

AWS



PENETRATION TESTING LAB SETUP

www.hackingarticles.in



Contents

Introduction	3
Prerequisites	3
Part 1: Setting up the Vulnerable Web Server (Ubuntu EC2 Instance)	3
Step 1: Sign in to AWS	3
Step 2: Navigate to EC2 Dashboard.....	5
Step 3: Launch a New EC2 Instance	5
Step 4: Configure Instance Details	7
Step 5: Connect to the Ubuntu Instance via SSH	9
Step 6: Configure Security Group for Web Access	11
Step 7: Deploy the SSRF Vulnerability Lab	12
Step 8: Create and Attach an IAM Role to the Instance	13
Part 2: Setting up the Attacker Machine (Kali Linux EC2 Instance)	16
Step 1: Launch a New EC2 Instance (for Kali).....	16
Step 2: Verify Kali Linux Instance State and Security Group	23
Step 3: Start the Ubuntu Web Server Instance (if stopped).....	24
Step 4: Test Connectivity from Kali Linux	26





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"**.

IAM user sign in ⓘ

Account ID or alias [\(Don't have?\)](#)

☐ Remember this account

IAM username

Password

☐ Show Password [Having trouble?](#)

Sign in

[Sign in using root user email](#)

[Create a new AWS account](#)

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



☒ **Root user**
Account owner that performs tasks requiring unrestricted access. [Learn more](#)

☐ **IAM user**
User within an account that performs daily tasks. [Learn more](#)

Root user email address

@gmail.com

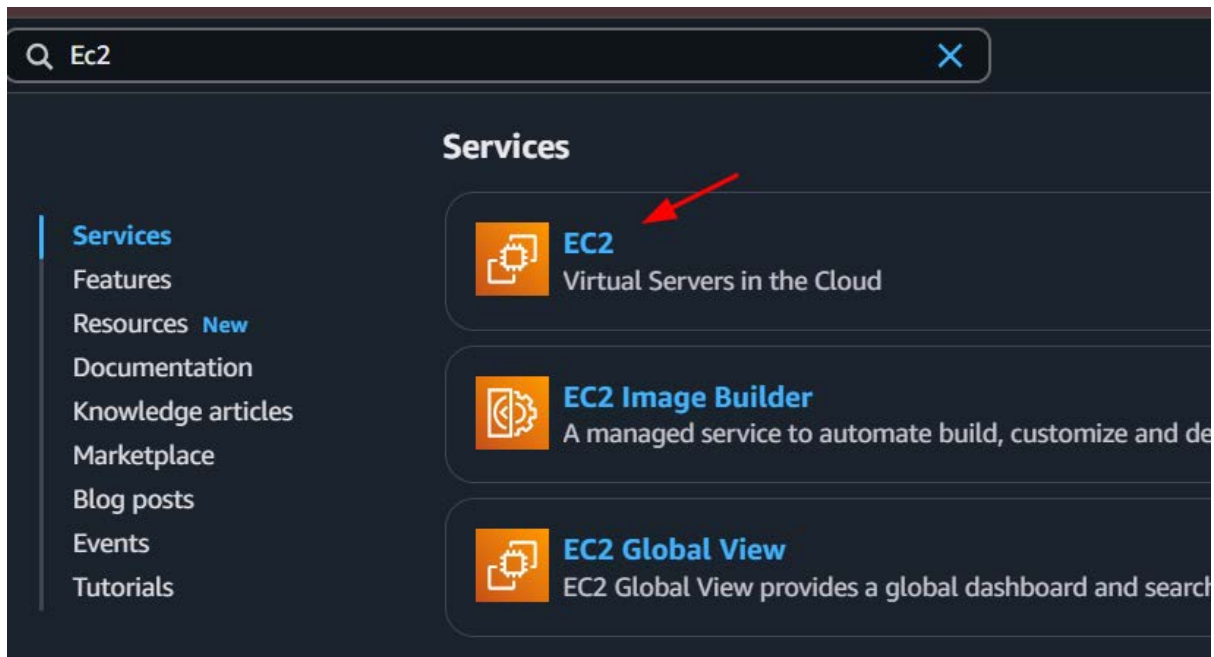
Next

- Follow the prompts to complete the login process.

