JASVEENA - 224001588

TASK 5.2C

CLOUD COMPUTING

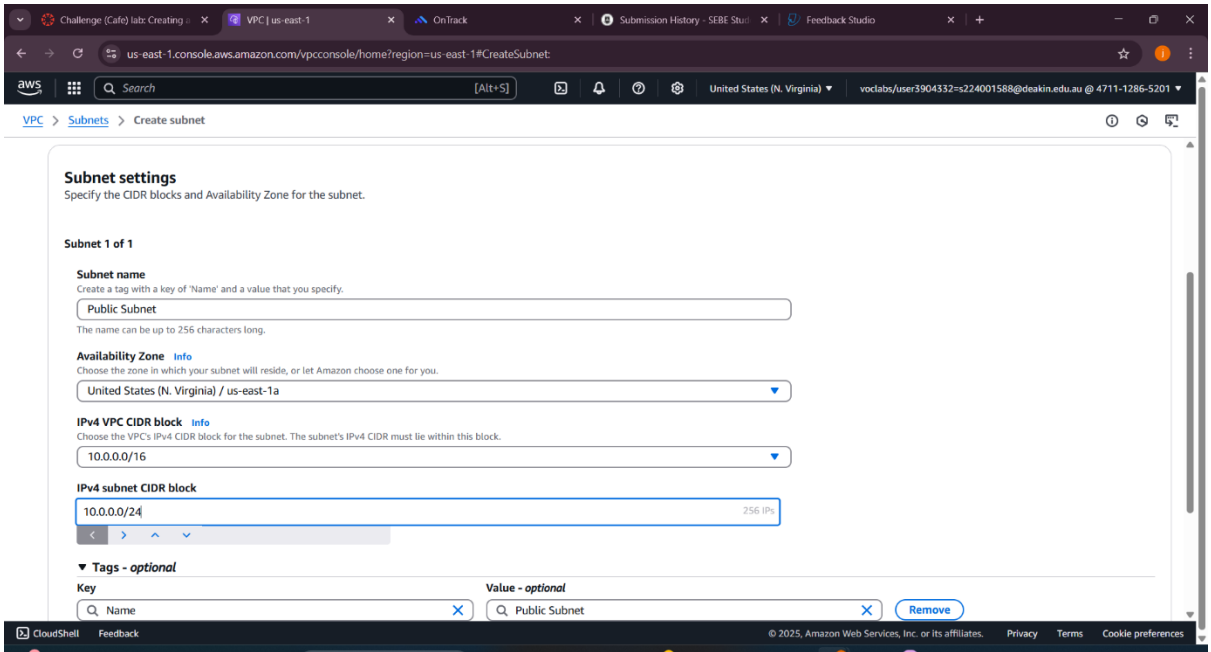
Creating a VPC Networking Environment for the Café

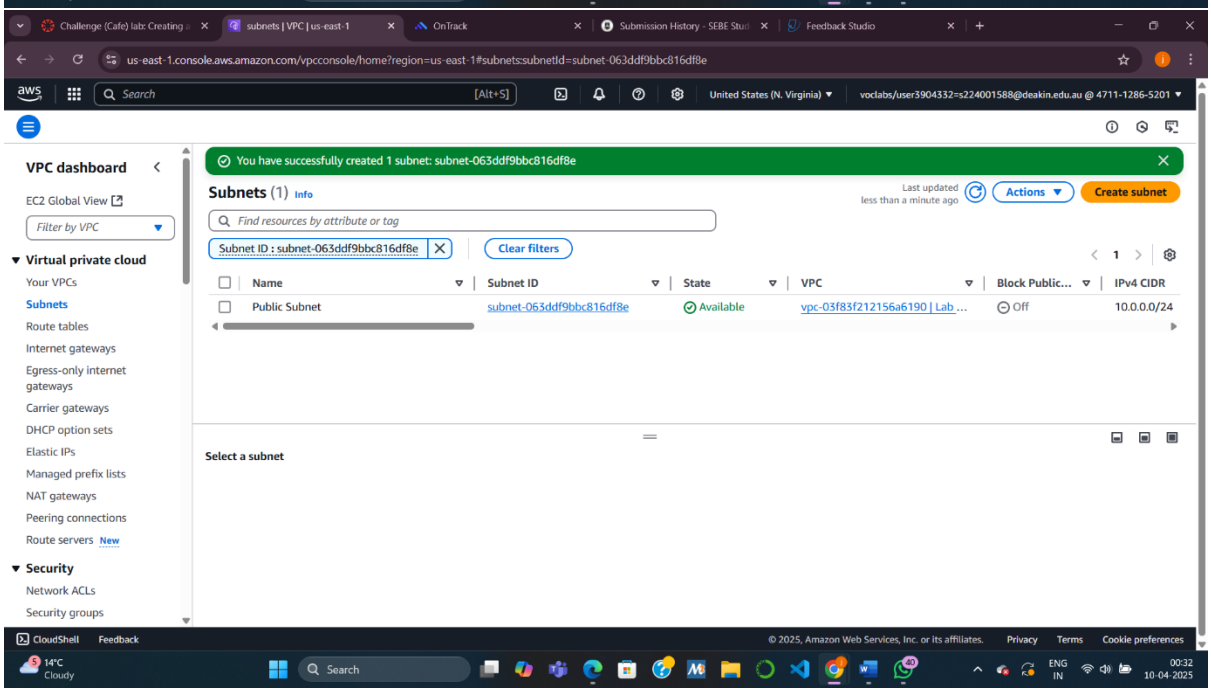
Challenge 1: Set up Secure Admin Access & Internet Access for Private Instances

Task 1: Creating a Public Subnet

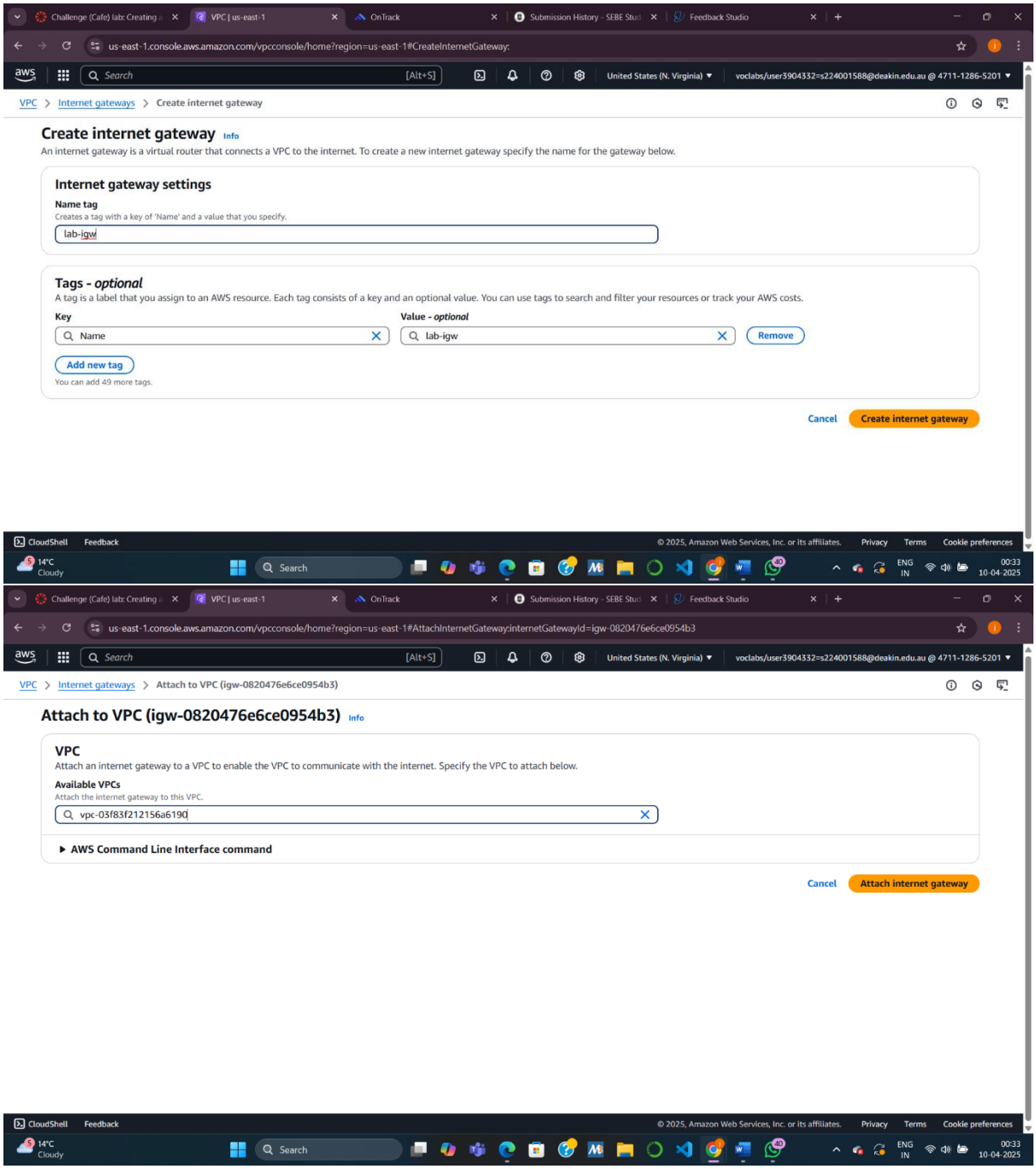
- **Purpose:** Create a subnet that is connected to the internet.
- **Steps:**
    - Create a subnet (CIDR: 10.0.0.0/24) in **Availability Zone A**.
    - Create and attach an **Internet Gateway** to the Lab VPC.
    - Update the **Route Table** associated with this subnet to direct internet traffic (0.0.0.0/0) through the internet gateway.

