Home / AWS / Guided Lab / Find vulnerabilities on EC2 instance using Amazon Inspector

Find vulnerabilities on EC2 instance using Amazon Inspector

Level: **Intermediate**

Amazon Inspector Amazon Web Services

0h 3m 38s left

15 MIN

End Lab

Open Console

Validation

Lab Credentials

User Name

Whiz_User_80425.87361784

Password

b1728cb3-a108-4f6f-a813-b379e32b30ee

Access Key

AKIASVIAO3JRBYUQ4ZHK

Secret Key

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

Lab Resources

No Lab Resources Found

Support Documents

No Support Documents Found

Need help?

How to use Hands on Lab

Troubleshooting Lab

FAQs

Submit Feedback | Share

Lab Overview | Lab Steps | Lab Validation | Lab FAQs

Cloud Security Engineer

Security

Lab Steps

Task 1: Sign in to AWS Management Console

1. Click on the **Open Console** button, and you will get redirected to AWS Console in a new browser tab.
2. On the AWS sign-in page,
    - Leave the Account ID as default. Never edit/remove the 12 digit Account ID present in the AWS Console. otherwise, you cannot proceed with the lab.
    - Now copy your **User Name** and **Password** in the Lab Console to the **IAM Username and Password** in AWS Console and click on the **Sign in** button.
3. Once Signed In to the AWS Management Console, Make the default AWS Region as **US East (N. Virginia) us-east-1.**

Task 2 : Launching an EC2 Instance

1. Make sure you are in the US East **(N. Virginia) us-east-1** Region.
2. Navigate to EC2 by clicking on the **Services** menu in the top, then click on **EC2** in the **Compute** section.
3. Navigate to **Instances** on the left panel and click on **Launch Instances**

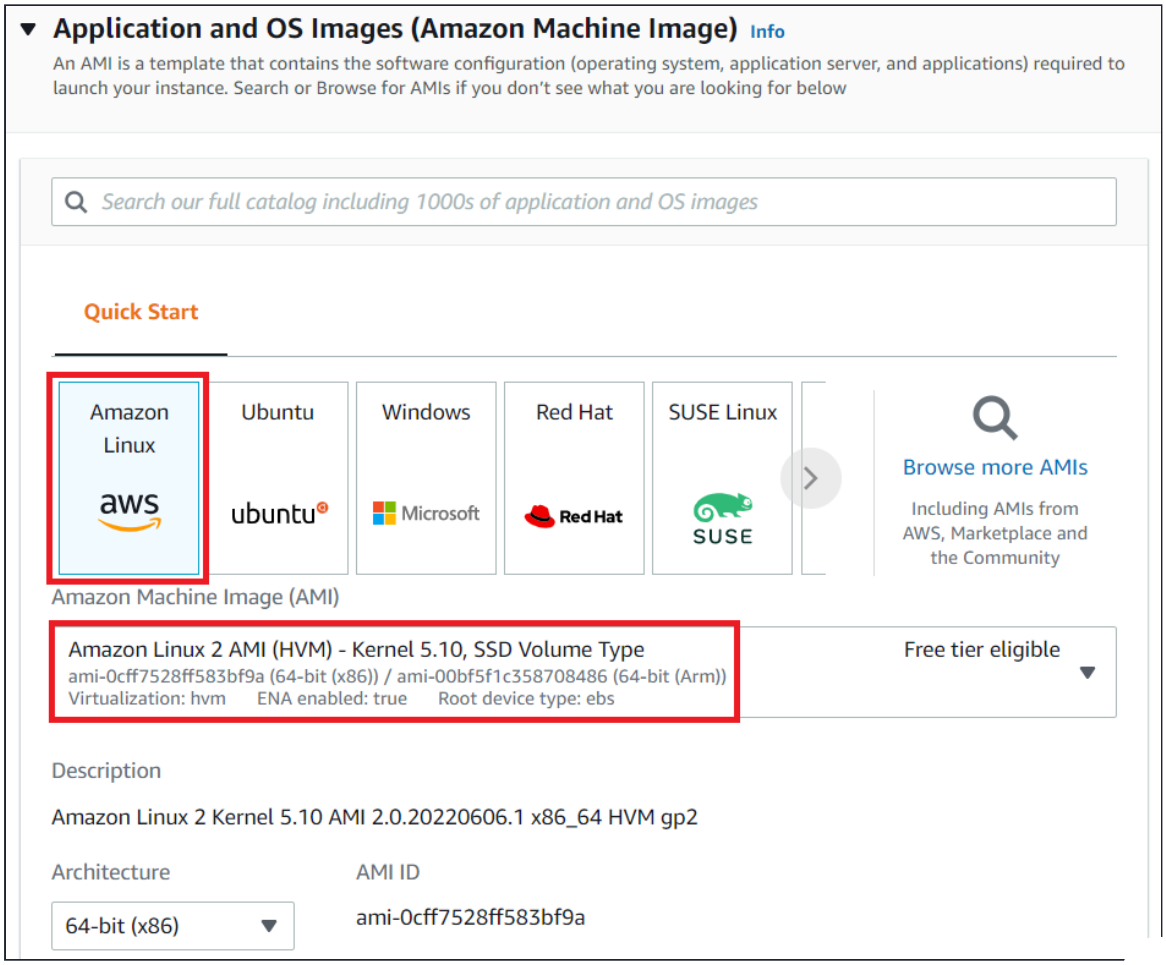
4. Under the **Name and tags** section :