Step 2: Navigate to EC2 Dashboard

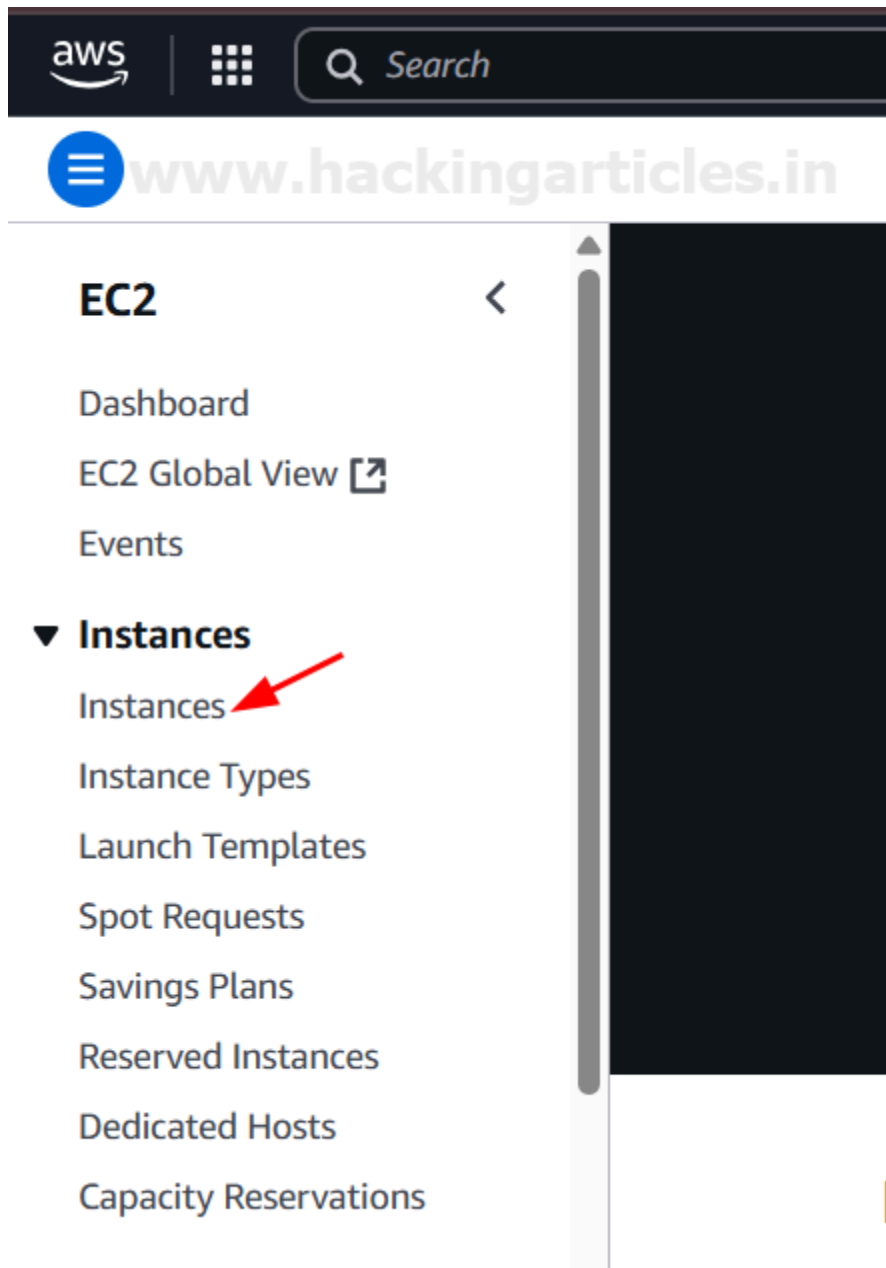
Once logged in, use the search bar at the top of the console.

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

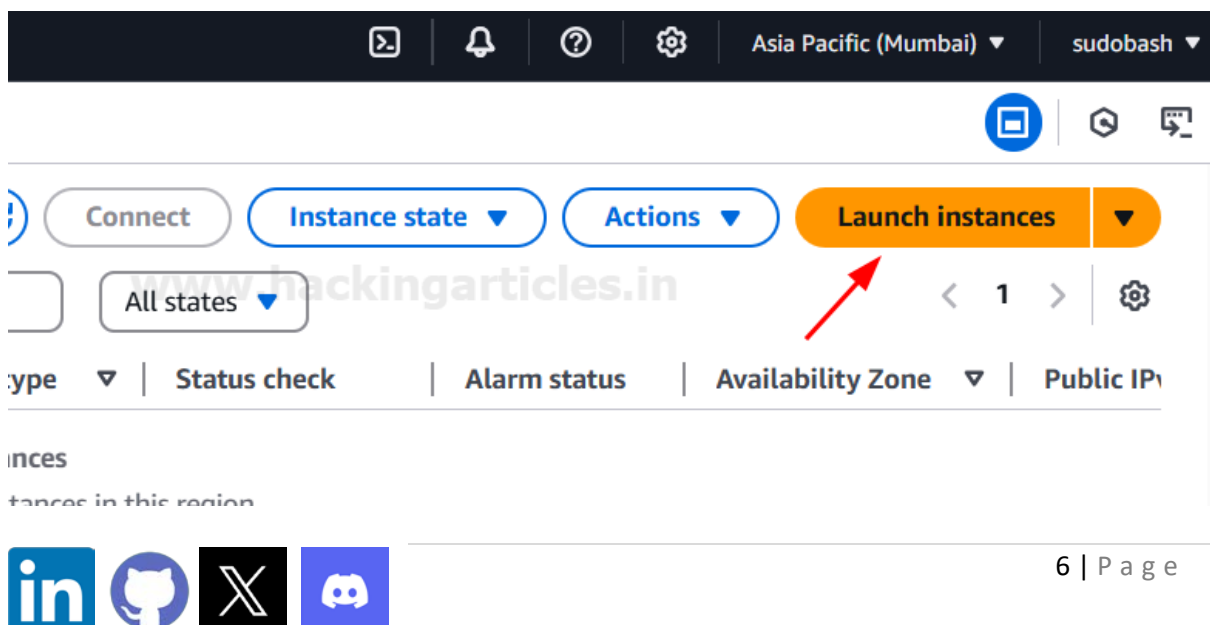


Step 3: Launch a New EC2 Instance

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.

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name

lgt_web1

Add additional tags

Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Quick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

SUSE Linux

SUSE

Debian

debian

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type
ami-0e35ddab05955cf57 (64-bit (x86)) / ami-0429d68a1cd41ca80 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Instance type & Key pair (login):

- Click "Create new key pair".

