

(۱) چون معمولا Client در پشت Firewall یا Nat است پس نمیتواند برای خودش پورت جدیدی باز کند، اما میتواند با دستگاه دیگری ارتباط برقرار کند. بدین سبب Server یک پورت رندوم باز کرده و در Control channel آن پورت را به Client گزارش میدهد و از این طریق Client به پورت گزارش شده ی سرور، متصل میشود.

(۲) تصاویر مربوط به ران کردن کلاینت و سرور

The screenshot shows a network setup. On the left, a terminal window titled 'C:\Windows\System32\cmd.exe - python client.py' displays the following commands and outputs:

```

Microsoft Windows [Version 10.0.19044.1586]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Lenovo\Desktop\Network>python client.py

HELP      : Show help
LIST      : Show all files and folders
DwLD filePath : Download a file in specific path
PWD       : Print working directory
CD dirName  : Change directory to specific path
QUIT      : Quit command

input : dfsd
Invalid input!

input : help

HELP      : Show help
LIST      : Show all files and folders
DwLD filePath : Download a file in specific path
PWD       : Print working directory
CD dirName  : Change directory to specific path
QUIT      : Quit command

input : list

<DIR> dir1
32 hi.txt

input : dwld hi
No such file or directory.

input : dwld hi.txt
Downloaded successfully

input : pwd
\

input : cd wdfsad
The system cannot find the path specified.

input : cd ..
The destination is unauthorized.

input : cd dir1
\dir1

input : _

```

On the right, a terminal window titled 'C:\Windows\System32\cmd.exe - python server.py' shows the server's output:

```

C:\Users\Lenovo\Desktop\Network>python server.py

The client with address ('127.0.0.1', 62597) was connected.
User with address ('127.0.0.1', 63361) downloaded file from path "hi.txt"

```

Below the terminal windows, a File Explorer window titled 'sources' shows the contents of the 'sources' directory:

Name	Date modified	Type	Size
dir1	3/30/2022 12:52	File folder	1 KB
hi.txt	3/30/2022 12:41	Text Document	1 KB

The screenshot shows a network setup. On the left, a terminal window titled 'C:\Windows\System32\cmd.exe' displays the following commands and outputs:

```

input : cd ..
The destination is unauthorized.

input : cd dir1
\dir1

input : pwd
\dir1

input : list

1048576 bigFile.bin
<DIR> inner

input : dwld big
No such file or directory.

input : dwld bigFile.bin
Downloaded successfully

input : cd ..
\

input : cd dir1\inner
\dir1\inner

input : dwld ..\inner\test.txt
Downloaded successfully

input : cd ..\..
\

input : list

<DIR> dir1
32 hi.txt

input : help

HELP      : Show help
LIST      : Show all files and folders
DwLD filePath : Download a file in specific path
PWD       : Print working directory
CD dirName  : Change directory to specific path
QUIT      : Quit command

input : quit
C:\Users\Lenovo\Desktop\Network>

```

On the right, a terminal window titled 'C:\Windows\System32\cmd.exe - python server.py' shows the server's output:

```

C:\Users\Lenovo\Desktop\Network>python server.py

The client with address ('127.0.0.1', 62597) was connected.
User with address ('127.0.0.1', 63361) downloaded file from path "hi.txt"
User with address ('127.0.0.1', 51228) downloaded file from path "dir1\bigFile.bin"
User with address ('127.0.0.1', 95641) downloaded file from path "dir1\inner\test.txt"

```

Below the terminal windows, a File Explorer window titled 'dir1' shows the contents of the 'dir1' directory:

Name	Date modified	Type	Size
inner	3/30/2022 12:52	File folder	
bigFile.bin	3/30/2022 12:51	BIN File	1,024 KB

نام حمله ای که مهاجم به فایل‌های سیستم دسترسی پیدا میکند، به Dot Dot Slash یا Directory Traversal و یا Directory Climbing مشهور است و طی این حمله، مهاجم میتواند به اطلاعات کامپیوتر قربانی دست پیدا کند.

(۴) سه عکس مربوط به handshaking

Wireshark packet capture showing TCP handshake between 127.0.0.1 and 127.0.0.1 on port 2121. The capture is titled "Capturing from Adapter for loopback traffic capture". The packet list shows five packets:

No.	Time	Source	Destination	Protocol	Length	Info
165	24.271098	127.0.0.1	127.0.0.1	TCP	56	54546 → 2121 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
166	24.271148	127.0.0.1	127.0.0.1	TCP	56	2121 → 54546 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
167	24.271214	127.0.0.1	127.0.0.1	TCP	44	54546 → 2121 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
168	24.271501	127.0.0.1	127.0.0.1	TCP	83	2121 → 54546 [PSH, ACK] Seq=1 Ack=1 Win=2619648 Len=39
169	24.271514	127.0.0.1	127.0.0.1	TCP	44	54546 → 2121 [ACK] Seq=1 Ack=40 Win=2619648 Len=0

