Nitin Nagavel

CPRE 431

Homework #5 (Due: Oct. 11)

Assignments will be submitted in PDF format via Canvas.

Please submit your homework online through Canvas. Late homework will not be accepted.
Important: Your submission must be in .pdf format ONLY!

1. Describe the differences between a host-based IDS and a network-based IDS. How can their advantages be combined into a single system?

   Host based can detect internal changes within a system while network based can detect unusual behavior or malicious packets being sent on the network. The advantages can be combined together to provide safer security both from a system standpoint and a network standpoint.

2. What are three benefits that can be provided by an IDS?
   Defense, Virus tracking Propagation, and clear visibility.

3. What is the difference between a false positive and a false negative in the context of an IDS?
   False positives detect safe software as potentially dangerous, while false negatives detect software that is dangerous as safe or fails to detect.

4. What is the difference between anomaly detection and signature intrusion detection?
   Signature based is used for detecting threats, while Anomaly based is used for detecting any changes in a System's software