Instance type [Info](#) [Get advice](#)

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory Current generation: true On-Demand Linux base pricing: 0.0124 USD per Hour On-Demand Windows base pricing: 0.017 USD per Hour On-Demand RHEL base pricing: 0.0268 USD per Hour On-Demand Ubuntu Pro base pricing: 0.0142 USD per Hour On-Demand SUSE base pricing: 0.0124 USD per Hour

Free tier eligible

All generations

Compare instance types

Additional costs apply for AMIs with pre-installed software

Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

Select

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.**

Create key pair



Key pair name

Key pairs allow you to connect to your instance securely.

igt_web1

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type



☒ **RSA**
RSA encrypted private and public key pair

☐ **ED25519**
ED25519 encrypted private and public key pair

Private key file format

☒ **.pem**
For use with OpenSSH

☐ **.ppk**
For use with PuTTY

 When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#) 

Cancel

Create key pair

Review and Launch:

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

▼ Summary

Number of instances | [Info](#)

1

Software Image (AMI)
Canonical, Ubuntu, 24.04, amd64...[read more](#)
ami-0e35ddab05955cf57

Virtual server type (instance type)
t2.micro

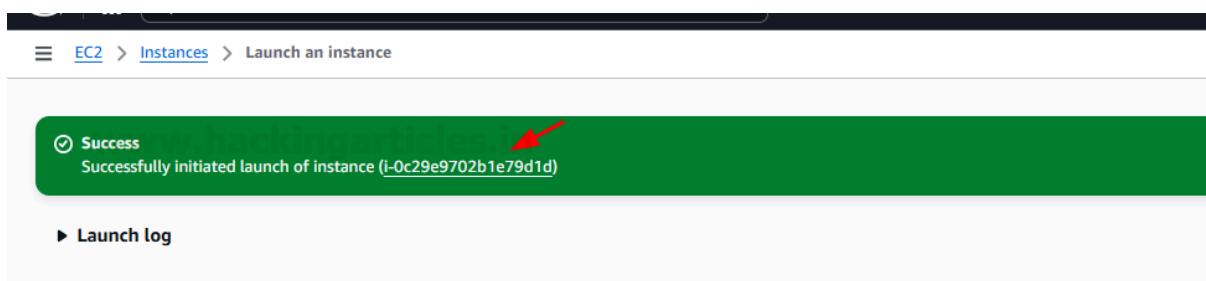
Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

[Cancel](#)[Launch instance](#)[Preview code](#)

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.



Connect to instance Info

Connect to your instance i-0c29e9702b1e79d1d (lgt_web1) using any of these options

EC2 Instance Connect Session Manager **SSH client** EC2 serial console

Instance ID
i-0c29e9702b1e79d1d (lgt_web1)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is lgt_web1.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
chmod 400 "lgt_web1.pem"
4. Connect to your instance using its Public DNS:
ec2-15-207-54-67.ap-south-1.compute.amazonaws.com

Example:

```
ssh -i "lgt_web1.pem" ubuntu@ec2-15-207-54-67.ap-south-1.compute.amazonaws.com
```

Note: In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

- 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>`.

```
PS C:\Users\raj\Desktop\aws> ssh -i lgt_web1.pem ubuntu@15.207.54.67
The authenticity of host '15.207.54.67 (15.207.54.67)' can't be established.
ED25519 key fingerprint is SHA256:YqFsvVVzNjHukCXdp0BjoB2ShjQfD5llwt/Y3iUhB8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '15.207.54.67' (ED25519) to the list of known hosts.
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-1024-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Thu May  8 16:50:26 UTC 2025

System load:  0.22           Processes:            107
Usage of /:   25.0% of 6.71GB Users logged in:          0
Memory usage: 20%           IPv4 address for enX0: 172.31.12.50
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-12-50:~$
```

- 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.

Successfully initiated rebooting of i-0c29e9702b1e79d1d

Instances (1/1) Info Last updated 10 minutes ago

Find Instance by attribute or tag (case-sensitive) All states

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
lgt_web1	i-0c29e9702b1e79d1d	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1b

i-0c29e9702b1e79d1d (lgt_web1)

IAM Role: -

Owner ID: 513869214449

Security groups

- sg-015fb41564bd936cd (launch-wizard-1)

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

Inbound rules (1) Manage tags Edit inbound rules

Search

Name	Security group rule ID	IP version	Type	Protocol	Port range
-	sgr-0f1a9647f67ac518e	IPv4	SSH	TCP	22

- 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**".



Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Security group rule ID	Type	Protocol	Port range	Source	Description - optional	Actions
sgr-Of1a9647f67ac518e	SSH	TCP	22	Cu...		Delete
-	All TCP	TCP	0 - 6553	An...	0.0.0.0/0	Delete
-	All UDP	UDP	0 - 6553	An...	0.0.0.0/0	Delete

[Add rule](#)

[Cancel](#) [Preview changes](#) [Save rules](#)

Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Step 7: Deploy the SSRF Vulnerability Lab

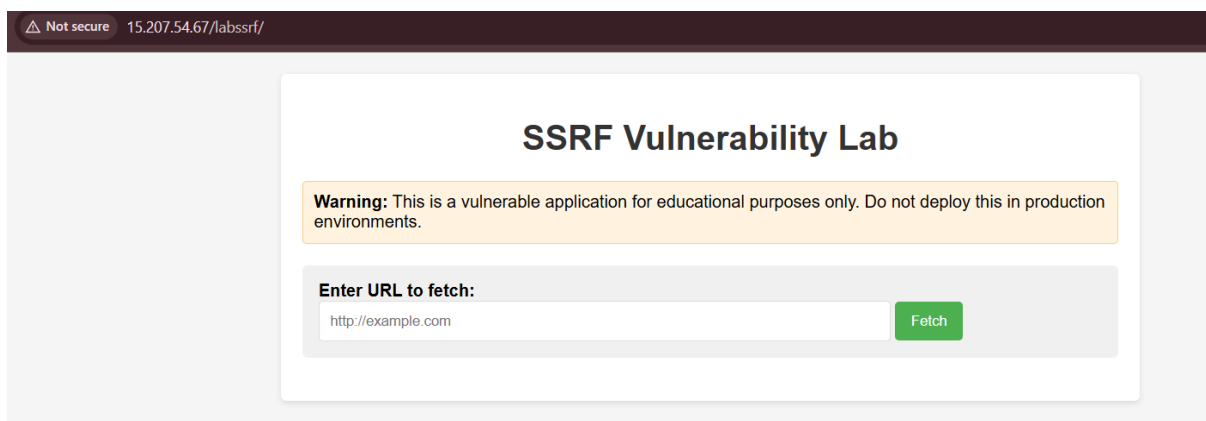
Once connected to your Ubuntu instance via SSH:

- 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).

```
root@ip-172-31-12-50:/var/www/html/labssrf# ls
index.php
root@ip-172-31-12-50:/var/www/html/labssrf#
```

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/`.

