HyperionDev

Welcome to this session:
Malware Analysis

The session will start shortly...

Questions? Drop them in the chat.
We'll have dedicated moderators
answering questions.

HyperionDev

What is Safeguarding?

Safeguarding refers to actions and measures aimed at protecting the human rights of adults, particularly vulnerable individuals, from abuse, neglect, and harm.

To report a safeguarding concern reach out to us via email:
safeguarding@hyperiondev.com

HyperionDev

Live Lecture Housekeeping:

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment for all - please engage accordingly.
- No question is daft or silly - ask them!
- For all non-academic questions, please submit a query: www.hyperiondev.com/support
- To report a safeguarding concern reach out to us via email: safeguarding@hyperiondev.com
- If you are hearing impaired, please kindly use your computer's function through Google chrome to enable captions.

HyperionDev

Lecture Overview

- → Introduction to malware
- → Types of malware analysis
- → How Python is used in malware analysis

Learning Outcomes

- Define malware analysis.
- Explain static and dynamic analysis.
- Implement safe malware analysis.
- Perform basic malware analysis using Python.

Polls

Please have a look at the poll notification and select an option.

What is the PRIMARY goal of malware analysis?

A. To delete infected files
B. To understand how malware works and what it does
C. To punish hackers
D. To encrypt sensitive data

Polls

Please have a look at the poll notification and select an option.

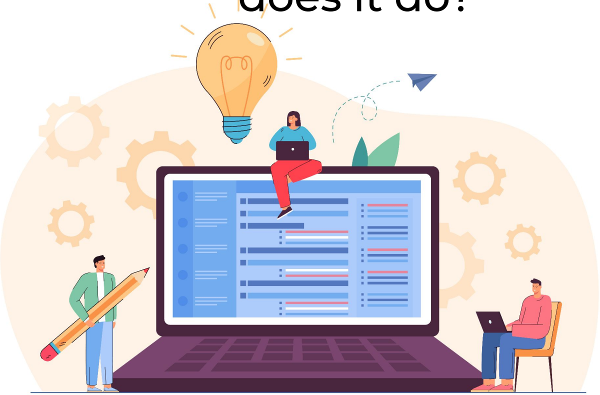
Which approach involves running malware to observe its behavior?

A. Static Analysis
B. Dynamic Analysis
C. Network Analysis
D. Forensic Analysis

HyperionDev

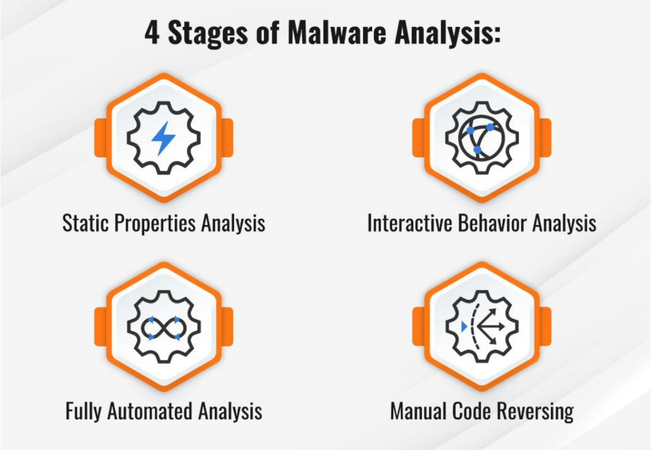
Malware Analysis

You’re a cybersecurity analyst, and your team receives a suspicious email with an attachment. The sender is unknown, and the file looks harmless, maybe a PDF or a Word document. But something feels off. Your boss asks, “Is this malware? What does it do?”



Malware Analysis

- **Definition:** The process of dissecting malicious software to understand its behavior, purpose, and impact.
- **Purpose:** Helps detect, prevent, and respond to cyber threats.



