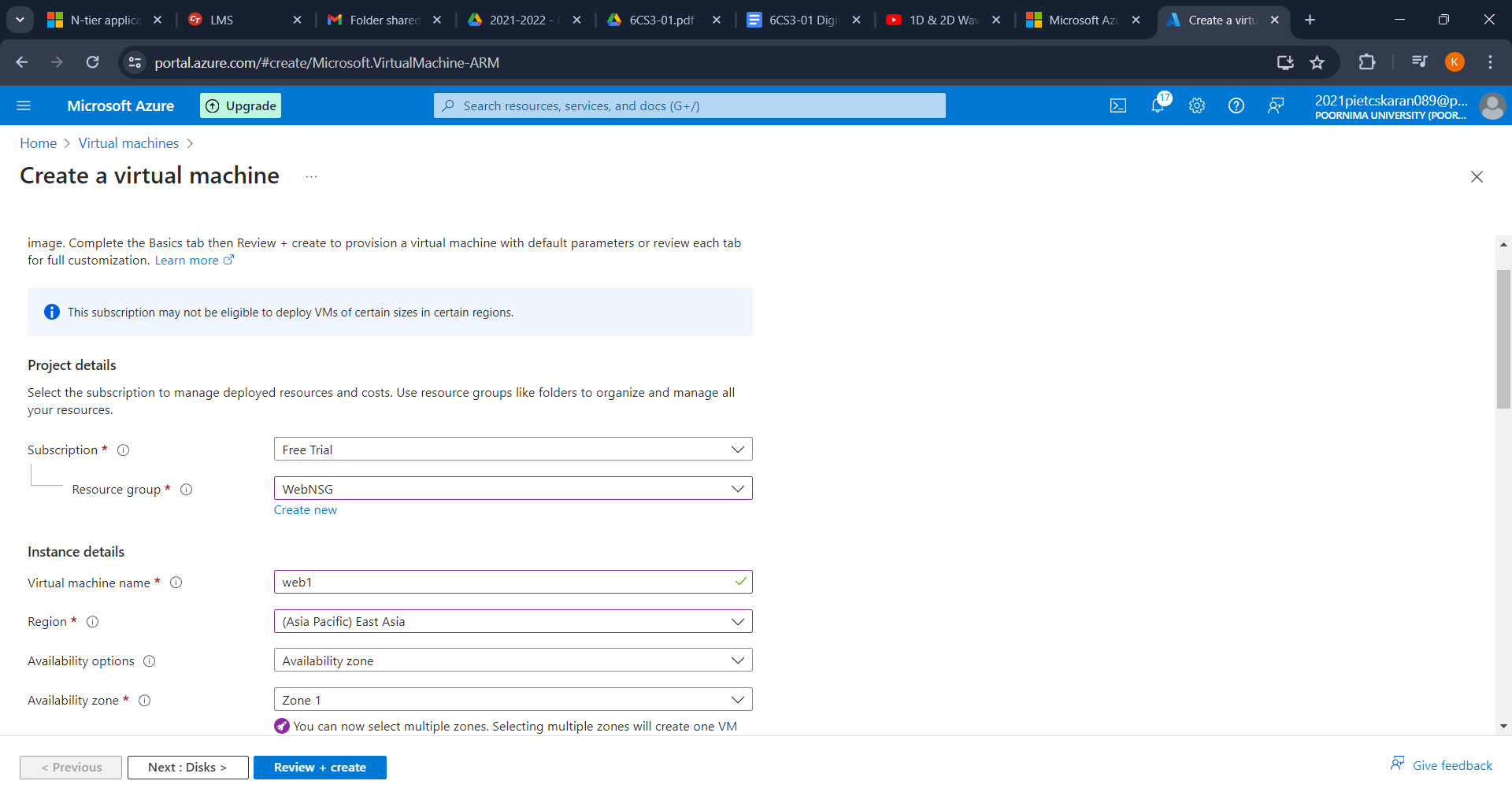
**Q1. Create three subnets : 1. Web tier 2. App tier 3. DB tier DB Tier should not access any tier(Web & App tier) App tier should access the DB tier and Web tier as well, Web tier should acccess only App tier. Only Web tier is allowed to connect to the internet.Deploy two VM's in each tier(One VM should be Linux & another should be Windows). Configure Apache Server on Linux VM's And IIS Server on Windows.**

