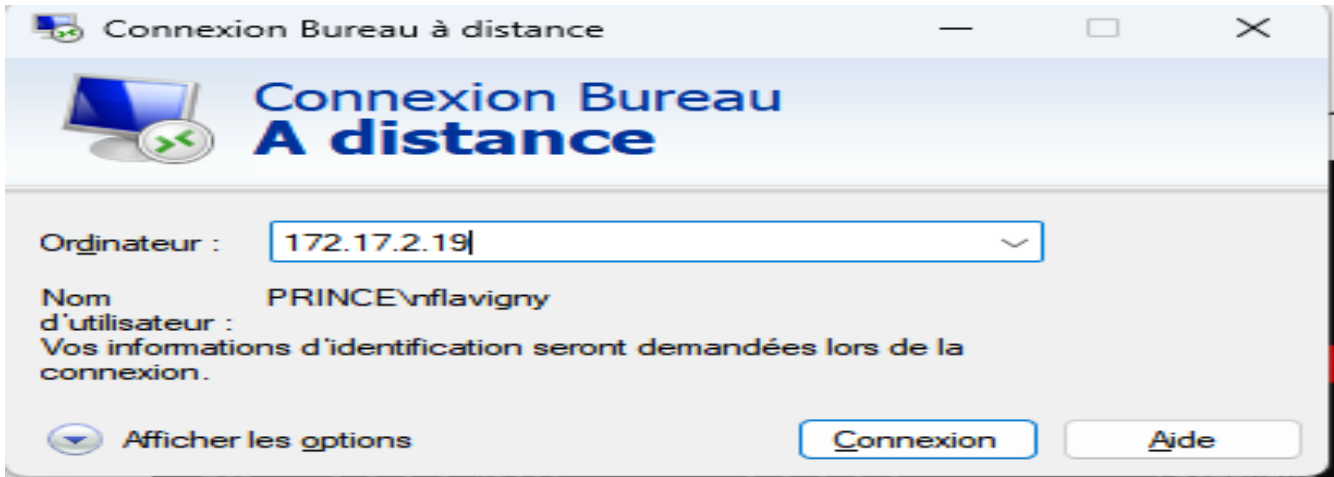
Proto Adresse locale Adresse distante État
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:2179 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
TCP 0.0.0.0:5040 0.0.0.0:0 LISTENING
TCP 0.0.0.0:7680 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING
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 172.17.2.21:139 0.0.0.0:0 LISTENING
TCP 172.17.2.21:7680 172.17.2.9:50211 TIME_WAIT
TCP 172.17.2.21:7680 172.17.2.9:50223 TIME_WAIT
TCP 172.17.2.21:7680 172.17.2.16:51359 TIME_WAIT
TCP 172.17.2.21:7680 172.17.2.24:57917 TIME_WAIT
TCP 172.17.2.21:7680 172.17.2.24:57918 TIME_WAIT
TCP 172.17.2.21:7680 172.17.2.24:57919 TIME_WAIT
```

\* Le port d'écoute du serveur Terminal Server est **3389**

→ On saisit **mstsc** dans la zone de recherche windows :



→ On saisit l'**adresse IP de notre voisin** puis on se connecte sur son bureau :



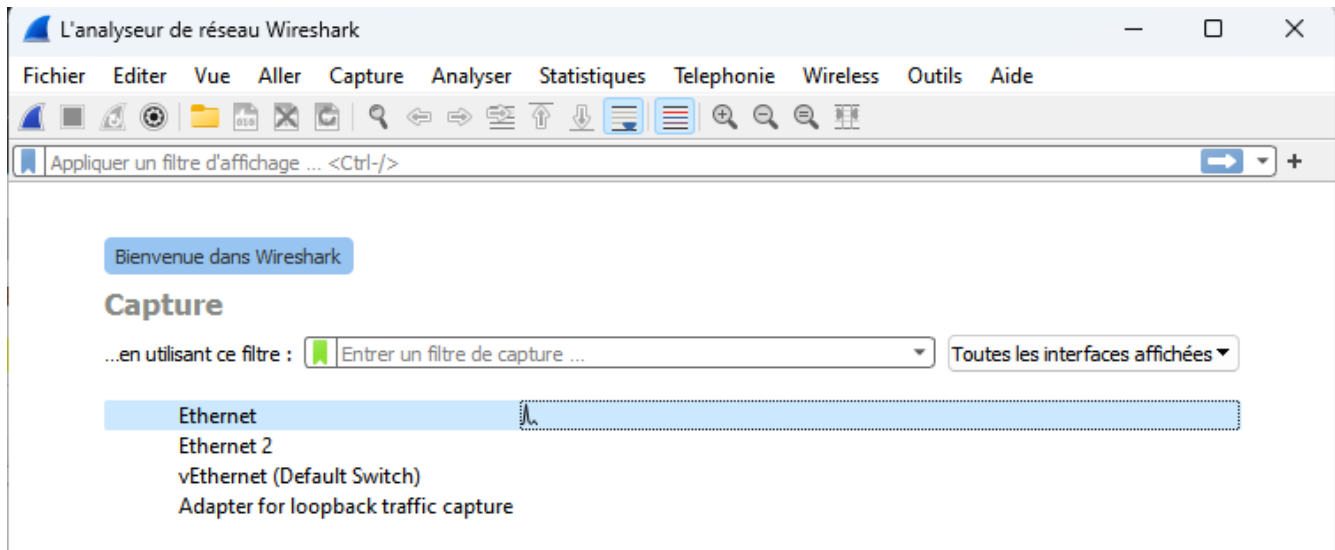
→ On saisit la commande **netstat -an** depuis son invite de commande :

