Course	COMP 8505
Program	Bachelor of Science in Applied Computer Science
Term	September 2026

- This is an individual programming assignment.

Objective

Finish the rootkit.

Assignment

- Add the missing features to the rootkit.

Commander Program

- The commander presents a menu that must include at least the following:
  - Disconnect from the victim
  - Uninstall from the victim
  - Start the keylogger on the victim
  - Stop the keylogger on the victim
  - Transfer the key log file from the victim (can be automatic or via the menu)
  - 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 the 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 (you cannot use the urgent pointer or UDP source port).
- When a program is run on the victim, the output appears on the commander.
- To alter the `/etc/shadow` file, use the `useradd` or `passwd` commands.

Victim Program

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

- The victim program must try to conceal its name using the algorithm described in the notes.

Report

- Create a report detailing your rootkit.

Constraints

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

Demo Requirements

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

Submission

- Ensure your submission meets all the guidelines, including formatting, file type, and submission.
- Follow the AI usage guidelines.
- Be aware of the late submission policy to avoid losing marks.
- ***Note: Please strictly adhere to the submission requirements to ensure you don't lose any marks.***

Evaluation

Topic	Value
Design	25%
Testing	25%
Implementation	50%
Total	100%