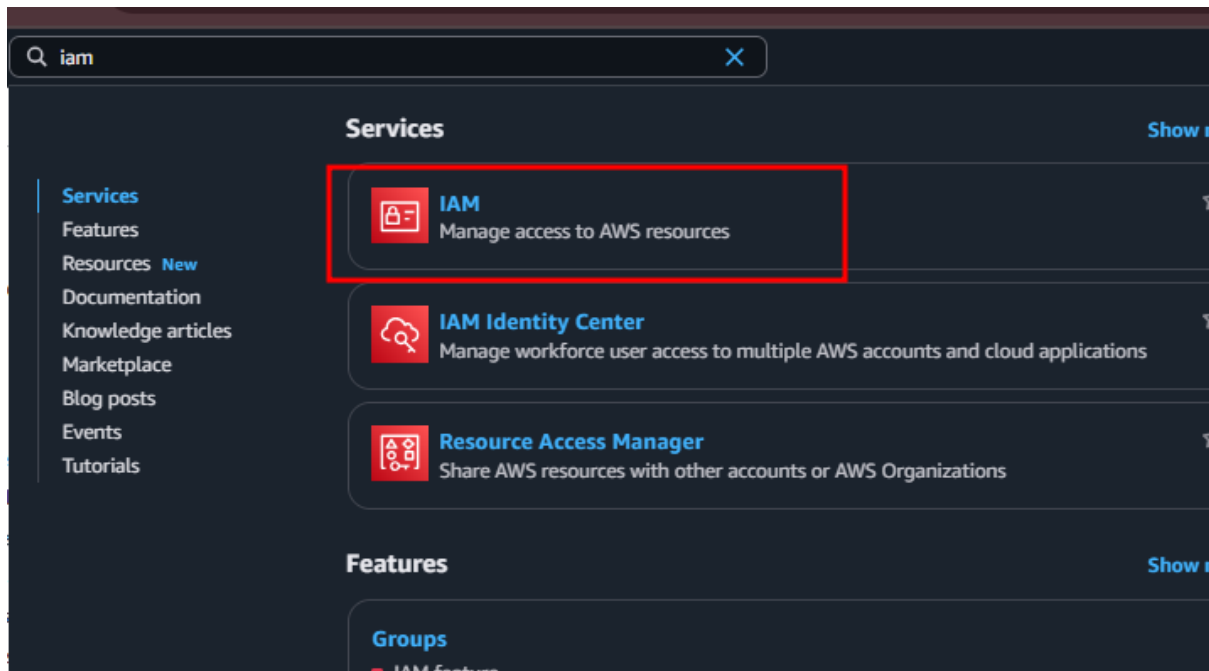


Step 8: Create and Attach an IAM Role to the Instance

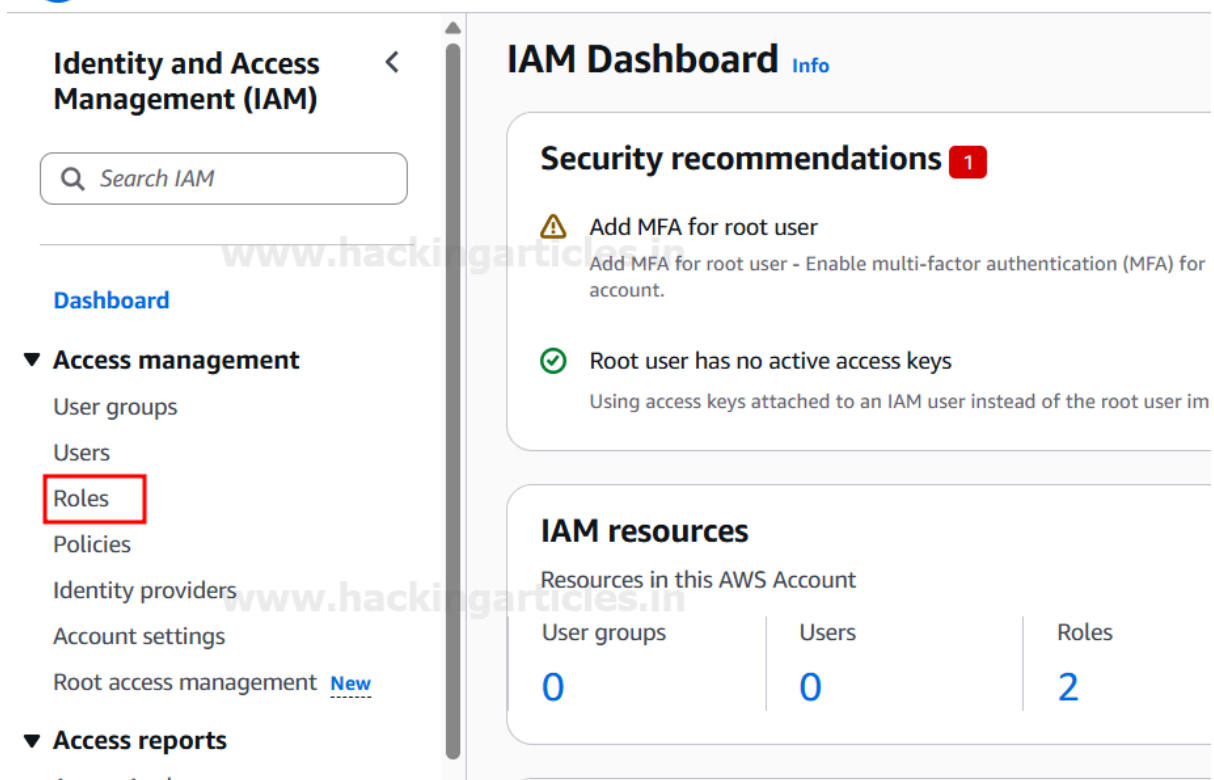
This step assigns an IAM role with specific permissions to your EC2 instance, which is crucial for certain types of attacks (like privilege escalation via EC2 metadata).

