Attack, Detect & Secure the Environment (AWS)

Student Name: Sanjana Thawait

College: Rungta College of Engineering and Technology

B.Tech CSE Cyber Security

ERP: 6604710

5TH SEM MAJOR PROJECT

ABSTRACT

Cloud computing environments are increasingly targeted by cyber attackers due to their public accessibility. This project implements a cloud-based security monitoring solution using Amazon Web Services (AWS). Unauthorized SSH login attempts are simulated on an EC2 instance, and authentication logs are collected using AWS CloudWatch Agent. These logs are analyzed using AWS CloudWatch Logs acting as a SIEM platform. The project demonstrates attack detection, centralized logging, and practical SIEM implementation

1. INTRODUCTION

Cloud computing has become the backbone of modern IT infrastructure. Organizations rely on platforms such as Amazon Web Services (AWS) for scalable and cost-effective solutions. However, publicly accessible cloud servers are frequent targets of cyber-attacks. One of the most commonly targeted services is Secure Shell (SSH), which attackers exploit using brute-force techniques. Security Information and Event Management (SIEM) systems help detect such threats by collecting and analyzing logs. AWS CloudWatch provides native monitoring capabilities that can be used as a lightweight SIEM solution. This project demonstrates real-world attack simulation and detection using AWS CloudWatch.

2. OBJECTIVES OF THE PROJECT

The primary objective of this project is to design and implement a cloud-based monitoring solution capable of detecting unauthorized access attempts. The project simulates SSH attacks, configures CloudWatch Agent

for log collection, and analyzes logs using AWS CloudWatch. The project bridges theoretical security concepts with practical cloud implementation.

3. TOOLS AND TECHNOLOGIES USED

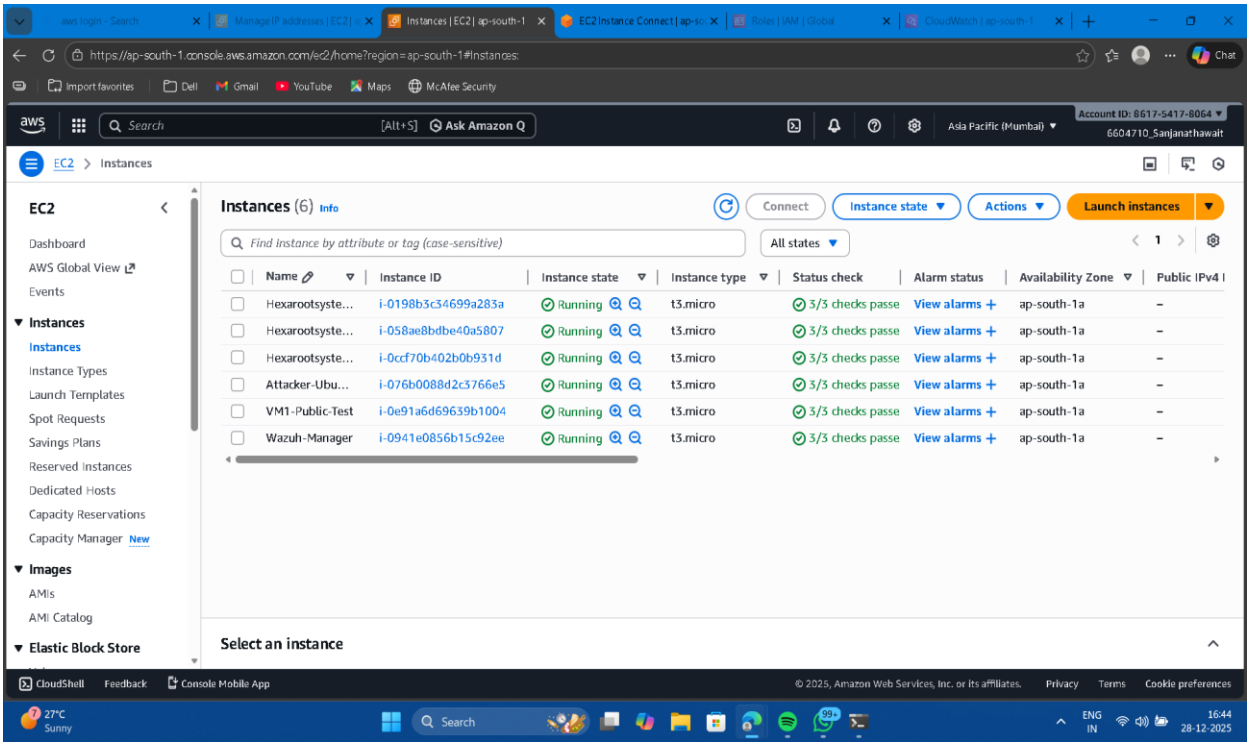
1.Amazon Web Services (AWS):
AWS provides the cloud infrastructure used in this project. It enables the deployment of virtual machines, monitoring services, and secure access control. AWS allows simulation of real-world attack scenarios in a controlled environment.

