Distributed Systems 14th-Oct-2022

TCP Analysis with tcpdump in paloalto.unileon.es

$ /usr/sbin/tcpdump -i eno1 -vvv -n -X tcp port 50001
tcpdump: listening on eno1, link-type EN10MB (Ethernet), capture size 262144 bytes

```
14:49:25.354585 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
    192.168.1.10.49699 > 192.168.1.88.50001: Flags [SEW], cksum 0x3f42 (correct), seq 1959256602, win 65535,
options [mss 1460,nop,wscale 6,nop,nop,TS val 1470971714 ecr 0,sackOK,eol], length 0
         0x0000:  4500 0040 0000 4000 4006 b705 c0a8 010a  E..@..@.@.......
         0x0010:  c0a8 0158 c223 c351 74c7 e21a 0000 0000  ...X.#.Qt.......
         0x0020:  b0c2 ffff   3f42 0000 0204 05b4 0103 0306  ....?B..........
         0x0030:  0101 080a 57ad 3f42 0000 0000 0402 0000  ....W.?B........


14:49:25.354631 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.1.88.50001 > 192.168.1.10.49699: Flags [S.E], cksum 0x83e1 (incorrect -> 0x00f0), seq 3404803869, ack
1959256603, win 65160, options [mss 1460,sackOK,TS val 4113457662 ecr 1470971714,nop,wscale 7], length 0
         0x0000:  4500 003c 0000 4000 4006 b709 c0a8 0158  E..<..@.@......X
         0x0010:  c0a8 010a c351 c223 caf1 2f1d 74c7 e21b  .....Q.#../.t...
         0x0020:  a052 fe88 83e1 0000 0204 05b4 0402 080a  .R..............
         0x0030:  f52e 61fe 57ad 3f42 0103 0307            ..a.W.?B....


14:49:25.354906 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.1.10.49699 > 192.168.1.88.50001: Flags [.], cksum 0x267b (correct), seq 1, ack 1, win 2058, options
[nop,nop,TS val 1470971714 ecr 4113457662], length 0
         0x0000:  4500 0034 0000 4000 4006 b711 c0a8 010a  E..4..@.@.......
         0x0010:  c0a8 0158 c223 c351 74c7 e21b caf1 2f1e  ...X.#.Qt...../.
         0x0020:  8010 080a 267b 0000 0101 080a 57ad 3f42  ....&{......W.?B
         0x0030:  f52e 61fe                                ..a.


14:49:25.354988 IP (tos 0x2,ECT(0), ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 67)
    192.168.1.10.49699 > 192.168.1.88.50001: Flags [P.], cksum 0x5148 (correct), seq 1:16, ack 1, win 2058, options
[nop,nop,TS val 1470971714 ecr 4113457662], length 15
         0x0000:  4502 0043 0000 4000 4006 b700 c0a8 010a  E..C..@.@.......
         0x0010:  c0a8 0158 c223 c351 74c7 e21b caf1 2f1e  ...X.#.Qt...../.
         0x0020:  8018 080a 5148 0000 0101 080a 57ad 3f42  ....QH......W.?B
         0x0030:  f52e 61fe 4865 6c6c 6f20 776f 726c 6420  ..a.Hello.world.
         0x0040:  3a2d 29                                  :-)


14:49:25.355008 IP (tos 0x0, ttl 64, id 12405, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.1.88.50001 > 192.168.1.10.49699: Flags [.], cksum 0x83d9 (incorrect -> 0x2c79), seq 1, ack 16, win 509,
options [nop,nop,TS val 4113457662 ecr 1470971714], length 0
         0x0000:  4500 0034 3075 4000 4006 869c c0a8 0158  E..40u@.@......X
         0x0010:  c0a8 010a c351 c223 caf1 2f1e 74c7 e22a  .....Q.#../.t..*
         0x0020:  8010 01fd 83d9 0000 0101 080a f52e 61fe  ..............a.
         0x0030:  57ad 3f42                                W.?B


14:49:25.355097 IP (tos 0x2,ECT(0), ttl 64, id 12406, offset 0, flags [DF], proto TCP (6), length 92)
    192.168.1.88.50001 > 192.168.1.10.49699: Flags [P.], cksum 0x8401 (incorrect -> 0xaa70), seq 1:41, ack 16, win
509, options [nop,nop,TS val 4113457662 ecr 1470971714], length 40
         0x0000:  4502 005c 3076 4000 4006 8671 c0a8 0158  E..\0v@.@..q...X
         0x0010:  c0a8 010a c351 c223 caf1 2f1e 74c7 e22a  .....Q.#../.t..*
         0x0020:  8018 01fd 8401 0000 0101 080a f52e 61fe  ..............a.
         0x0030:  57ad 3f42 536f 6c63 6974 7564 206e 6f20  W.?BSolcitud.no.
         0x0040:  7265 636f 6e6f 6369 6461 2070 6f72 2065  reconocida.por.e
         0x0050:  7374 6520 7365 7276 6964 6f72            ste.servidor


