iGNITE Technologies

AWS

PENETRATION TESTING LAB SETUP

www.hackingarticles.in

Contents

Introduction

This guide will walk you through setting up a web server with a simulated SSRF vulnerability and a Kali Linux instance on Amazon Web Services (AWS).

Prerequisites

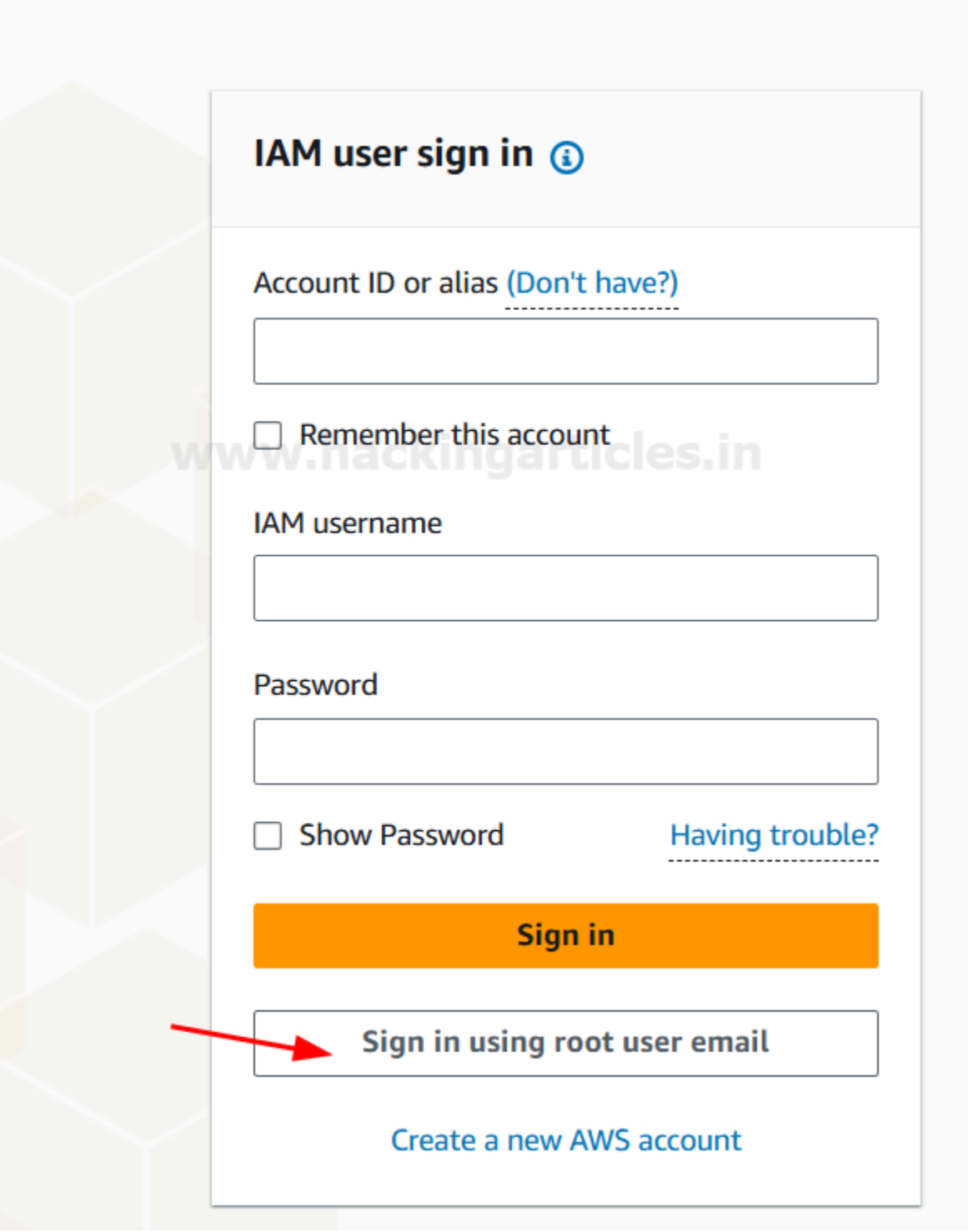
- An AWS account.
- Basic understanding of AWS EC2 and IAM.
- An SSH client (e.g., OpenSSH, PuTTY).

Part 1: Setting up the Vulnerable Web Server (Ubuntu EC2 Instance)

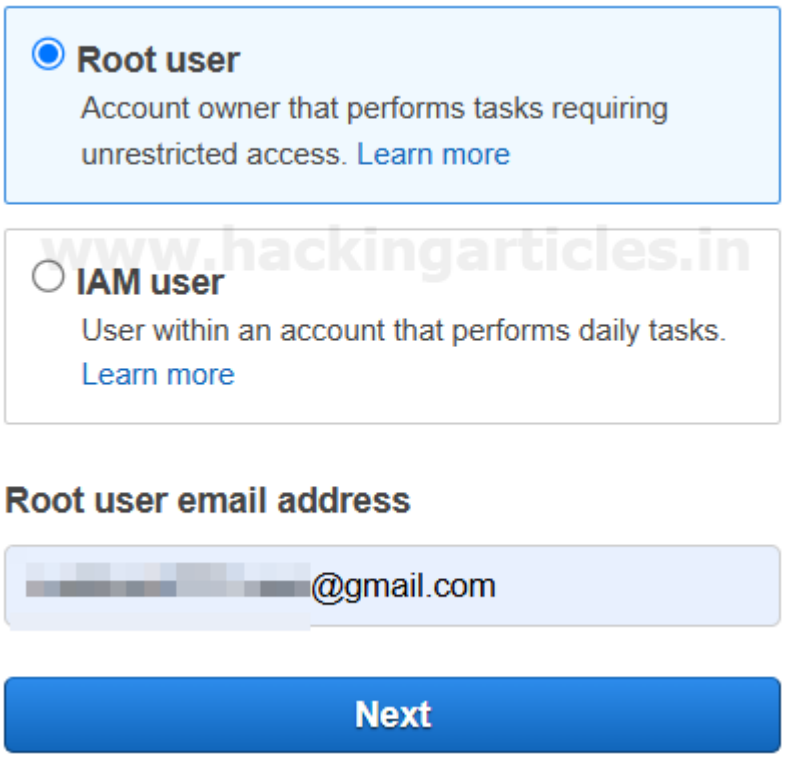
This section details the steps to launch an Ubuntu EC2 instance, configure its security, and deploy a basic web application.

Step 1: Sign in to AWS

- Firstly, go to the AWS Management Console login page.
- Then, select **"Sign in using root user email"**.



- Enter your root user email address and click **"Next"**.

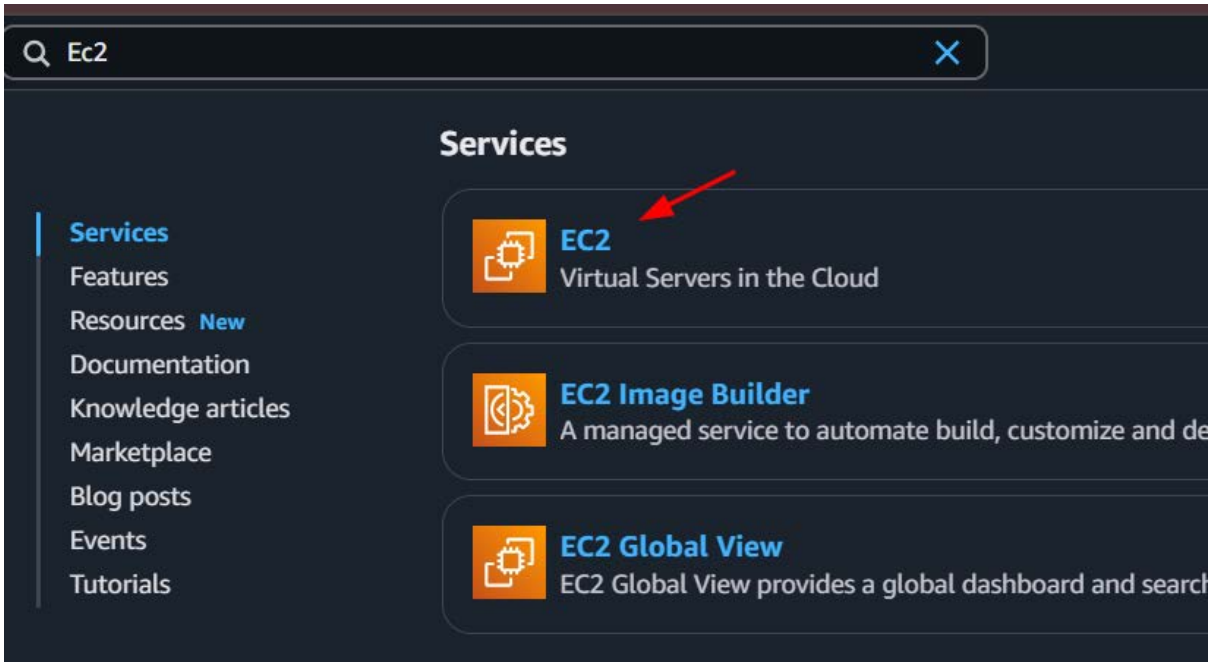


- Follow the prompts to complete the login process.

Step 2: Navigate to EC2 Dashboard

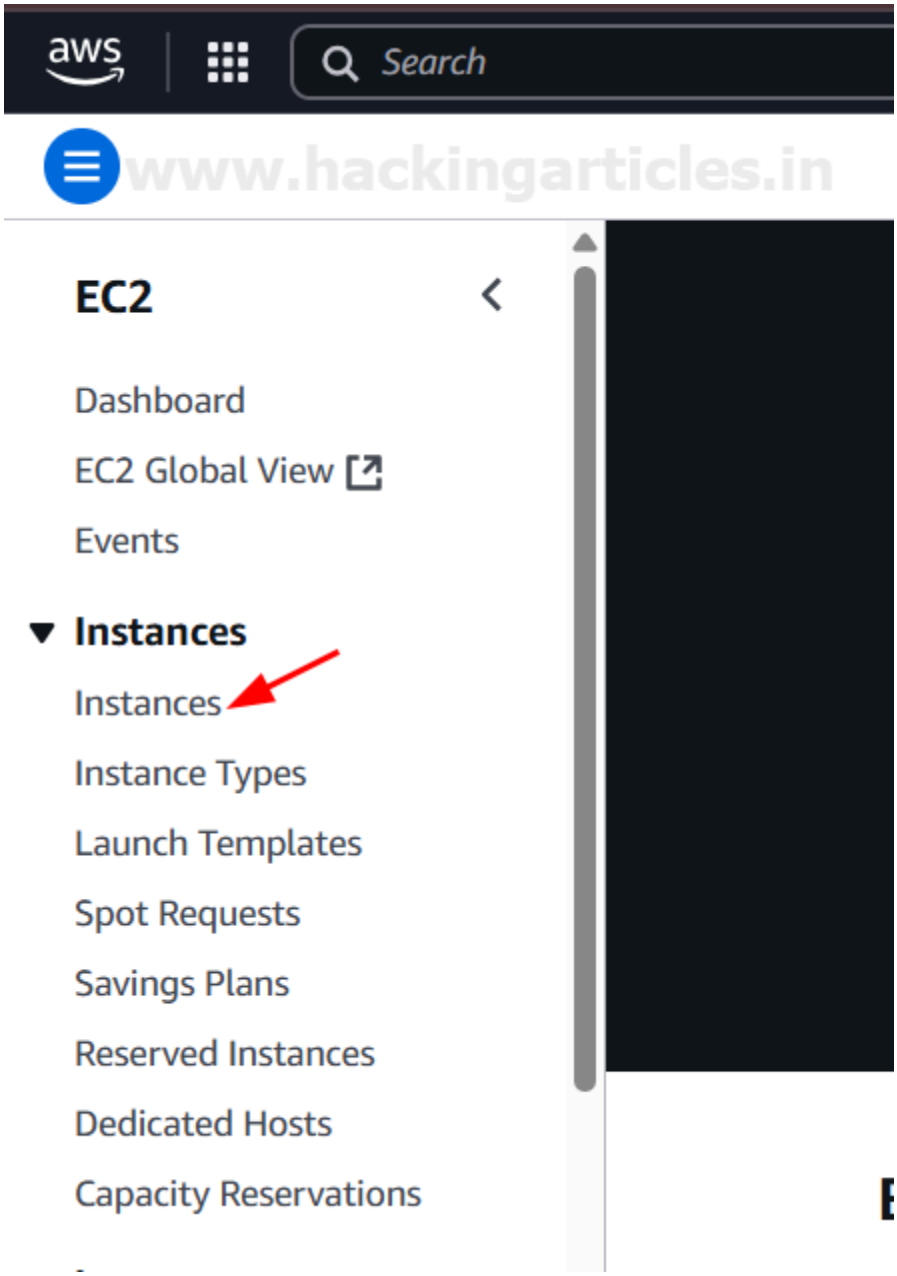
Once logged in, use the search bar at the top of the console.

Then, type "Ec2" and select **"EC2 - Virtual Servers in the Cloud"** from the services list.