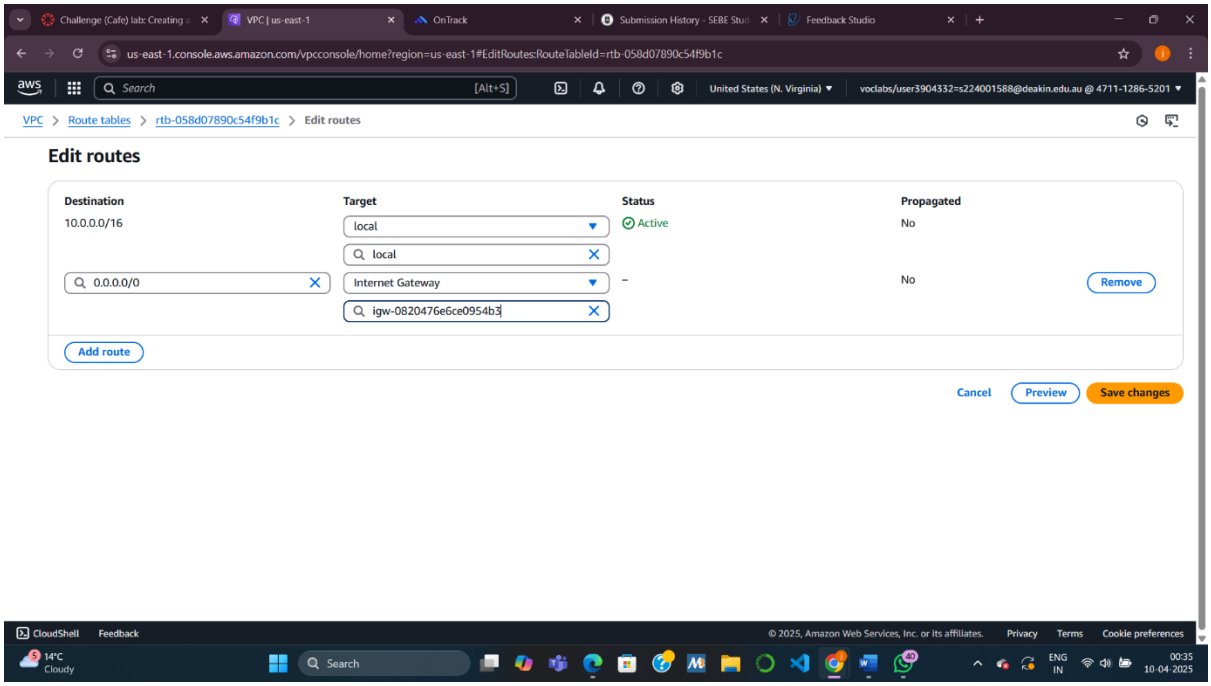
JASVEENA - 224001588





JASVEENA - 224001588

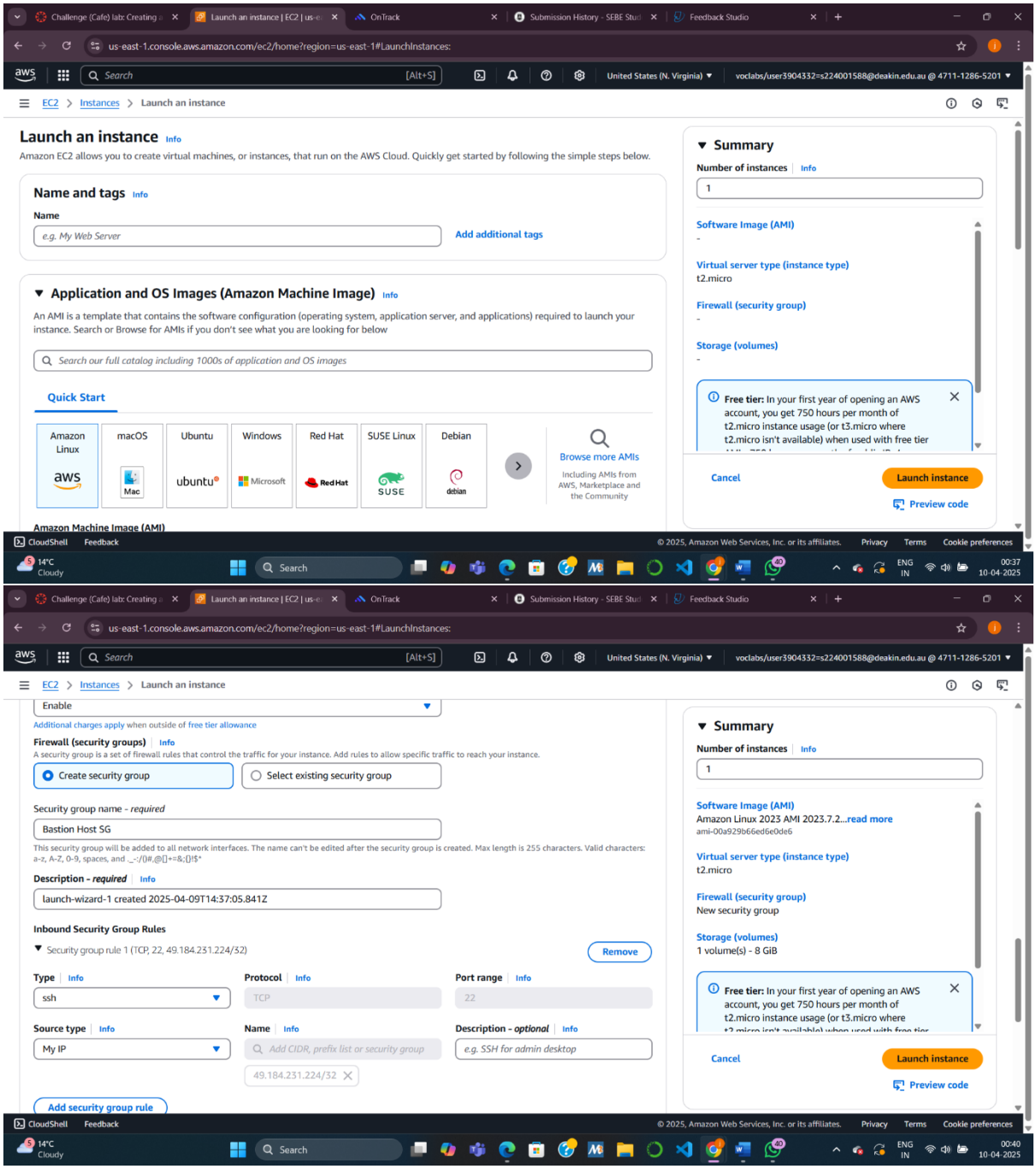


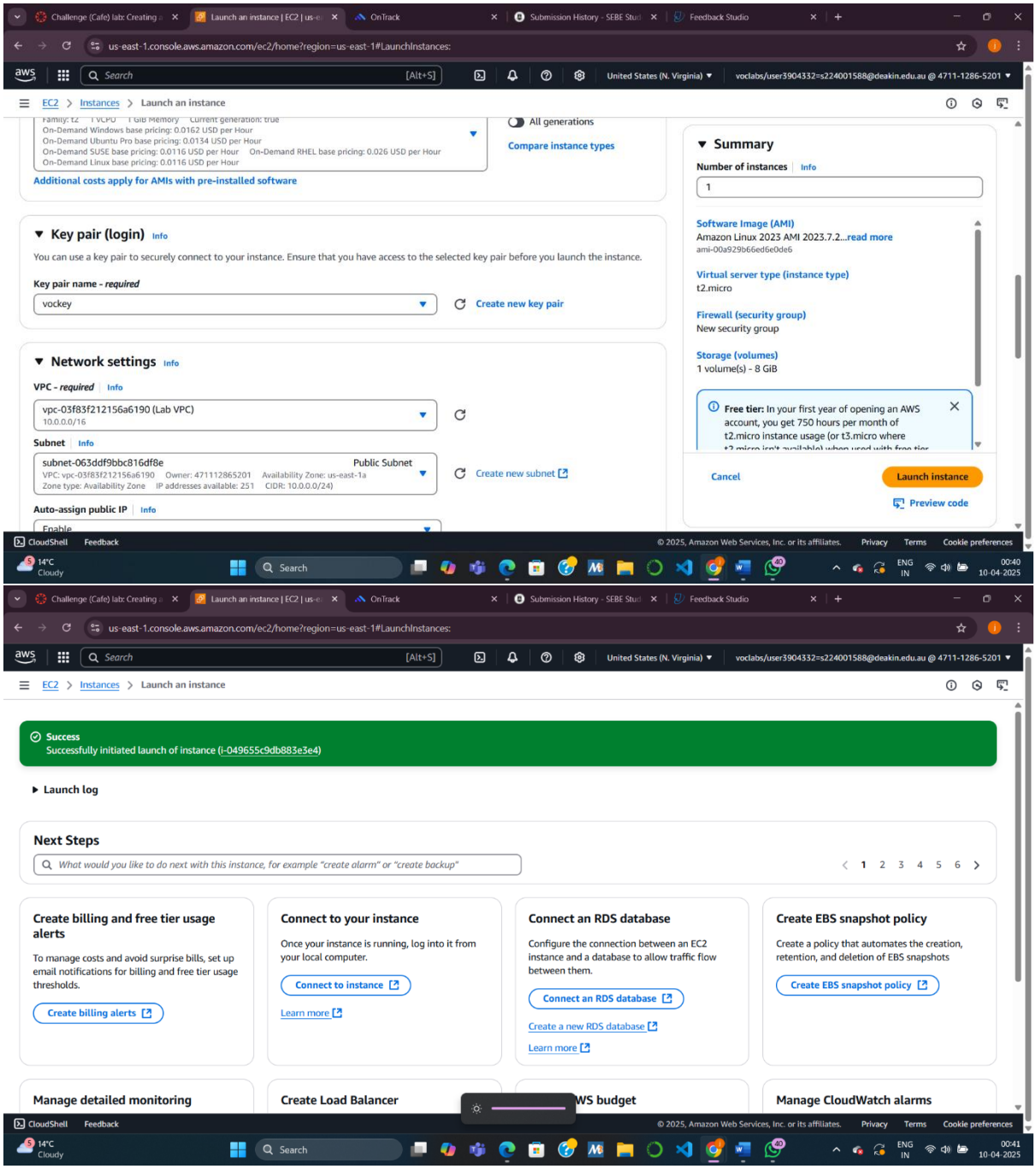


Task 2: Creating a Bastion Host

- **Purpose:** Set up a secure admin jump box for remote access to private instances.
- **Steps:**
  - Launch a **Linux EC2 instance** (t2.micro) in the public subnet.
  - Enable **public IP assignment**.
  - Create and assign a **Security Group (Bastion Host SG)** that allows **SSH (port 22)** access only from **your IP address**.
  - Use **Amazon Linux 2023 AMI** and key pair vockey.

