Project 2: Security Review and Hardening of an Existing AWS Environment

Detailed Report

Project Goal: Conduct a comprehensive security review and implement security enhancements in an existing AWS environment.

Guide

1. **Conduct Security Review:**
   - Use AWS Trusted Advisor to identify security gaps and generate reports.
2. **Fix Security Vulnerabilities:**
   - Review and adjust IAM roles and security groups.
   - Check S3 bucket encryption and security group settings.
3. **Implement MFA:**
   - Enable MFA for all IAM users to enhance security.
4. **Activate AWS GuardDuty:**
   - Set up GuardDuty for continuous monitoring and threat detection.
5. **Configure DDoS Protection:**
   - Implement AWS Shield and AWS WAF for protection against DDoS and web attacks.

Key Activities and Implementation:

1. **Security Review with AWS Trusted Advisor:**
   - Performed security checks with AWS Trusted Advisor.
   - Generated reports on security gaps and improvement suggestions.

```
bash
aws support describe-trusted-advisor-checks --language en
```

2. **Fix Security Vulnerabilities:**
   - Identified and reduced over-privileged IAM roles.
   - Addressed unencrypted S3 buckets and outbound connections in security groups.

```
bash
aws iam list-roles
aws s3api get-bucket-encryption --bucket my-bucket
aws ec2 describe-security-groups
```

3. **Implement Multi-Factor Authentication (MFA):**
   - Enabled MFA for all IAM users.

```
bash
aws iam enable-mfa-device --user-name Bob --serial-number
arn:aws:iam::123456789012:mfa/Bob --authentication-code-1 123456 --
authentication-code-2 654321
```

4. **Deploy AWS GuardDuty:**
   - Activated AWS GuardDuty for continuous monitoring and threat detection.

```
bash
```

```
aws guardduty create-detector --enable
```

5. **DDoS Protection:**
    - Configured AWS Shield and AWS WAF for protection against DDoS and web attacks.

```
bash
aws waf create-web-acl --name my-web-acl --metric-name myWebACL --
default-action Type=ALLOW --rules file://waf-rules.json
```

Result: Improved the security posture of the AWS environment, reduced risks, and increased resilience against attacks.