

# Network Security Project 2

## Attack Classification

Instructor: Shiuhpyng Shieh

TA: Su-Xin Chong, Wan-Yu Chen, Tsung-Hung Wu,  
Pei-Hsuan Hung, Zhong-Hao Liao

# Outline

- Background knowledge
  - Cyber Attacks
  - Log Analysis
- Project introduction
  - Project objectives
  - Attack categories
- Scoring
  - Demo notice
  - Submission rules

# 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
  - Distributed Denial of service attacks (DDoS)
  - Bruteforce attacks
  - IP/Port scanning, etc.

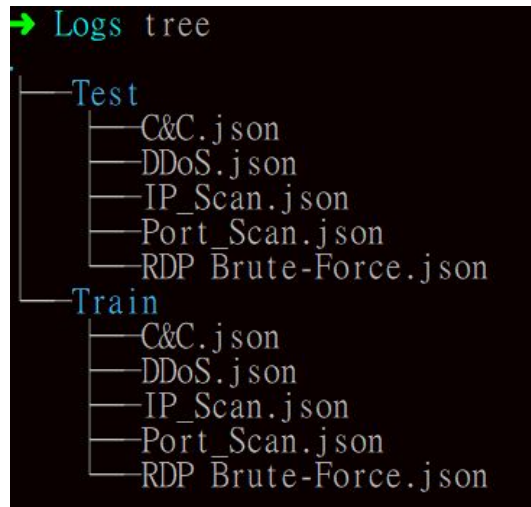
# Log Analysis

- Evaluation of logs
- Can be used in all sorts of scenarios
  - **Help mitigate various of risks**
  - Troubleshoot systems, computers or networks
  - Understand the behaviors of users (UBA)

# Introduction

- 5 attack categories
- Packetbeat logs for each categories with both training/testing datasets
- Build a model to classify which attack the log stands for
- The model will be evaluated with another dataset at demo time

Logs directory structure



# Detailed Steps

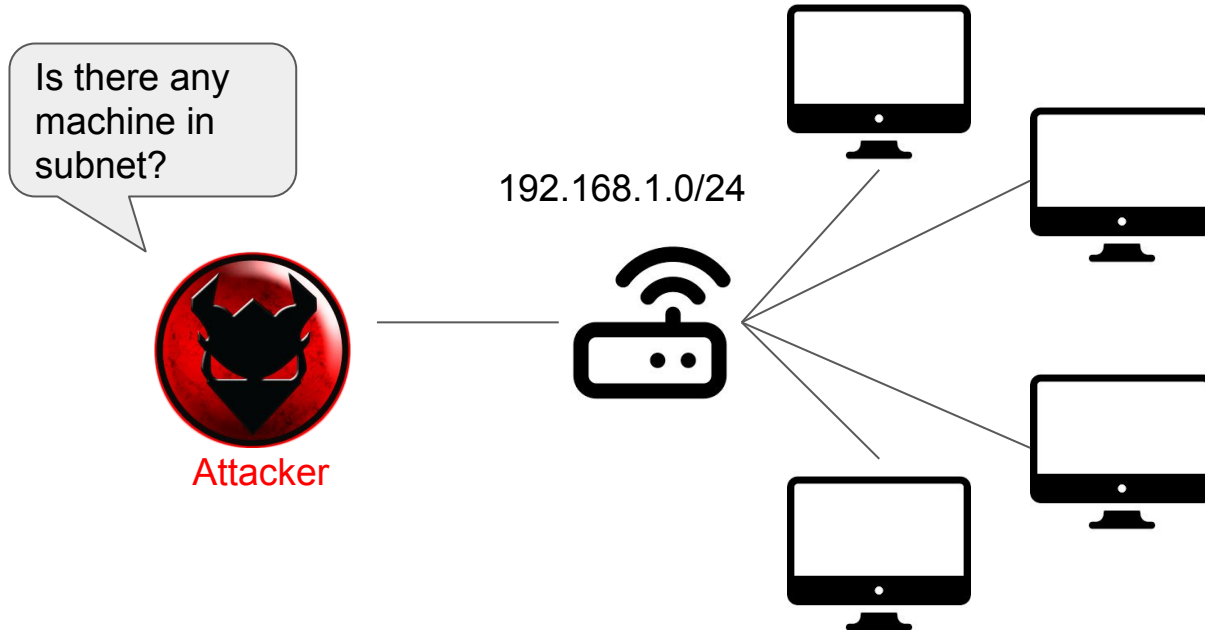
- Take a look at how the assigned attack categories work
  - Try to figure out possible features that this attack might generate
- Observe the logs (if needed)
  - Use elasticsearch-dump or other useful tools to import the logs to ELK
  - Elastic Cloud might help if you don't want to setup ELK stack on your machine locally (14-day trial)
- Design a model to classify the attacks
  - Your model can be either **rule-based** or **machine-learning based**
- Demonstrate your model at demo time
  - Your model will be tested on another dataset
  - The format is the same as your training/testing dataset