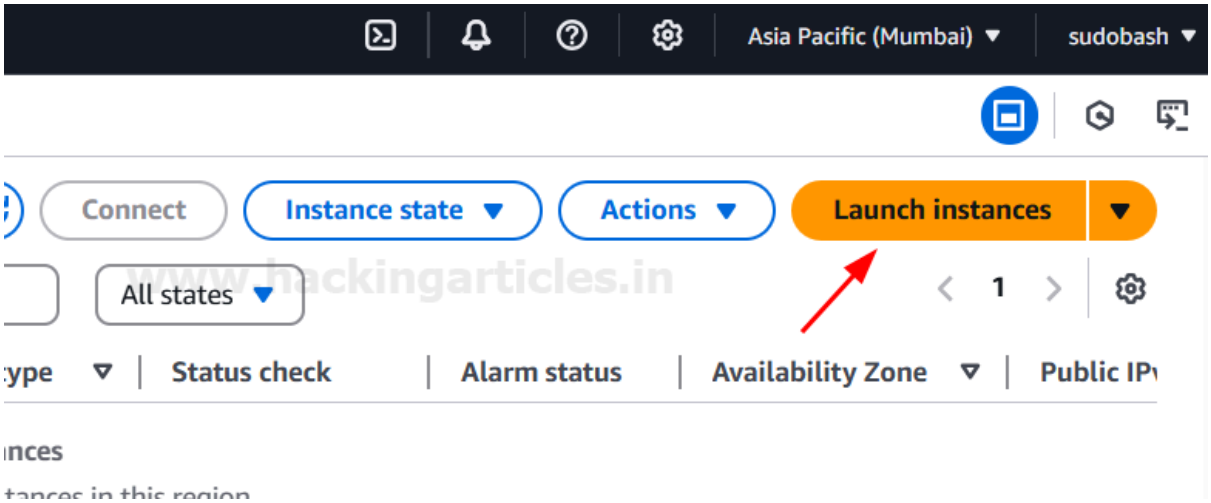


Step 3: Launch a New EC2 Instance

In the EC2 Dashboard, under "Instances," click on **"Instances"**.



Then, click the **"Launch instances"** button.



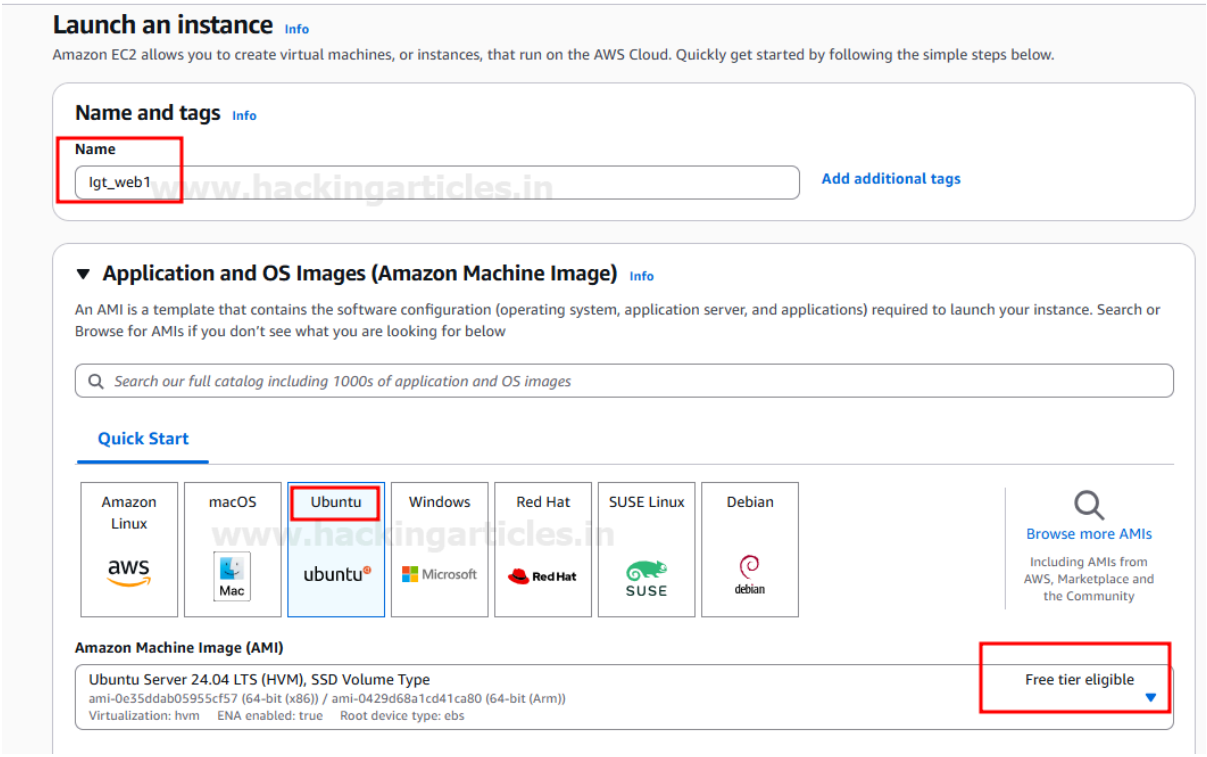
Step 4: Configure Instance Details

Name and tags:

- Give your instance a descriptive name, e.g., lgt_web1.

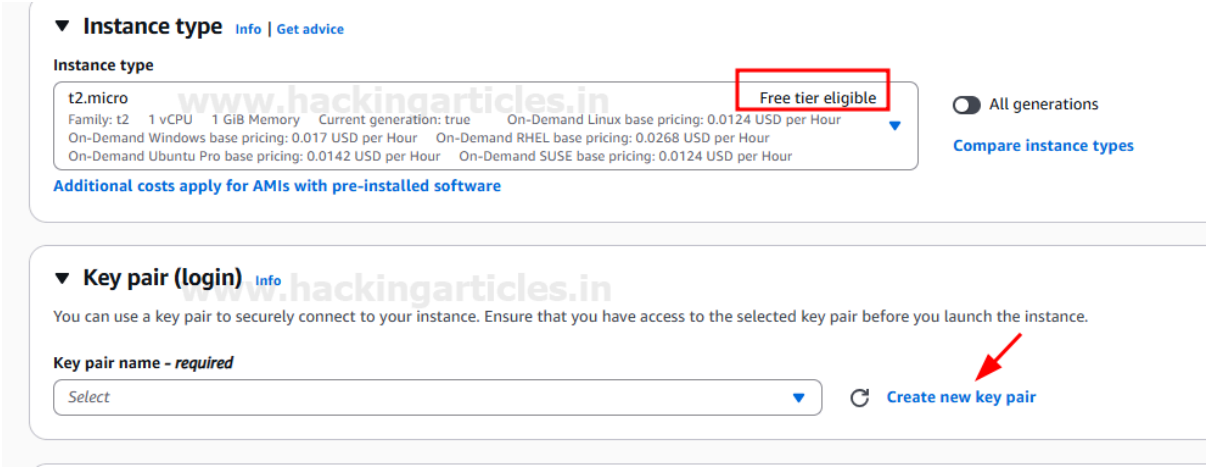
Application and OS Images (Amazon Machine Image - AMI):

- Select **"Ubuntu"** from the "Quick Start" options.
- Ensure "Free tier eligible" is selected if you are using a free tier account.



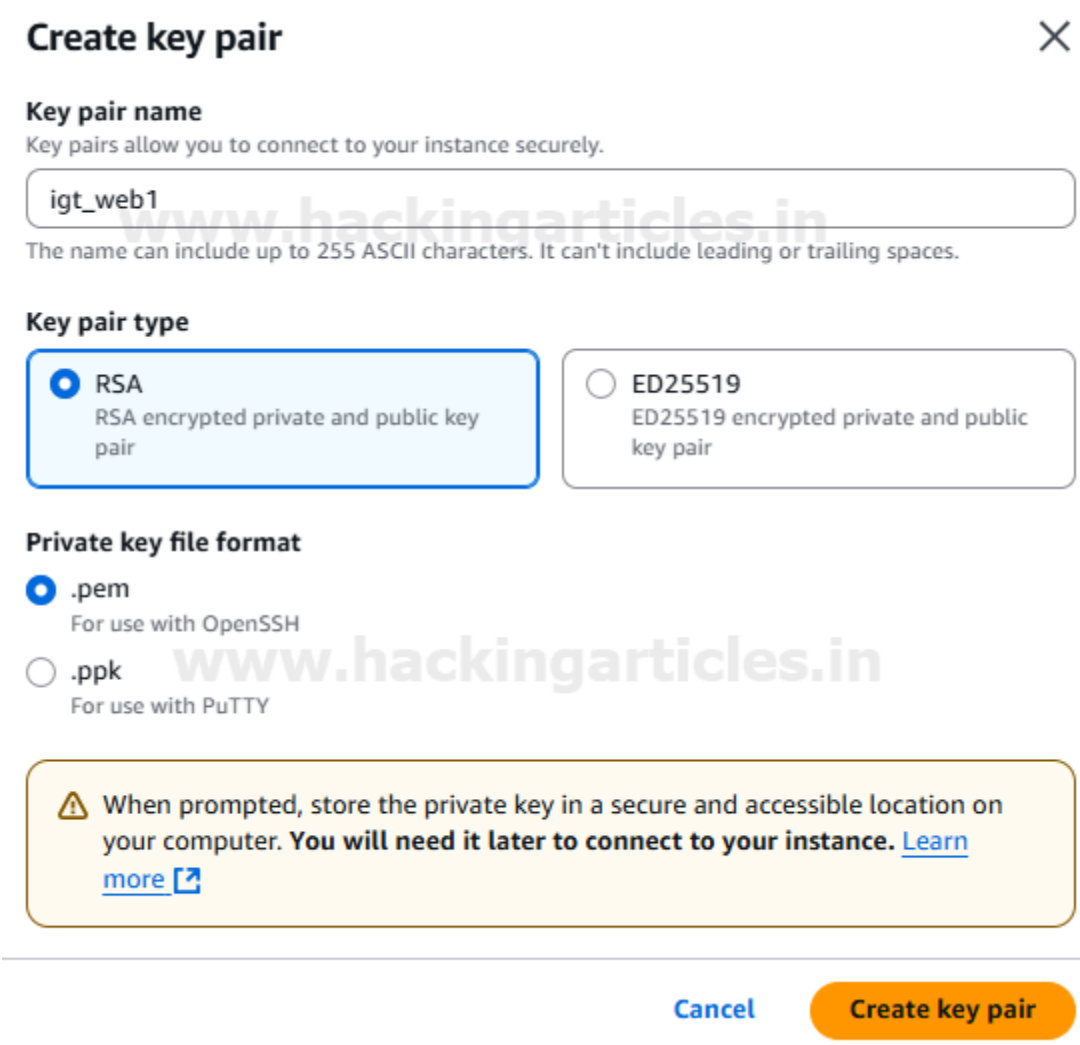
Instance type & Key pair (login):

- Click **"Create new key pair"**.



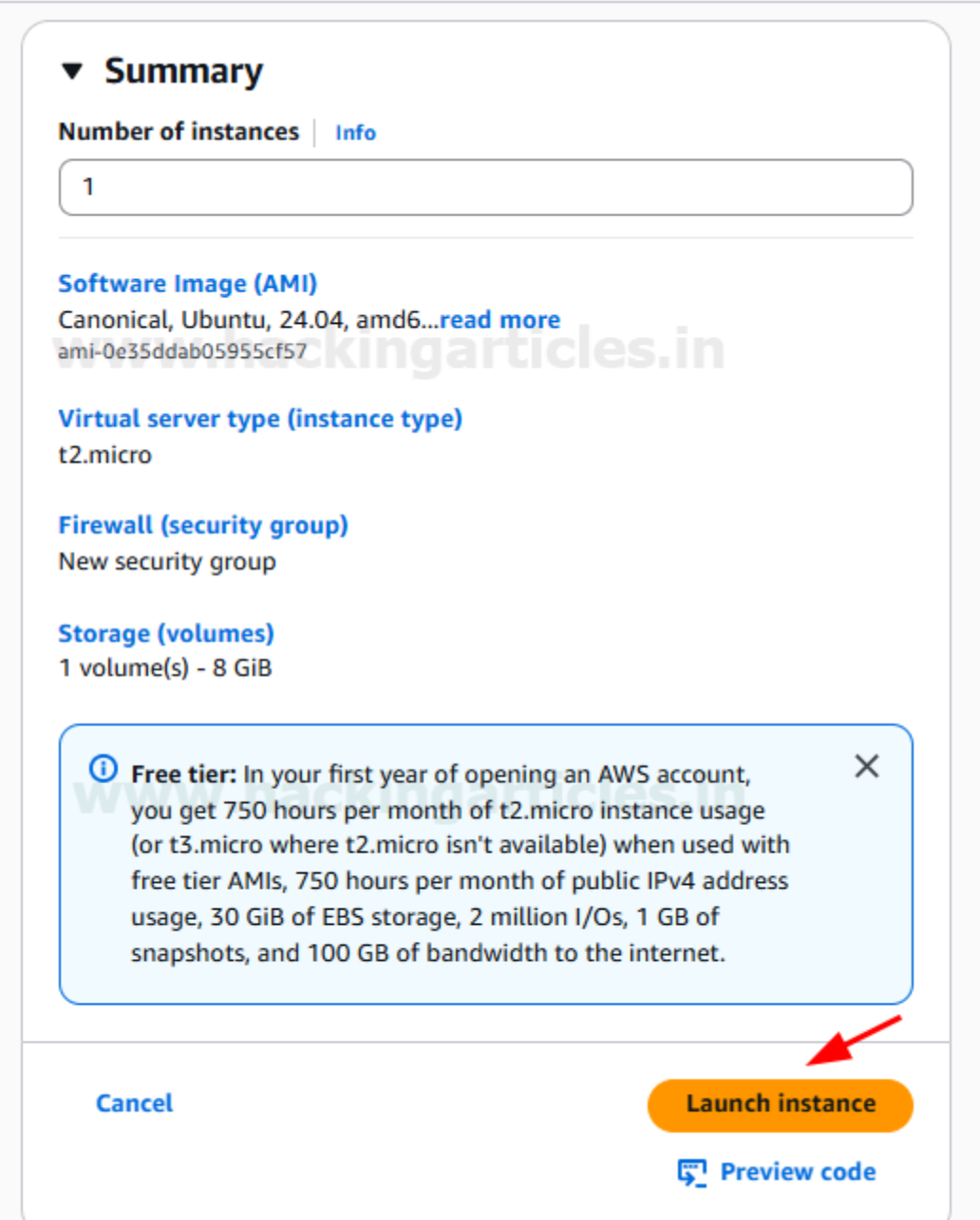
- Select an instance type that is "Free tier eligible," such as t2.micro.
- Enter a "Key pair name", e.g., lgt_web1.
    - Select **"RSA"** for Key pair type.
    - Choose **".pem"** for Private key file format.

