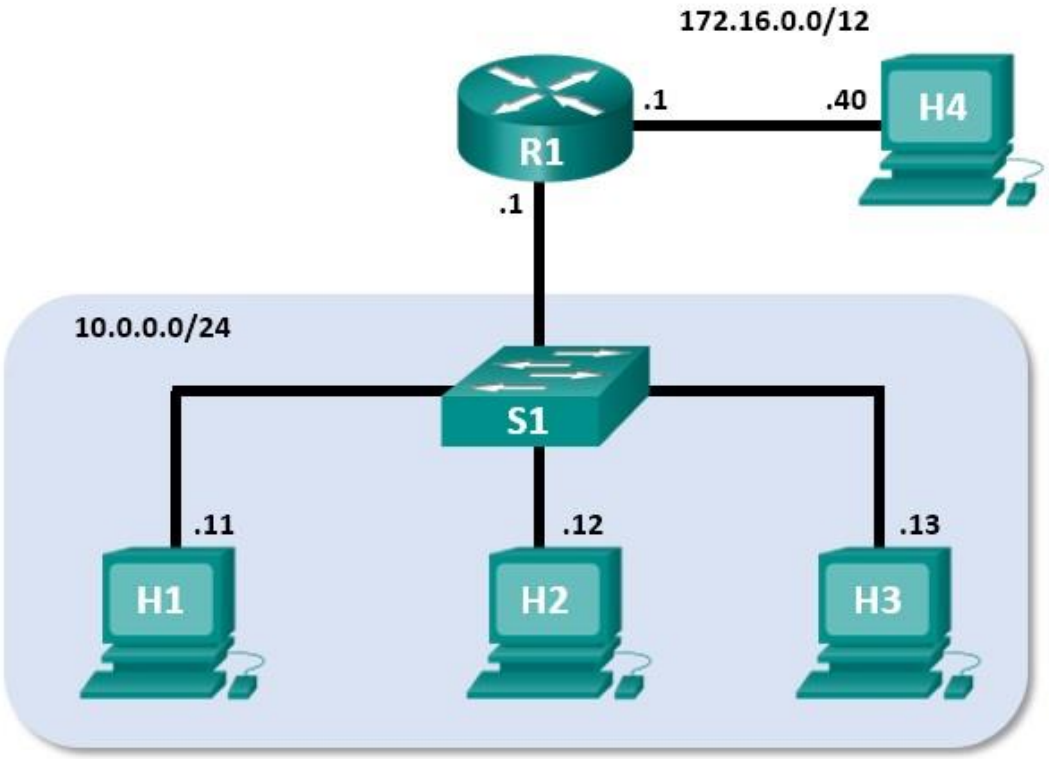
Travaux pratiques – Utilisation de Wireshark pour observer la connexion TCP en trois étapes

Topologie de Mininet



Objectifs

Partie 1 : Préparer les hôtes pour la capture du trafic

Partie 2 : Analyser les paquets à l'aide de Wireshark Partie

3 : Afficher les paquets à l'aide de tcpdump

Contexte/scénario

Au cours de ces travaux pratiques, vous utiliserez Wireshark pour capturer et examiner les paquets générés entre le navigateur de l'ordinateur en utilisant le protocole HTTP (Hypertext Transfer Protocol) et un serveur web, tel que www.google.com. Lorsqu'une application, comme le protocole HTTP ou FTP (File Transfer Protocol) démarre d'abord sur un hôte, TCP utilise la connexion en trois étapes pour établir une session TCP fiable entre les deux hôtes. Par exemple, lorsqu'un ordinateur utilise un navigateur web pour naviguer sur Internet, une connexion en trois étapes est lancée et une session est établie entre l'ordinateur hôte et le serveur web. Un ordinateur peut avoir des sessions TCP actives, multiples et simultanées avec différents sites web.

