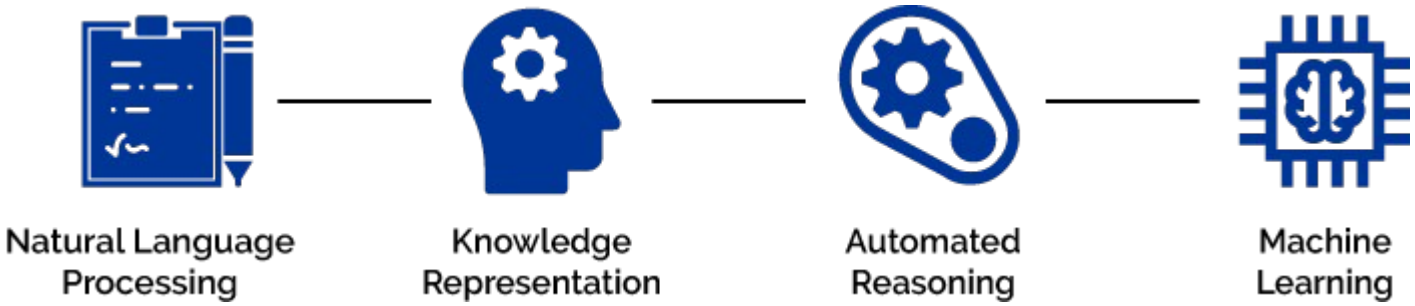
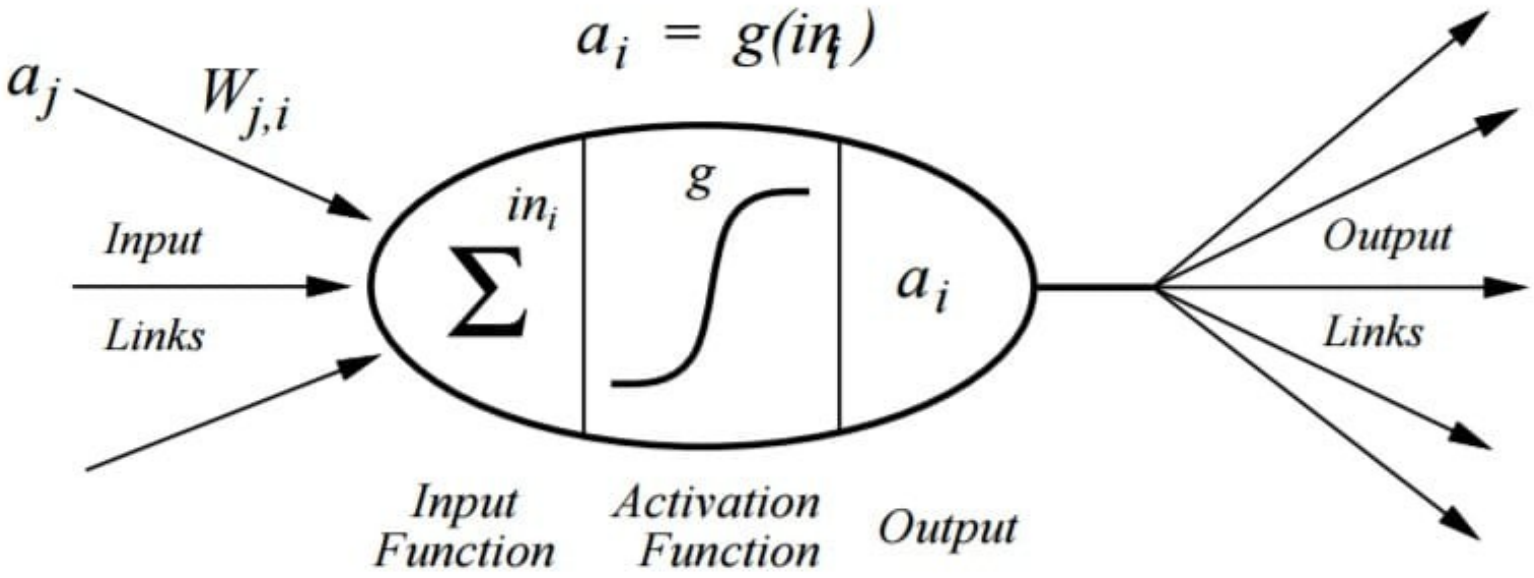
AI- based IDS

Types of AI


Natural Language Processing
Knowledge Representation
Automated Reasoning
Machine Learning

