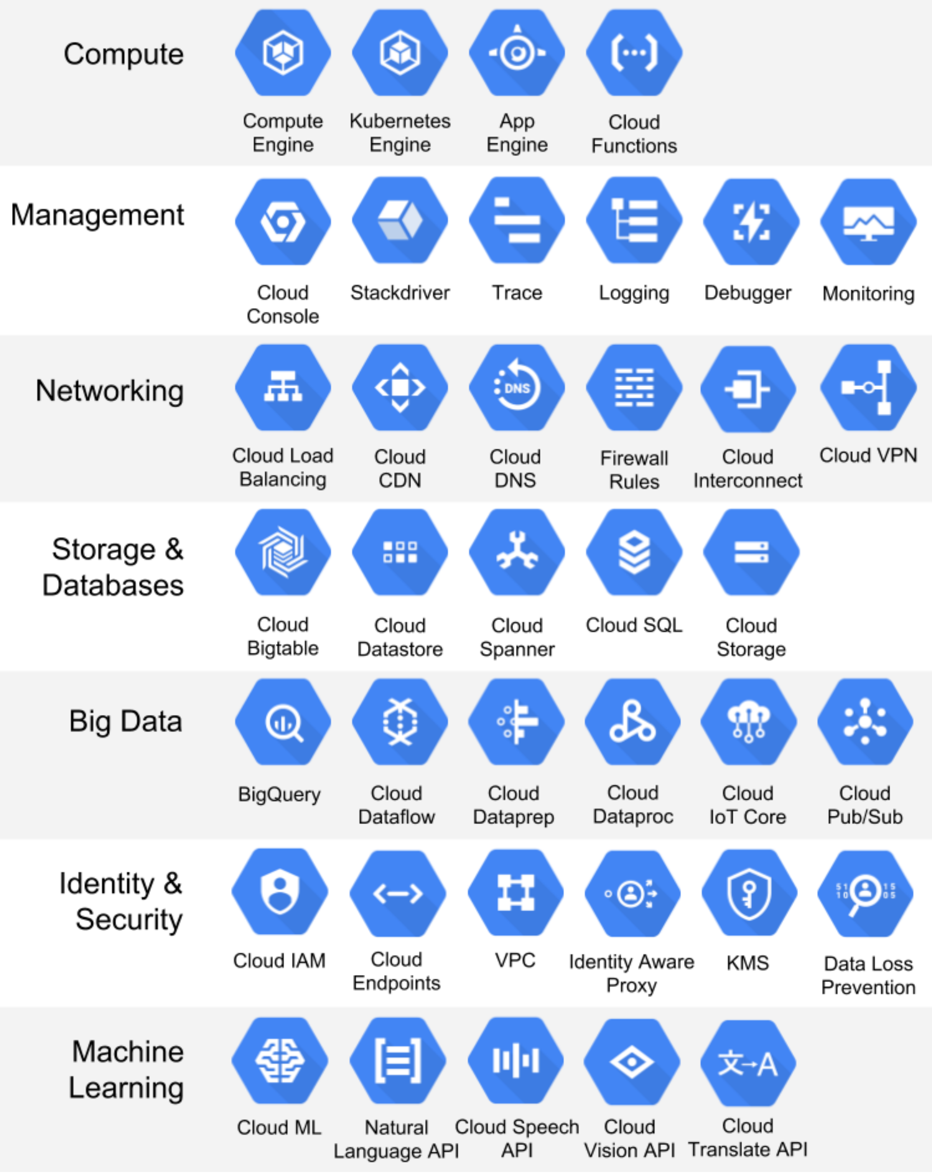
GOOGLE CLOUD – ATTACK OVERVIEW PT.1

Joas Antonio

https://www.linkedin.com/in/joas-antonio-dos-santos

GOOGLE CLOUD SERVICES



Compute	Compute Engine	Kubernetes Engine	App Engine	Cloud Functions		
Management	Cloud Console	Stackdriver	Trace	Logging	Debugger	Monitoring
Networking	Cloud Load Balancing	Cloud CDN	Cloud DNS	Firewall Rules	Cloud Interconnect	Cloud VPN
Storage & Databases	Cloud Bigtable	Cloud Datastore	Cloud Spanner	Cloud SQL	Cloud Storage	
Big Data	BigQuery	Cloud Dataflow	Cloud Dataprep	Cloud Dataproc	Cloud IoT Core	Cloud Pub/Sub
Identity & Security	Cloud IAM	Cloud Endpoints	VPC	Identity Aware Proxy	KMS	Data Loss Prevention
Machine Learning	Cloud ML	Natural Language API	Cloud Speech API	Cloud Vision API	Cloud Translate API	

