

About Scout Suite

Scout Suite is an open source multi-cloud security-auditing tool, which enables security posture assessment of cloud environments. Using the APIs exposed by cloud providers, Scout Suite gathers configuration data for manual inspection and highlights risk areas. Rather than going through dozens of pages on the web consoles, Scout Suite presents a clear view of the attack surface automatically.

Scout Suite was designed by security consultants/auditors. It is meant to provide a point-in-time security-oriented view of the cloud account it was run in. Once the data has been gathered, all usage may be performed offline.

Usage

Start up the ScoutSuite container:

```
root@ip-10-0-1-114:~# cd /shared/
root@ip-10-0-1-114:/shared# mkdir -p /shared/scoutsuite-report
root@ip-10-0-1-114:/shared# cnoio_scoutsuite
...
(scoutsuite) root@6888ac22c10d:~#
```

Run the audit and vulnerability scan via the service account credentials:

```
(scoutsuite) root@6888ac22c10d:~# scout gcp -s /shared/gcploit/key.json --all-projects
2021-07-27 03:47:55 6888ac22c10d scout[12] INFO Launching Scout
2021-07-27 03:47:55 6888ac22c10d scout[12] INFO Authenticating to cloud provider
2021-07-27 03:47:58 6888ac22c10d scout[12] INFO Gathering data from APIs
...
2021-07-27 03:48:51 6888ac22c10d scout[12] INFO Saving data to scoutsuite-report/scoutsuite-results/scoutsuite_results_gcp-test002@gcptraininggce001.iam.gserviceaccount.com.js
2021-07-27 03:48:51 6888ac22c10d scout[12] INFO Saving data to scoutsuite-report/scoutsuite-results/scoutsuite_exceptions_gcp-test002@gcptraininggce001.iam.gserviceaccount.com.js
2021-07-27 03:48:51 6888ac22c10d scout[12] INFO Saving data to scoutsuite-report/scoutsuite-results/scoutsuite_errors_gcp-test002@gcptraininggce001.iam.gserviceaccount.com.json
2021-07-27 03:48:51 6888ac22c10d scout[12] INFO Creating scoutsuite-report/gcp-test002@gcptraininggce001.iam.gserviceaccount.com.html
2021-07-27 03:48:51 6888ac22c10d scout[12] INFO Opening the HTML report
...
```

Now exit out of ScoutSuite...

```
...
(scoutsuite) root@6888ac22c10d:~# exit
...
root@ip-10-0-1-114:/shared#
```

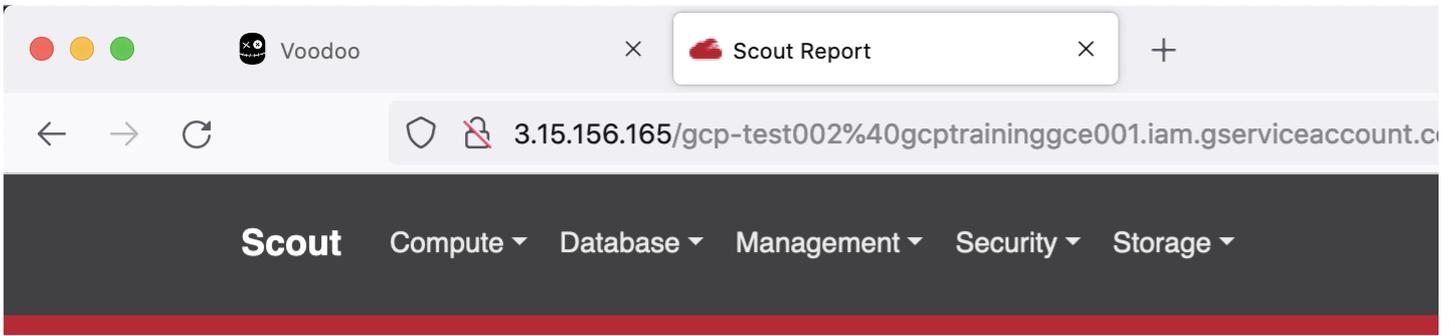
And host the files via the python SimpleHTTPServer...

```
root@ip-10-0-1-114:/shared# cd /shared/scoutsuite-report
root@ip-10-0-1-114:/shared/scoutsuite-report# curl ipcurl.net/n
3.15.156.165
root@ip-10-0-1-114:/shared/scoutsuite-report# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

And browse to the server...

```
http://ip.ip.ip:80
```

And then click on the HTML result file (e.g. gcp-test002@gcptraininggce001.iam.gserviceaccount.com.html):



 Google Cloud Platform > test002@gcptraininggce001

Dashboard

Service	Resources	Rules
<input type="radio"/> Cloud SQL	0	6
<input type="radio"/> Cloud Storage	2	4
<input type="radio"/> Compute Engine	36	11
<input type="radio"/> IAM	10	9
<input type="radio"/> KMS	0	0
<input type="radio"/> Kubernetes Engine	0	19
<input checked="" type="radio"/> Stackdriver Logging	2	1
<input type="radio"/> Stackdriver Monitoring	0	0

We can now view these findings via this web interface...

Voodoo Scout Report

3.15.156.165/gcp-test002%40gcptraininggce001.iam.gserviceaccount.c

Scout Compute Database Management Security Storage

Compute Engine Dashboard

Filter findings

Show All

Good

- ! Default Firewall Rule in Use
- ! Firewall INGRESS Rule Allows Public Access (0.0.0.0/0) to a Sensitive Port
- ! Firewall Rule Allows Internal Traffic
- ! Firewall Rule Allows Public Access (0.0.0.0/0)
- ! Firewall Rule Allows Public Access (0.0.0.0/0) to All Ports (0-65535)
- ! Firewall Rule Opens All Ports (0-65535)
- ! Instance Disk without Snapshots
- ! Instance without Deletion Protection

Above & Beyond!

- Try ScoutSuite on the AWS environment
- Try ScoutSuite on the Azure environment

References:

- ScoutSuite - <https://github.com/nccgroup/ScoutSuite>