Lab Assignment



Cybersecurity Professional Program

Digital Forensics &
Incident Response

# Incident Response Implementation

## DFIR-03-L2
## Containing an Attack

## Lab Objectives

Learn how to contain a program that is spreading infection or presumably being controlled by an intruder.

## Lab Mission

Learn how to *unplug* an infected virtual machine (VM), understand the concept of *air gapping*, and discuss its benefits and limitations.

## Lab Duration

10–20 minutes

## Requirements

- Basic knowledge of virtual machines and hypervisors

## Resources

- Environment & Tools
    - VirtualBox
    - Windows 10 FLARE

## Textbook References

- Chapter 3: Incident Response Implementation
    - Section 3: Containment

# Lab Task: Air Gapping

Take a virtual machine that is presumably infected and discover how to isolate it.

1. Start the FLARE VM.
2. Run a continuous ***ping*** to ***www.google.com***
3. Disconnect the VM network adapter.
4. Discuss with others if *disconnecting* (*air gapping*) the network is sufficient for isolation.

# Hints

## Lab Task

- Use the –***t*** flag for a continuous ***ping***.
- Disconnect the network adapter by clicking the VM's *network* icon.
- Search the internet for options to overcome air-gapped networks.