JASVEENA - 224001588



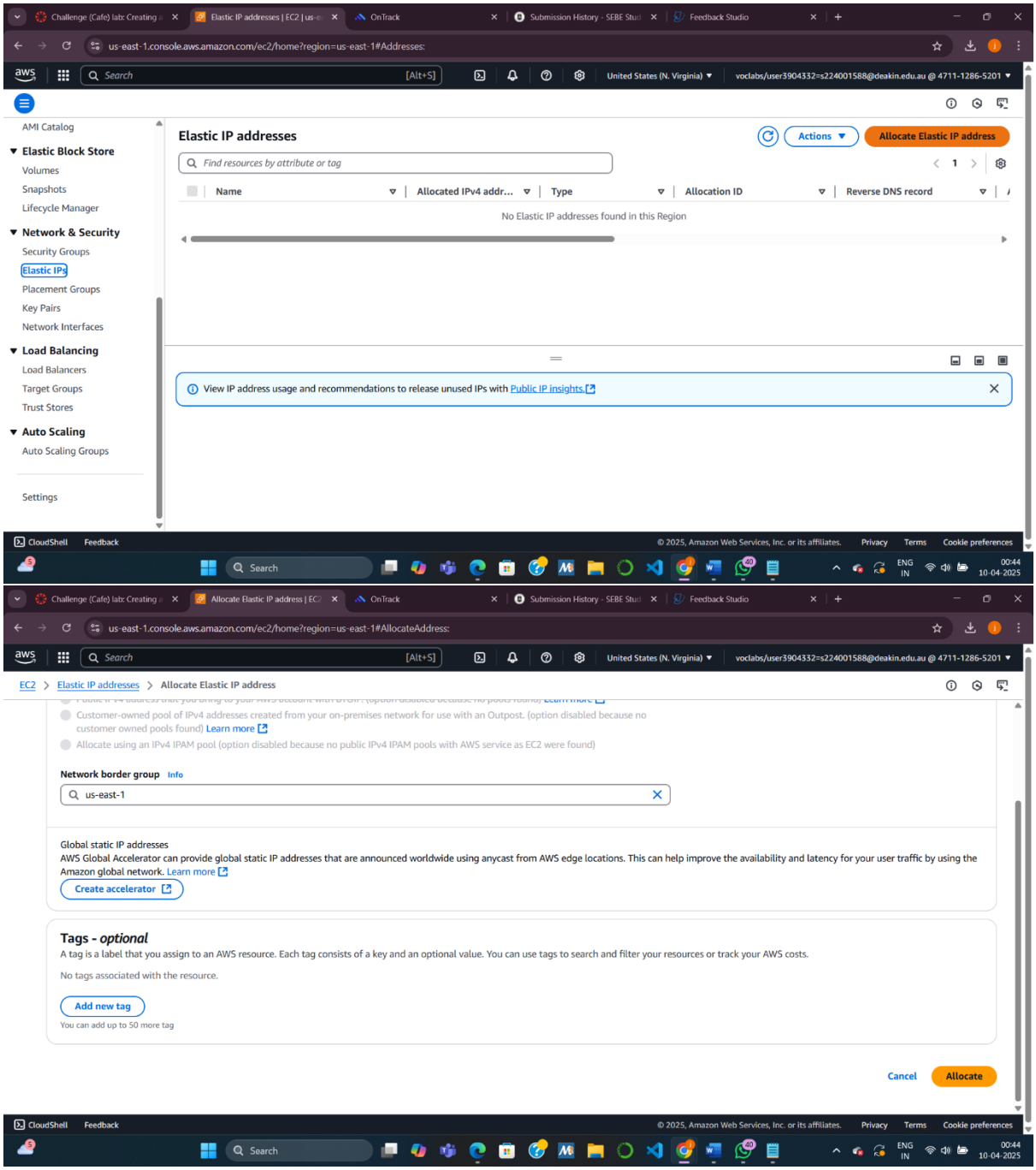


Task 3: Testing the Connection to the Bastion Host

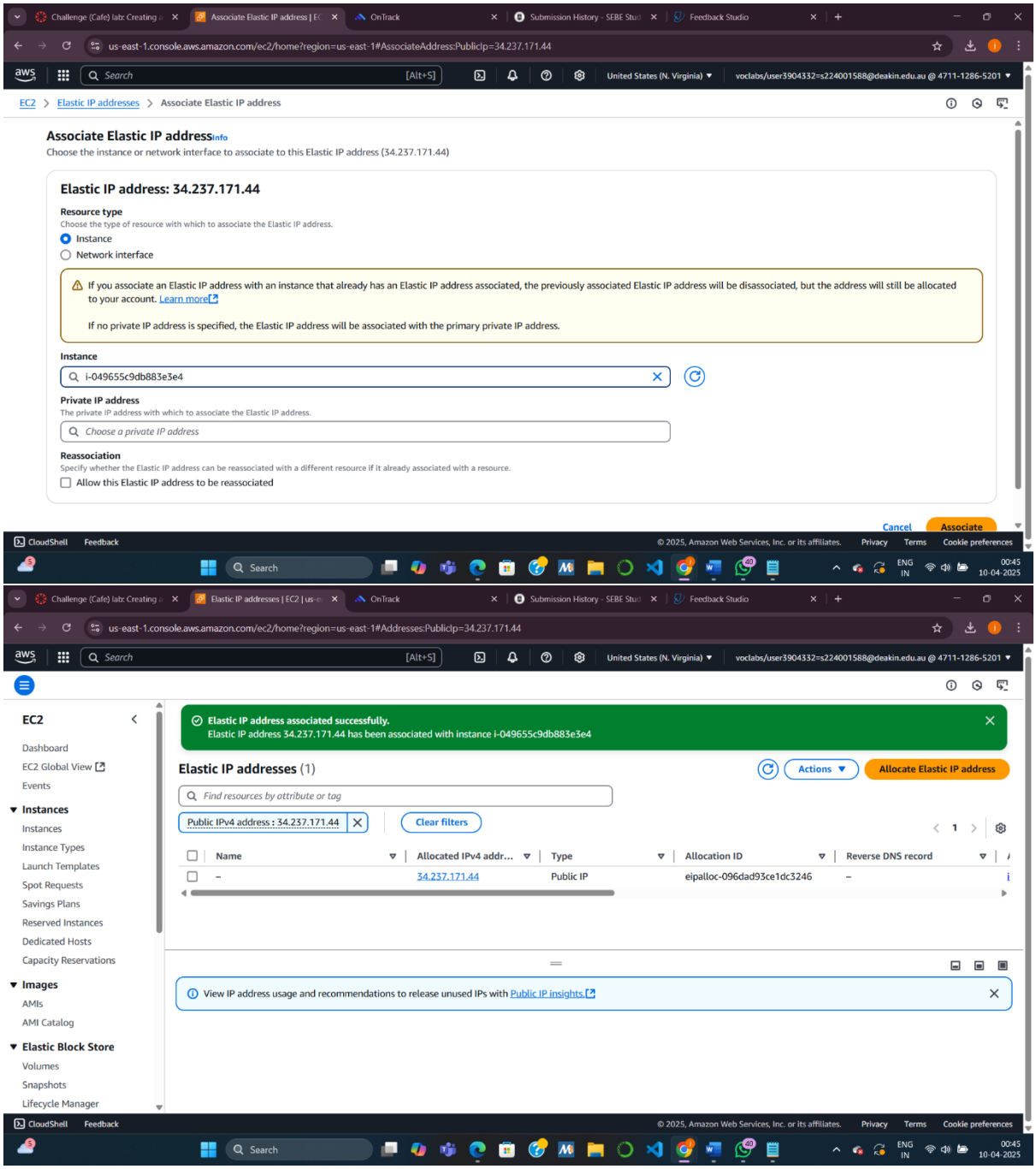
- **Purpose:** Ensure you can remotely connect to the bastion host using SSH.
- **Steps:**
  - Download the appropriate SSH key (.pem or .ppk).
  - Use an SSH client (e.g., PuTTY or terminal) to connect to the Bastion Host.

Task 4: Creating a Private Subnet

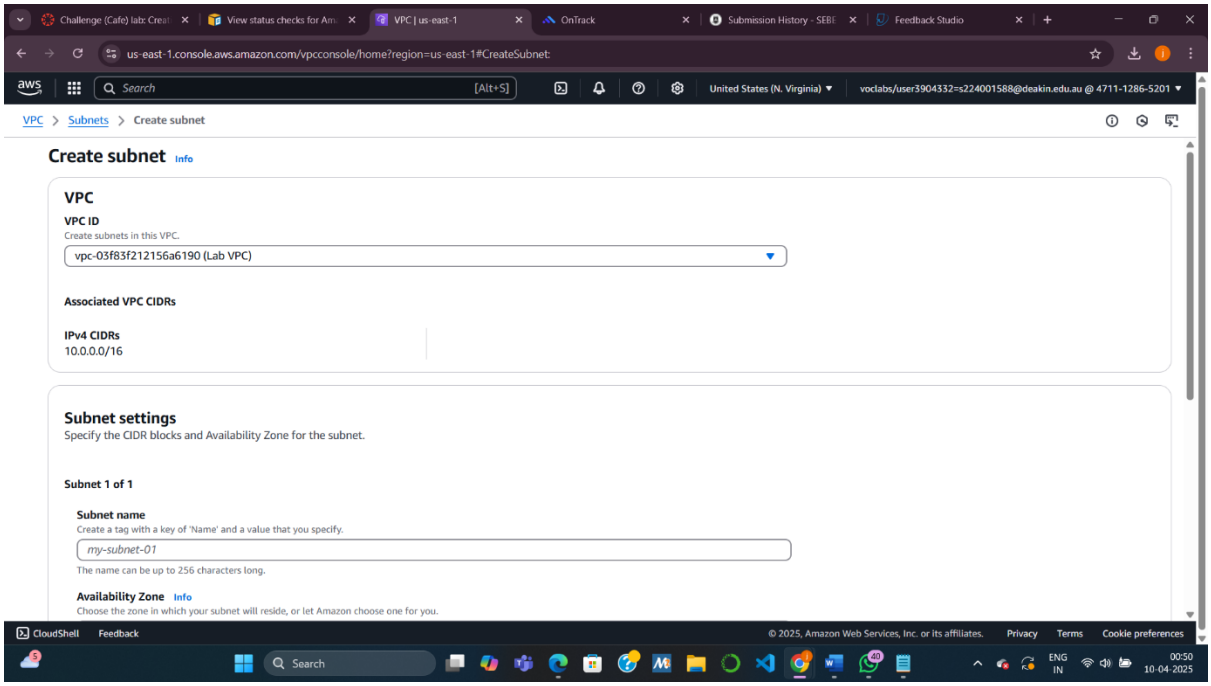
- **Purpose:** Isolate internal resources from direct internet access.
- **Steps:**
  - Create a **new subnet (CIDR: 10.0.1.0/24)** in the same AZ as the public subnet.
  - Do **not** attach an internet gateway or enable public IP assignment.

