

# PERFORMING S3 - ENUMERATION



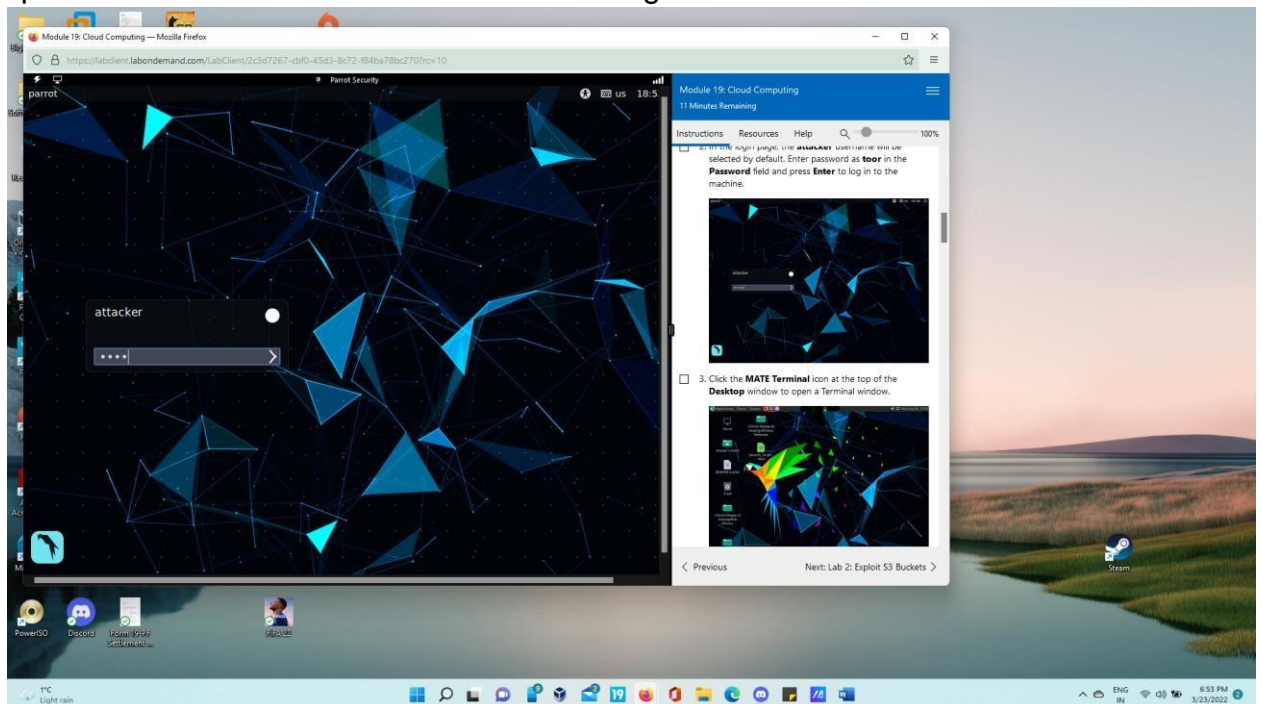
## Contents

Lab 1: Perform S3 Bucket Enumeration using Various S3 Bucket Enumeration Tools .....	2
Task 1: Enumerate S3 Buckets using lazys3 .....	2
Task 2: Enumerate S3 Buckets using S3Scanner .....	5
Lab 2: Exploit S3 Buckets .....	8
Lab 3: Perform Privilege Escalation to Gain Higher Privileges .....	15
Task 1: Escalate IAM User Privileges by Exploiting Misconfigured User Policy .....	15

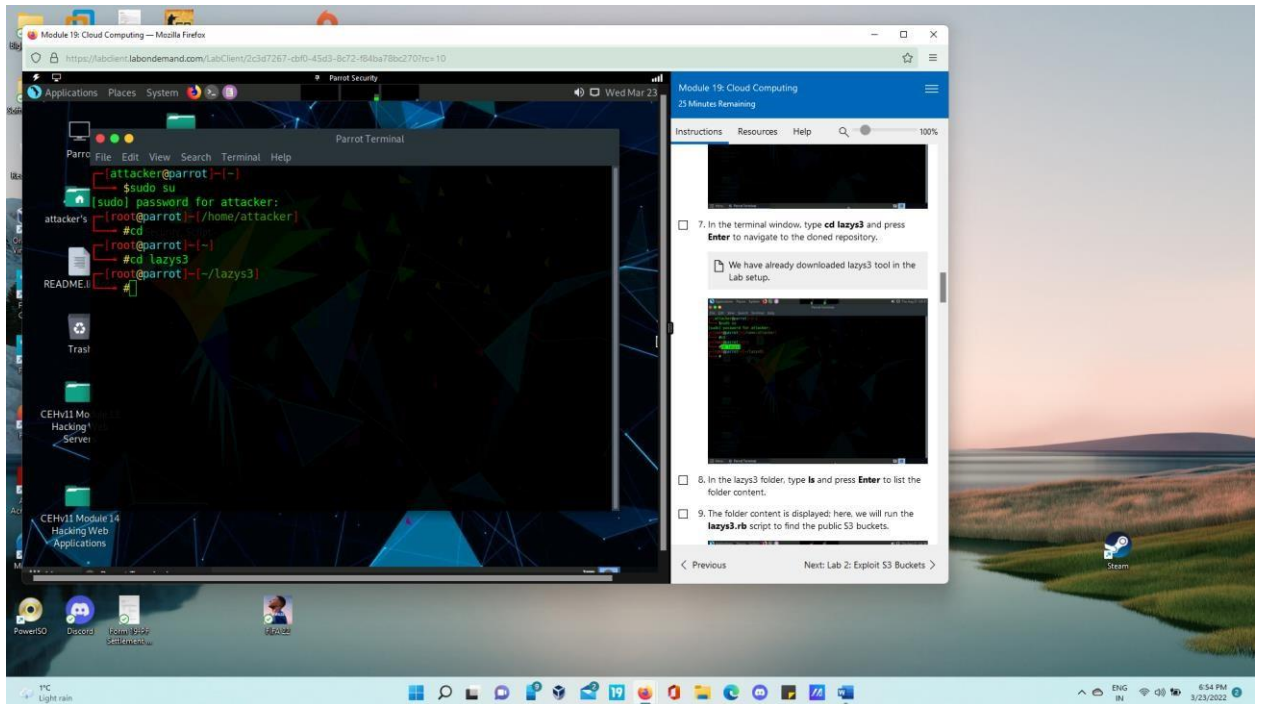
# Lab 1: Performing S3-Bucket Enumeration using S3-Bucket Enumeration Tools

## Task 1: Enumerate S3 Buckets using lazys3

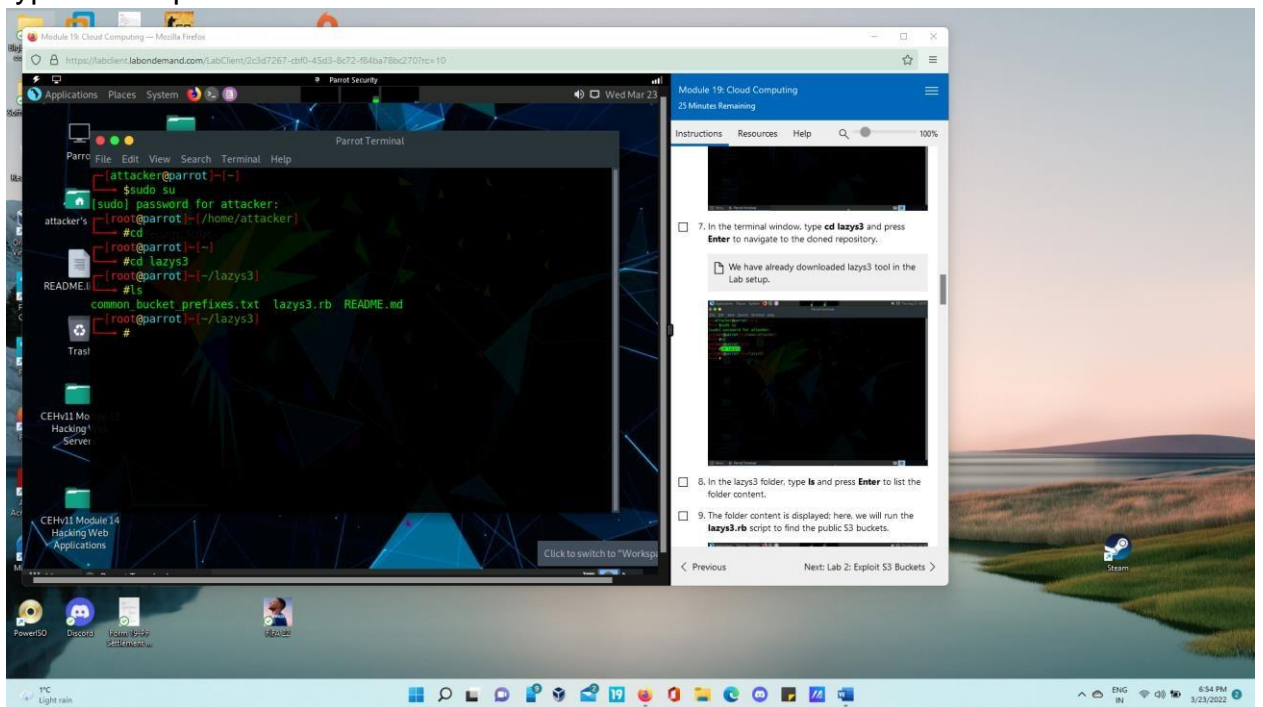
- Open Parrot Machine and in Mate terminal Login as root user.



