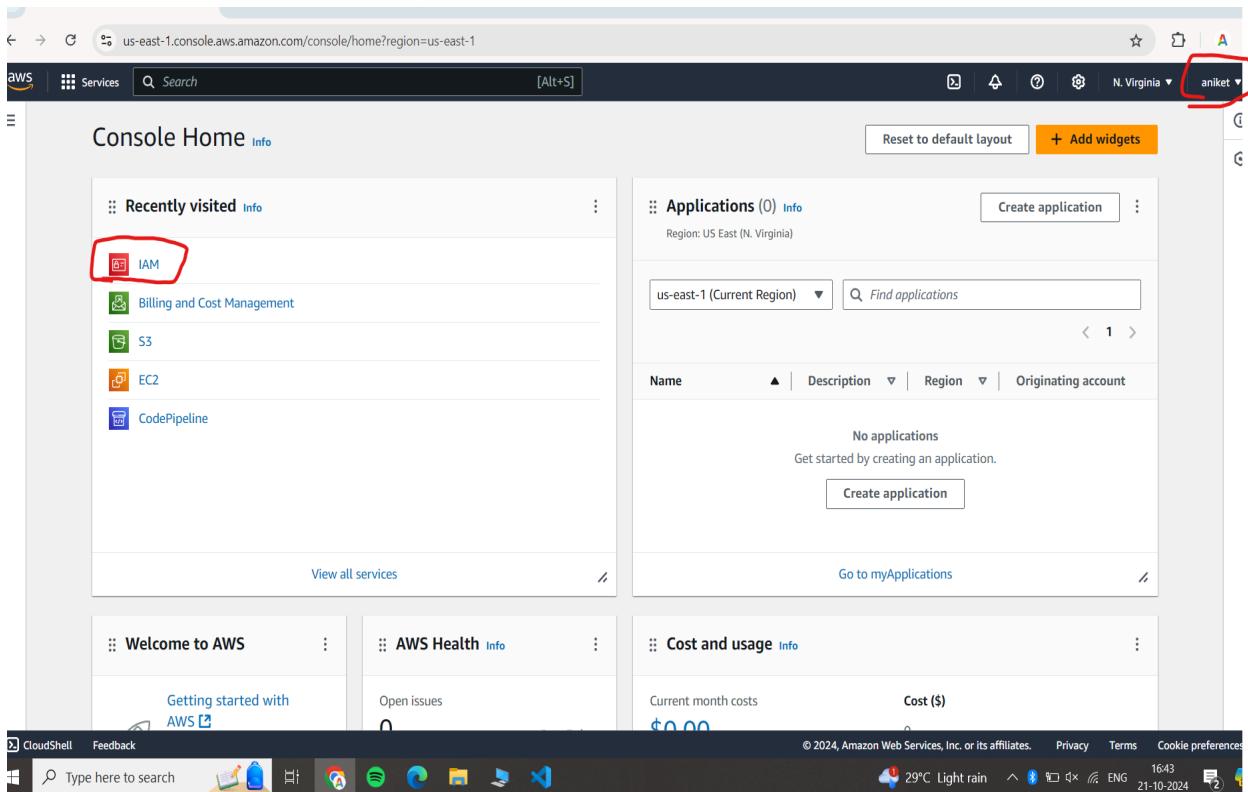


Module End Exam

Cloud

1. First we have to create IAM user using root account



2. Now we will create new user

The screenshot shows the AWS IAM service in the AWS Management Console. The left sidebar is collapsed. The main area displays the 'Users' page with a heading 'Users (0) Info'. A note states: 'An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.' Below this is a search bar and a table header with columns: User name, Path, Group, Last activity, MFA, Password age, and Console last sign-in. A message 'No resources to display' is shown. At the top right, there are 'Create' and 'Delete' buttons, and a 'Create user' button which is highlighted with a red circle. The bottom of the screen shows the Windows taskbar with various pinned icons.

3. Now we will specify user details and click next

The screenshot shows the 'Create user' wizard at Step 1: 'Specify user details'. The title is 'Specify user details'. On the left, a sidebar lists 'Step 1 Specify user details', 'Step 2 Set permissions', and 'Step 3 Review and create'. The main area has a section titled 'User details' with a 'User name' field containing 'Bigman'. Below it, a note says: 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = . , _ - (hyphen)'. There is also a checkbox for 'Provide user access to the AWS Management Console - optional' with a note: 'If you're providing console access to a person, it's a best practice [link] to manage their access in IAM Identity Center.' A callout box contains the text: 'If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more link]'. At the bottom right are 'Cancel' and 'Next' buttons, with 'Next' being highlighted with a red circle. The bottom of the screen shows the Windows taskbar.

4. Now we will set user permissions by attaching user policy

The screenshot shows the 'Create user' wizard in the AWS IAM console. The current step is 'Set permissions'. The 'Attach policies directly' option is selected and highlighted with a red circle. In the 'Permissions policies' list, the 'AmazonEC2FullAccess' policy is selected and highlighted with a red circle.

5. Now we will create review and create user

The screenshot shows the 'Create user' wizard in the AWS IAM console. The current step is 'Review and create'. The 'Create user' button is highlighted with a red circle.

6. User created successfully with the policy

The screenshot shows the AWS IAM service in a web browser. The main title bar says "Users | IAM | Global". Below it, the URL is "us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users". The left sidebar has sections for Dashboard, Access management (with "Users" selected), Access reports, CloudShell, and Feedback. The main content area shows a green banner at the top stating "User created successfully". Below this, a table lists "Users (1) info". A single row is shown for "Bigman", which is circled in red. The table includes columns for User name, Path, Groups, Last activity, MFA, Password age, and Console last sign-in.

7. Now inside the user we have to go to security credentials

The screenshot shows the "Bigman" user details page in the AWS IAM service. The title bar says "Bigman | IAM | Global". The URL is "us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/Bigman?section=permissions". The left sidebar is identical to the previous screenshot. The main content area shows the "Summary" section for the "Bigman" user. It includes fields for ARN (arn:aws:iam::108782077112:user/Bigman), Console access (Disabled), and Access key 1 (Create access key). Below this is the "Permissions" section, which shows one attached policy: "AmazonEC2FullAccess" (AWS managed, Directly). There are tabs for Permissions, Groups, Tags, Security credentials, and Last Accessed.

8.enable console access for login

The screenshot shows the AWS Identity and Access Management (IAM) service in a web browser. The user is viewing the details for a user named 'Bigman'. In the 'Security credentials' tab, there is a section titled 'Console sign-in' which includes a link to the AWS console sign-in page and a status indicating 'Console password Not enabled'. To the right of this section is a button labeled 'Enable console access' which is circled in red. Below this section is another titled 'Multi-factor authentication (MFA) (0)'.

9. Console access enabled

The screenshot shows the same AWS IAM User Details page as the previous one, but now the 'Console access' status is listed as 'Enabled without MFA'. A green banner at the top of the page also states 'Console access enabled.' This indicates that the 'Enable console access' step has been completed successfully.

10. Now we will create access key

The screenshot shows the AWS Identity and Access Management (IAM) console. The left sidebar is collapsed, showing 'Access management' with 'Users' selected. The main content area displays the 'Access keys (0)' section. A red oval highlights the 'Create access key' button at the top right of this section. Below it, another 'Create access key' button is visible. At the bottom of the page, there's a section for 'SSH public keys for AWS CodeCommit (0)'.