Quick review on Neural Network

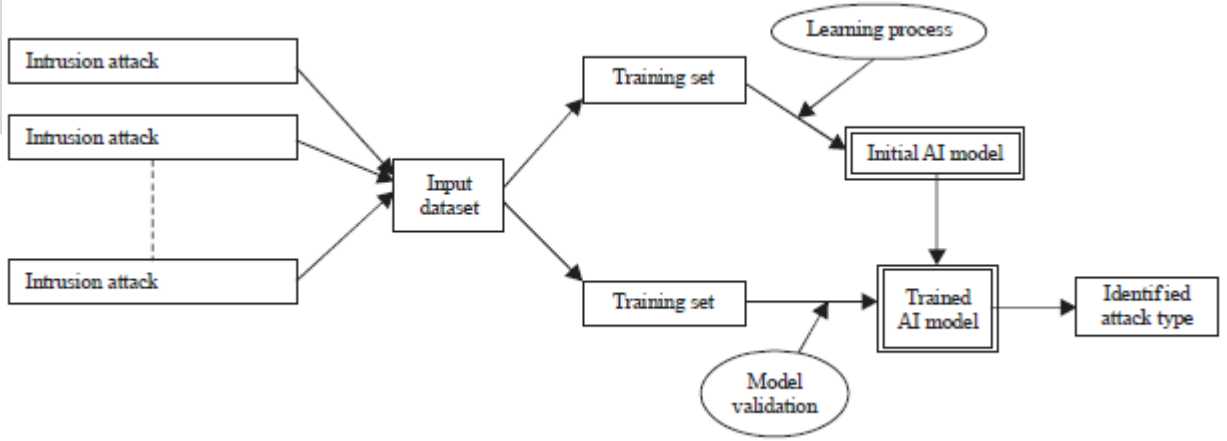


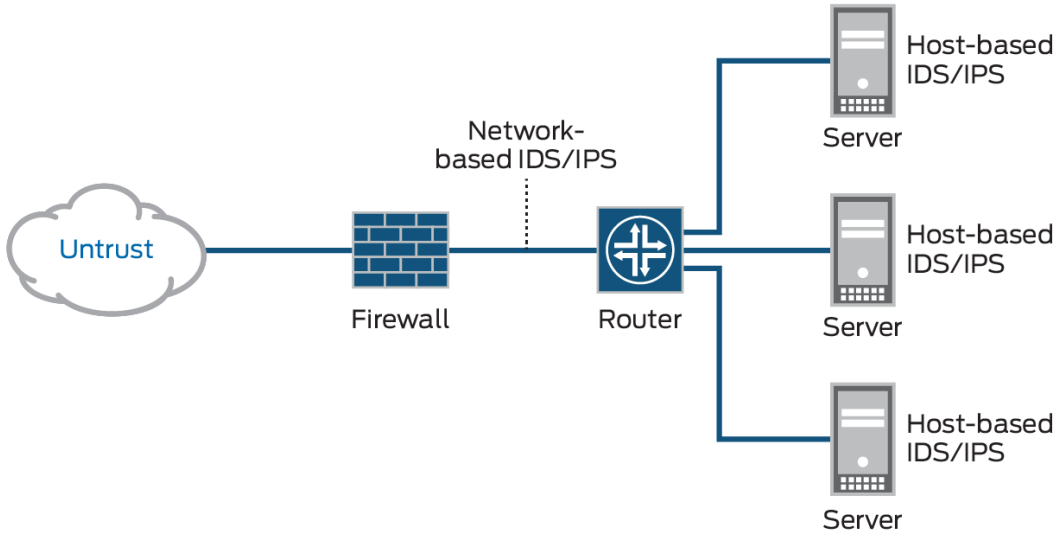
$$a_i = g(\sum_j W_{j,i} a_j)$$

Current IDS in industries

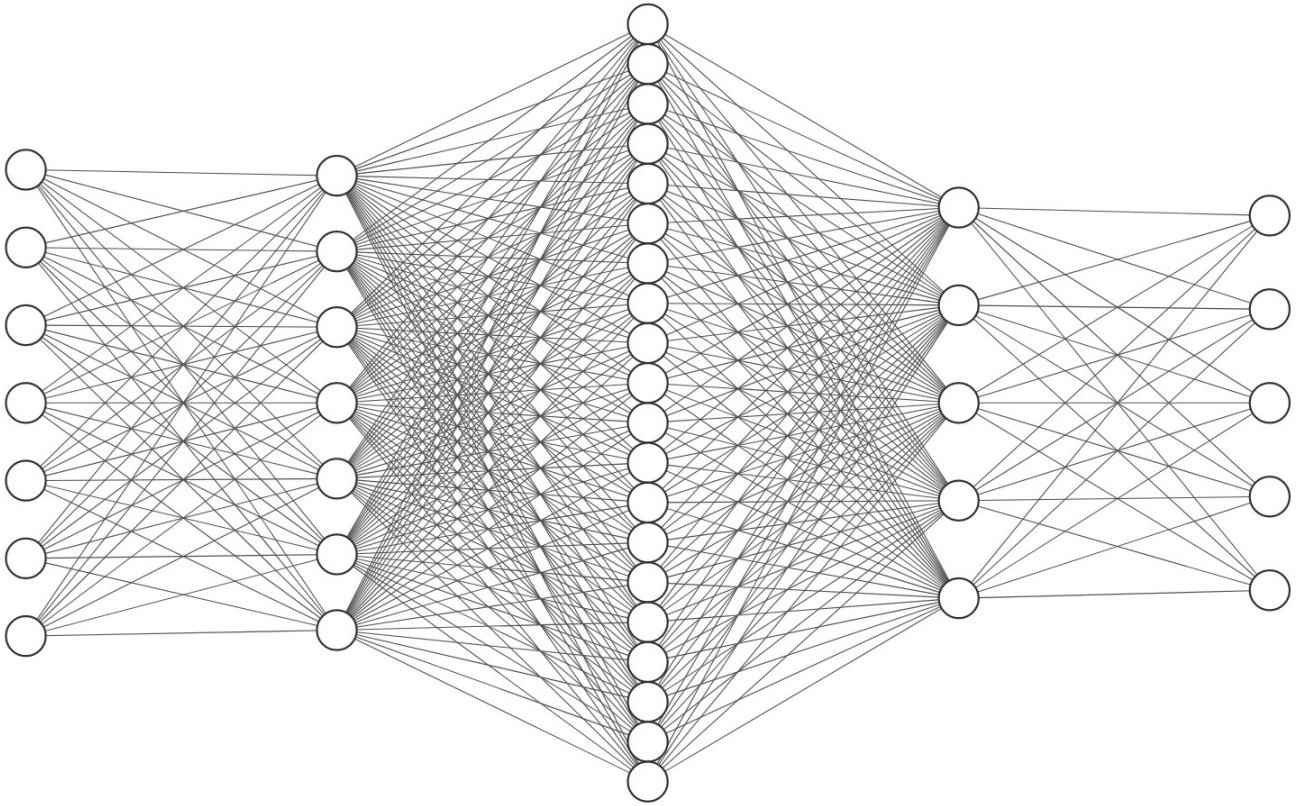
- Signature based
- Anomaly based

Compare between AI and Signature/Anomaly based IDS

