

به نام خدا

امیررضا حسینی ۹۸۲۰۳۶۳

## تکلیف عملی اول شبکه

اسکرین شات مربوط به عملکرد برنامه:

### Help

```
timeout
end of connection

[08/04/2022 22:07.48] python server.py
server is ready

Welcome to the FTP server.

To get started, connect a client.
new connection start at port ('127.0.0.1', 14185)

start receive command

[08/04/2022 22:07.48] python client.py
enter command#: help

welcome to ftp client.
call one of the following functions:

commands:
help      : display this manual
list      : display a list of files and their size and directories(directories start with >)
pwd       : print workspace directory
cd {file name} : change directory to {file name}
dwl {file_path} : download file_path
Exit      : close the client

enter command#: 
```

### List

```
[08/04/2022 22:16.26] python server.py
server is ready

Welcome to the FTP server.

To get started, connect a client.
new connection start at port ('127.0.0.1', 1314)

start receive command

receive list request

sending data

[08/04/2022 22:16.26] python client.py
enter command#: list
hi.txt      21
>dir1
all files size:21
enter command#: 
```

### PWD & CD

```
[08/04/2022 22:16.26] python server.py
server is ready

Welcome to the FTP server.

To get started, connect a client.
new connection start at port ('127.0.0.1', 1314)

start receive command

receive list request

sending data

change directory

receive change directory request

change directory to \dir1

[08/04/2022 22:16.26] python client.py
enter command#: list
hi.txt      21
>dir1
all files size:21
enter command#: pwd
/

enter command#: cd dir1
\dir1
enter command#: pwd
\dir1

enter command#: 
```

## Download

```
To get started, connect a client.
new connection start at port ('127.0.0.1', 1950)

start receive command
change directory
receive change directory request
change directory to \dir1
receive list request
sending data
receive download request
file name received
make a data channel
port number sent
start data channel
file sent

all files size:21
enter command#: pwd
/

enter command#: cd dir1
\dir1
enter command#: pwd
\dir1

enter command#: exit

C:\drives\e\in progress 2\Computer Networks 1\project\1\amirreza\Source\client
08/04/2022 22:21:09 python client.py
enter command#: cd dir1
\dir1
enter command#: list
bigFile.bin      1048576
img.png          1273495
>inner
all files size:2322071
enter command#: dwld img.png
received.
enter command#:
```

## Quit

```
server is ready
Welcome to the FTP server.

To get started, connect a client.
new connection start at port ('127.0.0.1', 1314)

start receive command
receive list request
sending data
change directory
receive change directory request
change directory to \dir1
end of connection

> When using SSH, your remote DISPLAY is automatically forwarded
> Each command status is specified by a special symbol (✓ or ✗)

Registered to DeltaFoX (99 users)

C:\drives\e\in progress 2\Computer Networks 1\project\1\...\client
08/04/2022 22:16:20 python client.py
enter command#: list
hi.txt      21
>dir1
all files size:21
enter command#: pwd
/

enter command#: cd dir1
\dir1
enter command#: pwd
\dir1

enter command#: exit

C:\drives\e\in progress 2\Computer Networks 1\project\1\...\server
08/04/2022 22:21:09 ✓

C:\drives\e\in progress 2\Computer Networks 1\project\1\amirreza\Source\client
08/04/2022 22:21:09
```

PC > New Volume (E:) > in progress 2 > Computer Networks 1 > project > 1 > amirreza > Source > client



سوال : چرا این روند برعکس نیست یعنی کلاینت يك پورت را باز نمی کند و آن را به سرور اطلاع دهد و سرور فایل را روی آن پورت برای کلاینت ارسال کند؟

جواب: چون در این صورت اگر سرور بتواند به پورتي که کلاینت ساخته دسترسی داشته باشد به علت وجود امنیت ها و privilege های read-write دسترسی آن توسط firewall بلاک میشود و با این کار جلوی هک و خرابکاری را میگیرد.

