Student Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. What are the two types of IDS systems?(10 Points) How are they different and what are the benefits of each one? (10 points) (Total 20 points)
2. What is the issue with using an IPS? When would you use an IDS and when would you use an IPS? (20 Points)
3. What are the four things to consider when selecting an IDS or an IPS? (20 Points)
4. You network environment seems to be sluggish. And so you decided to install snort on a pc / laptop an plug it to the same switch where the firewall is plugged into. Your install was 100% correct, With everything being correct you still are not seeing any scans. What are possible causes of why your snort does show any activity? (20 points)
5. Identify in which of the directories are the following files kept for snort for windows? (20 Points)
   1. Snort.conf \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
   2. Snort.exe \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
   3. Xyz.rules \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
   4. Alert.ids \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_