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".

Trusted entity type

☒ **AWS service**
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

☐ **AWS account**
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ **Web identity**
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

☐ **SAML 2.0 federation**
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

☐ **Custom trust policy**
Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

EC2

Choose a use case for the specified service.

Use case

☒ **EC2**
Allows EC2 instances to call AWS services on your behalf.

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

Permissions policies (1/1045) [Info](#)

Choose one or more policies to attach to your new role.

Filter by Type

All types

 1 match

<input checked="" type="checkbox"/>	Policy name	Type
<input checked="" type="checkbox"/>	AmazonEC2FullAccess	AWS managed

► Set permissions boundary - optional

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



Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.

Maximum 64 characters. Use alphanumeric and '+', '@', '_' characters.

Description
Add a short explanation for this role.

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: '_', '+', '@', '/', '[', ']', '#', '\$', '%', '^', '&', '=', '<', '>', '"', ''', '4', ':', '@', 'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z', '[', '\', ']', '^', '_', '`', 'a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z', '{', '|', '}', '~', '', '€', '', '‚', 'ƒ', '„', '…', '†', '‡', 'ˆ', '‰', 'Š', '‹', 'Œ', '', 'Ž', '', '', '‘', '’', '“', '”', '•', '–', '—', '˜', '™', 'š', '›', 'œ', '', 'ž', 'Ÿ', ' ', '¡', '¢', '£', '¤', '¥', '¦', '§', '¨', '©', 'ª', '«', '¬', '­', '®', '¯', '°', '±', '²', '³', '´', 'µ', '¶', '·', '¸', '¹', 'º', '»', '¼', '½', '¾', '¿', 'À', 'Á', 'Â', 'Ã', 'Ä', 'Å', 'Æ', 'Ç', 'È', 'É', 'Ê', 'Ë', 'Ì', 'Í', 'Î', 'Ï', 'Ð', 'Ñ', 'Ò', 'Ó', 'Ô', 'Õ', 'Ö', '×', 'Ø', 'Ù', 'Ú', 'Û', 'Ü', 'Ý', 'Þ', 'ß', 'à', 'á', 'â', 'ã', 'ä', 'å', 'æ', 'ç', 'è', 'é', 'ê', 'ë', 'ì', 'í', 'î', 'ï', 'ð', 'ñ', 'ò', 'ó', 'ô', 'õ', 'ö', '÷', 'ø', 'ù', 'ú', 'û', 'ü', 'ý', 'þ', 'ÿ'.