سوال : ورودی هایی برای دستورات CD و DWLD که باعث شود فایلی دانلود شود یا فولدري باز شود که در زیرشاخه های فولدر اصلی سرور قرار ندارد (مثل فایل های سیستم عامل) این حمله چه نام دارد؟

جواب: نام این حمله command injection نام دارد. مهمترین علت این حمل سهل انگاری در محافظت در دسترسی ها می باشد که برای پوشه ریشه در نظر گرفته نشده است. و مهاجم میتواند با دستورات مناسب به پوشه قبل از root دسترسی پیدا کند و فایل های سیستمی را بدون اجازه تغییر دهد.

## Whireshark

### Handshaking

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	TCP	56	57573 → 2121 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
2	0.000062	127.0.0.1	127.0.0.1	TCP	56	2121 → 57573 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
3	0.000134	127.0.0.1	127.0.0.1	TCP	44	57573 → 2121 [ACK] Seq=1 Ack=1 Win=2619648 Len=0

  

> Frame 1: 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: 57573, Dst Port: 2121, Seq: 0, Len: 0	

  

0000	02 00 00 00 45 00 00 34	bb fe 40 00 80 06 00 00	.....4..@.....
0010	7f 00 00 01 7f 00 00 01	e0 e5 08 49 bf 48 13 d1	.....I.H.....
0020	00 00 00 00 80 02 ff ff	ba a1 00 00 04 ff d7	.....[.....
0030	01 03 03 08 01 01 04 02		.....

سوال : آیا TCP محدودیتی برای اندازه بسته ها دارد؟ فایل های بزرگ چگونه توسط سوکت TCP ارسال میشوند؟

محدودیت اندازه بسته ها ۶۴ کیلو بایت است و سوکت tcp بسته های بزرگ دریافتی را به پکت هایی با حداکثر سائز ۶۴ کیلوبایت در می آورد و ارسال میکند.

سوال : براي مشاهده ي عملي جواب قسمت قبل، ابتدا وايرشارك را روشن كنيد و سپس در كلاينت درخواست دانلود فايل bigFile.txt را بدهيد. از نتايج وايرشارك اسكرين شات بگيريد. TCP براي دانلود اين فايل چند بسته فرستاده است؟

