Title: Analysis and Mitigation of SSH Misconfiguration in Cloud Environment using AWS
Submitted by: Bhavesh verma
Semester:5th

Course: Certified Ethical Hacking

Date: 25 dec 2025

Abstract

This project focuses on identifying, analyzing, and mitigating a common cloud security misconfiguration related to unrestricted SSH access. An AWS cloud environment was created using EC2 and VPC services. A security group was intentionally misconfigured to allow SSH access from the internet. AWS CloudTrail was enabled for monitoring and logging. The issue was later mitigated by restricting SSH access to a specific IP address.

INTRODUCTION

Cloud computing provides scalable and flexible infrastructure but also introduces security challenges if not configured properly. One of the most common cloud security issues is misconfigured network access rules. This project demonstrates how unrestricted SSH access can expose cloud servers to attacks and how such risks can be mitigated.

PROBLEM STATEMENT

The problem addressed in this project is a misconfigured security group that allows unrestricted SSH (port 22) access from the internet.Such configuration can lead to brute-force attacks and unauthorized access to cloud servers.

CLOUD ARCHITECTURE

The cloud architecture consists of an AWS VPC with a public subnet, an EC2 instance running Ubuntu Linux, and a security group controlling inbound traffic. The EC2 instance hosts a web server and is accessible through a public IP address.

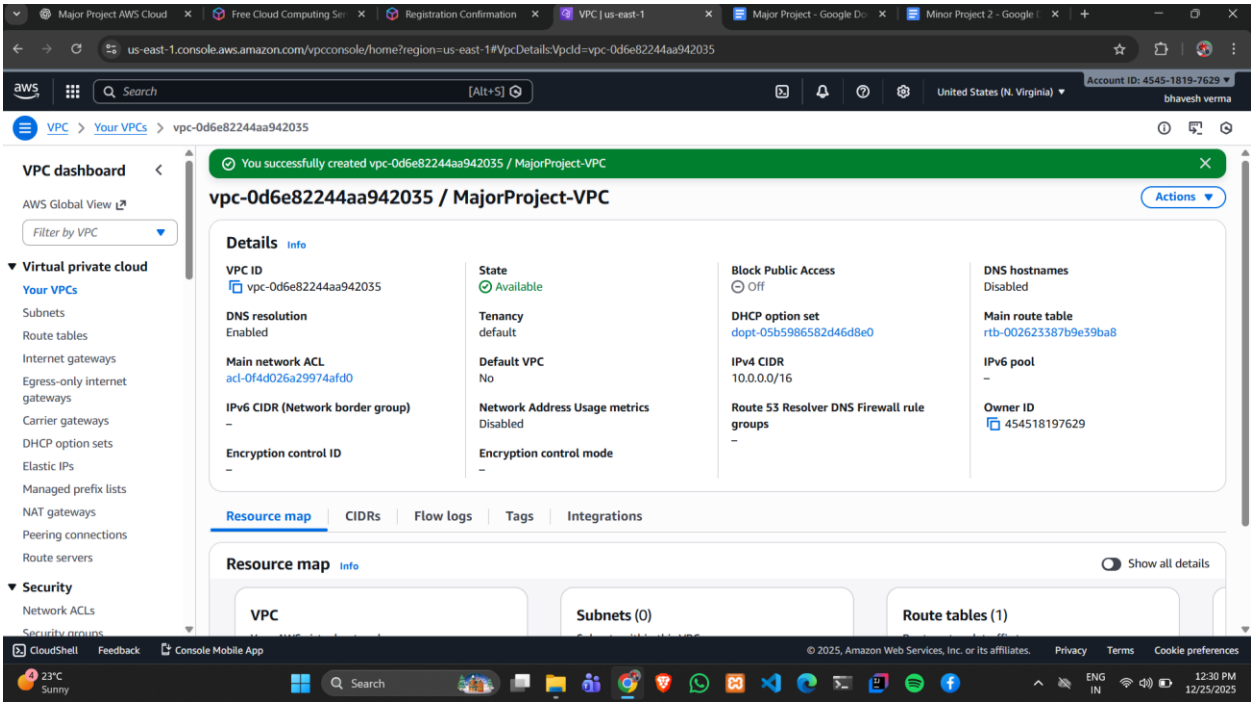


Figure 1: AWS VPC architecture with public subnet

IMPLEMENTATION DETAILS

An EC2 instance was launched in a public subnet using Ubuntu Server.

