M1 RES - Travaux sur machine encadrés 4/10

Transport : Mécanismes de TCP

1 Rappel des fonctionalités TCP

Cette première analyse a pour but d'observer les différents mécanismes protocolaires de TCP. Pour cela, nous nous appuierons sur la capture d'une connexion TCP encapsulant un échange HTTP.

1.1 Mise en place de la connexion HTTP

Voici la première trame échangée lors de l'ouverture de la connexion :

```
0000  00 50 7f 05 7d 40 00 10  a4 86 2d 0b 08 00 45 00   .P..}@.. ..-...E.
0010  00 3c 17 96 40 00 40 06  6d f3 0a 21 b6 b2 c0 37   .<..@.@. m..!...7
0020  34 28 84 b3 00 50 b6 94  b0 b7 00 00 00 00 a0 02   4(...P.. ........
0030  16 d0 e8 23 00 00 02 04  05 b4 04 02 08 0a 00 6f   ...#.... .......o
0040  a7 21 00 00 00 00 01 03  03 00                     .!...... ..
```

1. Pour vous échauffer, analysez **manuellement** (sans `ethereal`) la trame présentée ci-dessus.
2. Utilisez à présent (et seulement après avoir analysé trame précédente) le logiciel `ethereal` pour la suite. Chargez le fichier suivant : `/Infos/lmd/2004/master/ue/res-2004oct/tme4-htt.dmp.gz`. Identifiez les hôtes impliqués dans l'échange HTTP. Quels vont être leurs rôles respectifs dans l'échange présenté.
3. Dans les premières trames, quels sont les bits de contrôle (TCP *flags*) positionnés ? Que signifient-ils ?
4. Quelles informations peut-on déduire des ports contenus dans les segments ci-dessus ?
5. Rappelez le fonctionnement des numéros de séquences de TCP. Justifiez les valeurs présentes dans ces segments.
6. Que pouvez-vous dire du contrôle de flux pour les segments étudiés ?
7. Pouvez-vous trouvez des options dans les entêtes TCP ? Si oui, que signifient-elles ?

1.2 Suite de l'échange HTTP

Nous vous proposons de continuer l'analyse de cet échange...

Voici la représentation partiellement décodée de chaques trames grâce à l'outils UNIX `tcpdump` (basé sur la même bibliothèque de capture, `libpcap`, mais plus adapté pour une présentation textuelle) :

```
10:12:21.406418 galion.33971 > 192.55.52.40.www: S 3063197879:3063197879(0) win 5840
[A]                                              <mss 1460,sackOK,timestamp 7317281 0,nop,wscale 0> (DF)

10:12:21.576976 192.55.52.40.www > galion.33971: S 610765288:610765288(0) ack 3063197880 win 64240
[B]                                              <mss 1402,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> (DF)

10:12:21.577036 galion.33971 > 192.55.52.40.www: . ack 1 win 5840
[C]                                              <nop,nop,timestamp 7317298 0> (DF)

10:12:21.577237 galion.33971 > 192.55.52.40.www: P 1:486(485) ack 1 win 5840
[D]                                              <nop,nop,timestamp 7317298 0> (DF)

10:12:21.776923 192.55.52.40.www > galion.33971: . 1:1391(1390) ack 486 win 63755
[E]                                              <nop,nop,timestamp 19332362 7317298> (DF)

10:12:21.776978 galion.33971 > 192.55.52.40.www: . ack 1391 win 8340
[F]                                              <nop,nop,timestamp 7317318 19332362> (DF)

...
```

1. Tracez rapidement le chronogramme correspondant à cet échange.
2. Nous souhaitons étudier la demi-connexion correspondant à l'émission de données du serveur (`192.55.52.40.www`) vers le client (`10.33.182.178.33971`). Complétez le tableau suivant (numéros de séquence relatifs) :

action	base de la fenêtre	pointeur d'émission	fin de la fenêtre	taille de la fenêtre	*commentaire*
réception `A`	—	—	—	5840	*win 5840*
émission `B`	0 (610765288)	1	5840	—	*SYN, +1 pas d'émission*
réception `C`	1	1	5841	5840	*ACK*
réception `D`	1	1	5841	5840	*ACK*
émission `E`	1	1391	5841	—	
réception `F`	1391	1391	9731	8340	*ACK, win 8340*
...					

3. Commentez l'évolution des numéros de séquence.
4. Que pouvez vous dire sur la gestion des tampons ?
5. Observez-vous de nouvelles options ? Pouvez vous les expliquer.
6. Que pouvez dire à propos de la génération des acquittements par le récepteur ?
7. Comment se termine la communication ? Détaillez les échanges finaux.

2 Echanges TCP imbriqués *(facultatif)*

Utilisez `ethereal` pour chargez le fichier suivant : `/Infos/lmd/2004/master/ue/res-2004oct/tme4-ftp.dmp.gz`.

1. Observez l'échange capturé et expliquez les actions réalisées au niveau applicatif.
2. Tracez le chronogramme correspondant à ces échanges en utilisant une couleur différente par connexion.
3. Que pouvez vous dire de l'utilisation du *flag* `PUSH`