Ressources requises

- Poste de travail virtuel CyberOps
- Accès Internet

Partie 1 : Préparer les hôtes pour la capture du trafic

a. Démarrez la machine virtuelle CyberOps. Connectez-vous avec le nom d'utilisateur **analyst** et le mot de passe **cyberops**.

b. Démarrez Mininet.

```
[analyst@secOps ~]$ sudo lab.support.files/scripts/cyberops_topo.py
```

c. Démarrez les hôtes H1 et H4 sur Mininet.

```
*** À partir de l'interface de ligne de commande :
mininet> xterm H1 mininet>
xterm H4
```

d. Démarrez le serveur web sur H4.

```
[root@secOps analyst]#
/home/analyst/lab.support.files/scripts/reg_server_start.sh
```

e. Démarrez le navigateur sur H1. Ce processus peut prendre quelques instants.

```
[root@secOps analyst]# firefox &
```

f. Une fois la fenêtre Firefox ouverte, démarrez une session tcpdump sur le terminal **Node: H1** et envoyez la sortie vers un fichier appelé **capture.pcap**. L'option -v affiche la progression du processus. Le processus de capture s'arrête après la capture de 50 paquets, car il est configuré avec l'option -c 50.

```
[root@secOps analyst]# tcpdump -i H1-eth0 -v -c 50 -w
/home/analyst/capture.pcap
```

g. Après le démarrage de tcpdump, accédez rapidement à 172.16.0.40 dans le navigateur Firefox.

Partie 2 : Analyser les paquets à l'aide de Wireshark

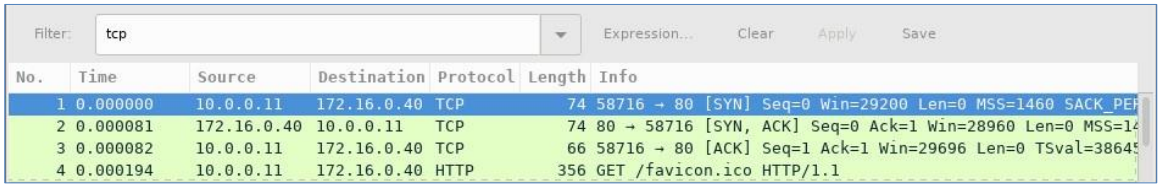
Étape 1 : Appliquez un filtre à la capture enregistrée.

a. Appuyez sur Entrée pour afficher l'invite de commande. Lancez Wireshark sur **Node: H1**. Lorsque le message d'avertissement s'affiche, cliquez sur **OK** pour confirmer l'exécution de Wireshark en tant que super utilisateur.

```
[root@secOps analyst]# wireshark-gtk &
```

b. Dans Wireshark, cliquez sur **File** > **Open**. Sélectionnez le fichier pcap enregistré sous /home/analyst/capture.pcap.

c. Appliquez un filtre **tcp** à la capture. Dans cet exemple, les 3 premières trames représentent le trafic d'intérêt.