The packet details pane for Frame 165 shows:

- Interface id: 0 (\Device\NPF_{...})
- Encapsulation type: NULL/Loopback (15)
- Arrival Time: Mar 30, 2022 16:58:16.654204000 Iran Daylight Time
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1648643296.654204000 seconds
- [Time delta from previous captured frame: 4.254457000 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 24.271098000 seconds]
- Frame Number: 165
- Frame Length: 56 bytes (448 bits)
- Capture Length: 56 bytes (448 bits)
- [Frame is marked: False]

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 02 00 00 00 45 00 00 34 66 12 40 00 80 06 00 00  ....E..4 f @.....
0010 7f 00 00 01 7f 00 00 01 d5 12 08 49 a3 52 87 c2  .......I.R..
0020 00 00 00 00 80 02 ff ff 6e 79 00 00 02 04 ff d7  ....ny.....
0030 01 03 03 08 01 01 04 02  .........
```

Wireshark packet capture showing TCP handshake between 127.0.0.1 and 127.0.0.1 on port 2121. The capture is titled "Capturing from Adapter for loopback traffic capture". The packet list shows five packets:

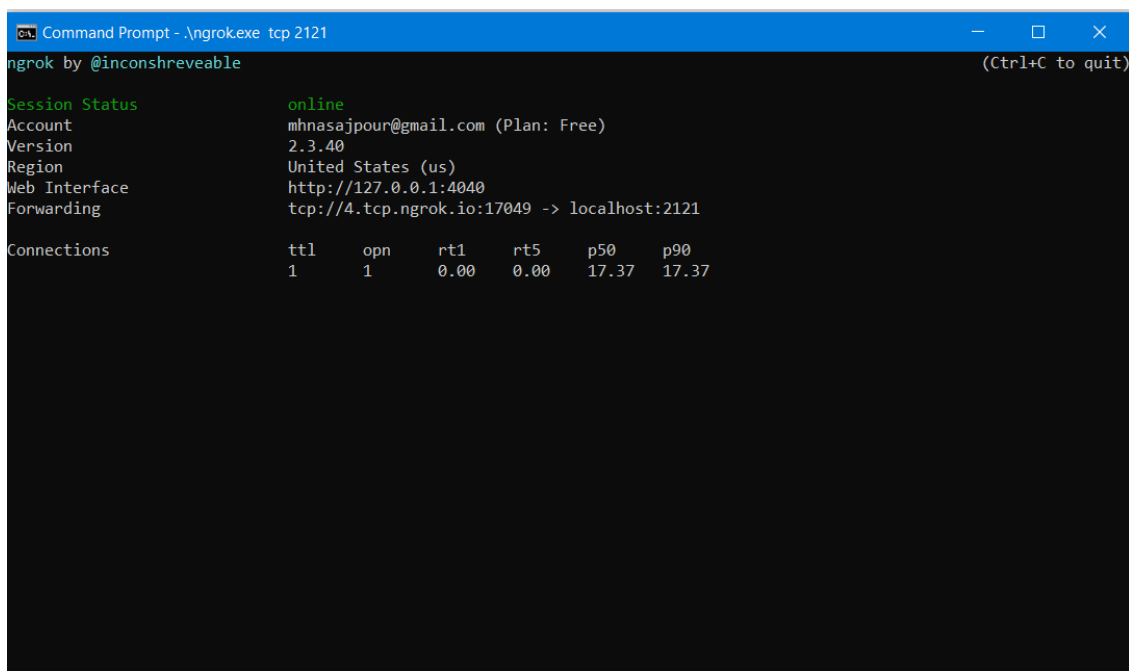
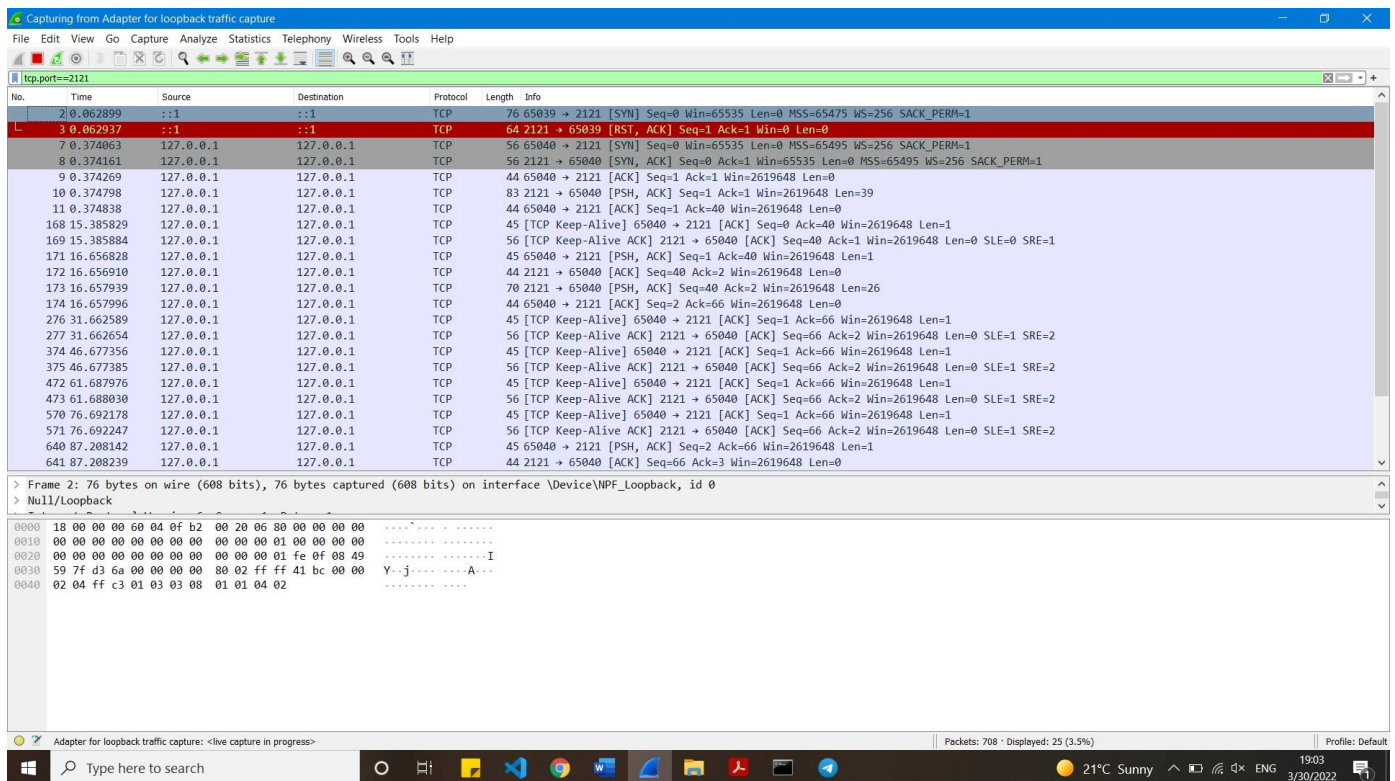
No.	Time	Source	Destination	Protocol	Length	Info
165	24.271098	127.0.0.1	127.0.0.1	TCP	56	54546 → 2121 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
166	24.271148	127.0.0.1	127.0.0.1	TCP	56	2121 → 54546 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
167	24.271214	127.0.0.1	127.0.0.1	TCP	44	54546 → 2121 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
168	24.271501	127.0.0.1	127.0.0.1	TCP	83	2121 → 54546 [PSH, ACK] Seq=1 Ack=1 Win=2619648 Len=39