2. Amazon EC2:
EC2 is used to deploy attacker and victim virtual machines. The victim instance runs the SSH service and generates authentication logs, while the attacker instance simulates unauthorized access attempts.

3. AWS IAM:
IAM is used to manage permissions securely. An IAM role is attached to the EC2 instance to allow CloudWatch Agent to send logs to CloudWatch without exposing credentials.

4. **AWS CloudWatch:**
   CloudWatch acts as the SIEM platform. It collects, stores, and displays authentication logs in log groups and log streams, enabling centralized monitoring and attack detection.
5. **CloudWatch Agent:**
   The agent runs on the victim EC2 instance and forwards system logs such as `/var/log/auth.log` to CloudWatch in near real time.
6. **Ubuntu Linux:**
   Ubuntu is used as the victim operating system. It generates SSH authentication logs whenever login attempts occur.
7. **SSH:**
   SSH is the target service. Failed login attempts are used as indicators of attack activity.

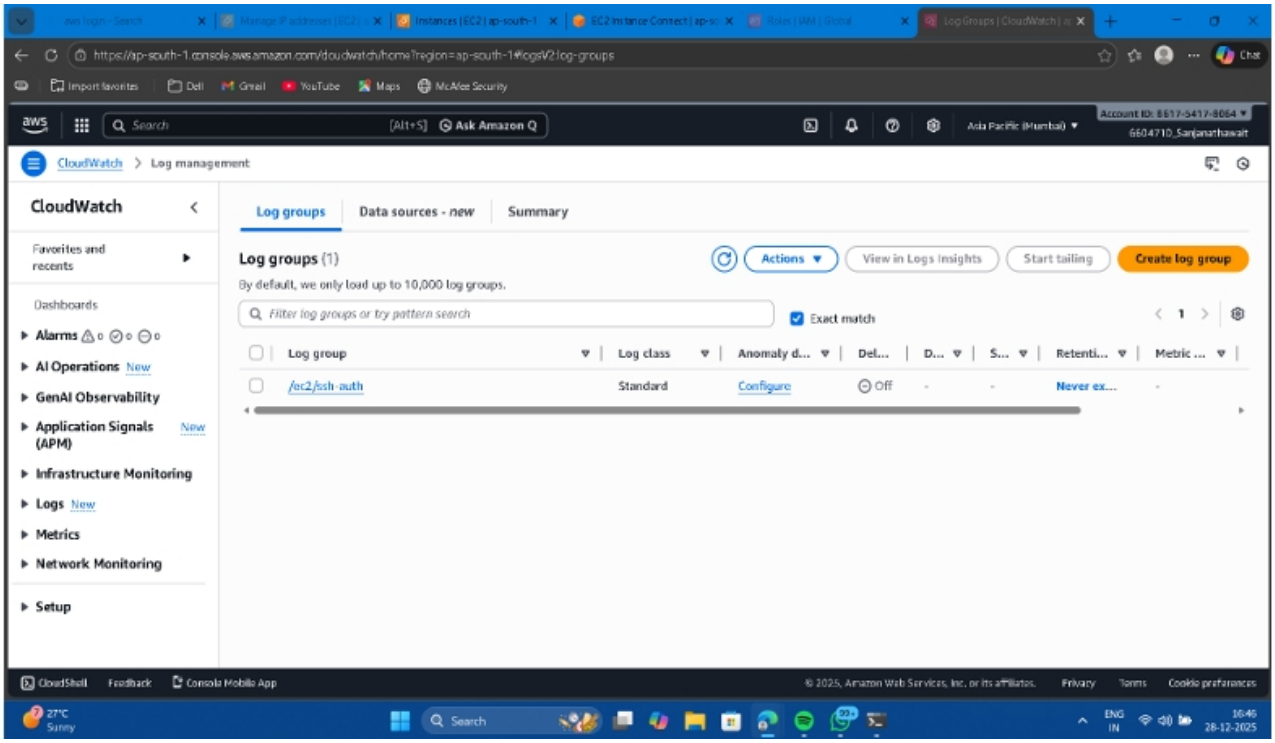
4. Screenshot-wise Explanation



EC2 Instances Overview

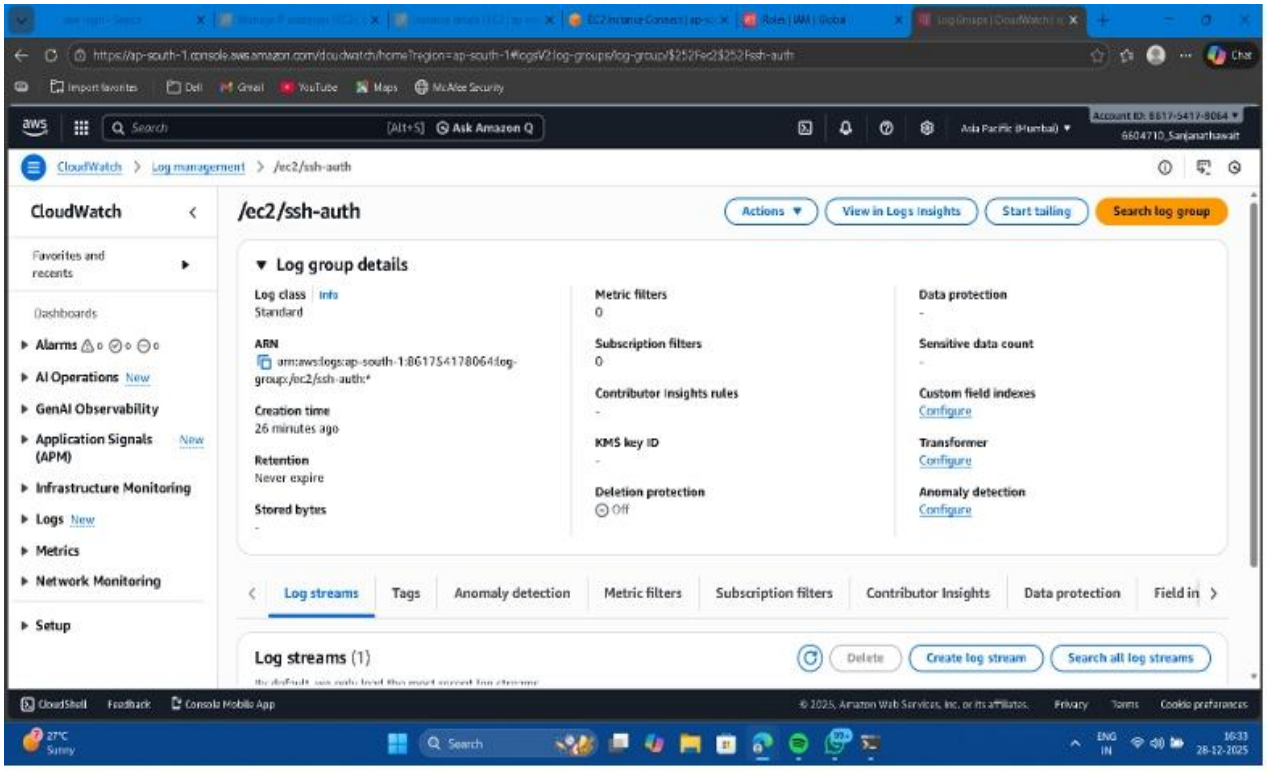
This screenshot shows multiple EC2 instances running in the AWS Mumbai region. It includes the attacker machine, victim machine, and Wazuh manager instance. This setup forms the foundation of the cloud security lab environment

