**Cybersecurity 401**

**Module 3 - Security Operations**

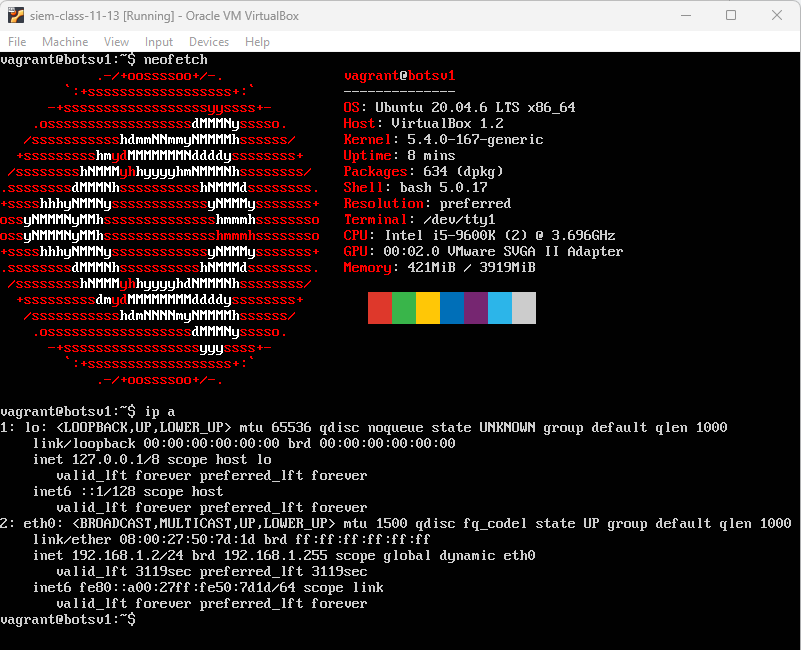
**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