A security group was created with inbound rules allowing SSH and HTTP traffic.

Apache web server was installed on the EC2 instance to verify public access.

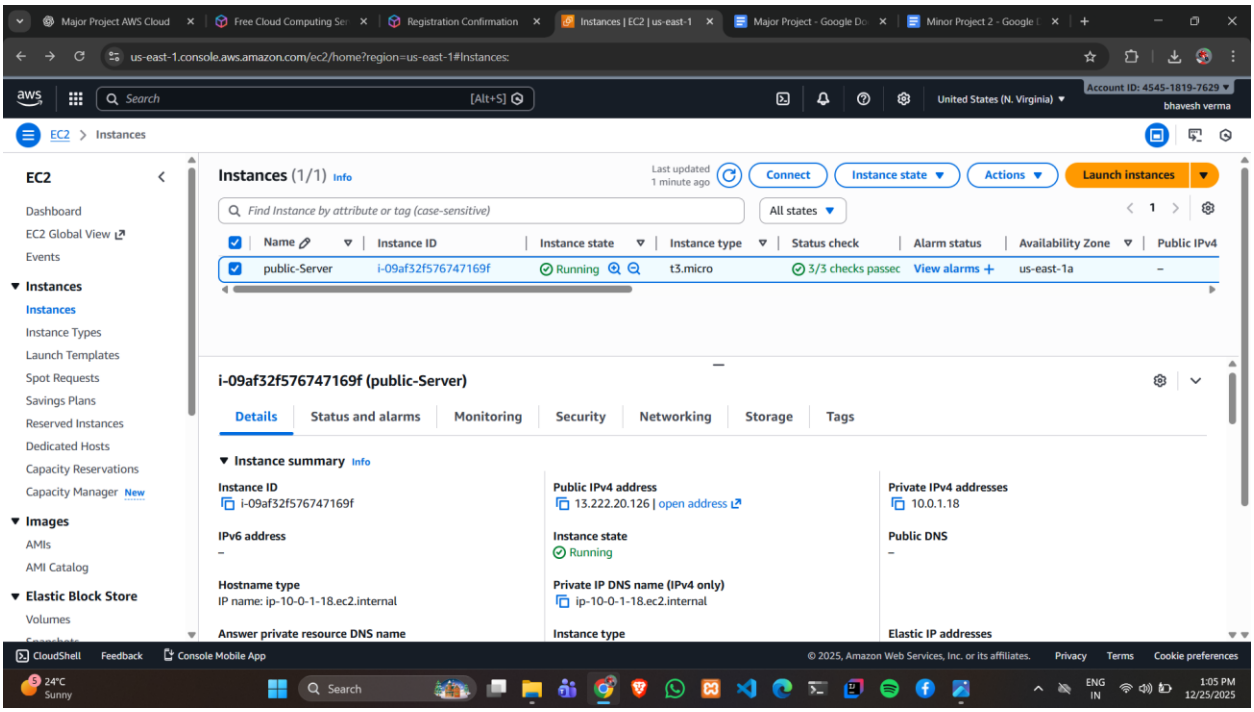
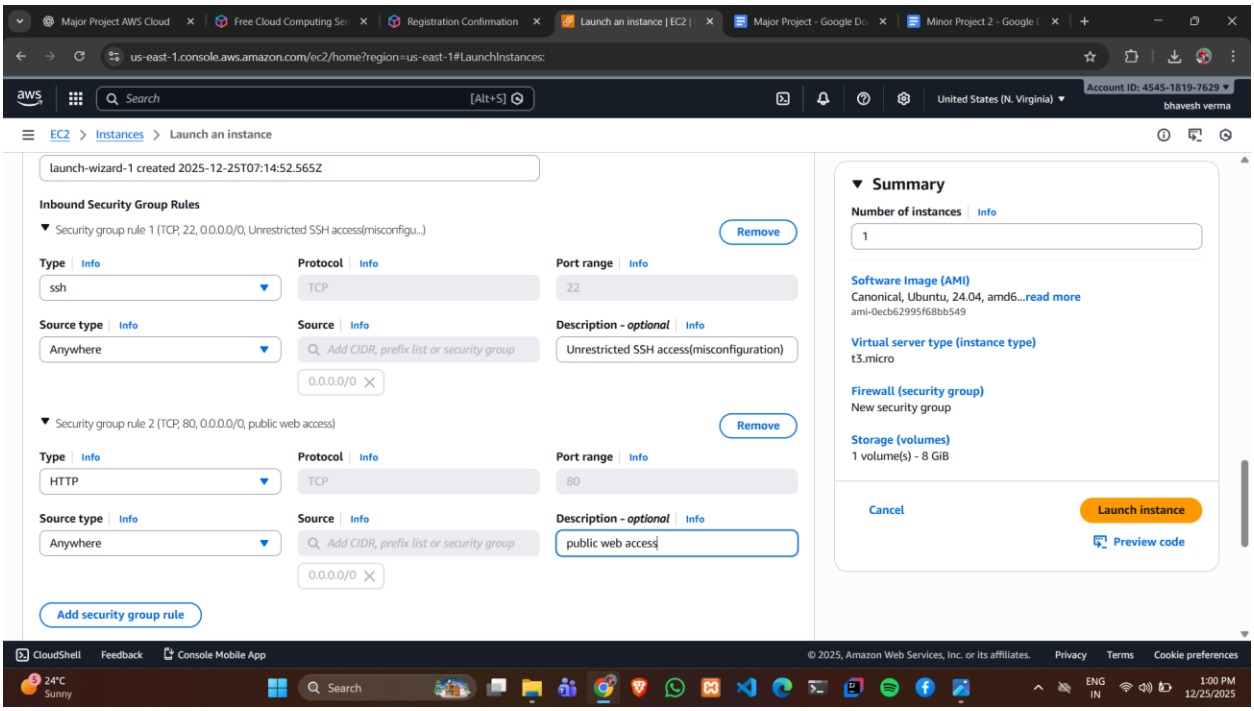


