

## به نام خدا

محمد یاسین کرباسیان ft علیرضا میرحسینی

پروژه اول شبکه‌های کامپیوتری (پروتکل FTP)

(۱) سوال بالا صفحه ۳ : چرا روند دانلود برعکس نیست که کلاینت یک پورت باز کند و آنرا به سرور اطلاع دهد و سرور فایل را از روی آن پورت برای کلاینت بفرستد؟

- چون کلاینت فایروال دارد که مانع این کار میشود ولی سرور فایروال ندارد.

(۲) سوال وسط صفحه ۳ : حمله‌ای که کلاینت با دادن ورودی که باعث شود فایلی دانلود شود یا فولدری باز شود که در زیر شاخه‌های فولدر اصلی سرور قرار ندارند چه نام دارد؟

Path Traversal Attack \_

(۳) دیدن سه بسته برای handshaking پروتکل TCP :

\*Adapter for loopback traffic capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Time	Source	Destination	Protocol	Length	Info
3	8.392458	127.0.0.1	127.0.0.1	TCP	56	12397 → 2121 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
4	8.392540	127.0.0.1	127.0.0.1	TCP	56	2121 → 12397 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
5	8.392585	127.0.0.1	127.0.0.1	TCP	44	12397 → 2121 [ACK] Seq=1 Ack=1 Win=327424 Len=0

سه بسته‌ی handshaking پروتکل TCP

> Frame 3: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF\_{...} id 0  
> Null/Loopback  
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  
> Transmission Control Protocol, Src Port: 12397, Dst Port: 2121, Seq: 0, Len: 0

0000 02 00 00 00 45 00 00 34 69 86 40 00 06 00 00 .....E..4 i..  
0010 7f 00 00 01 7f 00 00 01 30 6d 08 49 9d 81 c9 9f .....0m.I..  
0020 00 00 00 00 80 02 ff ff d7 12 00 00 02 04 ff d7 .....  
0030 01 03 03 08 01 01 04 02 .....  
Transmission Control Protocol: Protocol

Packets: 29 · Displayed: 3 (10.3%) · Dropped: 0 (0.0%) Profile: Default

09:56  
2022-04-22

۴) سوال ۴/۲ : آیا TCP محدودیتی برای اندازه پکت ها دارد؟ \_ بله 64kb است.

۵) فایل های بزرگ چگونه توسط سوکت TCP ارسال میشوند؟ \_ با شکستن به

چندین پکت با حداکثر سایز 64k این کار انجام میشود.