11.

The screenshot shows the 'Create access key' wizard, Step 2 - optional. On the left, under 'alternatives', there are three steps: 'Step 2 - optional', 'Set description tag', and 'Step 3' (which is 'Retrieve access keys'). The main content area is titled 'Use case' and lists several options. The 'Application running on an AWS compute service' option is selected (indicated by a blue border). Below it, the 'Alternative recommended' section is shown, containing a single 'Other' option: 'Your use case is not listed here.' The bottom of the screen shows a Windows taskbar with various icons.

12. Access key generated successfully

The screenshot shows the AWS IAM 'Create access key' page. At the top, a green banner says 'Access key created' with a note: 'This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.' Below the banner, the navigation path is IAM > Users > Bigman > Create access key. The main section is titled 'Retrieve access keys' with a sub-section 'Access key'. It displays the Access key (AKIAR5U7KYS4NHXE442Y) and Secret access key (XXXXXXXXXX). A 'Show' link is available for the secret key. To the right, there's a 'Done' button. On the left sidebar, there are three steps: Step 1 (Access key best practices & alternatives), Step 2 (optional Set description tag), and Step 3 (Retrieve access keys). Below the main content, there's a 'Access key best practices' section with tips like 'Never store your access key in plain text, in a code repository, or in code.' and a 'Download .csv file' button.

13. Sign to new IAM user

The screenshot shows the AWS Sign-In page. At the top, a message says 'Try the new sign in UI' with a link to 'Enable new sign in'. The main form is titled 'Sign in as IAM user' and requires 'Account ID (12 digits) or account alias' (108782077112), 'IAM user name' (Bigman), and 'Password' (XXXXXX). There's a 'Remember this account' checkbox and a 'Sign in' button. Below the form, links for 'Sign in using root user email' and 'Forgot password?' are visible. To the right of the form, there's an advertisement for 'Amazon Lightsail' with the text 'Lightsail is the easiest way to get started on AWS' and a 'Learn more »' button. The bottom of the screen shows the Windows taskbar with various icons and system status.

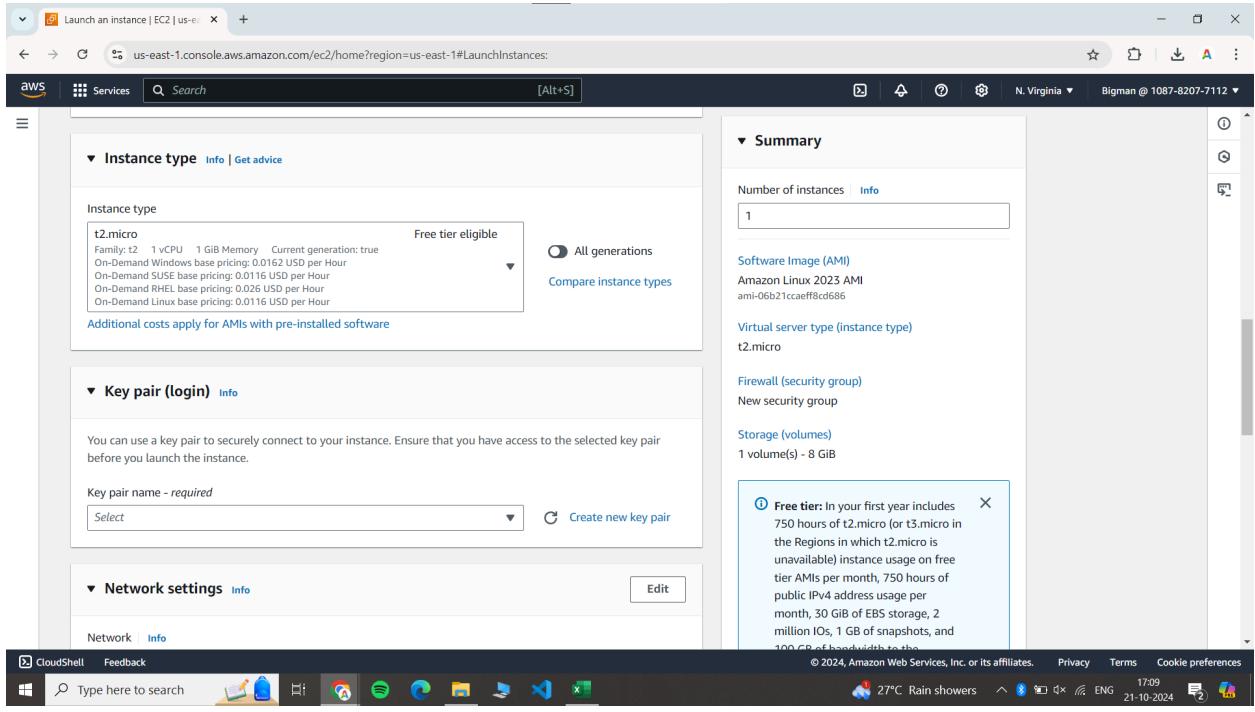
14.No we will launch instance

The screenshot shows the AWS EC2 Dashboard. On the left, there's a sidebar with navigation links for EC2 Global View, Events, Instances (with sub-links for Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity, and Reservations), Images (AMIs, AMI Catalog), and Elastic Block Store (Volumes, Snapshots, Lifecycle Manager). The main panel has a 'Resources' section with dropdown menus for Instances (running), Auto Scaling Groups, Capacity Reservations, Dedicated Hosts, Elastic IPs, Instances, Key pairs, Load balancers, Placement groups, Security groups, Snapshots, and Volumes. Below this is a 'Launch instance' section with a large orange 'Launch instance' button, which is circled in red. To the right of the launch button is a 'Service health' section showing an error message: 'An error occurred An error occurred retrieving service health information'. There's also a 'Zones' section. On the far right, there are sections for 'EC2 Free Tier Info', 'Account attributes', 'Settings', and 'Explore AWS'. The bottom of the screen shows the Windows taskbar with various pinned icons.

