D Y Patil International University

School of Computer Science, Engineering, and Applications

Academic Year 2022-2023

Practical Assignment No. 2

Class: MCA-SEM III **Subject: Computer Forensics**

Date 31 / 10 /2023

Name: - Udayan Mukund Pawar

PRN No.: - 20220804032

Experiments:

Aim:- AWS Inspector (Host Assessment and Network Assessment)

What is AWS?

AWS (Amazon Web Services) is a comprehensive, evolving cloud computing platform provided by Amazon that includes a mixture of infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS) and packaged-software-as-a-service (SaaS) offerings. AWS services can offer an organization tools such as compute power, database storage and content delivery services.

Amazon.com Web Services launched its first web services in 2002 from the internal infrastructure that Amazon.com built to handle its online retail operations. In 2006, it began offering its defining IaaS services. AWS was one of the first companies to introduce a pay-as-you-go cloud computing model that scales to provide users with compute, storage or throughput as needed.

AWS offers many different tools and solutions for enterprises and software developers that can be used in data centers in up to 190 countries. Groups such as government agencies, education institutions, non-profits and private organizations can use AWS services.

AWS Inspector

Amazon Inspector is a service that automates security assessments and network accessibility testing for AWS EC2 instances. It aids in the detection of vulnerabilities in your EC2 instances and apps. Furthermore, it enables you to make security testing a more frequent event as part of the development and IT operations.

Amazon Inspector displays a clear list of security and compliance issues that have been prioritized by severity level. Furthermore, these discoveries may be analyzed directly or as part of full

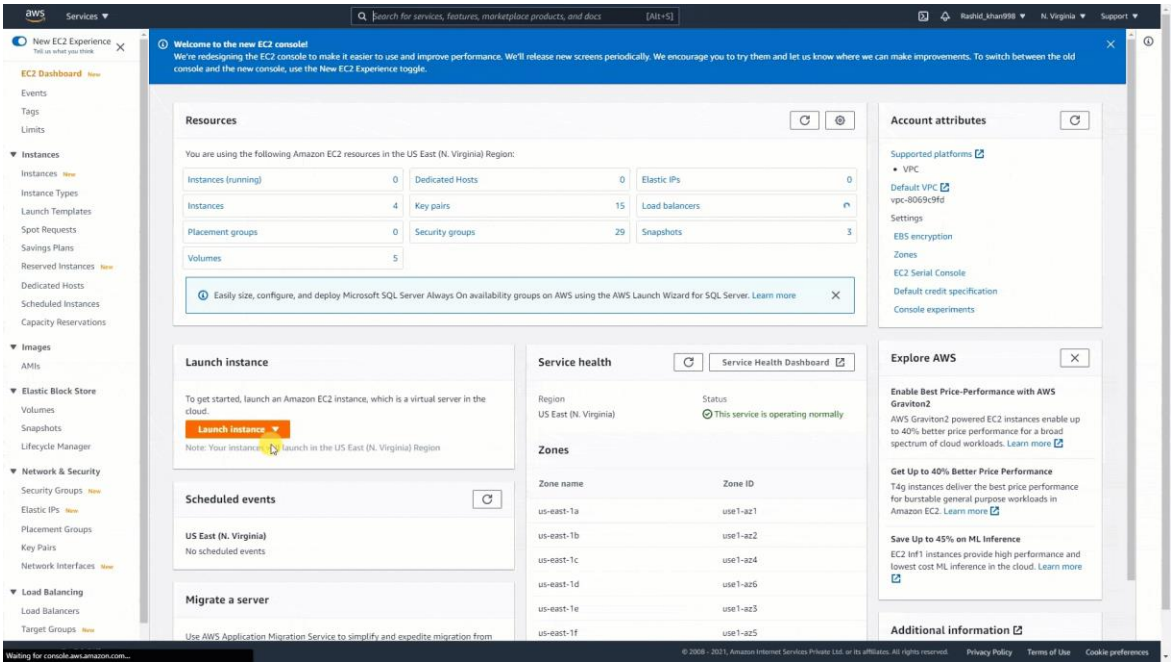
evaluation records accessible through the API or the AWS Inspector UI. AWS Inspector security evaluations assist you in detecting unauthorized network access to EC2 instances as well as vulnerabilities on those EC2 instances.

It operates by first defining a target set of resources using tags, then configuring an assessment template that defines what we're looking for (common vulnerabilities and exploits (CVEs), PCI requirements, and so on) and running an assessment against our target resources, examining the research results and reducing the issues discovered.