- Name : ***Inspector-EC2***

5. Under the **Application and OS Images (Amazon Machine Image)** section :

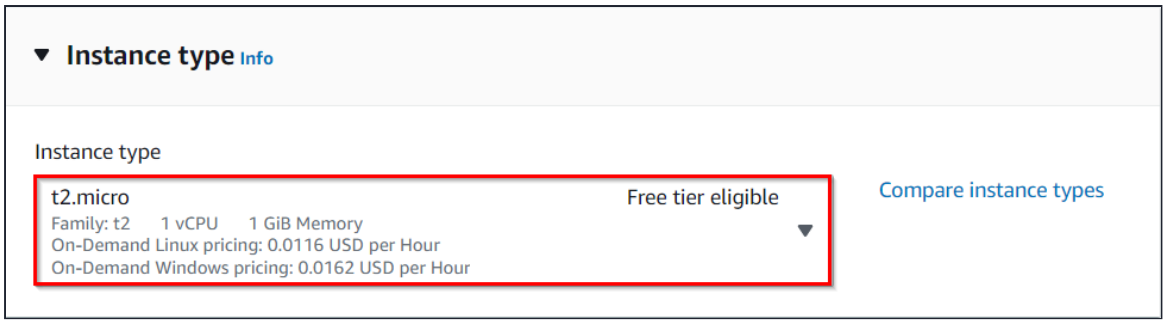
- Select **Quick Start** tab and **Amazon Linux** under it
- Amazon Machine Image (AMI) : select *Amazon Linux 2 AMI*

Note: if there are two AMI's present for Amazon Linux 2 AMI, choose any of them.



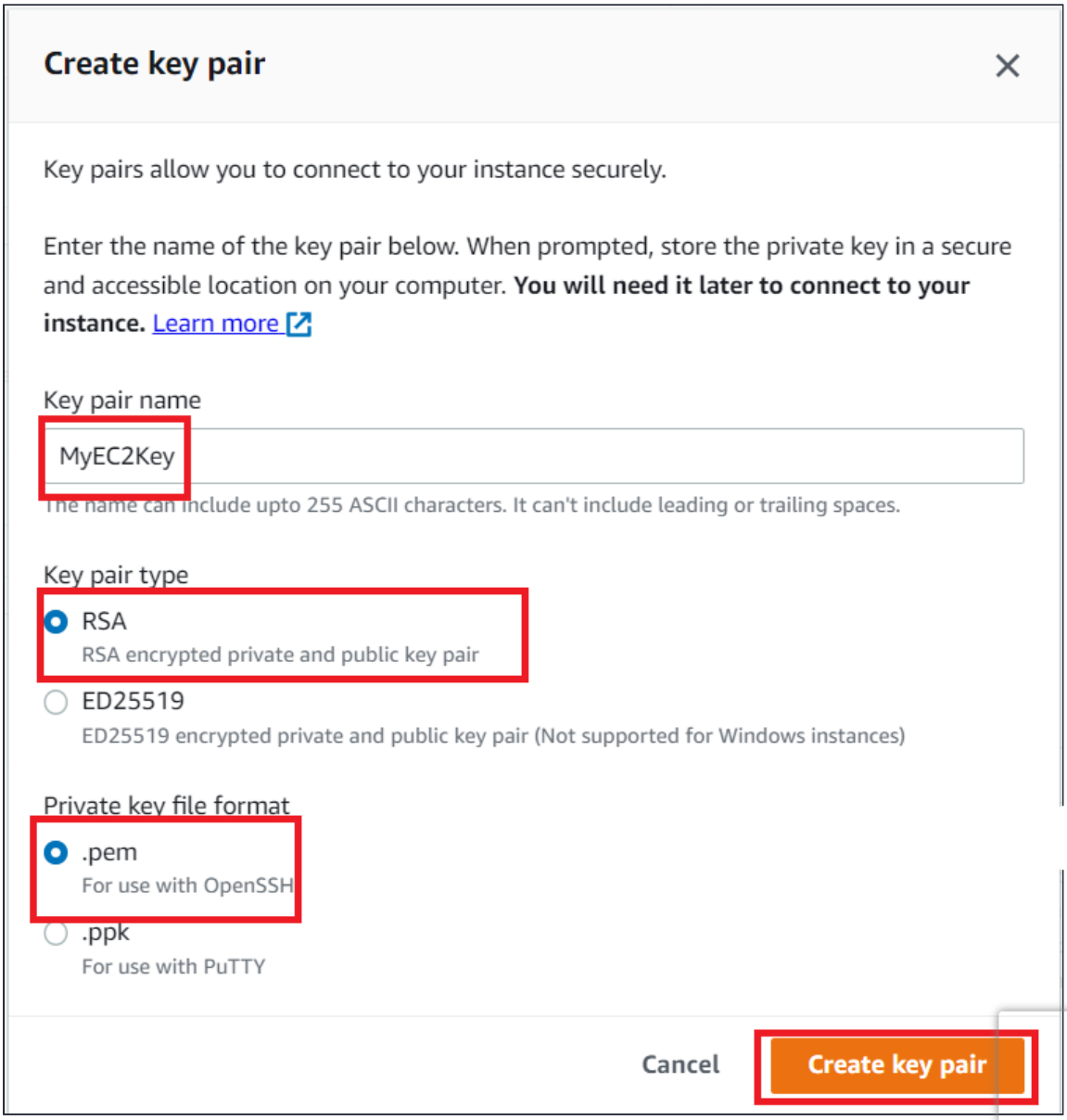
6. Under the **Instance Type** section **:**