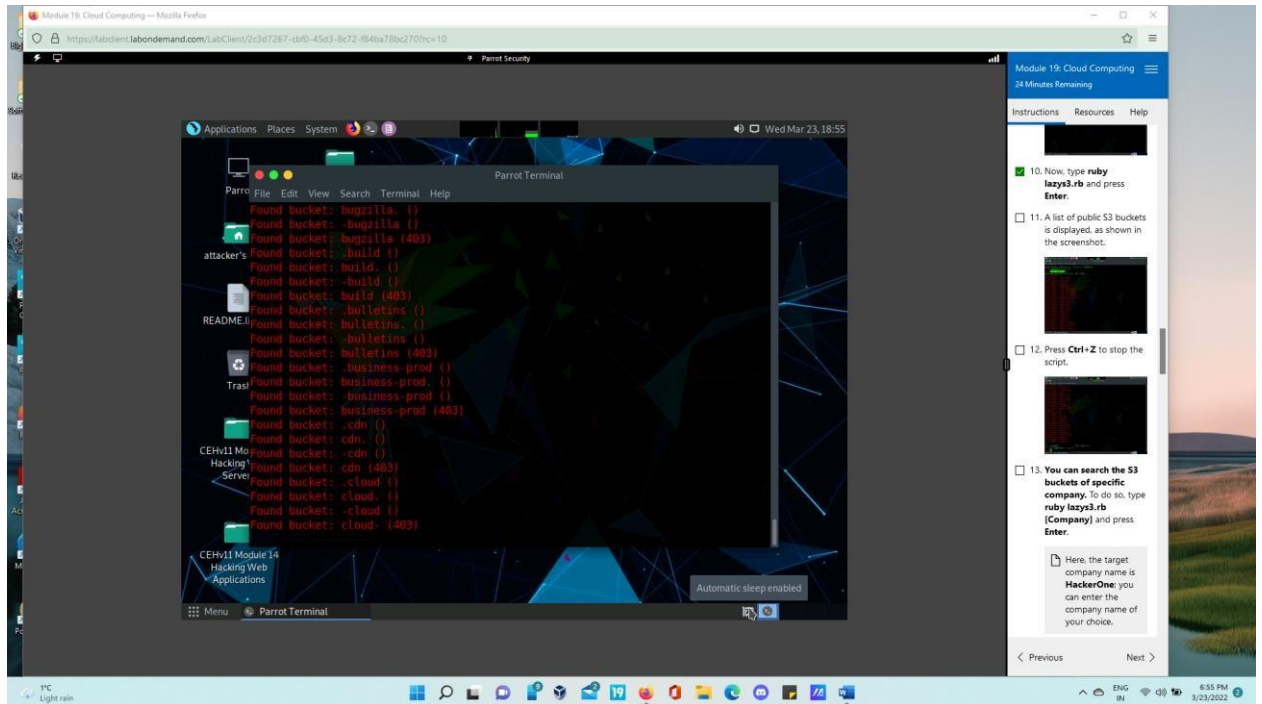
- In the terminal, type command `cd lazys3`.



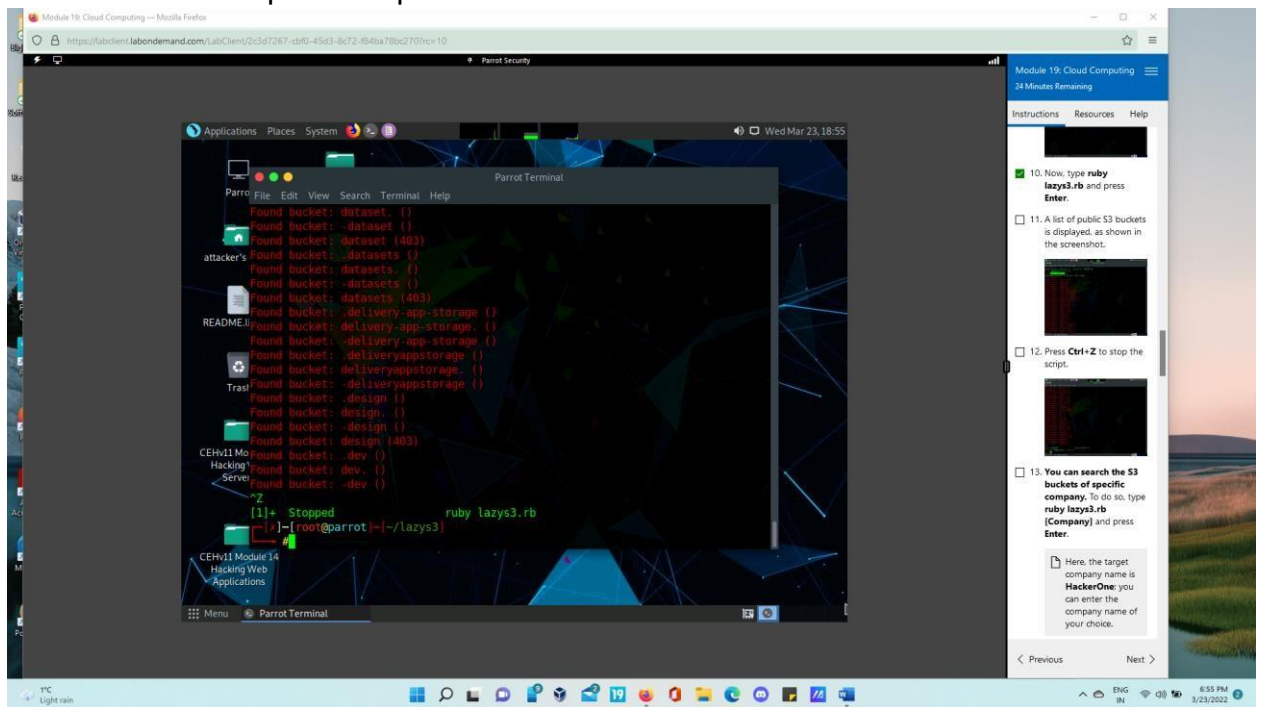
- Type **ls** and press **Enter**.



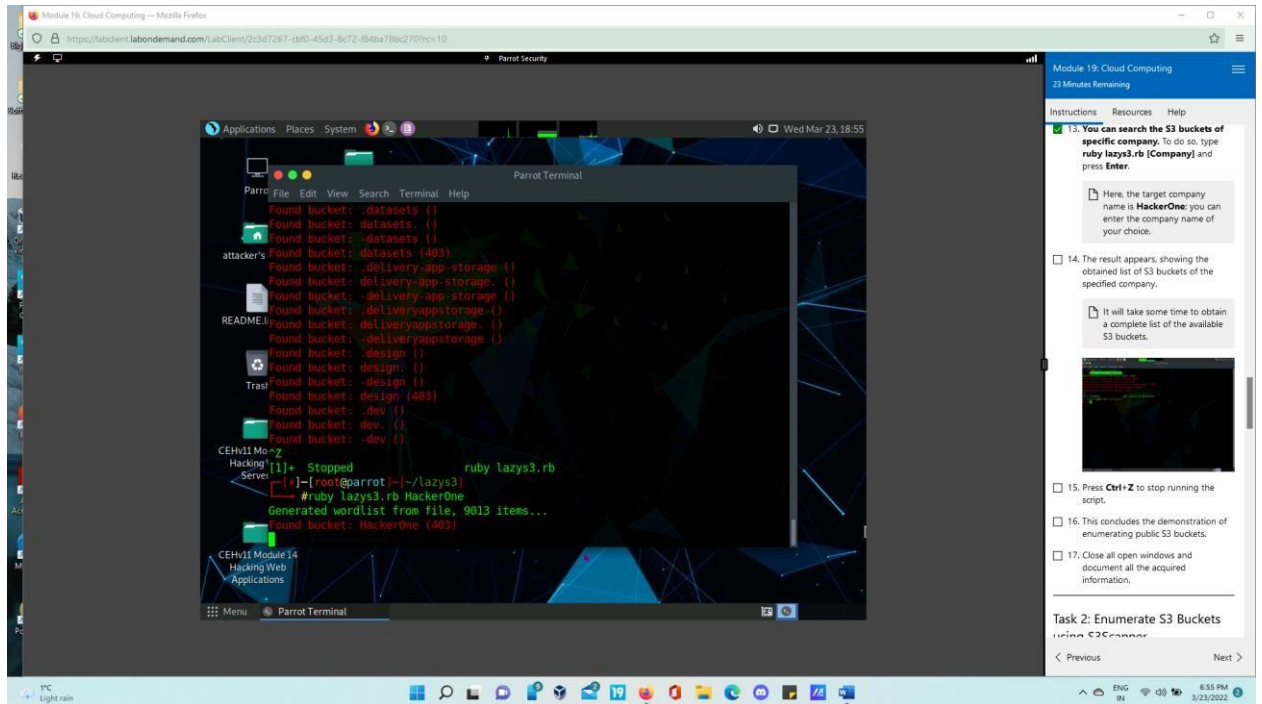
- Type **ruby lazys3.rb** and press **Enter** key.



- Press **Ctrl+Z** to stop the script.



- Type **ruby lazys3.rb [Company]** and press **Enter**.