GCP PLATFORM

https://cloud.google.com/blog/products/identity-security/getting-started-with-identity-platform

https://support.google.com/a/answer/106368?hl=en#:~:text=With%20Google%20Cloud%20Directory%20Sync,files)%20to%20your%20Google%20Account.

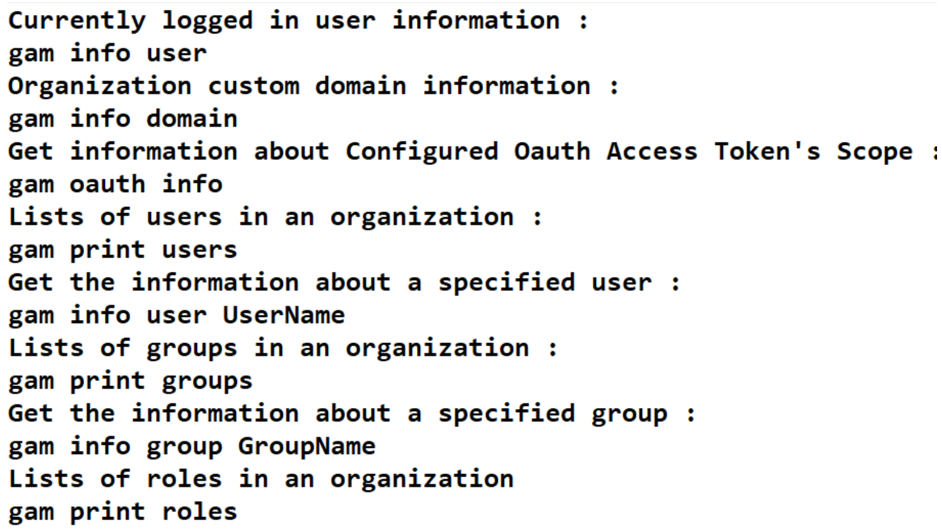
https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-synchronizing-user-accounts

https://www.youtube.com/watch?v=PJ0nR9vx38U (GSPS)

GCP PLATFORM #2

GAM is a command line tool for Google Workspace admins to manage domain and user settings quickly and easily.

GitHub - GAM-team/GAM: command line management for Google Workspace



```
Currently logged in user information :
gam info user
Organization custom domain information :
gam info domain
Get information about Configured Oauth Access Token's Scope :
gam oauth info
Lists of users in an organization :
gam print users
Get the information about a specified user :
gam info user UserName
Lists of groups in an organization :
gam print groups
Get the information about a specified group :
gam info group GroupName
Lists of roles in an organization
gam print roles
```

