16-124-836
Marcel Matti ZAUDER

12.2 Question 2

12.2.A What is the difference between misuse and anomaly detection in terms of accuracy and the ability to detect novel or unknown attacks? Justify.

Misuse or signature detection systems first need to be equipped with a well-defined set of attack signatures populated in their database. An anomaly detection system, on the other hand, defines a detailed and accurate profile of the normal behavior of the networks and hosts.
Therefore the misuse detection is not as suitable if it is known that many different, new and unknown attacks are prone to target the system. In this case an anomaly detection is much more suitable as it registers any misbehaviour of the system. On the other hand if an attack is made and the system still seems to work in a normal behaviour the anomaly detection is much less of a use and if that attack is a common one the misuse detection system is much more accurate in detecting these kind of attacks.