- Instance Type : Select **t2.micro**



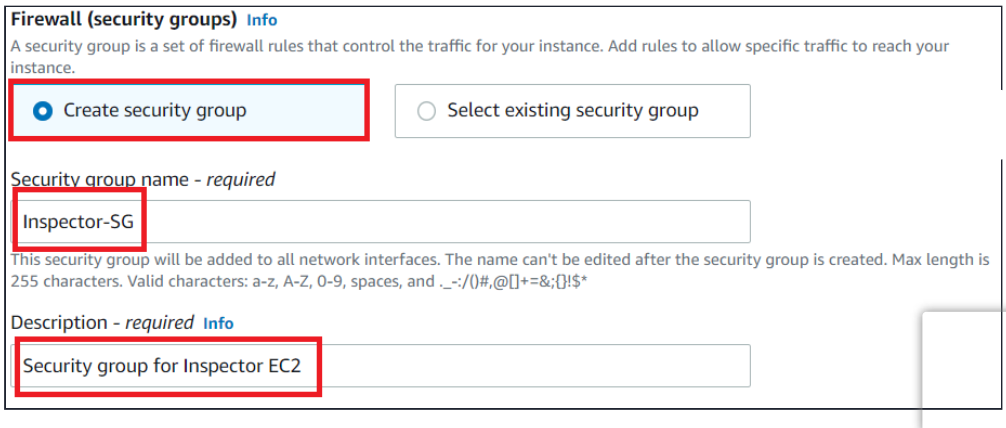
7. Under the **Key Pair (login)** section **:**

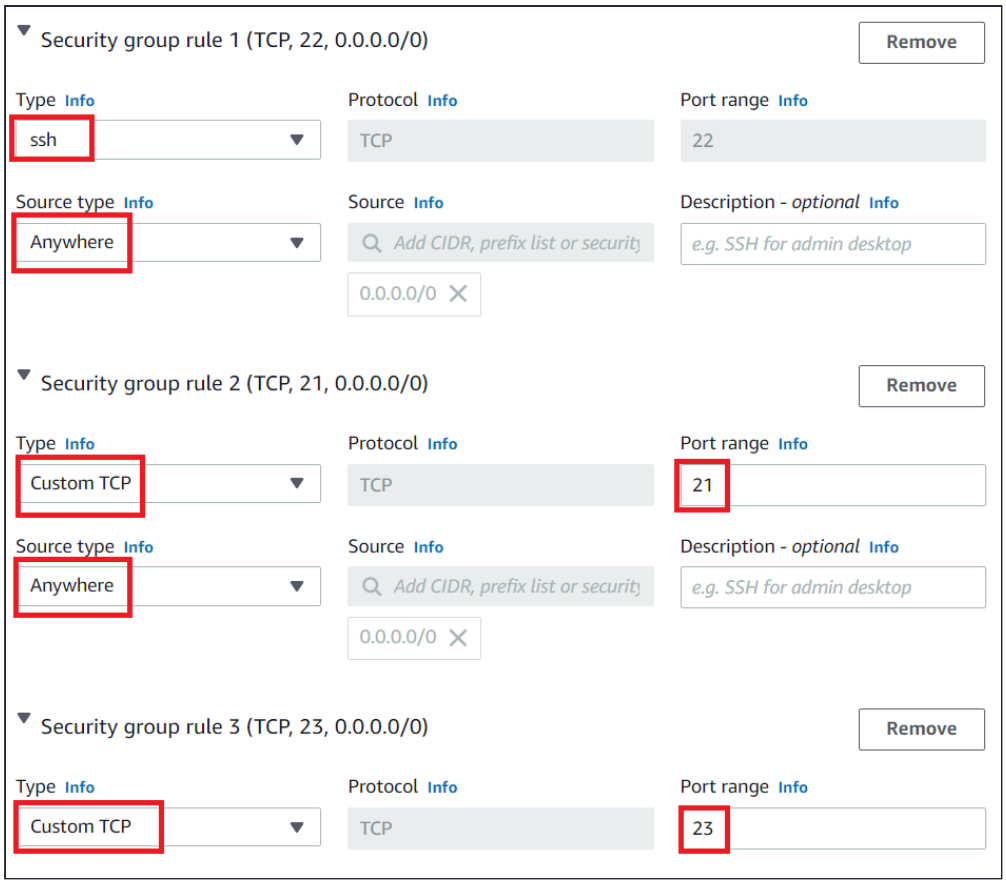
- Click on Create new key pair hyperlink
- Key pair name: ***MyEC2Key***
- Key pair type: **RSA**
- Private key file format: **.pem** or **.ppk**
- Click on Create key pair and select the created key pair



8. Under the **Network Settings** section **:**

- Click on **Edit** button
- Auto-assign public IP: select ***Enable***
- Firewall (security groups) : Select **Create a new security group**
  - Security group name : Enter ***Inspector-SG***
  - Description : Enter ***Security group for Inspector EC2***
  - To add **SSH:**
    - Choose Type: **SSH**
    - Source: **Anywhere** (From ALL IP addresses accessible).
  - For **Custom TCP Rule**, click on **Add security group rule**,
    - Choose Type: **Custom TCP**
    - Port range : *21*
    - Source: **Anywhere** (From ALL IP addresses accessible).
  - For **Custom TCP Rule**, click on **Add security group rule**,
    - Choose Type: **Custom TCP**
    - Port range : *23*
    - Source: **Anywhere** (From ALL IP addresses accessible).
  - For **Custom TCP Rule**, click on **Add security group rule**,
    - Choose Type: **Custom TCP**
    - Port range : *20*
    - Source: **Anywhere** (From ALL IP addresses accessible).





9. Keep everything else as default and click on the **Launch instance** button.
10. **Launch Status:** Your instance is now launching, Navigate to **Instances** page from the left menu and wait until the status of the EC2 Instance changes to **running**.
11. Note down the sample IPv4 Public IP Address of the EC2 instance. A sample is shown in the screenshot below.