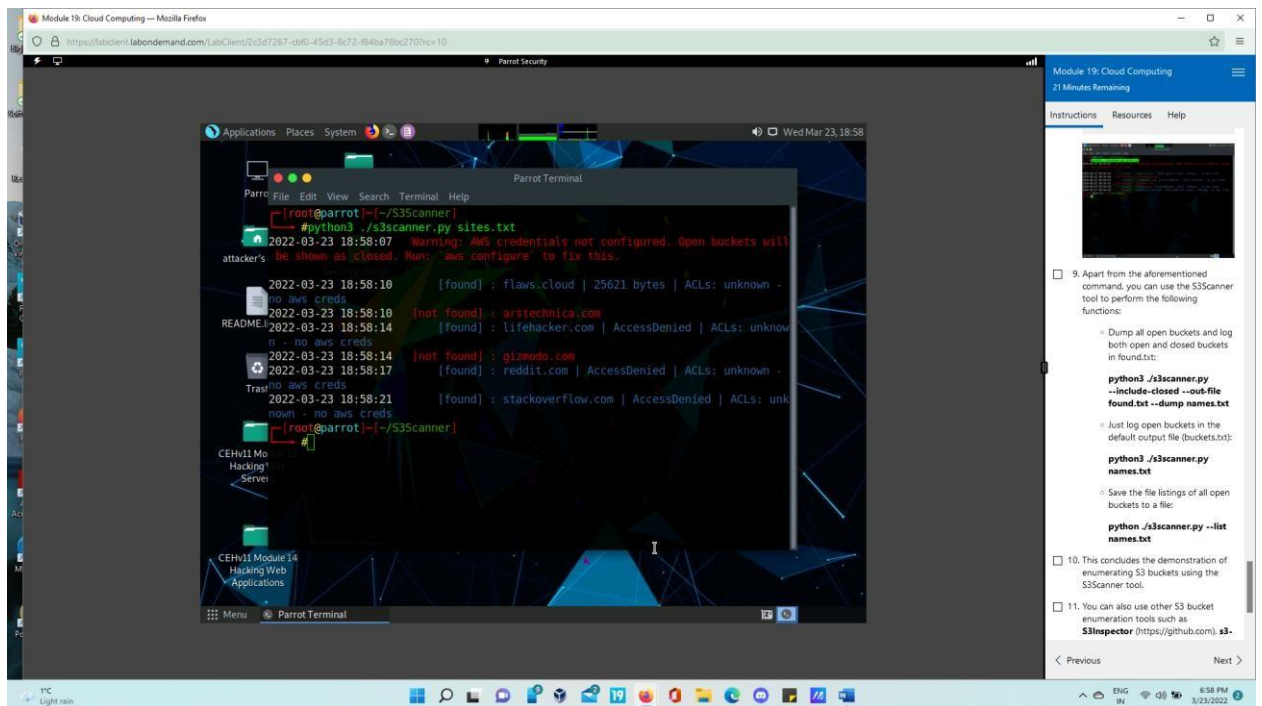
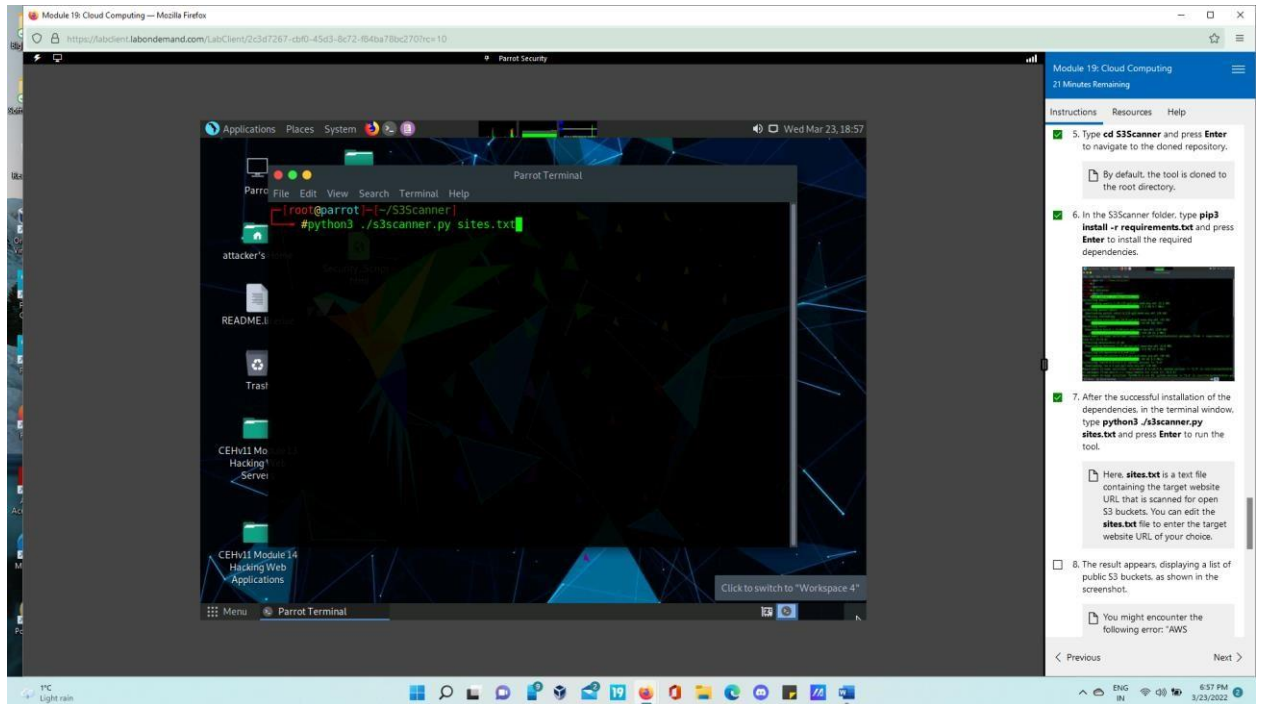
- Press **Ctrl+Z** to stop the running script.

## Task 2: Enumerate S3 Buckets using S3Scanner

- Click the **MATE Terminal** and login as root user.





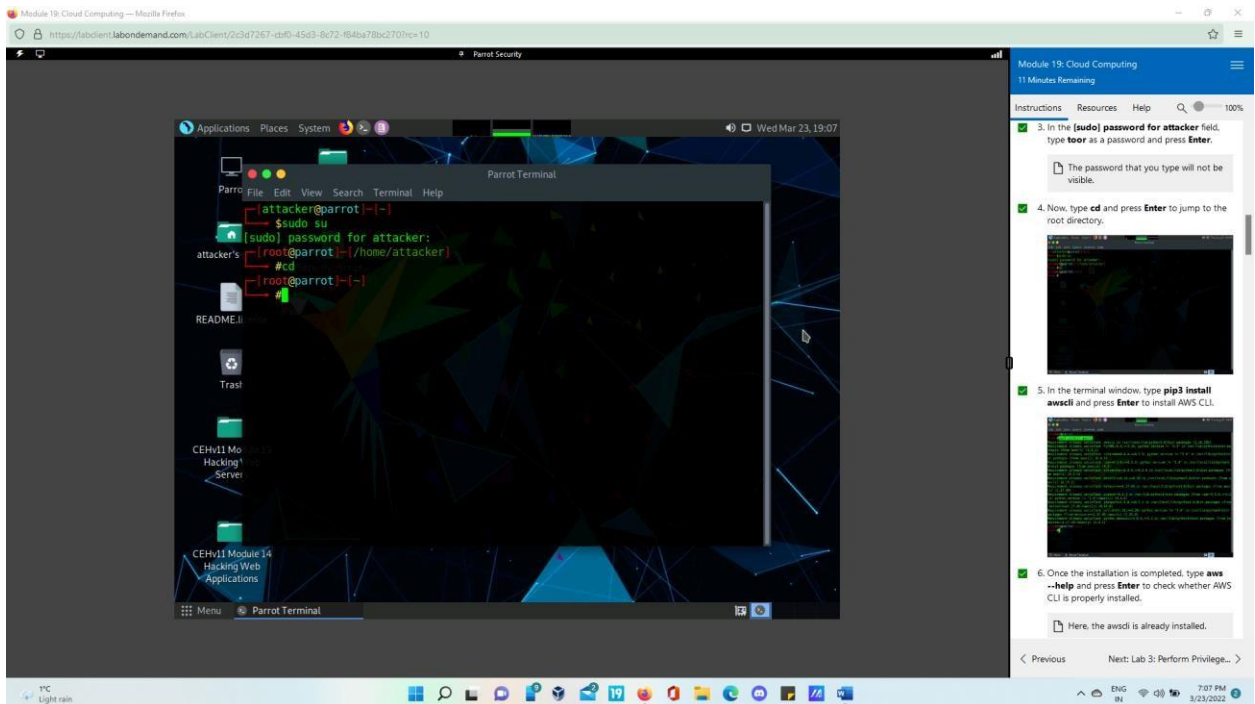


- This displays list of S3 buckets

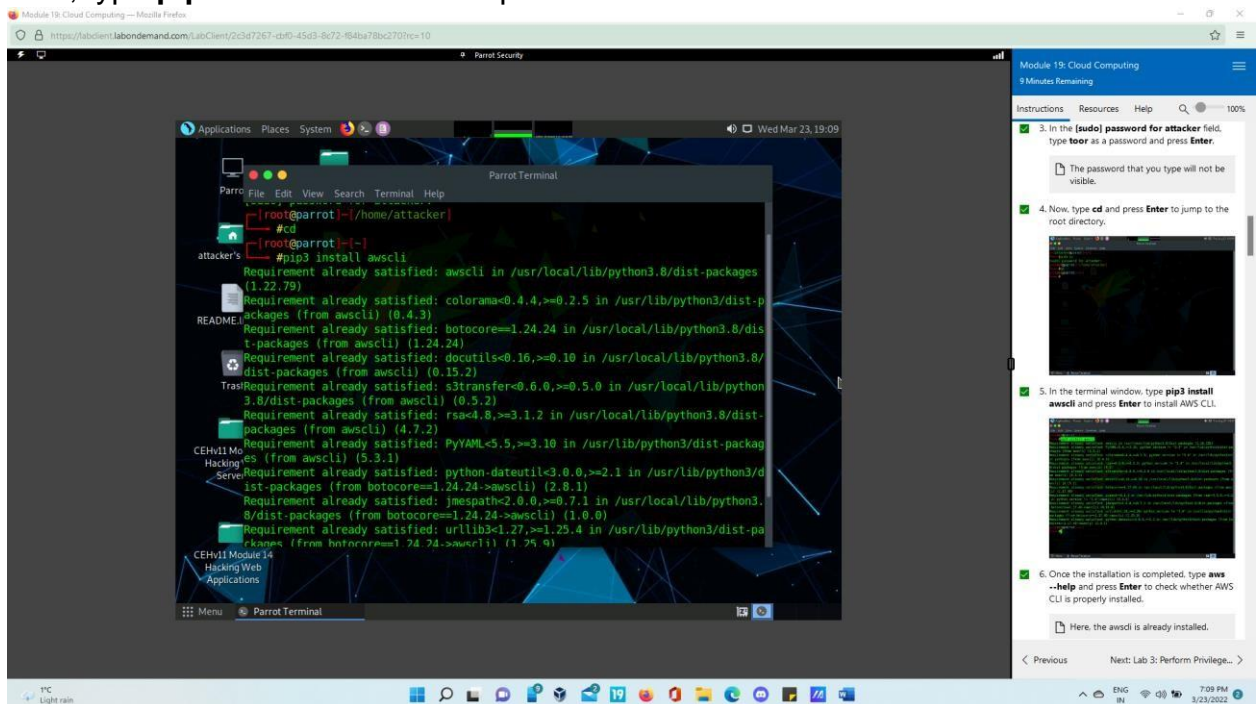
## Lab 2: Exploit S3 Buckets

- Login as root user.