# Attack Categories

- IP Scan
- Port Scan
- DDoS (Distributed Denial of service)
- RDP Brute-Force
- C&C (Command and Control)

# IP Scan

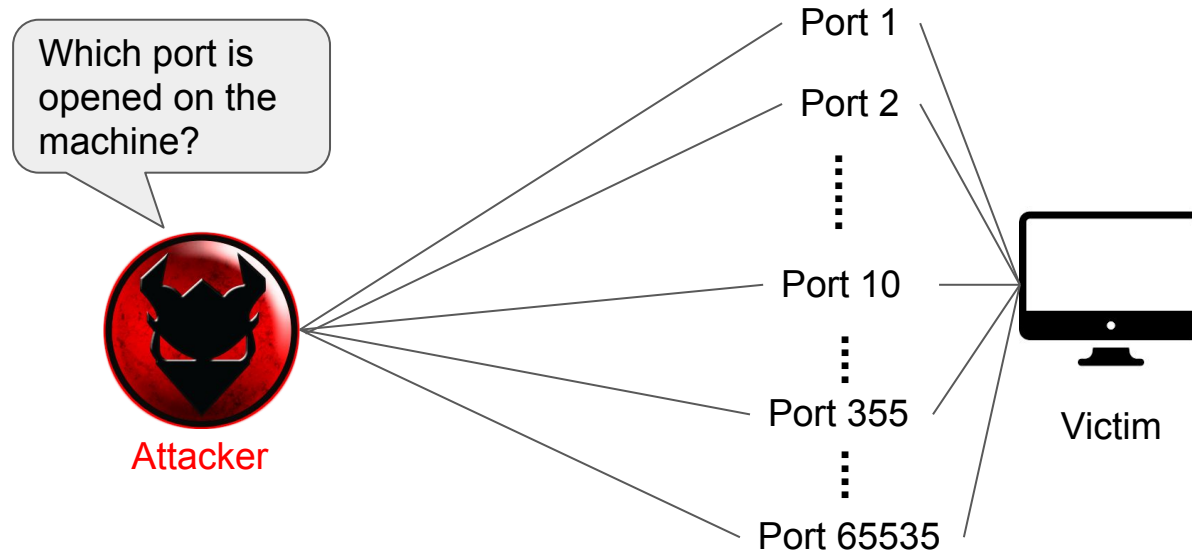
- Attackers **send packets to IP addresses in LAN within a short period of time** to seek if there exists other machines in the internal network