Task 3 : SSH into EC2 Instance

- Please follow the steps in SSH into EC2 Instance using **putty tool, or** you can use **Ec2 instance connect.**

Task 4: Install an AWS Agent

1. Switch to root user:

```
sudo su
```

2. Download the agent installation script by running one of the following commands:

```
wget https://inspector-agent.amazonaws.com/linux/latest/install
```

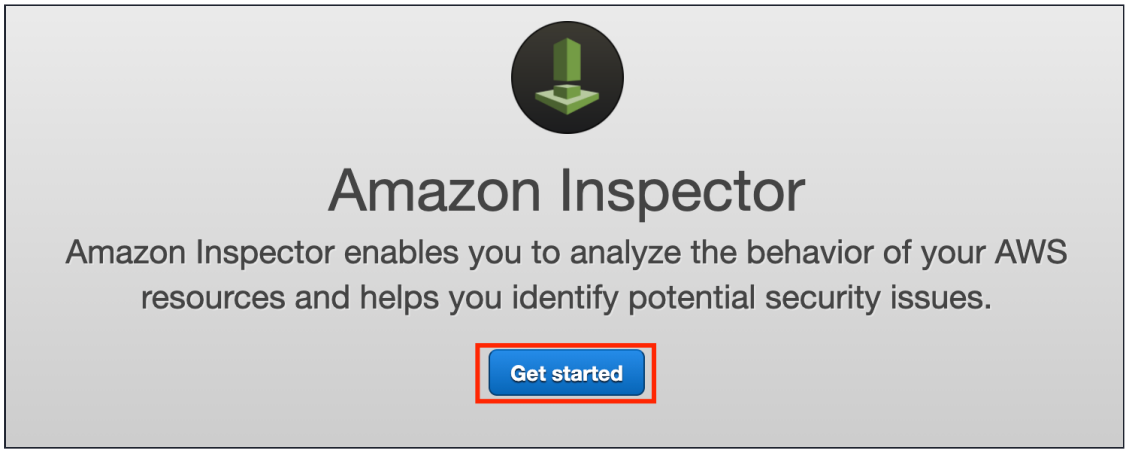
```
curl -O https://inspector-agent.amazonaws.com/linux/latest/install
```

3. To install the agent, run the following command:

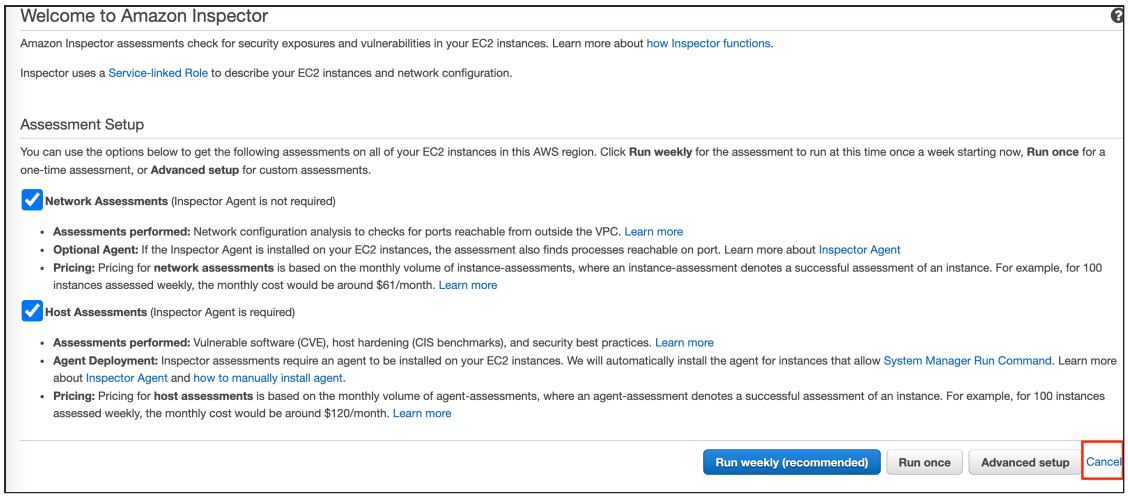
```
sudo bash install
```

Task 5: Create an assessment target

1. Navigate to **Inspector** by clicking on the Services menu in the top, then click on **Inspector** in the **Security, Identity & Compliance** section.
2. Expand the left side column and switch to **Amazon Inspector Classic**.
3. On the home page, click on the **Get started** button.



4. Click on the **Cancel** button present on the right bottom corner, to see the options. Run weekly, Run once and Advanced setup is for quick setup.



5. On the left side bar, click on the **Assessment targets.**

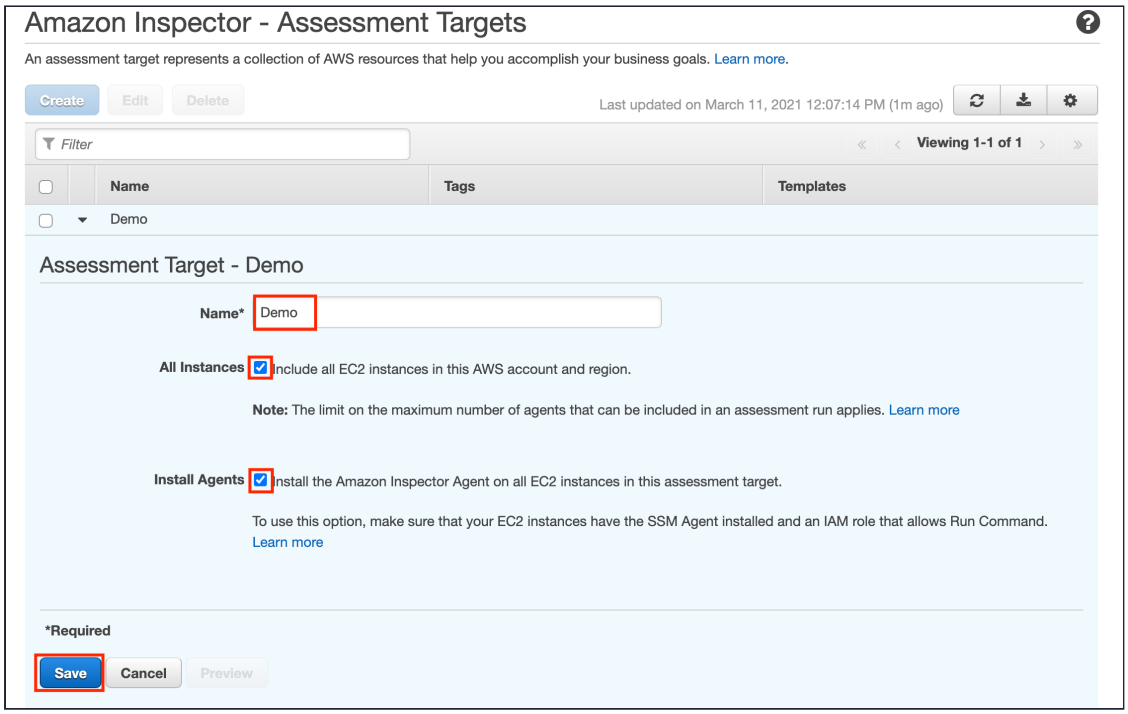
6. Click on the **Create**.

