INF6422E Advanced Concepts in Computer Security

Practical Work 1 – Winter 2026

Intrusion Detection System and Its Evaluation

Instructions:

- This work is to be submitted in a group of two and via Moodle only.
- The submitted report must be in pdf form and also include (.py, .ipynb) with it. You're free to build it in any format you want, however (.docx, .odt, .tex, etc.).
- The report must contain a title page including the course title, the lab title, your names and student ID numbers (Matricule).
- The report must be submitted by the 04th of February 2026 before 23h59. A penalty of 10% will be applied for each day after that date.
- There are 4 labs in total, each of 20 marks/10 weightage.

Objective:

This practical work introduces quantitative performance evaluation techniques for Intrusion Detection Systems (IDS). Students will design, evaluate, and compare classical machine learning-based IDS models using standard cybersecurity datasets. Emphasis is placed on evaluation metrics, trade-offs, and operational implications of IDS deployment in real-world environments.

Background and Introduction:

Intrusion Detection Systems (IDS) are a core component of modern cybersecurity infrastructures, designed to detect malicious activities that bypass traditional preventive mechanisms such as firewalls. Evaluating IDS performance is non-trivial due to the asymmetric cost of errors, evolving attack patterns, and operational constraints.

In this lab, you will explore how quantitative evaluation metrics influence IDS design decisions, and how different machine learning models trade off detection accuracy, false alarms, and robustness.

Key Learning Goals:

1. Understand the role of IDS within a broader cybersecurity defence strategy.
2. Apply quantitative evaluation methods to assess IDS performance.
3. Implement and compare classical machine learning models for intrusion detection.
4. Analyze trade-offs between false positives and false negatives in security contexts.

Resources:

The **CICIDS2017 dataset** is a single dataset composed of multiple CSV files, each corresponding to network traffic captured on different days and attack scenarios. The traffic was collected over five consecutive days, with Monday containing only benign traffic, and the remaining days including a mixture of benign and malicious activities.

Day	Traffic Type
Monday	Benign only
Tuesday	Benign + Brute Force
Wednesday	Benign + DoS + Heartbleed
Thursday	Benign + Web Attacks + Infiltration
Friday	Benign + Botnet + DDoS + Port Scan

For this practical work, students will construct one experimental dataset by merging traffic from Monday (benign baseline) with traffic from exactly one additional day containing attacks. This results in four possible dataset configurations, each combining normal and malicious traffic in a controlled manner.

Dataset Link: https://www.unb.ca/cic/datasets/ids-2017.html

or

https://drive.google.com/drive/folders/1nbGBRm1rsxYvdHYNUf8ovJPiELUeeCp_?usp=sharing

Group Assignment Policy

Each student group will be assigned one of the four dataset samples. The assignment of samples to groups will be coordinated in class to ensure balanced coverage of attack scenarios and to encourage comparative analysis across groups.

All groups must follow the same preprocessing, training, and evaluation methodology, enabling meaningful cross-group comparison during discussions.

1. Dataset Analysis and Preprocessing [4 Points]

1.1 Dataset Exploration

Analyze the selected IDS dataset:

- Number of samples
- Number of features
- Attack categories vs normal traffic

Deliverable:

Provide a short statistical summary and explain why dataset characteristics matter for IDS evaluation.

1.2 Dataset Preprocessing

Perform the following preprocessing steps:

- Feature normalization or standardization
- Encoding of categorical features (if applicable)
- Dataset split into:
  - Training set (70%)
  - Validation set (15%)
  - Test set (15%)

Deliverable:

Justify the chosen split strategy and explain how it helps prevent overfitting in IDS models.

2. Classical Machine Learning Models for IDS [4 Points]

2.1 Logistic Regression for Intrusion Detection

Train a Logistic Regression model for multi-class intrusion detection.

- Evaluate the model using:
  - Accuracy
  - Precision
  - Recall
  - F1-Score
  - AUC-ROC

Deliverable:

Present evaluation metrics

Interpret the confusion matrix

Discuss the impact of false positives vs false negatives in an IDS context

3. Ensemble-Based IDS and Performance Trade-offs [6 Points]

3.1 Random Forest for Intrusion Detection

Train a Random Forest classifier.
Tune at least two hyperparameters (e.g., number of trees).

Deliverable:

Performance metrics

Confusion matrix interpretation

Discussion on how ensemble methods improve IDS robustness

3.2 Feature Importance Analysis

Extract feature importance scores from the Random Forest model.
Identify the top 5 most influential features.

Deliverable:

Explain how the identified important features and dataset characteristics relate to:

Observed network behavior across normal and attack periods

Known attack scenarios and signatures described in the CICIDS2017 dataset

Anomaly detection principles, by contrasting deviations from baseline (benign) traffic

4. Comparative Performance Analysis [6 points]

4.1 Model Comparison

Summarize the results of all models in a comparison table.

- Compare the models in terms of:

- Detection accuracy
- False alarm rate
- Practical deployment feasibility

Deliverable:

Provide a cybersecurity-focused comparison, not just numerical results.

4.2 IDS Deployment Challenges

Discuss the challenges of deploying ML-based IDS in enterprise environments, including:

- Latency
- Scalability
- Adaptability to new attacks

References:

[1] Hozouri, A., Mirzaei, A. & Effatparvar, M. A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges. Discov Artif Intell 5, 314 (2025). https://doi.org/10.1007/s44163-025-00578-1
[2] Neto, E.C.P., Iqbal, S., Buffett, S. et al. Deep learning for intrusion detection in emerging technologies: a comprehensive survey and new perspectives. Artif Intell Rev 58, 340 (2025). https://doi.org/10.1007/s10462-025-11346-z
[3] https://www.unb.ca/cic/datasets/ids-2017.html