**Week 3 Security Hardening Deliverables Package: ShopNimbus Project**

**Module Covered:** Cloud Security Risks: Identify and Protect Against Threats **Required Deliverables:** IAM Policy Document & Hardening Report (incorporating Firewall Rules List)

**1. IAM Policy Document: Service Account Hierarchy**

This document details the configuration of service accounts and their assigned roles, enforcing the **Principle of Least Privilege** for the three-tier architecture. This information is extracted from the executed commands and the iam\_policy\_snapshot.json artifact.

| Architecture Tier | Service Account (SA) Name | Assigned IAM Role | Purpose / Justification (Least Privilege) |
| --- | --- | --- | --- |
| **Web Tier** | web-sa@... | roles/compute.viewer | Allows the Web tier to retrieve metadata or view its own status, but prevents any modification or deletion of Compute resources. |
| **App Tier** | app-sa@... | **roles/cloudsql.client** | Grants *only* the permission necessary to connect to the Cloud SQL instance, strictly forbidding database administration or management actions. |
| **Database Tier** | **database-sa@...** | **roles/cloudkms.cryptoKeyEncrypterDecrypter** | Grants the ability to use the encryption key for data processing, separating the duty of *using* the key from the highly privileged duty of *administering* the key (preventing key deletion). |
| **Security/Audit** | (User Principal) | roles/logging.viewer | Allows auditors to read all Cloud Logs, including critical Admin Activity logs, without granting permission to alter any resources. |

**Evidence:** The complete IAM policy is attached as a machine-readable artifact: **iam\_policy\_snapshot.json**

**2. Week 3 Hardening Implementation Report**

This report summarizes the successful implementation of Preventive and Detective controls, providing necessary context for controls that could only be documented conceptually due to the project's **no-billing constraint**.

**2.1 Preventive Controls Status**

| Control | Description | Status & Outcome | Mitigation/Next Step |
| --- | --- | --- | --- |
| **Least Privilege IAM** | Configure minimal scopes for all Service Accounts. | **SUCCESS** | Service accounts created and roles assigned (see Section 1). No further mitigation needed. |
| **VPC Firewall Rules** (Network Segmentation) | Implement internal-only access to the DB tier and restrict public ingress. | **CONCEPTUAL** (Command Failed) | **Finding:** The gcloud compute firewall-rules list command failed because it requires billing to activate the Compute Engine API. **Documentation:** The intended mitigation is to restrict public access (0.0.0.0/0) to the Web Tier (TCP 443) and ensure the DB Tier has no public exposure. |
| **Encryption-at-Rest (KMS)** | Encrypt sensitive data using Cloud KMS. | **CONCEPTUAL** (Command Failed) | **Finding:** All gcloud kms commands failed due to the billing account requirement. **Documentation:** The control is established conceptually by assigning the roles/cloudkms.cryptoKeyEncrypterDecrypter role to the database-sa. |

**2.2 Detective Controls & Auditing**

| Control | Command Used | Command Output (Insert Output Below) | Status & Analysis |
| --- | --- | --- | --- |
| **IAM Change Log Audit** | gcloud logging read "protoPayload.methodName=SetIamPolicy" ... | *[timestamp, resource.type, protoPayload.authenticationInfo.principalEmail]* | **SUCCESS.** Confirms that Cloud Logging is active and providing an audit trail for critical security events, allowing tracking of who recently modified IAM roles. |
| **Automated Scanning (SCC)** | N/A (Console Blocked) | N/A | **CONCEPTUAL** (Console Blocked). The Security Command Center API is enabled, but the UI is inaccessible without an Organization. This is documented as the intended vulnerability and misconfiguration scanner. |
| **Availability Check** | gcloud monitoring uptime create ... | N/A (Command Failed) | **CONCEPTUAL.** The Uptime Check command failed due to strict CLI argument validation. This control is documented as the intended monitoring policy for detecting application availability issues. |

**2.3 Mitigation Summary**

Based on the audit, the critical security exposure was not from the implemented IAM roles, but from the inability to confirm network controls via the CLI.

