CWL
CyberWarFare Labs

External Attack Surface for Initial Access in GCP Cloud

CyberWarFare Labs

CW Labs is a renowned UK based Ed-tech company specializing in cybersecurity cyber range labs. They provide on-demand educational services and recognize the need for continuous adaptation to evolving threats and client requirements.

aws
Cloud Security
RED TEAM
PURPLE TEAM
BLUE TEAM
AD
WEB
On-Premise Security
CI/CD
PLATFORM
NETWORK
INFINITE LEARNING EXPERIENCE

The company has two primary divisions :

1. **Cyber Range Labs**
2. **Up-Skilling Platform**

About Speaker:

Parth Agrawal

(Security Intern @CWL)

Is a cloud security enthusiast with a keen interest in the intricacies of cloud services offered by AWS, Azure, and GCP. Possessing a comprehensive understanding of these platforms, they are particularly drawn to exploring Red Team methodologies. Interested in Red Team methodologies, focusing on vulnerability testing and detection across external attack surfaces.

Table of Contents

- **Azure Services**
  - GCP Bucket
  - BigQuery Dataset
  - KMS Keys
  - VM Image
  - SQL Database Instances
- **Sample Public URLs**
- **Recon:**
  - Scenario 1: OSINT
  - Scenario 2: Unauthenticated Enumeration

CWL
CyberWarFare Labs

Google Cloud Services

GCP Bucket, BigQuery Dataset, KMS Keys, VM Image, SQL Database Instances

GCP Bucket

- A GCP bucket refers to a Google Cloud Storage bucket.
- It is a fundamental component of Google Cloud Platform's object storage service, which allows you to store and access large amounts of unstructured data.
- They can handle a large volume of data and scale as needed.

GCP BigQuery Dataset

- A GCP BigQuery dataset is a container that organizes and manages tables and views in Google BigQuery, Google's fully managed, serverless data warehouse service.
- It helps organize and manage data within BigQuery.
- It is used for running SQL-like queries on large datasets efficiently.

GCP KMS Keys

- ➢ GCP KMS (Key Management Service) keys are cryptographic keys used to manage encryption and decryption in Google Cloud Platform.
- ➢ It can work with other GCP services like Cloud Storage, BigQuery, and Compute Engine for data encryption.
- ➢ GCP KMS keys help in securing data at rest and in transit, ensuring that only authorized entities can access or manipulate the encrypted data.

GCP VM Image

- A GCP VM image is a virtual machine image used to create instances in Google Compute Engine.
- It contains the operating system and optional additional software pre-installed.
- GCP VM images are essential for quickly deploying standardized environments, ensuring consistency and efficiency in creating and managing virtual machine instances.

GCP SQL Database Instances

- ➢ GCP SQL database instances are managed relational database services provided by Google Cloud, supporting popular database engines like MySQL, PostgreSQL, and SQL Server.
- ➢ GCP SQL database instances are ideal for running traditional relational databases in a cloud environment with the benefits of management, scalability, and security provided by Google Cloud.

CWL
CyberWarFare Labs

Public URLs

For Available Services

GCP Services	Sample Public URL
GCP Bucket	http://BUCKET_NAME.storage.googleapis.com/OBJECT_NAME OR http://storage.googleapis.com/BUCKET_NAME/OBJECT_NAME
Cloud Functions	https://<region>-<project-gcp-name>.cloudfunctions.net/<func_name>
Compute Engine (VM Instance)	https://compute.googleapis.com/compute/v1/projects/{project}/zones/{zone}/instances/{instance}
GCP BigQuery	https://bigquery.googleapis.com/bigquery/v2/projects/{project}/datasets/{dataset}/tables/{table}
GCP Cloud Pub/Sub	https://pubsub.googleapis.com/v1/projects/{project}/topics/{topic}

Scenario 1: OSINT

RECON

GCP Bucket

CLI-based Recon:

- Cloud Enum:

```
./cloud_enum.py -k <KEYWORD> --disable-azure --disable-aws
```

- S3 Scanner:

```
./s3scanner -bucket <KEYWORD> -enumerate -json
```

GCP Bucket

Web-based Recon:

- Bucket search:
  - https://osint.sh/buckets
  - https://buckets.grayhatwarfare.com
  - https://builtwith.com/
  - https://s3browser.com/
- Dorks:
  - GitHub Dorks:

```
site:storage.googleapis.com
```

GCP Bucket

Web-based Recon:

- Dorks:
    - More Google Dorks:

```
site:console.cloud.google.com/storage/browser/_details
```

```
site:console.cloud.google.com/storage/browser
```

GCP BigQuery Dataset

Web-based Recon:

- Dorks:
  - Google Dorks:

```
site:cloud.google.com "BigQuery dataset"
```

```
site:*.cloud.google.com inurl:bigquery "dataset"
```

GCP KMS Keys

Web-based Recon:

- Dorks:
  - Google Dorks:

```
inurl:"keyRing" inurl:"cryptoKey" intext:"Google Cloud"
```

```
site:cloud.google.com "KMS" "keys"
```

```
filetype:pdf "kms" "keyRing" "cryptoKey"
```

```
filetype:pdf "bindings" "role" "serviceAccount" "kms"
```

GCP VM Image

Web-based Recon:

- Dorks:
  - Google Dorks:

```
intitle:"Google Cloud" inurl:"compute" "vm image"
```

```
site:github.com "google cloud" "vm image" filetype:yaml
OR filetype:json
```

```
inurl:"compute/docs/images" intitle:"Google Cloud"
```

GCP VM Image

Web-based Recon:

- Dorks:
  - GitHub Dorks:

```
filename:*.yaml "image:" "gce-vm-image"
```

```
filename:*.tf "source_image" "google_compute_instance"
```

```
filename:*.yml "hosts:" "tasks:" "google_compute"
```

GCP SQL Database Instances

Web-based Recon:

- Dorks:
  - Google Dorks:

```
intitle:"Google Cloud SQL" inurl:docs "instance"
```

```
site:*.com filetype:sql "google_cloud_sql"
```

```
site:github.com "google cloud sql" filename:*.tf
```

GCP SQL Database Instances

Web-based Recon:

- Dorks:
  - GitHub Dorks:

```
filename:.env "sql_password" OR "db_password"
```

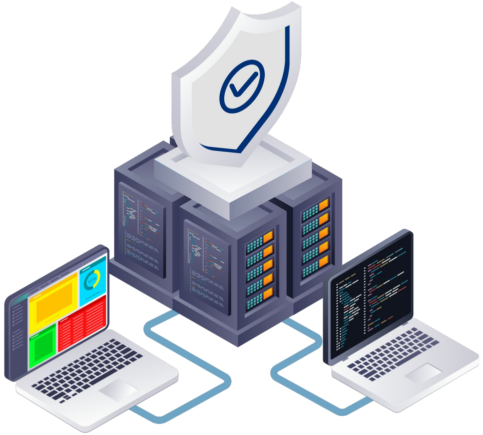
```
filename:credentials.json "type":"service_account"
"sqladmin.googleapis.com"
```

```
filename:*.json "databaseVersion"
"google_sql_database_instance"
```

CyberWarFare Labs

Scenario 2: Unauthenticated Enumeration

Enum



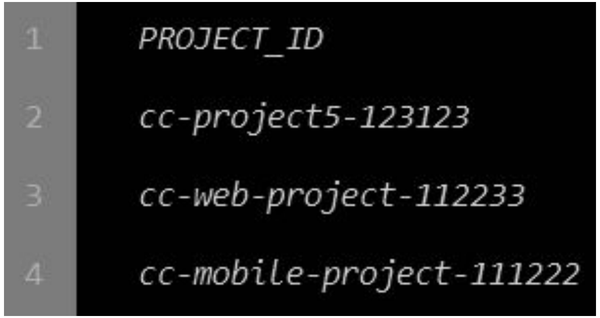
GCP Bucket Recon

CLI-based Recon:

- ➢ To list the IDs of all the Google Cloud Platform (GCP) projects available in your cloud account

```
gcloud projects list --format="table(projectId)"
```

★ **OUTPUT**



```
PROJECT_ID
cc-project5-123123
cc-web-project-112233
cc-mobile-project-111222
```

