

Offensive GCP Operations and Tactics Certification (OGOTC) Lab Guide





Offensive GCP Operations & Tactics Certification (OGOTC) Lab Guide

Table of Contents

Table of Contents	2
Version Control	13
Introduction	13
Course Approach	14
Course Support	14
Course Requirements	14
Required Hardware	14
Required Accounts	14
Required Software	14
Installing the Google Cloud SDK (gcloud)	15
Installing gcloud on Windows (Recommended)	15
Installing gcloud on Ubuntu / Debian (Using APT Method)	18
Installing Kubectl CLI	20
Setting Up Student Portal	21
Set Up a Google Cloud Account	21
Setting Up Your First Google Cloud Project	23
Creating a Service Account in Google Cloud	25
Creating a Service Account Key	25
Logging in to the Student Portal	27
Deploying Your Lab	28
Troubleshooting	29
Module 1: Introduction to Offensive GCP	30
Introduction of GCP	30
Simple example	30
Real World Example	30
Overview of GCP architecture and key services	31
Understanding GCP Identity and Access Management (IAM)	45



Roles and Permissions	48
Granting Basic Roles (e.g., Owner) in Google Cloud via GUI	50
Overview of Google Cloud APIs and Services.....	54
Basic Examples of Google Cloud APIs:.....	54
Security model: APIs, Service Accounts and Organization Policy	69
What is an Organization Policy?	72
Navigating Organization Policies via GCP Console	73
Default Organization Policies	75
Organization Policy Constraints in Google Cloud Platform	76
Types of Constraints	76
Organization policy in dry-run mode	78
Overview of Google Cloud Services.....	83
Module 2: Enumeration of Google Cloud.....	97
Google Cloud Storage Enumeration with Dorks.....	97
What is Google Dorking?	97
Real Life example	101
Real-World Example:	102
GitHub Dorking for Google Cloud: A Detailed Guide	106
Key GCP-Related Sensitive Information to Look For	106
Authenticated Enumeration	110
Cloud Storage Enumeration.....	110
Lab – Storage Bucket Enum.....	115
Lab Overview	115
Hands On: Storage Bucket Enum.....	115
Authenticate with Service Account.....	115
Verify Active Service Account	115
Configure the Active Project	116
Enumerating permission of service account	116
Enumerating Available Cloud Storage Buckets	117
Enumerating Contents of a Storage Bucket	117
Exfiltrate Sensitive Data from Bucket.....	118
Accessing Sensitive Files Using the Newer gcloud Storage Method	119
Mitigation	121
Remove public access from sensitive buckets.	121



Additional Mitigation Steps.....	123
Conclusion	123
Compute Engine	124
Enumerating Compute Engine Resources with roles/viewer.....	127
What Is BigQuery?.....	129
BigQuery Dataset Enumeration	129
BigQuery Viewer Role Overview.....	131
Service Account Enumeration	134
Cloud Function Enumeration	136
Cloud Pub/Sub Topics.....	138
Pub/Sub Subscriptions Enumeration	138
Secret Manager Enumeration.....	141
Cloud Logs Enumeration	142
Lab - Finding Secrets from Cloud Builds	146
Lab Overview	146
Authenticate with Service Account.....	146
Configure the Active Project	146
Listing Cloud Builds.....	146
Viewing Cloud Build Logs	147
Conclusion	147
Mitigation.....	148
Understanding VPC Networks in Google Cloud	149
What is a VPC Network?	149
Cloud Function to Storage: Code Dump Enumeration.....	152
Understanding and abusing GCP Metadata API.....	154
Wrap Up.....	158
Lab – Abuse Viewer-Role	159
Lab Overview	159
Authenticate with Service Account.....	159
Configure the Active Project	159
Storage Bucket Enumeration	160
Cloud Function Enumeration	164
Cloud Run Enumeration.....	167
Cloud Logging Enumeration	169



Artifact Registry Enumeration	173
Pub/Sub Enumeration	175
BigQuery Enumeration	177
Workflow Enumeration	179
Cloud Scheduler Enumeration	181
Cloud Task Enumeration	183
Cloud build Enumeration	183
Conclusion	185
Mitigation	185

Module 3: Initial Access..... 186

Gaining Access Through Leaked Credentials and Keys.....186

1. Public GitHub Repositories	186
-------------------------------------	-----

Initial Access Through Web Application Weaknesses in Google Cloud Environments189

Lab – Cloud Run SSTI.....192

Lab Overview	192
Checking the Vulnerable Cloud Run Service	192
SSTI Vulnerability in the Profile Generator	193
Exploiting the SSTI Vulnerability	194
Understanding the Advanced SSTI Payload for Metadata Access	195
Understanding the Retrieved Token and Validating It	197
Setting the Access Token in Windows	197
Setting the Access Token in Linux	198
Checking Service Account Roles with gcloud	198
Enumerating the Target Bucket Using the Compromised Access Token	199
Conclusion	199
Mitigation	199