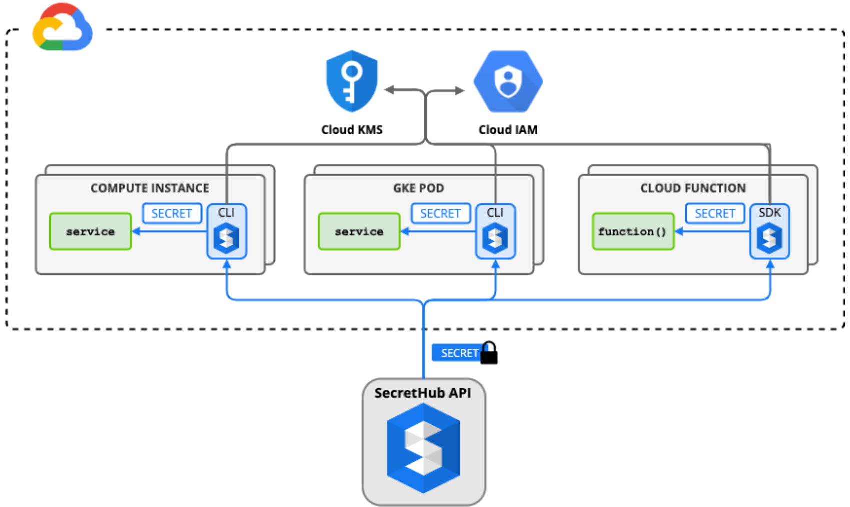
GCP PLATFFORM #3

Zones and Regions: https://cloud.google.com/compute/docs/regions-zones

API: https://cloud.google.com/apis/docs/overview

IAM: https://cloud.google.com/iam?hl=pt-br

https://www.trendmicro.com/cloudoneconformity-staging/knowledge-base/gcp/CloudIAM/



GCP PLATFORM #4

Type of member in GCP

○ Google Account

○ Service account

○ Google group

○ Google Workspace domain

○ Cloud Identity domain

○ All authenticated users

○ All users

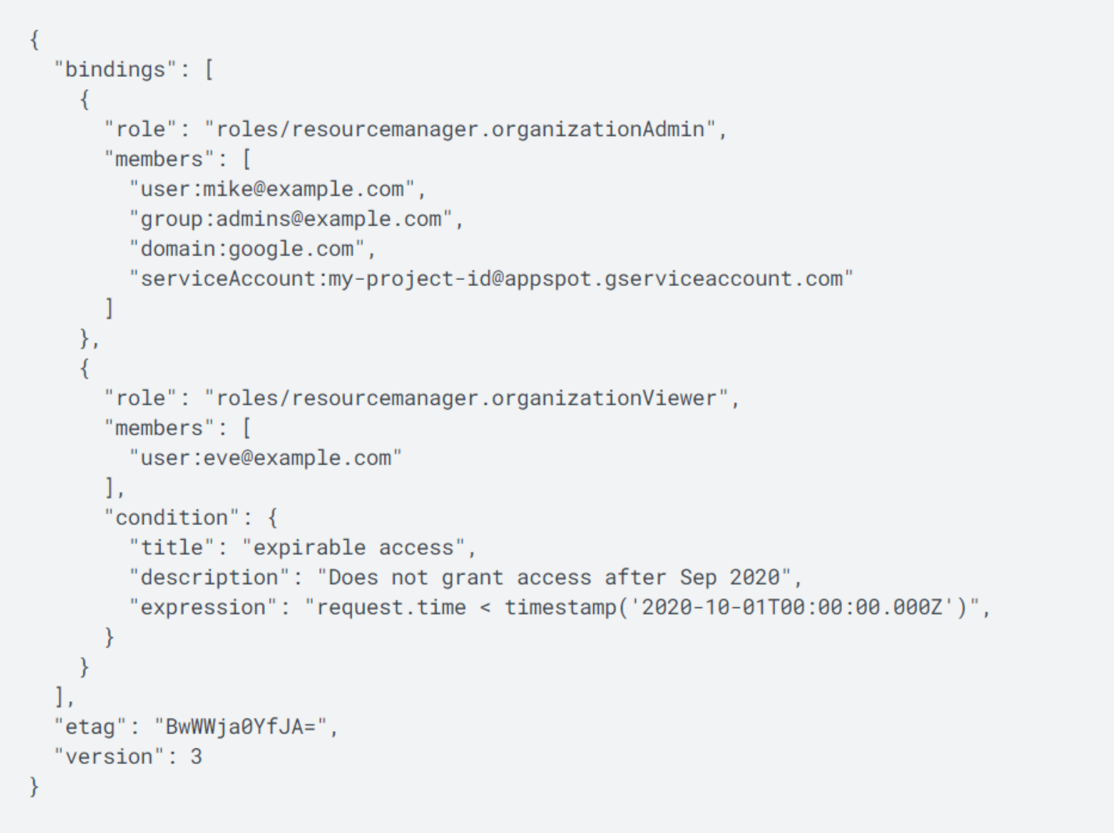
Type of roles in GCP

○ Basic roles: Roles historically available in the Google Cloud Console. These roles are Owner, Editor, and Viewer.

○ Predefined roles: Roles that give finer-grained access control than the basic roles.

