CPSC 526 - Assignment 1

Due date: January 29, 2017 @ 23:59.
Weight: 10% of your final grade.
Group work allowed, max. group size of 2.

In this assignment you are going to implement a simple backdoor program. You can write your program in C, C++ or Python. Your backdoor must be able to run on the Linux machines in the computer labs.

When your backdoor program starts, it will simply listen on some port for a client to connect. When the client connects, it should perform some very simple hand-shake mechanism, e.g. by accepting a hard-coded password. After the handshake is successfully finished, the server will start accepting commands from the client, execute them and return results. When a client disconnects, the backdoor resumes waiting for a new connection. If the handshake is unsuccessful, i.e. the first command sent is not correct, the backdoor will either drop the connection, or simply do nothing from then on.

Your backdoor should be usable by connecting to it using netcat. That means you do not need to write a client program for this assignment. Also, your backdoor program only needs to service one client at a time. There is no need to support multiple simultaneous clients.

At minimum, your backdoor must be able to understand the following commands:

Command	Description
`pwd`	returns current working directory
`cd <dir>`	changes current working directory to <dir>
`ls`	lists the contents of the current working directory
`cat <file>`	returns contents of the file
`help`	prints a list of commands
`off`	terminates the backdoor program

On top of the required commands, you must implement at least two additional commands of your own choice. You can be creative with these. Here are some suggestions:

Command	Description
`who`	list user[s] currently logged in
`net`	show current networking configuration
`ps`	show currently running processes
`nmap <params>`	run nmap with parameters <params>
`ext <program> <params>`	run program <program> with parameters <params>

Group work:

Although this is a very simple assignment, and it was designed to be easily completed by a single person, you are allowed to work on it with another student (max. group size is 2). Just beware that during the demo you will be asked to demonstrate your familiarity with all of the code. So if you do decide to group up, both of you should understand the code 100%.

Demo [90/100 points]

You are required to demo your assignments individually. During the demo you will be asked to run the backdoor program on one computer, and access the backdoor from another computer. Then you will be asked to demonstrate the functionality of your backdoor. You might be asked to adjust some functionality of the backdoor program to illustrate you are familiar with the internals of the implementation. The time for your demo will be arranged by your TAs.

Submissions [10/100 points]

Submit your code via D2L. If you decide to work in a group, each group member needs to submit the assignment. With your code you should submit a document (text or pdf) that includes: your name, ID and tutorial section, as well as the name of your partner (if applicable). The document should also include brief description of the functionality of your backdoor:

- how to run it;
- how to connect to it, including handshake details;
- supported commands.

Sample session:

```
$ nc 136.159.5.122 9312
pass p@ssw0rD
  welcome boss
help
  ls    ls cwd
  cd    change cwd
  pwd   print cwd
  cat   cat a file
  off   kill me
  ps    print process table
  net   ifconfig
cd /usr
  OK
ls
  drwxr-xr-x.  3 root root     4096 Apr 19  2016 abrt
  -rw-r--r--.  1 root root       18 Aug 17  2015 adjtime
  -rw-r--r--.  1 root root     1518 Feb 23  2015 aliases
  -rw-r-----.  1 root smmsp   12288 Apr 19  2016 aliases.db
  drwxr-xr-x.  2 root root     4096 Aug 17  2015 alsa
  …
cat passwd
```

```
  root:x:0:0:Mr. Rooter Fedora Workstation,,,:/root:/usr/bin/tcsh
  bin:x:1:1:bin:/bin:/sbin/nologin
  daemon:x:2:2:daemon:/sbin:/sbin/nologin
  adm:x:3:4:adm:/var/adm:/sbin/nologin
  lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
off
  I hate you.
```

General information about all assignments:

1. **Due time:** All assignments are due at **23:59** on the due date listed on the assignment. Late assignments or components of assignments will not be accepted for marking without approval for an extension beforehand. What you have submitted in D2L as of the due date is what will be marked.
2. **Extensions** may be granted for reasonable cases, but only by the course instructor, and only with the receipt of the appropriate documentation (e.g., a doctor's note). Typical examples of reasonable cases for an extension include: illness or a death in the family. Cases where extensions will not be granted include situations that are typical of student life, such as having multiple due dates, work commitments, etc. Forgetting to hand in your assignment on time is not a valid reason for getting an extension.
3. After you submit your work to D2L, make sure that you check the content of your submission. It's your responsibility to do this, so make sure that your submit your assignment with enough time before it is due so that you can double-check your upload, and possibly re-upload the assignment.
4. All assignments should include contact information, including full name, student ID and tutorial section, at the very top of each file submitted.
5. Although group work is allowed, you are not allowed to copy the work of others. For further information on plagiarism, cheating and other academic misconduct, check the information at this link: http://www.ucalgary.ca/pubs/calendar/current/k-5.html.
6. You can and should submit many times before the due date. D2L will simply overwrite previous submissions with newer ones. It's better to submit incomplete work for a chance of getting partial marks, than not to submit anything.
7. Only one file can be submitted per assignment. If you need to submit multiple files, you can put them into a single container. Supported container types are TAR or gzipped TAR. No other formats will be accepted.
8. Assignments will be marked by your TAs. If you have questions about assignment marking, contact your TA first. If you still have question after you have talked to your TA then you can contact your instructor.