- Click **"Create key pair"**. This will download the .pem file to your computer. **Store it securely.**

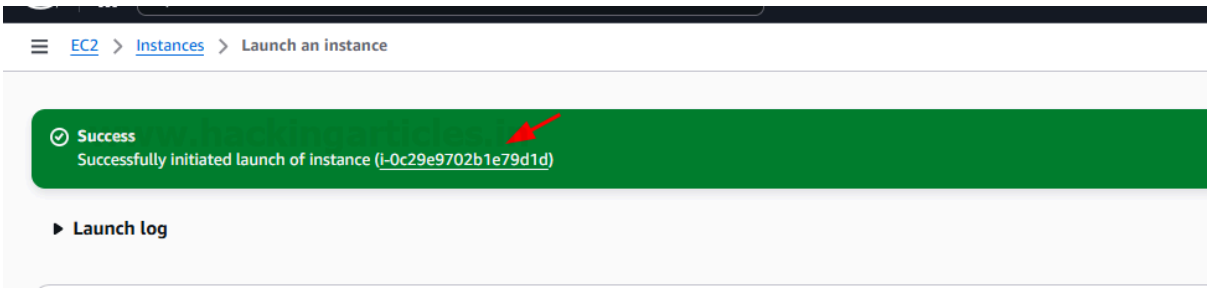


Review and Launch:

- Review the summary of your instance configuration.
- Click **"Launch instance"**.

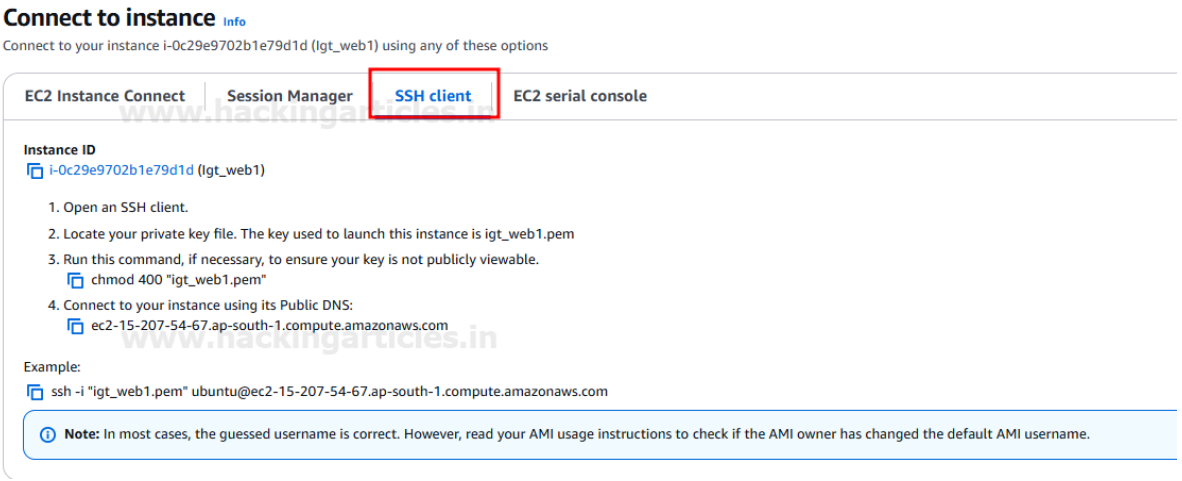


You will see a successful message confirming the launch, along with your instance ID .

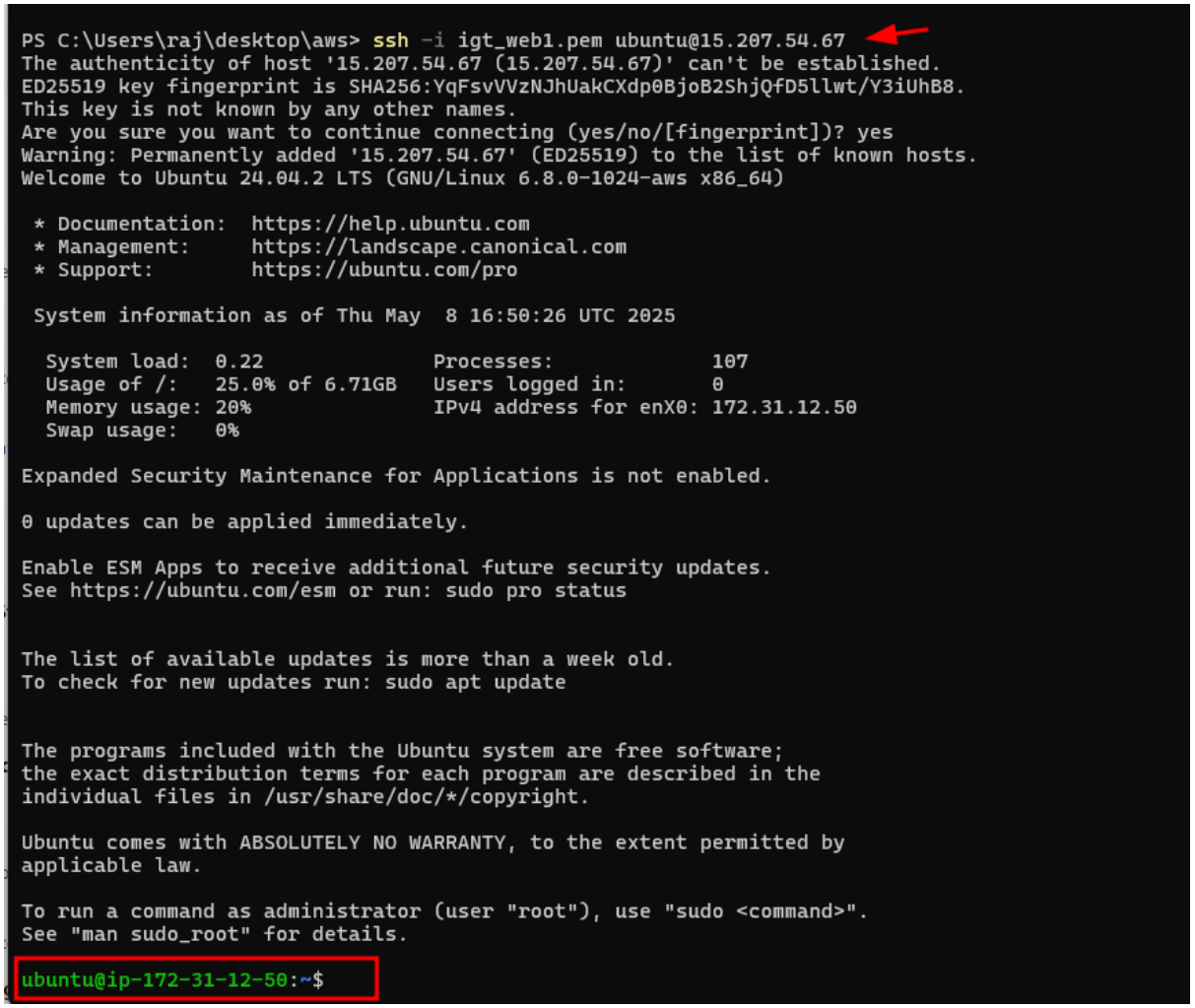


Step 5: Connect to the Ubuntu Instance via SSH

- From the EC2 Instances page, select your newly launched lgt_web1 instance.
- Click the **"Connect"** button.
- Go to the **"SSH client"** tab.



- Follow the instructions provided there:
    - Locate your private key file (lgt_web1.pem).
    - Set appropriate permissions for your private key: chmod 400 lgt_web1.pem
    - Connect using the command format: ssh -i "lgt_web1.pem" ubuntu@<Public DNS or IPv4 address>.

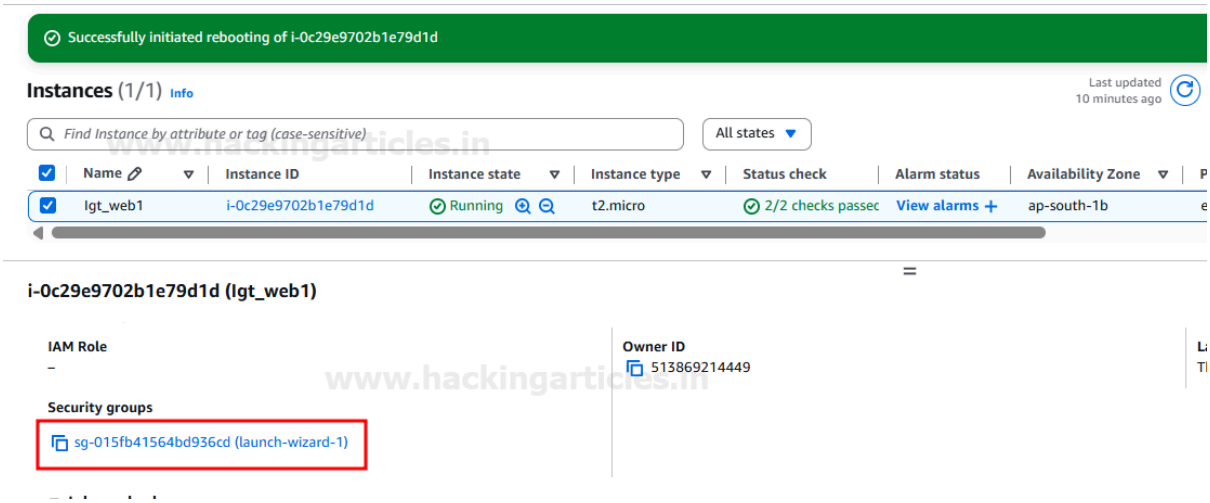


- If prompted about authenticity, type yes and press Enter.

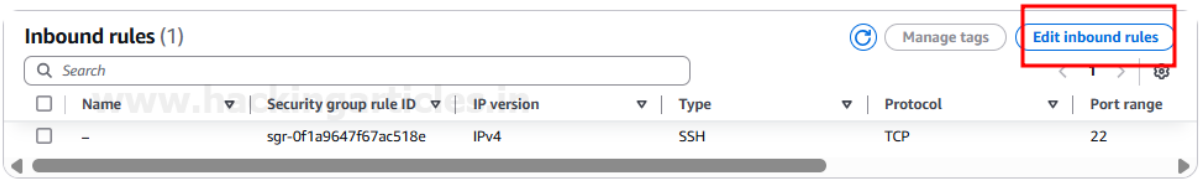
Step 6: Configure Security Group for Web Access

To allow access to your web server, you need to open HTTP and HTTPS ports in the instance's security group.

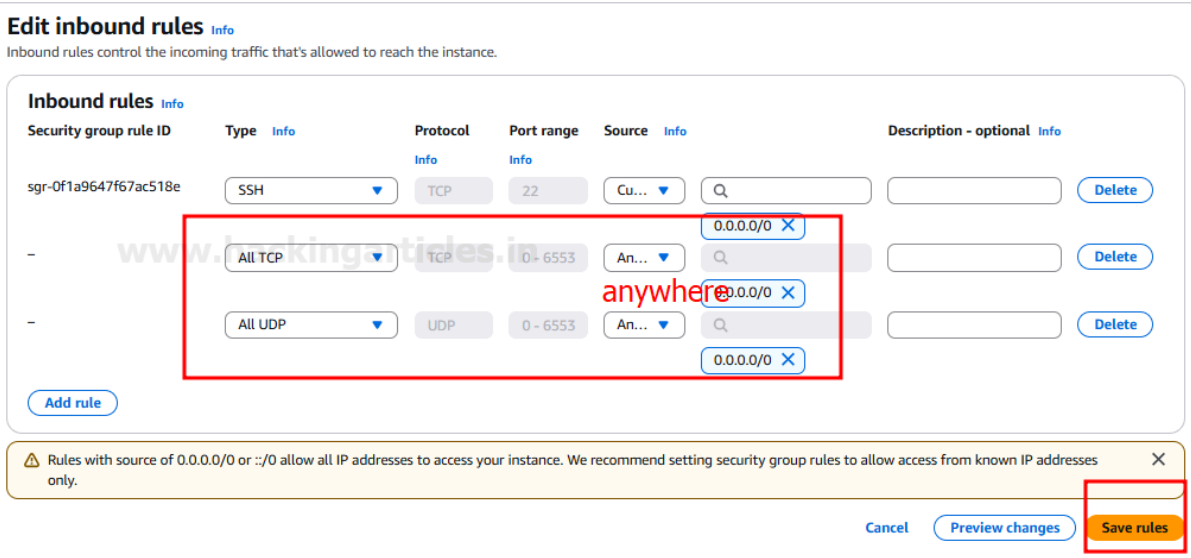
- From the EC2 Instances page, select your lgt_web1 instance.
- Scroll down to the "Security" tab and click on the **"Security groups"** link (e.g., sg-015f...). This will take you to the security group details.



- On the Security group page, go to the "Inbound rules" tab and click **"Edit inbound rules"**.



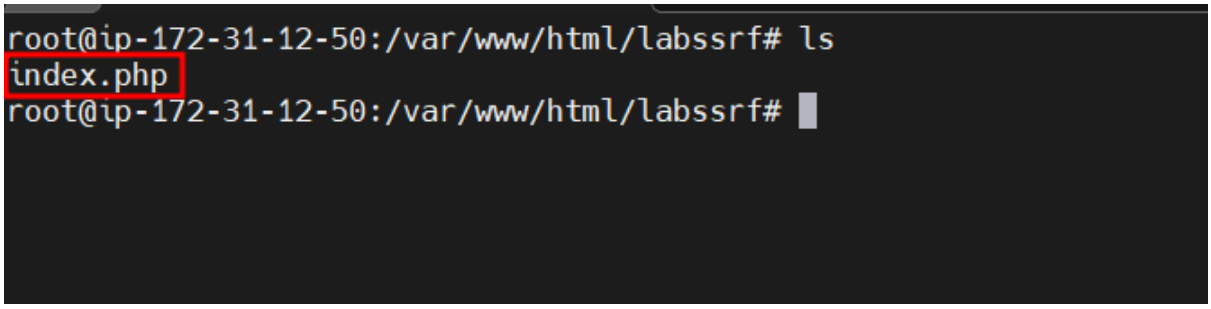
- Click **"Add rule"**.
  - For the first new rule:
    - Type: **"All TCP"**
    - Source: **"Anywhere-IPv4"** (0.0.0.0/0)
  - For the second new rule:
    - Type: **"All UDP"**
    - Source: **"Anywhere-IPv4"** (0.0.0.0/0).
- Click **"Save rules"**.



