**Comp 8505   Computer Systems Technology   May 2010.**

**Data Communication Applications**

**Assignment #2**

**Due**: June 8, 1800 hrs.

**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 optionally send the results back.
- Incorporate an encryption scheme of your choice into the backdoor.

**To Be Submitted (on disk):**

- Complete and well-documented design work and listings of your programs.
- Code **listings** and an **executable**
- Test results, complete with supporting data such as screen shots and traffic dumps

**Assignment #2 Evaluation:**

| | |
|---|---|
| Design: | 20 / 20 |
| Documentation (explanation, user guide, etc): | 10 / 10 |
| Testing and Supporting Data: | 25 / 25 |
| Functionality: | 45 / 45 |
| | |
| Total: | 100 / 100 |