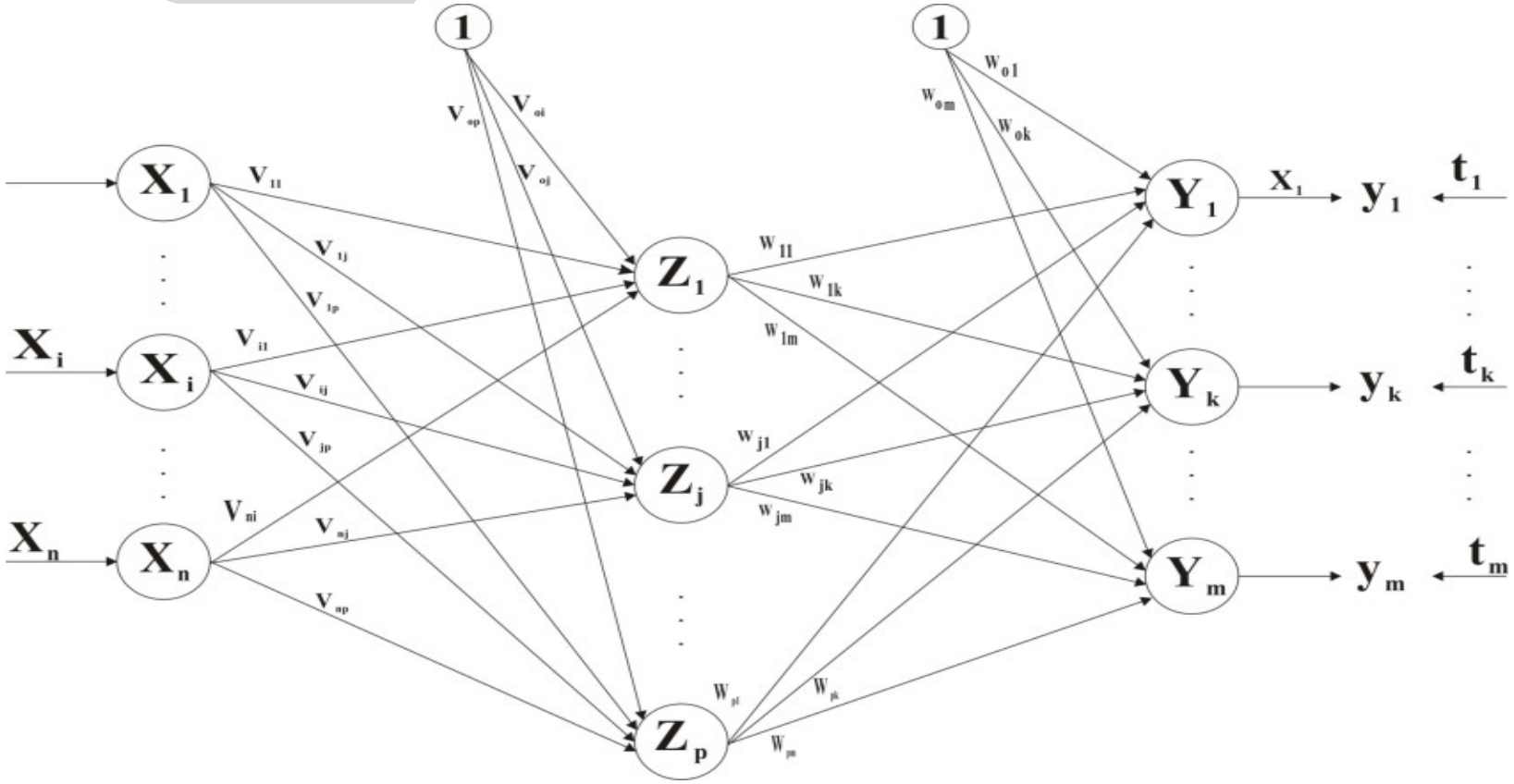




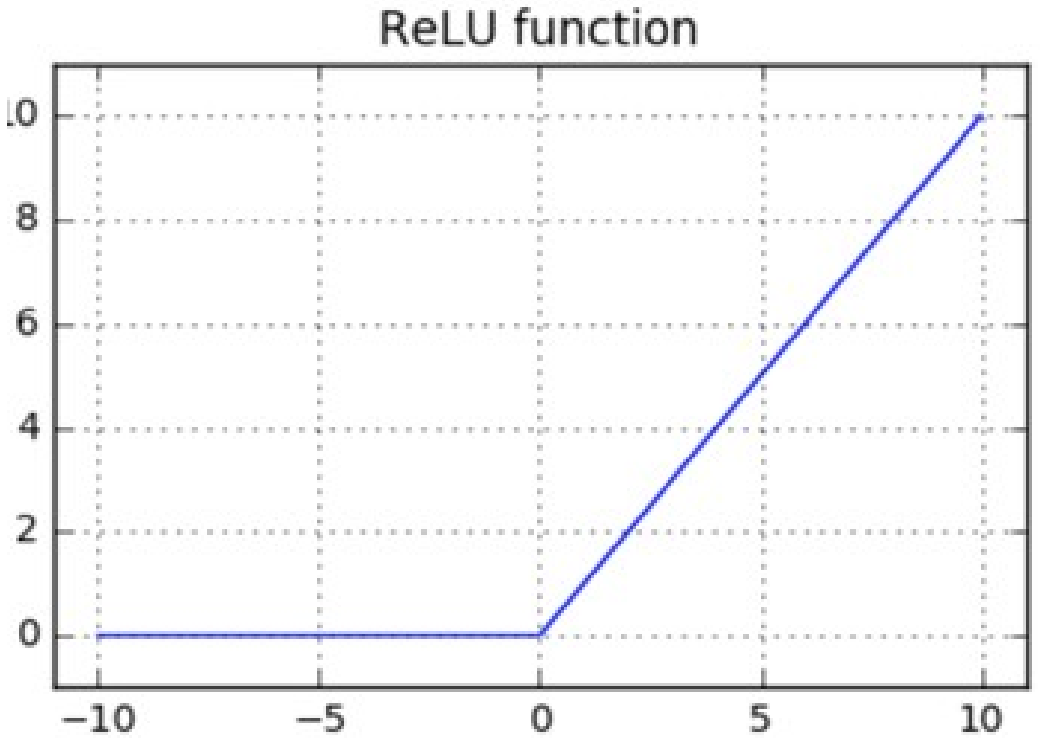
Neural Network

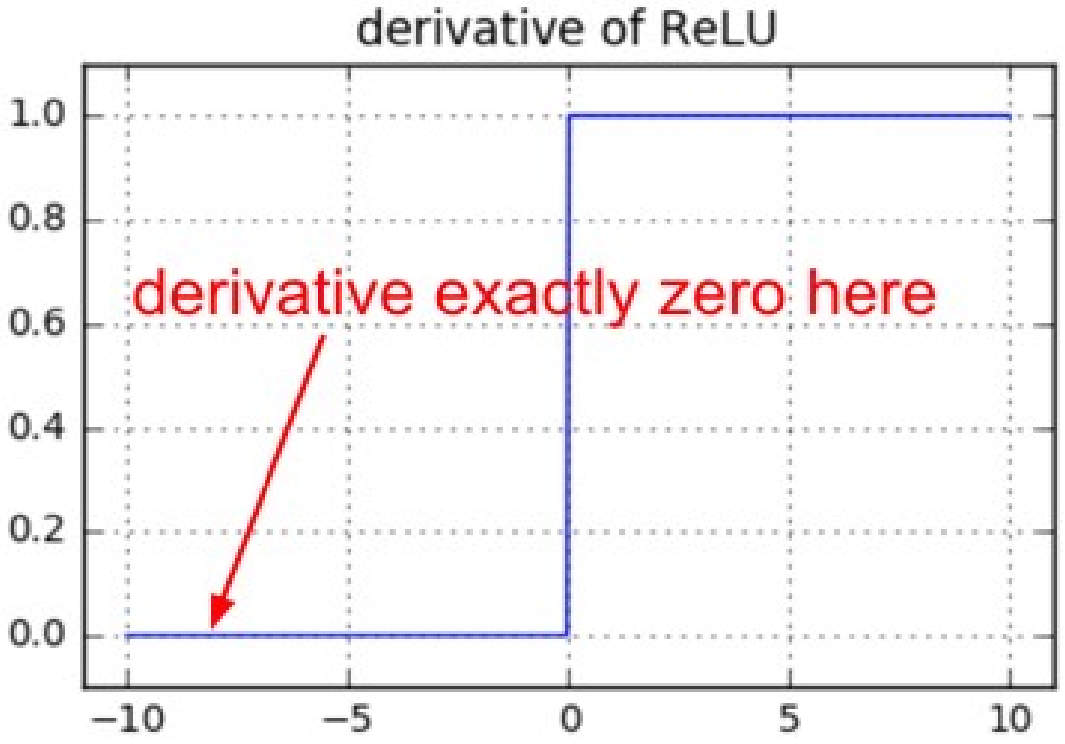


Feed Forward



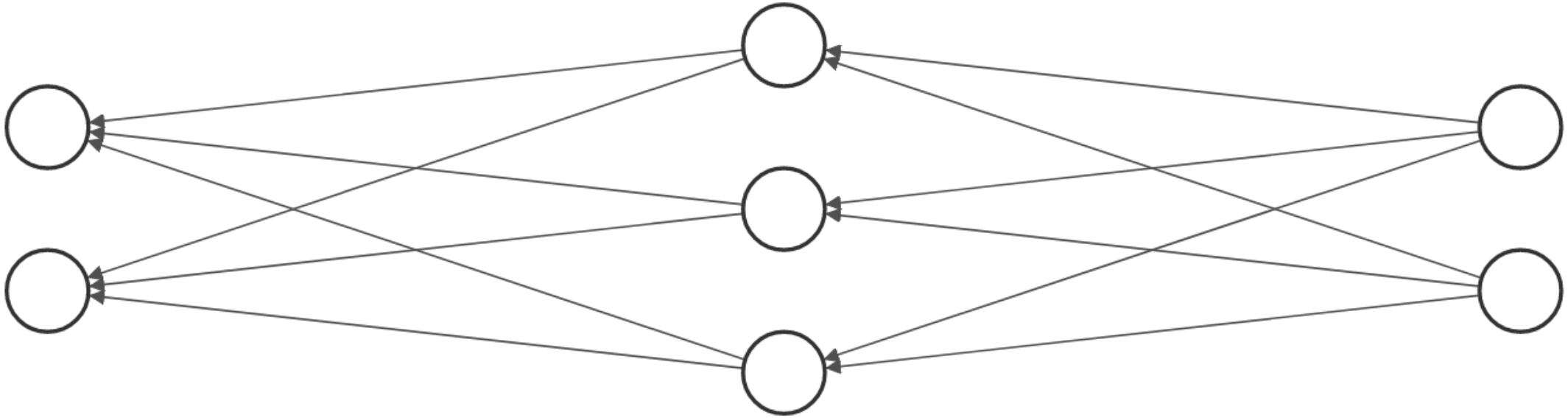
Backpropagation part 1





Backpropagation part 1

- Calclus and cost function

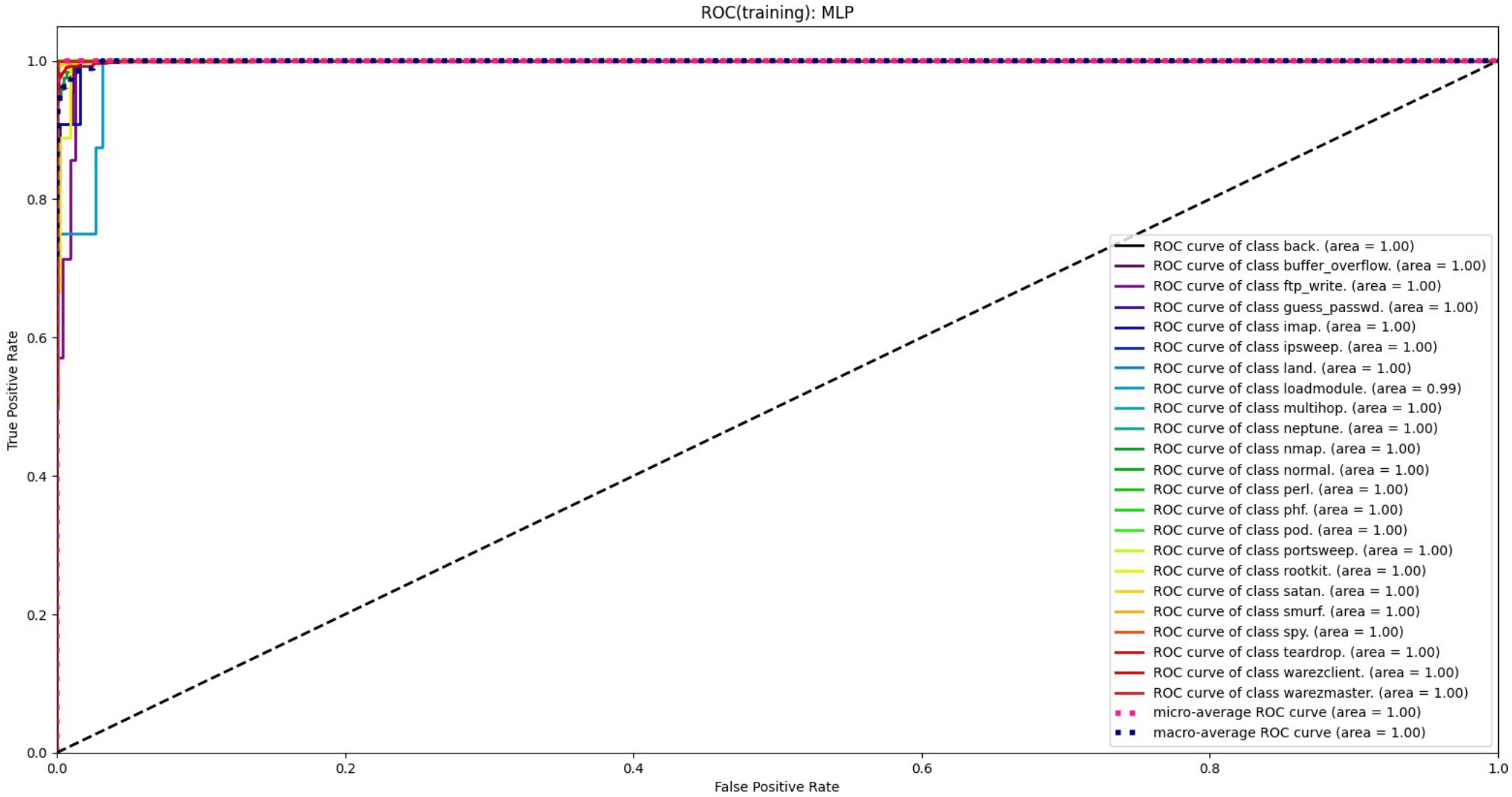


Results List