Step 7: Deploy the SSRF Vulnerability Lab

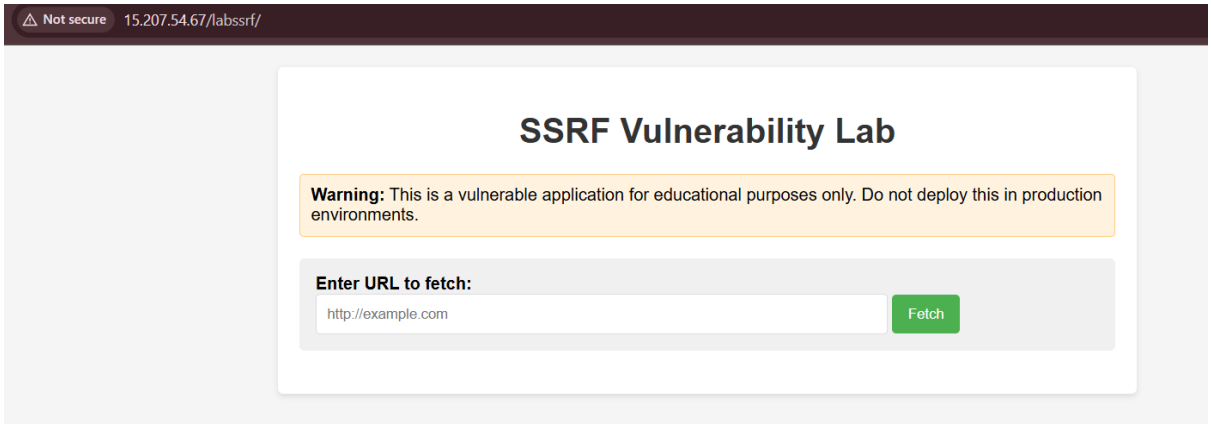
Once connected to your Ubuntu instance via SSH:

- Navigate to the web server directory (e.g., /var/www/html/). You might need to create a directory for your lab: sudo mkdir /var/www/html/labssrf
- Change to that directory: cd /var/www/html/labssrf
- Create an index.php file for the SSRF lab (Image below shows index.php in the directory).



You'll need to create this file and populate it with the vulnerable PHP code. (The document doesn't provide the code, but you'll place it here).

- After deploying, you should be able to access the SSRF lab in your web browser by navigating to http://<Your_Instance_Public_IP>/labssrf/.

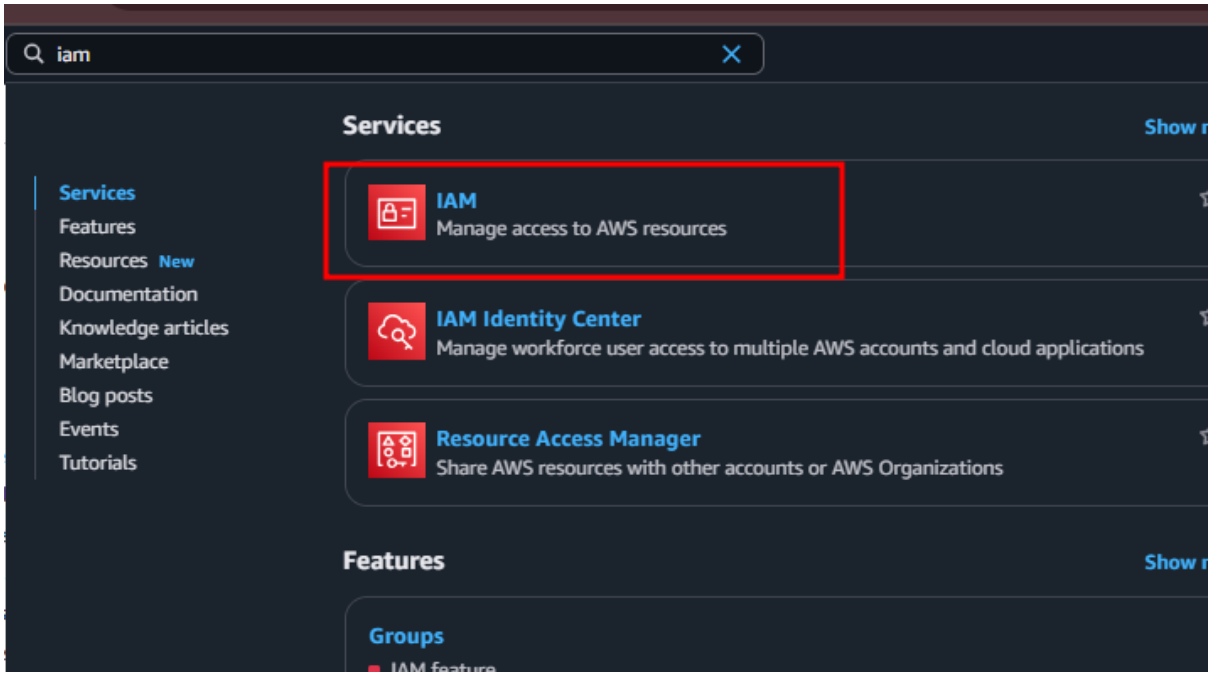


Step 8: Create and Attach an IAM Role to the Instance

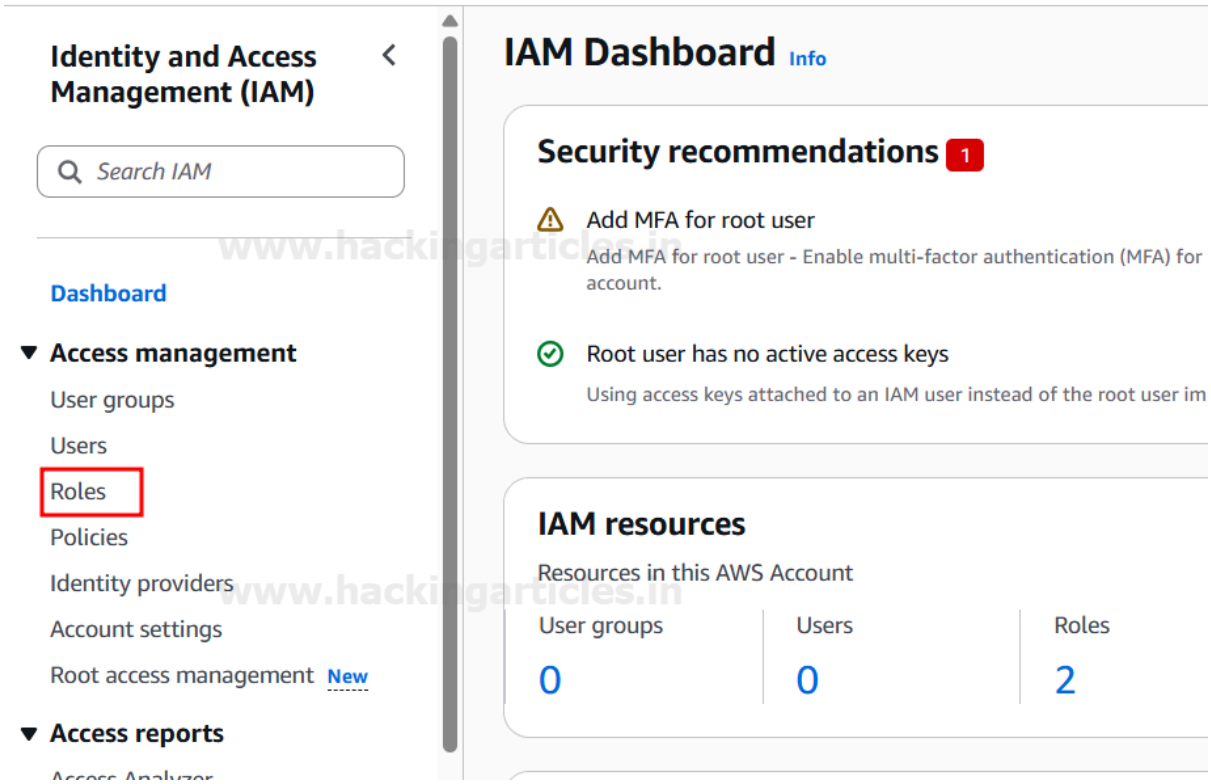
This step assigns an IAM role with specific permissions to your EC2 instance, which is crucial for certain types of attacks (like privilege escalation via EC2 metadata).

Create IAM Role:

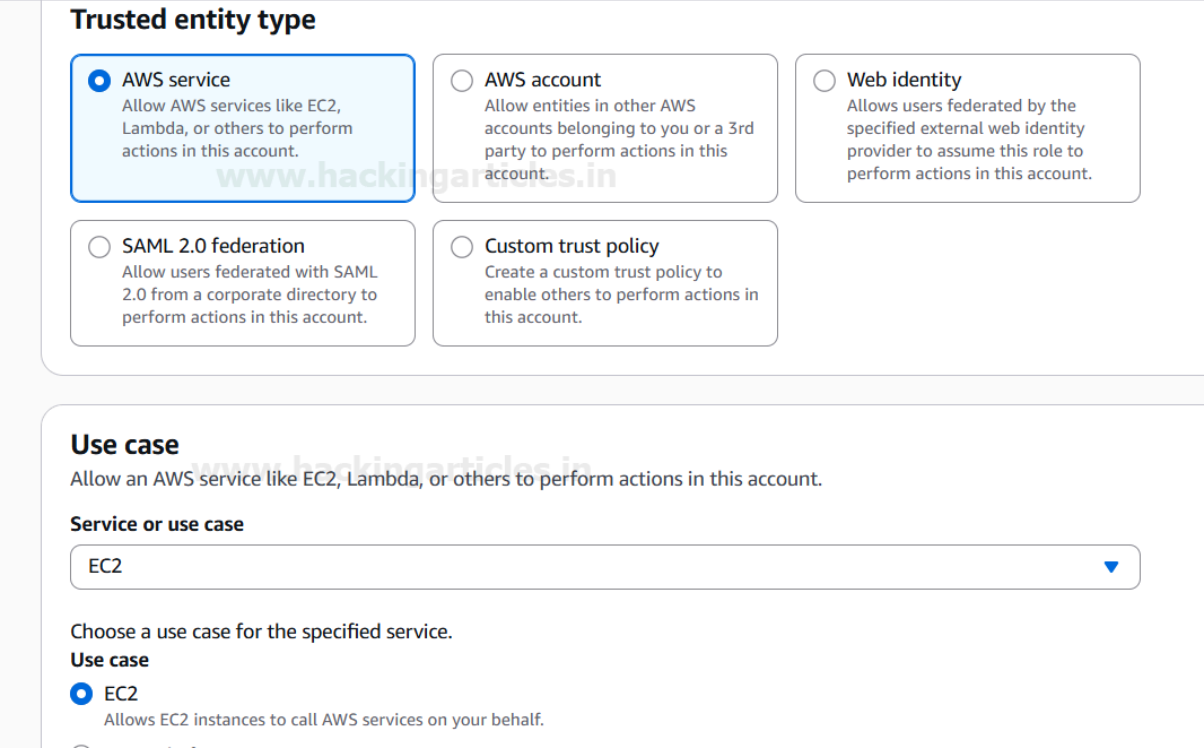
- In the AWS Management Console search bar, type "iam" and select **"IAM - Manage access to AWS resources"**.



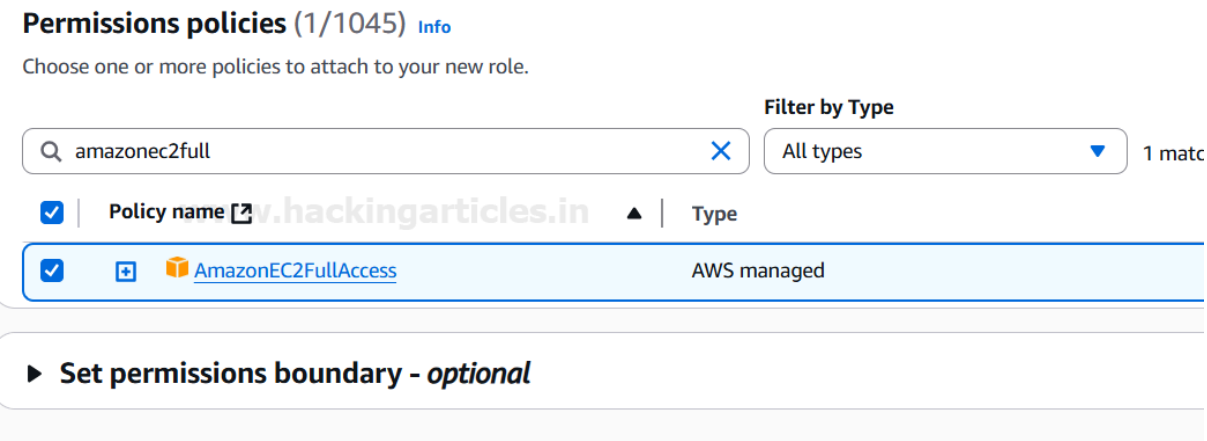
- In the IAM dashboard, click **"Roles"** under "Access management".



