



 Vue Hexa 2
  Vue Hexa 3
  Vue Hexa 4
  Vue Hexa 5
  Watch 1
  Locals
  Struct

"î ÷ |ý"

point d'arrêt « entry breakpoint » à <lab09-01.EntryPoint> (00403896) !



# What is Malware Analysis?

- Malware analysis is the process of understanding the behavior and purpose of malicious files, applications, or suspicious executables.
- Effective analysis allows for uncovering hidden indicators of compromise (IOCs), triage of incidents, improving threat alerts and detection, and provide additional context into the latest exploits and defense evasion techniques.



# Project Goals

- Assumes a complete beginner mindset into the world of malware investigation and analysis.
- **Overall Goal:** To enhance overall comprehension and provide exposure to malware infection techniques and popular tools used by security practitioners to aid in malware analysis.
- **Sub-Goals:**
  1. Learn the basics of malware infection tactics and common indicators of compromise (IOCs).
  2. Learn the foundations of basic static and dynamic malware analysis techniques.
  3. Investigate historical samples of malware with the help of written guides if necessary.

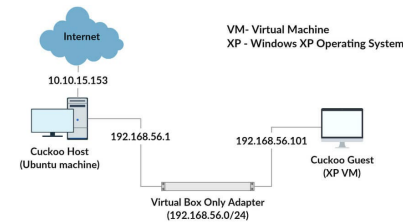


<https://cybercademy.org/the-malware-analysis-project-101>



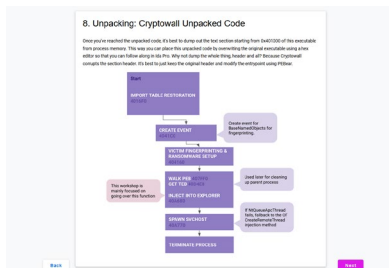
## Step 1: Practical Malware Analysis by Matt Kiely

Used as the foundational training program to learn the basics of malware, analysis techniques, deploying an isolated malware lab, and tools used in malware investigation. Taught by Matt Kiely (HuskyHacks) on TCM Academy, who is a security practitioner with 10 years of experience in IT and cybersecurity.



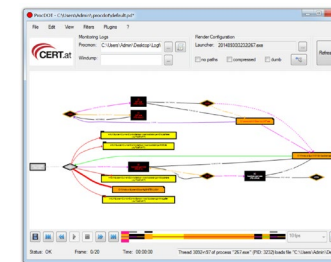
## Step 2: Create an Isolated Malware Lab Environment

Deploy an isolated malware lab environments through self-hosted virtual machines using Virtualbox and cloud-provisioned EC2 instances in AWS and Terraform. An isolated lab environment will provide a means of safely investigating malicious executables and programs.



### Step 3: Malware Analysis CTFs

Practice malware analysis by playing CTFs. Using MalwareUnicorn, play the PE Injection Study and MacOS DyLib Injection CTFs. And more!

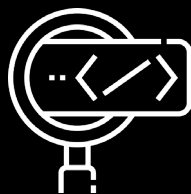


### Step 4: Investigate Live Malware Samples

Investigate live malware samples and create write-ups on findings. Using theZoo Live Malware Repository or vx-underground.org, install malicious programs and use malware analysis tools to collect artifacts. Write findings in a report. Use other write-ups if necessary.



# Analysis Techniques

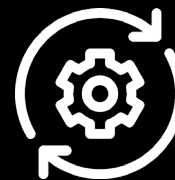


## Static

Does not require the code, program, or executable to run.

Examines for signs of malicious contents, including strings, file names, hashes, domains, IP addresses, and file header data.

## Hybrid



## Dynamic

The code, program, or executable in question is run in real-time.

Examines what happens when malware is executed. Provides more detail into how the malware operates.

# Tools

**There are many different free and commercial tools offered for static and dynamic malware analysis.**



## **FlareVM**

A collection of software installations scripts for Windows systems that allows you to easily setup and maintain a reverse engineering environment on a virtual machine (VM).



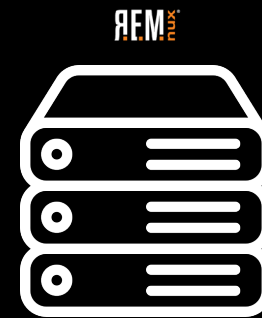
## **Remnux**

A Linux distribution for Malware Analysis. REMnux provides a curated collection of free tools created by the community. Used to investigate malware without having to find, install, and configure the tools. One of Remnux's many use cases is to be used as C2 server simulation to understand which URLs and malicious domains are probed when malware has been denoted.

# Topology






Virtual Machine



C2 Server



# Project Schedule

- Video #1: Project Launch! 
- Video #2: Setting up a Malware Analysis Lab
  -  Self-hosted Lab
  -  Cloud-hosted
- Video #3: Malware Analysis Crash Course – Analyzing a Banking Trojan



# Step 1: Practical Malware Analysis



Practical Malware Analysis By Matt Kiely

📢 Huge Shoutout!

# Warning & Disclaimers

- Safety is key when dealing with malware. Ensure you always are following protocols when it comes to downloading and detonating a malicious sample. Follow all instructions within the courses and listed resources.
- Disclaimers:
  1. I take no responsibility or accountability for infection of malicious software, programs, files onto any computer or workstation.
  2. This project and videos are for educational purposes only. I do not condone the development, use of, or spreading of programs to intentionally harm assets, networks, or individuals.