CPSC 526

Assignment 3

Tutorial: T01

Name: Sam Ao

ID: 10111222

Partner: Artin Rezaee-Anzabee

Running the program:

The program can be run by: python3 server.py <logOption> <replaceOption> <word to be replaced> <replace with> srcPort destAddress destPort.
To connect to server, open a new terminal and write: nc localhost <port>.
You can also use a browser as the client.
Server will bind to the user specified port and start listening for commands.
Server will create a connection to the speciefied destAddress via destPort and listen for server data.
The serve works with the back-door server from assignment2

Connecting to server and handshake details:

The server will be bound to the specified source port and will create a new connection to the destination address via the specified destination port on every new client.
The server will log the date and time of the new connection

Supported command:

Commands supported by the server are:

- -raw
- -strip
- -hex
- -autoN
- -replace

Server behaviour:

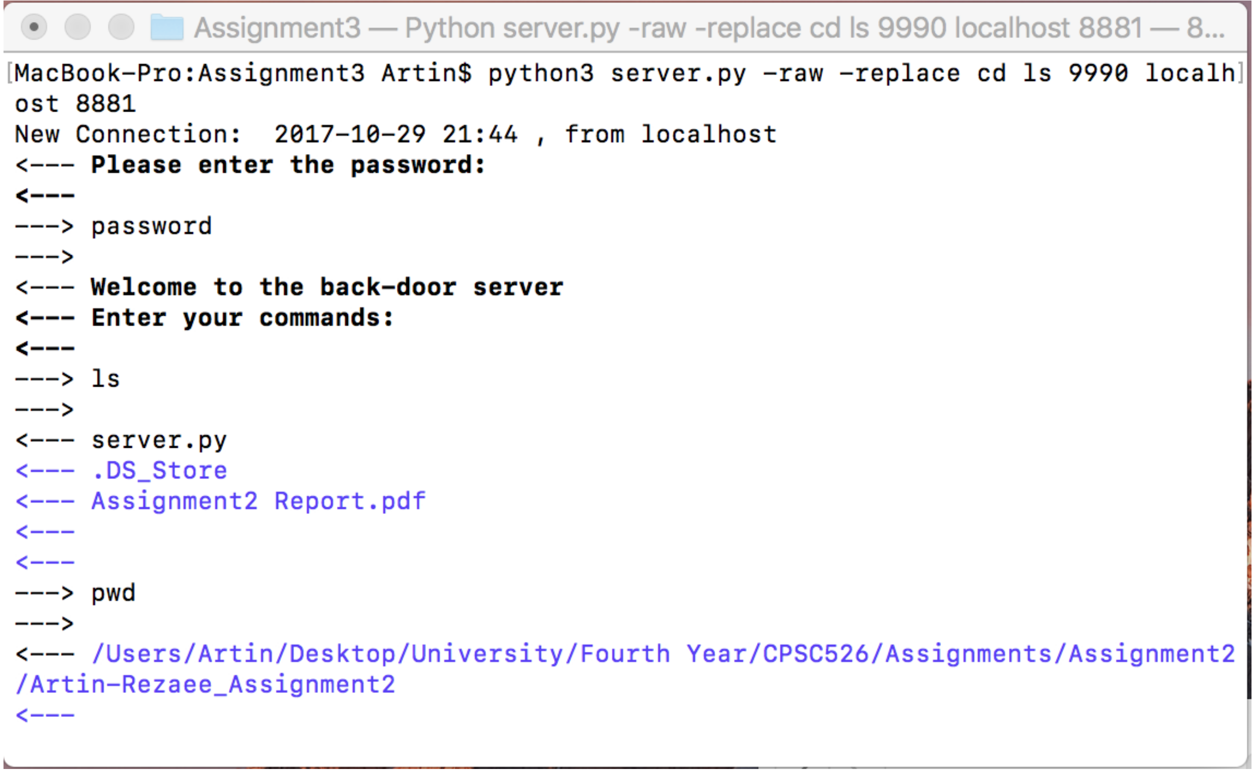
Depending on the log options and the presence of replace options.