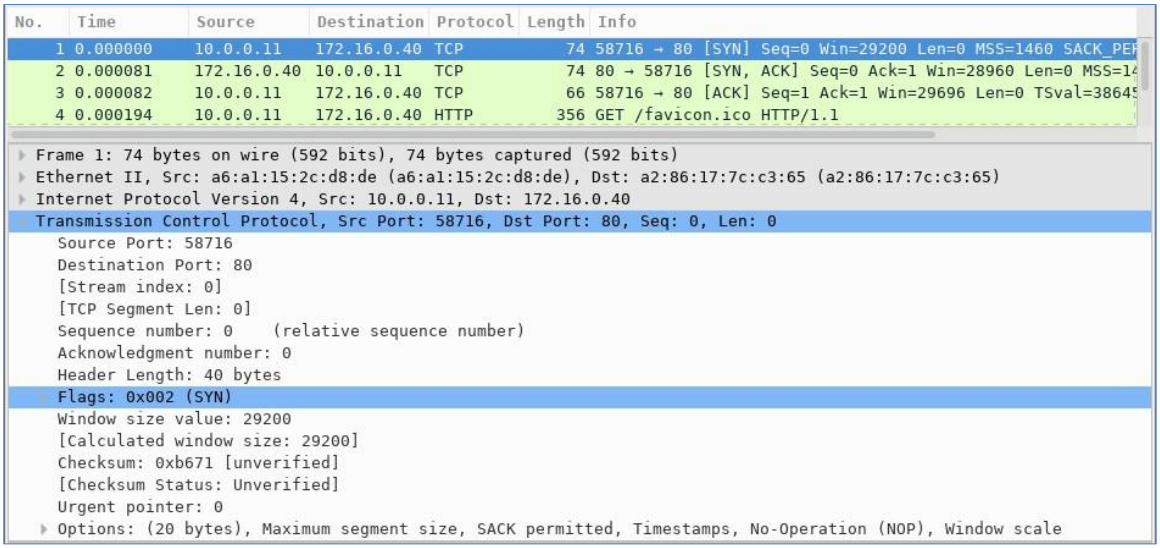
Étape 2 : Examinez les informations au sein des paquets, y compris les adresses IP, les numéros de port TCP et les indicateurs de contrôle TCP.

a. Dans cet exemple, la trame 1 correspond au début de la connexion en trois étapes entre l'ordinateur et le serveur sur H4. Dans le volet de la liste des paquets (section supérieure de la fenêtre principale), sélectionnez le premier paquet, le cas échéant.

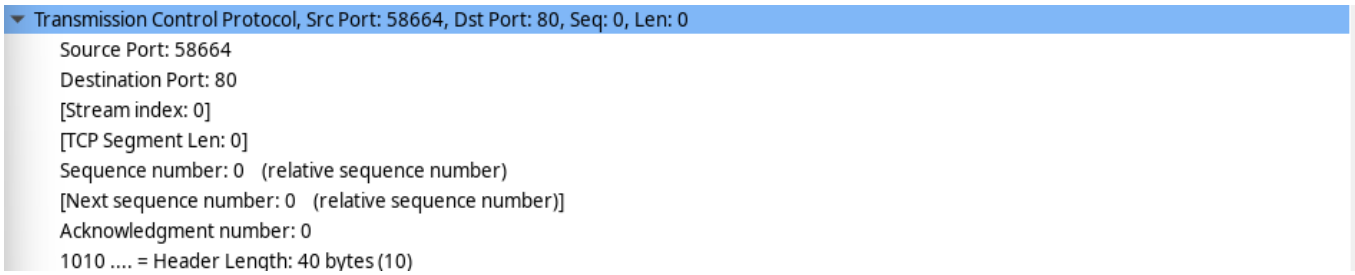
b. Cliquez sur la **flèche** à gauche du protocole TCP (Transmission Control Protocol) dans le volet de détails des paquets pour développer et examiner les données TCP. Localisez les informations sur les ports source et de destination.

c. Cliquez sur la **flèche** à gauche des indicateurs. Une valeur de 1 signifie que l'indicateur est défini. Repérez l'indicateur défini dans ce paquet.

Remarque : vous devrez peut-être modifier la taille des fenêtres du haut et du milieu dans Wireshark pour afficher les informations nécessaires.

