Objective

Finish the rootkit.

Assignment

- Add the missing features to the rootkit.

Commander Program

- The commander presents a menu that must include at least:
    - Disconnect from the victim
    - Uninstall from the victim
    - Start keylogger on the victim
    - Stop keylogger on the victim
    - Transfer key log file from the victim
    - Transfer a file to the victim
    - Transfer a file from the victim
    - Watch a file on the victim
    - Watch a directory on the victim
    - Run a program on victim
- The commander must port knock on the victim to initiate a session.
- Once a session is initiated, it continues until the commander selects the Disconnect menu item.
- All communication for the session must be done via covert channels.
- All communication has to be encrypted.
- When a program is run on the victim, the output appears on the commander.

Victim Program

- The victim program must implement all of the features listed in the commander.

Report

- Create a report detailing your rootkit.

Constraints

- You can use any language(s) you want.
- **All documents must be in PDF form**.

Submission

Use the following directory structure (omit directories that are not needed):

Directory	Purpose
source	Any source code files (if applicable to the assignment)
report	Report files in **.pdf** format
video	Video(s) demonstration of your working project (if applicable to the assignment)
testing	Any items used for testing (e.g. scripts, cover images, payloads) (if applicable to the assignment)
pcap	pcap files (if applicable to the assignment)

You must hand in a pax.Z file to the assignment submission folder on Learning Hub (https://learn.bcit.ca).

You can hand in as many versions as you like. The last submission, based on the timestamp, will be the one to be marked. **Replace # with the actual version number of your assignment (e.g. 1, 2, 3, etc.).**

```
pax -w source/ report/ video/ testing/ pcap/ -f project-v#.pax
compress -f project-v#.pax
```

Hand in the resulting project-v#.pax.Z file.

Note: Failure to follow the submission requirements may result in a loss of marks, up to 100%.

Demo Requirements

- The demo videos should cover each one of your test cases.
- During the test, you will capture network traffic related to the test on both machines and then submit the pcap files as specified above.

Evaluation

Topic	Value
Design	30

Testing	50
Report	20
Total	**100**

- You will demo your rootkit in the final class (the week before the exam).