- Server running with the raw command will simply log input and outputs, identified with □ and □ , in plain string.
- Server running with hex creates a log similar to the Linux hexdump –C command.
- Server running with strip option will replace all the non-printable characters with dots while printable characters are untouched.
- Server running with the autoN command, will divide and log the input and output data in N-byte long chunks and output them on their own line. Each byte in the chunk will be displayed based on its value. If the byte is a backslash, tab, newline or carriage return, it’ll be reported in escaped form, i.e. ‘\\’, ‘\t’, ‘\n’ and ‘\r’ respectively. If the byte is in range 32...127, it will be displayed in raw form. In all other cases the byte will be displayed with a leading slash, followed by a two-digit hexadecimal value of the byte.
- The replace option can be run along with each log option, the replace function will look for the word that it needs to replace and replace it with the user specified word. Server will then output the changed data to its client or server (MITM attack)

All options above will output data both to the client and server of the port forwarding server. All input logs from port-forwarding’s server are identified by □ and all outgoing logs from port-forwarding server which it has received from client is identified by □

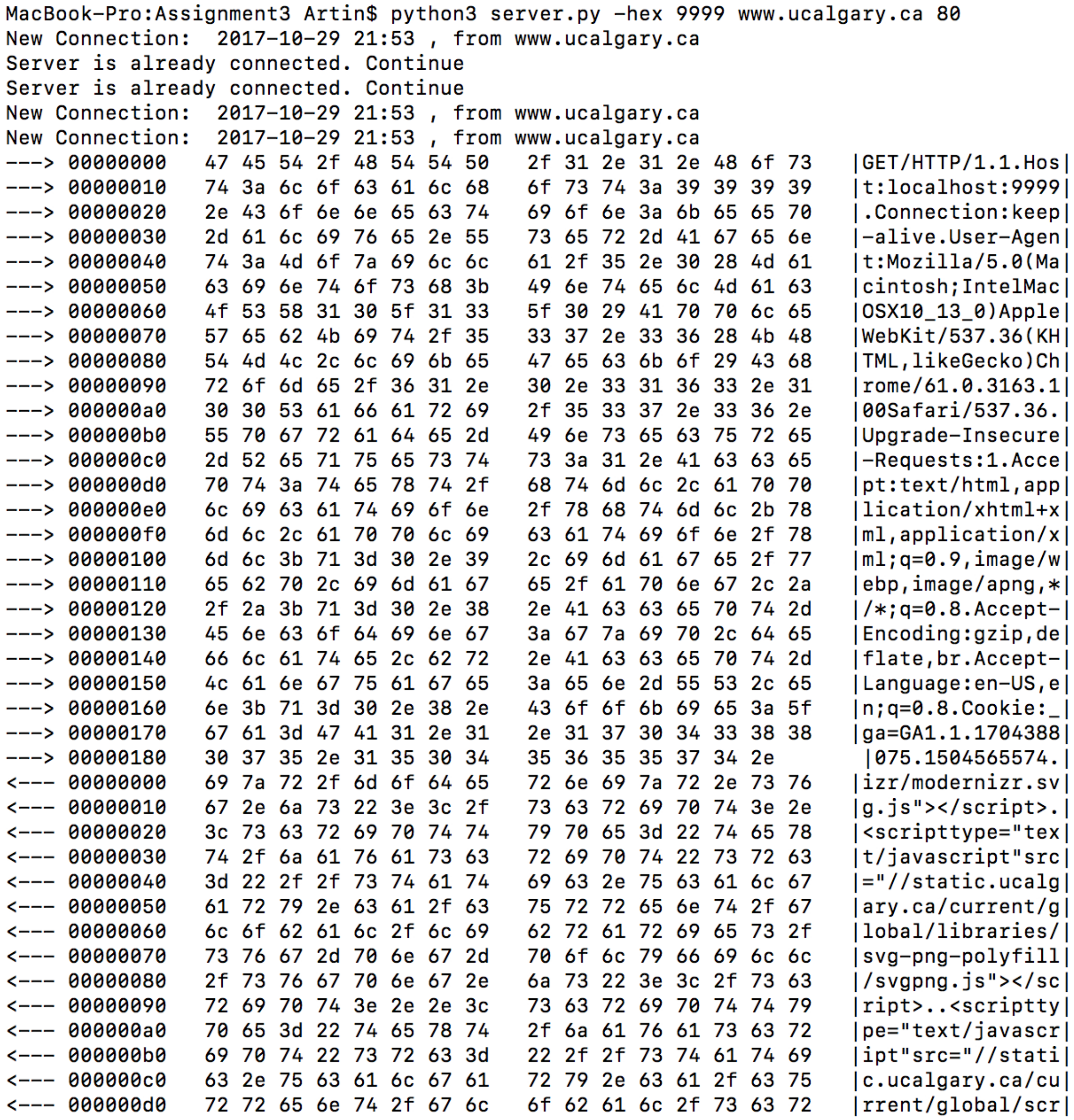
Examples:

