**CMPE 132 Homework #3 (Fall 2022)**

**Due: Feb. 21, 11:59 p.m. (Firm Deadline)**

We can work together with our peers, but you must write your homework yourself. Copy any information from the Internet or other resources will be 0 points. You can put citations when you refer to specific resources.

**[Q1] (13 points) Please explain the TCP SYN Flooding attack and list at least two defense methods to prevent this attack.**

**[Q2] (13 points) Please explain the UDP Flooding attack and list at least two defense methods to prevent this attack.**

**[Q3] (13 points) Please explain the HTTP Flooding attack and list at least two defense methods to prevent this attack.**

**[Q4] (13 points) What are DNS amplification attacks? Please list at least two defense methods.**

**[Q5] (13 points) Compared with the Flooding attacks, what is the difference in the Slowris attack? Please list one defense method against this Slows attack.**

**[Q6] (12 points) What are the characteristics of botnets?**

**[Q7] (13 points) What is the defense method against botnet-based attacks?**

**[Q8] (20 points) Please do Packet Sniffing and Spoofing Lab at SEED Labs.**

<https://seedsecuritylabs.org/Labs_20.04/Networking/Sniffing_Spoofing/>

**Please do Task 1.1 to Task 1.4 in the “Task Set 1: Using Scapy to Sniff and Spoof Packets.” on pages 1 – page 5.**

**[Q9] (20 points) Please do TCP Attack Lab at SEED Labs.**

<https://seedsecuritylabs.org/Labs_16.04/PDF/TCP_Attacks.pdf>

**Please do Task 1 and Task 2 only.**

**[Q10] (20 points) Please do the ARP Cache Poisoning Attack Lab at SEED Labs.**

[**https://seedsecuritylabs.org/Labs\_16.04/PDF/ARP\_Attack\_new.pdf**](https://seedsecuritylabs.org/Labs_16.04/PDF/ARP_Attack_new.pdf)

**Please do only “2 Task 1: ARP Cache Poisoning” on pages 1-2.**