○ Custom roles: Roles that you create to tailor permissions to the needs of your organization when predefined roles don't meet your needs.

GCP PLATFORM #5



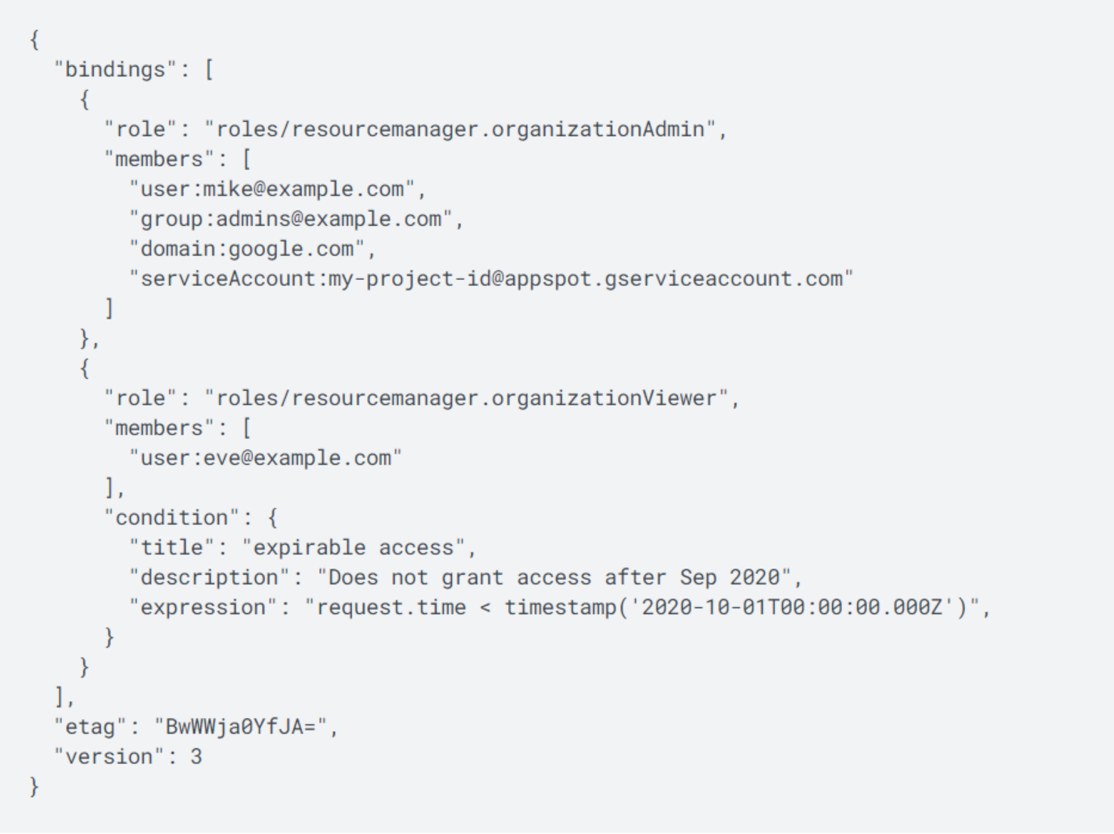
```
{
  "bindings": [
    {
      "role": "roles/resourcemanager.organizationAdmin",
      "members": [
        "user:mike@example.com",
        "group:admins@example.com",
        "domain:google.com",
        "serviceAccount:my-project-id@appspot.gserviceaccount.com"
      ]
    },
    {
      "role": "roles/resourcemanager.organizationViewer",
      "members": [
        "user:eve@example.com"
      ],
      "condition": {
        "title": "expirable access",
        "description": "Does not grant access after Sep 2020",
        "expression": "request.time < timestamp('2020-10-01T00:00:00.000Z')",
      }
    }
  ],
  "etag": "BwWWja0YfJA=",
  "version": 3
}
```

An Identity and Access Management (IAM) policy, which specifies access controls for Google Cloud resources.

A Policy is a collection of bindings. A binding binds one or more members, or principals, to a single role. Principals can be user accounts, service accounts, Google groups, and domains (such as G Suite). A role is a named list of permissions; each role can be an IAM predefined role or a user-created custom role.