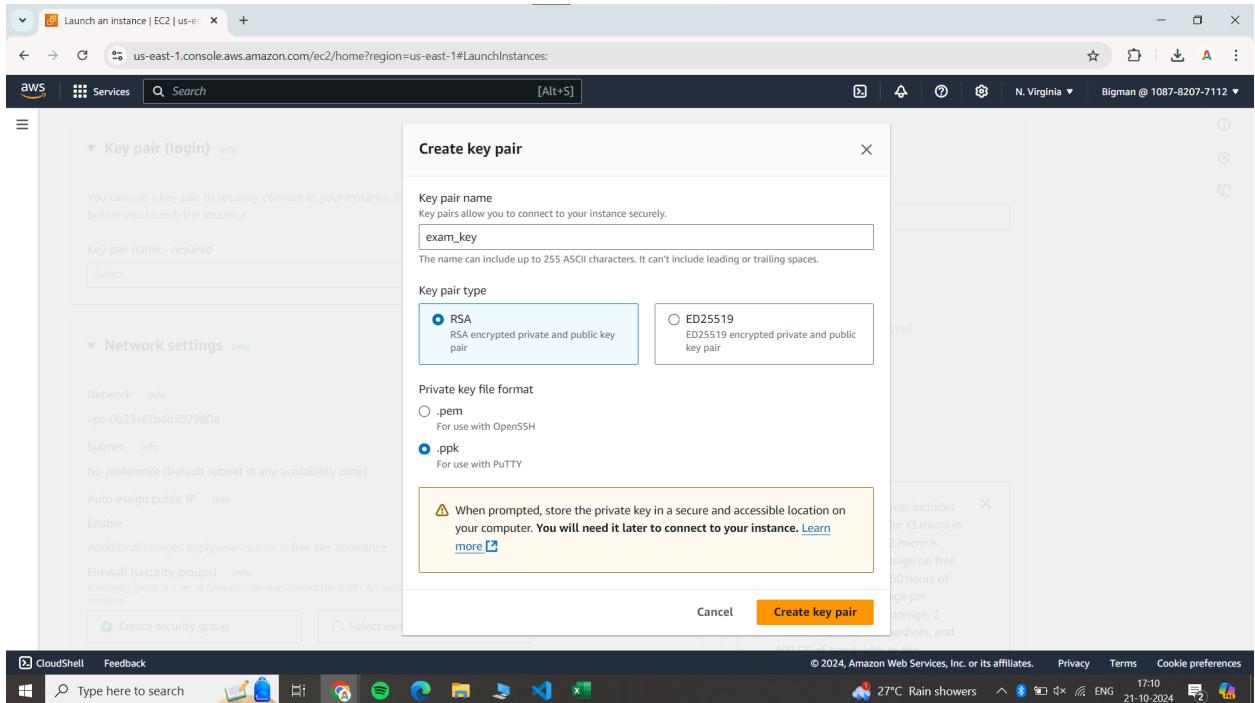
15.Now will give instance name and select os

The screenshot shows the 'Launch an instance' wizard. The first step, 'Name and tags', has a 'Name' field containing 'mywebserver'. The second step, 'Application and OS Images (Amazon Machine Image)', is highlighted with a red circle. It contains a search bar and a table with one row for 'Amazon Linux 2023 AMI'. This row has two status badges: 'Verified provider' (green) and 'Free tier eligible' (blue). To the right of the table is a 'Summary' section showing 'Number of instances' set to 1, 'Software Image (AMI)' as Amazon Linux 2023 AMI, 'Virtual server type (instance type)' as t2.micro, 'Firewall (security group)' as New security group, and 'Storage (volumes)' as 1 volume(s) - 8 GiB. A tooltip for the 'Free tier' badge provides details about included resources. The bottom of the screen shows the Windows taskbar.

16. Select instance type i.e. t2.micro



17.create key pair login



18. Enable network settings

The screenshot shows the 'Network settings' step of the EC2 launch wizard. It includes fields for 'Network' (vpc-0b23e6fb4b507980a) and 'Subnet' (No preference). Under 'Auto-assign public IP', 'Enable' is selected. A note about additional charges applies when outside the free tier allowance. A 'Firewall (security groups)' section allows creating a new security group ('Create security group') or selecting an existing one ('Select existing security group'). Below, it says we'll create a new security group called 'launch-wizard-9'. Rules listed include allowing SSH traffic from anywhere, HTTPS from the internet, and HTTP from the internet. A warning message at the bottom encourages setting security group rules to allow access from known IP addresses only.

19. Launch instance

The screenshot shows the 'Configure storage' step of the EC2 launch wizard. It specifies 1x 8 GiB gp3 Root volume (Not encrypted). A note indicates that free-tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Below, there's a 'Add new volume' button and a note to click refresh to view backup information. The 'Advanced details' section is also visible. On the right, the summary shows 1 instance, AMI (Amazon Linux 2025 AMI), Virtual server type (t2.micro), Firewall (New security group), and Storage (1 volume(s) - 8 GiB). A callout box highlights the 'Free tier' information. The 'Launch instance' button is highlighted with a red circle.

20.Instance launched and is in running state

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with options like EC2 Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity, and Reservations. Below that are Images (AMIs, AMI Catalog) and Elastic Block Store (Volumes, Snapshots, Lifecycle Manager). The main content area shows a table with one row for the instance 'mywebserver'. The instance details are as follows:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
mywebserver	i-021f3bf320662a09f	Running	t2.micro	Initializing	View alarms +	us-east-1d	ec2-3-95-37-245.compute-1.amazonaws.com

Below the table, there's a detailed view for the instance 'i-021f3bf320662a09f (mywebserver)' with tabs for Details, Status and alarms, Monitoring, Security, Networking, Storage, and Tags. The Details tab shows the following information:

Instance summary	Info
Instance ID	i-021f3bf320662a09f
IPv6 address	-
Hostname type	IP name: ip-172-31-26-194.ec2.internal
Answer private resource DNS name (IPv4)	-
Public IPv4 address	3.95.37.245 open address
Instance state	Running
Private IP DNS name (IPv4 only)	ip-172-31-26-194.ec2.internal
Instance type	t2.micro

The status bar at the bottom indicates the URL as <https://us-east-1.console.aws.amazon.com/cloudshell/home?region=us-east-1>.

