# Malware Analysis


Alvin

David Wambia

Ian Osoro

# What is Malware analysis?

- Learning how malware functions and any potential repercussions of a given malware.

# Malware analysis methods

- Static malware analysis
- Dynamic malware analysis
- Hybrid malware analysis

# Static malware analysis

## Types of Malware

- Packed
- Obfuscated

# Basic Static Analysis-Techniques

- Antivirus Scanning
- Hashing
- FInding Strings
- Detecting Packers with PEiD

# Dynamic Malware Analysis

Malware is analysed when executing;

Malware is run inside a sandbox(VM)

Direct Interaction with the malware

# Basic Dynamic Malware analysis

Involves basically observing malware behaviour as it executes to understand what kind of malware it is

Actions include:

- Check changes to the registry
- Files created/added after the malware has run

# Advanced Dynamic Malware analysis

Involves using a debugger to further examine the internal state of the malware,check processes e.t.c

Useful when static and basic dynamic analysis doesn't give results due to stealth nature of the malware.

# Hybrid malware analysis

- Combines techniques from both methodologies to cover each other’s shortcomings
- Malware is analysed before installation and also its execution behavior is logged. These sets of static and dynamic information are then used together to detect malicious behavior.

# THE END