Network Security Project 2
Log Analysis

Instructor: Shiuhpyng Shieh

TA: 13m0n, Tori, Liren

Log Analysis

- Log analysis is the evaluation of logs and is used in all sorts of scenarios. For instance, they are used to:
  - help mitigate various of risks.
  - troubleshoot systems, computers, or networks.
  - conduct forensics in the event of an investigation.
  - understand the behaviors of users(UBA).

Cyber Attack

- A cyber attack can be defined as a malicious act that seeks to disrupt digital life. This act could be the
  - Disruption of a communication pathway
  - Damage of data
  - Stealing data
- Hackers target enterprises, governments, institutions, or even individuals with valuable information. Threats posed by cyber-attacks include
  - Denial of service attacks (DoS)
  - Malware
  - Phishing emails
  - Etc.

Goal of this project

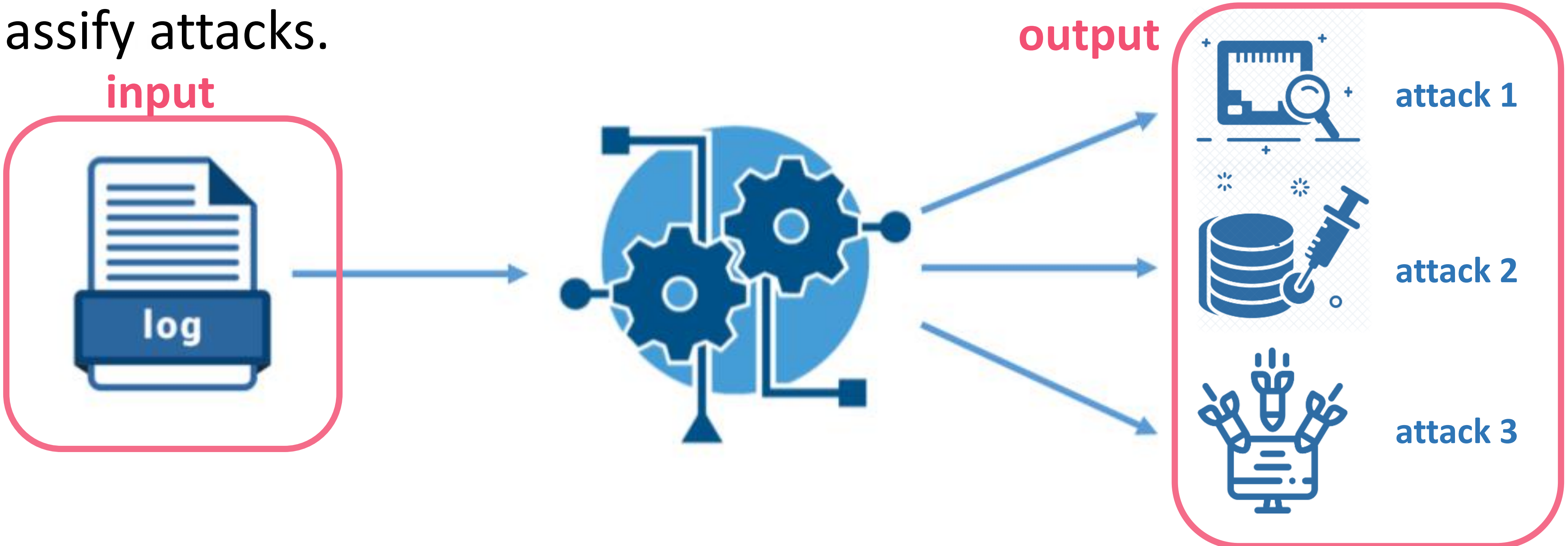
- Practice a simple case of cyber attack analysis:
  - Survey how different types of attacks work.
  - Observe logs.
  - Classify the attacks with logs.
- This is a personal project.

Things you need to do

- Parse log into the format you need later in analysis.
- Model Design
  - Rule-Based Method
  - Deep learning/Machine learning
  - Free play

Model I/O

- You will be provided with log data collected from a host when different attacks are carried out.
  - Including network logs and system logs
- You are asked to analyze the log data, and then develop a model to classify attacks.



Submission

- A zip file which includes:
  - Your model(source code)
  - Report file in PDF format:
    - The core logic of the model, result and accuracy.
    - Anything interesting you find or problems you encounter.
- Name the report file with your student ID, ex. “0756000.pdf”.
- Upload the file to New E3 platform.
- Deadline: 2020/12/13 (Sunday) 23:55

Q & A

You can post your issue on github to discuss with others.

Github: https://github.com/dsnslab/NetworkSecurity/

Email: TA@dsns.cs.nctu.edu.tw

Lab: EC622

(Please make an appointment with email before you go to lab.)