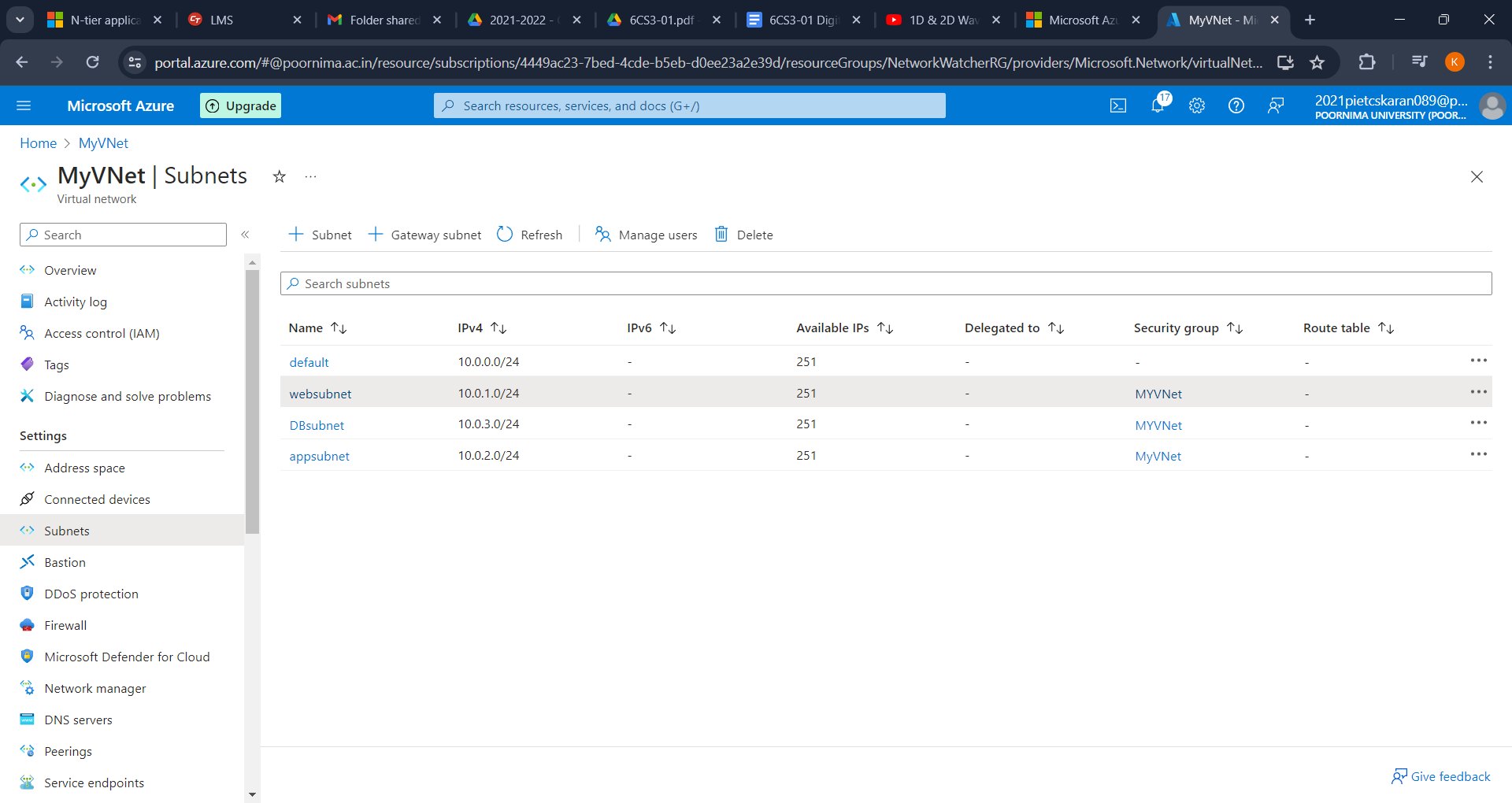
Ans. **Step 1: Create a Virtual Network (VNet)**

1. Go to the Azure Portal.
2. Navigate to "Create a resource" and search for "Virtual Network".
3. Click on "Create" and fill in the details:
4. Name: MyVNet
5. Address space: 10.0.0.0/16
6. Resource Group: Create a new or use an existing one.
7. Region: Select your preferred region.