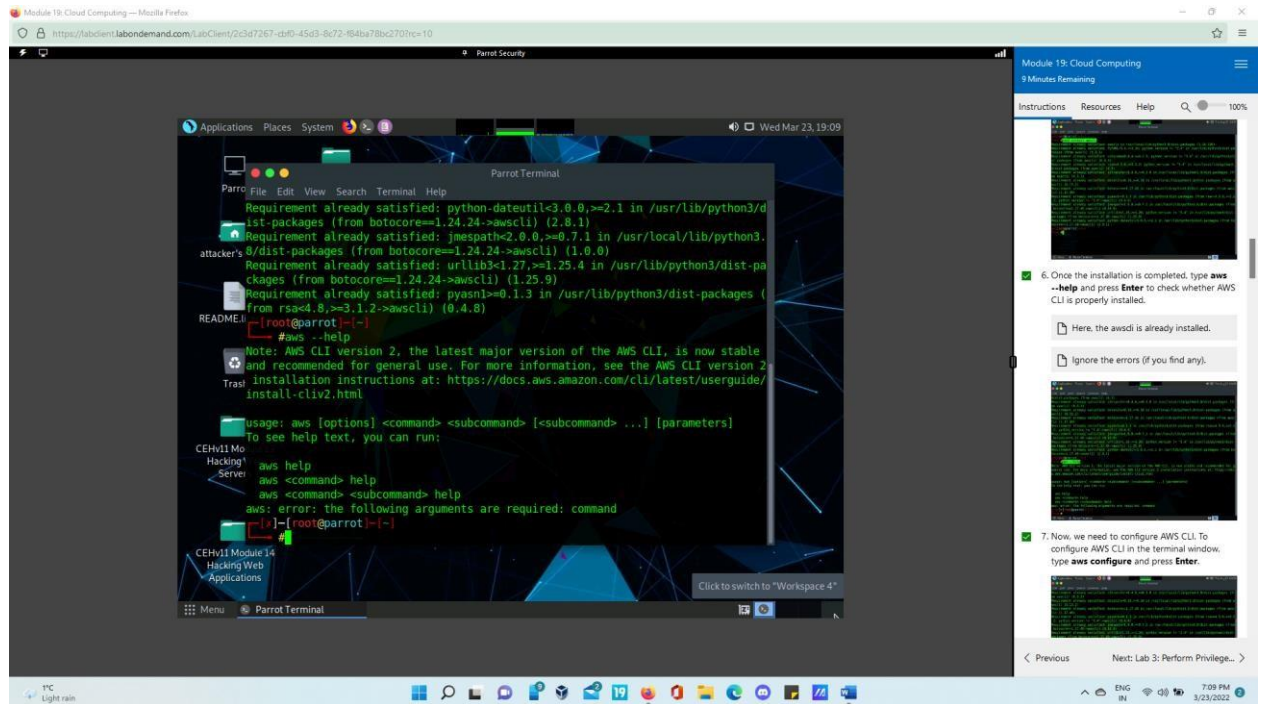




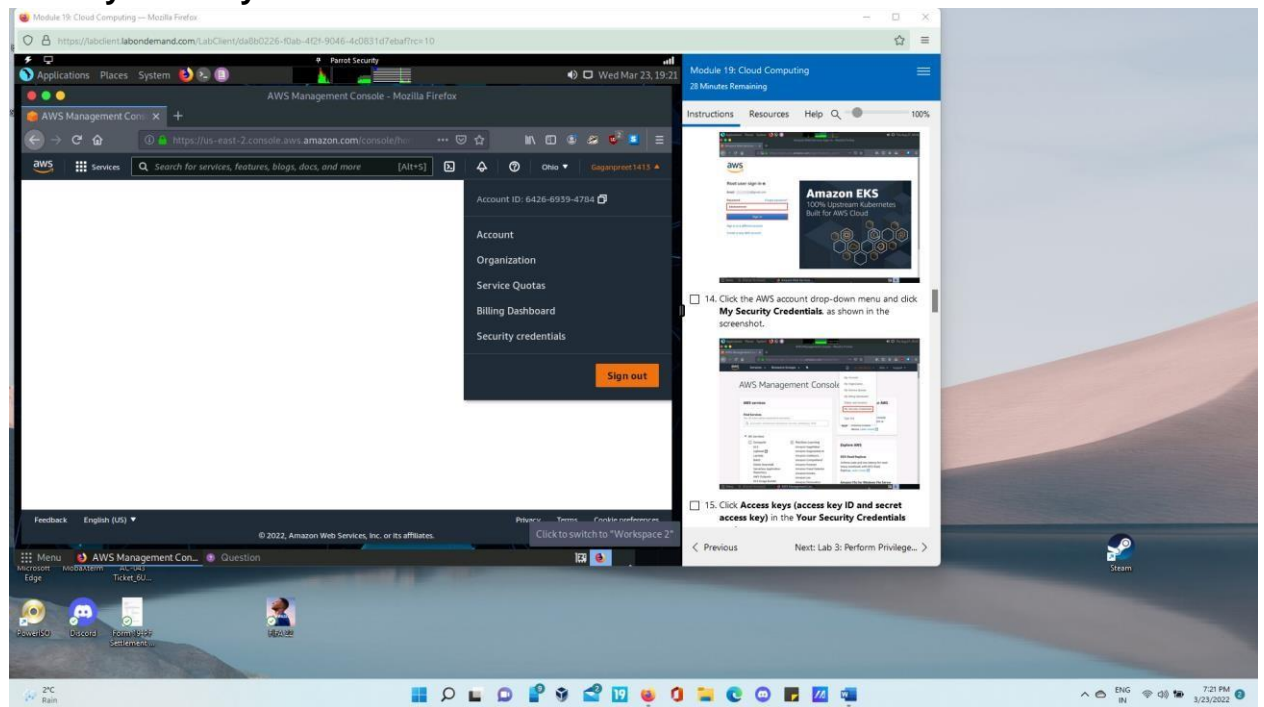
- Now, type **pip3 install awscli** and press **Enter**.



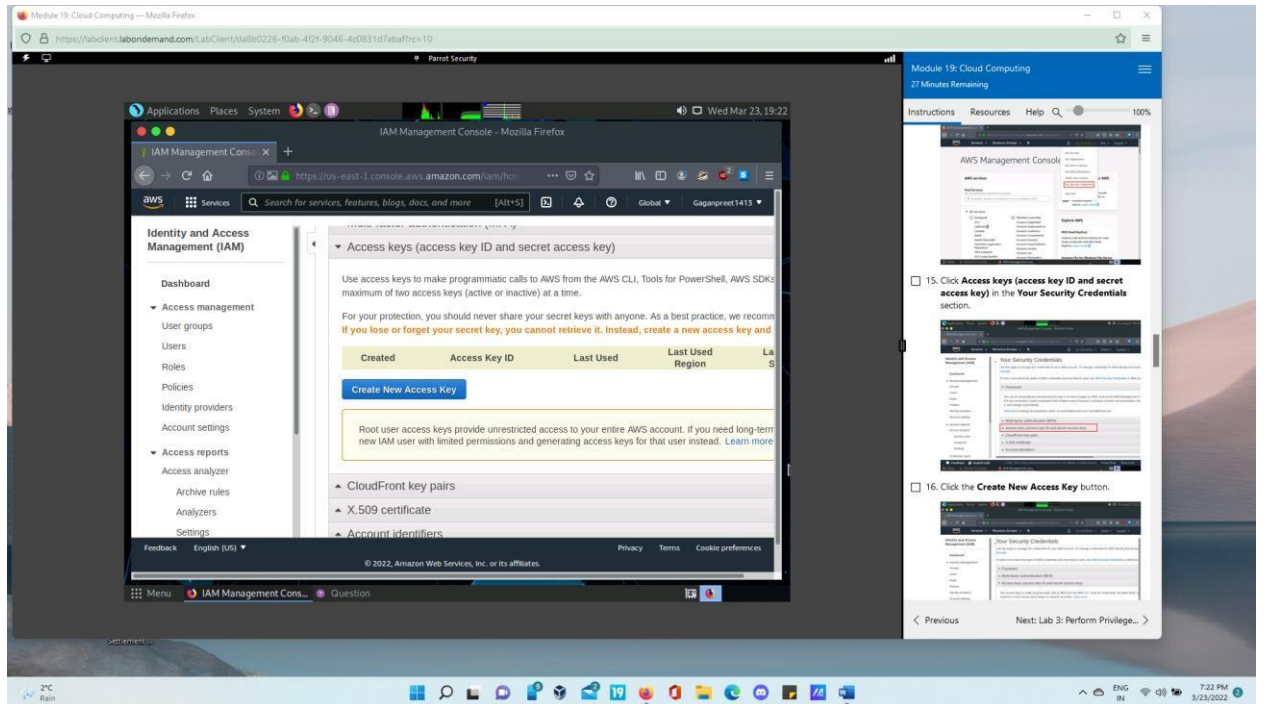
- Now type **aws --help** and press **Enter**



