# Various Attack Scenario Generation

Advisor 黃彥男
Mentor 李泓暐
Presented by 顏佐霏 黃郁涵

# Outline

Various Attack Scenario Generation

# Introduction

## Motivation

Many existing public intrusion datasets e.g. DARPA / ADFA are **outdated**.

## Purpose

Expand public intrusion datasets that **represent real world situation**.

## Idea

1. **Generate and Collect audit logs** from both *attack* and *benign* scenarios.
2. Develop algorithms to **form Synthetic Datasets.**

01

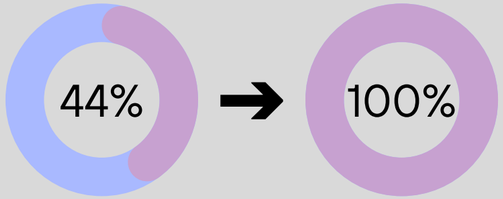
# Introduction

## Contribution :

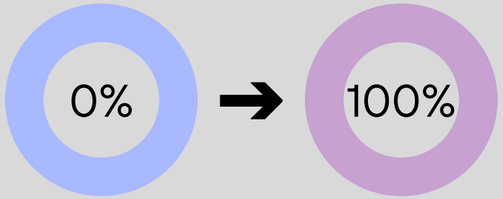
## *Process Automation*

Recording audit log → generating provenance graph :
**partially automatic** → **fully automatic**

