The Plan:

- Browse to the web application to discover a RCE vulnerability...

-- Typical Pod/Container on GKE: http://34.85.215.94/

-- Privileged Pod/Container on GKE: http://34.85.197.48/

- Create a Voodoo no inject stager

- Leverage the RCE vulnerability in the web app to execute the Voodoo stager

- Enumerate Containers via the below techniques with the amicontained tool

Analyze

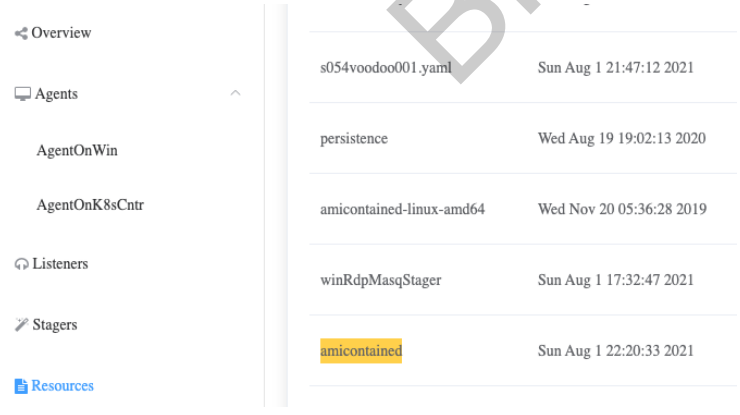
On the Voodoo LP, let's update the amicontained tool to the latest version via the following commands:

```
rm /shared/voodoo_ce/app/resources/amicontained

wget -O /shared/voodoo_ce/app/resources/amicontained https://public-astute-cloud-20200813-935672326788.s3.amazonaws.com/amicontained

chmod 644 -R /shared/voodoo_ce/app/resources

chown root:root -R /shared/voodoo_ce/app/resources

ls -alF /shared/voodoo_ce/app/resources/amicontained
```

We should see output similar to the following:

```
root@ip-10-0-1-110:/shared# rm /shared/voodoo_ce/app/resources/amicontained

root@ip-10-0-1-110:/shared# wget -O /shared/voodoo_ce/app/resources/amicontained https://public-astute-cloud-20200813-935672326788.s3.amazonaws.com/amicontained
--2021-08-01 22:21:48-- https://public-astute-cloud-20200813-935672326788.s3.amazonaws.com/amicontained
Resolving public-astute-cloud-20200813-935672326788.s3.amazonaws.com (public-astute-cloud-20200813-935672326788.s3.amazonaws.com)... 52.216.226.144
Connecting to public-astute-cloud-20200813-935672326788.s3.amazonaws.com (public-astute-cloud-20200813-935672326788.s3.amazonaws.com)|52.216.226.144|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6079078 (5.8M) [binary/octet-stream]
Saving to: '/shared/voodoo_ce/app/resources/amicontained'

/shared/voodoo_ce/app/resources/amicontained 100%
[=============================================================================================================================>]
5.80M 25.3MB/s in 0.2s

2021-08-01 22:21:49 (25.3 MB/s) - '/shared/voodoo_ce/app/resources/amicontained' saved [6079078/6079078]

root@ip-10-0-1-110:/shared# chmod 644 -R /shared/voodoo_ce/app/resources

root@ip-10-0-1-110:/shared# chown root:root -R /shared/voodoo_ce/app/resources

root@ip-10-0-1-110:/shared# ls -alF /shared/voodoo_ce/app/resources/amicontained
-rw-r--r-- 1 root root 6079078 Aug 1 22:20 /shared/voodoo_ce/app/resources/amicontained

root@ip-10-0-1-110:/shared# sha512sum /shared/voodoo_ce/app/resources/amicontained
bd239d597617f983f5c413818bc0a259d6a54747c1d6137030c8b3271876ef16089c4d65a4b6f3904a362b193bfcb11a7257315c2d773fba1f074384d0c0e480 /shared/voodoo_ce/app/resources/amicontained

root@ip-10-0-1-110:/shared#
```

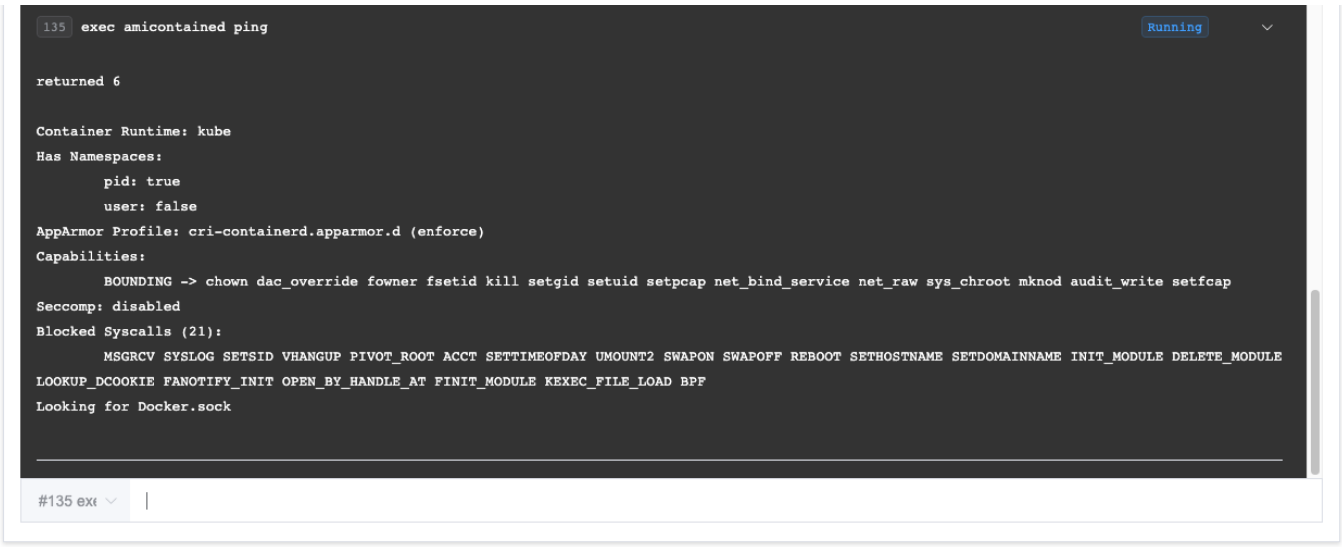
We should now see the amicontained binary in the "Resources" section of the Voodoo operator web interface...



Now we will execute the binary via the Voodoo web interface...

```
exec amicontained ping
```

We should see output similar to the following:



Note, sometimes this application hangs, if it does so for you, leverage the “stoptask” command in voodoo to stop the command gracefully.

First switch the voodoo prompt back to the operator interface, via clicking the dropdown in the lower left hand corner of the command interface and clicking on the ">" link...

Then leverage the “stoptask” command in voodoo to stop the command gracefully...

```
stoptask <Task # In Voodoo>
```

We should see output similar to the following:

References

References includes:

- https://github.com/genuinetools/amicontained/releases
- https://github.com/wagoodman/dive