

CPSC 526 Assignment #3

Steven Leong 10129668 T01
Josh Quines 10138118 T03

How to run: python3 proxy.py [logOptions] [replaceOptions] srcPort server destPort

Options Usage

[logOptions]: -raw, -strip, -hex, -auto<N> where N is an int
[replaceOptions]: -replace <target> <targetReplacement>

Supported Logging Options:

- raw: Raw output
- strip: Replace unprintable characters with "."
- hex: Hexdump
- autoN: Output in N-sized chunks

Sample Outputs:

-raw

```
[Stevens-MBP:CPSC_526_A3 Steven$ python3.6 proxy.py -raw 1231 localhost 1254
Port logger running: srcPort=1231 host=localhost dstPort=1254
New Connection: Sun Oct 29 23:12:40, from 127.0.0.1
<---- What's the password?
<---- p4$$w0rD
<---- Access Granted.
<---- off
<---- Terminating the backdoor
<---- No data provided. Connection closed.
```

```
[Stevens-MBP:~ Steven$ nc localhost 1231
What's the password?
p4$$w0rD
Access Granted.
off
Terminating the backdoor
Stevens-MBP:~ Steven$ ]
```

```
[Stevens-MacBook-Pro:CPSC_526_Asn2 Steven$ python3.6 A2.py 1254
Listening to PORT: 1254
127.0.0.1 is now connected
Password entered: p4$$w0rD
Correct password!
127.0.0.1 wrote: off
Backdoor has been terminated by the 127.0.0.1
Stevens-MacBook-Pro:CPSC_526_Asn2 Steven$ ]
```

-strip

The image shows three terminal windows side-by-side. The top window is titled "Steven — bash — 146x24" and contains a session where a user connects to port 1231 on localhost. The password is "p4\$\$w0rD". The user performs a "pwd", sees they are in "/Users/Steven/Documents/SchoolStuff/UofC/FALL2017/CPSC526/A2/CPSC_526_Asn2 A3 non printable:", and then types "off" to terminate the backdoor. The middle window is titled "CPSC_526_A3 — Python proxy.py -strip 1231 localhost 1254 — 137x31" and shows the proxy server configuration. It logs a connection from "127.0.0.1" at Sun Oct 29 23:13:54. The bottom window is titled "CPSC_526_Asn2 — bash — 65x24" and shows the user on the attacking machine connecting to the proxy at port 1254. The password "p4\$\$w0rD" is entered, and the user runs "python3.6 A2.py 1254". The backdoor terminates, and the message "Backdoor has been terminated by the 127.0.0.1" is displayed.

```
Stevens-MBP:~ Steven$ nc localhost 1231
What's the password?
p4$$w0rD
Access Granted.
pwd
Current working directory is: /Users/Steven/Documents/SchoolStuff/UofC/FALL2017/CPSC526/A2/CPSC_526_Asn2 A3 non printable:
[
off
Terminating the backdoor
Stevens-MBP:~ Stevens$
```

```
File "/Library/Frameworks/Python.framework/Versions/3.6/lib/python3.6/socket.py", line 205, in accept
    fd, addr = self._accept()
KeyboardInterrupt
Stevens-MBP:CPSC_526_A3 Stevens$ clear
Stevens-MBP:CPSC_526_A3 Stevens$ python3.6 proxy.py -strip 1231 localhost 1254
Port logger running: srcPort=1231 host=localhost dstPort=1254
New Connection: Sun Oct 29 23:13:54, from 127.0.0.1
<---- What's the password?
<---- p4$$w0rD
<---- Access Granted.
<---- 
<---- pwd
<---- Current working directory is: /Users/Steven/Documents/SchoolStuff/UofC/FALL2017/CPSC526/A2/CPSC_526_Asn2 A3 non printable: .
<---- 
<---- off
<---- 
<---- Terminating the backdoor
<---- 
No data provided. Connection closed.
```

```
[Stevens-MBP:~ Steven$ nc localhost 1254
Listening to PORT: 1254
127.0.0.1 is now connected
Password entered: p4$$w0rD
Correct password used
127.0.0.1 wrote: off
127.0.0.1 wrote: off
Backdoor has been terminated by the 127.0.0.1
Stevens-MacBook-Pro:CPSC_526_Asn2 Stevens$ ]
```