Figure 2: EC2 instance running with public IP address

ATTACK SIMULATION (NO REAL ATTACK)

No real attack was performed due to ethical and legal considerations. The attack was simulated by intentionally misconfiguring the security group to allow SSH access from anywhere (0.0.0.0/0), which represents a real-world attack surface for brute-force SSH login attempts.



Security Group – SSH 0.0.0.0/0 (Before Fix)

Figure 3: Misconfigured security group allowing unrestricted SSH access

---

SERVICE DEPLOYMENT VERIFICATION

Apache web server was installed and successfully accessed through the public IP address of the EC2 instance, confirming that the server was publicly reachable due to open inbound rules.

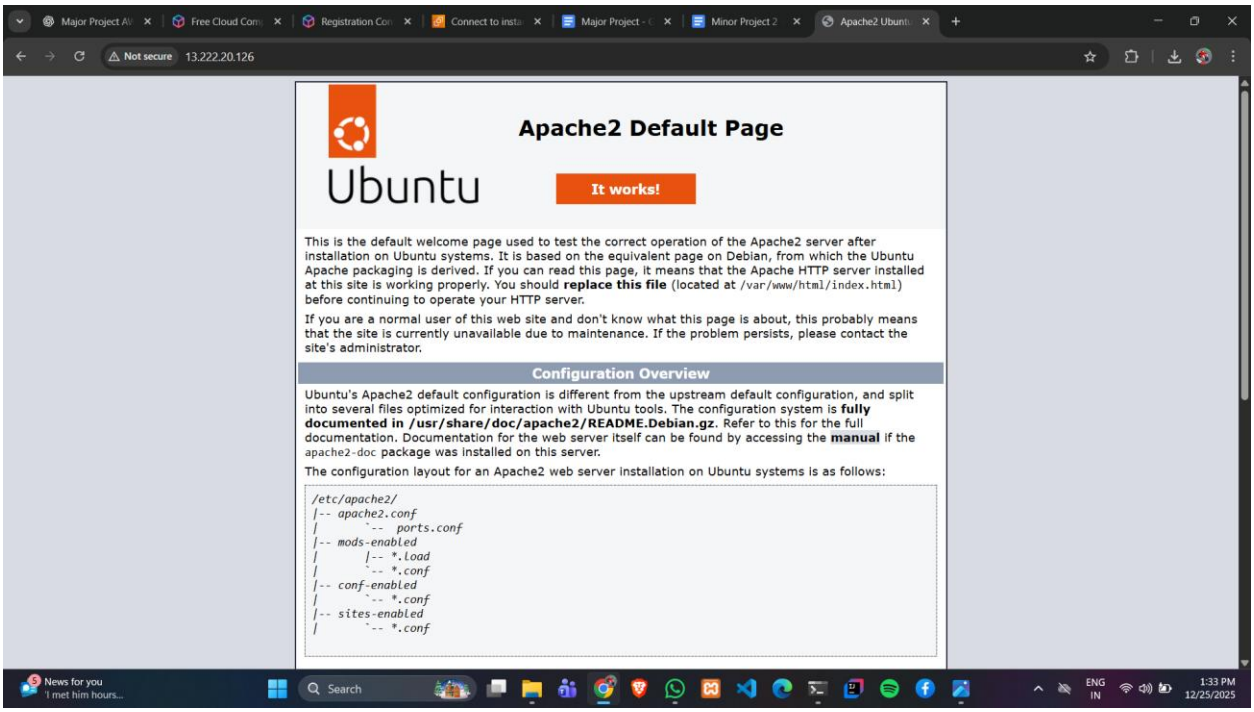


Figure 4: Publicly accessible web server running on EC2 instance

---

DETECTION AND LOGGING

AWS CloudTrail was enabled as a multi-region trail to monitor and log all management events.Any unauthorized access attempts or configuration changes would be recorded for analysis.