# **Lab 13 - Reconstructing a Cloud Attack Using Log Data**

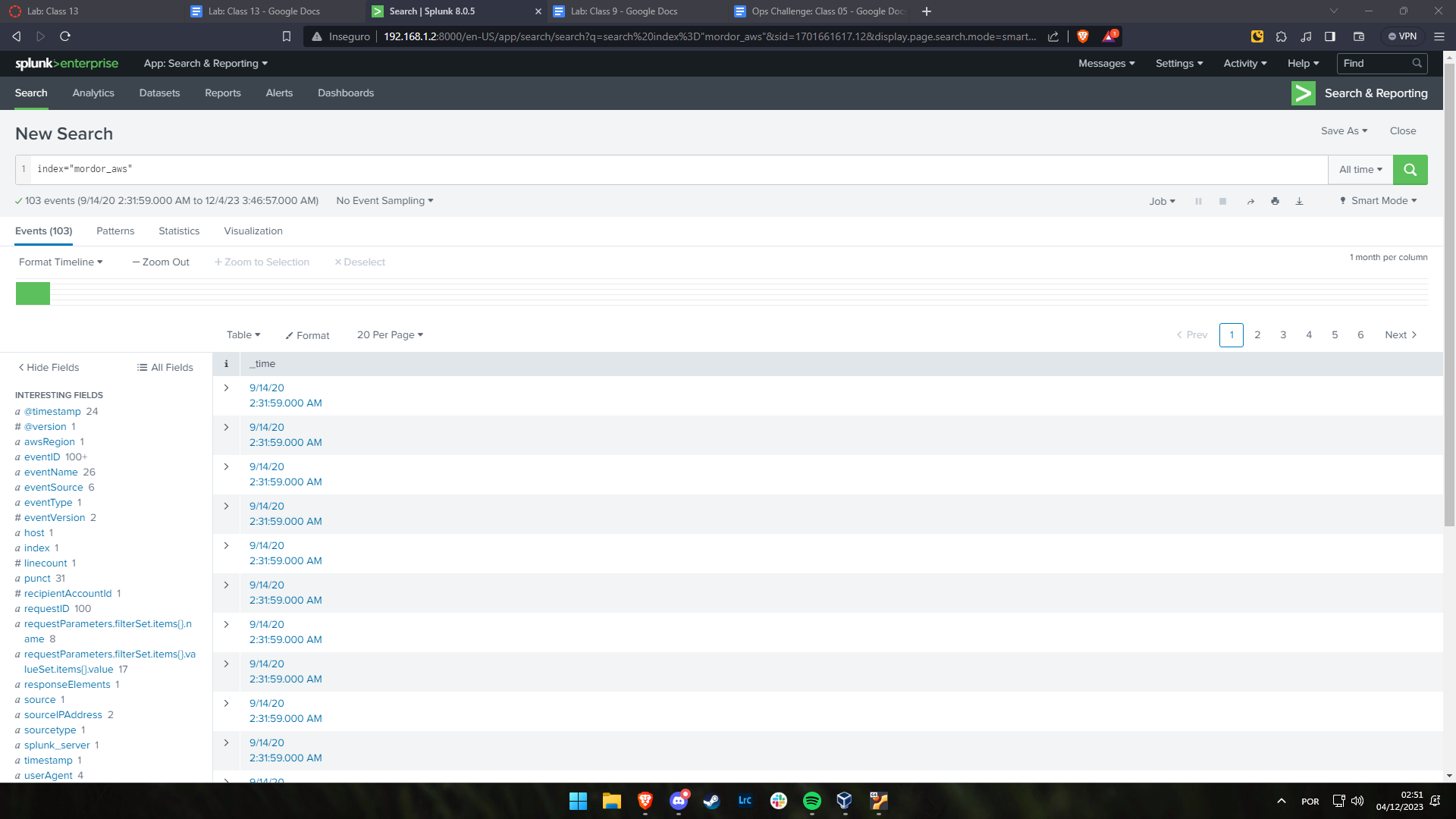
# 

**| Rodrigo Brasil 11/2023 |**

## **Part 1: Staging**

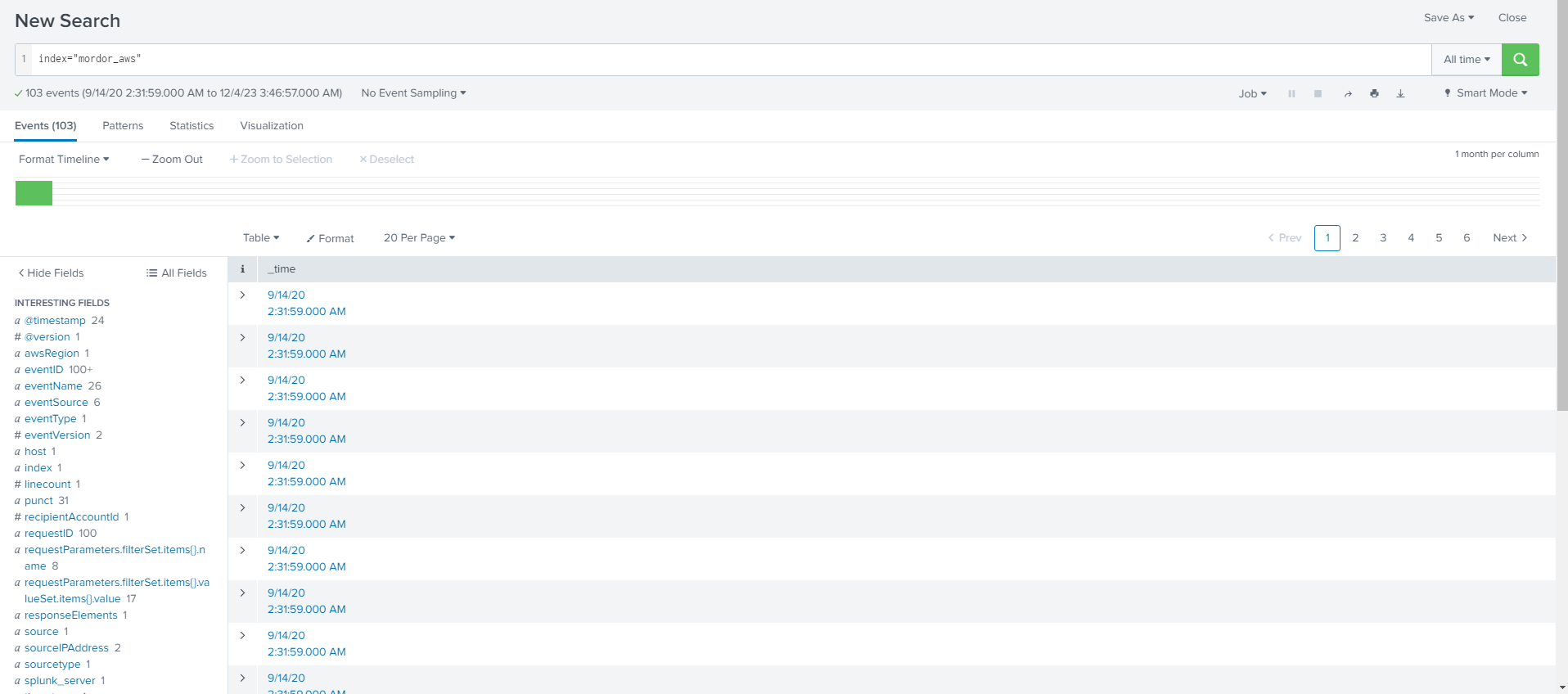
****

Splunk (ubuntu) VM deployed with the IP **192.168.1.2**



Splunk running on my host machine

## **Part 2: Log Analysis**



### Evidence

#### TA0001

#### TA0003

#### TA0004

#### TA0005

#### TA0009

## 

## **Part 3: Reporting**

* Summarize in your own words how the attacker was able to exfiltrate data from the S3 bucket. Be sure to include:
  + When did the attack take place?
  + How was the attacker interacting with AWS?
  + Did you find any information about the attacker/attack origin?