14:49:25.355131 IP (tos 0x0, ttl 64, id 12407, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.1.88.50001 > 192.168.1.10.49699: Flags [F.], cksum 0x83d9 (incorrect -> 0x2c50), seq 41, ack 16, win
509, options [nop,nop,TS val 4113457662 ecr 1470971714], length 0
         0x0000:  4500 0034 3077 4000 4006 869a c0a8 0158  E..40w@.@......X
         0x0010:  c0a8 010a c351 c223 caf1 2f46 74c7 e22a  .....Q.#../Ft..*
         0x0020:  8011 01fd 83d9 0000 0101 080a f52e 61fe  ..............a.
         0x0030:  57ad 3f42                                W.?B

14:49:25.355447 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.1.10.49699 > 192.168.1.88.50001: Flags [.], cksum 0x2644 (correct), seq 16, ack 41, win 2058, options
[nop,nop,TS val 1470971714 ecr 4113457662], length 0
         0x0000:  4500 0034 0000 4000 4006 b711 c0a8 010a  E..4..@.@.......
         0x0010:  c0a8 0158 c223 c351 74c7 e22a caf1 2f46  ...X.#.Qt..*../F
         0x0020:  8010 080a 2644 0000 0101 080a 57ad 3f42  ....&D......W.?B
         0x0030:  f52e 61fe                                ..a.

14:49:25.355464 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.1.10.49699 > 192.168.1.88.50001: Flags [.], cksum 0x2643 (correct), seq 16, ack 42, win 2058, options
[nop,nop,TS val 1470971714 ecr 4113457662], length 0
         0x0000:  4500 0034 0000 4000 4006 b711 c0a8 010a  E..4..@.@.......
         0x0010:  c0a8 0158 c223 c351 74c7 e22a caf1 2f47  ...X.#.Qt..*../G
         0x0020:  8010 080a 2643 0000 0101 080a 57ad 3f42  ....&C......W.?B
         0x0030:  f52e 61fe                                ..a.
```



```
14:49:25.355493 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.1.10.49699 > 192.168.1.88.50001: Flags [F.], cksum 0x2641 (correct), seq 16, ack 42, win 2058, options
[nop,nop,TS val 1470971715 ecr 4113457662], length 0
        0x0000:  4500 0034 0000 4000 4006 b711 c0a8 010a  E..4..@.@.......
        0x0010:  c0a8 0158 c223 c351 74c7 e22a caf1 2f47  ...X.#.Qt..*../G
        0x0020:  8011 080a 2641 0000 0101 080a 57ad 3f43  ....&A......W.?C
        0x0030:  f52e 61fe                                ..a.

14:49:25.355509 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.1.88.50001 > 192.168.1.10.49699: Flags [.], cksum 0x2c4d (correct), seq 42, ack 17, win 509, options
[nop,nop,TS val 4113457663 ecr 1470971715], length 0
        0x0000:  4500 0034 0000 4000 4006 b711 c0a8 0158  E..4..@.@......X
        0x0010:  c0a8 010a c351 c223 caf1 2f47 74c7 e22b  .....Q.#../Gt..+
        0x0020:  8010 01fd 2c4d 0000 0101 080a f52e 61ff  ....,M........a.
        0x0030:  57ad 3f43                                W.?C
```

Exercises

1. Explain the meaning of each of the TCP segments above according to the theory about TCP given on the lectures and labs
    a. Indicate whether the frame belongs in the 3-way handshake, the data transfer phase or the connection close
    b. Interpret the sequence numbers sent in each segment
    c. Check whether the ASNs are correct
    d. What's the purpose of sending segments with no payload
    e. Indicate which segments use *piggybacking*
    f. Check that all of segments sent in the data transfer have their ACK flag set
    g. Identify data transfer segments that have their SYN flag set

2. Which flags are set in the TCP segment which IP packet was sent at 14:49:25.355509. Interpret its HEX dump.

3. Connect to paloalto at port 60001 with ssh and check the credentials that I sent you via e-mail. Copy the text in your terminal and paste it in the solution to this exercise, or take a screen shot.

4. Login into paloalto and download the source code to the C/S practice that we did this week. Compile the client and server programs. You'll run them remotely next week in the lab. Copy the text in your terminal and paste it in the solution to this exercise, or take a screen shot.