For some types of Google Cloud resources, a binding can also specify a condition, which is a logical expression that allows access to a resource only if the expression evaluates to true. A condition can add constraints based on attributes of the request, the resource, or both. To learn which resources support conditions in their IAM policies, see the IAM documentation.

GCP PLATFORM #5



```
{
  "bindings": [
    {
      "role": "roles/resourcemanager.organizationAdmin",
      "members": [
        "user:mike@example.com",
        "group:admins@example.com",
        "domain:google.com",
        "serviceAccount:my-project-id@appspot.gserviceaccount.com"
      ]
    },
    {
      "role": "roles/resourcemanager.organizationViewer",
      "members": [
        "user:eve@example.com"
      ],
      "condition": {
        "title": "expirable access",
        "description": "Does not grant access after Sep 2020",
        "expression": "request.time < timestamp('2020-10-01T00:00:00.000Z')",
      }
    }
  ],
  "etag": "BwWWja0YfJA=",
  "version": 3
}
```

An Identity and Access Management (IAM) policy, which specifies access controls for Google Cloud resources.

A Policy is a collection of bindings. A binding binds one or more members, or principals, to a single role. Principals can be user accounts, service accounts, Google groups, and domains (such as G Suite). A role is a named list of permissions; each role can be an IAM predefined role or a user-created custom role.

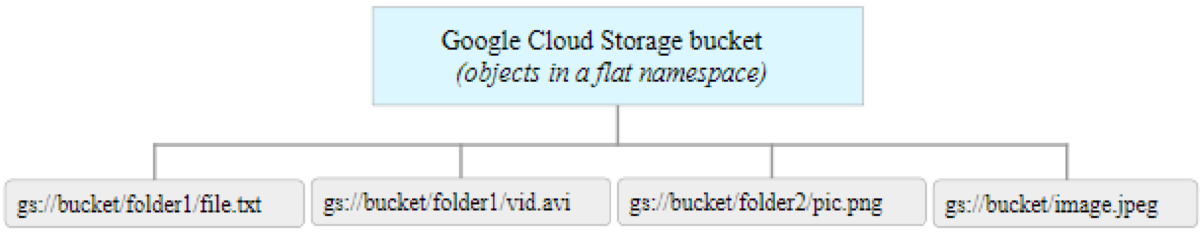
For some types of Google Cloud resources, a binding can also specify a condition, which is a logical expression that allows access to a resource only if the expression evaluates to true. A condition can add constraints based on attributes of the request, the resource, or both. To learn which resources support conditions in their IAM policies, see the IAM documentation.

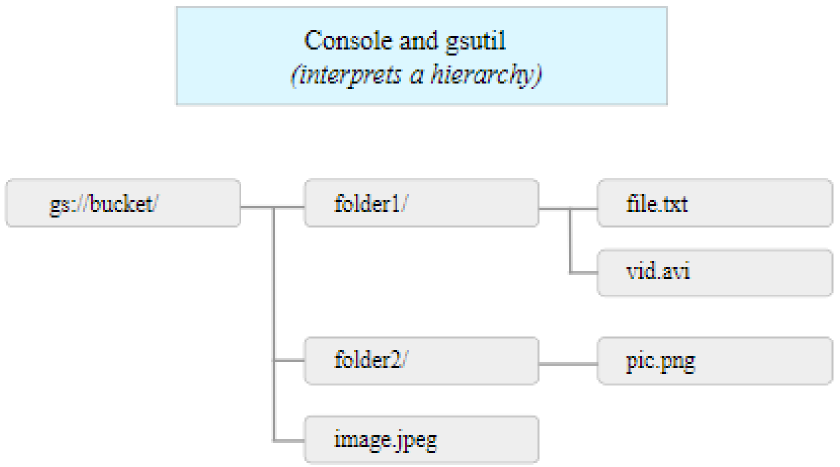
GCP PLATFORM #6

Auth methods:

- Web Access
- API – OAuth 2.0 protocol
- Access tokens – short lived access tokens for service accounts
- JSON Key Files – Long-lived key-pairs
- Credentials can be federated

GCP PLATFORM #7


Google Cloud Storage bucket
(objects in a flat namespace)
gs://bucket/folder1/file.txt
gs://bucket/folder1/vid.avi
gs://bucket/folder2/pic.png
gs://bucket/image.jpeg



The Buckets resource represents a bucket in Cloud Storage. There is a single global namespace shared by all buckets. For more information, see Bucket Name Requirements.

