**CMPE 132 Homework #2 (Spring 2023)**

**Due: March 10, 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] (10 points) Please explain the main difference between SDN and a tradition network.**

**[Q2] (20 points) Please explain each field of the header information in OpenFlow 1.0. There are 12 tuples in total in the header part.**

**[Q3] (10 points) Please explain the picture on page 24 in the Lec3-SDN and Security.pdf.**

**[Q4] (20 points) Please identify at least three vulnerabilities in SDN and explain each attack.**

**[Q5] (20 points) The class shared the network attack data and code. Here is the video for you.**

[**https://www.youtube.com/watch?v=-KgQLG7Q0s4**](https://www.youtube.com/watch?v=-KgQLG7Q0s4)

**Please show your work on how to improve accuracy by using Random Forest Algorithm.**

**[Q6] (10 points) Please list at least two benefits we use machine learning techniques for network intrusion detection.**

**[Q7] (10 points) Please list at least two benefits we use NFV.**

**[Q8] (30 points)** Please install Mininet (<http://mininet.org/>) with a SDN controller. Please conduct “Lab 3: Flooding Attacks to the SDN Data Plane” at <https://www.svcsi.org/general-6>

You can follow the instruction starting from Section 1.1. while ignoring the CloudLab setup part. Instead of CloudLab, you can use Mininet.

Reference website:

<https://courses.cs.washington.edu/courses/csep561/22sp/projects/project1/>