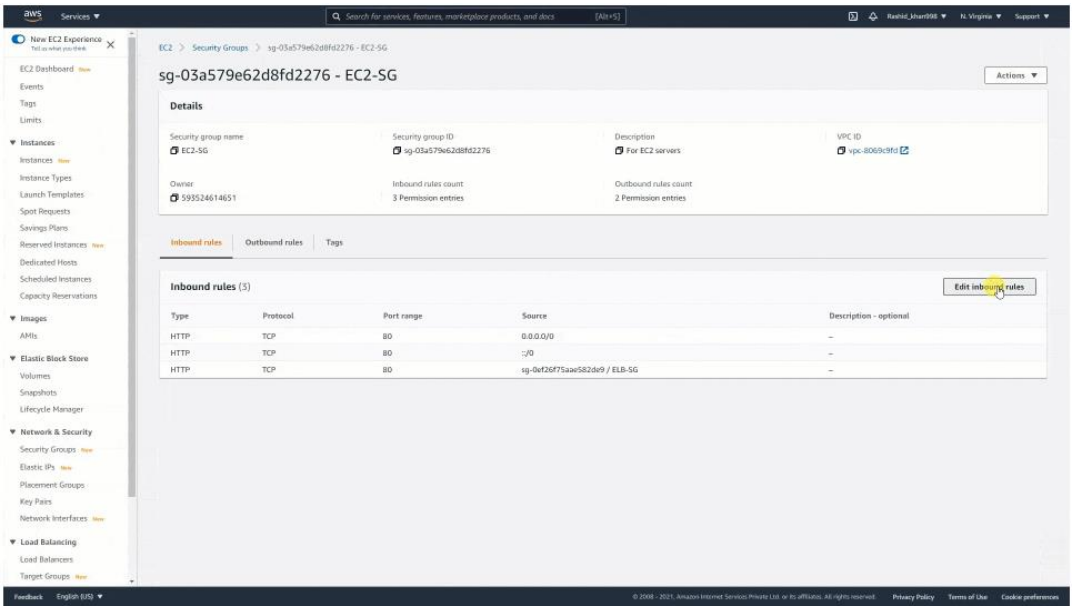
Procedure:-

Step 1: Create an EC2 instance: To begin, if you do not already have an AWS account, sign up for an AWS Free Tier Account. Second, we'll start a Linux EC2 instance.

1. Select Launch Instance.
2. Choose Amazon Linux AMI(HVM), SSD Volume Type from the drop-down menu.
3. Select Subnet and enable Auto-assignment of public IP addresses.
4. Create a Tag for your Amazon EC2 instance.
5. Configure the Security Group and choose EC2-SG (existing security group)