-Raw: port-forwarding server view


Assignment3 — Python server.py -raw -replace cd ls 9990 localhost 8881 — 8...

```
[MacBook-Pro:Assignment3 Artin$ python3 server.py -raw -replace cd ls 9990 localh]
 ost 8881
 New Connection:  2017-10-29 21:44 , from localhost
 <--- Please enter the password:
 <---
 ---> password
 --->
 <--- Welcome to the back-door server
 <--- Enter your commands:
 <---
 ---> ls
 --->
 <--- server.py
 <--- .DS_Store
 <--- Assignment2 Report.pdf
 <---
 <---
 ---> pwd
 --->
 <--- /Users/Artin/Desktop/University/Fourth Year/CPSC526/Assignments/Assignment2
 /Artin-Rezaee_Assignment2
 <---
```

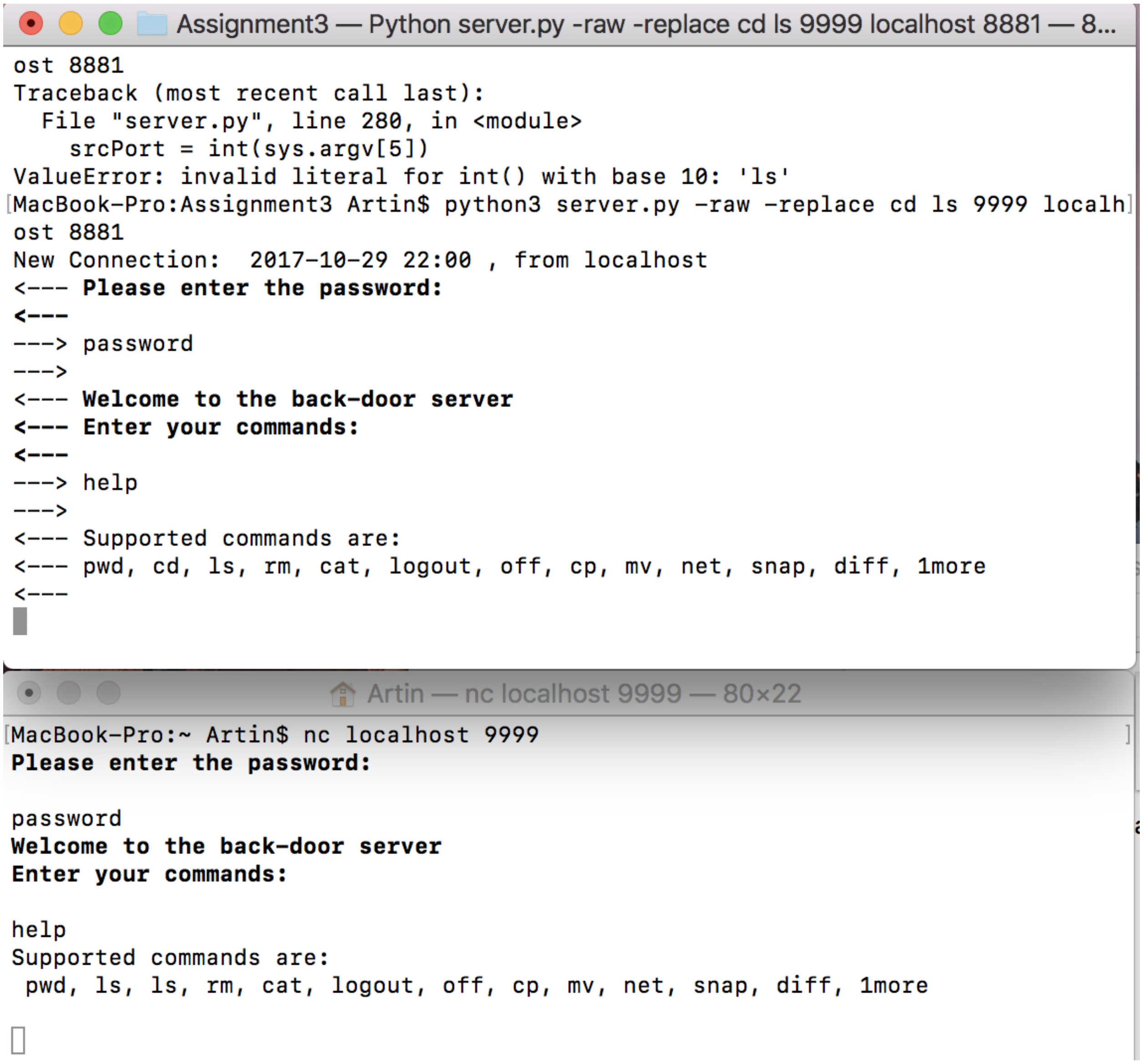
-Hex: port-forwarding server view



```
MacBook-Pro:Assignment3 Artin$ python3 server.py -hex 9999 www.ucalgary.ca 80
New Connection:  2017-10-29 21:53 , from www.ucalgary.ca
Server is already connected. Continue
Server is already connected. Continue
New Connection:  2017-10-29 21:53 , from www.ucalgary.ca
New Connection:  2017-10-29 21:53 , from www.ucalgary.ca
---> 00000000   47 45 54 2f 48 54 54 50   2f 31 2e 31 2e 48 6f 73   |GET/HTTP/1.1.Hos|
---> 00000010   74 3a 6c 6f 63 61 6c 68   6f 73 74 3a 39 39 39 39   |t:localhost:9999|
---> 00000020   2e 43 6f 6e 6e 65 63 74   69 6f 6e 3a 6b 65 65 70   |.Connection:keep|
---> 00000030   2d 61 6c 69 76 65 2e 55   73 65 72 2d 41 67 65 6e   |-alive.User-Agen|
---> 00000040   74 3a 4d 6f 7a 69 6c 6c   61 2f 35 2e 30 28 4d 61   |t:Mozilla/5.0(Ma|