21.Now we will connect through putty

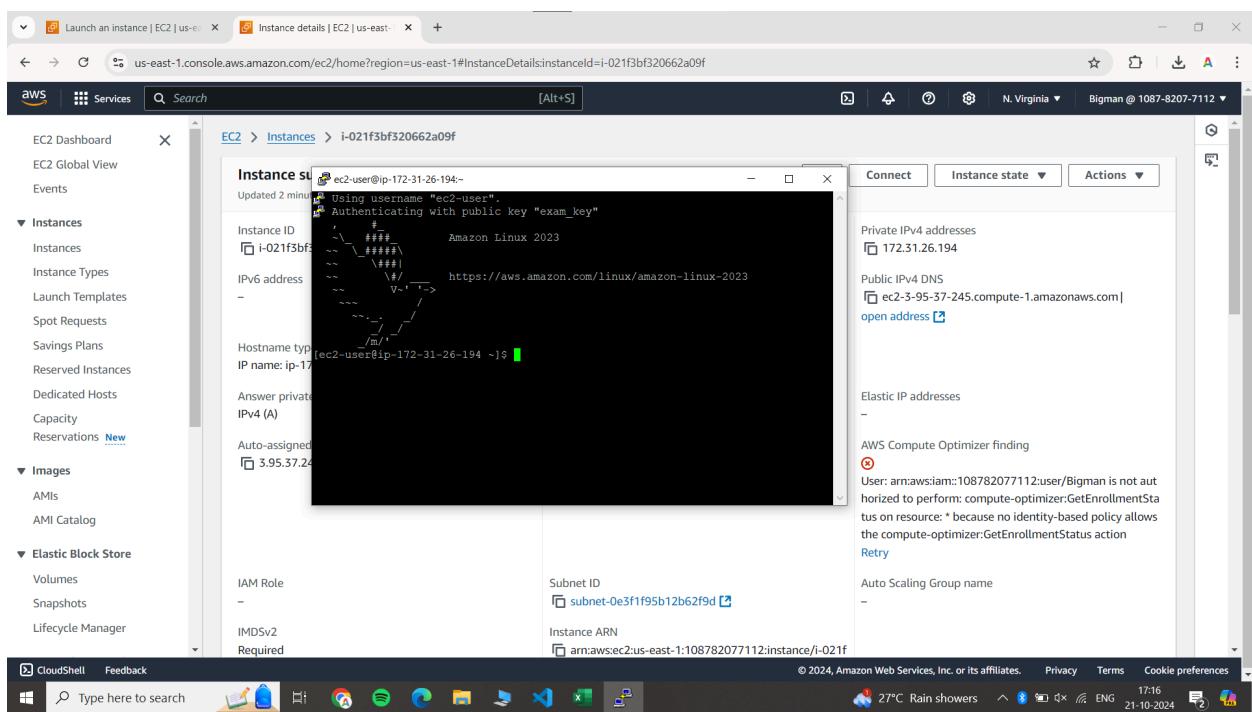
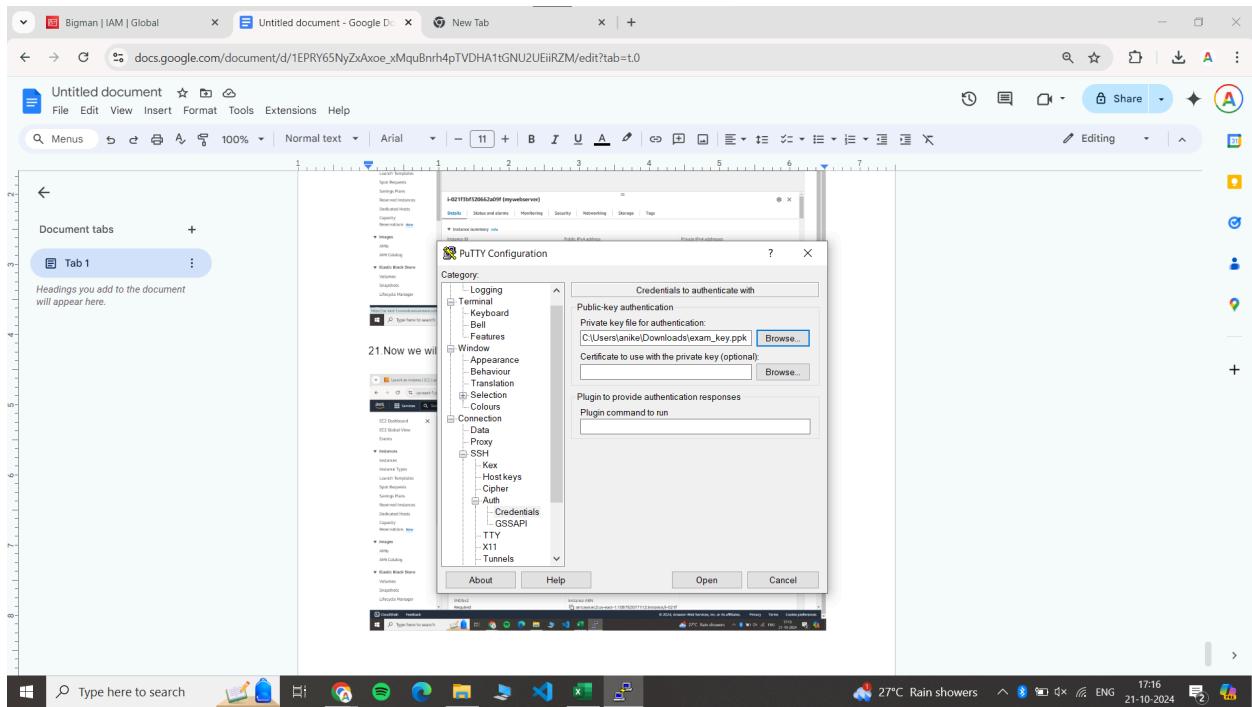
The screenshot shows the AWS EC2 Instance details page for the instance 'i-021f3bf320662a09f (mywebserver)'. The left sidebar is identical to the previous screenshot. The main content area shows the instance summary and a PuTTY Configuration dialog box. The PuTTY dialog has the following settings:

Category	Setting
Session	Host Name (or IP address): ec2-user@3.95.37.245
Session	Port: 22
Connection	Connection type: SSH
Session	Load, save or delete a stored session: Default Settings
Session	Close window on exit: Only on clean exit

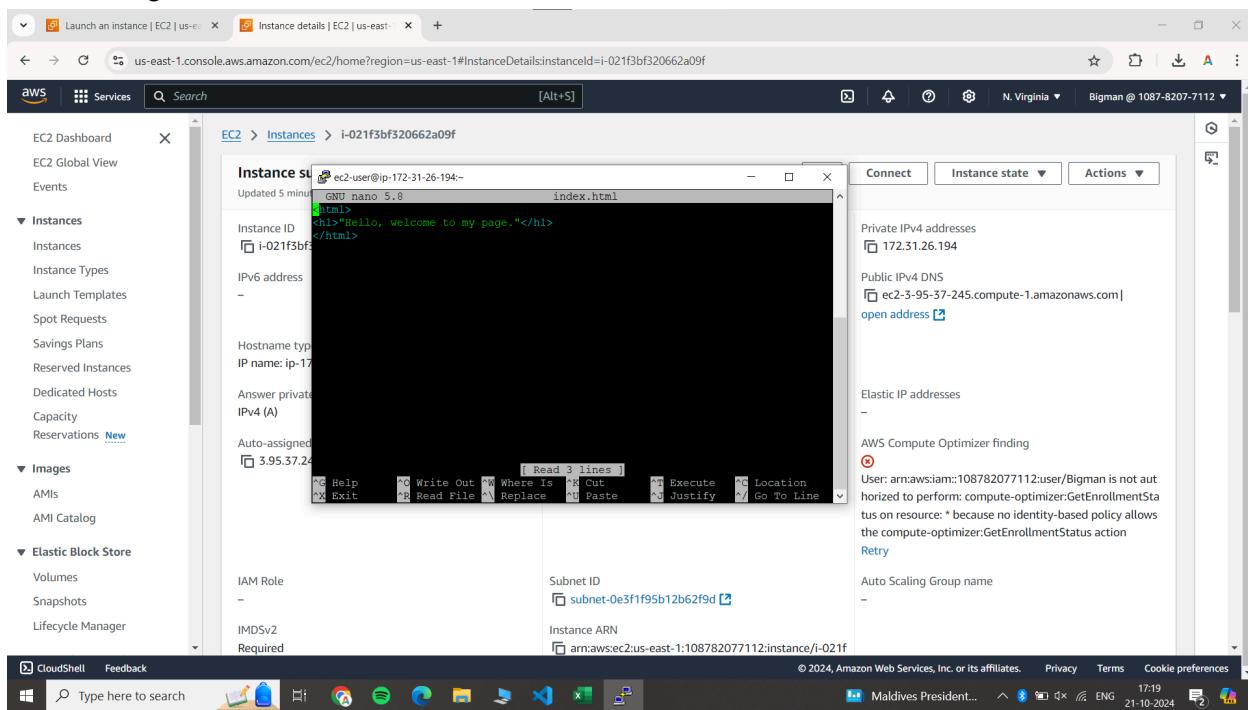
Below the PuTTY dialog, the instance details are shown again:

Category	Value
Instance ID	i-021f3bf320662a09f
IPv6 address	-
Hostname type	IP name: ip-172-31-26-194.ec2.internal
Answer private resource DNS name (IPv4)	-
Auto-assigned IP address	3.95.37.245 [Public IP]
IAM Role	-
IMDSv2 Required	-

