CPRE 431

Mod 5 Homework (Due: Oct. 11)

Sean Gordon (Sgordon4)

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 comoibned into a single system?
   - Host based systems work by running an agent on a host computer in order to monitor security related information. Network based systems work by adding a separate device onto the network to look for intrusive traffic.
   - Both systems can be used at once, with an NIDS hooked up to the internet to monitor for attacks, and an agent installed on any computer on that network to monitor for attacks that make it through the NIDS.

2. What are three benefits that can be provided by an IDS?
   - IDSs provide an extra layer of defense, keeping systems and information safer from threats.
   - IDSs can provide logs of goings on within the system, providing a basis for legal action in the event of an attack.
   - IDSs can track attacks as they happen, allowing for quicker response times.

3. What is the difference between a fasle positive and a false negative in the context of an IDS?
   - False Positive: A harmless process is flagged as malicious.
   - False Negative: A malicious process is not flagged, leaving it undetected.

4. What is the difference between anomaly detection and signature intrusion detection?
   - Anomaly detection compares current behavior against previous (normal) behavior to look for unusual activity. Signature intrusion detection compares current activity against a database of known threats to look for matches. The first finds new threats, the second finds old threats.