AWS Security Specialty – Lab Exercises

Lab 1: Preparation (Hands on)

Exercise 1: Download AWS CLI v2. Choose your OS and download

a. https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html

Exercise 2: Create EC2 Instance (Windows)

b. Login into EC2 Instance

Exercise 3: Running AWS Configure on Windows instance and input keys

c. Testing CLI is working correctly

Exercise 4: Download Putty & PuttyGen

Lab 2: Identity and Access Management (Hands On & Demo)

Exercise 1: Create a S3 Bucket

Exercise 2: Create an IAM User Policy

- Note down the Bucket ARN
- User must be given read-only permission to this bucket
- Write a JSON file

Exercise 3: Create a Resource Policy on a Bucket

- Note down Bucket ARN and User ARN (User ARN of your colleague)
- Write a resource policy to allow access to the bucket only for your colleague and no one else
- Check how the policy is evaluated when you use Allow and Deny

Exercise 4: Attaching Role to an instance

- Note down the name of the role created by the instructor
- Attach the role to an EC2 instance and test the role

Exercise 5: Understanding Permission Boundaries

- Test your S3 access and check if you can access S3
- Instructor will change the permission boundary for you as a user
- Check if you can use S3 after permission boundary has been changed

Demo 1: AWS Organizations

- Instructor will demo about the Service Control Policy

Lab 3: Infrastructure Security (Securing EC2 Instance)

Exercise 1: Writing rules for security Groups

- Write a security group which allows for incoming SSH traffic from 10.0.0.0/24
- Write a security group which allows SSH and HTTP traffic from anywhere
- Write a security group which allows RDP and HTTP from anywhere
- Write a security group which allows RDP traffic from 10.0.0.0/24
- Write a security group which allows SSH traffic from 10.0.0.0/16 and 192.168.0.0/16
- Write a security group which allows ICMP from anywhere

Lab 4: Infrastructure Security (Securing the Network/VPC)

Exercise 1: Build a VPC

- Create a VPC with CIDR 10.0.0.0/16
- Create two subnets with CIDRs, 10.0.0.0/24 and 10.0.1.0/24
- Attach an Internet Gateway to the VPC
- Create a public route table with the entry 0.0.0.0/0 being routed to Internet Gateway
- Attach public route table to the subnet 10.0.0.0/24
- Start one EC2 instance in each subnet
- Attach an Elastic IP to instance in subnet 1 (10.0.0.0/24)
- Connect to the instance with elastic IP
- From that first instance connect to instance in the second subnet (10.0.1.0/24)

Exercise 2: Writing NACL rules

- Create a NACL in subnet 2 which allows only RDP or SSH traffic from subnet 1
- Create a NACL in subnet 1 which allows for HTTP traffic and RDP traffic from everywhere

Demo 1: Peering

- Peering between two VPCs will be demonstrated