7. Fill in the details, Name: ***Demo***

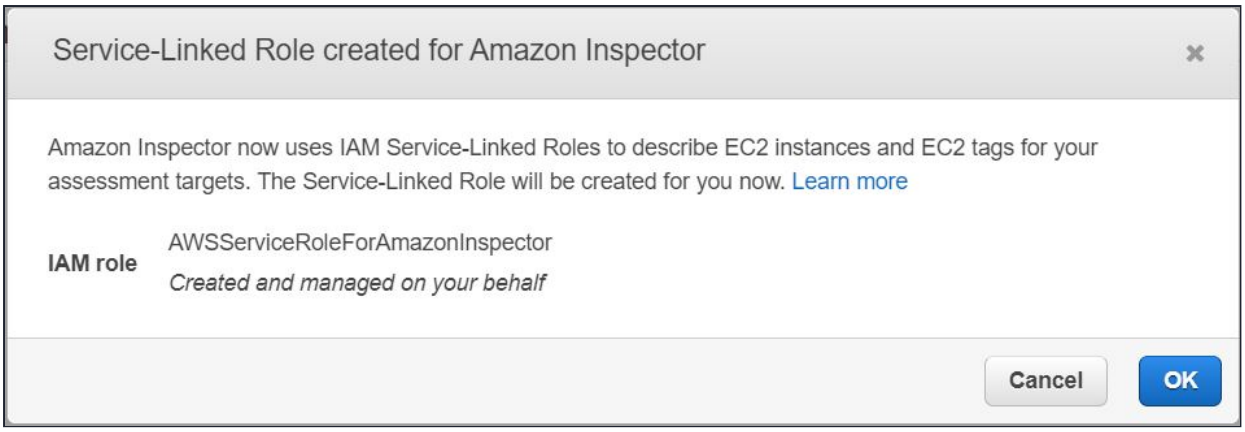
8. All instances: Select **Include all EC2 instances in this AWS account and region.**

9. Install Agents: **Selected by Default**

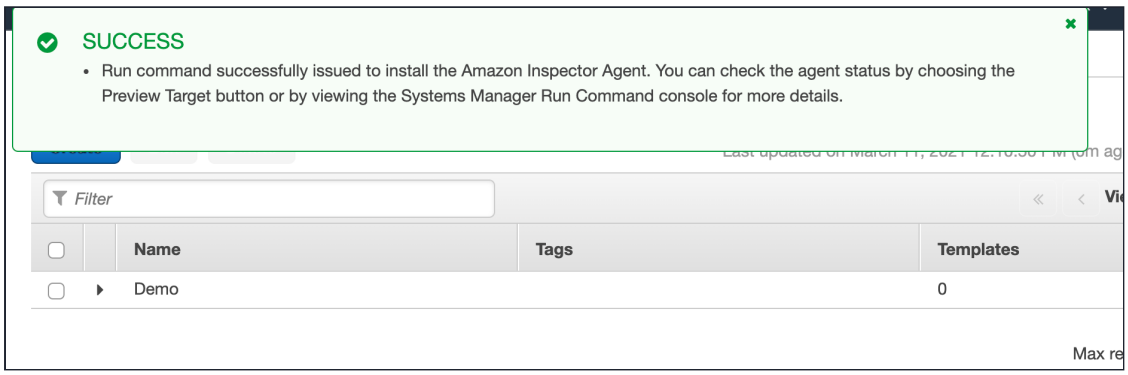
10. Click on the **Save** button, to create an Assessment Target.