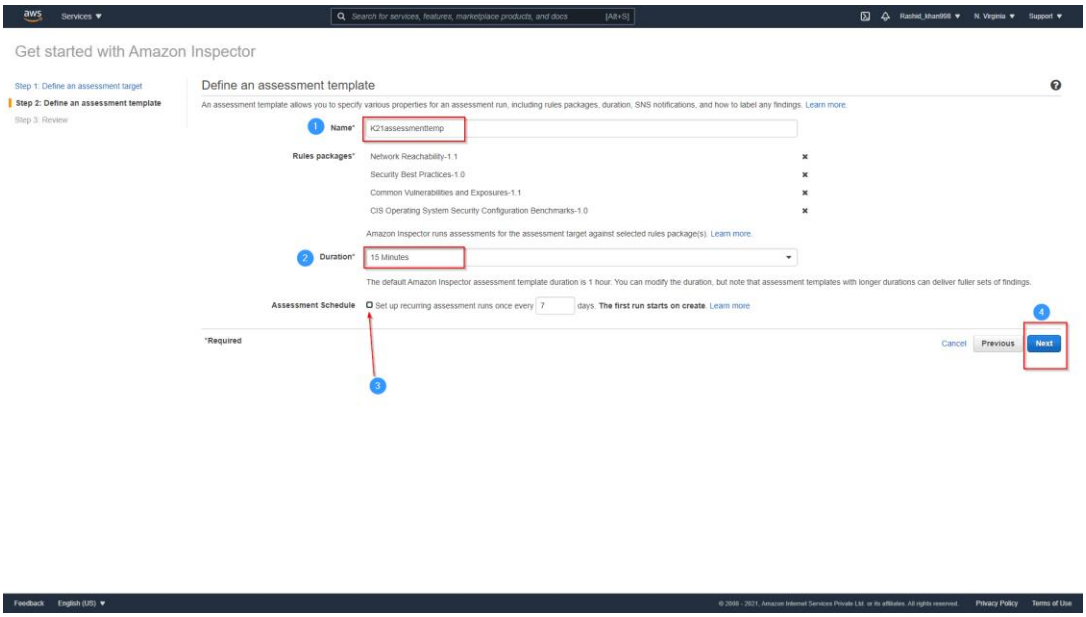


Step 2: Edit Security Group and Open Port 21: Once the EC2 instance has been launched, we must modify the security group and open port 21.

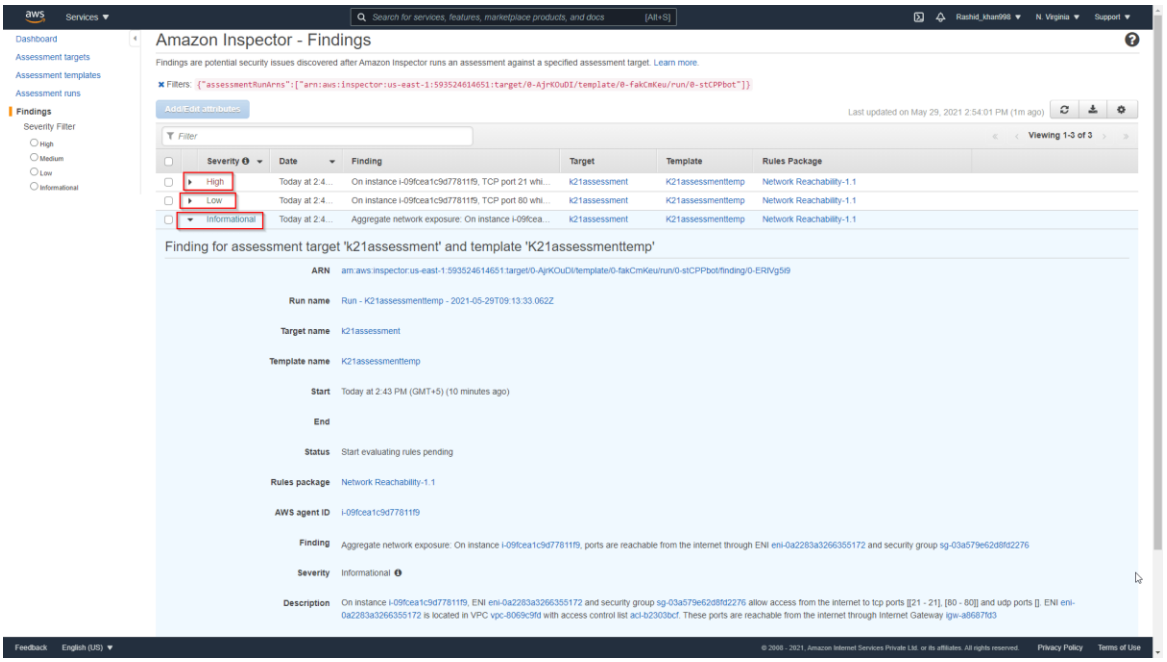


Step 3: Create an Assessment Template: Following the assessment aim, create an assessment template.