-hex

The image shows three terminal windows side-by-side. The top window is titled "Steven — bash — 92x24" and contains a session where a user connects to port 1231 on localhost. The password is "p4\$\$w0rD". The user performs a "pwd", sees they are in "/Users/Steven/Documents/SchoolStuff/UofC/FALL2017/CPSC526/A2/CPSC_526_Asn2 A3 non printable:", and then types "off" to terminate the backdoor. The middle window is titled "CPSC_526_A3 — Python proxy.py -hex 1231 localhost 1254 — 109x31" and shows the proxy server configuration. It logs a connection from "127.0.0.1" at Sun Oct 29 23:16:01. The bottom window is titled "CPSC_526_Asn2 — bash — 88x24" and shows the user on the attacking machine connecting to the proxy at port 1254. The password "p4\$\$w0rD" is entered, and the user runs "python3.6 A2.py 1254". The backdoor terminates, and the message "Backdoor has been terminated by the 127.0.0.1" is displayed.

```
Stevens-MBP:~ Steven$ nc localhost 1231
What's the password?
p4$$w0rD
Access Granted.
off
Terminating the backdoor
Stevens-MBP:~ Stevens$
```

```
[Stevens-MBP:~ Steven$ nc localhost 1254
Listening to PORT: 1254
127.0.0.1 is now connected
Password entered: p4$$w0rD
Correct password used
127.0.0.1 wrote: off
127.0.0.1 wrote: off
Backdoor has been terminated by the 127.0.0.1
Stevens-MacBook-Pro:CPSC_526_Asn2 Stevens$ ]
```

```
[Stevens-MBP:~ Steven$ nc localhost 1254
Listening to PORT: 1254
127.0.0.1 is now connected
Password entered: p4$$w0rD
Correct password used
127.0.0.1 wrote: off
127.0.0.1 wrote: off
Backdoor has been terminated by the 127.0.0.1
Stevens-MacBook-Pro:CPSC_526_Asn2 Stevens$ ]
```

-autoN

The image shows two terminal windows side-by-side. The left window is titled 'CPSC_526_A3 — Python proxy.py -auto3 1231 localhost 1254 — 109x31' and the right window is titled 'Steven — bash — 92x24'. Both windows show a terminal session where a user is connecting to a backdoor on port 1231. The user enters the password 'p4\$\$w0rD' and is granted access. The current working directory is '/Users/Steven/Documents/SchoolStuff/UofC/FALL2017/CPSC526/A2/CPSC_526_Asn2_A3 non printable'. The user then types 'off' to terminate the session.

```
[Stevens-MBP:CPSC_526_A3 Steven$ nc localhost 1231
[Stevens-MBP: Steven$ nc localhost 1231
[Stevens-MBP: Steven$ nc localhost 1231
What's the password?
p4$$w0rD
Access Granted.
pwd
Current working directory is: /Users/Steven/Documents/SchoolStuff/UofC/FALL2017/CPSC526/A2/CPSC_526_Asn2_A3 non printable:
off
Terminating the backdoor
Stevens-MBP:~ Steven$ ]
```

```
[Stevens-MacBook-Pro:CPSC_526_Asn2 Steven$ python3.6 A2.py 1254
Listening to PORT: 1254
127.0.0.1 is now connected
Password entered: p4$$w0rD
Correct password used
127.0.0.1 wrote: pwd
127.0.0.1 wrote: off
Backdoor has been terminated by the 127.0.0.1
Stevens-MacBook-Pro:CPSC_526_Asn2 Steven$ ]
```

-replace

The image shows two terminal windows side-by-side. The left window is titled 'CPSC_526_A3 — Python proxy.py -raw -replace random newtext 1231 localhost 1254 — 109x31' and the right window is titled 'Steven — bash — 92x24'. Both windows show a terminal session where a user is connecting to a backdoor on port 1231. The user enters the password 'p4\$\$w0rD' and is granted access. The user then runs the command 'ls' to list files in the directory, which includes 'A2.py', 'README.txt', 'StevenlongA2', 'StevenlongA2.zip', 'newtext.old', 'newtext.rf', 'newtext.txt', and 'tester'. The user then types 'off' to terminate the session.

```
[Stevens-MBP:CPSC_526_A3 Steven$ nc localhost 1231
[Stevens-MBP: Steven$ nc localhost 1231
[Stevens-MBP: Steven$ nc localhost 1231
What's the password?
p4$$w0rD
Access Granted.
ls
A2.py
README.txt
StevenlongA2
StevenlongA2.zip
newtext.old
newtext.rf
newtext.txt
tester

off
Terminating the backdoor
Stevens-MBP:~ Steven$ ]
```

```
[Stevens-MacBook-Pro:CPSC_526_Asn2 Steven$ python3.6 A2.py 1254
Listening to PORT: 1254
127.0.0.1 is now connected
Password entered: p4$$w0rD
Correct password used
127.0.0.1 wrote: ls
127.0.0.1 wrote: off
Backdoor has been terminated by the 127.0.0.1
Stevens-MacBook-Pro:CPSC_526_Asn2 Steven$ ]
```