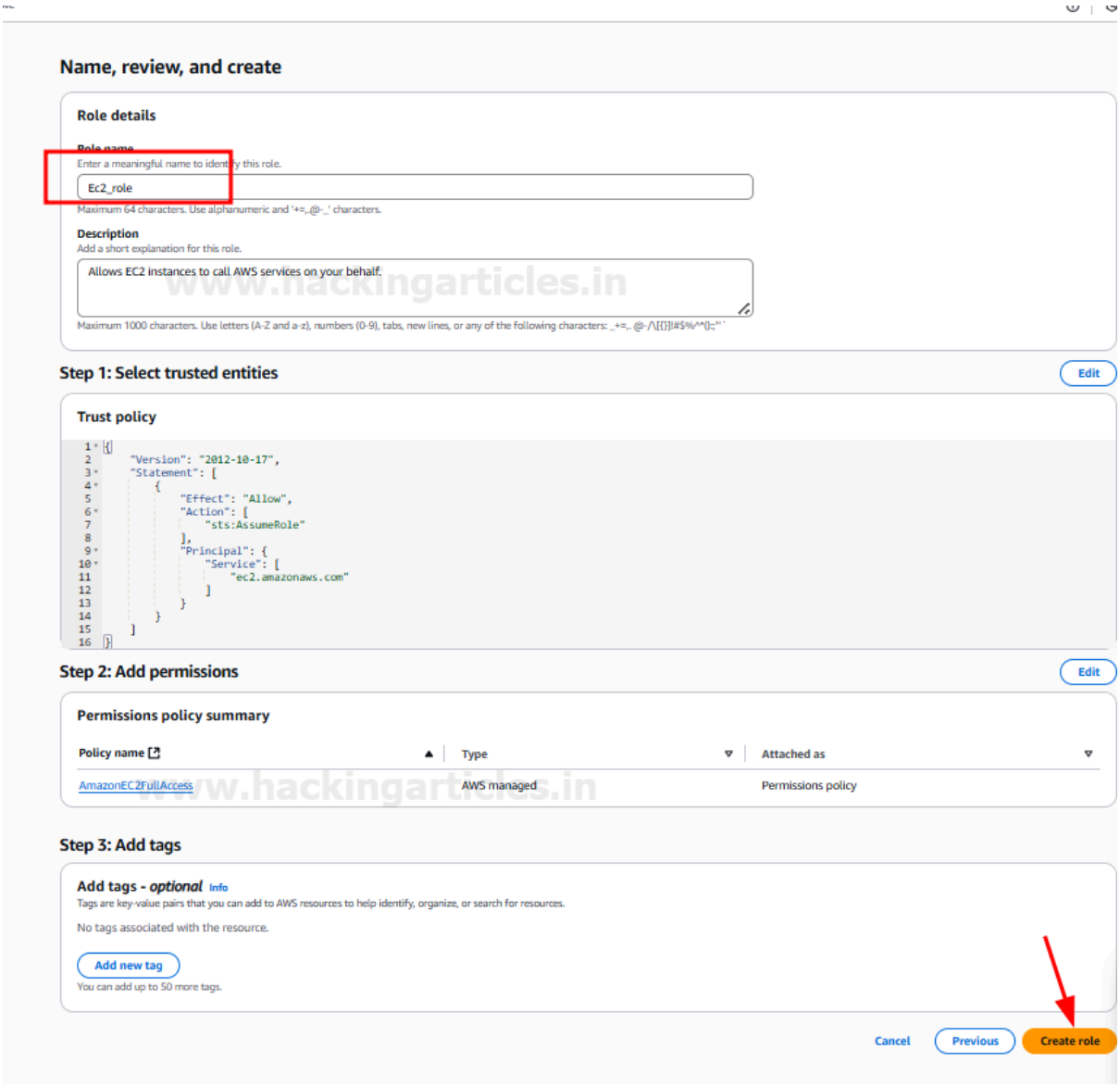
- Click **"Create role"**.
- **Trusted entity type:** Select **"AWS service"**.
- **Use case:** Select **"EC2"**.



- Click **"Next"**.
- **Permissions policies:** Search for amazonec2full and select **"AmazonEC2FullAccess"**.

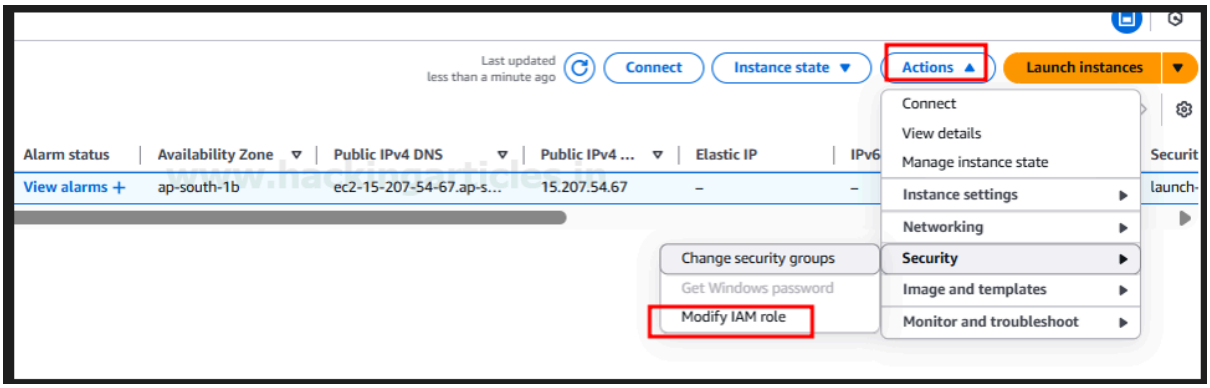


- Click **"Next"** & **Name, review, and create:**
    - Set a **"Role name"**, e.g., Ec2_role.
    - Review the policy and click **"Create role"**.

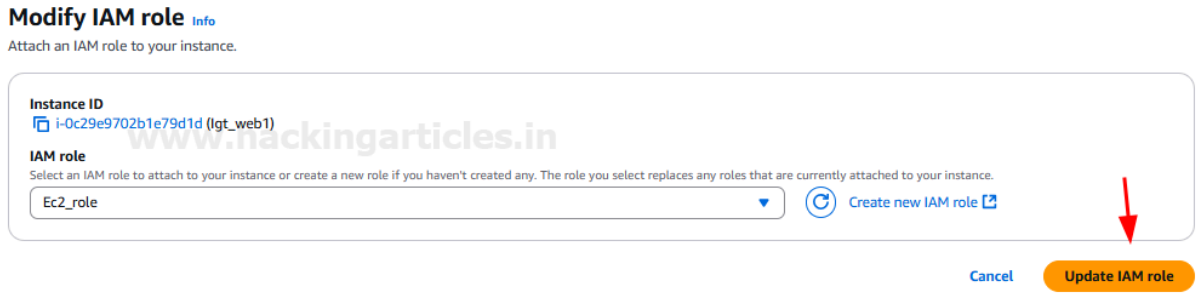


Attach IAM Role to Instance:

- Go back to the EC2 Instances page (select your lgt_web1 instance).
- Click **"Actions"** -> **"Security"** -> **"Modify IAM role"**.



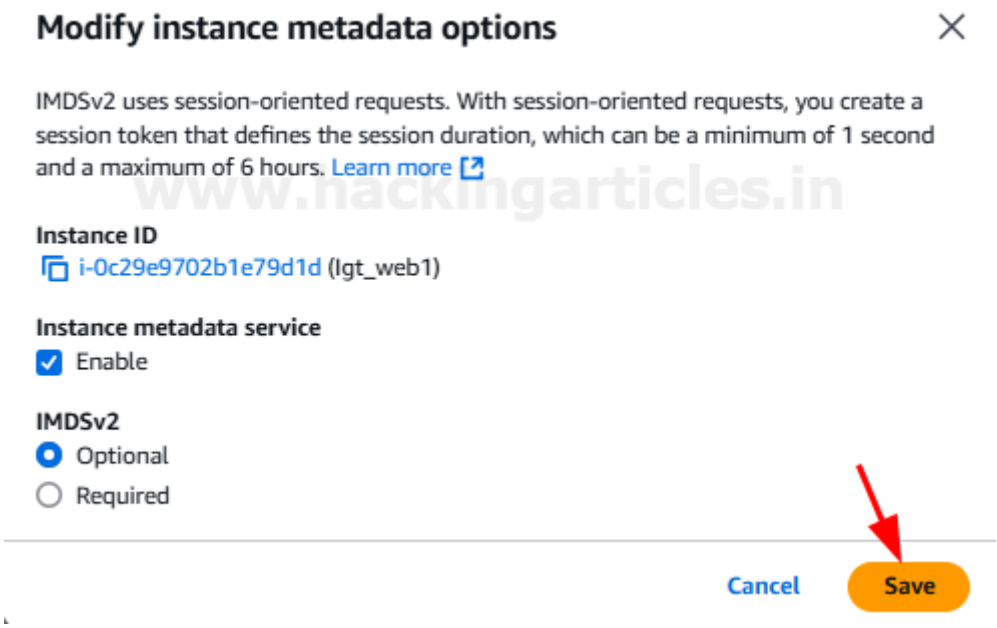
- In the "Modify IAM role" dialog, select the Ec2_role you just created from the dropdown. Click **"Update IAM role"**.



Step 9: Modify Instance Metadata Options (IMDSv2)

IMDSv2 adds a layer of security to the instance metadata service. For some lab scenarios, you might need to adjust this.

1. From the EC2 Instances page, select your lgt_web1 instance.
2. Firstly, click **"Actions"** -> **"Instance settings"** -> **"Modify instance metadata options"**.
3. Then, ensure "Enable" is checked for "Instance metadata service."
4. You can set IMDSv2 to "Optional" or "Required" depending on your lab's needs. The image shows "Optional". Click **"Save"**.

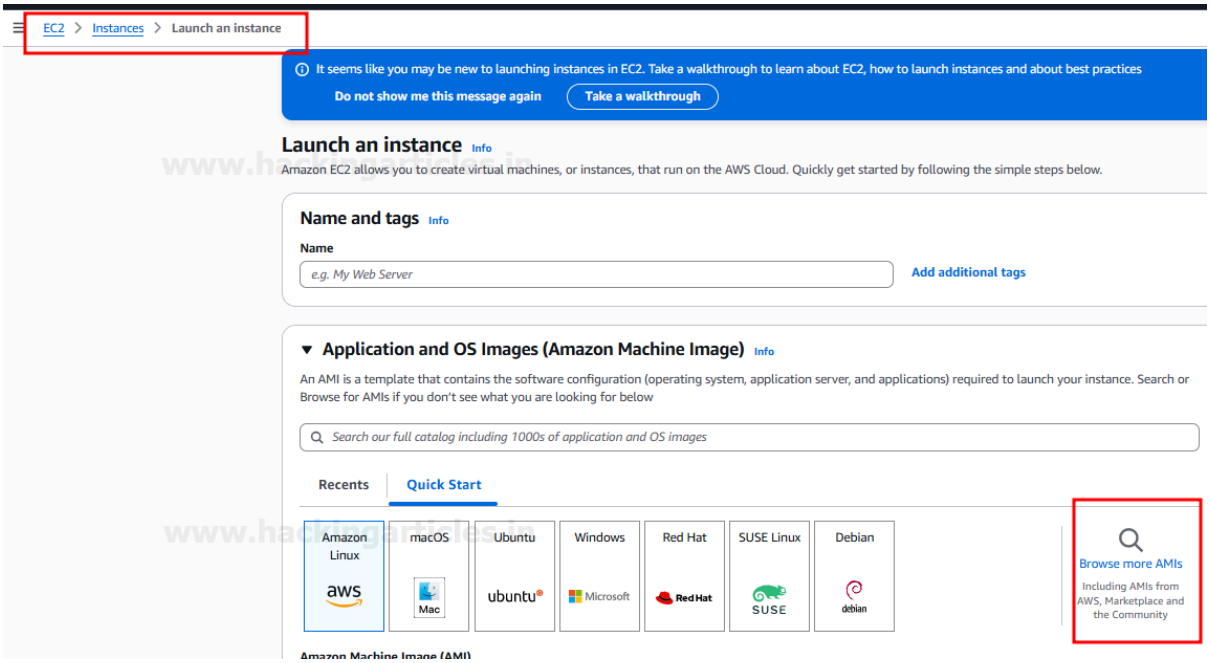


Part 2: Setting up the Attacker Machine (Kali Linux EC2 Instance)

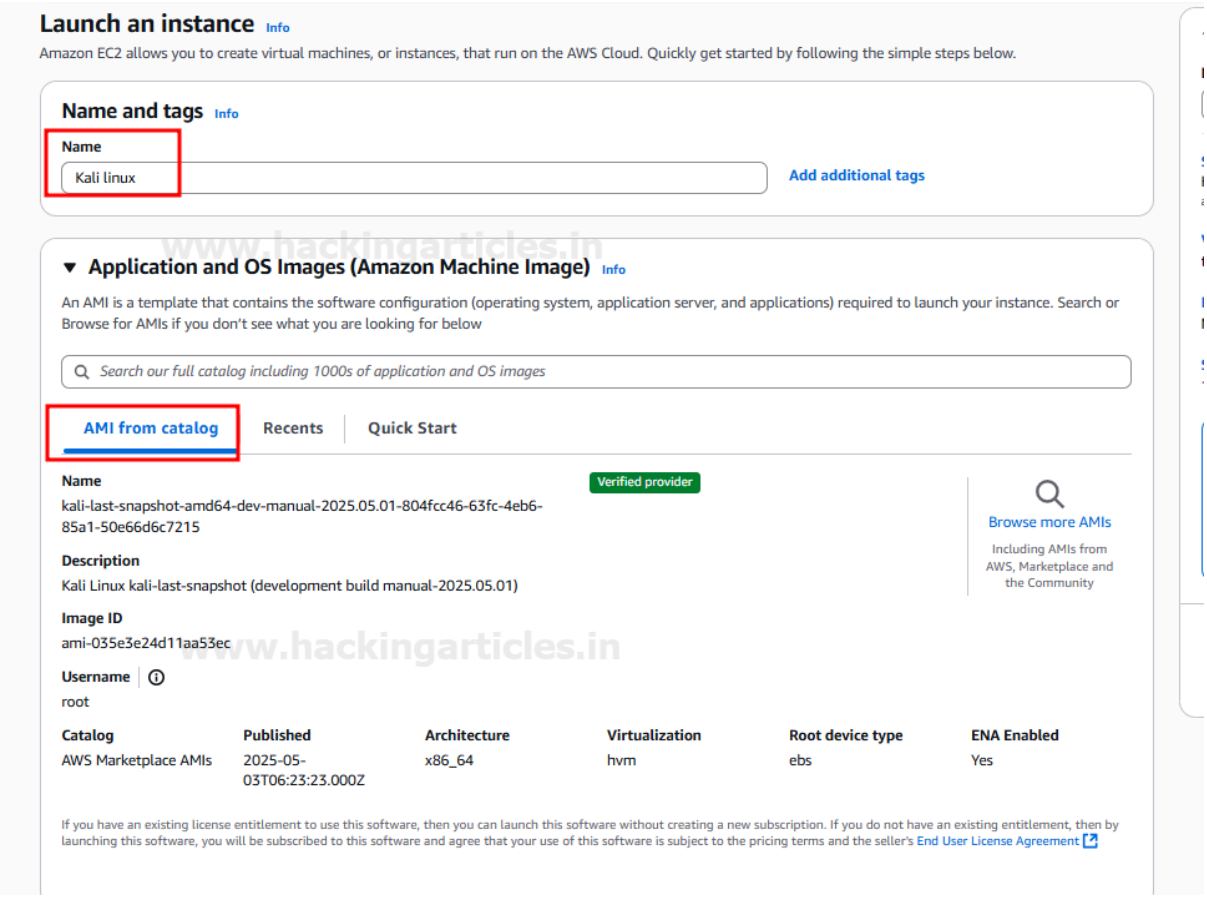
This section details the steps to launch a Kali Linux EC2 instance, which will serve as your attacker machine.