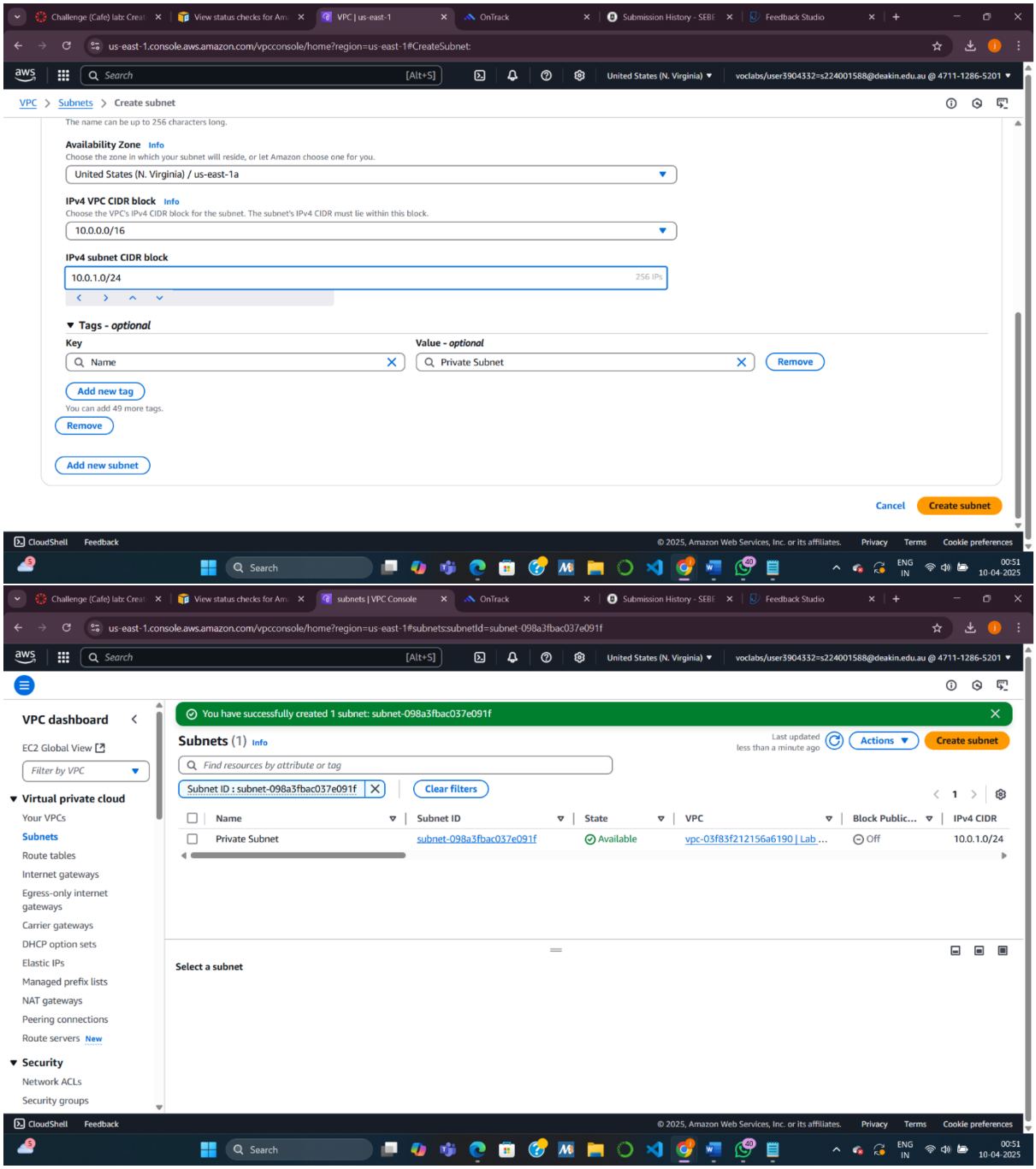


JASVEENA - 224001588



JASVEENA - 224001588

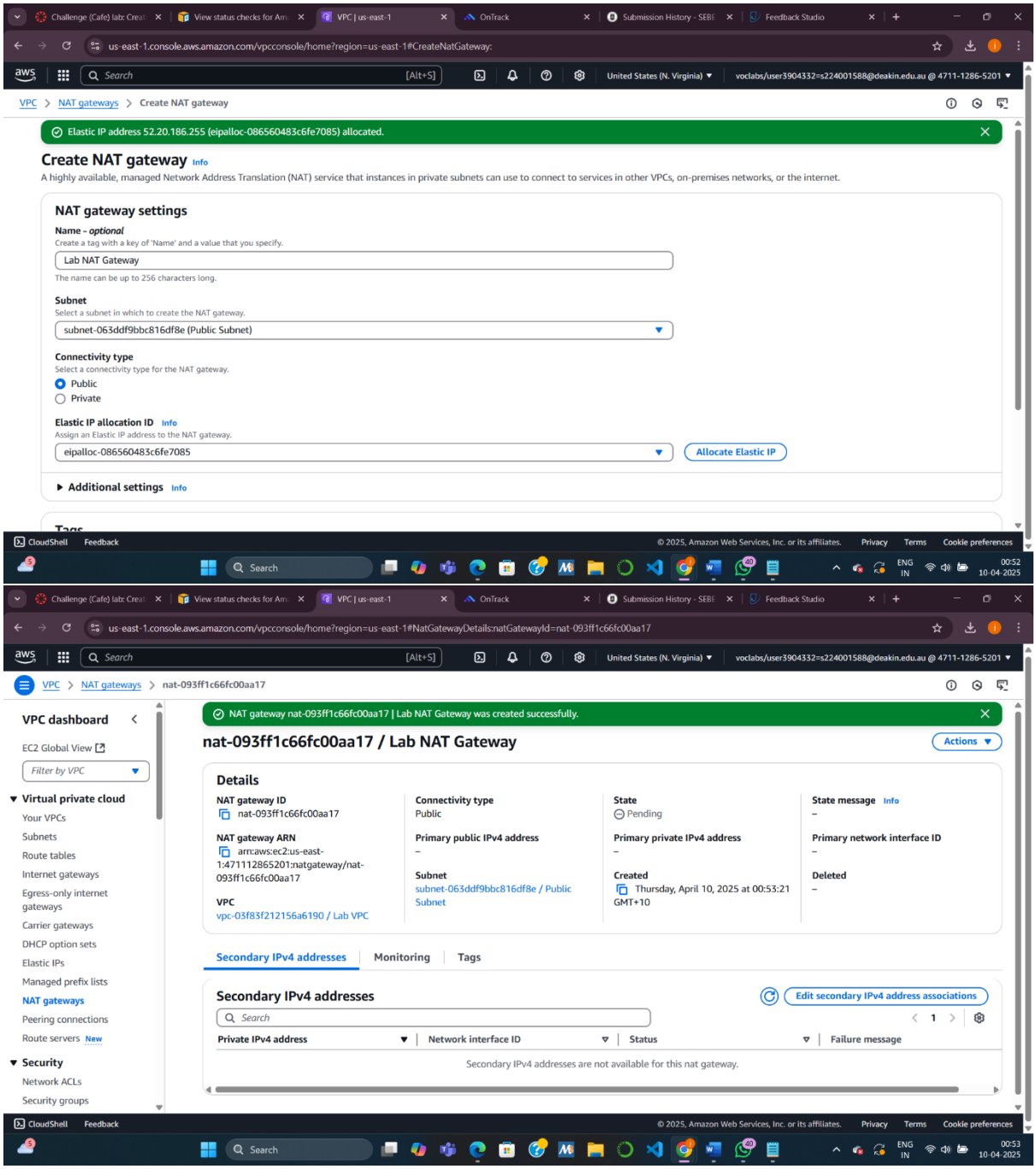




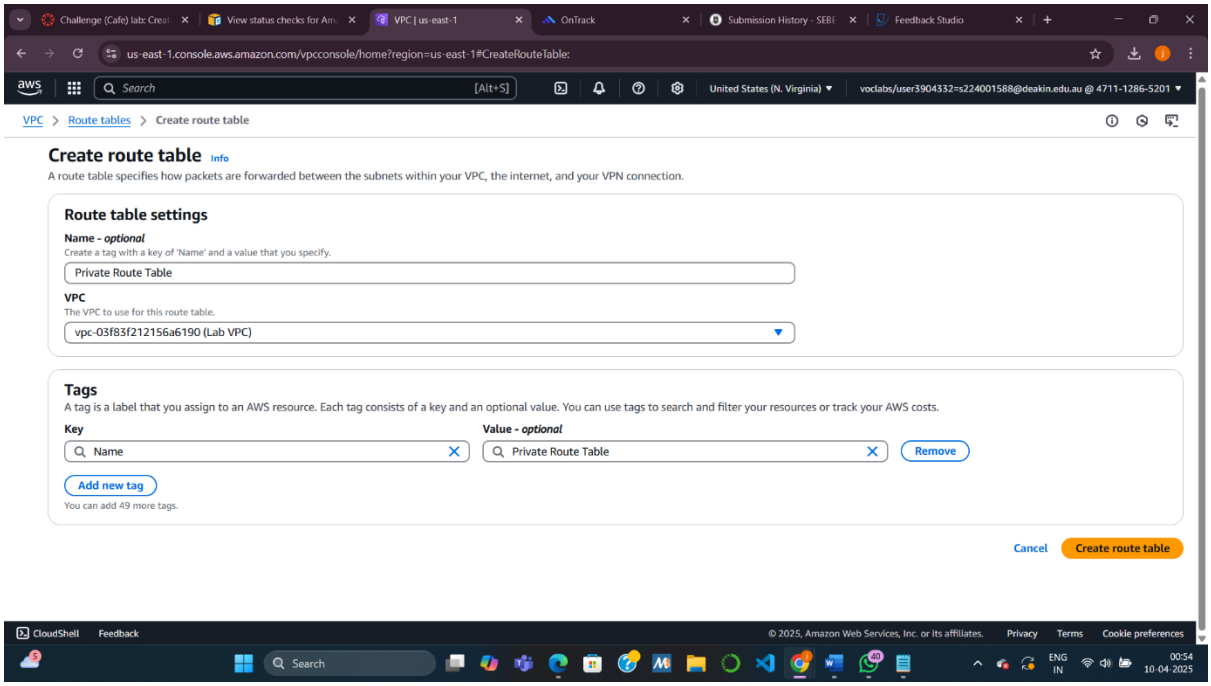
Task 5: Creating a NAT Gateway

- **Purpose:** Allow **outbound internet access** from private subnet instances (e.g., for updates).
- **Steps:**
  - Create a **NAT Gateway** in the **Public Subnet**, and allocate an **Elastic IP**.
  - Create a **new route table**, route all traffic (0.0.0.0/0) to the NAT Gateway.
  - Associate this route table with the **Private Subnet**.

