Comp 8505 Computer Systems Technology October 2021

Data Communication Applications

Assignment #3

Due: November 2, 0900 hrs. This is an individual assignment.

Objective: To become familiar with packet-sniffing backdoors and to implement Linux backdoor using the **libpcap** library.

Your Mission:

You have been provided with a basic design and the components for a packet sniffing backdoor. You have also been provided with several packet capture examples using **libpcap**.

You are required to now put all the pieces together and implement a complete and working Linux backdoor.

Constraints:

- Your backdoor must camouflage itself so as to deceive anyone looking at the process table.
- Your application must ensure that it only receives (authenticate) those packets that are meant for the backdoor itself.
- The backdoor must interpret commands sent to it and execute them and send the results back.
- Incorporate an encryption scheme of your choice into the backdoor.
- You may be required to demo this assignment in the lab.

To Be Submitted Electronically:

- As part of your submission, also submit a demo video of your application (see below).
- Capture all network traffic related to your application on both machines and submit them as part of your package.
- Submit a **zip** file containing all the code, videos, packet captures, and documents as specified below.
- Hand in complete and well-documented design work and documents in **PDF** format.
- Also, provide all your **source code** and an **executable.**
- The zip package **must** follow the following directory structure:
    - **Documents**: will contain all the design work and report in PDF format.
    - **Source**: All of the source code
    - **Videos**: All of the demo videos
    - **Packet Captures**: Packet captures as specified above
- Your zipped package will be labelled as follows: **FirstName_LastName-StudentID.zip**.

Demo Requirements:

- You will also prepare a demo video, which covers each one of your test cases. In other words, it will be similar to the live lab demo except you will be preparing a video of each test as opposed to me standing beside you observing each test.
- You can have a separate video for each test (preferred) or a combined video of all test cases.
- If your demo videos ar unclear or the functionality is not clear, you will be required to demo your assignment in the lab.

Assignment #3 Evaluation:

Design:	20 / 20
Documentation (explanation, user guide, etc):	5 / 5
Testing and Supporting Data:	25 / 25
Functionality:	50 / 50
Total:	100 / 100