Step 1: Launch a New EC2 Instance (for Kali)

- From the EC2 Instances page, click **"Launch instances"** again.

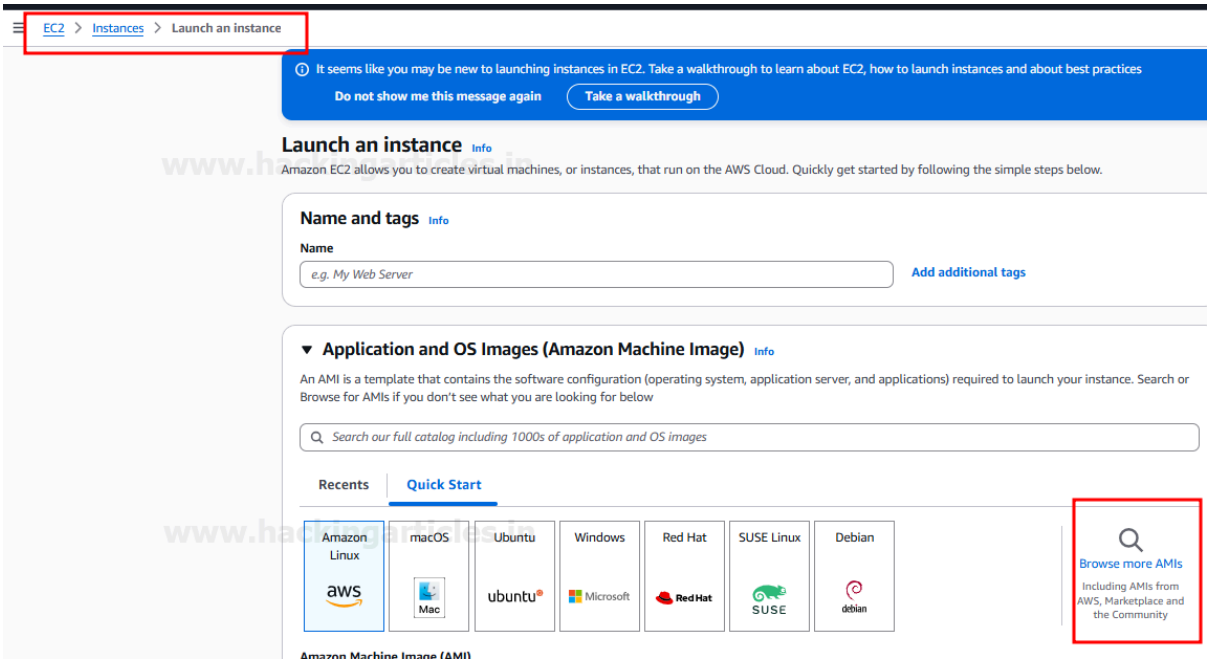


- **Name and tags:**
    - Give your instance a name, e.g., Kali linux.

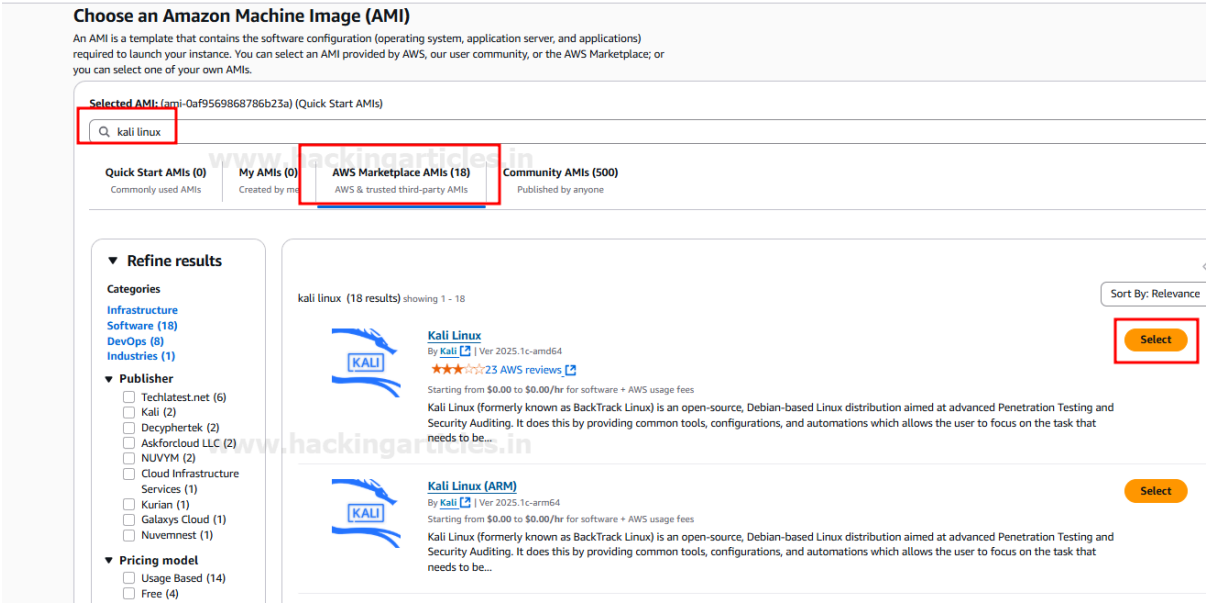


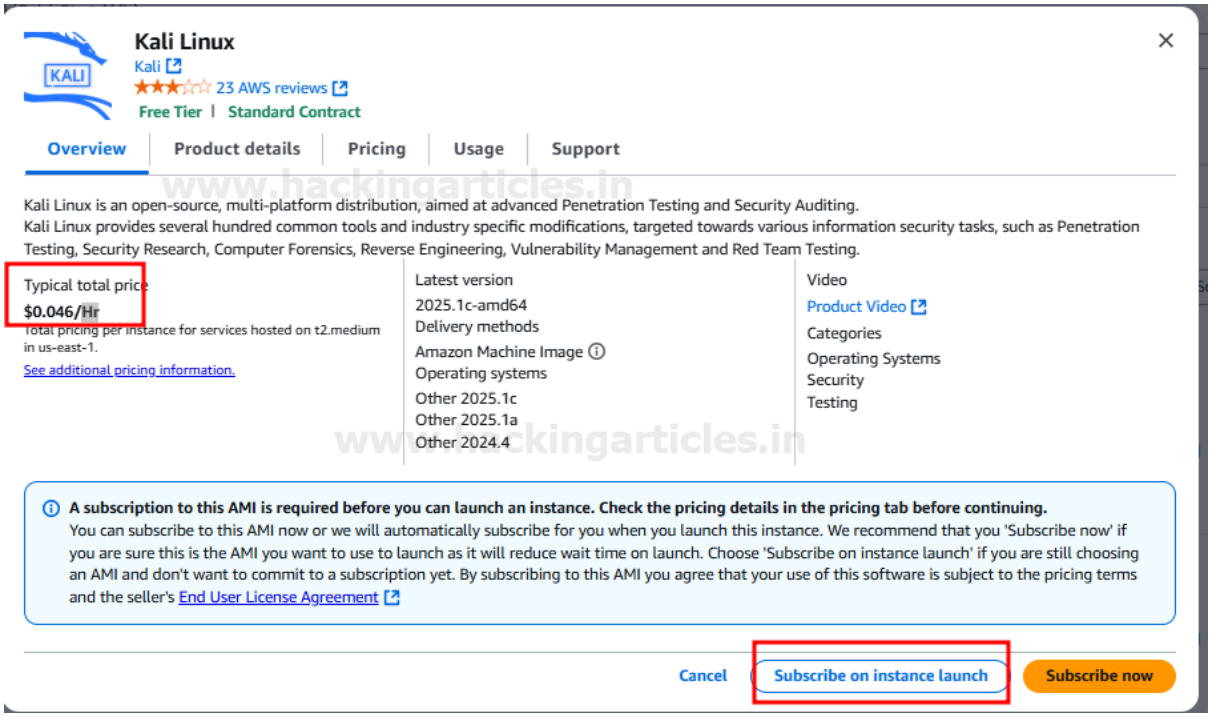
Application and OS Images (Amazon Machine Image - AMI):

- Click **"Browse more AMIs"**.



- Here, search for "kali linux" in the search bar.
- Now, go to the **"AWS Marketplace AMIs"** tab.
- Then, select the appropriate Kali Linux AMI. Note that Kali Linux AMIs often have an associated cost (e.g., $0.046/Hr as shown in the images.
- Click **"Subscribe on instance launch"**.



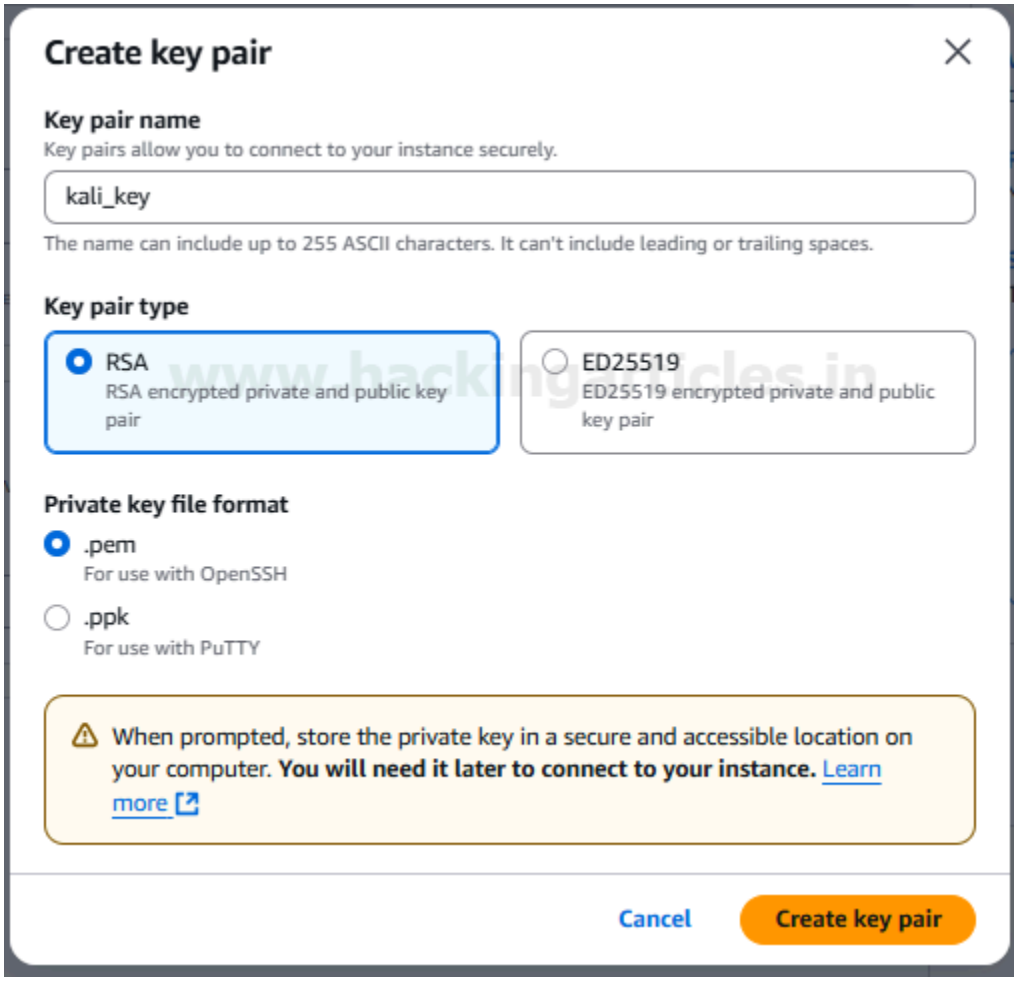


Instance type:

- Choose an instance type, usually t2.medium as shown in the example (Image 34 summary, though not explicitly chosen in a previous image).