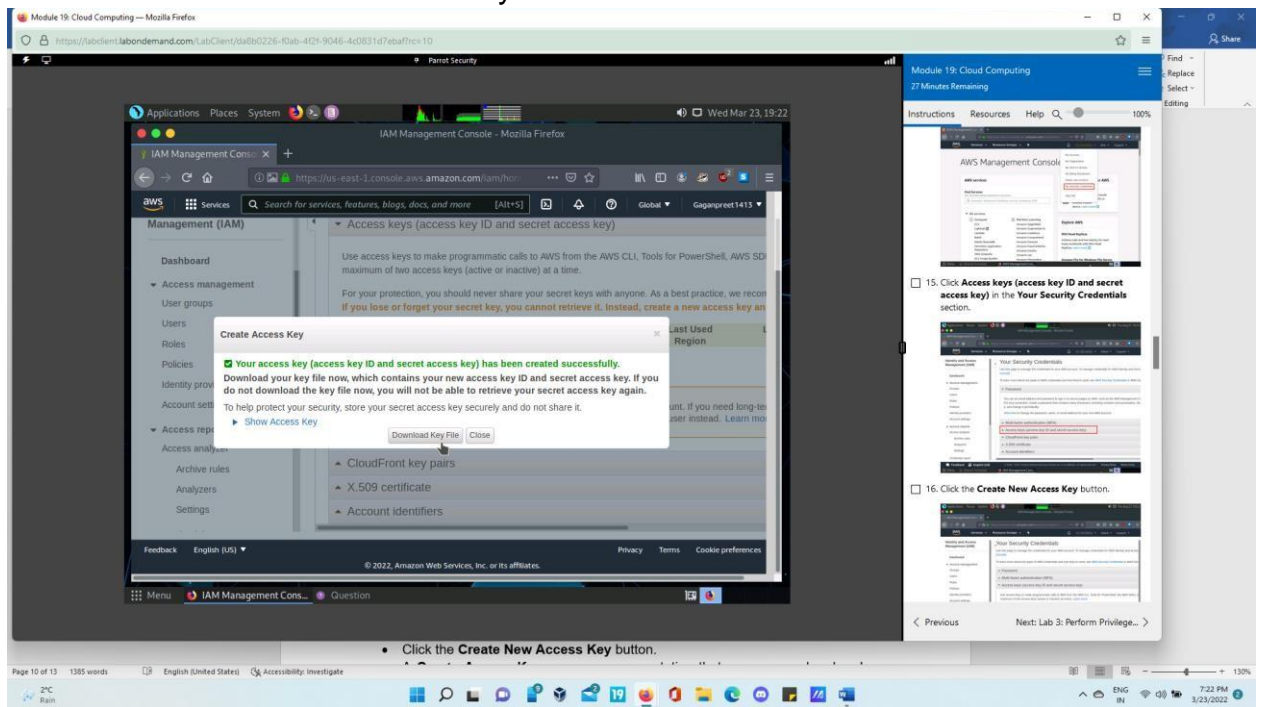
- click **My Security Credentials**.



- Click **Access keys** in the **Your Security Credentials**

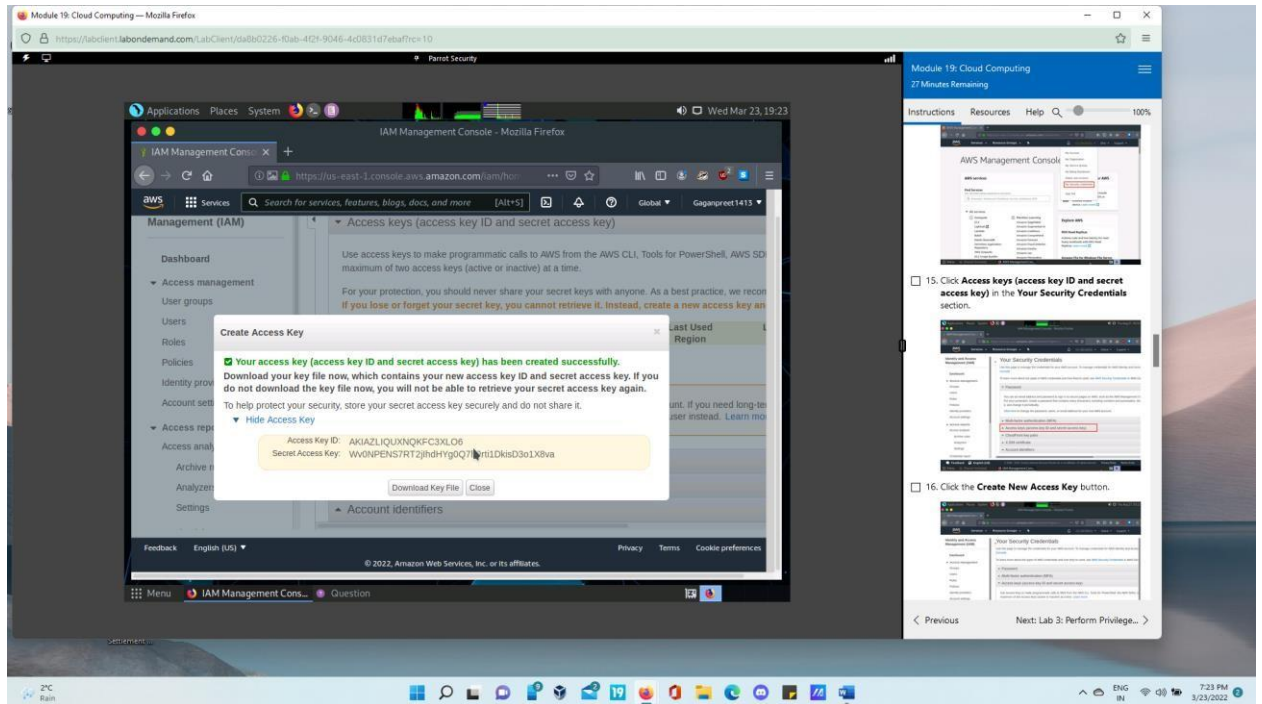


- Click on the create new access key button.

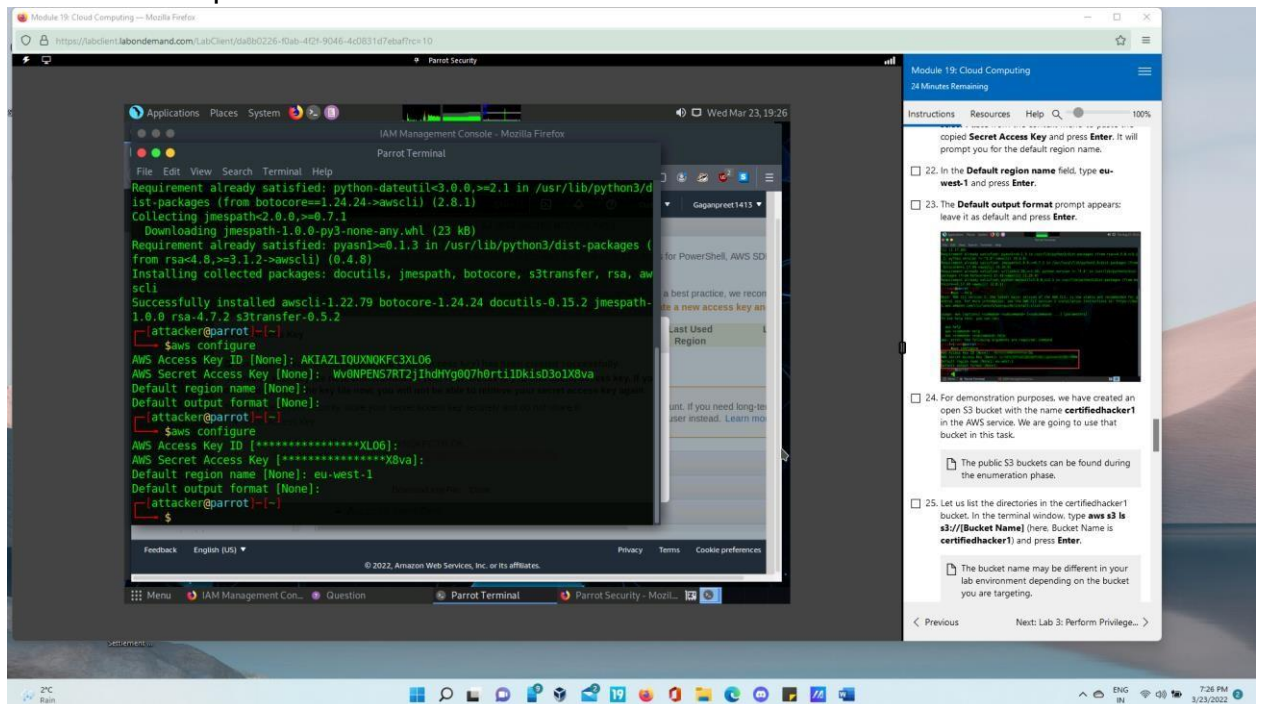


- Now click on Show Access key button.

