

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

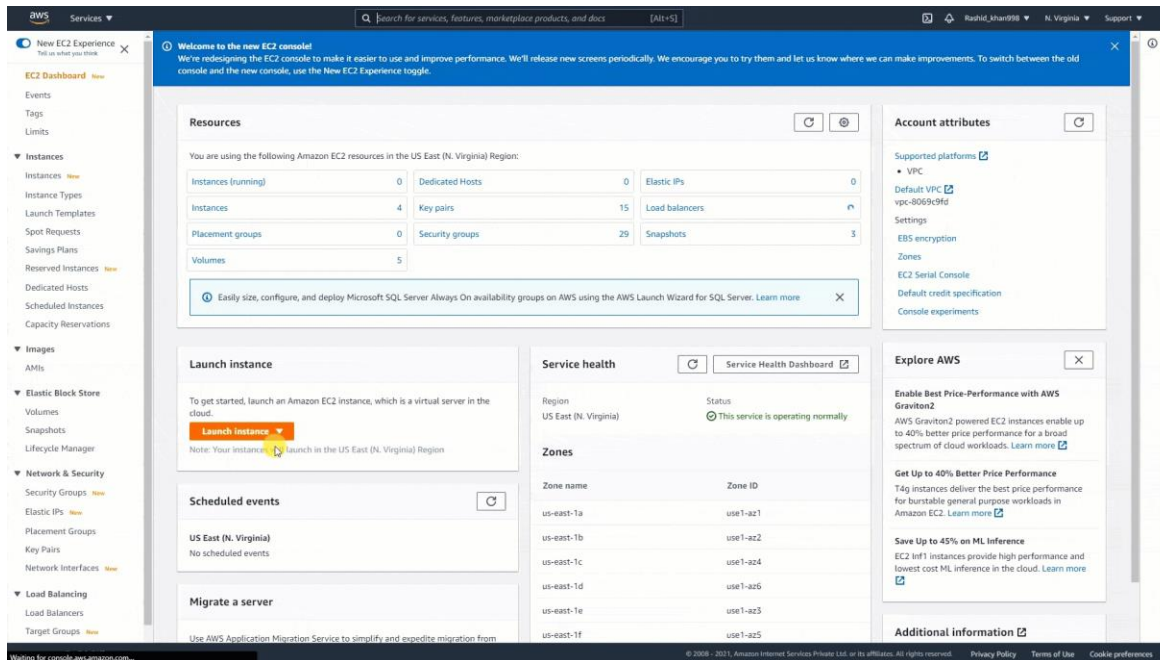
evaluation records accessible through the API or the AWS Inspector UI. AWS Inspector security evaluations assist you in detecting unauthorized network access to EC2 instances as well as vulnerabilities on those EC2 instances.

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.

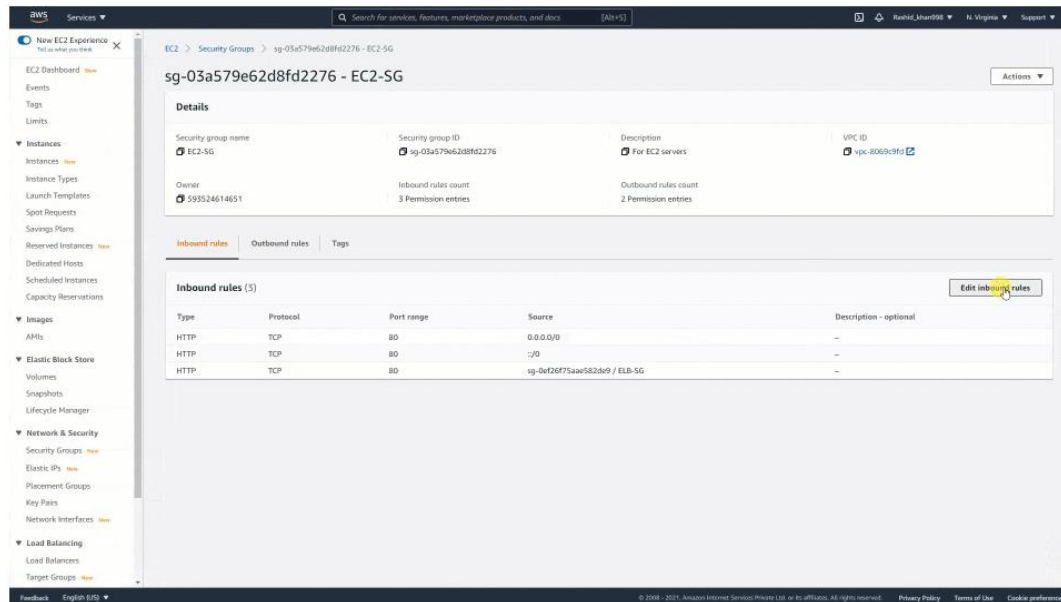
Procedure:-

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)