13474	653	748697612	127.0.0.1	127.0.0.1	TCP	32834 4782 - 45850 [PSH, ACK] Seq=688129 Ack=1 Win=65536 Len=32768 TSval=296774418 TSecr=296774418
13475	653	748702374	127.0.0.1	127.0.0.1	TCP	32834 [TCP Window Full] 4782 - 45850 [ACK] Seq=728097 Ack=1 Win=65536 Len=32768 TSval=296774418 TSecr=296774418
13476	653	748722903	127.0.0.1	127.0.0.1	TCP	66 [TCP ZeroWindow] 45850 - 4782 [ACK] Seq=1 Ack=753665 Win=0 Len=0 TSval=296774418 TSecr=296774418
13477	653	741084418	127.0.0.1	127.0.0.1	TCP	66 [TCP Window Update] 45850 - 4782 [ACK] Seq=1 Ack=753665 Win=48512 Len=0 TSval=296774419 TSecr=296774418
13478	653	741090890	127.0.0.1	127.0.0.1	TCP	32834 4782 - 45850 [PSH, ACK] Seq=753665 Ack=1 Win=65536 Len=32768 TSval=296774419 TSecr=296774419
13479	653	741619840	127.0.0.1	127.0.0.1	TCP	66 45850 - 4782 [ACK] Seq=1 Ack=786433 Win=65536 Len=0 TSval=296774419 TSecr=296774419
13480	653	741625577	127.0.0.1	127.0.0.1	TCP	32834 4782 - 45850 [ACK] Seq=786433 Ack=1 Win=65536 Len=32768 TSval=296774419 TSecr=296774419
13481	653	741631090	127.0.0.1	127.0.0.1	TCP	32834 [TCP Window Full] 4782 - 45850 [PSH, ACK] Seq=819201 Ack=1 Win=65536 Len=32768 TSval=296774419 TSecr=296774419
13482	653	741677235	127.0.0.1	127.0.0.1	TCP	66 [TCP ZeroWindow] 45850 - 4782 [ACK] Seq=1 Ack=851969 Win=0 Len=0 TSval=296774419 TSecr=296774419
13483	653	741974038	127.0.0.1	127.0.0.1	TCP	66 [TCP Window Update] 45850 - 4782 [ACK] Seq=1 Ack=851969 Win=48512 Len=0 TSval=296774420 TSecr=296774419
13484	653	741979520	127.0.0.1	127.0.0.1	TCP	32834 4782 - 45850 [ACK] Seq=851969 Ack=1 Win=65536 Len=32768 TSval=296774420 TSecr=296774420
13485	653	742707681	127.0.0.1	127.0.0.1	TCP	66 45850 - 4782 [ACK] Seq=1 Ack=884737 Win=65536 Len=0 TSval=296774420 TSecr=296774420
13486	653	742715755	127.0.0.1	127.0.0.1	TCP	32834 4782 - 45850 [PSH, ACK] Seq=884737 Ack=1 Win=65536 Len=32768 TSval=296774420 TSecr=296774420
13487	653	742721411	127.0.0.1	127.0.0.1	TCP	32834 [TCP Window Full] 4782 - 45850 [ACK] Seq=917505 Ack=1 Win=65536 Len=32768 TSval=296774420 TSecr=296774420
13488	653	742773337	127.0.0.1	127.0.0.1	TCP	66 [TCP ZeroWindow] 45850 - 4782 [ACK] Seq=1 Ack=950273 Win=0 Len=0 TSval=296774420 TSecr=296774420
13489	653	743166283	127.0.0.1	127.0.0.1	TCP	66 [TCP Window Update] 45850 - 4782 [ACK] Seq=1 Ack=950273 Win=48512 Len=0 TSval=296774421 TSecr=296774420
13490	653	743174606	127.0.0.1	127.0.0.1	TCP	32834 4782 - 45850 [PSH, ACK] Seq=950273 Ack=1 Win=65536 Len=32768 TSval=296774421 TSecr=296774421
13491	653	744076064	127.0.0.1	127.0.0.1	TCP	66 45850 - 4782 [ACK] Seq=1 Ack=983841 Win=65536 Len=0 TSval=296774422 TSecr=296774421
13492	653	744085586	127.0.0.1	127.0.0.1	TCP	32834 4782 - 45850 [ACK] Seq=983841 Ack=1 Win=65536 Len=32768 TSval=296774422 TSecr=296774422
13493	653	744091375	127.0.0.1	127.0.0.1	TCP	32834 [TCP Window Full] 4782 - 45850 [PSH, ACK] Seq=1015809 Ack=1 Win=65536 Len=32768 TSval=296774422 TSecr=296774422