4 Stages of Malware Analysis:

Static Properties Analysis

Interactive Behavior Analysis

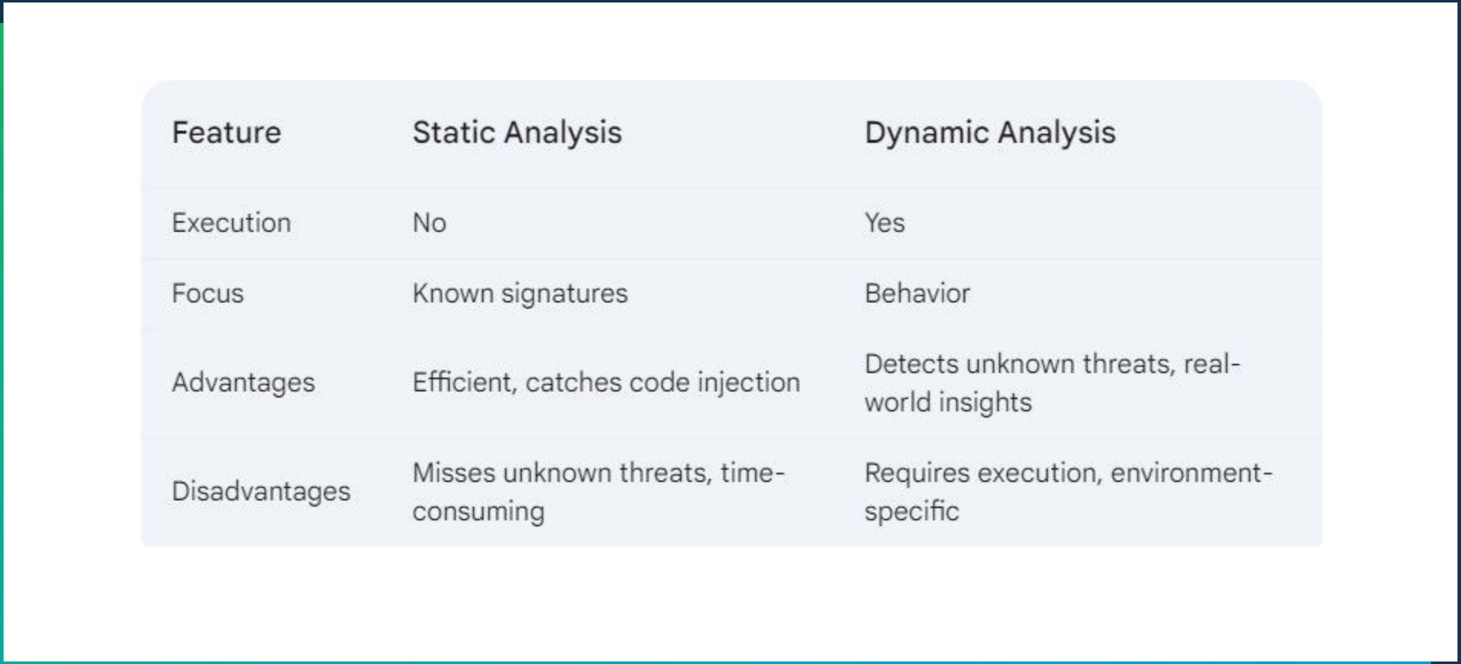
Fully Automated Analysis

Manual Code Reversing

Static vs Dynamic Analysis

- **Static Analysis:**
  - Examining the code without execution
  - Tools: Hex editors, disassemblers.
- **Dynamic Analysis:**
  - Observing behaviour by running malware
  - Sandboxes, debuggers

Static vs Dynamic Analysis



Feature	Static Analysis	Dynamic Analysis
Execution	No	Yes
Focus	Known signatures	Behavior
Advantages	Efficient, catches code injection	Detects unknown threats, real-world insights
Disadvantages	Misses unknown threats, time-consuming	Requires execution, environment-specific

Tools for Malware Analysis

- **Static Analysis Tools:**
  - Hex editors
  - Disassemblers
  - MetaData Inspectors
- **Dynamic Analysis Tools:**
  - Sandboxes (e.g., Cuckoo Sandbox).
  - Debuggers (e.g., OllyDbg).