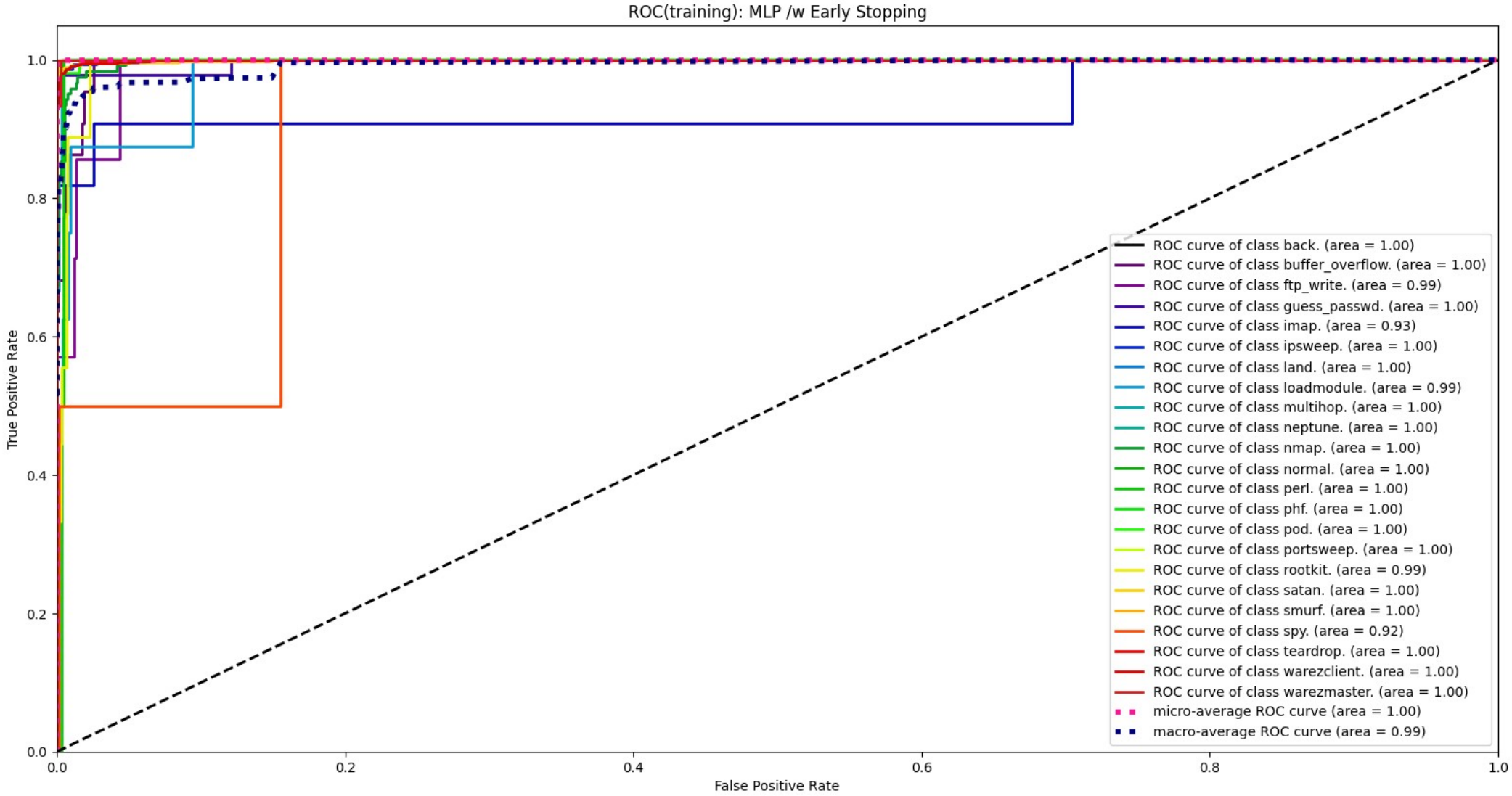
- Training
  - MLP: ROC and Precision-Recall
  - MLP /w Early Stopping: ROC and Precision-Recall
  - Random Forest: ROC and Precision-Recall

- Testing
  - MLP: ROC and Precision-Recall
  - MLP /w Early Stopping: ROC and Precision-Recall
  - Random Forest: ROC and Precision-Recall

