CSCI 345 – Homework 3
Network Attacks: DNS spoofing, DDoS

1. DNS Spoofing:
   a. Run the following experiment: https://witestlab.poly.edu/blog/redirect-traffic-to-a-wrong-or-fake-site-with-dns-spoofing-on-a-lan/
   b. Submit a report for the last part of the lab (copy pasted here, you can also find it at the end of the webpage):
      “Using the results of your own experiment, create three diagrams similar to the one above, one for each of the scenarios:

      i. Normal DHCP and DNS resolution of the bank's hostname.
      ii. DNS spoofing attack with ARP spoofing.
      iii. DNS spoofing attack with DHCP masquerade.
      In each diagram, show the relevant details of the ARP, DNS, and DHCP messages that you observed in your experiment for that scenario. Also, Label the client, "good" server, and attacker with their (real) MAC addresses. Show broadcast packets arriving at all other hosts in the LAN (except the sender).
      For the ARP spoofing experiment, you need only show one example of each ARP (you don't have to show repeated identical ARPs).
      The diagram above shows what relevant information to include for DNS and DHCP packets. Here is a template you can use for ARP messages:
      ARP: 10.10.1.2 is at 02:60:70:39:bf:e2
      02:60:70:39:bf:e2 > 02:0f:07:a6:c6:d8
      After each diagram, include the terminal output in which you observe the packets shown in the diagram. Make sure to label which host the output comes from. Don't just dump everything you see into your report - include only the relevant parts of your output, and highlight the important details.”

2. DDoS TCP SYN flood and Slowloris:
   a. Run the SYN flood: http://mountrouidoux.people.cofc.edu/CyberPaths/IntrusionDetectionSystemLabEasy.html
   b. Submit a snort rule that detects TCP SYN flood with an explanation why it works, why it is sensitive AND specific.
   c. Using the same topology as the SYN flood experiment:
      i. Study the slowhelix code (slowloris in python). Explain what each part of the code does in detail.
      ii. Submit a snort rule that detects Slowloris with an explanation why it works, why it is sensitive AND specific.

3. Blog Entry – Analyze a recently found vulnerability

For this blog entry, I would like you to find a recent vulnerability from the CVE database (https://cve.mitre.org/) and analyze it based on what you have learned in class in layman’s terms:
a. Explain the threat model in simple terms.
b. Find the impact factor of this vulnerability in CVSS and explain it. You should explain the whole model in your own words, assume none that reads this blog knows about CVSS.
c. Write your educated opinion on why this happened: developer error, policy error, etc.