---> 00000050   63 69 6e 74 6f 73 68 3b   49 6e 74 65 6c 4d 61 63   |cintosh;IntelMac|
---> 00000060   4f 53 58 31 30 5f 31 33   5f 30 29 41 70 70 6c 65   |OSX10_13_0)Apple|
---> 00000070   57 65 62 4b 69 74 2f 35   33 37 2e 33 36 28 4b 48   |WebKit/537.36(KH|
---> 00000080   54 4d 4c 2c 6c 69 6b 65   47 65 63 6b 6f 29 43 68   |TML,likeGecko)Ch|
---> 00000090   72 6f 6d 65 2f 36 31 2e   30 2e 33 31 36 33 2e 31   |rome/61.0.3163.1|
---> 000000a0   30 30 53 61 66 61 72 69   2f 35 33 37 2e 33 36 2e   |00Safari/537.36.|
---> 000000b0   55 70 67 72 61 64 65 2d   49 6e 73 65 63 75 72 65   |Upgrade-Insecure|
---> 000000c0   2d 52 65 71 75 65 73 74   73 3a 31 2e 41 63 63 65   |-Requests:1.Acce|
---> 000000d0   70 74 3a 74 65 78 74 2f   68 74 6d 6c 2c 61 70 70   |pt:text/html,app|
---> 000000e0   6c 69 63 61 74 69 6f 6e   2f 78 68 74 6d 6c 2b 78   |lication/xhtml+x|
---> 000000f0   6d 6c 2c 61 70 70 6c 69   63 61 74 69 6f 6e 2f 78   |ml,application/x|
---> 00000100   6d 6c 3b 71 3d 30 2e 39   2c 69 6d 61 67 65 2f 77   |ml;q=0.9,image/w|
---> 00000110   65 62 70 2c 69 6d 61 67   65 2f 61 70 6e 67 2c 2a   |ebp,image/apng,*|
---> 00000120   2f 2a 3b 71 3d 30 2e 38   2e 41 63 63 65 70 74 2d   |/*;q=0.8.Accept-|
---> 00000130   45 6e 63 6f 64 69 6e 67   3a 67 7a 69 70 2c 64 65   |Encoding:gzip,de|
---> 00000140   66 6c 61 74 65 2c 62 72   2e 41 63 63 65 70 74 2d   |flate,br.Accept-|
---> 00000150   4c 61 6e 67 75 61 67 65   3a 65 6e 2d 55 53 2c 65   |Language:en-US,e|
