CISC 367 – Spring 2016

Homework Assignment – DoS Attack

1. Review the Python programs of `port_scan.py` and `dos.py`.

2. Before you mount a DoS attack, you need to find out what ports are open on the target machine. The Python program `port_scan.py` does that. You may have command like

   ```
   port_scan.py 10.0.0.8 1 200
   ```

   to scan port 1 to port 200 target host at IP address 10.0.0.8.

3. Program `dos.py` uses the Python scapy module. Scapy is a powerful tool for creating packets in any of the first four layers of the TCP/IP protocol stack and that includes the Ethernet frames that reside at Layer 2. You can ask Scapy to create a packet, set its various fields, put it on the wire, and have it capture the response packet if there is one. Finally, you can have Scapy present both the sent and the received packets to you in an easy to understand format.

4. In `dos.py`, we ask Scapy in lines (6), (7), and (8) to first create an IP header with specific source and destination IP addresses; to then create a TCP header with specific source and destination ports, and with the SYN flag set; and, finally, to concatenate the two headers for creating a legal packet at the IP Layer. Finally, in line (10) we ask Scapy to send the packet to its destination. You may have command like

   ```
   sudo ./DoS5.py 10.0.0.19 10.0.0.8 22 3
   ```

   to send 3 packets with spoofed source IP 10.0.0.19 to port 22 on destination IP 10.0.0.8.

5. Design and desmonstrate DoS attach scenarios with the Raspberry Pis you have.