11. Click the **OK** button on the pop-up menu.

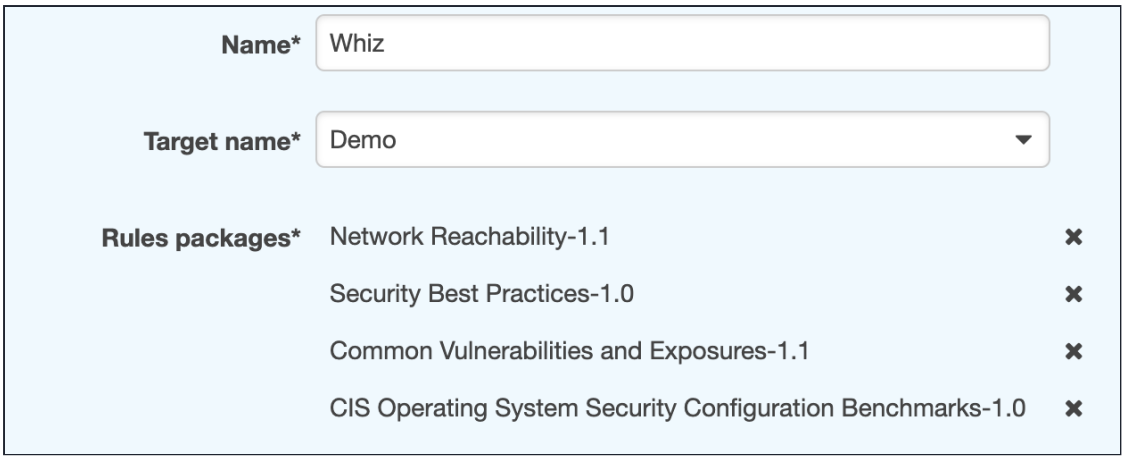


11. The assessment target is now created.

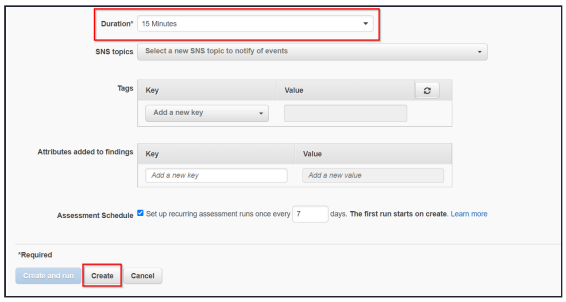


Task 6: Create an assessment template

1. On the left side bar, click on the **Assessment templates.**
2. Click on the **Create**.
3. Fill in the below details, as follows:
    - Name: Enter ***Whiz***
    - Target Name: Select **Demo**
    - Rules packages: **Select all four rules, one-by-one**

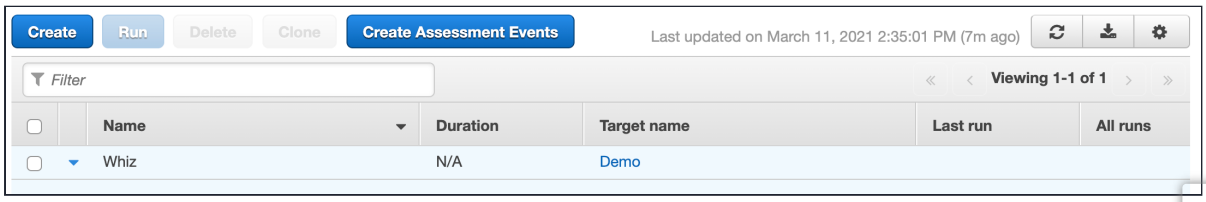


- Duration: **15 Minutes**
- Keep all other options as default.
- Click on the **Create** button.



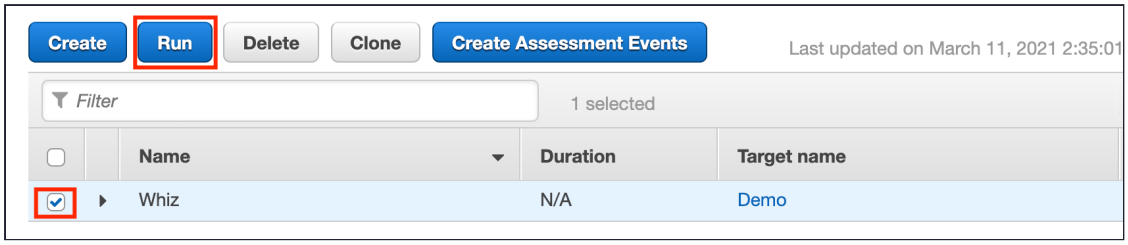
4. Assessment template **Whiz** is now getting created.

5. It's created, in the next step you will run the template to find the vulnerabilities on the created EC2 instance.

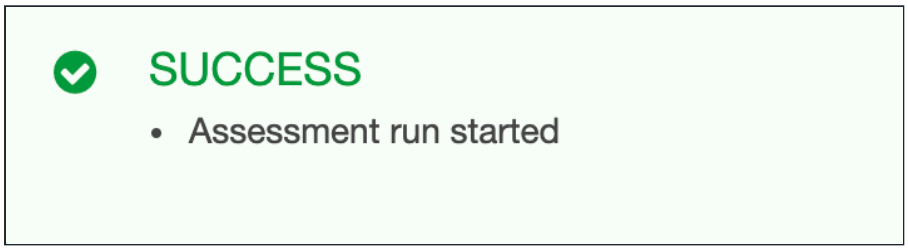


Task 7: Run the assessment template

1. Select Assessment templates **Whiz,** and click on the **Run** button.(If any error pops up stating error, ignore it.)



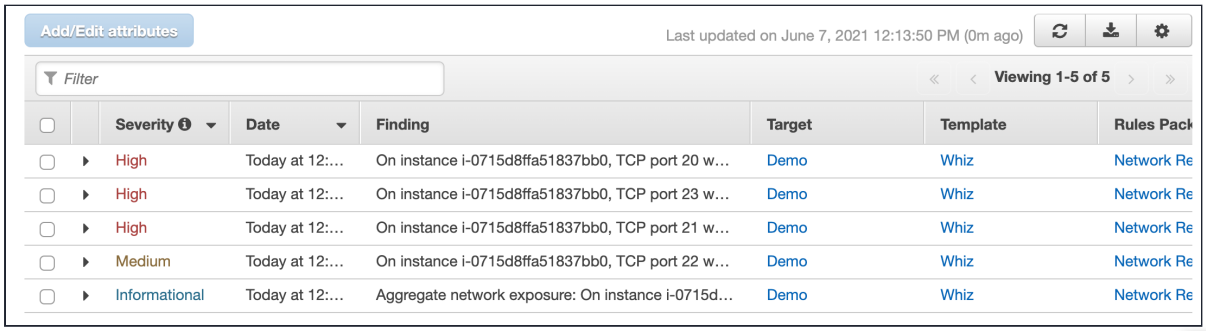
2. The assessment run has started.



