Cloud Security Fundamentals Project

Kobe Narcisse

The purpose of this project was to gain hands-on experience with cloud security fundamentals using Amazon Web Services (AWS). The primary goal was to design and deploy a secure cloud environment while following industry best practices related to identity management, network security, and audit logging. This project simulates real-world tasks commonly performed by cloud security analysts and cybersecurity professionals, while remaining within the AWS free tier.

The cloud environment was built within an AWS Virtual Private Cloud (VPC) to provide isolation from the public internet and to establish controlled network boundaries. A public subnet was created inside the VPC to host an EC2 instance running Amazon Linux. This instance functioned as a basic web server using the Apache HTTP service and was assigned a public IP address to allow external access. The network design demonstrated an understanding of cloud segmentation and secure infrastructure planning.

Access to the EC2 instance was controlled using AWS Security Groups, which act as stateful firewalls. Inbound rules were configured to allow HTTP traffic on port 80 from any IP address so that the website could be publicly accessible. Administrative access via SSH on port 22 was restricted to a specific trusted IP address to reduce the risk of unauthorized access and brute-force attacks. This approach followed the principle of minimizing the attack surface while maintaining required functionality.

Identity and access management was handled using AWS IAM. Separate IAM users were created to enforce least-privilege access. An administrative user was used for deployment purposes, while an auditor user was created with read-only permissions to review configurations without the ability to modify resources. Multi-factor authentication was enabled to provide an additional layer of security and protect against credential compromise.

Audit logging was implemented using AWS CloudTrail to record account activity and API calls across the environment. Logs were stored securely in an Amazon S3 bucket using server-side encryption. This logging capability allows for visibility into user actions and supports incident investigation and compliance monitoring. Enabling CloudTrail reinforced the importance of accountability and monitoring in cloud security environments.

As part of the learning process, common cloud security misconfigurations were intentionally introduced and remediated. One example included temporarily allowing SSH access from all IP addresses, which represents a significant security risk. This misconfiguration was identified, analyzed, and corrected by restricting SSH access to a trusted IP range. Another example involved overly permissive IAM permissions, which were reviewed and adjusted to align with least-privilege principles. These exercises emphasized the importance of continuous security assessment and remediation.

Overall, this project strengthened practical knowledge of cloud security fundamentals, including network segmentation, access control, and audit logging. The project successfully demonstrates foundational cloud security skills relevant to cybersecurity and cloud security internship roles.