

הסנפת תעבורת רשת של פרוטוקול שרת-לקוח

במסמך זה נסביר את הפקטות שהסנפנו ע"י wireshark שממחישות את תהליך הlogin-
אותנטיקציה של משתמש ע"י הclient ל-server

שלב 1: לאחר יצירת socket connection השרת שולח ללקוח
הודעת "Welcome! Please log in." (ניתן לראות במידע הטקסטואלי בתחתית הצילום)

The image shows a Wireshark packet capture of a TCP connection. The packet list pane at the top shows several packets, with packet 4 selected. The packet details pane below shows the structure of packet 4, which is a TCP segment with the payload 'Welcome! Please log in.'

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	TCP	56	58058 → 12345 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
2	0.000033	127.0.0.1	127.0.0.1	TCP	56	12345 → 58058 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
3	0.000049	127.0.0.1	127.0.0.1	TCP	44	58058 → 12345 [ACK] Seq=1 Ack=1 Win=2161152 Len=0
4	0.000235	127.0.0.1	127.0.0.1	TCP	71	12345 → 58058 [PSH, ACK] Seq=1 Ack=1 Win=2161152 Len=27
5	0.000250	127.0.0.1	127.0.0.1	TCP	44	58058 → 12345 [ACK] Seq=1 Ack=28 Win=2161152 Len=0
6	19.308039	127.0.0.1	127.0.0.1	TCP	83	58058 → 12345 [PSH, ACK] Seq=1 Ack=28 Win=2161152 Len=39
7	19.308066	127.0.0.1	127.0.0.1	TCP	44	12345 → 58058 [ACK] Seq=28 Ack=40 Win=2161152 Len=0
8	19.308143	127.0.0.1	127.0.0.1	TCP	76	12345 → 58058 [PSH, ACK] Seq=28 Ack=40 Win=2161152 Len=32
9	19.308163	127.0.0.1	127.0.0.1	TCP	44	58058 → 12345 [ACK] Seq=40 Ack=60 Win=2161152 Len=0

Frame 4: 71 bytes on wire (568 bits), 71 bytes captured (568 bi
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 12345, Dst Port: 58058
Data (27 bytes)

0000 02 00 00 00 45 00 00 43 85 86 40 00 80 06 00 00 ... E..C ..@ ..
0010 7f 00 00 01 7f 00 00 01 30 39 e2 ca 0e 2d ae 3709....-7
0020 da 93 44 06 50 18 20 fa 4b fc 00 00 00 00 00 17 ... D P .. K ..
0030 57 65 6c 63 6f 6d 65 21 20 50 6c 65 61 73 65 20 Welcome! Please
0040 6c 6f 67 20 69 6e 2e log in.

שלב 2: הלקוח שולח לשרת את פרטי האותנטיקציה שלו – שם משתמש וסיסמה בפורמט

User: Bob Password: simplepass

בנוסף, ניתן לראות את ה-header שהפרוטוקול מוסיף AUTH וכך השרת יודע לפרסר את סוג ההודעה והמידע הנלווה.

The image shows a Wireshark packet capture of a TCP connection between 127.0.0.1 and 127.0.0.1. The packets are as follows:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	TCP	56	58058 → 12345 [SYN, Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
2	0.000033	127.0.0.1	127.0.0.1	TCP	56	12345 → 58058 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
3	0.000049	127.0.0.1	127.0.0.1	TCP	44	58058 → 12345 [ACK] Seq=1 Ack=1 Win=2161152 Len=0
4	0.000235	127.0.0.1	127.0.0.1	TCP	71	12345 → 58058 [PSH, ACK] Seq=1 Ack=1 Win=2161152 Len=27
5	0.000250	127.0.0.1	127.0.0.1	TCP	44	58058 → 12345 [ACK] Seq=1 Ack=28 Win=2161152 Len=0
6	19.308039	127.0.0.1	127.0.0.1	TCP	83	58058 → 12345 [PSH, ACK] Seq=1 Ack=28 Win=2161152 Len=39
7	19.308066	127.0.0.1	127.0.0.1	TCP	44	12345 → 58058 [ACK] Seq=28 Ack=40 Win=2161152 Len=0
8	19.308143	127.0.0.1	127.0.0.1	TCP	76	12345 → 58058 [PSH, ACK] Seq=28 Ack=40 Win=2161152 Len=32
9	19.308163	127.0.0.1	127.0.0.1	TCP	44	58058 → 12345 [ACK] Seq=40 Ack=60 Win=2161152 Len=0