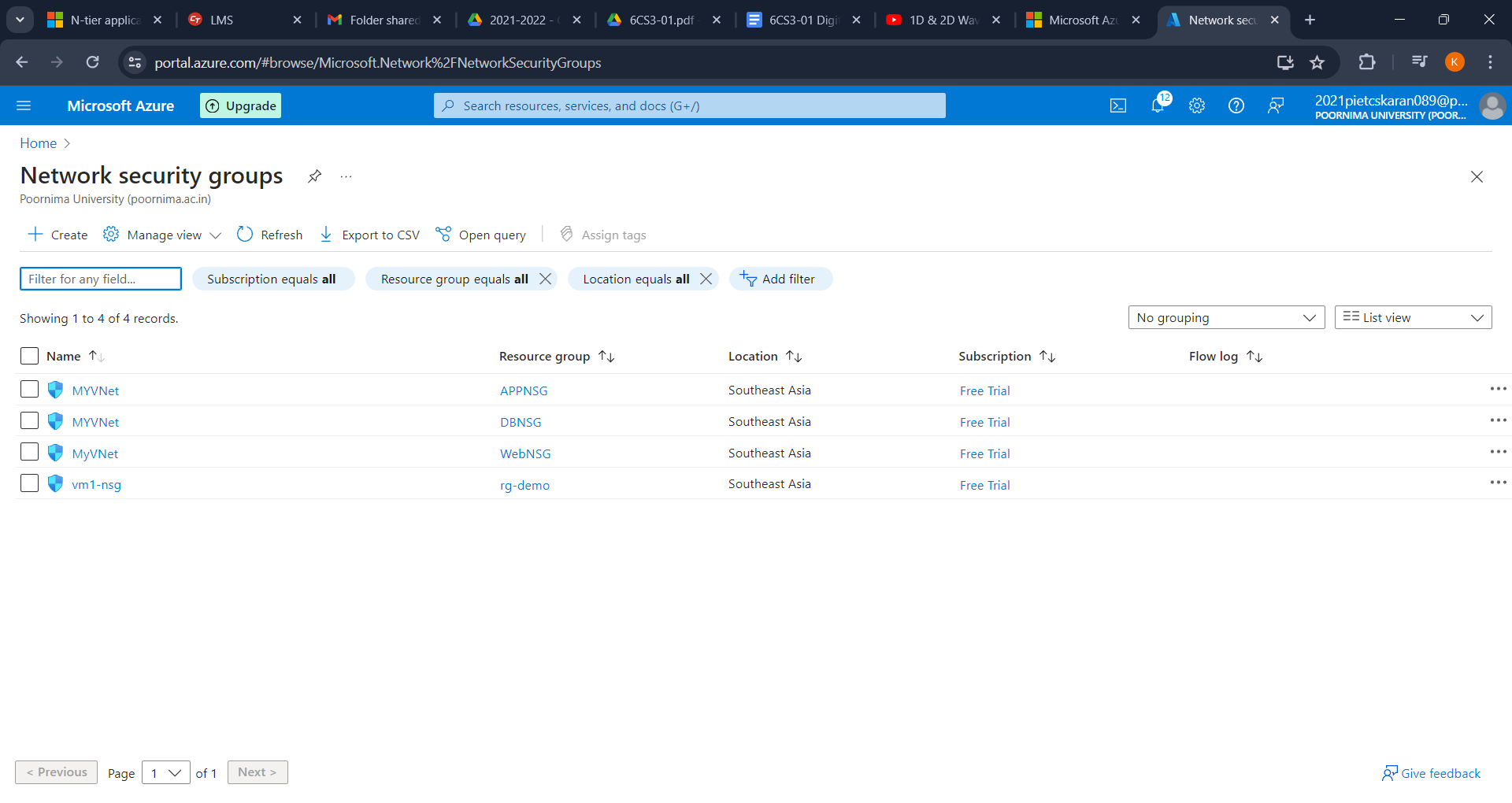
**Step 2: Create Subnets**

1. In the VNet creation process, add three subnets:
2. Web Tier Subnet:
3. Name: WebSubnet
4. Address range: 10.0.1.0/24
5. App Tier Subnet:
6. Name: AppSubnet
7. Address range: 10.0.2.0/24
8. DB Tier Subnet:
9. Name: DBSubnet
10. Address range: 10.0.3.0/24
11. 2. Configure Network Security Groups (NSGs)



**Step 3: Create Network Security Groups**

1. Go to "Create a resource" and search for "Network Security Group".
2. Create three NSGs:
3. WebNSG for the Web tier.
4. AppNSG for the App tier.
5. DBNSG for the DB tier.



**Step 4: Configure NSG Rules**

1. WebNSG:
2. Inbound rules:
3. Allow HTTP (port 80) from any source.
4. Allow SSH (port 22) and RDP (port 3389) from your IP address.
5. Outbound rules:
6. Allow traffic to AppSubnet.
7. AppNSG:
8. Inbound rules:
9. Allow traffic from WebSubnet on necessary ports (e.g., HTTP, custom application port).
10. Outbound rules:
11. Allow traffic to DBSubnet.
12. Allow traffic to WebSubnet.
13. DBNSG:
14. Inbound rules:
15. Allow traffic from AppSubnet on necessary ports (e.g., MySQL port 3306, SQL Server port 1433).
16. Outbound rules:
17. Deny all traffic (default rule).

**Step 5: Associate NSGs with Subnets**

1. **Navigate to each subnet and associate the corresponding NSG.**Outbound rules:
2. Deny all traffic (default rule).
3. Deploy Virtual machines.

**Step 6: Deploy VMs in Web Tier Subnet**

Go to "Create a resource" and search for "Virtual Machine".

1. Create two VMs:
2. Web1 (Linux VM):
3. Name: Web1
4. Image: Ubuntu
5. Size: Choose an appropriate size.
6. VNet: MyVNet
7. Subnet: WebSubnet
8. NSG: WebNSG
9. Public IP: Yes
10. Web2 (Windows VM):
11. Name: Web2
12. Image: Windows Server
13. Size: Choose an appropriate size.
14. VNet: MyVNet
15. Subnet: WebSubnet
16. NSG: WebNSG
17. Public IP: Yes