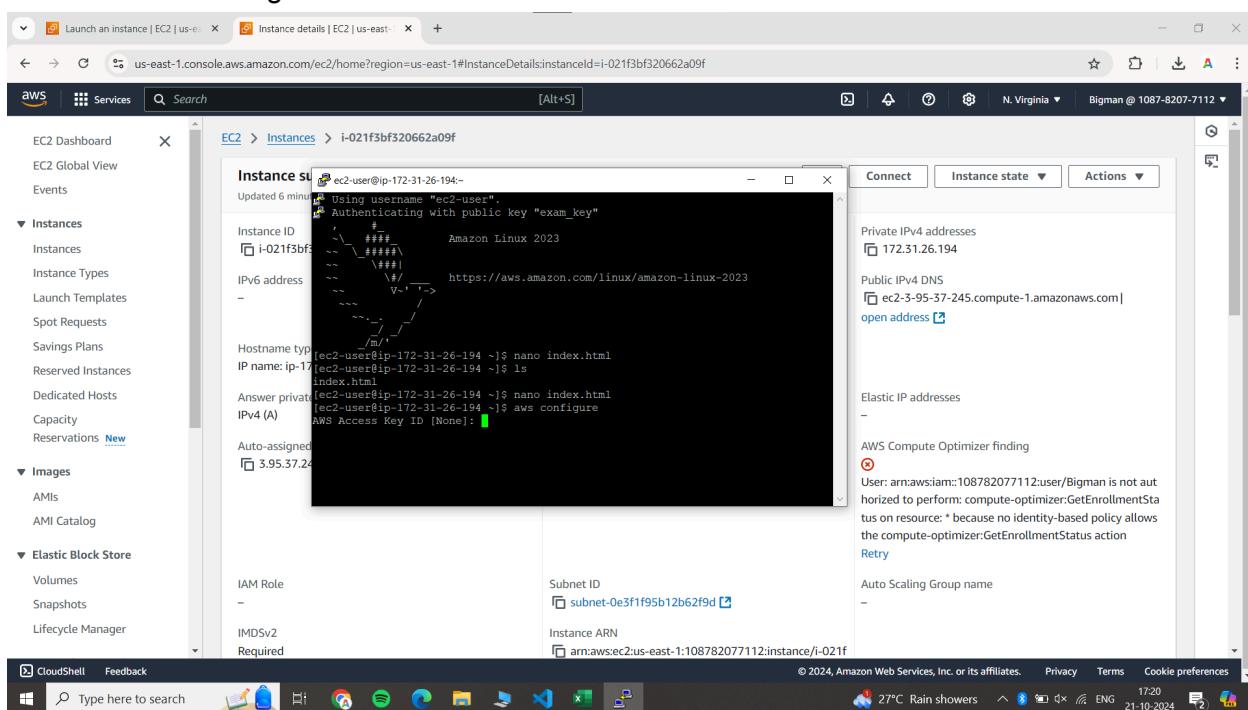
The status bar at the bottom indicates the URL as <https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#instanceDetails:instanceId=i-021f3bf320662a09f>.



24. Creating an html file



25. Now we will configure



26. Now we will give access key, secret access key and region

The screenshot shows a Google Docs document titled "Untitled document - Google Docs". A terminal window is embedded in the document, displaying the following session:

```
ec2-user@ip-172-31-26-194: ~
Using username "ec2-user".
Authenticating with public key "exam_key"
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-172-31-26-194 ~]$ nano index.html
[ec2-user@ip-172-31-26-194 ~]$ ls
index.html
[ec2-user@ip-172-31-26-194 ~]$ nano index.html
[ec2-user@ip-172-31-26-194 ~]$ aws configure
AWS Access Key ID [None]: AKIARUSUKYSA4NHEX442Y
AWS Secret Access Key [None]: 6aqg2kjmrP2z6YLgKSaOH4mG2l/fTotwSLrvvZKK
Default region name [None]: us-east-1
Default output format [None]: none
```

Below the terminal, the AWS CloudShell interface is visible, showing the AWS Lambda function configuration page.

27. File uploaded to s3 bucket successfully

The screenshot shows the AWS S3 console in a browser window. The left sidebar includes options like Buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Block Public Access settings, Storage Lens, and AWS Marketplace for S3.

The main area displays a terminal window showing the command-line session:

```
ec2-user@ip-172-31-26-194: ~
[ec2-user@ip-172-31-26-194 ~]$ nano index.html
[ec2-user@ip-172-31-26-194 ~]$ ls
index.html
[ec2-user@ip-172-31-26-194 ~]$ nano index.html
[ec2-user@ip-172-31-26-194 ~]$ aws configure
AWS Access Key ID [None]: AKIARUSUKYSA4NHEX442Y
AWS Secret Access Key [None]: 6aqg2kjmrP2z6YLgKSaOH4mG2l/fTotwSLrvvZKK
Default region name [None]: us-east-1
Default output format [None]: none
[ec2-user@ip-172-31-26-194 ~]$ aws s3 ls
```

An error message is displayed below the terminal:

An error occurred (AccessDenied) when calling the ListBuckets operation: User: arn:aws:iam::108782077112:user/Bigman is not authorized to perform: s3>ListAllMyBuckets because no identity-based policy allows the s3>ListAllMyBuckets action

On the right, a table shows the bucket details:

Bucket	Analyzer	Creation date
for us-east-1		October 21, 2024, 16:56:04 (UTC+05:30)

28.bucket is enabled to static hosting

The screenshot shows the AWS S3 console with the 'Edit static website hosting' page for the 'modexam' bucket. The 'Static website hosting' section is active, with 'Enable' selected for both static website hosting and redirect requests for objects. A note indicates that content must be publicly readable. The 'Index document' field contains 'index.html'. The browser taskbar at the bottom shows various open tabs and system status.

30.we can verify that our html file can be viewed in both root and iam user

The screenshot shows the AWS S3 console with the 'Objects' tab selected for the 'modexam' bucket. One object, 'index.html', is listed with details: Name: index.html, Type: html, Last modified: October 21, 2024, 17:31:05 (UTC+05:30), Size: 53.0 B, Storage class: Standard. The browser taskbar at the bottom shows various open tabs and system status.

The screenshot shows the AWS S3 console interface. On the left, a sidebar menu includes options like Buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Block Public Access settings, Storage Lens (Dashboards, Storage Lens groups, AWS Organizations settings), Feature spotlight, and AWS Marketplace for S3. The main content area displays the 'modexam' bucket. A sub-menu for 'index.html' is open, showing its properties: Name (index.html), Type (html), Last modified (October 21, 2024, 17:31:05 (UTC+05:30)), Size (53.0 B), and Storage class (Standard). Below these details is a table with columns: Name, Type, Last modified, Size, and Storage class. A single row is present for the 'index.html' object. At the top of the main content area, there are several buttons: Copy S3 URI, Copy URL, Download, Open, Delete, Actions (with a dropdown arrow), Create folder, and Upload.