۶) سوال ۴/۲.ب : ۱۶ بسته فرستاده است

25	41.684984	127.0.0.1	127.0.0.1	TCP	56	45160 → 12487 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
26	41.685037	127.0.0.1	127.0.0.1	TCP	44	12487 → 45160 [ACK] Seq=1 Ack=1 Win=327424 Len=0
27	42.039740	127.0.0.1	127.0.0.1	TCP	65539	45160 → 12487 [ACK] Seq=1 Ack=1 Win=2161152 Len=65495
28	42.039870	127.0.0.1	127.0.0.1	TCP	65539	45160 → 12487 [ACK] Seq=65496 Ack=1 Win=2161152 Len=65495
29	42.039998	127.0.0.1	127.0.0.1	TCP	65539	45160 → 12487 [ACK] Seq=130991 Ack=1 Win=2161152 Len=65495
30	42.040170	127.0.0.1	127.0.0.1	TCP	65539	45160 → 12487 [ACK] Seq=196486 Ack=1 Win=2161152 Len=65495
31	42.040717	127.0.0.1	127.0.0.1	TCP	44	12487 → 45160 [ACK] Seq=1 Ack=261981 Win=327424 Len=0
32	42.040855	127.0.0.1	127.0.0.1	TCP	65539	45160 → 12487 [ACK] Seq=261981 Ack=1 Win=2161152 Len=65495
33	42.040979	127.0.0.1	127.0.0.1	TCP	65539	45160 → 12487 [ACK] Seq=327476 Ack=1 Win=2161152 Len=65495
34	42.041147	127.0.0.1	127.0.0.1	TCP	65539	45160 → 12487 [ACK] Seq=392971 Ack=1 Win=2161152 Len=65495
35	42.041359	127.0.0.1	127.0.0.1	TCP	65539	45160 → 12487 [ACK] Seq=458466 Ack=1 Win=2161152 Len=65495
36	42.041850	127.0.0.1	127.0.0.1	TCP	44	12487 → 45160 [ACK] Seq=1 Ack=523961 Win=327424 Len=0
37	42.041974	127.0.0.1	127.0.0.1	TCP	65539	45160 → 12487 [ACK] Seq=523961 Ack=1 Win=2161152 Len=65495
38	42.042115	127.0.0.1	127.0.0.1	TCP	65539	45160 → 12487 [ACK] Seq=589456 Ack=1 Win=2161152 Len=65495
39	42.042326	127.0.0.1	127.0.0.1	TCP	65539	45160 → 12487 [ACK] Seq=654951 Ack=1 Win=2161152 Len=65495
40	42.042529	127.0.0.1	127.0.0.1	TCP	65539	45160 → 12487 [ACK] Seq=720446 Ack=1 Win=2161152 Len=65495
41	42.043375	127.0.0.1	127.0.0.1	TCP	44	12487 → 45160 [ACK] Seq=1 Ack=785941 Win=65280 Len=0
42	42.045519	127.0.0.1	127.0.0.1	TCP	197	2121 → 12485 [PSH, ACK] Seq=347 Ack=36 Win=2161152 Len=153
43	42.045599	127.0.0.1	127.0.0.1	TCP	44	12485 → 2121 [ACK] Seq=36 Ack=500 Win=2160640 Len=0
44	42.061773	127.0.0.1	127.0.0.1	TCP	44	[TCP Window Update] 12487 → 45160 [ACK] Seq=1 Ack=785941 Win=327424 Len=0
45	42.061874	127.0.0.1	127.0.0.1	TCP	65539	45160 → 12487 [ACK] Seq=785941 Ack=1 Win=2161152 Len=65495
46	42.061982	127.0.0.1	127.0.0.1	TCP	65539	45160 → 12487 [ACK] Seq=851436 Ack=1 Win=2161152 Len=65495
47	42.061952	127.0.0.1	127.0.0.1	TCP	65539	45160 → 12487 [ACK] Seq=916931 Ack=1 Win=2161152 Len=65495
48	42.062082	127.0.0.1	127.0.0.1	TCP	65539	45160 → 12487 [ACK] Seq=982426 Ack=1 Win=2161152 Len=65495
49	42.062051	127.0.0.1	127.0.0.1	TCP	700	45160 → 12487 [FIN, PSH, ACK] Seq=1047921 Ack=1 Win=2161152 Len=656
50	42.062177	127.0.0.1	127.0.0.1	TCP	44	12487 → 45160 [ACK] Seq=1 Ack=1048578 Win=64768 Len=0

از شروع تا پایان داخلود

۷) سوال ۵/۱ : اجرای دستورات به جز DWLD با استفاده از ngrok :

```
client.py
1 from socket import *
2
3 host = '7.tcp.eu.ngrok.io'
4 port = 14406
5 clientSocket = socket(AF_INET, SOCK_STREAM)
6 clientSocket.connect((host, port))
7 while True:
8     command = input('root# ')
9     clientSocket.send(command.encode())
10
11 if command[4:] == "DWLD":
12     pass

server.py
77 host = '127.0.0.1'
78 port = 2121
79 serverSocket = socket(AF_INET, SOCK_STREAM)
80 serverSocket.bind((host, port))
81 serverSocket.listen(10)
82 print('now server is ready :)')
83 privateSocket, address = serverSocket.accept()
84 while(True):
85     command = privateSocket.recv(2048).decode()
86     print(f'from client {command} received.')
87     command = command.split()
88     if command[0] == 'HELP':
89         print('IndexError: list index out of range')
```

```
PS D:\Projects vscode\FTP\with ngrok\Server> python server.py
now server is ready :)
from client HELP received.
from client LIST received.
from client CD inner received.
from client PWD received.
from client PWD received.
from client received.
Traceback (most recent call last):
  File "D:\Projects vscode\FTP\with ngrok\Server\server.py", line 88, in <module>
    if command[0] == 'HELP':
IndexError: list index out of range
PS D:\Projects vscode\FTP\with ngrok\Server> python server.py
now server is ready :)
from client HELP received.
from client LIST received.
from client CD inner received.
from client PWD received.
from client CD .. received.
from client LIST received.
```

