Collaborative Discussion 1 – Peer Response 1 – Aldo Madrid

Thank you Aldo for your interesting post about Anomaly Based Detection.

A major disadvantage of Anomaly Based Detection mechanisms is that they only work with a larger number of sent packets, since they only react with a statistically significant number of malicious packets (Shimeall & Spring, 2014). This can make a system vulnerable to attacks that are carried out by just one or a few information packets, as is the case with an attack such as the Ping of Death.

Another problem arises from the fact that network traffic is dependent on human behavior. Even if a certain predictability of human behavior is possible, the flexibility of humans can be reduced by a detection mechanism based on anomaly (Jyothsna et al., 2011). While the system registers and fends off simple attacks, it is susceptible to advanced attacks, which are therefore not recognized, but are of particular interest for a secure system.

Further problems can be derived from this. It can be a fine line balancing act between an inadequately and inadequately set up anomaly based detection mechanism. Because wanted functions can be exploited in order to execute unwanted applications, since the usage behavior of the unwanted application is very similar to the wanted one and is thus within the statistically significant value. On the other hand, an intended application can be mistakenly recognized as a danger.

References:

Shimeall, T. & Spring, J. (2014) Introduction to Information Security, Syngress. Available from: https://doi.org/10.1016/B978-1-59749-969-9.00012-2. [Accessed: 21.09.2021]

Jyothsna, V., Rama Prasad, V. & Munivara Prasad, K. (2011) A Review of Anomaly based Intrusion Detection Systems. International Journal of Computer Applications (0975-8887) Available from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.259.1390&rep=rep1&type=pdf [Accessed: 21.09.2021]