**Step 1: Problem Statement**

**Problem Statement**

Cloud environments, while flexible and scalable, are increasingly targeted by attackers due to misconfigurations, overly permissive access, and lack of monitoring. Many organizations fail to implement secure architecture from the ground up, especially in development or small-scale environments using free-tier services like AWS. This project addresses how to build a secure-by-default AWS cloud architecture using Infrastructure as Code (Terraform), even within the limitations of the free tier.

**Step 2: Project Objectives**

**Objectives**

* Design and implement a secure Virtual Private Cloud (VPC) using AWS and Terraform.
* Define and enforce network boundaries using **subnets, route tables, internet gateways, and NATs**.
* Apply the **principle of least privilege** via IAM roles and policies.
* Configure **strict ingress and egress rules** using security groups and NACLs.
* Harden an EC2 instance via bootstrap scripting (instance\_setup.sh).
* Enable **CloudTrail** and **VPC flow logs** to monitor activity and detect anomalies.
* Automate deployment and change management using **GitHub Actions**.

**Step 3: Project Scope**

**In-Scope:**

* Terraform provisioning of AWS infrastructure (VPC, EC2, SGs, etc.)
* EC2 configuration with hardened SSH
* IAM least-privilege policy examples
* Security group rule definition
* Logging setup (VPC Flow Logs + CloudTrail)
* GitHub Actions for CI/CD validation
* Documentation and architecture diagram

**Out-of-Scope:**

* Multi-region HA architecture
* Advanced intrusion detection systems (e.g., GuardDuty)
* Paid services beyond AWS Free Tier (e.g., premium CloudWatch)

**Next Steps: File Content Plan**

| **File** | **Purpose** |
| --- | --- |
| README.md | Overview, features, architecture, how to use |
| terraform/main.tf | Core resources (VPC, subnets, EC2, etc.) |
| terraform/variables.tf | Inputs for modularity |
| terraform/outputs.tf | Key outputs (e.g., public IP, VPC ID) |
| terraform/provider.tf | AWS provider config |
| scripts/instance\_setup.sh | Harden EC2 setup (e.g., disable root login, install updates) |
| security/security\_group\_rules.txt | Document rule intent (why 22 is open, for example) |
| security/iam\_policy\_least\_privilege.json | Custom IAM policy definition |
| logs-monitoring/cloudtrail\_setup.md | Instructions or Terraform for enabling logging |
| documentation/setup\_steps.md | Step-by-step guide to deploy everything |
| documentation/risk\_assessment.md | Potential vulnerabilities + mitigations |
| documentation/test\_report.md | Manual tests and results (e.g., port scan results) |