Cloud DDoS Simulation & Mitigation Report

Introduction

This report documents a controlled DDoS simulation to test the resilience of a cloud-hosted web application and evaluate the effectiveness of native DDoS mitigation tools provided by the cloud provider. The test was designed to ensure compliance with ethical guidelines and acceptable use policies.

Test Environment Setup

A basic static HTML page was hosted on an AWS EC2 instance using Apache HTTP Server. Baseline metrics such as average response time (~100ms) and uptime (100%) were monitored using AWS CloudWatch.

DDoS Simulation Details

The attack was simulated using the hping3 tool from a separate VM in the same VPC. Traffic consisted of SYN flood packets over a 5-minute window at a low-impact level. The test was carefully monitored to ensure minimal disruption and stayed within the terms of service.

Monitoring & Impact Observations

During the simulation, AWS CloudWatch showed increased CPU utilization and network in metrics. No service crash was observed, but response time increased by 60-80ms. AWS Shield Standard provided automatic protection, absorbing the traffic without requiring user intervention. No alerts were triggered due to the controlled scale.

Mitigation Strategies

In addition to AWS Shield, further protection could include:

- Web Application Firewall (AWS WAF): Filters malicious traffic based on rules.
- Rate Limiting: Limits the number of requests from a single IP.
- Geo-blocking: Prevents access from non-relevant regions.
- CDN Integration (e.g., CloudFront): Distributes traffic globally and absorbs spikes.
- Auto Scaling: Automatically adds more instances under heavy load.

Cloud DDoS Simulation & Mitigation Report

Conclusion

The simulation confirmed that AWS Shield Standard provides baseline protection against low-scale DDoS attacks. To handle larger or more complex threats, additional layers such as WAF, rate limiting, and CDN integration are recommended. A multi-layered security strategy enhances resilience and ensures application availability.