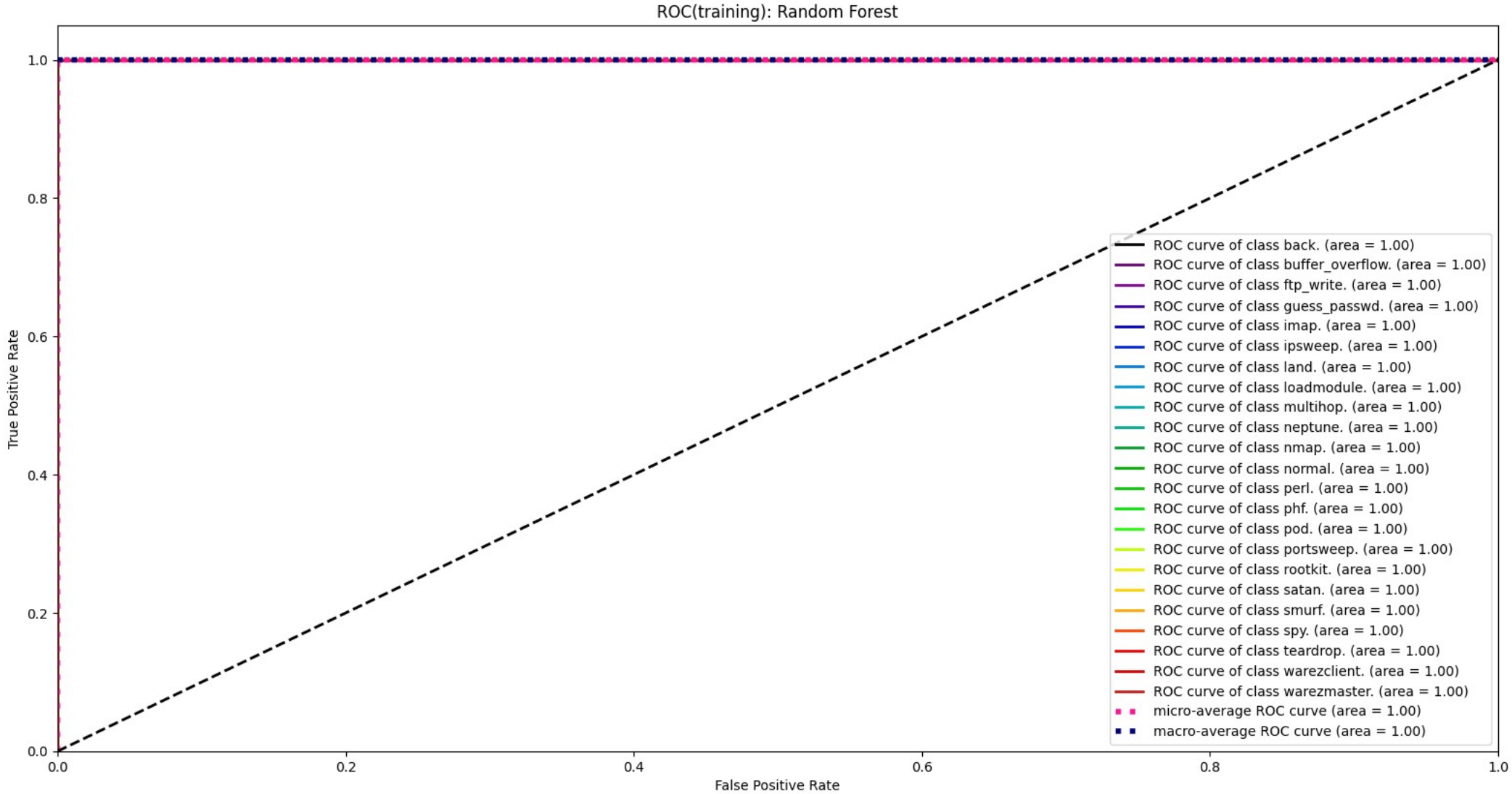
Results: MLP (Training), ROC



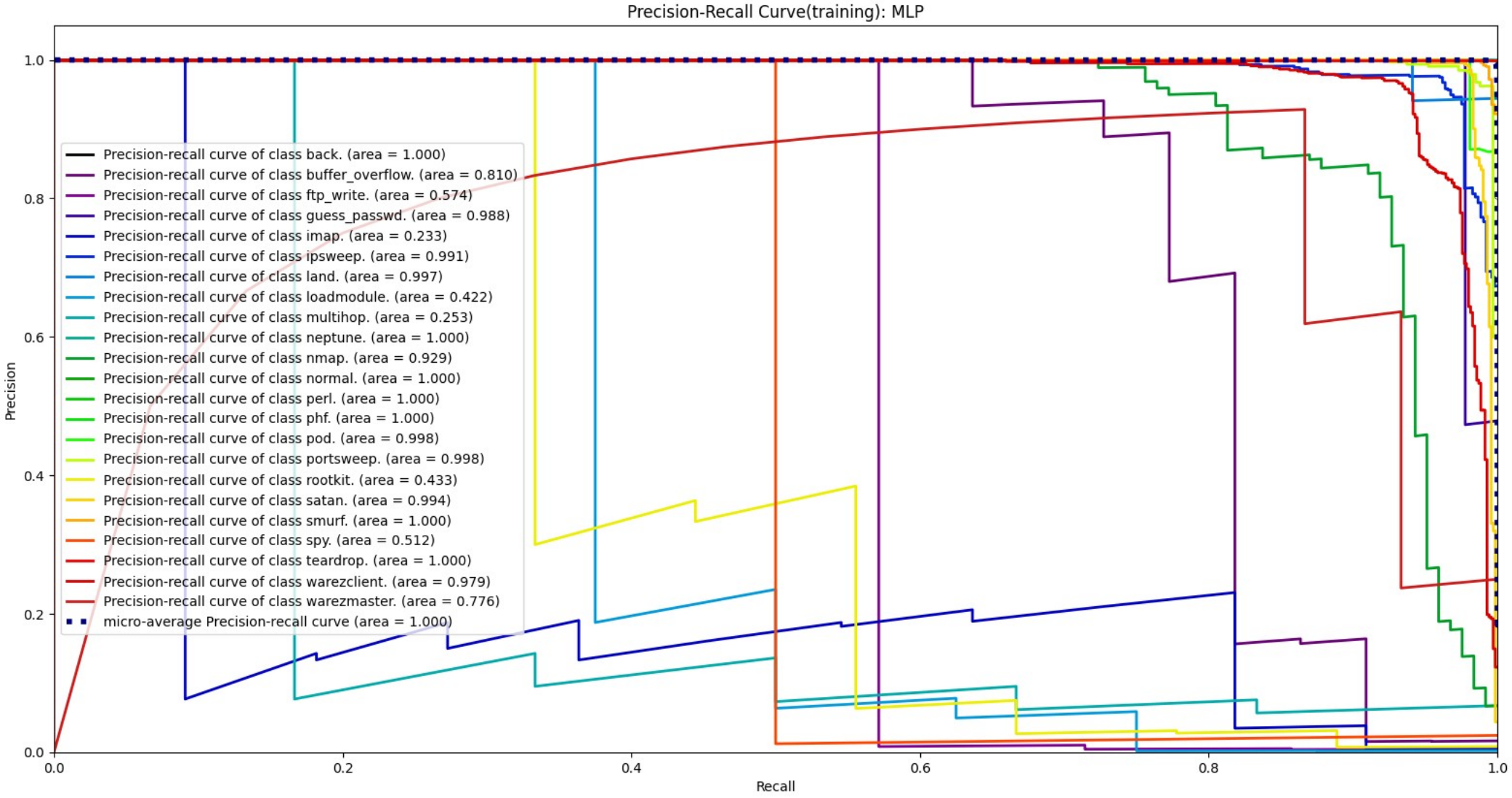
Results: MLP /w Early Stopping (Training), ROC