31.By granting public access

The screenshot shows the AWS S3 console interface, specifically the 'Permissions' tab for the 'index.html' object in the 'modexam' bucket. The sidebar on the left is identical to the previous screenshot. The main content area shows the 'index.html' object with its properties and the 'Permissions' tab selected. The 'Access control list (ACL)' section contains three entries:

Grantee	Object	Object ACL
Object owner (your AWS account) Canonical ID: f5ad040039d861179288e6947ab707412d24c34cea55e16335b9a19ff82566a8	Read	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	△ Read	△ Read
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	△ Read	△ Read

At the bottom of the screenshot, a Windows taskbar is visible with icons for File Explorer, Edge, Spotify, Google Chrome, File Manager, and Microsoft Word. The system tray shows the date (21-10-2024), time (17:37), battery level (26°C Rain showers), and network status (ENG).

32.Our website is publicly accessible



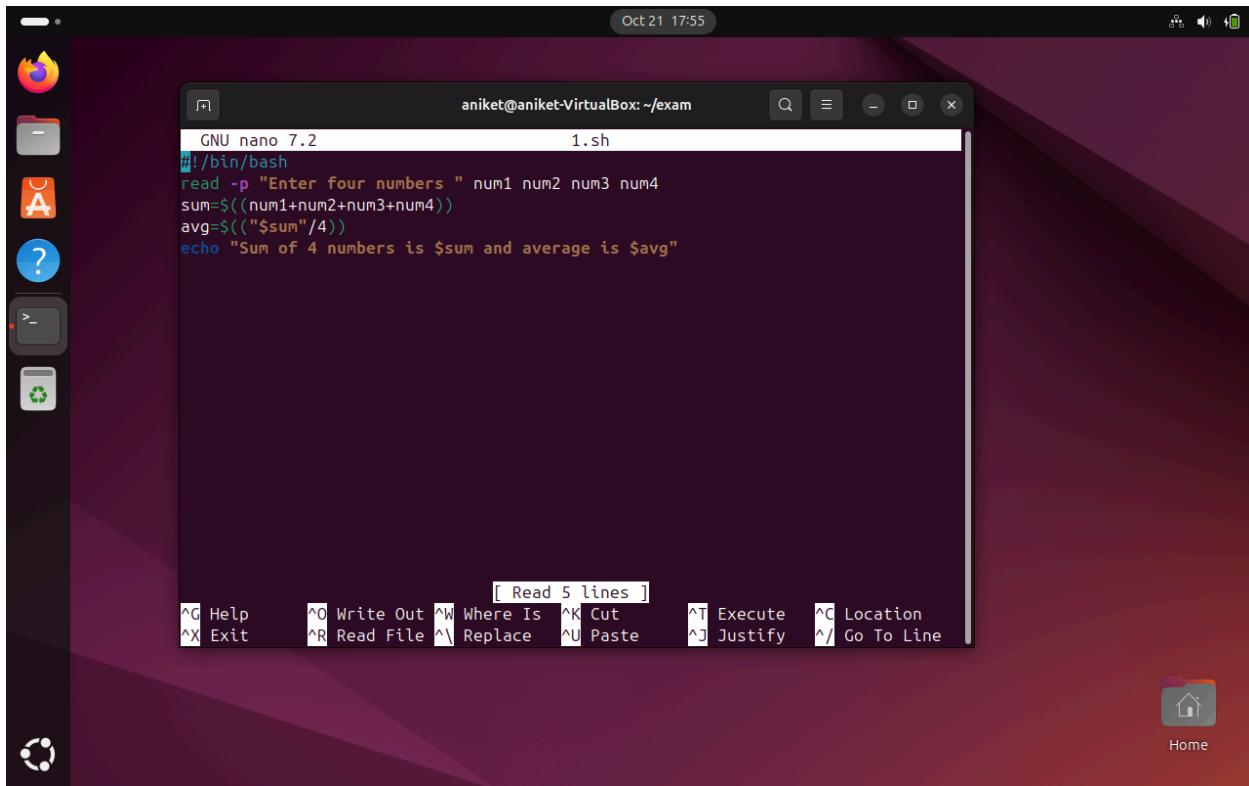
Link of website: <https://modexam.s3.amazonaws.com/index.html>



Linux

Q1

script



The screenshot shows a Linux desktop environment with a dark theme. A terminal window titled "aniket@aniket-VirtualBox: ~/exam" is open, displaying a script named "1.sh". The script reads four numbers from the user, calculates their sum and average, and prints the results. The terminal window has a dark background with light-colored text. At the bottom, there is a menu bar with various keyboard shortcuts. The desktop background is also dark.

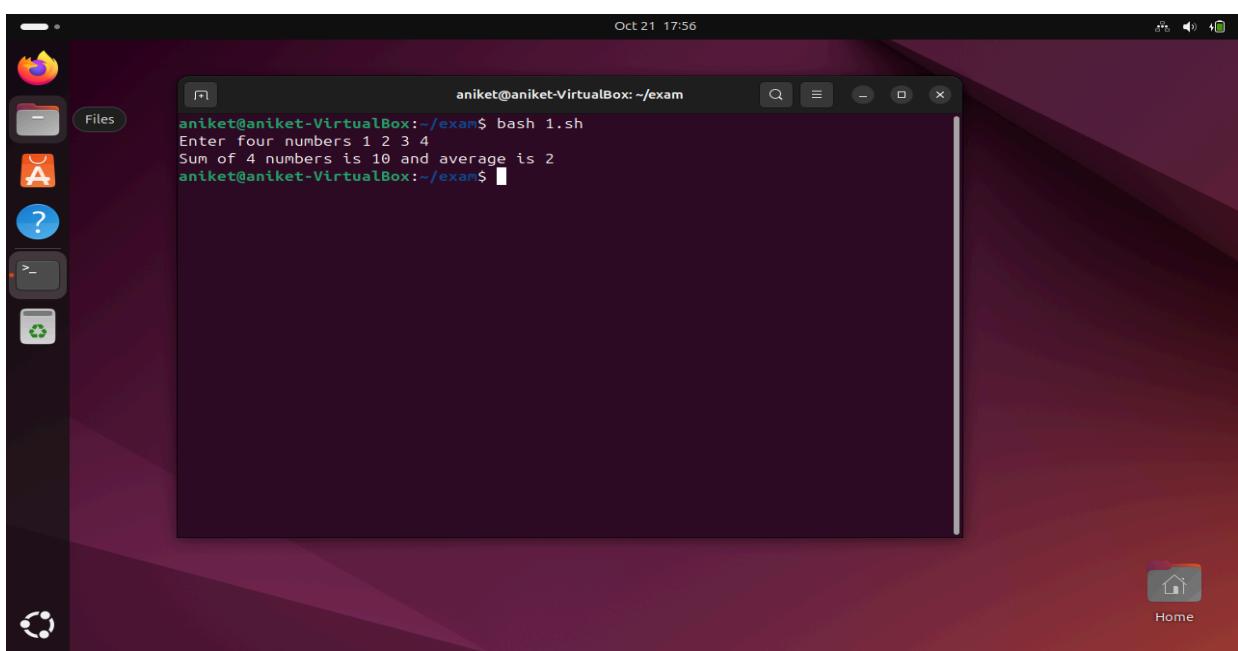
```
GNU nano 7.2          1.sh
#!/bin/bash
read -p "Enter four numbers " num1 num2 num3 num4
sum=$((num1+num2+num3+num4))
avg=$(($sum/4))
echo "Sum of 4 numbers is $sum and average is $avg"
```

[Read 5 lines]

