**Cybersecurity 401**

**Module 7 - Threat Hunting**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

## **Lab 33 - Threat Hunting with Zeek, RITA**

## 

**| Rodrigo Brasil 12/2023 |**

## Part 1: Staging

The lab today utilizes the following tools:

* Wireshark
* tshark
* Zeek
* Rita
* LibreOffice Calc

Use the Rita VM provided which already has Zeek and Rita installed for you.

## Part 2: Active Countermeasures Labs

Complete all four of the [Active Countermeasures Threat Hunting Labs.](https://activecm.github.io/threat-hunting-labs/)

Take notes as you work through the AC lab segments. Document your experiences in your submission today.