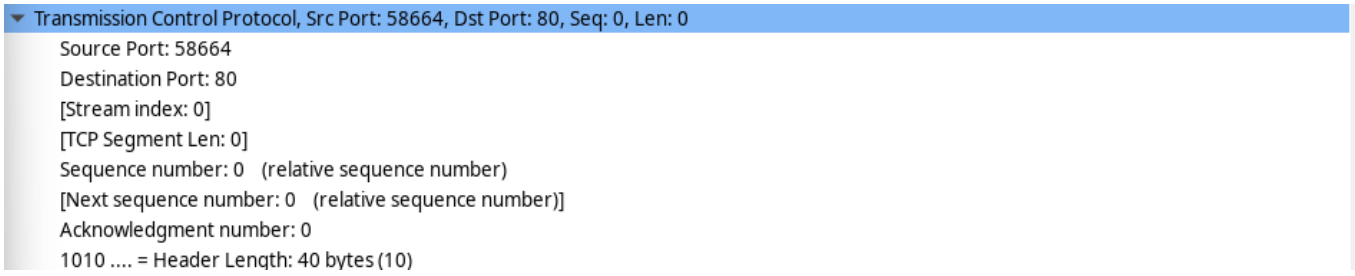


Quel est le numéro du port source TCP ? port source : 58664



Comment classifieriez-vous le port source ? c'est un port pas connu car il est au-dessus 1024

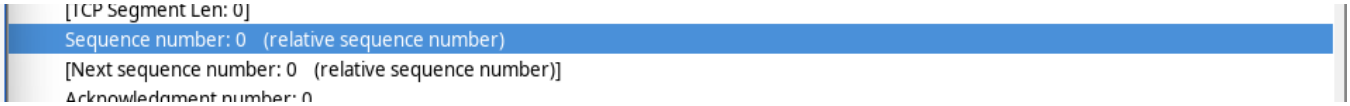
Quel est le numéro du port de destination TCP ? port 80



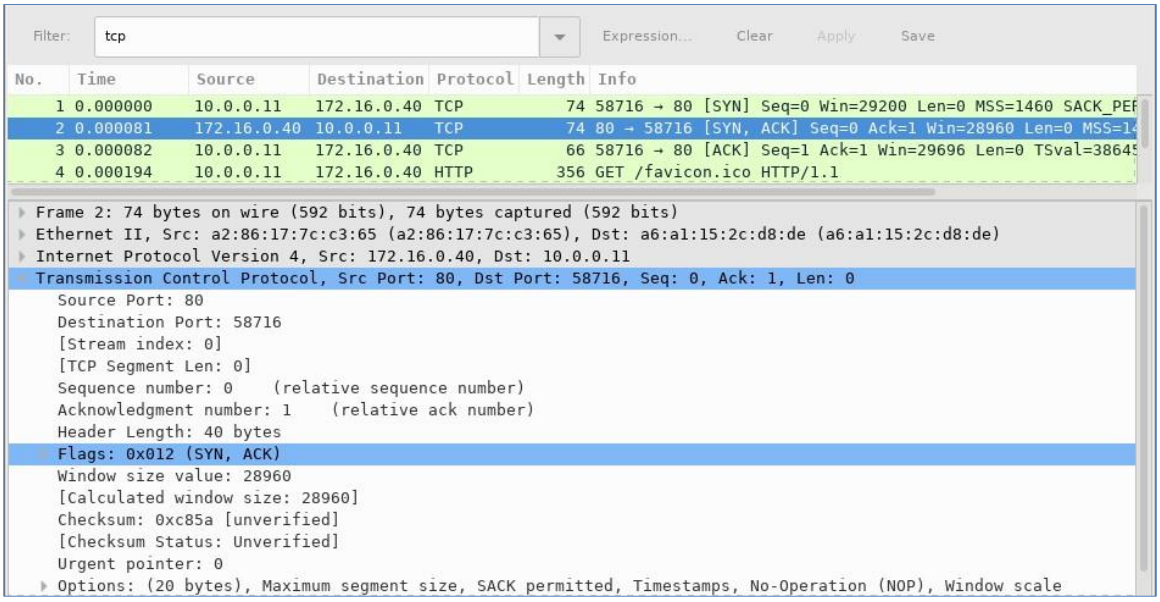
Comment classifieriez-vous le port de destination ? port le source est 80 ce qui veut dire qu'on accéder a un serveur HTTP