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line

Result

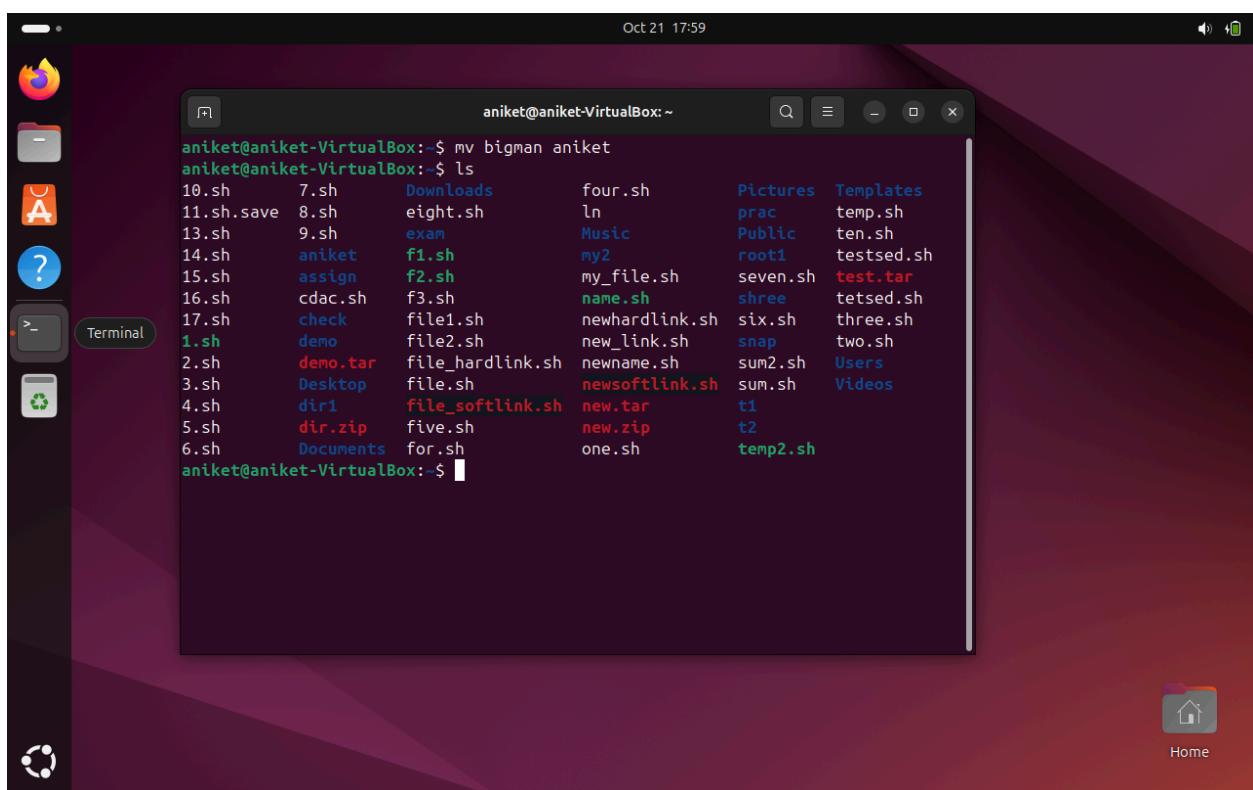
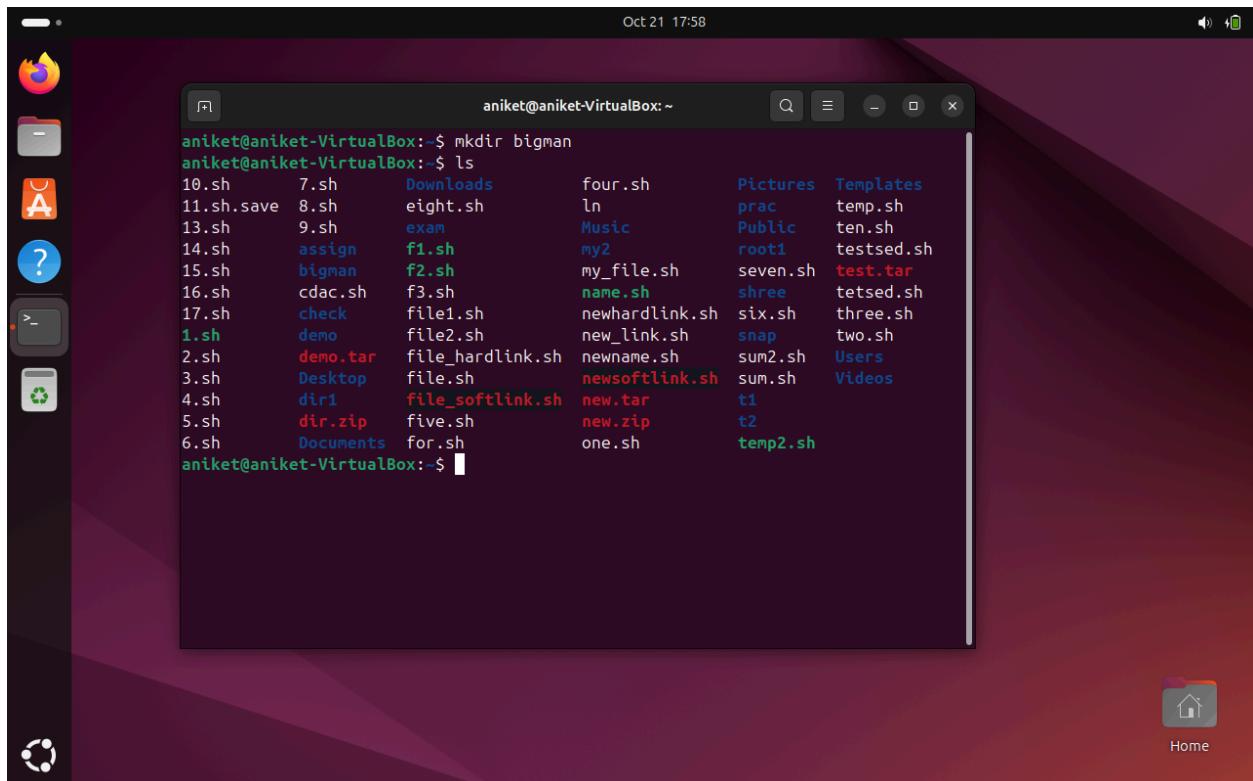
:

