T81-558: Security Deep Learning Project

Jeff Heaton

Due: 2018-04-27

Please read the following paper.

Diep, N. N. (2017). Intrusion detection using deep neural network. *Southeast Asian Journal of Sciences*, *5*(2), 111–125.

You can find a copy of this paper's PDF here: `http://sajs.ntt.edu.vn/index.php/sajs/article/download/151/103`

Once you have read the above paper, answer the following questions about it. For each question write a minimum of 2-4 sentences, but use as many as you need to answer.

1. What is an Intrusion Detection System (IDS)?
2. What data set does this paper use? Where can you obtain this data set? When was this data set released?
3. Describe the input and output layers of this neural network. Where do each of the inputs come from? What do the output neuron(s) mean?
4. Describe the hidden layers of the neural network. How many layers did the author's use? How did they determine how many hidden layers they used (do they say)?
5. What (if anything) is novel about their approach? What does this paper contribute to research?
6. How does this paper prove/substantiate their results?
7. Give me the details on their architecture? (What software did they use, what is the structure of the network, how did they train the network, did they use any regularization, was this classification, regression, or something else)

8. How was softmax used in this paper?
9. What do you like about this paper (what did they do well)?
10. What are this paper's weaknesses (it is not flawless)?