3. To see the Assessment Run and its result, click on the **Assessment runs** present on the left sidebar.

4. Click on the number of findings to know about the vulnerabilities found by Inspector on the EC2 instance.

5. There are currently **5** findings.

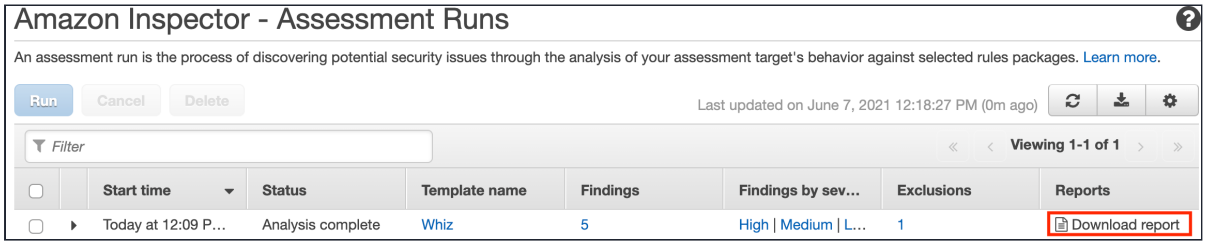


6. Click on the expand button for the first finding, to see the details.

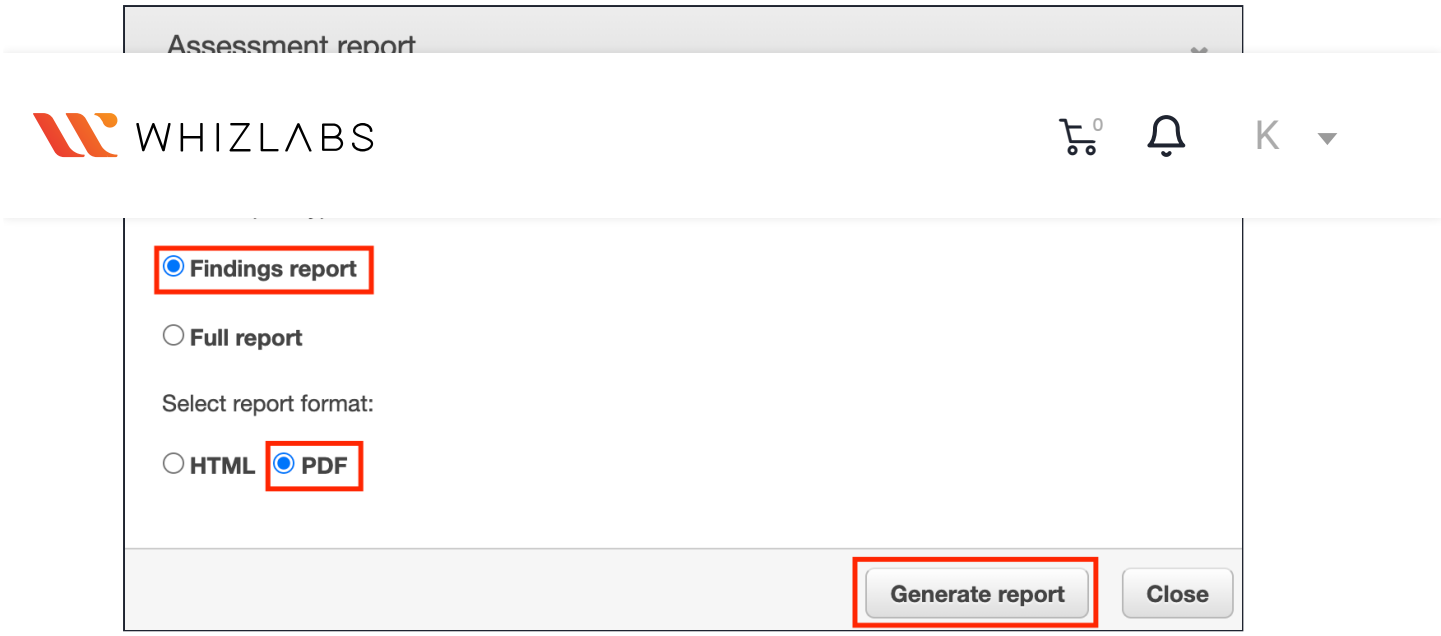
7. The **description** field has details about the finding, while the **Recommendation** field has the message to solve the issue and avoid this finding.

Task 8: Download the assessment run report

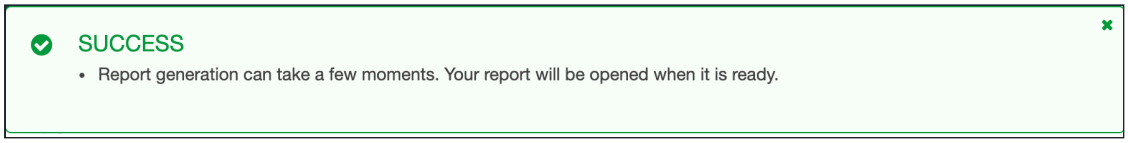
1. Click on the Assessment runs, present on the left sidebar**.**
2. Wait for Collection status in Assessement to become Analysis Completed. It may take 10 minutes to complete Otherwise you can't download report
3. Choose the **Download report** button.



