# IT 6823 LM 9. Intrusion Detection System

# Learning Material

**Note**: The learning material is composed of a list of web links, videos, and other materials screened and/or created by the instructor. The material is organized by student outcomes. Essential information is included in this document and students are recommended to go to the links to learn more about a specific topic.

## Overview

The module gives an overview of different intrusion detection system. There are a lot of terms and concepts. The learning material is mainly based on the following survey paper which is provided in the D2L course website as a PDF file. We refer it as The Survey Paper thereafter the remaining of the document.

Khraisat, A., Gondal, I., Vamplew, P. et al. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecur **2,** 20 (2019). <https://doi.org/10.1186/s42400-019-0038-7>

Intrusion Detection System is in Detect phase in the NITS security framework.

## Student Learning Outcomes

* **Define Intrusion Detection System and its main benefits**
* Intrusion: Intrusion can be defined as any kind of unauthorized activities
* An IDS is a software or hardware system that identifies malicious actions on computer systems in order to allow for system security to be maintained.
* Zero-day attack - An attack that exploits a previously unknown hardware, firmware, or software vulnerability. Source: <https://csrc.nist.gov/glossary/term/Zero_Day_Attack>
* **Compare and contrast SIDS and AIDS**
* What’s SIDS and AIDS
* Pros and cons of each system:

 

Source: Page 3 and table 2 of The Survey Paper

* **Compare and contrast HIDS and NIDS**
* What’s HIDS and NIDS
* Pros and cons of each system:



Source: Page 4 “Intrusion Data Sources” and Table 4 of The Survey Paper

* **Describe the techniques for the implementation AIDS**
* Three main groups: statistics-based, knowledge-based, machine learning based.
* Don’t need to know the details of each techniques. But need to what each technique is about.



Source: “Techniques for implementing AIDS” section of The Survey Paper.

* **Explain the performance metrics of IDS**

“Performance metrics of IDS” section of The Survey Paper.