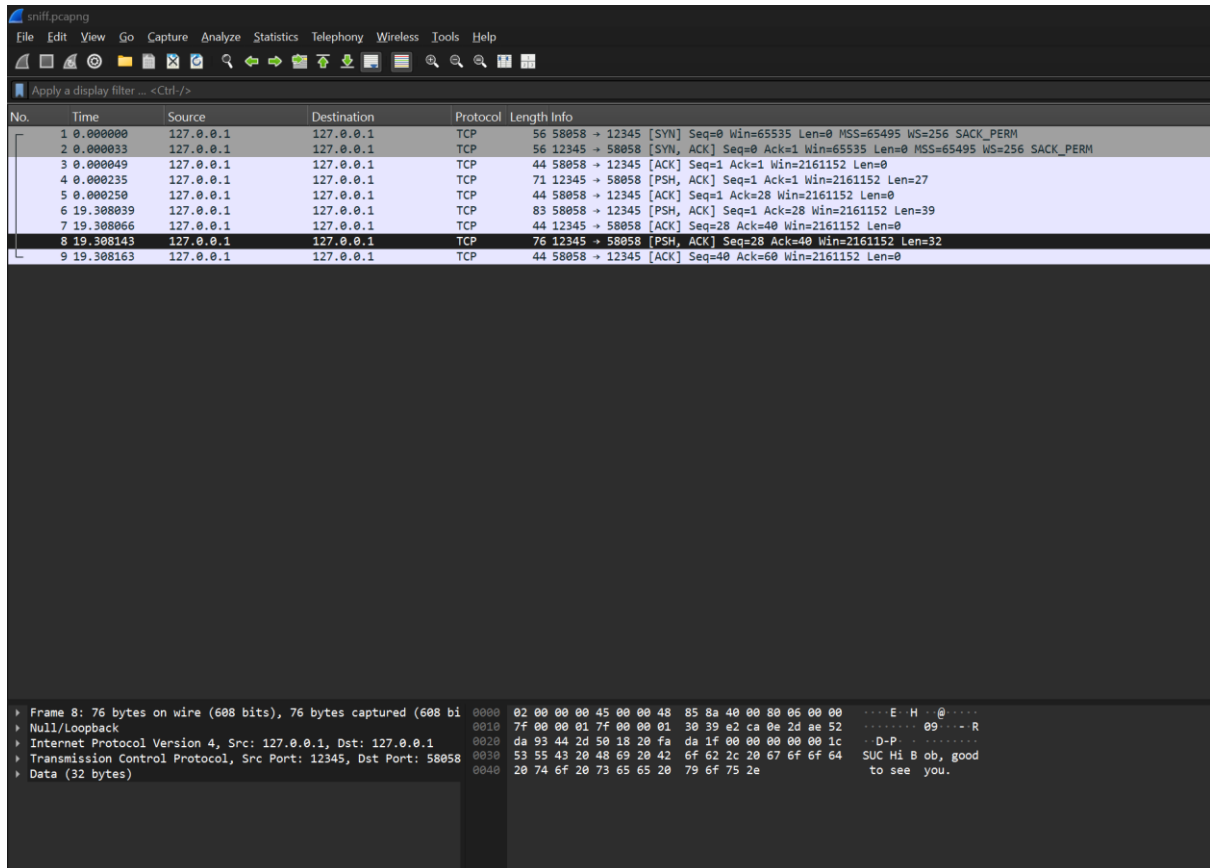
The packet details for packet 6 are as follows:

- Frame 6: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface
- Null/Loopback
- Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
- Transmission Control Protocol, Src Port: 58058, Dst Port: 12345
- Data (39 bytes)

The raw data for packet 6 is as follows:

```
0000 02 00 00 00 45 00 00 4f 85 88 40 00 80 06 00 00  ....E..O..@....
0010 7f 00 00 01 7f 00 00 01 e2 ca 30 39 da 93 44 06  .........09..D
0020 0e 2d ae 52 50 18 20 fa 62 18 00 00 00 00 23  --RP...b.....#
0030 41 55 54 48 2c 55 73 65 72 3a 20 42 6f 62 2c 50  AUTH,User: Bob,P
0040 61 73 73 77 6f 72 64 3a 20 73 69 6d 70 6c 65 70  assword: simplep
0050 61 73 73                                     ass
```

שלב 3 : השרת עונה ללקוח על הצלחת ההתחברות על ידי פקטה שבה יש header של הפרוטוקול
 SUC המייצג את success, כלומר תהליך האותנטיקציה הצליח
 לאחר ה-header מופיעה ההודעה שבה השרת מברך לשלום את המשתמש שחזר לsession חדש



כעת, הלקוח יכול לשלוח פקודות לביצוע לשרת כמבוקש בתרגיל ובזה תם תהליך האותנטיקציה לשרת.