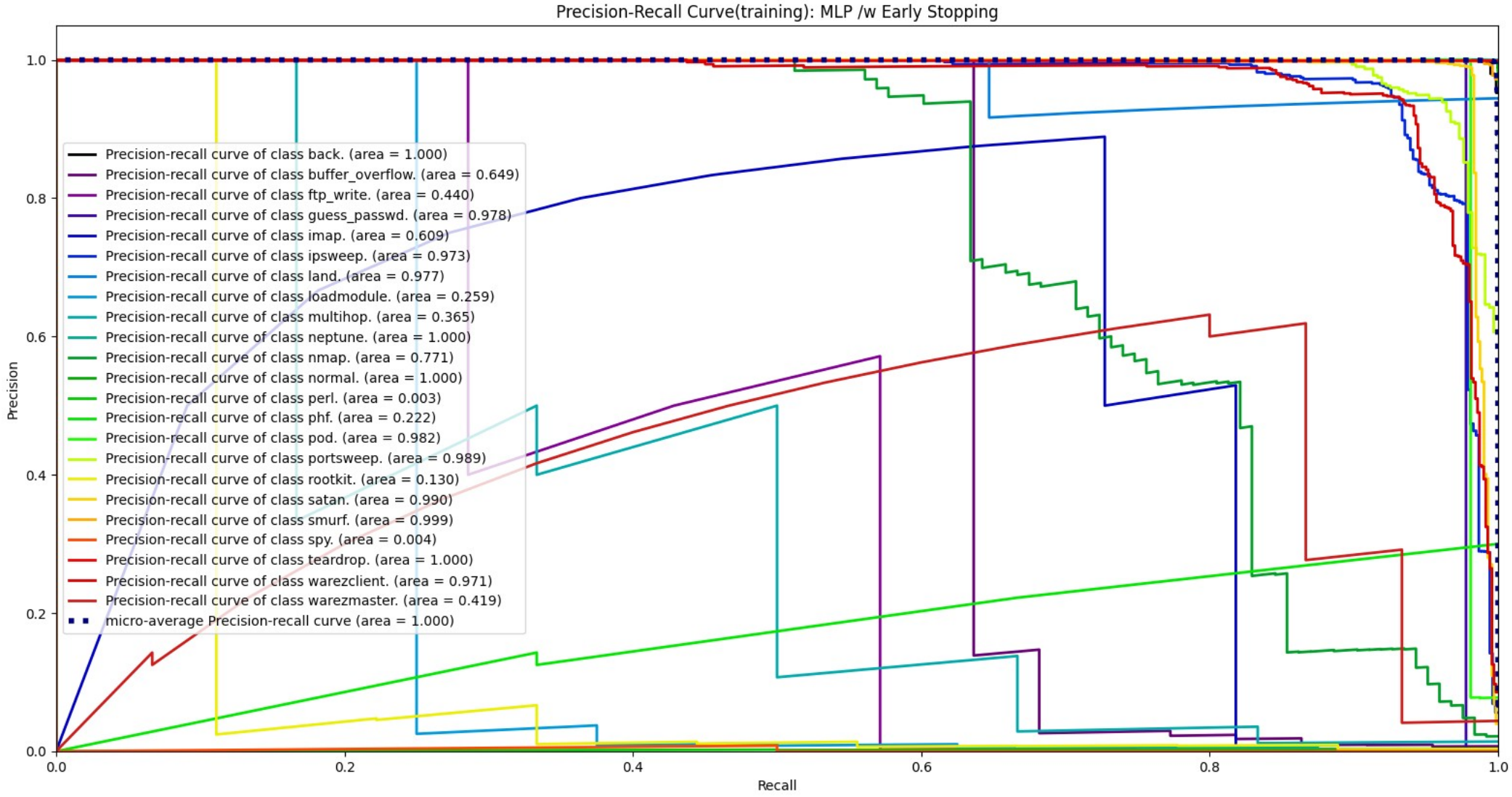
Results: Random Forest (Training), ROC



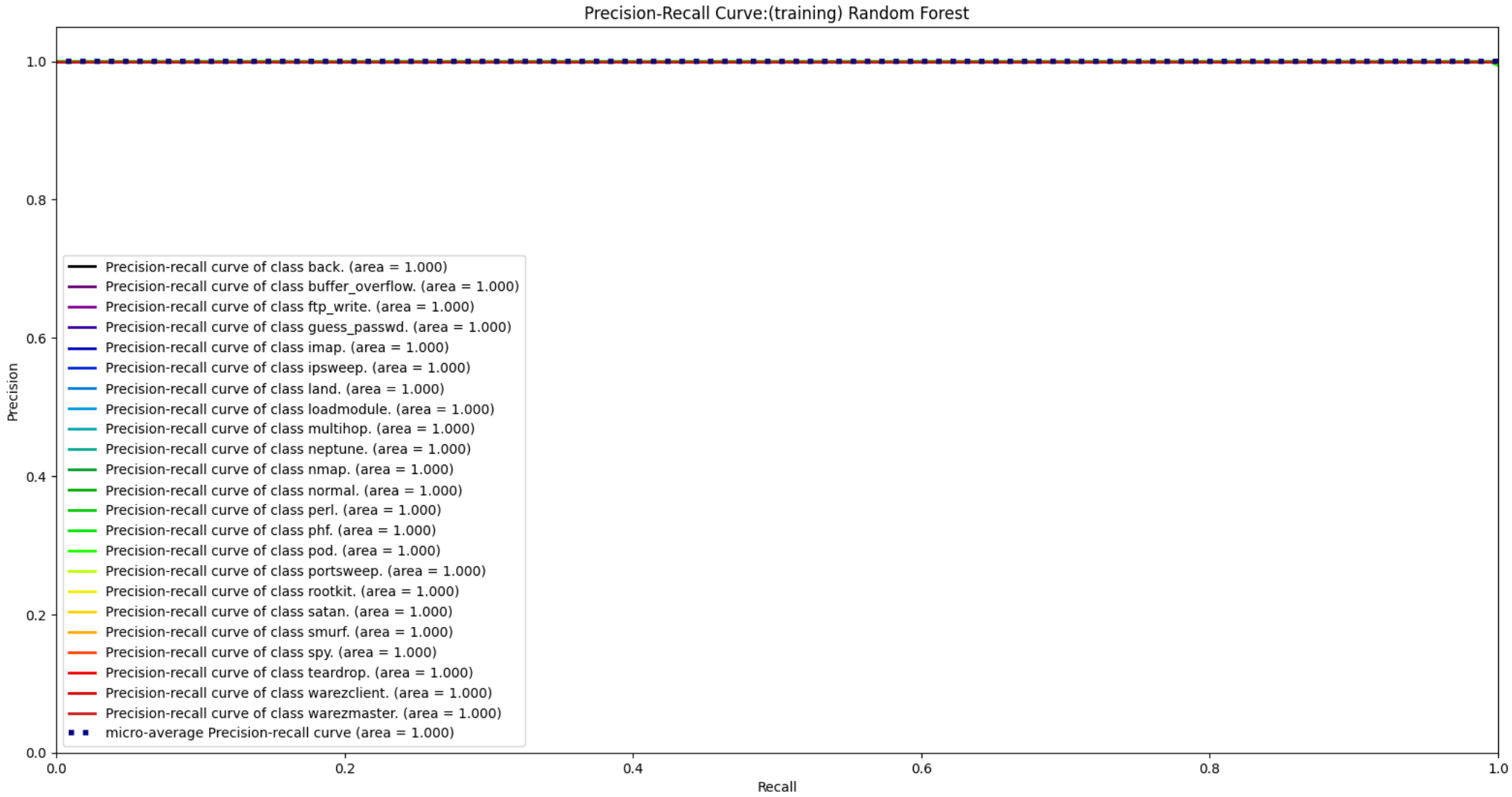
Results: MLP (Training), Precision Recall



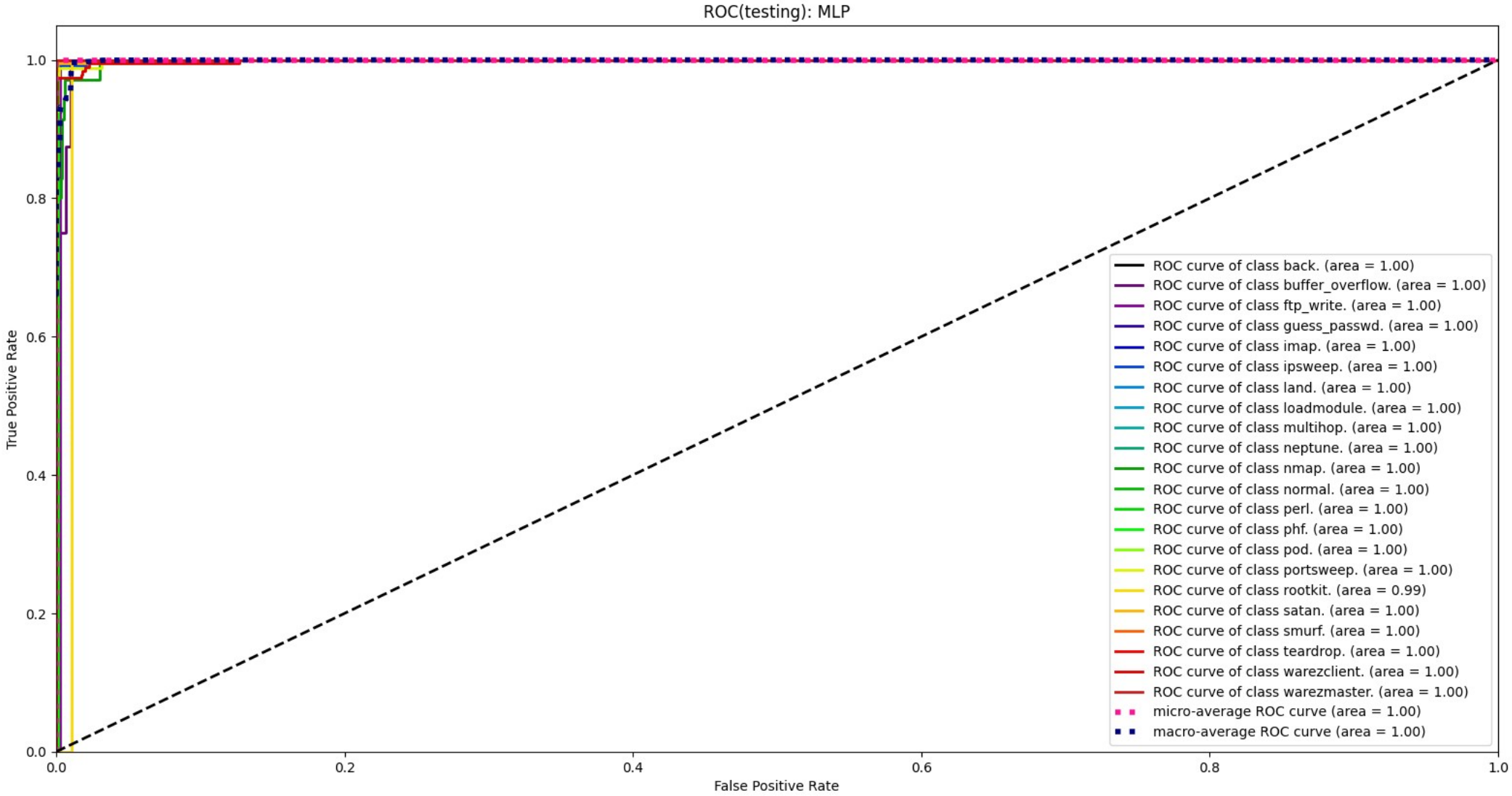
Results: MLP /w Early Stopping (Training), Precision Recall



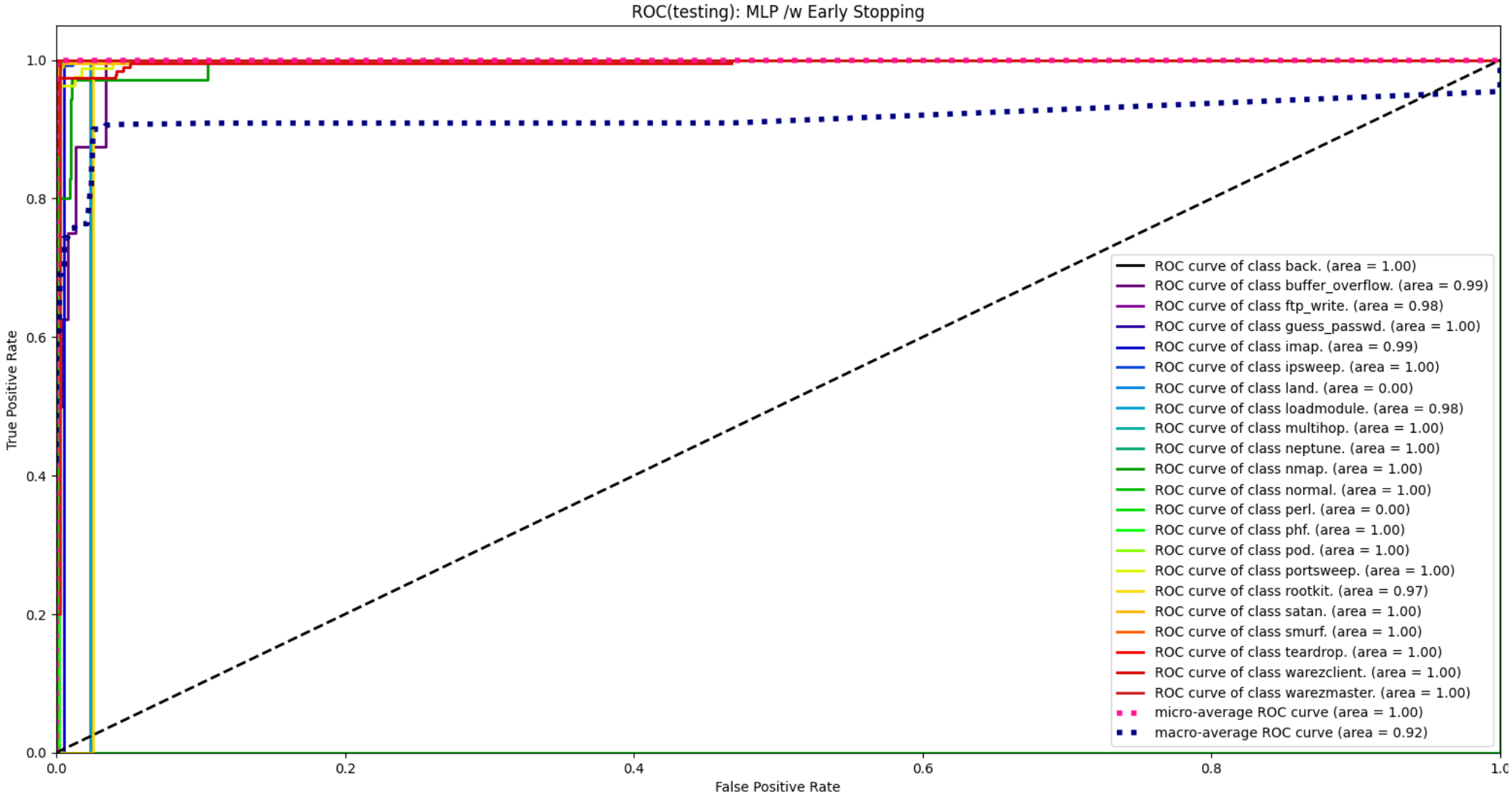
Results: Random Forest (Training), Precision Recall