---> 00000160   6e 3b 71 3d 30 2e 38 2e   43 6f 6f 6b 69 65 3a 5f   |n;q=0.8.Cookie:_|
---> 00000170   67 61 3d 47 41 31 2e 31   2e 31 37 30 34 33 38 38   |ga=GA1.1.1704388|
---> 00000180   30 37 35 2e 31 35 30 34   35 36 35 35 37 34 2e       |075.1504565574.|
<--- 00000000   69 7a 72 2f 6d 6f 64 65   72 6e 69 7a 72 2e 73 76   |izr/modernizr.sv|
<--- 00000010   67 2e 6a 73 22 3e 3c 2f   73 63 72 69 70 74 3e 2e   |g.js"></script>.|
<--- 00000020   3c 73 63 72 69 70 74 74   79 70 65 3d 22 74 65 78   |<scripttype="tex|
<--- 00000030   74 2f 6a 61 76 61 73 63   72 69 70 74 22 73 72 63   |t/javascript"src|
<--- 00000040   3d 22 2f 2f 73 74 61 74   69 63 2e 75 63 61 6c 67   |="//static.ucalg|
<--- 00000050   61 72 79 2e 63 61 2f 63   75 72 72 65 6e 74 2f 67   |ary.ca/current/g|
<--- 00000060   6c 6f 62 61 6c 2f 6c 69   62 72 61 72 69 65 73 2f   |lobal/libraries/|
<--- 00000070   73 76 67 2d 70 6e 67 2d   70 6f 6c 79 66 69 6c 6c   |svg-png-polyfill|
<--- 00000080   2f 73 76 67 70 6e 67 2e   6a 73 22 3e 3c 2f 73 63   |/svgpng.js"></sc|
<--- 00000090   72 69 70 74 3e 2e 2e 3c   73 63 72 69 70 74 74 79   |ript>..<scriptty|
<--- 000000a0   70 65 3d 22 74 65 78 74   2f 6a 61 76 61 73 63 72   |pe="text/javascr|
<--- 000000b0   69 70 74 22 73 72 63 3d   22 2f 2f 73 74 61 74 69   |ipt"src="//stati|
<--- 000000c0   63 2e 75 63 61 6c 67 61   72 79 2e 63 61 2f 63 75   |c.ucalgary.ca/cu|
<--- 000000d0   72 72 65 6e 74 2f 67 6c   6f 62 61 6c 2f 73 63 72   |rrent/global/scr|
```