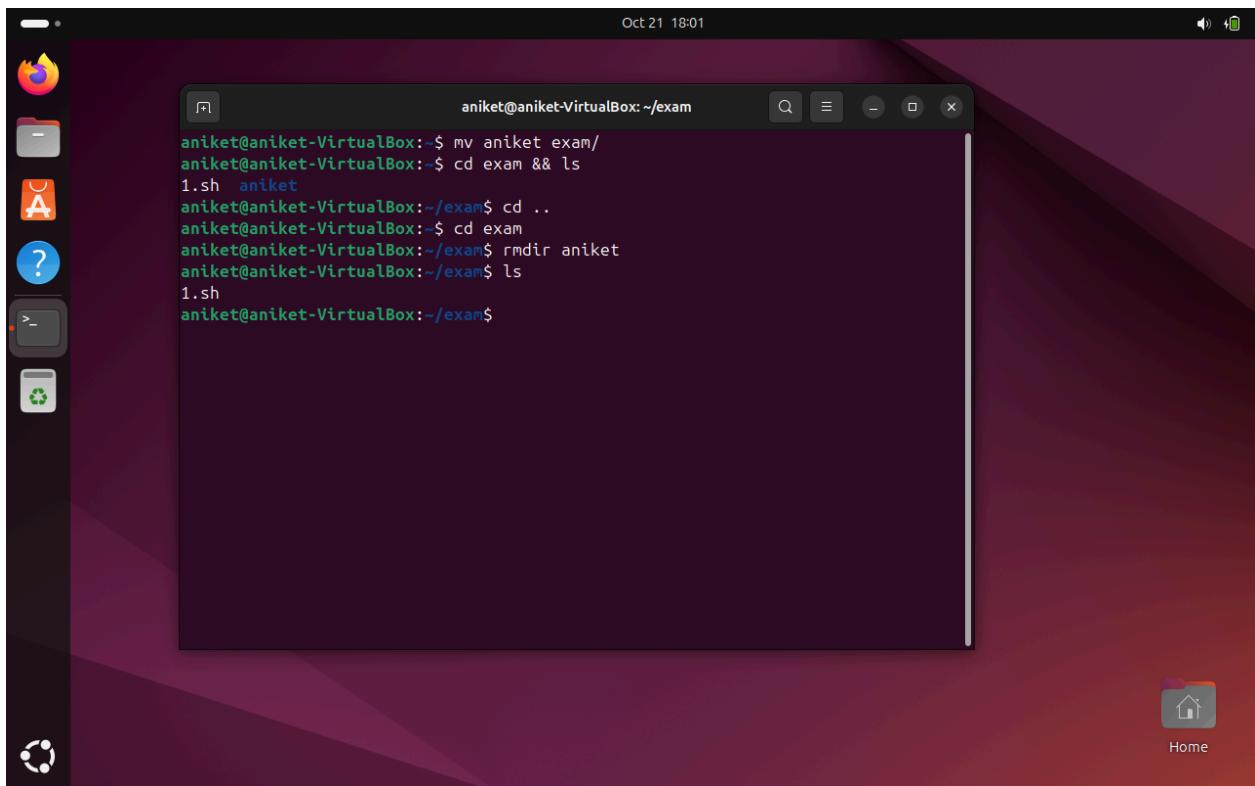
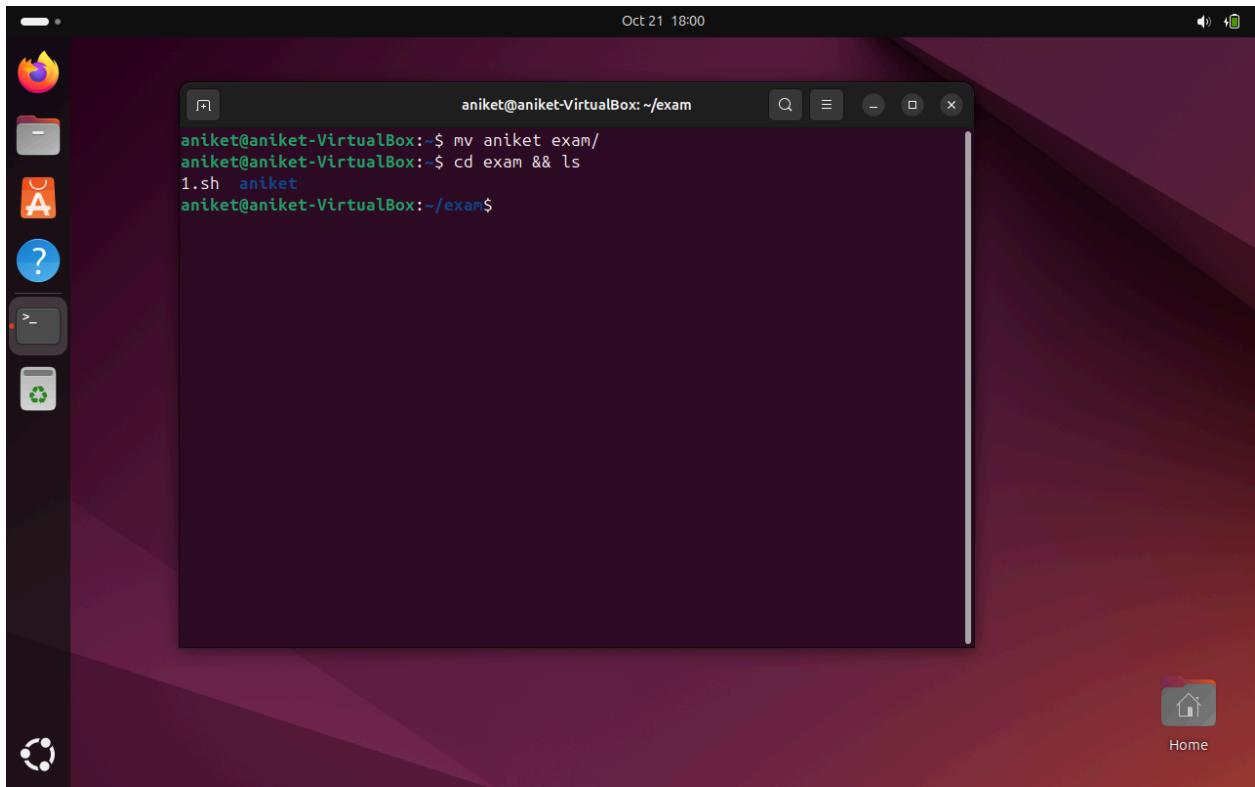


The screenshot shows a Linux desktop environment with a dark theme. A terminal window titled "aniket@aniket-VirtualBox: ~/exam" is open, displaying the output of the script "1.sh". The user enters four numbers (1, 2, 3, 4) and the script outputs the sum (10) and average (2). The terminal window has a dark background with light-colored text. The desktop background is dark.

```
aniket@aniket-VirtualBox:~/exam$ bash 1.sh
Enter four numbers 1 2 3 4
Sum of 4 numbers is 10 and average is 2
aniket@aniket-VirtualBox:~/exam$
```

Q2.





Oct 21 18:06

```
aniket@aniket-VirtualBox:~$ touch fileexam.txt
aniket@aniket-VirtualBox:~$ ln fileexam.txt newhard.txt
aniket@aniket-VirtualBox:~$ ls
10.sh    7.sh     eight.sh      for.sh      new.tar   t1
11.sh.save 8.sh     exam        four.sh     new.zip   t2
13.sh    9.sh     f1.sh       ln          one.sh    temp2.sh
14.sh    assign   f2.sh       Music       Pictures  Templates
15.sh    cdac.sh  f3.sh       my2        prac      temp.sh
16.sh    check    file1.sh    my_file.sh  Public    ten.sh
17.sh    demo     file2.sh    name.sh    root1    testsed.sh
1.sh     demo.tar fileexam.txt newhardlink.sh seven.sh test.tar
2.sh     Desktop  file_hardlink.sh newhard.txt shree    tetsed.sh
3.sh     dir1     file.sh     new_link.sh six.sh   three.sh
4.sh     dir.zip  file_softlink.sh newlink.txt snap     two.sh
5.sh     Documents file.txt    newname.sh sum2.sh Users
6.sh     Downloads five.sh    newsoftlink.sh sum.sh  Videos
aniket@aniket-VirtualBox:~$
```



Home