(۸) سوال ۵/۲ : ابتدا ngrok را اجرا کردیم ...

```
C:\Windows\System32\cmd.exe - .\ngrok.exe tcp 2121
ngrok
Session Status      online
Account             shapoordisco78@gmail.com (Plan: Free)
Version             3.0.2
Region              Europe (eu)
Latency              116.0114ms
Web Interface        http://127.0.0.1:4040
Forwarding           tcp://0.tcp.eu.ngrok.io:14022 -> localhost:2121

Connections
t1l    opn    rt1    rt5    p50    p90
2      0      0.00   0.00   268.11 423.29
```

سپس در سیستم من سرور را ران کردیم و در حالت loopback به نتایج زیر رسیدیم :

\*Adapter for loopback traffic capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Time	Source	Destination	Protocol	Length	Info
28	46.630189	127.0.0.1	127.0.0.1	TCP	45	[TCP Keep-Alive] 4986 → 2121 [ACK] Seq=7 Ack=222 Win=1278 Len=1
29	46.630250	127.0.0.1	127.0.0.1	TCP	56	[TCP Keep-Alive ACK] 2121 → 4986 [ACK] Seq=222 Ack=8 Win=8442 Len=0 SLE=7 SRE=8
57	61.630679	127.0.0.1	127.0.0.1	TCP	45	[TCP Keep-Alive] 4986 → 2121 [ACK] Seq=7 Ack=222 Win=1278 Len=1
58	61.630759	127.0.0.1	127.0.0.1	TCP	56	[TCP Keep-Alive ACK] 2121 → 4986 [ACK] Seq=222 Ack=8 Win=8442 Len=0 SLE=7 SRE=8
59	73.178613	127.0.0.1	127.0.0.1	TCP	48	4986 → 2121 [PSH, ACK] Seq=8 Ack=222 Win=1278 Len=4
60	73.178664	127.0.0.1	127.0.0.1	TCP	44	2121 → 4986 [ACK] Seq=222 Ack=12 Win=8442 Len=0
61	73.180127	127.0.0.1	127.0.0.1	TCP	264	2121 → 4986 [PSH, ACK] Seq=222 Ack=12 Win=8442 Len=220
62	73.180182	127.0.0.1	127.0.0.1	TCP	44	4986 → 2121 [ACK] Seq=12 Ack=442 Win=1277 Len=0
68	88.190761	127.0.0.1	127.0.0.1	TCP	45	[TCP Keep-Alive] 4986 → 2121 [ACK] Seq=11 Ack=442 Win=1277 Len=1
69	88.190803	127.0.0.1	127.0.0.1	TCP	56	[TCP Keep-Alive ACK] 2121 → 4986 [ACK] Seq=442 Ack=12 Win=8442 Len=0 SLE=11 SRE=12
73	102.673961	127.0.0.1	127.0.0.1	TCP	47	4986 → 2121 [PSH, ACK] Seq=12 Ack=442 Win=1277 Len=3
74	102.674017	127.0.0.1	127.0.0.1	TCP	44	2121 → 4986 [ACK] Seq=442 Ack=15 Win=8442 Len=0
75	102.674501	127.0.0.1	127.0.0.1	TCP	45	2121 → 4986 [PSH, ACK] Seq=442 Ack=15 Win=8442 Len=1
76	102.674570	127.0.0.1	127.0.0.1	TCP	44	4986 → 2121 [ACK] Seq=15 Ack=443 Win=1277 Len=0
84	117.687064	127.0.0.1	127.0.0.1	TCP	45	[TCP Keep-Alive] 4986 → 2121 [ACK] Seq=14 Ack=443 Win=1277 Len=1
85	117.687105	127.0.0.1	127.0.0.1	TCP	56	[TCP Keep-Alive ACK] 2121 → 4986 [ACK] Seq=443 Ack=15 Win=8442 Len=0 SLE=14 SRE=15
89	132.700249	127.0.0.1	127.0.0.1	TCP	45	[TCP Keep-Alive] 4986 → 2121 [ACK] Seq=14 Ack=443 Win=1277 Len=1
90	132.700334	127.0.0.1	127.0.0.1	TCP	56	[TCP Keep-Alive ACK] 2121 → 4986 [ACK] Seq=443 Ack=15 Win=8442 Len=0 SLE=14 SRE=15
92	147.714901	127.0.0.1	127.0.0.1	TCP	45	[TCP Keep-Alive] 4986 → 2121 [ACK] Seq=14 Ack=443 Win=1277 Len=1
93	147.714967	127.0.0.1	127.0.0.1	TCP	56	[TCP Keep-Alive ACK] 2121 → 4986 [ACK] Seq=443 Ack=15 Win=8442 Len=0 SLE=14 SRE=15
103	162.723446	127.0.0.1	127.0.0.1	TCP	45	[TCP Keep-Alive] 4986 → 2121 [ACK] Seq=14 Ack=443 Win=1277 Len=1
104	162.723518	127.0.0.1	127.0.0.1	TCP	56	[TCP Keep-Alive ACK] 2121 → 4986 [ACK] Seq=443 Ack=15 Win=8442 Len=0 SLE=14 SRE=15
132	177.727080	127.0.0.1	127.0.0.1	TCP	45	[TCP Keep-Alive] 4986 → 2121 [ACK] Seq=14 Ack=443 Win=1277 Len=1