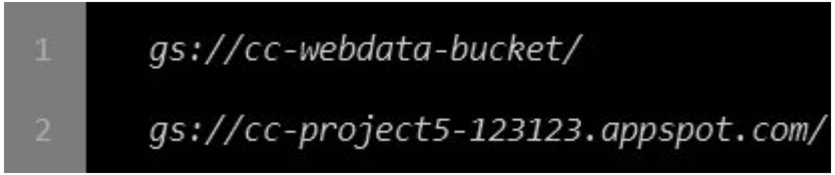
GCP Bucket Recon

CLI-based Recon:

➢ To list the identifier (name) of each storage bucket created for the specified GCP project.

```
gsutil ls -p <Project_ID>
```

★ **OUTPUT**



```
gs://cc-webdata-bucket/
gs://cc-project5-123123.appspot.com/
```

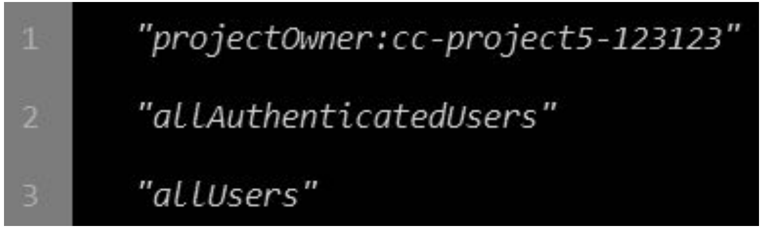
GCP Bucket Recon

CLI-based Recon:

➢ To determine name of the IAM member(s) associated with the selected bucket.

```
gsutil iam get gs://cc-webdata-bucket/
--format=json | jq '.bindings[].members[]'
```

➔ **"allUsers"** and/or **"allAuthenticatedUsers"** means the selected Google Cloud Storage bucket is publicly accessible.



```
"projectOwner:cc-project5-123123"
"allAuthenticatedUsers"
"allUsers"
```

★ **OUTPUT**

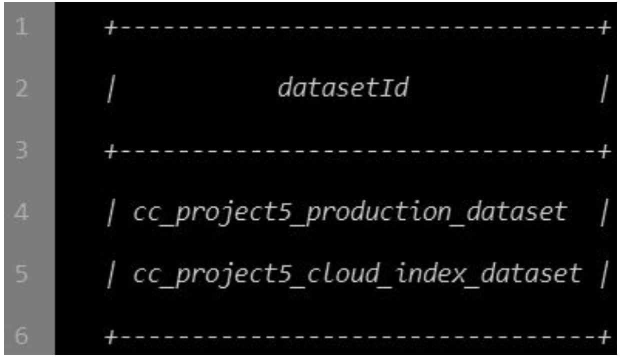
BigQuery Dataset Recon

CLI-based Recon:

➢ To list the identifier (name) of each BigQuery dataset created for the specified Google Cloud project.

```
bq ls --project_id cc-project5-123123 --format=pretty
```

★ **OUTPUT**



```
+------------------------------+
|           datasetId          |
+------------------------------+
| cc_project5_production_dataset  |
| cc_project5_cloud_index_dataset |
+------------------------------+
```

BigQuery Dataset Recon

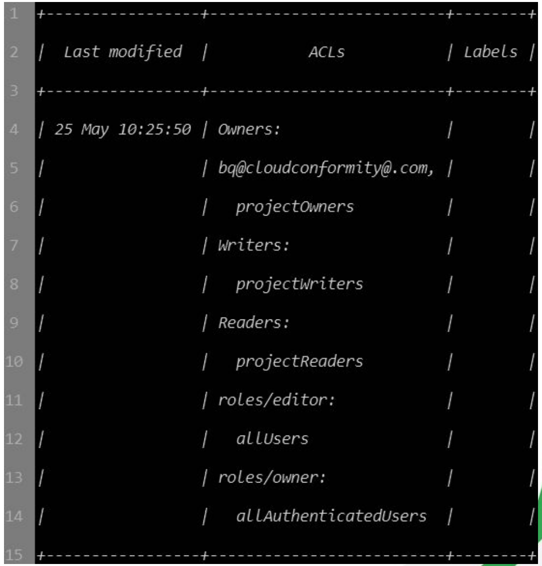
CLI-based Recon:

➢ To list the identifier (name) of each storage bucket created for the specified GCP project.

```
bq show --format=pretty
cc-project5-123123:cc_project5_production_dataset
```

➔ If one or more roles are using the "**allUsers**" and/or "**allAuthenticatedUsers**" members, the selected Google Cloud BigQuery dataset is publicly accessible.