Buckets contain objects which can be accessed by their own methods. In addition to the acl property, buckets contain bucketAccessControls, for use in fine-grained manipulation of an existing bucket's access controls.

A bucket is always owned by the project team owners group.

https://cloud.google.com/storage/docs/json_api/v1/buckets

GCP PHISHING TECHNIQUES #1

Phising G-Suite:

- Calendar Event Injection
- Silently injects events to target calendars
- No email required
- Google API allows to mark as accepted
- Bypasses the “don’t auto-add” setting
- Creates urgency w/ reminder notification
- Include link to phishing page

GCP POST COMPROMISE TECHNIQUES #1

Post-compromise

- Cloud Storage, Compute, SQL, Resource manager, IAM
- ScoutSuite from NCC group

https://github.com/nccgroup/ScoutSuite

- Tool for auditing multiple different cloud security providers
- Create Google JSON token to auth as service account

GCP ENUMERATION TECHNIQUES #1

```
# Authentication with gcloud and retrieve info

gcloud auth login

gcloud auth activate-service-account --key-file creds.json

gcloud auth activate-service-account --project=<projectid> --key-file=filename.json

gcloud auth list

gcloud init

gcloud config configurations activate stolenkeys

gcloud config list

gcloud organizations list

gcloud organizations get-iam-policy <org ID>
```

```
gcloud projects get-iam-policy <project ID>

gcloud iam roles list  --project=<project ID>

gcloud beta asset search-all-iam-policies --query policy:"projects/xxxxxxxx/roles/CustomRole436" --project=xxxxxxxx

gcloud projects list

gcloud config set project <project name>

gcloud services list

gcloud projects list

gcloud config set project [Project-Id]

gcloud source repos list

gcloud source repos clone <repo_name>
```

GCP ENUMERATION TECHNIQUES #2

```
gcloud compute instances list

gcloud compute instances list --impersonate-service-account AccountName

gcloud compute instances list --configuration=stolenkeys

gcloud compute instances describe <instance id>

gcloud compute instances describe <InstanceName> --zone=ZoneName --format=json | jq -c '.serviceAccounts[].scopes[]'

gcloud beta compute ssh --zone "<region>" "<instance name>" --project "<project name>"

# Puts public ssh key onto metadata service for project

gcloud compute ssh <local host>

curl http://metadata.google.internal/computeMetadata/v1/instance/service-accounts/default/scopes -H &#39;Metadata-Flavor:Google’

# Use Google keyring to decrypt encrypted data

gcloud kms decrypt --ciphertext-file=encrypted-file.enc --plaintext-file=out.txt --key <crypto-key> --keyring <crypto-keyring> --location global
```

GCP ENUMERATION TECHNIQUES #3

```
# Storage Buckets
```

List Google Storage buckets

```
gsutil ls

gsutil ls -r gs://<bucket name>

gsutil cat gs://bucket-name/anyobject

gsutil cp gs://bucketid/item ~/
```

```
# Webapps & SQL

gcloud app instances list

gcloud sql instances list

gcloud spanner instances list

gcloud bigtable instances list

gcloud sql databases list --instance <instance ID>

gcloud spanner databases list --instance <instance name>> --location global
```

GCP ENUMERATION TECHNIQUES #4

```
# Networking

gcloud compute networks list

gcloud compute networks subnets list

gcloud compute vpn-tunnels list

gcloud compute interconnects list

gcloud compute firewall-rules list

gcloud compute firewall-rules describe
<rulename>
```

```
# Containers

gcloud container clusters list

# GCP Kubernetes config file
~/.kube/config gets generated when you
are authenticated with

gcloud container clusters get-credentials
<cluster name> –-region <region>

kubectl cluster-info
```