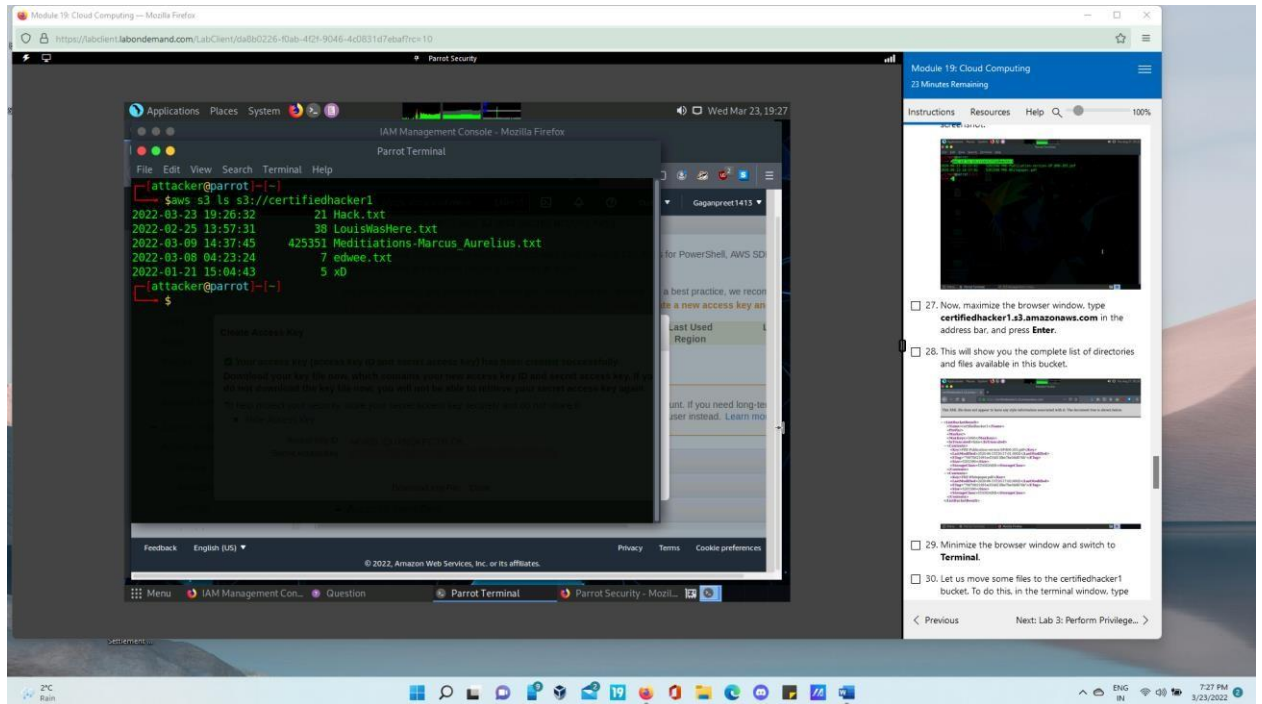




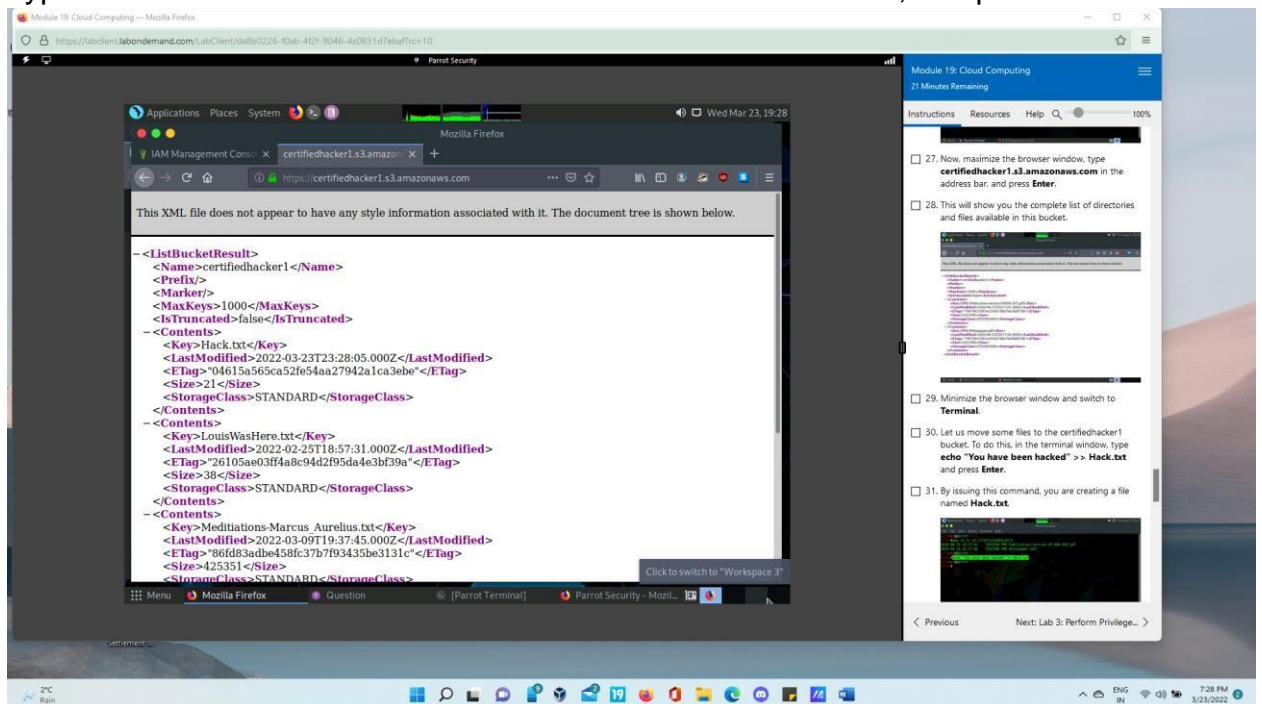
- In the terminal window, select **Paste** from the context menu to paste the copied **Secret Access Key** and press **Enter**. In the **Default region name** field, type **eu-west-1** and press **Enter**.



- The **Default output format** prompt appears; leave it as default and press **Enter**.
- Type **aws s3 ls s3://certifiedhacker1)** and press **Enter**.

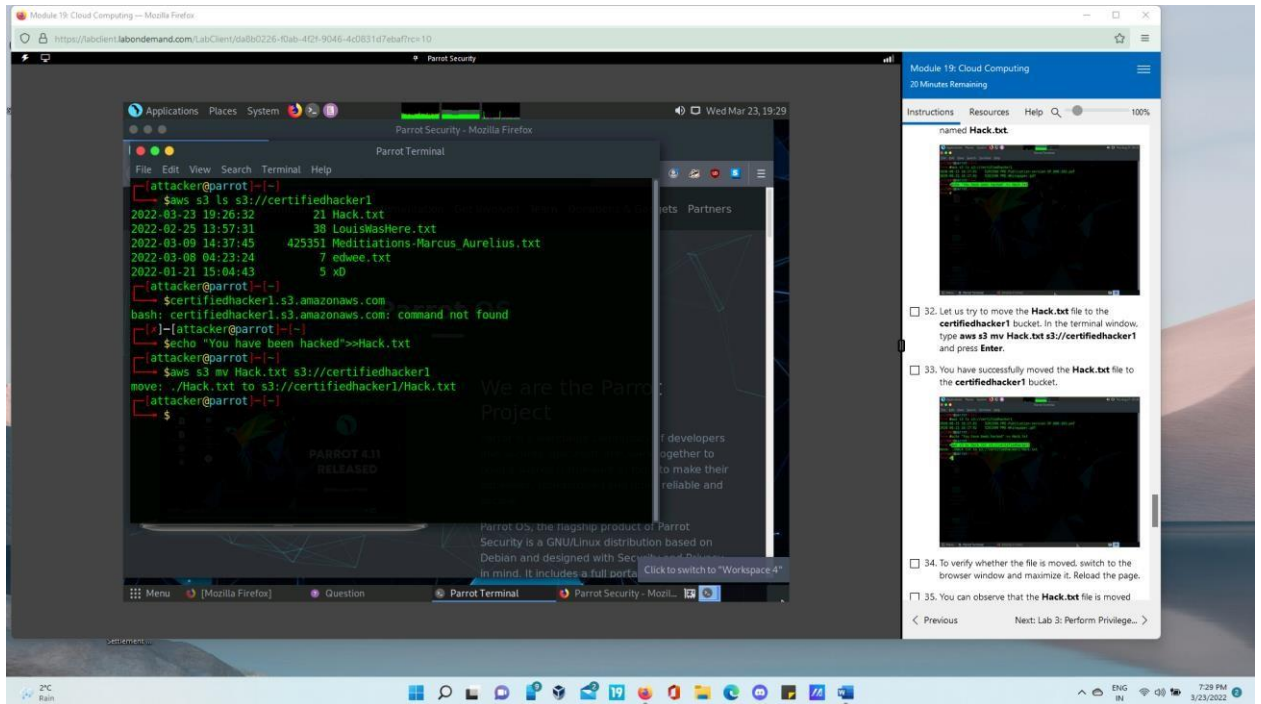


- Type **certifiedhacker1.s3.amazonaws.com** in the address bar, and press **Enter**.