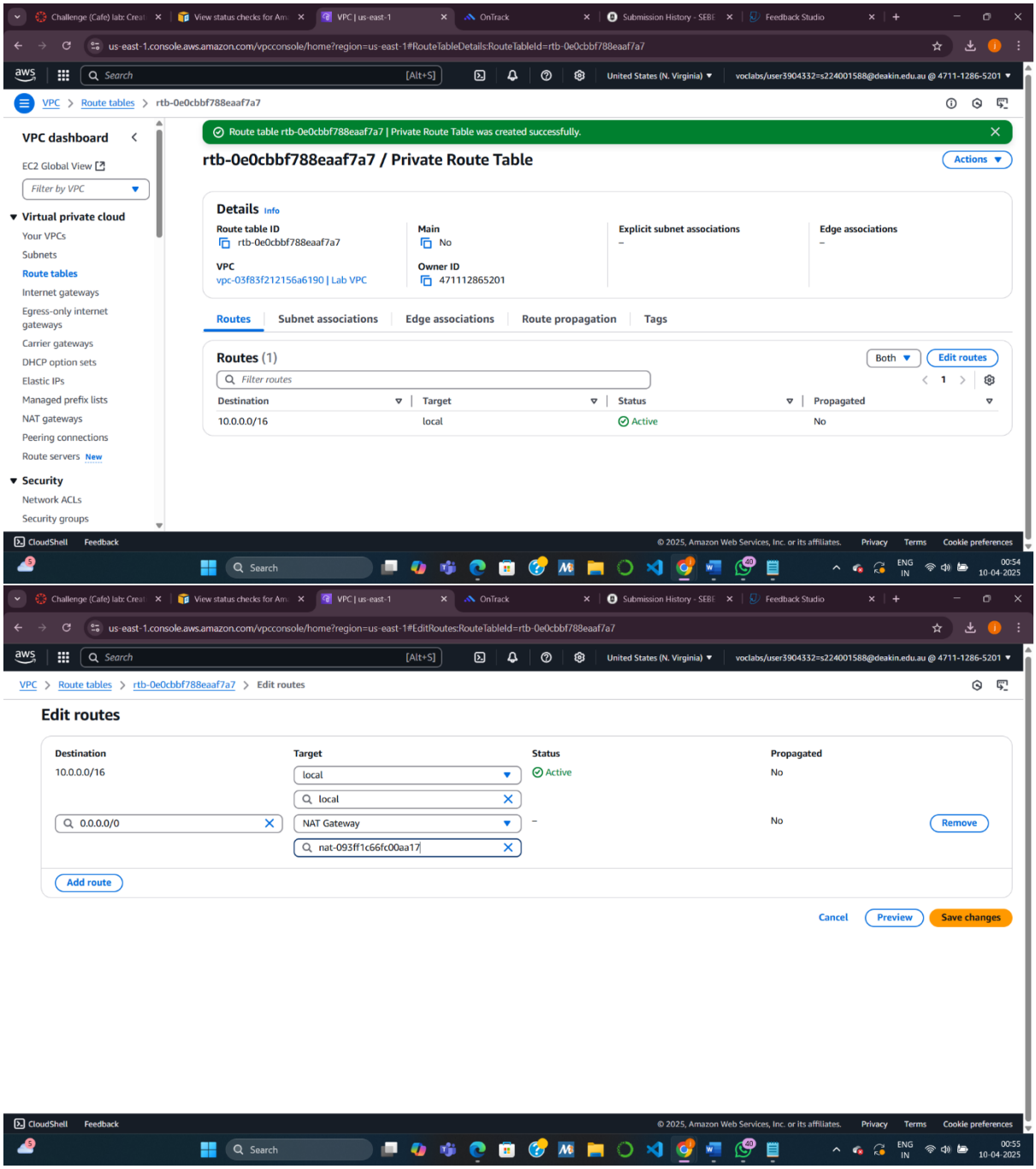
JASVEENA - 224001588

- 

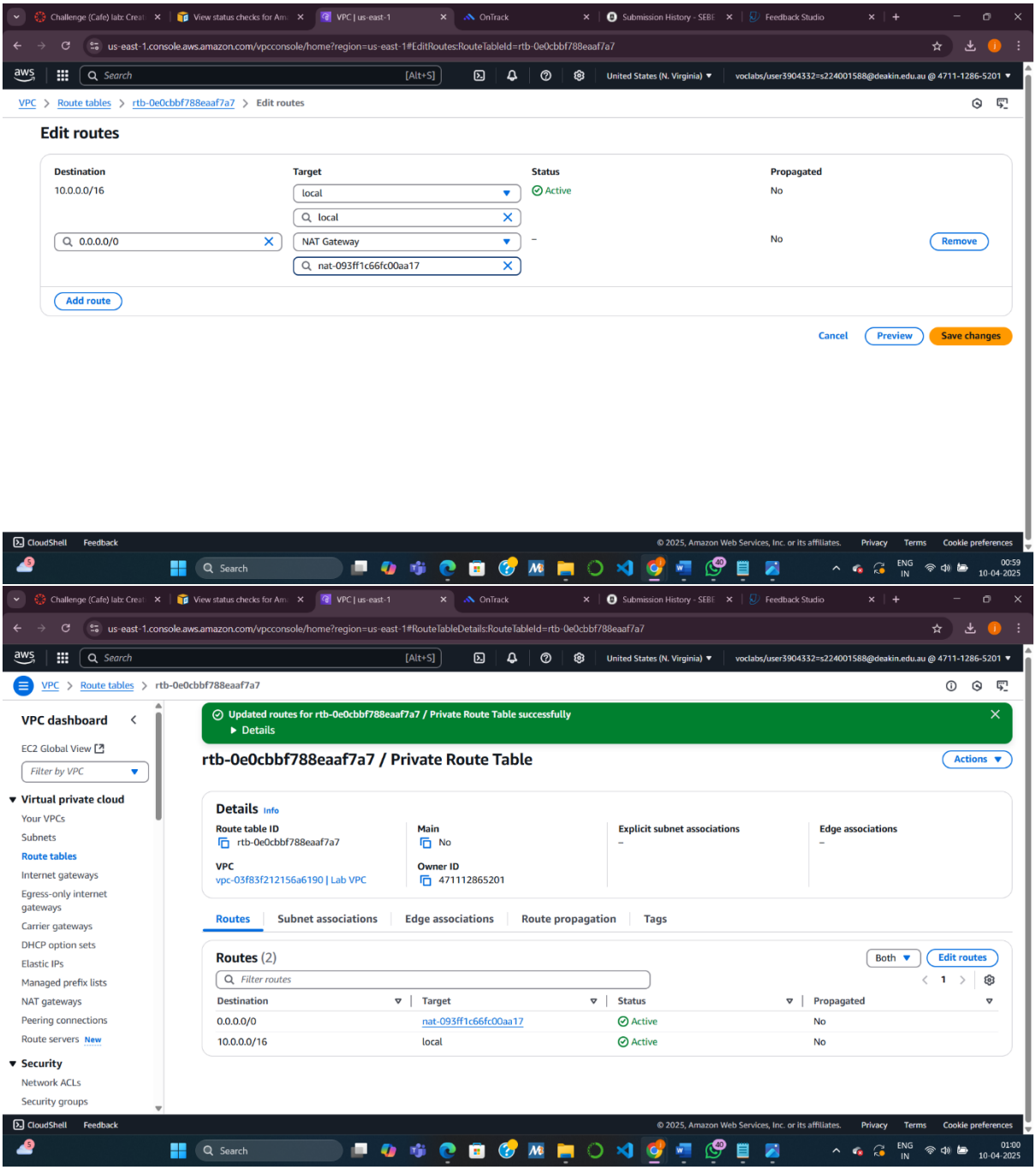
JASVEENA - 224001588

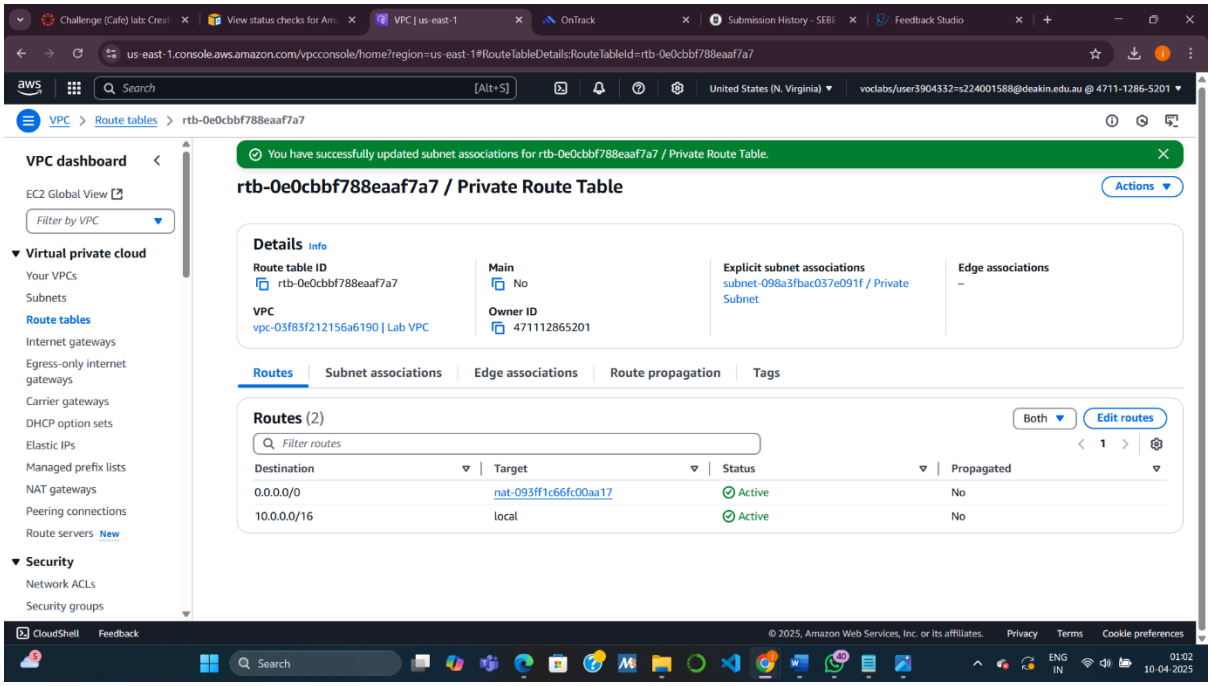


JASVEENA - 224001588

- 

JASVEENA - 224001588

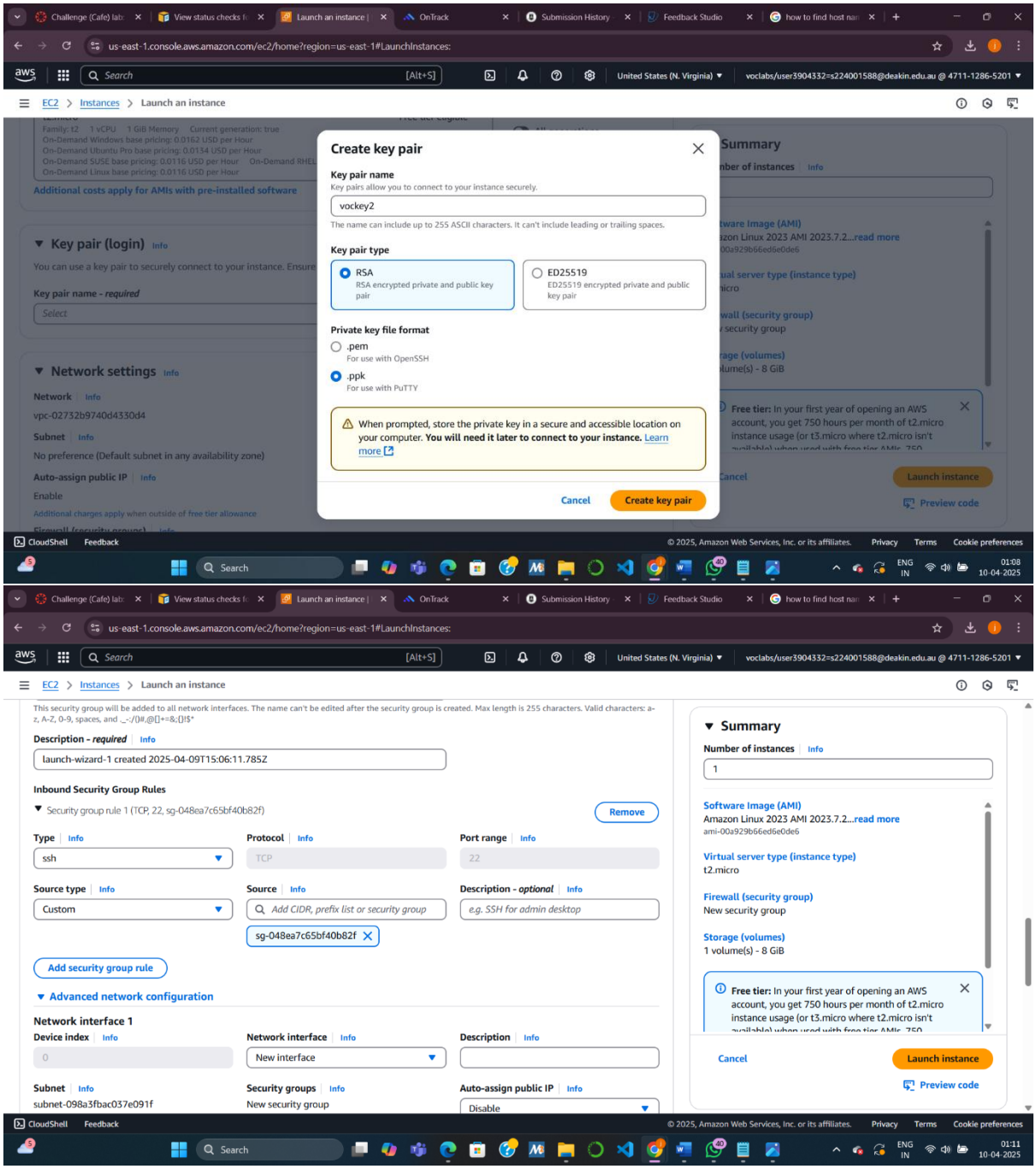


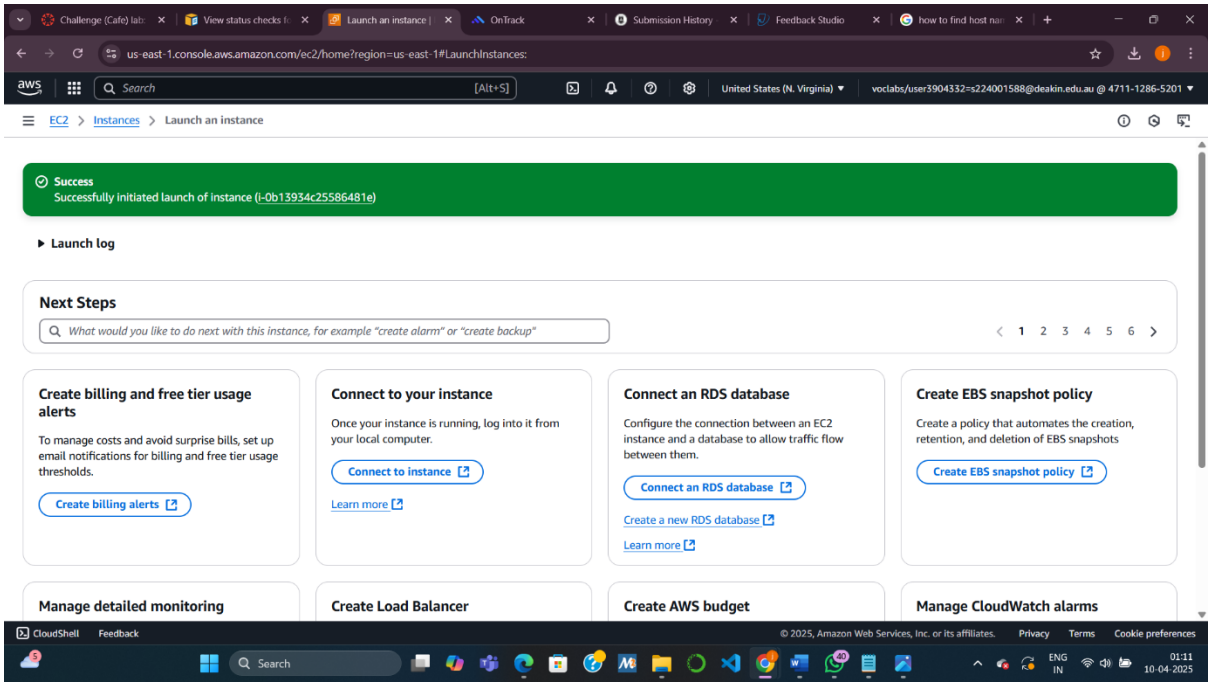


Task 6: Creating an EC2 Instance in the Private Subnet

- **Purpose:** Deploy a backend EC2 instance with no direct internet access.
- **Steps:**
  - Create a **new key pair** (vockey2).
  - Launch an **EC2 instance** (t2.micro, Amazon Linux 2023) in the **Private Subnet** using vockey2.
  - Create a **Security Group (Private Instance SG)** that allows **SSH (port 22)** only from the **Bastion Host SG**.