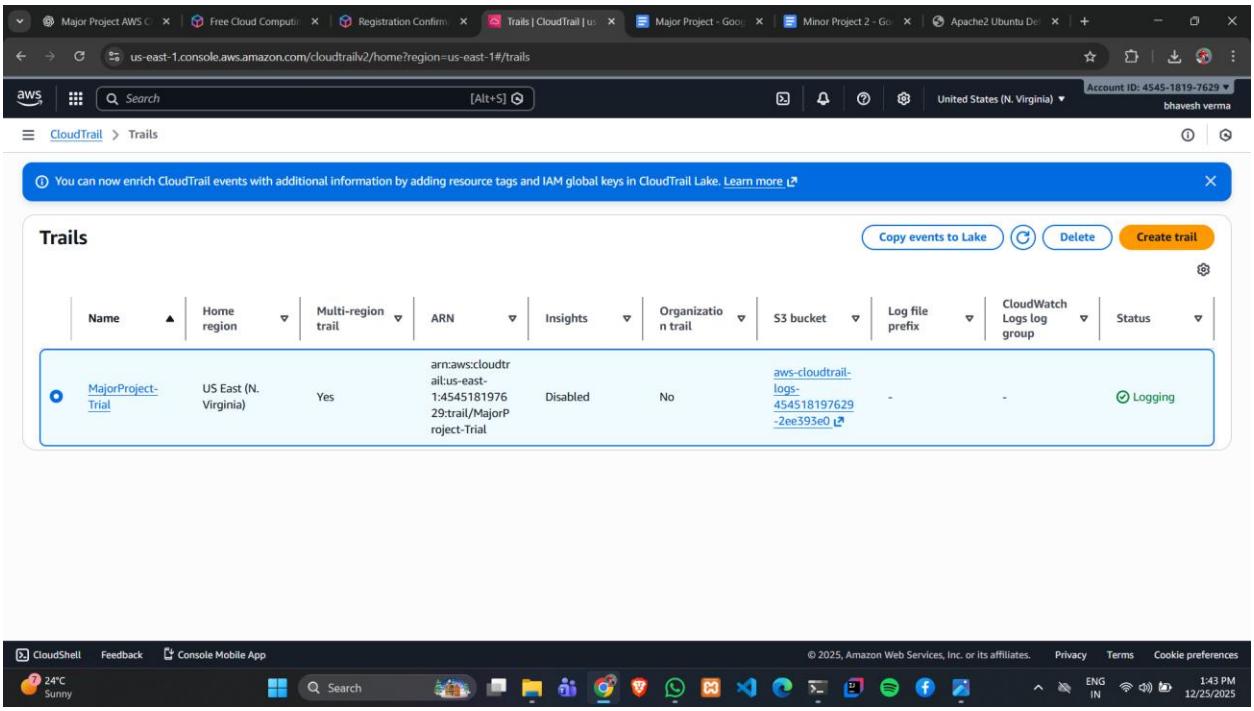


Figure 5: AWS CloudTrail enabled with multi-region logging

🔟 MITIGATION / SOLUTION

To mitigate the identified vulnerability, SSH access was restricted to the administrator's IP address.This ensured that only authorized users could access the server, eliminating the risk of external brute-force attacks.

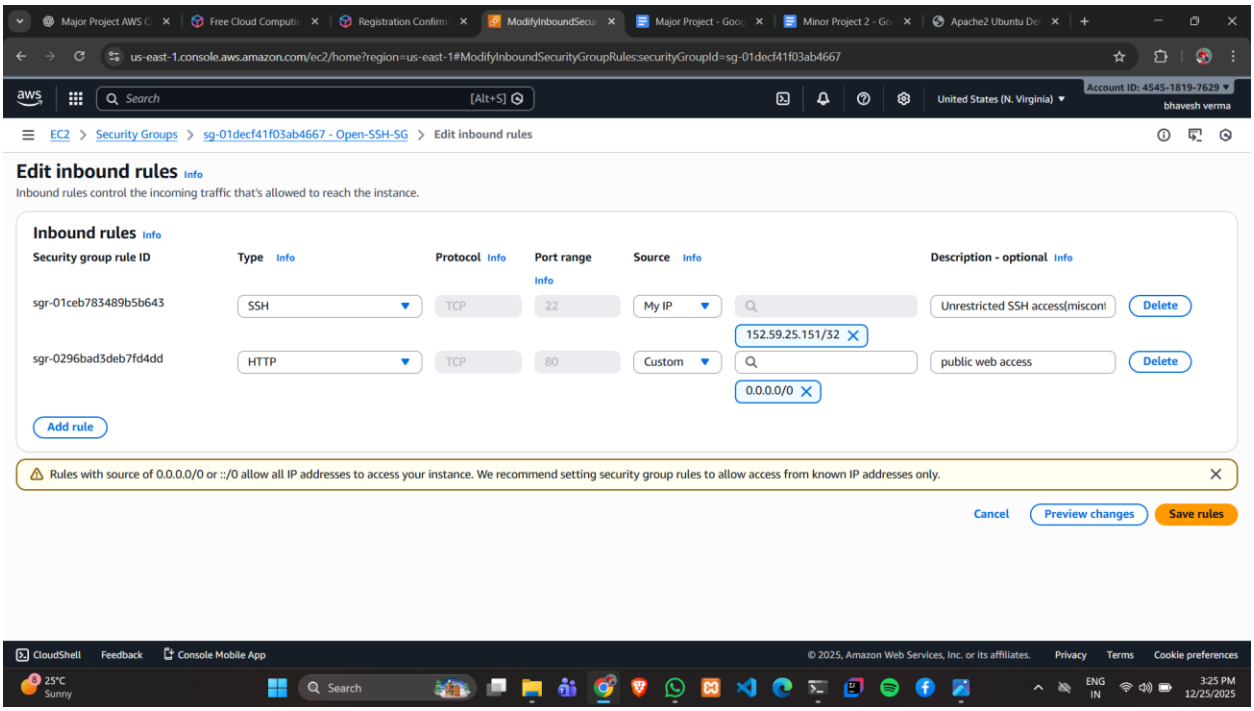


Figure 6: SSH access restricted to administrator IP as a mitigation step

---

CONCLUSION

This project demonstrated how simple cloud misconfigurations can expose systems to security risks.By identifying the vulnerability, enabling logging, and applying proper mitigation techniques,the cloud environment was secured following best security practices.