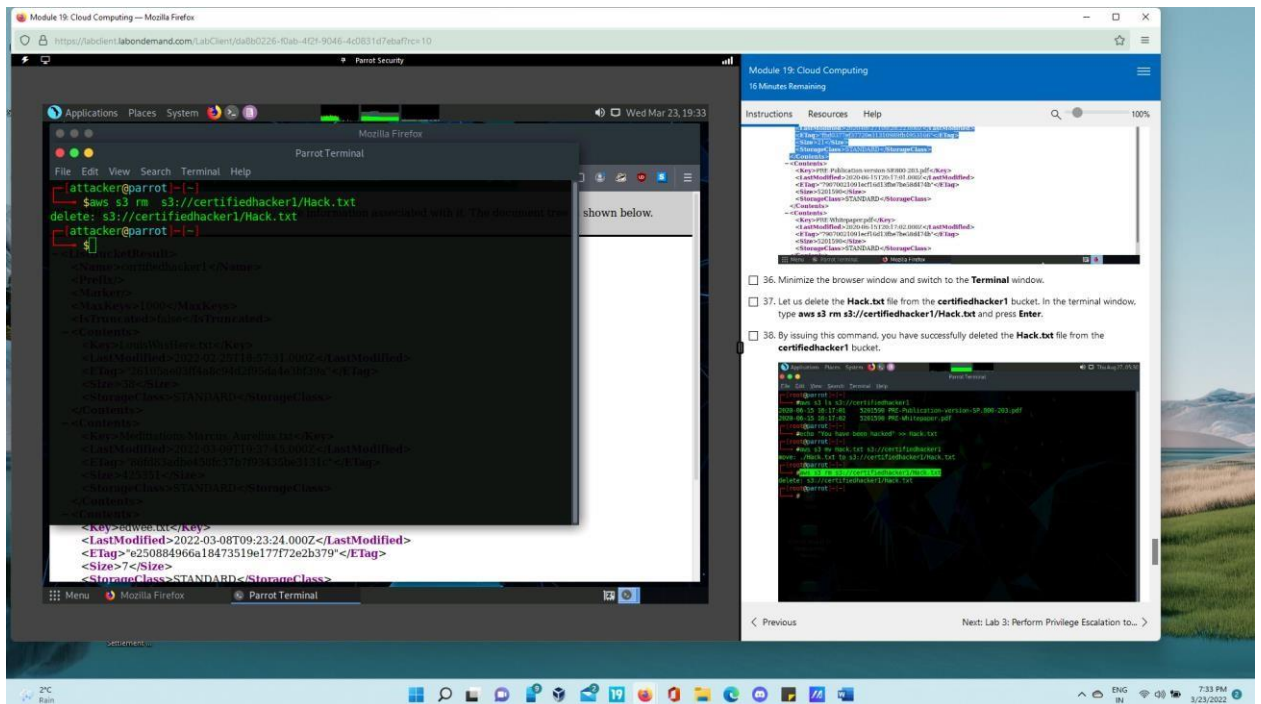


- Now, type **echo "You have been hacked" >> Hack.txt** and press **Enter**. Move the **Hack.txt** file to the **certifiedhacker1** bucket. Type **aws s3 mv Hack.txt s3://certifiedhacker1** and press **Enter**.

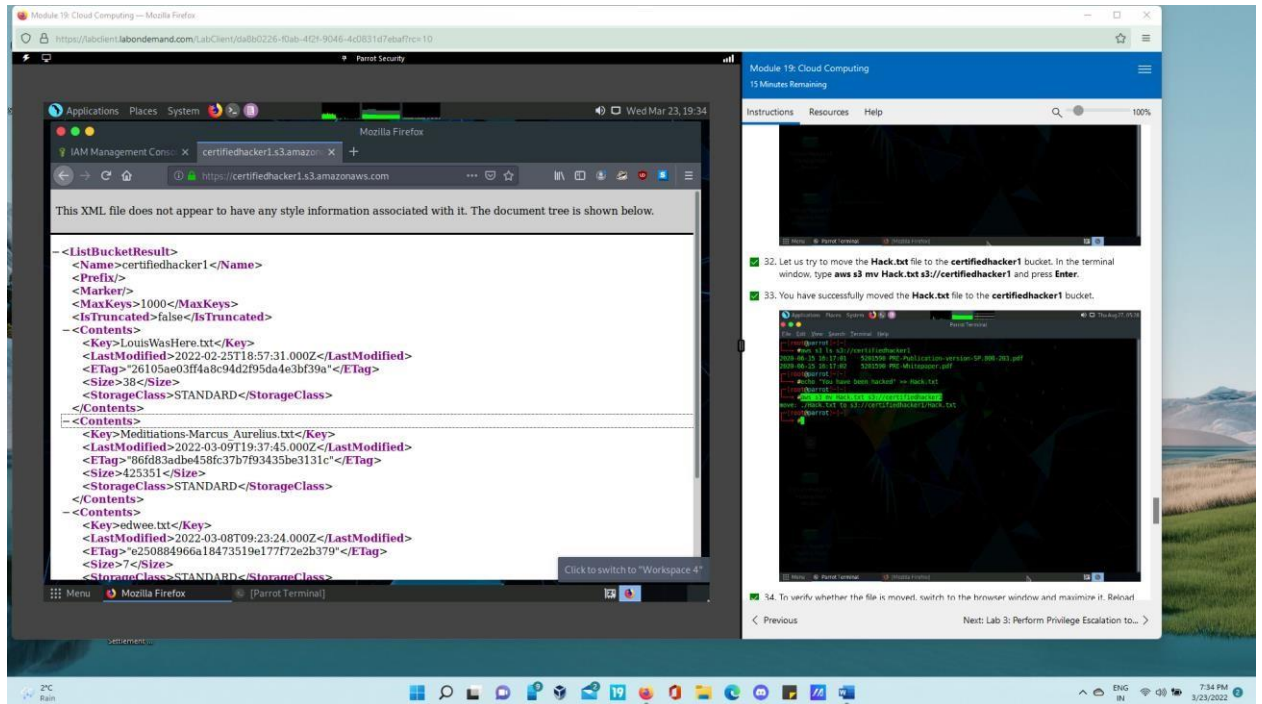




- Type `aws s3 rm s3://certifiedhacker1/Hack.txt` and press Enter to delete the file.



- The hack.txt file is deleted.

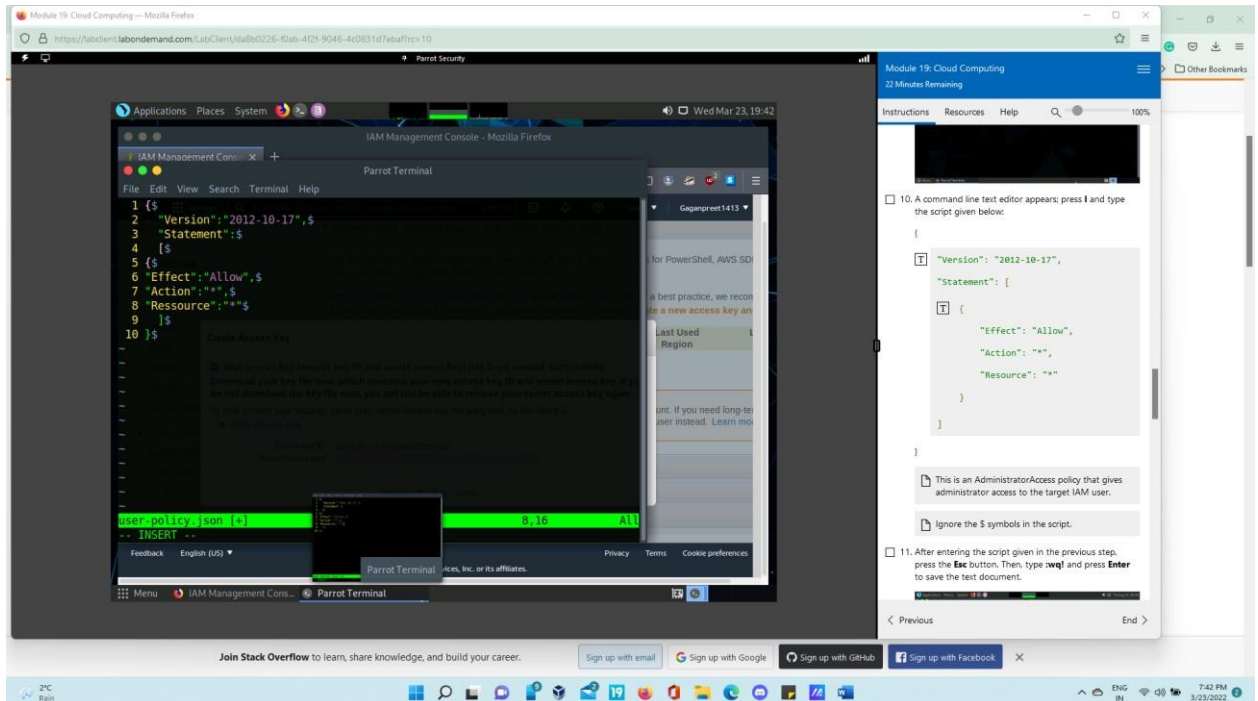


# Lab 3: Perform Privilege Escalation to Gain Higher Privileges

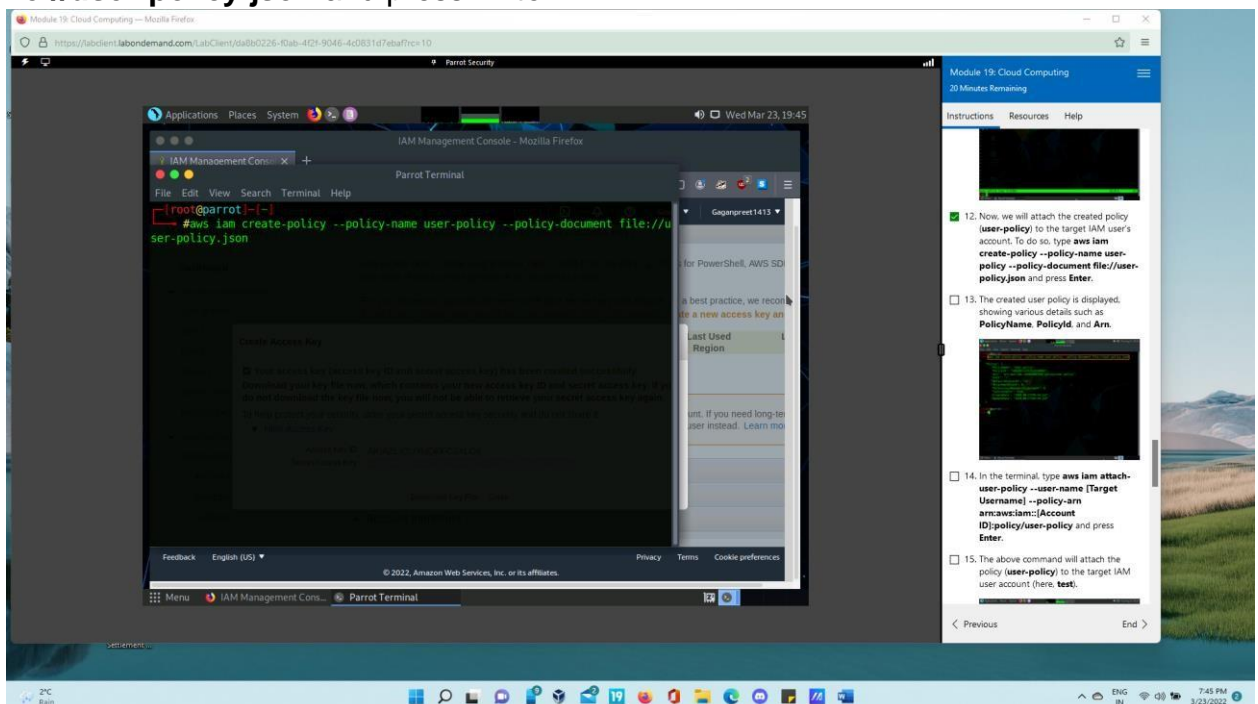
## Task 1: Escalate IAM User Privileges by Exploiting Misconfigured User Policy

- In the **Parrot Security** machine, login as root user.