```
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 0.0.0.0:50126 0.0.0.0:0 LISTENING
TCP 172.17.2.19:139 0.0.0.0:0 LISTENING
TCP 172.17.2.19:3389 172.17.2.21:51066 ESTABLISHED
TCP 172.17.2.19:7680 172.17.2.16:51381 TIME_WAIT
TCP 172.17.2.19:7680 172.17.2.16:51410 TIME_WAIT
TCP 172.17.2.19:7680 172.17.2.20:56879 TIME_WAIT
TCP 172.17.2.19:10300 172.17.2.16:51410 ESTABLISHED
```

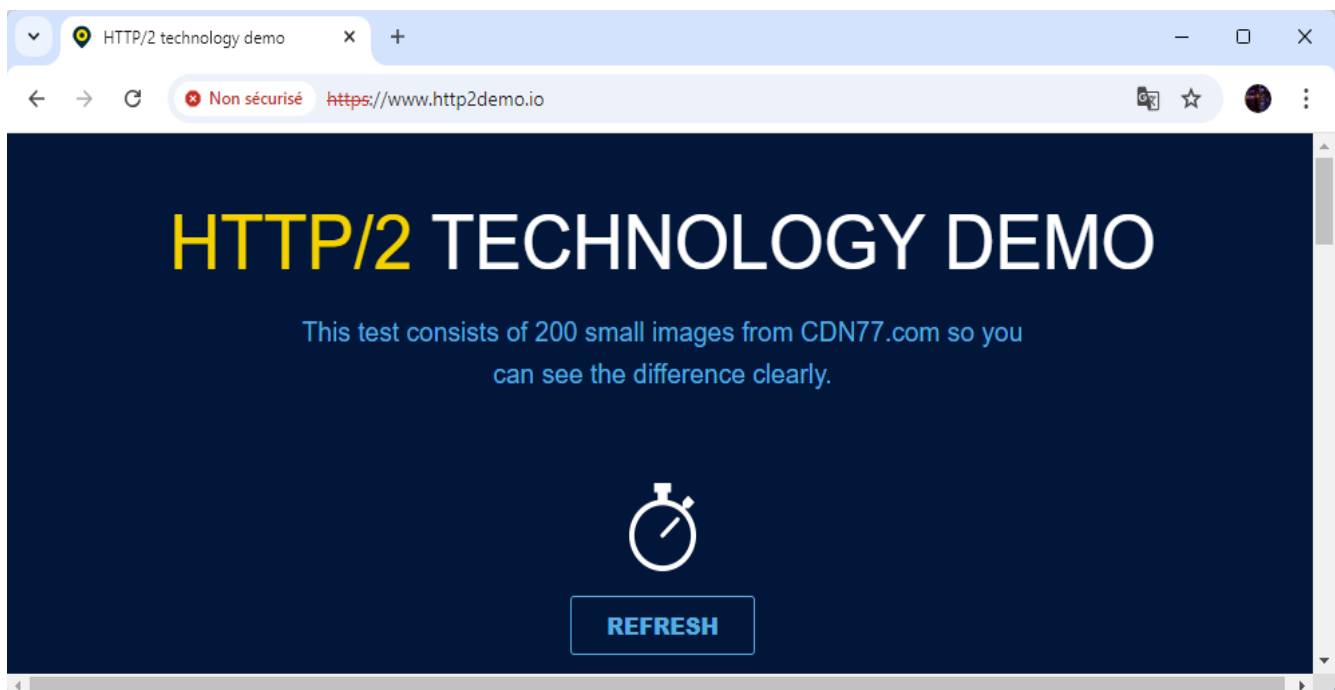
\* On se déconnecte de sa session en appuyant sur **déconnecter**

### 3. Capture de trames HTTP

→ On lance **Wireshark** en tant qu'**Administrateur** sur la machine physique puis on sélectionne la carte réseau :



→ On ouvre le navigateur internet et on affiche la page d'accueil du site <http://www.http2demo.io/> :



→ On saisit la commande **nslookup www.http2demo.io** pour trouver l'adresse IP du **serveur http** :

