ShopNimbus Cloud Security Project

Week 3: IAM and Network Security Hardening

1. Project Context

This report summarizes the implementation of Identity and Access Management (IAM) and Network Security Hardening activities conducted within the Google Cloud project shopnimbus-security-group7. The goal was to enhance the project’s security posture by enforcing least-privilege access, restricting network exposure, enabling encryption, and ensuring effective logging and monitoring — in line with Google Cloud Platform (GCP) security best practices.

2. APIs and Services Enabled

Identity and Access Management (IAM API) – Role and permission management

Cloud Key Management Service (KMS API) – Encryption and key rotation

Cloud Logging API – Audit logging and system event tracking

Cloud Monitoring API – System monitoring and alert setup

Cloud Resource Manager API – Resource and policy administration

Cloud SQL, Cloud Storage, and Cloud Trace – Database, storage, and traceability services

Security Command Center API – Enabled but limited to organizational accounts

3. IAM Hardening

IAM hardening was achieved through the review and adjustment of project-level roles and permissions using Cloud Shell commands. The principle of least privilege was enforced so that users and service accounts were only assigned minimal access.

Command executed:

gcloud projects get-iam-policy $DEVSHELL\_PROJECT\_ID --format="table(bindings.role, bindings.members)"

This listed all members and roles, allowing identification of overly broad privileges such as roles/editor or roles/owner. Adjustments were made to align with least-privilege policies.

4. Network and Firewall Hardening

Firewall configurations were reviewed to detect publicly exposed ports or unrestricted inbound rules.

Command:

gcloud compute firewall-rules list --format="table(name, direction, sourceRanges, allowed)"

Findings revealed that some default rules (e.g., SSH access open to 0.0.0.0/0) could expose the project to threats. Rules were restricted to internal IP ranges to minimize exposure and enforce segmentation.

5. Logging and Audit Trail Configuration

Cloud Logging was enabled to track and audit IAM policy changes and system activity.

Command:

gcloud logging read "protoPayload.methodName=SetIamPolicy" --limit 10 --format="table(timestamp, resource.type, protoPayload.authenticationInfo.principalEmail)"

Audit logs confirmed tracking of IAM configuration changes, providing visibility and strengthening detective controls.

6. Encryption and Key Management (KMS)

Encryption was implemented using:

gcloud kms keyrings create my-keyring --location=us-central1

gcloud kms keys create my-key --location=us-central1 --keyring=my-keyring --purpose=encryption

These steps ensured all sensitive data is encrypted at rest, protecting confidentiality.

7. Monitoring and Alerting

Cloud Monitoring was configured to detect unusual activity and downtime.

Command:

gcloud monitoring uptime-checks create http web-tier-check --display-name="Web Tier Uptime Check" --http-path="/" --host="example.com"

This established a monitoring policy to verify web-tier availability.

8. Preventive, Detective, and Corrective Controls

Control Type Description Example Applied

Preventive Blocks security risks before they occur. Restricted IAM roles, tightened firewall rules, enabled encryption.

Detective Detects security incidents in real time. Cloud Logging for IAM and network events, uptime monitoring.

Corrective Mitigates issues post-detection. Revoke compromised credentials, rotate encryption keys, rollback misconfigurations.

9. Final Outcome and Conclusion

These configurations achieved robust IAM and network-level hardening aligned with GCP security standards. Access was limited to authorized users, network exposure minimized, data-at-rest encryption validated, and system monitoring enabled. Although the Security Command Center interface remained inaccessible due to lack of an organizational node, equivalent project-level tools provided comprehensive visibility, ensuring confidentiality, integrity, and availability across the three-tier architecture.

**Executive Summary**

This report provides a technical overview of the Identity and Access Management (IAM) and Network Security Hardening activities performed on the Google Cloud project “shopnimbus-security-group7”. The implementation focused on strengthening project-level access control, network defense, encryption, and monitoring mechanisms to ensure alignment with Google Cloud Platform (GCP) security best practices.

Using Cloud Shell commands, essential APIs such as IAM, Cloud KMS, Logging, and Monitoring were enabled to establish a secure foundation. IAM policies were reviewed and modified to enforce the principle of least privilege, minimizing the risk of unauthorized access. Network firewall configurations were analyzed and refined to eliminate unrestricted public access (e.g., SSH rules open to 0.0.0.0/0). Encryption at rest was implemented through Cloud Key Management Service (KMS), ensuring data confidentiality, while Cloud Logging and Monitoring provided continuous visibility and alerting across system components.

Preventive, detective, and corrective controls were implemented to create a multi-layered defense model. Preventive measures included strict IAM permissions and encryption; detective controls relied on logging and uptime monitoring; and corrective procedures ensured timely remediation through access revocation, key rotation, and policy rollback.

Although the Security Command Center interface could not be utilized due to the absence of an organizational node, equivalent tools such as IAM Recommender, Policy Analyzer, and Cloud Logging were leveraged to achieve the same level of operational visibility.

Overall, the project successfully enhanced the confidentiality, integrity, and availability (CIA) of the cloud environment, setting a strong foundation for subsequent compliance and monitoring phases.