Initial Access via Exposed Google Cloud Functions201

Lab - Cloud Functions for RCE202

Lab Overview	202
Assessing the Provided Cloud Function	202
Testing the Cloud Function for Remote Command Execution (RCE)	202
Querying the Metadata Server for the Function's Access Token	203
Understanding the Retrieved Token and Validating It	204
Setting the Access Token in Windows	204



Setting the Access Token in Linux.....	205
Checking Service Account Roles with gcloud.....	205
Enumerating the Target Bucket Using the Compromised Access Token.....	205
Downloading the ZIP File from the Bucket	206
Conclusion	207
Mitigation.....	207
Initial Access via Vulnerable GKE Workloads Exposing Metadata	209
Initial Access via Firebase – How It Leads to GCP Compromise	209
Lab – Abuse Firestore DB	211
Lab Overview	211
Authenticate with Service Account.....	211
Configure the Active Project	211
Extracting the Access Token	212
Enumerate All Firestore Collections.....	212
Conclusion	219
Mitigation.....	219
Credential theft through phishing.....	220
Understanding Evilginx	220
Understanding Phishlets	220
The Google Workspace (G Suite) Phishlet Explanation	221
Module 4: Post-Exploitation Technique	223
Data Exfiltration	223
Lab – Big Query Enum.....	231
Lab Overview	231
Hands On: Big Query Enum	231
Authenticate with Service Account.....	231
Verify Active Service Account	231
Enumerating permission of service account	232
Enumerate Datasets	232
List Tables in a Dataset Using	233
View Critical Data in BigQuery Tables	233
Exfiltrate BigQuery Data as CSV to Local Machine.....	234
Mitigation.....	234
Conclusion	235



Gaining unauthorized access to Secrets Manager and environment variables.....	236
Lab – Extract Secrets.....	239
Authenticate with Service Account.....	239
Configure the Active Project	239
Accessing the Secret	239
Conclusion	240
Mitigation.....	240
Lab – Extract & Decrypt the Encrypted Secret	241
Lab Overview	241
Authenticate with Service Account.....	241
Configure the Active Project	241
Listing Secrets.....	241
Revealing Secret Value	242
Enumerating KeyRings	243
Retrieve the CryptoKey.....	243
Prepare Ciphertext for Decryption	244
Decrypting the Ciphertext	244
Conclusion	245
Mitigations	245
Persistence techniques	246
Backdooring Service Accounts and Roles	246
Command and control (C2) in GCP	253
Google Calendar Command & Control	253
Command and control (C2) in GCP (Google slides).....	260
Conclusion	264
Module 5: Lateral Movement Techniques in GCP	265
Leveraging IAM Role Misconfigurations for Lateral Movement.....	265
Privilege Abuse with Over-permissive Roles	265
Deploy Cloud Function with High Privilege Service Account Privilege Escalation	267
Enabling High-Risk APIs and Assessing the Resulting Attack Surface.....	269
Lab – Public Docker Image info	271
Lab Overview	271
Authenticate with Service Account.....	271
Configure the Active Project	271



Artifact Registry Enumeration	271
Describing the Target Artifact Repository	273
Enumerating Docker Images	273
Pulling the Docker Image	274
Running the Docker Image and Getting Shell Access	274
Accessing the Json File Inside the Container	274
Authenticating with the Extracted Service Account Key	275
Conclusion	276
Mitigation	276
Lab – Gaining Access To VM	277
Lab Overview	277
Authenticate with Service Account	277
Configure the Active Project	277
Enumerating Compute Instances	277
Inspecting a Selected VM Instance	278
Unauthorized SSH Access via gcloud	278
Mitigations	279
Conclusion	279
Abuse (Cloud Storage Buckets):	280
Project Creation & Ownership Escalation Abuse	281
Abuse of Firewall Rules in GCP	283
Automated Google Cloud Management Toolkit: Overview and Functionality	284
Moving Laterally via Service Accounts	293
Abusing Service Account Impersonation in GCP	293
API Calls for Resource Discovery and Access	299
Enumerate Folders	300
IAM / Service Accounts	301
Custom Project Roles	302
Cloud Storage (GCS)	302
Cloud Function	303
Cloud Run Services	304
Cloud Logging	304
Metrics for Activity Logs	305
Secret Manager	305
Lab – Assign Privilege Identity to VM	307