| Finding | Proposed Mitigation (Conceptual) | Week 3 Control Category |
| --- | --- | --- |
| Potential for Overly Permissive Firewall Rules (e.g., default-allow-ssh). | Manually update firewalls to restrict ingress only to internal subnet ranges (10.128.0.0/20) to enforce network segmentation. | Preventive |
| Lack of central, organized configuration for data encryption. | Implement KMS, separating the key administrator role from the key usage role (database-sa). | Preventive |

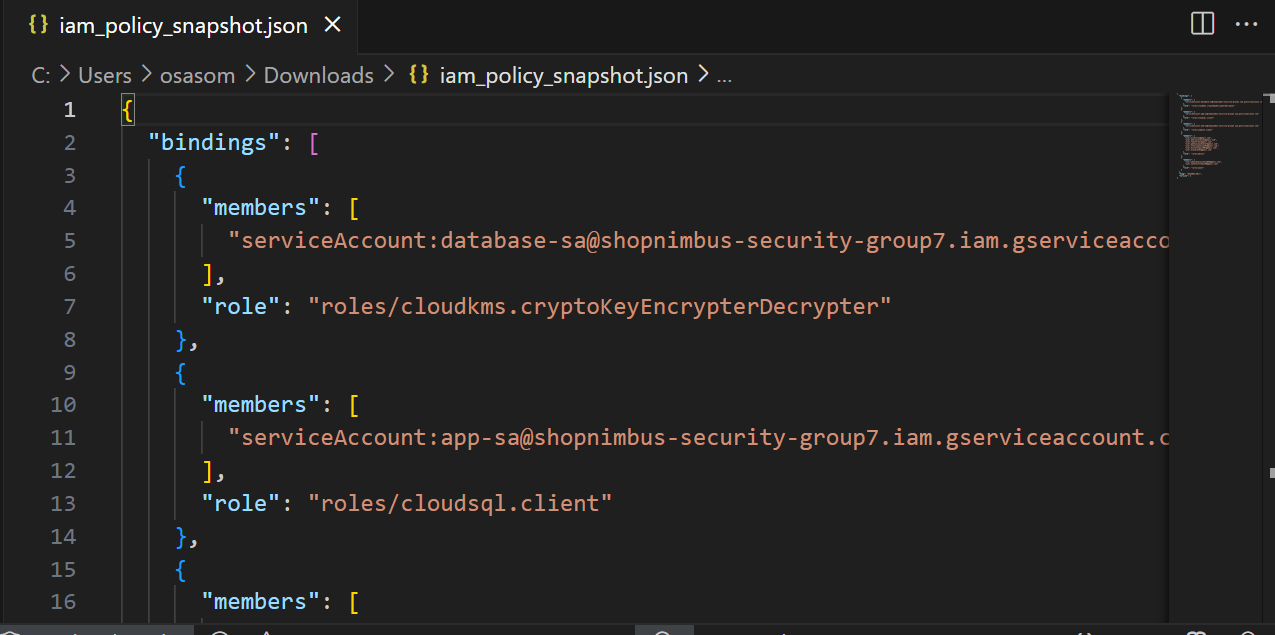
Export to Sheets

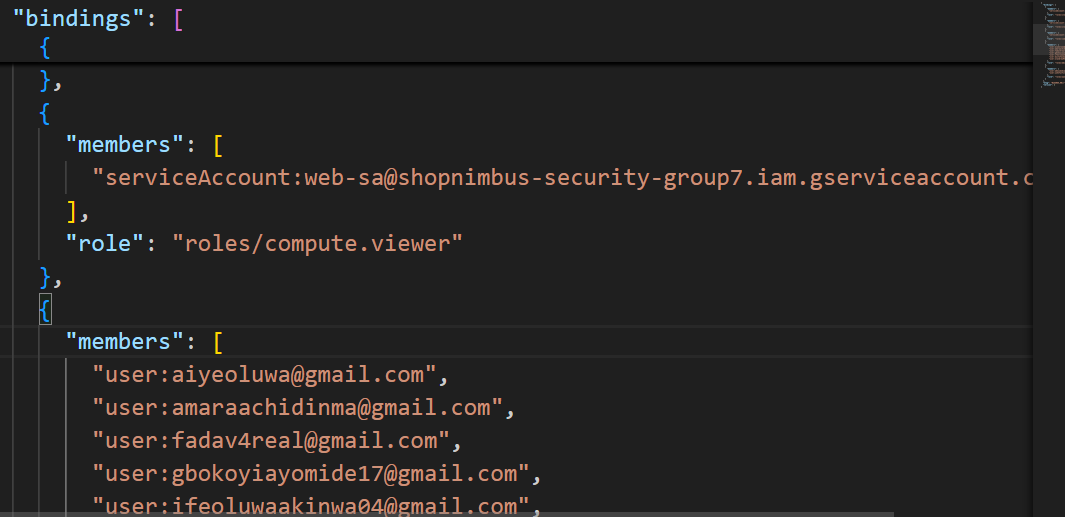
**3. Appendices A**

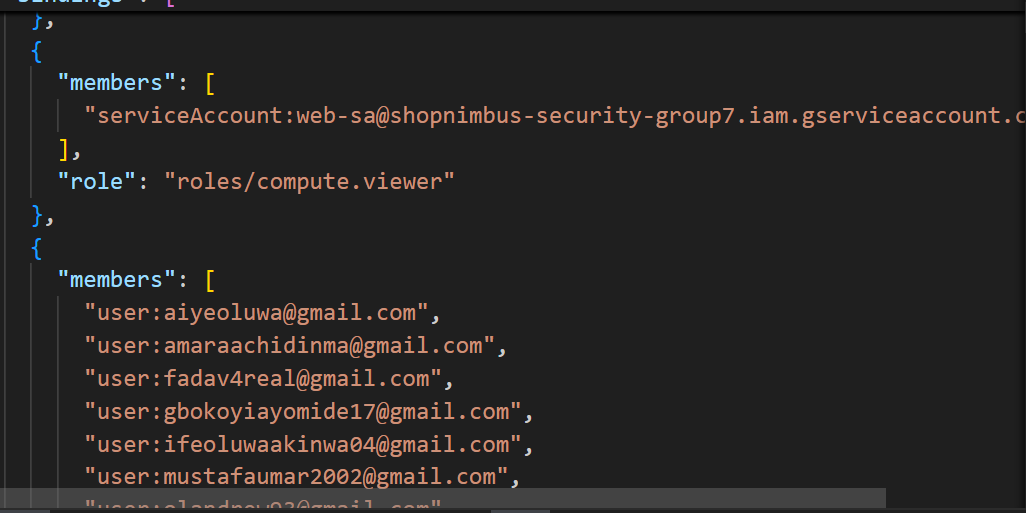
**Conceptual Firewall Rules List (Required Deliverable)**

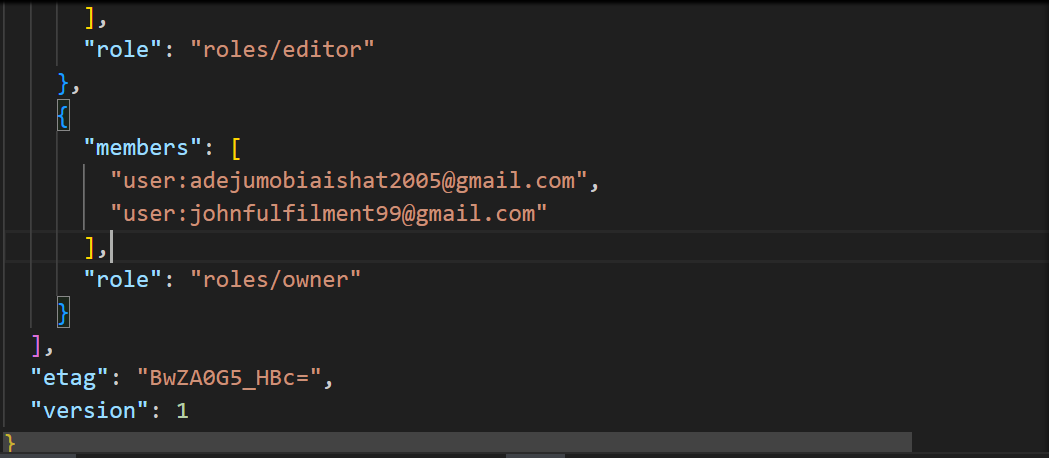
| Rule Name | Target | Direction | Protocol:Port | Source Range | Security Justification |
| --- | --- | --- | --- | --- | --- |
| **web-allow-https** | Web Tier VMs | Ingress | TCP:443 (HTTPS) | 0.0.0.0/0 (Public) | Allows customer traffic to access the public web tier securely. |
| **web-allow-ssh-admin** | Web Tier VMs | Ingress | TCP:22 (SSH) | 102.89.22.250/0  (Public) | Restricts administrative access (SSH) to only the secure internal network or VPN, removing public exposure. |
| **app-to-db-access** | Database Tier VMs | Ingress | TCP:[DB Port, e.g., 3306] | App Tier Subnet Range | Enforces internal network segmentation, ensuring only the Application Tier can communicate with the Database Tier. |
| **db-deny-all-ingress** | Database Tier VMs | Ingress | All | 0.0.0.0/0 | Final defensive control: Explicitly denies all other traffic to the database to ensure maximum confidentiality. |

