Practical 11 : Configure Server using any open-source tool.

LLO 11.1: Configure Server for Security
Task: *Configure Server using any open-source tool.*
Relevant CO: CO6

In OpenStack, this usually means configuring the server to detect and mitigate security issues.
We'll perform the same concept on **Google Cloud Platform (GCP)** using **Security Command Center (SCC)** — a built-in **open-source–style monitoring and threat analysis tool**.

You'll do this **100% free on Google Cloud Skill Boost (Qwiklabs)** — no credit card, no billing setup.

Objective

To configure and secure a cloud server using Google Cloud's **Security Command Center**, and understand how to identify and fix potential security vulnerabilities.

Platform & Free Lab

Google Cloud Skill Boost (Qwiklabs)

Lab Title: 🧠 *"Exploring the Security Command Center"*
Direct Link:
https://www.cloudskillsboost.google/focuses/4421?parent=catalog

This lab demonstrates:

- How to enable and use Security Command Center
- How to review active findings (vulnerabilities, misconfigurations)
- How to secure resources in GCP

Step-by-Step Procedure

Step 1: Start the Lab

1. Go to https://www.cloudskillsboost.google
2. Search for **"Security Command Center"**
3. Click **Start Lab** — you'll get credentials and a live GCP project.

Step 2: Open Security Command Center

1. In the Console → Navigation Menu → **Security → Security Command Center**
2. Click **Activate Security Command Center** (if prompted)
3. It will start scanning your GCP project for any potential issues

Step 3: Review Security Findings

After activation:

1. Click **Findings** → view detected issues
   (e.g., overly permissive IAM roles, open firewall ports, or unprotected storage buckets)
2. Each finding shows:
   - Severity (Low / Medium / High)
   - Resource affected
   - Recommendation to fix

This shows how GCP continuously monitors and audits your cloud setup — just like open-source tools such as **Nagios**, **Snort**, or **OpenVAS**.

Step 4: Fix a Security Issue (Simulated)

If you see a finding like "Publicly accessible storage bucket," you can:

1. Go to **Storage → Buckets**
2. Select that bucket → Permissions
3. Remove "Public access" entry
4. Return to Security Command Center → **Re-scan**

You've now simulated real-time cloud threat mitigation.

Step 5: Optional — Add IAM Role Restrictions

1. Go to **IAM & Admin → IAM**
2. Modify user role (e.g., change Editor → Viewer)
3. Security Command Center will note improved security posture.

Step 6: Verify Security Posture

From the **Dashboard**, you'll see:

- Number of high/medium/low findings
- Resource risk summary
- Recommendations section

This shows the overall security health of your project.

Step 7: End the Lab

Click **End Lab** on Skill Boost — your sandbox is deleted automatically (no charges).

Journal Format for PR11

Title:
Configure and Secure Server using Security Command Center in GCP

Objective:
To configure server security and monitor cloud infrastructure for threats using Google Cloud's Security Command Center.

Theory:

- **Server Security:** Involves protecting cloud resources from unauthorized access and vulnerabilities.
- **Security Command Center (SCC):** Centralized security management tool in GCP that detects, investigates, and helps remediate misconfigurations and threats.
- It works like open-source tools (Nagios, OpenVAS, Snort) but integrated within the GCP environment.
- SCC scans resources like Compute Engine, IAM, and Cloud Storage for risks.

Procedure:

1. Logged into Google Cloud Skill Boost and started the "Exploring the Security Command Center" lab.
2. Activated Security Command Center for the project.
3. Reviewed findings and identified potential risks (e.g., public access, weak roles).
4. Fixed misconfigurations using IAM or storage permissions.
5. Verified updated security posture from the dashboard.

Output:

- Screenshot of Security Command Center dashboard
- Screenshot of sample "finding" (risk alert)
- Screenshot after resolving the issue

Conclusion:
Successfully configured and monitored server security using GCP's Security Command Center, understanding cloud-based threat detection and mitigation methods