1. Launch and configure an EC2 and install apache web server on it
2. Allocate an elastic ip to the instance and change instance type
3. Create and attach additional volume to the instance
4. Configure snapshot lifecycle policy for the volume
5. Take backup and restore using the ami of the instance .
6 . Try and perform all the console level activities listed above using aws cli commands .
7. Try and address the question " How to recover a instance if we lose the key "
8. Create a load balancer with 3 instances , all should be in seperate azs
make sure all resources are deleted post practice

9. Create an S3 bucket ,
Bucket should have versioning , CRR , Lifecycle rule enabled.
Also should have a static website hosted on it.
Bucket policy should restrict all users to put new objects in the bucket .

10.
S3 and IAM use case
- Create 3 Users in IAM :
- Create a S3 Bucket in North Virginia Region.
- Create a "home" directory under this Bucket in NV Region.
- Create directories like : home/user1, home/user2 , home/user3 in the same Bucket.
- Create a IAM policy that should only allow specific IAM users to upload files in their respective folder only.
- For e.g : user1 should only be allowed to download and upload files in "home/user1" directory.
Also, user1 should not be able to view,list,download,upload any data in another user's directory.
- Enable CRR on this Bucket to another region for Backup.
Acceptance Criteria:
- Apply the IAM policy to users/group and Test the Above scenario.

11.
Create a VPC
3 subnets need to be created inside it
add igw via route table for the subnets
Create a new NACL which will be dedicated for 1 subnet . Default NACL for other 2
Launch EC2 instance in each subnet , and check if we are able to connect to them
Additionally also check if we are able to ping the other instance from each other using private ip (modify the security group accordingly)

12.
Launching EC2 instance in Default VPC:
- Launch multiple Amazon Linux 2 Instance in different AZs.
- Install apache webserver on EC2 instances.
- Create Additional Volume and attach it to one of the EC2.
- Resize the EBS Volume.
- Create Snapshot of Volume of one of the EC2 and copy snapshot to another Region.
- Create AMI of an instance and copy to another region, launch EC2 using custom AMI.
- Verify subnets and Private IPs assigned to EC2 instances in the Default VPCs.

13.
S3 Bucket Policies Use Cases:
Create a Bucket Policy on below scenarios:
1)Everyone including anonymous, is allowed to List the bucket and perform GET Object operations on all objects in the bucket
- Only users belonging the IAM Group BI-Team in the specified account are allowed full access.
- Users inside this Group should only be able to Upload,Delete Objects from specified Organization's Public IP(This can be your IP)
2)User should be able to access the S3 Objects only from a particular Domain:
- Like only users accessing www.flipkart.com, Objects should be accessible when access is tried from this domain only.
3) Only Root user should be able to delete objects or buckets in S3.
Acceptance Criteria:
- Apply the policy and test all the positive and negative cases to be sure that Policy Works in all scenarios.

14.
Access S3 Buckets using VPC Endpoint for S3 Service from Private Instance
1. Create a new VPC, IGW and attach to VPC, Create two subnets in your VPC: one private and one public.
2. Launch one instance, the bastion instance, in the public subnet. Launch another instance, the private instance, in the private subnet. You will use the bastion instance to reach the private instance. The private instance will be used to access Amazon S3.
3. Configure security groups such that the bastion instance to be accessible over SSH 22 from your IP address only. The private instance should be accessible over SSH 22 from the bastion instance only.
4. Create a route table for both the private and public subnet. Associate the route tables
with their respective subnets. Associate IGW route for Public Route Table.
5. Create an Amazon S3 bucket, Upload an object such as a text file into the bucket.
6. Use Secure Shell (SSH) to access the bastion instance. Access S3 bucket from Public Instance and this should work as you are using the Internet to access the Amazon S3 endpoint. SSH to private instance,You should not be able to access the Amazon S3 file from the private instance.
7. Create VPC Endpoint Gateway for S3 and Specify the private subnet in your VPC that will use the endpoint.Check the route table entries for the private subnet. It should now include a route to the endpoint for the Amazon S3 prefix list.
8. Access the Amazon S3 object from your private instance.

An Architecture Diagram using draw.io for above setup is to be created and shared here.

15.
- How to connect to an EC2 instance if the Private Key used to connect to that instance is lost.
- What are the possible options when an error occurs "public key authentication failed"