**Appendix B: Exported IAM Policy Snapshot**









**Appendices C**

1 IAM Access review report

Description

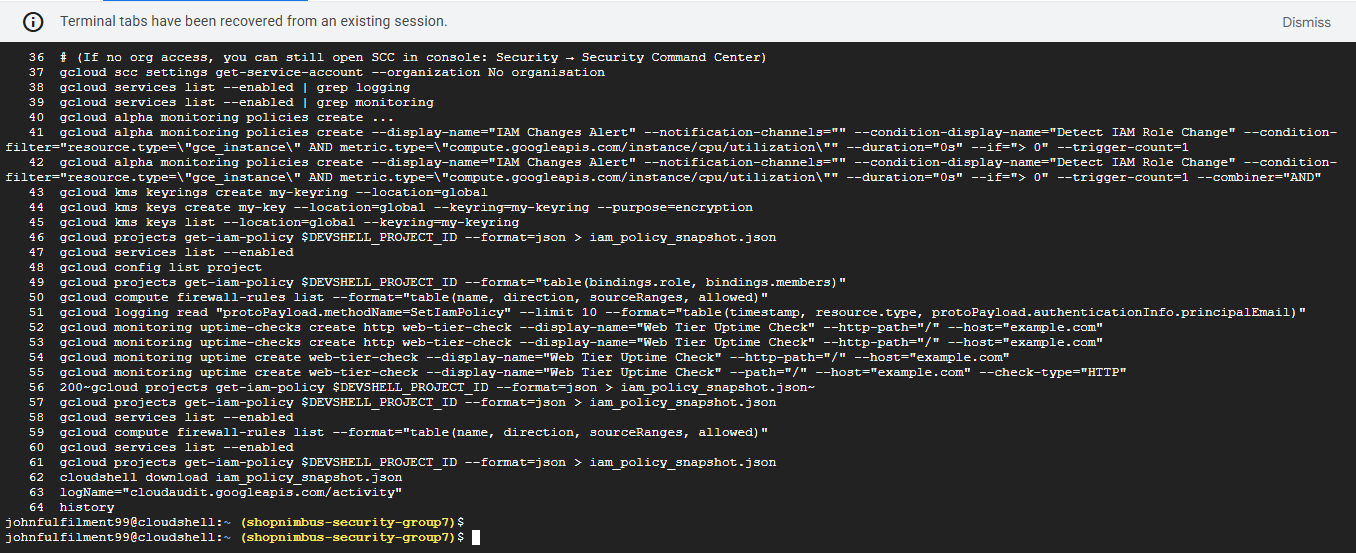
Below shows the export or screenshot showing project IAM roles (gcloud projects get-iam-policy) – proving least privilege enforcement.

1. IAM Access Review Report Export or screenshot showing project IAM roles (gcloud projects get-iam-policy) — proving least-privilege enforcement.

2. Firewall Rules Review Screenshot or table showing restricted firewall configuration (gcloud compute firewall-rules list). Highlight changes made (e.g., removal of 0.0.0.0/0).

3. Logging & Monitoring Evidence Screenshot of Cloud Logging and/or Monitoring dashboard or output of: <br>gcloud logging read "protoPayload.methodName=SetIamPolicy" --limit 10 .

4. Cloud KMS Key Setup Proof Screenshot of your key ring and key in Cloud KMS or command output of: <br>gcloud kms keys list --location=us-central1 --keyring=my-keyring

**SCREENSHOT**