-Replace: Both client and port-forwarding server view

The server has replaced all occurrences of cd with ls. Hence, the result of the help command includes 2 instances of ls


Assignment3 — Python server.py -raw -replace cd ls 9999 localhost 8881 — 8...

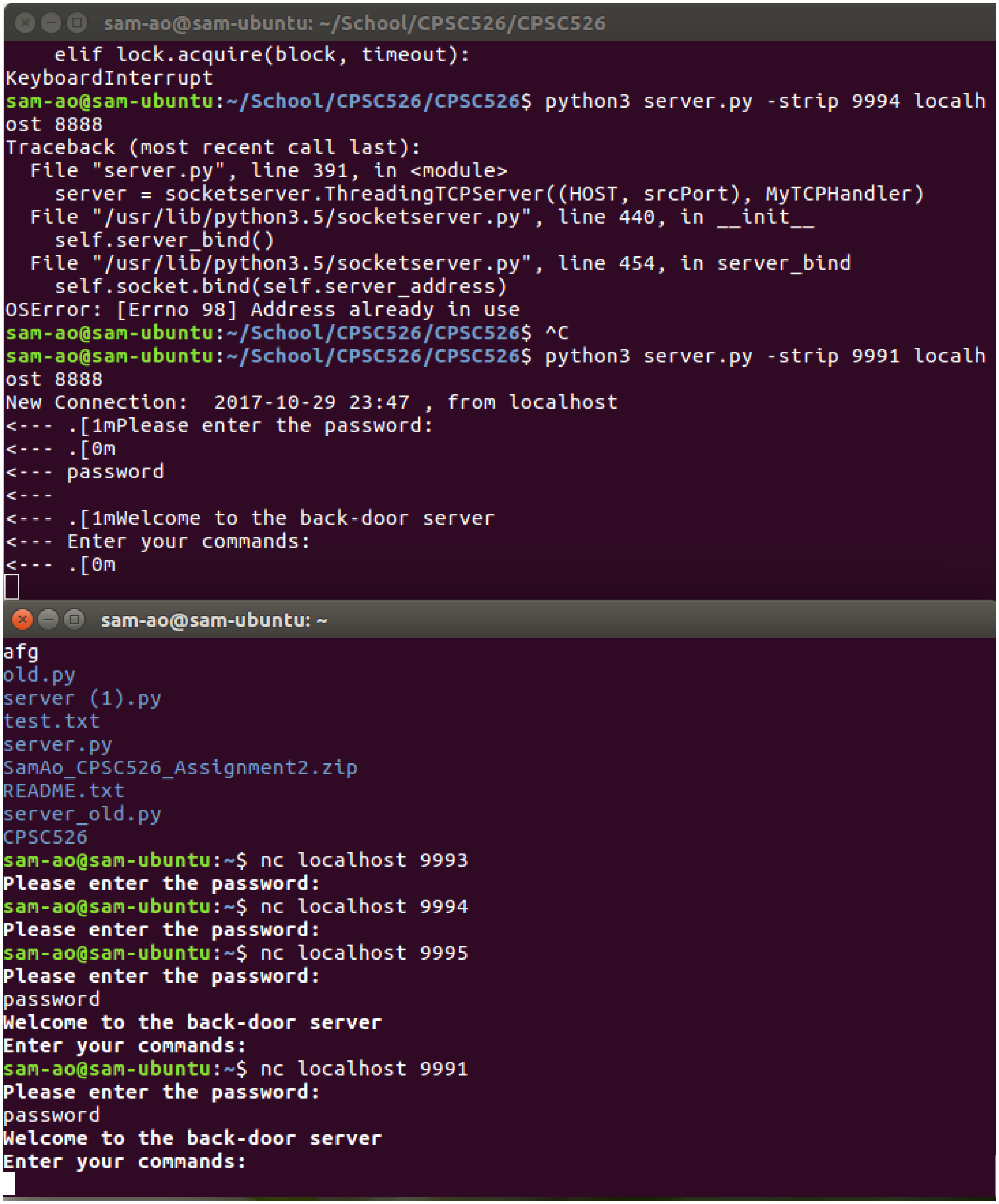
```
ost 8881
Traceback (most recent call last):
  File "server.py", line 280, in <module>
    srcPort = int(sys.argv[5])
ValueError: invalid literal for int() with base 10: 'ls'
[MacBook-Pro:Assignment3 Artin$ python3 server.py -raw -replace cd ls 9999 localh]
ost 8881
New Connection:  2017-10-29 22:00 , from localhost
<--- Please enter the password:
<---
---> password
--->
<--- Welcome to the back-door server
<--- Enter your commands:
<---
---> help
--->
<--- Supported commands are:
<--- pwd, cd, ls, rm, cat, logout, off, cp, mv, net, snap, diff, 1more
<---
```

```
[MacBook-Pro:~ Artin$ nc localhost 9999                                        ]
Please enter the password:

password
Welcome to the back-door server
Enter your commands:

help
Supported commands are:
 pwd, ls, ls, rm, cat, logout, off, cp, mv, net, snap, diff, 1more
```