```
C:\Windows\system32>nslookup www.http2demo.io
Server:      bbox.lan
Address:     192.168.1.254

Non-authoritative answer:
Name:       1906714720.rsc.cdn77.org
Addresses:  2a02:6ea0:ca00::8
            2a02:6ea0:ca00::7
            84.17.50.9
            89.187.167.38
Aliases:   www.http2demo.io
```

No.	Source	Destination	Time	Protocol	Length	Info
786	192.168.1.5	84.17.50.9	8.716461	HTTP	675	GET / HTTP/1.1
788	84.17.50.9	192.168.1.5	8.756269	HTTP	385	HTTP/1.1 304 Not Modified
789	192.168.1.5	84.17.50.9	8.788369	HTTP	548	GET /css/style.css
790	192.168.1.5	84.17.50.9	8.788585	HTTP	552	GET /css/jssocials
804	192.168.1.5	84.17.50.9	8.815580	HTTP	563	GET /css/jssocials
811	192.168.1.5	84.17.50.9	8.816117	HTTP	556	GET /css/font-awes
812	192.168.1.5	84.17.50.9	8.816204	HTTP	600	GET /img/refresh-i
813	192.168.1.5	84.17.50.9	8.816294	HTTP	597	GET /img/cdn77logo
818	84.17.50.9	192.168.1.5	8.830074	HTTP	380	HTTP/1.1 304 Not Modified
819	84.17.50.9	192.168.1.5	8.835088	HTTP	384	HTTP/1.1 304 Not Modified
826	192.168.1.5	195.181.172.3	8.853423	HTTP	578	GET /http2/http1.h
827	84.17.50.9	192.168.1.5	8.856066	HTTP	384	HTTP/1.1 304 Not Modified

→ On applique un **filtre** où on spécifie l'adresse IP du **serveur http** qu'on vient de trouver :

No.	Time	Source	Destination	Protocol	Length	Info
8	2.187468	192.168.1.16	84.17.50.8	HTTP	703	GET / HTTP/1.1
19	2.211809	84.17.50.8	192.168.1.16	HTTP	426	HTTP/1.1 304 Not Modified
51	2.245654	192.168.1.16	84.17.50.8	HTTP	576	GET /css/style.css HTTP/1.1
56	2.249606	192.168.1.16	84.17.50.8	HTTP	580	GET /css/jssocials.css HTTP/1.1
57	2.251069	192.168.1.16	84.17.50.8	HTTP	591	GET /css/jssocials-theme-flat.css HTTP/1.1
58	2.251275	192.168.1.16	84.17.50.8	HTTP	584	GET /css/font-awesome.css HTTP/1.1
59	2.251350	192.168.1.16	84.17.50.8	HTTP	628	GET /img/refresh-icon.png HTTP/1.1
60	2.251954	192.168.1.16	84.17.50.8	HTTP	625	GET /img/cdn77logo.png HTTP/1.1
69	2.284817	84.17.50.8	192.168.1.16	HTTP	384	HTTP/1.1 304 Not Modified
70	2.287802	84.17.50.8	192.168.1.16	HTTP	380	HTTP/1.1 304 Not Modified
71	2.289786	84.17.50.8	192.168.1.16	HTTP	384	HTTP/1.1 304 Not Modified
72	2.290798	84.17.50.8	192.168.1.16	HTTP	384	HTTP/1.1 304 Not Modified

→ On récupère la **trame** correspondant à la **requête http** puis on développe la section **protocole applicatif** :

The screenshot shows a Wireshark capture of network traffic. The top pane, 'Packet List', shows a list of packets. Packet 8 is highlighted in red, with its details expanded in the bottom pane. The details pane shows the following information:

```

GET / HTTP/1.1\r\n
Host: www.http2demo.io\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6611.116 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
Cookie: _ga=GA1.2.634314130.1727374079; _gid=GA1.2.1674129542.1727374079; _gat=UA1.2.1727374079; _ga=GA1.2.634314130.1727374079; _gid=GA1.2.1674129542.1727374079; _gat=UA1.2.1727374079\r\n
If-None-Match: W/"5aa91b6d-19b00"\r\n
\r\n
[Response in frame 19]
[Full request URI: http://www.http2demo.io/]
  
```

→ On développe l'en-tête de transport :

```

▶ Frame 8: 703 bytes on wire (5624 bits), 703 bytes captured (5624
▶ Ethernet II, Src: Intel_b7:eb:84 (d8:3b:bf:b7:eb:84), Dst: Sagemc
▶ Internet Protocol Version 4, Src: 192.168.1.16, Dst: 84.17.50.8
▼ Transmission Control Protocol, Src Port: 60564, Dst Port: 80, Seq
  Source Port: 60564
  Destination Port: 80
  [Stream index: 2]
  [Stream Packet Number: 1]
  ▶ [Conversation completeness: Incomplete (12)]
  [TCP Segment Len: 649]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 2850996978
  [Next Sequence Number: 650 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 3770150408
  0101 .... = Header Length: 20 bytes (5)
  ▶ Flags: 0x018 (PSH, ACK)
  Window: 1026
  [Calculated window size: 1026]
  [Window size scaling factor: -1 (unknown)]
  Checksum: 0x4a75 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  ▶ [Timestamps]
  ▶ [SEQ/ACK analysis]
  TCP payload (649 bytes)
  Hypertext Transfer Protocol
  
```

\* Le nom du **protocole** utilisé par une trame http est le protocole **TCP**.

\* Le nom du **PDU** encapsulant les **données applicatives http** est un **segment**.

\* La longueur de l'**en-tête de transport** est de **20 octets**.

\* Les valeurs **décimales** correspondant aux **port source** et aux **port destination** sont les ports **60564** et **80**. Les valeurs **hexadécimales** correspondantes sont **ec 94** et **00 50**.

→ On développe l'en-tête Réseau :

```

▶ Frame 8: 703 bytes on wire (5624 bits), 703 bytes captured (5624
▶ Ethernet II, Src: Intel_b7:eb:84 (d8:3b:bf:b7:eb:84), Dst: Sagemc
▼ Internet Protocol Version 4, Src: 192.168.1.16, Dst: 84.17.50.8
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 689
  Identification: 0xe73d (59197)
  ▶ 010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.16
  Destination Address: 84.17.50.8
  [Stream index: 1]
  Transmission Control Protocol, Src Port: 60564, Dst Port: 80, Seq
  Hypertext Transfer Protocol
  
```

\* La **longueur de l'en-tête réseau** est de **20 octets**.

\* La valeur du **champ protocole** figurant dans l'en-tête réseau est **06**. Elle représente le **protocole TCP**.

\* Les valeurs **décimales** des **adresses ip source** et **destination** sont **192.168.1.16** et **87.17.50.8** soit **c0 a8 01 10** et **54 11 32 08** en **hexadécimale**.

→ On développe **l'en-tête Ethernet** :

