TCP Attack Experiment

Note: This experiment is **not** required to submit but it will be certainly covered in the final exam.

P1 (SYN Flooding Attack). Follow the steps in PPT to conduct the syn flooding attack using c program.

- Briefly outline how the attack program works.
- Provide your screenshot on the failure of client to telnet the server.
- Screen shot the result $ **netstat –tna** on the server.

P2. (**Reset Attack to telnet session**) Follow the steps below to conduct reset attack to a telnet session. Still we use attacker **A**, client **C** and server **S**.

Step 1. run telnet from telnet client to telnet server

$telnet -l seed S

Step 2. Run **reset_auto.py** on attacker **A**.

Step 3. run any command on the telnet session. We can see that the telnet session is broken.

Requirement: describe the reset_auto.py how the above succeeds. Take a screenshot for the broken telnet session at **client**.

P3. In this lab, you will practise the TCP hijacking attack. We will three players:

Telnet Client **C** and telnet server **S** and attacker **A**

Follow the steps below.

Step 1. From **C**, telnet to **S**
Step 2. (on attacker **A**) start tcp server with port number **5000**
$ nc –lnvp 5000
Step 3. (On **A**) Modify and run you **hijack_auto.py**
Step **4**. (on **C**) run any command (such as ls **several** times) on telnet session.
Step 5. Confirm that your tcp server has taken over the TCP session. Taken a screenshot on your TCP server.

Requirement: Describe how the **hijack_auto.py** works and attach your screen shot in step 5.