**Cybersecurity 401**

**Module 3 - Security Operations**

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

# **Read 16 - Cloud Identity and Access Management (IAM) with AWS**

# 

**| Rodrigo Brasil 12/2023 |**

1. **What were the three commands used for the attack?**
   1. The three commands used were: Get Credentials, List Buckets and Download Files
2. **What misconfiguration of AWS components allowed the attacker to access sensitive data?**
   1. The IAM roles had excessive permissions so after getting temporary credentials to one, the attacker was able to see the s3 buckets
3. **What are two of the AWS Governance practices that could have prevented such attack?**
   1. Ensure each application, EC2 instance, or autoscaling group has its own IAM role.
   2. Use CloudTrail, CloudWatch, and/or AWS lambda services to review and automate specific actions taken on S3 resources.