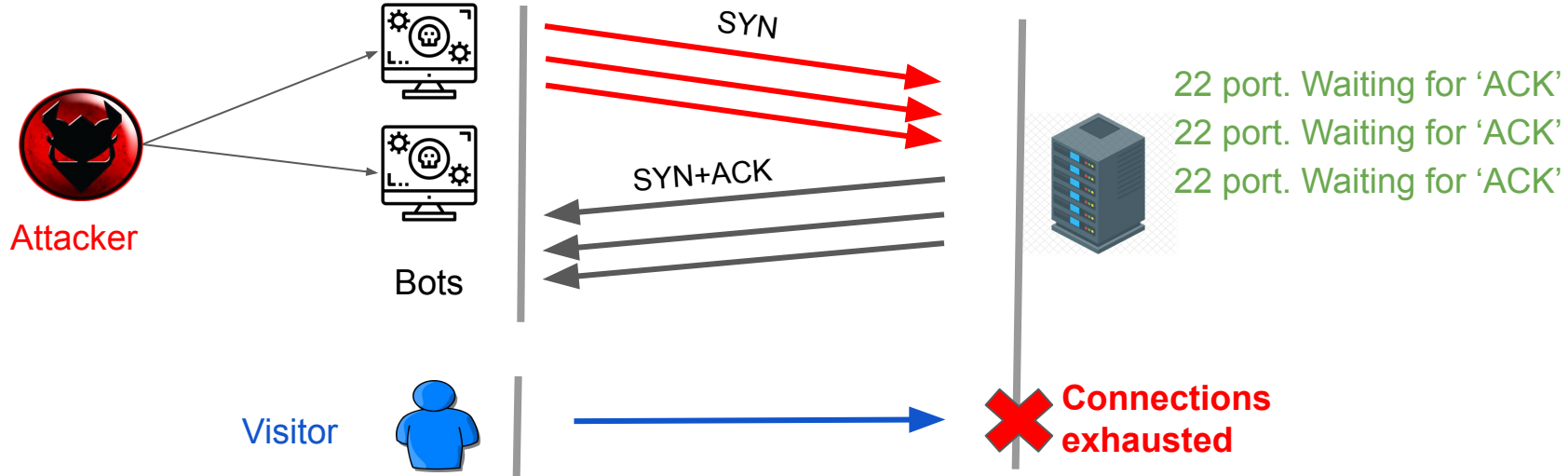
# Port Scan

- Attackers try to **send packets to different ports in a short time** to figure out an active port/service on victim machine



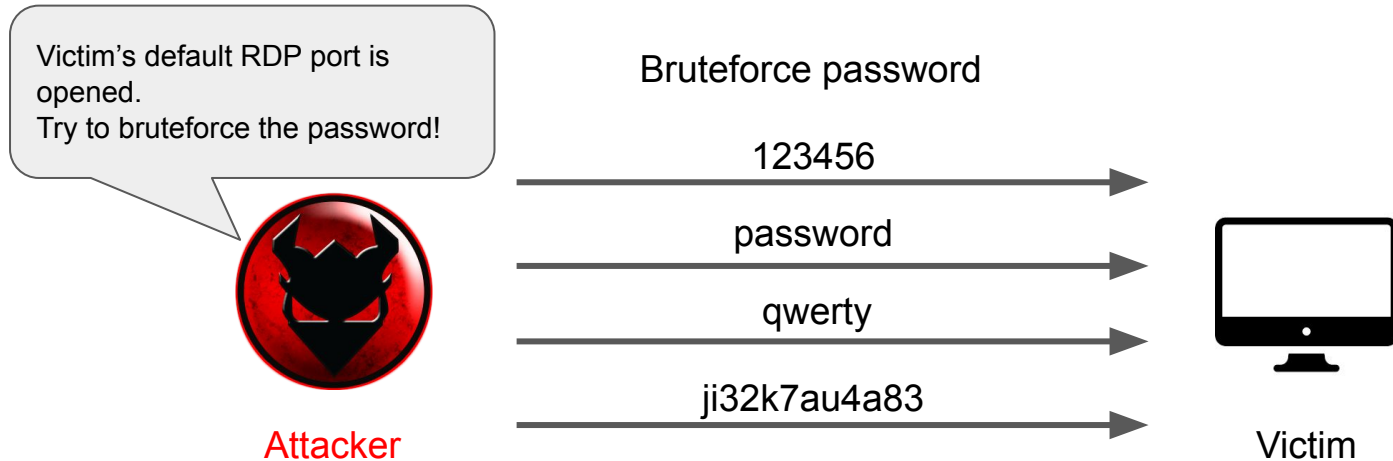
# DDoS (Distributed Denial of Service)

- Attackers flood the targeted machine with overwhelmed requests to prevent legitimate requests from accessing the normal service
- In this project, the attacker tries to **flood the victim's ssh service(port 22)** to prevent normal user from logging in



# RDP Brute-Force

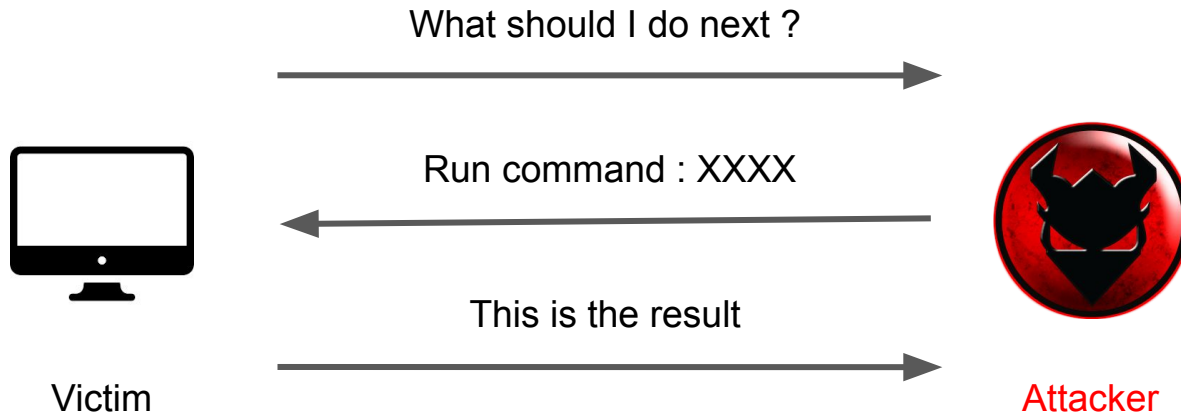
- Attackers seek if **default RDP port** is opened on the victim machine and seek to bruteforce the user's password to gain access to the machine