```

▶ Frame 8: 703 bytes on wire (5624 bits). 703 bytes captured (5624
▼ Ethernet II, Src: Intel_b7:eb:84 (d8:3b:bf:b7:eb:84), Dst: SagemcomBroa_11:d5:45 (b0:bb:e5:11:d5:45)
  Destination: SagemcomBroa_11:d5:45 (b0:bb:e5:11:d5:45)
  Source: Intel_b7:eb:84 (d8:3b:bf:b7:eb:84)
  Type: IPv4 (0x0800)
  [Stream index: 2]
▶ Internet Protocol Version 4, Src: 192.168.1.16, Dst: 87.17.50.8
▶ Transmission Control Protocol, Src Port: 60564, Dst Port: 80, Seq: 662110, Win: 64240, Len: 0
▶ Hypertext Transfer Protocol
0000  b0 bb e5 11 d5 45 d8 3b bf b7 eb 84 08 00 45 00 .....E.;
0010  02 b1 e7 3d 40 00 80 06 00 00 c0 a8 01 10 54 11 ...=@...
0020  32 08 ec 94 00 50 a9 ee c2 f2 e0 b7 ee 08 50 18 2... P..
0030  04 02 4a 75 00 00 47 45 54 20 2f 20 48 54 54 50 ..Ju..GE
0040  2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e /1.1..Ho
0050  68 74 74 70 32 64 65 6d 6f 2e 69 6f 0d 0a 43 6f http2dem
0060  6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnection
0070  6c 69 76 65 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 live..Ca
0080  72 6f 6c 3a 20 6d 61 78 2d 61 67 65 3d 30 0d 0a rol: max
0090  55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 Upgrade-

```

\* Le **champ EtherType** se situe sur les **2 derniers octets** de l'en-tête Ethernet soit les octets **13** et **14**. La valeur contenue est **08 00** qui signifie **IPv4**.

\* Les valeurs des **adresses MAC destination** et **source** sont **b0:bb:e5:11:d5:45** et **d8:3b:bf:b7:eb:84**.

→ On modifie le **filtre** et on réalise une capture d'écran des **3 trames** mettant en place la **connexion TCP** entre le client et le serveur :

16	192.168.71.28	84.17.50.9	1.274791	TCP	54 62091 → 80 [FIN, ACK] Seq=1 Ack=1 Win=511 Len=0
17	192.168.71.28	84.17.50.9	1.274826	TCP	54 62089 → 80 [FIN, ACK] Seq=1 Ack=1 Win=515 Len=0
18	192.168.71.28	84.17.50.9	1.274860	TCP	54 62092 → 80 [FIN, ACK] Seq=1 Ack=1 Win=514 Len=0
19	192.168.71.28	89.187.167.38	1.275226	TCP	66 62109 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=146...
20	192.168.71.28	89.187.167.38	1.338044	TCP	66 62110 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=146...
23	89.187.167.38	192.168.71.28	1.475707	TCP	66 80 → 62109 [SYN, ACK] Seq=0 Ack=1 Win=61320 Le...
24	89.187.167.38	192.168.71.28	1.475707	TCP	66 80 → 62110 [SYN, ACK] Seq=0 Ack=1 Win=61320 Le...
25	195.181.172.3	192.168.71.28	1.475707	TCP	54 80 → 62096 [ACK] Seq=1 Ack=2 Win=3108 Len=0
28	192.168.71.28	89.187.167.38	1.475885	TCP	54 62109 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0
29	192.168.71.28	89.187.167.38	1.475981	TCP	54 62110 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0
30	84.17.50.9	192.168.71.28	1.476173	TCP	54 80 → 62092 [ACK] Seq=1 Ack=2 Win=1946 Len=0
31	84.17.50.9	192.168.71.28	1.476173	TCP	54 80 → 62091 [ACK] Seq=1 Ack=2 Win=1981 Len=0
32	84.17.50.9	192.168.71.28	1.476173	TCP	54 80 → 62090 [ACK] Seq=1 Ack=2 Win=1912 Len=0
33	195.181.172.3	192.168.71.28	1.476173	TCP	54 80 → 62097 [ACK] Seq=1 Ack=2 Win=3093 Len=0
34	195.181.172.3	192.168.71.28	1.476173	TCP	54 80 → 62098 [ACK] Seq=1 Ack=2 Win=3107 Len=0
35	195.181.172.3	192.168.71.28	1.476173	TCP	54 80 → 62094 [ACK] Seq=1 Ack=2 Win=3124 Len=0

53	192.168.71.28	89.187.167.38	1.607353	HTTP	552 GET /css/jssocials.css HTTP/1.1
54	192.168.71.28	89.187.167.38	1.608158	TCP	66 62111 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=146...
55	192.168.71.28	89.187.167.38	1.608437	TCP	66 62112 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=146...
56	192.168.71.28	89.187.167.38	1.608672	TCP	66 62113 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=146...
57	192.168.71.28	89.187.167.38	1.608905	TCP	66 62114 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=146...
63	89.187.167.38	192.168.71.28	1.633430	TCP	66 80 → 62114 [SYN, ACK] Seq=0 Ack=1 Win=61320 Le...
64	89.187.167.38	192.168.71.28	1.633430	TCP	66 80 → 62112 [SYN, ACK] Seq=0 Ack=1 Win=61320 Le...
65	89.187.167.38	192.168.71.28	1.633430	TCP	66 80 → 62113 [SYN, ACK] Seq=0 Ack=1 Win=61320 Le...
66	192.168.71.28	89.187.167.38	1.633659	TCP	54 62114 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0
67	192.168.71.28	89.187.167.38	1.633736	TCP	54 62112 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0
68	192.168.71.28	89.187.167.38	1.633761	TCP	54 62113 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0

\* Il y a ici **5 connexions TCP** établies.