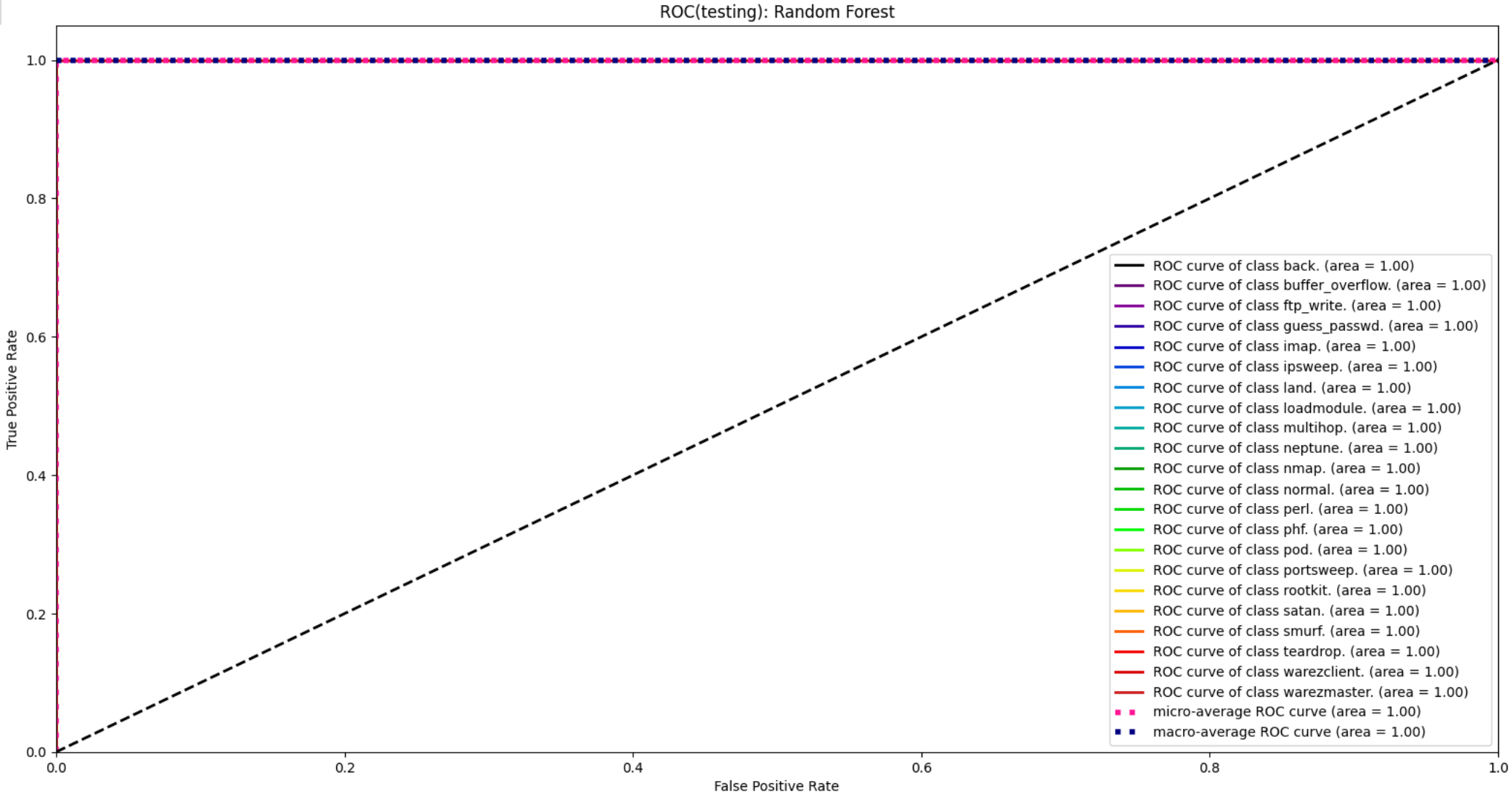
Results: MLP (Testing), ROC



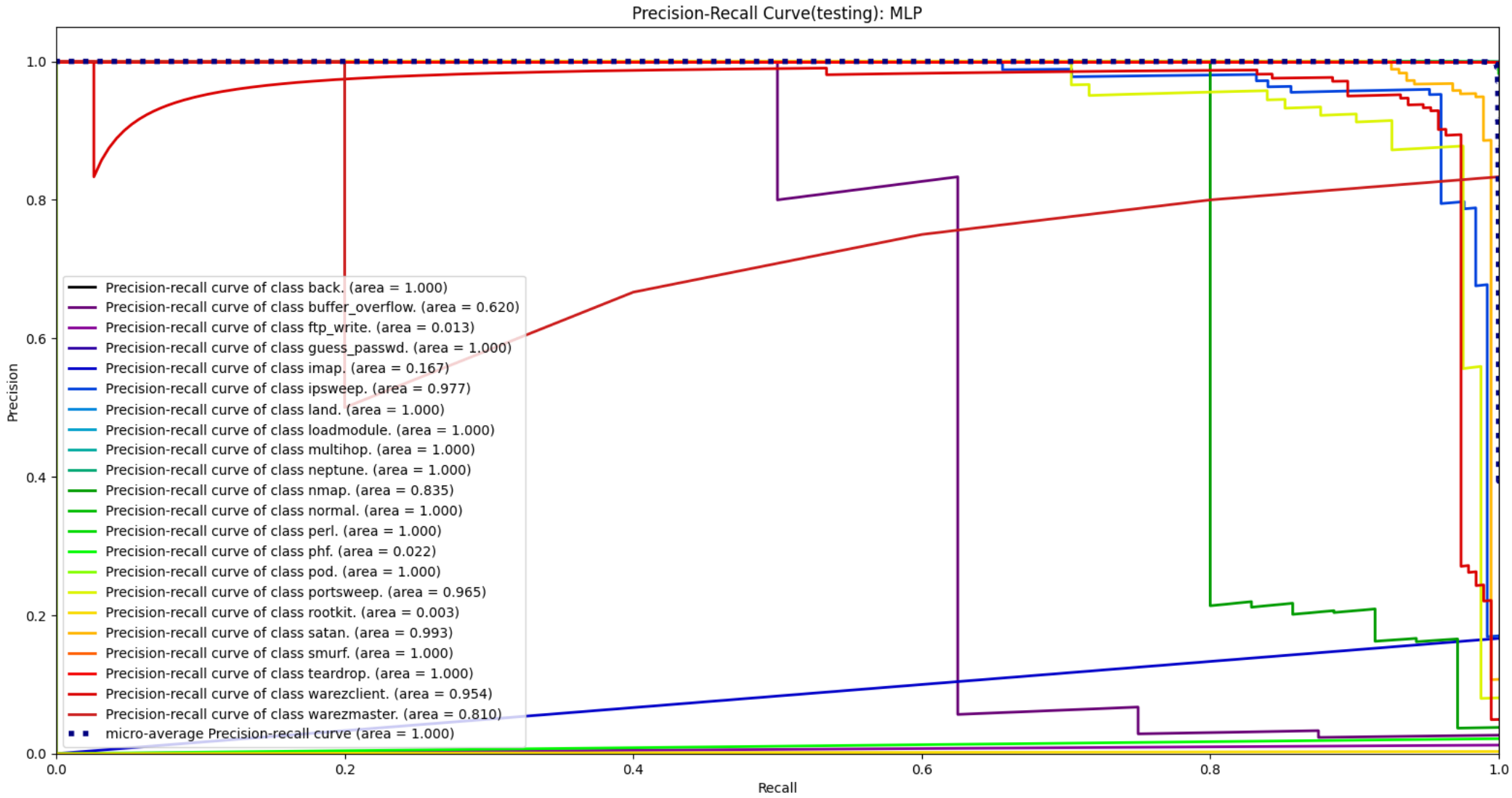
Results: MLP /w Early Stopping (Testing), ROC



