

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

Objectifs

Analyser les paquets à l'aide de Wireshark

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 avec Wireshark

Analyser les paquets à l'aide de Wireshark

Étape 1: Appliquez un filtre à la capture enregistrée.

- Lancez Wireshark sur votre ordinateur.
 - Lancez une capture
 - Depuis votre navigateur, accédez à un site Web
 - Dès que la page d'accueil s'affiche, arrêter la capture sous Wireshark
- e. Appliquez un filtre **tcp** à la capture. Dans cet exemple, les 3 premières trames représentent un exemple de trafic.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.11	172.16.0.40	TCP	74	58716 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PER
2	0.000081	172.16.0.40	10.0.0.11	TCP	74	80 → 58716 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=14
3	0.000082	10.0.0.11	172.16.0.40	TCP	66	58716 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=38645
4	0.000194	10.0.0.11	172.16.0.40	HTTP	356	GET /favicon.ico HTTP/1.1

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.

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

- 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.
- 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.
- 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.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.11	172.16.0.40	TCP	74	58716 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERFECT
2	0.000081	172.16.0.40	10.0.0.11	TCP	74	80 → 58716 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460
3	0.000082	10.0.0.11	172.16.0.40	TCP	66	58716 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=38645
4	0.000194	10.0.0.11	172.16.0.40	HTTP	356	GET /favicon.ico HTTP/1.1

▶ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▶ Ethernet II, Src: a6:a1:15:2c:d8:de (a6:a1:15:2c:d8:de), Dst: a2:86:17:7c:c3:65 (a2:86:17:7c:c3:65)
▶ Internet Protocol Version 4, Src: 10.0.0.11, Dst: 172.16.0.40
Transmission Control Protocol, Src Port: 58716, Dst Port: 80, Seq: 0, Len: 0
Source Port: 58716
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Acknowledgment number: 0
Header Length: 40 bytes
Flags: 0x002 (SYN)
Window size value: 29200
[Calculated window size: 29200]
Checksum: 0xb671 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
▶ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale

Quel est le numéro du port source TCP

53085

Comment classifieriez-vous le port source ?

C'est un port réseau pour la connexion TCP du PC

Quel est le numéro du port de destination TCP ?

443

Comment classifieriez-vous le port de destination ?

C'est le port correspondant au HTTPS sur le serveur

Quel indicateur est défini ? (Plusieurs réponses possibles)

SYN à la valeur 1

Sur quoi le numéro d'ordre relatif est-il défini ?

0

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

- 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.

The image shows a Wireshark packet capture with the filter 'tcp'. The packet list shows four packets. Packet 2 is selected, showing details for Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The TCP details show a SYN, ACK flag set, sequence number 0, and acknowledgment number 1.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.11	172.16.0.40	TCP	74	58716 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERFECT
2	0.000081	172.16.0.40	10.0.0.11	TCP	74	80 → 58716 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460
3	0.000082	10.0.0.11	172.16.0.40	TCP	66	58716 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=38643
4	0.000194	10.0.0.11	172.16.0.40	HTTP	356	GET /favicon.ico HTTP/1.1

Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

Ethernet II, Src: a2:86:17:7c:c3:65 (a2:86:17:7c:c3:65), Dst: a6:a1:15:2c:d8:de (a6:a1:15:2c:d8:de)

Internet Protocol Version 4, Src: 172.16.0.40, Dst: 10.0.0.11

Transmission Control Protocol, Src Port: 80, Dst Port: 58716, Seq: 0, Ack: 1, Len: 0

Source Port: 80
Destination Port: 58716
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Acknowledgment number: 1 (relative ack number)
Header Length: 40 bytes
Flags: 0x012 (SYN, ACK)
Window size value: 28960
[Calculated window size: 28960]
Checksum: 0xc85a [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale

Quelles sont les valeurs des ports source et de destination ?

Port source : 443 Port de destination : 53078

Quels sont les indicateurs définis ?

SYN et ACK à la valeur 1

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

0

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

The image shows a Wireshark packet capture with the filter 'tcp'. The packet list shows four packets. Packet 3 is selected, showing details for Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The TCP details show an ACK flag set, sequence number 1, and acknowledgment number 1.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.11	172.16.0.40	TCP	74	58716 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERFECT
2	0.000081	172.16.0.40	10.0.0.11	TCP	74	80 → 58716 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460
3	0.000082	10.0.0.11	172.16.0.40	TCP	66	58716 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=38643
4	0.000194	10.0.0.11	172.16.0.40	HTTP	356	GET /favicon.ico HTTP/1.1

Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)

Ethernet II, Src: a6:a1:15:2c:d8:de (a6:a1:15:2c:d8:de), Dst: a2:86:17:7c:c3:65 (a2:86:17:7c:c3:65)

Internet Protocol Version 4, Src: 10.0.0.11, Dst: 172.16.0.40

Transmission Control Protocol, Src Port: 58716, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Source Port: 58716
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
Acknowledgment number: 1 (relative ack number)
Header Length: 32 bytes
Flags: 0x010 (ACK)
Window size value: 58
[Calculated window size: 29696]
[Window size scaling factor: 512]
Checksum: 0xb669 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0

Examinez le troisième et dernier paquet de la connexion.

Quel indicateur est défini ? (plusieurs réponses possibles)

ACK à la valeur 1

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.