JASVEENA - 224001588

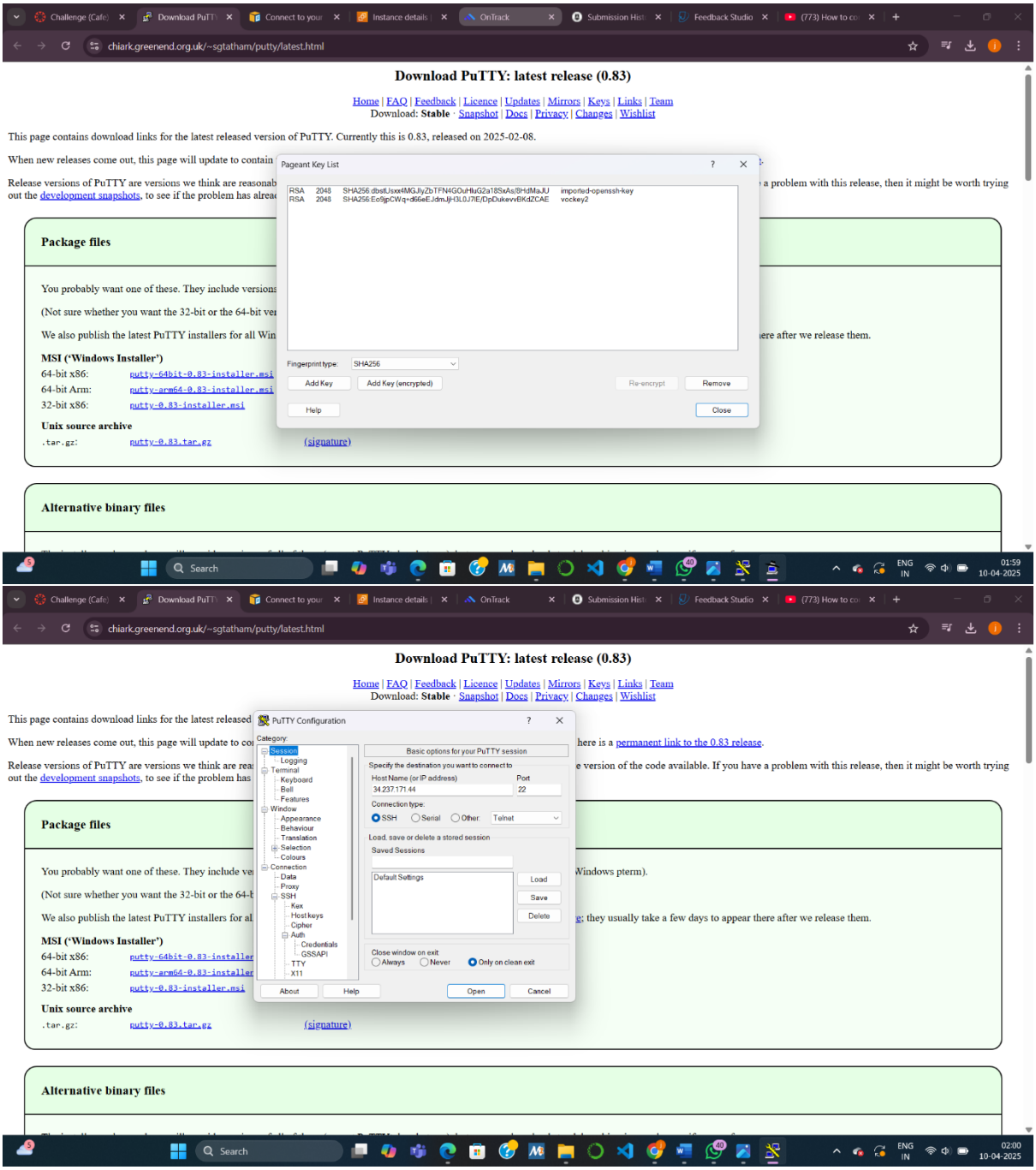


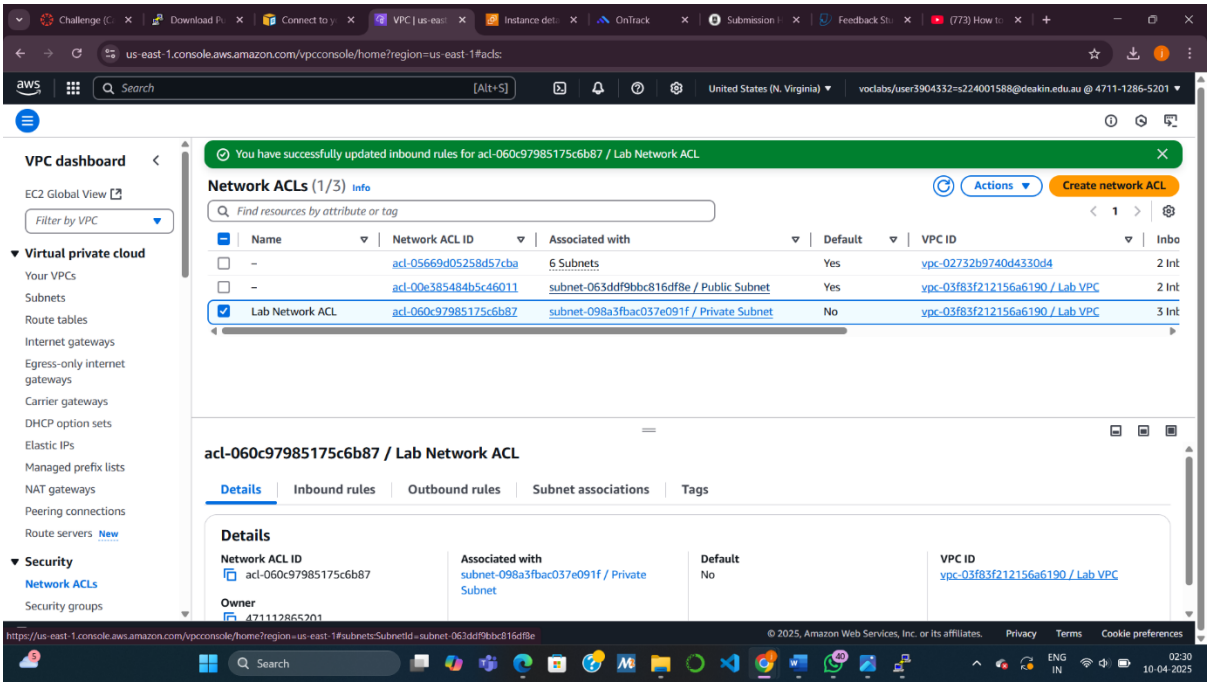


Task 7: Configuring SSH Passthrough (Agent Forwarding)

- **Purpose:** Access the private instance **through the Bastion Host** without copying key files.
- **Steps:**
  - **macOS/Linux:** Use ssh-add to load both vockey and vockey2 into the ssh-agent.
  - **Windows:** Use **Pageant** to load both .ppk files.
  - Enable **agent forwarding** so you can jump from Bastion Host to the Private Instance using the correct key.

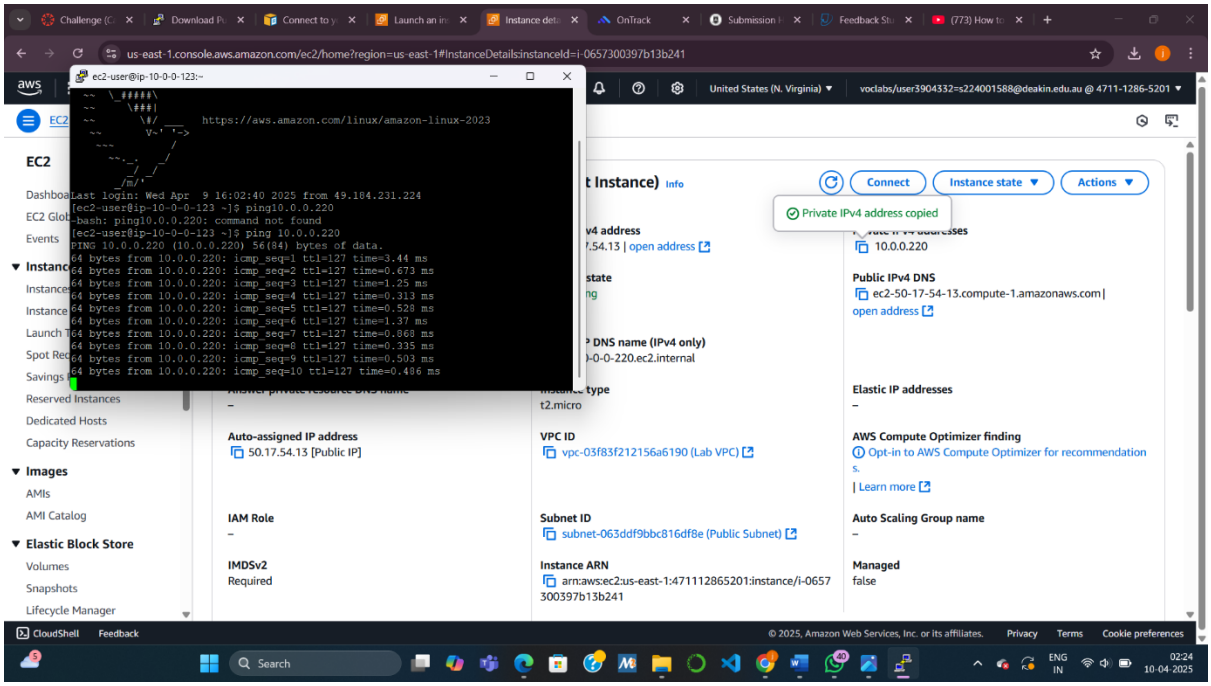
JASVEENA - 224001588

- 



Task 8: Testing the SSH Connection from Bastion to Private Instance

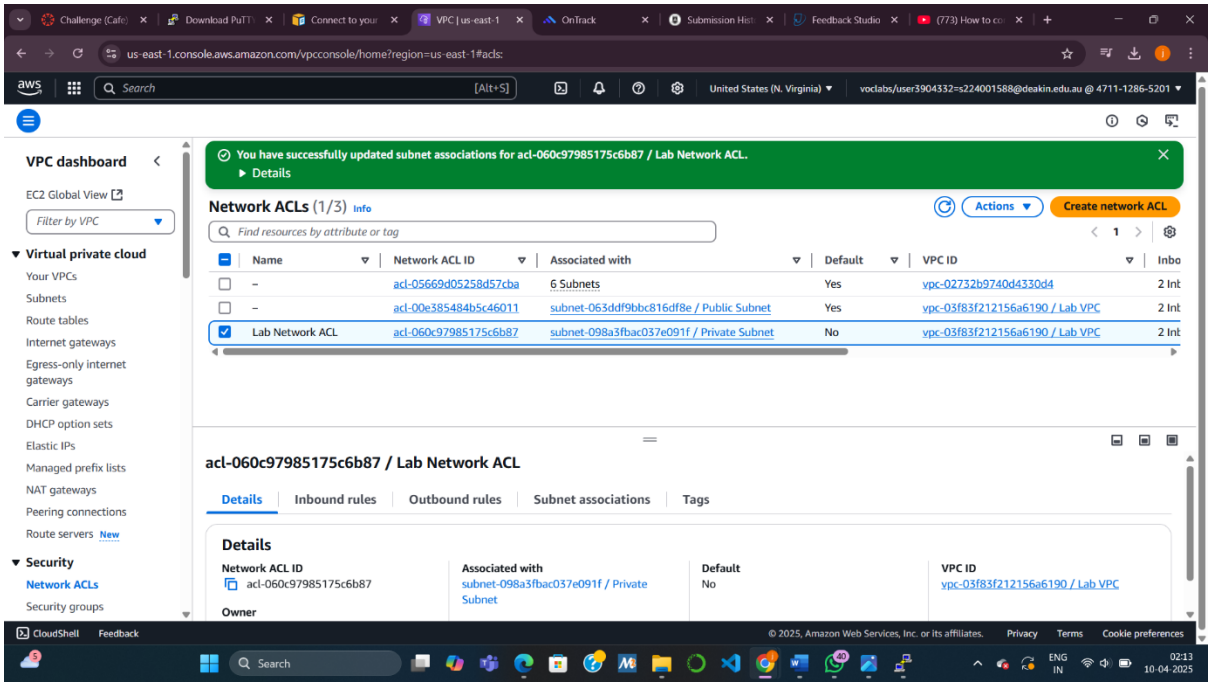
- **Purpose:** Confirm successful passthrough SSH.
- **Steps:**
  - SSH to Bastion Host with agent forwarding enabled.
  - From there, SSH into the **Private EC2 instance** using its **private IP address**.
  - Test internet access from the private instance using ping 8.8.8.8.