Quel indicateur est défini ? (plusieurs réponses possibles) c'est 0

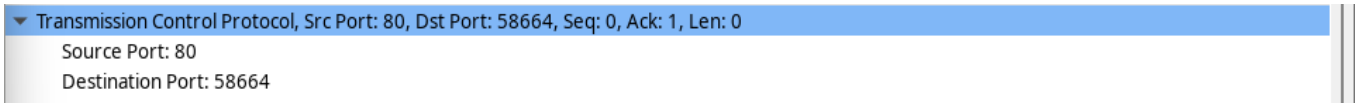
Sur quoi le numéro d'ordre relatif est-il défini ? sur la prochaine séquence



d. Sélectionnez le paquet suivant dans la connexion en trois étapes. Dans cet exemple, il s'agit de la trame 2. C'est la réponse du serveur web à la requête initiale de démarrage d'une session.



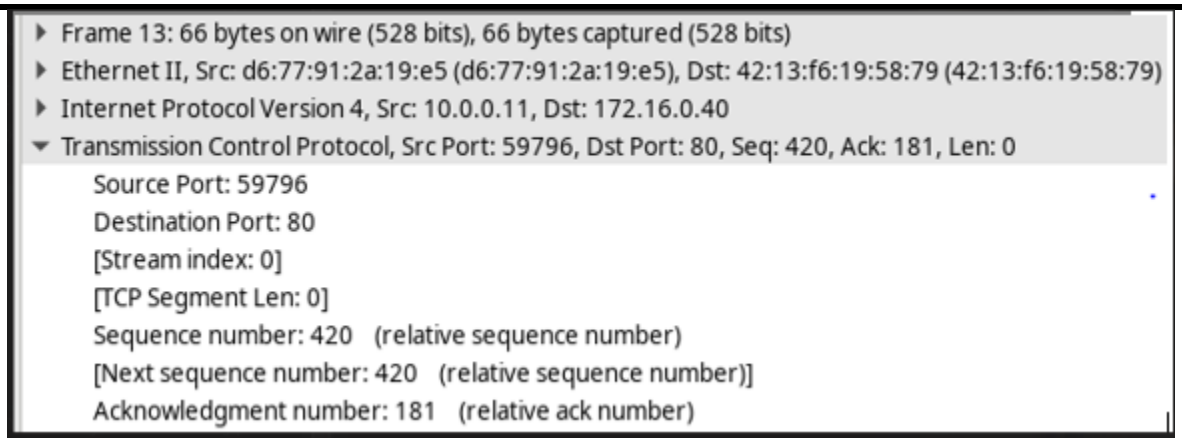
Quelles sont les valeurs des ports source et de destination ? port de destisnation : 58664 et le port source : 80



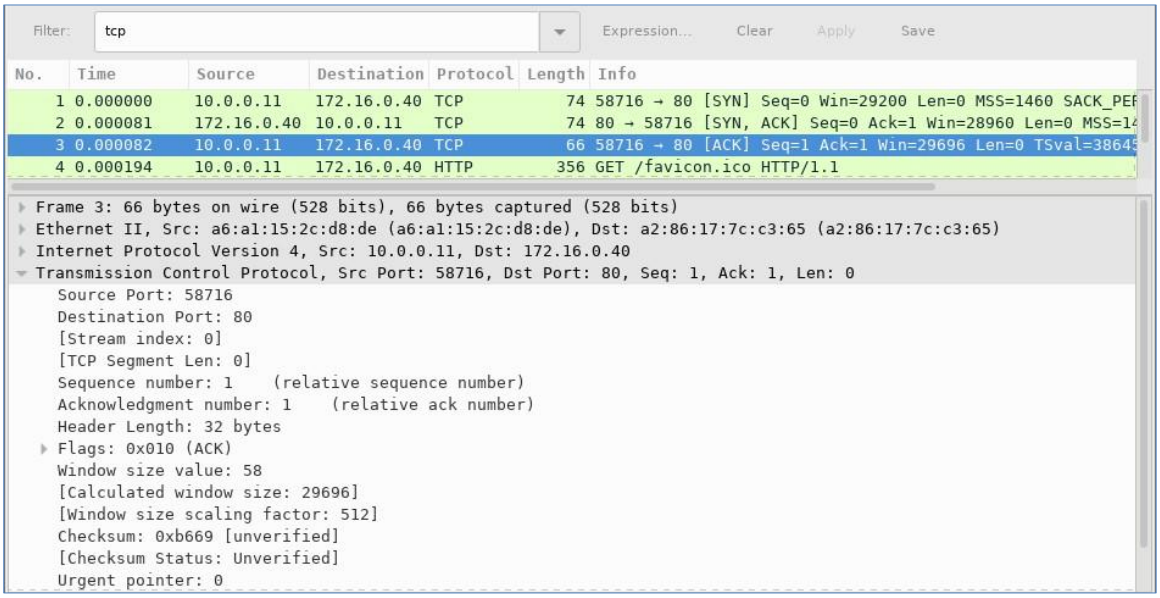
Quels sont les indicateurs définis ?