# C&C (Command and Control)

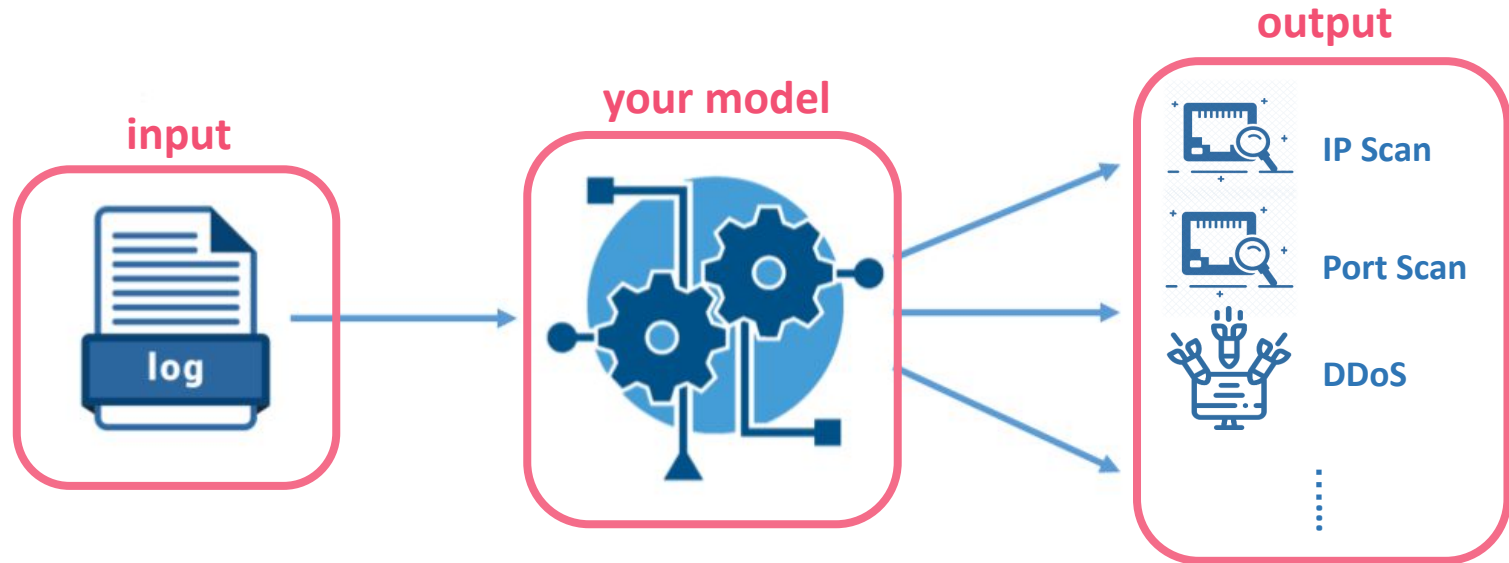
- A tactic commonly used by attacker to control the compromised machine
- Attackers won't need to hard-code the fixed command in the malware in this fashion
- Malwares need to communicate to remote server periodically to know what command to execute
- Malwares usually exfiltrate information of infected machine to the attacker.
  - In this project, the attacker exfiltrate some files from the victim on an **unusual port**