Step 1: Select trusted entities Edit

Trust policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "sts:AssumeRole"
8       ],
9       "Principal": {
10        "Service": [
11          "ec2.amazonaws.com"
12        ]
13      }
14    ]
15  }
16 }
```

Step 2: Add permissions Edit

Permissions policy summary

Policy name	Type	Attached as
AmazonEC2FullAccess	AWS managed	Permissions policy

Step 3: Add tags

Add tags - optional [Info](#)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

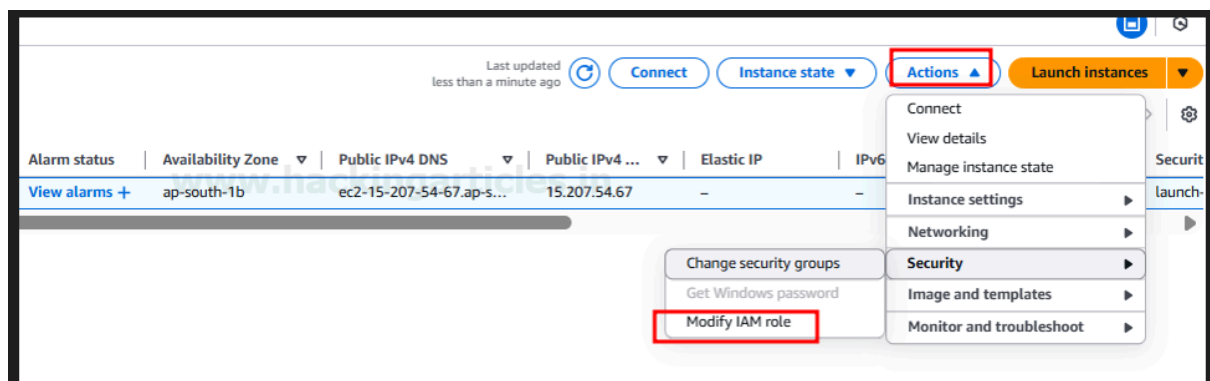
[Add new tag](#)

You can add up to 50 more tags.

Cancel Previous 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".



Modify IAM role [Info](#)

Attach an IAM role to your instance.

Instance ID
i-0c29e9702b1e79d1d (lgt_web1)

IAM role
Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

Ec2_role

[Create new IAM role](#)

[Cancel](#) [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".

Modify instance metadata options

IMDSv2 uses session-oriented requests. With session-oriented requests, you create a session token that defines the session duration, which can be a minimum of 1 second and a maximum of 6 hours. [Learn more](#)

Instance ID

i-0c29e9702b1e79d1d (lgt_web1)

Instance metadata service

☒ Enable

IMDSv2

☒ Optional

☐ Required

[Cancel](#)

[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.



EC2 > Instances > Launch an instance

It seems like you may be new to launching instances in EC2. Take a walkthrough to learn about EC2, how to launch instances and about best practices

[Do not show me this message again](#) [Take a walkthrough](#)

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name

[Add additional tags](#)

▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Recents **Quick Start**

Amazon Linux

macOS

Ubuntu

Windows

Red Hat

SUSE Linux

Debian

[Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

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

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name

[Add additional tags](#)

▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

AMI from catalog Recents Quick Start

Name

kali-last-snapshot-amd64-dev-manual-2025.05.01-804fcc46-63fc-4eb6-85a1-50e66d6c7215 Verified provider

Description

Kali Linux kali-last-snapshot (development build manual-2025.05.01)

Image ID

ami-035e3e24d11aa53ec

Username ⓘ

root

Catalog	Published	Architecture	Virtualization	Root device type	ENA Enabled
AWS Marketplace AMIs	2025-05-03T06:23:23.000Z	x86_64	hvm	ebs	Yes

If you have an existing license entitlement to use this software, then you can launch this software without creating a new subscription. If you do not have an existing entitlement, then by launching this software, you will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's [End User License Agreement](#)

[Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community



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

- Click "Browse more AMIs".

EC2 > Instances > Launch an instance

It seems like you may be new to launching instances in EC2. Take a walkthrough to learn about EC2, how to launch instances and about best practices

Do not show me this message again Take a walkthrough

Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Name
e.g. My Web Server Add additional tags

Application and OS Images (Amazon Machine Image)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Recents Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Linux Debian

Browse more AMIs
Including AMIs from AWS, Marketplace and the Community

- 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".

Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Selected AMI: ami-0af9569868786b23a (Quick Start AMIs)

Search: kali linux

Quick Start AMIs (0) My AMIs (0) **AWS Marketplace AMIs (18)** Community AMIs (500)

Commonly used AMIs Created by me AWS & trusted third-party AMIs Published by anyone

Refine results

Categories
Infrastructure
Software (18)
DevOps (8)
Industries (1)

Publisher
☐ Techlatest.net (6)
☐ Kali (2)
☐ Decyphertek (2)
☐ Askforcloud LLC (2)
☐ NUJYV (2)
☐ Cloud Infrastructure Services (1)
☐ Kurian (1)
☐ Galaxys Cloud (1)
☐ Nuvernest (1)

Pricing model
☐ Usage Based (14)
☐ Free (4)

kali linux (18 results) showing 1 - 18

Sort By: Relevance

Kali Linux
By Kali | Ver 2025.1c-amd64
★★★★★ 23 AWS reviews
Starting from \$0.00 to \$0.00/hr for software + AWS usage fees
Kali Linux (formerly known as BackTrack Linux) is an open-source, Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. It does this by providing common tools, configurations, and automations which allows the user to focus on the task that needs to be...