Sequence number: 0 (relative sequence number)
[Next sequence number: 0 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)

Sur quelle valeur les numéros d'ordre relatif et d'accusé de réception sont-ils définis ?

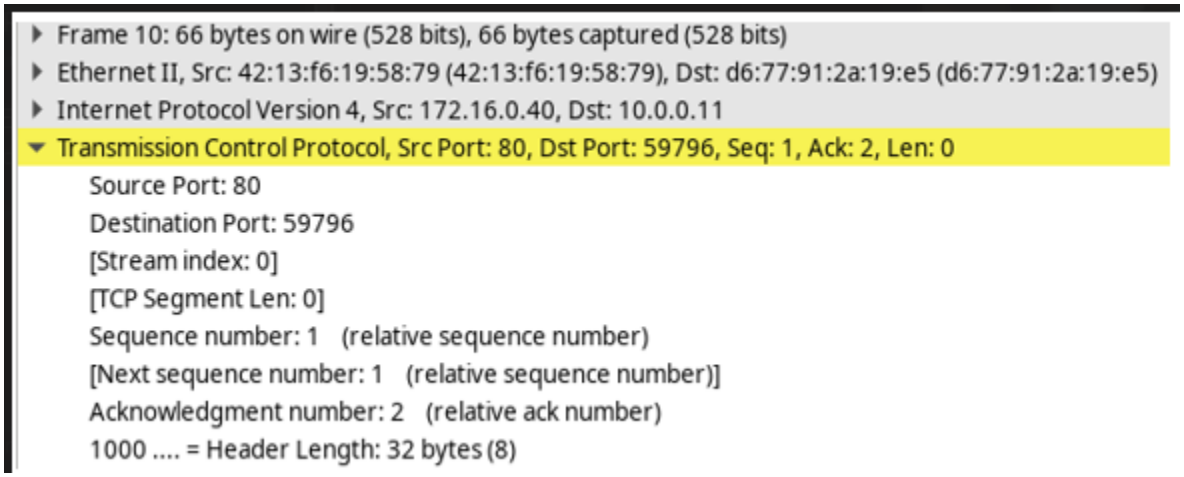


e. Enfin, sélectionnez le troisième paquet dans la connexion en trois étapes.



Examinez le troisième et dernier paquet de la connexion.

Quel indicateur est défini ? (plusieurs réponses possibles)



Les numéros d'ordre relatif et d'accusé de réception sont définis sur 1 comme point de départ. La connexion TCP est désormais établie et la communication entre l'ordinateur source et le serveur web peut commencer.

Partie 3 : Afficher les paquets à l'aide de tcpdump

Vous pouvez également afficher le fichier pcap et appliquer un filtre pour obtenir les informations souhaitées.

a. Ouvrez une nouvelle fenêtre du terminal et saisissez **man tcpdump**. **Remarque** : vous devrez peut-être appuyer sur Entrée pour afficher l'invite.