# C&C (Command and Control)



# Design a Model

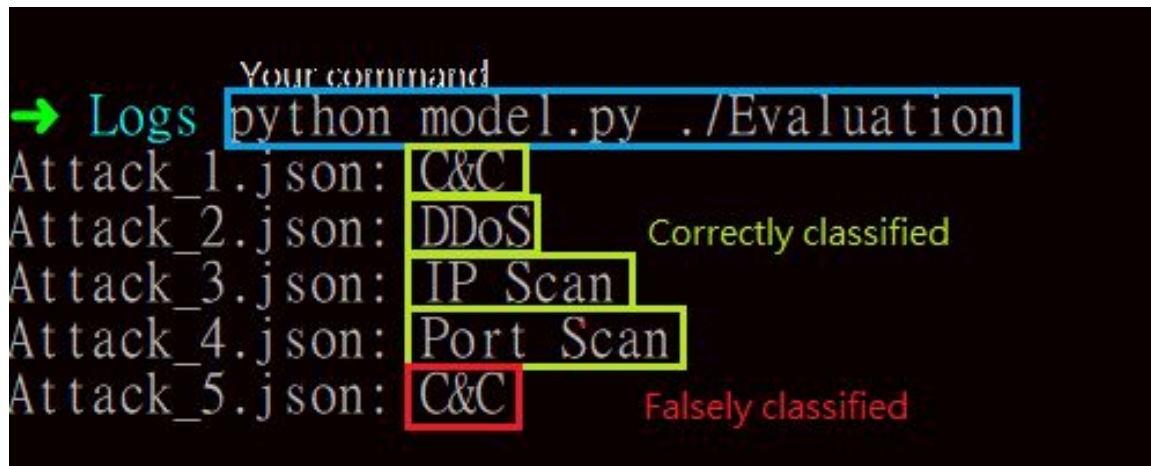
- You are given logs collected from packetbeat in host when different attacks are carried out
- Try to figure out the characteristics of each attacks, and develop a model to classify them



# Model I/O

- Input: Read the directory of files from command line argument
- Output: Input filename with the classified category in

**<filename>: <category>** format



A terminal window with a black background. At the top, a green arrow points to the word 'Logs'. To its right, the command 'python model.py ./Evaluation' is entered and highlighted with a blue box. Below the command, five lines of output are shown, each with a filename and a category. The categories are highlighted with yellow boxes, except for the last one which is highlighted with a red box. To the right of the output, the text 'Correctly classified' is written in yellow, and 'Falsely classified' is written in red.

```
→ Logs python model.py ./Evaluation
Attack_1.json: C&C
Attack_2.json: DDoS
Attack_3.json: IP Scan
Attack_4.json: Port Scan
Attack_5.json: C&C
```

Correctly classified

Falsely classified

# Elasticdump (Optional)

- Tool for moving and saving indices on Elasticsearch
  - Import JSON data to Elasticsearch
  - Export data from Elasticsearch to JSON file
  - Migrate data between Elasticsearch servers
- Installation/Usage
  - <https://github.com/dsnslab/NetworkSecurity/blob/master/109-2/Project2/Elasticdump.pdf>
- Reference
  - <https://github.com/elasticsearch-dump/elasticsearch-dump>



# Scoring

- Part A: Report (25%)
  - A report in PDF format that contains:
    - What model or algorithm you use?
    - What features/rules you used for your model?
    - Why do you select them? Please describe as much detail as possible
    - Anything interesting things you find or problems you encounter
  - A folder that contains:
    - Source code of your model
    - A README file explaining how to execute the model
- Part B: Demo (75%)

# Demo

- Your model will be evaluated **with another dataset**
- Bring your own device
- Your model should be executed on-site during the demo period. Make sure the result shows up within a reasonable time
  
- Time : 5/31(Mon.), 6/1(Tue.), 6/4(Fri.)
  - The exact time and venue will be further noticed a week before the deadline

# Submission

- Upload a zip file named "<STUDENT ID>.zip" to E3 platform
- A zip file which includes:
  - The source code of your model.  
(The model can be written in any language, but needs to be executed on-site at demo time)
  - Report in PDF format:
    - The core logic of the model, result and accuracy.
    - Anything interesting you find or problems you encounter.
- Deadline: 2021/05/30 (Sunday) 23:55
- The penalty for late submission is 10% per day, and 10 points will be deducted for handing in wrong file format.
- **Plagiarism is strictly prohibited!**

# Q&A

- Questions and answers for Project 2 from last semester
  - <https://github.com/dsnslab/NetworkSecurity/issues?q=label%3A109-1-pj2>
- Feel free to contact us via email or Github issue if you have any questions.  
(You are encouraged to discuss with other classmates in issues)
- Email: TA@dsns.cs.nctu.edu.tw
- TA Hour:
  - Mon. 13:00~15:00 @EC622
  - Tue. 13:00~15:00 @EC622