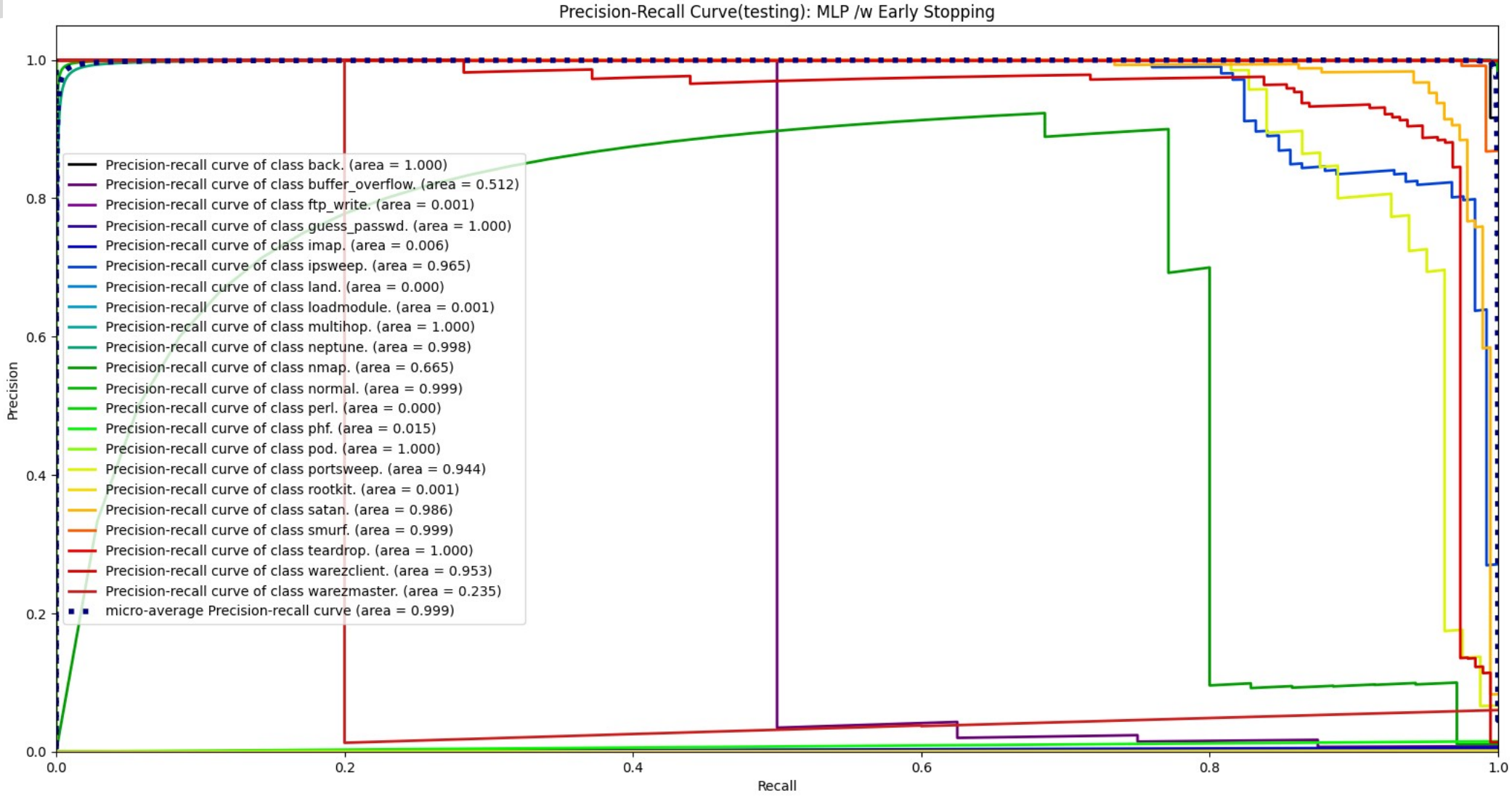
Results: Random Forest (Testing), ROC



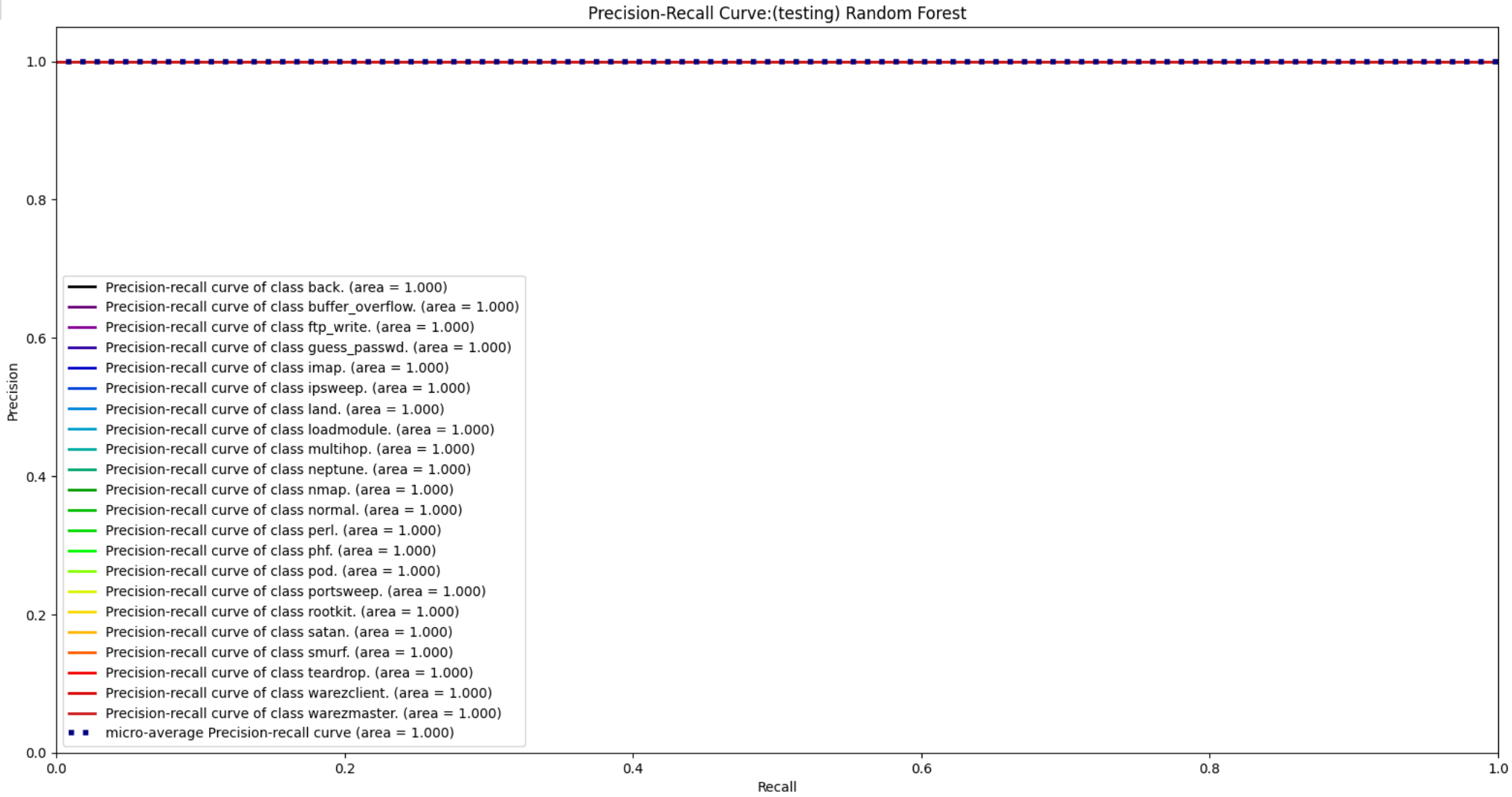
Results: MLP (Testing), Precision Recall



Results: MLP /w Early Stopping (Testing), Precision Recall



Results: Random Forest (Testing), Precision Recall



Final Thoughts

- Use of individual classifiers for set of attack vectors
  - distinguish via discriminator (concept from GANs)
  - apply weighted-voting approach
  - All these are ways to minimise False positives in anomaly detection

Thank You