Parcourez ou recherchez dans les pages de manuel fournies avec le système d'exploitation Linux les options pour sélectionner les informations souhaitées dans le fichier pcap.

```
[analyst@secOps ~]# man tcpdump
TCPDUMP(1)                  General Commands Manual                 TCPDUMP(1)
 NOM        tcpdump - dump traffic on a
network
 SYNOPSIS        tcpdump [ -AbdDefhHIJKlLnNOpqStuUvxX# ] [ -B
buffer_size ]                [ -c count ]
               [ -C file_size ] [ -G rotate_seconds ] [ -F file ]
               [ -i interface ] [ -j tstamp_type ] [ -m module ] [ -M secret ]
               [ --number ] [ -Q in|out|inout ]
               [ -r file ] [ -V file ] [ -s snaplen ] [ -T type ] [ -w file ]
               [ -W filecount ]
               [ -E spi@ipaddr algo:secret,...  ]
               [ -y datalinktype ] [ -z postrotate-command ] [ -Z user ]
               [ --time-stamp-precision=tstamp_precision ]
               [ --immediate-mode ] [ --version ]
               [ expression ] <some
output omitted>
```

Pour effectuer une recherche dans les pages de manuel, vous pouvez utiliser les symboles / (recherche vers le bas) ou ? (recherche vers le haut) pour rechercher des termes spécifiques, **n** pour afficher la correspondance suivante et **q** pour quitter la fenêtre de recherche. Par exemple, pour rechercher les informations concernant le commutateur -r, saisissez **/r**. Saisissez **n** pour afficher la correspondance suivante. Comment se comporte le routeur **-r** ?

```
-r file
       Read packets from file (which was created with the -w option  or
       by  other  tools  that  write  pcap or pcap-ng files).  Standard
       input is used if file is ``-''.
```

b. Sur le même terminal, ouvrez le fichier de capture à l'aide de la commande suivante pour afficher les 3 premiers paquets TCP capturés :

```
[analyst@secOps ~]# tcpdump -r /home/analyst/capture.pcap tcp -c 3 reading
from file capture.pcap, link-type EN10MB (Ethernet)
13:58:30.647462 IP 10.0.0.11.58716 > 172.16.0.40.http: Flags [S], seq
2432755549, win 29200, options [mss 1460,sackOK,TS val 3864513189 ecr
0,nop,wscale 9], length 0
13:58:30.647543 IP 172.16.0.40.http > 10.0.0.11.58716: Flags [S.], seq
1766419191, ack 2432755550, win 28960, options [mss 1460,sackOK,TS val
50557410 ecr 3864513189,nop,wscale 9], length 0
```

```
13:58:30.647544 IP 10.0.0.11.58716 > 172.16.0.40.http: Flags [.], ack 1, win
58, options [nop,nop,TS val 3864513189 ecr 50557410], length 0
```