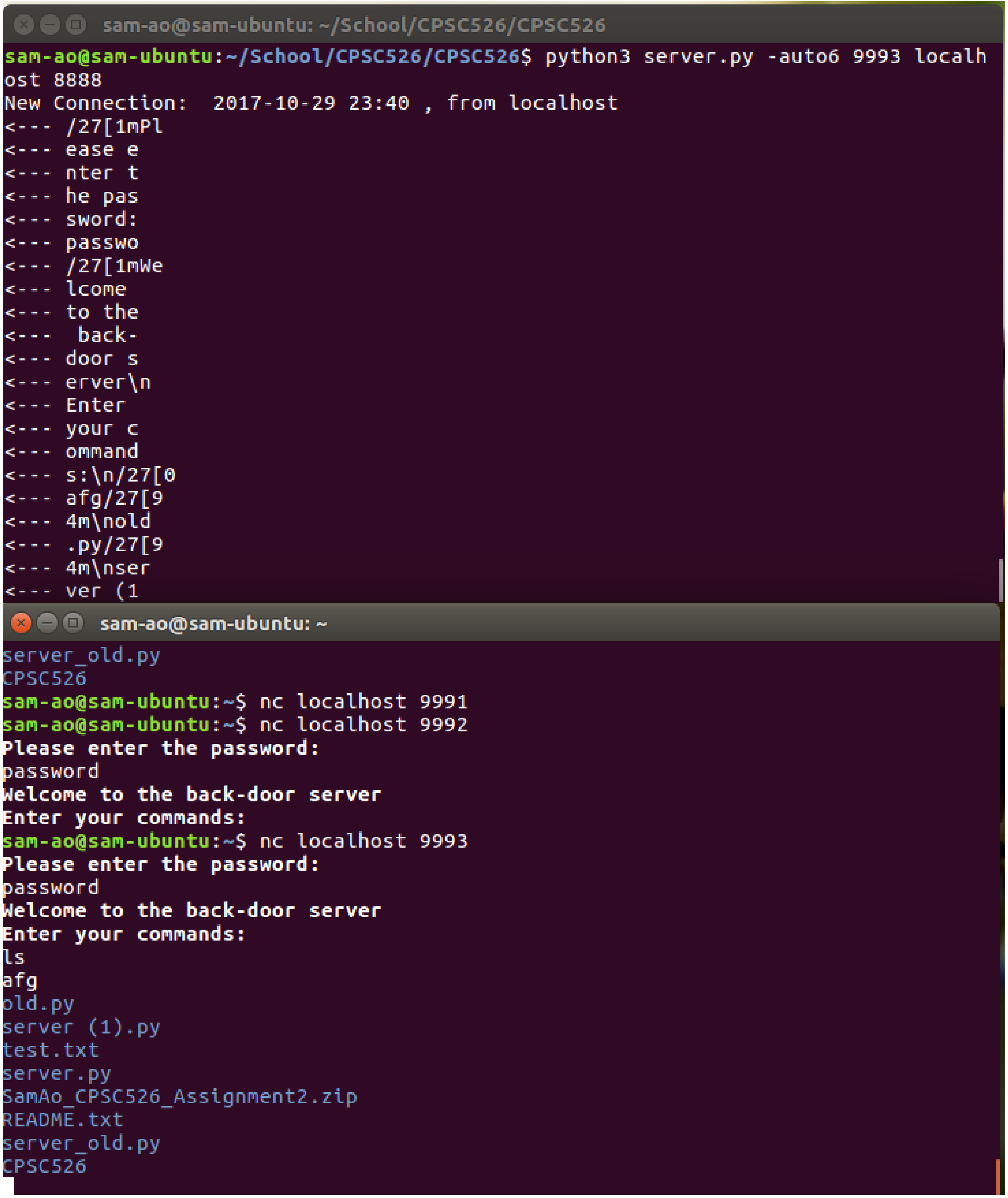
-Strip: Port-forwarding server and client view



```
    elif lock.acquire(block, timeout):
KeyboardInterrupt
sam-ao@sam-ubuntu:~/School/CPSC526/CPSC526$ python3 server.py -strip 9994 localh
ost 8888
Traceback (most recent call last):
  File "server.py", line 391, in <module>
    server = socketserver.ThreadingTCPServer((HOST, srcPort), MyTCPHandler)
  File "/usr/lib/python3.5/socketserver.py", line 440, in __init__
    self.server_bind()
  File "/usr/lib/python3.5/socketserver.py", line 454, in server_bind
    self.socket.bind(self.server_address)
OSError: [Errno 98] Address already in use
sam-ao@sam-ubuntu:~/School/CPSC526/CPSC526$ ^C
sam-ao@sam-ubuntu:~/School/CPSC526/CPSC526$ python3 server.py -strip 9991 localh
ost 8888
New Connection:  2017-10-29 23:47 , from localhost
<--- .[1mPlease enter the password:
<--- .[0m
<--- password
<---
<--- .[1mWelcome to the back-door server
<--- Enter your commands:
<--- .[0m
```

```
afg
old.py
server (1).py
test.txt
server.py
SamAo_CPSC526_Assignment2.zip
README.txt
server_old.py
CPSC526
sam-ao@sam-ubuntu:~$ nc localhost 9993
Please enter the password:
sam-ao@sam-ubuntu:~$ nc localhost 9994