Lab Overview	307
Authenticate with Service Account.....	307
Configure the Active Project	307
Enumerating Compute Instances.....	307
Inspecting a Selected VM Instance.....	308
Attached Editor service account (Victim Service Account) on VM and verifying role	308
Starting VM Instances with Batch Agent Privileges	309
Stopping VM Instances through Batch Agent Privileges	309
Unauthorized SSH Access via gcloud	309
Discovering the Attached Service Account from Inside the VM	310
Accessing and Understanding the Default Service Account Token Inside the VM	310
Verifying the Editor Binding from the VM	311
Mitigation	311
Conclusion	311

Modules 6: Hacking Kubernetes..... 312

Intro to Kubernetes and its architecture 312

Kubernetes Architecture	312
What is a Cluster in GKE?	312
Creating Simple Cluster in Google Cloud	313
Prerequisites (Before Creating GKE Cluster via CLI).....	316
Create a GKE Cluster via CLI	317
Running Kubernetes Clusters in GKE.....	319
Node Configuration	322
Node Networking.....	323
Node Security.....	324
Node Automation in GKE.....	325
Cluster Networking (Control Plane Access).....	326
GKE Security.....	327
Creating a GKE Autopilot Cluster	329
Networking Control Plane Access.....	331
Auto-Pilot Cluster Advance settings.....	332
Auto-pilot (cli mode)	333

Understanding basic components of K8s..... 334

Understanding Node	335
--------------------------	-----



Understanding Namespace	336
Understanding Pods.....	337
Kube API Server (The Front Desk of Kubernetes)	338
Understanding ConfigMap	339
Understanding Secrets	340
Understanding Deployment	340
Understanding Services	341
Understanding Ingress	341
Exposed Prometheus Instances Revealing GKE Pod Details	342
Exposed Prometheus /targets Endpoint Leaking GKE Pod and Cluster Insights	343
Prometheus Service Discovery Leaking GKE Pod and Cluster Info	344
Prometheus Runtime and Build Info Revealing Version & Environment Details	345
Prometheus Configuration Page Leaking Scrape and Auth Details	346
Compromising K8 pod.....	347
Creating Cluster	347
Cluster Credentials.....	348
Installing Helm v3.....	348
Adding &Updating OTWLD Helm.....	348
Deploying Ollama Application	349
Displaying External IP	349
Setup for Attacker Machine.....	350
Creating Firewall Policy	350
Running the Exploit	351
Root Cause Analysis (RCA) — CVE-2024-37032 ("Problama").....	353
Creating Kubernetes Pods	354
Kubernetes Networking in GKE	361
Abusing Kubernetes (K8s) Roles in GKE	373
Wrapping Up	380
Lab – Abuse GKE.....	381
Lab Overview	381
Generating an Access Token for Kubernetes API Access	381
Enumerating Pods Across the Cluster	382
Describing Pods in the Vulnerable Namespace	383
Inspecting ConfigMaps	384



Viewing ConfigMap in YAML Format	385
Enumerating Secrets Across All Namespaces	385
Accessing the Specific Secret in the Vulnerable Namespace	386
Extracting and Decoding the Sensitive Kubernetes Secret Using a Raw Access Token	386
Conclusion	387
Mitigation.....	387
Module 7: Privilege Escalation and GCP Abuse.....	389
Privilege escalation techniques	389
IAM Misconfigurations Service Account.....	389
Exploiting Over-Permissive Service Accounts via Cloud Functions	392
Function Code Overview	393
Deploying a Cloud Function with Attacker-function	395
Privilege Escalation via Service Account Impersonation (signBlob Abuse in GCP)	399
Lab - Sign JWT	404
Lab Overview	404
Authenticate with Service Account.....	404
Configure the Active Project	404
Authenticating and Obtaining an Access Token	404
Enumerating Service Accounts in the Project.....	405
Why the Pub/Sub Identity Can Generate and Exchange JWTs	405
Automating JWT Signing & Impersonation (Access-Token Flow)	406
Setting the Impersonated Access Token	409
Verifying IAM Policy for the Service Account.....	410
Mitigation.....	410
Conclusion	410
Undocumented API	411
Lab – Abuse Service API Key.....	415
Lab Overview	415
Authenticate with Service Account.....	415
Configure the Active Project	415
Listing API Keys in the Project.....	415
Retrieving the Plain API Key String	416
Enumeration With an API Key	416
Mitigation.....	417



Conclusion	417
Abusing Compute Engine for Escalation	418
AI Privilege Escalation.....	424
Overview of ML Engineer on Steroids	424
AI Platform Service Agent on Steroids.....	427
Agent Privilege Escalation	431
Cloud API Gateway Service Agent	431
Apigee Service Agent.....	432
BigQuery Continuous Query Service Agent	435

SAMPLE