Pour afficher la connexion en trois étapes, vous devrez peut-être augmenter le nombre de lignes après l'option **-c**.

```
[analyst@secOps ~]$ tcpdump -r /home/analyst/capture.pcap tcp -c 3 reading from file capture.pcap, link-type EN10MB (E
bash: syntax error near unexpected token `('
[analyst@secOps ~]$  tcpdump -r /home/analyst/capture.pcap1 tcp -c  3
reading from file /home/analyst/capture.pcap1, link-type EN10MB (Ethernet)
04:20:36.331875 IP 10.0.0.11.58664 > 172.16.0.40.http: Flags [S], seq 2885782902, win 29200, options [mss 1460,sackOK,
04:20:36.332065 IP 172.16.0.40.http > 10.0.0.11.58664: Flags [S.], seq 4148295028, ack 2885782903, win 28960, options
op,wscale 9], length 0
04:20:36.332112 IP 10.0.0.11.58664 > 172.16.0.40.http: Flags [.], ack 1, win 58, options [nop,nop,TS val 131949178 ecr
[analyst@secOps ~]$  tcpdump -r /home/analyst/capture.pcap1 tcp -c  5
reading from file /home/analyst/capture.pcap1, link-type EN10MB (Ethernet)
04:20:36.331875 IP 10.0.0.11.58664 > 172.16.0.40.http: Flags [S], seq 2885782902, win 29200, options [mss 1460,sackOK,
04:20:36.332065 IP 172.16.0.40.http > 10.0.0.11.58664: Flags [S.], seq 4148295028, ack 2885782903, win 28960, options
op,wscale 9], length 0
04:20:36.332112 IP 10.0.0.11.58664 > 172.16.0.40.http: Flags [.], ack 1, win 58, options [nop,nop,TS val 131949178 ecr
04:20:36.332337 IP 10.0.0.11.58664 > 172.16.0.40.http: Flags [P.], seq 1:419, ack 1, win 58, options [nop,nop,TS val 1
HTTP/1.1
04:20:36.332357 IP 172.16.0.40.http > 10.0.0.11.58664: Flags [.], ack 419, win 59, options [nop,nop,TS val 1038233159
```

c. Accédez au terminal utilisé pour démarrer Mininet. Arrêtez Mininet en saisissant quit dans la fenêtre du terminal principale de la machine virtuelle CyberOps.

```
mininet> quit
*** Stopping 0 controllers

*** Stopping 2 terms
*** Stopping 5 links .....
*** Stopping 1 switches s1
*** Stopping 5 hosts
H1 H2 H3 H4 R1
*** Done
[analyst@secOps ~]$
```

d. Une fois Mininet arrêté, saisissez **sudo mn -c** pour supprimer les processus démarrés par Mininet. Saisissez le mot de passe **cyberops** lorsque vous y êtes invité.

```
[analyst@secOps scripts]$ sudo mn -c [sudo]
password for analyst:
```

```
[analyst@secOps ~]$ sudo mn -c
[sudo] password for analyst:
*** Removing excess controllers/ofprotocols/ofdatapaths/pings/noxes
killall controller ofprotocol ofdatapath ping nox_core lt-nox_core ovs-openflowd ovs-controller udpbwtest mnexec ivs
killall -9 controller ofprotocol ofdatapath ping nox_core lt-nox_core ovs-openflowd ovs-controller udpbwtest mnexec iv
pkill -9 -f "sudo mnexec"
*** Removing junk from /tmp
rm -f /tmp/vconn* /tmp/vlogs* /tmp/*.out /tmp/*.log
*** Removing old X11 tunnels
*** Removing excess kernel datapaths
ps ax | egrep -o 'dp[0-9]+' | sed 's/dp/nl:/'
***  Removing OVS datapaths
ovs-vsctl --timeout=1 list-br
ovs-vsctl --timeout=1 list-br
*** Removing all links of the pattern foo-ethX
ip link show | egrep -o '([-_.[:alnum:]]+-eth[[:digit:]]+)'
ip link show
*** Killing stale mininet node processes
pkill -9 -f mininet:
*** Shutting down stale tunnels
pkill -9 -f Tunnel=Ethernet
pkill -9 -f .ssh/mn
rm -f ~/.ssh/mn/*
*** Cleanup complete.
[analyst@secOps ~]$
```

Remarques générales

1. Des centaines de filtres sont disponibles dans Wireshark. Un réseau de grande taille peut avoir de nombreux filtres et de nombreux types de trafic. Indiquez trois filtres qui pourraient être utiles à un administrateur réseau.

   Les trois filtres qui pourraient être utiles à un administrateur réseau sont TCP, ICMP SMTP

2. De quelles autres façons Wireshark pourrait-il être utilisé dans un réseau de production ?

   Wireshark peut être utilisé pour sécuriser un réseau contre des tentatives d'intrusion mais également a optimiser la performance d'un réseau