گزارشکار Wire Shark

سرگروه: فاطمه فرهادی

عضو گروه: سوده زارعی

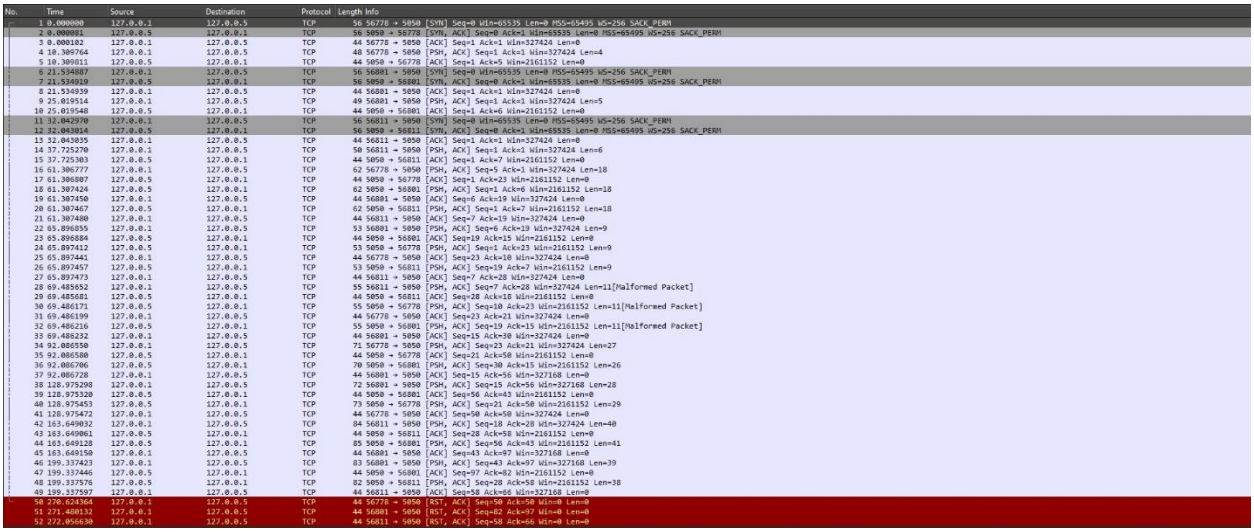
عضو گروه: اشکان عظیمی

تغییرات اعمال شده روی کد، در گزارشکار مربوط به کد توضیح داده شده است.

در اینجا، ارتباطات بین یک سرور و سه کلاینت را بررسی خواهیم کرد.

در عکس بالا، سه دوست را می‌بینیم که در حال مکالمه با یکدیگر هستند.