Please enter the password:
sam-ao@sam-ubuntu:~$ nc localhost 9995
Please enter the password:
password
Welcome to the back-door server
Enter your commands:
sam-ao@sam-ubuntu:~$ nc localhost 9991
Please enter the password:
password
Welcome to the back-door server
Enter your commands:
```

-AutoN: Port-forwarding server and client view



```
sam-ao@sam-ubuntu:~/School/CPSC526/CPSC526$ python3 server.py -auto6 9993 localh
ost 8888
New Connection:  2017-10-29 23:40 , from localhost
<--- /27[1mPl
<--- ease e
<--- nter t
<--- he pas
<--- sword:
<--- passwo
<--- /27[1mWe
<--- lcome
<--- to the
<---  back-
<--- door s
<--- erver\n
<--- Enter
<--- your c
<--- ommand
<--- s:\n/27[0
<--- afg/27[9
<--- 4m\nold
<--- .py/27[9
<--- 4m\nser
<--- ver (1
```

```
server_old.py
CPSC526
sam-ao@sam-ubuntu:~$ nc localhost 9991
sam-ao@sam-ubuntu:~$ nc localhost 9992
Please enter the password:
password
Welcome to the back-door server
Enter your commands:
sam-ao@sam-ubuntu:~$ nc localhost 9993
Please enter the password:
password
Welcome to the back-door server
Enter your commands:
ls
afg
old.py
server (1).py
test.txt
server.py
SamAo_CPSC526_Assignment2.zip
README.txt
server_old.py
CPSC526
```