CMPSC443 - TCP/IP Attack Lab

The learning objective of this lab is for students to gain first-hand experience on vulnerabilities, as well as on attacks against these vulnerabilities. Wise people learn from mistakes. In security education, we study mistakes that lead to software vulnerabilities. Studying mistakes from the past not only help students understand why systems are vulnerable, why a "seemly-benign" mistake can turn into a disaster, and why many security mechanisms are needed. More importantly, it also helps students learn the common patterns of vulnerabilities, so they can avoid making similar mistakes in the future. Moreover, using vulnerabilities as case studies, students can learn the principles of secure design, secure programming, and security testing.

The vulnerabilities in the TCP/IP protocols represent a special genre of vulnerabilities in protocol designs and implementations; they provide an invaluable lesson as to why security should be designed in from the beginning, rather than being added as an afterthought. Moreover, studying these vulnerabilities help students understand the challenges of network security and why many network security measures are needed.

SYN Flooding Attack

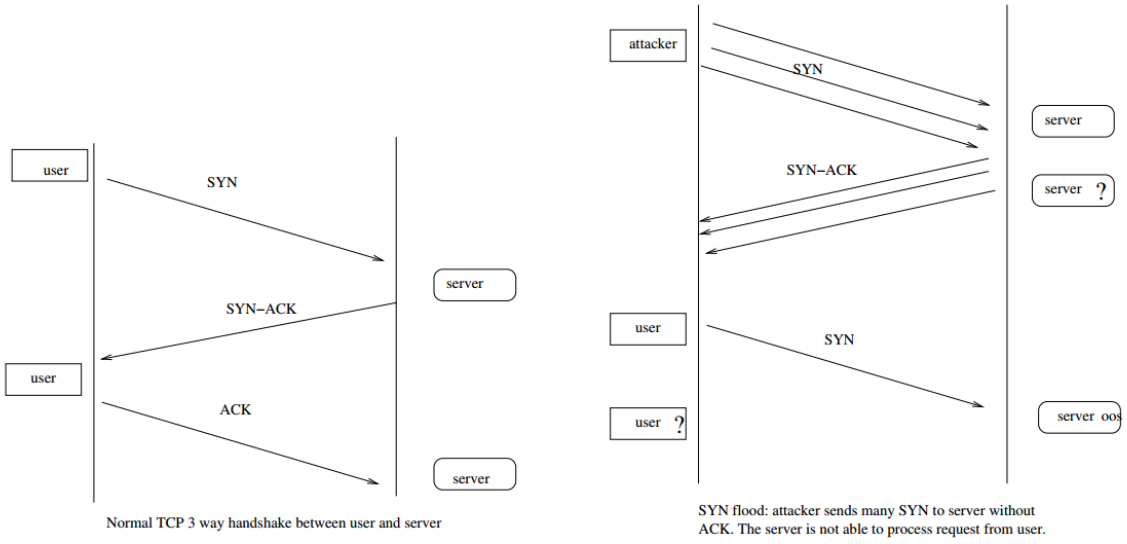

Figure 1: SYN Flood

SYN flood is a form of DoS attack in which attackers send many SYN requests to a victim's TCP port, but the attackers have no intention to finish the 3-way handshake procedure. Attackers either use spoofed IP address or do not continue the procedure. Through this attack, attackers can flood the victim's queue that is used for half-opened connections, i.e. the connections that has finished SYN, SYN-ACK, but has not yet got a final ACK back. When this queue is full, the victim cannot take any more connection. The size of the queue

has a system-wide setting. In Linux, we can check the system queue size setting using the following command:

```
# sysctl -q net.ipv4.tcp_max_syn_backlog
```

We can use command "`netstat -antp`" to check the usage of the queue, i.e., the number of half opened connection associated with a listening port. The state for such connections is SYN-RECV. If the 3-way handshake is finished, the state of the connections will be ESTABLISHED.

In this task, you need to demonstrate the SYN flooding attack.

- As we do not have a networked environment (i.e., two virtual machines that can talk to each other) in the lab, the attack will be targeting the same Kali VM. That being said, you will attack your own IP.
- Use the tutorial at http://www.binarytides.com/python-syn-flood-program-raw-sockets-linux/ to prepare for the script. The code posted on the webpage has some problems that you need fix in order to successfully launch the attack.
- Run wireshark on Kali, and then run the flooding script, it is easy to see the generated raw packet can be captured and displayed in wireshark.
- If your script manages to send the correct SYN packet, you may start flooding your own Kali machine, and observe the number of half-opened connections are kept.
- You may use "`watch netstat -antp`" to watch the real time tcp connections.
- Your experiment is successful if at a point of time the tcp connection queue is full and you cannot even access Google from the Kali web browser.

Submission

- Submit your report in word/pdf and the script you write.
- Describe your attack step by step in the report; please also include screenshots.