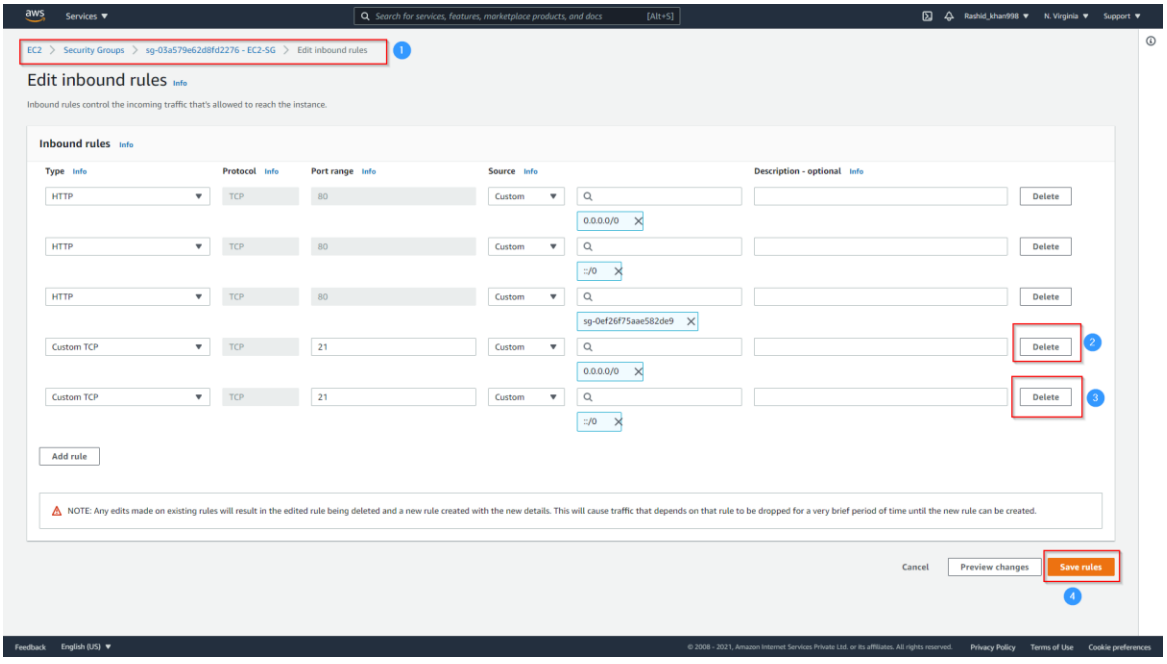
1. Please provide a name for it: K21assessmenttemp
2. Set Duration: 15 minutes (as its demo)
3. Uncheck the Assessment Schedule and then press Next.



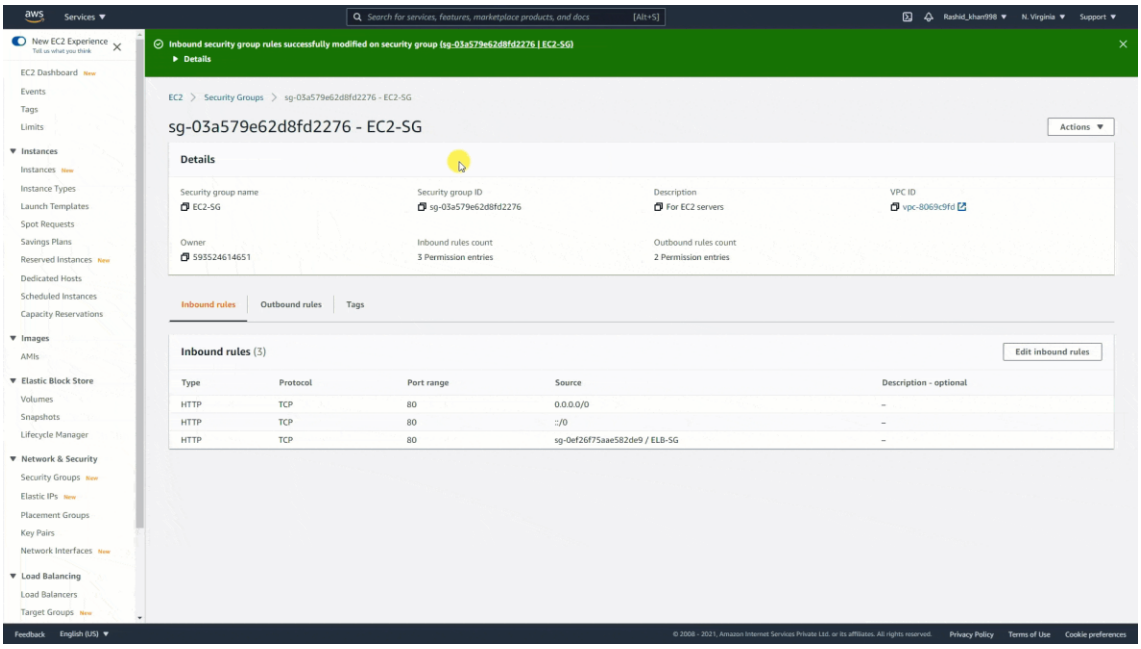
Step 4: Assessment Run will begin automatically. Now, go back to the findings and go over the risk.



Step 5: Delete Open Ports: Return to EC2 and delete open ports.



Step 6: Once the open ports have been successfully deleted, we will conduct the Assessment and analyze the findings; this time, there is no High-risk showing.



Result :-

AWS Inspector Launch Successfully.