HyperionDev

Let’s take a break

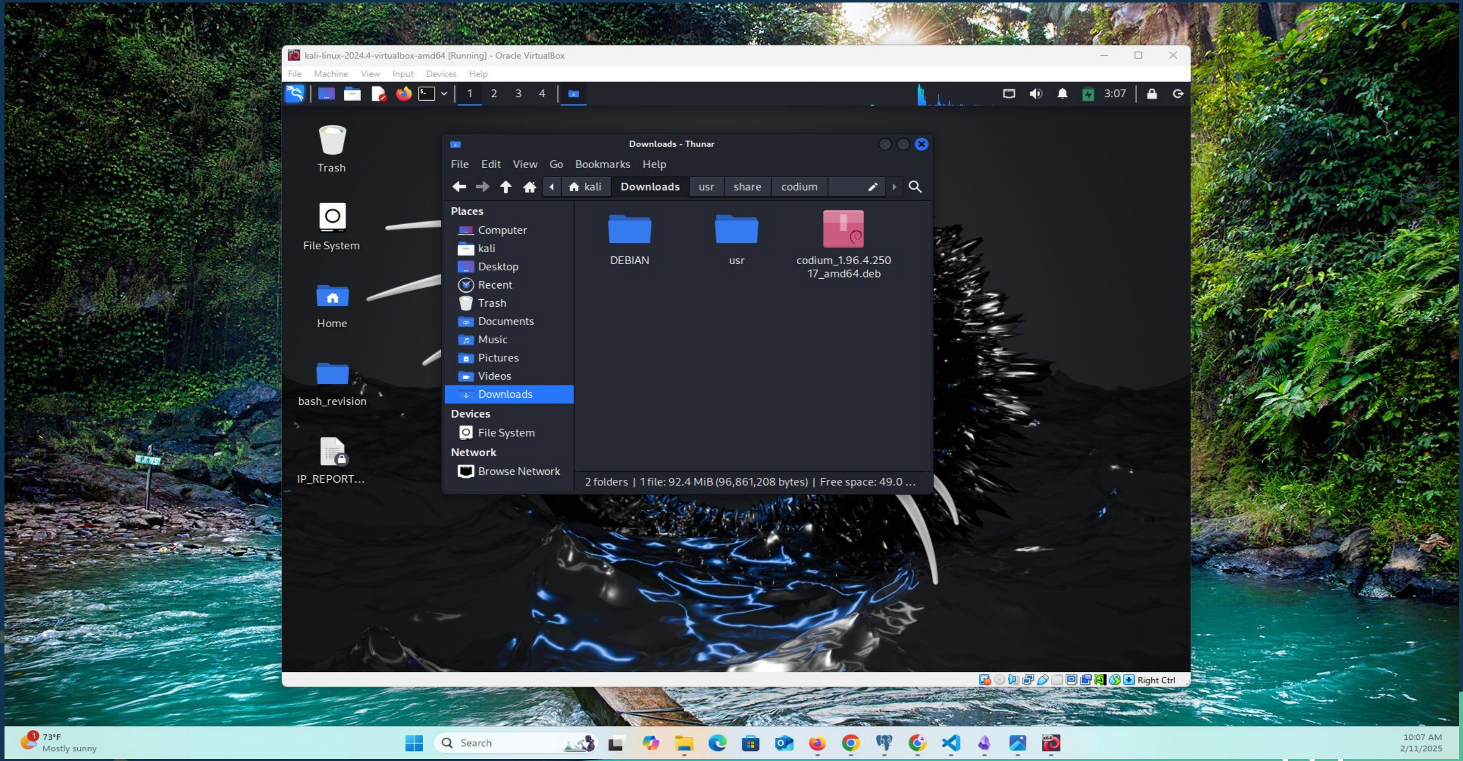
HyperionDev

Safety in Handling Malware

Key Tips:

- Use isolated environments (e.g., virtual machines).
- Disable shared folders and network access.
- Never analyze malware on a production system.

Isolated Environment



kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox

Downloads - Thunar

2 folders | 1 file: 92.4 MiB (96,861,208 bytes) | Free space: 49.0 ...

Wrap Up

Key Takeaways:

- Understand static vs. dynamic analysis.
- Use the right tools for the job.
- Always prioritize safety

Polls

Please have a look at the poll notification and select an option.

What is the MOST important safety measure when analyzing malware?

A. Using a virtual machine or sandbox
B. Running malware on your personal computer
C. Sharing malware samples with colleagues
D. Ignoring network isolation

Polls

Please have a look at the poll notification and select an option.

Which tool is BEST suited for static analysis of malware?

A. Cuckoo Sandbox
B. Wireshark
C. Firewall
D. Hex Editor

HyperionDev

Q & A SECTION

Please use this time to ask any questions relating to the topic, should you have any.

Thank you for attending

HyperionDev