Frame 61: 264 bytes on wire (2112 bits), 264 bytes captured (2112 bits) on interface \Device\NPF\_{...} id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

> Transmission Control Protocol, Src Port: 2121, Dst Port: 4986, Seq: 222, Ack: 12, Len: 220

> Data (220 bytes)

0000 02 00 00 00 45 00 01 04 6d 04 00 00 40 06 00 00 ...E...m...@...  
0010 7f 00 00 01 7f 00 00 01 08 49 13 7a 2b c1 45 e3 ...I...z+E...  
0020 63 5c cf 7b 50 18 20 fa b8 81 00 00 64 69 72 31 c\...{P...dir...  
0030 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  
0040 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  
0050 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

wireshark\_NPF\_{...}.pcapng

Packets: 159 · Displayed: 48 (30.2%) · Dropped: 0 (0.0%)

Profile: Default

13:00 2022-04-22

و در سیستم آقای کرباسیان در وایرشارک در حالت Wi-Fi به نتایج زیر رسیدیم :

Wireshark network traffic capture showing a TCP connection. The packet list shows a sequence of packets including PSH, ACK, and Keep-Alive. The packet details pane shows the 'Urgent pointer' field set to 0. A red arrow points to the 'Urgent pointer' field in the packet details pane, with a red handwritten note in Persian: 'و اینجا در سمت کلاینت رانسان می دهد' (and here on the client side it gives).

۹) سوال ۵/۳ : خیر نمیتوان دانلود کرد چون اولاً اکانت Permium در خوده ngrok نداریم فقط یکی توکن به ما میدهد و نمیتوانیم دوتا توکن داشته باشیم تا یکی برای Data Channel و یکی برای Control Channel تخصیص بدهیم و تقریباً باید این دو چنل را ادغام کنیم و از یکی برای هردو استفاده کنیم .

با این حال با وارد کردن کامند DWLD برنامه کرش میکند. مشکلی که این است که چون در تابع DWLD ما داریم یک پورت جدید میسازیم و باید به نحوی این را به ngrok هم بفهمانیم که پورت جدید ( همان پورت رندوم بین ۳۰۰۰ تا ۵۰۰۰ ) را برای کلاینت بفرستد. راهکاری که برای حل این مشکل پیدا نمودیم این است که در تابع DWLD به نحوی ngrok را اجرا کنیم و از بخش forwarding آن ، آرگومانهای host و port را برای کلاینت بفرستیم تا کلاینت بتواند هاست و پورت خودش را آپدیت کند و بتواند عملیات دانلود را انجام دهد.