**Step 7: Deploy VMs in App Tier Subnet**WebNSG:

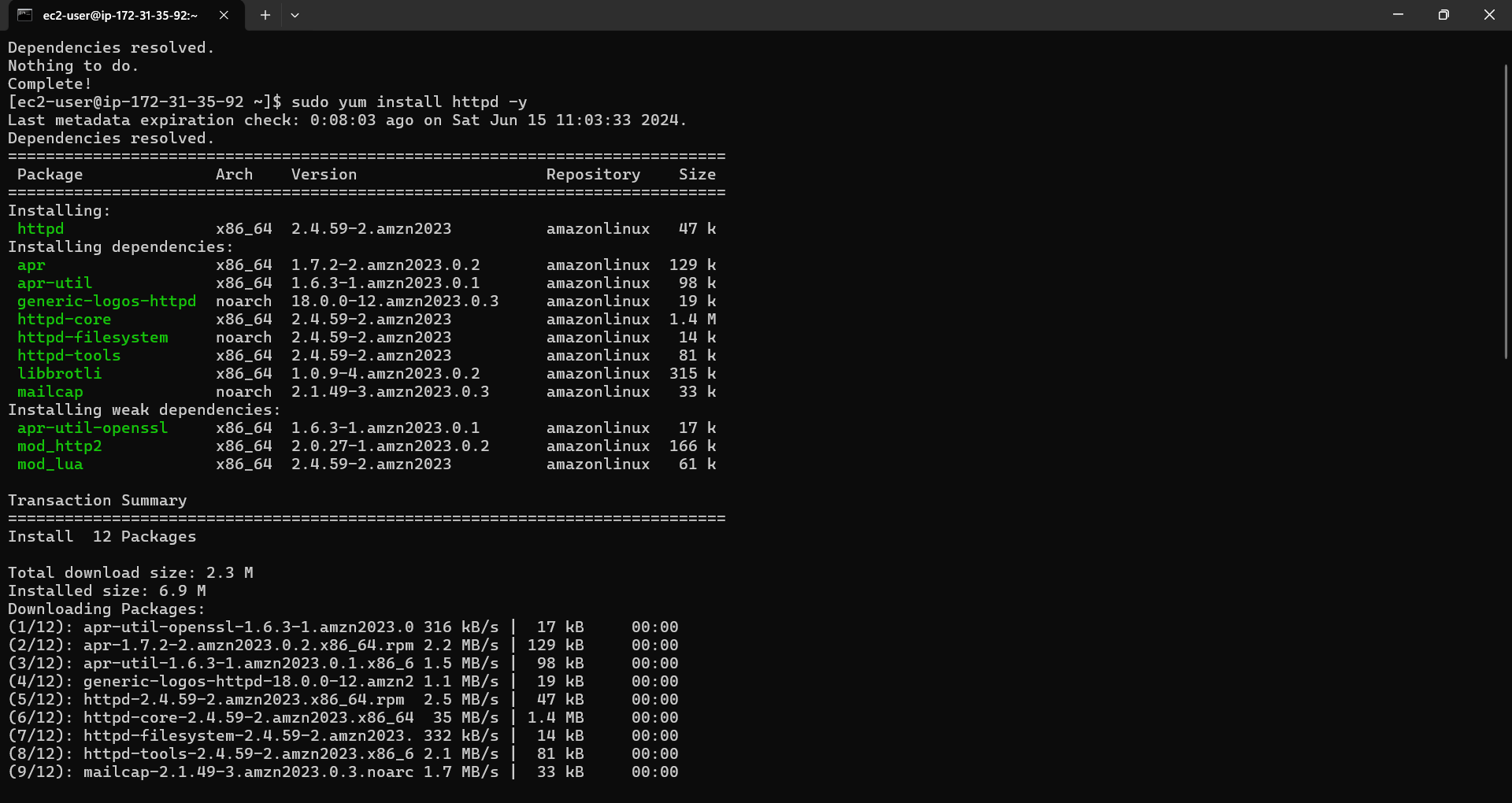
1. Repeat the VM creation process for the App tier:
2. App1 (Linux VM):
3. Name: App1
4. Image: Ubuntu
5. VNet: MyVNet
6. Subnet: AppSubnet
7. NSG: AppNSG
8. Public IP: No
9. App2 (Windows VM):
10. Name: App2
11. Image: Windows Server
12. VNet: MyVNet
13. Subnet: AppSubnet
14. NSG: AppNSG
15. Public IP: No

**Step 8: Deploy VMs in DB Tier Subnet**

1. Repeat the VM creation process for the DB tier:
2. DB1 (Linux VM):
3. Name: DB1
4. Image: Ubuntu
5. VNet: MyVNet
6. Subnet: DBSubnet
7. NSG: DBNSG
8. Public IP: No
9. DB2 (Windows VM):
10. Name: DB2
11. Image: Windows Server
12. Subnet: DBSubnet
13. NSG: DBNSG
14. Public IP: No

**Step 9: Configure Apache on Linux VMs**

1. sudo yum update -y
2. sudo yum install httpd -y
3. sudo systemctl start httpd
4. sudo systemctl enable httpd



**Step 10: Configure IIS on Windows VMs**

1. RDP into Web2 and App2 and install IIS

**Step 11: Configure Access and Restrictions**

1. Ensure that the App Tier can access the DB Tier by configuring necessary database connections.
2. Confirm that the DB Tier cannot access the Web or App Tiers by using NSG rules.

**Step 12: Testing**

1. Test connectivity between tiers to ensure configurations are correct.
2. Verify that the web servers are accessible from the internet and that the database servers are not.
3. Public IP: No