GCP ENUMERATION TECHNIQUES #5

```
 Serverless (Lambda functions)

gcloud functions list

gcloud functions describe <function name>

gcloud functions logs read <function name> --limit <number of lines>

# Gcloud stores creds in ~/.config/gcloud/credentials.db Search home directories

sudo find /home -name "credentials.db

# Copy gcloud dir to your own home directory to auth as the compromised user

sudo cp -r /home/username/.config/gcloud ~/.config

sudo chown -R currentuser:currentuser ~/.config/gcloud

gcloud auth list
```

```
# Databases

gcloud sql databases list

gcloud sql backups list --instance=test

# Metadata Service URL

# metadata.google.internal = 169.254.169.254

curl "http://metadata.google.internal/computeMetadata/v1/?recursive=true&alt=text" -H

"Metadata-Flavor: Google"
```

https://github.com/six2dez/pentest-book/blob/master/enumeration/cloud/gcp.md

GCP ATTACKS #1

https://gitlab.com/gitlab-com/gl-security/threatmanagement/redteam/redteam-public/red-team-tech-notes/-/blob/master/gcp-post-exploitation-feb-2020/README.md

https://www.youtube.com/watch?v=E1Yz4ofKEz0

https://www.youtube.com/watch?v=AwXswDg-rKc

https://www.youtube.com/watch?v=GvO2Xtx8p9w

GCP ATTACKS #2

https://rhinosecuritylabs.com/gcp/privilege-escalation-google-cloud-platform-part-1/

https://rhinosecuritylabs.com/cloud-security/privilege-escalation-google-cloud-platform-part-2/

https://rhinosecuritylabs.com/gcp/google-cloud-platform-gcp-bucket-enumeration/

https://rhinosecuritylabs.com/gcp/iam-privilege-escalation-gcp-cloudbuild/

https://rhinosecuritylabs.com/cloud-security/kubelet-tls-bootstrap-privilege-escalation/

https://cloud.google.com/blog/products/identity-security/announcing-mitre-attck-mappings-released-for-google-cloud-security-capabilities

https://medium.com/@tomaszwybraniec/google-cloud-platform-pentest-notes-service-accounts-b960dc59d93a

GCP ATTACKS #3

The PrivEscScanner Folder

Contains a permissions enumerator for all members in a GCP account and an associated privilege escalation scanner that reviews the permissions in search of privilege escalation vulnerabilities.

First run enumerate_member_permissions.py to enumerate all members and permissions and then run check_for_privesc.py to check for privilege escalation in the environment.

The ExploitScripts Folder

Contains exploit scripts for each of the privilege escalation methods outlined in the blog post, as well as a Cloud Function and Docker image for some of the methods that require them.

https://github.com/RhinoSecurityLabs/GCP-IAM-Privilege-Escalation

GCP ATTACKS #4

https://medium.com/swlh/kubernetes-attack-path-part-2-post-initial-access-1e27aabda36d

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

https://about.gitlab.com/blog/2020/02/12/plundering-gcp-escalating-privileges-in-google-cloud-platform/

https://cloud.google.com/kubernetes-engine/docs/resources/security-patching?hl=pt-br

https://www.youtube.com/watch?v=L_ej12aahNI

https://89berner.medium.com/persistant-gcp-backdoors-with-googles-cloud-shell-2f75c83096ec

https://sysdig.com/blog/gcp-security-best-practices/

https://www.netskope.com/blog/gcp-oauth-token-hijacking-in-google-cloud-part-1

https://www.netskope.com/blog/targeted-attacks-abusing-google-cloud-platform-open-redirection

https://www.systoolsgroup.com/how-to/report-ip-abuse/

https://threatpost.com/hackers-abuse-google-cloud-platform-to-attack-d-link-routers/143492/

https://github.com/dxa4481/AttackingAndDefendingTheGCPMetadataAPI

https://github.com/4ndersonLin/awesome-cloud-security

EXTRAS AND TRAININGS

https://github.com/kh4sh3i/cloud-penetration-testing

https://github.com/Littlehack3r/awesome-gcp-pentesting

https://www.cyberwarfare.live/

https://www.sans.org/cyber-security-courses/cloud-penetration-testing/

https://www.getastra.com/blog/security-audit/google-cloud-penetration-testing/