فرآیند مکالمه این سه نفر را در صفحات بعدی بررسی می‌کنیم.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.5	TCP	56	56778 → 5050 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
2	0.000081	127.0.0.5	127.0.0.1	TCP	56	5050 → 56778 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
3	0.000102	127.0.0.1	127.0.0.5	TCP	44	56778 → 5050 [ACK] Seq=1 Ack=1 Win=327424 Len=0
4	10.309764	127.0.0.1	127.0.0.5	TCP	48	56778 → 5050 [PSH, ACK] Seq=1 Ack=1 Win=327424 Len=4
5	10.309811	127.0.0.5	127.0.0.1	TCP	44	5050 → 56778 [ACK] Seq=1 Ack=5 Win=2161152 Len=0
6	21.534887	127.0.0.1	127.0.0.5	TCP	56	56801 → 5050 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
7	21.534919	127.0.0.5	127.0.0.1	TCP	56	5050 → 56801 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
8	21.534939	127.0.0.1	127.0.0.5	TCP	44	56801 → 5050 [ACK] Seq=1 Ack=1 Win=327424 Len=0
9	25.019514	127.0.0.1	127.0.0.5	TCP	49	56801 → 5050 [PSH, ACK] Seq=1 Ack=1 Win=327424 Len=5
10	25.019548	127.0.0.5	127.0.0.1	TCP	44	5050 → 56801 [ACK] Seq=1 Ack=6 Win=2161152 Len=0
11	32.042970	127.0.0.1	127.0.0.5	TCP	56	56811 → 5050 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
12	32.043014	127.0.0.5	127.0.0.1	TCP	56	5050 → 56811 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
13	32.043035	127.0.0.1	127.0.0.5	TCP	44	56811 → 5050 [ACK] Seq=1 Ack=1 Win=327424 Len=0
14	37.725270	127.0.0.1	127.0.0.5	TCP	50	56811 → 5050 [PSH, ACK] Seq=1 Ack=1 Win=327424 Len=6
15	37.725303	127.0.0.5	127.0.0.1	TCP	44	5050 → 56811 [ACK] Seq=1 Ack=7 Win=2161152 Len=0
16	61.306777	127.0.0.1	127.0.0.5	TCP	62	56778 → 5050 [PSH, ACK] Seq=5 Ack=1 Win=327424 Len=18
17	61.306807	127.0.0.5	127.0.0.1	TCP	44	5050 → 56778 [ACK] Seq=1 Ack=23 Win=2161152 Len=0
18	61.307424	127.0.0.5	127.0.0.1	TCP	62	5050 → 56801 [PSH, ACK] Seq=1 Ack=6 Win=2161152 Len=18
19	61.307450	127.0.0.1	127.0.0.5	TCP	44	56801 → 5050 [ACK] Seq=6 Ack=19 Win=327424 Len=0
20	61.307467	127.0.0.5	127.0.0.1	TCP	62	5050 → 56811 [PSH, ACK] Seq=1 Ack=7 Win=2161152 Len=18
21	61.307480	127.0.0.1	127.0.0.5	TCP	44	56811 → 5050 [ACK] Seq=7 Ack=19 Win=327424 Len=0
22	65.896855	127.0.0.1	127.0.0.5	TCP	53	56801 → 5050 [PSH, ACK] Seq=6 Ack=19 Win=327424 Len=9
23	65.896884	127.0.0.5	127.0.0.1	TCP	44	5050 → 56801 [ACK] Seq=19 Ack=15 Win=2161152 Len=0
24	65.897412	127.0.0.5	127.0.0.1	TCP	53	5050 → 56778 [PSH, ACK] Seq=1 Ack=23 Win=2161152 Len=9
25	65.897441	127.0.0.1	127.0.0.5	TCP	44	56778 → 5050 [ACK] Seq=23 Ack=10 Win=327424 Len=0
26	65.897457	127.0.0.5	127.0.0.1	TCP	53	5050 → 56811 [PSH, ACK] Seq=19 Ack=7 Win=2161152 Len=9
27	65.897473	127.0.0.1	127.0.0.5	TCP	44	56811 → 5050 [ACK] Seq=7 Ack=28 Win=327424 Len=0
28	69.485652	127.0.0.1	127.0.0.5	TCP	55	56811 → 5050 [PSH, ACK] Seq=7 Ack=28 Win=327424 Len=11[Malformed Packet]
29	69.485681	127.0.0.5	127.0.0.1	TCP	44	5050 → 56811 [ACK] Seq=28 Ack=18 Win=2161152 Len=0
30	69.486171	127.0.0.5	127.0.0.1	TCP	55	5050 → 56778 [PSH, ACK] Seq=10 Ack=23 Win=2161152 Len=11[Malformed Packet]
31	69.486199	127.0.0.1	127.0.0.5	TCP	44	56778 → 5050 [ACK] Seq=23 Ack=21 Win=327424 Len=0
32	69.486216	127.0.0.5	127.0.0.1	TCP	55	5050 → 56801 [PSH, ACK] Seq=19 Ack=15 Win=2161152 Len=11[Malformed Packet]
33	69.486232	127.0.0.1	127.0.0.5	TCP	44	56801 → 5050 [ACK] Seq=15 Ack=30 Win=327424 Len=0
34	92.086550	127.0.0.1	127.0.0.5	TCP	71	56778 → 5050 [PSH, ACK] Seq=23 Ack=21 Win=327424 Len=27
35	92.086580	127.0.0.5	127.0.0.1	TCP	44	5050 → 56778 [ACK] Seq=21 Ack=50 Win=2161152 Len=0
36	92.086706	127.0.0.5	127.0.0.1	TCP	70	5050 → 56801 [PSH, ACK] Seq=30 Ack=15 Win=2161152 Len=26
37	92.086728	127.0.0.1	127.0.0.5	TCP	44	56801 → 5050 [ACK] Seq=15 Ack=56 Win=327168 Len=0
38	128.975298	127.0.0.1	127.0.0.5	TCP	72	56801 → 5050 [PSH, ACK] Seq=15 Ack=56 Win=327168 Len=28
39	128.975320	127.0.0.5	127.0.0.1	TCP	44	5050 → 56801 [ACK] Seq=56 Ack=43 Win=2161152 Len=0
40	128.975453	127.0.0.5	127.0.0.1	TCP	73	5050 → 56778 [PSH, ACK] Seq=21 Ack=50 Win=2161152 Len=29
41	128.975472	127.0.0.1	127.0.0.5	TCP	44	56778 → 5050 [ACK] Seq=50 Ack=50 Win=327424 Len=0
42	163.649032	127.0.0.1	127.0.0.5	TCP	84	56811 → 5050 [PSH, ACK] Seq=18 Ack=28 Win=327424 Len=40
43	163.649061	127.0.0.5	127.0.0.1	TCP	44	5050 → 56811 [ACK] Seq=28 Ack=58 Win=2161152 Len=0
44	163.649128	127.0.0.5	127.0.0.1	TCP	85	5050 → 56801 [PSH, ACK] Seq=56 Ack=43 Win=2161152 Len=41
45	163.649150	127.0.0.1	127.0.0.5	TCP	44	56801 → 5050 [ACK] Seq=43 Ack=97 Win=327168 Len=0
46	199.337423	127.0.0.1	127.0.0.5	TCP	83	56801 → 5050 [PSH, ACK] Seq=43 Ack=97 Win=327168 Len=39
47	199.337446	127.0.0.5	127.0.0.1	TCP	44	5050 → 56801 [ACK] Seq=97 Ack=82 Win=2161152 Len=0
48	199.337576	127.0.0.5	127.0.0.1	TCP	82	5050 → 56811 [PSH, ACK] Seq=28 Ack=58 Win=2161152 Len=38
49	199.337597	127.0.0.1	127.0.0.5	TCP	44	56811 → 5050 [ACK] Seq=58 Ack=66 Win=327168 Len=0
50	270.624364	127.0.0.1	127.0.0.5	TCP	44	56778 → 5050 [RST, ACK] Seq=50 Ack=50 Win=0 Len=0
51	271.480132	127.0.0.1	127.0.0.5	TCP	44	56801 → 5050 [RST, ACK] Seq=82 Ack=97 Win=0 Len=0
52	272.056630	127.0.0.1	127.0.0.5	TCP	44	56811 → 5050 [RST, ACK] Seq=58 Ack=66 Win=0 Len=0