Kali Linux (ARM)
By Kali | Ver 2025.1c-arm64
Starting from \$0.00 to \$0.00/hr for software + AWS usage fees
Kali Linux (formerly known as BackTrack Linux) is an open-source, Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. It does this by providing common tools, configurations, and automations which allows the user to focus on the task that needs to be...



Kali Linux
Kali
★★★★★ 23 AWS reviews
Free Tier | Standard Contract

Overview | Product details | Pricing | Usage | Support

Kali Linux is an open-source, multi-platform distribution, aimed at advanced Penetration Testing and Security Auditing. Kali Linux provides several hundred common tools and industry specific modifications, targeted towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics, Reverse Engineering, Vulnerability Management and Red Team Testing.

Typical total price \$0.046/Hr Total pricing per instance for services hosted on t2.medium in us-east-1. See additional pricing information.	Latest version 2025.1c-amd64 Delivery methods Amazon Machine Image Operating systems Other 2025.1c Other 2025.1a Other 2024.4	Video Product Video Categories Operating Systems Security Testing
---	---	--

A subscription to this AMI is required before you can launch an instance. Check the pricing details in the pricing tab before continuing.
You can subscribe to this AMI now or we will automatically subscribe for you when you launch this instance. We recommend that you 'Subscribe now' if you are sure this is the AMI you want to use to launch as it will reduce wait time on launch. Choose 'Subscribe on instance launch' if you are still choosing an AMI and don't want to commit to a subscription yet. By subscribing to this AMI you agree that your use of this software is subject to the pricing terms and the seller's [End User License Agreement](#) .

[Cancel](#) [Subscribe on instance launch](#) [Subscribe now](#)

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.



Create key pair

Key pair name

Key pairs allow you to connect to your instance securely.

kali_key

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

☒ RSA
RSA encrypted private and public key pair

☐ ED25519
ED25519 encrypted private and public key pair

Private key file format

☒ .pem
For use with OpenSSH

☐ .ppk
For use with PuTTY

⚠ When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. [Learn more](#)

Cancel

Create key pair

Network settings:

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

▼ Network settings [Info](#)

Network [Info](#)

vpc-06529505139f177ce

Subnet [Info](#)

No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group

☐ Select existing security group

We'll create a new security group called 'Kali Linux-2025.1c-amd64-AutogenByAWSMP--1' with the following rules:

☒ Allow SSH traffic from
Recommended rule from AMI

Anywhere
0.0.0.0/0

☐ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

☐ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Edit



- 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.

▼ Network settings Info

VPC - required Info

vpc-06529505139f177ce (default) 172.31.0.0/16

Subnet Info

No preference

Create new subnet

Auto-assign public IP Info

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group ☐ Select existing security group

Security group name - required

Kali Linux-2025.1c-amd64-AutogenByAWSMP--1

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _-:/()#,@[]+=&{}!\$*

Description - required Info

Kali Linux-2025.1c-amd64-AutogenByAWSMP--1 created 2025-05-14T17:21:33.309Z

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0) Remove

Type Info <div>ssh</div>	Protocol Info <div>TCP</div>	Port range Info <div>22</div>
Source type Info <div>Anywhere</div>	Source Info <div>Add CIDR, prefix list or security group 0.0.0.0/0</div>	Description - optional Info <div>e.g. SSH for admin desktop</div>

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Add security group rule



▼ Security group rule 2 (TCP; 0-65535, 0.0.0.0/0) [Remove](#)

Type Info	Protocol Info	Port range Info
All TCP 	TCP	0-65535
Source type Info	Source Info	Description - optional Info
Anywhere 	<input type="text" value="0.0.0.0/0"/> 	<input type="text" value="e.g. SSH for admin desktop"/>

▼ Security group rule 3 (UDP; 0-65535, 0.0.0.0/0) [Remove](#)

Type Info	Protocol Info	Port range Info
All UDP 	UDP	0-65535
Source type Info	Source Info	Description - optional Info
Anywhere 	<input type="text" value="0.0.0.0/0"/> 	<input type="text" value="e.g. SSH for admin desktop"/>

Review and Launch:

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



▼ Summary

Number of instances [Info](#)