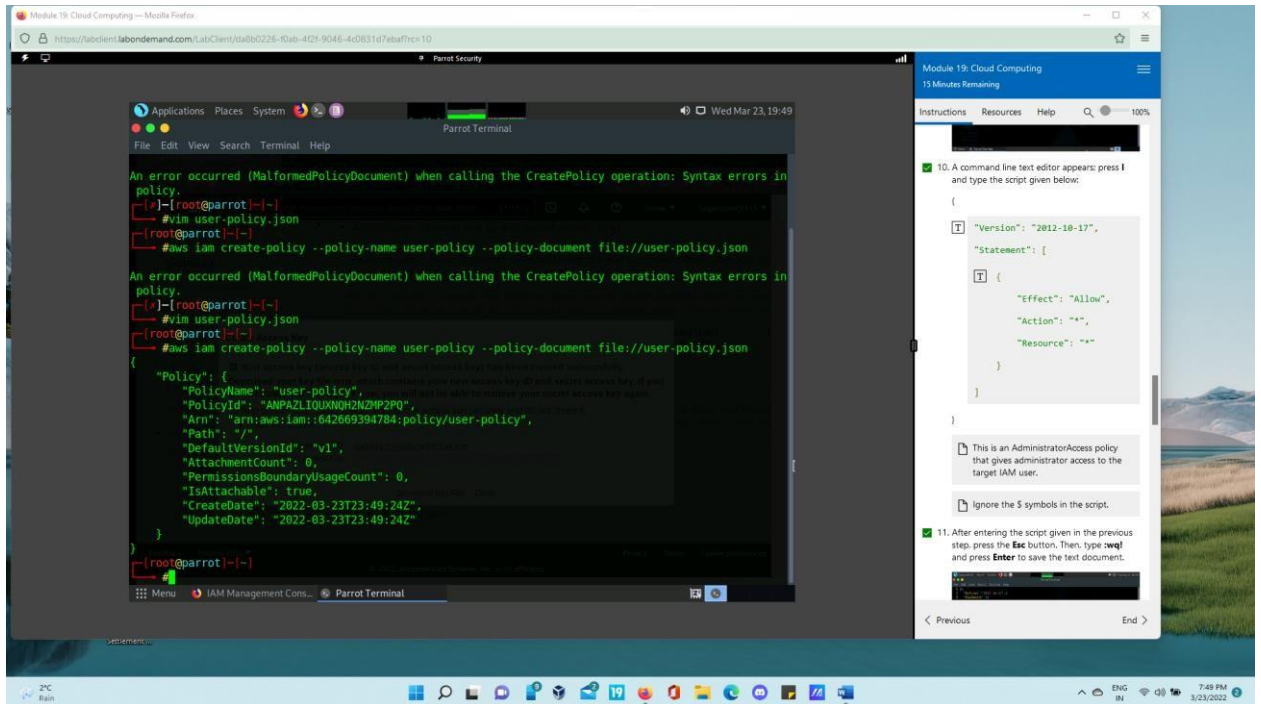


- Now, press the **Esc** button. Then, type **:wq!** and press **Enter** to save the text document.
- Type **aws iam create-policy --policy-name user-policy --policy-document file://user-policy.json** and press **Enter**.

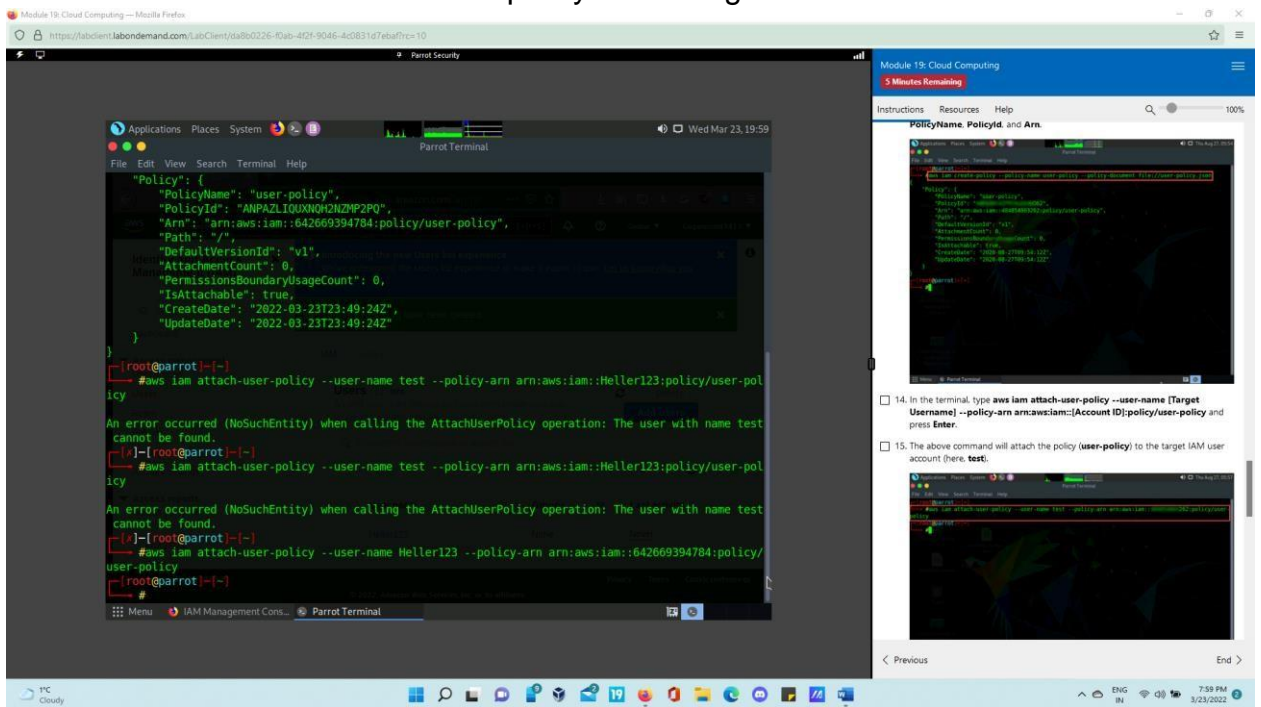


- Now, type **aws iam attach-user-policy --user-name [Target Username] --policy-arn arn:aws:iam::[Account ID]:policy/user-policy** and press **Enter**.





- The above command will attach the policy to the target IAM user account.



- Now, type **aws iam list-attached-user-policies --user-name Heller123** and press **Enter**.



Module 19: Cloud Computing — Mozilla Firefox

https://labdemon.com/LabClient/sa1b0226-f0ab-4021-9046-4c0831d7eba1frc10

Parrot Security

Applications Places System Parrot Terminal

File Edit View Search Terminal Help

```
[root@parrot:~]# aws iam list-attached-user-policies --user-name Heller123
{
  "AttachedPolicies": [
    {
      "PolicyName": "IAMUserChangePassword",
      "PolicyArn": "arn:aws:iam::aws:policy/IAMUserChangePassword"
    },
    {
      "PolicyName": "user-policy",
      "PolicyArn": "arn:aws:iam::642669394784:policy/user-policy"
    }
  ]
}
```

Users

Menu IAM Management Console Parrot Terminal

Module 19: Cloud Computing

4 Minutes Remaining

Instructions Resources Help

press **Enter**.

15. The above command will attach the policy (**user-policy**) to the target IAM user account (here, **test**).

16. Now, type **aws iam list-attached-user-policies --user-name [Target Username]** and press **Enter** to view the attached policies of the target user (here, **test**).

17. The result appears, displaying the attached policy name (**user-policy**) as shown in the screenshot.

< Previous End >

- Type **aws iam list-users** and press **Enter** to list users with escalated privileges.

Module 19: Cloud Computing — Mozilla Firefox

https://labdemon.com/LabClient/sa1b0226-f0ab-4021-9046-4c0831d7eba1frc10

Parrot Security

Applications Places System Parrot Terminal

File Edit View Search Terminal Help

```
[root@parrot:~]# aws iam list-users
{
  "Users": [
    {
      "Path": "/",
      "UserName": "Heller123",
      "UserId": "AIDAZLIQXNQC6KPRKF6C",
      "Arn": "arn:aws:iam::642669394784:user/Heller123",
      "CreateDate": "2022-03-23T23:55:58Z"
    }
  ]
}
```

Users

Menu IAM Management Console Parrot Terminal

Module 19: Cloud Computing

4 Minutes Remaining

Instructions Resources Help

in the screenshot.

18. Now that you have successfully escalated the privileges of the target IAM user account, you can list all the IAM users in the AWS environment. To do so, type **aws iam list-users** and press **Enter**.

19. The result appears, displaying the list of IAM users, as shown in the screenshot.

< Previous End >