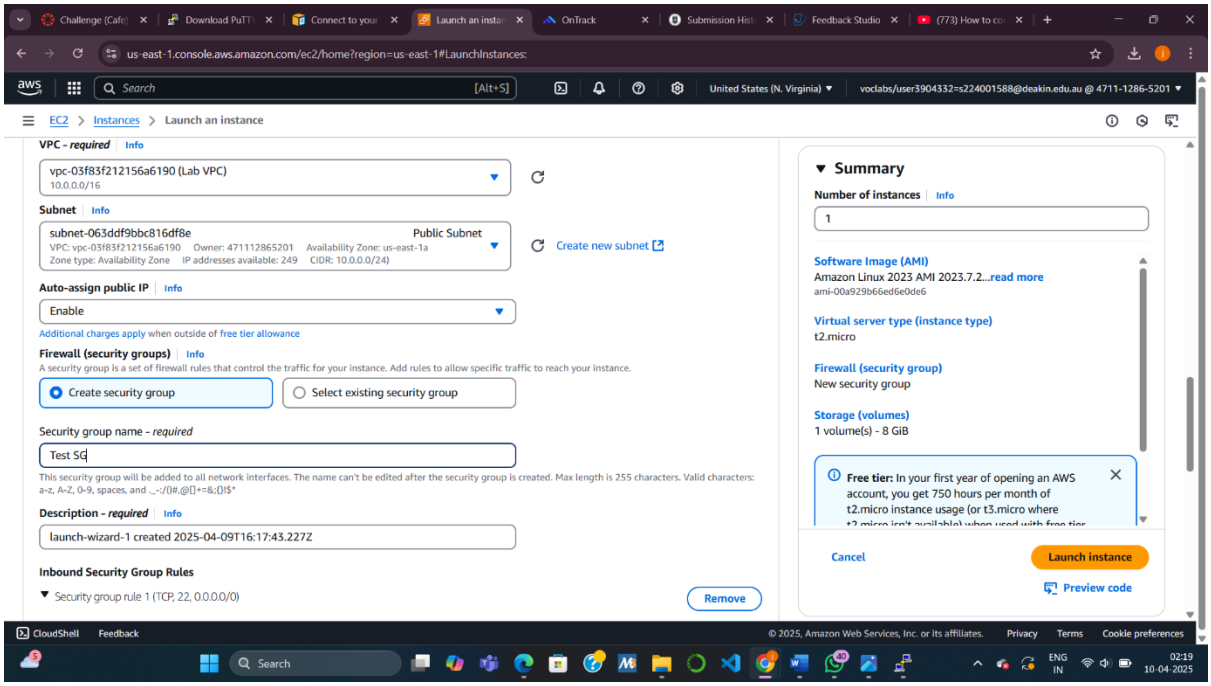


🔒 Challenge 2: Implement Additional Security with Network ACLs

Task 9: Creating a Network ACL

- **Purpose:** Add **another security layer** for the private subnet.
- **Steps:**
  - Create a **custom network ACL** (Lab Network ACL).
  - By default, all traffic is denied.
  - Add **inbound and outbound rules** to allow **all traffic** initially.
  - Associate this ACL with the **Private Subnet**.

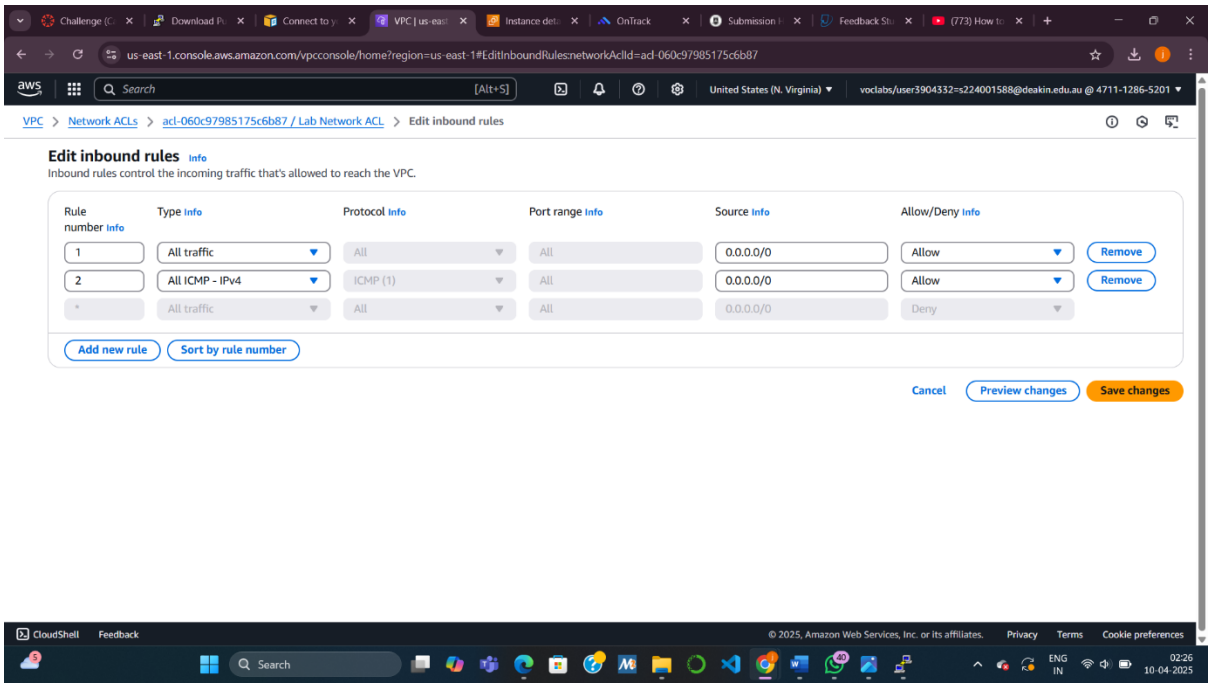




Task 10: Testing Your Custom Network ACL

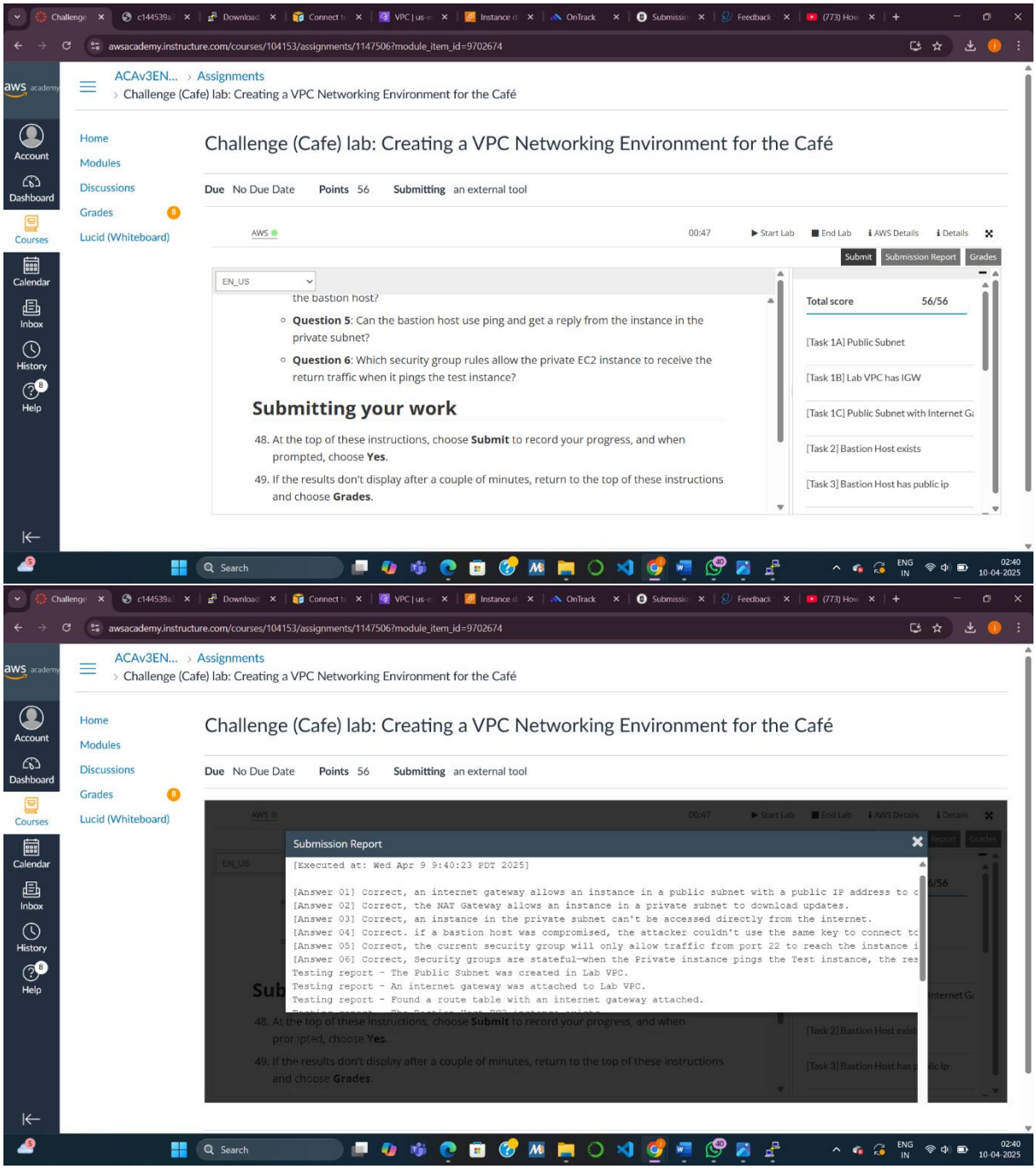
- **Purpose:** Demonstrate control over subnet traffic with the custom ACL.
- **Steps:**
    - Launch a **Test EC2 instance** in the **Public Subnet** with ICMP (ping) enabled via its **Security Group**.
    - From the **Private EC2 instance**, ping the **Test Instance's private IP** — it should respond.
    - Now **modify the ACL** to **deny ICMP IPv4** to the Test Instance's private IP (/32).

- Verify that ping **fails**, showing that traffic is blocked.



JASVEENA - 224001588

JASVEENA - 224001588



What is the purpose of a Bastion Host?
To securely access private instances in a VPC by acting as a jump point from a public subnet.

Why do we need an Elastic IP address?
To provide a **static public IP** for the NAT Gateway so that private instances can access the internet reliably.

Why do we need to use SSH pass through in this lab?
To connect from your local machine → bastion host → private instance **without copying private keys** to the bastion host (enhances security using SSH agent forwarding).