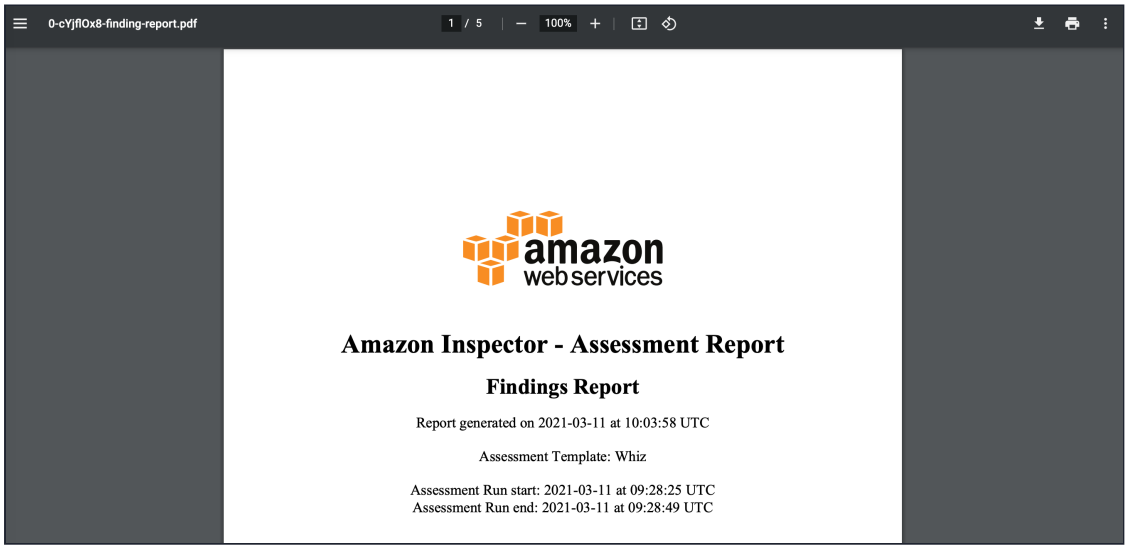
4. After you click on the **Download report** option, you will be prompted with a screen to select the report type and format.
5. Keep the option default, Report type as **Findings report,** and report format as **PDF**. Click on the **Generate Report** button.



6. It would take a couple of seconds to generate the report.



7. Once ready, it will open in the new tab of your browser.



8. **Note: Vulnerabilities of Informational severity will not be shown in the report. To see that regenerate the report with the Full report option.**

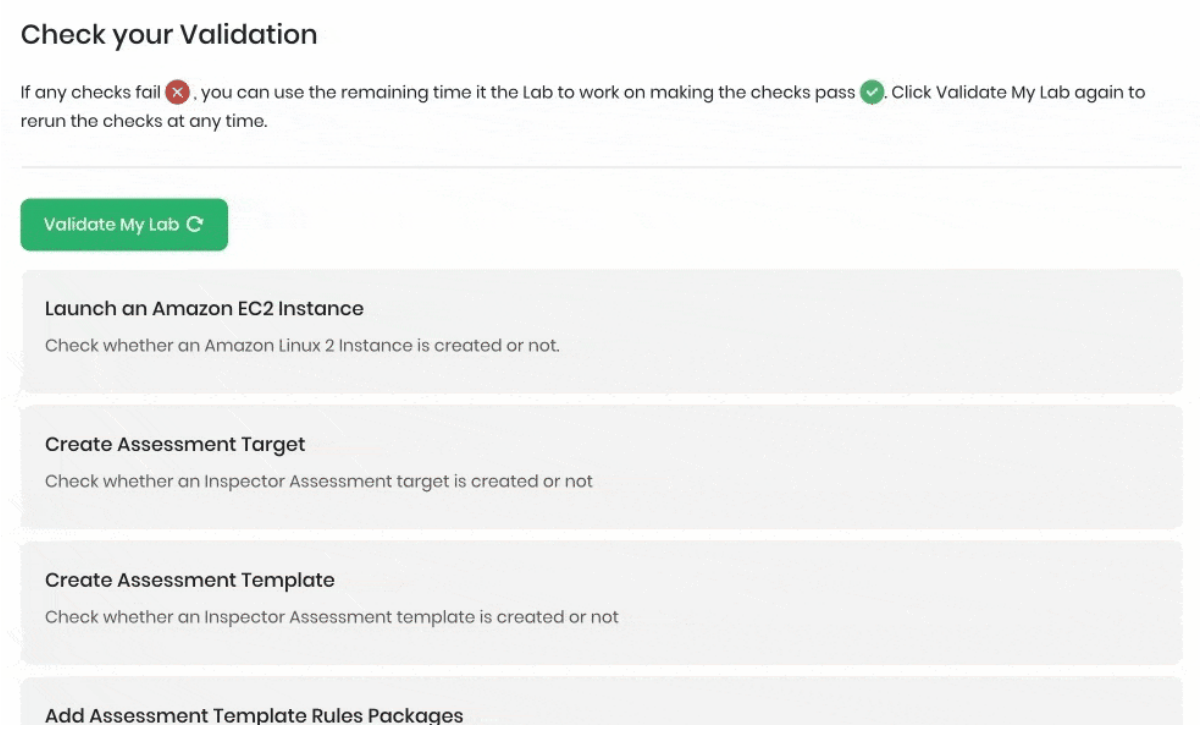
9. If there are more than 3 vulnerabilities found, it is recommended to generate the report and check the issue.

Do You Know ?

Amazon Inspector supports not only system-level vulnerability assessments but also offers specific rules packages for assessing compliance with industry standards and best practices.

Task 9: Validation Test

1. Once the lab steps are completed, please click on the **Validate** button on the left side panel.
2. This will validate the resources in the AWS account and displays whether you have completed this lab successfully or not.
3. Sample output :



Completion and Conclusion

1. You have successfully created and launched Amazon EC2 Instance.
2. You have successfully created an Inspector assessment target and template.
3. You have successfully found the vulnerabilities on the configured EC2 instance.

End Lab

1. Sign out of AWS Account.
2. You have successfully completed the lab.

3. Once you have completed the steps, click on **End Lab** from your whizlabs lab console and wait till the process gets completed.