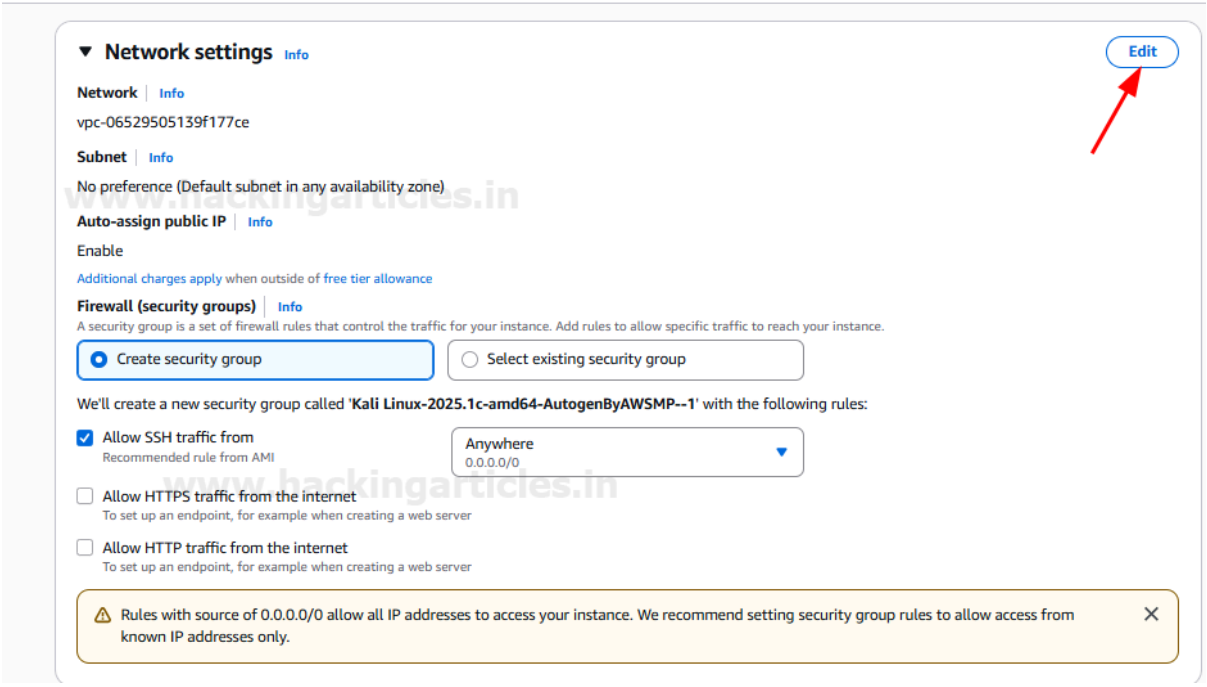
Key pair (login):

- Then, create a new key pair for Kali, e.g., kali_key, similar to how you did for the Ubuntu instance.

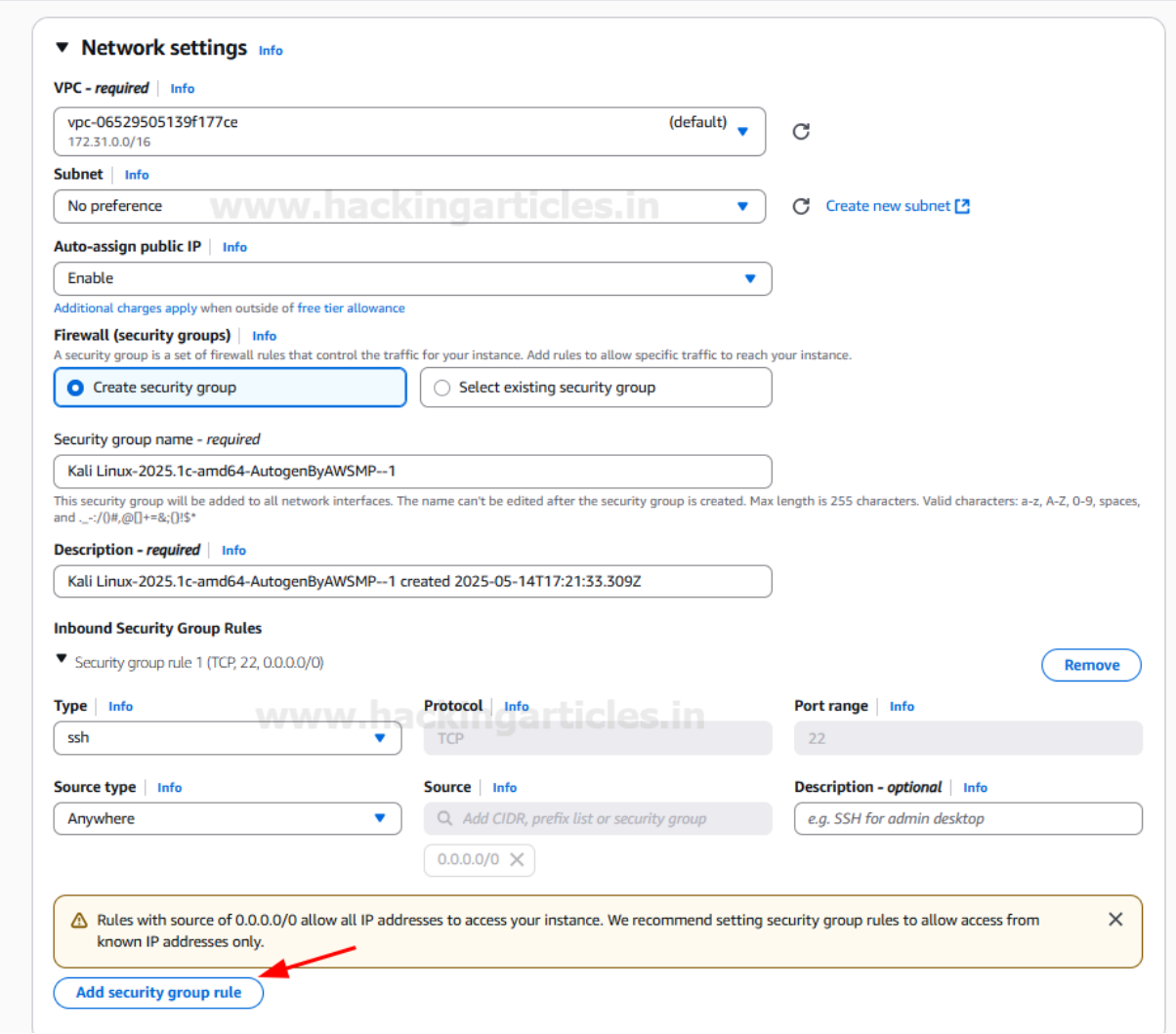


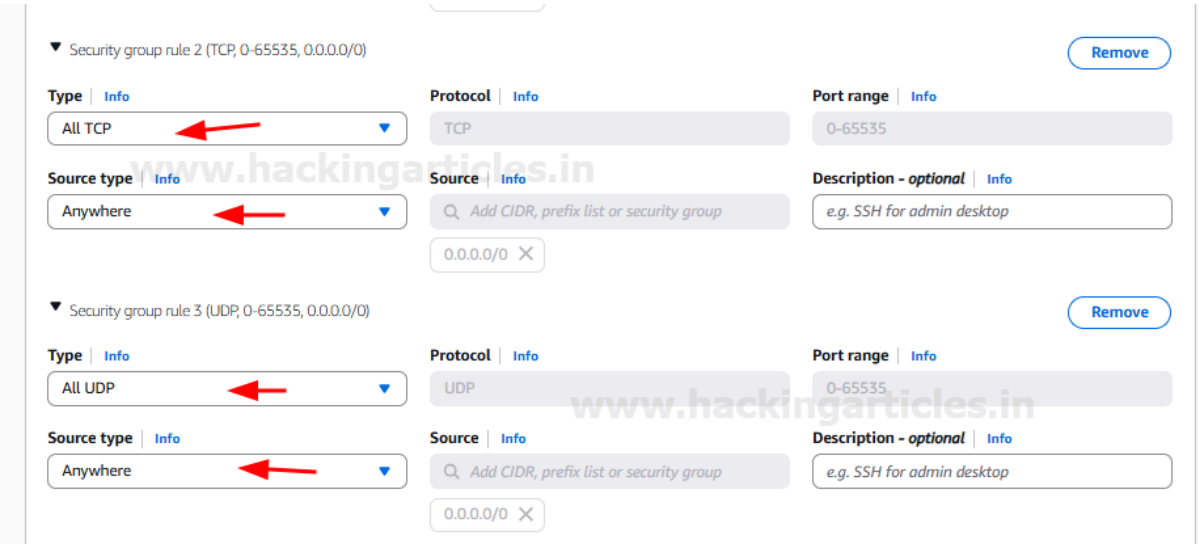
Network settings:

- Firstly, click **"Edit"** next to "Network settings".



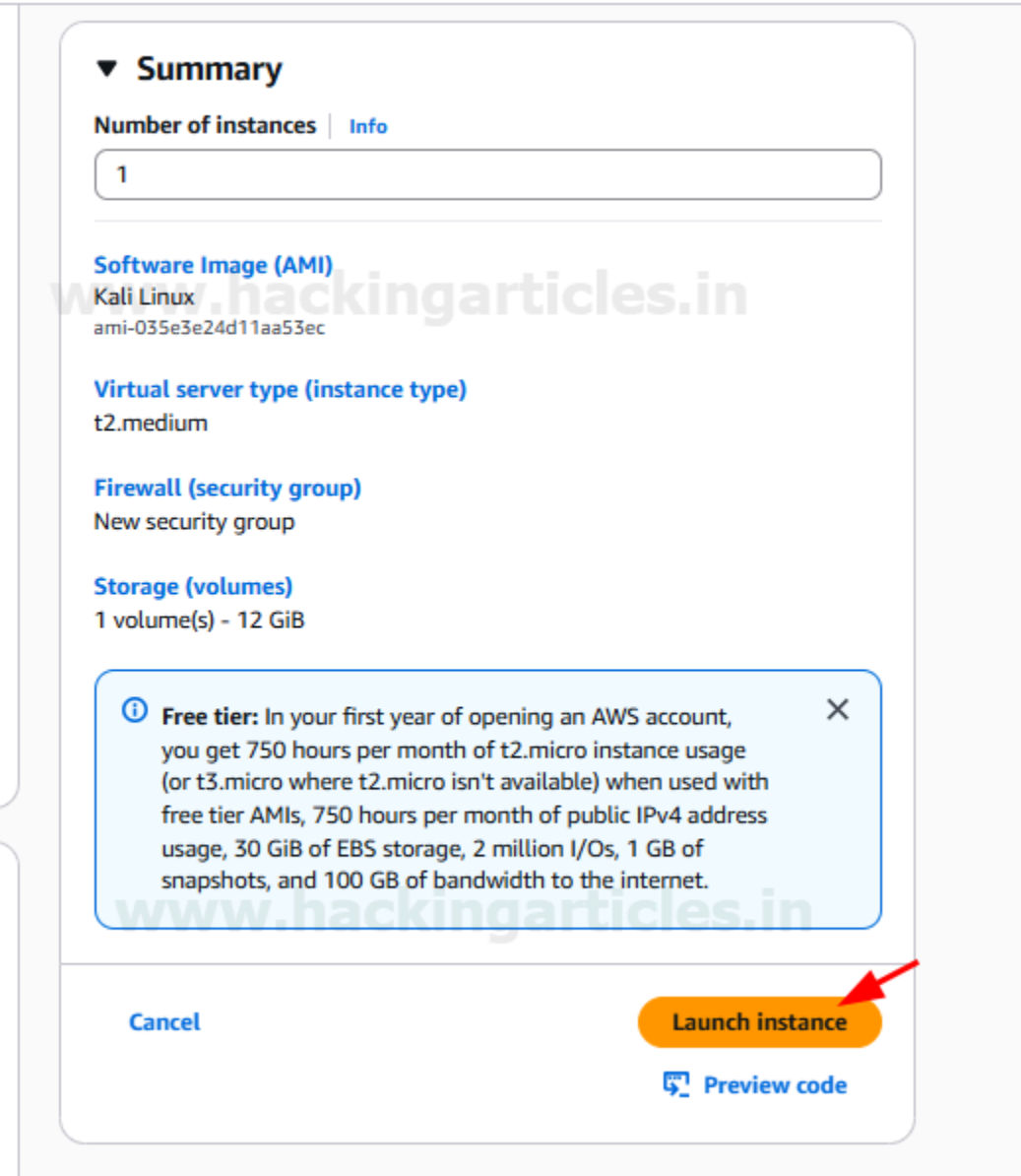
- Ensure "Auto-assign public IP" is enabled.
- For **"Firewall (security groups)"**, choose **"Create security group"**.
- Add inbound rules:
    - Add a rule for **"All TCP"** from "Anywhere" (0.0.0.0/0).
    - Add a rule for **"All UDP"** from "Anywhere" (0.0.0.0/0)
- Click **"Add security group rule"** as needed.





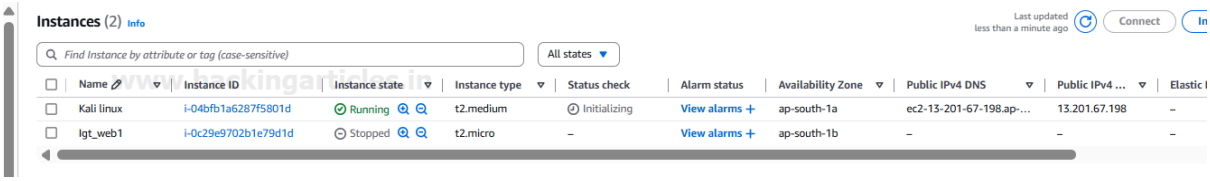
Review and Launch:

- Review the summary and click **"Launch instance"**.\

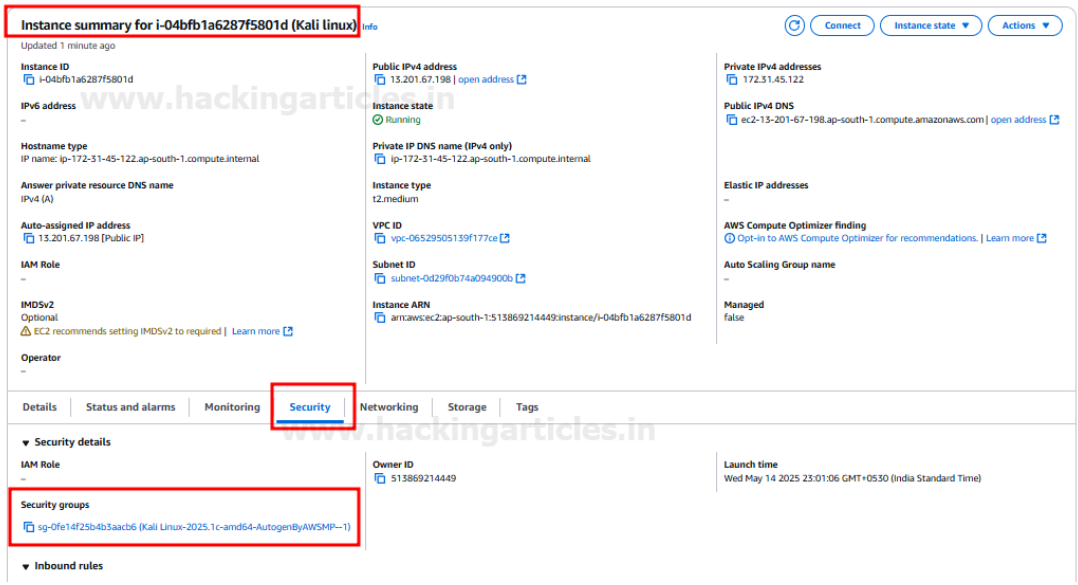


Step 2: Verify Kali Linux Instance State and Security Group

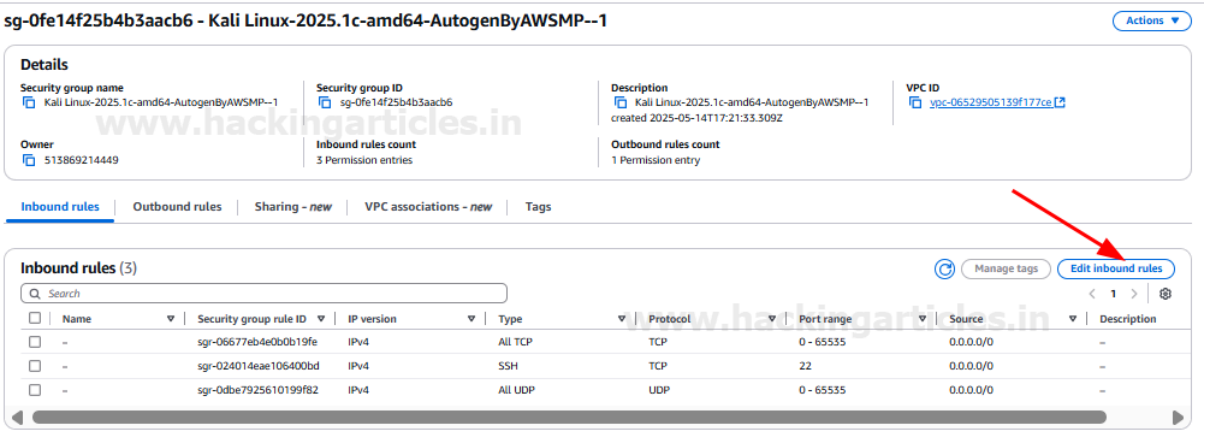
- After launching, go back to the EC2 Instances page. You should see both your lgt_web1 (Ubuntu) and Kali linux instances. The Kali instance will likely be in an "Initializing" state initially.



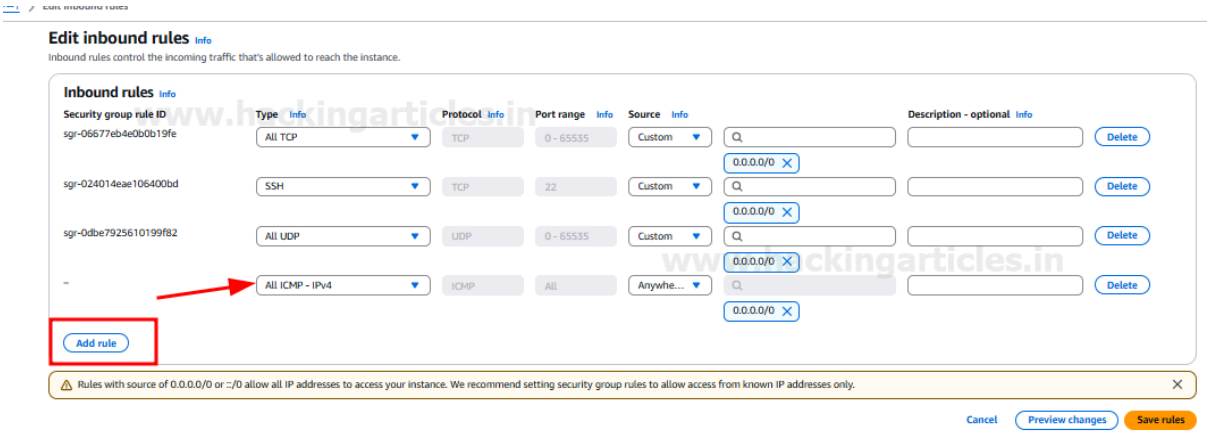
- Once Kali linux is running, select it.
- Then, go to the **"Security"** tab and click on the associated **"Security groups"** link.



- On the security group page, click **"Edit inbound rules"**.



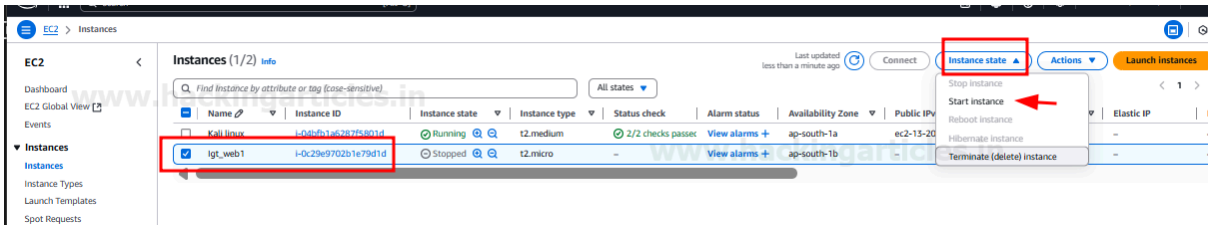
- Add an **"All ICMP - IPv4"** rule with "Anywhere" (0.0.0.0/0) source to allow ping requests. Click **"Save rules".**



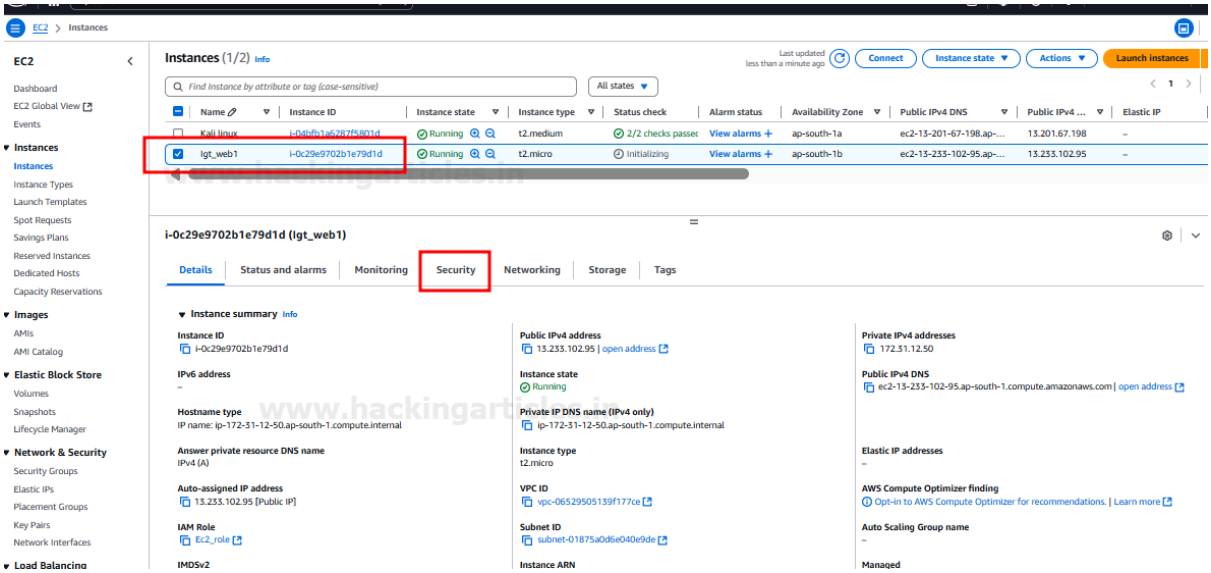
Step 3: Start the Ubuntu Web Server Instance (if stopped)

If your lgt_web1 instance was stopped, you can start it:

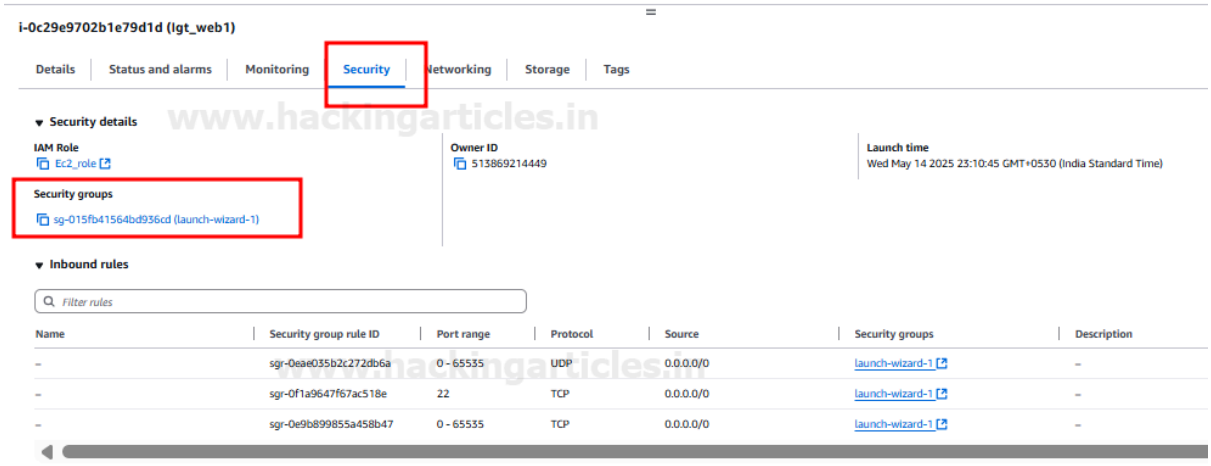
- Firstly, select lgt_web1 from the EC2 Instances page.
- Then. click **"Instance state"** -> **"Start instance"**.

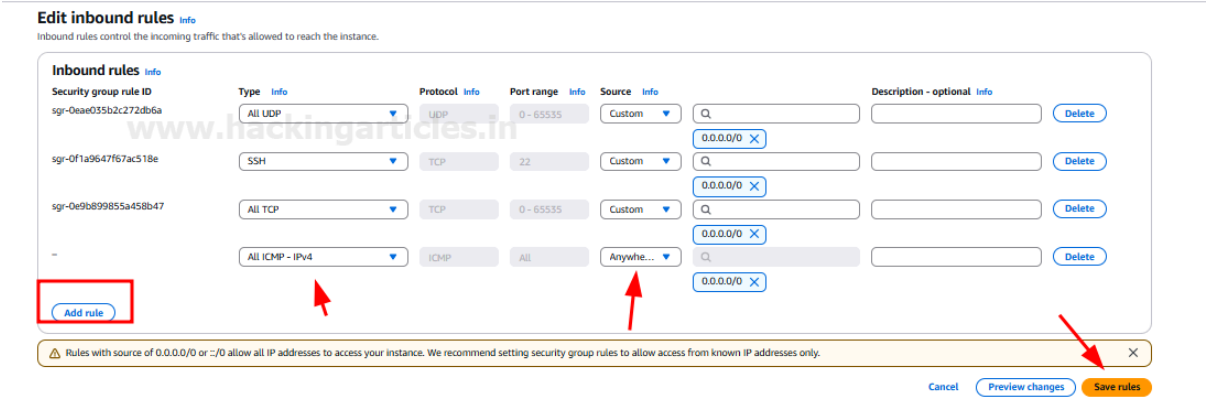


- Verify the instance is running.



- Ensure its security group has the necessary rules.





Step 4: Test Connectivity from Kali Linux

1. Firstly, connect to your Kali Linux instance via SSH using its key pair and public IP/DNS, like how you connected to the Ubuntu instance.
2. Then once connected to Kali, try to ping your Ubuntu instance's public IP address (or private IP if they are in the same VPC and allowed by security groups).
    - Example: ping 13.233.102.95 (Replace with your Ubuntu instance's IP).

```
└─(Run: "touch ~/.hushlogin" to hide this message)
┌──(kali㉿kali)-[~]
└─$ ping 13.233.102.95
PING 13.233.102.95 (13.233.102.95) 56(84) bytes of data.
64 bytes from 13.233.102.95: icmp_seq=1 ttl=63 time=1.13 ms
64 bytes from 13.233.102.95: icmp_seq=2 ttl=63 time=1.53 ms
^C
--- 13.233.102.95 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.134/1.331/1.528/0.197 ms

┌──(kali㉿kali)-[~]
└─$
```

    - A successful ping indicates network connectivity between your Kali attacker machine and the vulnerable web server.

Finally, this completes the setup of your AWS lab environment with a vulnerable web server and an attacker Kali Linux machine. You can now proceed with your security testing and exploit development.

To learn more about Cloud Security. Follow this link.

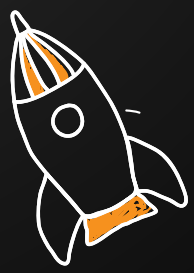
iGNITE Technologies

JOIN OUR TRAINING PROGRAMS

CLICK HERE

BEGINNER

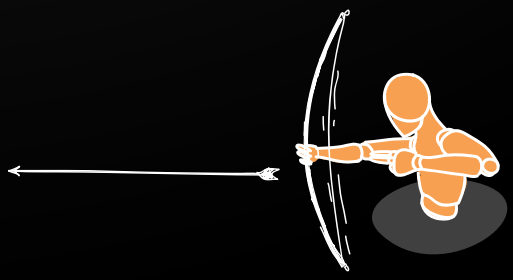
- Ethical Hacking
- Network Pentest
- Bug Bounty
- Wireless Pentest
- Network Security Essentials



ADVANCED

- Burp Suite Pro
- Android Pentest
- Web Services-API
- Advanced Metasploit
- Pro Infrastructure VAPT
- CTF
- Computer Forensics

EXPERT



- Red Team Operation
  - APT's - MITRE Attack Tactics
  - Active Directory Attack
  - MSSQL Security Assessment
- Privilege Escalation
  - Windows
  - Linux