1

Software Image (AMI)
Kali Linux
ami-035e3e24d11aa53ec

Virtual server type (instance type)
t2.medium

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 12 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

[Cancel](#) [Launch instance](#) [Preview code](#)

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.

Instances (2) [Info](#)

Last updated less than a minute ago [Connect](#) [In](#)

Find Instance by attribute or tag (case-sensitive) [All states](#)

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic I
<input type="checkbox"/>	Kali linux	i-04bfb1a6287f5801d	Running	t2.medium	Initializing	View alarms +	ap-south-1a	ec2-13-201-67-198.ap...	13.201.67.198	-
<input type="checkbox"/>	lgt_web1	i-0c29e9702b1e79d1d	Stopped	t2.micro	-	View alarms +	ap-south-1b	-	-	-

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



Instance summary for i-04bfb1a6287f5801d (Kali linux)

Updated 1 minute ago

Instance ID: i-04bfb1a6287f5801d

IPv6 address: --

Hostname type: IP name: ip-172-31-45-122.ap-south-1.compute.internal

Answer private resource DNS name: IPv4 (A)

Auto-assigned IP address: 13.201.67.198 [Public IP]

IAM Role: --

IMDSv2: Optional
EC2 recommends setting IMDSv2 to required | Learn more

Operator: --

Public IPv4 address: 13.201.67.198 | open address

Instance state: **Running**

Private IP DNS name (IPv4 only): ip-172-31-45-122.ap-south-1.compute.internal

Instance type: t2.medium

VPC ID: vpc-06529505139f177ce

Subnet ID: subnet-0d29f0b74a094900b

Instance ARN: arn:aws:ec2:ap-south-1:513869214449:instance/i-04bfb1a6287f5801d

Private IPv4 addresses: 172.31.45.122

Public IPv4 DNS: ec2-13-201-67-198.ap-south-1.compute.amazonaws.com | open address

Elastic IP addresses: --

AWS Compute Optimizer finding: Opt-in to AWS Compute Optimizer for recommendations. | Learn more

Auto Scaling Group name: --

Managed: false

Details | Status and alarms | Monitoring | **Security** | Networking | Storage | Tags

▼ Security details

IAM Role: --

Owner ID: 513869214449

Launch time: Wed May 14 2025 23:01:06 GMT+05:30 (India Standard Time)

Security groups: sg-0fe14f25b4b3aacb6 (Kali Linux-2025.1c-amd64-AutogenByAWSMP--1)

▼ Inbound rules

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

sg-0fe14f25b4b3aacb6 - Kali Linux-2025.1c-amd64-AutogenByAWSMP--1

Details

Security group name: Kali Linux-2025.1c-amd64-AutogenByAWSMP--1

Security group ID: sg-0fe14f25b4b3aacb6

Description: Kali Linux-2025.1c-amd64-AutogenByAWSMP--1 created 2025-05-14T17:21:33.309Z

VPC ID: vpc-06529505139f177ce

Owner: 513869214449

Inbound rules count: 3 Permission entries

Outbound rules count: 1 Permission entry

Inbound rules | Outbound rules | Sharing - new | VPC associations - new | Tags

Inbound rules (3)

Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
-	sg-06677eb4e0b0b19fe	IPv4	All TCP	TCP	0 - 65535	0.0.0.0/0	-
-	sg-024014eae106400bd	IPv4	SSH	TCP	22	0.0.0.0/0	-
-	sg-0dbe7925610199f82	IPv4	All UDP	UDP	0 - 65535	0.0.0.0/0	-

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

Edit inbound rules

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules

Security group rule ID	Type	Protocol	Port range	Source	Description - optional	Actions
sg-06677eb4e0b0b19fe	All TCP	TCP	0 - 65535	Custom	0.0.0.0/0	Delete
sg-024014eae106400bd	SSH	TCP	22	Custom	0.0.0.0/0	Delete
sg-0dbe7925610199f82	All UDP	UDP	0 - 65535	Custom	0.0.0.0/0	Delete
-	All ICMP - IPv4	ICMP	All	Anywhere...	0.0.0.0/0	Delete

Add rule

Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel | Preview changes | **Save rules**

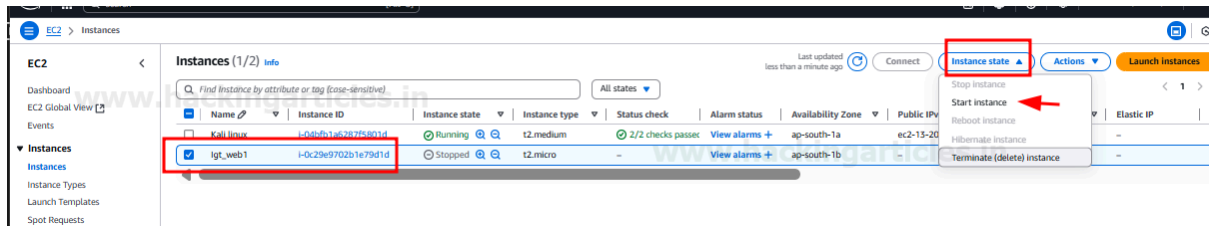
Step 3: Start the Ubuntu Web Server Instance (if stopped)

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

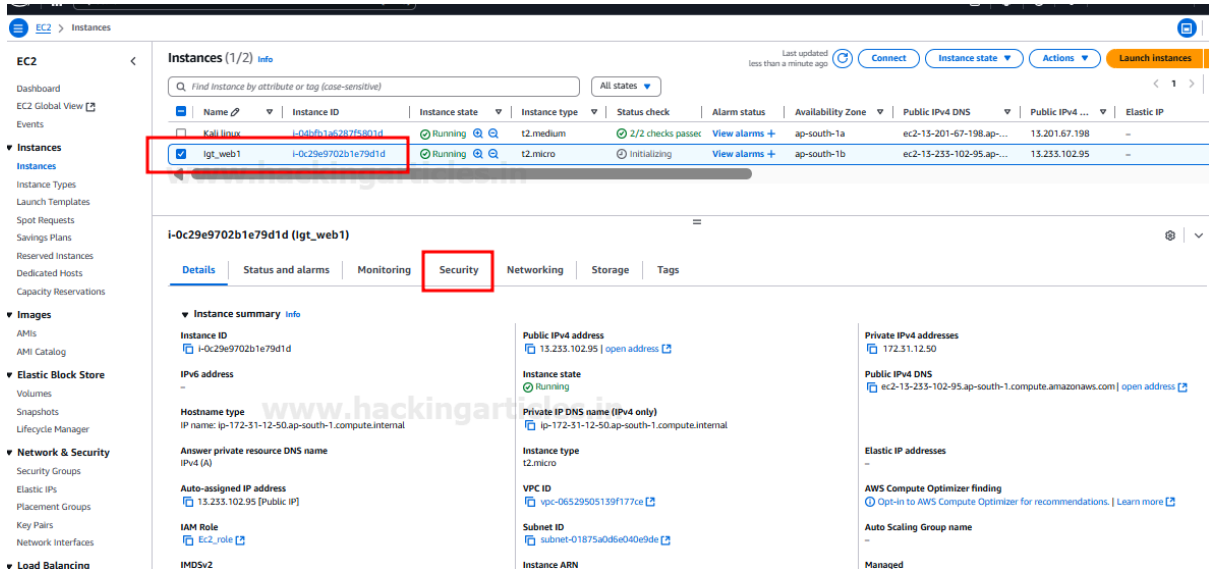




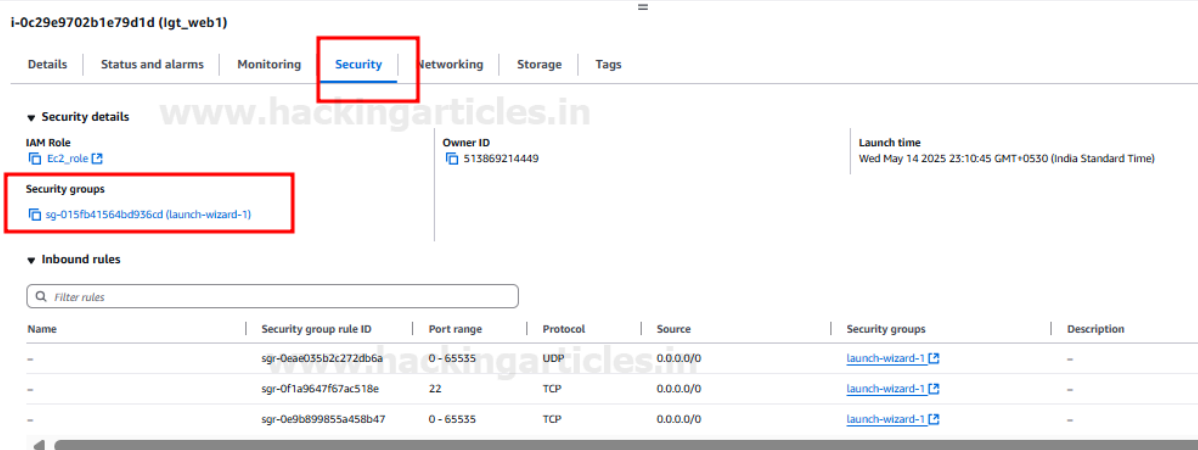
- Firstly, select lgt_web1 from the EC2 Instances page.
- Then, click "Instance state" -> "Start instance".



- Verify the instance is running.



- Ensure its security group has the necessary rules.



Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Security group rule ID	Type	Protocol	Port range	Source	Description - optional	Actions
sg-0eae035b2c272db6a	All UDP	UDP	0 - 65535	Custom	Q	Delete
sg-0f1a9647f67ac518e	SSH	TCP	22	Custom	Q	Delete
sg-0e9b899855a458b47	All TCP	TCP	0 - 65535	Custom	Q	Delete
-	All ICMP - IPv4	ICMP	All	Anywhere...	Q	Delete

Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel Preview changes Save 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).
 - o 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)-[~]
```

- o 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](#).

JOIN OUR TRAINING PROGRAMS