13494	653	744102268	127.0.0.1	127.0.0.1	TCP	66 [TCP ZeroWindow] 45850 - 4782 [ACK] Seq=1 Ack=1048577 Win=0 Len=0 TSval=296774422 TSecr=296774422
13495	653	744522123	127.0.0.1	127.0.0.1	TCP	66 [TCP Window Update] 45850 - 4782 [ACK] Seq=1 Ack=1048577 Win=48512 Len=0 TSval=296774422 TSecr=296774422
13496	653	744528589	127.0.0.1	127.0.0.1	TCP	32834 4782 - 45850 [ACK] Seq=1048577 Ack=1 Win=65536 Len=32768 TSval=296774422 TSecr=296774422
13497	653	745333501	127.0.0.1	127.0.0.1	TCP	66 45850 - 4782 [ACK] Seq=1 Ack=1081345 Win=65536 Len=0 TSval=296774423 TSecr=296774422
13498	653	745340861	127.0.0.1	127.0.0.1	TCP	32834 4782 - 45850 [PSH, ACK] Seq=1081345 Ack=1 Win=65536 Len=32768 TSval=296774423 TSecr=296774423
13499	653	745345092	127.0.0.1	127.0.0.1	TCP	32834 [TCP Window Full] 4782 - 45850 [ACK] Seq=1114113 Ack=1 Win=65536 Len=32768 TSval=296774423 TSecr=296774423
13500	653	745401268	127.0.0.1	127.0.0.1	TCP	66 [TCP ZeroWindow] 45850 - 4782 [ACK] Seq=1 Ack=1146881 Win=0 Len=0 TSval=296774423 TSecr=296774423
13501	653	745775220	127.0.0.1	127.0.0.1	TCP	66 [TCP Window Update] 45850 - 4782 [ACK] Seq=1 Ack=1146881 Win=48512 Len=0 TSval=296774423 TSecr=296774423
13502	653	745783148	127.0.0.1	127.0.0.1	TCP	32834 4782 - 45850 [PSH, ACK] Seq=1146881 Ack=1 Win=65536 Len=32768 TSval=296774423 TSecr=296774423
13503	653	746608252	127.0.0.1	127.0.0.1	TCP	66 45850 - 4782 [ACK] Seq=1 Ack=1179649 Win=65536 Len=0 TSval=296774424 TSecr=296774423
13504	653	746614096	127.0.0.1	127.0.0.1	TCP	32834 4782 - 45850 [ACK] Seq=1179649 Ack=1 Win=65536 Len=32768 TSval=296774424 TSecr=296774424
13505	653	746618901	127.0.0.1	127.0.0.1	TCP	32834 [TCP Window Full] 4782 - 45850 [PSH, ACK] Seq=1212417 Ack=1 Win=65536 Len=32768 TSval=296774424 TSecr=296774424
13506	653	746676197	127.0.0.1	127.0.0.1	TCP	66 [TCP ZeroWindow] 45850 - 4782 [ACK] Seq=1 Ack=1245185 Win=0 Len=0 TSval=296774424 TSecr=296774424
13507	653	747066843	127.0.0.1	127.0.0.1	TCP	66 [TCP Window Update] 45850 - 4782 [ACK] Seq=1 Ack=1245185 Win=48512 Len=0 TSval=296774425 TSecr=296774424
13508	653	747072209	127.0.0.1	127.0.0.1	TCP	32834 4782 - 45850 [ACK] Seq=1245185 Ack=1 Win=65536 Len=32768 TSval=296774425 TSecr=296774425
13509	653	747957403	127.0.0.1	127.0.0.1	TCP	66 45850 - 4782 [ACK] Seq=1 Ack=1277953 Win=65536 Len=0 TSval=296774426 TSecr=296774425
13510	653	747963238	127.0.0.1	127.0.0.1	TCP	24359 4782 - 45850 [FIN, PSH, ACK] Seq=1277953 Ack=1 Win=65536 Len=24293 TSval=296774426 TSecr=296774426
13511	653	755363260	127.0.0.1	127.0.0.1	TCP	66 45850 - 4782 [FIN, ACK] Seq=1 Ack=1302247 Win=65536 Len=0 TSval=296774433 TSecr=296774426
13512	653	755374706	127.0.0.1	127.0.0.1	TCP	66 4782 - 45850 [ACK] Seq=1302247 Ack=2 Win=65536 Len=0 TSval=296774433 TSecr=296774433

بسته هایی با سايز حدودا ۳۲كيلوبايت ارسال شده مجموعا ۳۲بسته ارسال شده. ۳۱بسته ۳۲كيلو بايتی و سايز بسته آخر هم حدودا ۲۴ كيلوبايت است.