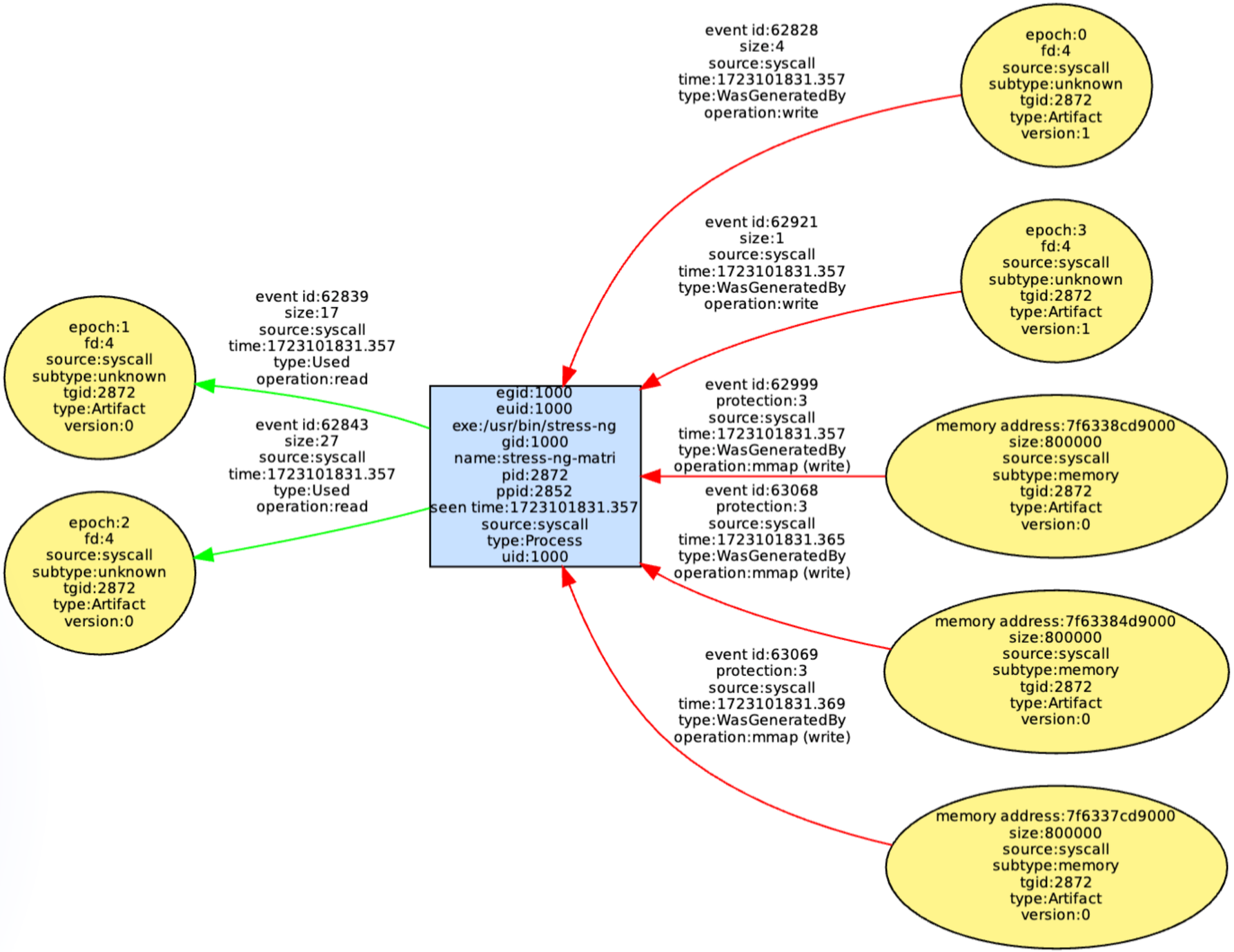
**Attack workload**




**Benign workload**



# Provenance Graph



01

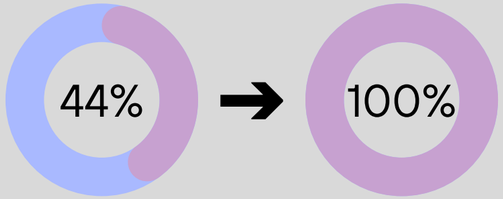
# Introduction

## Contribution :

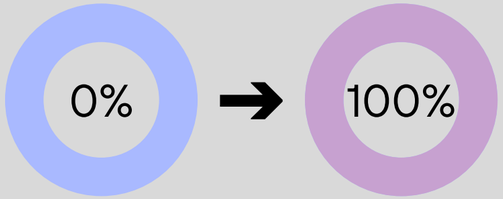
## *Process Automation*

Recording audit log → generating provenance graph :
**partially automatic** → **fully automatic**