169	24.271514	127.0.0.1	127.0.0.1	TCP	44	54546 → 2121 [ACK] Seq=1 Ack=40 Win=2619648 Len=0

The packet details pane for Frame 166 shows:

- Interface id: 0 (\Device\NPF_{...})
- Encapsulation type: NULL/Loopback (15)
- Arrival Time: Mar 30, 2022 16:58:16.654254000 Iran Daylight Time
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1648643296.654254000 seconds
- [Time delta from previous captured frame: 0.000050000 seconds]
- [Time delta from previous displayed frame: 0.000050000 seconds]
- [Time since reference or first frame: 24.271148000 seconds]
- Frame Number: 166
- Frame Length: 56 bytes (448 bits)
- Capture Length: 56 bytes (448 bits)
- [Frame is marked: False]

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 02 00 00 00 45 00 00 34 66 13 40 00 80 06 00 00  ....E..4 f @.....
0010 7f 00 00 01 7f 00 00 01 08 49 d5 12 e3 d1 ad cb  .......I.....
0020 a3 52 87 c3 80 12 ff ff dc ca 00 00 02 04 ff d7  ....R.....
0030 01 03 03 08 01 01 04 02  .........
```

۷ زمانی که از ngrok استفاده میکنیم دستورات ابتدا از بستر اینترنت به سرورهای آن رفته و سپس به کامپیوتر می آید. اما اگر از ngrok استفاده نکنیم، دستورات در همین کامپیوتر فرستاده میشوند و به سرورها فرستاده نمیشوند.

با این مکانیزم و با ngrok نمیتوانم فایلی ارسال کنیم. در مکانیزم انتقال فایل ابتدا سرور پورت جدیدی باز میکند و آنرا به کلاینت اطلاع میدهد. اما در این بین ngrok پورت خود را تعویض نمیکند و کانال داده و کانال کنترل دچار کانفیلیکت میشوند.

برای حل این مشکل میتوان از یک پورت کانستنت به جای رندوم استفاده کرد که این راه نیز مشکلاتی از جمله پاسخ دهی به کلاینت ها را در بر دارد.