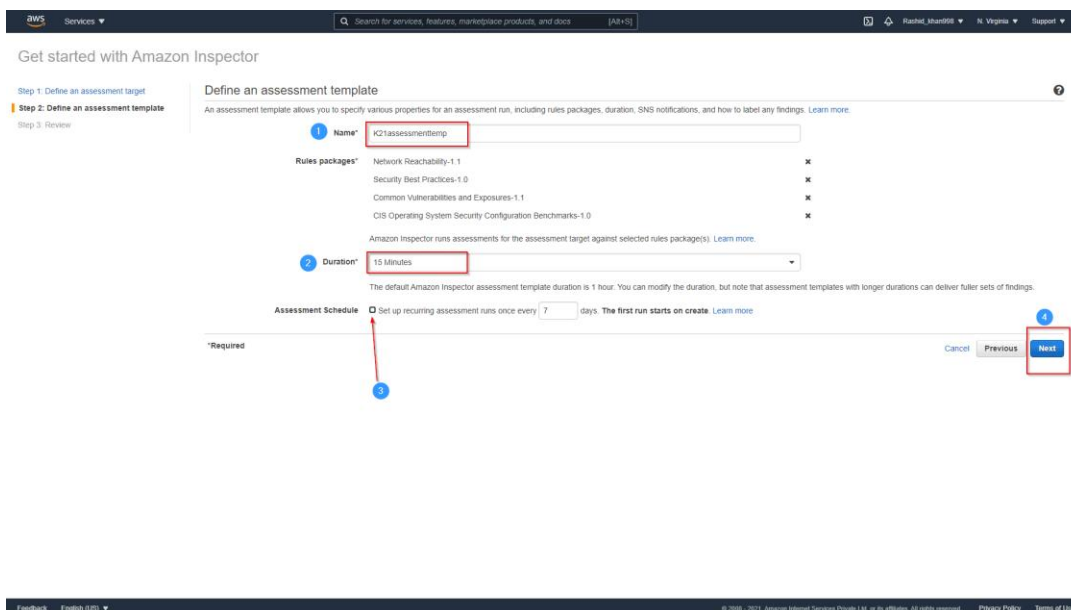


Step 2: Edit Security Group and Open Port 21: Once the EC2 instance has been launched, we must modify the security group and open port 21.



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.

The screenshot shows the Amazon Inspector Findings console. On the left, there's a sidebar with 'Findings' selected. The main area displays a table of findings. The first finding is highlighted with a red box, showing a severity of 'High'. Below the table, there's a detailed view of a finding for assessment target 'k21assessment' and template 'K21assessmenttemp'. The finding is titled 'Aggregate network exposure: On instance i-09fcea1c9d77811f9, ports are reachable from the internet through ENI eni-0a2283a3266355172 and security group sg-03a579e62d8f02276'. The severity is 'Informational'.

Severity	Date	Finding	Target	Template	Rules Package
High	Today at 2:4...	On instance i-09fcea1c9d77811f9, TCP port 21 whi...	k21assessment	K21assessmenttemp	Network Reachability-1.1
Low	Today at 2:4...	On instance i-09fcea1c9d77811f9, TCP port 80 whi...	k21assessment	K21assessmenttemp	Network Reachability-1.1
Informational	Today at 2:4...	Aggregate network exposure: On instance i-09fcea...	k21assessment	K21assessmenttemp	Network Reachability-1.1

Findings for assessment target 'k21assessment' and template 'K21assessmenttemp'

ARN: am:aws:inspector:us-east-1:593524614651:target/0-ApK0u0I/template/0-fakCmKeun/0-sCPpbot/finding/0-ERVg569

Run name: Run - K21assessmenttemp - 2021-05-29T09:13:33.062Z

Target name: k21assessment

Template name: K21assessmenttemp

Start: Today at 2:43 PM (GMT+5) (10 minutes ago)

End:

Status: Start evaluating rules pending

Rules package: Network Reachability-1.1

AWS agent ID: i-09fcea1c9d77811f9

Finding: Aggregate network exposure: On instance i-09fcea1c9d77811f9, ports are reachable from the internet through ENI eni-0a2283a3266355172 and security group sg-03a579e62d8f02276

Severity: Informational

Description: On instance i-09fcea1c9d77811f9, ENI eni-0a2283a3266355172 and security group sg-03a579e62d8f02276 allow access from the internet to tcp ports [21 - 21], [80 - 80] and udp ports []. ENI eni-0a2283a3266355172 is located in VPC vpc-8069c9d with access control list acl-b2303b0f. These ports are reachable from the internet through Internet Gateway igw-a966793

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

The screenshot shows the AWS Management Console 'Edit inbound rules' page for a security group. The page lists several inbound rules. The first three rules are for HTTP on port 80, and the last two are for Custom TCP on port 21. The 'Delete' button for the Custom TCP rule on port 21 is highlighted with a red box. The 'Save rules' button at the bottom right is also highlighted with a red box.

Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	Custom	0.0.0.0/0
HTTP	TCP	80	Custom	0.0.0.0/0
HTTP	TCP	80	Custom	0.0.0.0/0
Custom TCP	TCP	21	Custom	sg-0ef26f75aee582de9
Custom TCP	TCP	21	Custom	0.0.0.0/0

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

Cancel Preview changes Save rules

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.

The screenshot displays the AWS Management Console interface. A green notification banner at the top states: "Inbound security group rules successfully modified on security group (sg-03a579e62d8fd2276) [EC2-SG]". The main content area shows the details for the security group "sg-03a579e62d8fd2276 - EC2-SG".

Details:

- Security group name: EC2-SG
- Security group ID: sg-03a579e62d8fd2276
- Description: For EC2 servers
- VPC ID: vpc-806b2cfd
- Owner: 595524614651
- Inbound rules count: 3 Permission entries
- Outbound rules count: 2 Permission entries

Inbound rules (3):

Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	0.0.0.0/0	--
HTTP	TCP	80	:::0	--
HTTP	TCP	80	sg-0ef26f75aae582de9 / ELB-SG	--

Result :-

AWS Inspector Launch Successfully.