★ **OUTPUT**



```
+----------------+-------------------------+--------+
|  Last modified |           ACLs          | Labels |
+----------------+-------------------------+--------+
| 25 May 10:25:50 | Owners:                |        |
|                | bq@cloudconformity@.com, |      |
|                |   projectOwners         |        |
|                | Writers:                |        |
|                |   projectWriters        |        |
|                | Readers:                |        |
|                |   projectReaders        |        |
|                | roles/editor:           |        |
|                |   allUsers              |        |
|                | roles/owner:            |        |
|                |   allAuthenticatedUsers |        |
+----------------+-------------------------+--------+
```

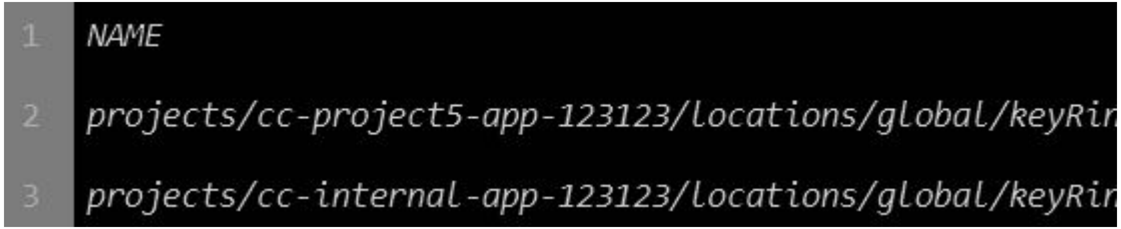
KMS Keys Recon

CLI-based Recon:

➢ To list the IDs of all the KMS key rings available in your GCP account.

```
gcloud kms keyrings list --location=global
```

★ **OUTPUT**



```
NAME
projects/cc-project5-app-123123/locations/global/keyRin
projects/cc-internal-app-123123/locations/global/keyRin
```

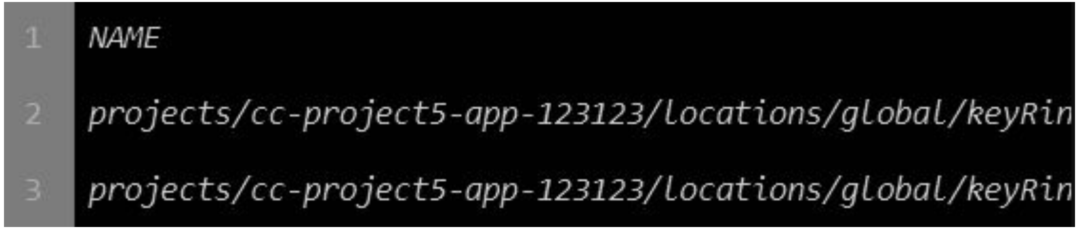
KMS Keys Recon

CLI-based Recon:

- ➢ To list the resource ID of each KMS cryptographic key created for the selected key ring.

```
gcloud kms keys list
--keyring=projects/cc-project5-app-123123/locations/global/keyRi
ngs/cc-project5-key-ring
--location=global --format="table(name)"
```

★ **OUTPUT**



```
NAME
projects/cc-project5-app-123123/locations/global/keyRin
projects/cc-project5-app-123123/locations/global/keyRin
```

KMS Keys Recon

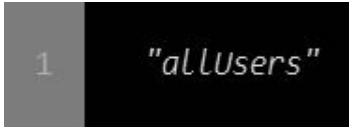
CLI-based Recon:

➢ To list the identifier (name) of each storage bucket created for the specified GCP project.

```
gcloud kms keys get-iam-policy
projects/cc-project5-app-123123/locations/global/keyRings/cc-pro
ject5-key-ring/cryptoKeys/cc-prod-cryptokey
--keyring=projects/cc-project5-app-123123/locations/global/keyRi
ngs/cc-project5-key-ring
    --location=global --format=json | jq '.bindings[].members[]'
```

➔ "**allUsers**" or "**allAuthenticatedUsers**", means the selected Google Cloud Platform (GCP) KMS key is publicly accessible to the Internet.