Attack Simulation from Attacker VM



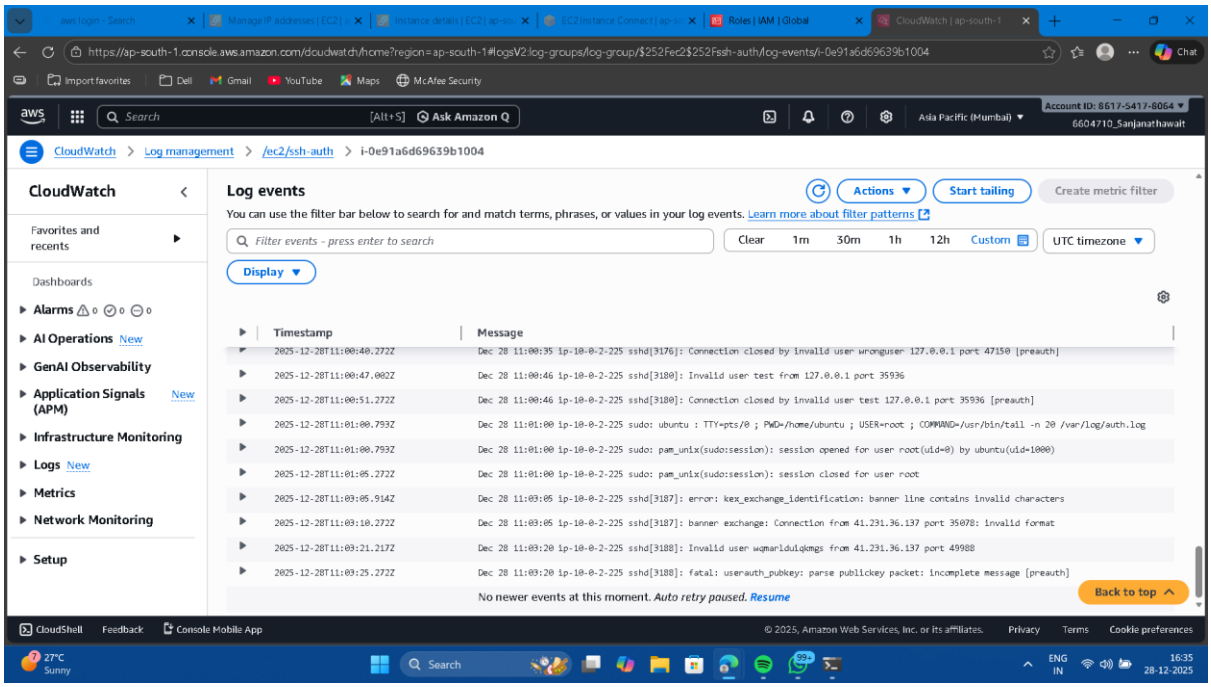
This screenshot demonstrates SSH attack attempts initiated from the attacker virtual machine. Multiple invalid login attempts are generated to simulate a brute-force attack scenario.

CloudWatch Log Group Creation



This screenshot shows the creation of the CloudWatch log group '/ec2/ssh-auth'. The log group stores authentication logs collected from the victim EC2 instance

SSH Authentication Logs in CloudWatch



This screenshot displays SSH authentication logs in CloudWatch. Events such as invalid users, failed login attempts, and connection resets are visible, confirming successful attack detection.

5. Conclusion

This project successfully demonstrates the implementation of a cloud-based SIEM solution using AWS CloudWatch. By simulating real-world SSH attacks and analyzing authentication logs, the project highlights the importance of centralized logging and continuous monitoring in cloud environments. The results confirm that AWS CloudWatch can effectively detect unauthorized access attempts and provide valuable security insights. This project enhances practical understanding of cloud security concepts and prepares students for real-world cybersecurity challenges

6. FUTURE SCOPE

Future enhancements of this project include configuring automated alerts using CloudWatch Alarms, integrating AWS GuardDuty for advanced threat detection, and implementing automated incident response using AWS Lambda. The project can also be extended by integrating enterprise-grade SIEM tools such as Wazuh or ELK Stack for large-scale environments.