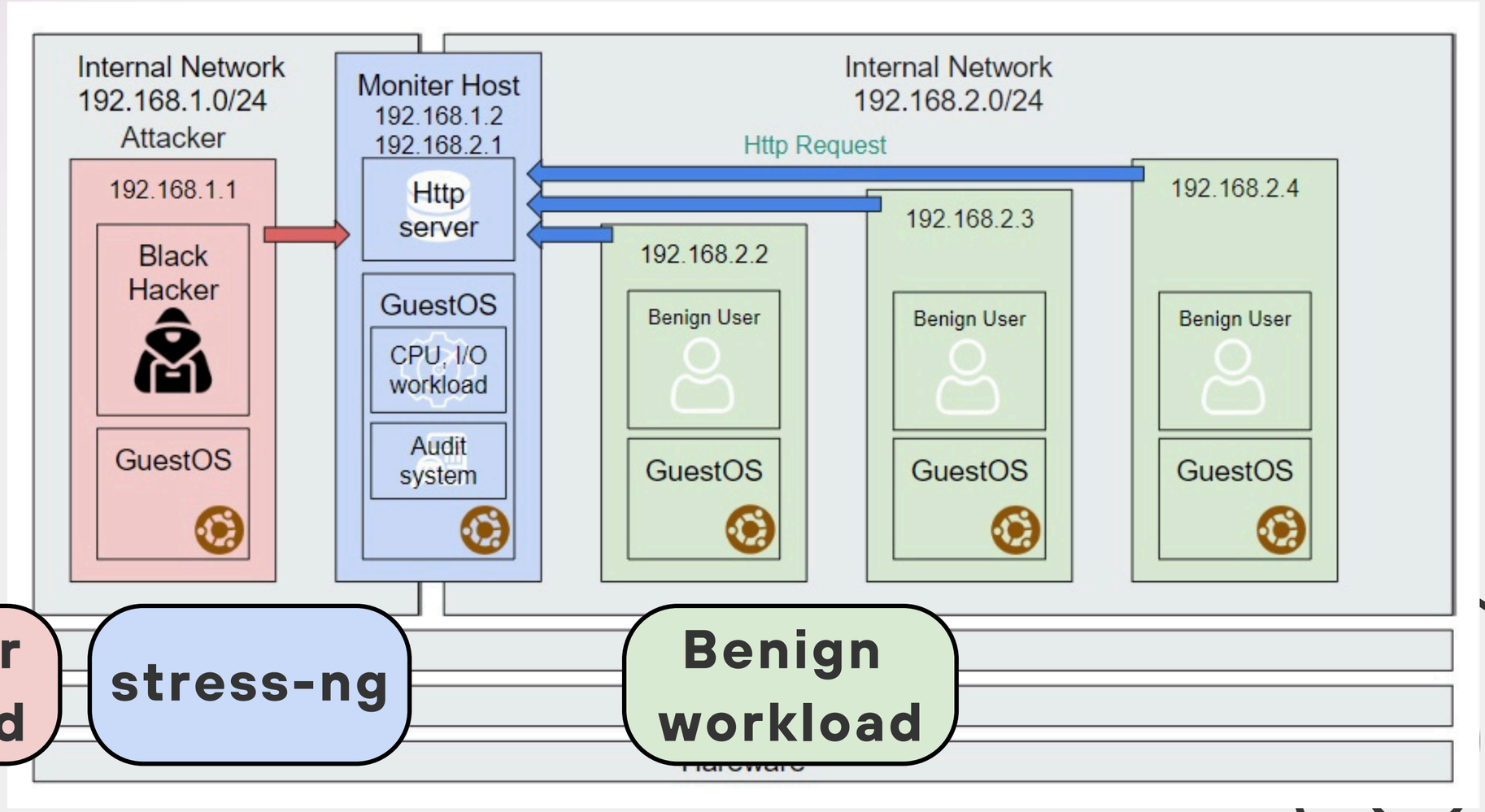
**Attack workload**




**Benign workload**



# Progress -Overview




**Attacker workload**

**stress-ng**

**Benign workload**

# Progress

02

## -Attacker Workload

### SPADE

- track data object and record logs
- generate provenance graphs

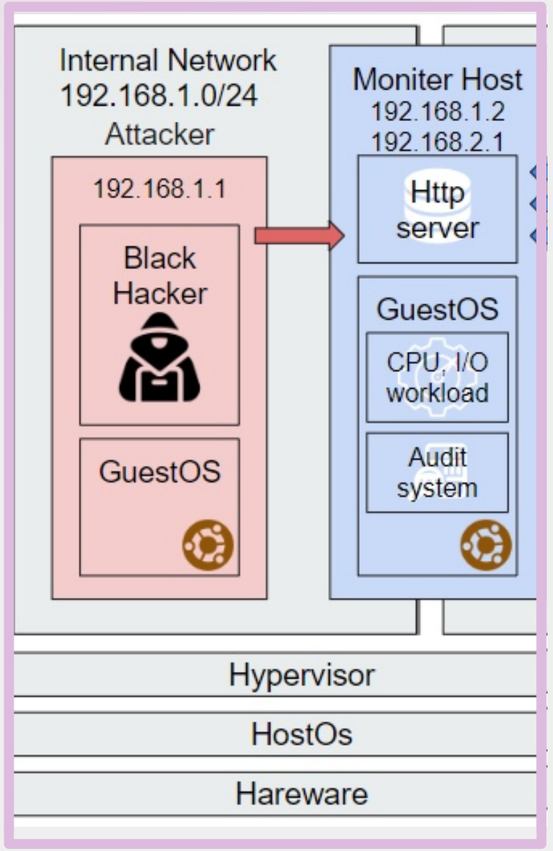
### CALDERA

- automated adversary emulation system
- replicate real-world attack scenarios

# Progress

02

## -Attacker Workload




- **Handover**

  collect logs and transform graphs

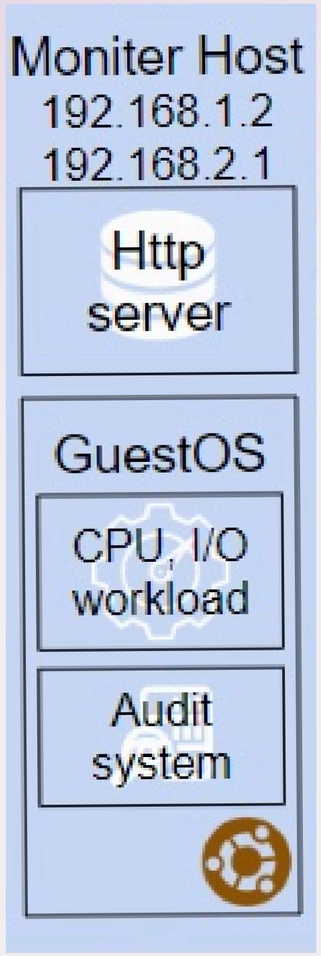
  successfully transform: **172 over 394 set of data**

- **Improvement**

  successfully generate **all provenance graph**

# Progress -stressng

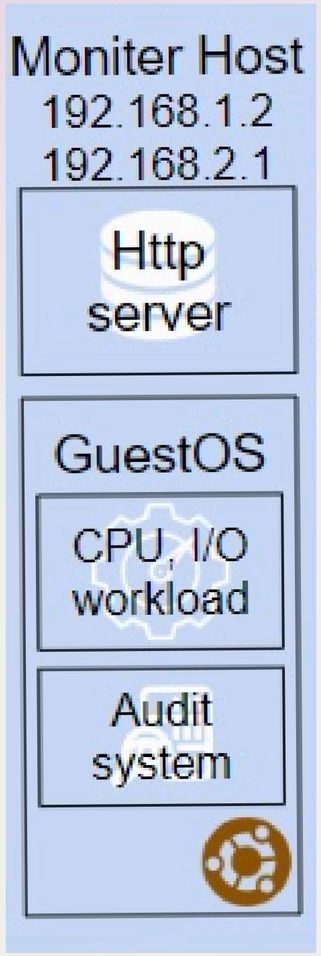
02




- **Stress-ng**
  - Workload generator : **simulate various system operations**
    - CPU load
    - memory operations
    - disk IO
    - network IO
    - system calls
    - multi-processes / multi-threads
    - virtual memory

# Progress -stressng

02




- **Handover**
  - basic structure and scripts : **no automation**
- **Improvement**
  - **Intergrate stress-ng into Monitor Host**
    - collect all audit log
    - transform all audit logs into provenance graph
  - **Process automation**

# Results

## Attacker workload

- successfully transform: **394 sets of data** (include filtered log and provenance graph)
- the entire process could be run **automatically**

## stress-ng

- successfully transform: **356 different tasks**
- the entire process could be run **automatically**

03

# Conclusion & Vision

04

- Process Automation
- stress-ng Integration
- Extend Benign Workload
  - http
- Develop Synthetic Dataset Algorithm

# Thank You