در پکت‌های ۱ تا ۳، کلاینت اول (56778) به سرور (5050) متصل شده است و سرور تاییدیه وصل شدن را برای کلاینت اول ارسال کرده است.

در پکت‌های ۴ و ۵، کلاینت اول دیتایی با طول ۴ که نامش است را برای سرور ارسال کرده و سرور این دریافت را تایید کرده و برای کلاینت اول فرستاده. (از این پس کلاینت اول را Sude می‌نامیم)

در پکت‌های ۶ تا ۸، کلاینت دوم (56801) فرآیند وصل شدن به سرور را همانند کلاینت اول طی کرده است.

در پکت‌های ۹ و ۱۰، کلاینت دوم نام خود را ارسال کرده و سرور تاییدیه دریافت خود را به کلاینت دوم اعلام کرده است. (از این پس کلاینت دوم را Shima می‌نامیم)

در پکت‌های ۱۱ تا ۱۳، کلاینت سوم (56811) فرآیند وصل شدن به سرور را طی کرده است.

در پکت‌های ۱۴ و ۱۵، کلاینت سوم نام خود را ارسال کرده و سرور تاییدیه دریافت خود را به کلاینت سوم اعلام کرده است. (از این پس کلاینت سووم را Ashkan می‌نامیم)

در پکت‌های ۱۶ و ۱۷، Sude یک پیام برای سرور ارسال کرده است و تاییدیه دریافت خود را برای او فرستاده است.

در پکت‌های ۱۸ و ۱۹، سرور تغییراتی را برروی پیام اعمال کرده و برای Shima فرستاده است و Shima دریافت خود را اعلام کرده است.

در پکت‌های ۲۰ و ۲۱، سرور تغییراتی را برروی پیام اعمال کرده و برای Ashkan فرستاده است و Ashkan دریافت خود را اعلام کرده است.

در پکت‌های ۲۲ تا ۲۷، Shima یک پیام را برای سرور فرستاده و سرور پیام او را برای Sude و Ashkan فرستاده است (همانند روند قبلی).

در پکت‌های ۲۸ تا ۳۳، Ashkan یک پیام را برای سرور فرستاده و سرور پیام او را برای Sude و Shima فرستاده است (همانند روندهای قبلی). (پیام اشکان ممکن است خطاهایی دریافت کرده باشد زیرا پیام ، malformed packet مشاهده می شود.)

در پکت‌های ۳۴ تا ۳۷، Sude یک پیام خصوصی را برای سرور ارسال کرده و این بار سرور پیام را پس از اعمال تغییرات، فقط برای Shima ارسال می‌کند و این پیام برای Ashkan قابل مشاهده نیست.

در پکت‌های ۳۸ تا ۴۱، Shima یک پیام خصوصی برای سرور ارسال کرده و سرور آن را فقط برای Sude ارسال می‌کند و توسط بقیه قابل مشاهده نیست.

در پکت‌های ۴۲ تا ۴۹، شاهد رد و بدل شدن پیام‌های خصوصی بین Shima و Ashkan هستیم که فقط برای این دو کلاینت قابل مشاهده است و برای بقیه چیزی ارسال نمی شود.

در آخر، در پکت‌های ۵۰ تا ۵۲، هر سه کلاینت ارتباط خود را با سرور قطع کرده‌اند.

چون در کد از حالت Sock_stream استفاده کرده‌ایم که پروتکل رو روی tcp قرار میدهد.

در ستون source و destination یک الگوی واضح را می‌توانیم ببینیم و علتش اینه که برنامه های در حال اجرا، روی آیپی 197.0.0.1 هستند و فقط پورت‌هایشان با یکدیگر فرق می‌کند.