★ **OUTPUT**



```
"allUsers"
```

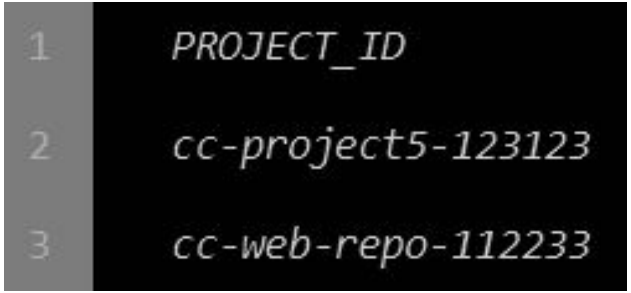
VM Image Recon

CLI-based Recon:

➢ To list the IDs of all the Google Cloud Platform (GCP) projects available in your Google Cloud account.

```
gcloud projects list --format="table(projectId)"
```

★ **OUTPUT**



```
PROJECT_ID
cc-project5-123123
cc-web-repo-112233
```

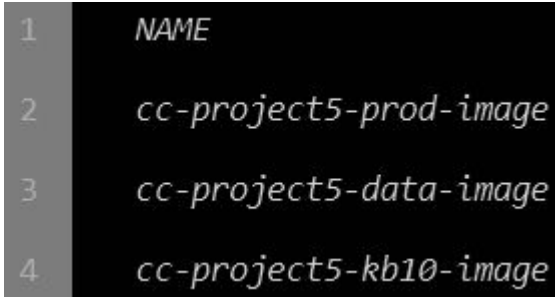
VM Image Recon

CLI-based Recon:

➢ To list all the virtual machine (VM) disk images available for the selected project.

```
gcloud compute images list --project <project_id>
     --no-standard-images --format="table(name)"
```

★ **OUTPUT**



```
NAME
cc-project5-prod-image
cc-project5-data-image
cc-project5-kb10-image
```

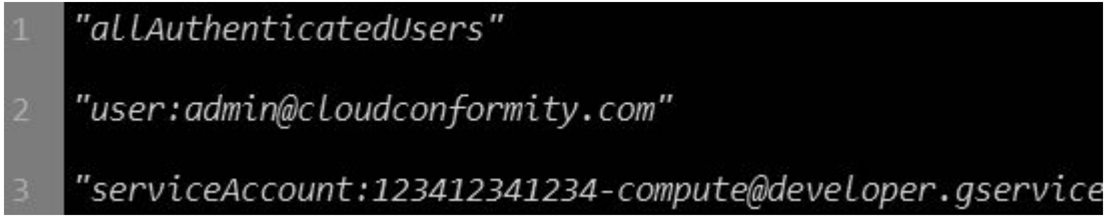
VM Image Recon

CLI-based Recon:

➢ To describe name of the IAM member(s) associated with the selected image.

```
gcloud compute images get-iam-policy prod-instance-image
--format=json
```

★ **OUTPUT**



```
"allAuthenticatedUsers"

"user:admin@cloudconformity.com"

"serviceAccount:123412341234-compute@developer.gservice
```

➔ If the command output include "**allAuthenticatedUsers**", the selected virtual machine (VM) disk image is publicly shared with all other Google Cloud accounts.

VM Image Recon

CLI-based Recon:

- To Create a new image of it.

```
gcloud compute images create stage-instance-image
--source-image=<Image_Name>
--source-image-project=long-base-324712
```

- To view image.

```
gcloud compute images list
```

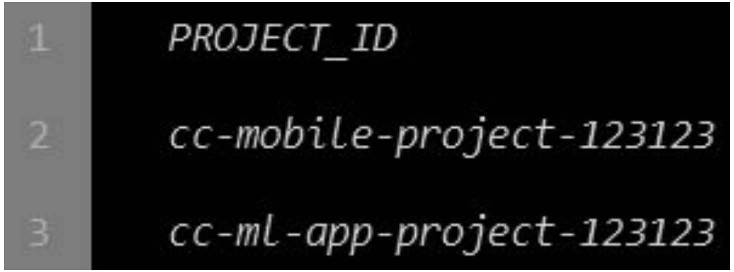
SQL Database Instances Recon

CLI-based Recon:

➢ To list the IDs of all the Google Cloud Platform (GCP) projects available in your Google Cloud account.

```
gcloud projects list --format="table(projectId)"
```

★ **OUTPUT**



```
PROJECT_ID
cc-mobile-project-123123
cc-ml-app-project-123123
```

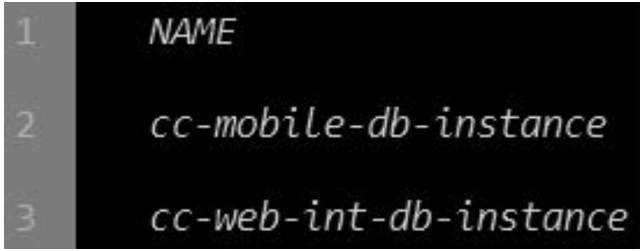
SQL Database Instances Recon

CLI-based Recon:

➢ To describe the name of each Cloud SQL database instance provisioned for the selected Google Cloud project.

```
gcloud sql instances list --project cc-mobile-project-123123
--format="(NAME)"
```

★ **OUTPUT**



```
NAME
cc-mobile-db-instance
cc-web-int-db-instance
```

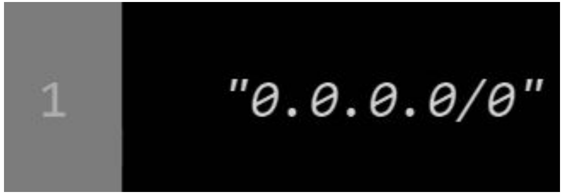
SQL Database Instances Recon

CLI-based Recon:

➢ To describe name of the IAM member(s) associated with the selected image.

```
gcloud sql instances describe cc-mobile-db-instance --format=json
    | jq '.settings.ipConfiguration.authorizedNetworks[].value'
```

★ **OUTPUT**



```
"0.0.0.0/0"
```

➔ If output contains "**0.0.0.0/0**", there is at least one authorized network that allows database access to anyone on the Internet, therefore the selected Google Cloud SQL database instance is publicly accessible.

CWL
CyberWarFare Labs

Thank You

For Professional Red Team / Blue Team / Purple Team / Cloud Cyber Range labs / Trainings please contact

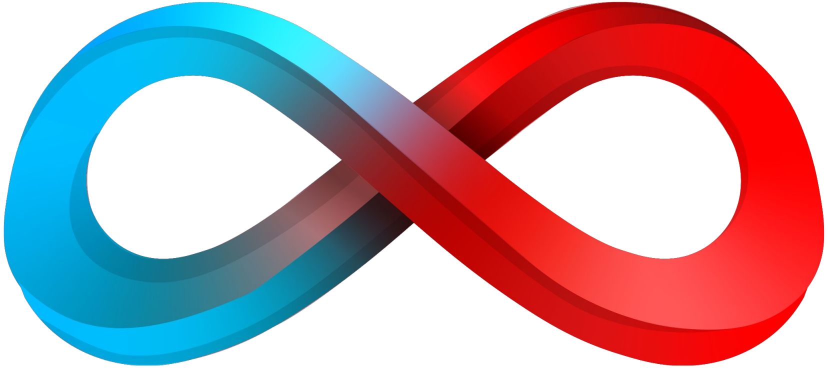
support@cyberwarfare.live

To know more about our offerings, please visit: **https://cyberwarfare.live**

CWL
CyberWarFare Labs

Infinity Learning

- ➢ Cyber War Simulation & Detection: Dive into realistic scenarios and sharpen your skills.
- ➢ Plug & Play Labs: Directly access our hands-on labs and start learning right away.
- ➢ Continuous Learning: Explore various challenges designed to elevate your skills



URL🔗: https://infinity.cyberwarfare.live/

Infinity Learning is for you!!

- ➔ Cyber Security Beginners / Professionals
- ➔ Anyone Interested in Cloud Security / Cloud Red Teaming Domains / Cloud Blue Teaming Domains / Cloud Purple Teaming Domains